JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

FRANZ LEMMERMEYER

Unramified quaternion extensions of quadratic number fields

Journal de Théorie des Nombres de Bordeaux, tome 9, nº 1 (1997), p. 51-68

<http://www.numdam.org/item?id=JTNB_1997__9_1_51_0>

Journal de Théorie des Nombres de Bordeaux **9** *(1997), 51-68*

Unramified Quaternion Extensions of Quadratic Number Fields

par FRANZ LEMMERMEYER

RÉSUMÉ. Des résultats classiques dûs à Rédei, Reichardt et Scholz montrent que les extensions cycliques non ramifiées de degré 4 d'un corps de nombre quadratique k correspondent à certaines factorisations du discriminant disc k. Dans cet article, on généralise ces résultats aux extensions quaternionniennes non ramifiées et galoisiennes sur $\mathbb{Q}$. On montre aussi comment les construire explicitement.

ABSTRACT. Classical results of Rédei, Reichardt and Scholz show that unramified cyclic quartic extensions of quadratic number fields k correspond to certain factorizations of its discriminant disc k. In this paper we extend their results to unramified quaternion extensions of k which are normal over $\mathbb{Q}$, and show how to construct them explicitly.

Introduction

The first mathematician who studied quaternion extensions (H_8-extensions for short) was Dedekind [6]; he gave $\mathbb{Q}(\sqrt{(2+\sqrt{2})(3+\sqrt{6})}\ )$ as an example. The question whether given quadratic or biquadratic number fields can be embedded in a quaternion extension was extensively studied by Rosenblüth [33], Reichardt [32], Witt [37], and Damey and Martinet [5]; see the surveys [15] and [10] for more details. Later, Fujisaki [8], Kiming [16] and Vaughan [36] gave simple constructions of H_8-extensions of $\mathbb{Q}$.

In [1], Bachoc and Kwon studied H_8-extensions of cyclic cubic number fields from an arithmetic viewpoint. The corresponding problem for certain sextic fields was dealt with by Jehanne [14] and Cassou-Noguès and Jehanne [2].

Quaternion extensions of $\mathbb{Q}$ also played a central role in the theory of the Galois module structure of the ring of integers of algebraic number fields (see Martinet's papers [27, 28]), and the Introduction of [7] for a detailed account). As Cohn [4] showed, quaternion extensions can also be used to explain congruences between certain binary quadratic forms.

Manuscrit reçu le 24 avril 1996.

Since quaternion extensions of $\mathbb{Q}$ always ramify over their biquadratic subfield (see Cor. 2 below), they do not occur as Hilbert class fields of quadratic or biquadratic number fields. In order to find unramified H_8-extensions one has to look at base fields $\neq \mathbb{Q}$. Already Furtwängler [9] knew that such extensions exist, but it was Kisilevsky [17] who showed that the second Hilbert 2-class field of e.g. $k = \mathbb{Q}(\sqrt{-30})$ is an H_8-extension of k. Hettkamp [12] found criteria for the existence of unramified H_8-extensions of certain real quadratic number fields, and finally M. Horie [13] gave the first explicit example of such an extension. Recently, Louboutin and Okazaki [23, 24, 25] have computed relative class numbers of quaternion CM-extensions of $\mathbb{Q}$ as well as of unramified quaternion extensions of real quadratic number fields ([26]).

In [21, 22] we have shown how to construct unramified quaternion extensions of a number field k which is a quadratic extension of a field F, and F is totally real and has odd class number in the strict sense. In this article we will show that this construction can be carried out with completely elementary methods as long as we restrict ourselves to quadratic number fields.

1. Preliminaries

We begin by introducing some notation. Let k be a quadratic number field with discriminant d. An extensions K/k is said to be unramified if $\operatorname{disc}(K/k) = (1)$, i.e. if no finite primes ramify. The genus class field k_{gen} of k is defined as the maximal unramified extension of k which is abelian over $\mathbb{Q}$. It is known that k_{gen} is the compositum of all unramified quadratic extensions of k, and that $k_{\text{gen}} = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_t})$, where $d = d_1 \cdots d_t$ is the factorization of d into prime discriminants. Since we intend this article to be as self contained as possible, we will give a proof for the part of genus theory we need. First, however, we recall some basic facts from Hilbert's theory of ramification in Galois extensions (see, for example, [3] for proofs). Let K/F be a finite normal extension of number fields and put $G = \operatorname{Gal}(K/F)$. Moreover, let $\mathfrak{P}$ be a prime ideal in $\mathcal{O}_K$. Then the stabiliser of $\mathfrak{P}$,

$$Z_{\mathfrak{P}}(K/F) = \{\sigma \in G : \mathfrak{P}^\sigma = \mathfrak{P}\},$$

is called the *decomposition group*, and its subgroup

$$T_{\mathfrak{P}}(K/F) = \{\sigma \in Z_{\mathfrak{P}}(K/F) : \alpha^\sigma \equiv \alpha \bmod \mathfrak{P} \text{ for all } \alpha \in \mathcal{O}_K\}$$

the *inertia group* of $\mathfrak{P}$. The order of $T_{\mathfrak{P}}(K/F)$ is equal to the ramification index of $\mathfrak{P}$ in K/F. The residue class field $\mathcal{O}_K/\mathfrak{P}$ is a finite extension of $\mathcal{O}_F/\mathfrak{p}$ with Galois group isomorphic to $Z_{\mathfrak{P}}/T_{\mathfrak{P}}$; in particular, $T_{\mathfrak{P}}$ is a *normal* subgroup of $Z_{\mathfrak{P}}$. We will make use of the following properties of the Hilbert sequence:

PROPOSITION 1. *Let K/F be a finite normal extension of number fields, and let $\mathfrak{P}$ be a prime ideal in $\mathcal{O}_K$ lying over the prime ideal $\mathfrak{p}$ in $\mathcal{O}_F$.*

(1) *$\mathfrak{p}$ splits completely in a normal subextension k/F ($\mathfrak{p} \in \mathrm{Spl}(k/F)$) if and only if $Z_{\mathfrak{p}} \subseteq \mathrm{Gal}(K/k)$;*
(2) *Let $\mathfrak{p}_k = \mathfrak{P} \cap \mathcal{O}_k$ be the prime ideal in $\mathcal{O}_k$ lying below $\mathfrak{P}$; then $\mathfrak{p}_k$ is unramified in k/F if and only if $T_{\mathfrak{P}}(K/F) \subseteq \mathrm{Gal}(K/k)$;*
(3) *Let $T(K/F)$ be the subgroup of $\mathrm{Gal}(K/F)$ generated by all the inertia subgroups $T_{\mathfrak{p}}(K/F)$; then the fixed field k of $T(K/F)$ is the maximal unramified extension of F contained in K, and k/F is normal.*

COROLLARY 1. *(Chebotarev's Monodromy Theorem) Let k be a quadratic number field, and suppose that K/k is unramified and that $K/\mathbb{Q}$ is normal. Then the Galois group of $K/\mathbb{Q}$ is generated by elements of order 2 not contained in $\mathrm{Gal}(K/k)$.*

Proof. Since $\mathbb{Q}$ does not have nontrivial unramified extensions, the group T generated by all inertia subgroups must fix $\mathbb{Q}$ (by Prop. 1, part. 3.); this shows that $T = \mathrm{Gal}(K/\mathbb{Q})$. Since K/k is unramified, we have $T \cap \mathrm{Gal}(K/K) = \{1\}$.

COROLLARY 2. *If $K/\mathbb{Q}$ is an H_8-extension of $\mathbb{Q}$, then there exists a prime with ramification index 4. In particular, K is ramified over every quadratic subfield of $K/\mathbb{Q}$.*

Proof. Since H_8 cannot be generated by elements of order 2, there must be some inertia group $T_{\mathfrak{P}}$ of order divisible by 4. Then $\mathfrak{P}$ is completely ramified over its (quadratic) inertia subfield; in particular, $\mathfrak{P}$ ramifies in K/k, where k is the biquadratic subfield of $K/\mathbb{Q}$.

COROLLARY 3. *Let K/F be a cyclic quartic extension with quadratic subfield k. Then every prime ramifying in k/F also ramifies in K/k.*

Proof. Since $\mathfrak{p}$ ramifies in k/F and K/F is cyclic of prime power degree, F must be the inertia subfield of $\mathfrak{p}$ in K/F.

The following result is well known ([3], 14.33):

PROPOSITION 2. *Let k be a quadratic number field with discriminant d. Then d can be written uniquely as a product of prime discriminants.*

Finally, the next proposition contains all the genus theory we will need:

PROPOSITION 3. *Let k be a quadratic number field and suppose that K/k is an unramified quadratic extension. Then $K/\mathbb{Q}$ is normal, and $\mathrm{Gal}(K/k) \simeq (2,2)$.*

Proof. If $K/\mathbb{Q}$ is not normal, let σ be the nontrivial automorphism of $k/\mathbb{Q}$. Then $N = KK^\sigma$ is the normal closure of $K/\mathbb{Q}$, and $\mathrm{Gal}(N/\mathbb{Q})$ is a nonabelian group of order 8 with a subgroup $\mathrm{Gal}(N/k)$ of type $(2,2)$. The only such group is the dihedral group of order 8. Since K/k is unramified, so are K^σ/k and N/k. Let F be the quadratic subfield of $N/\mathbb{Q}$ over which N is cyclic, and let M be its quadratic subextension. Since N/M is unramified, so is M/F by Cor. 3. But then M is unramified over k and F. Since $M/\mathbb{Q}$ is bicyclic, it contains three quadratic subfields, k, F, and $\widetilde{k}$, say. Let p be any prime ramified in $\widetilde{k}/\mathbb{Q}$. Since M/k is unramified, p has inertia degree 2 in $M/\mathbb{Q}$, hence its inertia subfield in M is k or F. But this contradicts the fact that M/k and M/F are unramified.

2. Construction of H_8-Extensions

Now let M/k be an unramified normal extension of k with Galois group

$$\mathrm{Gal}(M/k) = H_8 = \langle \sigma, \tau : \sigma^2 = \tau^2 = -1, \sigma\tau = -\tau\sigma \rangle,$$

the quaternion group of order 8 (observe that -1 denotes a central involution, i.e. an automorphism of order 2 contained in the center of the group). We will also assume that M is normal over $\mathbb{Q}$.

Our first claim is that $\Gamma = \mathrm{Gal}(M/\mathbb{Q}) \simeq D_4 \oplus_Z C_4$ (this is the direct product of D_4 and C_4 where the central involutions of D_4 and C_4 are identified, also called the push-out of D_4 and C_4 with respect to the central subgroups Z of order 2 in D_4 and C_4; see Lang's Algebra [19], p. 81. It is the group 16.008 in [11] and [35]). In fact, let K be the quartic subextension of M/k; then K/k is an elementary abelian unramified extension of k, hence contained in the genus class field of k. In particular we see that $\mathrm{Gal}(K/\mathbb{Q}) \simeq (2,2,2)$; therefore Γ is a group of order 16 with a subgroup of type H_8 and a factor group of type $(2,2,2)$. There are only two such groups (see [11] or [35]), i.e. $C_2 \times H_8$ and $D_4 \oplus_Z C_4$. But $C_2 \times H_8$ cannot be generated by elements of order 2, therefore we must have $\Gamma \simeq D_4 \oplus_Z C_4$.

Now we put $\Gamma = \langle \rho, \sigma, \tau : \rho^2 = \sigma^2 = \tau^2 = -1, [\rho,\sigma] = [\rho,\tau] = 1, \sigma\tau = -\tau\sigma \rangle$. Γ has seven subgroups of order 8; three of them (those containing ρ) have type $(2,4)$, three are dihedral groups (namely $\Delta_1 = \langle \sigma, \rho\tau \rangle$, $\Delta_2 = \langle \tau, \rho\sigma \rangle$, and $\Delta_3 = \langle \rho\sigma, \rho\tau \rangle$), and one of them is the quaternion subgroup $\langle \sigma, \tau \rangle$ fixing the field k (see Table 1).

The fixed field of Δ_j $(1 \le j \le 3)$ is a quadratic number field k_j with discriminant d_j. We claim that the d_j are relatively prime. In fact, assume that $\mathfrak{p}$ is a prime ideal which ramifies in at least two of the three fields $k_j = \mathbb{Q}(\sqrt{d_j}\,)$, say in k_1 and k_2; let $T_\mathfrak{p}(M/\mathbb{Q})$ denote the inertia subgroup of Γ. Then $T_\mathfrak{p}(M/\mathbb{Q})$ has the following properties:

(1) $T_\mathfrak{p}(M/\mathbb{Q})$ has order 2: this follows from M/k being unramified;

(2) $T_\mathfrak{p}(M/\mathbb{Q}) \cap \Delta_1 = T_\mathfrak{p}(M/\mathbb{Q}) \cap \Delta_2 = \{1\}$, because $\mathfrak{p}$ cannot ramify in M/k_j $(1 \le j \le 2)$.

But now we see that $\Delta_1 \cup \Delta_2$ contains all seven elements of order 2, hence at least one of them must contain the element of order 2 which generates $T_\mathfrak{p}(M/\mathbb{Q})$. The same argument applied to an infinite prime yields that at most one of the discriminants d_j can be negative.

TABLE 1

G	fixed field of G	$G \simeq$
$\langle -1, \rho\sigma\tau \rangle$	$K_{12} = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$	$(2,2)$
$\langle -1, \rho\sigma \rangle$	$K_{23} = \mathbb{Q}(\sqrt{d_2}, \sqrt{d_3})$	$(2,2)$
$\langle -1, \rho\tau \rangle$	$K_{13} = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_3})$	$(2,2)$
$\langle \rho \rangle$	$L_0 = \mathbb{Q}(\sqrt{d_1 d_2}, \sqrt{d_1 d_3})$	(4)
$\langle \sigma \rangle$	$L_1 = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2 d_3})$	(4)
$\langle \tau \rangle$	$L_2 = \mathbb{Q}(\sqrt{d_2}, \sqrt{d_1 d_3})$	(4)
$\langle \sigma\tau \rangle$	$L_3 = \mathbb{Q}(\sqrt{d_3}, \sqrt{d_1 d_2})$	(4)
$\langle \sigma, \tau \rangle$	$k = \mathbb{Q}(\sqrt{d})$	H_8
$\langle \rho, \sigma\tau \rangle$	$k_{12} = \mathbb{Q}(\sqrt{d_1 d_2})$	$(2,4)$
$\langle \rho, \sigma \rangle$	$k_{23} = \mathbb{Q}(\sqrt{d_2 d_3})$	$(2,4)$
$\langle \rho, \tau \rangle$	$k_{13} = \mathbb{Q}(\sqrt{d_1 d_3})$	$(2,4)$
$\langle \sigma, \rho\tau \rangle$	$k_1 = \mathbb{Q}(\sqrt{d_1})$	D_4
$\langle \tau, \rho\sigma \rangle$	$k_2 = \mathbb{Q}(\sqrt{d_2})$	D_4
$\langle \rho\sigma, \rho\tau \rangle$	$k_3 = \mathbb{Q}(\sqrt{d_3})$	D_4
$\langle \rho, \sigma, \tau \rangle$	$\mathbb{Q}$	$D_4 \oplus_Z C_4$

Now K contains the three quadratic subfields k_j; from degree considerations it is clear that we must have $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3})$. In particular, K contains the quadratic number field with discriminant $d' = d_1 d_2 d_3$; we claim that $d = d'$. Since $K \subseteq k_{\text{gen}}$, we see that $d_1 d_2 d_3$ divides d (otherwise K/k would ramify). On the other hand, $\mathbb{Q}(\sqrt{d}) \subset K$ shows that d is the product of some of the d_i; therefore we must have the equality $d = d_1 d_2 d_3$.

So far we have seen: if there is an unramified quaternion extension M/k, then $d = \operatorname{disc} k = d_1 d_2 d_3$ is the product of three relatively prime discriminants d_j, at most one of which is negative.

Next we will study the decomposition of primes in $M/\mathbb{Q}$. To this end, consider a prime $p \mid d_1$; then $p\mathcal{O}_1 = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$ in the ring of integers $\mathcal{O}_1$ of k_1. Let F be the fixed field of $\langle\sigma\rangle$; then F contains the fixed field k of $\langle\sigma,\tau\rangle$, the fixed field k_1 of $\langle\sigma,\rho\tau\rangle$ and the fixed field $k_{23} = \mathbb{Q}(\sqrt{d_2d_3}\,)$ of $\langle\sigma,\rho\rangle$. We claim that p splits in $k_{23}/\mathbb{Q}$. We already know that the inertia subgroup $T = T_p(M/\mathbb{Q})$ has order 2; since the prime ideal $\mathfrak{p}$ above p in k_1 does not ramify in M/k_1, we must have $T \cap \Delta_1 = \{1\}$. Enumerating the subgroups of order 2 in Γ shows that there are only the possibilities $T = \langle\rho\sigma\rangle$ and $T = \langle-\rho\sigma\rangle$. But now the normaliser of T in Γ equals $N_\Gamma(T) = \langle\rho,\sigma\rangle$. Since T is a normal subgroup of the decomposition group $Z = Z_p(M/\mathbb{Q})$ of p, we conclude that $Z \subseteq \langle\rho,\sigma\rangle$. But this means that the fixed field k_{23} of $\langle\rho,\sigma\rangle$ is contained in the decomposition field for p, i.e. p splits in $k_{23}/\mathbb{Q}$, and we have $(d_2d_3/p_1) = +1$ for all primes p_1 dividing d_1. By symmetry we conclude

PROPOSITION 4. *Let k be a quadratic number field with discriminant d. If there exists an unramified extension M/k with* $\operatorname{Gal}(M/k) \simeq H_8$ *and which is normal over $\mathbb{Q}$, then*

1. $\operatorname{Gal}(M/\mathbb{Q}) \simeq D_4 \oplus_Z C_4$*;*
2. *there is a factorization $d = d_1d_2d_3$ of d into three discriminants d_1, d_2, d_3, at most one of which is negative;*
3. *for all primes $p_i \mid d_i$ we have $(d_1d_2/p_3) = (d_2d_3/p_1) = (d_3d_1/p_2) = +1$.*

Remark. We will call a factorization $d = d_1d_2d_3$ of d into discriminants an H_8-factorization, if the condition $(d_1d_2/p_3) = (d_2d_3/p_1) = (d_3d_1/p_2) = +1$ is satisfied for all $p_i \mid d_i$. It is an easy exercise to show that the quadratic reciprocity law implies that at most one of the d_i is negative.

Our next task is the explicit construction of the unramified H_8-extension M/k. To this end, assume that we have already found it, and let $\Gamma = \operatorname{Gal}(M/\mathbb{Q})$ be as above. Then $K_{13} = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_3}\,)$ is the fixed field of $\langle-1,\rho\tau\rangle$ (we will write $K_{13} \overset{\text{gal}}{\longleftrightarrow} \langle-1,\rho\tau\rangle$); therefore M/K_{13} is an extension of type $(2,2)$ with subfields $K_{13}(\sqrt{d_2}\,) \overset{\text{gal}}{\longleftrightarrow} \langle-1\rangle$, $N = K_{13}(\sqrt{\mu}\,) \overset{\text{gal}}{\longleftrightarrow} \langle\rho\tau\rangle$ and $N' = K_{13}(\sqrt{\nu}\,) \overset{\text{gal}}{\longleftrightarrow} \langle-\rho\tau\rangle$ for some $\mu, \nu \in K_{13}$. Now σ and ρ act on $\langle-1,\rho\tau\rangle$, σ is trivial on $\mathbb{Q}(\sqrt{d_1}\,)$ and ρ on $\mathbb{Q}(\sqrt{d_3}\,)$. Since $(\rho\tau)^\sigma = -\rho\tau$ and $(\rho\tau)^\rho = \rho\tau$, we see that $N^\sigma = N'$, $N^\rho = N$ and $N^{\rho\sigma} = N'$. In particular we can choose $\nu = \mu^\sigma$.

Of course, any $\mu \in L$ can be written in the form $\mu = x + y\sqrt{d_1} + z\sqrt{d_3} + w\sqrt{d_1d_3}$. But for the construction of the class fields it would be preferable if μ could be factorized into elements coming from subfields of K_{13}. Let us therefore put $\mu = (x_1 + y_1\sqrt{d_1}\,)(x_3 + y_3\sqrt{d_3}\,)(x\sqrt{d_1} + y\sqrt{d_3}\,)$, where the coefficients are rational. Since $K_{13}(\sqrt{\mu\mu^\sigma}) = K_{13}(\sqrt{d_2})$, we conclude that $\mu\mu^\sigma \overset{2}{=} d_2$ (the symbol $\overset{2}{=}$ indicates that the two sides differ only by a square in K_{13}). We find:

$$\begin{aligned} \mu^{1+\sigma} &= (x_1 + y_1\sqrt{d_1})^2(x_3^2 - d_3y_3^2)(d_1x^2 - d_3y^2) \overset{2}{=} d_2 \\ \mu^{1+\rho} &= (x_1^2 - d_1y_1^2)(x_3^2 - d_3y_3^2)(x\sqrt{d_1} + y\sqrt{d_3})^2 \overset{2}{=} -1 \\ \mu^{1+\rho\sigma} &= (x_1^2 - d_1y_1^2)(x_3 + y_3\sqrt{d_3})^2(-d_1x^2 + d_3y^2) \overset{2}{=} -d_2 \end{aligned}$$

If we put $a := x_1^2 - d_1y_1^2$, then the second equation yields $-a \overset{2}{=} x_3^2 - d_3y_3^2$, and from the first equation we get $d_1x^2 - d_3y^2 \overset{2}{=} -ad_2$. This suggests that in order to construct $D_4 \oplus_Z C_4$-extensions of $\mathbb{Q}$ we should try to solve the following system of diophantine equations over $\mathbb{Z}$:

$$\begin{array}{rcll} d_1X_1^2 - d_2X_2^2 &=& -ad_3X_3^2 & (I) \\ Y_1^2 - d_1Y_2^2 &=& aY_3^2 & (II) \\ Z_1^2 - d_2Z_2^2 &=& -aZ_3^2 & (III) \end{array}$$

The same system of equations was given by M. Horie [13]; moreover, the construction presented by Minác and Smith [29] uses three equations which can easily be shown to be equivalent to (I)-(III). In the form of the ”common slot property” (cf. T. Smith [34], Prop. 1.1.2) of quaternion algebras it seems to have been well known to people familiar with Brauer groups. Now we claim

PROPOSITION 5. *Let k be a quadratic number field with discriminant d, and suppose that $d = d_1d_2d_3$ is an H_8-factorization. Then there exists an odd squarefree $a \in \mathbb{Z}$ such that the system (I) - (III) of diophantine equations has nontrivial solutions in $\mathbb{Z}$. If $x_i, y_i, z_i \in \mathbb{Z}$ form a solution, put*

$$\mu \;=\; (x_1\sqrt{d_1} + x_2\sqrt{d_2})(y_1 + y_2\sqrt{d_1})(z_1 + z_2\sqrt{d_2})/r,$$

where $r \in \mathbb{Z}$ is an arbitrary nonzero integer.
Then $M = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3}, \sqrt{\mu})$ is an H_8-extension of k which is normal over $\mathbb{Q}$ with $\mathrm{Gal}(M/\mathbb{Q}) \simeq D_4 \oplus_Z C_4$. If we choose $r \in \mathbb{Z}$ in such a way that μ is integral and not divisible by any rational prime p, then there is a 2-primary element in $\{\pm\mu\}$ if $d_1d_2 \equiv 0, 1 \bmod 8$, and in $\{\mu, 2\mu\}$ if $d_1d_2 \equiv 4 \bmod 8$.

Existence of a. We want to show that the diophantine equations (I)–(III) have nontrivial solutions if we choose $a \in \mathbb{Z}$ suitably. To this end we write $d_1 = \prod d_{1,i}$ and $d_2 = \prod d_{2,i}$ as products of prime discriminants. We will assume without loss of generality that $d_2 > 0$ (otherwise we simply exchange d_1 and d_2 – recall that at most one of the d_i is negative). Then we claim that (I)–(III) are nontrivially solvable in $\mathbb{Z}$ if and only if the following conditions are satisfied:

(1) $a > 0$ if $d_1 < 0$;
(2) $(d_1/a) = (d_2/a) = +1$;
(3) $(d_{1,i}/a) = +1$ for all discriminants $d_{1,i} \mid d_1$;
(4) $(d_{2,i}/a) = \operatorname{sign}(d_{2,i})$ for all discriminants $d_{2,i} \mid d_2$.

Before we prove this, let us show that such $a \in \mathbb{Z}$ actually exist. If d_2 is a sum of two squares, then we can obviously choose $a = 1$. If not, then we can find an odd prime a satisfying properties (1), (3) and (4) by making use of quadratic reciprocity and Dirichlet's theorem on primes in arithmetic progressions (here we use that d_1 and d_2 are relatively prime). We claim that all such primes satisfy condition (2) automatically. In fact this is obvious for the condition on d_1; since d_2 was assumed to be positive, the number of negative $d_{2,i}$ is even, and this implies $1 = \prod(d_{2,i}/a) = (d_2/a)$.

Now consider the diophantine equation (I): $d_1X_1^2 - d_2X_2^2 = -ad_3X_3^2$. We have to show that it has solutions in the reals, modulo a and modulo every odd prime dividing d (we can neglect the prime 2 because of the product formula). Solvability in $\mathbb{R}$ is clear: if (II) is solvable in $\mathbb{R}$ then $d_1 < 0$ clearly implies $a > 0$. Moreover, this condition suffices for the solvability in $\mathbb{R}$ of (I) and (II); since $d_2 > 0$, (III) always has real solutions. If we reduce (I) modulo a, then we get $d_1X_1^2 \equiv d_2X_2^2$; since $(d_1/a) = (d_2/a) = +1$, this equation is indeed solvable. Now let p be an odd prime dividing d_1; we get $d_2X_2^2 \equiv ad_3X_3^2 \bmod p$. The condition $(d_2/p) = (d_3/p)$ shows that solvability is equivalent to $(a/p) = +1$. Quadratic reciprocity shows that this is equivalent to $(p^*/a) = +1$, where $p^* = (-1)^{(p-1)/2}p$ is the unique prime discriminant divisible by p; now condition (3) guarantees solvability. Next assume that $p \mid d_2$; then we have to solve $d_1X_1^2 \equiv -ad_3X_3^2 \bmod p$. Again, the condition $(d_1/p) = (d_3/p)$ reduces this to a proof of $(-a/p) = +1$. If $p \equiv 1 \bmod 4$, this is equivalent to $(p/a) = +1$, which holds because of (4). If $p \equiv 3 \bmod 4$, then $(-a/p) = +1 \iff (a/p) = -1 \iff (p^*/a) = -1$, and again this is true by (4). Finally let $p \mid d_3$; then $d_1X_1^2 \equiv d_2X_2^2 \bmod p$ is clearly solvable. The equations (II) and (III) can be treated similarly.

Computation of the Galois Group. Let $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3})$; then K/k is unramified and we have $\mathrm{Gal}(K/k) \simeq (2,2)$. If $\alpha, \beta \in K^\times$ satisfy an equation $\alpha = \beta\xi^2$ for some $\xi \in K^\times$, then we write $\alpha \overset{2}{=} \beta$. For the computation of $\mathrm{Gal}(M/k)$ we need a result which was stated without proof by Furtwängler [9]:

LEMMA 1. *Let K/F be a quartic extension with $\mathrm{Gal}(K/F) \simeq (2,2)$; let σ, τ and $\sigma\tau$ denote its nontrivial automorphisms, and put $M = K(\sqrt{\mu})$. Then M/F is normal if and only if $\mu^{1-\rho} \overset{2}{=} 1$ for all $\rho \in \mathrm{Gal}(K/F)$. If this is the case, write $\mu^{1-\sigma} = \alpha_\sigma^2$, $\mu^{1-\tau} = \alpha_\tau^2$ and $\mu^{1-\sigma\tau} = \alpha_{\sigma\tau}^2$. It is easy to see that $\alpha_\rho^{1+\rho} = \pm 1$ for all $\rho \in \mathrm{Gal}(K/F)$; define $S(\mu, K/F) = (\alpha_\sigma^{1+\sigma}, \alpha_\tau^{1+\tau}, \alpha_{\sigma\tau}^{1+\sigma\tau})$ and identify vectors which coincide upon permutation of their entries. Then*

$$\mathrm{Gal}(M/F) \simeq \begin{cases} (2,2,2) & \Longleftrightarrow \quad S(\mu,K/F) = (+1,+1,+1), \\ (2,4) & \Longleftrightarrow \quad S(\mu,K/F) = (-1,-1,+1), \\ D_4 & \Longleftrightarrow \quad S(\mu,K/F) = (-1,+1,+1), \\ H_8 & \Longleftrightarrow \quad S(\mu,K/F) = (-1,-1,-1). \end{cases}$$

Moreover, M is cyclic over the fixed field of $\langle\rho\rangle$ if and only if $\alpha_\rho^{1+\rho} = -1$, and has type $(2,2)$ otherwise.

Proof. Let K/k be a quadratic extension and put $M = K(\sqrt{\mu})$ for some $\mu \in K$. Let σ denote the nontrivial automorphism of K/k. Then M/k is normal if and only if $M^\sigma = M$, and by Kummer Theory this is equivalent to $\mu^\sigma \overset{2}{=} \mu$, i.e. to $\mu^{1-\sigma} = \alpha_\sigma^2$ for some $\alpha_\sigma \in K^\times$. Since $(\alpha_\sigma^2)^{1+\sigma} = \mu^{(1-\sigma)(1+\sigma)} = 1$, we see that $\alpha_\sigma = \pm 1$.

Next suppose that M/k is normal; then $\tilde{\sigma} : a + b\sqrt{\mu} \longmapsto a^\sigma + b^\sigma\alpha_\sigma\sqrt{\mu}$ defines an automorphism of M/k whose restriction to K/k coincides with σ. But now $\tilde{\sigma}^2 : a+b\sqrt{\mu} \longmapsto a+b\alpha^{1+\sigma}\sqrt{\mu}$, hence $\tilde{\sigma}$ has order 4 if $\alpha^{1+\sigma} = -1$ and order 2 if $\alpha^{1+\sigma} = +1$.

Now clearly M/F will be normal if and only if $\mu^\rho \overset{2}{=} \mu$ for all $\rho \in \mathrm{Gal}(K/F)$, i.e. if and only if M/k_i is normal for all three quadratic subextensions k_i of K/k. Moreover, the noncyclic groups of order 8 can be classified by their number of automorphisms of order 4: this number is $0, 1, 2$ or 3 if $G \simeq (2,2,2), D_4, (2,4)$ or H_8, respectively. The claims of Lemma 1 now follow.

Lemma 1 reduces the verification of $\mathrm{Gal}(M/k) \simeq H_8$ to a simple computation; in order to simplify the notation, put $\beta = (x_1\sqrt{d_1} + x_2\sqrt{d_2})$, $\gamma = (y_1 + y_2\sqrt{d_1})$ and $\delta = (z_1 + z_2\sqrt{d_2})$; then $\mu = r\beta\gamma\delta$, and we find

$$\begin{array}{llll} \alpha_\sigma & = ax_3z_3\sqrt{d_3}/(\beta^\sigma\delta^\sigma), & \alpha_\sigma^{1+\sigma} & = -1 \\ \alpha_\tau & = ax_3y_3\sqrt{d_2}/(\beta^\sigma\gamma^\tau), & \alpha_\tau^{1+\tau} & = -1 \\ \alpha_{\sigma\tau} & = ay_3z_3/(\gamma^\tau\delta^\sigma), & \alpha_{\sigma\tau}^{1+\sigma\tau} & = -1. \end{array}$$

Therefore $\mathrm{Gal}(M/k) \simeq H_8$. Next we check that $M/\mathbb{Q}$ is normal. To this end, let ρ be an extension of the nontrivial automorphism of $k/\mathbb{Q}$, say

$\rho : \sqrt{d_i} \longmapsto -\sqrt{d_i}$ for $1 \leq i \leq 3$. Then $M/\mathbb{Q}$ is normal if and only of $M^\rho = M$, i.e. if $\mu^{1-\rho} \overset{2}{=} 1 \bmod K^\times$. A small computation shows that $\mu^{1-\rho} = (ay_3z_3/(\gamma^\tau\delta^\sigma))^2$ and $\alpha_\rho^{1+\rho} = -1$.

Finally we verify that $M/\mathbb{Q}(\sqrt{d_i})$ is a D_4-extension for $1 \leq i \leq 3$ (by using Lemma 1 again); this implies that $\mathrm{Gal}(M/\mathbb{Q})$ is not isomorphic to $C_2 \times H_8$, and now $\mathrm{Gal}(M/\mathbb{Q}) \simeq D_4 \oplus_Z C_4$ follows.

Ramification outside 2∞. We start with $r = 1$ and integral solutions x_i, y_i, z_i of our system of equations. Let $\mathfrak{p}$ be a prime ideal in K lying above an odd prime p.

Suppose first that $p \nmid d$. If $\mathfrak{p}$ ramifies in M/K, then $\mathfrak{p} \mid \mu$; since $M/\mathbb{Q}$ is normal, all conjugates of $\mathfrak{p}$ also ramify, hence also divide μ, and we find that $p \mid \mu$. Replacing r by r/p we see that we can find an $r \in \mathbb{Q}$ such that μ is integral and not divisible by any prime not dividing $2d$, and that the corresponding μ defines a quaternion extension M/k which is unramified outside $2d\infty$.

Now assume that $p \mid d$ is odd. Then $\mathfrak{p}$ is unramified in K/k, so if $\mathfrak{p}$ ramifies in M/K then the ramification index $e_p(M/\mathbb{Q})$ must equal 4. The inertia subfield M_T of p has therefore degree 4 over $\mathbb{Q}$, and all such fields are easily seen to be V_4-extensions of $\mathbb{Q}$. If we assume (without loss of generality) that $p \mid d_3$, then since p does not ramify in its inertia field, we must have $M_T = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. But now M/M_T is a V_4-extension, so that only primes above 2 can ramify completely. This shows that all odd $p \mid d$ are unramified in M/k.

Ramification above 2. We will assume that

$$\mu = r(x_1\sqrt{d_1} + x_2\sqrt{d_2})(y_1 + y_2\sqrt{d_1})(z_1 + z_2\sqrt{d_2}) \in K_{12} = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$$

is integral and not divisible by any rational prime p; moreover, we suppose that d_1d_2 is odd, i.e. that 2 is unramified in $K_{12}/\mathbb{Q}$. We have to show that μ or $-\mu$ is 2-primary in K, i.e. that 2 does not ramify in at least one of the extensions $K(\sqrt{\mu})/K$ or $K(\sqrt{-\mu})/K$.

Since $2 \nmid \mu$ and 2 is not ramified, there is a prime ideal $\mathfrak{Q}$ above $2\mathcal{O}_K$ which does not divide μ. If we can show that μ is $\mathfrak{Q}$-primary, then $\mathfrak{Q}$ does not ramify in M/K; but $M/\mathbb{Q}$ is normal, so if $\mathfrak{Q}$ does not ramify, neither does any other prime ideal above 2, and our claim follows. It is obviously sufficient to show that $\pm\mu$ is $\mathfrak{Q}$-primary in K_{12}.

Suppose that 2 splits completely in $K_{12}/\mathbb{Q}$. Then $\mathcal{O}_{12}/\mathfrak{Q}^m \simeq \mathbb{Z}/2^m\mathbb{Z}$, hence $\mu \equiv a \bmod \mathfrak{Q}^2$ for some odd integer a. But either a or $-a$ is congruent to 1 mod 4, hence $\pm\mu \equiv 1 \bmod \mathfrak{Q}^2$ is 2-primary.

Next assume that $\mathfrak{Q}$ has inertia degree 2 in $K_{12}/\mathbb{Q}$. Since the norm of μ to the three quadratic subfields is either a square or d_3 times a square, these norms are 2-primary. Now we use the following

LEMMA 2. *Let K/k be a quadratic extension, and let $\mathfrak{q}$ be a prime ideal in $\mathcal{O}_k$ above 2; assume moreover that $\mathfrak{q}$ is inert in K/k. If $N_{K/k}\mu$ is $\mathfrak{q}$-primary in $\mathcal{O}_k$ and $\mathfrak{q} \nmid \mu$ then there exists an $\alpha \in \mathcal{O}_k \setminus \mathfrak{q}$ such that $\mu\alpha$ is $\mathfrak{q}$-primary.*

Assuming the truth of the lemma for the moment, we find that it is sufficient to show that $\alpha \in k_i$ is $\mathfrak{q}$-primary. But since 2 splits in $k_i/\mathbb{Q}$, we have $\alpha \equiv \pm 1 \bmod \mathfrak{q}^2$, and we are done.

Proof. [Proof of Lemma 2] We first claim that there exists a $\xi \in \mathcal{O}_k \setminus \mathfrak{q}$ such that $\mu\xi^2 + \mu'\xi'^2 \not\equiv 0 \bmod \mathfrak{q}$, where μ' denotes the conjugate of μ with respect to K/k. In fact if $\mathfrak{q} \nmid (\mu + \mu')$ then we can take $\xi = 1$; assume therefore that $\mathfrak{q} \mid (\mu + \mu')$. Since the trace is surjective in extensions of finite fields, there exists a $\xi \in \mathcal{O}_K$ such that $\xi + \xi' \equiv 1 \bmod \mathfrak{q}$. From $\mathfrak{q} \mid 2$ we get $\mu\xi^2 + \mu'\xi'^2 \equiv \mu(\xi + \xi')^2 \bmod \mathfrak{q}$. Put $\nu = \mu\xi^2$; then $K(\sqrt{\mu}) = K(\sqrt{\nu})$. Since $\mu\mu' \equiv \eta_0^2 \bmod \mathfrak{q}^2$ for some $\eta_0 \in \mathcal{O}_k$, we find $\nu\nu' = \mu\mu'(\xi\xi')^2 \equiv \eta^2 \bmod \mathfrak{q}^2$ for $\eta = \eta_0(\xi\xi') \in \mathcal{O}_k$. This implies at once that $\sqrt{\nu\nu'} \equiv \eta \bmod \mathfrak{q}$ in $\mathcal{O}_L$, where $L = k(\sqrt{\mu\mu'})$. Put $\alpha = \nu + \nu' + 2\eta$; then $\alpha \in \mathcal{O}_k$, $\mathfrak{q} \nmid \alpha$, and $\alpha\nu \equiv \nu(\nu + \nu' + 2\sqrt{\nu\nu'}) = (\nu + \sqrt{\nu\nu'})^2 \bmod \mathfrak{q}^2$. Therefore $\mu\alpha$ is $\mathfrak{q}$-primary in KL; but since L/k is unramified above $\mathfrak{q}$, this implies that $\mu\alpha$ is $\mathfrak{q}$-primary in K.

It remains to prove our claims if 2 ramifies in $K_{12}/\mathbb{Q}$. To this end we need

LEMMA 3. *Let k be a quadratic number field with discriminant $d = d_1d_2d_3$ and assume that $M = K(\sqrt{\mu})$ and $N = K(\sqrt{\nu})$ are two H_8-extensions of k, both constructed as in Prop. 5. In particular, they have the common subfield $K = k(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3})$. Then there exists a $\delta \in \mathbb{Z}$ such that $\nu \overset{2}{=} \delta\mu$. If, moreover, M/k and N/k are unramified outside ∞, then δ can be chosen to be a discriminant dividing d.*

Proof. Let $\mathrm{Gal}(K/\mathbb{Q}) = \langle \rho, \sigma, \tau \rangle \simeq (2,2,2)$. If $M = N$, then $\nu \overset{2}{=} \mu$ and there is nothing to prove. Assume therefore that MN is a quartic extension of K and let L denote the third quadratic subfield of MN/K. The computations after Lemma 1 showed that $\mu^{1-\psi} = \alpha_\psi^2, \nu^{1-\psi} = \beta_\psi^2$, and $\alpha_\psi^{1+\psi} = \beta_\psi^{1+\psi} = -1$ for $\psi \in \{\rho, \sigma, \tau\}$. The proof of Lemma 1 shows immediately that $\mathrm{Gal}(L/\mathbb{Q}) \simeq (2,2,2,2)$, and this proves our claim that $\nu \overset{2}{=} \delta\mu$ for some $\delta \in \mathbb{Z}$. If M/k and N/k are unramified outside ∞, then so is L/k, and now the last claim follows from Prop. 3.

Now let $M = K(\sqrt{\mu})$ be the unramified H_8-extension of k constructed above (i.e. $\mu \in \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ with d_1d_2 odd), and put $N = K(\sqrt{\nu})$, where $\nu \in \mathbb{Q}(\sqrt{d_1}, \sqrt{d_3})$. By Lemma 3 we know that over K we have $\nu \overset{2}{=} 2\delta\mu$ for some $\delta \in \mathbb{Z}$. Since μ is 2-primary, so is $m\mu$ or $-m\mu$ for every odd $m \in \mathbb{Z}$; we may therefore assume without loss of generality that $\delta \in \{\pm 1, \pm 2\}$.

If $4 \nmid d_3$ and $\delta = \pm 1$, then we are done. If $d_3 \equiv 0 \bmod 8$, then 2 or -2 is 2-primary in K, and our claims also follow. Finally, if $d_3 \equiv 4 \bmod 8$, then one of $\{\nu, 2\nu\}$ must be 2-primary (note that -1 is 2-primary in this case). This completes the proof of Prop. 5.

We have already remarked that the construction of the quaternion extension is much simpler when one of the discriminants is a sum of two squares: assume for example that $d_2 = s^2 + t^2$; then we can choose $a = 1$, and $z_1 = s$, $z_2 = 1$ and $z_3 = t$ solve equation (III), $y_1 = y_3 = 1$ and $y_2 = 0$ solve (II). The following congruences help to choose the correct signs:

$$\begin{array}{lcll}
(1 + \sqrt{2a}\frac{1+\sqrt{b}}{2})^2 & \equiv & (\sqrt{b} + \sqrt{2a})(1 + \sqrt{2a}) & \text{if } \begin{cases} a \equiv 1 \bmod 2 \\ b \equiv 1 \bmod 8, \end{cases} \\
(1 + \sqrt{2a}\frac{1-\sqrt{b}}{2})^2 & \equiv & (\sqrt{b} + \sqrt{2a})(1 - \sqrt{2a}) & \text{if } \begin{cases} a \equiv 1 \bmod 2 \\ b \equiv 5 \bmod 8, \end{cases} \\
(2\sqrt{a} + \sqrt{b})(2 + \sqrt{b}) & \equiv & 1 \bmod 4 & \text{if } \begin{cases} a \equiv 1 \bmod 4 \\ b \equiv 1 \bmod 4, \end{cases} \\
(2\sqrt{a} - \sqrt{b})\sqrt{b} & \equiv & (1 + \sqrt{ab})^2 \bmod 4 & \text{if } \begin{cases} a \equiv 3 \bmod 4 \\ b \equiv 1 \bmod 4. \end{cases}
\end{array}$$

See Table 2 for some numerical examples.

TABLE 2

d	d_1	d_2	d_3	μ	Cl(k)
3848	8	13	37	$(12\sqrt{2} + 5\sqrt{13})(18 - 5\sqrt{13})$	(2,2)
2120	5	8	53	$(3\sqrt{5} + 7\sqrt{2})(1 + \sqrt{2})$	(2,2)
1480	5	8	37	$(3\sqrt{5} + 2\sqrt{2})(2 - \sqrt{5})$	(2,2)
520	5	8	13	$(3\sqrt{2} + \sqrt{5})(1 + \sqrt{2})$	(2,2)
−120	−3	5	8	$(2\sqrt{2} + \sqrt{5})(2 + \sqrt{5})$	(2,2)
−255	−3	5	17	$(\sqrt{5} + 2\sqrt{-3})(2 + \sqrt{5})$	(2,2,3)
−420	−4	5	21	$(4i - \sqrt{5})(2 + \sqrt{5})$	(2,2,2)
−455	−7	5	13	$(2\sqrt{13} - 3\sqrt{5})(2 + \sqrt{5})$	(2,2,5)
−520	−8	5	13	$(2\sqrt{-2} + \sqrt{5})(2 + \sqrt{5})$	(2,2)

We will collect our main results in

THEOREM 1. *Let k be a quadratic number field with discriminant d. Then the following assertions are equivalent:*

(1) *There exists an unramified H_8-extension M/k such that $M/\mathbb{Q}$ is normal;*

(2) *There is a factorization $d = d_1d_2d_3$ of d into three discriminants which are relatively prime and which satisfy the conditions $(d_1d_2/p_3) = (d_2d_3/p_1) = (d_3d_1/p_2) = +1$ for all $p_i \mid d_i$.*

Next we will show that this unramified H_8-extension is unique if the discriminants d_i are prime:

PROPOSITION 6. *Let k be a quadratic number field with discriminant $d = d_1d_2d_3$ and assume that $M = K(\sqrt{\mu})$ and N are unramified H_8-extensions of k with common subfield $K = k(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3})$; then there exists a discriminant $\delta \mid d$ such that $N = K(\sqrt{\delta\mu})$.*

Proof. This is proved exactly as Lemma 3: MN contains a subfield L such that L/k is unramified of type $(2,2,2)$ over k. Then Prop. 3 shows that $L = K(\sqrt{\delta})$ for some discriminant δ dividing d.

COROLLARY 4. *Suppose that $d = d_1d_2d_3$ and that the d_i are prime discriminants; then there exists at most one unramified H_8-extension of k.*

Proof. Since the d_i are prime discriminants, we see $\sqrt{\delta} \in K$; this implies $M = N$ in Prop. 6.

3. Ramification at ∞

Assume that $d = d_1d_2d_3$ is an H_8-factorization. If d has a prime factor $q \equiv 3 \bmod 4$, then there always exists an H_8-extension of k containing $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3})$ which is unramified everywhere. In fact, the element μ constructed in Prop. 5 is either totally positive or totally negative (since $K(\sqrt{\mu})/\mathbb{Q}$ is normal); if $\mu \gg 0$, $K(\sqrt{\mu})/k$ is the sought extension, and if $\mu \ll 0$, then we take $K(\sqrt{-q\mu})/k$.

If, on the other hand, d is the sum of two squares, then either every unramified H_8-extension of k is also unramified at ∞, or none is. The following proposition tells us that this depends only on certain biquadratic reciprocity symbols (the special case where all the d_i are prime discriminants such that $(d_i/d_j) = -1$ for $i \neq j$ is due to Hettkamp [12]):

PROPOSITION 7. *Let d_1, d_2, d_3 be positive discriminants, none of which is divisible by a prime $q \equiv 3 \bmod 4$, and assume that $d = d_1d_2d_3$ is an H_8-factorization. Then any H_8-extension M/k of $k = \mathbb{Q}(\sqrt{d})$ containing $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3})$ and unramified outside ∞ is totally real if and only if*

$$\Big(\frac{d_1d_2}{d_3}\Big)_4\Big(\frac{d_2d_3}{d_1}\Big)_4\Big(\frac{d_3d_1}{d_2}\Big)_4 = \Big(\frac{d_1}{d_2}\Big)\Big(\frac{d_2}{d_3}\Big)\Big(\frac{d_3}{d_1}\Big).$$

Here $(d_1d_2/d_3)_4 = \prod_{p_3|d_3}(d_1d_2/p_3)_4$, *and* $(d/2)_4 = (-1)^{(d-1)/8}$.

Proof. Let us first assume that $d \equiv 1 \bmod 4$. If (x, y, z) is a solution of

$$(1) \qquad d_1x^2 - d_2y^2 = -d_3z^2,$$

then x is even and yz is odd. Write $d_2 = a^2 + b^2$ as a sum of squares with $2 \mid b$. Then the square root of $\mu = (x\sqrt{d_1} + y\sqrt{d_2})(b + \sqrt{d_2})$ generates the unramified H_8-extension of k if and only if μ is 2-primary. But the congruences $xb \equiv 0$, $b\sqrt{d_2} \equiv b$, $x\sqrt{d_1d_2} \equiv x \bmod 4$ show that $\mu \equiv b + x + y \bmod 4$. Therefore, μ is 2-primary if and only if $b + x + y \equiv 1 \bmod 4$. This can be achieved by replacing μ by $-\mu$; assume therefore that μ is 2-primary.

Changing the sign of b does not affect the primarity of μ. We are therefore allowed to assume that $b > 0$. Then μ is totally positive if and only if $y > 0$.

Next we compute a few residue symbols from Eq. (1). Since it implies the congruence $d_1x^2 \equiv d_2y^2 \bmod d_3$, we find

$$\Big(\frac{d_1d_2}{d_3}\Big)_4 = \Big(\frac{xy}{d_3}\Big)\Big(\frac{d_2}{d_3}\Big).$$

Here we have used that d_3 is not divisible by any prime $q \equiv 3 \bmod 4$. In a similar way we get

$$\Big(\frac{d_2d_3}{d_1}\Big)_4 = \Big(\frac{yz}{d_1}\Big)\Big(\frac{d_3}{d_1}\Big) \quad \text{and} \quad \Big(\frac{d_3d_1}{d_2}\Big)_4 = \Big(\frac{-1}{d_2}\Big)_4\Big(\frac{zx}{d_2}\Big)\Big(\frac{d_3}{d_2}\Big).$$

Multiplying these equation yields

$$\Big(\frac{d_1d_2}{d_3}\Big)_4\Big(\frac{d_2d_3}{d_1}\Big)_4\Big(\frac{d_3d_1}{d_2}\Big)_4 = \Big(\frac{xy}{d_3}\Big)\Big(\frac{d_2}{d_3}\Big)\Big(\frac{yz}{d_1}\Big)\Big(\frac{d_3}{d_1}\Big)\Big(\frac{-1}{d_2}\Big)_4\Big(\frac{d_3}{d_2}\Big)\Big(\frac{zx}{d_2}\Big).$$

Now $(d_1d_2/d_3) = 1$ by assumption; moreover $(-1/d_2)_4 = (-1)^{b/2}$. On the other hand, looking at (1) modulo y and z we get $(d_1/y) = (-1/y)(d_3/y)$ and $(d_1/z) = (d_2/z)$. In order to compute (x/d_2) we write $x = 2^jx'$, where x' is the odd part of x. Then $(x/d_2) = (2/d_2)^j(x'/d_2) = (2/d_2)^j(d_2/x')$ and $(x/d_3) = (2/d_3)^j(x'/d_3) = (2/d_3)^j(d_3/x')$; from Eq. (1) we get $(d_2/x') = (d_3/x')$. Moreover, $j = 1 \iff x \equiv 2 \bmod 4 \iff d_2d_3 \equiv 5 \bmod 8$, hence $(2/d_2)^j(2/d_3)^j = (2/d_2d_3) = (-1)^{x/2}$. Collecting everything gives

$$\begin{aligned}\Big(\frac{d_1d_2}{d_3}\Big)_4\Big(\frac{d_2d_3}{d_1}\Big)_4\Big(\frac{d_3d_1}{d_2}\Big)_4 &= (-1)^{b/2}(-1)^{x/2}\Big(\frac{-1}{y}\Big)\Big(\frac{d_3}{d_2}\Big)\\ &= (-1)^{(b+x+|y|-1)/2}\Big(\frac{d_3}{d_2}\Big).\end{aligned}$$

Now the congruence $b + x + y \equiv 1 \bmod 4$ shows that $y > 0$ is equivalent to

$$\Big(\frac{d_1d_2}{d_3}\Big)_4\Big(\frac{d_2d_3}{d_1}\Big)_4\Big(\frac{d_3d_1}{d_2}\Big)_4 = \Big(\frac{d_3}{d_2}\Big).$$

Our claim follows since $(d_1/d_2)(d_3/d_1) = (d_2d_3/d_1) = +1$.

If one of the prime discriminants is divisible 8 then there are a few complications, but the very same proof shows that the result is valid also in this case. We may assume without loss of generality that $8 \mid d_2$. We start with the equation

$$d_1x^2 - 2my^2 = -d_3z^2, \tag{2}$$

(where $m \equiv 1 \bmod 4$) and put $\mu = (x\sqrt{d_1} + y\sqrt{2m})(t + \sqrt{2m})$, where $2m = t^2 + u^2$ for some $t \equiv 1 \bmod 4$; observe that $xyz \equiv 1 \bmod 2$. Then μ is 2-primary if and only if $y \equiv (2/d_1) \bmod 4$. As above, we find

$$\left(\frac{8md_1}{d_3}\right)_4 = \left(\frac{xy}{d_3}\right), \quad \left(\frac{8md_3}{d_1}\right)_4 = \left(\frac{yz}{d_1}\right), \quad \left(\frac{d_3d_1}{8m}\right)_4 = (-1)^{(d_1d_3-1)/8}.$$

Now $(x/d_3) = (d_3/x) = (d_2/x) = (2m/x)$, $(y/d_3) = (-1/y)(y/d_1)$ and $(z/d_1) = (2/z)$; a routine computation modulo 16 shows that $(2/x)(2/z) = (d_3d_1/8m)_4$. This gives

$$\left(\frac{8md_1}{d_3}\right)_4\left(\frac{8md_3}{d_1}\right)_4\left(\frac{d_3d_1}{8m}\right)_4 = \left(\frac{-1}{y}\right) = (-1)^{(|y|-1)/2}.$$

As in the case $d \equiv 1 \bmod 4$ above, this implies that a 2-primary μ is totally positive if and only if $(8md_1/d_3)_4(8md_3/d_1)_4(d_1d_3/8m)_4 = (2/d_1)$; since $(2/d_3)(d_3/2) = +1$, our claim follows.

4. Unramified Dihedral Extensions

Of course, the very same methods allow us to treat unramified dihedral extensions of quadratic number fields. In fact, the proofs in this case are much simpler than those for quaternion extensions and are left as an exercise (for complete proofs in a more general situation, see [22]). In fact, it is easy to see that unramified extensions M/k of quadratic number fields k which are normal over $\mathbb{Q}$ have Galois group $D_4 \times C_2$. Using the decomposition and inertia groups one finds that the existence of such an extension implies a factorization $d = \operatorname{disc} k = d_1d_2 \cdot d_3$ into three (relatively prime) discriminants such that $(d_1/p_2) = (d_2/p_1) = +1$ for all $p_j \mid d_j$ $(j = 1, 2)$. On the other hand, such a factorization implies the existence of an unramified C_4-extension L of $\mathbb{Q}(\sqrt{d_1d_2})$, and it is easy to see that the compositum $M = kL$ is an unramified D_4-extension of k such that $\operatorname{Gal}(M/\mathbb{Q}) \simeq D_4 \times C_2$. We find

THEOREM 2. *Let k be a quadratic number field with discriminant d and M/k an unramified D_4-extension such that $M/\mathbb{Q}$ is normal.*
Then $\operatorname{Gal}(M/\mathbb{Q}) \simeq D_4 \times C_2$, *and there exists a ”$D_4$-factorization” $d = d_1d_2 \cdot d_3$ into discriminants d_i such that*

(i) $(d_i, d_j) = (1)$ *for $i \neq j$, and at most one of d_1 or d_2 is negative;*

(ii) $(d_1/p_2) = (d_2/p_1) = +1$ *for all primes* $p_1 \mid d_1$ *and* $p_2 \mid d_2$.

Moreover, $M/k(\sqrt{d_j})$ *is cyclic for* $j = 3$ *and of type* $(2,2)$ *for* $j = 1,2$.

If, on the other hand, $k/\mathbb{Q}$ *is a quadratic extension with discriminant* $d = \operatorname{disc} k$, *and if* $d = d_1 d_2 \cdot d_3$ *is a* D_4*-factorization, then there is an* $\alpha \in k(\sqrt{d_1})$ *such that* $M = k(\sqrt{d_1}, \sqrt{d_2}, \sqrt{\alpha})$ *is a* D_4*-extension with the following properties:*

(1) M/k *is unramified outside* ∞;

(2) $M/k(\sqrt{d_3})$ *is cyclic;*

(3) $M/\mathbb{Q}$ *is normal with Galois group* $D_4 \times C_2$.

Acknowledgement

The author would like to thank R. Okazaki and K. Yamamura for numerous suggestions, as well as the Laboratoire d'Algorithmique Arithmétique eXpérimental at the University of Bordeaux for their hospitality, and the DFG, whose support has made his visit there possible.

References

[1] C. Bachoc, S.-H. Kwon, *Sur les extensions de groupe de Galois* $\widetilde{A}_4$, Acta Arith. **62** (1992), 1-10.

[2] Ph. Cassou-Noguès, A. Jehanne, *Parité du nombre de classes des* S_4*-extensions de* $\mathbb{Q}$ *et courbes elliptiques*, J. Number Theory **57** (1996), 366–384

[3] H. Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields*, Springer Verlag 1978.

[4] H. Cohn, *Quaternion compositum genus*, J. Number Theory **11** (1979), 399-411

[5] P. Damey, J. Martinet, *Plongement d'une extension quadratique dans une extension quaternionienne*, J. Reine Angew. Math. **262/263** (1973), 323–338.

[6] R. Dedekind, *Konstruktion von Quaternionenkörpern*, Ges. Werke II, Nachlaß, Braunschweig 1931, 376–384.

[7] A. Fröhlich, *Galois Module Structure of Algebraic Integers*, Ergebnisse der Mathematik, Springer Verlag Heidelberg, 1983

[8] G. Fujisaki, *An elementary construction of Galois quaternionic extensions*, Proc. Japan Acad. **66** (1990), 80–83.

[9] P. Furtwängler, *Über das Verhalten der Ideale des Grundkörpers im Klassenkörper*, Monatsh. Math. Phys. **27** (1916), 1-15.

[10] H. G. Grundman, T. L. Smith, J. R. Swallow, *Groups of order* 16 *as Galois groups*, Expo. Math. **13** (1995), 289–319.

[11] M. Hall, J. K. Senior, *The groups of order* 2^n $(n \leq 6)$, Macmillan, New York 1964.

[12] W. Hettkamp, *Quadratischer Restcharakter von Grundeinheiten und* 2*-Klassengruppen quadratischer Zahlkörper*, Diss. Univ. Münster, 1981

[13] M. Horie, *On central extensions of elementary abelian fields*, J. Number Theory **36** (1990), 95–107.

[14] A. Jehanne, *Sur les extensions de* $\mathbb{Q}$ *à groupe de Galois* S_4 *et* $\tilde{S}_4$, Acta Arith. **70** (1995), 259–276.

[15] C. U. Jensen, N. Yui, *Quaternion extensions*, Algebraic Geometry and Commutative Algebra (1987), 155–182.

[16] I. Kiming, *Explicit classifications of some* 2*-extensions of a field of characteristic different from* 2, Can. J. Math. **42** (1990), 825–855.

[17] H. Kisilevsky, *Number fields with class number congruent to* $4 \bmod 8$ *and Hilbert's Theorem 94*, J. Number Theory **8** (1976), 271–279.

[18] H. Koch, *Über den 2-Klassenkörperturm eines quadratischen Zahlkörpers*, J. Reine Angew. Math. **214/215** (1963), 201–206

[19] S. Lang, *Algebra*, third edition, Addison-Wesley 1993.

[20] A. Ledet, *On* 2*-groups as Galois groups*, Canad. J. Math. **47** (1995), no. 6, 1253–1273.

[21] F. Lemmermeyer, *Die Konstruktion von Klassenkörpern*, Diss. Univ. Heidelberg 1995.

[22] F. Lemmermeyer, *Class Field Towers*, monograph, in preparation.

[23] S. Louboutin, *Calcul des nombres de classes relatifs: application aux corps quaternioniques à multiplication complexe*, C. R. Acad. Sci. Paris **317** (1993), 643–646.

[24] S. Louboutin, *Determination of all quaternion octic CM-fields with class number* 2, J. London Math. Soc. (1996)

[25] S. Louboutin, R. Okazaki, *Determination of all non-normal quartic CM-fields and of all non-abelian normal octic CM-fields with class number one*, Acta Arith. **67** (1994), 47–62.

[26] S. Louboutin, R. Okazaki, *The class number one problem for some non-abelian normal CM-fields of* 2*-power degrees*, preprint 1996

[27] J. Martinet, *Sur les extensions à groupe de Galois quaternionien*, C. R. Acad. Sci. Paris **274** (1972), 933–935.

[28] J. Martinet, H_8, Algebraic Number Fields: L-functions and Galois Properties (A. Fröhlich, ed.), 525–538, Acadenic Press New York 1977

[29] J. Minác, T. J. Smith, *A characterization of C-fields via Galois groups*, J. Algebra **137** (1991), 1–11

[30] L. Rédei *Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*, J. Reine Angew. Math. **171** (1934), 55–60

[31] L. Rédei, H. Reichardt, *Die Anzahl der durch* 4 *teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. Reine Angew. Math. **170** (1934), 69–74

[32] H. Reichardt, *Über Normalkörper mit Quaternionengruppe*, Math. Z. **41** (1936), 218–222.

[33] E. Rosenblüth, *Die arithmetische Theorie und die Konstruktion der Quaternionenkörper auf klassenkörpertheoretischer Grundlage*, Monatsh. Math. Phys. **41** (1934), 85–125.

[34] T. J. Smith, *Extra-special groups of order* 32 *as Galois groups*, Can. J. Math. **46** (1994), 886–896

[35] A. D. Thomas, G. V. Wood, *Group Tables*, Shiva Publishing Ltd, Kent, UK 1980

[36] T. P. Vaughan, *Constructing quaternionic fields*, Glasgow Math. J. **34** (1992), 43–54.

[37] E. Witt, *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f*, J. Reine Angew. Math. **174** (1936), 237–245.

Franz LEMMERMEYER
Erwin-Rohde-Str. 19
69120 Heidelberg
e-mail: hb3@ix.urz.uni-heidelberg.de