COMPOSITIO MATHEMATICA

JOSEPH E. CARROLL

On determining the quadratic subfields of Z_2-extensions of complex quadratic fields

Compositio Mathematica, tome 30, nº 3 (1975), p. 259-271

<http://www.numdam.org/item?id=CM_1975__30_3_259_0>

COMPOSITIO MATHEMATICA, Vol. 30. Fasc. 3, 1975, pag. 259–271
Noordhoff International Publishing
Printed in the Netherlands

ON DETERMINING THE QUADRATIC SUBFIELDS OF 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 $\mathfrak{p}$, a prime of F, let $U_\mathfrak{p}$ denote the group of units in the completion, $F_\mathfrak{p}$, of F at $\mathfrak{p}$. Let

$$J^S = \prod_{\mathfrak{q} \in S} \{1\} \times \prod_{\mathfrak{p} \notin S} U_\mathfrak{p},$$

a subgroup of the idèle group, J, of F. By class field theory, $\overline{F^* J^S}$ corresponds to the maximal abelian 2-ramified (i.e., unramified at all primes outside S) extension of F. We can write canonically, $J/\overline{F^* J^S} = G \times G'$, 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, 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 β to an even power. Let A be the subgroup of all such β 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,

$$0 \to U_S/U_S^2 \to A/F^{*2} \xrightarrow{f} (C_S)_2 \to 0 \tag{1}$$

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 (β) 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 $G \approx \mathbb{Z}_2 \times \mathbb{Z}_2 \times T$, 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

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

and taking 2 power torsion parts we get another exact sequence

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

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

$$0 \to H \to T \to \operatorname{im} T \to 0 \tag{2'}$$

splits if and only if $d \equiv -1(8)$. *If* $d \not\equiv \pm 1(8)$ *or* $d = 1$, *then* H *is trivial.*

Proof: Since F is complex quadratic, U is finite and so $U = \bar{U}$. (In fact F^*J^S is closed also). Thus, if $\mu_{\mathfrak{q},2}$ denotes the group of 2-power roots of 1 in $F_\mathfrak{q}$, $H = (\prod_{\mathfrak{q} \in S} \mu_{\mathfrak{q},2})/\{\pm 1\}$ (if $d = 1$ we get $\{\pm i, \pm 1\}$ in the denominator). If $d \not\equiv 1(8)$, then $\mu_{\mathfrak{q},2} = \{\pm 1\}$ for $\mathfrak{q} \in S$ and if $d \not\equiv -1(8)$, 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

$$(\cdots, \underset{\mathfrak{p}_1}{x_{\mathfrak{p}_1}}, \cdots, \underset{\mathfrak{p}_2}{x_{\mathfrak{p}_2}}, \cdots, \underset{\mathfrak{p}_r}{x_{\mathfrak{p}_r}}, \cdots)$$

denote the idèle of F which has components $x_{\mathfrak{p}_i}$ in the $\mathfrak{p}_i^{th}$ slot and 1 elsewhere. If $d \equiv 1(8)$ and $\mathfrak{q}|2$, then

$$(\underset{\mathfrak{q}}{1-i},\cdots)^2 = (\underset{\mathfrak{q}}{-2i},\cdots) \equiv (\underset{\mathfrak{q}}{i},\cdots) \bmod F^*J^S$$

so the sequence (2′) does not split in this case. To complete the proof, it is enough to show that if $d \equiv -1(8)$ and, $\mathfrak{q}, \mathfrak{q}'|2$ then

$$(\underset{\mathfrak{q}}{-1}, \underset{\mathfrak{q}'}{1},\cdots) \notin T^2, \qquad \text{for then} \quad (\underset{\mathfrak{q}}{-1}, \underset{\mathfrak{q}'}{1},\cdots)$$

would generate a pure subgroup of T and (2′) would split. Suppose that there is an idèle $(x_\mathfrak{p})$ such that

$$(x_\mathfrak{p})^2 = (\underset{\mathfrak{q}}{-1}, \underset{\mathfrak{q}'}{1},\cdots)(\alpha)(u_\mathfrak{p}), \qquad \text{where} \quad \alpha \in F^*, \ (u_\mathfrak{p}) \in J^S.$$

Then the principal ideal, (α), is a square in D, the ideal group of F. Since F is complex quadratic $N_{F/}\mathbb{Q}\alpha = m^2$, $m \in \mathbb{Q}$. The equation above now yields $x_\mathfrak{q}^2 x_{\mathfrak{q}'}^2 = -N_{F/} \ \alpha = -m^2$, implying the contradiction that $-1 \in \mathbb{Q}_2^{*2}$.

COROLLARY (3): *If* $C_2 = C(2)$ *then* $T = T_2$ *unless* $1 \neq d \equiv 1(8)$. *If* $1 = d \equiv 1(8)$ *and* $C_2 = C(2)$ *then* $|T/T_2| = 2$ *and* $(1 \underset{\mathfrak{q}}{-} i,\cdots)$ *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* $\varepsilon = 0$ *if* $d \equiv 3(8)$ *or if all odd primes dividing d are congruent to* $\pm 1(8)$ *and let* $\varepsilon = 1$ *otherwise. Then* $|T_2| = 2^{|S|-\varepsilon-1}|C_2|$.

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, $|A/F^{*2}| = 2^{|S|+1}|(C_S)_2|$. 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* ε *is as in the statement of Proposition* 4.

PROOF: Let $\mathfrak{q}|2$. We have the exact sequence

$$0 \to \tilde{\mathfrak{q}}C^2/C^2 \to C/C^2 \to C_S/C_S^2 \to 0$$

where $\tilde{\mathfrak{q}}$ denotes the class of $\mathfrak{q}$ in C. This sequence tells us that we must show that $\tilde{\mathfrak{q}} \in C^2$ if and only if $\varepsilon = 0$. If $d \equiv 3(8)$, then $\tilde{\mathfrak{q}} = (\tilde{2})$ is trivial in C. In general, if $\mathscr{D}$ is the discriminant of F, there is an isomorphism

$$C/C^2 \simeq \prod_{p|\mathscr{D}}' \{\pm 1\}, \qquad \tilde{\mathfrak{A}} \mapsto (\cdots, (N_{F/Q}\mathfrak{A}, \mathscr{D})_p, \ldots)$$

where $\prod'$ means the subgroup of elements $(\cdots, \eta_p, \cdots)$ of $\prod_{p|\mathscr{D}}\{\pm 1\}$ such that $\prod_{p|\mathscr{D}} \eta_p = 1$, and $(,)_p$ denotes the rational Hilbert 2-symbol at p[(3, § 26, 29)]. But if $d \not\equiv 3(8)$, then

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

(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 $\mathfrak{q}$, $\mathfrak{q}'$ primes in S, and by $\mathfrak{p}$ the prime dividing $p|d'$.

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

$$x_p = (\underset{\mathfrak{q}}{\sqrt{p^*}}, \cdots, \underset{\mathfrak{p}}{\sqrt{-d}}, \cdots) \qquad \text{if} \quad p \equiv \pm 1(8)$$

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

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

Proof: If $p \equiv \pm 1(8)$, then $x_p^2 \equiv (p^*)(\cdots, -d/_{\mathfrak{p}}p^*, \cdots) \bmod J^S$; if $p \equiv \pm 3(8)$, then $x_p^2 = (-d \cdot p^*/d'^*)(\cdots, d'^*/_{\mathfrak{p}}p^*, \cdots) \bmod J^S$. Thus $x_p \in T_2$ for all $p|d'$. Furthermore, in the sequence (2), $x_p \mapsto \tilde{\mathfrak{q}}\tilde{\mathfrak{p}}$ if $p \equiv \pm 3(8)$ and $2|d$, and $x_p \mapsto \tilde{\mathfrak{p}}$ otherwise. Thus since $\tilde{\mathfrak{q}}$ and the images of the x_p generate C_2, we have $|C_2|/|\langle\{x_p| \ p|d'\}\rangle| \leqq 2$ 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:*

$$x_p = (\underset{\mathfrak{q}|2}{\sqrt{p^*}}, \cdots, \underset{\mathfrak{p}}{\sqrt{-d}}, \cdots) \qquad \textit{if} \quad p \equiv \pm 1(8)$$

$$x_p = (\underset{\mathfrak{q}|2}{\sqrt{p^*p_0^*}}, \cdots, \underset{\mathfrak{p}_0}{\sqrt{-d}}, \cdots, \underset{\mathfrak{p}}{\sqrt{-d}}, \cdots) \qquad \textit{if} \quad p \equiv \pm 3(8)$$

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

$$\underset{\mathfrak{q}}{(-1,}\ \underset{\mathfrak{q}'}{1,}\cdots)$$

if 2 *splits in* F, *is a set of generators for* T_2.

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

$$x_p^2 \equiv (p^*p_0^*)(\cdots, \underset{\mathfrak{p}_0}{-d/p^*p_0^*}, \cdots, \underset{\mathfrak{p}}{-d/p^*p_0^*}, \cdots) \bmod J^S,$$

so again all $x_p \in T_2$. In the sequence (2), $x_p \to \tilde{\mathfrak{p}}$ if $p \equiv \pm 1(8)$ and $x_p \to \tilde{\mathfrak{p}}\tilde{\mathfrak{p}}_0$ if $p \equiv \pm 3(8)$. If $d \not\equiv 1(8)$, $\tilde{\mathfrak{p}}_0$ and the images of the x_p generate C_2 so. $(C_2 : \mathrm{im}\ \langle\{x_p|\ p|d'\}\rangle) \leqq 2^\varepsilon$ where ε is as in Proposition 4. Proposition 4 completes the proof in this case after noting that

$$\underset{\mathfrak{q}}{(-1,}\ \underset{\mathfrak{q}}{1,}\cdots)$$

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

$$(C_2 : \mathrm{im}\ \langle\{x_p|\ p|d'\}\rangle) \leqq 2^{\varepsilon+1}.$$

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

$$\prod_{\substack{p|d' \\ p \neq p_0}} x_p \equiv (\sqrt{-d} \cdot p_0^{*(m-2)/2})(\cdots, \underset{\mathfrak{p}_0}{-d/p_0}, \cdots)^{(m-2)/2}(\underset{\mathfrak{q}}{i}, \cdots)$$

$$\equiv (\underset{\mathfrak{q}}{i}, \cdots) \bmod F^*J^S$$

Thus $\langle\{x_p|\ p|d'\}\rangle$ contains the kernel in the sequence (2) and $|C_2|/|\langle\{x_p|\ p|d'\}\rangle| \leqq 2^\varepsilon$. 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, $A/F^{*2} \times G/G^2 \to \{\pm 1\}$ (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 $J/\overline{F^*J^SJ^2}$, the pairing translates by class field theory into the pairing,

$$A/F^{*2} \times J/\overline{F^*J^*J^2} \to \{\pm 1\}, (a, (x_\mathfrak{p})) \to \prod_\mathfrak{p} (a, x_\mathfrak{p})_\mathfrak{p}$$

where $(,)_{\mathfrak{p}}$ denotes the Hilbert 2-symbol on $F_{\mathfrak{p}}$. This is because if $x_{\mathfrak{p}}$ corresponds by local class field theory to $\sigma_{\mathfrak{p}} \in \mathrm{Gal}\,(F_{\mathfrak{p}}(\sqrt{a})/F_{\mathfrak{p}})$ which we identify with the decomposition group of $\mathfrak{p}$ in $\mathrm{Gal}\,(F(\sqrt{a})/F)$, then $(x_{\mathfrak{p}})$ corresponds to $\prod_{\mathfrak{p}} \sigma_{\mathfrak{p}}$ in global class field theory [2, Ch. 7, § 10]. But $(a, x_{\mathfrak{p}})_{\mathfrak{p}} = \sigma_{\mathfrak{p}}(\sqrt{a})/\sqrt{a}$ and $\mathrm{Gal}\,(F(\sqrt{a})/F)$ 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 $\tilde{\mathfrak{q}} \in C^2$, for all $\mathfrak{q}|2$. In this case we pick $\mathfrak{q}|2$, $\mathfrak{A} \in D$ such that $\mathfrak{q}\mathfrak{A}^2$ is principal and define $\alpha \in F$ by $(\alpha) = \mathfrak{q}\mathfrak{A}^2$. We have only determined α 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 $\pm 1(8)$, α, 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

$$(-1)^{\varepsilon_{-1}} 2^{\varepsilon_2} \Big(\prod_{p|d'} p^{\varepsilon_p}\Big)\alpha \in F^{*2},$$

where the ε'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 (α), 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 α 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 $(,)_{E_i}$ denotes the Hilbert 2-symbol on E_i, and if $\beta \in E_2$, $c \in E_1$, then $(\beta, c)_{E_2} = (N_{E_2/E_1}\beta, c)_{E_1}$ [1].

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

(i) $x_p = (\underset{\mathfrak{q}|2}{\sqrt{p^*}}, \cdots, \underset{\mathfrak{p}}{\sqrt{-d}}, \cdots) \Rightarrow (a, x_p) = (a, d)_p$

(ii) $x_p = (\underset{\mathfrak{q}}{\sqrt{(-d)p^*/d'^*}}, \cdots, \underset{\mathfrak{p}}{\sqrt{-d}}, \cdots) \Rightarrow (a, x_p) = (a, d)_2(a, d)_p$

(iii) $x_p = (\underset{\mathfrak{q}|2}{\sqrt{p^* p_0^*}}, \cdots, \underset{\mathfrak{p}_0}{\sqrt{-d}}, \cdots, \underset{\mathfrak{p}}{\sqrt{-d}}, \cdots) \Rightarrow (a, x_p) = (a, d)_{p_0}(a, d)_p$.

PROOF: For (i),

$$(a, x_p) = \Big(\prod_{\mathfrak{q}|2} (a, \sqrt{p^*})_{\mathfrak{q}}\Big) \cdot (a, \sqrt{-d})_{\mathfrak{p}}$$
$$= (a, \sqrt{p^*})_2^2 (a, d)_p = (a, d)_p.$$

For (ii)

$$(a, x_p) = (a, \sqrt{-d})_{\mathfrak{q}} (a, \sqrt{p^*/d'^*})_{\mathfrak{q}} (a, \sqrt{-d})_{\mathfrak{p}}$$
$$= (a, d)_2 (a, \sqrt{p^*/d'^*})_2^2 (a, d)_p = (a, d)_2 (a, d)_p.$$

Case (iii) is similar.

PROPOSITION (10): *Suppose* $p \equiv \pm 1(8)$ *for all* $p|d'$. *Let* $\alpha = a + b\sqrt{-d}$ *with* $(\alpha) = \mathfrak{q}\mathfrak{A}^2$ *for some* $\mathfrak{q}|2$. *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* $p|d'$.

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

$$(\alpha, x_p) = \Big(\prod_{\mathfrak{q}|2} (\alpha, \sqrt{p^*})\Big) \cdot (\alpha, \sqrt{-d})_{\mathfrak{p}} = (2s^2, \sqrt{p^*})_2 (\alpha, \sqrt{-d})_{\mathfrak{p}}$$
$$= (-1)^{(p^*-1)/8} (\alpha, \sqrt{-d})_{\mathfrak{p}}.$$

Now,

$$(a + b\sqrt{-d}, \sqrt{-d})_{\mathfrak{p}} = (a, \sqrt{-d})_{\mathfrak{p}} (1 + b\sqrt{-d}/a, \sqrt{-d})_{\mathfrak{p}}$$
$$= (a, d)_p (1 + b\sqrt{-d}/a, -b\sqrt{-d}/a)_{\mathfrak{p}} (1 + b\sqrt{-d}/a, -a/b)_{\mathfrak{p}}$$
$$= (a, d)_p (2s^2/a^2, -a/b)_p = (a, d)_p.$$

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

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

Now $p \nmid a$, and if $p|m$, we would have $p|a^2 - s^2 = s^2 - b^2 d$, so $p|s$, 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 $(2+\sqrt{2})(2-\sqrt{2}) = 2 \in F_p^{*2}$. Since $p^2 \equiv 1(16)$, $\mathbb{F}_{p^2}$ contains the sixteenth roots of 1. Let ζ be a primitive eight 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 $A/F^{*2} \times T/T^2 \to \pm 1$ 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 $A/\langle 2\rangle F^{*2} \times T/T^2 \to \pm 1$, and we wish to compute the kernel on the left. We choose a particular set of generators for $A/\langle 2\rangle F^{*2}$, namely the p^* for all but one $p|d'$, -2, and if all $p|d'$ are congruent to $\pm 1(8)$, α. Further, if $d \equiv -1(8)$, we choose α so that $\alpha \equiv 1(4)$ in $F_{\mathfrak{q}'} \approx \mathbb{Q}_2$. In this case, the p^* and α generate the subgroup of $A/\langle 2\rangle F^{*2}$ orthogonal to

$$(\underset{\mathfrak{q}}{-1}, \underset{\mathfrak{q}'}{1}, \cdots).$$

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 $d \not\equiv -1(8)$, and, if all $p|d'$ are congruent to $\pm 1(8)$, α, with the sign of α chosen so that $\alpha \equiv 1(4)$ in $F_{\mathfrak{q}'}$ 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 $\theta : B/B^2 \to \prod_{p|d'}\{\pm 1\}$ as follows. Let π_p be projection onto the p factor. If $y \in \mathbb{Q} \cap B$,*

$$\pi_p \circ \theta(y) = (y, d)_p \qquad \textit{for } p \equiv \pm 1(8) \textit{ and all } p \textit{ if } d \equiv 3(8)$$

$\pi_p \circ \theta(y) = (y, d)_2 (y, d)_p$ *for* $p \equiv \pm 3(8)$ *when* $d' \equiv \pm 3(8)$ *and* $d \not\equiv 3(8)$

$\pi_p \circ \theta(y) = (y, d)_{p_0} (y, d)_p$ *for* $p \equiv \pm 3(8)$ *when* $d' \equiv \pm 1(8)$

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

$$\pi_p \circ \theta(\alpha) = (m, d)_p.$$

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* $p|d'$ *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 $d \equiv 3(8)$, $(-2, d)_2 = (p^*, d)_2 = 1$. If $d \equiv -1(8)$, B generates the subgroup of $A/\langle 2 \rangle F^{*2}$ orthogonal to

$$(\underset{\mathfrak{q}}{-1}, 1, \cdots).$$

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

$$(\underset{\mathfrak{q}}{1 - i}, \cdots)$$

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

$$(y, (\underset{\mathfrak{q}}{1 - i}, \cdots)) = (y, 1 - i)_{\mathfrak{q}} = (y, 2)_2.$$

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

$$(y, (\underset{\mathfrak{q}}{1 - i}, \cdots)) = 1$$

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

$$(\alpha, (\underset{\mathfrak{q}}{1 - i}, \cdots)) = (-1)^{(d-1)/8}$$

Now,

$$(\pm\alpha\bar{\alpha}, 1-i)_{\mathfrak{q}} = (\pm 2s^2, 2)_2 = 1,$$

so

$$(\alpha, 1-i)_{\mathfrak{q}} = (\bar{\alpha}, 1-i)_{\mathfrak{q}} = (-\alpha, 1-i)_{\mathfrak{q}} = (-\bar{\alpha}, 1-i)_{\mathfrak{q}},$$

and there is no loss in assuming that if $\alpha = a+b\sqrt{-d} = a+ib\sqrt{d}$ in $F_{\mathfrak{q}} \approx \mathbb{Q}_2(i)$, then $a \equiv \sqrt{d} \equiv -b \equiv 1(4)$ (we may assume that $2 \nmid \alpha$ since $(2, 1-i)_{\mathfrak{q}} = 1$, so s is odd). Because $a^2+b^2d = 2s^2$, 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 $u \equiv 1(\mathfrak{q}^5)$. But then $u \in F_{\mathfrak{q}}^{*2}$ by the theory of local fields, so

$$\begin{aligned}(\alpha, 1-i)_{\mathfrak{q}} &= (\alpha/1-i, 1-i)_{\mathfrak{q}} \\ &\qquad \text{since} \quad (1-i, 1-i)_{\mathfrak{q}} = (-1, 1-i)_{\mathfrak{q}} = (i, 1-i)_{\mathfrak{q}}^2 = 1 \\ &= (\sqrt{d}, 1-i)_{\mathfrak{q}} \quad \text{since } u \text{ is a square} \\ &= (\sqrt{d}, 2)_2 = (-1)^{(d-1)/8}.\end{aligned}$$

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 $\ell | m \Rightarrow \ell | a^2 - s^2 = s^2 - b^2 d$) 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 θ by

$$\prod_{\substack{p|\mathscr{D}\\ p\neq 2}}{}' \{\pm 1\} \quad \text{if} \quad d' \equiv \pm 3(8), \quad \text{and by} \prod_{\substack{p|\mathscr{D}\\ p\neq p_0}} \{\pm 1\} \quad \text{if} \quad d' \equiv \pm 1(8),$$

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 θ is surjective, etc. It is this form of the map θ 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. $F(\sqrt{\sqrt{-2}})$, lie in a $\mathbb{Z}_2$-extension of F.

5. We illustrate with two examples.

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

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

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 $|T| \geqq 4$.
(b) If $p \equiv 1(8)$ and $(p/q) = -1$ then $T = T_2 \approx \mathbb{Z}/2\mathbb{Z}$ and $F(\sqrt{-2})$ lies in L
(c) If $p \equiv 5(8)$ and $(p/q) = 1$ then $T = T_2 \approx \mathbb{Z}/2\mathbb{Z}$ and $F(\sqrt{p})$ lies in L
(d) If $p \equiv 5(8)$ and $(p/q) = -1$ then $T = T_2 \approx \mathbb{Z}/2\mathbb{Z}$ 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^S. Any such z would map to a square root of $\tilde{\mathfrak{p}}_{73}$ in C. Let $\beta = \frac{73}{2} + \frac{3}{2}\sqrt{-219}$. Since $N_{F/Q}\beta = 73.5^2$, we have $(\beta) = \mathfrak{p}_{73}\mathfrak{p}_5^2$ for some $\mathfrak{p}_5 | 5$ (5 splits in F), and $\tilde{\mathfrak{p}}_{73} = \tilde{\mathfrak{p}}_5^{-2}$ in C. Thus as a first guess for z we use

$$(\cdots, \underset{\mathfrak{p}_5}{\tfrac{1}{5}}, \cdots).$$

Now

$$(\cdots, \underset{\mathfrak{p}_5}{\tfrac{1}{5}}, \cdots)^2 \equiv (\beta)(\cdots, 1/5^2, \cdots) \equiv (\underset{\mathfrak{q}}{\beta}, \cdots, \underset{\mathfrak{p}_5}{73/\bar{\beta}}, \cdots, \underset{\mathfrak{p}_{73}}{\beta}, \cdots)$$
$$\equiv (\underset{\mathfrak{q}}{\beta}, \cdots, \underset{\mathfrak{p}_{73}}{\sqrt{-219}}, \cdots) \bmod F^*J^S$$

since $\mathfrak{p}_5 \not| \bar{\beta}$ and β and $\sqrt{-219}$ are both exactly divisible by $\mathfrak{p}_{73}$. Now,

$$x_{73} = (\underset{\mathfrak{q}}{\sqrt{73}}, \cdots, \underset{\mathfrak{p}_{73}}{\sqrt{-219}}),$$

so if we can find a square root, γ, of $\sqrt{73}/\beta$ in $F_{\mathfrak{q}}$, then we can take

$$z = (\underset{\mathfrak{q}}{\gamma}, \cdots, \underset{\mathfrak{p}_5}{\tfrac{1}{5}}, \cdots).$$

In $F_{\mathfrak{q}} = \mathbb{Q}_2(\sqrt{-3})$ we have $\beta/\sqrt{73} = \sqrt{73}/2+\frac{3}{2}\sqrt{-3}$.
$3^2 \equiv 73(64)$, so $3 \equiv \sqrt{73}(32)$, $\frac{3}{2} \equiv \sqrt{73}/2(16)$, thus

$$\beta/\sqrt{73} \equiv -3(-\tfrac{1}{2}-\tfrac{1}{2}\sqrt{-3})(16)$$

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

$$(-2, z) = (-2, \gamma)_{\mathfrak{q}}(-2, \tfrac{1}{5})_{\mathfrak{p}_5} = (-2, 1/\rho\sqrt{-3})_{\mathfrak{q}}(-2, \tfrac{1}{5})_5$$

since $\rho\sqrt{-3}/\sqrt{\beta/\sqrt{73}} \in F_{\mathfrak{q}}^2$ and 5 splits. Thus

$$(-2, z) = (-2, \tfrac{1}{3})_2(-2, \tfrac{1}{5})_5 = 1\cdot(-1) = -1.$$

It follows that z generates T (and so $|T| = 4$) because $A/\langle 2\rangle F^{*2} \times \langle z\rangle/\langle z\rangle^2$ has kernel on the left of order 2. To finish, we observe

$$(73, z) = (73, 1/\rho\sqrt{-3})_{\mathfrak{q}}(73, \tfrac{1}{5})_{\mathfrak{p}_5} = (73, \tfrac{1}{3})_2(73, \tfrac{1}{5})_5 = 1\cdot(-1) = -1.$$

Thus $F(\sqrt{-146})$ begins a Z_2-extension of F.

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

$$\theta(17) = ((17, 119)_7, (17, 119)_{17}) = ((\tfrac{17}{7}), (17, -7)_{17}) = ((\tfrac{17}{7}), (\tfrac{-7}{17})) = (-1, -1)$$

$$\theta(\alpha) = ((\tfrac{1}{2}, 119)_7(\tfrac{1}{2}, 119)_{17}) = (1, 1).$$

Since θ has kernel of order 2 generated by α, 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

[1] EDWARD A. BENDER: *A Lifting Formula for the Hilbert Symbol*. Proc. Am. Math. Soc., Vol. 40. No. 1, Sept. 1973.

[2] J. W. S. CASSELS and A. FRÖHLICH: *Algebraic Number Theory*, Thompson Book Company, 1967.

[3] HELMUT HASSE: *Zahlentheorie*, Akademie-Verlag, 1949.
[4] JEAN-PIERRE SERRE: *Classes Des Corps Cyclotomic*, Seminairé Bourbaki, Dec. 1958.
[5] JEAN-PIERRE SERRE: *Corps Locaux*, Hermann, 1962.

(Oblatum 28–IX–1974)

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