Franz Halter-Koch

Construction of continuous idele class characters in quadratic number fields, and imbedding problems for dihedral and quaternion fields

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 17, nº 1 (1975-1976), exp. nº 14, p. 1-13

<http://www.numdam.org/item?id=SDPP_1975-1976__17_1_A13_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
17e année, 1975/76, n° 14, 13 p.

12 janvier 1976

CONSTRUCTION OF CONTINOUS IDELE CLASS CHARACTERS IN QUADRATIC NUMBER FIELDS, AND IMBEDDING PROBLEMS FOR DIHEDRAL AND QUATERNION FIELDS

by Franz HALTER-KOCH

The imbedding problem for algebraic number fields with abelian kernel has been studied in detail by NEUKIRCH [7] on the basis of the duality theorems of Tate and Poitou. We established a local-global-principle which says, that in almost all cases an imbedding problem with abelian kernel has a (global) solution if, and only if, all associated local imbedding problems are soluble. POITOU [8] dealt with the exceptional case which, in case of cyclic kernel, only occurs if it contains an element of order 8 . He proved that in this case there is at most one global condition which guarantees the solubility of the (global) imbedding problem if all the associated local problem have a solution. Furthermore, he presented a cohomological description of the additional global confition.

In the present paper, I deal with the problem of imbedding a dihedral field of 2-power degree in a dihedral or quaternion field of higher degree. These are the simplest examples of imbedding problems with abelian kernel for which the solubility of all associated local problems is not sufficient for the existence of a global solution. I do not use the cohomological formalism established by NEUKIRCH and POITOU (it seems to be very difficult to carry out the necessary calculations in the present case) ; I shall solve the problem by an explicit construction of the defining idele class character in that quadratic number field over which all considered dihedral and quaternion fields are cyclic. This method traces back to HASSE's paper [6] on cubic fields and has also been used in [3], [9] and [11] ; it has the disadvantage of beeing very special but the advantage of beeing constructive modulo Dirichlet's theorem on primes in arithmetic progression.

1. Class field theoretic characterisation of extensions with dihedral or quaternion group of order 2^{n+1} .

For $n \geq 0$, let

$$D_n = \langle S , T ; \; S^{2^n} = T^2 = 1 , \; ST = TS^{-1} \rangle$$

be the dihedral group of order 2^{n+1} and

$$H_n = \langle S , T ; \; S^{2^n} = 1 , \; T^2 = S^{2^{n-1}} , \; ST = TS^{-1} \rangle$$

the quaternion group of order 2^{n+1} . Both groups have the canonical normal series

$$\langle S , T \rangle \supset \langle S \rangle \supset \langle S^2 \rangle \supset \dots \supset \langle S^{2^\nu} \rangle \supset \dots \supset \langle 1 \rangle ,$$

and for any $0 \leqslant \nu < n$ the group $\langle S, T\rangle/\langle S^{2^\nu}\rangle$ is a dihedral group of order $2^{\nu+1}$.

Let k be an algebraic number field and Ω_n/k an extension with Galois group $\langle S, T\rangle$ (in the sequel I shall call Ω_n a dihedral or a quaternion field over k). For $\nu \geqslant 0$, let Ω_ν be the fixed field of S^{2^ν}; then I have

$$k \subset \Omega_0 \subset \Omega_1 \subset \dots \subset \Omega_\nu \subset \dots \subset \Omega_n ,$$

where Ω_ν/k is a dihedral field of degree $2^{\nu+1}$ for any $\nu < n$, and Ω_ν/Ω_0 is cyclic for any $\nu \leqslant n$. Let I_0 be the idele group of Ω_0; Ω_n is class field to an idele class character of degree 2^n of Ω_0, that means, to a continuous surjective homomorphism $L : I_0 \longrightarrow \underset{\sim}{Z}/2^n \underset{\sim}{Z}$, which is trivial on $\Omega_0^\times \subset I_0$. Let $\tau = T|\Omega_0$ be the generating automorphism for Ω_0/k, and L^τ be defined by $L^\tau(\alpha) = L(\alpha^\tau)$ for any idele $\alpha \in I_0$. Then I derive $L^\tau = -L$ according to the relation $T^{-1}ST = S^{-1}$ and, by computing the kernel of the transfer $\langle S,T\rangle \longrightarrow \langle S\rangle$, I obtain $L|I_k = \underset{\sim}{0}$ in the dihedral case and $L|I_k \neq \underset{\sim}{0}$ in the quaternion case, more precisely, in the quaternion case $L|I_k$ defines the extension Ω_0/k (I_k denotes the idele group of k).

Conversely, if Ω_0/k is any quadratic extension of algebraic number fields with generating automorphism τ_0, and $L : I_0 \longrightarrow \underset{\sim}{Z}/2^n \underset{\sim}{Z}$ is an idele class character of degree 2^n with associated class field Ω_n, then Ω_n/k is dihedral or quaternion if, and only if, $L^\tau = -L$; it is dihedral if $L|I_k = \underset{\sim}{0}$ and quaternion if $L|I_k$ defines Ω_0/k.

2. Construction of idele class characters.

Let ℓ be a prime, $n \geqslant 1$, k an algebraic number field with idele group I and $\underset{\sim}{P}$ be the set of all places of k. For any $\mathfrak{p} \in \underset{\sim}{P}$, I denote by $k_\mathfrak{p}$ the local completion of k at $\mathfrak{p}$; if $\mathfrak{p} \in \underset{\sim}{P}$ is finite then $U_\mathfrak{p}$ is the group of units, and $U_\mathfrak{p}^1$ the group of einseinheiten of $k_\mathfrak{p}$; if $\mathfrak{p} \in \underset{\sim}{P}$ is archimedian, I set $U_\mathfrak{p} = k_\mathfrak{p}^\times$, $U_\mathfrak{p}^1 = \underset{\sim}{R}_+^\times$, if $\mathfrak{p}$ is real, and $U_\mathfrak{p}^1 = \underset{\sim}{C}^\times$ if $\mathfrak{p}$ is complex. Let $c_1, \dots, c_h \in I$ be representatives of a system of generators for the ℓ-class-group of k, that means, for the ℓ-Sylow subgroup of $I/(\prod_{\mathfrak{p}\in\underset{\sim}{P}} U_\mathfrak{p}).k^\times$. Let $A = \langle c_1, \dots, c_h\rangle \subset I$ be the free abelian group generated by $c_1, \dots, c_h$; then multiplication of ideles defines a homomorphism

$$\Phi : A \times \prod_{\mathfrak{p}\in\underset{\sim}{P}} U_\mathfrak{p} \longrightarrow I/k^\times$$

and, an idele class character $L : I \longrightarrow \underset{\sim}{Z}/\ell^n \underset{\sim}{Z}$ of degree ℓ^n of k is uniquely determined by its "restricted local components"

$$L_A = L|A : A \longrightarrow \underset{\sim}{Z}/\ell^n \underset{\sim}{Z} \quad \text{and} \quad L_\mathfrak{p} = L|U_\mathfrak{p} : U_\mathfrak{p} \longrightarrow \underset{\sim}{Z}/\ell^n \underset{\sim}{Z} .$$

If on the other hand a homomorphism $L_A : A \longrightarrow \underset{\sim}{Z}/\ell^n \underset{\sim}{Z}$ and a family of continuous homomorphisms $(L_\mathfrak{p} : U_\mathfrak{p} \longrightarrow \underset{\sim}{Z}/\ell^n \underset{\sim}{Z})_{\mathfrak{p}\in\underset{\sim}{P}}$ (almost all equal 0) are given, they are the restricted local components of an idele class character if, and only if, for all pairs $(\prod_{\nu=1}^{h} c_\nu^{u_\nu}, (\beta_p)_{p\in \underset{\sim}{P}}) \in \ker \Phi$ the relation

$$L_A(\prod_{\nu=1}^{h} c_\nu^{u_\nu}) + \sum_{p\in \underset{\sim}{P}} L_p(\beta_p) = 0$$

holds ; of course, this condition must only be satisfied by a system of generators for $\ker \Phi$. Let $\Gamma \subset k^\times$ be the group of all $\alpha \in k^\times$ whose associated principal ideal $\langle\alpha\rangle$ is an ℓ-th power and, let $(\gamma_i)_{i\in I} \subset k^\times$ be representatives of a system of generators for $\Gamma/k^{\times\ell}$. The principal ideles (γ_i) can be written in the form

$$(\gamma_i) = \prod_{\nu=1}^{h} c_\nu^{u_{\nu i}}\cdot(\beta_p^{(i)})_{p\in \underset{\sim}{P}}\cdot(\alpha_i^\ell)$$

with $u_{\nu i} \in \underset{\sim}{Z}$, $u_{\nu i} \equiv 0 \bmod \ell$, $\beta_p^{(i)} \in U_p$, $\alpha_i \in k^\times$, and the elements

$$(\prod_{\nu=1}^{h} c_\nu^{u_{\nu i}}, (\beta_p^{(i)})_{p\in \underset{\sim}{P}})_{i\in I}$$

generate $\ker \Phi$.

Now it is obvious that $(L_A, (L_p)_{p\in \underset{\sim}{P}})$ is the system of restricted local components of an idele class character if, and only if, it satisfies the "compatibility conditions"

$$(C_i) \qquad \sum_{\nu=1}^{h} u_{\nu i}\cdot L_A(c_\nu) + \sum_{p\in \underset{\sim}{P}} L_p(\beta_p^{(i)}) = 0$$

for all $i \in I$.

If an idele class character $L : I \longrightarrow \underset{\sim}{Z}/\ell^n \underset{\sim}{Z}$ is given by its restricted local components $(L_A, (L_p)_{p\in \underset{\sim}{P}})$ the full local components $\overline{L}_p : k_p^\times \longrightarrow \underset{\sim}{Z}/\ell^n \underset{\sim}{Z}$ can be computed as follows : Let $\pi \in k$ be a prime element of k_p ; then for a suitable integer $r \not\equiv 0 \bmod \ell$ there is a representation

$$(\pi^r) = \prod_{\nu=1}^{h} c_\nu^{u_\nu}\cdot(\xi_p)_{p\in \underset{\sim}{P}}\cdot(\omega)$$

with $u_\nu \in \underset{\sim}{Z}$, $\xi_p \in U_p$, $\omega \in k^\times$, and consequently

$$\overline{L}_p(\pi) = \frac{1}{r}\cdot[L_A(\prod_{\nu=1}^{h} c_\nu^{u_\nu}) + \sum_{p\in \underset{\sim}{P}} L_p(\xi_p)] .$$

The advantage of the description of an idele class character by restricted local components consists in the fact, that the conditions (C_i) under which a system of given restricted local components can be put together are rather simple.

3. Description of dihedral and quaternion fields over $\underset{\sim}{Q}$.

In the following considerations I restrict myself to the case $k = \underset{\sim}{Q}$, though part of it might be carried out in general. Let $\Omega_0 = \underset{\sim}{Q}(\sqrt{D})$ be a quadratic number field, $D \in \underset{\sim}{Z}$ square-free, $D = \pm d$ or $D = \pm 2d$, where $d = p_1 \dots p_t$ with different odd primes $p_1, \dots, p_t$ $(t \geqslant 0)$. Let τ be the generating automorphism, $\underset{\sim}{P}$ the set of all places, and I_0 the idele group of Ω_0 . Let $\hat{p}_1, \dots, \hat{p}_h$ be prime ideals of first degree of Ω_0 such that their ideal classes generate the 2-class group of Ω_0 , and let $\hat{p}_1, \dots, \hat{p}_h$ be the associated primes. I denote by c_ν that idele of Ω_0 whose p_ν-component is $\hat{p}_\nu$ and whose other components are 1 , and then I set $A = \langle c_1 , \ldots , c_h \rangle \subset I_0$.

Now let $L : I_0 \longrightarrow \underset{\sim}{Z}/2^n \underset{\sim}{Z}$ be an idele class character of degree 2^n and L_A , $(L_p)_{p \in \tilde{P}}$ be its restricted local components. Then L defines a dihedral or quaternion field over $\underset{\sim}{Q}$ if, and only if, the following conditions are satisfied :

(1) For any prime p which splits in Ω_0 ; $p \cong pp'$, and any $(\beta, \beta') \in U_p \times U_{p'} \subset I_0$ with $(\beta , \beta')^\tau = (\tilde{\beta} , \tilde{\beta}') \in U_p \times U_{p'}$, I have

$$L_p(\beta\tilde{\beta}) + L_{p'}(\beta' \tilde{\beta}') = 0 .$$

(2) For any prime p which is inert in Ω_0 , $p \cong p$, and any $\beta \in U_p$, I have

$$L_p(\beta^{1+\tau}) = 0 .$$

(3) For any p which ramifies in Ω_0 , $p \cong p^2$, and any $\beta \in U_p = U_p \cap \underset{\sim}{Q}_p$, I have

$$L_p(\beta) = \begin{cases} 2^{n-1} + 2^n \underset{\sim}{Z} & \text{in the quaternion case, if } (\beta , \Omega_{0p}/\underset{\sim}{Q}_p) \neq 1 \\ 0 & \text{in all other cases.} \end{cases}$$

A corresponding condition for the c'_ν s is automatically satisfied by my choice of them. Conditions (1), (2) and (3) I call the restricted local dihedral, resp. quaternion conditions. Of course, if L defines a dihedral or quaternion field, the full local components $\bar{L}_p$ satisfy analogous conditions.

Now, I give a summary of all possible local components $\bar{L}_p : \Omega_{0p}^\times \longrightarrow \underset{\sim}{Z}/2^n \underset{\sim}{Z}$ which satisfy the local dihedral, resp. quaternion conditions. If $z \in \Omega_{0p}$ is a prime element for p , then $\bar{L}_p$ is uniquely determinated by L_p and the value $\bar{L}_p(z) \in \underset{\sim}{Z}/2^n \underset{\sim}{Z}$.

1° p <u>infinite</u>. – If p is complex, then $\bar{L}_p = 0$; therefore, on account of condition (3), Ω_0 cannot be complex in the quaternion case. If p is real and $p' = p^\tau$, then $\bar{L}_p$ is determined by $\bar{L}_p(-1)$, and on account of (1),

$$\bar{L}_{p'}(-1) = -\bar{L}_p(-1)$$

holds.

2° p <u>finite</u>, $p \nmid 2$. – Let $p \neq 2$ be the associated prime ; then U_p^1 is a pro-p-group, L_p is uniquely determinated by its value on a primitive root π for p .

(a) $p \cong pp'$: Let $\pi_p \in \underset{\sim}{Z}$ be a primitive root for p , then $\pi_p \in U_p$ is one for p , and $\pi_p \in U_{p'}$ is one for p' . If I set $L_p(\pi_p) = X_p \in \underset{\sim}{Z}/2^n \underset{\sim}{Z}$, then $(p-1)X_p = 0$, and $L_{p'}(\pi_p) = -X_p$ on account of (1). p is a prime element for p and p' , and $\bar{L}_{p'}(p) = -\bar{L}_p(p) \in \underset{\sim}{Z}/2^n \underset{\sim}{Z}$.

(b) $p \cong p$: Let $\pi_p \in U_p$ be a primitive root for p and $L_p(\pi_p) = Y_p \in \underset{\sim}{Z}/2^n \underset{\sim}{Z}$; then, condition (2) is equivalent to $(p+1)Y_p = 0$. p is a prime element, and

$\overline{L}_p(p) = 0$, resp. 2^{n-1} [1] in the dihedral, resp. quaternion case.

(c) $p \cong p^2$: Let $\pi \in \underset{\sim}{Z}$ be a primitive root for p ; then, it is also one for p , and if I set $L_p(\pi) = X_p \in \underset{\sim}{Z}/2^n \underset{\sim}{Z}$, then (3) is equivalent to

$$X_p = \begin{cases} 0 & \text{in the dihedral case,} \\ 2^{n-1} & \text{in the quaternion case.} \end{cases}$$

$\sqrt{D}$ is a prime element for p , and if $\overline{L}_p(\sqrt{D}) = W_p \in \underset{\sim}{Z}/2^n \underset{\sim}{Z}$, then

$$2W_p = \begin{cases} 2^{n-1} & \text{in the quaternion case if } p \equiv -1 \mod 4 , \\ 0 & \text{in all other cases.} \end{cases}$$

It follows that the quaternion case with $n = 1$ is only possible if $p \equiv 1 \mod 4$.

3° $p = \mathfrak{z} | 2$.

(a) $D \equiv 1 \mod 8$: $2 \cong \mathfrak{z}\mathfrak{z}'$, $U_{\mathfrak{z}} = U_{\mathfrak{z}'} = U_2 \subset \underset{\sim}{Q}_2$, $\{-1 , 5\}$ is a $\underset{\sim}{Z}_2$-basis for $U_{\mathfrak{z}}$, and 2 is a prime element for $\mathfrak{z}$. If I set $W_0 = \overline{L}_{\mathfrak{z}}(2)$, $W_1 = L_{\mathfrak{z}}(-1)$ and $W_2 = L_{\mathfrak{z}}(5) \in \underset{\sim}{Z}/2^n \underset{\sim}{Z}$, then $2W_1 = 0$, $\overline{L}_{\mathfrak{z}'}(2) = -W_0$, $L_{\mathfrak{z}'}(-1) = W_1$ and $L_{\mathfrak{z}'}(5) = -W_2$.

(b) $D \equiv 5 \mod 8$: $2 \cong \mathfrak{z}$, 2 is a prime element for $\mathfrak{z}$, and $\{-1, \sqrt{D}, -1+2\sqrt{D}\}$ is a $\underset{\sim}{Z}_2$-basis for the 2-component of $U_{\mathfrak{z}}$. I set $\overline{L}_{\mathfrak{z}}(2) = W_0$, $L_{\mathfrak{z}}(-1) = W_1$, $L_{\mathfrak{z}}(\sqrt{D}) = W_2$, and $L_{\mathfrak{z}}(-1 + 2\sqrt{D}) = W_3 \in \underset{\sim}{Z}/2^n \underset{\sim}{Z}$; then, condition (2) is equivalent to $W_1 = 2W_2 = 0$, $W_0 = 2^{n-1}$ in the quaternion case, and $W_0 = 0$ in the dihedral case.

(c) $D \equiv 2 \mod 4$: $2 \cong \mathfrak{z}^2$, $\sqrt{D}$ is a prime element for z , and $\{-1, 5, 1+\sqrt{D}\}$ is a Z_2-basis for $U_{\mathfrak{z}}$. If I set $W_0 = \overline{L}_{\mathfrak{z}}(\sqrt{D})$, $W_1 = L_{\mathfrak{z}}(-1)$, $W_2 = L_{\mathfrak{z}}(5)$ and $W_3 = L_{\mathfrak{z}}(1 + \sqrt{D}) \in \underset{\sim}{Z}/2^n \underset{\sim}{Z}$; then, condition (3) is equivalent to the following ones :

$2W_0 = W_1 = W_2 = 0$ in the dihedral case ;

$2W_0 = W_1 = 0$, $W_2 = 2^{n-1}$ in the quaternion case, if $D \equiv 2 \mod 8$;

$2W_0 = W_1 = W_2 = 2^{n-1}$ in the quaternion case, if $D \equiv -2 \mod 8$.

(d) $D \equiv -1 \mod 8$: $2 \cong \mathfrak{z}^2$, $\sqrt{-1}$ is an element of $\Omega_{0\mathfrak{z}}$, $1 + \sqrt{-1}$ is a prime element for z , and $\{\sqrt{-1} , 5 , -1 + 2\sqrt{D}\}$ is a $\underset{\sim}{Z}_2$-basis for $U_{\mathfrak{z}}$. If I set $W_0 = \overline{L}_{\mathfrak{z}}(1 + \sqrt{-1})$, $W_1 = L_{\mathfrak{z}}(\sqrt{-1})$, $W_2 = L_{\mathfrak{z}}(5)$ and

$$W_3 = L_{\mathfrak{z}}(-1 + 2\sqrt{D}) \in \underset{\sim}{Z}/2^n \underset{\sim}{Z} ;$$

then, condition (3) is equivalent to the following ones :

$2W_0 = W_1$, $2W_1 = W_2 = 0$ in the dihedral case ;

$2W_0 = W_1$, $2W_1 = 2^{n-1}$, $W_2 = 0$ in the quaternion case.

From this, one easily sees, that in the quaternion case I must have $n \geqslant 3$.

---

[1] Here and in the following, 2^{n-1} stands for $2^{n-1} + 2^n \underset{\sim}{Z}$.

(e) $D \equiv 3 \mod 8$: $2 \cong \mathfrak{z}^2$, $1+\sqrt{D}$ is a prime element for $\mathfrak{z}$, and

$$\{-1 , \sqrt{D} , (1+\sqrt{D})^2/2\}$$

is a $\underset{\sim}{Z}_2$-basis for $U_{\mathfrak{z}}$. I set $W_0 = \overline{L}_{\mathfrak{z}}(1+\sqrt{D})$, $W_1 = L_{\mathfrak{z}}(-1)$, $W_2 = L_{\mathfrak{z}}(\sqrt{D})$ and $W_3 = L_{\mathfrak{z}}((1+\sqrt{D})^2/2) \in \underset{\sim}{Z}/2^n\underset{\sim}{Z}$; then, condition (3) is equivalent to

$$W_1 = 2W_2 = \begin{cases} 0 & \text{in the dihedral case,} \\ 2^{n-1} & \text{in the quaternion case.} \end{cases}$$

Now assume, that a system $(L_A , (L_p)_{p\in \underset{\sim}{P}})$ satisfies the restricted local dihedral, resp. quaternion conditions ; I shall give a detailed description of the compatibility conditions (C_i) ; to make life easy I assume $L_{\hat{\mathfrak{p}}_1} = \dots = L_{\hat{\mathfrak{p}}_h} = 0$. Let Γ be the group of all $\alpha \in \Omega_0^\times$ for which the associated principal ideal $\langle\alpha\rangle$ is a square and $\Gamma_+ = \{\gamma \in \Gamma ; N_{\Omega_0/\underset{\sim}{Q}}(\gamma) > 0\}$; then

$$(\Gamma:\Gamma_+) = \begin{cases} 2 , & \text{if } -1 \in N_{\Omega_0/\underset{\sim}{Q}}\,\Omega_0^\times \\ 1 , & \text{if } -1 \notin N_{\Omega_0/\underset{\sim}{Q}}\,\Omega_0 \end{cases}$$

and a set of representatives of a basic for the $\underset{\sim}{F}_2$-vector space $\Gamma_+/\Omega_0^{\times 2}$ is given by

$\{\sqrt{-1}\}$, if $\Omega_0 = \underset{\sim}{Q}(\sqrt{-1})$

$\{-1\}$, if $\Omega_0 = \underset{\sim}{Q}(\sqrt{\pm 2})$

$\{-1 , p_1 , \dots , p_{t-1}\}$, if $D \equiv 1 \mod 4$

$\{-1 , 2 , p_1 , \dots , p_{t-1}\}$, if $D \not\equiv 1 \mod 4$ and $\Omega_0 \neq \underset{\sim}{Q}(\sqrt{-1})$, $\underset{\sim}{Q}(\sqrt{\pm 2})$.

If $D \not\equiv 1 \mod 4$ (that is, if 2 ramifies in Ω_0), I set $p_0 = 2$. In the following, I omit the case $\Omega_0 = \underset{\sim}{Q}(\sqrt{-1})$, which needs separate (but simple) considerations. The compatibility condition for (-1) is a consequence of the restricted local dihedral and quaternion conditions.

If $-1 \in N_{\Omega_0/\underset{\sim}{Q}}\,\Omega_0^\times$ I take $\gamma^* \in \Gamma \setminus \Gamma_+$; then I have $N_{\Omega_0/\underset{\sim}{Q}}(\gamma^*) = -c^{*2}$ with $c^* \in \underset{\sim}{Z}$ and

$$(\gamma^*) = \prod_{\nu=1}^{h} c_\nu^{u_\nu^*}.(\beta_p^*)_{p\in\underset{\sim}{P}}.(\alpha^{*2})$$

with $u_\nu^* \in \underset{\sim}{Z}$, $u_\nu^* \equiv 0 \mod 2$, $\beta_p^* \in U_p$ and $\alpha^* \in \Omega_0^\times$. Now the compatibility condition reads

$$(C^*) \qquad \Lambda^* = 0 ,$$

where

$$\Lambda^* = \sum_{\nu=1}^{h} u_\nu^*.L_A(c_\nu) + \sum_{p\in\underset{\sim}{P}} L_p(\beta_p^*) .$$

For $i \geqslant 0$, I obtain

$$(p_i) = \prod_{\nu=1}^{h} c_\nu^{u_{\nu i}}.(\beta_p^{(i)})_{p\in\underset{\sim}{P}}.(\alpha_i^2)$$

with $u_{\nu i} \in \underset{\sim}{Z}$, $u_{\nu i} \equiv 0 \mod 2$, $\beta_p^{(i)} \in U_p$, $\alpha_i \in \Omega_0^\times$; $\beta_p^{(i)} = p_i/\alpha_i^2$ for all

$\mathfrak{p} \notin \{\hat{\mathfrak{p}}_1 , \dots , \hat{\mathfrak{p}}_h\}$, $N_{\Omega_0/\mathbb{Q}}(\beta_{\mathfrak{p}}^{(i)}) = c_i^2$ and $N_{\Omega_0/\mathbb{Q}}(\alpha_i) = \pm (p_i/c_i)$, where

$$c_i = \prod_{\nu=1}^{h} \hat{p}_\nu^{u_{\nu i}/2} .$$

The compatibility conditions have the form

$$\sum_{\nu=1}^{\ell} u_{\nu i} \cdot L_A(c_\nu) + \sum_{\mathfrak{p}\in \underset{\sim}{P}} L_{\mathfrak{p}}(p_i/\alpha_i^2) = 0 .$$

Now I set $\underset{\sim}{P}_0 = \{\mathfrak{p} \in \underset{\sim}{P} ;\ \mathfrak{p}$ unramified over $\mathbb{Q}\}$,

$$z = \begin{cases} \sqrt{D} & , \text{ if } D \equiv 2 \mod 4 \\ 1 + \sqrt{-1} & , \text{ if } D \equiv -1 \mod 8 \\ 1 + \sqrt{D} & , \text{ if } D \equiv 3 \mod 8 \end{cases}$$

and, for $i \geqslant 1$,

$$\Lambda^{(i)} = \sum_{\nu=1}^{h} (u_{\nu i}/2) . L_A(c_\nu) - \sum_{\mathfrak{p}\in \underset{\sim}{P}_0} L_{\mathfrak{p}}(\alpha_i) - \{L_{\mathfrak{z}}(\alpha_i)\} ,$$

where the term $\{\dots\}$ only occurs if 2 ramifies in Ω_0 ,

$$\Lambda^{(0)} = \sum_{\nu=1}^{h} (u_{\nu 0}/2) . L_A(c_\nu) - \sum_{\mathfrak{p}\in \underset{\sim}{P}_0} L_{\mathfrak{p}}(\alpha_0) + L_{\mathfrak{z}}(z/\alpha_0) ;$$

then a simple (but lengthy) computation shows that the compatibility conditions are equivalent to

$$(C_i) \qquad 2\Lambda^{(i)} = \begin{cases} 2^{n-1} & \text{in the quaternion case if } p_i \equiv -1 \mod 4 , \\ 0 & \text{otherwise} \end{cases}$$

for $i \geqslant 1$, and

$$(C_0) \begin{cases} \text{If } D \equiv 2 \mod 4 \text{, then} \\ \qquad 2\Lambda^{(0)} = \begin{cases} 2^{n-1} & \text{in the quaternion case if } d \equiv -1 \mod 4 , \\ 0 & \text{otherwise.} \end{cases} \\ \text{If } D \equiv -1 \mod 8 \text{, then } 2\Lambda^{(0)} - W_1 = 0 . \\ \text{If } D \equiv 3 \mod 8 \text{, then} \\ \qquad 2\Lambda^{(0)} - W_3 = \begin{cases} 2^{n-1} & \text{in the quaternion case,} \\ 0 & \text{otherwise.} \end{cases} \end{cases}$$

Now, I assume that the restricted local dihedral, resp. quaternion conditions, are fulfilled by the system $(L_A , (L_{\mathfrak{p}})_{\mathfrak{p}\in \underset{\sim}{P}})$; let L be the associated idele class character. Then, in the dihedral case, I obtain

$$\Lambda^{(i)} = \begin{cases} L_{p_i}(\sqrt{D}) & , \text{ if } i \geqslant 1 \\ L_{\mathfrak{z}}(z) & , \text{ if } i = 0 \end{cases}$$

while in the quaternion case this is at least valid mod 2^{n-1} . In any case, I find (C_i) to be equivalent with that part of the local conditions which concern the prime element.

Let me return to the equation $N_{\Omega_0/\mathbb{Q}}(\alpha_i) = \pm (p_i/c_i)$ for $i \geq 0$, and notice that genus theory in quadratic number fields yields the equivalence of the following conditions :

(a) c_i is a square in $\mathbb{Q}$, $c_i = \tilde{c}_i^2$;

(b) $u_{\nu i} \equiv 0 \mod 4$ for all ν ;

(c) p_i lies in the principal genus of Ω_0 ;

(d) $\pm p_i \in N_{\Omega_0/\mathbb{Q}} \Omega_0^\times$.

In the case $i = 0$, there is $2 \in N_{\Omega_0/\mathbb{Q}} \Omega_0^\times$ if, and only if, $p_i \equiv \pm 1 \mod 8$ for all $i \geq 1$.

4. The imbedding problem.

Let $\Omega_n/\mathbb{Q}$ be a dihedral field of degree 2^{n+1}, Ω_n/Ω_0 cyclic of degree 2^n, S a generating automorphism for Ω_n/Ω_0, and Ω_ν the fixed field of S^{2^ν}. I shall obtain necessary and sufficient conditions on Ω_n to have an imbedding in a dihedral or quaternion field Ω_{n+k} of degree 2^{n+k+1} over $\mathbb{Q}$ $(k \geq 1)$, and I shall establish a method which allows me to construct the idele class character of Ω_0 which defines Ω_{n+k} from that which defines Ω_n. First let me summarize the conditions on Ω_n, which guarantee the solubility of all associated local imbedding problems. These conditions follow immediately from the explicit description given in the previous chapter, but now I state them in terms of the global extension $\mathbb{Q} \subset \Omega_0 \subset \Omega_n$:

Local conditions :

1° If, for any prime $p > 2$ which splits in Ω_0, $\varkappa \in \{1, 2, \ldots, n+k\}$ is maximal with $p \equiv 1 \mod 2^\varkappa$, then

$$p \text{ is unramified in} \begin{cases} \Omega_n & , \text{ if } \varkappa \leq k ; \\ \Omega_{n+k-\varkappa} & , \text{ if } \varkappa \geq k . \end{cases}$$

2° If, for any prime $p > 2$ which is inert in Ω_0, $\varkappa$ $\{1, 2, \ldots, n+k\}$ is maximal with $p \equiv -1 \mod 2^\varkappa$, then

$$p \text{ is unramified in} \begin{cases} \Omega_n & , \text{ if } \varkappa \leq k , \\ \Omega_{n+k-\varkappa} & , \text{ if } \varkappa \geq k . \end{cases}$$

3° If a prime $p > 2$ is ramified in Ω_0, $p \cong \mathfrak{p}^2$, then

(a) $\mathfrak{p}$ splits in Ω_n into prime ideals of relative degree 2, if I am in the quaternion case with $k = 1$ and $p \equiv -1 \mod 4$;

(b) $\mathfrak{p}$ splits completely in Ω_n in all other cases.

4° If Ω_0 is real, Ω_n is real, too. In the quaternion case, Ω_0 is real.

5° If $\mathfrak{z}$ is a prime divisor of 2 in Ω_0, and $\mathfrak{Z}$ is a prime divisor of $\mathfrak{z}$ in

Ω_n , then the following conditions are fulfilled :

(a) If $D \equiv 1 \mod 8$, then $(-1 , \Omega_{n\mathfrak{z}}/\Omega_{0\mathfrak{z}}) = 1$ $(W_1 = 0)$.

(b) If $D \equiv 5 \mod 8$, then $(\sqrt{D} , \Omega_{n\mathfrak{z}}/\Omega_{0\mathfrak{z}}) = 1$ $(W_2 = 0)$.

(c) If $D \equiv 2 \mod 4$, then

$$(\sqrt{D} , \Omega_{n\mathfrak{z}}/\Omega_{0\mathfrak{z}}) = \begin{cases} -1 & \text{in the quaternion case if } k = 1 \quad (W_0 = 2^{n-1}) \\ 1 & \text{in all other cases} \quad (W_0 = 0) . \end{cases}$$

(d) If $D \equiv -1 \mod 8$, then

$$(\sqrt{-1} , \Omega_{n\mathfrak{z}}/\Omega_{0\mathfrak{z}}) = \begin{cases} -1 & \text{in the quaternion case if } k = 1 \quad (W_1 = 2^{n-1}) , \\ 1 & \text{otherwise} \quad (W_1 = 0) , \end{cases}$$

and

$$(1 + \sqrt{-1} , \Omega_{n\mathfrak{z}}/\Omega_{0\mathfrak{z}}) = \begin{cases} -1 & \text{in the quaternion case if } k = 2 \quad (W_0 = 2^{n-1}) , \\ 1 & \text{in all other cases if } k \geqslant 2 \quad (W_0 = 0) . \end{cases}$$

(e) If $D \equiv 3 \mod 8$, then

$$(\sqrt{D} , \Omega_{n\mathfrak{z}}/\Omega_{n\mathfrak{z}}) = \begin{cases} -1 & \text{in the quaternion case if } k = 1 \quad (W_2 = 2^{n-1}) \\ 1 & \text{otherwise} \quad (W_2 = 0) . \end{cases}$$

Now I can prove the following theorem.

THEOREM. - Let Ω_n/Q be a dihedral field of degree 2^{n+1} , Ω_n/Ω_0 cyclic of degree 2^n , and $k \geqslant 1$; then the following assertions hold :

(1) If $k = 1$, the local conditions 5°, for $p = 2$, are a consequence of 1° to 4° (consequently, all local conditions at $p = 2$, with exception of the second condition in the case $D \equiv -1 \mod 8$, $k \geqslant 2$, can be omitted).

(2) The local conditions are sufficient for the existence of an imbedding of Ω_n in a dihedral or quaternion field of degree 2^{n+k+1} unless we deal with one of the following cases :

(a) $D \equiv -1 \mod 8$, $D \neq -1$, $2 \in N_{\Omega_0/Q}\, \Omega_0^\times$, $k \geqslant 3$.

(b) $D \equiv -2 \mod 8$, $D \neq -2$, $2 \in N_{\Omega_0/Q}\, \Omega_0^\times$, $k \geqslant 3$.

(3) If $D \equiv -1 \mod 8$ or $D \equiv -2 \mod 8$, $D \neq -1$, $D \neq -2$, $2 \in N_{\Omega_0/Q}\, \Omega_0^\times$, $k \geqslant 3$, and if all local conditions are fulfilled, then Ω_n has an imbedding in a dihedral or quaternion field of degree 2^{n+k+1} if, and only if,

$$(\mathfrak{w} , \Omega_n/\Omega_0) = \begin{cases} -1 & \text{in the quaternion case if } k = 3 \text{ and } D \equiv -1 \mod 8 , \\ 1 & \text{otherwise,} \end{cases}$$

for an idele $\mathfrak{w}$ of Ω_0 with the property

$$\mathfrak{w}^2 = e_z \cdot \mathfrak{s} . (\gamma) ,$$

where e_z is that idele whose $\mathfrak{z}$-component is z and whose other components are 1 , $\mathfrak{s}$ is a unit idele with $(\mathfrak{s}\ ,\ \Omega_n/\Omega_0) = 1$ and $\gamma \in \Omega_0^\times$ (the ideal associated with $\mathfrak{w}$ lies in the class whose square is the class of $\mathfrak{z}$).

If $n = 0$ in the above theorem, I obtain as a corollary the results of DAMEY and MARTINET [1].

Proof. – Let Ω_n be given by its defining idele class character L of Ω_0 with restricted local components $(L_A\ ,\ (L_p)_{p\in \underset{\sim}{P}})$, and let me use the notation of the previous chapter. Then assertion (1) follows from the fact that $\sum_{i=0}^{t} \Lambda^{(i)}$ is the L-value of the idele $(\ldots\ ,\ 1\ ,\ \sqrt{D}\ ,\ \ldots\ ,\ \sqrt{D}\ ,\ z\ ,\ 1\ ,\ \ldots)$ (if 2 is unramified in Ω_0 , I set $\Lambda^{(0)} = 0$, $z = 1$). To handle the condition stated in (3) observe that, in the case $D \equiv -1\ ,\ -2 \mod 8$, $D \neq -1\ ,\ -2$, $2 \in N_{\Omega_0/\mathbb{Q}}\, \Omega_0^\times$, $k \geqslant 3$, I obtain

$$\Lambda^{(0)} = 2L(\mathfrak{w})$$

for any $\mathfrak{w} \in I_0$ as in assertion (3) wherefore the condition stated there is equivalent to

$$\frac{1}{2}\Lambda^{(0)} = \begin{cases} 2^{n-1} & \text{in the quaternion case if } k = 3 \text{ and } D \equiv 1 \mod 8\ , \\ 0 & \text{otherwise.} \end{cases}$$

The local conditions 1°, 2°, 4° and 5° guarantee the existence of liftings $\tilde{L}_p\ :\ U_p \longrightarrow \underset{\sim}{Z}/2^{n+k}\,\underset{\sim}{Z}$ of $L_p\ :\ U_p \longrightarrow \underset{\sim}{Z}/2^{n}\,\underset{\sim}{Z}$ which satisfy the restricted local dihedral or quaternion conditions. Constructing a dihedral of quaternion field $\Omega_{n+k} \supset \Omega_n$ is equivalent to construct liftings $(\tilde{L}_A\ ,\ (\tilde{L}_p)_{p\in \underset{\sim}{P}})$ of $(L_A\ ,\ (L_p)_{p\in \underset{\sim}{P}})$ such that they satisfy the restricted local conditions and the compatibility conditions. To carry out this construction I first assume that I have found any liftings which satisfy the restricted local conditions and then I shall modify them little by little to obtain finally a system which satisfies all requirements.

Let $(\tilde{L}_A\ ,\ (\tilde{L}_p)_{p\in \underset{\sim}{P}})$ be liftings of $(L_A\ ,\ (L_p)_{p\in \underset{\sim}{P}})$ which satisfy the restricted local dihedral, resp. quaternion, conditions and let $\tilde{\Lambda}^*$, $\tilde{\Lambda}^{(i)}$ be quantities formed from $(\tilde{L}_A\ ,\ (\tilde{L}_p)_{p\in \underset{\sim}{P}})$ in the same manner as Λ^* , $\Lambda^{(i)}$ are formed from $(L_A\ ,\ (L_p)_{p\in \underset{\sim}{P}})$; then $\tilde{\Lambda}^* + 2^n\,\underset{\sim}{Z} = \Lambda^*$, $\tilde{\Lambda}^{(i)} + 2^n\,\underset{\sim}{Z} = \Lambda^{(i)}$.

Assume that for a $\varkappa \in \{0\ ,\ 1\ ,\ \ldots\ ,\ k\}$ the following conditions are fulfilled :

(A) For any $i \in \{1\ ,\ \ldots\ ,\ t-1\}$,

$$\tilde{\Lambda}^{(i)} \equiv \begin{cases} 2^{n+k-2} \mod 2^{n+\varkappa-1} & \text{in the quaternion case if } p_i \equiv -1 \mod 4\ , \\ 0 \mod 2^{n+\varkappa-1} & \text{otherwise.} \end{cases}$$

(B) If $D \equiv 2 \mod 4$, then

$$\tilde{\Lambda}^{(0)} \equiv \begin{cases} 2^{n+k-2} \mod 2^{n+\varkappa-1} & \text{in the quaternion case if } D \equiv -2 \mod 8\ , \\ 0 \mod 2^{n+\varkappa-1} & \text{otherwise.} \end{cases}$$

(C) If $D \equiv -1 \mod 8$, then

$$2\tilde{\Lambda}^{(0)} - \tilde{W}_1 \equiv 0 \mod 2^{n+\varkappa}$$

(D) If $D \equiv 3 \mod 8$, then

$$2\tilde{\Lambda}^{(0)} - \tilde{W}_3 \equiv \begin{cases} 2^{n+k-1} \mod 2^{n+\varkappa} & \text{in the quaternion case,} \\ 0 \mod 2^{n+\varkappa} & \text{otherwise.} \end{cases}$$

(E) If $-1 \in N_{\Omega_0/\mathbb{Q}}\, \Omega_0^{\times}$, then

$$\tilde{\Lambda}^* \equiv 0 \mod 2^{n+\varkappa-1} .$$

Obviously, if $\varkappa = 0$, then (A) to (E) are true. I now have to modify a finite number of the $\tilde{L}_p$'s by terms $\equiv 0 \mod 2^n$ such that in the case $\varkappa = k$ the congruence (E) is valid $\mod 2^{n+k}$, and that in the case $\varkappa < k$ the congruences (A), (B) and (E) are valid $\mod 2^{n+\varkappa}$, while (C) and (D) are valid $\mod 2^{n+\varkappa+1}$.

If $-1 \in N_{\Omega_0/\mathbb{Q}}\, \Omega_0^{\times}$, I first modify (E) ; assume $\tilde{\Lambda}^* \equiv 0 \mod 2^{n+\varkappa+1}$, $\not\equiv 0 \mod 2^{n+\varkappa}$ $(\varkappa \geqslant 1)$. Take a prime $p \equiv -1 \mod 2^{k-\varkappa+1}$ ($p \equiv -1 \mod 4$ if $k = \varkappa$) which is inert in Ω_0 ; β_p^* is a quadratic non-residue mod p, whence there exists $\tilde{L}_p \equiv 0 \mod 2^{n+\varkappa-1}$ with $\tilde{L}_p(\beta_p^*) \equiv 2^{n+\varkappa-1} \mod 2^{n+\varkappa}$; this does the job.

Next, in the case $D \not\equiv 1 \mod 4$, $\pm 2 \in N_{\Omega_0/\mathbb{Q}}\, \Omega_0^{\times}$, I first deal with (B), (C) or (D) while in all other cases I first deal with (A). To obtain the congruences (A) $\mod 2^{n+\varkappa}$, I consider the field $M = \Omega_0^{(2^{k-\varkappa+1})}(\sqrt{c_1}, \ldots, \sqrt{c_{t-1}})$ (2) and observe that $p_1, \ldots, p_{t-1}$ are quadratic independent in M ; so there exist infinitely many systems $(\tilde{q}_1, \ldots, \tilde{q}_{t-1})$ of prime ideals of first degree in M such that $(p_i/\tilde{q}_j) = (-1)^{\delta_{ij}}$. If $(q_1, \ldots, q_{t-1})$ is the restriction of such a system to Ω_0, there exist $\tilde{L}_{q_1}, \ldots, \tilde{L}_{q_{t-1}}$ such that

$$\sum_{j=1}^{t-1} \tilde{L}_{q_j}(\alpha_i) + \tilde{L}_{q_j'}(\alpha_i)$$

has prescribed value $2^{n+\varkappa-1}.e_i \mod 2^{n+\varkappa}$ ($e_i = 0$ or $e_i = 1$). If furthermore 2 ramifies in Ω_0 and $\pm 2 \in N_{\Omega_0/\mathbb{Q}}\, \Omega_0^{\times}$, I must only choose $\tilde{q}_j$ in such a way that the associated primes satisfy $q_j \equiv -1 \mod 8$ to get $\tilde{L}_{q_j}(\alpha_0) + \tilde{L}_{q_j'}(\alpha_0) \equiv 0 \mod 2^{n+\varkappa}$.

As to the congruences (B), (C) and (D) I only consider (B) which is the most difficult one ; the others can be done in a similar manner. So I assume $D \equiv 2 \mod 4$, $\varkappa \geqslant 1$ and

$$\tilde{\Lambda}^{(0)} \not\equiv \begin{cases} 2^{n+k-2} \mod 2^{n+\varkappa-1} & \text{in the quaternion case if } D \equiv -2 \mod 8, \\ 0 \mod 2^{n+\varkappa-1} & \text{otherwise.} \end{cases}$$

I have to distinguish several cases :

(a) $\pm 2 \notin N_{\Omega_0/\mathbb{Q}}\, \Omega_0^{\times}$: This case can simultaneously be done with congruence (A) by

---

(2) $\Omega_0^{(m)}$ denotes the field of m-th roots of unity over Ω_0.

considering the field

$$M = \Omega_0^{(2^{k-\varkappa+1})}(\sqrt{2}\ ,\ \sqrt{c_1}\ ,\ \dots\ ,\ \sqrt{c_{t-1}})$$

instead of

$$M = \Omega_0^{(2^k-\varkappa+1)}(\sqrt{c_1}\ ,\ \dots\ ,\ \sqrt{c_{t-1}})\ ,$$

and observing that $c_0\ ,\ p_1\ ,\ \dots\ ,\ p_{t-1}$ are quadratic independant in M.

(b) $\pm 2 \in N_{\Omega_0/\underset{\sim}{Q}}\ \Omega_0^\times$, $k = 2$: Take a prime $p \equiv 5 \mod 8$ which splits in Ω_0 , $p \cong \mathfrak{p}\mathfrak{p}'$; then α_0 has opposite quadratic characters mod $\mathfrak{p}$ and mod $\mathfrak{p}'$, and therefore exists $\tilde{L}_p \equiv 0 \mod 2^n$ such that $\tilde{L}_{\mathfrak{p}}(\alpha_0) + L_{\mathfrak{p}'}(\alpha_0) \equiv 2^n \mod 2^{n+1}$; the congruences (A) remain unchanged mod $2^{n+\varkappa-1}$, (E) remains unchanged mod $2^{n+\varkappa}$.

(c) $-2 \in N_{\Omega_0/\underset{\sim}{Q}}\ \Omega_0^\times$, $k \geqslant 3$, $D \equiv -2 \mod 8$: Then $N_{\Omega_0/\underset{\sim}{Q}}(\alpha_0) = -(2/c_0)$; take a prime $p \equiv -1 \mod 2^{k-\varkappa+1}$ (at least $p \equiv -1 \mod 8$) which is inert in Ω_0 , $\mathfrak{p} \cong p$. On account of $(\alpha_0/\mathfrak{p}) = -1$ there exists $\tilde{L}_{\mathfrak{p}} \equiv 0 \mod 2^{n+\varkappa-1}$ such that $\tilde{L}_{\mathfrak{p}}(\alpha_0) \equiv 2^{n+\varkappa-1} \mod 2^{n+\varkappa}$, and this does the job.

(d) $+2 \in N_{\Omega_0/\underset{\sim}{Q}}\ \Omega_0^\times$, $k \geqslant 3$, $D \equiv -2 \mod 8$: On account of (3), I have $\varkappa \geqslant 2$. I consider the field

$$M = \Omega_0^{(2^{k-\varkappa+2})}(\sqrt{2}\ ,\ \sqrt[4]{c_0}\ ,\ \sqrt{c_1}\ ,\ \dots\ ,\ \sqrt{c_{t-1}})$$

and observe that the numbers $\alpha_0\sqrt{2}\ ,\ p_1\ ,\ \dots\ ,\ p_{t-1}$ are quadratic independznt in M whence there exist infinitely many prime ideals $\tilde{\mathfrak{q}}_0$ of first degree in Ω_0 for which $(\alpha_0\sqrt{2}/\tilde{\mathfrak{q}}_0) = -1$ and $(p_i/\tilde{\mathfrak{q}}_0) = +1$ if $i \geqslant 1$. Let q_0 be the restriction of such a $\tilde{\mathfrak{q}}_0$ to Ω_0 and $q_0 \equiv 1 \mod 2^{k-\varkappa+2}$ be the associated prime. Let $\pi \in \underset{\sim}{Z}$ be a primitive root for q_0 and set $\tilde{L}_{\mathfrak{q}_0}(\pi) = 2^{n+\varkappa-2}$. Then

$$\tilde{L}_{\mathfrak{q}_0}(\alpha_0) + \tilde{L}_{\mathfrak{q}_0'}(\alpha_0) = 2^{n+\varkappa-2}(x_0 - x_0')$$

where $\alpha_0 \equiv \pi^{x_0} \mod \mathfrak{q}_0$, $\alpha_0 \equiv \pi^{x_0'} \mod \mathfrak{q}_0'$.

Now I use the equations

$$N_{\Omega_0/\underset{\sim}{Q}}(\alpha_0) = \frac{2}{c_0}\ ,\quad \left(\frac{\alpha_0\sqrt{2}}{\mathfrak{q}_0}\right) = -1\ ,$$

and the fact that c_0 is a square in $\underset{\sim}{Q}$ to conclude $x_0 - x_0' \equiv 2 \mod 4$.

(e) $\pm 2 \in N_{\Omega_0/\underset{\sim}{Q}}\ \Omega_0^\times$, $k \geqslant 3$, $D \equiv 2 \mod 8$, $\varkappa \geqslant 2$: I proceed as in (d) with the following modification : If $-1 \in N_{\Omega_0/\underset{\sim}{Q}}\ \Omega_0^\times$, I consider the field

$$M^* = M(\sqrt[4]{(\gamma^*/\alpha^{*2})^{1-\tau}})$$

instead of M to guarantee that $\tilde{\Lambda}^*$ remains unchanged mod $2^{n+\varkappa}$.

(f) $\pm 2 \in N_{\Omega_0/\underset{\sim}{Q}}\ \Omega_0^\times$, $k \geqslant 3$, $D \equiv 2 \mod 8$, $\varkappa = 1$: If

$$\sqrt{D}/\alpha_0 = (-1)^{w_1}.5^{w_2}.(1+\sqrt{D})^{w_3}$$

then

$$w_3 \equiv \begin{cases} 1 \mod 2 & \text{if } N_{\Omega_0/\mathbb{Q}}(\alpha_0) > 0 \\ 0 \mod 2 & \text{if } N_{\Omega_0/\mathbb{Q}}(\alpha_0) < 0 \ . \end{cases}$$

If $-1 \in N_{\Omega_0/\mathbb{Q}}\,\Omega_0^\times$ and $\beta_\delta^* = \gamma^*/\alpha^{*2} = (-1)^{w_1^*}.5^{w_2^*}.(1+\sqrt{D})^{w_3^*}$, then $w_3^* \equiv 1$ mod 2 .

Let $p \equiv -1 \mod 2^k$ be a prime which is inert in Ω_0 , $p \cong \mathfrak{p}$, then α_0 is a quadratic residue mod $\mathfrak{p}$ if, and only if, $N_{\Omega_0/\mathbb{Q}}(\alpha_0) > 0$. If π is a primitive root for $\mathfrak{p}$, and if I set $\tilde{L}_{\mathfrak{p}}(\pi) = 2^n$, then

$$\tilde{L}_{\mathfrak{p}}(\alpha_0) \equiv \begin{cases} 2^n \mod 2^{n+1} & \text{if } N_{\Omega_0/\mathbb{Q}}(\alpha_0) < 0 \\ 0 \mod 2^{n+1} & \text{if } N_{\Omega_0/\mathbb{Q}}(\alpha_0) > 0 \end{cases}$$

while $\tilde{L}_{\mathfrak{p}}(\gamma^*/\alpha^{*2}) \equiv 2^n \mod 2^{n+1}$. Replacing $\tilde{W}_3$ by $\tilde{W}_3 + 2^n$ and setting $\tilde{L}_{\mathfrak{p}}$ as above yields the desired result.

REFERENCES

[1] DAMEY (P.) et MARTINET (J.). – Plongement d'une extension quadratique dans une extension quaternionienne, J. für reine und angew. Math., t. 262/263, 1973, p. 323-338.

[2] FRÖHLICH (A.). – A rational characterisation of certain sets of relatively abelian extensions, Phil. Trans. royal Soc. London, Series A, t. 251, 1959, p. 385-425.

[3] HALTER-KOCH (F.). – Arithmetische Theorie der Normalkörper von 2-Potenzgrad mit Diedergruppe, J. of Number Theory, t. 3, 1971, p. 412-443.

[4] HALTER-KOCH (F.). – Einseinheitengruppen und prime Restklassengruppen in quadratischen Zahlkörpern, J. of Number Theory, t. 4, 1972, p. 70-77.

[5] HASSE (H.). – Zahlentheorie. 3te Aufl. – Berlin, Akademie Verlag, 1970.

[6] HASSE (H.). – Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage, Math. Z., t. 31, 1930, p. 565-582.

[7] NEUKIRCH (J.). – Über das Einbettungsproblem der algebraischen Zahlentheorie, Invent. Math., t. 21, 1973, p. 59-116.

[8] POITOU (G.). – Einbettungsprobleme mit abelschem Kern, Oberwolfach, 1975.

[9] PORUSCH (I.). – Arithmetik in Zahlkörpern, deren zugehörige Galoissche Körper spezielle metabelsche Gruppen besitzen, auf klassenkörpertheoretischer Grundlage, Math. Z., t. 37, 1933, p. 134-160.

[10] RICHTER (H.). – Über die Lösbarkeit einiger nicht-abelscher Einbettungsprobleme, Math. Annalen, t. 112, 1936, p. 700-726.

[11] ROSENBLÜTH (E.). – Die arithmetische Theorie und Konstruktion der Quaternionenkörper auf klassenkörpertheoretischer Grundlage, Monatsh. Math. Phys., t. 41, 1934, p. 85-125.

[12] TATE (J.). – Global class field theory, "Algebraic number theory", p. 162-203. – New York, Academic Press, 1967.

(Texte reçu le 12 janvier 1976)

Franz HALTER-KOCH
Universität Essen
Gesamthochschule
2 Unionstrasse
Fachbereich 6
D-43 ESSEN (Allemagne fédérale)