ACTA ARITHMETICA
165.2 (2014)

Quaternion extensions with restricted ramification

by

PETER SCHMID (Tübingen)

1. Introduction. Dedekind [5] showed that the field

$$\mathfrak{D} = \mathbb{Q}\big(\sqrt{(2+\sqrt{2})(3+\sqrt{6})}\,\big)$$

is Galois over the rationals with group Q_8, the quaternion group of order 8. Only the primes 2 and 3 ramify in this Q_8-field, and $\mathfrak{D}$ is totally real. Thus $\mathfrak{D}$ belongs to $\mathcal{K}_S^+(Q_8)$ for $S = \{2,3\}$. Here for any set S of finite rational primes and any finite group G we denote by $\mathcal{K}_S(G)$ the set of Galois number fields (within $\mathbb{C}$) with group G over $\mathbb{Q}$ which are unramified outside $S \cup \{\infty\}$, and where $\mathcal{K}_S^+(G)$ is its subset consisting of the totally real fields (being unramified outside S). As in [19], we shall treat only cases where G is a 2-group, thus eventually appearing as a quotient group of the absolute Galois group $G_S(2)$ of the maximal 2-extension $\mathbb{Q}_S(2)$ of $\mathbb{Q}$ unramified outside $S \cup \{\infty\}$. For general properties of such pro-2-groups the reader is referred to [9], [15], [18].

The Dedekind field $\mathfrak{D}$ is of extraordinary nature, because if $\mathcal{K}_S(Q_8) \neq \emptyset$ for some S, then S must contain at least two distinct primes. Moreover, complex conjugation on a Q_8-field must be either trivial or the unique central involution in the group (so that its fixed field must be totally real). In fact, the following holds:

THEOREM 0. *Suppose S is a finite set of rational primes which is minimal subject to having $\mathcal{K}_S(Q_8) \neq \emptyset$. Then one of the following holds:*

(i) $S = \{2,p\}$ *for some prime* $p \equiv 1$ *or* $3 \pmod 8$.
(ii) $S = \{p,q\}$ *for distinct primes* $p \equiv q \equiv 1 \pmod 4$ *satisfying* $\left(\frac{q}{p}\right) = 1$ $(= \left(\frac{p}{q}\right))$.

Conversely, the cardinality of $\mathcal{K}_S(Q_8)$ is 2 when S is of type (i), *and is* 1 *otherwise.*

2010 *Mathematics Subject Classification*: 11F80, 11R32, 11S15.
Key words and phrases: Galois theory, quaternion extensions, restricted ramification.

It follows from the work of Witt [23] that S must be of type (i) or (ii), by minimality, and that then $\mathbb{Q}(\sqrt{2},\sqrt{p})$ respectively $\mathbb{Q}(\sqrt{p},\sqrt{q})$ can be embedded into a Q_8-field (see Lemmas 2.1 and 2.2 below). The converse statement is due to Fröhlich [7]; it may be obtained from the known structure of the maximal pro-2-quotient group with class 2 of the corresponding absolute Galois group $G_S(2)$ (see [9, Chap. 4]). In this note we shall present an elementary and constructive approach which enables us to compute the fields explicitly (at least for small primes).

As observed by Jensen–Yui [13], one can also write

$$\mathfrak{D} = \mathbb{Q}\big(\sqrt{(2+\sqrt{2})(3+\sqrt{3})}\big).$$

Indeed, $\mathfrak{D}$ is the unique field belonging to $\mathcal{K}_S^+(Q_8)$ for $S=\{2,3\}$.

Theorem 1. *Let $S=\{2,p\}$ for some prime $p\equiv 1$ or $3 \pmod 8$. Then $\mathcal{K}_S^+(Q_8)$ contains a single field $L_p=\mathbb{Q}(\sqrt{\beta})$. Here β may be written in the form $\beta=(2+\sqrt{2})(ap+b\sqrt{p})$ with positive odd integers a and b satisfying $a^2p-b^2=2^r$, where $r=1$ if $p\equiv 3 \pmod 8$ and r is odd with $3\le r\le h(p)+2$ otherwise, $h(p)$ denoting the class number of $\mathbb{Q}(\sqrt{p})$. Also, $\mathcal{K}_S(Q_8)=\{L_p,L_p^-\}$ where $L_p^-=\mathbb{Q}(\sqrt{-\beta})$.*

The integers a, b may be altered by multiplying $ap+b\sqrt{p}$ with a totally positive unit in $\mathbb{Q}(\sqrt{p})$. For $p=11,17,19,41,43$ we may let $(a,b)=(1,3),(1,3),(3,13),(3,19),(9,59)$, respectively. Note that always $a\equiv 1$ or $3 \pmod 8$, because $-2^r\equiv b^2 \pmod a$ with positive odd integers r,a, and therefore the Jacobi symbol $\left(\frac{-2}{a}\right)$ equals $+1$. There is an associated dihedral field $\mathbb{Q}\big(\sqrt{ap+b\sqrt{p}},\sqrt{2}\big)$, which is cyclic over $\mathbb{Q}(\sqrt{2})$. For $p\equiv 1 \pmod 8$ we can avoid reference to the (odd) class number $h(p)$ by using another dihedral field (see below).

Theorem 2. *Let $S=\{p,q\}$ for distinct primes $p\equiv q\equiv 1 \pmod 4$ satisfying $\left(\frac{q}{p}\right)=1$. There exists a unique normal number field F of absolute degree 8 containing $K=\mathbb{Q}(\sqrt{p},\sqrt{q})$ such that no finite prime of K ramifies in F. There is also a unique subfield E of the pqth cyclotomic field $\mathbb{Q}(\zeta_{pq})$ such that $[E:K]=2$ but $E\not\subseteq K(\zeta_p)$ and $E\not\subseteq K(\zeta_q)$. Then $\mathcal{K}_S(Q_8)=\{L_{pq}\}$ where L_{pq} is the unique proper subfield of EF containing K properly which is distinct from E and from F. The field L_{pq} is real if and only if F and E are both real or both nonreal.*

There are some comments in order. The cyclotomic field E is real if and only if p and q are in the same residue class modulo 8 (so $p\equiv q\equiv 1$ or $5 \pmod 8$). The field F is a subfield of the narrow Hilbert 2-class field of $\mathbb{Q}(\sqrt{pq})$, so it has a dihedral Galois group over $\mathbb{Q}$ and a cyclic one over $\mathbb{Q}(\sqrt{pq})$. It is real if and only if the (ordinary) class number $h(pq)$ of $\mathbb{Q}(\sqrt{pq})$ is divisible by 4 (and so F is in the Hilbert class field of $\mathbb{Q}(\sqrt{pq})$), and this happens precisely when the biquadratic Legendre symbols $\left(\frac{p}{q}\right)_4$ and $\left(\frac{q}{p}\right)_4$ are equal. These symbols can be easily (and rationally) computed in the present situation (Lemma 2.4). We shall describe F explicitly as a quadratic extension of $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ (Proposition 5.1), thus giving the necessary information on $h(pq)$ in a different way. Unramified Q_8-extensions of quadratic number fields which are normal over $\mathbb{Q}$ are studied by Lemmermeyer [17].

For $p \equiv 1 \pmod 8$, the narrow class number $h_+(8p)$ of $\mathbb{Q}(\sqrt{2p})$ (having discriminant $8p$) likewise is divisible by 4, so that we can construct the Q_8-field L_p in a corresponding way. If $h_+(8p)$, or $h_+(pq)$ when S is of type (ii), is divisible by 8, one observes in this manner that $\mathcal{K}_S(Q_{16})$ contains fields which are cyclic over $\mathbb{Q}(\sqrt{2p})$, respectively $\mathbb{Q}(\sqrt{pq})$. Here Q_{16} denotes the (generalized) quaternion group of order 16.

Theorem 3. *Let $G = Q_{2^n}$ be the* (*generalized*) *quaternion group of order 2^n $(n > 3)$, and let $S = \{2, p\}$ for some prime $p \equiv 1 \pmod{2^{n-1}}$. Then there are unique real and complex fields in $\mathcal{K}_S(G)$ which are cyclic over $\mathbb{Q}(\sqrt{2})$.*

This may be seen as a supplement to the work of Damey–Martinet [4], and to that of Fröhlich [8]. By Dirichlet's prime number theorem (or directly) there exist infinitely many primes $p \equiv 1 \pmod{2^{n-1}}$. One might ask whether for any integer $n \geq 3$ there exist distinct primes $p \equiv q \equiv 1 \pmod 4$ (with $\left(\frac{q}{p}\right) = 1$) such that $h(8p)$, respectively $h(pq)$, is divisible by 2^n (see [11], [22] for the cases $n = 2, 3, 4$). The Hilbert class fields of real quadratic number fields with discriminant less than 2000 are given by Cohen [3, Section 12.1.1].

If $S = \{2, p\}$ for some prime $p \equiv 3 \pmod 8$, then $\mathcal{K}_S(Q_{2^n}) = \emptyset$ for all $n > 3$. In this case we are indeed able to determine the 2-groups G for which $\mathcal{K}_S^+(G) \neq \emptyset$, and the complete lattice structure of the fields appearing (Proposition 7.2). This (infinite) lattice turns out to be independent of the particular prime $p \equiv 3 \pmod 8$, up to isomorphism.

There is a close relationship between the Galois theory of the quaternion group Q_{2^n} and that of the dihedral group D_{2^n} (of order 2^n). This will be made precise in Section 3, where the ground field may be any field of characteristic $\neq 2$. Otherwise we restrict ourselves to the ground field $\mathbb{Q}$, treating just the ramification types (i), (ii) given in Theorem 0.

2. Preliminaries. We shall refer to the celebrated work of Witt [23], where the general question is treated of when a biquadratic extension of a field of characteristic $\neq 2$ can be embedded into a Q_8-field (see also [7], [13]). Recall that the quaternion group Q_{2^n}, the dihedral group D_{2^n} and the semidihedral group SD_{2^n} are the (nonabelian) 2-groups X of maximal class (nilpotency class $n-1$) and order 2^n ($n \geq 3$, identifying $SD_8 = D_8$ when $n = 3$). Here the commutator subgroup $X' = X^2$ is the Frattini subgroup, the centre $Z(X) \cong Z_2$ has order 2 and is contained in X', and $G = X/Z(X) \cong D_{2^{n-1}}$ (where we let $D_4 = V$ be the elementary group of order 4). In particular, the Schur multiplier $M(G) = H_2(G, \mathbb{Z})$ of $G = D_{2^{n-1}}$ has order 2, and Q_{2^n}, D_{2^n}, SD_{2^n} are the unique Schur covers of G, up to group isomorphism.

LEMMA 2.1. *Suppose that $L/\mathbb{Q}$ is a Galois extension with group $X \cong Q_{2^n}$ $(n \geq 3)$. Let $K' \subseteq K$ be the fixed fields in L of $X' \supseteq Z(X)$. Then K is (totally) real, and at least two rational primes are ramified in K'. Let $L = K(\sqrt{\beta})$ for some $\beta \in K$. Then $L = \mathbb{Q}(\sqrt{\beta})$, and $L' = \mathbb{Q}(\sqrt{-\beta})$ is a normal Q_{2^n}-field distinct from L. Exactly one of L, L' is real.*

Proof. Obviously $K' = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ is biquadratic over $\mathbb{Q}$, where we may assume that a and b are distinct square-free integers. Then every prime dividing a or b is ramified in K'. Complex multiplication on L is either trivial (for L real) or the unique (central) involution in X having fixed field K ($\mathrm{Gal}(K/\mathbb{Q}) \cong D_{2^{n-1}}$). So K is real in any case. Clearly β exists (as $[L : K| = 2$), and L is real if and only if β is totally positive. Let $H = \mathrm{Gal}(L/\mathbb{Q}(\sqrt{\beta}))$. Then $H \cap Z(X) = 1$ and so $H = 1$, because every nontrivial subgroup of X contains $Z(X)$. Finally, L' is the unique proper subfield of $L(i)$ which contains $K = L \cap K(i)$ properly and is distinct from L and from $K(i)$ ($i = \zeta_4$, $\zeta_r = e^{2\pi i/r}$). Now $\mathrm{Gal}(L(i)/\mathbb{Q}) \cong X \times Z_2$, and so $\mathrm{Gal}(L'/\mathbb{Q}) \cong X$. ∎

Whenever we have two fields $k_1 \neq k_2$ of characteristic $\neq 2$ (in a common overfield) which are of degree 2 over $k_1 \cap k_2$ (and so $\mathrm{Gal}(k_1k_2/k_1 \cap k_2) \cong V$), the *companion field* of k_1 and k_2 is the unique further subfield of k_1k_2 quadratic over $k_1 \cap k_2$.

LEMMA 2.2. *Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ for some distinct (finite) rational primes p, q. Then K can be embedded into a Q_8-field if and only if one of the following holds:*

(i) $q = 2$ *(say) and* $p \equiv 1$ *or* $3 \pmod 8$.
(ii) $p \equiv q \equiv 1 \pmod 4$ *and* $\left(\frac{q}{p}\right) = 1$.

Proof. For nonzero rational numbers a, b let (a, b) denote the class of the quaternion algebra $\left(\frac{a,b}{\mathbb{Q}}\right)$ in the Brauer group $\mathrm{Br}(\mathbb{Q})$. Then $(-a, -b) = (-1, -1)$ if and only if the quadratic forms $aX^2 + bY^2 + abZ^2$ and $X^2 + Y^2 + Z^2$ are equivalent over $\mathbb{Q}$. This forces that $a > 0$, $b > 0$, and by Witt's theorem the latter condition is fulfilled if and only if $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ can be embedded into a Q_8-field. By the Hasse–Minkowski principle the quadratic forms are equivalent over $\mathbb{Q}$ if and only if they are equivalent over all completions $\mathbb{Q}_r$, r a prime or $r = \infty$ ($\mathbb{Q}_\infty = \mathbb{R}$; see e.g. Serre [20, Theorem 9, p. 44]). This in turn means that we have to compute the local Hilbert symbols $(-a, -b)_r$.

Now let $a = p$ and $b = q$ be distinct primes, and apply [20, Theorem 1, p. 20]. Note that $(-1,-1)_2 = -1$ and $(-1,-1)_r = 1$ for all odd finite primes r, as well as $(-p,-q)_r = 1$ whenever $r \notin \{p,q,\infty\}$. Check the remaining few cases. $\square$

LEMMA 2.3. *Let $K = \mathbb{Q}(\sqrt{a},\sqrt{b})$ be a biquadratic field which can be embedded into a Q_8-field $L = K(\beta)$ over the rationals. Then every Q_8-field containg K is of the form $K(\sqrt{c\beta})$ for some rational number $c \neq 0$, where $L = K(\sqrt{c\beta})$ if and only if $c \in K^{*2}$.*

This is immediate from Witt [23]; see also [13, Proposition I.1.8].

LEMMA 2.4. *Suppose p and q are distinct odd primes satisfying $p \equiv q \equiv 1 \pmod 4$ and $\left(\frac{q}{p}\right) = 1$. Write uniquely $p = a^2 + b^2$ and $q = c^2 + d^2$ with positive integers a,b,c,d, where b and d are even. Then $\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = (-1)^{(p-1)/4}\left(\frac{ad-bc}{p}\right)$, and this is $+1$ if and only if the class number $h(pq)$ of $\mathbb{Q}(\sqrt{pq})$ is divisible by 4.*

In the above situation $\left(\frac{p}{q}\right)_4 = \pm 1$, the positive sign holding when p is a 4th power modulo q. The first statement is due to Burde [2]; the statement on the class number follows from Theorem 5.6 of Fröhlich [9]. For the next lemma see also [9] and [24].

LEMMA 2.5. *For any prime p the class number h of $\mathbb{Q}(\sqrt{p})$ is odd. The narrow class number h_+ of $\mathbb{Q}(\sqrt{p})$ is equal to h if and only if its fundamental unit has norm -1, and $h_+ = 2h$ otherwise. Also, $h_+ = h$ is odd if $p \equiv 1 \pmod 4$.*

LEMMA 2.6. *Let $q < p$ be primes such that $p \equiv 1 \pmod 8$ if $q = 2$, and $p \equiv q \equiv 1 \pmod 4$ and $\left(\frac{q}{p}\right) = 1$ otherwise. Then the narrow class number of $\mathbb{Q}(\sqrt{pq})$ is divisible by 4, and its narrow Hilbert 2-class field has a dihedral Galois group over the rationals and is cyclic over $\mathbb{Q}(\sqrt{pq})$.*

One knows that $\mathbb{Q}(\sqrt{p},\sqrt{q})$ is the (narrow) genus field of $\mathbb{Q}(\sqrt{pq})$ (Hasse [10]). Hence the first statement follows from [9, Theorem 5.2]. The rest is immediate from Hasse's work.

LEMMA 2.7. *Let k be any field of characteristic $\neq 2$, and let $k_0 = k(\sqrt{d})$ be a quadratic extension. There exists $E \supset k_0$ which is cyclic over k of degree 4 and solves the embedding problem $(k_0/k, Z_4)$ if and only if d is a sum of two squares in k. If $k = \mathbb{Q}$ (or any Hilbertian field), the embedding problem $(k_0/k, Q_8)$ is solvable if and only if d is a sum of three squares in k.*

For the first statement we refer to Serre [21, Theorem 1.2.4], and for the second one to Jensen–Yui [13, Theorem II.2.1]. Cyclic extensions of the rationals are cyclotomic by the Kronecker–Weber theorem. We shall repeatedly use the solutions $B_2 = \mathbb{Q}\big(\sqrt{2+\sqrt{2}}\big)$ and $B_2^- = \mathbb{Q}\big(\sqrt{-2-\sqrt{2}}\big)$ of the embedding problem $(\mathbb{Q}(\sqrt{2})/\mathbb{Q}, Z_4)$. Here B_2 appears in the (cyclotomic) $\mathbb{Z}_2$-extension of $\mathbb{Q} = B_0$, with $B_1 = \mathbb{Q}(\sqrt{2})$.

The following is standard (see e.g. [13]).

Lemma 2.8. *Let k be any field of characteristic $\neq 2$, and let a, b be elements of k.*

(a) *The splitting field of the polynomial $X^4 + aX^2 + b$ is cyclic of degree 4 over k if $b \notin k^2$ but $b(a^2 - 4b) \in k^{*2}$.*

(b) *Suppose $K = k(\sqrt{a}, \sqrt{b})$ is a biquadratic extension field of k such that $(a, b) = 1$ in $\mathrm{Br}(k)$. Then there exist x, y in k such that $x^2 - ay^2 = b$, and $F = K(\sqrt{x + y\sqrt{a}})$ is a Galois extension of k with dihedral group (of order 8) which is cyclic over $k(\sqrt{ab})$.*

Assume in part (b) of the above lemma that the embedding problem $(k(\sqrt{ab})/k, Z_4)$ is solvable. Then $ab = u^2 + v^2$ is a sum of two squares in k (Lemma 2.7). Hence $ax^2 - a^2y^2 = ab = u^2 + v^2$, and therefore a and b are sums of three squares in k. We shall see in the next section that $K = k(\sqrt{a}, \sqrt{b})$ can be embedded into a Q_8-field over k.

3. Dihedral and quaternion fields. In this section k may be an arbitrary field of characteristic $\neq 2$. Every algebraic overfield of k is understood to be in a given algebraic closure of k.

Lemma 3.1. *Suppose L_1, L_2 are Galois extensions of k with groups X_i. Let $L = L_1L_2$ and $K = L_1 \cap L_2$. Then $\mathrm{Gal}(L/k) = X_1 \times_G X_2$ is the fibre product of X_1 and X_2 with respect to the natural epimorphisms (via restrictions) onto $G = \mathrm{Gal}(K/k)$.*

This is obvious (and certainly well known), because $\sigma \mapsto (\sigma_{|L_1}, \sigma_{|L_2})$ is a monomorphism of $\mathrm{Gal}(L/k)$ into the direct product $X_1 \times X_2$ whose image consists of those elements of X_1, X_2 which agree on K.

Hypothesis. Let K/k be a Galois extension with group $G \cong D_{2^{n-1}}$ $(n \geq 3)$.

Proposition 3.2. *Assume K is embedded into two fields $L_1 \neq L_2$ which are both Galois over k with groups $X_i \cong Q_{2^n}$. Then there is a subfield of $L = L_1L_2$ which is quadratic over k and not contained in K. An analogous statement holds when $X_i \cong D_{2^n}$ and $n \geq 4$, or $n = 3$ and the L_i are cyclic over the same subfield k_0 of K of degree 2 over k.*

Proof. Clearly $L_1 \cap L_2 = K$. Let $Y = \mathrm{Gal}(L/k)$ and $M = \mathrm{Gal}(L/K)$. Then $M = Z(Y)$ is elementary of order 4. Indeed, if $M_i = \mathrm{Gal}(L/L_i)$, then we may identify $X_i = Y/M_i$ and get $M/M_i = Z(X_i)$ $(i = 1, 2)$. Let L_0 be the companion field of L_1 and L_2, and let $M_0 = \mathrm{Gal}(L/L_0)$ and $X_0 = Y/M_0$. Then $M = M_1 \times M_2 = M_1 \times M_0$, and we may identify $G = Y/M$. The subfields of K quadratic over k are contained in the fixed field $K' \subseteq K$ of $G' = G^2$ (where $\mathrm{Gal}(K'/k) \cong V$).

Let us first consider the case $n = 3$ ($K' = K$). If X_1 and X_2 are quaternion, then L_1 and L_2 are cyclic over any subfield of degree 2 over k, implying that L_0 is elementary (of degree 4) over all these subfields. If X_1 and X_2 are dihedral, then L_1 and L_2 are cyclic over the same such subfield k_0 by assumption, and they are elementary over the other ones. Thus in both cases $\mathrm{Gal}(L_0/k) \cong Y/M_0$ is an elementary abelian group (of order 8).

Hence we may assume that $n > 3$. Let N be the inverse image in Y of the unique cyclic maximal subgroup of $G = Y/M$. Then N/M_1 and N/M_2 are the (unique) cyclic maximal subgroups of X_1 and X_2, respectively, and we let k_0 be the fixed field of N on L. Since $|M(G)| = 2$, we cannot have $M \subseteq Y'$. Using the fact that X_1, X_2 are Schur covers of G, this forces that $Y' \cap M = M_0$. Since $Y'M/M = G'$, we see that $A = Y/Y'$ is either elementary abelian of order 8 or abelian of type $(4, 2)$. We have to rule out the latter possibility.

Assume $A = Y/Y'$ is of type $(4, 2)$. Then $Y^2 = MY'$, and $V = Y/Y^2$ is elementary abelian of order 4. Since

$$M_1 \cap Y' = M_1 \cap (M \cap Y') = M_1 \cap M_0 = 1,$$

the assignment $y \mapsto (yM_1, yY')$ is an isomorphism of Y onto the fibre product $X_1 \times_V A$ with respect to the natural epimorphisms of X_1 and A onto V (Lemma 3.1). Two of the three nontrivial elements of V come from elements of order 4 in A, and the remaining one from an element of X_1 outside N/M_1.

Suppose $X_1 \cong D_{2^n}$. Since every element of X_1 outside N/M_1 is an involution, there is $y \in Y$ such that yM_1 is a noncentral involution in X_1 and yY' is of order 4. Then $y^2 \in M$ has trivial image in M/M_1 and a nontrivial one in A, that is, in M/M_0. Thus $y^2 \notin M_2$ and yM_2 is an element of order 4 in $X_2 = Y/M_2$ outside N/M_2. Hence X_2 is not dihedral, contrary to $X_1 \cong X_2$.

Suppose next that $X_1 \cong Q_{2^n}$. Since every element of X_1 outside N/M_1 has order 4, there is $y \in Y$ such that yM_1 is a noncentral element of order 4 in X_1 and yY' is of order 4. Then $y^2 \in M$ gives rise to the nontrivial elements in M/M_1 and M/M_0. It follows that y^2 is the generator of M_2 and that yM_2 is a noncentral involution in $X_2 = Y/M_2$. Hence X_2 is not quaternion, contrary to $X_1 \cong X_2$. ∎

Corollary. *Let $k = \mathbb{Q}$, and suppose K is a field in $\mathcal{K}_S^+(G)$ where S is as in Theorem* 0. *Then there is at most one field in $\mathcal{K}_S^+(Q_{2^n})$ containing K when S is of type* (i), *and at most one field in $\mathcal{K}_S(Q_{2^n})$ containing K when S is of type* (ii). *A similar statement holds for D_{2^n}, with the proviso that for $n = 3$, we only consider overfields of K which are cyclic over the same subfield of K of degree* 2 *over $\mathbb{Q}$.*

Otherwise there are fields $L_1 \neq L_2$ in the corresponding sets, and then $L = L_1L_2$ is unramified outside $S \cup \{\infty\}$ respectively S containing a quadratic field outside K. But the subfields of K quadratic over $\mathbb{Q}$ amount to all real quadratic fields in which only the primes in S are ramified.

Proposition 3.3. *Assume K is embedded into a field L_1 which is Galois over k with group $X_1 \cong D_{2^n}$. Let k_0 be the fixed field of the cyclic maximal subgroup of X_1. There is a field L_2 which is Galois over k with group $X_2 \cong Q_{2^n}$ and with $L_1 \cap L_2 = K$ if and only if there is a field $E \supset k_0$ such that E/k is cyclic of degree 4. In this case $[KE : K] = 2$ and $KE \neq L_1$, and L_2 is the companion field of L_1 and KE.*

Proof. Suppose first that L_2 exists as claimed. Let then $L = L_1L_2$, $Y = \mathrm{Gal}(L/k)$, and keep all further conventions introduced in the proof of Proposition 3.2. As before, $A = Y/Y'$ is of order 8, with $Y' \cap Z = Z_0$, and Y may be identified with the fibre product $X_1 \times_V A$ with respect to the natural epimorphisms of $X_1 = Y/M_1$ and A onto $V = Y/Y'M$. Here A cannot be elementary, because otherwise all noncentral elements of $X_2 = Y/M_2$ would be involutions. Thus A is of type $(4, 2)$. Assume there is $y \in Y$ such that $N/M_1 = \langle yM_1\rangle$ is the cyclic maximal subgroup of X_1 and yY' is of order 4 in A. Then there is $u \in Y$ such that uM_1 is a noncentral involution in X_1 and uY' is an involution in A. It follows that $u^2 \in M_1 \cap M_0 = 1$. Clearly $u \notin M_2$, and so uM_2 is a noncentral involution in $X_2 = Y/M_2$, contradicting the fact that $X_2 \cong Q_{2^n}$.

Hence there is $y \in Y$ such that yM_1 generates N/M_1 and yY' has order 2. Let $B = \langle Y', y\rangle$. Then $B \subset N$ and Y/B is cyclic of order 4. Since k_0 is the fixed field of N on L, the fixed field E of B is as required.

Conversely, if E exists (cyclic of degree 4 over k and containing k_0), then $E \cap L_1 = k_0$, and we let $L_0 = KE$ and $L = L_1L_0$, and L_2 is the companion field of L_1 and L_0. We are in quite the same situation as before. Let again $Y = \mathrm{Gal}(L/k)$ and $A = Y/Y'$. Then A is of type $(4, 2)$, and there is $y \in Y$ such that yM_1 generates N/M_1 and yY' has order 2. It follows that whenever $u \in Y$ is such that uM_1 is a noncentral involution in $X_1 = Y/M_1$, then uY' is of order 4. Then $u^2 \in M_1$ has a nontrivial image in M/M_0, so $u^2 \notin M_2$ and uM_2 is an element of $X_2 = Y/M_2$ of order 4 outside N/M_2. Consequently, $X_2 \cong Q_{2^n}$, as desired. ∎

Corollary. *Let $k = \mathbb{Q}$ in the preceding proposition, and let $k_0 = \mathbb{Q}(\sqrt{d})$ be the fixed field of the cyclic maximal subgroup of $X_1 \cong D_{2^n}$. Asssume that d is a sum of two rational squares. Then K is a real field for which the embedding problem $(K/\mathbb{Q}, Q_{2^n})$ is solvable.*

By Lemma 2.7 there is a field $E \supset k_0$ which is cyclic of degree 4 over the rationals. Then $L_1 \cap E = k_0$, and the companion field of L_1 and KE

is a solution of the embedding problem $(K/\mathbb{Q}, Q_{2^n})$ (Proposition 3.3). Now Lemma 2.1 implies that K is a real field.

4. Proof of Theorem 1. Let $S = \{2, p\}$ for some prime $p \equiv 1$ or $3 \pmod 8$. We know from Lemma 2.2 that this S is a candidate for having $\mathcal{K}_S^+(Q_8) \neq \emptyset$. In both cases $(-2, p) = 1$ in $\mathrm{Br}(\mathbb{Q})$ and so $x^2 - py^2 = -2$ for some rational numbers x, y. We need a slightly stronger statement.

Consider first the case $p \equiv 1 \pmod 8$. Then by Lemma 2.5 the class number $h = h(p)$ of $P = \mathbb{Q}(\sqrt{p})$ is odd, and the fundamental unit $u = (c + d\sqrt{p})/2$ of P has norm $(c^2 - pd^2)/4 = -1$. Here c, d are integers with the same parity. But they cannot both be odd, because then $-4 = c^2 - pd^2 \equiv 1 - p \equiv 0 \pmod 8$. Hence $c = 2c_0$ and $d = 2d_0$ are even, and $u = c_0 + d_0\sqrt{p}$. The prime 2 splits in P, so that there is a prime $\mathfrak{p}$ of P with absolute norm 2. Clearly $\mathfrak{p}^h = \left(\frac{b+a\sqrt{p}}{2}\right)$ is a principal ideal, b and a being rational integers with the same parity. It follows that the norm satisfies $N_{P/\mathbb{Q}}(b + a\sqrt{p}) = \pm 2^{h+2}$. If the sign is positive, then replace $b + a\sqrt{p}$ by $u(b + a\sqrt{p})$. In this case we have $b^2 - a^2 p = -2^r$ where $r = h + 2$ is odd. Dividing by a power of 4 if necessary, we may assume that b and a are odd, and then $a^2 p - b^2 \equiv p - 1 \equiv 0 \pmod 8$. Thus $a^2 p - b^2 = 2^r$ with positive odd integers a, b, r, and with $3 \leq r \leq h + 2$.

Let next $p \equiv 3 \pmod 8$. Then $(2) = \mathfrak{p}^2$ is ramified in $P = \mathbb{Q}(\sqrt{p})$ (discriminant $4p$). Since the class number $h(4p)$ of P is still odd, this forces that $\mathfrak{p} = (b + a\sqrt{p})$ is a principal ideal (a, b integers). As before, $\mathfrak{p}$ has norm 2 and so $N_{P/\mathbb{Q}}(b + a\sqrt{p}) = b^2 - a^2 p = \pm 2$. This implies that a and b are odd integers, and therefore $b^2 - a^2 p \equiv 1 - p \equiv -2 \pmod 8$. Consequently, $a^2 p - b^2 = 2$.

In both cases we may thus assume that a, b and r are positive odd integers, with $a^2p^2 - b^2 p = 2^r p = (ap + b\sqrt{p})(ap - b\sqrt{p})$. Let then $\beta = (2 + \sqrt{2})(ap + b\sqrt{p})$, an element of $K = \mathbb{Q}(\sqrt{2}, \sqrt{p})$, and let $L = K(\sqrt{\beta})$. For every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, the conjugate β^σ satisfies $\beta^\sigma \equiv \beta \pmod{K^{*2}}$ and $\beta^\sigma > 0$. Hence β is totally positive and L is a real Galois extension of $\mathbb{Q}$. Moreover, every prime $\mathfrak{q}$ of K dividing (β) lies above 2 or p as $N_{K/\mathbb{Q}}(\beta) = 2^{2(r+1)} \cdot p^2$, and only such a prime $\mathfrak{q}$ can ramify in $L = K(\sqrt{\beta})$. Thus L is unramified outside $S = \{2, p\}$.

In order to ensure that $\mathrm{Gal}(L/\mathbb{Q}) \cong Q_8$ it suffices to show that L is cyclic of degree 4 over $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{2p})$. Indeed, $\sqrt{\beta}$ is a root of the polynomial

$$X^4 - 2ap(2 + \sqrt{2})X^2 + 2^r p(2 + \sqrt{2})^2$$

over $\mathbb{Q}(\sqrt{2})$. Since $2^r p(2+\sqrt{2})^2 \equiv p \not\equiv 1 \pmod{\mathbb{Q}(\sqrt{2})^{*2}}$ but $p(4a^2p^2 - 4 \cdot 2^r p) = p(4b^2 p)$ is a square in $\mathbb{Q}(\sqrt{2})$, L is cyclic of degree 4 over $\mathbb{Q}(\sqrt{2})$ by

Lemma 2.8(a). Similarly, $\sqrt{\beta}$ is a root of the polynomial

$$X^4 - 4(ap + b\sqrt{p})X^2 + 2(ap + b\sqrt{p})^2$$

over $\mathbb{Q}(\sqrt{p})$, and application of Lemma 2.8(a) shows that L is cyclic of degree 4 over $\mathbb{Q}(\sqrt{p})$. Finally, $\sqrt{\gamma}$ is a root of

$$X^4 - 2(2ap + b\sqrt{2p})X^2 + 2 \cdot 2^r p$$

over $\mathbb{Q}(\sqrt{2p})$, and Lemma 2.8(a) applies again. Note that $2(2^r p) = 2^r(2p) \equiv 2^r \equiv 2 \pmod{\mathbb{Q}(\sqrt{2p})^{*2}}$ (as r is odd), but $2(4(2ap + b\sqrt{2p})^2 - 8(2^r p)) \equiv (ap + b\sqrt{2b})^2 \pmod{\mathbb{Q}(\sqrt{2p})^{*2}}$. Hence L is indeed a Q_8-field over the rationals. Lemma 2.1 now yields $L = \mathbb{Q}(\sqrt{\beta})$.

We may also argue on the basis of Proposition 3.3, and of Lemma 2.8(b). This part of the lemma readily implies that $F = K(\sqrt{ap + b\sqrt{p}})$ is a (real) Galois extension with dihedral group (of order 8) which is cyclic over $\mathbb{Q}(\sqrt{2})$. By Proposition 3.3 the companion field L of F and B_2K has the desired properties. It is obvious that L is as before. Uniqueness of $L = L_p$ in $\mathcal{K}_S^+(Q_8)$ follows from the Corollary to Proposition 3.2. (This may also be checked, more elementarily, using Lemma 2.3.) In view of Lemma 2.1 it is immediate that $L_p^- = \mathbb{Q}(\sqrt{-\beta})$ is the unique further (complex) field belonging to $\mathcal{K}_S(Q_8)$. ■

In the case $p \equiv 1 \pmod 8$, knowledge of the class number $h(p)$ may be helpful in Theorem 1. The smallest such prime where $h(p) > 1$ is $p = 257$, in which case $h(p) = 3$ and where $p - 15^2 = 2^5$ gives

$$L_p = \mathbb{Q}\big(\sqrt{(2 + \sqrt{2})(257 + 15\sqrt{257})}\big).$$

One can avoid reference to $h(p)$ by arguing as follows.

Remark. Let $p \equiv 1 \pmod 8$. Then there are positive integers x, y such that $x^2 - 2y^2 = p$. (Note that $h_+(8) = 1$ and $\left(\frac{2}{p}\right) = 1$, so either p splits in $\mathbb{Q}(\sqrt{2})$ or p is represented by the quadratic form $X^2 - 2Y^2$ (see [3, Satz 3, p. 65]).) Here x must be odd and y even. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{p})$ and $F = K\big(\sqrt{x + y\sqrt{2}}\big)$. Then F is a real Galois number field with group D_8 which is cyclic over $\mathbb{Q}(\sqrt{2p})$ (Lemma 2.8(b)). Moreover F is unramified outside $S = \{2, p\}$. Let P be the unique (real) subfield of $\mathbb{Q}(\zeta_p)$ of absolute degree 4, and let E be the companion field of $B_2(\sqrt{p})$ and $P(\sqrt{2})$ (which intersect in K). This E is cyclic over $\mathbb{Q}(\sqrt{2})$ and over $\mathbb{Q}(\sqrt{p})$, hence elementary over $\mathbb{Q}(\sqrt{2p})$. It follows that $E = E_1E_2$ where both E_i are solutions of the embedding problem $(\mathbb{Q}(\sqrt{2p})/\mathbb{Q}, Z_4)$. Application of Propositions 3.3 and 3.2 shows that L_p is the companion field of F and E.

By uniqueness of L_p, and by Lemma 2.6, either F is in the Hilbert 2-class field of $\mathbb{Q}(\sqrt{2p})$, or $K\big(\sqrt{-x - y\sqrt{2}}\big)$ is its narrow Hilbert 2-class field.

5. Proof of Theorem 2. Let $S = \{p, q\}$ where p and q are distinct primes satisfying $p \equiv q \equiv 1 \pmod 4$ and $\left(\frac{q}{p}\right) = 1$. By Lemma 2.2 this S is a candidate for having $\mathcal{K}_S(Q_8) \neq \emptyset$. Let $K_0 = \mathbb{Q}(\sqrt{pq})$, and $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ be its (narrow) genus field. By Lemma 2.6 there is a unique Galois number field $F \supset K$ of absolute degree 8 in which no finite prime of K_0 (or K) is ramified. This F has a dihedral Galois group over the rationals, and is cyclic over K_0. Also F is real if and only if the class number $h(pq)$ of K_0 is divisible by 4 (or that of K is even).

Let P and Q be the (unique) subfields of $\mathbb{Q}(\zeta_p)$ and $\mathbb{Q}(\zeta_q)$, respectively, with absolute degree 4. So P is real if and only if $p \equiv 1 \pmod 8$, and similarly for Q. Let E be the companion field of PK and QK. This E is real if and only if either $p \equiv q \equiv 1 \pmod 8$ or $p \equiv q \equiv 5 \pmod 8$. Moreover, E is cyclic over $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{q})$, since $PK/\mathbb{Q}(\sqrt{p})$ and $QK/\mathbb{Q}(\sqrt{q})$ are elementary. It follows that E is elementary over K_0 and that $E = E_1E_2$ where both E_i are solutions of the embedding problem $(K_0/\mathbb{Q}, Z_4)$. Of course, $E = KE_i$ for each i.

Let L be the companion field of F and E. By Propositions 3.3 and 3.2 this $L = L_{pq}$ is the unique field belonging to $\mathcal{K}_S(Q_8)$. ∎

Proposition 5.1. *The field F of Theorem 2 may be described as follows. There exist integers x, y with the same parity such that $x^2 - qy^2 = 4p^h$ where $h = h(q) = h_+(q)$ is odd. If x, y are odd, then choose the sign of x such that $x \equiv 3 \pmod 4$. If x, y are even, which happens when $q \equiv 1 \pmod 8$, then $x/2$ is odd and we choose the sign of x such that $x/2 \equiv 3 \pmod 4$ if $p \equiv 5 \pmod 8$ and $x/2 \equiv 1 \pmod 4$ if $p \equiv 1 \pmod 8$. In both cases we have $F = \mathbb{Q}(\sqrt{p}, \sqrt{\theta})$ where $\theta = \frac{1}{2}(x + y\sqrt{q})$. In particular, $h(pq)$ is divisible by 4 (hence F is real) if and only if $x > 0$ in these choices.*

Proof. We know that h is as asserted (Lemma 2.5), and p splits in $\mathbb{Q}(\sqrt{q})$ (as $\left(\frac{q}{p}\right) = 1$). We find integers x, y with the same parity such that $x^2 - qy^2 = 4p^h$. Suppose first that x, y are odd. Hence $1 - q \equiv 4 \pmod 8$ and $q \equiv 5 \pmod 8$. Choose then the sign of x such that $x \equiv 3 \pmod 4$. Suppose next that $x = 2x_0$ and $y = 2y_0$ are even. Then $x_0^2 - qy_0^2 = p^h$ and $p^h \equiv p \pmod 8$ as h is odd. From $p \equiv q \equiv 1 \pmod 4$ we get $x_0^2 - y_0^2 \equiv 1 \pmod 4$. It follows that x_0 must be odd and y_0 be even, and we choose the sign of x as defined above. In both cases we let $\theta = \frac{1}{2}(x + y\sqrt{q})$, and $F = \mathbb{Q}(\sqrt{\theta}, \sqrt{p})$.

It follows from Lemma 2.8(b) that F is Galois over the rationals with group D_8, and F is cyclic over $K_0 = \mathbb{Q}(\sqrt{pq})$. Also, F is unramified outside $S \cup \{\infty\}$ except possibly that some dyadic prime of $\mathbb{Q}(\sqrt{q})$ ramifies in $\mathbb{Q}(\sqrt{q}, \sqrt{\theta})$. We shall rule the latter out by showing that θ is a 2-primary integer in $\mathbb{Q}(\sqrt{q})$, that is, θ is an *odd* integer (relatively prime to 2) such that the congruence $X^2 \equiv \theta \pmod 4$ has a solution in the integers of $\mathbb{Q}(\sqrt{q})$

(see Hecke [12, Theorem 120]). Here θ is *odd* as its absolute norm equals p^h. If x, y are odd, then $(x-1)^2 \equiv 4 \pmod{16}$ as $x \equiv 3 \pmod 4$, and $\rho = (1 + y\sqrt{q})/2$ is a solution of the congruence since

$$\begin{aligned}\rho^2 - \theta &= \frac{1}{4}(1 + qy^2 - 2x) = \frac{1}{4}(1 - 2x + x^2 - 4p^h)\\ &= \frac{1}{4}(x-1)^2 - p^h \equiv 0 \pmod 4.\end{aligned}$$

Suppose next that $x = 2x_0$ and $y = 2y_0$ are even, where $x_0^2 - qy_0^2 = p^h$ and $\theta = x_0 + y_0\sqrt{q}$. Since x_0 is odd, we get $1 - qy_0^2 \equiv p \equiv 1$ or $5 \pmod 8$. Thus $y_0/2$ is even when $p \equiv 1 \pmod 8$, in which case $x_0 \equiv 1 \pmod 4$ and so $(q - x_0)/2$ is even likewise. If $p \equiv 5 \pmod 8$, then $y_0/2$ is odd, where by definition $x_0 \equiv 3 \pmod 4$ and hence $(q - x_0)/2$ is odd. Thus $\lambda = \frac{1}{4}(q - x_0 - y_0\sqrt{q})$ is an integer of $\mathbb{Q}(\sqrt{q})$, and $q - \theta = 4\lambda$. Hence $\sqrt{q}$ is a solution of the congruence in this case.

It follows that F is unramified outside $S \cup \{\infty\}$ (where $S = \{p, q\}$). Let E be as in the proof of Theorem 2. Then $F \cap E = \mathbb{Q}(\sqrt{p}, \sqrt{q})$, and by Proposition 3.3 the companion field L of F and E is quaternion over the rationals, and it is unramified outside $S \cup \{\infty\}$. Hence $L = L_{pq}$ by uniqueness. Thus $F \subset L_{pq}E$ is the companion field of L_{pq} and E, as desired. ∎

Example. In Proposition 5.1 the situation is symmetric in p and q. Let for instance $S = \{p, q\} = \{17, 101\}$. (In this case the absolute Galois group $G_S(2)$ is known to be infinite; see [6, Theorem 3.1].) Using $13^2 - 2^2 \cdot 17 = 101$ and $13^2 - 101 = 4 \cdot 17$ we deduce that

$$F = \mathbb{Q}\big(\sqrt{-13 + 2\sqrt{17}}, \sqrt{101}\,\big) = \mathbb{Q}\big(\sqrt{(-13 + \sqrt{101})/2}, \sqrt{17}\,\big)$$

is not real. Thus $h(pq)$ is not divisible by 4 in this case. Indeed $h(pq) = 2$ here, so that F is the narrow Hilbert class field of $\mathbb{Q}(\sqrt{pq})$. Note also that L_{pq} is real in this example.

6. Proof of Theorem 3. Let the prime p satisfy $p \equiv 1 \pmod{2^{n-1}}$ for some integer $n > 3$. We first show that there is a field in $\mathcal{K}_S(D_{2^n})$ which is cyclic over $k_0 = \mathbb{Q}(\sqrt{2})$. Let $H_0 = \mathrm{Gal}(k_0/\mathbb{Q})$ act on the cyclic group U_0 of order 2^{n-1} by inverting the elements. Embed k_0 into $E = \mathbb{Q}(\zeta_{2^{n-1}})$, and let $H = \mathrm{Gal}(E/\mathbb{Q})$. Then H_0 is an epimorphic image of H, whence $U_0H_0 \cong D_{2^n}$ is an epimorphic image of the semidirect product U_0H. We may also replace U_0 by any free $(\mathbb{Z}/2^{n-1}\mathbb{Z})H$-module $U \neq 0$ since U_0 is a quotient module of U.

The prime p splits totally in E. By Weber's theorem (see e.g. [9, p. 68]) the class number h of E is odd. Let $\mathfrak{p}$ be a prime of E above p. Then $\mathfrak{p}^h = (\alpha)$ for some $\alpha \in E$. We have $v_{\mathfrak{p}}(\alpha) = h$ and $v_{\mathfrak{q}}(\alpha) = 0$ for each prime $\mathfrak{q} \neq \mathfrak{p}$ of E. In particular, $v_{\mathfrak{p}}(\alpha^\sigma) = 0$ for all $1 \neq \sigma \in H$ (but $v_{\mathfrak{p}^\sigma}(\alpha^\sigma) = h$). Since

h is odd, the order of α, and of the α^σ, in $E^*/E^{*2^{n-1}}$ is 2^{n-1}. Let

$$\widehat{E} = E(\sqrt[2^{n-1}]{\alpha^\sigma} : \sigma \in H).$$

Then $U = \mathrm{Gal}(\widehat{E}/E)$ is a free $(\mathbb{Z}/2^{n-1})H$-module of rank 1 and, by Kummer theory, $\widehat{E}$ is a Galois extension of $\mathbb{Q}$ whose group is an extension of $H = \mathrm{Gal}(E/\mathbb{Q})$ by U. Hence the extension splits. (This argument follows closely that given by Serre [21, p. 18].)

By construction, $\widehat{E}$ is unramified outside $S \cup \{\infty\}$, where $S = \{2, p\}$. Moreover, $U_0H_0 \cong D_{2^n}$ is a quotient group of $\mathrm{Gal}(\widehat{E}/\mathbb{Q}) \cong UH$. Consequently, there is a field L_1 in $\mathcal{K}_S(D_{2^n})$ which is cyclic over $k_0 = \mathbb{Q}(\sqrt{2})$. Let $X_1 = \mathrm{Gal}(L_1/\mathbb{Q})$, and let K be the fixed field on L_1 of $Z(X_1)$ (so that $\mathrm{Gal}(K/\mathbb{Q}) \cong D_{2^{n-1}}$). Let L be the companion field of L_1 and B_2K. By Proposition 3.3 this L is a field in $\mathcal{K}_S(Q_{2^n})$, and it is cyclic over $\mathbb{Q}(\sqrt{2})$. We also know from the Corollary to Proposition 3.3 that K is real, and we may modify L, if necessary, so that it is a real field (Lemma 2.1).

Uniquenes of L in $\mathcal{K}_S^+(Q_{2^n})$ is settled by induction on n. In fact, this allows us to assume that K is the unique field in $\mathcal{K}_S^+(D_{2^{n-1}})$ which is cyclic over $\mathbb{Q}(\sqrt{2})$, and then the Corollary to Proposition 3.2 applies. ■

EXAMPLE. The prime $p = 113$ is the smallest prime congruent to 1 modulo 8 (here even $p \equiv 1 \pmod{16}$) for which the class number $h(8p)$ of $\mathbb{Q}(\sqrt{2p})$ is divisible by 8. Indeed, $h(8p) = 8$, and the Hilbert class field of $\mathbb{Q}(\sqrt{2p})$ is given explicitly by Cohen [3, p. 537]. By the Remark in Section 4 we know that there are subfields E_1, E_2 of $\mathbb{Q}(\zeta_{16p})$ containing $\mathbb{Q}(\sqrt{2p})$ and cyclic over $\mathbb{Q}$ of degree 4. Hence application of Proposition 3.3 and Lemma 2.1 shows that there are unique real and complex fields in $\mathcal{K}_S(Q_{16})$ for $S = \{2, p\}$ which are cyclic over $\mathbb{Q}(\sqrt{2p})$.

For any prime $p \equiv 1 \pmod 8$ there exist positive integers x, y such that $x^2 - 2y^2 = 2p$ (see [23, Satz 3, p. 65]). Then $F = \mathbb{Q}\big(\sqrt{x + y\sqrt{2}}, \sqrt{2p}\big)$ is a field in $\mathcal{K}_S^+(D_8)$ for $S = \{2, p\}$ which is cyclic over $\mathbb{Q}(\sqrt{p})$, by virtue of Lemma 2.8(b). From [16, Proposition 4.2] it follows that F can be embedded into a D_{16}-field or Q_{16}-field over the rationals if and only if $(-p, x) = 1$ in $\mathrm{Br}(\mathbb{Q})$. For $p = 113$ we have $26^2 - 2 \cdot 15^2 = 2 \cdot p$, and $(-p, 26) = 1$ in $\mathrm{Br}(\mathbb{Q})$. Since the (real) subfield E of $\mathbb{Q}(\zeta_p)$ of absolute degree 4 is a solution of the embedding problem $(\mathbb{Q}(\sqrt{p})/\mathbb{Q}, Z_4)$, we conclude that in this case there are also unique real and complex fields in $\mathcal{K}_S(Q_{16})$ which are cyclic over $\mathbb{Q}(\sqrt{p})$.

7. Fields of Dedekind type. In what follows we fix a prime $p \equiv 3 \pmod 8$, and let $S = \{2, p\}$. A normal number field L of 2-power degree is said to be of *Dedekind type* (with respect to p) if it is unramified outside S. Though these fields rely on the prime p chosen, the isomorphism type of the lattice formed by them will be independent of it.

The *Schur multiplier* of a profinite group Γ is the profinite (abelian) group $M(\Gamma) = H_2(\Gamma, \widehat{\mathbb{Z}})$ whose Pontryagin dual is the discrete (abelian) torsion group $H^2(\Gamma, \mathbb{Q}/\mathbb{Z})$ (see e.g. [18, Theorem 2.2.9]); for finite G this agrees with the usual definition. Given a prime p, $H_2(\Gamma, \mathbb{Z}_p)$ is the Sylow p-subgroup of $M(\Gamma)$, and we may write $M(\Gamma) = H_2(\Gamma, \mathbb{Z}_p)$ when Γ is a pro-p-group. Since the Leopoldt conjecture is true for $\mathbb{Q}$ (and for every abelian number field), $M(\Gamma) = 0$ for $\Gamma = G_S(2)$ (cf. [9, Theorem 4.9] or [18, Theorem 10.3.6]). We shall see that this also holds for $G_S^+(2)$, the absolute Galois group of the maximal 2-extension $\mathbb{Q}_S^+(2)$ of the rationals unramified outside S.

Let us introduce the 2-groups which will appear as (finite) quotient groups of $G_S^+(2)$. Define

$$G_m^n = G_m^n(p) = \langle x, y \mid x^{2^m} = 1 = y^{2^n},\, y^{-1}xy = y^p \rangle$$

for positive integers m, n with $m \leq n+1$, and let

$$\widetilde{G}_m^n = \widetilde{G}_m^n(p) = \langle x, y \mid x^{2^m} = 1,\, y^{2^n} = x^{2^{m-1}},\, y^{-1}xy = y^p \rangle$$

for $m \leq n+2$. Both G_m^n and $\widetilde{G}_m^n$ are metacyclic groups of order 2^{m+n}. They are abelian if and only if $m = 1$, and G_1^n is of type $(2, 2^n)$ whereas $\widetilde{G}_1^n \cong Z_{2^{n+1}}$ is cyclic of order 2^{n+1}. Also, $G_2^1 = D_8$ and $\widetilde{G}_2^1 = Q_8$, and $\widetilde{G}_3^1$ is the semidihedral group of order 16 (independent of the particular prime $p \equiv 3 \pmod 8$).

Lemma 7.1. *The Schur multiplier $M(G_m^n)$ of $G_m^n = G_m^n(p)$ has order* 2 *whereas that of $\widetilde{G}_m^n$ vanishes. If $m < n+1$, then G_{m+1}^n and $\widetilde{G}_{m+1}^n$ are* (*nonisomorphic*) *Schur covers of G_m^n, and $\widetilde{G}_{m+1}^n$ is a Schur cover of G_m^n when $m = n+1$.*

This follows from [1, Proposition 9.2]. We see that the groups G_m^n, $\widetilde{G}_m^n$ are not isomorphic, and their isomorphism type is determined by m, n and the prime p.

Proposition 7.2. *Let $S = \{2, p\}$ with $p \equiv 3 \pmod 8$, and let G be a finite noncyclic* 2*-group. Then $\mathcal{K}_S^+(G) \neq \emptyset$ if and only if G is isomorphic to $G_m^n(p)$ or $\widetilde{G}_m^n(p)$ for some positive integers m, n, in which cases $\mathcal{K}_S^+(G)$ consists of a single field $F_n^m(p)$ respectively $\widetilde{F}_n^m(p)$ when $m < n+2$, and has cardinality* 2 *when $m = n+2$ and hence $G \cong \widetilde{G}_{n+2}^n(p)$.*

Proof. Let $\Gamma = G_S^+(2)$. It follows from [14, Satz 6.3] that, as a pro-2-group, Γ is generated by two elements σ, τ with the defining relation $\tau^{-1}\sigma\tau = \sigma^p$. So we are in a situation similar to that studied in [19]. One knows that the commutator subgroup $\Gamma' = [\Gamma, \Gamma]$ is closed in Γ, as is every finite-index subgroup. Of course, $\mathcal{K}_S^+(G) \neq \emptyset$ if and only if $G \cong \Gamma/R$ is a quotient group of Γ, and then we have a natural epimorphism $M(G) \twoheadrightarrow (R \cap \Gamma')/[R, \Gamma]$ by the 5-term exact homology sequence (see e.g. [1, Lemma 4.1]). We shall confirm the Hopf–Schur relation

$$M(G) \cong (R \cap \Gamma')/[R, \Gamma]$$

for all such quotient groups, which will imply that $M(\Gamma) = 0$ [9, Proposition 4.1]. The relation trivially holds when $M(G) = 0$. We have $\Gamma/\Gamma' \cong \mathbb{Z}_2 \times Z_2$ since $B_\infty(\sqrt{p})$ is the maximal abelian subextension of $\mathbb{Q}_S^+$, were $B_\infty = \bigcup_{i\ge 0} B_i$ is the (cyclotomic) $\mathbb{Z}_2$-extension of $B_0 = \mathbb{Q}$. The cyclic subfields of $B_\infty(\sqrt{2})$ are easily described, and their Galois groups over $\mathbb{Q}$ have trivial multiplier.

Let $G \cong \Gamma/R$ be noncylic. Then G can be generated by two elements x, y such that $y^{-1}xy = x^p$. Suppose the normal subgroup $\langle x\rangle$ of G has order 2^m, and $|G/\langle x\rangle| = 2^n$. Then $m \ge 1$, $n \ge 1$ and $x^{2^m} = 1$ and $y^{2^n} = x^s$ for some positive integer s. Here 2^m must be a divisor of $p^{2^n} - 1 = (p^{2^{n-1}} - 1)(p^{2^{n-1}} + 1)$. Since $p \equiv 3 \pmod 8$, $p^2 - 1$ is divisible by 2^3 but not by 2^4, and $p^{2^{n-1}} + 1 \equiv 2 \pmod 8$ for $n > 1$. By induction we see that the 2-part $(p^{2^n} - 1)_2$ is 2^{n+2} and so $m \le n + 2$. One may "normalize" the presentation of G by demanding that s is a divisor of 2^m and of $((p^{2^n} - 1)/(p - 1))_2 = 2^{n+1}$ (cf. [1, Lemma 9.1]). Now $G' = \langle [x, y]\rangle$ has order 2^{m-1} (as $[x, y] = x^{p-1}$ and $p - 1 \equiv 2 \pmod 8$), and from $1 = [x^s, y] = [x, y]^s = x^{s(p-1)}$ we infer that 2^m is a divisor of $2s$. Thus either $s = 2^m$ and $m \le n + 1$, or $s = 2^{m-1}$ and $m \le n + 2$.

Consequently, G is isomorphic to G_m^n or to $\widetilde{G}_m^n$ for $m \le n + 1$, or $G \cong \widetilde{G}_{n+2}^n$. In the case where $G \cong \widetilde{G}_{n+2}^n$ we have $s = 2^{n+1}$ and $M(G) = 0$, but $\langle yx\rangle$ is a complement to $\langle x\rangle$ in G (as $(yx)^{2^n} = y^{2^n} x^{1+p+\dots+p^{2^n-1}} = y^{2^n} x^{(p^{2^n}-1)/(p-1)} = y^{2^n} x^{2^{n+1}} = 1$). So in this particular case G is also a split extension (as it is when $G \cong G_m^n$ with $m \le n + 1$).

By definition (and [14, Satz 6.3]) the groups $G_m^n, \widetilde{G}_m^n$ appear as quotient groups of Γ. Fix n in what follows. Since G_1^n is abelian of type $(2, 2^n)$, we may write uniquely $G_1^n = \Gamma/R_1^n$ by the structure of Γ/Γ', so that $F_n^1(p) = B_n(\sqrt{2})$ is the fixed field of R_1^n on $\mathbb{Q}_S^+$. We show by induction on m that, for $2 \le m \le n + 2$, $G_m^n = \Gamma/R_m^n$ and $\widetilde{G}_m^n = \Gamma/\widetilde{R}_m^n$, for *unique* normal subgroups $R_m^n, \widetilde{R}_m^n$ of Γ. By the above lemma $M(G_1^n)$ has order 2 and maps onto $\Gamma'/[R_1^n, \Gamma]$. Now $R_1^n/\Gamma' \cong \mathbb{Z}_2$ is a free pro-2-group (of rank 1), so that there are exactly $|\mathrm{Hom}(\mathbb{Z}_2, \Gamma'/[R_1^n, \Gamma])|$ complements to $\Gamma'/[R_1^n, \Gamma]$ in $R_1^n/[R_1^n, \Gamma]$. Both G_2^n and $\widetilde{G}_2^n$ are (nonisomorphic) Schur covers of G_1^n, and they appear as quotient groups Γ/R_2^n respectively $\Gamma/\widetilde{R}_2^n$ of Γ such that $R_2^n/[R_1^n, \Gamma]$ and $\widetilde{R}_2^n/[R_1^n, \Gamma]$ are such complements. We conclude that the Hopf–Schur formula holds for G_1^n (and trivially also for $\widetilde{G}_1^n$), and that we have just two complements. This proves uniqueness of R_2^n and $\widetilde{R}_2^n$. Now we proceed by induction using $R_{m-1}^n/(R_{m-1}^n \cap \Gamma') \cong \mathbb{Z}_2$ and $|\mathrm{Hom}(\mathbb{Z}_2, M(G_{m-1}^n))| = 2$.

Hence we have $\mathcal{K}_S^+(G_m^n)=\{F_n^m\}$ and $\mathcal{K}_S^+(\widetilde{G}_m^n)=\{\widetilde{F}_n^m\}$ for $2\le m<n+2$, where F_n^m and $\widetilde{F}_n^m$ are the fixed fields of R_m^n and $\widetilde{R}_m^n$, respectively, on $\mathbb{Q}_S^+$. For $m=n+2$ the group $\widetilde{G}_m^n$ is, up to isomorphism, the unique Schur cover of $G_{m-1}^n=\Gamma/R_{m-1}^n$ appearing as a quotient group of Γ. But there are still two distinct complements and fixed fields $F_n^m\ne\widetilde{F}_n^m$. Hence $\mathcal{K}_S^+(\widetilde{G}_m^n)=\{F_n^m,\widetilde{F}_n^m\}$ has cardinality 2 in this exceptional case. ∎

Corollary 1. *The lattice of the fields of Dedekind type* (*with respect to* p) *is completely determined by the above. Indeed*, $F_n^m(p)\subseteq F_{n'}^{m'}(p)$ *if and only if* $n\le n'$ *and* $m\le m'$, *and* $\widetilde{F}_n^m(p)$ *is the companion field of* $F_n^m(p)$ *and* $F_{n+1}^{m-1}(p)$ $(2\le m\le n+2)$.

By the above for $2\le m\le n+2$ we have $G_{m-1}^n=\Gamma/R_{m-1}^n$, $R_m^n\widetilde{R}_m^n=R_{m-1}^n$ and $R_m^n\cap\widetilde{R}_m^n\supseteq[R_{m-1}^n,\Gamma]$. From Lemma 7.1 we infer that $(R_m^n\cap\widetilde{R}_m^n)\Gamma'$ $=R_1^{n+1}$ (and $\Gamma/R_1^{n+1}=G_1^{n+1}$). Consequently, $R_1^{m+1}\cap R_{m-1}^n=R_{m-1}^{n+1}$ and $R_1^{n+1}\cap R_m^n=R_m^{n+1}=R_m^n\cap\widetilde{R}_m^n$, by considering the corresponding fibre products of G_1^{n+1} with G_{m-1}^n and G_m^n. This also holds in the exceptional case $m=n+2$ where Γ/R_m^n and $\Gamma/\widetilde{R}_m^n$ are copies of $\widetilde{G}_m^n$. Finally, note that if G_m^n is an epimorphic image of $G_{m'}^{n'}$, then by the orders of the groups and their commutator factor groups, $2^{m+n}\le 2^{m'+n'}$ and $2^{n+1}\le 2^{n'+1}$.

Recall that $\bigcup_{n\ge1}F_n^1(p)=B_\infty(\sqrt{2})$, and we may similarly introduce the fields $F_\infty^m(p)=\bigcup_{n\ge m}^\infty F_n^m(p)$ for all $m\ge1$. Then

$$\mathbb{Q}_S^+(2)=\bigcup_{m\ge1}F_\infty^m(p).$$

Corollary 2. *We have* $M(G_S^+(2))=0$, *and* $\mathcal{K}_S(Q_{2^n})=\emptyset$ *for all* $n>3$.

The first statement has already been settled in the course of the proof of the proposition. Since Q_{2^n} is not isomorphic to $G_{n-1}^1(p)$ or $\widetilde{G}_{n-1}^1(p)$ for $n>3$, we also find that then $\mathcal{K}_S^+(Q_{2^n})=\emptyset$. We finish by applying Lemma 2.1.

Example. As before let $S=\{2,p\}$ with $p\equiv3 \pmod 8$. By Theorem 1 there exist positive odd integers a,b such that $a^2p-b^2=2$ (yielding $L_p=\widetilde{F}_1^2(p)$). Combining Lemma 2.8(b) and Proposition 7.2, we see that

$$F_1^2(p)=\mathbb{Q}\big(\sqrt{ap+b\sqrt{p}},\sqrt{2}\big)$$

is the unique field belonging to $\mathcal{K}_S^+(D_8)$, and it is cyclic over $\mathbb{Q}(\sqrt{2})$. Observe that $F_1^2(p)$ can be embedded into the semidihedral fields $F_1^3(p)$ and $\widetilde{F}_1^3(p)$.

Added in proof (August 2014). Let $G=Q_{2^n}$ for some $n>3$, and let $S=\{p,q\}$ for some distinct odd primes p,q. It follows from Theorems A, B in [6] that $\mathcal{K}_S(G)\ne\emptyset$ only when $p\equiv q\equiv1 \pmod 4$ and $(\frac{p}{q})=1$. The recent work of Kisilevsky, Neftin and Sonn on semiabelian groups [Compos. Math. 146 (2010), 599–606] yields the following: Suppose that in addition $p\equiv1 \pmod{2^n}$ and that the fundamental unit u of $\mathbb{Q}(\sqrt{q})$ is a

2^{n-1}th power in the residue class fields of the primes above p, which just requires that p splits completely in $\mathbb{Q}(\sqrt{q}, \zeta_{2^n}, \sqrt[2^{n-1}]{u})$ (Chebotarev). Then there is a unique field in $\mathcal{K}_S(G)$ which is cyclic over $\mathbb{Q}(\sqrt{q})$.

References

[1] F. R. Beyl, U. Felgner and P. Schmid, *On groups occurring as center factor groups*, J. Algebra 61 (1979), 161–177.

[2] K. Burde, *Ein rationales biquadratisches Reziprozitätsgesetz*, J. Reine Angew. Math. 235 (1969), 175–184.

[3] H. Cohen, *Advanced Topics in Computational Number Theory*, Springer, New York, 2000.

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

[5] R. Dedekind, *Konstruktion von Quaternionenkörpern*, Ges. Math. Werke, Vol. 2, Vieweg, Braunschweig, 1931.

[6] B. Eick and H. Koch, *On maximal 2-extensions of $\mathbb{Q}$ with given ramification*, in: Amer. Math. Soc. Transl. (2) 219, Amer. Math. Soc., Providence, RI, 2006, 87–102.

[7] A. Fröhlich, *Artin root numbers and normal integral bases for quaternion fields*, Invent. Math. 17 (1972), 143–166.

[8] A. Fröhlich, *Artin root numbers, conductors, and representations for generalized quaternion groups*, Proc. London Math. Soc. (3) 28 (1974), 402–438.

[9] A. Fröhlich, *Central Extensions, Galois Groups, and Ideal Class Groups of Number Fields*, Contemp. Math. 24, Amer. Math. Soc., Providence, RI, 1983.

[10] H. Hasse, *Zur Geschlechtertheorie in quadratischen Zahlkörpern*, J. Math. Soc. Japan 3 (1951), 45–51.

[11] H. Hasse, *Über die Teilbarkeit durch 2^3 der Klassenzahl der quadratischen Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern*, Math. Nachr. 46 (1970), 61–70.

[12] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Springer, New York, 1981.

[13] C. U. Jensen and N. Yui, *Quaternion extensions*, in: Algebraic Geometry and Commutative Algebra, Vol. I, Kinokuniya, Tokyo, 1988, 155–182.

[14] H. Koch, *l-Erweiterungen mit vorgegebenen Verzweigungsstellen*, J. Reine Angew. Math. 209 (1965), 30–61.

[15] H. Koch, *Galois Theory of p-Extensions*, Springer, Berlin, 2002.

[16] A. Ledet, *On 2-groups as Galois groups*, Canad. J. Math. 47 (1995), 1253–1273.

[17] F. Lemmermeyer, *Unramified quaternion extensions of quadratic number fields*, J. Théor. Nombres Bordeaux 9 (1997), 51–68.

[18] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of Number Fields*, Springer, Berlin, 2008.

[19] P. Schmid, *On 2-extensions of the rationals with restricted ramification*, Acta Arith. 163 (2014), 111–125.

[20] J.-P. Serre, *A Course in Arithmetic*, Springer, New York, 1973.

[21] J.-P. Serre, *Topics in Galois Theory*, Jones and Bartlett, Boston, 1992.

[22] P. Stevenhagen, *Divisibility by 2-powers of certain quadratic class numbers*, J. Number Theory 43 (1993), 1–19.

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

[24] D. B. Zagier, *Zetafunktionen und quadratische Körper*, Springer, Berlin, 1981.

Mathematisches Institut
Universität Tübingen
Auf der Morgenstelle 10
D-72076 Tübingen, Germany
E-mail: peter.schmid@uni-tuebingen.de

Received on 4.9.2013
and in revised form on 14.5.2014 (7573)