ACTA ARITHMETICA
163.2 (2014)

On 2-extensions of the rationals with restricted ramification

by

Peter Schmid (Tübingen)

1. Introduction. For a finite set S of rational primes and a finite group G let $\mathcal{K}_S(G)$ denote the set of normal number fields (within $\mathbb{C}$) with Galois group G which are unramified outside $S \cup \{\infty\}$. We say that G belongs to $\mathcal{K}_S$ if $\mathcal{K}_S(G) \neq \emptyset$, and we write $\mathcal{K}_p(G)$ if $S = \{p\}$ consists of a single prime p. Thus G belongs to $\mathcal{K}_S$ if and only if it is a quotient group of the absolute Galois group $G_S = \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$, where $\mathbb{Q}_S$ is the maximal extension of $\mathbb{Q}$ unramified outside $S \cup \{\infty\}$. General facts on the structure of the profinite group G_S, and its maximal pro-p-quotient groups $G_S(p)$ for primes p, can be found in the monographs [13], [10].

In this paper we are just concerned with the situation that G is a 2-group. Thus G belongs to $\mathcal{K}_S$ if and only if it is a quotient group of $G_S(2)$. This is of interest *per se* but certainly also because of the lack of a simple approach to the inverse problem of Galois theory for finite 2-groups (like that given by Reichardt–Scholz in the odd case; see Serre [15, Chap. 2]). Recently the groups $G_S(2)$ have been studied thorougly for sets S of *odd* rational primes [11], and when S consists of certain pairs or triplets of *odd* primes [2], [3], [5]. Here we shall treat the rather different, and special, situation where $S = \{2\}$. In this case the structure of $G_S(2)$ is known since many years (Markšaitis [12], Shafarevich [17], Koch [9]). This gives rise to the following basic observation.

Theorem 0. *Let G be a finite 2-group, and let $\Omega(G)$ denote the set of ordered pairs $(x, y) \in G \times G$ such that $G = \langle x, y\rangle$ and $y^2 = 1$. Then $\mathcal{K}_2(G) \neq \emptyset$ if and only if $\Omega(G) \neq \emptyset$; indeed the cardinalities satisfy $|\mathcal{K}_2(G)| = |\Omega(G)|/|\mathrm{Aut}(G)|$.*

Hence just those nontrivial finite 2-groups belong to $\mathcal{K}_2$ which can be generated by two elements, one being an involution. Usually it is not easy to

2010 *Mathematics Subject Classification*: Primary 11F80, 11R32; Secondary 11S15.
Key words and phrases: Galois theory, restricted ramification, central group and field extensions, Schur multipliers, ring class fields.

DOI: 10.4064/aa163-2-2

compute the cardinality of $\mathcal{K}_2(G)$ in the way indicated above; we just carry this out when G is dihedral (Lemma 2.3). It is more convenient to argue on the basis of the theory of central group and field extensions (Fröhlich, Shafarevich). Given $K \in \mathcal{K}_2(G)$ we shall see that there exist just $|M(G)|$ normal number fields $L \supseteq K$ whose Galois group is a Schur cover of G (Proposition 3.3). Here $M(G) = H_2(G, \mathbb{Z})$ denotes the Schur multiplier of G.

We shall compute $\mathcal{K}_2(G)$ explicitly (not only its cardinality) for certain distinguished 2-groups G appearing. These groups come up as follows.

THEOREM 1. *Let G be a finite 2-group. Then $\mathcal{K}_2(G) \neq \emptyset$ if and only if one of the following holds:*

(i) *G is cyclic or abelian of type $(2^{n-2}, 2)$ for some $n \geq 3$.*
(ii) *G is a dihedral, semidihedral or modular 2-group.*
(iii) *There is a unique normal subgroup G^* of G having index 2 in the commutator subgroup $G' = [G, G]$ of G and G/G^* is a semimodular 2-group. Either $G^* = 1$ or some noncentral involution of G/G^* lifts to an involution in G.*

Recall that the (generalized) quaternion group Q_{2^n}, the dihedral group D_{2^n}, the semidihedral group SD_{2^n} and the modular group M_{2^n} are the only nonabelian 2-groups of order 2^n having a cyclic subgroup of index 2 [8, Satz I.14.9]. They are pairwise nonisomorphic (letting $n \geq 4$ in the latter two cases). For $G = M_{2^n}$ the commutator subgroup has order 2 and G/G' is of type $(2^{n-2}, 2)$. Up to isomorphism, the semimodular group SM_{2^n} is the unique group of order 2^n, $n \geq 4$, with the corresponding properties but having two conjugacy classes of noncentral involutions (and not just one as for M_{2^n}; see Lemma 4.2 below).

We shall describe $\mathcal{K}_2(G)$ when G is dihedral, semidihedral, modular or semimodular. For $n \geq 1$ let E_n be the ring class field for the order $\mathbb{Z}[2^n i]$ in $\mathbb{Q}(i)$ and F_n that for the order $\mathbb{Z}[2^{n-1} i\sqrt{2}]$ in $\mathbb{Q}(i\sqrt{2})$ ($i = \zeta_4$, $\zeta_r = e^{2\pi i/r}$). Then $E_1 = \mathbb{Q}(i)$, $F_1 = \mathbb{Q}(i\sqrt{2})$ and $E_2 = F_2 = \mathbb{Q}(\zeta_8)$. Neither E_n nor F_n contains the 16th roots of unity, and $E_n \cap F_n = \mathbb{Q}(\zeta_8)$ for $n \geq 2$ (Lemma 5.3). For $n \geq 3$ let $\widetilde{E}_n$ be the field properly between E_{n-1} and $E_n(\zeta_{16})$ and distinct fom E_n and $E_{n-1}(\zeta_{16})$, and define $\widetilde{F}_n$ similarly.

THEOREM 2. *For $n \geq 3$ we have $\mathcal{K}_2(D_{2^n}) = \{E_n, F_n\}$, and we have $\mathcal{K}_2(SD_{2^n}) = \{\widetilde{E}_n, \widetilde{F}_n\}$ for $n \geq 4$. Also, $\mathcal{K}_2(M_{2^n}) = \{\mathbb{Q}(\sqrt[4]{2} \cdot \zeta_{2^{n+1}})\}$ and $\mathcal{K}_2(SM_{2^n}) = \{\mathbb{Q}(\sqrt[4]{2}, \zeta_{2^n})\}$ for $n \geq 4$.*

By complex multiplication we may generate ring class fields by singular values of the modular j-function (cf. Cox [4, Theorem 11.1]). Thus we have $E_n = \mathbb{Q}(i, j(2^n i))$ and $F_n = \mathbb{Q}(i\sqrt{2}, j(2^{n-1} i\sqrt{2}))$. The absolute values of the coefficients of the minimum polynomials over $\mathbb{Q}$ of these singular j-values are known to grow very rapidly (with n), and the same holds for the

unique 3rd root γ_2 of j which is real-valued on the imaginary axis (and has the same generating property by [4, Theorem 12.2]; see also Schertz [14, Theorem 6.3.1]). In the last section of the paper we give simple generating polynomials for some of the fields appearing in Theorem 2.

2. Basic observations. Recall that we regard number fields as subfields of $\mathbb{C}$ (algebraic over the rationals). Following Gras–Jaulent [7] number fields unramified outside $\{2, \infty\}$ are called 2-*ramified*.

Suppose $G \neq 1$ is a finite abelian 2-group belonging to $\mathcal{K}_2$. If $G = Z_2$ is the group of order 2, then $\mathcal{K}_2(G) = \{\mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(i\sqrt{2})\}$, because these are the unique quadratic number fields in which only the prime 2 ramifies. If G is cyclic of order 2^{n-2} for some $n \geq 4$, then $\mathcal{K}_2(G) = \{\mathbb{Q}(\zeta_{2^n} + \zeta_{2^n}^{-1}), \mathbb{Q}(\zeta_{2^n} - \zeta_{2^n}^{-1})\}$. In all other cases G is of type $(2^{n-2}, 2)$ for some $n \geq 4$ and $\mathcal{K}_2(G) = \{\mathbb{Q}(\zeta_{2^n})\}$. This follows from the Kronecker–Weber theorem and known ramification in cyclotomic fields, and determines the structure of

$$G_S(2)/G_S(2)' \cong \mathbb{Z}_2 \oplus Z_2$$

for $S = \{2\}$. Observe that the (usual) commutator group $G_S(2)'$ is closed in $G_S(2)$, as is every finite-index subgroup (cf. [16, Exercise 6 in Section I.4.2]).

LEMMA 2.1. *Let K be a normal 2-ramified number field having a finite nonabelian Galois 2-group $G = \mathrm{Gal}(K/\mathbb{Q})$. Then K contains $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$ as the fixed field of the Frattini subgroup $\Phi(G)$ of G, and $G = \langle x, y\rangle$ where y is complex conjugation on K and x is any element of G which is not trivial on $\mathbb{Q}(\sqrt{2})$.*

Proof. The fixed field of any maximal subgroup of G is one of $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(i\sqrt{2})$. Thus $|G : \Phi(G)| = 4$ (as G is not abelian), and $\mathbb{Q}(\zeta_8)$ is the fixed field of $\Phi(G)$. Complex conjugation y on K is an involution in G having the fixed field $\mathbb{Q}(\sqrt{2})$ when restricted to $\mathbb{Q}(\zeta_8)$. By Burnside's basis theorem [8, Satz III.3.15] there is $x \in G$ such that $G = \langle x, y\rangle$ is generated by x and y. We may choose x arbitrarily, just taking care that x is not trivial on $\mathbb{Q}(\sqrt{2})$ (so that $x \notin \Phi(G)$ and $\Phi(G)x \neq \Phi(G)y$). ∎

Note that in the above situation K cannot be cyclic or quaternion over $\mathbb{Q}(\sqrt{2})$, because otherwise complex conjugation y on K would be a central involution of G and $G/\langle y\rangle$ would be cyclic, whence G would be abelian.

PROPOSITION 2.2 (= Theorem 0). *For a finite 2-group G we have $|\mathcal{K}_2(G)| = |\Omega(G)|/|\mathrm{Aut}(G)|$ (where $\Omega(G) = \{(x, y) \in G \times G \mid G = \langle x, y\rangle, y^2 = 1\}$).*

Proof. Let $S = \{2\}$. The absolute Galois group $\Gamma = G_S(2)$ of the maximal 2-ramified 2-extension $\mathbb{Q}_S(2)$ of the rationals is known to be the pro-2-completion of the free product $\mathbb{Z} * Z_2$ or, equivalently, the pro-2-group with two generators σ, τ and defining relation $\tau^2 = 1$ (say). For a proof we refer to

the (classical) papers [12, 17, 9] already mentioned in the Introduction, or to the recent paper [7]. One knows that τ represents the unique conjugacy class of involutions in Γ; it may be identified with complex conjugation on $\mathbb{Q}_S(2)$.

We may assume that G is nonabelian. By Lemma 2.1, $\mathcal{K}_2(G) \neq \emptyset$ only if $\Omega = \Omega(G) \neq \emptyset$. Given $(x, y) \in \Omega$ there is a (continuous) epimorphism $\pi : \Gamma \twoheadrightarrow G$ defined by $\pi(\sigma) = x$ and $\pi(\tau) = y$. By a standard argument this gives G the structure of the Galois group of some normal number field K unramified outside $\{2, \infty\}$. Indeed, let K be the fixed field of the kernel of π, and let G act on K through the inverse of the isomorphism $\Gamma/\mathrm{Ker}(\pi) \xrightarrow{\sim} G$ induced by π.

Suppose we have two pairs (x_i, y_i) in Ω $(i = 1, 2)$. These pairs define epimorphisms $\pi_i : \Gamma \twoheadrightarrow G$ (via $\sigma \mapsto x_i$, $\tau \mapsto y_i$). Then $\mathrm{Ker}(\pi_1) = \mathrm{Ker}(\pi_2)$ if and only if $\pi_2 = \alpha \circ \pi_1$ for some automorphism $\alpha \in \mathrm{Aut}(G)$. Of course $\mathrm{Aut}(G)$ acts semiregularly on Ω, that is, each orbit has size $|\mathrm{Aut}(G)|$. Hence $|\mathcal{K}_2(G)| = |\Omega|/|\mathrm{Aut}(G)|$, as desired. ∎

LEMMA 2.3. *We have* $|\mathcal{K}_2(D_{2^n})| = 2$ $(n \geq 3)$.

Proof. Let $G = D_{2^n}$, and let N be its unique cyclic maximal subgroup. There are 2^{n-1} noncentral involutions in G (outside N), and for each such involution y there are 2^{n-1} elements x of G such that $G = \langle x, y\rangle$, namely the 2^{n-2} generators of N and the 2^{n-2} noncentral involutions of G not conjugate to y in G. Thus $\Omega = \Omega(G)$ has cardinality 2^{2n-2}. Let $A = C_{\mathrm{Aut}(G)}(N)$. Then $A \cong Z^1(G/N, N)$ acts regularly on the set of noncentral involutions [8, Hilfssatz VI.7.14]. Moreover, every automorphism of N can be extended to G as it acts trivially on $H^2(G/N, N)$ (which has order 2 as G/N inverts the elements of N). Hence $\mathrm{Aut}(G)/A$ has order 2^{n-2} and $|\mathrm{Aut}(G)| = 2^{2n-3}$. Consequently, $|\mathcal{K}_2(G)| = |\Omega|/|\mathrm{Aut}(G)| = 2$ by Proposition 2.2 (Theorem 0). ∎

PROPOSITION 2.4. *Let G be a finite 2-group with $d \geq 2$ generators, and let $K = \mathbb{Q}(\zeta_{2^n})$ or $\mathbb{Q}(\zeta_{2^{n+1}} - \zeta_{2^{n+1}}^{-1})$ where $2^{n-2} + 1 \geq d$. Then G can be realized as a 2-ramified Galois group over K.*

Proof. In both cases K is 2-ramified with degree $[K : \mathbb{Q}] = 2^{n-1}$, so that $K \subseteq \mathbb{Q}_S(2)$ for $S = \{2\}$. It follows that K is a 2-rational number field (in the notation introduced in [7]). By assumption $n \geq 2$ (as $d \geq 2$), so that K is totally imaginary admitting 2^{n-2} complex places. Hence from [7, Theorem 0] it follows that $\mathrm{Gal}(\mathbb{Q}_S(2)/K)$ is a free pro-2-group of rank $2^{n-2} + 1$. Now use that $2^{n-2} + 1 \geq d$ by hypothesis. ∎

For the special case $d = n = 2$ see also [16, Exercise (f) in Section I.4.1]. So every 2-generator 2-group can be realized as a 2-ramified Galois group over $\mathbb{Q}(i)$ and $\mathbb{Q}(i\sqrt{2})$.

3. Central group and field extensions. Let G be a finite group. The Schur multiplier of G is defined as $M(G) = H_2(G, \mathbb{Z})$ (often identified with its character group $H^2(G, \mathbb{C}^*)$). If $R \rightarrowtail \Gamma \twoheadrightarrow G$ is any free presentation of G, by the celebrated Hopf–Schur formula we have

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

(see [8, Hauptsatz V.23.5]). Of course $M(G)$ is finite of exponent dividing $|G|$. Let $C \rightarrowtail X \twoheadrightarrow G$ be a *central* extension of G (with $C \subseteq Z(X)$). Then we may choose Γ such that it maps onto X, and the universal property of free groups gives rise to the natural exact sequence

$$C \otimes X/X' \to M(X) \to M(G) \xrightarrow{\varrho} C \to X/X' \to G/G' \to 1$$

(see e.g. [1, Lemma 4.1]). Here $C \otimes X/X' \to M(X)$ is the so-called Ganea map, and the remainder is known as the 5-term exact homology sequence, $\varrho : M(G) \to C = H_1(C, \mathbb{Z})$ being the transgression map. The extension is called *stem* if ϱ is an epimorphism, that is, if $C \subseteq X'$, and it is a *Schur cover* of G (sometimes called covering or representation group, or stem cover) if ϱ is an isomorphism. (So X is a Schur cover of G provided $C \subseteq X' \cap Z(X)$ and $|C| = |M(G)|$.)

LEMMA 3.1. *If X is a Schur cover of the group G, then $M(X)$ is an epimorphic image of $M(G) \otimes G/G'$.*

This is immediate from the above exact sequence noting that ϱ is an isomorphism (and $X/X' \cong G/G'$). Using that $R/(R \cap \Gamma') \cong R\Gamma'/\Gamma'$ is a free abelian group, there exist complements $T/[R, \Gamma]$ to $(R \cap \Gamma')/[R, \Gamma] \cong M(G)$ in $R/[R, \Gamma]$, so that Γ/T is a Schur cover of G. Indeed, all Schur covers may be obtained in this way (up to isomorphism).

Schur's theory nicely extends from the category of finite groups to that of profinite groups. If $R \rightarrowtail \Gamma \twoheadrightarrow G$ is a free presentation of a profinite group G, then we may describe (and define) $M(G)$ by the very same Hopf–Schur formula (taking topological closures for the commutator groups). In particular $M(\Gamma) = 0$ if Γ is a free profinite group.

LEMMA 3.2. *Let Γ be a profinite group. Then $M(\Gamma) = 0$ if and only if $M(\Gamma/R) \cong (R \cap \Gamma')/[R, \Gamma]$ for all open normal subgroups R of Γ.*

The proof is standard (cf. Fröhlich [6, Proposition 4.1]).

PROPOSITION 3.3. *If G is a finite 2-group belonging to $\mathcal{K}_2$, then also some Schur cover of G belongs to $\mathcal{K}_2$. In fact, given $K \in \mathcal{K}_2(G)$ there are exactly $|M(G)|$ normal number fields $L \supseteq K$ such that $\mathrm{Gal}(L/\mathbb{Q})$ is a Schur cover of G of this kind. These fields L are the maximal central extensions of $K/\mathbb{Q}$ which are unramified outside $\{2, \infty\}$ and contain the same roots of unity as K.*

Proof. Let $\Gamma = G_S(2)$ be the Galois group of the maximal 2-extension of the rationals unramified outside $\{2, \infty\}$ ($S = \{2\}$). Then $\Gamma/\Gamma' \cong \mathbb{Z}_2 \oplus Z_2$ (as seen in the previous section). From Theorem 4.9 and Proposition 4.2 in [6] it follows that $M(\Gamma) = 0$. Regarding $G = \Gamma/R$ as a quotient group of Γ we therefore have $M(G) \cong (R \cap \Gamma')/[R, \Gamma]$ by Lemma 3.2. Let K be the fixed field of R on $\mathbb{Q}_S(2)$ (so that $G = \mathrm{Gal}(K/\mathbb{Q})$). Recall that every finite-index subgroup of Γ is open (and closed).

Without loss we may assume that G is not cyclic (otherwise $M(G) = 0$). Then $G/G' \cong \Gamma/R\Gamma'$ is not cyclic. We infer that $R/(R \cap \Gamma') \cong R\Gamma'/\Gamma'$ is isomorphic to $\mathbb{Z}_2$ (which is the free pro-2-group of rank 1). Hence there are complements $T/[R, \Gamma]$ to $(R \cap \Gamma')/[R, \Gamma] \cong M(G)$ in $R/[R, \Gamma]$, and the number of these complements equals $|\mathrm{Hom}(\mathbb{Z}_2, M(G))| = |M(G)|$. For such a complement T the group $X = \Gamma/T$ is a central extension of $G = \Gamma/R$ where $R/T \subseteq X'$ (as $T\Gamma' = R\Gamma'$) and $R/T \cong M(G)$. Hence X is a Schur cover of G. The fixed field L of T on $\mathbb{Q}_S(2)$ is a 2-ramified normal number field $L \supseteq K$ with $X = \mathrm{Gal}(L/\mathbb{Q})$. From $\mathrm{Gal}(L/K) \subseteq X'$ we infer that each root of unity contained in L already is in K (Kronecker–Weber).

Conversely, if L_0 is a central extension of $K/\mathbb{Q}$ which is 2-ramified and contains the same roots of unity (of 2-power order) as K, then $X_0 = \mathrm{Gal}(L_0/\mathbb{Q})$ is a stem extension of G and $X_0 = \Gamma/T_0$ for some normal subgroup $T_0 \subseteq R$ of Γ satisfying $T_0\Gamma' = R\Gamma'$. It follows that $T_0/(T_0 \cap \Gamma') \cong \mathbb{Z}_2$ and that there is a complement $T/[R, \Gamma]$ to $(T_0 \cap \Gamma')/[R, \Gamma]$ in $T_0/[R, \Gamma]$. Thus X_0 is an epimorphic image of the Schur cover $X = \Gamma/T$ of G belonging to $\mathcal{K}_2$ and $L_0 \subseteq L$ where L is the fixed field of T. This completes the proof. ∎

Example 3.4. Let $G = D_4 = Z_2 \oplus Z_2$ be the noncyclic group of order 4. Then $\mathcal{K}_2(G) = \{\mathbb{Q}(\zeta_8)\}$ and $|M(G)| = 2$. Indeed, up to isomorphism Q_8 and D_8 are the unique Schur covers of G (see below). Since Q_8 does not belong to $\mathcal{K}_2$ (Lemma 2.1), there are just $|M(G)| = 2$ distinct 2-ramified normal number fields E_3 and F_3 (say) with group D_8. These fields cannot be cyclic over $\mathbb{Q}(\sqrt{2})$, for otherwise complex conjugation would give the unique central involution in the Galois groups. The splitting field of the polynomial X^4-2 over the rationals must be one of these fields, say E_3. Then $E_3 = \mathbb{Q}(i, \sqrt{4})$ is cyclic over $\mathbb{Q}(i)$. Let $\widetilde{E}_3$ be the unique proper intermediate field between $\mathbb{Q}(\zeta_8)$ and $E_3(\zeta_{16})$ different from E_3 and from $\mathbb{Q}(\zeta_{16})$. Then $\widetilde{E}_3$ is 2-ramified and nonabelian over $\mathbb{Q}$ of degree 8. Consequently, $F_3 = \widetilde{E}_3$, and this is cyclic over $\mathbb{Q}(i\sqrt{2})$.

4. Some distinguished 2-groups. By a classical result of Olga Taussky a finite nonabelian 2-group G with $|G : G'| = 4$ is isomorphic to Q_{2^n}, D_{2^n} or SD_{2^n} for some n (see [8, Satz III.11.9]). These are the (nonabelian) 2-groups of maximal class. We infer that we must have $G' = \Phi(G)$, $Z(G) \subseteq G'$ and

$|Z(G)| = 2$. Moreover, $M(G/Z(G))$ has order 2. It is easy to see that the centre quotient groups of Q_{2^n}, D_{2^n} and SD_{2^n} are all dihedral, so that these groups are all the distinct Schur covers of $D_{2^{n-1}}$ up to isomorphism. (For $n = 3$ we identify $SD_8 = D_8$, and D_4 is the elementary group of order 4.) We may also deduce that Q_{2^n} for $n \geq 3$ and SD_{2^n} for $n \geq 4$ have trivial Schur multiplier (which of course is well known). By Lemma 2.1 we have $\mathcal{K}_2(Q_{2^n}) = \emptyset$.

We are going to define the semimodular group SM_{2^n} as a fibre product of D_8 and an abelian group of type $(2^{n-2}, 2)$. This will enable us to determine $\mathcal{K}_2(SM_{2^n})$ quite easily.

LEMMA 4.1. *Let $G = D_{2^r}$ for some $r \geq 3$, and let A be an abelian group of type $(2^{n-2}, 2)$ for some $n \geq 4$. Up to isomorphism there is a unique fibre product $H = G \curlywedge A$ of G and A amalgamating the Frattini quotients and admitting a noncentral involution. The centre $Z(H)$ is of type $(2^{n-3}, 2)$, H' is cyclic of order 2^{r-2} and $|Z(H) \cap H'| = 2$. There are just two conjugacy classes of noncentral involutions in H, which are all outside $\Phi(H) = Z(H) \cdot H'$.*

Proof. Two of the three elements of order 2 in G/G' result from noncentral involutions y, y' in G which are not conjugate (and are outside G'), the remaining one from a generator x of the unique cyclic subgroup of G of index 2. Let $A = \langle a \rangle \times \langle b \rangle$ with a of order 2^{n-2} and b of order 2. Two of the three elements of order 2 in $A/\Phi(A)$ come from elements of order 2^{n-2} of A, namely from a and ab, the remaining one from an involution, namely from b or $a^{2^{n-3}}b$. Let V be an elementary group of order 4. There are group epimorphisms γ, δ from G and A to V, respectively, such that $\gamma(y) = \delta(b)$ $(= \delta(a^{2^{n-3}}b))$. Let $H = G \curlywedge A$ be the fibre product (pullback) of G and A with respect to these epimorphisms, regarded as a subgroup of the direct product $G \times A$.

The centre $Z(H)$ of H maps onto $Z(G)$, which has order 2 and is contained in $G' = \Phi(G)$. Thus $Z(H)$ and H' have the asserted structures. Also, $\Phi(H) = Z(H)H'$ and $|Z(H) \cap H'| = 2$. By construction H admits the involutions (y, b) and $(y, a^{2^{n-3}}b)$, which are not contained in $\Phi(H)$ and are not conjugate in H. These represent the two distinct conjugacy classes of noncentral involutions in H.

It remains to prove uniqueness of H. There is a (noninner) automorphism of $G = D_{2^r}$ centralizing x and sending y to y', and there is an automorphism of A centralizing a and mapping b to $a^{2^{n-3}}b$. Hence uniqueness of H, up to isomorphism, follows from the universal property of a pullback. ∎

The above fibre product $H = G \curlywedge A$ belongs to $\mathcal{K}_2$ (Theorem 0). Indeed, if K is a field in $\mathcal{K}_2(G)$, then $K(\zeta_{2^n})$ is in $\mathcal{K}_2(H)$ (noting that $\mathcal{K}_2(A) =$

$\{\mathbb{Q}(\zeta_{2^n})\}$). There are other such fibre product constructions of groups belonging to $\mathcal{K}_2$, determining the composita of corresponding fields of realization.

DEFINITION. The fibre product $SM_{2^n} = D_8 \leftthreetimes (Z_{2^{n-2}} \times Z_2)$ (in the above sense) is called the *semimodular group* of order 2^n ($n \geq 4$).

LEMMA 4.2. *Let $n \geq 4$. The semimodular group $G = SM_{2^n}$ is characterized by any of the following equivalent conditions:*

(i) *G has order 2^n and a noncentral involution but no cyclic subgroup of index 2, and $Z(G) = \Phi(G)$ has order 2^{n-2}.*
(ii) *G is a Schur cover of an abelian group of type $(2^{n-2}, 2)$ and has two distinct conjugacy classes of noncentral involutions.*

Proof. For $G = SM_{2^n}$ we have $Z(G) = \Phi(G)$ by definition and Lemma 4.1, and this has index 4 in G. Further G' has order 2 and G/G' is of type $(2^{n-2}, 2)$, and G has just two conjugacy classes of noncentral involutions. In order to get (ii) use that the Schur multiplier of an abelian group of type $(2^{n-2}, 2)$ has order 2 by the Künneth theorem [8, Satz V.25.10].

If G is a group of order 2^n for which $Z(G) = \Phi(G)$ has order 2^{n-2}, then necessarily $|G'| = 2$, and G/G' is of type $(2^{n-2}, 2)$ if there is a noncentral involution in G. Also, if G is a Schur cover of an abelian group of type $(2^{n-2}, 2)$, then $Z(G) = \Phi(G)$ $(= G^2)$ has order 2^{n-2} by Theorem 3.2 and Proposition 7.3 in [1]. If in addition G has two conjugacy classes of noncentral involutions, G cannot be of type M_{2^n} and so has no cyclic subgroup of index 2.

In both cases (i), (ii) therefore G has a cyclic subgroup $X = \langle x \rangle$ of order 2^{n-2} such that $X \cap G' = 1$, and an involution y such that $G/G' = XG'/G' \times \langle G'y \rangle$. Then $N = X \cap \Phi(G) = X \cap Z(G)$ is a normal subgroup of G and G/N is nonabelian of order 8. We must have $G/N \cong D_8$ (as it belongs to $\mathcal{K}_2$), so that $G \cong D_8 \leftthreetimes A$ where $A \cong G/G'$ is of type $(2^{n-2}, 2)$. This completes the proof. ∎

LEMMA 4.3. *Suppose G is a finite nonabelian 2-group belonging to $\mathcal{K}_2$. Assume that $|G : G'| = 2^{n-1}$ for some $n \geq 4$. Then G has a unique normal subgroup G^* having index 2 in G', and G/G^* is isomorphic either to M_{2^n} or to SM_{2^n}.*

Proof. We know that G/G' is of type $(2^{n-2}, 2)$. Hence $M(G/G')$ has order 2. Clearly there is a normal subgroup G^* of G having index 2 in G'. Then $\bar{G} = G/G^*$ is a Schur cover of G/G'. By hypothesis, $\bar{G}$ belongs to $\mathcal{K}_2$. Hence there is an involution in $\bar{G}$ outside $\Phi(\bar{G})$ by Lemma 2.1.

If $\bar{G}$ has a cyclic normal subgroup of index 2, then $\bar{G} \cong M_{2^n}$. Otherwise $\bar{G}$ is isomorphic to the semimodular group SM_{2^n} by Lemma 4.2.

It remains to prove the uniqueness statement for G^*. Assume there is a further normal subgroup $G^\diamond$ of G having index 2 in G'. Then $N = G^* \cap G^\diamond$ is a normal subgroup of G having index 4 in G'. Clearly G'/N is in the centre of G/N. Thus G/N is a stem extension of G/G' and so $|M(G/G')|$ divisible by 4. However, this is not true. ∎

Proof of Theorem 1. It suffices to consider nonabelian groups. If G is a nonabelian 2-group belonging to $\mathcal{K}_2$ which is neither dihedral nor semidihedral, then by Lemma 4.3 there is a unique normal subgroup G^* of G having index 2 in G', and G/G^* is isomorphic to M_{2^n} or to SM_{2^n} for some $n \geq 4$. Assume $G^* \neq 1$. We assert that then $G/G^* \cong SM_{2^n}$. Assume that this is false. There is a normal subgroup N of G having index 2 in G^*. Since $G^* \subseteq G'$, the central extension $Z_2 \rightarrowtail G/N \twoheadrightarrow G/G^* \cong M_{2^n}$ is *stem*, and this implies that the Schur multiplier of M_{2^n} is not trivial. However this is not true. In fact, the (metacyclic) group M_{2^n}, having two distinct cyclic subgroups of index 2, can be presented by the generators x, y and the relations $x^{2^{n-1}} = 1$, $y^2 = x^2$ and $x^y = x^{1+2^{n-2}}$. Now [1, Proposition 9.2] applies.

Thus $G/G^* \cong SM_{2^n}$, and from Lemma 2.1 it follows that some involution of G must map to a noncentral involution of G/G^*. Conversely, from Theorem 0 we see that the groups described in (ii) belong to $\mathcal{K}_2$, and if (iii) holds, then either $G \cong SM_{2^n}$ for some $n \geq 4$, where Theorem 0 applies again, or G has a unique normal subgroup $G^* \neq 1$ having index 2 in G' and $G/G^* \cong SM_{2^n}$ for some $n \geq 4$ (as seen above). In the latter case by hypothesis some involution in G maps to a noncentral involution of G/G^*. Since the Frattini quotient groups of G and G/G^* are isomorphic (of order 4), application of Theorem 0 shows that G belongs to $\mathcal{K}_2$ also in case (iii). ∎

For convenience we give presentations $G = \langle x, y \mid R \rangle$ of the 2-generator 2-groups we are concerned here, as well as the structure of the multiplier $M(G)$.

G	R	MG
Q_{2^n}	$x^{2^{n-2}} = y^2,\ x^y = x^{-1}$	0
D_{2^n}	$x^{2^{n-1}} = y^2 = 1,\ x^y = x^{-1}$	Z_2
SD_{2^n}	$x^{2^{n-1}} = y^2 = 1,\ x^y = x^{-1+2^{n-2}}$	0
M_{2^n}	$x^{2^{n-1}} = y^2 = 1,\ x^y = x^{1+2^{n-2}}$	0
SM_{2^n}	$x^{2^{n-2}} = y^2 = [x, y, x] = [x, y, y] = 1$	$Z_2 \oplus Z_2$

Here $n \geq 3$ for the quaternion and dihedral groups, and $n \geq 4$ otherwise. We use the commutators $[x, y] = x^{-1}y^{-1}xy = x^{-1}x^y$ and $[x, y, z] = [[x, y], z]$. To obtain the presentation of M_{2^n} used above one has to replace y by xy and x by $x^{1+2^{n-3}}$. The presentation of SM_{2^n} is obtained by taking x, y as in the proof of Lemma 4.2.

It remains to show that $M(SM_{2^n}) \cong Z_2 \oplus Z_2$. We know that SM_{2^n} is a Schur cover of the abelian group A of type $(2^{n-2}, 2)$. Hence by Lemma 3.1 its Schur multiplier is an epimorphic image of $M(A) \otimes A \cong Z_2 \oplus Z_2$. By definition and by Example 3.4, $E_3(\zeta_{2^n}) = F_3(\zeta_{2^n})$ is a field in $\mathcal{K}_2(SM_{2^n})$. The fields E_3, F_3 are ring class fields, and from Lemma 5.3 below it will follow that $\mathrm{Gal}(E_4F_4(\zeta_{2^n})/\mathbb{Q})$ represents a central stem extension of SM_{2^n} with kernel of order $[E_4F_4 : E_3F_3] = 4$. Hence the result.

5. Ring class fields. For convenience we summarize some basic facts needed in this paper. Let K be an imaginary quadratic number field, and let $\mathfrak{o}$ be an order in K with *conductor* f, that is, $f = |\mathfrak{o}_K : \mathfrak{o}|$ where $\mathfrak{o}_K$ is the maximal order in K. Then, by class field theory, one can associate to $\mathfrak{o}$ an abelian extension L/K such that $\mathrm{Gal}(L/K) \cong \mathrm{Cl}(\mathfrak{o})$, where the ideal class group $\mathrm{Cl}(\mathfrak{o})$ has order

$$h(\mathfrak{o}) = \frac{h(\mathfrak{o}_K)f}{|\mathfrak{o}_K^* : \mathfrak{o}^*|} \prod_{p|f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right)$$

(see [4, Theorem 7.24]); here $\left(\frac{\cdot}{p}\right)$ denotes the Kronecker symbol, which vanishes if p is ramified in K, and d_K is the discriminant of K (or $\mathfrak{o}_K$). One knows that L is Galois over $\mathbb{Q}$ and that the conductor $\mathfrak{f}(L/K)$ in the sense of class field theory agrees with $f\mathfrak{o}_K$ when 2 is ramified in K, except when $f = 2$ and $K = \mathbb{Q}(i)$. (In the exceptional case $\mathfrak{o} = \mathbb{Z}[2i]$ has class number 1.) By the Ramification Theorem of class field theory just the primes (places) dividing the conductor are ramified in the corresponding class field. If $K = \mathbb{Q}(\sqrt{-d})$ for some positive integer d and $\mathfrak{o} = \mathbb{Z}[\sqrt{-d}]$, then $-4d$ is the discriminant of $\mathfrak{o}$ and so $-4d = f^2 d_K$. Using the fact that $h(\mathfrak{o}_K) = 1$ for $K = \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(\sqrt{-2^{2n}})$ and for $\mathbb{Q}(\sqrt{-2}) = \mathbb{Q}(\sqrt{-2^{2n+1}})$ this yields the following.

LEMMA 5.1 *Let E_n be the ring class field of $\mathbb{Z}[2^n i]$ in $\mathbb{Q}(i)$, and let F_n be the ring class field of $\mathbb{Z}[2^{n-1}i\sqrt{2}]$ in $\mathbb{Q}(i\sqrt{2})$ $(n \geq 1)$. Then E_n, F_n are 2-ramified Galois extensions of the rationals of degree 2^n.*

We observe that $E_1 = \mathbb{Q}(i)$, $F_1 = \mathbb{Q}(i\sqrt{2})$ and $E_2 = F_2 = \mathbb{Q}(\zeta_8)$. One knows that the Galois group of a ring class field L to some order in K over the rationals is *generalized* dihedral, that is, a semidirect product of the abelian group $A = \mathrm{Gal}(L|K)$ by some group $\langle y \rangle$ of order 2 where y inverts the elements of A [4, Lemma 9.3]. In the present situation A is even cyclic:

LEMMA 5.2. *Both E_n and F_n have D_{2^n} as Galois group over the rationals, where E_n is cyclic over $\mathbb{Q}(i)$ and F_n over $\mathbb{Q}(i\sqrt{2})$ $(n \geq 3)$. In particular, E_n and F_n do not contain the 16th roots of unity.*

Proof. Let $G = \mathrm{Gal}(E_n/\mathbb{Q})$; F_n is treated similarly. Then $A = \mathrm{Gal}(E_n/\mathbb{Q}(i))$ is an abelian subgroup of G of index 2 and $G = A\langle y\rangle$ for some involution y inverting the elements of A. Thus $(ay)^2 = a(yay) = aa^y = aa^{-1} = 1$ for all $a \in A$. Consequently, $\Phi(G) = G^2 = A^2$ has index $2|A : A^2|$ in G. By Lemma 5.1 we know that G belongs to $\mathcal{K}_2$. Hence $|G : \Phi(G)| = 4$ by Lemma 2.1. This implies that $|A : A^2| = 2$, and therefore A is cyclic. The last statement follows from the Kronecker–Weber theorem. ∎

LEMMA 5.3. *For $n, m \geq 3$ we have $E_n \cap F_m = \mathbb{Q}(\zeta_8)$, and the compositum E_nF_m contains the 2^4th but not the 2^5th roots of unity.*

Proof. Let $K = E_n \cap F_m$. We know that $K \supseteq \mathbb{Q}(\zeta_8)$. By Lemma 5.2, $\mathrm{Gal}(K/\mathbb{Q})$ has two distinct cyclic subgroups of index 2, namely $\mathrm{Gal}(K/\mathbb{Q}(i))$ and $\mathrm{Gal}(K/\mathbb{Q}(i\sqrt{2}))$. This forces that $\mathrm{Gal}(K/\mathbb{Q})$, being an epimorphic image of a dihedral 2-group, is elementary of order 4, whence $K = \mathbb{Q}(\zeta_8)$.

Let $L = E_nF_m$ and $G = \mathrm{Gal}(L/\mathbb{Q})$. By Lemma 5.1, L is 2-ramified, so that $\mathbb{Q}(\zeta_8)$ is the fixed field of $\Phi(G)$ (Lemma 2.1). Let $N = \mathrm{Gal}(L/E_n)$ and $M = \mathrm{Gal}(L/F_m)$. By the preceding paragraph, $\Phi(G) = N \times M$. Now G' is a proper subgroup of $\Phi(G)$, because otherwise G is of maximal class by Taussky's theorem (and so dihedral or semidihedral). On the other hand, $[N, G]$ has index 2 in N since $N \cong \Phi(G)/M$ as G-modules and $G/M \cong D_{2^m}$ is of maximal class. Similarly $|M : [M, G]| = 2$. Using the fact that $G' \supseteq [\Phi(G), G] = [N, G] \times [M, G]$ and $NG' = \Phi(G) = MG'$ (as G/N and G/M are dihedral) we obtain $|\Phi(G) : G'| = 2$. Hence G/G' has order 8, giving the result (in view of Kronecker–Weber). ∎

REMARK. Clearly $E_n \subset E_{n+1}$ and $F_n \subset F_{n+1}$ for all n. Let $E_\infty = \bigcup_{n\geq 1} E_n$, and define F_∞ similarly. Then, besides the cyclotomic $\mathbb{Z}_2$-extension, E_∞ is the unique further $\mathbb{Z}_2$-extension of $E_1 = \mathbb{Q}(i)$ (in agreement with the Leopoldt conjecture). A similar statement holds for $F_1 = \mathbb{Q}(i\sqrt{2})$ and F_∞. Both E_∞ and F_∞ are normal over $\mathbb{Q}$ having a pro-dihedral Galois 2-group, and $E_\infty \cap F_\infty = \mathbb{Q}(\zeta_8)$.

6. Proof of Theorem 2. We have to determine the fields in $\mathcal{K}_2(G)$ for the groups $G = D_{2^n}$, SD_{2^n}, M_{2^n} and SM_{2^n}. In view of Example 3.4 we may assume that $n \geq 4$. Recall that both D_{2^n} and SD_{2^n} are Schur covers of $D_{2^{n-1}}$, and both M_{2^n} and SM_{2^n} are Schur covers of an abelian group of type $(2^{n-2}, 2)$.

$\{D_{2^n}, SD_{2^n}\}$: It follows from Lemmas 5.1 and 5.2 that $\mathcal{K}_2(D_{2^n}) \supseteq \{E_n, F_n\}$. By Lemma 2.3 we must have equality. This may also be obtained on the basis of Proposition 3.3, arguing by induction. The fields $\widetilde{E}_n$, $\widetilde{F}_n$, defined in the Introduction, are normal over the rationals of degree 2^n, and they are unramified outside $\{2, \infty\}$. Moreover, the fields do not contain the

16th root of unity (but the 8th ones). It follows that their Galois groups over the rationals are either dihedral or semidihedral. By Lemma 5.3 the fields are distinct from E_n, F_n. Hence

$$\{\widetilde{E}_n, \widetilde{F}_n\} \subseteq \mathcal{K}_2(SD_{2^n}).$$

This inclusion again must be an equality, because if $L \in \mathcal{K}_2(SD_{2^n})$, then L must contain one of E_{n-1} or F_{n-1}, and Proposition 3.3 implies that $L = \widetilde{E}_n$ or $L = \widetilde{F}_n$.

$\{M_{2^n}, SM_{2^n}\}$: Let A be an abelian group of type $(2^{n-2}, 2)$, and let $K = \mathbb{Q}(\zeta_{2^n})$. We know that $\mathcal{K}_2(A) = \{K\}$. By Proposition 3.3 (and Theorem 0), M_{2^n} and SM_{2^n} are the unique Schur covers of A belonging to $\mathcal{K}_2$, and both $\mathcal{K}_2(M_{2^n}) = \{\widetilde{L}\}$ and $\mathcal{K}_2(SM_{2^n}) = \{L\}$ must consist of single fields (as the groups are not isomorphic). We assert that $L = K(\sqrt[4]{2})$ and that $\widetilde{L} = \mathbb{Q}(\sqrt[4]{2} \cdot \zeta_{2^{n+1}})$.

It follows from the definition of SM_{2^n}, as a fibre product of D_8 and A, that $L = E_3(\zeta_{2^n})$. We have already seen that E_3 is the splitting field of X^4-2 over the rationals (Example 3.4). Consequently L is as asserted. Now $\widetilde{L}$ must be the unique field properly between K and $L(\zeta_{2^{n+1}})$ but different from L and from $\mathbb{Q}(\zeta_{2^{n+1}})$. It follows that $\widetilde{L}$ is generated over K by $\alpha = \sqrt[4]{2} \cdot \zeta_{2^{n+1}}$. Since $\sqrt{2} \in \mathbb{Q}(\zeta_8) \subset K$ we see that $K = \mathbb{Q}(\alpha^2)$ and $\widetilde{L} = \mathbb{Q}(\alpha)$. This completes the proof. ∎

Remark. The maximal subgroups of SD_{2^n} are cyclic, dihedral and quaternion. Now $\widetilde{E}_n$ is cyclic over $\mathbb{Q}(i)$ (as is E_n) and cannot be quaternion over $\mathbb{Q}(\sqrt{2})$. Thus $\widetilde{E}_n$ is quaternion over $\mathbb{Q}(i\sqrt{2})$. A similar statement holds for $\widetilde{F}_n$. (The noncyclic maximal subgroups of D_{2^n} are dihedral.)

7. Some defining polynomials. The field $L = \mathbb{Q}(\sqrt[4]{2}, \zeta_{2^n})$ appearing in the statement of Theorem 2 is the splitting field of the binomial $X^{2^n} - 2^{2^{n-2}} = (X^{2^{n-1}} - 2^{2^{n-3}})(X^{2^{n-1}} + 2^{2^{n-3}})$ over the rationals ($n \geq 4$). For if β is a root of the first factor and γ of the second one, then $(\gamma/\beta)^{2^{n-1}} = -1$ and so γ/β is a primitive 2^nth root of unity. The splitting field contains $\sqrt[4]{2}$ and has degree 2 over $\mathbb{Q}(\zeta_{2^n})$ by Kummer theory (as $\sqrt{2} \in \mathbb{Q}(\zeta_{2^n})$).

The field $\widetilde{L} = \mathbb{Q}(\sqrt[4]{2} \cdot \zeta_{2^{n+1}})$ is the splitting field of the normal binomial $f = X^{2^n} + 2^{2^{n-2}}$ over the rationals ($n \geq 4$). Just observe that $\alpha = \sqrt[4]{2} \cdot \zeta_{2^{n+1}}$ is a root of f, and that we know from Theorem 2 that $\widetilde{L}$ is Galois over the rationals of degree 2^n. (For a direct proof note that f is irreducible over $\mathbb{Q}$, because $a = -2^{2^{n-2}}$ is not a rational square and $a \notin -4\mathbb{Q}^4$. Further $(\alpha^4/2)^{2^{n-2}} = \alpha^{2^n}/2^{2^{n-2}} = -1$. Hence $\alpha^4/2$ is a primitive 2^{n-1}th root of unity contained in $\mathbb{Q}(\alpha)$. In particular $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2}) \subseteq \mathbb{Q}(\alpha)$. Now $(\alpha^2/\sqrt{2})^2 = \alpha^4/2$ and so even $\mathbb{Q}(\zeta_{2^n}) \subseteq \mathbb{Q}(\alpha)$.)

In principle the minimal polynomials over the rationals of the real algebraic integers $\gamma_2(2^n i)$ and $\gamma_2(2^{n-1} i\sqrt{2})$ can be computed on the basis of [14, Theorem 6.3.1]. Their splitting fields are E_n respectively F_n ($n \geq 3$). However, the absolute values of the coefficients (except the leading ones) of these polynomials increase very rapidly with n. One might suspect that certain (*double*) *η-quotients* as described in Sections 6.4 and 6.6 of [14] give rise to simpler generators (Schertz).

LEMMA. *Suppose that* $E_n = \mathbb{Q}(\zeta_8, \alpha)$ *for some* α *satisfying* $\alpha^2 \in E_{n-1}$ ($n \geq 3$). *Then* $\widetilde{E}_n = \mathbb{Q}(\zeta_8, \zeta_{16} \cdot \alpha)$. *An analogous statement holds for* F_n, $\widetilde{F}_n$.

Proof. Let $K = \mathbb{Q}(\zeta_8, \zeta_{16} \cdot \alpha)$. We know that E_{n-1} and E_n contain the 8th but not the 16th roots of unity (as $n \geq 3$). It follows that $K \not\subseteq E_n = \mathbb{Q}(\zeta_8, \alpha)$. By assumption $(\zeta_{16} \cdot \alpha)^2 = \zeta_8 \cdot \alpha^2 \in E_{n-1}(\zeta_8) = E_{n-1}$. We infer that $E_{n-1} = \mathbb{Q}(\zeta_8, \alpha^2) \subseteq K$ and that $[K : E_{n-1}] = 2$. We have $K \neq E_{n-1}(\zeta_{16})$, because otherwise $K = \mathbb{Q}(\zeta_{16}, \alpha) = E_n(\zeta_{16})$. Clearly $K \subseteq E_n(\zeta_{16})$. Hence $K = \widetilde{E}_n$ by definition. ∎

E_3: The minimal polynomial of $\gamma_2(8i)$ over $\mathbb{Q}$ is $X^4 - 18909120X^3 - 2115244152X^2 - 72777744864X - 1021025075202$. However, we already know that E_3 is the splitting field of $X^4 - 2$ over the rationals (see also [4, Proposition 9.5]). Since $2^3 = (-2)(1+i)^4$, by Kummer theory it is the splitting field of $X^4 + 2$ as well.

F_3: The minimal polynomial of $\gamma_2(4i\sqrt{2})$ over $\mathbb{Q}$ is $X^4 - 139760X^3 - 112700X^2 - 329092000X - 7016042500$. But we know that $F_3 = \widetilde{E}_3$ and that $E_3 = \mathbb{Q}(i, \alpha)$ where $\alpha = \sqrt[4]{2}$. Let $\beta = \zeta_{16} \cdot \alpha$. Then $\beta^2 = \zeta_8\sqrt{2} = 1 + i$ and $(\beta^2 - 1)^2 = i^2 = -1$, and $\alpha^2 = \sqrt{2} \in E_2$. Hence $\widetilde{E}_3 = \mathbb{Q}(\zeta_8, \beta)$ by the above lemma. Now β is a root of $X^4 - 2X^2 + 2$ (which is $(X^2 - (1+i))(X^2 - (1-i))$ over $\mathbb{Q}(i)$). The splitting field of this polynomial contains i and $\sqrt{2}$, hence ζ_8. Consequently, F_3 is the splitting field of $X^4 - 2X^2 + 2$.

E_4: We do not give the polynomial for $\gamma_2(16i)$ (since it would take too much space, e.g. 29 digits for the constant term, and since we have a simpler generator). Indeed, we claim that E_4 is (also) the splitting field of $f = X^8 + 2$ over $\mathbb{Q}$. Let K denote this splitting field, and let $\alpha \in K$ be a root of f. Of course f is irreducible over $\mathbb{Q}$ and its discriminant is divisible only by the prime 2. Hence K is 2-ramified. Since

$$f = (X^4 - i\sqrt{2})(X^4 + i\sqrt{2})$$

over $\mathbb{Q}(i\sqrt{2})$, and since $(i\sqrt{2})^5 = -i\sqrt{2}(1+i)^4$ is not a square in $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, i\sqrt{2})$, by Kummer theory $K/\mathbb{Q}(\zeta_8)$ is cyclic of degree 4. Now α^2 is a root of $X^4 + 2$, so that $\mathbb{Q}(i, \alpha^2) = E_3$ as seen above. Of course E_3 is cyclic over $\mathbb{Q}(i)$. It follows that $K = E_3(\alpha)$ is cyclic over $\mathbb{Q}(i)$, because $G = \mathrm{Gal}(K/\mathbb{Q}(i))$ is a group of order 8 having normal subgroups $X \subset Y$

such that G/X and Y are cyclic of order 4. The above decomposition of f over $\mathbb{Q}(i\sqrt{2})$ shows that $K/\mathbb{Q}(i\sqrt{2})$ is dihedral. We know that K cannot be quaternion over $\mathbb{Q}(\sqrt{2})$ (as K is 2-ramified). Consequently, $\mathrm{Gal}(K/\mathbb{Q}) \cong D_{16}$ and $K = E_4$ (Lemma 5.2).

$\widetilde{E}_4$: Since $E_4 = \mathbb{Q}(i, \alpha)$ where $\alpha^8 = -2$ and $(\zeta_{16} \cdot \alpha)^8 = 2$, and since $\alpha^2 \in E_3$, from the lemma it follows that $\widetilde{E}_4$ is the splitting field of $X^8 - 2$ over the rationals.

F_4: We finally give the minimal polynomial of $\gamma_2(8i\sqrt{2})$ over the rationals:

$$\begin{aligned} X^8 &- 19533082240X^7 - 106834200105200X^6 - 182265445467992000X^5 \\ &- 5911248911063839750 0X^4 - 1896606188766024800000X^3 \\ &- 270260620352248185000 00X^2 - 22473773104031915000000 0X \\ &- 9306960658513592851562500. \end{aligned}$$

Acknowledgements. The author is indebted to Reinhard Schertz for his assistance in computing the minimal polynomials of $\gamma_2(2^n i)$ and $\gamma_2(2^{n-1}i\sqrt{2})$ over the rationals.

References

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

[2] N. Boston and C. Leedham-Green, *Explicit computation of Galois groups unramified at p*, J. Algebra 256 (2002), 402–413.

[3] N. Boston and D. Perry, *Maximal 2-extensions with restricted ramification*, J. Algebra 232 (2000), 664–672.

[4] D. A. Cox, *Primes of the Form $x^2 + ny^2$*, Wiley, New York, 1989.

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

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

[7] G. Gras and J.-F. Jaulent, *Note on 2-rational fields*, J. Number Theory 129 (2009), 495–498.

[8] B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967.

[9] H. Koch, *ℓ-Erweiterungen mit vorgegebenen Verzweigungsstellen*, J. Reine Angew. Math. 219 (1965), 30–61.

[10] H. Koch, *Galois Theory of p-Extensions*, Springer, New York, 2002.

[11] J. Labute and J. Mináč, *Mild pro-2-groups and 2-extensions of $\mathbb{Q}$ with restricted ramification*, J. Algebra 332 (2011), 136–158.

[12] G. N. Markšaitis, *On p-extensions with one critical number*, Izv. Akad. Nauk SSSR Ser. Mat. 20 (1963), 463–466 (in Russian).

[13] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of Number Fields*, Springer, New York, 2008.

[14] R. Schertz, *Complex Multiplication*, Cambridge Univ. Press, Cambridge, 2009.
[15] J.-P. Serre, *Topics in Galois Theory*, Jones and Bartlett, Boston, 1992.
[16] J.-P. Serre, *Galois Cohomology*, Springer, New York, 1997.
[17] I. R. Shafarevich, *Extensions with prescribed ramification points*, Inst. Études Sci. Publ. Math. 18 (1963), 463–466 (in Russian).

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

Received on 5.11.2012
and in revised form on 16.10.2013 (7253)