UNIVERSITAT DE BARCELONA

Contribución al estudio de las extensiones galoisianas de grupo diedral

Griselda Pascual Xufré

UNIVERSIDAD DE BARCELONA FACULTAD DE MATEMATICAS

CONTRIBUCION AL ESTUDIO DE LAS EXTENSIONES GALOISIANAS DE GRUPO DIEDRAL.

Memoria presentada por
Griselda Pascual Xufré
para aspirar al grado
de Doctor.
Diciembre 1974.

ÍNDICE

I N T R O D U C C I O N

En 1894, Dedekind en su obra "Uber die Theorie der ganzen algebraischen Zahlen", demuestra que el anillo A de los enteros de un cuerpo K de números es un Z-módulo libre. Por otra parte se sabe, que si K es galoisiana sobre Q, K posee una base normal sobre Q, es decir, es Q[G]-libre. Se presenta entonces la cuestión de si en este caso también A es Z[G]-libre de rango uno, es decir , de la existencia de una base normal de A sobre Z.

En 1897, Hilbert demuestra que si K es una extensión galoisiana y abeliana de Q, y el grado de K sobre Q es primo con el discriminante de K sobre Q, entonces A posee una Z-base normal.

En 1916, Speiser considera un cuerpo de números K, extensión galoisiana finita de un cuerpo de números F, y demuestra que si el anillo de los enteros B de K posee una base normal sobre el anillo de los enteros A de F, entonces K es moderadamente ramificada sobre F.

Emmy Nöether, en 1931, [14] observa que esta propiedad es válida en el caso local, y da para este caso una condición suficiente, es decir, demuestra el siguiente teorema: "Para cada

primo $\mathfrak{p}$, tal que $\mathfrak{p}$ no divide al grado de K sobre F, existe una base normal local", y además, "Si K es moderadamente ramificada sobre F, existe una base normal local para todo primo de F",

El teorema de Nöether se generaliza para un anillo A de Dedekind semi-local cualquiera, de la manera siguiente: [12], "Si A es un anillo de Dedekind semi-local, K su cuerpo de fracciones, L una extensión galoisiana finita de K, moderadamente ramificada, B la clausura entera de A en L; si la característica de K no divide al orden del grupo de Galois G(L/K), B es un $A[G]$-módulo libre.

Si el anillo A no es semi-local - que es precisamente el caso de Z, y por tanto de un cuerpo de números - la cuestión se presenta mucho más dificil, y en general no está resuelta. En el caso de ser el grupo de Galois G abeliano, y K un cuerpo de números, se puede utilizar el teorema de Kronecker-Weber, según el cual, ([2] C.8 § 2 T.6) cada extensión abeliana finita del cuerpo Q de los racionales es un cuerpo ciclotómico, es decir es un subcuerpo de un cuerpo $Q(\zeta)$, donde ζ es una raiz primitiva de la unidad, ya que la estructura del anillo de los enteros de estos cuerpos es completamente conocida.

Sin embargo, Leopoldt en 1959, [9] hace notar que este método conduce a cálculos muy complicados y a una extensa casuis-

tica, y haciendo uso de los caracteres del grupo de Galois de la extensión, da un teorema general de estructura del anillo A de los enteros de un cuerpo de números K como Z[G]-módulo, cuando K es galoisiana y abeliana sobre Q y su grupo de Galois es G. Demuestra que A posee una base normal sobre Z si y sólo si K es moderadamente ramificada sobre Q.

En 1962, Fröhlich [7] estudia el caso de las extensiones de Kummer sobre dominios de Dedekind y da condiciones necesarias y suficientes para la existencia de base normal comparando el método que él utiliza con el de Leopoldt, haciendo notar que la ventaja de que él goza es la de que el cuerpo base posee tantas raices de la unidad como le sean necesarias, pero sin embargo tiene el inconveniente de partir de un anillo que no es principal. Además resalta también el hecho de no poseer en su caso un teorema de inmersión análogo al de Kronecker-Weber.

Siguiendo en la línea de las extensiones K de Q finitas galoisianas y abelianas, Ullom en 1969 [18], considera los ideales de K que son G-módulos, siendo G el grupo de Galois de K sobre Q, a los que denomina ideales ambiguos, estudia la existencia de bases normales para los mismos dando una condición suficiente cuando la extensión es moderadamente ramificada.

Pasando ahora a extensiones galoisianas no abelianas, se

encuentra en 1968 un trabajo de Martinet-Payan [11] que estudia las bases del anillo de los enteros de las extensiones galoisianas y no abelianas de los racionales, basado en otro trabajo anterior de los mismos autores , 1967, [10] sobre las extensiones cúbicas no galoisianas de los racionales y su clausura galoisiana.

En 1969, Martinet [12] generaliza este estudio al caso de extensiones galoisianas de grupo de Galois diedral de orden 2p p primo impar, y demuestra los siguientes teoremas:

1) " Sea A un anillo principal, $\mathcal{K}$ su cuerpo de fracciones; se supone que la característica de $\mathcal{K}$ no divide 2p y que A/pA es un cuerpo que posee p elementos. Si N es una extensión de de grado 2p, galoisiana, no abeliana , de grupo de Galois G , K un subcuerpo de grado p de N, k el subcuerpo cuadrático de N, A_k , A_K , A_N las clausuras enteras de A en k, K, N respectivamente. Entonces, si A_K y A_k poseen A-bases normales, A_N es A[G]-libre".

2) " Sea N una extensión galoisiana, no abeliana, de grado 2p del cuerpo Q de los racionales, G su grupo de Galois, Z el anillo de los enteros racionales, S una parte multiplicativa de Z que no contiene el cero, A el subanillo $S^{-1}Z$ de Q, B la clausura entera de A en N. Se supone que N es moderadamente ramificada sobre Q. Entonces B es un A[G]-módulo libre".

Es decir, en particular demuestra que si N es una extensión de Q, galoisiana de grupo de Galois diedral de orden 2p (p primo impar) moderadamente ramificada, entonces el anillo de los enteros de N posee una Z-base normal.

Todo lo dicho hasta aquí, parece que induce a pensar, que siempre que N fuera moderadamente ramificada sobre Q, podría probarse la existencia de una base normal sobre Z del anillo de los enteros de N, sin embargo, Martinet en 1971 ,[13], da un contraejemplo en el caso de las extensiones cuaternionianas.

En esta memoria, nos proponemos dar alguna contribución al estudio de la aritmética de las extensiones de cuerpos de números, galoisianas, no abelianas, cuyo grupo de Galois G sea de uno de los tipos siguientes: diedral de orden $2p^n$ (p primo impar), diedral de orden 2pq (p,q primos impares).

En el primer capítulo se considera un tipo especial de ideales llamados invariantes, y que coinciden con los que Ullom llama ambiguos, en el caso de extensiones de Q diedrales de orden 2p, y se da una condición suficiente de existencia de bases normales para dichos ideales. El capítulo segundo está destinado al estudio de ramificaciones y cálculo de discriminantes en el caso $2p^n$. En los capítulos tercero y cuarto se estudia el anillo de los enteros A_N de la extensión N, considerado como $A[G]$-módulo, siendo A el anillo de Dedekind sobre cuyo cuer-

po de fracciones $\mathcal{X}$ se construye la extensión N de grupo de Galois G de orden $2p^n$ y se dan algunas condiciones suficientes para que A_N sea $A[G]$-módulo libre. En el capítulo quinto se estudia la ramificación y se calculan discriminantes en el caso de una extensión diedral de orden 2pq, y se dan condiciones suficientes para que A_N sea $A[G]$-proyectivo.

Finalmente, quiero manifestar mi gratitud a todos cuantos me han ayudado en la confección de esta memoria. A D. Enrique Linés en primer lugar, por ser quien me introdujo en el estudio de la Teoría de Números y haber aceptado el dirigirmela; a D. Rafael Mallol, Jefe del Departamento de Algebra de esta Facultad, y a D. Tomás Montull , Director del Instituto Maragall, por haberme brindado la posibilidad de trabajo; y de una manera muy especial a Dª. Pilar Bayer, por el ánimo que me ha dado y las acertadas observaciones que me ha hecho durante la redacción de la misma.

C A P I T U L O I

BASES NORMALES PARA IDEALES INVARIANTES

INTRODUCCION.- En este capítulo se consideran en primer lugar cuerpos K de números, extensiones galoisianas de Q de grupo de Galois G diedral de orden 2p (p primo impar), y se da una condición de existencia de bases normales para los ideales invariantes de K, que son los que son G-módulos. Puesto que se impone la condición de que K ha de ser moderadamente ramificada sobre Q, se estudian a continuación algunos casos en los que dicha condición se cumple. Finalmente se considera la existencia de bases normales para los ideales invariantes cuando el cuerpo base es un cuerpo Q_p completo respecto a una valoración discreta y la extensión es también galoisiana de grupo de Galois diedral de orden 2p (p primo impar).

Para facilitar la lectura, se dan al principio sin demostración, las propiedades y definiciones más importantes que se utilizarán a lo largo del capítulo, ya conocidas.

1. PROPIEDADES GENERALES

Definición (1.1) . Un anillo de Dedekind es un anillo A conmutativo, noetheriano, con elemento unidad, enteramente cerrado y en el que todo ideal primo no nulo es maximal.

Proposición (1.2). Si A es de Dedekind, la clausura entera B de A en cualquier extensión finita L de su cuerpo de fracciones $\mathcal{K}$, es también de Dedekind.

Demostración: [5] c.7 § 2, Cor.3 a Prop. 5.

Proposición (1.3) . Con las notaciones de (1.2) y L separable sobre $\mathcal{K}$, B es un A-módulo de tipo finito.

Con la hipótesis de separable, se puede aplicar [17] C.I § 4, Prop. 8.

Definición (1.4) . Para cada ideal primo nó nulo $\mathfrak{p}$ de A, el ideal $\mathfrak{p}B$ se escribe de manera única en la forma:

$$\mathfrak{p}B = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}}} \qquad \mathfrak{P} \text{ primo}$$

El entero $e_{\mathfrak{P}}$ se denomina índice de ramificación de $\mathfrak{P}$ en la extensión $L|\mathcal{K}$.

El cuerpo $B/\mathfrak{P}$ es una extensión de grado finito de $A/\mathfrak{p}$. El grado de esta extensión se denomina grado residual de $\mathfrak{P}$ en la extensión $L|\mathcal{K}$, y se indica por $f_{\mathfrak{P}} = \left[B/\mathfrak{P} : A/\mathfrak{p}\right]$.

Definición (1.5) . [6] . a)) Se dice que $L|\mathcal{K}$ es totalmente ramificada en un primo $\mathfrak{p}$ de A si hay un sólo primo $\mathfrak{P}$ de B que divide a $\mathfrak{p}$, y $f_{\mathfrak{P}}$ es igual a 1.

b)Se dice que $L|\mathcal{K}$ es no ramificada en $\mathfrak{P}$ de B, si $e_{\mathfrak{P}} = 1$, y $B/\mathfrak{P}$ es separable sobre $A/\mathfrak{p}$. Si $L|\mathcal{K}$ es no ramificada para todos los primos $\mathfrak{P}$ que dividen a $\mathfrak{p}$, se dice que es no ramificada en $\mathfrak{p}$.

c) Se dice que $L|\varkappa$ es moderadamente ramificada en $\mathfrak{P}$, si $B/\mathfrak{P}$ es separable sobre $A/\mathfrak{p}$ y la característica de $A/\mathfrak{p}$ no divide a $e_{\mathfrak{P}}$. La extensión $L|\varkappa$ se dice que es moderadamente ramificada, si lo es en todo ideal primo no nulo de B.

Proposición (1.6). Si $L|\varkappa$ es galoisiana, $\mathfrak{p}$ es un ideal primo de A y $\mathfrak{P}$ es un ideal primo de B que divide a $\mathfrak{p}$, los enteros $e_{\mathfrak{P}}$, $f_{\mathfrak{P}}$ dependen sólo de $\mathfrak{p}$, y si se designan por $e_{\mathfrak{p}}$ y $f_{\mathfrak{p}}$, se tiene:

$$n = e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}}$$

donde n es el grado de L sobre $\varkappa$, y $g_{\mathfrak{p}}$ el número de primos de B que dividen a $\mathfrak{p}$.

Demostración: [17] C.I § 7 Cor a Prop.19.

2. NOTACIONES Y DEFINICIONES.

Sea K una extensión galoisiana de Q de grupo de Galois G(K|Q) diedral de orden 2p, (p primo impar. Sea A_K el anillo de los enteros de K, es decir, la clausura entera de Z en K, q un primo de Z y $\mathfrak{Q}$ un ideal primo de A_K que divide a qA_K. Sean e y f el índice de ramificación y el grado residual respectivamente correspondientes a $\mathfrak{Q}$. Se tiene $2p = efg$, siendo g el número de ideales primos de A_K que dividen a qA_K. Se indican por k_K y F_q los cuerpos residuales de K y Q correspondientes a $\mathfrak{Q}$ y q respectivamente. Puesto que F_q es finito, se sabe que k_K es separable sobre F_q.

Definición (2.1) . Un ideal fraccionario $\mathcal{A}$ de K se denomina G-invariante, o simplemente invariante -cuando no hay lugar a confusión- si es un G-módulo, es decir si es estable frente a la acción de G.

Definición (2.2) . Un ideal invariante $\mathcal{A}$ de K se dice que posee una base normal sobre Z, si considerado como Z[G]-módulo, es isomorfo a Z[G]. Es decir, si existe un $\alpha \in \mathcal{A}$ tal que para cada $\beta \in \mathcal{A}$ es $\beta = \sum_{\sigma \in G} a_\sigma \sigma(\alpha)$ donde $a_\sigma \in Z$, únicos.

Definición (2.3) . Se dice que $\mathcal{A}$ considerado como Z[G]-módulo es Z[G]-debilmente proyectivo, si existe un Z-endomorfismo $\rho : \mathcal{A} \longrightarrow \mathcal{A}$ tal que $\sum_{\sigma \in G} \sigma \rho(\sigma^{-1}\alpha) = \alpha$ para todo $\alpha \in \mathcal{A}$.

3. TEOREMA DE EXISTENCIA.

Proposición (3.1). Si K es moderadamente ramificada sobre Q, cada ideal invariante $\mathcal{A}$ de K es Z[G]-debilmente proyectivo.

En efecto: Por ser K moderadamente ramificada sobre Q se tiene $Tr_{K/Q}(A_K) = Z$ por tanto, existe un $\beta \in A_K$ tal que $Tr_{K/Q}(\beta) = 1$. Sea ρ_β el Z-endomorfismo de $\mathcal{A}$ que consiste en multiplicar por β cada elemento de $\mathcal{A}$. Entonces

$$Tr_{K/Q}(\rho_\beta) = \sum_{\sigma \in G} \sigma \cdot \rho_\beta = \sum_{\sigma \in G} \sigma \rho_\beta \sigma^{-1}$$

y si $Tr_{K/Q}(\beta) = 1$ es $Tr_{K/Q}(\rho_\beta) = Id$. Este endomorfismo cumple la condición requerida para que $\mathcal{A}$ sea Z[G]-debilmente pro-

yectivo.

Proposición (3.2). En las hipótesis de la proposición (3.1) cada ideal invariante $\mathcal{A}$ de K es Z[G]-proyectivo.

En efecto: $\mathcal{A}$ es Z-libre ya que por ser un ideal fraccionario de K es de generación finita y por estar contenido en un cuerpo es libre de torsión. Por ser $\mathcal{A}$, Z-libre y Z[G]-debilmente proyectivo, es Z[G]-proyectivo. ([15] (2.3)).

Proposición (3.3). En las hipótesis de (3.1), A_K es isomorfo como Z[G]-módulo a Z[G].

En efecto: En [12] se ha demostrado que es un Z[G]-módulo libre, y por ser K una extensión de Q es de rango uno ya que $\dim_Z A_K = 2p$.

Observación (3.4) . Puesto que Z[G]-proyectivo es equivalente a cohomologicamente trivial [15], la proposición (3.2) puede enunciarse también diciendo que si K es moderadamente ramificada sobre Q, cada ideal invariante $\mathcal{A}$ de K es cohomologicamente trivial.

Sea $\mathcal{P}_Z$ la clase de todos los Z[G]-módulos proyectivos de generación finita y $\mathcal{F}_Z$ la clase de todos los Z[G]-módulos libres de generación finita. Es $\mathcal{F}_Z \subset \mathcal{P}_Z$. Se sabe que se define en $\mathcal{P}_Z$ la siguiente relación de equivalencia:

$P_1, P_2 \in \mathcal{P}_Z$, $P_1 \sim P_2 \Leftrightarrow \exists\ F_1, F_2 \in \mathcal{F}_Z$ tales que $P_1 \oplus F_1 \simeq P_2 \oplus F_2$.

El conjunto de las clases de Z[G]-módulos proyectivos respecto

a esta relación de equivalencia, con la operación $(P_1,P_2)\to P_1 \mathfrak{F} P_2$ forman un grupo que se indicará por $P(G)$.

Proposición (3.5). Sea G un grupo diedral de orden 2p (p primo impar), entonces P(G) es isomorfo al grupo de las clases de ideales del subcuerpo real maximal del cuerpo de las raices p-ésimas de la unidad. P_i pertenece a la clase 0 si y sólo si es $Z[G]$-libre.

La demostración ha sido dada por Lee en [8] .

Teorema (3.6) . Sea K una extensión de Q, galoisiana de grupo de Galois G diedral de orden 2p (p primo impar) moderadamente ramificada; si el número de clases del subcuerpo real maximal del cuerpo de las raices p-ésimas de la unidad es uno, entonces cada ideal invariante $\mathfrak{A}$ de K posee una $Z[G]$-base normal.

En efecto: En virtud de (3.2) cada ideal invariante de $\mathfrak{A}$ es un módulo de generación finita $Z[G]$-proyectivo, por tanto, si el número de clases del subcuerpo real maximal del cuerpo de las raices p-ésimas de la unidad es uno, en virtud del isomorfismo establecido en (3.5), P(G) consta de un sólo elemento formado por las clases de los $Z[G]$-módulos libres de generación finita, por tanto, cada ideal invariante de K es $Z[G]$-libre. Por ser $\mathfrak{A}$ un ideal fraccionario de K, es $\dim_Z \mathfrak{A} \leq 2p$, ya que existe un $\alpha \in K$ tal que $\alpha\mathfrak{A} \subset A_K$ y $\dim_Z A_K = 2p$. Por tanto $\mathfrak{A}$ es $Z[G]$-libre de rango uno es decir $\mathfrak{A}$ es isomorfo como $Z[G]$-módulo a $Z[G]$.

Nota (3.7) . El número de clases del subcuerpo real maximal de un cuerpo ciclotómico no siempre es uno. Esta cuestión ha sido estudiada por Ankeny-Chowla- Hasse en [1] , donde se demuestra que si $p = (2qn)^2 + 1$ con q primo y $n \geq 1$ entero, es primo, y H(p) es el número de clases del cuerpo $K = Q(\zeta_p + \zeta_p^{-1})$ donde ζ es una raiz p-ésima de la unidad, entonces H(p) es mayor que uno. En particular se sabe que esto ocurre para los siguientes valores de p : 257, 401, 577, 1297, 1601, 2917, 3137, 4357, 7057, 8101 .

4. CONDICIONES PARA QUE K SEA MODERADAMENTE RAMIFICADA SOBRE Q.

Proposición (4.1). Sea $\mathfrak{P}$ un primo de A_K que divide a qA_K. Si $q \neq p$ y $q \neq 2$ la extensión K es moderadamente ramificada sobre Q, en $\mathfrak{P}$.

Es consecuencia inmediata de la igualdad $2p = efg$.

Proposición (4.2) . Sea D el discriminante de K sobre Q. Si D es impar y $D \not\equiv 0 \pmod{p}$ la extensión K es moderadamente ramificada sobre Q.

En efecto: Un primo q de Q ramifica en K si y sólo si q divide a D; puesto que los únicos primos que pueden ramificar fuertemente en K son 2 o p, sólo en el caso en que 2 o p o ambos dividan a D la extensión podrá ser no moderadamente ramificada.

Proposición (4.3). Si K es moderadamente ramificada sobre Q

es $D \equiv f^{2(p-1)} \pmod 4$ siendo f un entero no nulo.

En efecto: Sea k el subcuerpo de K extensión cuadrática de Q y sea d el discriminante de k sobre Q. K moderadamente ramificada sobre Q implica, K moderadamente ramificada sobre k, y k moderadamente ramificada sobre Q. Por ser k una extensión cuadrática de Q, k ramifica moderadamente sobre Q si y sólo si $d \equiv 1 \pmod 4$. Por otra parte, se sabe que $D = d^p f^{2(p-1)}$ donde f es un entero no nulo ([12] Prop. 13, §7, Cap. IV) y por tanto $d \equiv 1 \pmod 4$ implica $D \equiv f^{2(p-1)} \pmod 4$.

5. CASO EN QUE EL CUERPO BASE SEA Q_p .

Previo al estudio de los ideales invariantes, se presenta la cuestión de la existencia de extensiones galoisianas de Q_p de grupo de Galois diedral de orden 2p (p primo impar). Esta se resuelve mediante el siguiente

Teorema (5.1) . Sea K una extensión galoisiana de Q, de grupo de Galois diedral de orden 2p (p primo impar); sea D el discriminante de K sobre Q, d el discriminante de la subextensión k de K cuadrática sobre Q; para los cuerpos Q_q tales que q cumple una de las dos condiciones siguientes:

1) $q = p$, q divide a d

2) $q \neq p$, q no divide a d, q divide a D, q no descompone en A_K

existe una extensión galoisiana de Q_q de grupo de Galois diedral de orden 2p (p primo impar) .

En efecto: Sean K_i los completados de K por las valoraciones w_i que prolongan a K la valoración v definida en Q por q. Si e_i y f_i son los índices de ramificación y los grados residuales correspondientes se tiene:

1) K_i es una extensión de Q_q de grado $n_i = e_i f_i$.

2) K_i es separable sobre Q_q

3) Si D_i es el grupo de descomposición de w_i en G, la extensión K_i sobre Q_q es galoisiana de grupo de Galois D_i.

Por tanto, condición suficiente para que K_i sea una extensión de Q_p galoisiana de grupo de Galois diedral de orden 2p, p primo impar, es que el grupo de descomposición D_i de w_i coincida con el grupo de Galois G. Puesto que el índice de D_i en G es igual al número g_q de ideales primos de A_K que dividen a q, $D_i = G$ si y sólo si existe un sólo primo $\mathfrak{P}$ que divide a q. Esta condición se cumple en los siguientes casos: [12]

1) $q = p$, q divide a d, y entonces $qA_K = \mathfrak{P}^{2p}$

2) $q \neq p$, q no divide a d, q divide a D, q no descompone en A_K y entonces $qA_K = \mathfrak{P}^{p}$

con lo cual queda demostrado el teorema.

Proposición (5.2). Si K es una extensión galoisiana finita de un cuerpo F completo respecto a una valoración discreta y A_F es el anillo de los enteros de F, la extensión K es moderadamente ramificada sobre F si y sólo si cada ideal invariante posee una A_F base normal.

Demostración: [19] T. 1.

Teorema (5.3). Sea K una extensión de Q_q, galoisiana, diedral de orden 2p (p primo impar) y tal que cumple las condiciones 2) del teorema (5.1), entonces cada ideal invariante de K posee una Z_q- base normal.

En efecto: Puesto que la característica del cuerpo residual es $q \neq p$, y el índice de ramificación es $e = p$, q no divide a e, y por tanto la extensión es moderadamente ramificada. En virtud de la proposición (5.2) en estas condiciones, cada ideal invariante posee una Z_p-base normal.

C A P I T U L O II

RAMIFICACION. CASO $2p^n$.

INTRODUCCION.- En este capítulo se considera un anillo A de Dedekind de cuerpo de fracciones $\mathcal{K}$, y una extensión N de $\mathcal{K}$ galoisiana, no abeliana de grupo de Galois G diedral de orden $2p^n$, p primo impar y $n>1$. Se estudian las ramificaciones de N sobre el cuerpo cuadrático correspondiente k, y de N sobre una subextensión K de grado p^n sobre $\mathcal{K}$, calculando los discriminantes respectivos. Como resultados previos sólo se incluirán los que no figuran en el Capítulo I.

1. NOTACIONES E HIPOTESIS PREVIAS.

Notaciones (1.1). A es un anillo de Dedekind, $\mathcal{K}$ su cuerpo de fracciones, p un número primo impar, N una extensión galoisiana de $\mathcal{K}$, no abeliana, diedral de orden $2p^n$ (n entero mayor que uno) y G su grupo de Galois. La presentación de G es:

$$G = \langle \sigma, \tau ;\ \sigma^{p^n} = 1 \quad \tau^2 = 1 \quad \tau\sigma\tau = \sigma^{-1} \rangle .$$

y tiene los siguientes subgrupos:

n subgrupos cíclicos H^i $i=0,1,\ldots,n-1$, divisores normales de G, generados por σ^{p^i};

p^n subgrupos de orden dos no divisores normales de G conjugados del subgrupo g de G generado por τ;

para cada $i=1,\ldots,n-1$, j subgrupos diedrales de orden $2p^i$ con $j+i=n$, no divisores normales de G, conjugados del subgrupo diedral h_i generado por $\langle \tau, \sigma^{p^i} \rangle$,

Se indicará por k el subcuerpo de N fijo por H^o, y por L_i los subcuerpos de N fijos por H^i $i=1,\ldots,n-2$. H^{n-1} se indicará simplemente por H y el subcuerpo de N fijo correspondiente, por L. El cuerpo L es una extensión galoisiana de $\mathfrak{K}$, de grupo de Galois diedral de orden $2p^{n-1}$; los cuerpos L_i son extensiones galoisianas de $\mathfrak{K}$, de grupo de Galois diedral de orden $2p^i$, $1 \leq i \leq n-2$ k es una subextensión de N cuadrática sobre $\mathfrak{K}$.

El subgrupo g se puede considerar como correspondiente a una subextensión K de N de grado p^n sobre $\mathfrak{K}$. K no es galoisiana sobre $\mathfrak{K}$, y los cuerpos conjugados de K corresponden a los subgrupos de G conjugados de g por los automorfismos internos de G. N es una extensión galoisiana de K de grado 2.

Cada subgrupo h_i se puede considerar como correspondiente a una subextensión K_i de N de grado p^j, $j+i=n$, sobre $\mathfrak{K}$. K_i no es galoisiana sobre $\mathfrak{K}$, y los cuerpos conjugados de K_i se corresponden con los subgrupos conjugados de h_i en G, por los automorfismos internos de G. N es una extensión de K_i galoisiana de grupo de Galois diedral de orden $2p^i$. K_i es pues un subcuerpo de K y de todos los conjugados de K por los elementos del subgrupo de G generado por σ^{p^i}.

Se indicará por A_N la clausura entera de A en N, y por A_k,

A_L, A_{L_i}, A_K, A_{K_i}, las clausuras enteras de A en k, L, L_i, K, K_i respectivamente.

Hipótesis previas (1.2). Sobre el anillo A se hacen además las siguientes hipótesis:

a) la característica de $\mathfrak{x}$ es distinta de p ;

b) los cuerpos residuales de A son perfectos ;

H) p es inversible en A o pA es el producto de ideales maximales distintos.

2. PROPIEDADES GENERALES.

Definición (2.1). Sea A un anillo de Dedekind de cuerpo de fracciones $\mathfrak{x}$, y L una extensión galoisiana de $\mathfrak{x}$ de grupo de Galois G. Sea B la clausura entera de A en L, y $\mathfrak{P}$ un ideal primo de B. El subgrupo de G definido por:

$$D_{\mathfrak{P}} = \left\{ s \in G \; ; \quad s(\mathfrak{P}) = \mathfrak{P} \right\}$$

se denomina el grupo de descomposición del primo $\mathfrak{P}$ en la extensión $L/\mathfrak{x}$.

Definición (2.2). El subgrupo $G_i(\mathfrak{P})$ $i \geq -1$ definido por

$$G_i(\mathfrak{P}) = \left\{ \sigma \in G \; ; \; \forall x \in A_L \quad \sigma(x) \equiv x \pmod{\mathfrak{P}^{i+1}} \right\}$$

se denomina el i-ésimo grupo de ramificación de G referido a $\mathfrak{P}$.

Proposición (2.3). Los $G_i(\mathfrak{P})$ forman una sucesión decreciente de subgrupos invariantes de $D_{\mathfrak{P}}$. Para i suficientemente grande se tiene $G_i = Id$, $G_{-1} = D_{\mathfrak{P}}$ y G_o es el subgrupo de iner-

cia de G.

Demostración: [17] Cap.IV § 1, Prop.1 .

Proposición (2.4). Si H es un subgrupo de G y K la subextensión correspondiente, los grupos de ramificación de $\mathfrak{P} \cap A_K$ son $H_i = G_i \cap H$.

Demostración: [17] Cap.IV § 1. Prop. 2.

Proposición (2.5). El grupo G_o / G_1 es cíclico.

Demostración : [17] Cap. IV § 1 Cor.1 a Prop.7.

Proposición (2.6). Si $s \in G_o$, $r \in G_i$ y $r \notin G_{i+1}$, $i \geq 1$, entonces $srs^{-1}r^{-1} \in G_{i+1}$ si y sólo si $s^i \in G_1$.

Demostración: [17] Cap.IV § 1 Cor.1 a Prop. 9.

Proposición (2.7). Sea L una extensión cíclica de $\varkappa$ de grado p, $\mathfrak{p}$ un ideal primo no nulo de A totalmente ramificado en L y $\mathfrak{P}$ un ideal primo de A_L tal que $\mathfrak{p} = \mathfrak{P} \cap A$. Se supone que $\mathfrak{p}$ divide a pA y que e es el exponente de $\mathfrak{p}$ en pA. Entonces: $1 \leq t \leq \left[\frac{pe}{p-1}\right]$ donde $[x]$ designa la parte entera de x, y t es un entero tal que $G_t(\mathfrak{P}) \neq Id.$ y $G_{t+1}(\mathfrak{P}) = Id$.

Demostración: [10] Lema III.1.

Proposición (2.8). Sea $M \supset L \supset \varkappa$, M separable sobre L y de grado finito n, y sea C la clausura entera de B en M, si se designa por $\mathfrak{d}_{B/A}$ y $\mathfrak{d}_{C/B}$ los discriminantes de B sobre A y C sobre B respectivamente, se tiene:

$$\mathfrak{d}_{C/A} = (\mathfrak{d}_{B/A})^n . N_{L/\varkappa}(\mathfrak{d}_{C/B}) .$$

Demostración: [17] Cap III. §4 Prop.8

Proposición (2.9). Sea $\mathfrak{p}$ un ideal primo de A. $L/\mathcal{K}$ es no ramificada en $\mathfrak{p}$ si y sólo si $\mathfrak{p}$ no divide a $\mathfrak{d}_{B/A}$.

Demostración: [17] Cap.III § 5 Cor.1 a Teor. 1.

Proposición (2.10). Sea e el índice de ramificación y f el grado residual de un primo $\mathfrak{p}$ de A en L, el exponente de $\mathfrak{p}$ en $\mathfrak{d}_{B/A}$ es igual a (e-1)f si y sólo si la extensión $L/\mathcal{K}$ es moderadamente ramificada.

Es consecuencia de [17] Cap III § 6 Prop. 13 y de ser

$$\mathfrak{d}_{B/A} = N_{L/\mathcal{K}}(\mathfrak{D}_{B/A}) \quad \text{y} \quad N_{L/\mathcal{K}}(\mathfrak{P}) = \mathfrak{p}^f$$

donde $\mathfrak{D}_{B/A}$ es la diferente de la extensión L sobre $\mathcal{K}$.

Definición (2.11). Sea V un espacio vectorial de dimensión finita sobre $\mathcal{K}$. Un sub-A-módulo X que genera V y es de tipo finito sobre A se denomina una red de V sobre A.

Si A es un anillo principal, se puede definir la red X diciendo que es un A-módulo libre de rango igual a la dimensión de V sobre $\mathcal{K}$.

Con la hipótesis de ser A principal, (lo que se puede conseguir siempre localizando), se puede definir el discriminante de la red de la siguiente manera:

Definición (2.12). Sea X una red de base $\{e_1,\ldots,e_n\}$; se denomina discriminante de X respecto a la forma bilineal traza y se indica por $\mathfrak{d}_{X,T}$ al ideal principal generado por

$\det (\mathrm{Tr} (e_i e_j))$.

Proposición (2.13). Si X y X' son dos redes de V sobre A tales que $X' \subset X$, se tiene:

$$\vartheta_{X';T} = \vartheta_{X,T}\, \mathcal{O}\!\mathcal{l}^2$$

siendo $\mathcal{O}\!\mathcal{l}$ un ideal de A.

Demostración: [17] Cap.III § 3. Cor a Prop.5.

Proposición (2.14) . Sea $L/\mathcal{K}$ una extensión galoisiana de grupo de Galois G diedral de orden 2p (p primo impar) y sea k la subextensión cuadrática correspondiente. Sea $\mathfrak{p}$ un ideal primo no nulo de A ramificado en k, y sea $\mathfrak{p} A_k = \bar{\mathfrak{p}}^2$. Entonces $\bar{\mathfrak{p}}$ en A_L no puede permanecer nunca primo. Si además $\mathfrak{p}$ no divide pA, $\bar{\mathfrak{p}}$ descompone en A_L en el producto de p ideales primos distintos.

Demostración: [12] Prop.III.3.

Proposición (2.15). Si $L/\mathcal{K}$ cumple las condiciones de la proposición (2,14), si además se supone A de valoración discreta y que cumple la hipótesis H, se tiene:

a) si $\mathfrak{p}$ no divide a pA es $\vartheta_{L/k} = \mathfrak{p}^{p-1}$

b) si se supone que $\mathfrak{p}$ divide a pA y que $\mathfrak{p}$ no ramifica en k se tiene $\vartheta_{L/k} = \mathfrak{p}^{2(p-1)}$

c) si se supone que $\mathfrak{p}$ divide a pA, $\mathfrak{p}$ ramifica en k, y es p mayor o igual que 5, es $\vartheta_{L/K} = \mathfrak{p}^{p-1}$ .Si p es

3 se puede presentar un caso excepcional.

Demostración: [12] Teor. III.1.

Proposición (2.16). En las hipótesis de (2.14) y suponiendo que A verifica la hipótesis H, $\vartheta_{L/k}$ es la potencia p-1 de un ideal $\mathfrak{p}$ de A.

Demostración: [12] Teor. III 1.

Proposición (2.17). En las hipótesis de (2.14), sea K un cuerpo fijo por un subgrupo de G de orden 2, A_K el anillo de los enteros de K. Sea $\mathfrak{p}$ un ideal primo no nulo de A y $\mathfrak{P}_i$ los ideales primos de A_K que dividen a $\mathfrak{p}$. Entonces $\vartheta_{N/K}$ es divisible por uno de los $\mathfrak{P}_i$ si y sólo si $\mathfrak{p}$ divide a $\vartheta_{k/\kappa}$, y en este caso uno sólo de los $\mathfrak{P}_i$ divide $\vartheta_{N/K}$.

Demostración: [12] Prop.III 5.

3. RAMIFICACIÓN EN N DE LOS IDEALES PRIMOS DE A

Proposición (3.1). Sea $\mathfrak{p}$ un ideal primo no nulo de A que no divide a pA, ramificado en k, y sea $\bar{\mathfrak{p}}$ un primo de A_k tal que $\mathfrak{p} A_k = \bar{\mathfrak{p}}^2$. Entonces, $\bar{\mathfrak{p}}$ es en A_N el producto de p^n ideales primos distintos.

Demostración: Por inducción sobre n.

n=1, es el caso estudiado en (2.14)

En virtud de la hipótesis de inducción es $\bar{\mathfrak{p}} A_L = \mathfrak{P}_1 \ldots \mathfrak{P}_{p^{n-1}}$. Puesto que N/L es cíclica de orden p, para cada primo $\mathfrak{P}$ de A_L

que divide a $\bar{\mathfrak{p}}$ sólo pueden presentarse en A_N los casos siguientes:

1) $\mathfrak{P} A_N = \bar{\mathfrak{P}}$ (queda primo)

2) $\mathfrak{P} A_N = \bar{\mathfrak{P}}^p$

3) $\mathfrak{P} A_N = \bar{\mathfrak{P}}_1 \cdots \bar{\mathfrak{P}}_p$.

Se ha de probar la imposibilidad de 1) y 2).

Imposibilidad de 1). Obsérvese en primer lugar que por ser N galoisiana sobre $\mathfrak{K}$, todos los primos $\mathfrak{P}_i$ de A_L que dividen a un mismo primo $\bar{\mathfrak{p}}$ de A_k se comportarán al pasar a A_N de la misma manera en cuanto a la ramificación.

Sea $D_{\bar{\mathfrak{P}}}$ el grupo de descomposición de $\bar{\mathfrak{P}}$ en N sobre $\mathfrak{K}$. Puesto que en la descomposición de $\bar{\mathfrak{p}} A_N$ aparecen p^{n-1} factores primos distintos, el orden de $D_{\bar{\mathfrak{P}}}$ es 2p, y por tanto $D_{\bar{\mathfrak{P}}}$ es un subgrupo de G diedral de orden 2p. Por permanecer $\bar{\mathfrak{P}}$ primo en N sobre L es $H_{-1}(\bar{\mathfrak{P}}) = H$ y $H_0(\bar{\mathfrak{P}}) = Id$. Pero $\bar{\mathfrak{P}}$ ha ramificado en N sobre $\mathfrak{K}$, y por tanto $G_0(\bar{\mathfrak{P}}) \neq Id$. Por otra parte se tiene: $Id = H_0(\bar{\mathfrak{P}}) = G_0(\bar{\mathfrak{P}}) \cap H$, lo que implica que $G_0(\bar{\mathfrak{P}})$ ha de ser un subgrupo de $D_{\bar{\mathfrak{P}}}$ de orden 2. Puesto que $G_0(\bar{\mathfrak{P}})$ es un divisor normal de $D_{\bar{\mathfrak{P}}}$, se ha llegado a una contradicción.

Obsérvese que para probar esta imposibilidad no se ha utilizado en ningún momento la hipótesis de que $\mathfrak{p}$ no divide a pA, lo que significa que el razonamiento es también válido si $\mathfrak{p}$ divide a pA.

Imposibilidad de 2).

$$\mathfrak{p} A_k = \bar{\mathfrak{p}}^2 , \quad \bar{\mathfrak{p}} A_L = \mathfrak{P}_1 \cdots \mathfrak{P}_{p^{n-1}} , \quad \mathfrak{P} A_N = \bar{\mathfrak{P}}^p$$

implica, $\mathfrak{p} A_N = \bar{\mathfrak{P}}_1^{2p} \cdots \bar{\mathfrak{P}}_{p^{n-1}}^{2p}$. Para cada $\bar{\mathfrak{P}}_i$ que divide a $\bar{\mathfrak{p}}$, $D_{\bar{\mathfrak{P}}_i}$ es un subgrupo de G diedral de orden 2p. Por ser el orden de $G_o(\bar{\mathfrak{P}}_i)$ igual a 2p es $D_{\bar{\mathfrak{P}}_i} = G_o(\bar{\mathfrak{P}}_i)$. Puesto que $\mathfrak{p}$ no divide a pA la característica de $A/\mathfrak{p}$ y por tanto la de $A_L/\mathfrak{P}_i$ es distinta de p, y N es moderadamente ramificada en $\bar{\mathfrak{P}}_i$ sobre L, pues el índice de ramificación de $\bar{\mathfrak{P}}_i$ en N sobre L es p. Se tiene pues, $H_1(\bar{\mathfrak{P}}_i) = Id$, y por ser $H_1(\bar{\mathfrak{P}}_i) = G_1(\bar{\mathfrak{P}}_i) \cap H$ ha de ser $G_1(\bar{\mathfrak{P}}_i) = Id$ ó $G_1(\bar{\mathfrak{P}}_i)$ ha de ser un subgrupo de $D_{\bar{\mathfrak{P}}_i}$ de orden dos, y esto último no es posible ya que $G_1(\bar{\mathfrak{P}}_i)$ es un divisor normal de $D_{\bar{\mathfrak{P}}_i}$. Entonces, $G_1(\bar{\mathfrak{P}}_i) = Id$ implica $G_o(\bar{\mathfrak{P}}_i)/G_1(\bar{\mathfrak{P}}_i) \simeq G_o(\bar{\mathfrak{P}}_i)$ y por tanto, por (2.5), $G_o(\bar{\mathfrak{P}}_i)$ ha de ser un grupo cíclico, lo que contradice el hecho de ser diedral de orden 2p.

Proposición (3.2). Sea $\mathfrak{p}$ un ideal primo no nulo de A que divide a pA, totalmente ramificado en N, es decir, $\mathfrak{p} A_N = \bar{\mathfrak{P}}^{2p^n}$. Sea G_i la sucesión de grupos de ramificación de G y H_i la sucesión de grupos de ramificación de H correspondientes a $\bar{\mathfrak{P}}$, t el entero para el cual $G_t \neq Id$, $G_{t+1} = Id$, y t' el entero para el cual $H_{t'} \neq Id$, $H_{t'+1} = Id$. Entonces $t' = t \geq 1$, y t es un número impar.

En efecto: Puesto que N sobre $\mathfrak{x}$ ramifica totalmente en $\bar{\mathfrak{P}}$ es $G_{-1}(\bar{\mathfrak{P}}) = G$ y $G_o(\bar{\mathfrak{P}}) = G$. La característica de $A/\mathfrak{p}$ es p, ya que $\mathfrak{p}$ divide a pA, y por ser $2p^n$ el índice de ramificación de $\bar{\mathfrak{P}}$, N no es moderadamente ramificada sobre $\mathfrak{x}$ en $\bar{\mathfrak{P}}$,

por tanto $G_1(\overline{\mathfrak{P}}) \neq Id$ y $t \geq 1$. Por ser $H_i = G_i \cap H$ y G_i divisor normal de G, ha de ser $H_i = G_i \cap H = H \neq Id$ si $G_i \neq Id$, pues G_i ha de ser un subgrupo cíclico de orden una potencia de p. Por tanto $H_i = Id$ si y sólo si $G_i = Id$. Es decir $t' = t$.

Para probar que t es un número impar, basta aplicar (2.6) con $s = \tau \in G_o$, $r = \sigma^{p^i}$, $i = t$. Las condiciones de la proposición (2.6) se cumplen ya que por ser $G_i \neq Id$, existe un σ^{p^j} que pertenece a G_i y no pertenece a G_{i+1}. Se tiene además $\tau\sigma^{p^j}\tau\sigma^{-p^j} = \sigma^{-2p^j} \neq Id$, por tanto $\tau\sigma^{p^j}\tau\sigma^{-p^j} \notin G_{i+1}$ lo que implica $\tau^t \notin G_1$ es decir t es impar.

Teorema (3.3). El discriminante $\vartheta_{N/k}$ es la potencia $p-1$ de un ideal $\mathfrak{J}$ de A.

Demostración: Se procede por inducción sobre el exponente n de p. Para $n = 1$ es la proposición (2.16).

Puesto que N/L es galoisiana de grado p, y L/k es galoisiana de grado p^{n-1}, en virtud de (2.8) se tiene:

$$\vartheta_{N/k} = (\vartheta_{L/k})^p N_{L/k}(\vartheta_{N/L}) .$$

En virtud de la hipótesis de inducción es $\vartheta_{L/k} = \mathfrak{J}_1^{p-1}$, por tanto,

$$\vartheta_{N/k} = \mathfrak{J}_1^{(p-1)p} N_{L/k}(\vartheta_{N/L}) . \qquad (1)$$

Se trata pues de calcular $N_{L/k}(\vartheta_{N/L})$. Para ello se estudia-

rá el comportamiento en A_N de los primos $\mathfrak{p}$ de A, y se puede suponer que A es un anillo de valoración discreta de ideal maximal $\mathfrak{p}$, distinguiendo los diversos casos según la ramificación de $\mathfrak{p}$ en N. Puesto que $N/\varkappa$ es galoisiana, $\mathfrak{D}_{N/\varkappa}$ es un ideal de A_N G-invariante, por tanto, si $\mathfrak{p}A_k = \bar{\mathfrak{p}}_1\bar{\mathfrak{p}}_2$, es $v_{\bar{\mathfrak{p}}_1}(\mathfrak{d}_{N/k}) = v_{\bar{\mathfrak{p}}_2}(\mathfrak{d}_{N/k})$.

caso a)). Se supone que $\mathfrak{p}$ no divide a pA. Si $\mathfrak{p}$ divide a $\mathfrak{d}_{k/\varkappa}$ en virtud de (3.1) $\mathfrak{p}$ no divide a $\mathfrak{d}_{N/L}$. Si $\mathfrak{p}$ no divide $\mathfrak{d}_{k/\varkappa}$ se pueden presentar dos casos según que $\mathfrak{p}$ divida $\mathfrak{J}_1$ o que $\mathfrak{p}$ no divida $\mathfrak{J}_1$.

caso a,1) $\mathfrak{p} \nmid pA$, $\mathfrak{p} \nmid \mathfrak{d}_{k/\varkappa}$, $\mathfrak{p} \nmid \mathfrak{J}_1$.

Sea $\bar{\mathfrak{p}}$ un ideal de A_k tal que $\bar{\mathfrak{p}} \mid \mathfrak{p}A_k$. Si $\bar{\mathfrak{p}}$ no ramifica en N, $\bar{\mathfrak{p}}$ y $\mathfrak{d}_{N/L}$ son primos entre sí. Supóngase pues que $\bar{\mathfrak{p}}$ ramifica en N, en virtud de las hipótesis hechas sobre $\mathfrak{p}$, $\bar{\mathfrak{p}} \mid \mathfrak{d}_{N/L}$. Sea $\mathfrak{P}$ un primo de A_L tal que $\mathfrak{P} \mid \bar{\mathfrak{p}}A_L$. Es $\mathfrak{P}A_N = \bar{\mathfrak{P}}^p$. Puesto que $\mathfrak{p} \nmid pA$, $\mathfrak{P} \nmid pA$ y por tanto la característica de $A_L/\mathfrak{P}$ es distinta de p, y N es moderadamente ramificada en $\bar{\mathfrak{P}}$ sobre L. Se tiene pues : $v_{\mathfrak{P}}(\mathfrak{d}_{N/L}) = p - 1$. Puesto que $\bar{\mathfrak{p}} \nmid \mathfrak{J}_1$ es $v_{\bar{\mathfrak{p}}}(N_{L/k}(\mathfrak{d}_{N/L})) = (p-1)f_{\bar{\mathfrak{p}}}\, g_{\bar{\mathfrak{p}}} = (p-1)p^{n-1}$, y $v_{\mathfrak{p}}(N_{L/k}(\mathfrak{d}_{N/L})) = (p-1)p^{n-1}$.

En virtud de (2.8) se tiene pues:

$$v_{\mathfrak{p}}(\mathfrak{d}_{N/k}) = (p-1)\,p^{n-1}.$$

caso a,2) . $\mathfrak{p} \nmid pA$, $\mathfrak{p} \nmid \mathfrak{d}_{k/\varkappa}$, $\mathfrak{p} \mid \mathcal{J}_1$.

Puesto que $\mathfrak{p} \mid \mathcal{J}_1$, $\mathfrak{p} A_L$ ha ramificado en A_L y por tanto será de la forma

$$\mathfrak{p} A_L = \prod_i \mathfrak{P}_i^{p^j} \qquad i+j \leq n-1 \quad (i,\ j \text{ fijos})$$

Si $\mathfrak{P}_i A_N$ no ramifica en A_N, $\mathfrak{P}_i$ y $\mathfrak{d}_{N/L}$ son primos entre si. Si ramifica lo hace total y moderadamente, por tanto:

$v_{\mathfrak{P}_i}(\mathfrak{d}_{N/L}) = p-1$ y $v_{\bar{\mathfrak{p}}}(N_{L/K}(\mathfrak{d}_{N/L})) = (p-1) f_{\bar{\mathfrak{p}}}\, g_{\bar{\mathfrak{p}}} =$

$(p-1)p^{n-(j+1)}$ ya que $f_{\bar{\mathfrak{p}}}\, g_{\bar{\mathfrak{p}}} = p^{n-1} : p^j$ por ser $e_{\mathfrak{p}} = p^j$.

Por tanto, en virtud de (1) se tiene:

$$v_{\mathfrak{p}}(\mathfrak{d}_{N/k}) = (p-1)p^{n-(j+1)} + v_{\mathfrak{p}}(\mathcal{J}_1)p(p-1) =$$

$$= p(p-1)\left[p^{n-(j+2)} + v_{\mathfrak{p}}(\mathcal{J}_1)\right] .$$

caso b. Si $\mathfrak{p}$ divide a pA puede ocurrir que $\mathfrak{p}$ divida $\mathfrak{d}_{k/\varkappa}$ o que $\mathfrak{p}$ no divida a $\mathfrak{d}_{k/\varkappa}$ y en cada uno de ellos, que $\mathfrak{p}$ divida a $\mathcal{J}_1$ o que $\mathfrak{p}$ no divida a $\mathcal{J}_1$. Se tiene pues:

caso b,1.1 . $\mathfrak{p} \mid pA$, $\mathfrak{p} \nmid \mathfrak{d}_{k/\varkappa}$, $\mathfrak{p} \nmid \mathcal{J}_1$

Si $\mathfrak{p} A_L$ no ramifica en A_N, no divide a $\mathfrak{d}_{N/L}$. Si ramifica puede hacerlo no moderadamente. Sea $\mathfrak{P}$ un primo de A_L tal que $\mathfrak{P} \mid \mathfrak{p} A_L$ y $\mathfrak{P} A_N = \bar{\mathfrak{P}}^p$. Puesto que $\bar{\mathfrak{P}}$ ha ramificado totalmente en N/L es $v_{\bar{\mathfrak{P}}}(\mathfrak{d}_{N/L}) = (p-1)(t+1)$ siendo t el entero para el cual $H_t(\bar{\mathfrak{P}}) \neq Id$ y $H_{t+1}(\bar{\mathfrak{P}}) = Id$. Teniendo en cuenta que A verifica la hipótesis H, y que L es galoisiana sobre $\varkappa$, se puede aplicar (2.7) con e=1 y puesto que $p \geq 3$ se tiene t=1.

Es pues $v_{\mathfrak{P}}(\vartheta_{N/L}) = 2(p-1)$ y $v_{\bar{\mathfrak{p}}}(N_{L/k}(\vartheta_{N/L})) = 2(p-1)p^{n-1}$

y por tanto $v_{\mathfrak{p}}(\vartheta_{N/k}) = 2(p-1)p^{n-1}$.

caso b.1.2. $\mathfrak{p} \mid pA$, $\mathfrak{p} \nmid \vartheta_{k/\kappa}$, $\mathfrak{p} \mid \mathcal{J}_1$

El mismo razonamiento que en el caso anterior conduce a $v_{\mathfrak{P}}(\vartheta_{N/L}) = (p-1)(t+1)$ siendo $\mathfrak{P}$ un primo de A_L tal que $\mathfrak{P} \mid \mathfrak{p} A_L$. Puesto que $\mathfrak{p} \mid \mathcal{J}_1$, $\mathfrak{P}$ ha ramificado en A_L con $v_{\mathfrak{P}}(\bar{\mathfrak{p}} A_L) = p^i$ $1 \leq i \leq n-1$, i fijo para todos los primos de A_L que dividen a $\bar{\mathfrak{p}} A_L$, siendo $\bar{\mathfrak{p}}$ un primo de A_k que divide a $\mathfrak{p} A_k$. Se puede pues aplicar (2.7) con $e=p^i$ y se tiene para t la siguiente acotación : $1 \leq t \leq \left[p^{i+1}/(p-1)\right]$ es decir $1 \leq t \leq \sum_{j=0}^{i} p^j$. Por tanto:

$$v_{\bar{\mathfrak{p}}}(N_{L/k}(\vartheta_{N/L})) = (t+1)(p-1)p^j \qquad j+i = n-1$$

y como consecuencia:

$$v_{\mathfrak{p}}(\vartheta_{N/k}) = (t+1)(p-1)p^j + v_{\mathfrak{p}}(\mathcal{J}_1)p(p-1) =$$
$$= p(p-1)((t+1)p^{j-1} + v_{\mathfrak{p}}(\mathcal{J}_1))$$

de donde resulta:

$$v_{\mathfrak{p}}(\vartheta_{N/k}) = p(p-1)((t+1)p^{j-1} + v_{\mathfrak{p}}(\mathcal{J}_1)) \qquad 1 \leq t \leq \sum_{j=0}^{i} p^j \quad j+i=n-1.$$

caso b.2.1. $\mathfrak{p} \mid pA$, $\mathfrak{p} \mid \vartheta_{k/\kappa}$ $\mathfrak{p} \nmid \mathcal{J}_1$.

Puesto que $\mathfrak{p} \mid \vartheta_{k/\kappa}$ es $\mathfrak{p} A_k = \bar{\mathfrak{p}}^2$ y si $\mathfrak{P}$ es un primo de A_L tal que $\mathfrak{P} \mid \bar{\mathfrak{p}} A_L$, que ramifica en A_N , se tendrá $v_{\mathfrak{P}}(\vartheta_{N/L}) = (t+1)(p-1)$. Puesto que por hipótesis $\mathfrak{p}$ no ha ramificado en L/k se puede aplicar (2.7) con e=2 y se tiene

$1 \leq t \leq [2p/p-1]$, y puesto que t es impar, será $t=1$, si $p>3$, y $t=1,3$ si $p=3$. En ambos casos $t+1$ es un número par y teniendo en cuenta (3.1) resulta:

$$v_{\bar{\mathfrak{p}}}(N_{L/k}(\vartheta_{N/L})) = (t+1)(p-1)p^{n-1}$$

y por tanto:

$$v_{\bar{\mathfrak{p}}}(N_{L/k}(\vartheta_{N/L})) = 2(p-1)p^{n-1} \qquad \text{si} \quad p>3$$

$$v_{\bar{\mathfrak{p}}}(N_{L/k}(\vartheta_{N/L})) = 2^i(p-1)p^{n-1} \qquad i=1,2 \quad \text{si} \quad p=3$$

resultando finalmente:

$$v_{\mathfrak{p}}(\vartheta_{N/k}) = (p-1)p^{n-1} \qquad \text{si} \quad p>3$$

$$v_{\mathfrak{p}}(\vartheta_{N/k}) = 2^i(p-1)p^{n-1} \qquad i=0,1 \quad \text{si} \quad p=3$$

<u>caso b,2,2.</u> $\mathfrak{p} \mid pA$, $\mathfrak{p} \mid \vartheta_{k/\varkappa}$, $\mathfrak{p} \mid \mathfrak{J}_1$.

Razonando igual que en el caso anterior es $v_{\mathfrak{P}}(\vartheta_{N/L})=(t+1)(p-1)$ donde $\mathfrak{P}$ es un primo de A_L tal que $\mathfrak{P} \mid \mathfrak{p} A$. Puesto que $\mathfrak{P}$ ha ramificado en A_L con $e^{\mathfrak{P}}=p^i$ la acotación de t vendrá dada por $1 \leq t \leq [2p^{i+1}/(p-1)]$ o sea $1 \leq t \leq 2\sum_{j=0}^{i} p^j$ con la condición además de ser t un número impar. Por tanto:

$$v_{\bar{\mathfrak{p}}}(N_{L/k}(\vartheta_{N/L})) = (t+1)(p-1)p^j \qquad j+i = n-1$$

de donde resulta:

$$v_{\mathfrak{p}}(N_{L/k}(\vartheta_{N/L})) = 1/2\ (t+1)(p-1)p^j \qquad j+i=n-1 \quad t \text{ impar}$$

se tiene pues:

$$v_{\mathfrak{P}}(\vartheta_{N/k}) = p(p-1)((t+1)/2)p^{j-1} + v_{\mathfrak{P}}(\mathcal{J}_1)) \qquad j+i=n-1$$

$$1 \leq t \leq 2\sum_{\ell=0}^{i} p^{\ell}$$

$$t \equiv 1 \pmod 2$$

Corolario (3.5). Si $\mathfrak{P}$ es un primo de A tal que $\mathfrak{P} \mid \vartheta_{k/x}$ entonces:

$$\mathfrak{P}^{A_N} = \frac{p^i-1}{\prod_{l=0}} \overline{\mathfrak{P}}_{\mathfrak{L}}^{2p^j} \qquad i+j = n$$

En efecto: Si $\mathfrak{P} \mid \vartheta_{k/x}$ y $\mathfrak{P} \nmid pA$ en virtud de (3.1) $\mathfrak{P} \nmid \mathcal{J}$ y por tanto se tiene $\mathfrak{P}.A_N = \overline{\mathfrak{P}}_o^2 \cdots \overline{\mathfrak{P}}_{p^n-1}^2$ (puesto que $\overline{\mathfrak{P}}$ no puede permanecer primo), que es la expresión dada con i=n y j=0. Si $\mathfrak{P} \mid \vartheta_{k/x}$ y $\mathfrak{P} \mid \mathcal{J}$ entonces por (3.1) $\mathfrak{P} \mid pA$ y $\mathfrak{P}^{A_N} = \overline{\mathfrak{P}}_o^{2p^j} \cdots \overline{\mathfrak{P}}_{p^i-1}^{2p^j}$ $\quad i+j = n \quad 1 \leq j \leq n$ (i, j fijos) que corresponden al caso b.2.1 de (3.4) si j=1, y al caso b.2.2 de (3.4) si j>1. En particular, si j=n es $\mathfrak{P}^{A_N} = \overline{\mathfrak{P}}^{2p^n}$ y la extensión N/x es totalmente ramificada en $\overline{\mathfrak{P}}$.

Corolario (3.6). $$\vartheta_{N/x} = \vartheta_{N/k}^{p^n} \mathcal{J}^{2(p-1)}$$

En efecto: Aplicando (2.8) es:

$$\vartheta_{N/x} = (\vartheta_{k/x})^{p^n} (N_{k/x}(\vartheta_{N/k}))$$

y por tanto en virtud de (3.3)

$$\vartheta_{N/x} = (\vartheta_{k/x})^{p^n} \mathcal{J}^{(p-1).2}$$

4. RAMIFICACION EN K DE LOS IDEALES PRIMOS DE A.

Proposición (4.1). Sea $\mathfrak{p}$ un ideal primo no nulo de A, y $\mathfrak{P}$ un ideal primo no nulo de A_K tal que $\mathfrak{P} \mid \mathfrak{p}$. Entonces, si $\mathfrak{P}$ divide $\vartheta_{N/K}$, , $\mathfrak{p}$ divide $\vartheta_{k/x}$.

En efecto: Por ser K y k subextensiones de N linealmente disjuntas sobre x , si (ω_1, ω_2) es una A-base de A_k, ω_1 y ω_2 son linealmente independientes sobre A_K. Localizando en $\mathfrak{P}$ se puede suponer A_K principal y si X es la red de N sobre K generada por (ω_1, ω_2) su discriminante , en virtud de (15.1), es $\vartheta_{X,T} = \vartheta_{k/x} A_K$. Por (16.1) se verifica $\vartheta_{X,T} = {}_{N/K}\mathfrak{a}^2$ donde $\mathfrak{a}$ es un ideal de A_K. Por tanto $\vartheta_{k/x} A_K = \vartheta_{N/K}\, \mathfrak{a}^2$ Es decir $\vartheta_{N/K}$ divide $\vartheta_{k/x}$. En consecuencia:

$$\mathfrak{p} \mid \mathfrak{P} \,,\ \mathfrak{P} \mid \vartheta_{N/K} \,,\ \vartheta_{N/K} \mid \vartheta_{k/x} \implies \mathfrak{p} \mid \vartheta_{k/x} \,.$$

Proposición (4.2) . Para cada ideal $\mathfrak{p} \neq 0$ de A que divide $\vartheta_{k/x}$ primo, existe un ideal primo $\mathfrak{P}_i$ de A_K y uno sólo que divide a $\mathfrak{p}$ y tal que $\mathfrak{P}_i$ divide a $\vartheta_{N/K}$.

En efecto: En virtud de (3.5) si $\mathfrak{p} \mid \vartheta_{k/x}$ es $\mathfrak{p} A_N = \prod_{s=0}^{p^j-1} \overline{\mathfrak{P}}_s^{2p^i}$ con $i+j = n$. Los grupos de descomposición $D_{\overline{\mathfrak{P}}_s}$ en N/x de los primos que dividen a $\mathfrak{p}$ son pues subgrupos de G de orden $2p^i$ y por tanto diedrales de orden $2p^i$. Sea $h_i = \langle \tau, \sigma^{p^i} \rangle$. el correspondiente a $\overline{\mathfrak{P}}_o$ (esto es siempre posible mediante

un cambio de subíndices si es preciso) y sea K_i el subcuerpo de N fijo por h_i. K_i es un subcuerpo del cuerpo K que es el subcuerpo de N fijo por g. Los $\overline{\mathfrak{P}}_s$ $1 \leq s \leq p^j-1$ son conjugados de $\overline{\mathfrak{P}}_o$ por los automorfismos internos de G que transforman $D_{\overline{\mathfrak{P}}_o}$ en $D_{\overline{\mathfrak{P}}_s}$, es decir, $\overline{\mathfrak{P}}_s = \sigma^s(\overline{\mathfrak{P}}_o)$.

Se tiene:

$$\mathfrak{p}^{A_K} = (N_{N/K}(i(\mathfrak{p}^{A_N})))^{1/2} = N_{N/K}\Big(\prod_{s=o}^{p^j-1} \sigma^s(\overline{\mathfrak{P}}_o)\Big)^{p^i} =$$

$$\prod_{s=o}^{p^j-1} (N_{N/K}(\sigma^s(\overline{\mathfrak{P}}_o))^{p^i}$$

donde $i(\mathfrak{p}^{A_N})$ representa el homomorfismo de inyección. Si se pone $\mathfrak{P}_o = \overline{\mathfrak{P}}_o \cap A_K$ y $\mathfrak{P}_s = N_{N/K}(\sigma^s(\overline{\mathfrak{P}}_o))$ es:

$$\mathfrak{p}^{A_K} = \mathfrak{P}_o^{p^i} \prod_{s=1}^{p^j-1} \mathfrak{P}_s^{p^i}$$

y se tiene $\mathfrak{p}^{A_K}$ descompuesto en el producto de p^j ideales primos de A_K, que se verá que no son todos distintos. Puesto que N es galoisiana sobre K de grado dos, el número máximo de primos de A_N que pueden tener la misma norma en A_K es dos, y uno será la imagen del otro por $\tau \in g$. Por tanto:

$$\mathfrak{P}_{s_1} = \mathfrak{P}_{s_2} \iff \overline{\mathfrak{P}}_{s_1} = \tau(\overline{\mathfrak{P}}_{s_2})$$

Pero:

$$\overline{\mathfrak{P}}_{s_1} = \sigma^{s_1}(\overline{\mathfrak{P}}_o) \quad \text{y} \quad \overline{\mathfrak{P}}_{s_2} = \sigma^{s_2}(\overline{\mathfrak{P}}_o)$$

por tanto

$$\mathfrak{P}_{s_1} = \mathfrak{P}_{s_2} \iff \sigma^{s_1}(\bar{\mathfrak{P}}_o) = \tau\sigma^{s_2}(\bar{\mathfrak{P}}_o)$$

y puesto que $\bar{\mathfrak{P}}_o = \tau\bar{\mathfrak{P}}_o$,

$$\mathfrak{P}_{s_1} = \mathfrak{P}_{s_2} \iff \sigma^{s_1} = \tau\sigma^{s_2}\tau \iff s_1 = -s_2 .$$

Es decir, los primos $\mathfrak{P}_s$ son dos a dos iguales. Se tiene pues:

$$\mathfrak{p}^{A_K} = \mathfrak{P}_o^{p^i}\,\mathfrak{P}_1^{2p^i}\cdots\mathfrak{P}_{1/2(p^j-1)}^{2p^i} \qquad (2)$$

donde los primos $\mathfrak{P}$ que aparecen son todos distintos entre si. Por tanto $\mathfrak{P}_o$ y sólo $\mathfrak{P}_o$ ha ramificado en N sobre K.

Proposición (4.3). $N_{k/\varkappa}(\mathfrak{d}_{N/K}) = \mathfrak{d}_{k/\varkappa}$.

En efecto: En virtud de (4.1) y (4.2) es $\mathfrak{d}_{k/\varkappa} = \mathfrak{p}_1^{\alpha_1}\cdots\mathfrak{p}_r^{\alpha_r}$ y $\mathfrak{d}_{N/K} = \mathfrak{P}_1^{\beta_1}\cdots\mathfrak{P}_r^{\beta_r}$ donde para cada i, $1 \le i \le r$ es $\mathfrak{P}_i \mid \mathfrak{p}_i$. Si $\mathfrak{p} \mid pA$, puesto que $k/\varkappa$ y N/K son de grado dos, serán ambas moderadamente ramificadas y por tanto $\mathfrak{d}_{k/\varkappa} = \mathfrak{p}_1\cdots\mathfrak{p}_r$ y $\mathfrak{d}_{N/K} = \mathfrak{P}_1\cdots\mathfrak{P}_r$. Se tiene,

$$N_{K/\varkappa}(\mathfrak{d}_{N/K}) = \prod_{i=1}^{r} N_{K/\varkappa}(\mathfrak{P}_i) = \prod_{i=1}^{r} \mathfrak{p}_i^{f_{\mathfrak{P}_i}}$$

donde $f_{\mathfrak{P}_i}$ es el grado residual de $\mathfrak{P}_i$ en la extensión $K/\varkappa$. Teniendo en cuenta la expresión de $\mathfrak{p}^{A_K}$ dada en (2) de (4.2) es:

$$p^n = p^i\left(f_{\mathfrak{P}_o} + 2f_{\mathfrak{P}_1} + \cdots + 2f_{\mathfrak{P}_{\frac{p^j-1}{2}}}\right) \geqslant p^i.p^j = p^n$$

lo que implica $f_{\mathfrak{P}_0} = 1$. Por tanto $f_{\mathfrak{P}_i} = 1$ para cada $\mathfrak{P}_i$ de A_K que divide a un $\mathfrak{p}_i$ de A que divide a $\mathfrak{d}_{k/\mathfrak{x}}$, con lo cual queda demostrada la proposición para este caso.

Si $\mathfrak{p} \nmid pA$ y $\mathfrak{p} \mid \mathfrak{d}_{k/\mathfrak{x}}$ es :

$$\mathfrak{p}A_k = \bar{\mathfrak{p}}^2 \quad , \quad \mathfrak{p}A_K = \mathfrak{P}_0 \mathfrak{P}_1^2 \cdots \mathfrak{P}_{p^n-1}^2 \quad , \quad \mathfrak{p}A_N = \bar{\mathfrak{P}}_0^2 \cdots \bar{\mathfrak{P}}_{p^n-1}^2$$

En este caso, las extensiones N/K y k/$\mathfrak{x}$ pueden no ser moderadamente ramificadas y el razonamiento anterior no es válido. Considerando las cadenas de extensiones $N \supset k \supset \mathfrak{x}$ y $N \supset K \supset \mathfrak{x}$,se tiene $\bar{\mathfrak{P}}_0 \mid \bar{\mathfrak{p}} \mid \mathfrak{p}$ y $\bar{\mathfrak{P}}_0 \mid \mathfrak{P}_0 \mid \mathfrak{p}$ respectivamente. Si se completa A por $\mathfrak{p}$, se tiene el anillo $\hat{A}_{\mathfrak{p}}$ de valoración discreta y cuerpo de fracciones $\hat{\mathfrak{x}}$. En $N/\mathfrak{x}$ es $e_{\bar{\mathfrak{P}}_i} = 2$ y $f_{\bar{\mathfrak{P}}_i} = 1$, por tanto en virtud del isomorfismo definido en [17] Cap.II §3 T.1(iii), $N \otimes_{\mathfrak{x}} \hat{\mathfrak{x}}$ se identifica al producto de p^n cuerpos cuadráticos que son completados de N por los primos $\bar{\mathfrak{P}}_i$. Es decir:

$$N \otimes_{\mathfrak{x}} \hat{\mathfrak{x}} = \prod_{i=0}^{p^n-1} \hat{N}_{\bar{\mathfrak{P}}_i} \quad \text{y} \quad \left[\hat{N}_{\bar{\mathfrak{P}}_i} : \hat{\mathfrak{x}}\right] = 2 .$$

Por la misma razón:

$$k \otimes_{\mathfrak{x}} \hat{\mathfrak{x}} = \hat{k}_{\bar{\mathfrak{p}}} \quad \text{y} \quad \left[\hat{k}_{\bar{\mathfrak{p}}} : \hat{\mathfrak{x}}\right] = 2 .$$

Puesto que $\hat{N}_{\bar{\mathfrak{P}}_0} \supseteq \hat{k}_{\bar{\mathfrak{p}}} \supseteq \hat{\mathfrak{x}}$ ha de ser $\hat{N}_{\bar{\mathfrak{P}}_0} = \hat{k}_{\bar{\mathfrak{p}}}$.
Por otra parte $\hat{N}_{\bar{\mathfrak{P}}_0} \supseteq \hat{K}_{\mathfrak{P}_0} \supseteq \hat{\mathfrak{x}}$ y puesto que $\bar{\mathfrak{P}}_0$ ha ramificado en N/K es $\hat{K}_{\mathfrak{P}_0} = \hat{\mathfrak{x}}$.

Teniendo en cuenta [17] Cap.III §4 Cor. a Prop. 10, y que $\mathfrak{P}_o \subset A_K$ es el único primo que divide a $\mathfrak{p} \subset A$ y que ramifica en A_N es $\vartheta_{\hat{N}_{\bar{\mathfrak{P}}_o}/\hat{K}_{\mathfrak{P}_o}} = \vartheta_{N/K}$ donde $\vartheta_{N/K}$ representa el ideal de $(\hat{A}_K)_{\mathfrak{P}_o}$ generado por $\vartheta_{N/K}$. Por análoga razón es $\vartheta_{\hat{k}_{\bar{\mathfrak{p}}}/\hat{x}_{\mathfrak{p}}} = \vartheta_{k/x}$ donde $\vartheta_{k/x}$ representa el ideal de $\hat{A}_{\mathfrak{p}}$ generado por $\vartheta_{k/x}$.

Puesto que $\vartheta_{\hat{N}_{\bar{\mathfrak{P}}_o}/\hat{K}_{\mathfrak{P}_o}} = \vartheta_{\hat{k}_{\mathfrak{p}}/\hat{x}}$ resulta $\vartheta_{N/K} = \vartheta_{k/x}$.

<u>Teorema (4.4)</u>. $\vartheta_{K/x} = \vartheta_{k/x}^{1/2(p^n-1)}\, \mathfrak{J}^{p-1}$

En efecto:

$$\vartheta_{K/x}^{2}\, N_{K/x}(\vartheta_{N/K}) = \vartheta_{N/x} = \vartheta_{k/x}^{p^n}\, \mathfrak{J}^{2(p-1)}$$

En virtud de (4.3) es:

$$\vartheta_{K/x}^{2}\, \vartheta_{k/x} = \vartheta_{k/x}^{p^n}\, \mathfrak{J}^{2(p-1)}$$

lo que implica el enunciado del teorema.

<u>Teorema (4.5)</u>. <u>Sea</u> $\mathfrak{p}$ <u>un primo no nulo de</u> A. $\mathfrak{p}$ <u>ramifica en</u> K/x <u>si y sólo si</u> $\mathfrak{p}$ <u>divide a</u> $\vartheta_{K/x}$; <u>si</u> $\mathfrak{p}$ <u>divide a</u> $\vartheta_{k/x}$ <u>es</u> $\mathfrak{p} A_K = \mathfrak{P}_o^{p^i} \mathfrak{P}_1^{2p^i} \cdots \mathfrak{P}_{1/2(p^j-1)}^{2p^i}$ <u>con i y j fijos pudiendo tomar los valores</u> $0 \leq i \leq n-1$, $i+j = n$. <u>Si</u> $\mathfrak{p}$ <u>no divide a</u> $\vartheta_{k/x}$ <u>es</u> $\mathfrak{p} A_K = \mathfrak{P}_o^{p^i} \mathfrak{P}_1^{p^i} \cdots \mathfrak{P}_{p^j}^{p^i}$ <u>donde i y j son fijos y pueden tomar los valores</u> $1 \leq i \leq n-1$, $j+i = n$.

En efecto: Es evidente la primera proposición del teorema. Si $\mathfrak{p}$ divide a $\vartheta_{k/\varkappa}$ la expresión de $\mathfrak{p}\,A_K$ es la obtenida en (4.2. (2)). Si $\mathfrak{p}$ no divide a $\vartheta_{k/\varkappa}$ y ramifica en $K/\varkappa$ en virtud de (4.4) $\mathfrak{p}$ divide a $\mathcal{J}$ y por tanto ramifica en N/k. Puesto que $\mathfrak{p}$ no ramifica en $k/\varkappa$ se pueden presentar los dos casos siguientes:

a) $\mathfrak{p}\,A_k = \bar{\mathfrak{p}}_1 \bar{\mathfrak{p}}_2 \qquad \bar{\mathfrak{p}}_1 A_N = \bar{\mathfrak{P}}_1^{p_1^i} \bar{\mathfrak{P}}_2^{p_1^i} \cdots \bar{\mathfrak{P}}_p^{p_j^i}$ con $1 \leq i \leq n-1$, $i+j = n$

y puesto que $\bar{\mathfrak{p}}_2 = \tau \bar{\mathfrak{p}}_1$ es $\mathfrak{p}\,A_N = \bar{\mathfrak{P}}_1^{p_1^i} \tau \bar{\mathfrak{P}}_1^{p_1^i} \cdots \bar{\mathfrak{P}}_p^{p_j^i} \tau \mathfrak{P}_p^{p_j^i}$

y por tanto $\mathfrak{p}\,A_K = N_{N/K}(i\,\mathfrak{p})^{1/2} = \mathfrak{P}_1^{p_1^i} \cdots \mathfrak{P}_p^{p_j^i}$ donde

$\mathfrak{P}_r = N_{N/K}(\bar{\mathfrak{P}}_r) = N_{N/K}(\tau \bar{\mathfrak{P}}_r)$.

b) $\mathfrak{p}\,A_k = \bar{\mathfrak{p}} \qquad \mathfrak{p}\,A_N = \bar{\mathfrak{P}}_1^{p_1^i} \cdots \bar{\mathfrak{P}}_p^{p_j^i}$ con $1 \leq i \leq n-1$ $i+j = n$

Si $\mathfrak{P}$ es un primo no nulo de A_K que divide a $\mathfrak{p}$, en virtud de (4.1) $\mathfrak{P}$ no ramifica en N/K por tanto:

$\mathfrak{p}\,A_K = N_{N/K}(i\,\mathfrak{p})^{1/2} = N_{N/K}(\bar{\mathfrak{P}}_1^{p_1^i} \cdots \bar{\mathfrak{P}}_p^{p_j^i})^{1/2} = \mathfrak{P}_1^{p_1^i} \cdots \mathfrak{P}_p^{p_j^i}$

donde $N_{N/K}(\bar{\mathfrak{P}}_i) = \mathfrak{P}_i^2$ puesto que el grado residual $f_{\mathfrak{P}_i}$ es 2.

C A P I T U L O III

BASES NORMALES . CASO $2p^n$.

INTRODUCCION.- Se supone en este capítulo que A es un anillo de Dedekind de cuerpo de fracciones $\mathfrak{X}$, y N una extensión de $\mathfrak{X}$ galoisiana, de grupo de Galois G, finito; K es una subextensión de N, no galoisiana sobre $\mathfrak{X}$ cuya clausura galoisiana es N. Se generaliza la conocida definición de base normal en cuerpos que son extensiones galoisianas finitas, al caso de extensiones no galoisianas finitas. Se da una definición de A-base normal del anillo A_N de los enteros de N, y una definición de base normal y base casi normal para las clausuras enteras de A de subextensiones no galoisianas de N. Se particulariza finalmente al caso en que G sea diedral de orden $2p^n$, y se da para este caso una definición de H-base para el anillo de los enteros A_K de K. En la hipótesis de existencia de H-bases para A_K e imponiendo al anillo A y a la extensión $N/\mathfrak{X}$ algunas condiciones complementarias, se demuestra que el anillo de los enteros A_N de N es $A[G]$-libre, siendo G el grupos de Galois de la extensión $N/\mathfrak{X}$. De la existencia de H-bases se tratará en el capítulo IV.

1. DEFINICIONES Y RESULTADOS PREVIOS

Proposición (1.1). Sea K un cuerpo extensión separable finita de $\mathfrak{x}$, N la clausura galoisiana de K sobre $\mathfrak{x}$, G el grupo de Galois de N sobre $\mathfrak{x}$,y g el subgrupo de G que deja fijo K. Se supone $[N:\mathfrak{x}] = n$ y $[K:\mathfrak{x}] = m$. Sea $\theta \in N$ tal que $N = \mathfrak{x}[G]\text{-}\theta$ y sea (σ_i) un sistema de representantes de las clases por la derecha de G, módulo g. Entonces $\theta_i = \mathrm{Tr}_{N/K}(\sigma_i\theta)$ forma una $\mathfrak{x}$-base de K, (es decir, una base de K como espacio vectorial sobre $\mathfrak{x}$).

En efecto: Sea $\alpha \in K$. Es $\alpha = \sum_{j=1}^{n} \lambda_j \rho_j(\theta)$ donde $\rho_j \in G$ y $\lambda_j \in \mathfrak{x}$, puesto que $K \subset N$. Agrupando los sumandos por clases por la derecha módulo g de G, se tiene:

$$\alpha = \sum_{i=1}^{n:m} \left(\sum_{j=1}^{m} \lambda_{ij} \tau_i \sigma_j (\theta) \right) \qquad \tau_i \in g$$

y por ser K fijo por g resulta:

$$\alpha = \tau_h \alpha = \sum_{i=1}^{n:m} \left(\sum_{j=1}^{m} \lambda_{ij} \tau_h \tau_i \sigma_j (\theta) \right)$$

para todo $\tau_h \in g$. Puesto que θ es una $\mathfrak{x}$-base normal de N las λ_{ij} que corresponden a un mismo valor de j son iguales entre si. Se tiene pues para cada $\alpha \in K$,

$$\alpha = \sum_{j=1}^{m} \left(\sum_{i=1}^{n:m} \tau_i \right) \lambda_j \sigma_j(\theta) = \sum_{j=1}^{m} \lambda_j \mathrm{Tr}_{N/K}(\sigma_j \theta) .$$

Evidentemente, los elementos $\theta_j = \sum_{i=1}^{n:m} \tau_i(\sigma_j\theta)$ son linelamente independientes sobre $\mathfrak{x}$.

Definición (1.2). La $\mathfrak{x}$ -base de K formada por los elementos $\theta_i \in K$ definidos en la proposición (1.1) se denomina una base normal de K.

Definición (1.3). Con las hipótesis de (1.1), sea $\theta \in N$ tal que $Tr_{N/K}(\sigma_i\theta) = \theta_i$ es una $\mathfrak{x}$-base de K, pero sin que θ sea una base normal de N sobre $\mathfrak{x}$. Entonces se dice que los θ_i forman una base pseudo-normal de K sobre $\mathfrak{x}$.

Definición (1.4). Sea A un anillo de Dedekind de cuerpo de fracciones $\mathfrak{x}$, y N una extensión galoisiana finita de grupo de Galois G. Sea A_N la clausura entera de A en N. Si existe un $\theta \in A_N$ tal que $A_N = A[G]-\theta$, entonces se dice que θ es una A-base normal de A_N. Es decir, A_N posee una A-base normal si como $A[G]$-módulo es isomorfo a $A[G]$.

Definición (1.5). Sea A un anillo de Dedekind de cuerpo de fracciones $\mathfrak{x}$, K una extensión separable finita de $\mathfrak{x}$, A_K la clausura entera de A en K y N una clausura galoisiana de K. Si existe un $\theta \in N$ tal que $N = \mathfrak{x}[G]-\theta$, y un sistema de representantes (σ_i) de clases de restos por la derecha del grupo $G(N/\mathfrak{x})$ de Galois de N sobre $\mathfrak{x}$, módulo el grupo $G(N/K)$ de Galois de N sobre K, tales que $Tr_{N/K}(\sigma_i\theta) = \theta_i$ forman una A-base de A_K , se dice que las θ_i forman una

A-base normal de A_K.

Definición (1.6). Si se cumplen todas las condiciones de la definición (1.5), salvo la de ser $N = x[G]-\theta$, se dice entonces que las θ_i forman una base pseudo-normal de A_K respecto A.

Definición (1.7). Con las mismas notaciones de (1.5), si existe un $\theta \in N$ tal que $N = x[G]-\theta$ y un sistema (σ_i) de representantes de clases por la derecha de $G(N/x)$ módulo $G(N/K)$ tales que $1, Tr_{N/K}(\sigma_2\theta) = \theta_2, \ldots, Tr_{N/K}(\sigma_s\theta) = \theta_s$, $s=n:m$ forman una A base de A_K, se dice que $(1, \theta_2, \ldots, \theta_s)$ es una A base casi normal de A_K.

Proposición (1.8). Si A_K admite una base normal sobre A, A_K admite también una base casi normal sobre A.

En efecto: Si $\theta_1, \theta_2, \ldots, \theta_s$ es una A-base normal de A_K, entonces $1, \theta_2, \ldots, \theta_s$ es una A base casi normal de A_K. Pues:

$$1 \in A_K \Rightarrow 1 = \sum_{i=1}^{s} a_i \theta_i \qquad a_i \in A,$$

y por ser 1 fijo por los automorfismos de $G(N/x)$ los a_i han de ser todos iguales entre si, es decir $1 = a\sum_{i=1}^{s}\theta_i$ $a \in A$.

Además $\sum_{i=1}^{s}\theta_i = \sum_{i=1}^{s} Tr_{N/K}\,\sigma_i(\theta) = \sum_{i=1}^{s}\sum_{j=1}^{m}\tau_j\sigma_i\theta = Tr_{N/x}(\theta)$.

Puesto que $\sum_{i=1}^{s}\theta_i \in A_K$ y $Tr_{N/x}(\theta) \in x$ es $\sum_{i=1}^{s}\theta_i \in A_K \cap x = A$.

Por tanto $\sum_{i=1}^{s}\theta_i \in A \Rightarrow a$ es un elemento inversible de A , y

$(1, \theta_2, \ldots, \theta_s)$ es una A-base de A_K.

Observación: El recíproco de (1.8) en general no es cierto. Un contraejemplo se encuentra en [10] Cap.III § 8 nota.

Proposición (1.9). En las hipótesis de (1.5), si A_K posee una A-base normal, las trazas sobre $\mathfrak{x}$ de los elementos de esta base son elementos inversibles de A, y por tanto $Tr_{K/\mathfrak{x}}(A_K)=A$.

En efecto:

$$Tr_{K/\mathfrak{x}}(\theta_i) = Tr_{K/\mathfrak{x}}(Tr_{N/K}\sigma_i(\theta)) = Tr_{N/\mathfrak{x}}(\sigma_i\theta)$$

y en la demostración de (1.8) se ha visto que $Tr_{N/\mathfrak{x}}(\sigma_i\theta) = \sum\theta_i$ y que $\sum\theta_i$ es un elemento inversible de A.

Proposición (1.10). En las hipótesis de (1.5), sean K y k dos subextensiones de N linealmente disjuntas sobre $\mathfrak{x}$; si A_K y A_k poseen A-bases normales, entonces $N/\mathfrak{x}$ es moderadamente ramificada.

En efecto: Si A_K y A_k poseen A-bases normales, en virtud de (1.9) es $Tr_{K/\mathfrak{x}}(A_K) = A$ y $Tr_{k/\mathfrak{x}}(A_k) = A$, por tanto existen $\varphi\in A_K$ y $\omega\in A_k$ tales que $Tr_{k/\mathfrak{x}}(\omega) = 1$ y $Tr_{K/\mathfrak{x}}(\varphi) = 1$. Entonces $Tr_{N/\mathfrak{x}}(\varphi\omega) = 1$, y puesto que $\varphi\omega\in A_N$, $Tr_{N/\mathfrak{x}}(A_N)=A$ y N es moderadamente ramificada sobre $\mathfrak{x}$.

Proposición (1.11). Sea $N/\mathfrak{x}$ galoisiana de grupo de Galois G diedral de orden 2n (n impar), H el subgrupo cíclico de G de orden n, g un subgrupo de orden 2, K el cuerpo fijo por g, A_K la clausura entera de A en K. Entonces, si A_K posee una

A-base pseudo normal y la característica de $\mathfrak{x}$ es distinta de dos y de los primos que dividen a n, A_K posee una A-base normal.

En efecto: Sea $\theta \in N$ tal que $\theta_i = \sigma^{-i}\theta + \tau\sigma^{-i}\theta \quad 0 \leq i \leq n-1$ forman una A-base pseudo-normal de A_K. Por (1,6), entre θ y sus conjugados por G existe una relación de la forma:

$$\sum_{j=0}^{n-1} a_j \sigma^j \theta + a'_j \tau \sigma^j \theta = 0 \qquad a_j, a'_j \in \mathfrak{x} \text{ no todos nulos.}$$

Haciendo operar sobre esta relación $(1 + \tau)\sigma^{-i} \quad 0 \leq i \leq n-1$, se tienen n relaciones de la forma (con subíndices calculados mod n

$$\sum_{j \bmod n} (a_{j-i} + a'_{j+i})(1 + \tau)\sigma^j \theta = 0$$

que pueden escribirse en la forma:

$$\sum_{j \bmod n} (a_{j-i} + a'_{j+i})\theta_j = 0 \qquad a_{j-i} + a'_{j+i} \in \mathfrak{x}$$

Puesto que θ_i son linealmente independientes sobre $\mathfrak{x}$, es $a_{j-i} + a'_{j+i} = 0$ para $i, j = 0, 1, \ldots, n-1$. De estas igualdades resulta: $-a'_i = a_i = a_o$ para $0 \leq i \leq n-1$. Por tanto:

$$a_o \neq 0 \quad \text{y} \quad a_o(1-\tau)\sum_{j=0}^{n-1} \sigma^j \theta = 0 \quad \Rightarrow \quad (1-\tau)\sum_{j=0}^{n-1} \sigma^j \theta = 0.$$

Sea $\lambda \in A_k$ no nulo tal que $\mathrm{Tr}_{k/\mathfrak{x}}(\lambda) = 0$ y $\theta' = \theta + \lambda$. Poniendo $\theta'_i = \sigma^i \theta' + \tau\sigma^i \theta'$, es $\theta'_i = \theta_i$ y,

$$\sum_{j=0}^{n-1} a_o(1-\tau)\sigma^j \theta' = 2a_o n \lambda.$$

Puesto que $a_o \neq 0$ y $\lambda \neq 0$, si la característica de $\mathcal{K}$ es distinta de dos y de los divisores primos de n, $2a_o n \lambda \neq 0$ y θ'_i es una A-base normal de A_K.

Definición (1.12) En las condiciones de (1.11) y suponiendo $n \geqslant 5$, se dice que un par (φ, ψ) de elementos de A_K es una H-base de A_K, si los n elementos: $1, \varphi, \psi, \sigma^i\varphi + \sigma^{-i}\varphi$, $\sigma^i\psi + \sigma^{-i}\psi$, $1 \leq i \leq (n-3)/2$ donde σ es un generador de H, forman una A-base de A_K.

Nota: El caso n=3 ha sido estudiado en [11].

Proposición (1.13). Sea A un anillo de Dedekind semi-local de cuerpo de fracciones $\mathcal{K}$, L una extensión galoisiana de grupo de Galois G, B la clausura entera de A en L, si L es moderadamente ramificada sobre $\mathcal{K}$, y la característica de $\mathcal{K}$ no divide al orden de G, entonces B es A[G]-libre.

Demostración: [12] Cap:II 6 Cor.

Proposición (1.14). Sea A un anillo principal y $\mathcal{K}$ su cuerpo de fracciones. N una extensión de $\mathcal{K}$ galoisiana de grupo de Galois diedral de orden 2p (p primo impar). K un subcuerpo de grado p de N, y k el subcuerpo cuadrático. Si la característica de $\mathcal{K}$ no divide 2p, si A/pA es isomorfo a Z/pZ y A_k y A_K poseen A-bases normales, entonces A_N es A[G]-libre.

Demostración: [12] Teor. VI.5.

2. BASES NORMALES DE A_K. CASO $2p^n$.

En este párrafo las notaciones son las de (II.1.1) y el anillo A se supone en algún caso que se indica, o principal o A/p^nA finito

Proposición (2.1). Si A_K posee una H-base (1.12), entonces:

a). si p es inversible en A, A_K posee una H-base (φ, ψ) tal que $Tr_{K/\mathfrak{X}}(\varphi) = Tr_{K/\mathfrak{X}}(\psi) = 1$.

b) si pA es un ideal maximal de A, A principal o A/p^nA finito

1) Si K es moderadamente ramificada en cada primo $\mathfrak{P}$ de A_K que divide a pA_K, sobre $\mathfrak{X}$, A_K posee una H-base (φ, ψ) tal que $Tr_{K/\mathfrak{X}}(\varphi) = Tr_{K/\mathfrak{X}}(\psi) = 1$.

2) Si K no es moderadamente ramificada sobre $\mathfrak{X}$ en ningún primo $\mathfrak{P}$ que divide a pA_K, A_K posee una H-base (φ, ψ), tal que $Tr_{K/\mathfrak{X}}(\varphi) = Tr_{K/\mathfrak{X}}(\psi)$ y puede ser 0 ó p^i donde $1 \leq i \leq n$.

Demostración:

a). Sea (φ', ψ') una H-base de A_K, con $Tr_{K/\mathfrak{X}}(\varphi') = T$ y $Tr_{K/\mathfrak{X}}(\psi') = U$, donde $T, U \in A$. Puesto que p es inversible en A, $T/p^n \in A$ y $U/p^n \in A$. Se consideran los elementos $\varphi = \varphi' - T/p^n + 1/p^n$ $\psi = \psi' - U/p^n + 1/p^n$ que evidentemente forman una H-base de A_K, y se tiene, $Tr_{K/\mathfrak{X}}(\varphi) = Tr_{K/\mathfrak{X}}(\psi) = 1$.

b) Si pA es maximal en A, pA es primo en A, y teniendo en cuenta las expresiones obtenidas en la demostración de (II,4,2),

se pueden presentar sólo los dos casos siguientes:

1) K es moderadamente ramificada en cada primo $\mathfrak{P}$ de A_K que divide a pA_K, sobre $\mathfrak{x}$.

2) K no es moderadamente ramificada sobre $\mathfrak{x}$ en ningún primo $\mathfrak{P}$ de A_K que divide pA_K

1) En este caso es $Tr_{K/\mathfrak{x}}(A_K) = A$. Sea $Tr_{K/\mathfrak{x}}(\varphi') = T$ y $Tr_{K/\mathfrak{x}}(\psi') = U$. Se tiene $Tr_{K/\mathfrak{x}}(1) = p^n$,

$Tr_{K/\mathfrak{x}}(\sigma^i(\varphi') + \sigma^{-i}(\varphi')) = 2T$ $Tr_{K/\mathfrak{x}}(\sigma^i(\psi') + \sigma^{-i}(\psi')) = 2U$,

por tanto, U , T, p^n son generadores del ideal $Tr_{K/\mathfrak{x}}(A_K) = A$, y por consiguiente ó U, ó T no pertenecen a pA. Sea T por ejemplo el que no pertenece a pA. Entonces, existen $a,b \in A$ tales que $aT + bp^n = 1$. Poniendo $\psi'' = \psi' - aU\varphi' - bU + 1$ se tiene: $Tr_{K/\mathfrak{x}}(\psi'') = p^n$, y puesto que

$\sigma^i(\psi') + \sigma^{-i}(\psi') = \sigma^i(\psi'') + \sigma^{-i}(\psi'') + aU(\sigma^i\varphi' + \sigma^{-i}\varphi') + 2bU - 2$,

(φ', ψ'') forma una H-base de A_K. Poniendo ahora:

$$\varphi = a\varphi' + b\psi''$$
$$\psi = (a - p^n)\varphi' + (b + T)\psi''$$

se obtiene una H-base (φ, ψ) tal que $Tr_{K/\mathfrak{x}}(\varphi) = Tr_{K/\mathfrak{x}}(\psi) = 1$. En efecto:

$$\sigma^i\varphi + \sigma^{-i}\varphi = a(\sigma^i\varphi' + \sigma^{-i}\varphi') + b(\sigma^i\psi'' + \sigma^{-i}\psi'')$$
$$\sigma^i\psi + \sigma^{-i}\psi = (a - p^n)(\sigma^i\varphi' + \sigma^{-i}\varphi') + (b + T)(\sigma^i\psi'' + \sigma^{-i}\psi'').$$

Pero $\begin{vmatrix} a & b \\ a-p^n & b+T \end{vmatrix} = 1$,

por tanto, se pueden expresar $(\sigma^i\varphi' + \sigma^{-i}\varphi')$, $(\sigma^i\psi'' + \sigma^{-i}\psi'')$ como combinación lineal de $(\sigma^i\varphi + \sigma^{-i}\varphi)$, $(\sigma^i\psi + \sigma^{-i}\psi)$ a coeficientes en A, por lo cual, $1, \varphi, \psi, \sigma^i\varphi + \sigma^{-i}\varphi, \sigma^i\psi + \sigma^{-i}\psi$ $1 \leq i \leq (p^n-3)/2$ forman una A-base de A_K, es decir, (φ, ψ) es una H-base, con $Tr_{K/\mathfrak{X}}(\varphi) = Tr_{K/\mathfrak{X}}(\psi) = 1$.

2. En este caso es $Tr_{K/\mathfrak{X}}(A_K) \neq A$.(Ver nota al final de la proposición). Se tiene:

$$Tr_{K/\mathfrak{X}}(1) = p^n \Rightarrow Tr_{K/\mathfrak{X}}(A_K) \supset p^n A$$

y puesto que pA es maximal y por tanto primo, $Tr_{K/\mathfrak{X}}(A_K) = p^i A$ donde i es un número fijo comprendido entre 1 y n . Si $i=n$ $U \in p^n A$ y $T \in p^n A \Rightarrow U/p^n \in A$ y $T/p^n \in A$. Haciendo :

$\varphi = \varphi' - T/p^n$ $\quad \psi = \psi' - U/p^n$, evidentemente (φ, ψ) es una H-base de A_K tal que $Tr_{K/\mathfrak{X}}(\varphi) = Tr_{K/\mathfrak{X}}(\psi) = 0$.

Si $i < n$, puesto que p^n , T , U generan $Tr_{K/\mathfrak{X}}(A_K)$ ocurre que ó T ó U pertenecerán a $p^i A$ y no pertenecerán a $p^{i+1} A$. Sea por ejemplo T. Entonces T y p^n generan $p^i A$ y por tanto existen $a, b \in A$ tales que $aT + bp^n = p^i$. Poniendo $p^i T' = T$ es $aT' + bp^{n-i} = 1$. Sea $U = U' p^i$. Se define:

$$\psi'' = \psi' - aU'\varphi' + bU' + 1$$

y se tiene $Tr_{K/\mathfrak{X}}(\psi'') = p^n$.

Poniendo

$$\left.\begin{aligned} \varphi &= a\varphi' + b\psi'' \\ \psi &= (a - p^{n-i})\varphi' + (b + T')\psi'' \end{aligned}\right\}$$

se conprueba que (φ, ψ) constituye una H-base de A_K ya que

$$\begin{vmatrix} a & b \\ a-p^{n-i} & b+T' \end{vmatrix} = 1$$

y se tiene:

$$Tr_{K/\mathfrak{x}}(\varphi) = Tr_{K/\mathfrak{x}}(\psi)) = p^i \quad .$$

Nota: En el caso 2b de la proposición anterior se puede asegurar que $Tr_{K/\mathfrak{x}}(A_K) \neq A$ en virtud del hecho siguiente:

La traza de $K/\mathfrak{x}$ de A_K es exhaustiva si y sólo si para todo ideal primo $\mathfrak{p}$ de A, existe un ideal primo $\mathfrak{P}$ de A_K que divide a $\mathfrak{p} A_K$, tal que la extensión $K/\mathfrak{x}$ es moderadamente ramificada en $\mathfrak{P}$.

Para su demostración ver: [3] 1 Prop 1.

Proposición (2.2). Si A_K posee una H-base con $Tr_{K/\mathfrak{x}}(\varphi) = Tr_{K/\mathfrak{x}}(\psi)$ entonces A_K posee una base casi-normal, y recíprocamente.

Para la demostración de esta proposición se requieren los siguientes lemas previos:

Lema (2.3). Sea M un sub-A[G]-módulo proyectivo de A_N que contiene A_K y A_k y sean φ y ψ dos elementos de A_K que tie-

nen la misma traza sobre $\mathfrak{X}$, entonces existe un elemento $\theta \in M$ tal que $Tr_{N/K}(\theta) = \varphi$ y $Tr_{N/K}(\sigma\theta) = \psi$

Demostración:

M es $A[G]$-proyectivo $\Rightarrow$ M cohomologicamente trivial.

Se considera primero el caso $\varphi = 0$. Entonces $Tr_{K/\mathfrak{X}}(\varphi)) = Tr_{K/\mathfrak{X}}(\psi)) = 0$. Puesto que M es cohomologicamente trivial y $A_K \subset M$ es el conjunto de los elementos de M fijos por g, si I_G designa el ideal de aumentación de $Z[G]$ y $\hat{H}^o$ y $\hat{H}_o$ los grupos de cohomología modificados en el sentido de Tate de índice 0, [17] Cap VII §1, se tiene:

$$\hat{H}^o(g, M) = {}^{A_K}/_{Tr_{N/K}(M)} = 0 \Longrightarrow A_K = Tr_{N/K}(M) .$$

Puesto que $\psi \in A_K$ existe un $u \in M$ tal que $\psi = Tr_{N/K}(u)$ y tal que

$$Tr_{N/\mathfrak{X}}(u) = Tr_{K/\mathfrak{X}}(Tr_{N/K}(u)) = Tr_{K/\mathfrak{X}}(\psi) = 0.$$

$$A_k \subset M \Longrightarrow Tr_{N/k}(u) \in A_k$$

$$Tr_{k/\mathfrak{X}}(Tr_{N/k}(u)) = 0 \Longrightarrow Tr_{N/k}(u)) \in \ker (Tr_{k/\mathfrak{X}}(A_k))$$

$$\hat{H}_o(g, A_k)) = \ker (Tr_{k/\mathfrak{X}}(A_k)) \,/\, I_g A_k = 0 \Rightarrow$$

$$\ker (Tr_{k/\mathfrak{X}}(A_k))) = I_g A_k .$$

Por tanto, existe un $v \in A_k$ tal que $Tr_{N/k}(u) = v - \tau v$.

$\hat{H}^0(H,M) = {}^{A_k}/_{\mathrm{Tr}_{N/k}(M)} = 0 \Rightarrow A_k = \mathrm{Tr}_{N/k}(M) \Rightarrow$ existe $\omega \in M$ tal que $\mathrm{Tr}_{N/k}(\omega) = v$. Por tanto $\mathrm{Tr}_{N/k}(u-(\omega - \tau\omega)) = 0$.

$\hat{H}_0(H,M) = {}^{\ker(\mathrm{Tr}_{N/k}(M))}/_{I_H M} = 0 \Rightarrow u - (\omega - \tau\omega) \in I_H M$

Puesto que H es cíclico, $I_H M$ es de la forma $(\sigma - 1)M$ donde σ es un generador de H, y puesto que 2 no divide a p, σ^2 es también un generador de H, por tanto $I_H M = (\sigma - \sigma^{-1})M$. Existe pues un elemento $\theta' \in M$ que verifica $u - (\omega - \tau\omega) = (\sigma - \sigma^{-1})\theta'$. Poniendo $\theta = \theta' - \tau\theta'$, evidentemente es $\mathrm{Tr}_{N/K}(\theta) = 0$ y $\mathrm{Tr}_{N/K}(\sigma\theta) = \psi$.

Si $\varphi \neq 0$, puesto que $\hat{H}^0(g,M) = 0$ y $\varphi \in A_K$, existe un elemento $\theta' \in M$ tal que $\mathrm{Tr}_{N/K}(\theta') = \varphi$. Sea $\psi' = \mathrm{Tr}_{N/K}(\sigma\theta')$. Es $\mathrm{Tr}_{K/\mathbb{Q}}(\psi - \psi') = 0$. En virtud del caso anterior, se puede encontrar un $\theta'' \in M$ tal que $\mathrm{Tr}_{N/K}(\theta'') = 0$ y $\mathrm{Tr}_{N/K}(\sigma\theta'') = \psi - \psi'$. Poniendo $\theta = \theta' + \theta''$ es inmediato que $\mathrm{Tr}_{N/K}(\theta) = \varphi$ y $\mathrm{Tr}_{N/K}(\sigma\theta) = \psi$.

Lema (2.4). El elemento θ determinado en (2.3)) es único salvo la suma de un elemento de A_k de traza nula sobre $\mathbb{Q}$.

En efecto: Sean θ y θ' dos posibles soluciones, y $\lambda = \theta - \theta'$ Puesto que $\mathrm{Tr}_{N/K}(\theta) = \mathrm{Tr}_{N/K}(\theta') = \varphi$ y $\mathrm{Tr}_{N/K}(\sigma\theta) = \mathrm{Tr}_{N/K}(\sigma\theta') = \psi$, se tiene: $\lambda + \tau\lambda = 0$ y $\sigma\lambda + \tau\sigma\lambda = 0$, y como consecuencia $\lambda = \sigma^2\lambda$ y por tanto $\lambda \in A_k$.

Obsérvese que en las demostraciones de (2.3) y (2.4) no interviene en ningún momento cuál sea el entero n que determina el grado 2n de la extensión, y por tanto son las mismas dadas en [12] para el caso $n = p$. Sin embargo, dada la importancia de los mismos, se ha creido necesario el repetirlas aquí.

Corolarios a los lemas (2.3) y (2.4) son los siguientes:

Corolario (2.5). Si $N/\mathfrak{x}$ es moderadamente ramificada y φ, ψ son dos elementos de A_K que tienen la misma traza sobre $\mathfrak{x}$ existe un $\theta \in A_N$ tal que $Tr_{N/K}(\theta) = \varphi$ y $Tr_{N/K}(\sigma\theta) = \psi$. Dos elementos $\theta, \theta' \in A_N$ que cumplan estas condiciones, difieren en un elemento λ de traza nula sobre A.

Corolario (2.6). Si φ, ψ son dos elementos de K que tienen la misma traza sobre $\mathfrak{x}$, existe un elemento $\theta \in N$ tal que $Tr_{N/K}(\theta) = \varphi$, $Tr_{N/K}(\sigma\theta) = \psi$, y dos elecciones distintas de θ difieren en un elemento de k de traza nula sobre $\mathfrak{x}$.

Demostración de la proposición (2.2).

En virtud de (2.6), existe un $\theta \in N$ tal que $\theta + \tau\theta = \varphi$ $\sigma\theta + \tau\sigma\theta = \psi$. Poniendo $\theta_i = \sigma^i\theta + \tau\sigma^{-i}\theta$ se tieme $\theta_o = \varphi$, $\theta_1 = \psi$, $\sigma^i\varphi + \sigma^{-i}\varphi = \theta_i + \theta_{-i}$ $\sigma^i\psi + \sigma^{-i}\psi = \theta_{i+1} + \theta_{-i+1}$ con $1 \leq i \leq (p^n-3)/2$, por tanto, los elementos de la H-base se expresan por medio de 1 y de θ_i linealmente. Estas mismas fórmulas permiten cal-

cular las θ_i linealmente en función de los elementos de la H-base.

Proposición (2.7). Si A_K posee una H-base y se cumplen las condiciones de (2.1.) , entonces A_K posee A-bases normales. Si además $N/\mathcal{K}$ es moderadamente ramificada, A_K posee bases normales sobre A formadas a partir de un elemento de A_N.

En efecto: Sea (φ', ψ') una H-base de A_K. Si $K/\mathcal{K}$ es moderadamente ramificada en p, en virtud de (2.1.) se puede encontrar una H-base (φ, ψ) tal que $Tr_{K/\mathcal{K}}(\varphi) = 1$. En virtud de (2.2) A_K posee una base casi normal y sea $\theta \in N$ el elemento que determina dicha base. Se observa que en esta base casi normal aparecen todos los subíndices comprendidos entre 0 y p^{n-1} salvo el que corresponde a $i = (p^n+1)/2$. Pero, $\theta_{(p^n+1)/2} = \theta_{-(p^n-1)/2} = (1+\tau)(\sigma^{(p^n+1)/2}\theta)$ y $1 = Tr_{K/\mathcal{K}}(\varphi) = Tr_{K/\mathcal{K}}(\theta + \tau\theta) = (1+\tau)\sum_{i=0}^{p^n-1}\sigma^i\theta$, permiten expresar $\theta_{(p^n+1)/2}$ como combinación lineal de 1 y θ_i con $0 \leq i \leq p^n-1$ y $i \neq (p^n+1)/2$.

Si además $N/\mathcal{K}$ es moderadamente ramificada, en virtud de (2.5) θ se puede tomar en A_N.

Proposición (2.8). Sea $\theta \in N$ tal que los $\theta_i = \sigma^i\theta + \tau\sigma^i\theta$ $0 \leq i \leq p^n-1$ forman una A-base normal de A_K , y $u, v \in A[G]$.

Si $(u\theta)_i = \sigma^i(u\theta) + \tau\sigma^i(u\theta)$ y $(v\theta)_i = \sigma^i(v\theta) + \tau\sigma^i(v\theta)$ $0 \leq i \leq p^n-1$ forman A-bases normales de A_K, $(u\theta)_i = (v\theta)_i$ si y sólo si $u - v = a_o(1-\tau)\sum_{j \bmod p^n} \sigma^j$ con $a_o \in A$.

En efecto: $(u\theta)_i = (v\theta)_i$ si y sólo si $(1+\tau)\sigma^{-i}(u-v)\theta = 0$ $0 \leq i \leq p^n-1$. Puesto que u y v pertenecen a $A[G]$ y los elementos de $A[G]$ son de la forma $\sum_{i=o}^{p^n-1} (a_i + a_i'\tau)\sigma^i$, $a_i, a_i' \in A$ es $u - v = \sum_{i=o}^{p^n-1} (a_i + a_i'\tau)\sigma^i$. Por tanto:

$$(u\theta)_i = (v\theta)_i \iff \sum_{j \bmod p^n} (a_{j-i} + a_{j+i}')(1+\tau)\sigma^j\theta = 0$$

y esto tiene lugar si y sólo si $a_i = -a_i' = a_o$ con $0 \leq i \leq p^n-1$, y por tanto u-v ha de ser de la forma $u - v = a_o(1-\tau)\sum_{j \bmod p^n} \sigma^j$ con $a_o \in A$.

Se trata pues ahora de estudiar el comportamiento en el anillo $A[G]$ de los elementos de la forma $a_o(1-\tau)\sum_{j \bmod p^n} \sigma^j$. Se comprueba por cálculo directo que $(1-\tau)\sum_{j=o}^{p^n-1} \sigma^j$ y $\sum_{j=o}^{p^n-1} \sigma^j$ son elementos del centro de $A[G]$ y que $A(1-\tau)\sum_{i=o}^{p^n-1} \sigma^i$ es un ideal bilátero de $A[G]$. Se considera el álgebra $\mathcal{O}$ definida por $\mathcal{O} = A[G] / A(1-\tau)\sum_{i=o}^{p^n-1} \sigma^i$ con lo cual la proposición (2.8) se puede expresar en la forma:

$(u\theta)_i = (v\theta)_i \iff u, v \in A[G]$ representan el mismo elemento de $\mathcal{O}$.

Nota: Para un estudio más detallado del álgebra $\mathcal{O}_L$ ver [12] Cap. VI § 3 .

Proposición (2.9). Sea $\theta \in N$ tal que los $\theta_i = \sigma^i\theta + \tau\sigma^i\theta$ $0 \leq i \leq p^n-1$ forman una A-base normal de A_K, y u un elemento de $A[G]$. $(u\theta)_i = \sigma^i(u\theta) + \tau\sigma^i(u\theta)$ es una A-base normal de A_K, si y sólo si la imagen $\bar{u}$ de u en $\mathcal{O}_L$ es un elemento inversible de $\mathcal{O}_L$.

En efecto:

a) Para probar que es suficiente, basta ver que si $\bar{u}$ es inversible en $\mathcal{O}_L$, las θ_i se pueden expresar como combinación lineal de las $(u\theta)_i$ a coeficientes en A. Y esto ocurre ya que: si $\bar{u}$ es inversible en $\mathcal{O}_L$, existe un v perteneciente a $A[G]$ tal que $vu = 1 + a(1-\tau)\sum_{i=0}^{p^n-1}\sigma^i$ con $a \in A$, y por tanto $(vu\theta)_i = \theta_i$. Puesto que $v = \sum_{j \bmod p^n}(a_j + a'_j\tau)\sigma^j$ con a_j , $a'_j \in A$ es :

$$\theta_i = (1+\tau)\sigma^i v(u\theta) = (1+\tau)\sigma^i \sum_{j \bmod p^n}(a_j + a'_j\tau)\sigma^j(u\theta) = \sum_{j \bmod p^n}(a_{j-i} + a'_{j+i})(u\theta)_j \quad \text{con} \quad a_{j-i} + a'_{j+i} \in A.$$

b) Para probar que es necesaria, se considera el conjunto U formado por los elementos $\bar{u} \in \mathcal{O}_L$ que son inversibles, y el conjunto $\mathcal{B}$ formado por las A-bases normales de A_K. Se define una aplicación Π de U en $\mathcal{B}$ de la siguiente manera: Sea $\theta \in N$

un elemento fijo tal que los Θ_i correspondientes formen una A-base normal de A_K. Para cada $\bar{u} \in U$ es $\Pi(\bar{u}) = (u\Theta)_i$ que en virtud de lo demostrado en a) es un elemento de $\mathfrak{B}$. Que Π es una aplicación es evidente en virtud de (2.8). Se prueba:

1) Π es exhaustiva

Sea $B' \in \mathfrak{B}$, y $\Theta' \in N$ una $\mathfrak{o}[G]$-base de N tal que los Θ'_i forman la base B'. Puesto que Θ y Θ' son $\mathfrak{o}[G]$-bases de N, existen dos elementos u, $u' \in \mathfrak{o}[G]$ inversos uno del otro tales que $\Theta' = u\Theta$ y $\Theta = u'\Theta'$. Se tiene:

$$\Theta'_i = (1+\tau)\sigma^i(u\Theta) = \sum_{i=0}^{p^n-1} (a_{j-i}+a'_{j+i})\Theta_i \qquad a_{j-i}+a'_{j+i} \in \mathfrak{o}$$

Puesto que los Θ'_i pertenecen a A_K y $\Theta_i \in A_K$ forman una A-base de A_K, $a_{j-i}+a'_{j+i} \in A$ para todo i comprendido entre 0 y p^n-1, por tanto para todos estos valores de i es $(1+\tau)\sigma^i(u)$ un elemento de $A[G]$. Analogamente $(1+\tau)\sigma^i(u') \in A[G]$. En virtud de [12] §3 Prop. VI 5, existen elementos $v, v' \in A[G]$ tales que

$$(1+\tau)\sigma^i(u) = (1+\tau)\sigma^i(v) \qquad (1+\tau)\sigma^i(u') = (1+\tau)\sigma^i(v')$$

para todo i comprendido entre 0 y p^n-1. Se tiene pues un elemento $v \in A[G]$ tal que $\Theta'_i = (v\Theta)_i$ $0 \leq i \leq p^n-1$ y bastará con probar que $\bar{v}$ es inversible en $\mathfrak{A}$. Puesto que $uu' = 1$ es $vv' - uu' = vv' - 1 \in A[G]$. Ya que $u - v$ y $u' - v'$ son elementos de $\mathfrak{o}[G]$ se comprueba facilmente que son de la forma $\lambda(1-\tau)\sum_{i=0}^{p^n-1}\sigma^i$ con $\lambda \in \mathfrak{o}$ y se tiene:

$uu' = vv' + \mu(1-\tau)\sum_{i=0}^{p^n-1}\sigma^i \qquad \mu \in \mathfrak{x}$, es decir:

$uu' - vv' \in A[G] \cap \mathfrak{x}(1-\tau)\sum_{i=0}^{p^n-1}\sigma^i = A(1-\tau)\sum_{i=0}^{p^n-1}\sigma^i$

Por tanto, $vv' = 1 + a(1-\tau)\sum_{i=0}^{p^n-1}\sigma^i$, es decir $\overline{v}$, es inversible en $\mathfrak{O}$. La base $B' \in \mathfrak{B}$ tiene por tanto como antiimagen por Π en U por lo menos $\overline{v}$.

2. Π es inyectiva.

Sean $\overline{u}$, $\overline{v}$ dos elementos de U con la misma imagen por Π en $\mathfrak{B}$ y sean u , v respectivos representates de ellos en $A[G]$. Para todo i comprendido entre 0 y p^n-1 ha de ser

$$(1+\tau)\sigma^i(u\theta) = (1+\tau)\sigma^i(v\theta) \Rightarrow (1+\tau)\sigma^i(u-v)\theta = 0$$

y puesto que θ es una $\mathfrak{x}[G]$-base de N ha de ser:

$(1+\tau)\sigma^i(u-v) = 0, \quad 0 \leq i \leq p^n-1$, lo que implica

$u - v \in A(1-\tau)\sum_{i=0}^{p^n-1}\sigma^i$, es decir $\overline{u} = \overline{v}$.

La aplicación Π de U en $\mathfrak{B}$ definida, es por tanto una aplicación biyectiva, con lo cual queda probada la proposición.

Proposición (2.10). Sea r un entero tal que $0 \leq r \leq p^n-1$. Si $2r+1$ es primo con p, el elemento $1 + (1-\tau)\sum_{i=1}^{r}\sigma^i \in \mathfrak{O}$ es inversible en $\mathfrak{O}$ y su inverso es:

$1 + (1-\tau)\sum_{i=1}^{h} \sigma^{(2r+1)i} \in \mathfrak{A}$ donde h es un entero tal que

$r + (2r+1)h \equiv 0 \pmod{p^n}$.

En efecto, operando resulta:

$$(1 + (1-\tau)\sum_{i=1}^{r} \sigma^{i})\,(1 + (1-\tau)\sum_{i=1}^{h} \sigma^{(2r+1)i}) =$$

$$1 + (1-\tau)\left[\sum_{i=1}^{r}\sigma^{i} + \sum_{i=-r}^{r} \sigma^{i}\sum_{i=1}^{h} \sigma^{(2r+1)i}\right].$$

Si son $2r+1$ y p primos entre si, existen h y a tales que

$r + (2r+1)h = p^n a$. Se tiene pues la identidad:

$$\sum_{i=-r}^{r}\sigma^{i}\sum_{i=1}^{h} \sigma^{(2r+1)i} = \sum_{i=r+1}^{p^n a} \sigma^{i} = a\sum_{i=1}^{p^n} \sigma^{i} - \sum_{i=1}^{r} \sigma^{i}.$$

Por tanto:

$$(1 + (1-\tau)\sum_{i=1}^{r}\sigma^{i})\,(1 + (1-\tau)\sum_{i=1}^{h} \sigma^{(2r+1)i}) =$$

$$1 + (1-\tau)a\sum_{i=1}^{p^n} \sigma^{i} ,$$

es decir:

$$(1 + (1-\tau)\sum_{i=1}^{r} \sigma^{i})\,(1 + (1-\tau)\sum_{i=1}^{h} \sigma^{(2r+1)i}) \equiv 1$$

$$\mod\ (A(1-\tau)\sum_{i=1}^{p^n} \sigma^{i}).$$

Corolario (2.11). El número de elementos del conjunto $\mathcal{B}$ definido en (2.9) es mayor o igual a $\varphi(p^n)$.

Es consecuencia inmediata de las proposiciones (2.9) y (2.10).

3. ESTUDIO DE A_N COMO $A[G]$-MODULO.

Lema (3.1). Si M es un sub-$A[G]$-módulo proyectivo de A_N que contiene A_K y A_k, entonces $M = A_N$.

Es consecuencia inmediata de (2.3) y (2.6).

Proposición (3.2). Sea $\Theta \in A_N$. Si el A-módulo $[A]G - \Theta$ contiene A_K y A_k, entonces $A[G] - \Theta = A_N$.

En efecto: $A[G] - \Theta$ como $A[G]$-módulo es libre, por tanto es $A[G]$-proyectivo y en virtud de (3.1) es igual a A_N.

Esta proposición se utilizará como criterio para deducir la existencia de bases normales.

Teorema (3.3). Si p es inversible en A y A_k y A_K poseen A-bases normales, entonces A_N es $A[G]$-libre.

En efecto: En virtud de (1.10) si A_K y A_k poseen A-bases normales, N es moderadamente ramificada sobre $\mathfrak{X}$, y por (2.7) A_K posee una base normal obtenida a partir de un elemento $\theta \in A_N$ que se puede suponer de traza uno sobre $\mathfrak{X}$, y A_k una base normal obtenida a partir de un elemento $\omega \in A_k$ de traza uno sobre $\mathfrak{X}$. Se tiene entonces, $Tr_{N/k}(\theta) - \omega \in A_k$ y

$Tr_{k/\mathfrak{x}}(Tr_{N/k}(\theta) - \omega) = 0$, por tanto $Tr_{N/k}(\theta) - \omega$ es un elemento de A_k de la forma $a(\omega - \tau\omega)$ con $a \in A$. Poniendo

$\theta' = \theta - (a/p^n)(\omega - \tau\omega)$ es $Tr_{N/K}(\theta') = Tr_{N/k}(\theta)$ y $Tr_{N/k}(\theta') = \omega$. Entonces $A[G]\cdot\theta'$ es un A-módulo que contiene A_K y A_k y por tanto $A[G]\cdot\theta' = A_N$.

Teorema (3.4). Sea A un anillo principal, $\mathfrak{x}$ su cuerpo de fracciones. Se supone que la característica de $\mathfrak{x}$ no divide a 2p, que A/pA es isomorfo a Z/pZ y A/p^nA es isomorfo a Z/p^nZ.

Sea N una extensión de $\mathfrak{x}$ de grado $2p^n$, galoisiana, no abeliana, de grupo de Galois G diedral de orden $2p^n$, K un subcuerpo de N de grado p^n sobre $\mathfrak{x}$, k el subcuerpo de N cuadrático sobre $\mathfrak{x}$, A_N, A_K, A_k las clausuras enteras de A en N, K, k respectivamente.

Entonces, si A_K y A_k poseen A-bases normales, A_N es $A[G]$-libre.

En efecto:

Puesto que A_K y A_k poseen A-bases normales, en virtud de (1.10) N es moderadamente ramificada sobre $\mathfrak{x}$, y puesto que por (2.2) A_K posee una H-base, por (2.7) A_K posee bases normales formadas a partir de un elemento $\theta \in A_N$. En virtud de (1.9) se puede escoger $\theta \in A_N$ de manera que la base normal de A_K, $\theta_i = \sigma^i\theta + \tau\sigma^i\theta$ $0 \leq i \leq p^n - 1$ sea tal que $Tr_{K/\mathfrak{x}}(\theta_i) = 1$. Analogamente se puede escoger una ω, base normal de A_k, tal que $Tr_{k/\mathfrak{x}}\omega = \omega + \tau\omega = 1$.

Sea $Tr_{N/k}(\theta) = \lambda$. Se tiene $\lambda + \tau\lambda = Tr_{K/\mathfrak{x}}(Tr_{N/k}(\theta)) = Tr_{K/\mathfrak{x}}(\theta_i) = 1$.

Otra base normal de A_K deducida de θ podrá obtenerse multiplicando θ por un elemento u^r inversible en $\mathfrak{O}$, (2.9) de los que se sabe que hay por lo menos $\varphi(p^n)$ (2.11). Si se indica por θ^r el elemento $u^r\theta$, $(\theta^r)_i = \sigma^i(\theta^r) + \tau\sigma^i(\theta^r)$ $0 \leq i \leq p^n-1$ serán bases normales de A_K.

Sea $\lambda_r = Tr_{N/k}(\theta^r)$. Teniendo en cuenta la expresión de u^r dada en (2.10) resulta:

$$\lambda_r = Tr_{N/k}(\theta^r) = \sum_{j=0}^{p^n-1} \sigma^j(1 + (1-\tau)\sum_{i=0}^{r} \sigma^i)\theta =$$

$$=(r+1)Tr_{N/k}\,\theta - r\,\tau Tr_{N/k}\,\theta = (1 + r(1-\tau))\lambda$$

y $Tr_{k/\mathfrak{x}}(\lambda_r) = 1$. Si es posible determinar un valor de r tal que $\lambda_r = \omega$, en virtud de (3.2) estaría demostrado el teorema.

Puesto que $\lambda_r + \tau\lambda_r = 1 = \omega + \tau\omega$, si se consigue determinar un valor de λ_r para el cual $\lambda_r - \tau\lambda_r = \omega - \tau\omega$, puesto que la característica de $\mathfrak{x}$ es distinta de dos, será $\lambda_r = \omega$. Supóngase que $\lambda_r - \tau\lambda_r \equiv \omega - \tau\omega \pmod{p^n A_k}$ y sea $\theta^r \in A_N$ el elemento que corresponde a λ_r; sumando a θ^r un $\mu \in A_k$ tal que $Tr_{k/\mathfrak{x}}(\mu) = 0$, puesto que $Tr_{N/k}(\theta^r + \mu) = \lambda_r + p^n\mu$ se puede conseguir un valor de λ_r tal que $\lambda_r - \tau\lambda_r = \omega - \tau\omega$.

Basta pues ver si es posible encontrar un λ_r tal que

$\lambda_r - \tau\lambda_r \equiv \omega - \tau\omega \pmod{p^n A_k}$.

Por la forma como se ha escogido ω, es $\omega + \tau\omega \equiv 1 \pmod{p^n A_k}$ y por ser $(\omega, \tau\omega)$ una A-base de A_k es $\omega - \tau\omega \neq 0$ pues de lo contrario $\omega \in A$. Además $\omega - \tau\omega \not\equiv 0 \pmod{pA_k}$, pues si lo fuera, existirían $a, b \in A$ tales que $(1-pa)\omega + (-1-pb)\tau\omega = 0$ lo que implicaría que p fuese inversible en A, contra la hipótesis. El número de valores disitintos que podrá tomar $\omega \pmod{p^n A_k}$ será por tanto igual al número de elementos $\mu \in A_k$, distintos módulo $p^n A_k$ que verifiquen $\mu + \tau\mu \equiv 1 \pmod{p^n A_k}$ y tales que $\mu - \tau\mu \not\equiv 0 \pmod{pA_k}$. Para calcular este número, sea

$\mu = x_1\omega + x_2\tau\omega$, $x_1, x_2 \in A$, entonces:

$\mu + \tau\mu \equiv 1 \pmod{p^n A_k} \iff (x_1 + x_2)(\omega + \tau\omega) \equiv 1 \pmod{p^n A_k}$

Por tanto en virtud de las hipótesis hechas, μ podrá tomar p^n valores distintos que cumplan esta condición. ya que por ser $\omega + \tau\omega = 1$ esto ocurre si y sólo si $x_1 + x_2 \equiv 1 \pmod{p^n A}$.

Se trata de ver ahora cuantos de entre ellos verifican $\mu - \tau\mu \equiv 0 \pmod{pA_k}$. Puesto que $\omega - \tau\omega \not\equiv 0 \pmod{pA_k}$ y $\mu - \tau\mu = (x_1 - x_2)(\omega - \tau\omega)$, $\mu - \tau\mu \equiv 0 \pmod{pA_k}$ si y sólo si $x_1 - x_2 \equiv 0 \pmod{pA}$. Por tanto el número de valores distintos que puede tomar $x_1 - x_2$ es $\varphi(p^n)$ y para cada uno de ellos, puesto que la característica de $\mathfrak{K}$ es distinta de dos se tendría el correspondiente valor de μ.

Para estudiar el número de posibles valores de λ_r que verifican estas condiciones, se demostrará en primer lugar que $(1-\tau)\lambda \not\equiv 0 \pmod{pA_k}$. Para ello se procede de la siguiente manera:

Puesto que $A/pA \simeq Z/pZ$, pA es un ideal primo de A; localizando en pA, se tiene un anillo A_p local cuyo cuerpo de fracciones es $\mathfrak{X}$ y se indicará por $(A_p)_N$ la clausura entera de A_p en N. Puesto que A es de Dedekind, A_p es también de Dedekind y por ser $N/\mathfrak{X}$ moderadamente ramificada y la característica distinta de 2 y de p, en virtud de (1.13), $(A_p)_N$ es $A_p[G]$-libre. Sea θ' una $A_p[G]$-base de $(A_p)_N$. Entonces $Tr_{N/k}(\theta') = \lambda'$ es una $A_p[G/H]$-base de $(A_p)_k$ (donde H es el subgrupo de G de orden p^n) y $\lambda' - \tau\lambda' \not\equiv 0 \pmod{p(A_p)_k}$, pues si lo fuera p sería inversible en A_p lo que es absurdo. Sea $(A_p)_K$ la clausura entera de A_p en K ; puesto que $A_K \subset (A_p)_K$, la A-base normal θ_i , $0 \leq i \leq p^n-1$ dada para A_K, será también una A_p-base normal de $(A_p)_K$ y por tanto, existirá un elemento $\bar{u} \in \mathfrak{A}$ inversible en $\mathfrak{A}$, siendo en este caso

$$\mathfrak{A} = A_p[G]/A_p(1-\tau)\sum_{i=0}^{p^n-1}\sigma^i \quad , \text{ tal que} \quad \theta' = \bar{u}\,\theta \ .$$

Se tiene:

$$Tr_{N/k}(\theta') = \sum_{i=0}^{p^n-1}\sigma^i(\theta') = \sum_{i=0}^{p^n-1}\sigma^i\left(\sum_{j \bmod p^n} a_j\sigma^j + a_j\tau\sigma^j\right)\theta =$$

$$\left(\sum_{j \bmod p^n} a_j + \sum_{j \bmod p^n} a'_j \right) \mathrm{Tr}_{N/k}\theta \qquad \text{con } a_j,\ a'_j \in A_p.$$

Se tiene por tanto:

$$\lambda' = \left(\sum_{j \bmod p^n} a_j + \tau \sum_{j \bmod p^n} a'_j \right) \lambda \qquad \text{y}$$

$$(1-\tau)\lambda' = (1-\tau) \sum_{j \bmod p^n} (a_j - a'_j)\lambda \qquad \text{y por tanto ,}$$

es $(1-\tau)\lambda \not\equiv 0 \pmod{pA_k}$.

De aquí se deduce sin más que $\lambda_r - \tau\lambda_r \not\equiv 0 \pmod{pA_k}$ ya que $\lambda_r - \tau\lambda_r = (2r+1)(1-\tau)\lambda$ y $2r+1$ no es múltiplo de p. Por tanto el número de valores de r para los que se cumple esta condición es $\varphi(p^n)$. Finalmente, puesto que $\lambda_{r_1} - \lambda_{r_2} = (r_1-r_2)(1-\tau)\lambda$, $\lambda_{r_1} = \lambda_{r_2}$ si y sólo si $r_1=r_2$, se tienen $\varphi(p^n)$ valores de λ_r distintos , y estos coinciden con los valores posibles de ω con lo cual está demostrado el teorema.

Observación (3.5). En el teorema (3.4) se hacen hipótesis complementarias sobre el anillo A que se sabe que se cumplen en el anillo Z de los enteros racionales. Cabría entonces preguntarse sobre la existencia de extensiones N sobre $\mathfrak{X}$ del tipo de las consideradas; sin embargo esta cuestión queda resuelta mediante el siguiente teorema debido a Safarevic [16]:

"Sea k un cuerpo de números y G un grupo resoluble finito; existe siempre una extensión K de k galoisiana, tal que

el grupo de Galois de K sobre k es G".

Observación (3.6). El único cuerpo de números que es cuerpo de fracciones de un anillo de Dedekind A que verifica las hipótesis de (3.4) es el cuerpo Q.

En efecto: Sea n el grado de $\mathfrak{X}$ sobre Q,

$p^n = N_{\mathfrak{X}/Q}(pA) = \text{car}\ (A/pA) = p \quad \Longrightarrow \quad n = 1$.

C A P I T U L O IV

EXISTENCIA DE H-BASES. CASO $2p^n$.

INTRODUCCION.- En el teorema (3.4) del Capítulo III, el ser A_N libre como $A[G]$-módulo, está condicionado a la existencia de A-bases normales para los anillos A_K y A_k de las subextensiones de N de grados p^n y 2 sobre $\mathcal{K}$ respectivamente. La existencia de estas bases en el caso de A_k no presenta ningún problema. En el caso de A_K, la proposición (II,2,7) asegura su existencia cuando A_K posee una H-base y K es moderadamente ramificada en p sobre $\mathcal{K}$. En este capítulo se da una condición suficiente de existencia de H-bases para algún tipo de extensiones galoisianas diedrales de orden $2p^n$ (n mayor que uno y p primo impar. Para ello se construyen unas extensiones del cuerpo $\mathcal{K}$ considerado, adjuntándole raices p^n-ésimas de la unidad. Haciendo uso de las resolventes de Lagrange, se construye el cuerpo $\tilde{k}$, y se define un homomorfismo de la subextensión K de N de grado p^n sobre $\mathcal{K}$, en $\tilde{k}$, considerados como espacios vectoriales sobre $\mathcal{K}$. Este homomorfismo es el que permitirá establecer las condiciones suficientes para la existencia de H-bases del anillo A_K.

1. EXTENSIONES POR ADJUNCION DE RAICES p^n-ESIMAS DE LA UNIDAD.

(1.1). Hipótesis previas, definiciones y casos posibles.

En todo este capítulo, a las hipótesis hechas sobre Λ en (II,1.2) se añadirá la

Hipótesis H': El polinomio ciclotómico $(X^{p^{n-1}})^{p-1}+\ldots+X^{p^{n-1}}+1$ es irreducible sobre $\mathfrak{x}$.

Obsérvese que si $\mathfrak{x}$ es un cuerpo de números, la hipótesis H' es consecuencia de la hipótesis H. Para su demostración ver [20] Cap III $\S$.12 Teor. III 12 B.

Sea $\mathfrak{x}'$ el cuerpo extensión de $\mathfrak{x}$ por adjunción de las raices p^n-ésimas de la unidad. En virtud de la hipótesis H' es $[\mathfrak{x}' : \mathfrak{x}] = \varphi(p^n)$ y el grupo de Galois de $\mathfrak{x}'$ sobre $\mathfrak{x}$ es isomorfo a $(Z/p^nZ)^*$ y por tanto es un grupo cíclico de orden $\varphi(p^n)$.

Sea N la extensión de $\mathfrak{x}$ galoisiana de grupo de Galois G diedral de orden $2p^n$. Puesto que N y $\mathfrak{x}'$ son ambas extensiones de $\mathfrak{x}$, se considerarán las extensiones M de $\mathfrak{x}$ que son a la vez subextensiones de $\mathfrak{x}'$ y de N. Cada M será pues un subcuerpo de N fijo por algún subgrupo de G y un subcuerpo de $\mathfrak{x}'$ fijo por algún subgrupo del grupo $G(\mathfrak{x}'/\mathfrak{x})$ de Galois de $\mathfrak{x}'$ sobre $\mathfrak{x}$. Puesto que $G(\mathfrak{x}'/\mathfrak{x})$ es cíclico de orden $\varphi(p^n)$, M es galoisiana sobre $\mathfrak{x}$, y $G(M/\mathfrak{x})$ será cíclico de orden hp^j con h divisor de (p-1) y j menor o igual que (n-1). Ade-

más, $G(N/M)$ tendrá que ser un divisor normal de G y por tanto cíclico de orden p^i, lo que implica que $G(M/\mathfrak{x})$ sea diedral de orden $2p^{n-i}$. Por tanto se pueden presentar sólo los dos casos siguientes:

Caso A: $G(M/\mathfrak{x}) = Id. \Rightarrow N \cap \mathfrak{x}' = \mathfrak{x}$

Caso B: $G(M/\mathfrak{x})$ = cíclico de orden dos $\Rightarrow N \cap \mathfrak{x}' = k$.

Estudio del Caso A. (1.2).

Sean N' y k' las respectivas extensiones de N y k por adjunción de las raices p^n-ésimas de la unidad. Se tiene:

$$G(N'/N) \simeq G(k'/k) \simeq G(\mathfrak{x}'/\mathfrak{x}) \simeq (Z/p^nZ)^*$$

$$G(N'/\mathfrak{x}') \simeq G(N/\mathfrak{x}) = G.$$

El grupo de Galois $G(N'/\mathfrak{x})$ es el producto directo del grupo G por $G(\mathfrak{x}'/\mathfrak{x})$ y este último es el centro de $G(N'/\mathfrak{x})$. $G(N'/\mathfrak{x})$ está generado por los generadores σ y τ de G y por el generador de $G(\mathfrak{x}'/\mathfrak{x})$. Tiene la siguiente presentación:

$$\langle \sigma, \tau, s \; ; \; \tau^2 = 1, \; \sigma^{p^n} = 1, \; s^{\varphi(p^n)} = 1, \; s\tau = \tau s, \; s\sigma = \sigma s, \; \sigma\tau = \tau\sigma^{-1} \rangle$$

Estudio del caso B. (1.3). Con las mismas notaciones que en el caso A, puesto que $k \subset \mathfrak{x}'$ es $k' = \mathfrak{x}'$ y por tanto $G(N'/\mathfrak{x}') = G(N'/k') \simeq G(N/k)$.

Por ser $N' \supset \mathfrak{x}' \supset \mathfrak{x}$ y $\mathfrak{x}'$ galoisiana sobre $\mathfrak{x}$, $G(N/k)$, que es isomorfo a $G(N'/\mathfrak{x}')$, es un divisor normal de $G(N'/\mathfrak{x})$.

Puesto que k es el subcuerpo de k' fijo por el único subgrupo de índice 2 de $G(\mathfrak{x}'/\mathfrak{x})$, $G(\mathfrak{x}'/k)$ está formado por los elementos de $G(\mathfrak{x}'/\mathfrak{x})$ que son cuadrados. Por ser $N' \supset N \supset \mathfrak{x}$ y N galoisiana sobre $\mathfrak{x}$, $G(\mathfrak{x}'/\mathfrak{x})^2 = G(\mathfrak{x}'/k) \simeq G(N'/N)$ es un divisor normal de $G(N'/\mathfrak{x})$.

Puesto que $G(N/k) \cap G(\mathfrak{x}'/\mathfrak{x})^2 = \mathrm{Id}.$ y $G(N/k)$ y $G(\mathfrak{x}'/\mathfrak{x})^2$ son divisores normales de $G(N'/\mathfrak{x})$, para cada $s \in G(\mathfrak{x}'/\mathfrak{x})^2$ y cada $h \in G(N/k)$ es $shs^{-1} = h$. Si $s \notin G(\mathfrak{x}'/\mathfrak{x})^2$, se puede considerar como un automorfismo de N' sobre $\mathfrak{x}$, que no deja fijo N y por tanto, restringido a N se puede mirar como un automorfismo de N sobre $\mathfrak{x}$ que no deja fijo k, que será por tanto de la forma $\sigma\tau$. Para cada $h \in G(N/k)$ es pues:

$shs^{-1} = (\tau\sigma)h(\sigma^{-1}\tau^{-1}) = \tau h \tau^{-1} = h^{-1}$.

De aquí resulta que $G(N'/\mathfrak{x})$ es el producto semidirecto de $G(N/k)$ por $G(\mathfrak{x}'/\mathfrak{x})$ y el centro de $G(N'/\mathfrak{x})$ es $G(\mathfrak{x}'/\mathfrak{x})^2$.

Se tiene pues:

$$G(N'/\mathfrak{x}) = \langle \sigma, s ; \sigma^{p^n} = 1, s^{\varphi(p^n)} = 1, s\sigma = \sigma^{-1}s \rangle .$$

Puesto que G contiene un elemento de orden 2, que no es permutable con los elementos de $G(N/k)$, $G(N'/\mathfrak{x})$ tiene un subgrupo isomorfo a G si y sólo si tiene un elemento de orden dos que no pertenece al centro. Puesto que los elementos de $G(N/k)$ no son permutables con los elementos de $G(\mathfrak{x}'/\mathfrak{x})$, este elemento si existe será un elemento de orden dos que no sea cuadrado.

Si $p \equiv 1 \pmod 4$ todos los elementos de orden dos son cuadra-

dos y por tanto todos pertenecen al centro. Si $p \equiv 3 \pmod 4$, el elemento $s^{1/2(p-1)p^{n-1}}$ es de orden dos y no es cuadrado; este elemento con $G(N/k)$ generan un subgrupo de $G(N'/\mathfrak{x})$ que es isomorfo a G.

Estos dos casos B, distintos, que pueden presentarse se indicarán por B_1 si $p \equiv 1 \pmod 4$ y por B_2 si $p \equiv 3 \pmod 4$.

(1.4) Estudio de las $\mathfrak{x}$-bases de $\mathfrak{x}'$, y de las Λ-bases de A'

Para las propiedades de los cuerpos ciclotómicos se ha consultado [4].

Proposición (1.4.1). Si ζ es una raiz p^n- ésima de la unidad, $\Omega = (\zeta, \zeta^2, \ldots, \zeta^{1/2\varphi(p^n)}, \zeta^{-1/2\varphi(p^n)}, \ldots, \zeta^{-1})$ es una $\mathfrak{x}$ base de $\mathfrak{x}'$.

En efedto: Se sabe que $B = (1, \zeta, \ldots, \zeta^{\varphi(p^n)-1})$ es una $\mathfrak{x}$-base de $\mathfrak{x}'$. Puesto que el número de elementos de Ω coincide con el de B, basta probar que los elementos de Ω son linealmente independientes sobre $\mathfrak{x}$. Supóngase que fuera

$$\sum_{i=1}^{1/2\varphi(p^n)} \lambda_i \zeta^i + \sum_{j=1}^{1/2\varphi(p^n)} \mu_j \zeta^{-j} = 0 \qquad (1)$$

con λ_i, μ_j elementos de $\mathfrak{x}$ no todos nulos. Se observa que las ζ^i que figuran en el primer sumatorio, son todas ellas elementos de B, y analogamente, las del segundo sumatorio tales que $1/2(p-1)p^{n-1} \geqslant j \geqslant p^{n-1}$, puesto que $p^n - j < p^{n-1}(p-1)$ implica $j > p^{n-1}$. Para las restantes se tiene:

$$\zeta^{-h} = -\sum_{i=1}^{p-1} \zeta^{ip^{n-1}-h} \qquad -1 \geq h \geq -(p^{n-1}-1).$$

Sustituyendo en (1) resulta:

$$\sum_{i=1}^{1/2\varphi(p^n))} \lambda_i \zeta^i + \sum_{j=1/2(p+1)p^{n-1}}^{\varphi(p^n)-1} \mu_j \zeta^j - \sum_{j=1}^{p^{n-1}-1} \mu_j \sum_{i=1}^{p-1} \zeta^{ip^{n-1}-j}$$

$$= \sum_{i=1}^{\varphi(p^n)-1} \rho_i \zeta^i = 0 \qquad (2)$$

donde $\rho_i = 0$ para $1 \leq i \leq \varphi(p^n) - 1$ y son de una de las dos formas siguientes: $\lambda_i - \mu_j$ o $\mu_i - \mu_j$. Teniendo en cuenta la expresión (2) resulta :

$$\rho_i = \mu_j \quad \text{para} \quad 1/2(p+1)p^{n-1}-1 > i > 1/2(p+1)p^{n-1}-(p^{n+1}-1)$$

y por tanto para estos valores de i ha de ser $\mu_j = 0$. Esto implica la anulación del tercer sumatorio de (2). Por tanto

$$\sum_{i=1}^{1/2\varphi(p^n)} \lambda_i \zeta^i + \sum_{j=1/2(p+1)p^{n-1}}^{\varphi(p^n)-1} \mu_j \zeta^j = 0$$

implica $\lambda_i = \mu_j = 0$ para todo i , j.

Proposición (1.4.2). Los elementos de la forma $\zeta^i + \zeta^{-i}$ $1 \leq i \leq 1/2\,\varphi(p^n)$ forman una A-base del anillo A'_o de los enteros de la subextensión x'_o definida por $x'_o = x(\zeta + \zeta^{-1})$

En efecto, puesto que se cumple la hipótesis H'el polinomio

ciclotómico correspondiente a la extensión $\mathfrak{X}'$ sobre $\mathfrak{X}$ es irreducible sobre $\mathfrak{X}$ y $(1, \zeta, \ldots, \zeta^{(p^n)-1})$ es una A-base del anillo de los enteros A' de $\mathfrak{X}'$. ([20] Teor.III 12 E). Puesto que para $n>1$ la extensión $\mathfrak{X}'$ no es moderadamente ramificada sobre $\mathfrak{X}$, A' no posee base normal sobre A. Pero la base Ω obtenida en (1.4.1) es una base entera de A' sobre A, ya que los elementos de B que no pertenecen a Ω se pueden expresar como combinación lineal entera de elementos de Ω.

Sea $\alpha \in A'_o$. Puesto que $\alpha \in A'$ es $\alpha = \sum_{i=1}^{1/2\varphi(p^n)} a_i \zeta^i + b_i \zeta^{-i}$

donde a'_i y b'_i son elementos de A, y por pertenecer α a A'_o ha de ser $s_{-1}\alpha = \alpha$. Por tanto:

$$\sum_{i=1}^{1/2\varphi(p^n)} a_i \zeta^i + b_i \zeta^{-i} = \sum_{i=1}^{1/2\varphi(p^n)} a_i \zeta^{-i} + b_i \zeta^i$$

lo que implica $a_i = b_i$ para $1 \leq i \leq 1/2\varphi(p^n))$ y por tanto $\zeta^i + \zeta^{-i}$, $1 \leq i \leq 1/2\varphi(p^n)$ forman una A-base de A'_o.

2. CONSTRUCCION DEL CUERPO $\tilde{k}$.

Sea K la subextensión de N sobre $\mathfrak{X}$ de grado p^n fija por el grupo g, subgrupo de orden dos de G, y H el grupo de Galois de N sobre k. Se designará por H^* el grupo de los caracteres de H, que es isomorfo al grupo de las raices p^n-ésimas de la unidad.

Definición (2.1). Sea $\theta \in K$ y $\chi \in H^*$. Se denomina resolvente de Lagrange correspondiente al caracter χ, del elemento θ,

al elemento de N' definido de la manera siguiente:

$$\langle \theta , \chi \rangle = \sum_{\sigma \in H} \chi(\sigma^{-1})(\sigma\theta).$$

Propiedades (2.2). Para estudiar las propiedades de las resolventes de Lagrange, se tendrán en cuenta los tres tipos de caracteres que pueden presentarse, según que el generador de H se aplique en el 1, en una raiz no primitiva p^n-ésima de la unidad, o en una raiz primitiva p^n-ésima de la unidad; estos caracteres se designarán por caracter trivial, no primitivo y primitivo de H respectivamente. Cuando no se especifique nada se entenderá que la propiedad es válida en todos los casos.

a) Si χ_o es el caracter trivial se tiene:

$$\langle \theta , \chi_o \rangle = \sum_{\sigma \in H} \sigma(\theta) = \mathrm{Tr}_{N/k}(\theta).$$

b)) $\forall \sigma \in H \quad \sigma \langle \theta, \chi \rangle = \langle \sigma\theta , \chi \rangle = \chi(\sigma)\langle \theta, \chi \rangle$

se comprueba por cálculo directo.

c)

$$\sum_{\chi \in H^*} \langle \theta, \chi \rangle = p^n \theta .$$

Se comprueba por cálculo directo teniendo en cuenta que

$$\sum_{\chi \in H^*} \chi(\sigma) = 0 \quad \text{si} \quad \sigma \neq \mathrm{Id}, \qquad \sum_{\chi \in H^*} \chi(\mathrm{Id}) = p^n.$$

d) Sea ζ una raiz p^n-ésima de la unidad, $s_i \in G(x'/x)$ $i \not\equiv 0 \pmod p$ tal que $s_i(\zeta) = \zeta^i$. Si χ es un caracter primitivo de H se tiene:

caso A: $s_i\langle\theta,\chi\rangle = \langle\theta,\chi^i\rangle$

Se comprueba por cálculo directo teniendo en cuenta que $\theta \in N$ y que N es el subcuerpo de N' fijo por $G(N'/N)$.

caso B: $s_i\langle\theta,\chi\rangle = \langle\theta,\chi^i\rangle$ si $\left(\frac{i}{p}\right) = 1$

$s_i\langle\theta,\chi\rangle = \langle\theta,\chi^{-i}\rangle$ si $\left(\frac{i}{p}\right) = -1$

Puesto que en este caso N es invariante por $G(N'/N)^2$, si $s_i \in G(N'/N)^2$ se tiene $s_i\langle\theta,\chi\rangle = \langle\theta,\chi^i\rangle$. Si $s_i \in G(N'/N)$ y $s_i \notin G(N'/N)^2$ puesto que $s_i\sigma = \sigma^{-1}s_i$ se tiene: $s_i\langle\theta,\chi\rangle = \langle s_i(\theta), \chi^{-i}\rangle$ pero $\theta \in K$ y K es un subcuerpo de N' fijo por s_i por tanto $s_i\langle\theta,\chi\rangle = \langle\theta,\chi^{-i}\rangle$. Utilizando como notación los símbolos de Legendre se tiene pues el resultado.

e)). En el caso A $\tau\langle\theta,\chi\rangle = \langle\theta,\chi^{-1}\rangle$.

Para comprobarlo se tendrá en cuenta que $\theta \in K$ y K es fijo por τ.

f) En el caso A, si χ es un caracter primitivo de H, se tiene:

$$\tau\, s_{-1}\langle\theta,\chi\rangle = \langle\theta,\chi\rangle$$

Es consecuencia inmediata de d) y e).

g) Si χ es un caracter no primitivo de H se tiene:

$$\langle\theta,\chi\rangle = \sum_{i=0}^{p^{n-1}-1}\left(\chi(\sigma)^{-i}\sum_{\lambda=0}^{p-1}\sigma^{i+\lambda p^{n-1}}(\theta)\right)$$

Puesto que $\chi(\theta)$ es un caracter no primitivo de H, es $\left[\chi(\sigma)\right]^{p^{n-1}} = 1$. Por tanto

$\left[\chi(\sigma)\right]^{i} = \left[\chi(\sigma)\right]^{j} \iff \left[\chi(\sigma)\right]^{i-j} = 1$ es decir, sólo en el caso en que $i \equiv j \pmod{p^{n-1}}$, y la expresión dada resulta por cálculo directo.

h)

$$\sum_{\substack{\chi \text{ no prim.} \\ \chi=\chi_0}} \langle \theta, \chi \rangle = p^{n-1} \operatorname{Tr}_{N/L}(\theta)$$

Teniendo en cuenta g) resulta:

$$\sum_{\substack{\chi \text{ no prim.} \\ \chi=\chi_0}} \langle \theta, \chi \rangle = p^{n-1} \sum_{\lambda=0}^{p-1} \sigma^{\lambda p^{n-1}}(\theta) + \left(\sum_{i=0}^{p^{n-1}-1} \chi(\sigma)^{-i} \right) \left(\sum_{i=0}^{p^{n-1}-1} \sum_{\lambda=1}^{p-1} \sigma^{i+\lambda p^{n-1}}(\theta) \right) =$$

$$= p^{n-1} \sum_{\lambda=0}^{p-1} \sigma^{\lambda p^{n-1}}(\theta) = p^{n-1} \operatorname{Tr}_{N/L}(\theta).$$

i) Sea $\theta \in K \cap L$ y χ un caracter primitivo de H. Entonces $\langle \theta, \chi \rangle = 0$.

En efecto:

$$\langle \theta, \chi \rangle = \sum_{\sigma \in H} \chi(\sigma^{-1}) \sigma(\theta) = \theta \sum_{\lambda=0}^{p-1} \chi\left(\sigma^{\lambda p^{n-1}}\right) +$$

$$+ \sigma\theta \sum_{\lambda=0}^{p-1} \chi\left(\sigma^{\lambda p^{n-1}+1}\right) + \cdots + \sigma^{p-1}(\theta) \sum_{\lambda=0}^{p-1} \chi\left(\sigma^{\lambda p^{n-1}+(p-1)}\right)$$

Pero $\theta \in L \Rightarrow \sigma^{p^{n-1}}\theta = \sigma^{\lambda p^{n-1}}\theta = \theta \qquad 0 \leq \lambda \leq p-1$.

Por otra parte:

$$\sum_{\lambda=0}^{p-1} \chi\left(\sigma^{\lambda p^{n-1}+k}\right)\theta = \chi(\sigma^k)\sum_{\lambda=0}^{p-1}\chi\left(\sigma^{\lambda p^{n-1}}\right)\theta$$

Por tanto

$$\langle \theta, \chi \rangle = \sum_{\lambda=0}^{p-1}\chi\left(\sigma^{\lambda p^{n-1}}\right)\sum_{k=0}^{p-1}\chi(\sigma^k)\sigma^k(\theta)$$

Puesto que

$$\sum_{\lambda=0}^{p-1}\chi\left(\sigma^{\lambda p^{n-1}}\right) = \sum_{\lambda=0}^{p-1}\zeta^{\lambda p^{n-1}} = 0$$

siendo ζ una raiz primitiva p^n-ésima de la unidad, se tiene $\langle \theta, \chi \rangle = 0$ si $\theta \in K_1 = K \cap L$.

Obsérvese que si χ es un caracter no primitivo, esta propiedad no se cumple.

Definición (2.3). El cuerpo obtenido adjuntado a α las potencias p^n de las resolventes de Lagrange de los elementos de K se designará por $\tilde{k}$.

Proposición (2.4). $\tilde{k}$ es un subcuerpo de k:

En efecto: Puesto que k' es una subextensión de N' fija por H, bastará probar que $\sigma\langle \theta, \chi \rangle^{p^n} = \langle \theta, \chi \rangle^{p^n}$ y esto es consecuencia inmediata de (2.2.b).

Proposición (2.5). Sea $\theta \in N$ tal que $(\sigma\theta)_{\sigma \in H}$ forma una k-base normal de N. Entonces $\langle \theta, \chi \rangle \neq 0$ para todo $\chi \in H^*$.

En efecto: Si para algún $\chi \in H^*$ fuera $\langle \theta, \chi \rangle = 0$, se tendría

$\sum_{\sigma \in H} \chi(\sigma^{-1})\sigma(\theta) = 0$ con $\chi(\sigma^{-1}) \neq 0$ para todo $\sigma \in H$ y por (2.2.b) $\langle \sigma\theta, \chi \rangle = 0$ para todo $\sigma \in H$. Por tanto:

$$\sum_{\sigma_j \in H} \chi(\sigma_j^{-1})(\sigma_j \sigma_i(\theta)) = 0 \qquad 1 \leq i \leq p^n$$

y $\sum_{j=1}^{p^n} \chi(\sigma_j^{-1})(\sigma_j \sigma_i)(\theta) = 0 \quad 1 \leq i \leq p^n$, tendría una solución distinta de la trivial, lo que implicaría $\det(\sigma_i \sigma_j \theta) = 0$ contra la hipótesis de ser θ una base normal de N sobre $\varkappa$.

Proposición (2.6). Sea $\theta \in K$ tal que $(\sigma\theta)_{\sigma \in H}$ forman una k-base normal de N; si χ_1 , χ_2 son dos caracteres distintos de H $\langle \theta, \chi_1 \rangle^{p^n}$ y $\langle \theta, \chi_2 \rangle^{p^n}$ son distintos.

En efecto: Si $\langle \theta, \chi_1 \rangle^{p^n} = \langle \theta, \chi_2 \rangle^{p^n}$ es $\langle \theta, \chi_1 \rangle = \omega \langle \theta, \chi_2 \rangle$ donde ω es una raiz p^n-ésima de la unidad. En virtud de (2.2.b) para cada $\sigma \in H$ es $\chi_1(\sigma)\langle \theta, \chi_1 \rangle = \omega\, \chi_2(\sigma)\langle \theta, \chi_2 \rangle$ y por (2.5) $\chi_1(\sigma) = \chi_2(\sigma)$ para cada $\sigma \in H$, es decir

$$\chi_1 = \chi_2 \ .$$

Proposición (2.7). En el caso A, $\tilde{k}$ es una subextensión cíclica de k' de grado $\varphi(p^n)$ sobre $\varkappa$.

En efecto: En virtud de (2.2.d) si $\chi \in H^*$ es un caracter primitivo, los $\langle \theta, \chi \rangle^{p^n}$ son elementos de $\tilde{k}$ conjugados de uno de ellos, pues

$$s_i \langle \theta, \chi \rangle = \langle \theta, \chi^i \rangle \Rightarrow s_i\left(\langle \theta, \chi \rangle^{p^n}\right) = \langle \theta, \chi^i \rangle^{p^n}.$$

Como consecuencia de (2.4) y (2.6) se tiene:

$$p^{n-1}(p-1) \leq \left[\tilde{k} : \varkappa\right] \leq 2p^{n-1}(p-1)$$

y puesto que por (2.2.f), $\tilde{k}$ es fijo por τs_{-1}, $\tilde{k}$ no puede coincidir con k' y por tanto $[\tilde{k} : \alpha] = \varphi(p^n)$.

Puesto que $G(\tilde{k}/\alpha)$ es isomorfo por restricción a $G(k'/k)$, $\tilde{k}$ es cíclica sobre α.

Corolario (2.8). La subextensión α'_o de α' de grado $1/2\,\varphi(p^n)$ definida por $\alpha'_o = \alpha(\zeta + \zeta^{-1})$, ζ es una raiz primitiva p^n-esima de la unidad, es una subextensión de $\tilde{k}$, y $[\tilde{k} : \alpha'_o] = 2$.

Para probarlo basta tener en cuenta que $\zeta + \zeta^{-1}$ es fijo por $s_{-1}\tau$.

Proposición (2.9). En el caso B_1 se tiene $\tilde{k} = k'$ y en el caso B_2, $\tilde{k}$ es un subcuerpo de k'que coincide con α'_o.

Para demostrarlo probaremos primero el siguiente

Lema (2.10). En el caso B_1 las $\langle \theta, \chi \rangle^{p^n}$ correspondientes a caracteres primitivos, son elementos conjugados de uno de ellos en la extensión $\tilde{k}$ sobre α. En el caso B_2, si χ_1 es un caracter primitivo cualquiera $\langle \theta, \chi_1 \rangle^{p^n}$ y $\langle \theta, \chi_1^{-1} \rangle^{p^n}$ no son conjugados entre si, y los $\langle \theta, \chi \rangle^{p^n}$ que corresponden a los restantes caracteres primitivos son conjugados, cada uno, de uno de ellos.

En efecto: En virtud de (2.2.d) se tiene:

$$s_i \langle \theta, \chi \rangle^{p^n} = \langle \theta, \chi^i \rangle^{p^n} \qquad si \quad \left(\frac{i}{p}\right) = 1$$

$$s_i \langle \theta, \chi \rangle^{p^n} = \langle \theta, \chi^{-i} \rangle^{p^n} \qquad si \quad \left(\frac{i}{p}\right) = -1.$$

En el caso B_1, $\left(\frac{-1}{p}\right) = 1$ y por tanto $s_i\langle\theta,\chi\rangle^{p^n}$ son elementos todos ellos distintos.

En el caso B_2, $\left(\frac{-1}{p}\right) = -1$ y por tanto $s_{-1}\langle\theta,\chi\rangle = \langle\theta,\chi\rangle$ y $s_{-1}\langle\theta,\chi\rangle^{p^n} = \langle\theta,\chi\rangle^{p^n}$ cualesquiera que sean $\theta \in K$ y $\chi \in H^*$. Puesto que el número de restos cuadráticos mod p es $1/2\,\varphi(p^n)$ se tiene demostrado el lema.

Demostración de (2.9).

Caso B_1 : Teniendo en cuenta (2.4) y (2.10) resulta:

$$p^{n-1}(p-1) \leqslant \left[\tilde{k} : \alpha\right] \leqslant p^{n-1}(p-1)$$

por tanto $\left[\tilde{k} : \alpha\right] = \varphi(p^n)$ y puesto que $\tilde{k}$ es un subcuerpo de k' es $\tilde{k} = k'$.

Caso B_2 : Puesto que el número de restos cuadráticos módulo p es $1/2\,\varphi(p^n)$ ha de ser $\left[\tilde{k} : \alpha\right] \geqslant 1/2\,\varphi(p^n)$ y puesto que $\tilde{k}$ es fijo por s_{-1}, no puede coincidir con k'. Se tiene pues $\left[\tilde{k} : \alpha\right] = 1/2\,\varphi(p^n)$ y por ser α'_0 fijo por s_{-1} y $\alpha'_0 \subset \tilde{k}$ es $\alpha'_0 = \tilde{k}$.

3. CONSTRUCCION DE H-BASES. CASO A.

Se sabe por (2.7) y (3.8) que $\tilde{k}$ es una extensión de α de grado $\varphi(p^n)$ y una extensión cuadrática de α'_0, por tanto se puede considerar $\tilde{k}$ como un espacio vectorial V sobre α de dimensión $\varphi(p^n)$, o como un espacio vectorial sobre α'_0 de dimensión 2. Puesto que K es una extensión de α de grado

p^n, se puede considerar también como espacio vectorial sobre $\mathfrak{x}$ de dimensión p^n. En estas condiciones se tiene:

Proposición (3.1). Sea $\chi \in H^*$ un caracter primitivo de H y $\theta_o \in K$ tal que $(\sigma\theta_o)_{\sigma\in H}$ es una base normal de N sobre k. Se define una aplicación $f:K \longrightarrow V$ de la siguiente manera:

$$f(\theta) = \frac{\langle \theta, \chi \rangle}{\langle \theta_o, \chi \rangle} \qquad \text{para cada } \theta \in K$$

La aplicación $f: K \to V$ así definida es un homomorfismo de espacios vectoriales.

En efecto: Para ver que f es una aplicación de K en V basta comprobar que cualquiera que sea $\theta \in K$, $\frac{\langle \theta, \chi \rangle}{\langle \theta_o, \chi \rangle} \in \tilde{k}$, es decir, que este cociente es invariante por H y por $s_{-1}\tau$, y esto es consecuencia de (2.2.b)) y (2.2.f) puesto que en virtud de (2.5) $\langle \theta_o, \chi \rangle$ es distinto de cero.

Que es homomorfismo resulta de ser

$$\langle \theta + \theta', \chi \rangle = \langle \theta, \chi \rangle + \langle \theta', \chi \rangle \qquad \theta, \theta' \in K$$

$$\langle \lambda\theta, \chi \rangle = \lambda \langle \theta, \chi \rangle \qquad \lambda \in k, \ \theta \in K.$$

Proposición (3.2). El núcleo de f es el cuerpo $K_1 = K \cap L$, (donde L es la subextensión de N de grado $2p^{n-1}$ sobre $\mathfrak{x}$), y la aplicación f es exhaustiva.

En efecto: Por definición de f, $f(\theta) = 0 \iff \langle \theta, \chi \rangle = 0$. Teniendo en cuenta (2.2.dA), si $\langle \theta, \chi \rangle = 0$, χ primitivo,

$\langle \theta, \chi^i \rangle = 0$ para todo $i \not\equiv 0 \pmod{p}$ es decir serán nulas todas las resolventes correspondientes a caracteres primitivos. Por tanto, por (2.2.g) y (2.2.c)) es:

$$p^n \theta = \sum_{\substack{\chi \text{ no prim} \\ \chi = \chi_0}}' \langle \theta, \chi \rangle = p^{n-1} \operatorname{Tr}_{N|L} \theta \Rightarrow \operatorname{Tr}_{N|L} \theta = p\theta \Rightarrow \theta \in L$$

Puesto que $\theta \in K$ es $\theta \in K \cap L = K_1$ es decir $\ker f \subset K_1$.

Reciprocamente, si $\theta \in K_1$ en virtud de (2.2.i), puesto que χ es primitivo, es $\langle \theta, \chi \rangle = 0$ y por tanto $K_1 \subset \ker f$.

Por ser K_1 un subcuerpo de L fijo por $\{1, \tau\}$, es un subcuerpo de N fijo por el subgrupo de G generado por σ^p y τ y por tanto es una extensión de grado p^{n-1} de $\mathfrak{X}$. Puesto que $\dim_{\mathfrak{X}} K = p^n$, $\dim_{\mathfrak{X}} \tilde{k} = \varphi(p^n)$ y $\dim_{\mathfrak{X}} K_1 = p^{n-1}$ queda probado que f es exhaustiva.

Proposición (3.3). Si X es una red de K respecto a A, f(X) es una red de V respecto a A.

En efecto:

X es A-módulo de tipo finito $\Rightarrow$ f(X) es A-módulo de tipo finito

Por otra parte $\mathfrak{X} f(X) = f(\mathfrak{X} X) = f(K) = V$.

Proposición (3.4). f(X) es una red de V respecto A'_0 si y sólo si para cada $\theta \in X$ y cada $\sigma \in H$ es $\sigma\theta + \sigma^{-1}\theta = X + K_1$.

En efecto: En virtud de (1.4.2) bastará probar que la condición se cumple si y sólo si f(X) es estable por el producto por $\zeta + \zeta^{-1}$, siendo ζ una raiz primitiva p^n-ésima de la unidad,

es decir, si y sólo si $(\zeta + \zeta^{-1})f(X) \subset f(X)$. Sea $\theta \in K$; en particular se puede considerar $\theta \in X$. Se tiene:

$$(\zeta + \zeta^{-1})f(\theta) = (\zeta + \zeta^{-1})\frac{\langle \theta, \chi \rangle}{\langle \theta_0, \chi \rangle}$$

Puesto que χ es por hipótesis un caracter primitivo de H , ζ es raiz primitiva p^n-ésima de la unidad, existe un $\sigma \in H$ tal que $\chi(\sigma) = \zeta$. Se puede escribir pues:

$$\left(\zeta + \zeta^{-1}\right)f(\theta) = \left[\chi(\sigma) + \chi(\sigma^{-1})\right]\frac{\langle \theta, \chi \rangle}{\langle \theta_0, \chi \rangle} = \frac{\chi(\sigma)\langle \theta, \chi \rangle}{\langle \theta_0, \chi \rangle} + \frac{\chi(\sigma^{-1})\langle \theta, \chi \rangle}{\langle \theta_0, \chi \rangle} =$$

$$= \frac{\langle \sigma\theta, \chi \rangle}{\langle \theta_0, \chi \rangle} + \frac{\langle \sigma^{-1}\theta, \chi \rangle}{\langle \theta_0, \chi \rangle} = f(\sigma\theta + \sigma^{-1}\theta).$$

Por tanto:

$$(\zeta + \zeta^{-1})f(\theta) = f(\sigma\theta + \sigma^{-1}\theta) \in f(X) \Longleftrightarrow \sigma\theta + \sigma^{-1}\theta \in X + K_1.$$

Corolario (3.5). $f(A_K)$ es una red de V respecto A'_0.

En efecto: A_K es una red de K respecto a A y para todo $\theta \in A_K$ se tiene $\sigma\theta + \sigma^{-1}\theta \in A_K$ por ser A_K fijo por $\{1, \tau\}$.

Teorema (3.6). Sean $\varphi, \psi \in A_K$. Si $(f(\varphi), f(\psi))$ es una A'_0-base del A'_0-módulo $f(A_K)$ y $(Tr_{K/K_1}\varphi , Tr_{K/K_1}\psi)$ es una H_1-base del A-módulo A_{K_1} , entonces si A es principal , (φ, ψ) es una H-base del A-módulo A_K.

En efecto: Si $(f(\varphi), f(\psi))$ es una A_o'-base de $f(A_K)$ se tiene $f(A_k) = A_o' f(\varphi) + A_o' f(\varphi)$. Teniendo en cuenta (1.4.2) es $A_o' = \sum_{i=1}^{1/2\varphi(p^n)} A(\zeta^i + \zeta^{-i})$ por tanto:

$$f(A_K) = \left(\sum_{i=1}^{\frac{1}{2}\varphi(p^n)} A(\zeta^i+\zeta^{-i}) f(\varphi)\right) + \left(\sum_{i=1}^{\frac{1}{2}\varphi(p^n)} A(\zeta^i+\zeta^{-i})(\psi)\right) =$$

$$= \sum_{i=1}^{\frac{1}{2}\varphi(p^n)} A f(\sigma^i\varphi + \sigma^{-i}\varphi) + \sum_{i=1}^{\frac{1}{2}\varphi(p^n)} A f(\sigma^i\psi + \sigma^{-i}\psi).$$

Por otra parte se tiene la sucesión exacta:

$$0 \longrightarrow A_{K_1} \longrightarrow A_K \longrightarrow f(A_K)) \longrightarrow 0$$

Puesto que $f(A_K)$ es un A-módulo proyectivo, por ser de tipo finito, sin torsión y rango mayor que cero, esta sucesión descompone y existe una sección g de f tal que $g: f(A_K) \to A_K$ y

$$A_K \simeq A_{K_1} \oplus gf(A_K) .$$

Sean $g(f(\sigma^i\varphi + \sigma^{-i}\varphi)) = x_i$ $\quad g(f(\sigma^i\psi + \sigma^{-i}\psi)) = y_i$ entonces es

$$A_K \simeq A_{K_1} \oplus \left[\sum_{i=1}^{\frac{1}{2}\varphi(p^n)} A\, x_i + \sum_{i=1}^{\frac{1}{2}\varphi(p^n)} A\, y_i\right]$$

Puesto que $f(\sigma^i\varphi + \sigma^{-i}\varphi) = f(x_i)$ $\quad f(\sigma^i\psi + \sigma^{-i}\psi) = f(y_i)$ es $\sigma^i\varphi + \sigma^{-i}\varphi = a_i + x_i$ y $\sigma^i\psi + \sigma^{-i}\psi = b_i + y_i$

donde a_i , $b_i \in A_{K_1}$. Por tanto:

$$(1). \quad A_K = A_{K_1} + \sum_{i=1}^{\frac{1}{2}q(p^n)} A\,(\sigma^i\varphi + \sigma^{-i}\varphi) + \sum_{i=1}^{\frac{1}{2}\varphi(p^n)} A(\sigma^i\psi + \sigma^{-i}\psi)$$

En esta expresión no aparecen explicitamente $1/2(p^{n-1}-3)$ de los elementos de la H-base de A_K. Se probará que estos aparecen en la H_1-base de A_{K_1} considerada. En efecto; puesto que K es de grado p sobre K_1 se tiene:

$$\varphi_1 = Tr_{K|K_1}\varphi = \sum_{i=1}^{\frac{1}{2}(p-1)} \left(\sigma^{ip^{n-1}} + \sigma^{-ip^{n-1}}\right)\varphi$$

$$\psi_1 = Tr_{K|K_1}\psi = \sum_{i=1}^{\frac{1}{2}(p-1)} \left(\sigma^{ip^{n-1}} + \sigma^{-ip^{n-1}}\right)\psi.$$

Si (φ_1, ψ_1) es una H_1-base de A_{K_1} sus elementos serán de la forma:

$$\sigma^j(Tr_{K/K_1}\varphi) + \sigma^{-j}(Tr_{K/K_1}\varphi) \quad , \quad \sigma^j(Tr_{K/K_1}\psi) + \sigma^{-j}(Tr_{K/K_1}\psi)$$

donde j toma los valores comprendidos entre 1 y $1/2(p^{n-1}-3)$ y por tanto:

$$\sigma^j(\varphi_1) + \sigma^{-j}(\varphi_1) = \sigma^j\left(\varphi + \sum_{i=1}^{\frac{1}{2}(p-1)} \left(\sigma^{ip^{n-1}} + \sigma^{-ip^{n-1}}\right)\varphi\right) +$$

$$\sigma^{-j}\left(\varphi + \sum_{i=1}^{\frac{1}{2}(p-1)} \left(\sigma^{ip^{n-1}} + \sigma^{-ip^{n-1}}\right)\varphi\right) =$$

$$= \left(\sigma^{j}\varphi + \sigma^{-j}\varphi\right) + \sum_{i=1}^{\frac{1}{2}(p-1)} \left(\sigma^{j+ip^{n-1}}\varphi + \sigma^{-(j+ip^{n-1})}\varphi\right) +$$

$$+ \sum_{i=1}^{\frac{1}{2}(p-1)} \left(\sigma^{j-ip^{n-1}}\varphi + \sigma^{-(j-ip^{n-1})}\varphi\right) \qquad 1 \leq j \leq \frac{p^n-3}{2}.$$

y analogamente para $\sigma^{j}(\psi_1) + \sigma^{-j}(\psi_1)$. Se observa que dándole al segundo sumatorio del último miembro de la igualdad a i el valor 1/2(p-1) y a j todos los valores posibles, aparecen todos los elementos de la H-base (φ, ψ) que faltaban en la expresión (1). Expresando A_{K_1} en (1) por medio de la H_1-base (φ_1, ψ_1) queda probado que (φ, ψ) es una H-base de A_K.

C A P I T U L O V

RAMIFICACION. CASO 2pq.

INTRODUCCION.- Como un ápendice a los capítulos anteriores, se estudia en este capítulo la ramificación en el caso en que el grado de la extensión sea 2pq, p y q primos impares. $\underline{A}$, es como siempre un anillo de Dedekind de cuerpo de fracciones $\mathcal{K}$ y N una extensión de $\mathcal{K}$ galoisiana de grupo de Galois G diedral de orden, en este caso, 2pq con p y q primos impares. Se estudia en primer lugar la ramificación en A_N (anillo de los enteros de N) de los primos de A, calculando el discriminante de N respecto a la subextensión cuadrática correspondiente, y el discriminante de N sobre $\mathcal{K}$. Se considera despúes la ramificación de los primos de A en una subextensión de N sobre $\mathcal{K}$ no galoisiana maximal y el comportamiento al pasar a N, de los primos de esta extensión. Finalmente se da una propiedad de A_N como $A[G]$-módulo. Para las definiciones y resultados previos que se utiliza se hará referencia a los capítulos I y II .

1. NOTACIONES E HIPOTESIS PREVIAS.

(1.1). Notaciones.- Sea A un anillo de Dedekind , $\mathfrak{K}$ su cuerpo de fracciones, p y q números primos impares distintos. Sea N una extensión galoisiana, no abeliana de $\mathfrak{K}$, de grupo de Galois G diedral de orden 2pq.

Se sabe que la presentación de G es:

$$G = \langle \sigma, \tau ; \quad \sigma^{pq} = 1, \quad \tau^2 = 1, \quad \tau\sigma\tau = \sigma^{-1} \rangle$$

y que tiene los siguientes subgrupos:

un subgrupo H_p cíclico de orden p de generador σ^p

un subgrupo H_q cíclico de orden q de generador σ^q

un subgrupo H cíclico de orden pq que tiene H_p y H_q como subgrupos; H_p y H_q son divisores normales de G y $H_p \cap H_q = Id$.

pq subgrupos de orden 2, no divisores normales de G, conjugados de uno de ellos g generado por τ .

q subgrupos diedrales de orden 2p, no divisores normales de G, conjugados de uno de ellos h_q generado por $\langle \tau , \sigma^q \rangle$

p subgrupos diedrales de orden 2q, no divisores normales de G, conjugados de uno de ellos h_p generado por $\langle \tau , \sigma^p \rangle$

Se designa por k el subcuerpo de N fijo por H y por L_p y L_q los subcuerpos fijos por H_p y H_q respectivamente. L_p y L_q son extensiones galoisianas de $\mathfrak{K}$ de grupos de Galois diedrales de ordenes 2q y 2p respectivamente, y k es una subextensión

cuadrática de $\mathfrak{K}$, tal que $L_p \cap L_q = k$.

El grupo g se puede considerar como correspondiente a una subextensión K de N de grado pq sobre $\mathfrak{K}$. K no es galoisiana sobre $\mathfrak{K}$ y los cuerpos conjugados de K se corresponden con los subgrupos de G conjugados de g por los automorfismos internos de G. N es galoisiana de grado dos sobre K.

Los subgrupos h_p y h_q se pueden considerar como correspondientes a subextensiones K_p y K_q de grados sobre $\mathfrak{K}$ q y p respectivamente, no galoisianas y los cuerpos conjugados de K_p y K_q se corresponden con los grupos conjugados de h_p y h_q respectivamente en G. K_p y K_q son por tanto por la elección hecha, subcuerpos de K, y N es galoisiana sobre K_p de grupo de Galois diedral de orden 2q, y sobre K_q de grupo de Galois diedral de orden 2p.

A_N, A_{L_p}, A_{L_q}, A_k, A_K, A_{K_p}, A_{K_q} representan las clausuras enteras de A en N, L_p, L_q, k, K, K_p, K_q respectivamente.

(1.2). Hipótesis previas. Sobre el anillo A se harán además las siguientes hipótesis suplementarias:

a) la característica de $\mathfrak{K}$ es distinta de p y de q

b) los cuerpos residuales de A son perfectos

H) p y q son inversibles en A o son producto de ideales maximales distintos.

(1.3) Observación. Téngase en cuenta que los ideales pA y qA no pueden tener ningún ideal primo no nulo en común; pues si la característica de $\mathcal{K}$ es cero, A contiene Z, y si la característica de $\mathcal{K}$ es distinta de cero, de p y de q, p y q son inversibles en A y por tanto pA = qA = A.

2. RAMIFICACION EN N DE LOS IDEALES PRIMOS DE A.

Proposición (2.1). Sea $\bar{\mathfrak{p}}$ un ideal primo de A_k, y $\mathfrak{P}$ un ideal primo de A_{L_p} tal que $\mathfrak{P}$ divide a $\bar{\mathfrak{p}} \cdot \mathfrak{P}$ ramifica en A_N si y sólo si $\bar{\mathfrak{p}}$ ramifica en A_{L_q}.

En efecto:

$$\bar{\mathfrak{p}} \text{ ramifica en } A_{L_q} \Longrightarrow \bar{\mathfrak{p}} A_{L_q} = \mathfrak{q}^p \quad \text{siendo } \mathfrak{q} \text{ primo de } A_{L_q}.$$

Se pueden presentar entonces los tres casos siguientes:

$$\mathfrak{q} A_N = \bar{\mathfrak{q}} \quad \text{o} \quad \mathfrak{q} A_N = \bar{\mathfrak{q}}^q \quad \text{o} \quad \mathfrak{q} A_N = \prod_{i=1}^{q} \bar{\mathfrak{q}}_i$$

y por tanto en correspondencia, puede ser:

$$\bar{\mathfrak{p}} A_N = \bar{\mathfrak{q}}^p \quad \text{o} \quad \bar{\mathfrak{p}} A_N = \bar{\mathfrak{q}}^{pq} \quad \text{o} \quad \bar{\mathfrak{p}} A_N = \prod_{i=1}^{q} \bar{\mathfrak{q}}_i^{\,p}$$

siendo $\bar{\mathfrak{q}}$ y $\bar{\mathfrak{q}}_i$ primos de A_N.

Por otra parte se tiene:

$$(\bar{\mathfrak{p}} A_{L_p})^p = N_{N/L_p}(i(\bar{\mathfrak{p}} A_{L_p}))$$

donde i es la aplicación inyección de A_{L_p} en A_N, y puesto que el grado residual correspondiente a un primo $\mathfrak{P}$ de A_{L_p} en A_N sólo puede ser uno o p, será uno en cada caso, y resulta:

1) $(\overline{\mathfrak{p}}A_{L_p})^p = N_{N/L_p}(\overline{\mathfrak{q}}^p)) = \mathfrak{P}^p \quad \Longrightarrow \quad \overline{\mathfrak{p}}A_{L_p} = \mathfrak{P}$

siendo $\mathfrak{P}$ un primo tal que $\overline{\mathfrak{q}}$ divide a $\mathfrak{P}$ y por tanto $\mathfrak{P}$ ramifica en A_N.

2) $(\overline{\mathfrak{p}}A_{L_p})^p = N_{N/L_p}(\overline{\mathfrak{q}}^{pq}) = \mathfrak{P}^{pq} \quad \Longrightarrow \overline{\mathfrak{p}}A_{L_p} = \mathfrak{P}^q$

es decir $\mathfrak{P}$ ramifica en A_N.

3) $(\overline{\mathfrak{p}}A_{L_p})^p = N_{N/L_p}(\prod_{i=1}^{q}\overline{\mathfrak{q}}_i^{\,p}) = (\prod_{i=1}^{q}N_{N/L_p}(\overline{\mathfrak{q}}_i))^p = (\prod_{i=1}^{q}\mathfrak{P}_i)^p$

$$\Longrightarrow \quad \overline{\mathfrak{p}}A_{L_p} = \prod_{i=1}^{q}\mathfrak{P}_i \quad ,$$

es decir. cada $\mathfrak{P}_i$ que divide a $\overline{\mathfrak{p}}$ ramifica en A_N.

Reciprocamente, sea $\mathfrak{P}$ un primo de A_{L_p} que divide a $\overline{\mathfrak{p}}$, primo de A_k, y que ramifica en A_N. Se tiene $\mathfrak{P}A_N = \overline{\mathfrak{P}}^p$. Puesto que las extensiones son galoisianas, todos los primos que dividen a $\overline{\mathfrak{p}}$ se comportan de la misma manera y por tanto se pueden presentar los casos siguientes:

$$\overline{\mathfrak{p}}A_{L_p} = \mathfrak{P} \qquad \overline{\mathfrak{p}}A_{L_p} = \mathfrak{P}^q \qquad \overline{\mathfrak{p}}A_{L_p} = \prod_{i=1}^{q}\mathfrak{P}_i \quad \text{con } \mathfrak{P} = \mathfrak{P}_i$$

y los correspondientes:

$$\overline{\mathfrak{p}}A_N = \overline{\mathfrak{P}}^p \qquad \overline{\mathfrak{p}}A_N = \overline{\mathfrak{P}}^{pq} \qquad \overline{\mathfrak{p}}A_N = \prod_{i=1}^{q}\overline{\mathfrak{P}}_i^{\,p}$$

$\bar{\mathfrak{p}}$ ramifica en A_N con índice de ramificación en cada caso múltiplo de p, por tanto teniendo en cuenta $[N:L_q] = q$ y $[L_q:k] = p$ $\bar{\mathfrak{p}}$ ramifica en L_q con índice de ramificación p.

Proposición (2.2). Ningún primo $\mathfrak{p}$ de A puede ramificar totalmente en A_N.

En efecto: Si $\mathfrak{p} \nmid \mathfrak{d}_{k/x}$, no ramifica en A_k y por tanto no puede ramificar totalmente en A_N. Si $\mathfrak{p} \mid \mathfrak{d}_{k/x}$, sea $\bar{\mathfrak{p}}^2 = \mathfrak{p} A_k$; si $\mathfrak{p} \nmid pA$ y $\mathfrak{p} \nmid qA$, $\bar{\mathfrak{p}}$ descompondrá totalmente en A_{L_p} y en A_{L_q} (II,2.14) y por tanto no puede ramificar en A_N. Si $\mathfrak{p} \nmid pA$ y $\mathfrak{p} / qA$ o $\mathfrak{p} / pA$ y $\mathfrak{p} \nmid qA$, $\mathfrak{p}$ podrá ramificar en A_{L_p} o en A_{L_q} pero no en ambas.

Para el cálculo del discriminante de N sobre k se supondrá que A es de valoración discreta estudiando los diversos casos que pueden presentarse según el comportamiento del ideal maximal $\mathfrak{p}$ considerado.

Proposición (2.3). Si $\mathfrak{p}$ es un ideal de A tal que $\mathfrak{p} \mid \mathfrak{d}_{k/x}$ siendo $\bar{\mathfrak{p}}^2 = \mathfrak{p} A_k$, entonces si $p \geq 5$ y $\bar{\mathfrak{p}}$ ramifica en N es:

$$\mathfrak{d}_{N/k} = \mathfrak{p}^{(p-1)q} \qquad \text{si} \qquad \mathfrak{p} \mid pA$$

$$\mathfrak{d}_{N/k} = \mathfrak{p}^{(q-1)p} \qquad \text{si} \qquad \mathfrak{p} \mid qA$$

En efecto: En virtud de (2.2) $\bar{\mathfrak{p}}$ puede ramificar en A_{L_p} o

en A_{L_q} pero no en ambos. Por tanto, si $\mathfrak{p} \mid qA$ y es $\mathfrak{p} A_k = \bar{\mathfrak{p}}^2$ y $\bar{\mathfrak{p}} A_{L_p} = \mathfrak{P}^q$, $\mathfrak{P}$ no puede ramificar en A_N por (2.1) y por tanto $\mathfrak{P} \nmid \vartheta_{N/L_p}$. Teniendo en cuenta (II.2.8) y (II 2.15c)) resulta:

$$\vartheta_{N/k} = (\vartheta_{L_p/k})^p N_{L_p/k}(\vartheta_{N/L_p}) = \mathfrak{p}^{(q-1)p}$$

El mismo razonamiento aplicado al caso $\mathfrak{p} \mid pA$ da:

$$\vartheta_{N/k} = (\vartheta_{L_q/k})^q N_{L_q/k}(\vartheta_{N/L_q})) = \mathfrak{p}^{(p-1)q}$$

Observación (2.4). Si uno de los primos p o q fuera igual a tres, sea p, si $\mathfrak{p} \mid pA$ tiene que tenerse en cuenta que puede presentarse algún caso en que el discriminante $\vartheta_{N/k}$ sea $\mathfrak{p}^{2(p-1)q}$. Si este caso efectivamente se presenta no se sabe.

Proposición (2.5). Si $\mathfrak{p} \nmid \vartheta_{k/x}$ y $\mathfrak{p}$ ramifica en A_{L_p} y A_{L_q} se tiene:

a) $\mathfrak{p} \nmid pA$, $\mathfrak{p} \nmid qA$ $\Longrightarrow$ $\vartheta_{N/k} = \mathfrak{p}^{pq-1}$

b) $\mathfrak{p} \nmid pA$, $\mathfrak{p} \mid qA$ $\Longrightarrow$ $\vartheta_{N/k} = \mathfrak{p}^{p(2q-1)-1}$

c) $\mathfrak{p} \nmid qA$, $\mathfrak{p} \mid pA$ $\Longrightarrow$ $\vartheta_{N/k} = \mathfrak{p}^{q(2p-1)-1}$

En efecto: Si $\bar{\mathfrak{p}}$ es un ideal de A_k que divide a $\mathfrak{p}A_k$, es:

a) $\bar{\mathfrak{p}}$ ramifica total y moderadamente en A_N y por tanto $v_{\bar{\mathfrak{p}}}(\mathfrak{d}_{N/k}) = pq-1$. Puesto que todos los primos de A_k que dividen a $\mathfrak{p}$ se comportan de igual manera es $\mathfrak{d}_{N/k} = \mathfrak{p}^{pq-1}$.

b) $\bar{\mathfrak{p}}$ ramifica fuertemente en A_{L_p} y es $\bar{\mathfrak{p}}A_{L_p} = \mathfrak{P}^q$, y $\mathfrak{P}$ ramifica moderadamente en A_N y es $\mathfrak{P}A_N = \bar{\mathfrak{P}}^p$. En virtud de (II.(2.15) 1b)es $\mathfrak{d}_{L_p/k} = \bar{\mathfrak{p}}^{2(q-1)}$ y además $\mathfrak{d}_{N/L_p} = \mathfrak{P}^{p-1}$

Por tanto:

$$\mathfrak{d}_{N/k} = (\mathfrak{d}_{L_p/k})^p N_{L_p/k}(\mathfrak{d}_{N/L_p}) = \bar{\mathfrak{p}}^{2p(q-1)} N_{L_p/k}(\mathfrak{P}^{p-1}) =$$

$$\bar{\mathfrak{p}}^{2p(q-1)}\bar{\mathfrak{p}}^{p-1} = \bar{\mathfrak{p}}^{p(2q-1)-1}$$

Puesto que todos los $\bar{\mathfrak{p}}$ de A_k que dividen a $\mathfrak{p}$ tienen el mismo exponente en $\mathfrak{d}_{N/k}$ es $\mathfrak{d}_{N/k} = \mathfrak{p}^{p(2q-1)-1}$

c) la demostración es análoga a la del caso b).

<u>Proposición (2.6)</u> . <u>Si</u> $\mathfrak{p} \nmid \mathfrak{d}_{k/\mathbb{Q}}$ <u>y</u> $\mathfrak{p}$ <u>ramifica sólo en</u> A_{L_p} <u>o sólo en</u> A_{L_q} <u>se tiene</u>:

a) <u>ramifica en</u> A_{L_q} ; <u>si</u> $\mathfrak{p} \nmid pA \Longrightarrow \mathfrak{d}_{N/k} = \mathfrak{p}^{(p-1)q}$

<u>si</u> $\mathfrak{p} \mid pa \Longrightarrow \mathfrak{d}_{N/k} = \bar{\mathfrak{p}}^{2(p-1)q}$

b) <u>ramifica en</u> A_{L_p} ; <u>si</u> $\mathfrak{p} \nmid qA \Longrightarrow \mathfrak{d}_{N/k} = \mathfrak{p}^{(q-1)p}$

<u>si</u> $\mathfrak{p} \mid qA \Longrightarrow \mathfrak{d}_{N/k} = \mathfrak{p}^{2(q-1)p}$

Es consecuencia inmediata de (II. (2.15) 1 a,b) .

Como consecuencia de las proposiciones (2.3), (2.5), (2.6) y observando que por ser p y q números primos los exponentes que aparecen afectando a $\mathfrak{p}$ en las expresiones obtenidas en ellas son todos números pares, se puede enunciar el siguiente:

Teorema (2.7). El discriminante $\vartheta_{N/k}$ es el cuadrado de un ideal $\mathcal{J}$ de A cuya expresión es la siguiente:

$$\mathcal{J} = \prod_1 \left(\mathfrak{p}^{\frac{p-1}{2}q}\right) \prod_2 \left(\mathfrak{p}^{\frac{q-1}{2}p}\right) \prod_3 \left(\mathfrak{p}^{\frac{pq-1}{2}}\right) \prod_4 \left(\mathfrak{p}^{(p-1)q}\right) \prod_5 \left(\mathfrak{p}^{(q-1)p}\right) \prod_6 \left(\mathfrak{p}^{\frac{p(q-1)q}{2}}\right) \prod_7 \left(\mathfrak{p}^{\frac{q(2p-1)-1}{2}}\right)$$

$\prod_1 : \left(\mathfrak{p} \mid \vartheta_{k|x}\,,\ \mathfrak{p} \mid pA\right)$ ó $\left(\mathfrak{p} \nmid \vartheta_{k|x},\ \mathfrak{p} \nmid pA,\ \mathfrak{p} \mid \vartheta_{L_q|k},\ \mathfrak{p} \nmid \vartheta_{L_p|k}\right)$

$\prod_2 : \left(\mathfrak{p} \mid \vartheta_{k|x},\ \mathfrak{p} \mid qA\right)$ ó $\left(\mathfrak{p} \nmid \vartheta_{k|x},\ \mathfrak{p} \nmid qA,\ \mathfrak{p} \mid \vartheta_{L_p|k},\ \mathfrak{p} \nmid \vartheta_{L_q|k}\right)$

$\prod_3 : \left(\mathfrak{p} \nmid \vartheta_{k|x},\ \mathfrak{p} \nmid pA,\ \mathfrak{p} \nmid qA,\ \mathfrak{p} \mid \vartheta_{L_p|k},\ \mathfrak{p} \mid \vartheta_{L_q|k}\right)$

$\prod_4 : \left(\mathfrak{p} \nmid \vartheta_{k|x},\ \mathfrak{p} \mid pA,\ \mathfrak{p} \mid \vartheta_{L_q|k}\right)$

$\prod_5 : \left(\mathfrak{p} \nmid \vartheta_{k|x},\ \mathfrak{p} \mid qA,\ \mathfrak{p} \mid \vartheta_{L_p|k}\right)$

$\prod_6 : \left(\mathfrak{p} \nmid \vartheta_{k|x},\ \mathfrak{p} \mid qA,\ \mathfrak{p} \mid \vartheta_{L_p|k},\ \mathfrak{p} \mid \vartheta_{L_q|k}\right)$

$\prod_7 : \left(\mathfrak{p} \nmid \vartheta_{k|x},\ \mathfrak{p} \mid pA,\ \mathfrak{p} \mid \vartheta_{L_p|k},\ \mathfrak{p} \mid \vartheta_{L_q|k}\right)$

donde cada Π_i se extiende a los primos $\mathfrak{p}$ de A que cumplen las condiciones reseñadas.

Corolario (2.8). $\mathfrak{d}_{N/k} = \mathfrak{d}_{k/\mathfrak{x}}^{pq} \mathfrak{J}^4$.

En efecto: Por (II. 2.8) y (2.7) es :

$$\mathfrak{d}_{N/k} = \left(\mathfrak{d}_{k/\mathfrak{x}}\right)^{pq} N_{k/\mathfrak{x}}(\mathfrak{d}_{N/k}) = \left(\mathfrak{d}_{k/\mathfrak{x}}\right)^{pq} N_{k/\mathfrak{x}}(\mathfrak{J}^2)) = \mathfrak{d}_{k/\mathfrak{x}}^{pq} \mathfrak{J}^4 .$$

3. RAMIFICACION EN K DE LOS IDEALES PRIMOS DE A

Obsérvese en primer lugar que en la demostración de la proposición (II. 4.1) no interviene para nada el grado de la extensión K sobre $\mathfrak{x}$, y por tanto aquella proposición es también válida en este caso.

Proposición (3.1). Si $\mathfrak{p}$ es un ideal primo no nulo de A que divide a $\mathfrak{d}_{k/\mathfrak{x}}$, existe un ideal primo no nulo $\mathfrak{P}_i$ de A_K y uno sólo, que divide a $\mathfrak{p}$ y tal que $\mathfrak{P}_i$ divide a $\mathfrak{d}_{N/K}$.

Para la demostración de esta proposición se necesita el siguiente lema previo:

Lema (3.3). Sea $\mathfrak{p}$ un ideal primo no nulo de A tal que $\mathfrak{p} \mid \mathfrak{d}_{k/\mathfrak{x}}$, $\mathfrak{p} \nmid pA$, $\mathfrak{p} \nmid qA$ y $\mathfrak{p}A_k = \bar{\mathfrak{p}}^2$. Entonces $\bar{\mathfrak{p}}$ descompone en el producto de pq ideales primos distintos.

Es consecuencia de (2.14)del CapII.

Demostración de la proposición (3.1).

Se pueden presentar los dos casos siguientes:

Caso 1) $\mathfrak{p} \mid \mathfrak{d}_{k/\mathfrak{x}}$, $\mathfrak{p} \mid \mathfrak{J}$ $\Rightarrow$ $\mathfrak{p} \mid pA$ o $\mathfrak{p} \mid qA$.

Supóngase que $\mathfrak{p} \mid pA$ (si $\mathfrak{p} \mid qA$ se procedería de manera análoga). Se tiene: $\mathfrak{p}^{A_N} = \overline{\mathfrak{P}}_1^{2q} \dots \overline{\mathfrak{P}}_p^{2q} = \prod_{\sigma \in H_p} \overline{\mathfrak{P}}_\sigma^{2q}$ donde $\overline{\mathfrak{P}}_\sigma$ son los conjugados de $\overline{\mathfrak{P}}_1$ por los elementos de H_p. Los grupos de descomposición de los $\overline{\mathfrak{P}}_i$ en la extensión $N/\mathfrak{x}$ son los p grupos diedrales de orden 2q ,subgrupos de G, y por tanto se puede suponer que uno de ellos es el h_p que contiene g, cuyo cuerpo fijo es el subcuerpo K_q de K. Sea $\overline{\mathfrak{P}}_1$ el primo que corresponde a h_p. Se tiene:

$$\mathfrak{p}^{A_{K_q}} = N_{N/K_q}\Big(\prod_{\sigma \in H_p} \overline{\mathfrak{P}}_\sigma^{2q}\Big)^{1/2q} = \prod_{\sigma \in H_p} \big(N_{N/K_q}\, \overline{\mathfrak{P}}_\sigma\big)$$

Es $N_{N/K_q}(\overline{\mathfrak{P}}_1) = \overline{\mathfrak{P}}_1 \cap K_q = \mathfrak{P}_1$ y se indicará por $\mathfrak{P}_\sigma$ la $N_{N/K_q}\, \overline{\mathfrak{P}}_\sigma$ si σ es distinto de la identidad. Por tanto

$$\mathfrak{p}^{A_{K_q}} = \mathfrak{P}_1 \prod_{\substack{\sigma \in H_p \\ \sigma \neq \mathrm{Id.}}} \mathfrak{P}_\sigma \quad .$$

Puesto que K_q es el subcuerpo de L_q fijo por g. uno y sólo uno de estos primos, y precisamente el $\mathfrak{P}_1$ ramificará en A_{L_q} y por tanto uno y sólo uno dividirá a $\mathfrak{d}_{L_q/K_q}$. Aplicando la proposición (II.2.17) a la extensión L_q/K_q resulta que de los primos de K que dividen a $\mathfrak{p}$, sólo pueden dividir a $\mathfrak{d}_{N/K}$. los que dividen a $\mathfrak{P}_1$, y de estos uno y sólo uno.

Nota: Obsérvese que el anillo A_{K_q} no verificará en general

la hipótesis H. Sin embarho se puede aplicar la proposición (II 2.17) a la extensión L_q/K_q pues en su demostración no interviene dicha hipótesis.

Caso 2). $\mathfrak{p} \mid \mathfrak{d}_{k/\mathfrak{o}}$ y $\mathfrak{p} \nmid \mathcal{J}$ $\Longrightarrow$ $\mathfrak{p}A_k = \bar{\mathfrak{p}}^2$ $\bar{\mathfrak{p}}A_N = \prod_{i=1}^{pq} \bar{\mathfrak{P}}_i$

Teniendo en cuenta que los $\mathfrak{P}_i$ son conjugados de uno de ellos por los elementos $\sigma \in H$, $\bar{\mathfrak{p}}A_N$ se puede expresar de la siguiente manera:

$$\bar{\mathfrak{p}}A_N = \prod_{\sigma \in H} \bar{\mathfrak{P}}_\sigma \quad \text{donde} \quad \bar{\mathfrak{P}}_\sigma = \sigma(\bar{\mathfrak{P}}_1) \Longrightarrow \mathfrak{p}A_N = \prod_{\sigma \in H} \bar{\mathfrak{P}}_\sigma^2 .$$

Por otra parte:

$$\mathfrak{p}^{A_K} = (N_{N/K}(i(\mathfrak{p}A_K))^{1/2} = N_{N/K}(\prod_{\sigma \in H} \bar{\mathfrak{P}}_\sigma) = \prod_{\sigma \in H} N_{N/K}\, \bar{\mathfrak{P}}_\sigma$$

Los grupos de descomposición de $\bar{\mathfrak{P}}_\sigma$ en la extensión $N/\mathfrak{o}$ son subgrupos de G de orden 2 conjugados de uno de ellos, por tanto, se puede suponer que $\bar{\mathfrak{P}}_1$ es el primo que corresponde al grupo g (cambiando los subíndices si fuera necesario). Poniendo:

$\mathfrak{P}_1 = \bar{\mathfrak{P}}_1 \cap A_K$ y $\mathfrak{P}_\sigma = N_{N/K}(\bar{\mathfrak{P}}_\sigma)$ si σ es distinto de la identidad, se tiene:

$$\mathfrak{p}^{A_K} = \mathfrak{P}_1 \prod_{\substack{\sigma \in H \\ \neq \mathrm{Id.}}} \mathfrak{P}_\sigma .$$

Los ideales $\mathfrak{P}_\sigma$ son todos ellos ideales primos de A_K por tanto $\mathfrak{p}^{A_K}$ es el producto de pq ideales primos. Estos no son todos distintos sino que los pq-1 $\mathfrak{P}_\sigma$ son iguales dos a dos. En efec-

to, por ser N/K galoisiana de grupo de Galois de orden 2, el número máximo de primos de N que pueden dividir a un mismo primo de K es dos y esto tiene lugar si y sólo si uno es conjugado del otro respecto a un automorfismo del grupo de Galois, es decir: $\mathfrak{P}_i = \mathfrak{P}_j \iff \overline{\mathfrak{P}}_j = \tau\overline{\mathfrak{P}}_i$. Puesto que

$$\overline{\mathfrak{P}}_i = \sigma^i(\overline{\mathfrak{P}}_1) \quad , \quad \overline{\mathfrak{P}}_j = \sigma^j(\overline{\mathfrak{P}}_1) \quad , \quad \overline{\mathfrak{P}}_1 = \tau(\overline{\mathfrak{P}}_1)$$

resulta:

$$\mathfrak{P}_i = \mathfrak{P}_j \iff \tau\sigma^j\tau = \sigma^i \iff i = -j .$$

Se tiene pues:

$$\mathfrak{p}^{A_K} = \mathfrak{P}_1\mathfrak{P}_2^2 \cdots \mathfrak{P}_{1/2(pq+1)}^2$$

es decir, en A_N uno solo de los primos ramifica y los demás descomponen, por tanto, un primo y sólo uno ramifica en N sobre K.

<u>Proposición (3.4)</u>. $N_{K/\mathfrak{x}}(\mathfrak{d}_{N/K}) = \mathfrak{d}_{k/\mathfrak{x}}$

La demostración es análoga a la de (II 4.3).

<u>Teorema (3.5).</u> $\mathfrak{d}_{K/\mathfrak{x}} = \mathfrak{d}_{k/\mathfrak{x}}^{1/2(pq-1)} \mathfrak{J}^2$

En efecto:

$$\left(\mathfrak{d}_{K/\mathfrak{x}}\right)^2 N_{K/\mathfrak{x}}(\mathfrak{d}_{N/K}) = \mathfrak{d}_{N/\mathfrak{x}} = \mathfrak{d}_{K/\mathfrak{x}}^{pq} \mathfrak{J}^4$$

En virtud de (3.4)

$$\mathfrak{d}_{K/\mathfrak{x}}^2 \mathfrak{d}_{k/\mathfrak{x}} = \mathfrak{d}_{k/\mathfrak{x}}^{pq} \mathfrak{J}^4 \Rightarrow \mathfrak{d}_{K/\mathfrak{x}} = \mathfrak{d}_{k/\mathfrak{x}}^{1/2(pq-1)} \mathfrak{J}^2$$

Proposición (3.6). Sea A un anillo de Dedekind de cuerpo de fracciones $\mathfrak{K}$, N una extensión de $\mathfrak{K}$ galoisiana de grupo de Galois G diedral de orden 2pq (p, q primos impares). Se supone: que A es principal, que la característica de $\mathfrak{K}$ no divide a 2pq, que A/pA es isomorfo a Z/pZ y A/qA es isomorfo a Z/qZ. Entonces, si A_{K_p}, A_{K_q} y A_K poseen A-bases normales, A_N es un $A[G]$-módulo proyectivo.

En efecto: Puesto que L_p y L_q son extensiones de $\mathfrak{K}$, galoisianas, diedrales de ordenes 2p y 2q respectivamente que cumplen las hipótesis de ([12]1.IV), A_{L_p} es $A[h_q]$-libre y A_{L_q} es $A[h_p]$-libre, por tanto A_{L_p} es $A[h_q]$-proyectivo y A_{L_q} es $A[h_p]$- proyectivo y L_p y L_q son moderadamente ramificadas sobre $\mathfrak{K}$. De (2.1) resulta que N es moderadamente ramificada sobre $\mathfrak{K}$ y por tanto A_N es $A[G]$- proyectivo.

BIBLIOGRAFIA CITADA.

[1]. ANKENY-CHOWLA-HASSE
"On the class-number of the maximal real sub-field of cyclotomic fields".
Jour. reine angew. Math. 217. 1965 .

[2] . ARTIN-TATE
Class Field Theorie.
Benjamin. 1967

[3] . BAYER , Pilar
"Sobre la cohomología del anillo de los enteros de un cuerpo de números"
Jornadas Hispano-Lusitanas. Madrid 1973. (Por aparecer))

[4]. BIRCH , B.J.
Cyclotomic Fields and Kummer extensions.
Algebraic number theory. Procedings 1967.

[5]. BOURBAKI
Algêbre commutative. Chap.7 . Diviseurs.
Hermann. Paris 1965.

[6]. FROHLICH , A
Local Fields.
Algebraic number theory. Procedings. 1967.

[7]. FROHLICH , A
The module structure of Kummer extensions over Dedekind domains.
Jour. reine angew. Math. 209. 1962.

[8]. LEE , M. P.
"Integral representations of diedral groups of order 2p".
Trans. Ann. Soc. 110. 1964.

[9]. LEOPOLD, H. W.
"Uber die Hauptornung der ganzen Elemente eines abelschen Zahlkörpers".
Jour. rein. angew. Math. 201. 1959.

[10]. MARTINET-PAYAN
"Sur les extensions cúbiques non galoisiennes des rationnels et leur cloture galoisienne".
Jour. rein. angew. Math. 228.1967.

[11]. MARTINET- PAYAN
"Sur les bases d'entiers des extensions galoisiennes el non abelienes de degre 6 des rationnels.
Jour. rein. angew. Math. 229. 1968.

[12]. MARTINET, J.
"Sur l'arithmetique des extensions galoisennes a grpup de Galois diedral d'ordre 2p".
Ann. Inst. Fourier. Grenoble 19. 1 1969.

[13]. MARTINET, J.
"Modules sur l'algebre du group quaternionien".
Ann. Scient. Ecole Normal Sup. 4ºs. IV fas 3 1971.

[14]. NOETHER, EMMY
"Normal basis bei Körpern ohne höhere Verzweigung"
Jour. rein. angew. Math. 163 .1931

[15]. RIM, S
"Modules over finite groups".
Annals of Math. 69. 1959

[16]. SAFAREVIC
"Construction of fields of algebraic numbers with given solvable Galois group"
Amer. Math. Soc. Trans. 1960.

[17]. SERRE, J.P.
Corps Locaux
Hermann. Paris 1967.

[18]. ULLOM ,S.
"Normal basis in Galois extensions of number fields"
Nagoya Math. Jour. Vol. 34 . 1969.

[19]. ULLOM, S
"Integral normal basis en Galois extensions of local fields".
Nagoya Math. Jour. Vol 39. 1970.

[20]. WEIL, HERMANN
Algebraic theory of numbers.
Princeton 1940.