Author: Kilicer, P.
Title: The CM class number one problem for curves
Issue Date: 2016-07-05

Chapter 2

The CM class number one problem for curves of genus 2

ABSTRACT. In this chapter, we list all quartic CM fields that correspond to CM curves of genus 2 *defined over the reflex field. This chapter is an adaptation of a joint work with Marco Streng that appears as* The CM class number one problem for curves of genus 2 *[18]. The facts in Section 2.2 are presented only for quartic CM fields in the paper [18] and are presented in a more general form in this thesis so that they can be used in Chapter 3.*

2.1 Introduction

Let K be a non-biquadratic quartic (i.e., $\mathrm{Gal}(K/\mathbb{Q}) \not\cong C_2 \times C_2$) CM field and Φ be a primitive CM type of K. Let C be a curve of genus 2 with *simple* Jacobian $J(C)$ of type (K, Φ) with CM by $\mathcal{O}_K$. Let (K^r, Φ^r) be the reflex of (K, Φ) and let N_{Φ^r} be the type norm of (K^r, Φ^r) as defined in (1.2.1). Recall

$$I_0(\Phi^r) := \{\mathfrak{b} \in I_{K^r} : \ \mathrm{N}_{\Phi^r}(\mathfrak{b}) = (\alpha), \ \alpha\overline{\alpha} \in \mathbb{Q} \text{ for some } \alpha \in K^\times\}.$$

Theorem 1.5.6 implies that if C is defined over the reflex field K^r, then the CM class group $I_{K^r}/I_0(\Phi^r)$ is trivial. Murabayashi and Umegaki [31] listed all quartic CM fields K corresponding to the rational abelian surfaces with CM by $\mathcal{O}_K$. This list contains only cyclic quartic CM fields, but not the generic dihedral quartic CM fields because curves cannot be defined over $\mathbb{Q}$ in the dihedral case. The reason for this is that in the dihedral case the reflex field K^r is not normal over $\mathbb{Q}$ (see Figure 2.1) and hence the curve C is not defined over $\mathbb{Q}$ by Proposition 5.17 in Shimura [39] (see also Proposition 4.2.1 in Chapter 4). In this chapter, we give the *complete* list of CM class number one non-biquadratic quartic fields, thereby solving the *CM class number one problem for curves of genus* 2 and showing the list in Bouyer–Streng [9] is complete.

In the genus-2 case, the quartic CM field K is either cyclic Galois, biquadratic Galois, or non-Galois with Galois group D_4 (Shimura [40, Example 8.4(2)]). We restrict ourselves to CM curves with a simple Jacobian, which therefore have primitive CM types by Theorem 1.4.1. The corresponding CM fields of such curves are not biquadratic, by Example 8.4-(2) in Shimura [40]

Theorem 2.1.1. *There exist exactly* 63 *isomorphism classes of non-normal quartic CM fields with CM class number one. The fields are listed in Theorem 2.3.15.*

Theorem 2.1.2. *There exist exactly* 20 *isomorphism classes of cyclic quartic CM fields with CM class number one. The fields are listed in Theorem 2.4.5.*

Remark that the list in Theorem 2.4.5 contains the list in [31].

Corollary 2.1.3. *There are exactly* 125 *curves of genus* 2*, up to isomorphism over* $\overline{\mathbb{Q}}$*, defined over the reflex field with CM by* $\mathcal{O}_K$ *for some non-biquadratic quartic CM field* K*. The fields are the fields in Theorems 2.1.1 and 2.1.2, and the curves are those of Bouyer–Streng [9, Tables 1a, 1b, 2b, and 2c].*

Proof. This follows from the list given by Bouyer–Streng in [9] and Theorems 2.1.1–2.1.2. □

Corollary 2.1.4. *There are exactly* 21 *simple CM curves of genus* 2 *defined over* $\mathbb{Q}$*, up to isomorphism over* $\overline{\mathbb{Q}}$*. The fields and* 19 *of the* *curves are given in van Wamelen [45]. The other two curves are* $y^2 = x^6 - 4x^5 + 10x^3 - 6x - 1$ *and* $y^2 = 4x^5 + 40x^4 - 40x^3 + 20x^2 + 20x + 3$ *given in Theorem 14 of Bisson–Streng [7].*

Proof. The 19 curves given in [9] are the curves of genus 2 defined over $\mathbb{Q}$ with CM by $\mathcal{O}_K$, see [31] or Corollary 2.1.3. In [7], Bisson–Streng prove that there are only 2 curves of genus 2 defined over $\mathbb{Q}$ with CM by a non-maximal order inside one of the fields of Theorem 2.4.5. Theorem 2.1.2 and Proposition 5.17 in Shimura [39] (see also Proposition 4.2.1 in Chapter 4) finish the proof. □

Corollary 2.1.5. *There are only finitely many simple CM curves of genus 2 defined over the reflex field. The corresponding CM fields are those of Theorems 2.1.1–2.1.2, the complete list of orders can be computed using the methods of [7] and the curves using the methods of [9].* □

In Section 2.2, we present general facts about CM fields that we need in this chapter and Chapter 3. Then in Section 2.3, we prove Theorem 2.1.1. The strategy is as follows. We first show that there are only finitely many non-biquadratic quartic CM fields with CM class number one by bounding their absolute discriminant. The bound will be too large for practical purposes, but by using ramification theory and L-functions, we improve the bound which we then use to enumerate the CM fields. Section 2.4 proves Theorem 2.1.2 using the same strategy as in Section 2.3.

2.2 The relative class number

Let K be a CM field with the maximal totally real subfield F of degree g and $h_K^* := h_K/h_F$. In this section, we will present the sufficient conditions for CM class number one fields to satisfy $h_K^* = 2^{t_K-1}$, where t_K is the number of primes in F that are ramified in K.

Recall that I_K is the group of fractional ideals in K and P_K is the group of principal fractional ideals in K.

Lemma 2.2.1. *Let K be a CM field and let F be the maximal totally real subfield of K. Let H denote the group* $\mathrm{Gal}(K/F)$. *Put* $I_K^H = \{\mathfrak{b} \in I_K \mid \overline{\mathfrak{b}} =$

$\mathfrak{b}\}$ *and* $P_K^H = P_K \cap I_K^H$. *Then we have* $h_K^* = 2^{t_K} \frac{[I_K : I_K^H P_K]}{[P_K^H : P_F]}$, *where* t_K *is the number of primes in* F *that are ramified in* K.

Proof. We have the exact sequence

$$1 \to I_F \to I_K^H \to \bigoplus_{\mathfrak{p} \text{ prime of } F} \mathbb{Z}/e_{K/F}(\mathfrak{p})\mathbb{Z} \to 1 \tag{2.2.1}$$

and

$$\bigoplus_{\mathfrak{p} \text{ prime of } F} \mathbb{Z}/e_{K/F}(\mathfrak{p})\mathbb{Z} \quad \cong \quad (\mathbb{Z}/2\mathbb{Z})^{t_K}.$$

The map $\varphi : I_K^H \to I_K/P_K$ induces an isomorphism

$$I_K^H/P_K^H \cong \mathrm{im}(\varphi) = I_K^H P_K/P_K$$

so by (2.2.1), we have

$$h_F = [I_F : P_F] = \frac{[I_K^H : P_K^H][P_K^H : P_F]}{[I_K^H : I_F]} = 2^{-t_K}[I_K^H P_K : P_K][P_K^H : P_F],$$

hence

$$h_K^* := \frac{h_K}{h_F} = 2^{t_K} \frac{[I_K : I_K^H P_K]}{[P_K^H : P_F]}.$$

□

Lemma 2.2.2. *Let* K *be a CM field with the maximal totally real subfield* F. *Let* W_K *be the group of roots of unity of* K. *If the Hasse unit index* $Q_K := [\mathcal{O}_K^\times : W_K \mathcal{O}_F^\times]$ *is* 1, *then we have* $[P_K^H : P_F] = 2$ *and* $h_K^* = 2^{t_K - 1}[I_K : I_K^H P_K]$.

Proof. Define $\varphi : \mathcal{O}_K^\times \to \mathcal{O}_K^\times$ by $\varphi(\epsilon) = \epsilon/\overline{\epsilon}$. Then by the assumption $\mathcal{O}_K^\times = W_K \mathcal{O}_F^\times$, we have $\varphi(\epsilon) = \zeta/\overline{\zeta} = \zeta^2$, where $\epsilon = \zeta\epsilon_0$ with $\zeta \in W_K$ and $\epsilon_0 \in \mathcal{O}_F^\times$. Hence $\operatorname{Im}\varphi = W_K^2$.

There is a surjective group homomorphism $\lambda : P_K^H \to W_K/W_K^2$ given by $\lambda((\alpha)) = \alpha/\overline{\alpha}$. The map λ is well-defined because every generator of (α) equals $u \cdot \alpha$ for some $u \in \mathcal{O}_K^\times$ and $u/\overline{u} \in W_K^2$. It now suffices to prove that the kernel is P_F. Suppose $\alpha \in F^\times$. Then $\lambda((\alpha)) = \alpha/\overline{\alpha} = 1$, hence

$(\alpha) \in \ker(\lambda)$. Conversely, suppose $\lambda((\alpha)) \in W_K^2$. Then we have $\alpha \in F^\times$, hence $(\alpha) \in P_F$. It follows that $\ker(\lambda) = P_F$.

The latter equality follows from Lemma 2.2.1 and the fact $[P_K^H : P_F] = 2$.

□

Recall

$$I_0(\Phi^r) := \{\mathfrak{b} \in I_{K^r} :\ \mathrm{N}_{\Phi^r}(\mathfrak{b}) = (\alpha),\ \mathrm{N}_{K^r/\mathbb{Q}}(\mathfrak{b}) = \alpha\overline{\alpha} \text{ for some } \alpha \in K^\times\}.$$

Lemma 2.2.3. *Let (K, Φ) be a primitive CM pair. If for every $\mathfrak{a} \in I_K$, we have*

$$\mathrm{N}_{\Phi^r}\mathrm{N}_{\Phi}(\mathfrak{a}) = (\alpha)\mathfrak{a}\overline{\mathfrak{a}}^{-1} \text{ and } \alpha\overline{\alpha} \in \mathbb{Q}, \tag{2.2.2}$$

where $\alpha \in K^\times$, then we have $[I_K : I_K^H P_K] \leq [I_{K^r} : I_0(\Phi^r)]$.

Proof. To prove the assertion, we show that the kernel of the map $\mathrm{N}_\Phi : I_K \to I_{K^r}/I_0(\Phi^r)$ is contained in $I_K^H P_K$. Suppose $\mathrm{N}_\Phi(\mathfrak{a}) \in I_0(\Phi^r)$. Then by (2.2.2), we have $(\alpha)\mathfrak{a}\overline{\mathfrak{a}}^{-1} = (\lambda)$, where $\lambda \in K^\times$ and $\lambda\overline{\lambda} = \alpha\overline{\alpha} \in \mathbb{Q}$. Then $\mathfrak{a}\overline{\mathfrak{a}}^{-1} = (\delta)$ with $\delta = \lambda/\alpha$, and hence $\delta\overline{\delta} = 1$. There is a $\gamma \in K^\times$ such that $\delta = \frac{\overline{\gamma}}{\gamma}$ (this is a special case of Hilbert's Theorem 90, but can be seen directly by taking $\gamma = \overline{\epsilon} + \overline{\delta}\epsilon$ for any $\epsilon \in K$ with $\gamma \neq 0$). Thus we have $\mathfrak{a} = \overline{\gamma\mathfrak{a}} \cdot (\frac{1}{\gamma}) \in I_K^H P_K$ and therefore $[I_K : I_K^H P_K] \leq [I_{K^r} : I_0(\Phi^r)]$. □

Proposition 2.2.4. *Let K be a CM field and let F be the maximal totally real subfield of K. Suppose $I_0(\Phi^r) = I_{K^r}$. If K satisfies* (2.2.2)*, then we have $h_K^* = 2^T$ with $T \in \{t_K,\ t_K - 1\}$, where t_K is the number of primes in F that are ramified in K. Moreover, if $\mathcal{O}_K^\times = W_K\mathcal{O}_F^\times$ then $T = t_K - 1$.*

Proof. By Lemma 2.2.1, we have

$$h_K^* = 2^{t_K}\frac{[I_K : I_K^H P_K]}{[P_K^H : P_F]}.$$

Lemma 2.2.3 with the assumption $I_0(\Phi^r) = I_{K^r}$ implies $[I_K : I_K^H P_K] = 1$. Hence it follows that $h_K^* = 2^{t_K}[P_K^H : P_F]^{-1} = 2^T$ with $T \in \{t_K,\ t_K - 1\}$ as $[P_K^H : P_F] \in \{1,\ 2\}$.

Moreover, if $\mathcal{O}_K^\times = W_K\mathcal{O}_F^\times$, then by Lemma 2.2.2, we get $[P_K^H : P_F] = 1$ and hence $h_K^* = 2^{t_K - 1}$. □

2.3 Non-normal quartic CM fields

This section, which is the largest in this chapter, proves Theorem 2.1.1. The case of cyclic CM fields is much easier and is treated in Section 2.4.

Suppose that $K/\mathbb{Q}$ is a non-normal quartic CM field and F is the real quadratic subfield of K. The normal closure N is a dihedral CM field of degree 8 with Galois group $G := \mathrm{Gal}(N/\mathbb{Q}) = \langle x,\ y : y^4 = x^2 = (xy)^2 = \mathrm{id}\rangle$. Complex conjugation $\bar{\cdot}$ is y^2 in this notation and the CM field K is the subfield of N fixed by $\langle x\rangle$. Let Φ be a CM type of K with values in N'. We can (and do) identify N with a subfield of N' in such a way that $\Phi = \{\mathrm{id}, y|_K\}$. Then the reflex field K^r of Φ is the fixed field of $\langle xy\rangle$, which is a non-normal quartic CM field non-isomorphic to K with reflex type $\Phi^r = \{\mathrm{id}, y^3|_{K^r}\}$, (see [40, Examples 8.4., 2(C)]). Denote the quadratic subfield of K^r by F^r.

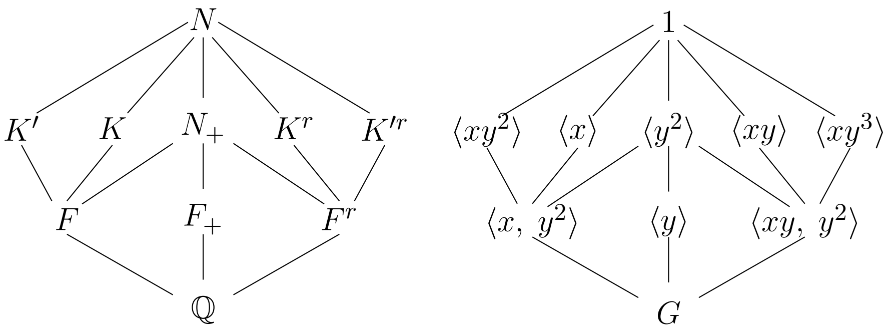

Figure 2.1: Lattice of subfields and subgroups

Let N_+ be the maximal totally real subfield of N, and let F_+ be the quadratic subfield of N_+ such that N/F_+ is cyclic.

2.3.1 An effective bound for CM class number one non-normal quartic fields

In this section, we find an effective upper bound for the absolute discriminant of non-normal quartic CM fields with CM class number one.

Proposition 2.3.1. *Let K be a non-biquadratic quartic CM field and let F be the real quadratic subfield of K. Assuming $I_0(\Phi^r) = I_{K^r}$, we have $h_K^* = 2^{t_K-1}$, where t_K is the number of primes in F that are ramified in K.*

Moreover, we have $h_{K^r}^* = 2^{t_{K^r}-1}$, where t_{K^r} is the number of primes in F^r that are ramified in K^r.

Proof. Since $\mu_K = \{\pm 1\}$, by Lemma 2.2.2, we have $h_K^* = 2^{t_K-1}[I_K : I_K^H P_K]$. For any $\mathfrak{a} \in I_K$, we can compute (see [38, (3.1)])

$$\mathrm{N}_{\Phi^r}\mathrm{N}_{\Phi}(\mathfrak{a}) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})\mathfrak{a}\overline{\mathfrak{a}}^{-1}.$$

Then, by Lemma 2.2.3, under the assumption $I_0(\Phi^r) = I_{K^r}$, the quotient $I_K/I_K^H P_K$ is trivial. Therefore, we have $h_K^* = 2^{t_K-1}$.

For the second statement, we claim $[I_{K^r} : I_{K^r}^{H'} P_{K^r}] \leq [I_{K^r} : I_0(\Phi^r)]$, where $H' = \mathrm{Gal}(K^r/F^r)$. For any $\mathfrak{b} \in I_{K^r}$, by [38, (3.2)], we have

$$\mathrm{N}_{\Phi}\mathrm{N}_{\Phi^r}(\mathfrak{b}) = \mathrm{N}_{K^r/\mathbb{Q}}(\mathfrak{b})\mathfrak{b}\overline{\mathfrak{b}}^{-1}.$$

Suppose $\mathfrak{b} \in I_0(\Phi^r)$. Then $N_{K^r/\mathbb{Q}}(\mathfrak{b})\mathfrak{b}\overline{\mathfrak{b}}^{-1} = (\alpha)$, where $\alpha \in K^{r\times}$ and $\alpha\overline{\alpha} = N_{\Phi}(N_{K^r/\mathbb{Q}}(\mathfrak{b})) = N_{K^r/\mathbb{Q}}(\mathfrak{b})^2 \in \mathbb{Q}$. We finish the proof of $\mathfrak{b} \in I_{K^r}^{H'} P_{K^r}$ exactly as in Lemma 2.2.3. So this proves $I_0(\Phi^r) \subset I_{K^r}^{H'} P_{K^r}$, hence the claim follows.

Since $\mu_{K^r} = \{\pm 1\}$, by Lemma 2.2.2, we have $h_{K^r}^* = 2^{t_{K^r}-1}[I_{K^r} : I_{K^r}^{H^r} P_{K^r}]$. By the assumption $I_0(\Phi^r) = I_{K^r}$, the claim above implies $[I_{K^r} : I_{K^r}^{H^r} P_{K^r}] = 1$, hence we get $h_{K^r}^* = 2^{t_{K^r}-1}$.

□

Remark 2.3.2. In the case where $K/\mathbb{Q}$ is cyclic quartic, this result is $(i) \Rightarrow (iii)$ of Proposition 4.5 in Murabayashi [30].

On the other hand, if K is a non-normal quartic CM field, Louboutin proves $h_K^* \approx \sqrt{d_K/d_F}$ with an effective error bound, see Proposition 2.3.3. Putting this together with the result in Proposition 2.3.1 gives approximately $\sqrt{d_K/d_F} \leq 2^{t_K-1}$. As the left hand side grows more quickly than the right, this relation will give a bound on the absolute value of the discriminant, precisely see Proposition 2.3.4.

The next step is to use the following bound from analytic number theory.

Let d_M denote the absolute value of the discriminant (absolute discriminant) of a number field M.

Proposition 2.3.3. *(Louboutin [26], Remark 27 (1)) Let N be the normal closure of a non-normal quartic CM field K with Galois group D_4. Assume $d_N^{1/8} \geq 222$. Then*

$$h_K^* \geq \frac{2\sqrt{d_K/d_F}}{\sqrt{e}\pi^2(\log(d_K/d_F)+0.057)^2}. \qquad \square \tag{2.3.1}$$

Proposition 2.3.4. *Let K be a non-normal quartic CM field and let F be the real quadratic subfield of K. Let Φ be a primitive CM type of K. Suppose $I_0(\Phi^r) = I_{K^r}$. Then we have $d_K/d_F \leq 2 \cdot 10^{15}$.*

Proof. Let

$$f(D) = \frac{2\sqrt{D}}{\sqrt{e}\pi^2(\log(D)+0.057)^2} \quad \text{and} \quad g(t) = 2^{-t+1}f(\Delta_t),$$

where $\Delta_k = \prod_{j=1}^{k} p_j$ and p_j is the j-th prime.

Here, if $D = d_K/d_F$, then f is the right hand side of the inequality (2.3.1) in Proposition 2.3.3. The quotient d_K/d_F is divisible by the product of rational primes that are ramified in K/F, so $d_K/d_F \geq \Delta_{t_K}$.

On the other hand, the function f is monotonically increasing for $D > 52$, so if $t_K \geq 4$ then $f(d_K/d_F) \geq f(\Delta_{t_K})$. Therefore, by Proposition 2.3.1, we get that if $I_0(\Phi^r) = I_{K^r}$, then

$$2^{t_K-1} \geq f(d_K/d_F) \geq f(\Delta_{t_K}) \tag{2.3.2}$$

and hence $1 \geq g(t_K)$. The function g is monotonically increasing for $t_K \geq 4$ and is greater than 1 if $t_K > 14$. Therefore, we get $t_K \leq 14$ and $h_K^* \leq 2^{13}$, hence $d_K/d_F < 2 \cdot 10^{15}$. $\square$

The bound that we get in Proposition 2.3.4 is unfortunately too large to list all the fields. In the following section we study ramification of primes in $N/\mathbb{Q}$ and find a sharper upper bound for d_{K^r}/d_{F^r}, see Proposition 2.3.14.

2.3.1.1 Almost all ramified primes are inert in F and F^r

In this section, under the assumption $I_0(\Phi^r) = I_{K^r}$, we study the ramification behavior of primes in $N/\mathbb{Q}$, and prove that almost all rational primes that are ramified in K^r/F^r are inert in F^r. We precisely prove the following proposition.

Proposition 2.3.5. *Let K be a non-normal quartic CM field and let F be its real quadratic subfield. Let Φ be a primitive CM type of K. Suppose $I_0(\Phi^r) = I_{K^r}$. Then $F = \mathbb{Q}(\sqrt{p})$ and $F^r = \mathbb{Q}(\sqrt{q})$, where p and q are prime numbers with $q \not\equiv 3 \pmod 4$ and $(p/q) = (q/p) = 1$. Moreover, all the rational primes (distinct from p and q) that are ramified in K^r/F^r are inert in F and F^r.*

This proposition implies that d_{K^r}/d_{F^r} grows as the square of the product of such ramified primes and we get a lower bound on $f(d_{K^r}/d_{F^r})$ of (2.3.2) that grows even faster with t_{K^r} than what we had in the proof of Proposition 2.3.4. Hence we obtain a better upper bound on d_{K^r}/d_{F^r}, see Proposition 2.3.14.

We begin the proof of Proposition 2.3.5 with exploring the ramification behavior of primes in $N/\mathbb{Q}$, under the assumption $I_0(\Phi^r) = I_{K^r}$.

Ramification of primes in $N/\mathbb{Q}$

Lemma 2.3.6. *Let M/L be a Galois extension of number fields and $\mathfrak{q}$ be a prime of M over an odd prime ideal $\mathfrak{p}$ (that is, the prime $\mathfrak{p}$ lies over an odd prime in $\mathbb{Q}$) of L. Then there is no surjective homomorphism from a subgroup of $I_{\mathfrak{q}}$ to a Klein four group V_4.*

Proof. For an odd prime ideal $\mathfrak{p}$ in L, suppose that there is a surjective homomorphism from a subgroup of $\mathrm{I}_{\mathfrak{q}}$ to V_4. In other words, suppose a prime of F over $\mathfrak{p}$ is totally ramified in a biquadratic intermediate extension E/F of M/L. Assume without loss of generality $E = M$ and $F = L$. The biquadratic intermediate extension E/F has three quadratic intermediate extensions $E_i = F(\sqrt{\alpha_i})$ for $i = 1,\ 2,\ 3$. Without loss of generality, take $\mathrm{ord}_{\mathfrak{p}}(\alpha_i) \in \{0,1\}$ for each i. Note $\mathcal{O}_{E_i}$ contains $\mathcal{O}_F[\sqrt{\alpha_i}]$ of relative discriminant $4\alpha_i$ over $\mathcal{O}_F$. Since $\mathfrak{p}$ is odd, this implies that the relative discriminant $\Delta(E_i/F)$ of $\mathcal{O}_{E_i}$ has $\mathrm{ord}_{\mathfrak{p}}(\Delta(E_i/F)) = \mathrm{ord}_{\mathfrak{p}}(\alpha_i)$. At the same time, we have $E_3 = F(\sqrt{\alpha_1\alpha_2})$ so $\mathfrak{p}$ ramifies in E_i for an even number of i's. In particular, $\mathfrak{p}$ is not totally ramified in E/F. $\square$

Lemma 2.3.7. *Let K be a non-normal quartic CM field and let F be the real quadratic subfield of K. Let Φ be a primitive CM type of K and K^r be the reflex field of (K, Φ) with the quadratic subfield F^r. Then the following assertions hold.*

(i) If a prime p is ramified in both F and F^r, then it is totally ramified in $K/\mathbb{Q}$ and $K^r/\mathbb{Q}$.

(ii) If an odd prime p is ramified in F (in F^r, respectively) as well as in F_+, then p splits in F^r (in F, respectively). Moreover, at least one of the primes above p in F^r is ramified in K^r/F^r (in K/F, respectively).

Proof. The statements (i) and (ii) are clear from Table 2.1 on page 32. Alternatively, one can also prove the statements as follows:

(i) Let $\mathfrak{p}_N$ be a prime of N above p that is ramified in both $F/\mathbb{Q}$ and $F^r/\mathbb{Q}$. Then the maximal unramified subextension of $N/\mathbb{Q}$ is contained in F_+. Therefore, the inertia group of $\mathfrak{p}_N$ contains $\mathrm{Gal}(N/F_+) = \langle y \rangle$. By computing ramification indices in the diagram of subfields one by one, we see that the prime p is totally ramified in K and K^r.

(ii) Let p be an odd prime that is ramified in $F/\mathbb{Q}$ and $F_+/\mathbb{Q}$ and $\mathfrak{p}_N$ be a prime above p in N. The inertia group of an odd prime cannot be a biquadratic group by Lemma 2.3.6, so $\mathrm{I}_{\mathfrak{p}_N}$ is a proper subgroup of $\mathrm{Gal}(N/F^r)$. Since $\mathrm{I}_{\mathfrak{p}_N}$ is a normal subgroup in $\mathrm{D}_{\mathfrak{p}_N}$, the group $\mathrm{D}_{\mathfrak{p}_N}$ cannot be the full Galois group $\mathrm{Gal}(N/\mathbb{Q})$. So $\mathrm{D}_{\mathfrak{p}_N}$ is a proper subgroup of $\mathrm{Gal}(N/F^r)$ and hence p splits in F^r. Moreover, since p is ramified in F, hence in K, hence in K^r, at least one of the primes above p in F^r is ramified in K^r. Since F and F^r are symmetric in $N/\mathbb{Q}$, the same argument holds for F^r as well.

$\square$

Lemma 2.3.8. *Let the notation be as in Lemma 2.3.7. Assuming $I_0(\Phi^r) = I_{K^r}$, if K^r has a prime $\mathfrak{p}$ of prime norm p with $\overline{\mathfrak{p}} = \mathfrak{p}$, then $F = \mathbb{Q}(\sqrt{p})$.*

Proof. By the assumption, we have

$$\mathrm{N}_{\Phi^r}(\mathfrak{p}) = (\alpha) \text{ for some } \alpha \in K^\times \text{such that } \alpha\overline{\alpha} = \mathrm{N}_{K^r/\mathbb{Q}}(\mathfrak{p}) = p.$$

Since $\overline{\mathfrak{p}} = \mathfrak{p}$, we have $(\alpha) = (\overline{\alpha})$, and so $\alpha = \epsilon\overline{\alpha}$ for a unit ϵ in $\mathcal{O}_K^\times$ with absolute value 1 (hence a root of unity). Since $\mu_K = \{\pm 1\}$, we get $\alpha^2 = \pm p$. The case $\alpha^2 = -p$ is not possible, since K has no imaginary quadratic intermediate field. Hence we have $\alpha^2 = p$ and so $\sqrt{p} \in F$. □

Corollary 2.3.9. *The notation being as in Lemma 2.3.7, suppose $I_0(\Phi^r) = I_{K^r}$. If p is totally ramified in $K^r/\mathbb{Q}$, or splits in $F^r/\mathbb{Q}$ and at least one of the primes over p in F^r ramifies in K^r/F^r, then $F = \mathbb{Q}(\sqrt{p})$.* □

Proposition 2.3.10. *Suppose $I_0(\Phi^r) = I_{K^r}$. Then $F = \mathbb{Q}(\sqrt{p})$, where p is a rational prime.*

Proof. Suppose that there is an odd prime p that is ramified in F. Then p is ramified either in F and F^r or in F and F_+.

If p is ramified in both F and F^r, then by Lemma 2.3.7-(i), the prime p is totally ramified in $K^r/\mathbb{Q}$. If p is ramified in F and F_+, then by Lemma 2.3.7-(ii), the prime p splits in F^r and at least one of the primes over p in F^r ramifies in K^r/F^r. In both cases, Corollary 2.3.9 tells us that $F = \mathbb{Q}(\sqrt{p})$.

Therefore, if an odd prime p is ramified in F, then we have $F = \mathbb{Q}(\sqrt{p})$. If no odd prime ramifies in F, then the only prime that ramifies in F is 2 so we have $F = \mathbb{Q}(\sqrt{2})$. □

Table 2.1: Ramification table of a non-normal quartic CM field

Table 2.3.1.1 lists all 19 pairs (I, D) where $1 \neq \mathrm{I} \lhd \mathrm{D} \leq D_4 = \langle x,\ y \rangle$ and D/I is cyclic, partitioned into 15 conjugacy classes (1) – (15). In particular, it contains all possible inertia and decomposition groups of ramified primes of N. This table is a corrected subset of [14, Table 3.5.1]. We restricted to $\mathrm{I} \neq 1$, added the case 8-(b), which is missing in [14, Table 3.5.1], and corrected the type norm column of some cases. The cases (11) – (15) can only occur for the prime 2, see Lemma 2.3.6. If there is a checkmark in the last column, then by Lemma 2.3.8, such splitting implies $\sqrt{p} \in F$ (i.e., $F = \mathbb{Q}(\sqrt{p})$) under the assumption $I_0(\Phi^r) = I_{K^r}$. The cases with * do not occur under the assumption $I_0(\Phi^r) = I_{K^r}$ because p is not ramified in F in these cases, but on the other hand $\sqrt{p} \in F$ by Lemma 2.3.8.

Case	I	D	decomp. of p in N	decomp. of p in K	decomp. of p in F	decomp. of p in F_+	decomp. of p in F^r	decomp. of p in K^r	$N_{\Phi^r}(\mathfrak{p}_{K^r,1})$	$\sqrt{p} \in F$
(1)*	$\langle y^2 \rangle$	$\langle y^2 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,x}^2\mathfrak{p}_{N,y}^2\mathfrak{p}_{N,xy}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}^2$	$\mathfrak{p}_{F,1}\mathfrak{p}_{F,y}$	$\mathfrak{p}_{F_+,1}\mathfrak{p}_{F_+,y}$	$\mathfrak{p}_{F^r,1}\mathfrak{p}_{F^r,y}$	$\mathfrak{p}_{K^r,1}^2\mathfrak{p}_{K^r,y}^2$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}$	✓
(2)	$\langle y^2 \rangle$	$\langle y \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}^2$	$\mathfrak{p}_{F,1}$	$\mathfrak{p}_{F_+,1}\mathfrak{p}_{F_+,y}$	$\mathfrak{p}_{F^r,1}$	$\mathfrak{p}_{K^r,1}^2$	p	
(3)	$\langle y^2 \rangle$	$\langle x,\ y^2 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}^2$	$\mathfrak{p}_{F,1}\mathfrak{p}_{F,y}$	$\mathfrak{p}_{F_+,1}$	$\mathfrak{p}_{F^r,1}$	$\mathfrak{p}_{K^r,1}^2$	p	
(4)*	$\langle y^2 \rangle$	$\langle xy,\ y^2 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}^2$	$\mathfrak{p}_{F,1}$	$\mathfrak{p}_{F_+,1}$	$\mathfrak{p}_{F^r,1}\mathfrak{p}_{F^r,y}$	$\mathfrak{p}_{K^r,1}^2\mathfrak{p}_{K^r,y}^2$	$\mathfrak{p}_{K,1}$	✓
(5) (a)	$\langle x \rangle$	$\langle x \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2\mathfrak{p}_{N,y^2}^2\mathfrak{p}_{N,y^3}^2$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}^2\mathfrak{p}_{K,y^2}$	$\mathfrak{p}_{F,1}\mathfrak{p}_{F,y}$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^2\mathfrak{p}_{K^r,y^2}^2$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}$	
(5) (b)	$\langle xy^2 \rangle$	$\langle xy^2 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2\mathfrak{p}_{N,y^2}^2\mathfrak{p}_{N,y^3}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}\mathfrak{p}_{K,y^3}$	$\mathfrak{p}_{F,1}\mathfrak{p}_{F,y}$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^2\mathfrak{p}_{K^r,y}^2$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y^3}$	
(6) (a)	$\langle x \rangle$	$\langle x,\ y^2 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}^2$	$\mathfrak{p}_{F,1}\mathfrak{p}_{F,y}$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^2$	p	
(6) (b)	$\langle xy^2 \rangle$	$\langle x,y^2 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}$	$\mathfrak{p}_{F,1}\mathfrak{p}_{F,y}$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^2$	p	
(7) (a)	$\langle xy \rangle$	$\langle xy \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2\mathfrak{p}_{N,y^2}^2\mathfrak{p}_{N,y^3}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y^3}^2$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}\mathfrak{p}_{F^r,y}$	$\mathfrak{p}_{K^r,1}^2\mathfrak{p}_{K^r,y}\mathfrak{p}_{K^r,y^3}$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y^3}$	✓
(7) (b)	$\langle xy^3 \rangle$	$\langle xy^3 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2\mathfrak{p}_{N,y^2}^2\mathfrak{p}_{N,y^3}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}^2$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}\mathfrak{p}_{F^r,y}$	$\mathfrak{p}_{K^r,1}\mathfrak{p}_{K^r,y}^2\mathfrak{p}_{K^r,y^2}$	$\mathfrak{p}_{K,1}^2$	✓
(8) (a)	$\langle xy \rangle$	$\langle xy,y^2 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}^2$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}\mathfrak{p}_{F^r,y}$	$\mathfrak{p}_{K^r,1}^2\mathfrak{p}_{K^r,y}$	$\mathfrak{p}_{K,1}$	✓
(8) (b)	$\langle xy^3 \rangle$	$\langle xy,y^2 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}^2$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}\mathfrak{p}_{F^r,y}$	$\mathfrak{p}_{K^r,1}\mathfrak{p}_{K^r,y}^2$	p	✓
(9)	$\langle y \rangle$	$\langle y \rangle$	$\mathfrak{p}_{N,1}^4\mathfrak{p}_{N,y}^4$	$\mathfrak{p}_{K,1}^4$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}\mathfrak{p}_{F_+,y}$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^4$	$\mathfrak{p}_{K,1}^2$	✓
(10)	$\langle y \rangle$	G	$\mathfrak{p}_{N,1}^4$	$\mathfrak{p}_{K,1}^4$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^4$	$\mathfrak{p}_{K,1}^2$	✓
(11)*	$\langle x,y^2 \rangle$	$\langle x,y^2 \rangle$	$\mathfrak{p}_{N,1}^4\mathfrak{p}_{N,y}^4$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}^2$	$\mathfrak{p}_{F,1}\mathfrak{p}_{F,y}$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^4$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}$	✓
(12)*	$\langle x,y^2 \rangle$	G	$\mathfrak{p}_{N,1}^4$	$\mathfrak{p}_{K,1}^2$	$\mathfrak{p}_{F,1}$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^4$	$\mathfrak{p}_{K,1}$	✓
(13)	$\langle xy,y^2 \rangle$	$\langle xy,y^2 \rangle$	$\mathfrak{p}_{N,1}^4\mathfrak{p}_{N,y}^4$	$\mathfrak{p}_{K,1}^4$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}\mathfrak{p}_{F^r,y}$	$\mathfrak{p}_{K^r,1}^2\mathfrak{p}_{K^r,y}^2$	$\mathfrak{p}_{K,1}^2$	✓
(14)	$\langle xy,y^2 \rangle$	G	$\mathfrak{p}_{N,1}^4$	$\mathfrak{p}_{K,1}^4$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}$	$\mathfrak{p}_{K^r,1}^2$	p	
(15)	G	G	$\mathfrak{p}_{N,1}^8$	$\mathfrak{p}_{K,1}^4$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^4$	$\mathfrak{p}_{K,1}^2$	✓

Lemma 2.3.11. *Suppose $I_0(\Phi^r) = I_{K^r}$. Then the following assertions are true.*

(i) If a rational prime l is unramified in both $F/\mathbb{Q}$ and $F^r/\mathbb{Q}$, but is ramified in $K/\mathbb{Q}$ or $K^r/\mathbb{Q}$, then all primes above l in F and F^r are ramified in K/F and K^r/F^r and l is inert in F^r.

(ii) If $F = \mathbb{Q}(\sqrt{p})$ with a prime number $p \equiv 3 \pmod 4$, then 2 is inert in F^r.

Proof. (i) It follows from Table 2.1 except for the statement that l is inert in F^r.

Suppose that l splits in F^r. Then by Corollary 2.3.9, we have $\sqrt{l} \in F$, contradicts unramifiedness of l in F. Therefore, the prime l is inert in F^r.

(ii) The prime 2 is ramified in F since $p \equiv 3 \pmod 4$. If 2 is also ramified in F^r, then by Lemma 2.3.7-(i), the prime 2 is totally ramified in K and K^r. If 2 splits in F^r, then by Table 2.1, at least one of the primes in F^r above 2 ramifies in K^r. In both cases by Corollary 2.3.9, we have $F = \mathbb{Q}(\sqrt{p})$ with $p = 2$, a contradiction. This implies that 2 is inert in F^r.

□

Equality of t_K and t_{K^r}

In the previous section, we proved that the primes that are unramified in F and F^r, but are ramified in K^r/F^r are inert in F^r. Thus these primes contribute to t_{K^r} (the number of primes in F^r that are ramified in K^r) with one prime, on the other hand they contribute to t_K (the number of primes in F that are ramified in K) with at least one prime and exactly two if the prime splits in $F/\mathbb{Q}$. So if we could prove $t_K = t_{K^r}$, then that would approximately say that all such primes are inert in both F and F^r.

Proposition 2.3.12. *(Shimura, [38, Proposition A.7.]) Let the notation be as above. Then we have $h_K^* = h_{K^r}^*$.*

Proof. The idea of the proof is to first show

$$\zeta_K(s)/\zeta_F(s) = \zeta_{K^r}(s)/\zeta_{F^r}(s) \tag{2.3.3}$$

and then use the analytic class number formula at $s=0$. Louboutin [23, Theorem A] shows the equality (2.3.3) by writing the Dedekind zeta functions of K, K^r, F and F^r as a product of Artin L-functions and finding relations between these combinations of L-functions (see [23, Theorem A]).

We can also get this equality by comparing the local factors of the Euler products of the Dedekind ζ-functions of the fields. By Table 2.1, we see that each ramified prime in $N/\mathbb{Q}$ has the same factors in the Euler products of the quotients of the Dedekind ζ-functions on both sides of (2.3.3). As an example, we take a rational prime p with ramification type (6 a) in Table 2.1, where the local factors for p of the Dedekind ζ-functions are as follows:

$$\begin{aligned}
\zeta_K(s)_p &= \frac{1}{1-\mathrm{N}\mathfrak{p}_{K,1}{}^{-s}}\cdot\frac{1}{1-\mathrm{N}\mathfrak{p}_{K,y}{}^{-s}} = \frac{1}{1-(p^2)^{-s}}\cdot\frac{1}{1-p^{-s}},\\
\zeta_F(s)_p &= \frac{1}{1-\mathrm{N}\mathfrak{p}_{F,1}{}^{-s}}\cdot\frac{1}{1-\mathrm{N}\mathfrak{p}_{F,y}{}^{-s}} = \left(\frac{1}{1-p^{-s}}\right)^2,\\
\zeta_{K^r}(s)_p &= \frac{1}{1-\mathrm{N}\mathfrak{p}_{K^r,1}{}^{-s}} = \frac{1}{1-(p^2)^{-s}},\\
\zeta_{F^r}(s)_p &= \frac{1}{1-\mathrm{N}\mathfrak{p}_{K^r,1}{}^{-s}} = \frac{1}{1-p^{-s}}.
\end{aligned}$$

So for such a prime, we get

$$\zeta_K(s)_p/\zeta_F(s)_p = \frac{1}{1+p^{-s}} = \zeta_{K^r}(s)_p/\zeta_{F^r}(s)_p.$$

Similarly, by using Table 3.5.1 in [14], we can get this equality for the unramified primes as well.

The analytic class number formula at $s=0$ (see, [46, Chapter 4]) says that the Dedekind zeta function $\zeta_M(s)$ of an algebraic number field M has a zero at $s=0$ and the derivative of $\zeta_M(s)$ at $s=0$ has the value

$$-\frac{h_M\cdot R_M}{\mu_M},$$

where h_M is the class number; R_M is the regulator; and μ_M is the order of the group of roots of unity W_M.

Since $\mu_K = 2 = \mu_F$ and $R_K = 2R_F$ (see Washington, [46, Proposition 4.16]), the analytic class number formula at $s = 0$ gives

$$\lim_{s\to 0} \frac{\zeta_K(s)}{\zeta_F(s)} = 2h_K^*.$$

Therefore, the equality of h_K^* and $h_{K^r}^*$ follows from the identity (2.3.3). □

Corollary 2.3.13. *The notation being as above, assuming $I_0(\Phi^r) = I_{K^r}$, we have $t_K = t_{K^r}$.*

Proof. By Proposition 2.3.1, we have $h_K^* = 2^{t_K-1}$ and $h_{K^r}^* = 2^{t_{K^r}-1}$. Then by Proposition 2.3.12, we get $t_K = t_{K^r}$. □

Proof of Proposition 2.3.5

Proposition 2.3.5. *Let K be a non-normal quartic CM field and let F be its real quadratic subfield. Let Φ be a primitive CM type of K. Suppose $I_0(\Phi^r) = I_{K^r}$. Then $F = \mathbb{Q}(\sqrt{p})$ and $F^r = \mathbb{Q}(\sqrt{q})$, where p and q are prime numbers with $q \not\equiv 3 \pmod 4$ and $(p/q) = (q/p) = 1$. Moreover, all the rational primes (distinct from p and q) that are ramified in K^r/F^r are inert in F and F^r.*

Proof. We first prove that if a prime l ramifies in both F and F^r, then it is equal to p, where $F = \mathbb{Q}(\sqrt{p})$.

Indeed, by Lemma 2.3.7-(i), the prime l is totally ramified in $K^r/\mathbb{Q}$ and hence by Corollary 2.3.9, we get $F = \mathbb{Q}(\sqrt{l})$, so $l = p$.

Now we see that there are four types of prime numbers that ramify in $N/\mathbb{Q}$:

(I) The prime p, which is ramified in F and possibly in F^r.

(II) The primes that are unramified in F, but ramified in F^r, say $q_1, \ldots, q_s$.

(III) The primes that are unramified in F and F^r, but ramified in K, say $r_1, \ldots, r_m$.

(IV) If $p \equiv 3 \pmod 4$, then $2 \neq p$ is ramified in F and is inert in F^r by Lemma 2.3.11-(ii).

We will compute the contribution of each ramification type to t_K (the number of primes in F that are ramified in K) and t_{K^r} (the number of primes in F^r that are ramified in K^r). Let f_p and f_p^r be the contributions of the primes over p to t_K and t_{K^r}, respectively. Set $i_2 = 1$ if $p \equiv 3 \pmod 4$, and $i_2 = 0$ if $p \not\equiv 3 \pmod 4$.

Claim. We have $t_K \geq f_p + s + m + i_2$ with equality only if all primes of type (III) are inert in F and $t_{K^r} = f_p^r + m + i_2$.

Proof. By Table 2.1 including Lemma 2.3.8, we see that for $i = 1, \ldots, s$ *exactly* one of the primes above q_i in F ramifies in K/F and the unique prime above q_i in F^r does not ramify in K^r/F^r. By Lemma 2.3.11-(i), we see that for $j = 1, \ldots, m$ the prime r_j is inert in F^r so contributes with *exactly* one prime to t_{K^r}, and with *at least* one prime to t_K and with exactly one if and only if r_j is inert in $F/\mathbb{Q}$. If $p \equiv 3$ (mod 4), then by Lemma 2.3.11-(ii), the prime 2 is inert in F^r. As furthermore 2 is ramified in F and $F \not\cong \mathbb{Q}(\sqrt{2})$, the prime 2 has the decomposition (14) in Table 2.1, so it contributes *exactly* with one prime to t_K and t_{K^r}. So we get $t_K \geq f_p + s + m + i_2$ with equality if and only if all primes of type (III) are inert in F and $t_{K^r} = f_p^r + m + i_2$, which proves the claim.

We observe that $s > 0$ holds. Indeed, if $s = 0$, then all primes that ramify in F^r also ramify in F. Hence d_{F^r} divides d_F, which is equal to p if $p \equiv 1$ (mod 4) and $4p$ otherwise. So $F^r \cong F$, a contradiction.

If p ramifies in both F and F^r, then by Lemma 2.3.7-(i), we have $f_p = f_p^r = 1$. The same is true if p is of type (14) in Table 2.1. By Corollary 2.3.13, we have $t_K = t_{K^r}$, so in this case $m + i_2 \geq s + m + i_2$, so $s = 0$, a contradiction. Therefore, the prime p is not ramified in F^r and is not of type (14), leaving only the possibility $(q/p) = 1$. By Table 2.1, we see that $f_p^r - f_p = 1$. Hence $t_K = t_{K^r}$ implies that all primes of type (III) are inert in F and $s = 1$. In particular, since p is unramified in F^r, we get $F^r = \mathbb{Q}(\sqrt{q})$ for a prime $q \not\equiv 3$ (mod 4). Moreover, Table 2.1 implies $(p/q) = 1$. □

A sharper bound for d_{K^r}/d_{F^r}

Proposition 2.3.14. *Let K be a non-normal quartic CM field and let F be its real quadratic subfield. Let Φ be a primitive CM type of K. Suppose $I_0(\Phi^r) = I_{K^r}$ and $d_N^{1/8} \geq 222$. Then we have $h^*_{K^r} \leq 2^5$ and $d_{K^r}/d_{F^r} \leq 3 \cdot 10^{10}$.*

Proof. Under the assumption $I_0(\Phi^r) = I_{K^r}$, in Propositions 2.3.10 and 2.3.5 we proved $F = \mathbb{Q}(\sqrt{p})$ and $F^r = \mathbb{Q}(\sqrt{q})$, where p and q are prime numbers. Additionally, we proved that at least one of the ramified primes above p in F^r is ramified in K^r/F^r, and the other ramified primes in K^r/F^r are inert in F^r, say $r_1, \ldots, r_{t_{K^r}-1}$. Therefore, we have $d_{K^r}/d_{F^r} \geq pqr_1^2 \cdots r_{t_{K^r}-1}^2$.

Let

$$f(D) = \frac{2\sqrt{D}}{\sqrt{e}\pi^2(\log(D)+0.057)^2} \quad \text{and} \quad g(t) = 2^{-t+1} f(p_t p_{t+1} \Delta_{t-1}^2),$$

where p_j is the j-th prime and $\Delta_k = \prod_{j=1}^{k} p_j$. If $D = d_{K^r}/d_{F^r}$, then we have $h_{K^r} \geq f(D)$ by Proposition 2.3.3.

Recall that, by the proof of Proposition 2.3.4, the function f is monotonically increasing for $D > 52$. Therefore, if $t_{K^r} > 3$, then we have $f(d_{K^r}/d_{F^r}) > f(p_{t_{K^r}} p_{t_{K^r}+1} \Delta_{t_{K^r}-1}^2)$. So in that case by Proposition 2.3.1 and Corollary 2.3.13, we have $h^*_{K^r} = 2^{t_{K^r}-1}$, hence we get $g(t_{K^r}) \leq 1$. Further, the function g is monotonically increasing for $t_{K^r} \geq 4$ and is greater than 1 for $t_{K^r} = 7$. So we get $t_{K^r} \leq 6$. □

2.3.2 Enumerating the fields

To specify non-biquadratic quartic CM fields, we use the following notation of the ECHIDNA database [13]. Given a non-biquadratic quartic CM field K, let D be the discriminant of the real quadratic subfield F of K. Write $K = F(\sqrt{-\alpha})$ where α is a totally positive element of $\mathcal{O}_F$ and take α such that $A := \mathrm{Tr}_{F/\mathbb{Q}}(\alpha) > 0$ is minimal and let $B := \mathrm{N}_{F/\mathbb{Q}}(-\alpha)$. We choose α with minimal B if there is more than one B with the same A. We use the triple $[D, A, B]$ to uniquely represent the isomorphism class of the CM field $K \cong \mathbb{Q}[X]/(X^4 + AX^2 + B)$.

Theorem 2.3.15. *There exist exactly* 63 *isomorphism classes of CM class number one non-normal quartic CM fields. The fields are given by* $K \cong \mathbb{Q}[X]/(X^4 + AX^2 + B) \supset \mathbb{Q}(\sqrt{D})$ *where* $[D, A, B]$ *ranges over*

$[5,13,41]$, $[5,17,61]$, $[5,21,109]$, $[5,26,149]$, $[5,34,269]$, $[5,41,389]$, $[8,10,17]$, $[8,18,73]$, $[8,22,89]$, $[8,34,281]$, $[8,38,233]$, $[13,9,17]$, $[13,18,29]$, $[13,29,181]$, $[13,41,157]$, $[17,5,2]$, $[17,15,52]$, $[17,46,257]$, $[17,47,548]$, $[29,9,13]$, $[29,26,53]$, $[41,11,20]$, $[53,13,29]$, $[61,9,5]$, $[73,9,2]$, $[73,47,388]$, $[89,11,8]$, $[97,94,657]$, $[109,17,45]$, $[137,35,272]$, $[149,13,5]$, $[157,25,117]$, $[181,41,13]$, $[233,19,32]$, $[269,17,5]$, $[281,17,2]$, $[389,37,245]$

with class number 1*;*

$[5,11,29]$, $[5,33,261]$, $[5,66,909]$, $[8,50,425]$, $[8,66,1017]$, $[17,25,50]$, $[29,7,5]$, $[29,21,45]$, $[101,33,45]$, $[113,33,18]$, $[8,14,41]$, $[8,26,137]$, $[12,8,13]$, $[12,10,13]$, $[12,14,37]$, $[12,26,61]$, $[12,26,157]$, $[44,8,5]$, $[44,14,5]$, $[76,18,5]$, $[172,34,117]$, $[236,32,20]$

with class number 2*;*

$[257,23,68]$

with class number 3*;*

$[8,30,153]$, $[12,50,325]$, $[44,42,45]$

with class number 4*.*

We begin the proof by combining the ramification results into the following explicit form for K^r.

Proposition 2.3.16. *Let* K *be a non-normal quartic CM field and let* F *be its real quadratic subfield. Let* Φ *be a primitive CM type of* K*. Suppose* $I_0(\Phi^r) = I_{K^r}$*. Then there exist prime numbers* p*,* q*, and* $s_1 < \cdots < s_u$ *with* $u \in \{t_{K^r} - 1,\ t_{K^r} - 2\}$ *such that all of the following hold. We have* $F = \mathbb{Q}(\sqrt{p})$ *and* $F^r = \mathbb{Q}(\sqrt{q})$ *with* $q \not\equiv 3 \pmod 4$ *and* $(p/q) = (q/p) = 1$*. There exists a prime* $\mathfrak{p}$ *lying above* p *in* F^r *that ramifies in* K^r*, an odd* $j \in \mathbb{Z}_{>0}$ *and a totally positive generator* π *of* $\mathfrak{p}^j$*. Moreover, for exactly one such* $\mathfrak{p}$ *and each such* π *and* j*, we have* $K^r \cong \mathbb{Q}(\sqrt{-\pi s_1 \cdots s_u})$*.*

Proof. By Proposition 2.3.5, we have $F = \mathbb{Q}(\sqrt{p})$ and $F^r = \mathbb{Q}(\sqrt{q})$, where p and q are prime numbers with $q \not\equiv 3 \pmod 4$ and $(p/q) = (q/p) = 1$.

There exists a totally positive element β in $(F^r)^\times$ such that $K^r = F^r(\sqrt{-\beta})$, where β is uniquely defined up to $((F^r)^\times)^2$ (without loss of generality, we can take β in $\mathcal{O}_{F^r}$).

Since $\mathcal{O}_{K^r} \supset \mathcal{O}_{F^r}[\sqrt{-\beta}] \supset \mathcal{O}_{F^r}$, the quotient of the discriminant ideals $\Delta(\mathcal{O}_{K^r}/\mathcal{O}_{F^r})/\Delta(\mathcal{O}_{F^r}[\sqrt{-\beta}]/\mathcal{O}_{F^r}) = \Delta(\mathcal{O}_{K^r}/\mathcal{O}_{F^r})/(-4\beta)$ is a square ideal in $\mathcal{O}_{F^r}$ (see Cohen [10, pp.79]). As β is unique up to squares, and we can take $\mathfrak{l}$-minimal $\beta' \in \beta(F^\times)^2$ for each prime $\mathfrak{l}$ of $\mathcal{O}_{F^r}$, we get

$$\mathrm{ord}_{\mathfrak{l}}((\beta)) \equiv \begin{cases} 1 \pmod 2 & \text{if } \mathfrak{l} \text{ is ramified in } K^r/F^r \text{ and } \mathfrak{l} \nmid 2, \\ 0 \pmod 2 & \text{if } \mathfrak{l} \text{ is not ramified in } K^r/F^r, \\ 0 \text{ or } 1 \pmod 2 & \text{if } \mathfrak{l} \text{ is ramified in } K^r/F^r \text{ and } \mathfrak{l} | 2. \end{cases} \tag{2.3.4}$$

Let $\mathfrak{l}_1, \ldots, \mathfrak{l}_{t_{K^r}} \subseteq \mathcal{O}_{F^r}$ be the primes above the prime numbers $l_1, \ldots, l_{t_{K^r}}$ that ramify in K^r/F^r respectively. Let $n_i > 0$ be minimal such that $\mathfrak{l}_i^{n_i}$ is generated by a totally positive $\lambda_i \in \mathcal{O}_{F^r}$. Since $F^r = \mathbb{Q}(\sqrt{q})$ with prime $q \not\equiv 3 \pmod 4$, genus theory implies that $\mathrm{Cl}_{F^r} = \mathrm{Cl}^+_{F^r}$ has odd order so n_i is odd. Let

$$\alpha = \prod_{i=1}^{t_{K^r}} \lambda_i^{(\mathrm{ord}_{\mathfrak{l}_i}((\beta)) \bmod 2)}.$$

By proving the following two claims we finish the proof.

Claim 1. We have $\alpha/\beta \in (F^{r\times})^2$.

Claim 2. We have $\alpha = \pi s_1 \cdots s_u$ with π, s_i and u as in the statement.

Proof of Claim 1. We first prove that $(\alpha/\beta) = (\alpha)/(\beta)$ is a square ideal in F^r. Let $\mathfrak{l}$ be any prime of F^r. If $\mathfrak{l}$ is unramified in K^r/F^r, then by (2.3.4), we have $\mathrm{ord}_{\mathfrak{l}}((\beta)) \equiv 0 \pmod 2$. So by the definition of α, we have $\mathrm{ord}_{\mathfrak{l}}((\alpha)) = 0$. If $\mathfrak{l}$ is ramified in K^r/F^r, then there exists $\mathfrak{l}_i$ such that $\mathfrak{l} = \mathfrak{l}_i$, so we get

$$\mathrm{ord}_{\mathfrak{l}}((\alpha)) \equiv \mathrm{ord}_{\mathfrak{l}_i}((\beta))\mathrm{ord}_{\mathfrak{l}_i}((\lambda_i)) \equiv \mathrm{ord}_{\mathfrak{l}_i}((\beta)) \pmod 2$$

as $n_i = \mathrm{ord}_{\mathfrak{l}_i}((\lambda_i))$ is odd. Therefore, the ideal (α/β) is a square of an ideal $\mathfrak{a}$ in $\mathcal{O}_{F^r}$. Thus $\mathfrak{a}^2$ is generated by the totally positive α/β. So the ideal class $[\mathfrak{a}]$ is of 2-torsion in $\mathrm{Cl}^+_{F^r}$, which has an odd order, so there is a totally positive element $\mu \in (F^r)^\times$ that generates $\mathfrak{a}$. So $\alpha/\beta = \mu^2 \cdot v$ for some $v \in (\mathcal{O}^\times_{F^r})^+$. Moreover, since $\mathrm{Cl}_{F^r} = \mathrm{Cl}^+_{F^r}$, the norm of the fundamental unit ϵ is negative. Therefore, a unit in $\mathcal{O}_{F^r}$ is totally positive if and only if it is a square in $\mathcal{O}_{F^r}$. Hence v is a square in $\mathcal{O}_{F^r}$ so we get $\alpha/\beta \in ({F^r}^\times)^2$.

Proof of Claim 2. For any given i, if l_i is inert in $F^r/\mathbb{Q}$, then $n_i = 1$ and $\lambda_i = l_i \in \mathbb{Z}_{>0}$ is prime. If l_i is not inert in $F^r/\mathbb{Q}$ then $l_i \in \{p,\ q\}$, by Proposition 2.3.5. If $l_i = q$, then $\mathfrak{l}_i$ is not ramified in K^r/F^r, otherwise by Corollary 2.3.9 we get $\sqrt{q} \in F$. So $l_i = p$.

Let

$$\{s_1, \ldots, s_u\} = \{l_i\ : l_i \text{ is inert in } F^r/\mathbb{Q} \text{ and ramified in } K^r/F^r \\ \text{and } \mathrm{ord}_{\mathfrak{l}_i}((\beta)) \equiv 1 \pmod 2\}.$$

Then $u \in \{t_{K^r} - 1,\ t_{K^r} - 2,\ t_{K^r} - 3\}$ by (2.3.4).

Let $p\mathcal{O}_{F^r} = \mathfrak{p}\mathfrak{p}'$. Then we have $\alpha = \pi^a \pi'^{a'} \prod_{i=1}^u s_i^{(1 \pmod 2)}$, where π and π' are totally positive generators of $\mathfrak{p}^j$ and $\mathfrak{p}'^j$ for some odd $j \in \mathbb{Z}_{>0}$. Here, we have $\prod_{i=1}^u s_i^{(1 \pmod 2)} \in \mathbb{Z}$ and $a,\ a' \in \{0,\ 1\}$. If $a = a'$, then $\alpha \in \mathbb{Z}$, which leads to a contradiction since K^r is non-biquadratic. So for a unique $\mathfrak{p}$, we can take $a_1 = 1$ and $a_2 = 0$. In particular, we have $u \in \{t_{K^r} - 1,\ t_{K^r} - 2\}$. □

Combining Proposition 2.3.16 and the bound on the discriminant in Proposition 2.3.14, we now have a good way of listing the fields. Next, we need a fast way of eliminating fields from our list if they have CM class number > 1.

The following lemma is a special case of Theorem D in Louboutin [23].

Lemma 2.3.17. *Let K be a non-biquadratic quartic CM field and let F be its real quadratic subfield. Let d_K and d_F be the absolute values of the discriminants of K and F. Then assuming $I_0(\Phi^r) = I_{K^r}$, if a rational prime l splits completely in $K^r/\mathbb{Q}$, then $l \geq \frac{\sqrt{d_K/{d_F}^2}}{4}$.*

Proof. Let l be a prime that splits completely in $K^r/\mathbb{Q}$. Let $\mathfrak{l}_{K^r}$ be a prime ideal in K^r above l. By the assumption $I_0(\Phi^r) = I_{K^r}$, there exists $\tau \in K^\times$ such that $\mathrm{N}_{\Phi^r}(\mathfrak{l}_{K^r}) = (\tau)$ and $\tau\overline{\tau} = l$. Here $\tau \neq \overline{\tau}$, since

$\sqrt{l} \notin K$. Then since $\mathcal{O}_K \supset \mathcal{O}_F[\tau]$ and $\Delta(\mathcal{O}_F[\tau]/\mathcal{O}_F) = (\tau - \overline{\tau})^2$, we have $d_K/d_F^2 = \mathrm{N}_{F/\mathbb{Q}}(d_{K/F}) = \mathrm{N}_{F/\mathbb{Q}}(\Delta(\mathcal{O}_K/\mathcal{O}_F)) \leq \mathrm{N}_{F/\mathbb{Q}}((\tau - \overline{\tau})^2)$. Moreover, since $\tau\overline{\tau} = l$, we have $\phi(\tau - \overline{\tau})^2 \leq (2\sqrt{l})^2$ for all embeddings $\phi : F \hookrightarrow \mathbb{R}$, hence $d_K/d_F^2 \leq \mathrm{N}_{F/\mathbb{Q}}((\tau - \overline{\tau})^2) \leq 16l^2$. □

Every prime s_i as in Proposition 2.3.16 divides $\Delta(K^r/F^r)$ so $s_i^2 | d_{K^r}$, hence $s_i^4 | d_N$. The primes p and q are ramified in F and F^r, so p^4 and q^4 divide the discriminant d_N of the normal closure N of degree 8. Hence $d_N \geq p^4 q^4 s_1^4 \cdots s_{t-1}^4$.

Algorithm 2.3.18. ***Output:*** *$[D,\ A,\ B]$ representations of all non-normal quartic CM fields K satisfying $I_0(\Phi^r) = I_{K^r}$.*

Step 1. *Find all square-free integers smaller than $3 \cdot 10^{10}$ having at most 8 prime divisors and find all square-free integers smaller than 222^2.*

Step 2. *Order the prime factors of each of these square-free integers as tuples of primes $(p, q, s_1, \ldots, s_u)$ with $s_1 < \cdots < s_u$ in $(u+1)(u+2)$-ways, then take only the tuples satisfying $q \not\equiv 3 \pmod 4$, $(p/q) = (q/p) = 1$ and $(p/s_i) = (q/s_i) = -1$ for all i.*

Step 3. *For each $(p, q, s_1, \ldots, s_u)$, let $F^r = \mathbb{Q}(\sqrt{q})$, write $p\mathcal{O}_{F^r} = \mathfrak{p}\mathfrak{p}'$, and take $\alpha = \pi \cdot s_1 \cdots s_u \in F^r$, where π is a totally positive generator of $\mathfrak{p}^j$ for the minimal $j \in \mathbb{Z}_{>0}$. Construct $K^r = F^r(\sqrt{-\alpha})$.*

Step 4. *Eliminate the fields K^r that have totally split primes in K^r below the bound $\sqrt{d_K/d_F^2}/4$.*

Step 5. *For each $\mathfrak{q}$ with norm Q below $12\log(|d_{K^r}|)^2$, check whether it is in $I_0(\Phi^r)$ as follows. List all quartic Weil Q–polynomials, that is, monic integer polynomials of degree 4 such that all roots in $\mathbb{C}$ have absolute value $\sqrt{Q}$. For each, take its roots in K and check whether $\mathrm{N}_{\Phi^r}(\mathfrak{q})$ is generated by such a root. If not, then $\mathfrak{q}$ is not in $I_0(\Phi^r)$, so we throw away the field.*

Step 6. *For each K^r, compute the class group of K^r and for a CM type Φ of K test $I_0(\Phi^r)/P_{K^r} = I_{K^r}/P_{K^r}$.*

Step 7. Find $[D,\ A,\ B]$ representations for the reflex fields K of the remaining pairs (K^r, Φ^r).

Proof. Note that Step 4 and Step 5 of the algorithm above do not affect the validity of the algorithm by Lemma 2.3.17. These two steps are only to speed up the computation. In Step 4 we eliminate most of the CM fields.

Suppose that a non-normal quartic CM field K satisfies $I_0(\Phi^r) = I_{K^r}$. Then by Proposition 2.3.16, we have $F = \mathbb{Q}(\sqrt{p})$ and $F^r = \mathbb{Q}(\sqrt{q})$, where p and q are prime numbers with $q \not\equiv 3 \pmod 4$ and $(p/q) = (q/p) = 1$. Also by Proposition 2.3.16, there exist a prime $\mathfrak{p}$ lying above p in F^r that ramifies in K^r and a totally positive element $\alpha = \pi s_1 \cdots s_u$, where π is a totally positive generator of $\mathfrak{p}^j$ for some odd $j \in \mathbb{Z}_{>0}$ such that $K^r = F^r(\sqrt{-\alpha})$. By Proposition 2.3.5, the ramified primes in K^r/F^r that are distinct from $\mathfrak{p}$ are inert in F and F^r. As $s_1, \ldots,\ s_u$ are such primes, we have $(p/s_i) = -1$ and $(q/s_i) = -1$. By Lemma 2.3.14, we have either $h^*_{K^r} = 2^{t_{K^r}-1} \leq 2^5$ and $d_{K^r}/d_{F^r} \leq 3 \cdot 10^{10}$ or $d_N < 222^8$. Therefore, the CM field K is listed. □

We implemented the algorithm in SAGE [36, 33, 42] and obtained the list of the fields in Theorem 2.3.15. The implementation is available online at [17]. This proves Theorems 2.3.15 and 2.1.1. □

This computation takes few weeks on a computer.

Remark 2.3.19. There are no fields eliminated in Step 6, because they turned out to be already eliminated in Step 5.

2.4 Cyclic quartic CM fields

In [31], Murabayashi and Umegaki determined *cyclic* quartic CM fields corresponding to simple CM curves of genus 2 defined over $\mathbb{Q}$. Such fields have CM class number one, however there are more examples, for example, the fields in Table 1b of [9] have CM class number one, but the CM curves corresponding to these cyclic sextic CM fields do not have a model over $\mathbb{Q}$. We apply the strategy in the previous section to cyclic quartic CM fields and list all of those with CM class number one.

Murabayashi [30, Proposition 4.5] proves that the relative class number of cyclic quartic CM fields with CM class number one is 2^{t_K-1}, where t_K is the number of primes in F that are ramified in K. This result also follows from Proposition 2.3.1 in Section 2.3.1.

Suppose that $K/\mathbb{Q}$ is a cyclic quartic CM field with $\mathrm{Gal}(K/\mathbb{Q}) = \langle y \rangle$. Since $K/\mathbb{Q}$ is normal, we consider CM types with values in K. The CM type, up to equivalence, is $\Phi = \{\mathrm{id}, y\}$, which is primitive. The reflex field K^r is K and the reflex type of Φ is the CM type $\{\mathrm{id}, y^3\}$ (Example 8.4(1) of Shimura [40]). In this notation complex conjugation $\bar{\cdot}$ is y^2.

Suppose $K \cong \mathbb{Q}(\zeta_5)$, where ζ_m denotes a primitive m-th root of unity. Then the class group of K is trivial, so the equality $I_0(\Phi^r) = I_K$ holds. Hence $K = \mathbb{Q}(\zeta_5)$ will occur in the list of cyclic quartic CM fields satisfying $I_0(\Phi^r) = I_K$.

From now on, suppose $K \ncong \mathbb{Q}(\zeta_5)$.

Lemma 2.4.1. *(Murabayashi [30], Lemma 4.2) If $I_0(\Phi^r) = I_{K^r}$, then there is exactly one totally ramified prime in $K/\mathbb{Q}$ (i.e., $F = \mathbb{Q}(\sqrt{p})$ with prime $p \not\equiv 3 \pmod 4$) and the other ramified primes of $K/\mathbb{Q}$ are inert in $F/\mathbb{Q}$.* □

Example 2.4.2. *Suppose $I_0(\Phi^r) = I_{K^r}$. The relative class number h_K^* equals 1 if and only if K/F has exactly one ramified prime. This ramified prime is $\sqrt{p}$ when $F = \mathbb{Q}(\sqrt{p})$.*

We now determine such CM fields by using a lower bound on their relative class numbers from analytic number theory.

Theorem 2.4.3. *(Louboutin [24], Theorem 5) Let K be a cyclic quartic CM field of conductor f_K and absolute discriminant d_K. Then we have*

$$h_K^* \geq \frac{2}{3e\pi^2}\left(1 - \frac{4\pi e^{1/2}}{d_K^{1/4}}\right)\frac{f_K}{(\log(f_K)+0.05)^2}. \tag{2.4.1}$$

□

Proposition 2.4.4. *Let the notation be as above. Suppose $I_0(\Phi^r) = I_{K^r}$. Then we have $h_K^* \leq 2^5$ and $f_K < 2.1 \cdot 10^5$.*

Proof. Under the assumption $I_0(\Phi^r) = I_{K^r}$, Lemma 2.4.1 implies that there is exactly one totally ramified prime in $K/\mathbb{Q}$ and the other ramified primes of $K/\mathbb{Q}$ are inert in $F/\mathbb{Q}$.

Let Δ_t be the product of the first t primes. Since the ramified primes in $K/\mathbb{Q}$ divide the conductor f_K, we have $f_K > \Delta_{t_K}$. Further, by Propositions 11.9 and 11.10 in Chapter VII [32], we have $d_K = f_K^2 \cdot d_F$ so $d_K > \Delta_{t_K}^2$. The right hand side of (2.4.1) is monotonically increasing with $f_K > 2$. Further, by Proposition 2.3.1, we have $h_K^* = 2^{t_K - 1}$ so by dividing both sides of (2.4.1) by 2^{t_K-1}, we obtain

$$1 \geq \frac{2}{3e\pi^2}\left(1 - \frac{4\pi e^{1/2}}{\Delta_{t_K}^{1/2}}\right)\frac{\Delta_{t_K}}{2^{t_K}(\log(\Delta_{t_K}) + 0.05)^2}. \tag{2.4.2}$$

The right hand side of (2.4.2) is monotonically increasing with $t_K \geq 2$, and if $t_K = 7$, then the right hand side is greater than 1. Hence $t \leq 6$. So we get $h_K^* \leq 2^5$, and therefore, we get $f_K < 2.1 \cdot 10^5$. □

Theorem 2.4.5. *There exist exactly* 20 *isomorphism classes of CM class number one cyclic quartic CM fields. The fields are given by* $K \cong \mathbb{Q}[X]/(X^4 + AX^2 + B) \supset \mathbb{Q}(\sqrt{D})$ *where* $[D, A, B]$ *ranges over*

$$[5,5,5],\ [8,4,2],\ [13,13,13],\ [29,29,29],$$

$$[37,37,333],\ [53,53,53],\ [61,61,549]$$

with class number 1*;*

$$[5,65,845],\ [5,85,1445],\ [5,10,20],\ [8,12,18],$$

$$[8,20,50],\ [13,65,325],\ [13,26,52],\ [17,119,3332]$$

with class number 2*;*

$$[5,30,180],\ [5,35,245],\ [5,15,45],\ [5,105,2205],\ [17,255,15300]$$

with class number 4*.*

We begin the proof with the following proposition.

Proposition 2.4.6. *If a cyclic quartic CM field* K *satisfies* $I_0(\Phi^r) = I_K$*, then there exist prime numbers* p, $s_1, \ldots, s_u \in \mathbb{Z}$ *such that* $F = \mathbb{Q}(\sqrt{p})$ *with* $p \not\equiv 3 \pmod 4$ *and* $(p/s_i) = -1$ *for all* i*, and we have* $K^r \cong \mathbb{Q}(\sqrt{-\epsilon s_1 \cdots s_u \sqrt{p}})$ *with* $u \in \{t_K - 1,\ t_K - 2\}$ *for every* $\epsilon \in \mathcal{O}_F^\times$ *with* $\epsilon\sqrt{p} \gg 0$*.*

Proof. By Proposition 2.4.1, we have $F = \mathbb{Q}(\sqrt{p})$, where p is a prime with $p \not\equiv 3 \pmod 4$. If there are t_K ramified primes in K/F, the ones that are distinct from the one above p are inert in $F/\mathbb{Q}$, by Proposition 2.4.1; denote them by $s_1, \ldots, s_{t_K}$.

There exists a totally positive element β in $F^\times$ (without loss of generality, we can take β in $\mathcal{O}_F$) such that $K = F(\sqrt{-\beta})$, where β is uniquely defined up to $(F^\times)^2$. As in the proof of Proposition 2.3.16 in the previous section, we will define a totally positive element $\alpha \in F^\times$ with respect to the ramified primes in K/F and show that α and β differ by a factor in $(F^\times)^2$.

Let $\epsilon \in \mathcal{O}_F^\times$ such that $\epsilon\sqrt{p} \gg 0$. Such an element exists since $p \not\equiv 3 \pmod 4$. As β is unique up to squares and we can take $\mathfrak{l}$-minimal $\beta' \in \beta(F^\times)^2$ for each prime $\mathfrak{l}$ of $\mathcal{O}_F$, then we get the cases in (2.3.4) for $\mathrm{ord}_{\mathfrak{l}}((\beta))$.

If $p \neq 2$ and the prime (2) in $\mathcal{O}_F$ is ramified in K/F with $\mathrm{ord}_{(2)}((\beta)) \equiv 0 \pmod 2$, then take $\alpha := \epsilon s_1 \cdots s_u \sqrt{p}$ with $u = t_K - 2$. If $p = 2$ and $\mathrm{ord}_{(\sqrt{2})}((\beta)) \equiv 0 \pmod 2$, then take $\alpha := s_1 \cdots s_u$ with $u = t_K - 1$. For all other cases in (2.3.4), take $\alpha := \epsilon s_1 \cdots s_u \sqrt{p}$ with $u = t_K - 1$.

By the definition of α, for all ideals $\mathfrak{l} \subset \mathcal{O}_F$ we have $\mathrm{ord}_{\mathfrak{l}}((\alpha/\beta)) \equiv 0 \pmod 2$. So $(\alpha/\beta) = \mathfrak{a}^2$ for a fractional $\mathcal{O}_F$-ideal $\mathfrak{a}$. The ideal $\mathfrak{a}$ is a 2-torsion element in Cl_F. Moreover, since $F = \mathbb{Q}(\sqrt{p})$ with $p \not\equiv 3 \pmod 4$, genus theory implies that $\mathrm{Cl}_F = \mathrm{Cl}_F^+$ has odd order. Therefore, there is a totally positive element μ that generates $\mathfrak{a}$. So $\alpha/\beta = \mu^2 \cdot v$ for some $v \in \mathcal{O}_F^+$. Furthermore, since $\mathrm{Cl}_F = \mathrm{Cl}_F^+$, the fundamental unit has a negative norm, and so $\mathcal{O}_F^+ = (\mathcal{O}_F)^2$. Hence v is a square in $\mathcal{O}_F$, and therefore we get $\alpha/\beta \in (F^\times)^2$.

In the case $p = 2$ and $\mathrm{ord}_{(\sqrt{2})}((\beta)) \equiv 0 \pmod 2$, we get the biquadratic field $K = F(\sqrt{-s_1 \cdots s_u})$ over $\mathbb{Q}$, contradiction. Therefore, we have

$$K = \mathbb{Q}(\sqrt{-\epsilon s_1 \cdots s_u \sqrt{p}}) \text{ with } u \in \{t_{K-1},\ t_{K-2}\}.$$

□

Algorithm 2.4.7. ***Output:*** *$[D,\ A,\ B]$ representations of all cyclic quartic CM fields K satisfying $I_0(\Phi^r) = I_K$.*

Step 1. Find all square-free integers less than $2.1 \cdot 10^5$ *and having at most* 6 *prime divisors.*

Step 2. *Order the prime factors of each of these square-free integers as tuples of primes* $(p, s_1, \ldots, s_u)$ *with* $s_1 < \ldots < s_u$ *in* $(u+1)$*-ways, then take only the tuples satisfying* $p \not\equiv 3 \pmod 4$ *and* $(p/s_i) = -1$ *for all* i*.*

Step 3. *For each* $(p, s_1, \ldots, s_u)$*, let* $F = \mathbb{Q}(\sqrt{p})$ *and take a totally positive element* $\alpha = \epsilon s_1 \cdots s_u \sqrt{p}$*, where* ϵ *is a fundamental unit in* F *such that* $\epsilon\sqrt{p} \gg 0$*. Construct* $K = F(\sqrt{-\alpha})$*.*

Step 4. *Eliminate the fields* K *that have totally split primes in* K *below the bound* $\sqrt{d_K/d_F^2}/4$*. (In this step we eliminate most of the CM fields.)*

Step 5. *For each* $\mathfrak{q}$ *with norm* Q *below* $12\log(|d_{K^r}|)^2$*, check whether it is in* $I_0(\Phi^r)$ *as follows. List all quartic Weil* Q*-polynomials, that is, monic integer polynomials of degree* 4 *such that all roots in* $\mathbb{C}$ *have absolute value* $\sqrt{Q}$*. For each, take its roots in* K *and check whether* $\mathrm{N}_{\Phi^r}(\mathfrak{q})$ *is generated by such a root. If not, then* $\mathfrak{q}$ *is not in* $I_0(\Phi^r)$*, so we throw away the field.*

Step 6. *For each* K *compute the class group of the fields* K *and for a primitive CM type* Φ *of* K *test* $I_0(\Phi^r)/P_K = I_K/P_K$*.*

Step 7. *Find* $[D,\ A,\ B]$ *representations for the quartic CM class number one fields* K*.*

Proof. The idea of the proof of this algorithm is exactly as the proof of Algorithm 2.3.18. In this algorithm, Step 1 follows from Proposition 2.4.4; Step 2 and 3 follow from Proposition 2.4.6; Step 4 follows from Lemma 2.3.17. □

We implemented the algorithm in SAGE [36, 33, 42] and obtained the list of the fields in Theorem 2.4.5. The implementation is available online at [17]. This proves Theorems 2.1.2 and 2.4.5. □

This computation takes few days on a computer.