JOSEPH E. CARROLL

On determining the quadratic subfields of $\mathbb{Z}_2$-extensions of complex quadratic fields

Compositio Mathematica, tome 30, n° 3 (1975), p. 259-271

<http://www.numdam.org/item?id=CM_1975__30_3_259_0>
ON DETERMINING THE QUADRATIC SUBFIELDS OF
$\mathbb{Z}_2$-EXTENSIONS OF COMPLEX QUADRATIC FIELDS

Joseph E. Carroll

Abstract

If $F$ is a complex quadratic field there is normal extension $L/F$ with Galois group topologically isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ where $\mathbb{Z}_2$ is the additive group of 2-adic integers. $F(\sqrt{2})$ always lies in $L$. In this paper we attempt to determine what the other quadratic subextensions of $L/F$ are. We show how this can be done under a hypothesis which is implied by but does not imply that the 2-primary part of the ideal class group of $F$ has exponent 2.

1. Let $F$ be a complex quadratic field, $F = \mathbb{Q}(\sqrt{-d})$. Let $S$ be the set of primes of $F$ lying above 2. For $p$, a prime of $F$, let $U_p$ denote the group of units in the completion, $F_p$, of $F$ at $p$. Let $J^S$ be a subgroup of the idèle group, $J$, of $F$. By class field theory, $F^*$ corresponds to the maximal abelian 2-ramified (i.e., unramified at all primes outside $S$) extension of $F$. We can write canonically, $J^S/J^S = G \times G'$, where $G$ is a pro-2 group and $G'$ is the product of pro-$p$ groups for odd primes $p$. If $M$ is the fixed field of $G'$, then $M$ contains $L$, the composite of all $\mathbb{Z}_2$-extensions of $F$. Since Leopoldt’s Conjecture is valid for $F$, $\text{Gal}(L/F) \approx \mathbb{Z}_2 \times \mathbb{Z}_2$.

PROPOSITION (1): $G$ is a finitely generated $\mathbb{Z}_2$-module.

PROOF: It is sufficient to show that $G/G^2$ is finite [4, §6], but $G/G^2$ is the Galois group of the composite of all 2-ramified quadratic extensions of $F$. Such an extension is of the form $F(\sqrt{\beta})$ where the primes outside $S$ divide $\beta$ to an even power. Let $A$ be the subgroup of all such $\beta$ in $F^*$. Let $C_S$ be the quotient of the ideal class group, $C$, of $F$ by the subgroup
generated by classes of primes in $S$; let $U_S$ be the subgroup of elements of $F^*$ divisible only by primes in $S$. Then we have an exact sequence,

$$0 \to U_S/U_S^2 \to A/F^{*2} \xrightarrow{f} (C_S)_2 \to 0$$

where $(C_S)_2$ is the subgroup of elements of $C_S$ of exponent 2 and $f(\beta)$ is the class of the ideal whose square is $(\beta)$ up to primes of $S$. But $C_S$ is finite and $U_S/U_S^2$ is finite by the $S$-unit theorem, so $A/F^{*2}$ is finite and we are done.

2. Let $T$ be the torsion subgroup of $G$. Then $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times T$, since $G$ is a finitely generated module over a P.I.D., and $L$ is the fixed field of $T$. We must know more about $T$ in order to find the quadratic subextensions of $L$. Let $U$ denote the unit group of $F$, and let $B(2)$ be the 2 power torsion part of $B$ for any abelian group $B$. The natural continuous map $J/F^* \to C$ induces an exact sequence

$$0 \to (\prod_{q \in S} U_q)/\bar{U} \to J/F^*f^S \to C \to 0$$

and taking 2 power torsion parts we get another exact sequence

$$0 \to ((\prod_{q \in S} U_q)/\bar{U})(2) \to T \to C(2)$$

**Proposition (2):** Let $H = ((\prod_{q \in S} U_q)/\bar{U})(2)$. If $d \equiv \pm 1(8)$ and $d \neq 1$, then $H \cong \mathbb{Z}/2\mathbb{Z}$ and the sequence

$$(2') \quad 0 \to H \to T \to \text{im } T \to 0$$

splits if and only if $d \equiv -1(8)$. If $d \neq \pm 1(8)$ or $d = 1$, then $H$ is trivial.

**Proof:** Since $F$ is complex quadratic, $U$ is finite and so $U = \bar{U}$. (In fact $F^*f^S$ is closed also). Thus, if $\mu_{n,2}$ denotes the group of 2-power roots of 1 in $F_q$, $H = (\prod_{q \in S} \mu_{n,2})/\{\pm 1\}$ (if $d = 1$ we get $\{\pm i, \pm 1\}$ in the denominator). If $d \neq 1(8)$, then $\mu_{n,2} = \{\pm 1\}$ for $q \in S$ and if $d \neq -1(8)$, then $|S| = 1$. Thus $H$ is generated by $i$ if $d \equiv 1(8)$ and by $(-1, 1)$ if $d \equiv -1(8)$; otherwise $H$ is trivial. Let

$$\left(\cdots, x_{p_1}, \cdots, x_{p_2}, \cdots, x_{p_r}, \cdots\right)$$

for $p_i$ primes in $S$, denote the idèle of $F$ which has components $x_{p_i}$ in the $p_i$th slot and 1 elsewhere. If $d \equiv 1(8)$ and $q | 2$, then
so the sequence (2') does not split in this case. To complete the proof, it is enough to show that if \( d = -1(8) \) and, \( q, q' \) then would generate a pure subgroup of \( \mathbb{T} \) and (2') would split. Suppose that there is an idèle \( (x, q) \) such that

\[
\text{Then the principal ideal, } (a), \text{ is a square in } D, \text{ the ideal group of } F. \text{ Since } F \text{ is complex quadratic } N_F/Q_1 = m^2, m \in \mathbb{Q}. \text{ The equation above now yields } x_2q_2 = N_F/Q_1 = -m^2, \text{ implying the contradiction that } -1 \in \mathbb{Q}^*_2. \]

**COROLLARY (3):** If \( C_2 = C(2) \) then \( T = T_2 \) unless \( 1 \leq d \leq 1(8) \). If \( 1 = d = 1(8) \) and \( C_2 = C(2) \) then \( |T/T_2| = 2 \) and \((1 - i, \cdots)\) generates \( T/T_2 \).

**PROOF:** This is immediate from sequence (2) and Proposition 2.

In the sequence (2), \( T \) does not necessarily map onto \( C(2) \). We can, however, compute the number of cyclic factors of \( T \).

**PROPOSITION (4):** Let \( d = 0 \) if \( d = 3(8) \) or if all odd primes dividing \( d \) are congruent to \( \pm 1(8) \) and let \( d = 1 \) otherwise. Then \( |T_2| = 2^{[8]-\varepsilon-1}|C_2|. \)

**PROOF:** Since \( G \approx T \times \mathbb{Z}_2 \times \mathbb{Z}_2 \), \( |T/T^2| = \frac{1}{4}|G/G^2| \). But \( |G/G^2| = |A/F^*2| \) (recall the proof of Proposition 1), and by the sequence (1) and the \( S \)-unit theorem, \( |A/F^*2| = 2^{[8]+1}|(C_S)_2| \). Since \( T \) is finite, \( |T_2| = |T/T^2| \), so we shall be done upon proving

**LEMMA (5):** \( |C_2| = 2^\varepsilon|(C_S)_2| \) where \( \varepsilon \) is as in the statement of Proposition 4.

**PROOF:** Let \( q|2 \). We have the exact sequence

\[
0 \to \tilde{q}C^2/C^2 \to C/C^2 \to C_S/C^2 \to 0
\]

where \( \tilde{q} \) denotes the class of \( q \) in \( C \). This sequence tells us that we must show that \( \tilde{q} \in C^2 \) if and only if \( \varepsilon = 0 \). If \( d = 3(8) \), then \( \tilde{q} = (\tilde{2}) \) is trivial in \( C \). In general, if \( D \) is the discriminant of \( F \), there is an isomorphism
where $\prod'$ means the subgroup of elements $\cdots, \eta_p, \cdots$ of $\prod_{p|\emptyset} \{-1, 1\}$ such that $\prod_{p|\emptyset} \eta_p = 1$, and $(,)_p$ denotes the rational Hilbert 2-symbol at $p[(3, \S 26, 29)]$. But if $d \equiv 3(8)$, then

$$(N_{F/Q} \mathfrak{B}, \mathfrak{D})_p = (2, -d)_p = \left(\frac{2}{p}\right) \text{ for } p \text{ odd}.$$  

(For properties of $(,)_p$ see [5, Ch. 14]). But $(2/p) = 1$ if and only if $p \equiv \pm 1(8)$.

With this information we can find a set of generators for $T_2$. Let $d'$ be the odd part of $d$. For any odd integer $m$, let $m^* = (-1)^{(m-1)/2}m$. We denote by $q, q'$ primes in $S$, and by $p$ the prime dividing $p|d'$.

**Proposition (6):** Let $d' \equiv \pm 3(8)$. For $p|d'$, define the idèle $x_p$ by:

$$x_p = (\sqrt{p^*}_q, \cdots, \sqrt{-d/p}, \cdots) \quad \text{if } p \equiv \pm 1(8)$$

$$x_p = (\sqrt{(d/p^*)^*}_q, \cdots, \sqrt{-d/p}, \cdots) \quad \text{if } p \equiv \pm 3(8),$$

then $T_2$ is generated by $\{x_p| p|d'\}$.

**Proof:** If $p \equiv \pm 1(8)$, then $x_p^2 \equiv (p^*)(\cdots, -d/p, p^*, \cdots) \mod J^S$; if $p \equiv \pm 3(8)$, then $x_p^2 = (-d \cdot p^*/d^*)^*(\cdots, d^*/p^*, \cdots) \mod J^S$. Thus $x_p \in T_2$ for all $p|d'$. Furthermore, in the sequence (2), $x_p \mapsto \eta_p$ if $p \equiv 3(8)$ and $2|d$, and $x_p \mapsto \bar{p}$ otherwise. Thus since $\eta$ and the images of the $x_p$ generate $C_2$, we have $|C_2|/|\{x_p| p|d'\}| \leq 2$ and this quotient is 1 if $d \equiv 3(8)$. Proposition 4 completes the proof.

**Proposition 7:** Let $d \equiv \pm 1(8)$. If there are any, let $p_0$ be a fixed prime, $p_0|d'$, $p_0 \equiv \pm 3(8)$. Define for $p|d'$ the idèle $x_p$:

$$x_p = (\sqrt{p^*}_q, \cdots, \sqrt{-d/p}, \cdots) \quad \text{if } p \equiv \pm 1(8)$$

$$x_p = (\sqrt{p^*_0}_q, \cdots, \sqrt{-d/p}, \cdots, \sqrt{-d/p^*_0}, \cdots) \quad \text{if } p \equiv \pm 3(8).$$

(if 2 splits in $F$, $q|2$ refers to two idèle components both of which are taken $\equiv 1(4)$). Then $\{x_p| p|d'\}$, along with
if 2 splits in \( F \), is a set of generators for \( T_2 \).

**Proof:** If \( p \equiv \pm 1(8) \), \( x^2_p \in F^*J^5 \) as in the proof of Proposition 6; if \( p \equiv \pm 3(8) \), then

\[
x^2_p \equiv (p^*p_0^*)(\cdots, -d/p^*p_0^*, \cdots, -d/p^*p_0^*, \cdots) \mod J^5,
\]

so again all \( x_p \in T_2 \). In the sequence (2), \( x_p \rightarrow \hat{p} \) if \( p \equiv 1(8) \) and \( x_p \rightarrow \hat{p}\hat{p}_0 \) if \( p \equiv 3(8) \). If \( d \not\equiv 1(8) \), \( \hat{p}_0 \) and the images of the \( x_p \) generate \( C_2 \) so.

\[C_2 : \text{im} \left< \{x_p | p|d'\} \right> \leq 2^e \]

where \( e \) is as in Proposition 4: Proposition 4 completes the proof in this case after noting that

\[
\begin{array}{c}
-1, 1, \cdots \\quad a \quad q
\end{array}
\]

is a nontrivial element of the kernel in the sequence (2) for \( d \equiv -1(8) \).

If \( d \equiv 1(8) \), reasoning analogous to that above gives

\[
(C_2 : \text{im} \left< \{x_p | p|d'\} \right>) \leq 2^{e+1}.
\]

Also the number, \( m \), of \( p \equiv \pm 3(8) \) is even, and

\[
\prod_{p|d'} x_p \equiv (\sqrt{-d} \cdot p_0^*(m-2)/2) (\cdots, -d/p_0^*, \cdots)^{(m-2)/2} \\mod F^*J^5
\]

Thus \( \left< \{x_p | p|d'\} \right> \) contains the kernel in the sequence (2) and \( |C_2|/|\left< \{x_p | p|d'\} \right>| \leq 2^e \). Now apply Proposition 4.

3. We now have explicit generators for \( T \) if \( T^2 = 1 \) or \( T^2 \approx \mathbb{Z}/2\mathbb{Z} \) and \( d \equiv 1(8) \). Whenever we have explicit generators for \( T \) we can determine the quadratic sub-extensions of \( L \). To do this we use the Kummer pairing, \( A/F^*2 \times G/G^2 \rightarrow \{ \pm 1 \} \) (recall again the proof of Proposition 1). If we consider \( T/T^2 \) as a subgroup of \( G/G^2 \), then the subgroup of \( A/F^*2 \) orthogonal to \( T/T^2 \) is the set of elements of \( A/F^*2 \) whose square roots are fixed by \( T \), i.e., lie in \( L \). If we identify \( G/G^2 \) with \( J/F^*J \), the pairing translates by class field theory into the pairing,

\[
A/F^*2 \times J/F^*J \rightarrow \{ \pm 1 \}, (a, (x_p)) \rightarrow \prod_p (a, x_p)_p
\]
where \( (,)_p \) denotes the Hilbert 2-symbol on \( F_p \). This is because if \( x_p \) corresponds by local class field theory to \( \sigma_p \in \text{Gal}(F_p(\sqrt{a})/F_p) \) which we identify with the decomposition group of \( p \) in \( \text{Gal}(F(\sqrt{a})/F) \), then \( (x_p) \) corresponds to \( \prod_p \sigma_p \) in global class field theory \([2, \text{Ch. 7, \S} 10]\). But \( (a, x_p)_p = \sigma_p(\sqrt{a})/\sqrt{a} \) and \( \text{Gal}(F(\sqrt{a})/F) \) is abelian. To work with this Kummer pairing we need a set of generators for \( A/F^*2 \). The proof of Lemma 5 tells us that if for all \( p|d' \), \( p \equiv \pm 1(8) \), then \( \tilde{q} \in C^2 \), for all \( q|2 \). In this case we pick \( q|2, \mathfrak{f} \in D \) such that \( q\mathfrak{f}^2 \) is principal and define \( \alpha \in F \) by \( \langle \alpha \rangle = q\mathfrak{f}^2 \). We have only determined \( \alpha \) up to units of \( F \) for the moment.

**Proposition (8):** Let \( d \neq 1, 2 \). The set consisting of \(-1, 2, \) all but one \( p|d' \) and, if all \( p|d' \) are congruent to \( \pm 1(8) \), \( \alpha \), is an independent set of generators of \( A/F^*2 \).

**Proof:** First, we show that this set is independent. It is clear, since one \( p|d' \) is missing from the set, that \(-1, 2 \) and the other \( p|d' \) are independent mod \( F^*2 \). Now suppose that for all \( p|d' \), \( p \equiv \pm 1(8) \) and

\[
(-1)^{-1}2^{\varepsilon_2}(\prod_{p|d'} p^{\varepsilon_p}) \xi \in F^*2,
\]

where the \( \varepsilon \)'s are 0 or 1. Then this number has even valuation at all primes in \( S \). But by looking at the prime decomposition of \( (2) \) and \( (\xi) \), we see that this cannot be the case. Thus, our set is independent. By Lemma 5 and the proof of Proposition 4, \(|A/F^*2| = 2|S| + 1 - \varepsilon|C_2| \). The subgroup of \( A/F^*2 \) generated by all but one \( p|d' \) and 2 has order \( 2|C_2| \) if \( d \equiv 3(4) \) and \( |C_2| \) otherwise. Therefore, throwing in \( -1 \) gives us \( 4|C_2| \) elements if \( d \equiv 3(4) \) and \( 2|C_2| \) otherwise. This is the correct number unless all \( p \equiv \pm 1(8) \) and then \( \alpha \) fills out the group.

We now explicitly compute the Kummer pairing with elements of \( T_2 \). We shall be using the fact that if \( E_2/E_1 \) is an extension of local fields, if \( (,)_E \) denotes the Hilbert 2-symbol on \( E_i \), and if \( \beta \in E_2, \alpha \in E_1 \), then \( (\beta, \alpha)_E = (N_{E_2/E_1}(\beta), \alpha)_E \) \([1]\).

**Proposition (9):** Let \( a \in \mathbb{Q} \cap A, p|d' \). Then, if \( (,)_E \) denotes the Kummer pairing, we have

(i) \[ x_p = (\sqrt{p^*}, \cdots, \sqrt{-d}, \cdots) \Rightarrow (a, x_p) = (a, d)_p \]

(ii) \[ x_p = (\sqrt{(-d)p^*/d'^*}, \cdots, \sqrt{-d}, \cdots) \Rightarrow (a, x_p) = (a, d)_2(a, d)_p \]

(iii) \[ x_p = (\sqrt{p^*}, \cdots, \sqrt{-d}, \cdots, \sqrt{-d'}, \cdots) \Rightarrow (a, x_p) = (a, d)_{p_0}(a, d)_p. \]
PROOF: For (i),

\[(a, x_p) = \left( \prod_{q \mid 2} (a, \sqrt{p^*}_q) \right) \cdot (a, \sqrt{-d})_p = (a, d)_p.\]

For (ii)

\[(a, x_p) = (a, \sqrt{-d})_p(a, \sqrt{p^*/d^*})_p(a, \sqrt{-d})_p = (a, d)_2(a, \sqrt{p^*/d^*})_2(a, d)_p = (a, d)_p.\]

Case (iii) is similar.

PROPOSITION (10): Suppose \( p \equiv \pm 1(8) \) for all \( p \mid d' \). Let \( \alpha = a + b\sqrt{-d} \) with \( (\alpha) = q \mathcal{A}^2 \) for some \( q \mid 2 \). If \( N_{F/Q} \alpha = 2s^2 \) and \( m = a + s \), then \( (\alpha, x_p) = (-1)^{(p^*-1)/8}(a, d)_p = (m, d)_p \) for all \( p \mid d' \).

PROOF: We may assume that \( \mathcal{A} \) is integral and divisible by no rational prime since altering \( \mathcal{A} \) to be so only changes \( \alpha, a, s, \) and \( m \) by rational squares. Therefore, no odd prime divides two of \( a, bd, \) and \( s \).

\[(\alpha, x_p) = \left( \prod_{q \mid 2} (\alpha, \sqrt{p^*}) \right) \cdot (\alpha, \sqrt{-d})_p = (2s^2, \sqrt{p^*})_2(\alpha, \sqrt{-d})_p = (-1)^{(p^*-1)/8}(\alpha, \sqrt{-d})_p.\]

Now,

\[(a + b\sqrt{-d}, \sqrt{-d})_p = (a, \sqrt{-d})_p(1 + b\sqrt{-d}/a, \sqrt{-d})_p = (a, d)_p(1 + b\sqrt{-d}/a, -b\sqrt{-d}/a)_p = (a, d)_p(2s^2/a^2, -a/b)_p = (a, d)_p.\]

We have proved the first equality for \( (\alpha, x_p) \). It remains to show that

\[(m/a, d)_p = (-1)^{(p^*-1)/8}.\]

Now \( p \nmid a \), and if \( p \mid m \), we would have \( p \mid a^2 - s^2 = s^2 - b^2d \), so \( p \mid s \), which is not the case. Thus \( (m/a, d)_p = (m/a)/p \),

\[\left( \frac{m/a}{p} \right) = \left( \frac{2m/a}{p} \right) = \left( \frac{2(a+s)/a}{p} \right) = \left( \frac{2 + 2s/a}{p} \right)\]
and $a^2 + b^2d = 2s^2$ implies that $(s/a)^2 \equiv \frac{1}{2}(p)$. Thus we shall be done if we prove the following

**Lemma (11):** Let $p \equiv \pm 1(8)$. Then $2 + \sqrt{2}$ is a square in $\mathbb{F}_p$ if and only if $p \equiv \pm 1(16)$.

**Proof:** Note first that the choice of $\sqrt{2}$ is unimportant since $(2 + \sqrt{2})(2 - \sqrt{2}) = 2 \in \mathbb{F}_p^*$. Since $p^2 \equiv 1(16)$, $\mathbb{F}_{p^2}$ contains the sixteenth roots of 1. Let $\zeta$ be a primitive eighth root of 1. Then

$$(\zeta + \zeta^{-1})^2 = \zeta^2 + \zeta^{-2} + 2 = 2.$$

Let $\eta^2 = \zeta$. Then

$$(\eta + \eta^{-1})^2 = \zeta + \zeta^{-1} + 2 = 2 + \sqrt{2}.$$

We wish to know when $\eta + \eta^{-1} \in \mathbb{F}_p$. But by Galois theory, $\eta + \eta^{-1} \in \mathbb{F}_p$ if and only if $(\eta + \eta^{-1})^p = \eta + \eta^{-1}$. And $(\eta + \eta^{-1})^p = \eta^p + \eta^{-p} = \eta + \eta^{-1}$ if $p \equiv \pm 1(16)$ and $-(\eta + \eta^{-1})$ if $p \equiv \pm 9(16)$. This completes the proof.

4. Because $(G/G^2 : T/T^2) = 4$, the kernel on the left in the pairing $A/F^* \times T/T^2 \rightarrow \pm 1$ has order 4. It is this kernel whose elements have square roots lying in $L$. We already know one, however: $F(\sqrt{2})$ begins the cyclotomic $Z_2$-extension of $F$. Thus we have a pairing $A/\langle 2 \rangle F^* \times T/T^2 \rightarrow \pm 1$, and we wish to compute the kernel on the left. We choose a particular set of generators for $A/\langle 2 \rangle F^*$, namely the $p^*$ for all but one $p|d'$, $-2$, and if all $p|d'$ are congruent to $+1(8)$, $a$. Further, if $d \equiv -1(8)$, we choose $a$ so that $a \equiv 1(4)$ in $F_q$. In this case, the $p^*$ and $a$ generate the subgroup of $A/\langle 2 \rangle F^*$ orthogonal to $\langle -1, 1, \cdots \rangle_{q, q'}$.

**Theorem (12):** Suppose $d \neq 1, 2$. Let $B$ be the subgroup of $F^*$ generated by the $p^*$ for all but one $p|d'$, $-2$ if $d \neq -1(8)$, and, if all $p|d'$ are congruent to $+1(8)$, $a$, with the sign of $a$ chosen so that $a \equiv 1(4)$ in $F_q$ if $d \equiv -1(8)$. If $d' \equiv \pm 1(8)$ but not all $p|d'$ are congruent to $\pm 1(8)$, let $p_0|d'$ be fixed, $p_0 \equiv \pm 3(8)$.

Define a homomorphism $\theta : B/B^2 \rightarrow \prod_{p|d'} \{\pm 1\}$ as follows. Let $\pi_p$ be projection onto the $p$ factor. If $y \in Q \cap B$,

$$\pi_p \circ \theta(y) = (y, d)_p \quad \text{for} \quad p \equiv \pm 1(8) \quad \text{and all} \quad p \quad \text{if} \quad d \equiv 3(8)$$
\[ \pi_p \circ \theta(y) = (y, d)_p \quad \text{for} \ p \equiv \pm 3(8) \ \text{when} \ d' \equiv \pm 3(8) \ \text{and} \ d \neq 3(8) \]
\[ \pi_p \circ \theta(y) = (y, d)_p \quad \text{for} \ p \equiv \pm 3(8) \ \text{when} \ d' \equiv \pm 1(8) \]

and if \( \alpha = a + b\sqrt{-d} \), \( N_{F/\mathbb{Q}}\alpha = 2s^2, m = a + s \)

\[ \pi_p \circ \theta(x) = (m, d)_p. \]

Then \( |\ker \theta| = 2 \) if and only if \( T^2 = 1 \), and, in this case, if \( \ker \theta = \langle x \rangle \), then \( F(\sqrt{x}) \) is a quadratic subextension of \( L \). Also, if \( d \equiv 1(8) \), then \( T^2 \approx \mathbb{Z}/2\mathbb{Z} \) if and only if (a) \( |\ker \theta| = 4 \), (b) \( \ker \theta \) contains only one rational integer, \( x \), with odd part congruent to \( \pm 1(8) \), and, (c) \( d \equiv 9(16) \) if all \( p \mid d' \) are congruent to \( \pm 1(8) \). In this case \( F(\sqrt{x}) \) is a quadratic subextension of \( L \).

**Proof:** Propositions 9 and 10 tell us that \( \pi_p \circ \theta(y) = (y, x_p) \) except for \( d \equiv 3(8) \). But when \( d \equiv 3(8) \), \( (-2, 2)_2 = (p^*, d)_2 = 1 \). If \( d \equiv -1(8) \), \( B \) generates the subgroup of \( A/\langle 2 \rangle F^* \) orthogonal to

\[ (-1, 1, \cdots). \]

Thus \( \ker \theta \) can be considered the subgroup of \( A/\langle 2 \rangle F*^2 \) orthogonal to \( T_2 \). Since the subgroup orthogonal to all of \( T \) has order 2, \( |\ker \theta| = 2 \) if and only if \( T = T_2 \cdot T^2 \), i.e., \( T = T_2 \). If \( d \equiv 1(8) \), \( T^2 \approx \mathbb{Z}/2\mathbb{Z} \) if and only if

\[ (1 - i, \cdots) \]

generates \( T/T^2 \), and this can happen if and only if \( |\ker \theta| = 4 \) and the pairing \( \ker \theta \times \langle (1 - i, \cdots) \rangle \rightarrow \pm 1 \) has kernel on the left of order 2. Now if \( y \in \mathbb{Q} \), then

\[ (y, (1 - i, \cdots)) = (y, 1 - i)_q = (y, 2)_2. \]

But \( (y, 2)_2 = 1 \) if and only if the odd part of \( y \) is congruent to \( \pm 1(8) \). If all \( p \mid d \) are congruent to \( \pm 1(8) \), then

\[ (y, (1 - i, \cdots)) = 1 \]

for \( y \in B \cap \mathbb{Q} \) since such \( y \) have odd part congruent to \( \pm 1(8) \). We are done if we show that

\[ (z, (1 - i, \cdots)) = (-1)^{(d - 1)/8}. \]
Now,

\[(\pm \alpha \bar{\alpha}, 1 - i)_q = (\pm 2s^2, 2)_2 = 1,\]

so

\[(\alpha, 1 - i)_q = (\bar{\alpha}, 1 - i)_q = (-\alpha, 1 - i)_q = (-\bar{\alpha}, 1 - i)_q,\]

and there is no loss in assuming that if \(a = b + d \in F_2 \approx \mathbb{Q}_2(i)\), then \(a = b \equiv 1(4)\) (we may assume that \(2 \nmid a\) since \((2, 1 - i)_q = 1\), so \(s\) is odd). Because \(a^2 + b^2 = 2s^2\), we see that 2 is a square modulo all primes dividing \(b\), so \(b \equiv -1(8)\). Since \(s^2 \equiv 1(8)\), we have \(2s^2 \equiv 2(16)\) and \(b^2 \equiv 1(16)\) from which we extract the congruence \(a^2 + d \equiv 2(16)\). Thus

\[a \equiv \sqrt{d} \equiv -b \sqrt{d} (8) \quad \text{and} \quad \alpha \equiv (1 - i) \sqrt{d}(8), \alpha/1 - i = \sqrt{d} \cdot u\]

where \(u \equiv 1(q^5)\). But then \(u \in F_a^{2^2}\) by the theory of local fields, so

\[(\alpha, 1 - i)_q = (\alpha/1 - i, 1 - i)_q\]

since \((1 - i, 1 - i)_q = (-1, 1 - i)_q = (i, 1 - i)_q = 1\)

\[= (\sqrt{d}, 1 - i)_q \quad \text{since} \quad u \text{ is a square}\]

\[= (\sqrt{d}, 2)_2 = (-1)^{d-1}/8.\]

This finishes the proof.

**Remark (13):** It is an easy consequence of reciprocity of the rational Hilbert 2-symbols, the fact that \((d/\ell) = 1\) for odd primes \(\ell|m\) (because \(\ell|m \Rightarrow \ell|a^2 - s^2 = s^2 - b^2d\)) and the fact, not proven here, that the odd part of \(m\) is congruent to \(1(4)\) if \(d \equiv 7(8)\) that we may replace the range group of \(\theta\) by

\[
\prod_{\substack{p|\mathcal{Q} \\ p \neq 2}} \{\pm 1\} \quad \text{if} \quad d' \equiv \pm 3(8), \quad \text{and by} \quad \prod_{\substack{p|\mathcal{Q} \\ p \neq p_0}} \{\pm 1\} \quad \text{if} \quad d' \equiv \pm 1(8),
\]

letting \(\pi_2 \circ \theta(y) = (y, d)_2\) for \(y \in \mathbb{Q}\) and \(\pi_2 \circ \theta(\alpha) = (m, d)_2\). Also, the order of these new range groups is \(\frac{1}{2} |B/B^2|\), so \(|\ker \theta| = 2\) if and only if \(\theta\) is surjective, etc. It is this form of the map \(\theta\) which shall be referred to in a later paper.
REMARK (14): The cases $d = 1, 2$ have been skipped over in some of the theorems. It is simple to work out the whole story in these cases. Namely, $T = 1$ in both cases and $F(\sqrt{1 - i})$, resp. $F(\sqrt{1 - 2})$, lie in a $\mathbb{Z}_2$-extension of $F$.

5. We illustrate with two examples.

EXAMPLE (15): Let $F = \mathbb{Q}(-pq)$, $p \equiv 1(4)$, $pq \equiv 3(8)$. In this case, $B$ is generated by $-2$ and $p$.

$$\theta(-2) = ((-2, d)_p, (-2, d)_q) = \left(\left(\frac{-2}{p}\right), \left(\frac{-2}{q}\right)\right)$$

$$\theta(p) = ((p, d)_p, (p, d)_q) = \left(\left(\frac{p}{q}\right), \left(\frac{p}{q}\right)\right) = \left(\left(\frac{-q}{p}\right), \left(\frac{p}{q}\right)\right).$$

It is easy to see directly or by using Remark 13 that $(-2/p) = (-2/q)$, $(-q/p) = (p/q)$. Thus we deduce, noting that $T$ is cyclic by Proposition 2,

(a) If $p \equiv 1(8)$ and $(p/q) = 1$ then $|T| \geq 4$.
(b) If $p \equiv 1(8)$ and $(p/q) = -1$ then $T = T_2 \cong \mathbb{Z}/2\mathbb{Z}$ and $F(\sqrt{-2})$ lies in $L$.
(c) If $p \equiv 5(8)$ and $(p/q) = 1$ then $T = T_2 \cong \mathbb{Z}/2\mathbb{Z}$ and $F(\sqrt{p})$ lies in $L$.
(d) If $p \equiv 5(8)$ and $(p/q) = -1$ then $T = T_2 \cong \mathbb{Z}/2\mathbb{Z}$ and $F(\sqrt{-2p})$ lies in $L$.

Case (a) is still up in the air. We consider a particular example: $p = 73$, $q = 3$. Hoping that $|T| = 4$, we compute a square root, $z$, of $x_{73} \mod F^*J^5$. Any such $z$ would map to a square root of $\tilde{p}_{73}$ in $C$. Let $\beta = \frac{73}{2} + \frac{1}{2}\sqrt{-219}$. Since $N_{F/Q}\beta = 73.5^2$, we have $(\beta) = p_{73}p_5^2$ for some $p_5|5$ (5 splits in $F$), and $\tilde{p}_{73} = p_5^2 \mod F^*J^5$. Thus as a first guess for $z$ we use

$$(\cdots, \frac{1}{5}, \cdots).$$

Now

$$(\cdots, \frac{1}{5}, \cdots)^2 \equiv (\beta \cdots, 1/5^2, \cdots) \equiv (\beta, \cdots, 73/\sqrt{219}, \cdots, \beta, \cdots) \mod F^*J^5$$

$$\equiv (\beta, \cdots, \sqrt{-219}, \cdots) \mod F^*J^5$$

since $p_5 \not|\beta$ and $\beta$ and $\sqrt{-219}$ are both exactly divisible by $p_{73}$. Now, $x_{73} = (\sqrt{73}, \cdots, \sqrt{-219}, \cdots)$. Now,
so if we can find a square root, \( \gamma \), of \( \sqrt{73} / \beta \) in \( F_\alpha \), then we can take

\[
z = (\gamma, \cdots, \frac{1}{p_5}, \cdots).
\]

In \( F_\alpha = \mathbb{Q}_2(\sqrt{-3}) \) we have \( \beta / \sqrt{73} = \sqrt{73/2 + 3\sqrt{-3}} \).

\[3^2 \equiv 73(64), \text{ so } 3 \equiv \sqrt{73(32)}, \frac{3}{2} \equiv \sqrt{73/2(16)}, \text{ thus}\]

\[
\beta / \sqrt{73} \equiv -3(-\frac{1}{2} - \frac{1}{2}\sqrt{-3})(16)
\]

and \( \sqrt{\beta / \sqrt{73}} \equiv \rho \sqrt{-3}(8) \) where \( \rho^3 = 1 \). Now we evaluate the Kummer pairing:

\[
(-2, z) = (-2, \gamma)_6(-2, \frac{1}{p_5})_6 = (-2, 1/\rho\sqrt{-3})_6(-2, \frac{1}{p_5})_6
\]

since \( \rho \sqrt{-3}/\sqrt{\beta / \sqrt{73}} \in F_\alpha^2 \) and 5 splits. Thus

\[
(-2, z) = (-2, \frac{1}{p_5})_2(-2, \frac{1}{p_5})_5 = 1 \cdot (-1) = -1.
\]

It follows that \( z \) generates \( T \) (and so \(|T| = 4\)) because \( A / \langle 2 \rangle F^* \times \langle z \rangle / \langle z \rangle^2 \)

has kernel on the left of order 2. To finish, we observe

\[
(73, z) = (73, 1/\rho\sqrt{-3})_6(73, \frac{1}{p_5})_5 = (73, \frac{1}{p_5})_2(73, \frac{1}{p_5})_5 = 1 \cdot (-1) = -1.
\]

Thus \( F(\sqrt{-146}) \) begins a \( \mathbb{Z}_2 \)-extension of \( F \).

**Example (16):** Let \( F = \mathbb{Q}(\sqrt{-7 \cdot 17}) \). \( B \) is generated by \( 17 \) and \( \alpha \), where we may take \( \alpha = (-9 + \sqrt{-119})/2 \). Then \( m = -\frac{9}{2} + 5 = \frac{1}{2} \).

Thus

\[
\theta(17) = ((17, 119)_7, (17, 119)_1) = ((\frac{1}{7}7), (17, -7)_1) = ((\frac{1}{7}7), (\frac{1}{7}7)) = (-1, -1)
\]

\[
\theta(\alpha) = ((\frac{1}{7}, 119)_7, (\frac{1}{7}, 119)_1) = (1, 1).
\]

Since \( \theta \) has kernel of order 2 generated by \( \alpha \), we see that \( F(\sqrt{\alpha}) \) begins a \( \mathbb{Z}_2 \)-extension of \( F \) and \( T \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \).

**References**


Determining quadratic subfields of $\mathbb{Z}_2$-extensions


(Oblatum 28–IX–1974)

Dept. Math.
California Institute of Technology
Pasadena, California 91109