



Universiteit  
Leiden  
The Netherlands

## The CM class number one problem for curves of genus 2

Kılıçer, P.; Streng, T.C.

### Citation

Kılıçer, P., & Streng, T. C. (2023). The CM class number one problem for curves of genus 2. *Research In Number Theory*, 9. doi:10.1007/s40993-022-00417-7

Version: Publisher's Version

License: [Licensed under Article 25fa Copyright Act/Law \(Amendment Taverne\)](#)

Downloaded from: <https://hdl.handle.net/1887/3566595>

**Note:** To cite this publication please use the final published version (if applicable).

RESEARCH



# The CM class number one problem for curves of genus 2

Pınar Kiliçer<sup>1\*</sup>  and Marco Streng<sup>2</sup> 

\*Correspondence:

p.kilicer@rug.nl

<sup>1</sup>Bernoulli Institute for Mathematics, Computer Science and Artificial Intelligence, University of Groningen, Nijenborgh 9, 9747 AG Groningen, The Netherlands

Full list of author information is available at the end of the article

## Abstract

Gauss's class number one problem, solved by Heegner, Baker, and Stark, asked for all imaginary quadratic fields for which the ideal class group is trivial. An application of this solution gives all elliptic curves that can be defined over the rationals and have a large endomorphism ring (CM). Analogously, to get all CM curves of genus two defined over the smallest number fields, we need to find all quartic CM fields for which the CM class group (a quotient of the ideal class group) is trivial. We solve this *CM class number one problem*. We prove that the list given in Bouyer–Streng [LMS J Comput Math 18(1):507–538, 2015, Tables 1a, 1b, 2b, and 2c] of maximal CM curves of genus two defined over the reflex field is complete. We also prove that there are exactly 21 simple CM curves of genus two over  $\mathbb{C}$  that can be defined over  $\mathbb{Q}$ .

**Keywords:** CM fields, CM types, Class number, Abelian varieties, Algebraic curves

**Mathematics Subject Classification:** 11G15, 11R29, 14K22, 14H45

## 1 Introduction

The endomorphisms of an elliptic curve  $E : y^2 = x^3 + ax + b$  with  $a, b \in \overline{\mathbb{Q}}$  are the rational maps  $E \rightarrow E$  sending the point  $O$  at infinity to  $O$  itself. These endomorphisms form a ring known as the *endomorphism ring*, and for most elliptic curves, this ring is simply  $\mathbb{Z}$ , its elements corresponding only to repeated chord-and-tangent additions.

In the case where the endomorphism ring is different from  $\mathbb{Z}$ , it is isomorphic to an order  $\mathcal{O} = \mathbb{Z}[\frac{1}{2}(\sqrt{D} + D)]$  in an imaginary quadratic field  $K = \mathbb{Q}(\sqrt{D})$  with  $D \equiv 0, 1 \pmod{4}$  and  $D < 0$ . This is called the case of *complex multiplication (CM)* as the period lattice  $\Lambda = \{\int_{\gamma} (2y)^{-1} dx : \gamma \in \pi_1(E(\mathbb{C}))\} \subset \mathbb{C}$  of  $E$  has non-real complex multiplications into itself in the sense that  $\alpha\Lambda \subset \Lambda$  for all  $\alpha \in \mathcal{O} \subset \mathbb{C}$ .

The question of finding all imaginary quadratic fields  $K$  corresponding to CM elliptic curves  $E$  with rational  $a, b$  is equivalent to Gauss' class number one problem of finding all imaginary quadratic fields of class number one. This problem was finally solved by Heegner [1], Baker [2] and Stark [3]; the fields are  $K \cong \mathbb{Q}(\sqrt{D})$  where  $-D \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$ .

We consider an analogous problem for curves of genus 2. The period lattice  $\Lambda$  becomes a four-dimensional lattice in  $\mathbb{C}^2$  and the integral domains of largest rank that can appear inside the endomorphism ring of  $\Lambda$  (or, equivalently, in the endomorphism ring of the

Jacobian of the curve) are orders  $\mathcal{O}$  in *CM number fields* of degree four. In the case where this maximum is attained, we say that the curve has *CM* by the quartic order  $\mathcal{O}$ .

There are two types of quartic CM fields whose orders can appear as endomorphism rings of curves of genus two over  $\mathbb{C}$ : the cyclic ones and the non-Galois ones. For non-Galois fields, it is known that the corresponding curves cannot be defined over  $\mathbb{Q}$ , as their fields of moduli always contain a real quadratic field (the real quadratic subfield of the *reflex field*). So in order to get a list that also features non-Galois CM fields, we find all CM fields for which there are curves that can be defined over this quadratic field.

The solution (of Uchida [4], Setzer [5] and Louboutin-Okazaki [6]) of the usual class number one problem for quartic CM fields does not suffice any more. Instead, we need to find all quartic CM fields for which a certain quotient of the class group (which we call the *CM class group*) is trivial.

Murabayashi and Umegaki [7] already found all non-biquadratic quartic CM fields  $K$  for which there exists a curve of genus 2 over  $\mathbb{Q}$  with CM by the maximal order  $\mathcal{O}_K$ . We extend their list by also including curves with CM by non-maximal orders and curves with CM defined over the reflex field.

Lists of fields and curves were given by van Wamelen [8], Bouyer–Streng [9], and Bisson–Streng [10]. We prove that their lists are complete.

**Theorem 3.26** *There exist exactly 63 isomorphism classes of non-Galois quartic CM fields with CM class number one. The fields are exactly those listed in Table 3.*

**Theorem 4.7** *There exist exactly 20 isomorphism classes of cyclic quartic CM fields with CM class number one. The fields are exactly those listed in Table 4.*

**Theorem 5.6** *There exist exactly 21 curves  $C/\mathbb{Q}$  of genus 2 up to  $\overline{\mathbb{Q}}$ -isomorphism such that  $\text{End}(J(C)_{\overline{\mathbb{Q}}})$  is an order in a quartic number field. The fields and 19 of the curves are those given in van Wamelen [8]. The other two curves are  $y^2 = x^6 - 4x^5 + 10x^3 - 6x - 1$  and  $y^2 = 4x^5 + 40x^4 - 40x^3 + 20x^2 + 20x + 3$ , which are given in Theorem 14 of Bisson–Streng [10].*

**Theorem 5.7** *There are exactly 231 curves of genus 2 over  $\overline{\mathbb{Q}}$  up to isomorphism, such that  $\text{End}(J(C)_{\overline{\mathbb{Q}}})$  is the ring of integers of a quartic CM field  $K$  and  $C$  has field of moduli contained in the reflex field. The corresponding CM fields  $K$  are those of Tables 3 and 4, and the curves are those of [9, Tables 1a, 1b, 2b, and 2c].*

**Theorem 5.8** *There are exactly 301 curves of genus 2 over  $\overline{\mathbb{Q}}$  up to isomorphism, such that  $\text{End}(J(C)_{\overline{\mathbb{Q}}})$  is an order in a quartic CM field  $K$  and  $C$  has field of moduli contained in the reflex field. The corresponding CM fields  $K$  are those of Tables 3 and 4.*

**Remark 1.1** We restrict to non-biquadratic quartic CM fields in Theorems 3.26 and 4.7 as they correspond to curves with absolutely simple Jacobian. The first steps towards the degenerate case of split Jacobians are made by G elin, Howe, Ritzenthaler [11], and Narbonne [12].

In Sect. 2, we define the notions that appear in Theorems 3.26 and 4.7. In Sect. 3, we prove Theorem 3.26. The plan is as follows. We first show that there are only finitely many non-Galois quartic fields with CM class number one by bounding their discriminant using a combination of genus theory and bounds of Louboutin [13] (Sect. 3.1). The bound will

be too large for practical purposes, but with a careful analysis of how the ramified primes decompose in  $K$ , we improve the bound (Sects. 3.2–3.6), as well as find a formula that is useful for enumerating the CM fields (Sect. 3.7). We then list all the candidate fields and check them with a computer.

Section 4 proves Theorem 4.7 in the same way. Finally, in Sect. 5, we give the relation with curves of genus two and derive Theorems 5.6–5.8.

We now mention some of the main difficulties compared to Murabayashi and Umegaki [7, 14]. First of all, they consider only the cyclic case, while the Galois group is more complicated in the non-Galois case, leading to many more different splitting types of ramified primes (Table 1). We therefore needed new ideas for proving that the ramified primes have square norm, which is important for showing that the discriminant grows quickly with the number of ramified primes. The many splitting types also made it more difficult to give an explicit formula for the CM fields in terms of the ramified primes, which is important for listing the fields, so we develop various tricks for obtaining such a formula. Moreover, the relative class number bounds for the main result of [7] are so small that all the fields they need are already listed by Park and Kwon [15], while in our case the bounds are too large for using existing tables even in the cyclic case. So we had to enumerate the fields on a computer ourselves, and as this results in fields of large discriminant, we needed to develop tricks for checking whether they have CM class number one without computing class groups.

Subsequent work applies our methods also to curves of genus three (Kılıçer [16, Chapter 3] and Kılıçer–Labrande–Lercier–Ritzenthaler–Sijtsling–Streng [17]) and to curves of genus six (Somoza [18]).

## 2 CM fields

In this section, we define the *CM class group*, which appears in the main theorems. In Sect. 5 we link this to the fields of definition of curves and abelian varieties with CM. We refer to Shimura–Taniyama [19] and Lang [20] for further information.

A *CM field* is a totally imaginary quadratic extension  $K$  of a totally real number field  $K_+$ , that is,  $K = K_+(\sqrt{D})$ , where the number field  $K_+$  and the element  $D \in K_+$  are such that all complex embeddings of  $K_+$  are real and map  $D$  to a negative number. For every CM field  $K$ , we will use the notation  $K_+$  to denote this maximal totally real subfield.

Let  $K$  be a CM field of degree  $2g$ . The automorphism of  $K$  given by  $\rho : \sqrt{D} \mapsto -\sqrt{D}$  and fixing  $K_+$  corresponds to complex conjugation for every embedding  $K \rightarrow \mathbb{C}$ . We call  $\rho$  *complex conjugation* and denote it also by  $\bar{\cdot}$ . For embeddings  $\phi$  of  $K$  into any field, we denote  $\phi \circ \bar{\cdot}$  by  $\bar{\phi}$ . Note that if the codomain of  $\phi$  is a CM field or  $\mathbb{C}$ , then we have  $\bar{\cdot} \circ \phi = \bar{\phi}$ .

Let  $N$  be a field of characteristic 0 with algebraic closure  $\bar{N}$ , and assume that  $N$  contains the image of every embedding  $K \rightarrow \bar{N}$ . A *CM type* of  $K$  with values in  $N$  is a subset  $\Phi \subset \text{Hom}(K, N)$  that contains exactly one element of each of the  $g$  complex conjugate pairs. For example, in the case  $g = 1$ , a CM type  $\Phi$  consists of one embedding, which is often taken to be the identity, so CM types are not mentioned in the literature for the case  $g = 1$ . By abuse of notation, we also refer to the pair  $(K, \Phi)$  as a *CM type*.

A CM type  $(K, \Phi)$  is *primitive* if there is no CM subfield  $K_1 \subsetneq K$  for which the set  $\{\phi|_{K_1} : K_1 \rightarrow N\}$  is a CM type.

It is sometimes computationally convenient to identify  $K$  with a subfield of  $N$  by making a choice of one embedding, and we do so from now on. We also assume from now on that  $N$  is a Galois extension of  $\mathbb{Q}$ .

The *reflex field* of  $(K, \Phi)$  is a CM field given by

$$K^r = \mathbb{Q}(\{\sum_{\phi \in \Phi} \phi(x) \mid x \in K\}) \subset N$$

and satisfies  $\text{Gal}(N/K^r) = \{\sigma \in \text{Gal}(N/\mathbb{Q}) : \sigma\Phi = \Phi\}$ . If the CM field  $K$  is Galois over  $\mathbb{Q}$  and the CM type  $\Phi$  is primitive (which is always true for  $g = 1$ ), then the reflex field  $K^r$  is equal to  $K$ , but in general, the fields  $K$  and  $K^r$  do not even have to have the same degree.

Let

$$\Phi_N = \{\sigma \in \text{Gal}(N/\mathbb{Q}) : \sigma|_K \in \Phi\}.$$

Then the set  $\Phi^r = \{\sigma^{-1}|_{K^r} : \sigma \in \Phi_N\}$  is a CM type of  $K^r$ , and the pair  $(K^r, \Phi^r)$  is called the *reflex* of  $(K, \Phi)$ .

The *type norm* of  $(K, \Phi)$  is the multiplicative map

$$\begin{aligned} N_\Phi : K &\rightarrow K^r, \\ x &\mapsto \prod_{\phi \in \Phi} \phi(x), \end{aligned}$$

satisfying  $N_\Phi(x)\overline{N_\Phi(x)} = N_{K/\mathbb{Q}}(x) \in \mathbb{Q}$ . The type norm induces a homomorphism between the groups of fractional ideals  $I_K$  and  $I_{K^r}$  by sending  $\mathfrak{b} \in I_K$  to  $\mathfrak{b}' \in I_{K^r}$  such that  $\mathfrak{b}'\mathcal{O}_N = \prod_{\phi \in \Phi} \phi(\mathfrak{b})\mathcal{O}_N$  (Shimura–Taniyama [19, Proposition 29 in Sect. 8.3]).

**Lemma 2.1** (cf. Example Sect. 8.4(2) of [19]) *Let  $K$  be a quartic CM field and  $N$  the normal closure of  $K$ . Then one of the following holds.*

- (1)  $K = N$  and  $\text{Gal}(K/\mathbb{Q}) \cong C_2 \times C_2$ ,
- (2)  $K = N$  and  $\text{Gal}(K/\mathbb{Q}) \cong C_4$ ,
- (3)  $[N : K] = 2$  and  $\text{Gal}(N/\mathbb{Q}) \cong D_4$ .

*In case (1), the field  $K$  has no primitive CM types. In cases (2) and (3), all CM types of  $K$  are primitive and for all pairs  $\Phi$  and  $\Psi$  of CM types of  $K$  there is an automorphism  $\gamma$  of  $N$  such that  $\Psi = \gamma\Phi$ .*

*Proof* Everything except the last sentence is in Example Sect. 8.4(2) of [19]. In cases (2) and (3) a primitive CM type  $\Phi_0$  is given in loc. cit. as follows. In case (2), we have  $\text{Gal}(K/\mathbb{Q}) = \langle y \rangle$  and  $\Phi_0 = \{1, y\}$ . In case (3), we have  $\text{Gal}(K/\mathbb{Q}) = \langle x, y \rangle$  with  $y$  of order 4 and  $x$  of order 2 with  $xyx = y^3$  and  $\Phi_0 = \{\text{id}_K, y|_K\}$ . In both cases we can compute that the four CM types  $y^i\Phi_0$  are distinct for  $i = 0, 1, 2, 3$ . As there are only four CM types, this proves existence of  $\gamma$  and primitivity of  $\Phi$ .

Thanks to Lemma 2.1 we can say that a quartic CM field is *primitive* or *non-primitive* without referring to a specific CM type. Moreover, in the primitive case the isomorphism class of the reflex field does not depend on the specific CM type.

Our goal is to find all quartic fields whose orders can occur as the geometric endomorphism ring of the Jacobian of a curve of genus two defined over the reflex field. We will see in Proposition 5.1 that these are exactly the primitive quartic CM fields for which the following group is trivial.

**Definition 2.2** We define the *CM class group* of a CM type  $(K, \Phi)$  to be the quotient  $I_{K^r}/I_0(\Phi^r)$  where

$$I_0(\Phi^r) := \{b \in I_{K^r} : N_{\Phi^r}(b) = (\alpha) \text{ and } \alpha\bar{\alpha} \in \mathbb{Q} \text{ for some } \alpha \in K^\times\}. \tag{2.1}$$

**Lemma 2.3** *Let  $K$  be a primitive quartic CM field. Then the isomorphism class of the CM class group of  $(K, \Phi)$  depends only on  $K$ , not on  $\Phi$ .*

*Proof* Let  $\Phi$  and  $\Psi$  be two CM types of  $K$ . By the final sentence of Lemma 2.1, we have  $\Psi = \gamma \circ \Phi$  for some  $\gamma \in \text{Gal}(N/\mathbb{Q})$ .

Denote the reflex fields of  $(K, \Phi)$  and  $(K, \Psi)$  by  $K_\Phi^r$  and  $K_\Psi^r$ . From the definition of the reflex, we get an isomorphism  $\gamma_0 = \gamma|_{K_\Phi^r} : K_\Phi^r \rightarrow K_\Psi^r$ , and an equality  $\Psi^r = \Phi^r \circ \gamma_0^{-1}$ . From the final equality, we get  $\Psi^r \circ \gamma_0 = \Phi^r$ . and hence

$$N_{\Psi^r} \circ \gamma_0 = N_{\Phi^r}. \tag{2.2}$$

The isomorphism  $\gamma_0$  also induces an isomorphism  $I_{K_\Phi^r} \rightarrow I_{K_\Psi^r}$ , which by (2.1) and (2.2) maps  $I_0(\Phi^r)$  onto  $I_0(\Psi^r)$ . This proves that  $\gamma_0$  induces an isomorphism from the CM class group of  $(K, \Phi)$  to the CM class group of  $(K, \Psi)$ . □

**Definition 2.4** We say that a CM field  $K$  is a *PQ1 field* (for “Primitive Quartic of CM class number 1”) if

- (1) it has degree 4 over  $\mathbb{Q}$ ;
- (2) it is non-Galois or cyclic; and
- (3) the CM class group of  $K$  is trivial (note that this condition does not depend on the CM type by Lemma 2.3).

Our main results, Theorems 3.26 and 4.7, give the complete list PQ1 fields. See Proposition 5.1 below for what this has to do with curves of genus 2 and why we call this a solution to the *CM class number one problem for curves of genus 2*.

### 3 Non-Galois PQ1 fields

Our main results, Theorems 3.26 and 4.7, together give the complete list of PQ1 fields.

In Sect. 3, we prove the hardest case, the case of non-Galois fields (Theorem 3.26). The plan is as follows. We first show that there are only finitely many non-Galois PQ1 fields by bounding their discriminant (Sect. 3.1). However, the bound we obtain there is too large for practical purposes. To find a better upper bound, in Sects. 3.2–3.4, we explore the ramification behaviour of primes in  $N/\mathbb{Q}$ . This study allows us to construct the reflex fields  $K^r$  of PQ1 fields explicitly (see Sect. 3.5), as well as obtain much sharper bounds (Sect. 3.6). Finally, in Sect. 3.7, we give an algorithm that computes all PQ1 fields and hence proves Theorem 3.26.

### 3.1 A first bound

In this section we will find an explicit upper bound for the discriminants of non-Galois PQ1 fields (Proposition 3.11).

We first prove the following relation between the relative class number  $h_K^* := h_K/h_{K_+}$  and the number  $t_K$  of primes in  $K_+$  that are ramified in  $K$ .

**Proposition 3.1** *Let  $K$  be a non-Galois PQ1 field. Then we have  $h_K^* = 2^{t_K-1}$ , where  $t_K$  is the number of primes in  $K_+$  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  $K_+^r$  that are ramified in  $K^r$ .*

*Remark 3.2* The analogue of this result in the case where  $K/\mathbb{Q}$  is cyclic quartic is (i)  $\Rightarrow$  (iii) of Proposition 4.5 in Murabayashi [14].

*Remark 3.3* Combining Proposition 3.1 with a result of Louboutin that gives roughly  $h_K^* \lesssim \sqrt{d_K/d_{K_+}}$  (where  $d_M$  denotes the discriminant of a number field  $M$ ), we will get roughly  $\sqrt{d_K/d_{K_+}} \lesssim 2^{t_K-1}$ . As  $t_K$  grows, the left hand side grows more quickly than the right, so this relation will give a bound on  $t_K$ . In turn, this will give a bound on  $h_K^*$  and on the discriminant (Proposition 3.11).

The proof of Proposition 3.1 has two main steps. In the first step (Lemma 3.4) we cut the relative class number  $h_K^*$  up into a part that is  $2^{t_K-1}$  and another part. In the second step (Lemma 3.6) we show that the other part is 1 for PQ1 fields.

Recall that  $I_K$  is the group of fractional ideals in  $K$ , let  $P_K \subset I_K$  be the subgroup of principal fractional ideals, and let  $H = \text{Gal}(K/K_+) = \langle \bar{\cdot} \rangle$ . Then the fixed subgroup  $I_K^H$  is the group of fractional ideals that are equal to their complex conjugate, and we have  $P_K^H = P_K \cap I_K^H$ . We get the following genus theory result.

**Lemma 3.4** *Let  $K$  be a CM field and let  $\mu_K$  be the group of roots of unity in  $K$ . If  $\mathcal{O}_{K_+}^\times = \mu_K \mathcal{O}_{K_+}^\times$ , then  $h_K^* = 2^{t_K-1} [I_K : I_K^H P_K]$ .*

*Proof* We have the exact sequence

$$1 \rightarrow I_{K_+} \rightarrow I_K^H \rightarrow \bigoplus_{\mathfrak{p} \text{ prime of } K_+} \mathbb{Z}/e_{K/K_+}(\mathfrak{p})\mathbb{Z} \rightarrow 1 \tag{3.1}$$

and

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

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

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

so by (3.1), we have

$$h_{K_+} = [I_{K_+} : P_{K_+}] = \frac{[I_K^H : P_K^H][P_K^H : P_{K_+}]}{[I_K^H : I_{K_+}]} = 2^{-t_K} [I_K^H P_K : P_K][P_K^H : P_{K_+}],$$

hence

$$h_K^* := \frac{h_K}{h_{K_+}} = 2^{t_K} \frac{[I_K : I_K^H P_K]}{[P_K^H : P_{K_+}]}.$$

It now suffices to prove  $[P_K^H : P_{K_+}] = 2$ .

Define  $\varphi : \mathcal{O}_K^\times \rightarrow \mathcal{O}_K^\times$  by  $\varphi(\epsilon) = \epsilon/\bar{\epsilon}$ . Then by the assumption  $\mathcal{O}_K^\times = \mu_K \mathcal{O}_{K_+}^\times$ , we have  $\varphi(\epsilon) = \zeta/\bar{\zeta} = \zeta^2$ , where  $\epsilon = \zeta\epsilon_0$  with  $\zeta \in \mu_K$  and  $\epsilon_0 \in \mathcal{O}_{K_+}^\times$ . Hence  $\text{im}(\varphi) = \mu_K^2$ .

There is a group homomorphism  $\lambda : P_K^H \rightarrow \mu_K/\mu_K^2$  given by  $\lambda((\alpha)) = \alpha/\bar{\alpha}$ . Indeed, the map  $\lambda$  is well-defined because every generator of the ideal  $(\alpha)$  equals  $\epsilon \cdot \alpha$  for some  $\epsilon \in \mathcal{O}_K^\times$  and  $\epsilon/\bar{\epsilon} \in \mu_K^2$ . As  $K = K_+(\sqrt{-\beta})$  with a totally positive element  $\beta$  in  $K_+$ , we have  $\lambda((\sqrt{-\beta})) = -1$ , which is non-square if  $4 \nmid \#\mu_K$ , so  $\lambda$  is surjective. Now suppose  $4 \mid \#\mu_K$ . Let  $\zeta \in \mu_K$  be an element of order the largest power of 2. Then we have  $\lambda((1 + \zeta)) = (1 + \zeta)/(1 + \bar{\zeta}) = \zeta$ , which is a non-square so  $\lambda$  is surjective.

It now suffices to prove that the kernel is  $P_{K_+}$ . Suppose  $\alpha \in K_+^\times$ . Then  $\lambda((\alpha)) = \alpha/\bar{\alpha} = 1$ , hence  $(\alpha) \in \ker(\lambda)$ . Conversely, suppose  $\lambda((\alpha)) = 1$ . Then we have  $\alpha/\bar{\alpha} = \zeta^2$  for some  $\zeta \in \mu_K$ , hence  $(\alpha) = (\alpha/\zeta) \in P_{K_+}$ . □

**Corollary 3.5** *Let  $K$  be a non-Galois quartic CM field. If  $K$  has no roots of unity other than  $\pm 1$ , then  $h_K^* = 2^{t_K-1}[I_K : I_K^H P_K]$ .*

*Proof* We have  $\mathcal{O}_K^\times = \mathcal{O}_{K_+}^\times$  by [21, Lemma 1] so the result follows from Lemma 3.4. □

**Lemma 3.6** *Let  $K$  be a primitive quartic CM field and let  $\Phi$  be a CM type of  $K$ . Then we have  $[I_K : I_K^H P_K] \leq [I_{K^r} : I_0(\Phi^r)]$ . Moreover, we have  $[I_{K^r} : I_{K^r}^{H'} P_{K^r}] \leq [I_{K^r} : I_0(\Phi^r)]$ , where  $H' = \text{Gal}(K^r/K_+^r)$ .*

*Proof* To prove the first assertion, we show that the kernel of the map  $N_\Phi : I_K \rightarrow I_{K^r}/I_0(\Phi^r)$  is contained in  $I_K^H P_K$ . For any  $\mathfrak{a} \in I_K$ , we can compute (see [22, (3.3)], which applies as we have  $[K^r : \mathbb{Q}] = 2^2$ ; or in detail, see [23, Lemma I.8.4]):

$$N_{\Phi^r} N_\Phi(\mathfrak{a}) = N_{K/\mathbb{Q}}(\mathfrak{a}) \frac{\mathfrak{a}}{\bar{\mathfrak{a}}} \tag{3.2}$$

Suppose  $N_\Phi(\mathfrak{a}) \in I_0(\Phi^r)$ . Then  $N_{K/\mathbb{Q}}(\mathfrak{a}) \frac{\mathfrak{a}}{\bar{\mathfrak{a}}} = (\alpha)$ , where  $\alpha \in K^\times$  and  $\alpha\bar{\alpha} = N_{K^r/\mathbb{Q}}(N_\Phi(\mathfrak{a})) = N_{K/\mathbb{Q}}(\mathfrak{a})^2 \in \mathbb{Q}$ . So  $\frac{\mathfrak{a}}{\bar{\mathfrak{a}}} = (\beta)$ , where  $\beta = N_{K/\mathbb{Q}}(\mathfrak{a})^{-1} \cdot \alpha$ , and hence  $\beta\bar{\beta} = 1$ . There is a  $\gamma \in K^\times$  such that  $\beta = \bar{\gamma}/\gamma$  (this is a special case of Hilbert’s Theorem 90, but can be seen directly by taking  $\gamma = \bar{\epsilon} + \beta\epsilon$  for any  $\epsilon \in K$  with  $\gamma \neq 0$ ). Thus we have  $\mathfrak{a} = \bar{\gamma}\bar{\mathfrak{a}} \cdot (\frac{1}{\gamma}) \in I_K^H P_K$  and therefore  $[I_K : I_K^H P_K] \leq [I_{K^r} : I_0(\Phi^r)]$ .

For the second assertion, we show  $I_0(\Phi^r) \subset I_{K^r}^{H'} P_{K^r}$ . By swapping  $(K, \Phi)$  with  $(K^r, \Phi^r)$  in (3.2), we get

$$N_\Phi N_{\Phi^r}(\mathfrak{b}) = N_{K^r/\mathbb{Q}}(\mathfrak{b}) \frac{\mathfrak{b}}{\bar{\mathfrak{b}}} \tag{3.3}$$

Suppose  $\mathfrak{b} \in I_0(\Phi^r)$ . Then we have  $N_{K^r/\mathbb{Q}}(\mathfrak{b}) \frac{\mathfrak{b}}{\bar{\mathfrak{b}}} = (\alpha)$ , where  $\alpha \in K^{r^\times}$  and  $\alpha\bar{\alpha} = N_\Phi(N_{K^r/\mathbb{Q}}(\mathfrak{b})) = N_{K^r/\mathbb{Q}}(\mathfrak{b})^2 \in \mathbb{Q}$ . We finish the proof of  $\mathfrak{b} \in I_{K^r}^{H'} P_{K^r}$  exactly as above. □

*Remark 3.7* The second assertion in Lemma 3.6 is also in Proposition A7-(ii) of Shimura [22]. Murabayashi [14] uses this result to show  $h_K^* = 2^{t_K-1}$  for cyclic quartic CM fields. In the non-Galois case, we use the first assertion to show  $h_K = 2^{t_K-1}$  and the second to show  $h_{K^r} = 2^{t_{K^r}-1}$ , see the following proof.



*Proof of Proposition 3.1* In case  $K \cong \mathbb{Q}(\zeta_5)$ , we have  $h_K^* = h_{K^r}^* = t_K = t_{K^r} = 1$  so the result follows. In all other cases, we have  $\mu_K = \{\pm 1\}$  and  $\mu_{K^r} = \{\pm 1\}$ , so by Corollary 3.5, we have  $h_K^* = 2^{t_K-1}[I_K : I_K^H P_K]$  and  $h_{K^r}^* = 2^{t_{K^r}-1}[I_{K^r} : I_{K^r}^{H^r} P_{K^r}]$ . As  $(K, \Phi)$  has CM class number one, we have  $[I_{K^r} : I_0(\Phi^r)] = 1$ , so Lemma 3.6 gives  $[I_K : I_K^H P_K] = [I_{K^r} : I_{K^r}^{H^r} P_{K^r}] = 1$ . This proves  $h_K^* = 2^{t_K-1}$  and  $h_{K^r}^* = 2^{t_{K^r}-1}$ . □

We get the following consequence, which will be very useful later.

**Corollary 3.8** *If  $K$  is a non-Galois PQ1 field, then we have  $t_K = t_{K^r}$ .*

*Proof* By Proposition 3.1, we have  $h_K^* = 2^{t_K-1}$  and  $h_{K^r}^* = 2^{t_{K^r}-1}$ . By Louboutin [21, Theorem A], we have  $h_K^* = h_{K^r}^*$  so we get  $t_K = t_{K^r}$ . The result  $h_K^* = h_{K^r}^*$  also follows from Shimura [22, Proposition A.7-(i)] or Uchida [24, proof of Corollary], combined with Washington [25, Proposition 4.16]. For context: the idea behind the proof of  $h_K^* = h_{K^r}^*$  in [21,22,24] is to first show an identity of  $L$ -functions and then combine this with the analytic class number formula. □

The next step is to use the following bound from analytic number theory. Let  $d_M$  denote the discriminant of a number field  $M$ .

**Proposition 3.9** (Louboutin) *Let  $N$  be the normal closure of a non-Galois quartic CM field  $K$ . Assume  $d_N^{1/8} \geq 222$ . Then*

$$h_K^* \geq \frac{2}{\sqrt{e}\pi^2} \frac{\sqrt{d_K/d_{K^+}}}{(\log(d_K/d_{K^+}) + 0.057)^2}. \tag{3.4}$$

*Proof* This is Remark 27 (1) of Louboutin [13]. □

**Lemma 3.10** *For real numbers  $D \geq 1$  and non-negative integers  $t$ , let*

$$f(D) = \frac{2}{\sqrt{e}\pi^2} \frac{\sqrt{D}}{(\log(D) + 0.057)^2} \quad \text{and} \quad g(t) = 2^{-t+1} f(5\Delta_{\lceil t/2 \rceil} \Delta_{\lfloor t/2 \rfloor}),$$

*where  $\Delta_t$  is the product of the first  $t$  prime numbers. Then  $f(D)$  increases monotonically for  $D \geq 52$  and  $g(t)$  increases monotonically for  $t \geq 12$ .*

*Proof* The function  $f(D)$  is differentiable for  $D \geq 1$  and the derivative of  $f(D)$  is positive for  $D \geq 52$ . Hence  $f(D)$  increases monotonically for  $D \geq 52$ .

We will now show that  $g(t + 1) \geq g(t)$  for all  $t \geq 13$ . Let  $p_t$  denote the  $t$ -th prime number, so  $\Delta_{t+1} = p_{t+1} \Delta_t$ . By the equality  $\lfloor \frac{t+1}{2} \rfloor = \lceil \frac{t}{2} \rceil$ , we have

$$\frac{\Delta_{\lceil (t+1)/2 \rceil} \Delta_{\lfloor (t+1)/2 \rfloor}}{\Delta_{\lceil t/2 \rceil} \Delta_{\lfloor t/2 \rfloor}} = p_{\lceil (t+1)/2 \rceil}.$$

Therefore, we get

$$\frac{g(t + 1)}{g(t)} = \frac{\sqrt{p_{\lceil (t+1)/2 \rceil}}}{2} \cdot \frac{(\log(5\Delta_{\lceil t/2 \rceil} \Delta_{\lfloor t/2 \rfloor}) + 0.057)^2}{(\log(5\Delta_{\lceil t/2 \rceil} \Delta_{\lfloor t/2 \rfloor} p_{\lceil (t+1)/2 \rceil}) + 0.057)^2}.$$

We claim that the second factor is  $> \frac{1}{2}$  for  $t \geq 8$ . Assuming the claim for now, for  $t \geq 12$  we have

$$\frac{g(t + 1)}{g(t)} > \frac{\sqrt{p_{\lceil (t+1)/2 \rceil}}}{2} \frac{1}{2} > 1$$

so that  $g$  increases monotonically for  $t \geq 12$ .

Proof of the claim. By Bertrand’s postulate [26], we have  $p_{s+1} < 2p_s$  for all integers  $s \geq 1$ . So we get for all integers  $s \geq 4$ :

$$p_{s+1}^4 < 2^4 p_s^4 < 2^6 p_s^2 p_{s-1}^2 < 5\Delta_s^2.$$

For all integers  $t \geq 8$ , taking  $s = \lfloor t/2 \rfloor$  gives

$$p_{\lfloor (t+1)/2 \rfloor}^4 = p_{s+1}^4 < 5\Delta_s^2 \leq 5\Delta_{\lfloor t/2 \rfloor} \Delta_{\lfloor t/2 \rfloor},$$

so

$$\log(p_{\lfloor (t+1)/2 \rfloor}) < \frac{1}{4} \log(5\Delta_{\lfloor t/2 \rfloor} \Delta_{\lfloor t/2 \rfloor}) < (\sqrt{2} - 1) \log(5\Delta_{\lfloor t/2 \rfloor} \Delta_{\lfloor t/2 \rfloor}),$$

hence

$$\log(5\Delta_{\lfloor t/2 \rfloor} \Delta_{\lfloor t/2 \rfloor}) + \log(p_{\lfloor (t+1)/2 \rfloor}) + 0.057 < \sqrt{2}(\log(5\Delta_{\lfloor t/2 \rfloor} \Delta_{\lfloor t/2 \rfloor}) + 0.057),$$

which proves the claim. □

**Proposition 3.11** *For every non-Galois PQ1 field  $K$ , we have*

$$d_K/d_{K_+} < 2 \cdot 10^{19}.$$

*Proof* Let  $N$  be a normal closure of  $K$ . If  $d_N < 222^8$ , then  $d_K/d_{K_+} < d_K < 222^4 < 2 \cdot 10^{19}$ . So from now on, assume  $d_N \geq 222^8$ .

Take  $f$  and  $g$  be as in Lemma 3.10. The quotient  $d_K/d_{K_+}^2$  is the norm of the relative discriminant of  $K/K_+$ , which is divisible by the product of the norms of the primes of  $K_+$  that are ramified in  $K/K_+$ . Moreover, as  $K_+$  is a quadratic field, we have  $d_{K_+} \geq 5$ . Hence we get  $d_K/d_{K_+} \geq 5\Delta_{\lfloor t_K/2 \rfloor} \Delta_{\lfloor t_K/2 \rfloor}$ , where  $t_K$  is the number of primes of  $K_+$  that are ramified in  $K$ .

By Lemma 3.10, the value  $f(D)$  increases monotonically for  $D \geq 52$ . As we have  $d_K/d_{K_+} \geq 5\Delta_{\lfloor t_K/2 \rfloor} \Delta_{\lfloor t_K/2 \rfloor} > 52$  for  $t_K \geq 3$ , we get  $f(d_K/d_{K_+}) \geq f(5\Delta_{\lfloor t_K/2 \rfloor} \Delta_{\lfloor t_K/2 \rfloor})$  if  $t_K \geq 3$ . Therefore, under the assumption  $I_0(\Phi^r) = I_{K^r}$ , by Proposition 3.1, we obtain (if  $t_K \geq 3$ )

$$2^{t_K-1} \geq f(d_K/d_{K_+}) \geq f(5\Delta_{\lfloor t_K/2 \rfloor} \Delta_{\lfloor t_K/2 \rfloor}) \tag{3.5}$$

and hence  $g(t_K) \leq 1$ .

On the other hand, by Lemma 3.10 the value  $g(t)$  increases monotonically for  $t \geq 13$ . We have  $g(t) > 1$  if  $t = 20$ . Therefore, we get  $t_K \leq 19$ .

Using (3.5) now gives  $f(d_K/d_{K_+}) \leq 2^{18}$ . On the other hand, we have  $f(2 \cdot 10^{19}) > 2^{18}$ , so monotonicity of  $f$  gives  $d_K/d_{K_+} < 2 \cdot 10^{19}$ . □

The bound that we get in Proposition 3.11 is unfortunately too large to list all non-Galois PQ1 fields.

### 3.2 Strategy

Next we study ramification of primes in a normal closure  $N/\mathbb{Q}$  of  $K$  in order to find a sharper upper bound.

The main idea is to show that, under the assumption  $I_0(\Phi^r) = I_{K^r}$ , almost all rational primes that are ramified in  $K^r/K_+^r$  are inert in  $K_+^r$  (Proposition 3.18) hence contribute extra

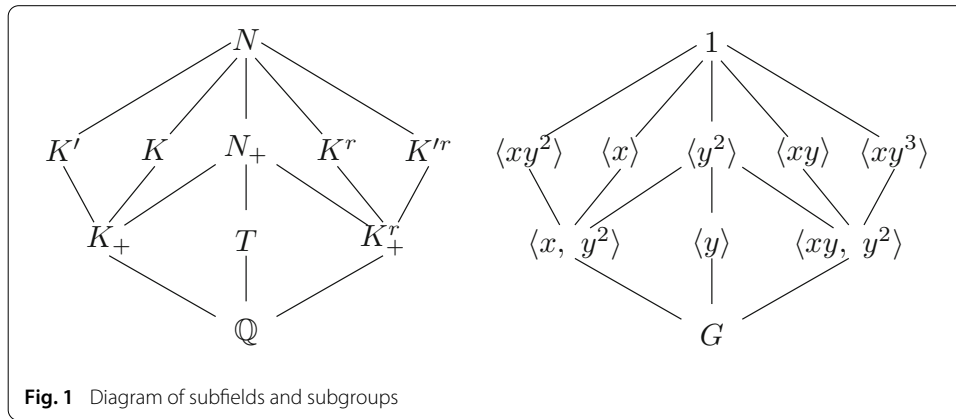


Fig. 1 Diagram of subfields and subgroups

strongly to  $d_{K^r}/d_{K_+^r}$ . This implies that  $d_{K^r}/d_{K_+^r}$  grows as the *square* of the product of such ramified primes. We thus get a new lower bound on the class number that grows much faster with  $t_K$  than what we had in (3.5). This gives us a better upper bound on  $d_{K^r}/d_{K_+^r}$  in Theorem 3.21.

As inert primes are generated by prime numbers, this will also make it easier to write down a formula for the fields that we are interested in (Proposition 3.19).

We begin by exploring the ramification behaviour of primes in  $N/\mathbb{Q}$ .

### 3.3 Non-Galois quartic CM fields

Let  $K/\mathbb{Q}$  be a non-Galois quartic CM field with real quadratic subfield  $K_+$ . By Lemma 2.1, the normal closure  $N$  is a dihedral CM field of degree 8 with Galois group

$$G := \text{Gal}(N/\mathbb{Q}) = \langle x, y : y^4 = x^2 = (xy)^2 = \text{id} \rangle.$$

We give the diagram of subgroups of  $G$  and the corresponding subfields of  $N$  in Fig. 1. Complex conjugation  $\bar{\phantom{x}}$  is  $y^2$  in this notation and the CM field  $K$  is the subfield of  $N$  fixed by  $\langle x \rangle$ . Let  $\Phi$  be a CM type of  $K$  with values in  $N$ . Without loss of generality (by changing the embedding of  $K$  into  $N$  and/or swapping  $y$  with  $y^{-1}$  if needed), we have  $\Phi = \{\text{id}, y|_K\}$ . Then the reflex field  $K^r$  of  $\Phi$  is the fixed field of  $\langle xy^3 \rangle$ , which is a non-Galois quartic CM field non-isomorphic to  $K$  with reflex type  $\Phi^r = \{\text{id}, y^3|_{K^r}\}$ , (see [19, Examples 8.4., 2(C)]). Denote the quadratic subfield of  $K^r$  by  $K_+^r$ .

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

### 3.4 Classification of the ramified primes in $N/\mathbb{Q}$

We will use the following well-known result.

**Lemma 3.12** *Let  $M/L$  be a Galois extension of number fields and  $\mathfrak{q}$  be a prime of  $M$  over an odd prime number. Then there is no surjective homomorphism from a subgroup of the inertia group  $I_{\mathfrak{q}}$  to a Klein four group  $V_4$ .*

*Proof* Suppose that there is a surjective homomorphism from a subgroup of  $I_{\mathfrak{q}}$  to  $V_4$ . In other words, there exists a biquadratic intermediate extension  $E/F$  of  $M/L$  such that  $\mathfrak{p} = \mathfrak{q} \cap F$  is totally ramified in  $E/F$ . Denote the three quadratic intermediate extensions by

$E_i = F(\sqrt{\alpha_i})$  for  $i = 1, 2, 3$ . Without loss of generality, take  $\alpha_i \in \mathcal{O}_F$  with  $\text{ord}_{\mathfrak{p}}(\alpha_i) \in \{0, 1\}$  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  $\text{ord}_{\mathfrak{p}}(\Delta(E_i/F)) = \text{ord}_{\mathfrak{p}}(\alpha_i)$ . 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. Contradiction.  $\square$

**Lemma 3.13** *Let  $(K, \Phi)$  be a primitive quartic CM type. Then the following assertions hold.*

- (i) *If a prime  $p$  is ramified in both  $K_+$  and  $K_+^r$ , then it is totally ramified in  $K/\mathbb{Q}$  and  $K^r/\mathbb{Q}$ .*
- (ii) *If an odd prime  $p$  is ramified in  $K_+$  (in  $K_+^r$ , respectively) as well as in the field  $T$  of Fig. 1, then  $p$  splits in  $K_+^r$  (in  $K_+$ , respectively). Moreover, at least one of the primes above  $p$  in  $K_+^r$  is ramified in  $K^r/K_+^r$  (in  $K/K_+$ , respectively).*

*Proof* In Table 1, we collect results about the primes in  $N$  and their factorization. The columns  $I$  and  $D$  list all possible inertia groups  $I$  and decomposition groups  $D$  of prime ideals of  $\mathcal{O}_N$  that are ramified over a rational prime  $p$ . The six columns after that list the factorization of  $p$  in some of the subfields of  $N$  listed in Fig. 1. By Lemma 3.12, cases (11)–(15) only occur for odd  $p$ . We will explain other columns (and prove the data in those columns) when we need them.

From the factorization columns, both statements (i) and (ii) follow.  $\square$

*Remark 3.14* It is also possible to prove Lemma 3.13 directly without a table, see the first author's PhD thesis [16, Lemma 2.3.7]. However, since we will need the table anyway, we gave a proof using the table.

**Lemma 3.15** *Let  $K$  be a non-Galois PQ1 field. If  $K^r$  has a prime  $\mathfrak{p}$  of prime norm  $p$  with  $\bar{\mathfrak{p}} = \mathfrak{p}$ , then we have  $K_+ = \mathbb{Q}(\sqrt{p})$ .*

*In particular, if  $p$  is totally ramified in  $K^r/\mathbb{Q}$  or splits in  $K_+^r/\mathbb{Q}$  and at least one of the primes over  $p$  in  $K_+^r$  ramifies in  $K^r/K_+^r$ , then we have  $K_+ = \mathbb{Q}(\sqrt{p})$ .*

*Proof* Since  $(K, \Phi)$  is a PQ1 type, it follows that

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

As  $\bar{\mathfrak{p}} = \mathfrak{p}$ , we have  $(\alpha) = (\bar{\alpha})$ . So we get  $\alpha = \epsilon\bar{\alpha}$  for a unit  $\epsilon$  in  $\mathcal{O}_K^\times$  with  $\epsilon\bar{\epsilon} = 1$ . It follows that  $\epsilon$  is 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  $\sqrt{p} \in K_+$ .  $\square$

**Proposition 3.16** *Let  $K$  be a non-Galois PQ1 field. Then  $K_+ = \mathbb{Q}(\sqrt{p})$ , where  $p$  is a prime number.*

*Proof* Suppose that there is an odd prime  $p$  that is ramified in  $K_+$ . Then  $p$  is ramified either in  $K_+$  and  $K_+^r$  or in  $K_+$  and  $T$ .

If  $p$  is ramified in both  $K_+$  and  $K_+^r$ , then by Lemma 3.13-(i), the prime  $p$  is totally ramified in  $K^r/\mathbb{Q}$ . If  $p$  is ramified in  $K_+$  and  $T$ , then by Lemma 3.13-(ii), the prime  $p$  splits in  $K_+^r$  and at least one of the primes over  $p$  in  $K_+^r$  ramifies in  $K^r/K_+^r$ . In both cases, Lemma 3.15 tells us that  $K_+ = \mathbb{Q}(\sqrt{p})$ .

**Table 1** Ramification table of a non-Galois quartic CM field

| Case  | $l$         | $D$         | Decomposition of $p$  |  |   |  |   |  | $N_{\Phi^r}(\mathfrak{p}_{K^r,1})$       | $\sqrt{p} \in K_+$ |
|-------|-------------|-------------|---|--|---|--|---|--|--|--------------------|
|       |             |             | in $N$  | in $K$   | in $K_+$                                    | in $T$                                 | in $K_+^r$                                      | in $K^r$   |  |                    |
| (1)*  | $(y^2)$     | $(y^2)$     | $\mathfrak{p}_{N,1}^2 \mathfrak{p}_{N,x}^2 \mathfrak{p}_{N,y}^2 \mathfrak{p}_{N,xy}^2$    | $\mathfrak{p}_{K,1}^2 \mathfrak{p}_{Ky}^2$                       | $\mathfrak{p}_{K_+,1} \mathfrak{p}_{K_+,y}$ | $\mathfrak{p}_{k,1} \mathfrak{p}_{ky}$ | $\mathfrak{p}_{K_+^r,1} \mathfrak{p}_{K_+^r,y}$ | $\mathfrak{p}_{K^r,1}^2 \mathfrak{p}_{K^r,y}^2$                          | $\mathfrak{p}_{K,1} \mathfrak{p}_{Ky}$   | ✓                  |
| (2)   | $(y^2)$     | $(y)$       | $\mathfrak{p}_{N,1}^2 \mathfrak{p}_{N,x}^2$   | $\mathfrak{p}_{K,1}^2$   | $\mathfrak{p}_{K_+,1}$                      | $\mathfrak{p}_{k,1} \mathfrak{p}_{kx}$ | $\mathfrak{p}_{K_+^r,1}$                        | $\mathfrak{p}_{K^r,1}^2$   | $\rho$                                   |                    |
| (3)   | $(y^2)$     | $(x, y^2)$  | $\mathfrak{p}_{N,1}^2 \mathfrak{p}_{N,y}^2$   | $\mathfrak{p}_{K,1}^2 \mathfrak{p}_{Ky}^2$                       | $\mathfrak{p}_{K_+,1} \mathfrak{p}_{K_+,y}$ | $\mathfrak{p}_{k,1}$                   | $\mathfrak{p}_{K_+^r,1}$                        | $\mathfrak{p}_{K^r,1}^2$   | $\rho$                                   |                    |
| (4)*  | $(y^2)$     | $(xy, y^2)$ | $\mathfrak{p}_{N,1}^2 \mathfrak{p}_{N,y}^2$   | $\mathfrak{p}_{K,1}^2$   | $\mathfrak{p}_{K_+,1}$                      | $\mathfrak{p}_{k,1}$                   | $\mathfrak{p}_{K_+^r,1} \mathfrak{p}_{K_+^r,y}$ | $\mathfrak{p}_{K^r,1}^2 \mathfrak{p}_{K^r,y}^2$                          | $\mathfrak{p}_{K,1}$                     | ✓                  |
| (5)   | (a)         | $(x)$       | $\mathfrak{p}_{N,1}^2 \mathfrak{p}_{N,y}^2 \mathfrak{p}_{N,y^2}^2 \mathfrak{p}_{N,y^3}^2$ | $\mathfrak{p}_{K,1}^2 \mathfrak{p}_{Ky}^2 \mathfrak{p}_{Ky^2}^2$ | $\mathfrak{p}_{K_+,1} \mathfrak{p}_{K_+,y}$ | $\mathfrak{p}_{k,1}^2$                 | $\mathfrak{p}_{K_+^r,1}^2$                      | $\mathfrak{p}_{K^r,1}^2 \mathfrak{p}_{K^r,y^2}^2$                        | $\mathfrak{p}_{K,1} \mathfrak{p}_{Ky}$   |                    |
|       | (b)         | $(xy^2)$    | $\mathfrak{p}_{N,1}^2 \mathfrak{p}_{N,y}^2 \mathfrak{p}_{N,y^2}^2 \mathfrak{p}_{N,y^3}^2$ | $\mathfrak{p}_{K,1}^2 \mathfrak{p}_{Ky}^2 \mathfrak{p}_{Ky^3}^2$ | $\mathfrak{p}_{K_+,1} \mathfrak{p}_{K_+,y}$ | $\mathfrak{p}_{k,1}^2$                 | $\mathfrak{p}_{K_+^r,1}^2$                      | $\mathfrak{p}_{K^r,1}^2 \mathfrak{p}_{K^r,y}^2$                          | $\mathfrak{p}_{K,1} \mathfrak{p}_{Ky^3}$ |                    |
| (6)   | (a)         | $(x)$       | $\mathfrak{p}_{N,1}^2 \mathfrak{p}_{N,y}^2$   | $\mathfrak{p}_{K,1}^2 \mathfrak{p}_{Ky}^2$                       | $\mathfrak{p}_{K_+,1} \mathfrak{p}_{K_+,y}$ | $\mathfrak{p}_{k,1}^2$                 | $\mathfrak{p}_{K_+^r,1}^2$                      | $\mathfrak{p}_{K^r,1}^2$   | $\rho$                                   |                    |
|       | (b)         | $(xy^2)$    | $\mathfrak{p}_{N,1}^2 \mathfrak{p}_{N,y}^2$   | $\mathfrak{p}_{K,1}^2 \mathfrak{p}_{Ky}^2$                       | $\mathfrak{p}_{K_+,1} \mathfrak{p}_{K_+,y}$ | $\mathfrak{p}_{k,1}^2$                 | $\mathfrak{p}_{K_+^r,1}^2$                      | $\mathfrak{p}_{K^r,1}^2$   | $\rho$                                   |                    |
| (7)   | (a)         | $(xy)$      | $\mathfrak{p}_{N,1}^2 \mathfrak{p}_{N,y}^2 \mathfrak{p}_{N,y^2}^2 \mathfrak{p}_{N,y^3}^2$ | $\mathfrak{p}_{K,1}^2 \mathfrak{p}_{Ky^3}^2$                     | $\mathfrak{p}_{K_+,1}^2$                    | $\mathfrak{p}_{k,1}^2$                 | $\mathfrak{p}_{K_+^r,1} \mathfrak{p}_{K_+^r,y}$ | $\mathfrak{p}_{K^r,1}^2 \mathfrak{p}_{K^r,y}^2 \mathfrak{p}_{K^r,y^3}^2$ | $\mathfrak{p}_{K,1} \mathfrak{p}_{Ky^3}$ | ✓                  |
|       | (b)         | $(xy^3)$    | $\mathfrak{p}_{N,1}^2 \mathfrak{p}_{N,y}^2 \mathfrak{p}_{N,y^2}^2 \mathfrak{p}_{N,y^3}^2$ | $\mathfrak{p}_{K,1}^2 \mathfrak{p}_{Ky}^2$                       | $\mathfrak{p}_{K_+,1}^2$                    | $\mathfrak{p}_{k,1}^2$                 | $\mathfrak{p}_{K_+^r,1} \mathfrak{p}_{K_+^r,y}$ | $\mathfrak{p}_{K^r,1}^2 \mathfrak{p}_{K^r,y}^2 \mathfrak{p}_{K^r,y^2}^2$ | $\mathfrak{p}_{K,1}^2$                   | ✓                  |
| (8)   | (a)         | $(xy)$      | $\mathfrak{p}_{N,1}^2 \mathfrak{p}_{N,y}^2$   | $\mathfrak{p}_{K,1}^2$   | $\mathfrak{p}_{K_+,1}^2$                    | $\mathfrak{p}_{k,1}^2$                 | $\mathfrak{p}_{K_+^r,1} \mathfrak{p}_{K_+^r,y}$ | $\mathfrak{p}_{K^r,1}^2 \mathfrak{p}_{K^r,y}^2$                          | $\mathfrak{p}_{K,1}$                     | ✓                  |
|       | (b)         | $(xy^3)$    | $\mathfrak{p}_{N,1}^2 \mathfrak{p}_{N,y}^2$   | $\mathfrak{p}_{K,1}^2$   | $\mathfrak{p}_{K_+,1}^2$                    | $\mathfrak{p}_{k,1}^2$                 | $\mathfrak{p}_{K_+^r,1} \mathfrak{p}_{K_+^r,y}$ | $\mathfrak{p}_{K^r,1}^2 \mathfrak{p}_{K^r,y}^2$                          | $\rho$                                   | ✓                  |
| (9)   | $(y)$       | $(y)$       | $\mathfrak{p}_{N,1}^4 \mathfrak{p}_{N,x}^4$   | $\mathfrak{p}_{K,1}^4$   | $\mathfrak{p}_{K_+,1}^2$                    | $\mathfrak{p}_{k,1} \mathfrak{p}_{kx}$ | $\mathfrak{p}_{K_+^r,1}^2$                      | $\mathfrak{p}_{K^r,1}^4$   | $\mathfrak{p}_{K,1}^2$                   | ✓                  |
| (10)  | $(y)$       | $G$         | $\mathfrak{p}_{N,1}^4$  | $\mathfrak{p}_{K,1}^4$   | $\mathfrak{p}_{K_+,1}^2$                    | $\mathfrak{p}_{k,1}$                   | $\mathfrak{p}_{K_+^r,1}^2$                      | $\mathfrak{p}_{K^r,1}^4$   | $\mathfrak{p}_{K,1}^2$                   | ✓                  |
| (11)* | $(x, y^2)$  | $(x, y^2)$  | $\mathfrak{p}_{N,1}^4 \mathfrak{p}_{N,y}^4$   | $\mathfrak{p}_{K,1}^2 \mathfrak{p}_{Ky}^2$                       | $\mathfrak{p}_{K_+,1} \mathfrak{p}_{K_+,y}$ | $\mathfrak{p}_{k,1}^2$                 | $\mathfrak{p}_{K_+^r,1}^2$                      | $\mathfrak{p}_{K^r,1}^4$   | $\mathfrak{p}_{K,1} \mathfrak{p}_{Ky}$   | ✓                  |
| (12)* | $(x, y^2)$  | $G$         | $\mathfrak{p}_{N,1}^4$  | $\mathfrak{p}_{K,1}^2$   | $\mathfrak{p}_{K_+,1}$                      | $\mathfrak{p}_{k,1}^2$                 | $\mathfrak{p}_{K_+^r,1}^2$                      | $\mathfrak{p}_{K^r,1}^4$   | $\mathfrak{p}_{K,1}$                     | ✓                  |
| (13)  | $(xy, y^2)$ | $(xy, y^2)$ | $\mathfrak{p}_{N,1}^4 \mathfrak{p}_{N,y}^4$   | $\mathfrak{p}_{K,1}^2$   | $\mathfrak{p}_{K_+,1}^2$                    | $\mathfrak{p}_{k,1}^2$                 | $\mathfrak{p}_{K_+^r,1} \mathfrak{p}_{K_+^r,y}$ | $\mathfrak{p}_{K^r,1}^2 \mathfrak{p}_{K^r,y}^2$                          | $\mathfrak{p}_{K,1}^2$                   | ✓                  |
| (14)  | $(xy, y^2)$ | $G$         | $\mathfrak{p}_{N,1}^4$  | $\mathfrak{p}_{K,1}^2$   | $\mathfrak{p}_{K_+,1}^2$                    | $\mathfrak{p}_{k,1}^2$                 | $\mathfrak{p}_{K_+^r,1}^2$                      | $\mathfrak{p}_{K^r,1}^2$   | $\rho$                                   |                    |
| (15)  | $G$         | $G$         | $\mathfrak{p}_{N,1}^8$  | $\mathfrak{p}_{K,1}^4$   | $\mathfrak{p}_{K_+,1}^2$                    | $\mathfrak{p}_{k,1}^2$                 | $\mathfrak{p}_{K_+^r,1}^2$                      | $\mathfrak{p}_{K^r,1}^4$   | $\mathfrak{p}_{K,1}^2$                   | ✓                  |

This table lists all 19 pairs  $(l, D)$  where  $1 \neq l \mid D \leq D_4 = (x, y)$  and  $D/l$  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 [27, Table 5]: we restricted to  $l \neq 1$  and corrected some entries in cases (4), (8), (10) and (15). The cases (11)–(15) can only occur for  $p = 2$  by Lemma 3.12. If there is a check mark in the last column, then by Lemma 3.15, such splitting implies  $\sqrt{p} \in K_+$  (i.e.,  $K_+ = \mathbb{Q}(\sqrt{p})$ ) 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  $K_+$  in these cases, but on the other hand  $\sqrt{p} \in K_+$  by Lemma 3.15

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

**Lemma 3.17** *Let  $K$  be a non-Galois PQ1 field. Then the following assertions are true.*

- (i) *If a rational prime  $l$  is unramified in both  $K_+/\mathbb{Q}$  and  $K_+^r/\mathbb{Q}$ , but is ramified in  $K/\mathbb{Q}$  or  $K^r/\mathbb{Q}$ , then all primes above  $l$  in  $K_+$  and  $K_+^r$  are ramified in  $K/K_+$  and  $K^r/K_+^r$  and  $l$  is inert in  $K_+^r$ .*
- (ii) *If  $K_+ = \mathbb{Q}(\sqrt{p})$  with a prime number  $p \equiv 3 \pmod{4}$ , then 2 is inert in  $K_+^r$ .*

*Proof* (i) Since  $(K, \Phi)$  is a PQ1 type, it satisfies  $I_0(\Phi^r) = I_{K^r}$ . So the only possible decomposition types for a prime that is ramified in  $K$  and unramified in both  $K_+$  and  $K_+^r$  are (2) and (3) in Table 1 (see the \* in the first column of Table 1). Hence the statement follows.

(ii) The prime 2 is ramified in  $K_+$  since  $p \equiv 3 \pmod{4}$ . By Table 1, we see that if 2 is ramified or split in  $K_+^r$ , then we have  $\sqrt{2} \in K_+$ , a contradiction. This implies that 2 is inert in  $K_+^r$ . □

The following proposition will be crucial when we construct PQ1 fields. It is the non-Galois analogue of Murabayashi [14, Proposition 4.5], but it required a completely new proof. The idea of the proof is to count the primes that ramify in the two extensions  $K^r/K_+^r$  and  $K/K_+$  using the restrictions that we collected in 3.15–3.17, and to use that these numbers of primes are equal by Corollary 3.8.

**Proposition 3.18** *Let  $K$  be a non-Galois PQ1 field. Then there exist prime numbers  $p$  and  $q$  such that the following hold.*

- (i) *We have  $K_+ = \mathbb{Q}(\sqrt{p})$  and  $K_+^r = \mathbb{Q}(\sqrt{q})$ , where  $p$  and  $q$  are prime numbers with  $q \not\equiv 3 \pmod{4}$ .*
- (ii) *The primes  $p$  and  $q$  are split in  $K_+^r$  and  $K_+$  respectively.*
- (iii) *All primes coprime to  $p$  and  $q$  that are ramified in  $K^r/K_+^r$  are inert in  $K_+/\mathbb{Q}$  and  $K_+^r/\mathbb{Q}$ .*

*Proof* Recall from Proposition 3.16 that we have  $K_+ = \mathbb{Q}(\sqrt{p})$  for a prime number  $p$ . If  $p \not\equiv 3 \pmod{4}$ , then  $p$  is the only prime that is ramified in  $K_+$ . If  $p \equiv 3 \pmod{4}$ , then  $p$  and 2 are two distinct primes that are ramified in  $K_+$ , and hence by the final column of Table 1, we get that 2 is of Case (14), hence inert in  $K_+^r$ . This shows that there are four types of prime numbers that ramify in  $N/\mathbb{Q}$ :

- (I) The prime  $p$ , which is ramified in  $K_+$  and possibly in  $K_+^r$ .
- (II) The primes that are unramified in  $K_+$ , but ramified in  $K_+^r$ , say  $q_1, \dots, q_s$ .
- (III) The primes that are unramified in  $K_+$  and  $K_+^r$ , but ramified in  $K$ , say  $r_1, \dots, r_m$ .
- (IV) If  $p \equiv 3 \pmod{4}$ , then  $2 \neq p$  is ramified in  $K_+$  and inert in  $K_+^r$  and is of Case (14) in Table 1.

Next, we compute the contribution of each ramification type to  $t_K$  and  $t_{K^r}$ . Let  $f_p$  and  $f_p^r$  be the contributions of the primes over  $p$ . Set  $i_2 = 1$  if  $p \equiv 3 \pmod{4}$ , and  $i_2 = 0$  if  $p \not\equiv 3 \pmod{4}$ .

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

*Proof of the claim.* The contributions of  $p$  (type (I)) are  $f_p$  and  $f_p^r$  by definition.

(II) By Table 1 including Lemma 3.15, we see that for  $i = 1, \dots, s$  the prime  $q_i$  splits in  $K_+$  and exactly one of the primes above  $q_i$  in  $K_+$  ramifies in  $K/K_+$  and the unique prime above  $q_i$  in  $K_+^r$  does not ramify in  $K^r/K_+^r$ .

(III) By Lemma 3.17-(i), we see that for  $j = 1, \dots, m$  the prime  $r_j$  is inert in  $K_+^r$  and all primes over  $r_j$  ramify in  $K^r/K_+^r$  and  $K/K_+$ . It follows that  $r_j$  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  $K_+/\mathbb{Q}$ .

(IV) If  $p \equiv 3 \pmod{4}$ , then by Case (14) of Table 1, we see that 2 contributes exactly 1 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  $K_+$  and  $t_{K^r} = f_p^r + m + i_2$ , exactly as claimed.

Corollary 3.8 gives  $t_K = t_{K^r}$ , which by the claim gives  $f_p^r - f_p \geq s$  with equality if and only if all primes of type (III) are inert in  $K_+$ .

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

By Table 1, we see  $1 \geq f_p^r - f_p$  with equality if and only if  $p$  splits in  $K_+^r$ .

Combining the three previous paragraphs, we get  $f_p^r - f_p = s = 1$ , all primes of type (III) are inert in  $K_+$  and  $p$  splits in  $K_+^r$ . As  $K_+^r$  has a unique ramified prime  $q = q_1$ , it is

$K_+^r = \mathbb{Q}(\sqrt{q})$  with  $q \not\equiv 3 \pmod{4}$ . And as mentioned in the proof of the claim, the prime  $q = q_1$  splits in  $K_+$ . □

### 3.5 Explicit construction of the fields

**Proposition 3.19** *Let  $K$  be a non-Galois PQ1 field. Then there exist prime numbers  $p, q$ , and  $s_1 < \dots < s_u$  with  $u \in \{t_{K^r} - 1, t_{K^r} - 2\}$  such that all of the following hold.*

- (i) *We have  $K_+ = \mathbb{Q}(\sqrt{p})$  and  $K_+^r = \mathbb{Q}(\sqrt{q})$  with  $q \not\equiv 3 \pmod{4}$  and the primes  $p$  and  $q$  are split in  $K_+^r$  and  $K_+$  respectively.*
- (ii) *The primes  $s_i$  are inert in both  $K_+$  and  $K_+^r$ .*
- (iii) *There exists a prime  $\mathfrak{p} \mid p\mathcal{O}_{K_+^r}$ , an odd integer  $j$  and a totally positive generator  $\pi$  of  $\mathfrak{p}^j$  such that  $K^r \cong K_+^r(\sqrt{-\pi s_1 \dots s_u})$ .*
- (iv) *For every prime  $\mathfrak{p} \mid p\mathcal{O}_{K_+^r}$ , every odd integer  $j$  and every totally positive generator  $\pi$  of  $\mathfrak{p}^j$ , we have  $K^r \cong \mathbb{Q}(\sqrt{-\pi s_1 \dots s_u})$ .*

*Proof* Proposition 3.18 states that there exist  $p$  and  $q$  such that (i) holds. The same proposition also states that all prime numbers different from  $p$  and  $q$  that ramify in  $K/\mathbb{Q}$  are inert in  $K_+/\mathbb{Q}$  and in  $K_+^r/\mathbb{Q}$ .

Let  $\beta$  be a totally positive element of  $\mathcal{O}_{K_+^r}$  such that  $K^r = K_+^r(\sqrt{-\beta})$ .

Since  $\mathcal{O}_{K^r} \supset \mathcal{O}_{K_+^r}[\sqrt{-\beta}] \supset \mathcal{O}_{K_+^r}$ , the quotient of the discriminant ideals

$$\Delta(\mathcal{O}_{K^r}/\mathcal{O}_{K_+^r})/\Delta(\mathcal{O}_{K_+^r}[\sqrt{-\beta}]/\mathcal{O}_{K_+^r}) = \Delta(\mathcal{O}_{K^r}/\mathcal{O}_{K_+^r})/(-4\beta)$$

is a square ideal in  $\mathcal{O}_{K_+^r}$  (see Cohen [28, p. 79]). As  $\beta$  is unique up to squares, and we can take  $\mathfrak{l}$ -minimal  $\beta' \in \beta(K_+^r)^\times$  for each prime  $\mathfrak{l}$  of  $\mathcal{O}_{K_+^r}$ , we get

$$\text{ord}_{\mathfrak{l}}((\beta)) \equiv \begin{cases} 1 \pmod{2} & \text{if } \mathfrak{l} \text{ is ramified in } K^r/K_+^r \text{ and } \mathfrak{l} \nmid 2, \\ 0 \pmod{2} & \text{if } \mathfrak{l} \text{ is not ramified in } K^r/K_+^r, \\ 0 \text{ or } 1 \pmod{2} & \text{if } \mathfrak{l} \text{ is ramified in } K^r/K_+^r \text{ and } \mathfrak{l} \mid 2. \end{cases} \tag{3.6}$$

Let  $\mathfrak{l}_1, \dots, \mathfrak{l}_{t_{K^r}} \subseteq \mathcal{O}_{K_+^r}$  be the primes that ramify in  $K^r/K_+^r$ , and let  $l_i \in \mathbb{Z}_{>0}$  be the prime number in  $l_i$ . Let  $n_i > 0$  be minimal such that  $\mathfrak{l}_i^{n_i}$  is generated by a totally positive  $\lambda_i \in \mathcal{O}_{K_+^r}$ . Choose such  $\lambda_i$ , and take  $\lambda_i \in \mathbb{Z}_{>0}$  whenever possible. Since we have  $K_+^r = \mathbb{Q}(\sqrt{q})$  with prime  $q \not\equiv 3 \pmod{4}$ , genus theory implies that  $\text{Cl}_{K_+^r} = \text{Cl}_{K_+^r}^+$  has odd order, so  $n_i$  is odd. Let

$$\alpha = \prod_{i=1}^{t_{K^r}} \lambda_i^{e_i}, \quad \text{where } e_i \in \{0, 1\}, e_i \equiv \text{ord}_{\mathfrak{l}_i}(\beta) \pmod{2}.$$

The following two claims together prove (ii) and (iii).

**Claim 1** *We have  $\alpha/\beta \in (K_+^r)^\times$ .*

**Claim 2** *We have  $\alpha = \pi s_1 \dots s_u$  for some  $\pi, s_i$  and  $u$  as in (iii).*

*Proof of Claim 1* We first prove that  $(\alpha/\beta) = (\alpha)/(\beta)$  is a square ideal in  $K_+^r$ . Let  $\mathfrak{l}$  be any prime of  $K_+^r$ . If  $\mathfrak{l}$  is unramified in  $K^r/K_+^r$ , then by (3.6), we have  $\text{ord}_{\mathfrak{l}}(\beta) \equiv 0 \pmod{2}$ . So by the definition of  $\alpha$ , we have  $\text{ord}_{\mathfrak{l}}(\alpha) = 0$ . If  $\mathfrak{l}$  is ramified in  $K^r/K_+^r$ , then there exists  $i$  such that  $\mathfrak{l} = \mathfrak{l}_i$ , so we get

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

as  $n_i = \text{ord}_{l_i}(\lambda_i)$  is odd. Therefore, the quotient  $(\alpha/\beta)$  is a square of a fractional ideal  $\mathfrak{a}$  of  $\mathcal{O}_{K_+^r}$ . Thus  $\mathfrak{a}^2$  is generated by the totally positive  $\alpha/\beta$ . So the class of  $\mathfrak{a}$  is 2-torsion in the group  $\text{Cl}_{K_+^r}^+$ , which has an odd order, so there is a totally positive element  $\mu \in (K_+^r)^\times$  that generates  $\mathfrak{a}$ . So  $\alpha/\beta = \mu^2 \cdot \nu$  for some totally positive  $\nu \in \mathcal{O}_{K_+^r}^\times$ . Moreover, since  $\text{Cl}_{K_+^r} = \text{Cl}_{K_+^r}^+$ , the norm of the fundamental unit  $\epsilon$  is negative. Therefore, a unit in  $\mathcal{O}_{K_+^r}$  is totally positive if and only if it is a square in  $\mathcal{O}_{K_+^r}$ . Hence  $\nu$  is a square in  $\mathcal{O}_{K_+^r}$  so we get  $\alpha/\beta \in (K_+^r)^\times$ .  $\square$

*Proof of Claim 2* For any given  $i$ , if  $l_i$  is inert in  $K_+^r/\mathbb{Q}$ , then  $n_i = 1$  and  $\lambda_i = l_i \in \mathbb{Z}_{>0}$  is prime. If  $l_i$  is not inert in  $K_+^r/\mathbb{Q}$  then  $l_i \in \{p, q\}$ , by Proposition 3.18. If  $l_i = q$ , then as  $l_i$  is ramified in  $K^r/K_+^r$ , by Lemma 3.15 we get  $\sqrt{q} \in K_+$ , contradiction. So if  $l_i$  is not inert in  $K_+^r/\mathbb{Q}$ , then  $l_i = p$ .

Let

$$\{s_1, \dots, s_u\} = \{l_i : i = 1, \dots, t_{K^r} \text{ such that } l_i \text{ is inert in } K_+^r/\mathbb{Q} \\ \text{and } \text{ord}_{l_i}(\beta) \equiv 1 \pmod{2}\}.$$

Write  $p\mathcal{O}_{K_+^r} = \mathfrak{p}\mathfrak{p}'$  and let  $j \in \mathbb{Z}_{>0}$  be minimal such that  $\mathfrak{p}^j$  is principal and generated by a totally positive generator  $\pi$ . Let  $\pi'$  be the quadratic conjugate of  $\pi$ . Then  $\pi'$  is a totally positive generator of  $(\mathfrak{p}')^j$  and we have  $\pi\pi' = \mathfrak{p}^j$ . We find  $\alpha = \pi^a \pi'^{a'} \prod_{i=1}^u s_i$  for some  $a, a' \in \{0, 1\}$ . If  $a = a'$ , then  $\alpha \in \mathbb{Z}$ , which leads to a contradiction since  $K^r$  is non-biquadratic. So we either have  $\alpha = \pi \prod_{i=1}^u s_i$  or  $\alpha = \pi' \prod_{i=1}^u s_i$ . Swapping  $\mathfrak{p}$  with  $\mathfrak{p}'$  and  $\pi$  with  $\pi'$  if necessary, we find that we are in the former case.

To finish the proof of Claim 2, it remains to show  $u \in \{t_{K^r} - 1, t_{K^r} - 2\}$ .

If  $p \neq 2$ , then by (3.6) we get that  $u$  is  $t_{K^r}$  minus 1 for  $\pi$  (or  $\pi'$ ), minus at most one for every ramified prime of  $K_+^r$  lying over  $2 \neq p$ . Since such primes are inert in  $K_+^r/\mathbb{Q}$ , we get that there is at most one such prime, so  $u \in \{t_{K^r} - 1, t_{K^r} - 2\}$ .

If  $p = 2$ , then by (3.6), as there are only two primes  $\mathfrak{p}$  and  $\mathfrak{p}'$  over 2 in  $K_+^r$ , we get  $u \in \{t_{K^r} - 1, t_{K^r} - 2\}$ . This proves Claim 2.

Taking a different choice of  $j$  or a different generator  $\pi$  as in (iv) does not change the field by the proof of Claim 1 above. Finally, note that  $K_+^r(\sqrt{\alpha}) = \mathbb{Q}(\sqrt{\alpha})$ , and as  $\pi \prod_{i=1}^u s_i$  and  $\pi' \prod_{i=1}^u s_i$  are conjugate, their square roots generate isomorphic number fields over  $\mathbb{Q}$ . This proves (iv).  $\square$

### 3.6 A sharper bound for $d_{K^r}/d_{K_+^r}$

**Lemma 3.20** *Let  $K$  be a non-Galois PQ1 field with normal closure  $N$ . Let the notation be as in Proposition 3.19 and let  $t = t_{K^r}$ . If  $u = t - 2$ , then let  $s_{t-1} = 2$ . Then we have*

$$p^4 q^4 s_1^4 \cdots s_{t-1}^4 \leq d_N \quad \text{and} \\ p q s_1^2 \cdots s_{t-1}^2 \leq d_{K^r}/d_{K_+^r}.$$

*Proof* Let  $\pi, \pi'$  and  $\mathfrak{p}$  be as in the proof of Proposition 3.19, and write  $\pi - \pi' = \sqrt{q}f$  with  $f \in \mathbb{Z}$ . Then the discriminant of  $\mathbb{Z}[\sqrt{-\pi s_1 \cdots s_u}] \subset \mathcal{O}_{K^r}$  is  $(s_1 \cdots s_u)^6 2^4 p q^2 f^4$ . As this is a square times the discriminant  $d_{K^r}$  of  $\mathcal{O}_{K^r}$ , we find that  $d_{K^r}$  is  $p$  times a square. As  $d_{K^r}/d_{K_+^r}^2$  is the norm of the relative discriminant of  $K^r/K_+^r$ , we find that it is divisible by the norm of every prime of  $K_+^r$  that ramifies in  $K^r$ . So  $d_{K^r}/d_{K_+^r}^2/p$  is a square integer divisible by



$s_1 \cdots s_u$  and if  $u = t - 2$ , then (as in the proof of Proposition 3.19) we have  $2 \nmid s_1 \cdots s_u$  and  $d_{K^r}/d_{K_+^r}^2/p$  is also divisible by 2. We get that  $d_{K^r}/d_{K_+^r}^2/p$  is divisible by  $(s_1 \cdots s_{t-1})^2$ , hence  $d_{K^r}/d_{K_+^r}$  is divisible by  $pq(s_1 \cdots s_{t-1})^2$ , which proves the second assertion.

We also get that  $d_{K^r}$  is divisible by  $p(qs_1 \cdots s_{t-1})^2$  and  $d_{K_+}$  is divisible by  $p$ , hence  $d_N$  is divisible by  $p^2(qs_1 \cdots s_{t-1})^4$  and by  $p^4$ . This proves the result except in the case  $p = 2$ ,  $u = t - 2$ . However, in that case  $d_{K_+} = 8$ , hence  $d_N$  is divisible by  $8^4 = 2^4 p^4 s_{t-1}^4$ , which proves the result.  $\square$

**Theorem 3.21** *Let  $K$  be a non-Galois PQ1 field with normal closure  $N$  and reflex field  $K^r$ . If  $d_N^{1/8} \geq 222$ , then we have  $h_{K^r}^* \leq 2^5$  and  $d_{K^r}/d_{K_+^r} < 2.3 \cdot 10^{10}$ .*

*Proof* By Lemma 3.20, we have

$$d_{K^r}/d_{K_+^r} \geq pq s_1^2 \cdots s_{t_{K^r}-1}^2 \geq p_{t_{K^r}} p_{t_{K^r}+1} \Delta_{t_{K^r}-1}^2,$$

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

Let

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

Then we have  $h_{K^r} \geq f(d_{K^r}/d_{K_+^r})$  by Proposition 3.9.

Recall that, by Lemma 3.10, the function  $f$  is monotonically increasing for  $D \geq 52$ . Therefore, if  $t_{K^r} \geq 3$ , then we have  $f(d_{K^r}/d_{K_+^r}) \geq f(p_{t_{K^r}} p_{t_{K^r}+1} \Delta_{t_{K^r}-1}^2)$ . So under the assumption  $I_0(\Phi^r) = I_{K^r}$ , by Proposition 3.1, we have

$$2^{t_{K^r}-1} \geq f(d_{K^r}/d_{K_+^r}) \geq f(p_{t_{K^r}} p_{t_{K^r}+1} \Delta_{t_{K^r}-1}^2),$$

and hence we get  $h(t_{K^r}) \leq 1$ .

The function  $h(t)$  is monotonically increasing for  $t \geq 4$  by arguments similar to those we used in Lemma 3.10. Indeed, by Bertrand's postulate [26], we have

$$p_t p_{t+2} < 2p_t p_{t+1} < p_t p_{t+1} \Delta_{t-1}^2$$

for  $t \geq 2$ . This yields

$$\begin{aligned} \log(p_{t+1} p_{t+2} \Delta_t^2) + 0.057 &= \log(p_t p_{t+2}) + \log(p_t p_{t+1} \Delta_{t-1}^2) + 0.057 \\ &< 2(\log(p_t p_{t+1} \Delta_{t-1}^2) + 0.057) \end{aligned}$$

for  $t \geq 2$ . Therefore, we get

$$\frac{h(t+1)}{h(t)} = \frac{\sqrt{p_t p_{t+2}} (\log(p_t p_{t+1} \Delta_{t-1}^2) + 0.057)^2}{2 (\log(p_{t+1} p_{t+2} \Delta_t^2) + 0.057)^2} > \frac{\sqrt{p_t p_{t+2}}}{8} > 1$$

whenever  $t \geq 4$ , which proves monotonicity.

We compute that  $h(t) > 1$  if  $t = 7$ . So we get  $t_{K^r} \leq 6$  and  $h_{K^r}^* \leq 2^5$ . We then compute  $f(23 \cdot 10^9) > 32$ , which by  $2^5 \geq h_{K^r}^* \geq f(D)$  and monotonicity of  $f$  proves the bound on  $D$ .  $\square$

Now that we have an upper bound for  $h_{K^r}^*$ , we can find an upper bound for the prime  $p$  and improve the bound for  $d_{K^r}/d_{K_+^r}$ .

**Table 2** Definition of  $D_v$  and  $B_v$ , used in Corollaries 3.22 and 3.23

| $v$ | $D_v$               | $B_v$               |
|-----|---------------------|---------------------|
| 0   | $3.5 \cdot 10^6$    | $5.5 \cdot 10^6$    |
| 1   | $2.2 \cdot 10^7$    | $3.3 \cdot 10^7$    |
| 2   | $1.32 \cdot 10^8$   | $1.875 \cdot 10^8$  |
| 3   | $7.5 \cdot 10^8$    | $1.05 \cdot 10^9$   |
| 4   | $4.2 \cdot 10^9$    | $5.75 \cdot 10^9$   |
| 5   | $2.3 \cdot 10^{10}$ | $2.3 \cdot 10^{10}$ |

**Corollary 3.22** *Let  $K$  be a non-Galois PQ1 field with normal closure  $N$ . Let  $v$  be such that  $h_{K^r}^* = 2^v$ . If  $d_N^{1/8} \geq 222$ , then we have  $d_{K^r}/d_{K^r_+} \leq D_v$  with  $D_v$  as defined in Table 2.*

*Proof* By Proposition 3.9 we have  $f(d_{K^r}/d_{K^r_+}) \leq h_{K^r}^*$  for some explicit function  $f(x)$ . The function  $f(x)$  is monotonically increasing for  $x \geq 52$  (Lemma 3.10). We can therefore verify the result by evaluating  $f$  in  $D_v$ , which we did using interval arithmetic in SageMath [29]. □

**Corollary 3.23** *Let  $K$  be a non-Galois PQ1 field with normal closure  $N$ . Let the notation be as in Proposition 3.19. If  $d_N^{1/8} \geq 222$ , then we have  $u \in \{0, 1, \dots, 5\}$  and  $pq < B_0$  with  $B_0$  as in Table 2. Moreover, for all positive integers  $i \leq u$ , we have  $s_1 \cdots s_i < \max\{\sqrt{B_i/(pq)}, 222^2/(pq)\}$  with  $B_i$  as defined in Table 2.*

*Proof* By Proposition 3.19, we have  $u \in \{t - 1, t - 2\}$ , where  $t = t_{K^r}$ .

Recall that by Proposition 3.1 and Theorem 3.21, we have  $2^{t-1} = h_{K^r} \leq 2^5$ , which gives  $u \leq 5$ .

As in Lemma 3.20, if  $u = t - 2$ , let  $s_{t-1} = 2$ .

If  $d_N < 222^8$ , then Lemma 3.20 gives  $s_1 \cdots s_{t-1} \leq d_N^{1/4}/(pq) < 222^2/(pq)$ . If  $d_N \geq 222^8$ , then by Corollary 3.22, we get

$$s_1 \cdots s_{t-1} \leq \sqrt{d_{K^r}/d_{K^r_+}/(pq)} < \sqrt{D_{t-1}/(pq)}$$

with  $D_{t-1}$  defined in Table 2.

In both cases, this proves

$$s_1 \cdots s_{t-1} < \max\{\sqrt{D_{t-1}/(pq)}, 222^2/(pq)\}, \tag{3.7}$$

which implies  $pq < \max\{D_{t-1}/\Delta_{t-1}^2, 222^2\}$ , where  $\Delta_{t-1}$  is the product of the first  $t - 1$  prime numbers. We check that for all  $v \in \{0, \dots, 5\}$ , we have  $D_v \leq \Delta_v^2 B_0$ , hence we get  $pq < B_0$ .

Moreover, in the case  $u = t - 2$ , inequality (3.7) gives  $s_1 \cdots s_u = s_1 \cdots s_{t-1} < \max\{\sqrt{D_{t-1}/(pq)}/2, 222^2/(pq)\}$ . So we conclude that if  $u < 5$ , then

$$\begin{aligned} s_1 \cdots s_u &< \max\{\sqrt{D_u/(pq)}, \sqrt{D_{u+1}/(pq)}/2, 222^2/(pq)\} \\ &= \max\{\sqrt{D_{u+1}/(pq)}/2, 222^2/(pq)\} \end{aligned}$$

and if  $u = 5$  then  $s_1 \cdots s_u < \max\{\sqrt{D_u/(pq)}, 222^2/(pq)\}$ .

The number  $B_v$  of Table 2 is given by

$$B_v = \begin{cases} D_{v+1}/4 & \text{if } v < 5 \\ D_v & \text{if } v = 5, \end{cases}$$

so we get  $s_1 \cdots s_u < \max\{\sqrt{B_u/(pq)}, 222^2/(pq)\}$ .

Now given an integer  $i$  with  $0 < i \leq u$ , this gives

$$\begin{aligned} s_1 \cdots s_i &\leq \max\{\sqrt{B_u/(pq)}, 222^2/(pq)\}/(s_{i+1} \cdots s_u) \\ &< \max\{\sqrt{3^{-2(u-i)}B_u/(pq)}, 222^2/(pq)\} \\ &\leq \max\{\sqrt{B_i/(pq)}, 222^2/(pq)\}. \end{aligned}$$

□

### 3.7 Enumerating non-Galois PQ1 fields

Combining Proposition 3.19 with the bound of Corollary 3.23, we now have a good way of listing candidate non-Galois PQ1 fields. Postponing the discussion of how to recognise which fields are PQ1 to Sect. 3.8 and Algorithm 3, we get the following algorithm.

---

#### Algorithm 1 Computing all non-Galois PQ1 fields

---

**Input:** Nothing.

**Output:** All non-Galois PQ1 fields.

1. Make a list  $L$  of all pairs  $(p, q)$  of primes with  $p \cdot q < 5.5 \cdot 10^6$  such that  $q \not\equiv 3 \pmod{4}$ ,  $p$  is split in  $\mathbb{Q}(\sqrt{q})$  and  $q$  is split in  $\mathbb{Q}(\sqrt{p})$ .
2. For each pair  $(p, q) \in L$ , iterate over all tuples  $s_1 < s_2 < \cdots < s_u$  of primes such that
  - (i)  $0 \leq u \leq 5$ ,
  - (ii)  $s_1, \dots, s_u$  are inert in  $\mathbb{Q}(\sqrt{p})$  and  $\mathbb{Q}(\sqrt{q})$ ,
  - (iii) for all  $i \leq u$ , we have  $s_1 \cdots s_i < \max\{\sqrt{B_i/(pq)}, 222^2/(pq)\}$  with  $B_i$  as in Table 2.

For each such tuple, do the following:

- a Create a field  $K^r$  from  $(p, q, s_1, \dots, s_u)$  as follows.
    - (i) Write  $p\mathcal{O}_{K^r} = \mathfrak{p}\mathfrak{p}'$ .
    - (ii) Let  $j$  be the order of  $\mathfrak{p}$  in the narrow class group of  $\mathbb{Q}(\sqrt{q})$ , which is odd because only the prime  $q$  is ramified in  $\mathbb{Q}(\sqrt{q})$ . Let  $\pi$  be a totally positive generator of  $\mathfrak{p}^j$ .
    - (iii) Let  $K^r = \mathbb{Q}(\sqrt{-\pi s_1 \cdots s_u})$ .
  - b Test whether the reflex field  $K$  of  $K^r$  has CM class number one, using Algorithm 3 below. If so, output  $K$ .
- 

*Proof of Algorithm 1* Let  $K$  be a non-Galois PQ1 field. Then Proposition 3.19 states that the reflex field  $K^r$  is isomorphic to the field constructed in Step 2a for some  $p, q, s_1, \dots, s_u$  satisfying the splitting and congruence conditions of Step 1 and the conditions 2(ii). Moreover, Corollary 3.23 states that  $p, q, s_1, \dots, s_u$  satisfy the bounds of Steps 1, 2(i) and 2(iii).

Finally, the field “ $K$ ” in Step 2b is isomorphic to  $K$  as the isomorphism class of the reflex field of  $K^r$  does not depend on the choice of a CM type by Lemma 2.1 (see also the paragraph below the proof of Lemma 2.1).  $\square$

### 3.8 Checking whether a field is PQ1

Now that we can enumerate all candidate non-Galois PQ1 fields, we need to check which of them actually have CM class number 1. Computing all class groups is too expensive, so we need fast ways to eliminate the fields of CM class number  $> 1$ .

Recall that the primitive quartic CM field  $K$  has CM class number 1 if for every fractional  $\mathcal{O}_{K^r}$ -ideal  $\mathfrak{b}$ , there is an element  $\alpha \in K^\times$  with  $N_{\Phi^r}(\mathfrak{b}) = (\alpha)$  and  $\alpha\bar{\alpha} \in \mathbb{Q}$  (2.1). Note that if  $\alpha$  exists, then in fact we have  $\alpha\bar{\alpha} = N_{K^r/\mathbb{Q}}(\mathfrak{b})$ .

Our first check is the following special case of Theorem D in Louboutin [21].

**Lemma 3.24** *Let  $(K, \Phi)$  be a non-Galois or cyclic quartic PQ1 type. If a rational prime  $l$  splits completely in  $K^r/\mathbb{Q}$ , then  $l \geq \frac{1}{4}\sqrt{d_K}/d_{K_+}$ .*

*Proof* Let  $l$  be a rational prime that splits completely in  $K^r/\mathbb{Q}$ . Let  $\mathfrak{b}$  be a prime ideal in  $K^r$  above  $l$ . By the assumption of CM class number 1, there exists  $\alpha \in K^\times$  such that  $N_{\Phi^r}(\mathfrak{b}) = (\alpha)$  and  $\alpha\bar{\alpha} = l$ . Here  $\alpha \neq \bar{\alpha}$ , since  $\sqrt{l} \notin K$ . Then since  $\mathcal{O}_K \supset \mathcal{O}_{K_+}[\alpha]$  and  $\Delta(\mathcal{O}_{K_+}[\alpha]/\mathcal{O}_{K_+}) = (\alpha - \bar{\alpha})^2$ , we have  $d_K/d_{K_+}^2 = N_{K_+/\mathbb{Q}}(d_{K/K_+}) = N_{K_+/\mathbb{Q}}(\Delta(\mathcal{O}_K/\mathcal{O}_{K_+})) \leq N_{K_+/\mathbb{Q}}((\alpha - \bar{\alpha})^2)$ . Moreover, since  $\alpha\bar{\alpha} = l$ , we have  $\phi(\alpha - \bar{\alpha})^2 \leq (2\sqrt{l})^2$  for all embeddings  $\phi : K_+ \hookrightarrow \mathbb{R}$ , hence  $d_K/d_{K_+}^2 \leq N_{K_+/\mathbb{Q}}((\alpha - \bar{\alpha})^2) \leq 16l^2$ .  $\square$

Lemma 3.24 allows us to discard many fields, but not enough, so we need a less crude test as well.

For recognising whether the ideals  $N_{\Phi^r}(\mathfrak{b})$  are generated by an element  $\alpha \in K^\times$  such that  $\alpha\bar{\alpha} = N_{K^r/\mathbb{Q}}(\mathfrak{b})$  we can use class groups and unit groups. However, for small primes  $\mathfrak{b}$ , it is faster to list *Weil numbers*, which are defined as follows. Let  $Q \in \mathbb{Z}$  be a positive integer (usually a prime power in the literature). A *Weil  $Q$ -number*  $\alpha$  is an algebraic integer such that all embeddings in  $\mathbb{C}$  have absolute value  $\sqrt{Q}$ . In particular, we want to check whether  $N_{\Phi^r}(\mathfrak{b})$  is generated by a Weil  $Q$ -number for  $Q = N(\mathfrak{b})$ .

---

#### Algorithm 2 Checking whether an ideal is generated by a Weil $Q$ -number

---

**Input:** An ideal  $\mathfrak{a} \subset \mathcal{O}_K$  in a quartic CM field  $K$  with totally real subfield  $K_0 = \mathbb{Q}(\sqrt{d})$  for a square-free integer  $d$ ; a positive integer  $Q$ .

**Output:** ‘True’ or ‘False’ according to whether  $\mathfrak{a}$  is generated by a Weil  $Q$ -number in  $K$ .

1. for all  $a \in [0, 2\sqrt{Q}] \cap \frac{1}{2}\mathbb{Z}$ ,
    - (a) let  $B = (2\sqrt{Q} - a)/\sqrt{d} \in \mathbb{R}$ .
    - (b) for all  $b \in [-B, B] \cap \frac{1}{2}\mathbb{Z}$ ,
      - (i) let  $\beta = a + b\sqrt{d} \in K_0 \subset K$ ,
      - (ii) if  $\beta^2 - 4Q$  is square in  $K$ , then let  $\alpha_{\pm} = (-\beta \pm \sqrt{\beta^2 - 4Q})/2$ ,
      - (iii) if  $\mathfrak{a}$  is generated by one of  $\alpha_{\pm}$ , then return ‘True’.
  2. return ‘False’.
-

*Proof* If  $\mathfrak{a}$  is generated by a Weil  $Q$ -number  $\alpha$ , then let  $\beta = \alpha + \bar{\alpha}$  and write  $\beta = a + b\sqrt{d}$ . Changing  $\alpha$  into  $-\alpha$  if needed, we get  $a \geq 0$ . We get  $\alpha = (-\beta \pm \sqrt{\beta^2 - 4Q})/2$  and we get  $|\beta| \leq 2\sqrt{Q}$  for all complex embeddings. As a consequence, the numbers  $a$  and  $b$  are in the intervals in the algorithm.

Conversely, if the output is true, then  $\alpha_{\pm}$  is a Weil  $Q$ -number that generates  $\mathfrak{a}$ . □

Algorithm 2 takes time linear in  $Q$ , so we only want to do it for small  $Q$ . Once we have done this for enough small-norm ideals  $\mathfrak{b}$  to convince ourselves that  $K$  has CM class number one, we do a final verification using the class group, which is possible as we then only have fields of small discriminant left.

For that final verification, we take generators  $\mathfrak{b}$  of the class group and check that  $N_{\Phi^r}(\mathfrak{b})$  is generated by  $\alpha \in K^\times$  such that  $\alpha\bar{\alpha} \in \mathbb{Q}$ . As we have computed the class group and unit group, we could use [30, Algorithm 2.8], which is available as `atomu`( $\Phi^r, \mathfrak{b}$ ) in [31]. In practice  $Q = N_{K^r/\mathbb{Q}}(\mathfrak{b})$  is small, so we use Algorithm 2 instead.

---

**Algorithm 3** Eliminating non-PQ1 fields

---

**Input:** A primitive quartic CM field  $K^r$ .

**Output:** ‘True’ or ‘False’ according to whether the reflex field  $K$  of  $K^r$  is PQ1.

1. Choose a CM type  $\Phi^r$  of  $K^r$ , calculate its reflex field  $K$  and the discriminants of  $K$  and  $K_+$ .
  2. If  $K^r$  has totally split primes in  $K^r$  below the bound  $\frac{1}{4}d_K^{1/2}/d_{K_+}$ , then return ‘False’.
  3. For each prime ideal  $\mathfrak{q}$  in  $\mathcal{O}_{K^r}$  with  $Q := N_{K^r/\mathbb{Q}}(\mathfrak{q}) < 12 \log(|d_{K^r}|)^2$ , use Algorithm 2 to check whether  $N_{\Phi^r}(\mathfrak{q})$  is generated by a Weil  $Q$ -number. If it is not, then return ‘False’.
  4. Compute representative prime ideals of a set of generators of the class group  $I_{K^r}/P_{K^r}$ . For each such ideal  $\mathfrak{q}$ , use Algorithm 2 to check whether  $N_{\Phi^r}(\mathfrak{q})$  is generated by a Weil  $Q$ -number for  $Q := N(\mathfrak{q})$ , and return ‘False’ if it is not.
  5. Return ‘True’.
- 

*Proof of Algorithm 3* Let  $(K, \Phi)$  be the reflex of  $(K^r, \Phi^r)$  with  $\Phi^r$  as in Step 1. Note that the isomorphism class of  $K$  does not depend on the choice of  $\Phi^r$  (see Lemma 2.1), and neither does the order of its CM class group (Lemma 2.3).

Steps 2 and 3 only eliminate fields with CM class number greater than 1 (in case of Step 2 by Lemma 3.24 and in case of Step 3 by definition). In particular, these steps (which are only meant to speed up the computation) have no effect on the validity of the output. Step 4 tests exactly (using the definition) whether the reflex  $(K, \Phi)$  has CM class number one. □

*Remark 3.25* Step 3 checks whether  $K$  is a PQ1 field or not under assumption of the generalized Riemann hypothesis (GRH), see Bach [32]. There are no fields eliminated in Step 4 as expected, as otherwise this would contradict the GRH.

To specify quartic CM fields, we use the following notation of the ECHIDNA database [33]. Given a quartic CM field  $K$ , let  $D$  be the discriminant of the real quadratic subfield  $K_+$  of  $K$ . Write  $K = K_+(\sqrt{-\alpha})$  where  $\alpha$  is a totally positive element of  $\mathcal{O}_{K_+}$  and take  $\alpha$  such that  $A := \text{Tr}_{K_+/\mathbb{Q}}(\alpha) > 0$  is minimal and let  $B := N_{K_+/\mathbb{Q}}(-\alpha)$ . We choose  $\alpha$  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  $K \cong \mathbb{Q}[X]/(X^4 + AX^2 + B)$ .

We implemented the algorithms in SageMath [29,31,34] and obtained the list of the fields in Table 3. The implementation is available online at [35]. This computation is easily parallelized and took 3.7 core-days using standard CPUs. In Step 4, we could choose to use `a_t_o_mu` instead of Algorithm 2, which would not change the computation time much (3.8 core-days instead of 3.7), but we do profit from having Algorithm 2 in Step 3, as otherwise the computation takes more than 242 core-days. Step 3 is therefore essential for keeping the computation manageable.

This proves the non-Galois case of our main result:

**Theorem 3.26** *There exist exactly 63 isomorphism classes of non-Galois quartic CM fields with CM class number one. The fields are exactly those listed in Table 3.*

### 4 Cyclic PQ1 fields

We now determine all cyclic PQ1 fields. Murabayashi and Umegaki [7,14] already determined those for which the curves with CM by the *maximal* order can be defined over  $\mathbb{Q}$ , but there are more cyclic PQ1 fields. We will show (Theorem 4.7) that Table 1b of [9] is complete, which is necessary for proving that the list of all absolutely simple genus-two CM curves over  $\mathbb{Q}$  in [10] is complete (Theorem 5.6).

Theorem 4.7 gives only a few more fields than [7], and indeed unlike the non-Galois case of Sect. 3, we do not need much beyond what is already in [7].

Suppose that  $K/\mathbb{Q}$  is a cyclic quartic CM field with  $\text{Gal}(K/\mathbb{Q}) = \langle y \rangle$ . In this notation complex conjugation is  $y^2$ . As the CM class number does not depend on the CM type (Lemma 2.3), we choose  $\Phi = \{\text{id}, y\}$ . This CM type is primitive and satisfies  $K^r = K$  and  $\Phi^r = \{\text{id}, y^3\}$ .

We start with the following result, of which Proposition 3.18 is a non-Galois analogue.

**Proposition 4.1** (Murabayashi) *A quartic cyclic CM field  $K$  is PQ1 if and only if all of the following hold:*

- (i) *there is exactly one totally ramified prime in  $K/\mathbb{Q}$ ;*
- (ii) *the other ramified primes of  $K/\mathbb{Q}$  are inert in  $K_+/\mathbb{Q}$ ;*
- (iii)  *$h_K^* = 2^{t_K-1}$  where  $t_K$  is the number of ramified primes in  $K/K_+$ .*

*Proof* This is Proposition 4.5 (i) and (iii) of Murabayashi [14]. For the notation used there, see Lemma 4.2 of [14] and the paragraph above it. □

By weakening the assumptions in [14, Theorem 4.12], we obtain the following result.

**Proposition 4.2** *Let  $K$  be a cyclic PQ1 field. Then there exist prime numbers  $p, s_1, \dots, s_u$  with  $u \in \{t_K - 1, t_K - 2\}$  such that all of the following hold.*

- (i) *We have  $K_+ = \mathbb{Q}(\sqrt{p})$  with  $p \not\equiv 3 \pmod{4}$ .*
- (ii) *The prime  $s_i$  is inert in  $K_+$  for all  $i$ .*
- (iii) *We have  $K \cong \mathbb{Q}(\sqrt{-\epsilon s_1 \cdots s_u \sqrt{p}})$  for every  $\epsilon \in \mathcal{O}_{K_+}^\times$  with  $\epsilon \sqrt{p} \gg 0$ .*

*Proof* Let  $\beta \in \mathcal{O}_{K_+}$  be a totally positive element such that  $K = K_+(\sqrt{-\beta})$ . We will construct a totally positive element  $\alpha \in K_+^\times$  in terms of the ramified primes in  $K/K_+$  and show that  $\alpha$  and  $\beta$  differ by a factor in  $(K_+^\times)^2$ .

**Table 3** Table of fields referenced in Theorem 3.26

| $D$ | $A$ | $B$  | $p$ | $q$ | $s_1 \cdots s_u$ | $h_{K_+}$ | $h_K^*$ | reflex $D, A, B$ |     |     |
|-----|-----|------|-----|-----|------------------|-----------|---------|------------------|-----|-----|
| 5,  | 11, | 29   | 5   | 29  | 1                | 1         | 2       | 29,              | 7,  | 5   |
| 5,  | 13, | 41   | 5   | 41  | 1                | 1         | 1       | 41,              | 11, | 20  |
| 5,  | 17, | 61   | 5   | 61  | 1                | 1         | 1       | 61,              | 9,  | 5   |
| 5,  | 21, | 109  | 5   | 109 | 1                | 1         | 1       | 109,             | 17, | 45  |
| 5,  | 26, | 149  | 5   | 149 | 1                | 1         | 1       | 149,             | 13, | 5   |
| 5,  | 33, | 261  | 5   | 29  | 3                | 1         | 2       | 29,              | 21, | 45  |
| 5,  | 34, | 269  | 5   | 269 | 1                | 1         | 1       | 269,             | 17, | 5   |
| 5,  | 41, | 389  | 5   | 389 | 1                | 1         | 1       | 389,             | 37, | 245 |
| 5,  | 66, | 909  | 5   | 101 | 3                | 1         | 2       | 101,             | 33, | 45  |
| 8,  | 10, | 17   | 2   | 17  | 1                | 1         | 1       | 17,              | 5,  | 2   |
| 8,  | 14, | 41   | 2   | 41  | 1                | 1         | 2       | 41,              | 7,  | 2   |
| 8,  | 18, | 73   | 2   | 73  | 1                | 1         | 1       | 73,              | 9,  | 2   |
| 8,  | 22, | 89   | 2   | 89  | 1                | 1         | 1       | 89,              | 11, | 8   |
| 8,  | 26, | 137  | 2   | 137 | 1                | 1         | 2       | 137,             | 13, | 8   |
| 8,  | 30, | 153  | 2   | 17  | 3                | 1         | 4       | 17,              | 15, | 18  |
| 8,  | 34, | 281  | 2   | 281 | 1                | 1         | 1       | 281,             | 17, | 2   |
| 8,  | 38, | 233  | 2   | 233 | 1                | 1         | 1       | 233,             | 19, | 32  |
| 8,  | 50, | 425  | 2   | 17  | 5                | 1         | 2       | 17,              | 25, | 50  |
| 8,  | 66, | 1017 | 2   | 113 | 3                | 1         | 2       | 113,             | 33, | 18  |
| 12, | 8,  | 13   | 3   | 13  | 2                | 1         | 2       | 13,              | 10, | 12  |
| 12, | 10, | 13   | 3   | 13  | 1                | 1         | 2       | 13,              | 5,  | 3   |
| 12, | 14, | 37   | 3   | 37  | 1                | 1         | 2       | 37,              | 7,  | 3   |
| 12, | 26, | 61   | 3   | 61  | 1                | 1         | 2       | 61,              | 13, | 27  |
| 12, | 26, | 157  | 3   | 157 | 1                | 1         | 2       | 157,             | 13, | 3   |
| 12, | 50, | 325  | 3   | 13  | 5                | 1         | 4       | 13,              | 25, | 75  |
| 13, | 9,  | 17   | 13  | 17  | 1                | 1         | 1       | 17,              | 15, | 52  |
| 13, | 18, | 29   | 13  | 29  | 1                | 1         | 1       | 29,              | 9,  | 13  |
| 13, | 29, | 181  | 13  | 181 | 1                | 1         | 1       | 181,             | 41, | 13  |
| 13, | 41, | 157  | 13  | 157 | 1                | 1         | 1       | 157,             | 25, | 117 |
| 17, | 5,  | 2    | 17  | 2   | 1                | 1         | 1       | 8,               | 10, | 17  |
| 17, | 15, | 52   | 17  | 13  | 1                | 1         | 1       | 13,              | 9,  | 17  |
| 17, | 25, | 50   | 17  | 2   | 5                | 1         | 2       | 8,               | 50, | 425 |
| 17, | 46, | 257  | 17  | 257 | 1                | 1         | 1       | 257,             | 23, | 68  |
| 17, | 47, | 548  | 17  | 137 | 1                | 1         | 1       | 137,             | 35, | 272 |
| 29, | 7,  | 5    | 29  | 5   | 1                | 1         | 2       | 5,               | 11, | 29  |
| 29, | 9,  | 13   | 29  | 13  | 1                | 1         | 1       | 13,              | 18, | 29  |
| 29, | 21, | 45   | 29  | 5   | 3                | 1         | 2       | 5,               | 33, | 261 |
| 29, | 26, | 53   | 29  | 53  | 1                | 1         | 1       | 53,              | 13, | 29  |
| 41, | 11, | 20   | 41  | 5   | 1                | 1         | 1       | 5,               | 13, | 41  |
| 44, | 8,  | 5    | 11  | 5   | 2                | 1         | 2       | 5,               | 14, | 44  |
| 44, | 14, | 5    | 11  | 5   | 1                | 1         | 2       | 5,               | 7,  | 11  |
| 44, | 42, | 45   | 11  | 5   | 3                | 1         | 4       | 5,               | 21, | 99  |
| 53, | 13, | 29   | 53  | 29  | 1                | 1         | 1       | 29,              | 26, | 53  |
| 61, | 9,  | 5    | 61  | 5   | 1                | 1         | 1       | 5,               | 17, | 61  |
| 73, | 9,  | 2    | 73  | 2   | 1                | 1         | 1       | 8,               | 18, | 73  |

**Table 3** continued

| $D$  | $A$ | $B$ | $p$ | $q$ | $s_1 \cdots s_u$ | $h_{K_+}$ | $h_K^*$ | reflex $D, A, B$ |     |      |
|------|-----|-----|-----|-----|------------------|-----------|---------|------------------|-----|------|
| 73,  | 47, | 388 | 73  | 97  | 1                | 1         | 1       | 97,              | 94, | 657  |
| 76,  | 18, | 5   | 19  | 5   | 1                | 1         | 2       | 5,               | 9,  | 19   |
| 89,  | 11, | 8   | 89  | 2   | 1                | 1         | 1       | 8,               | 22, | 89   |
| 97,  | 94, | 657 | 97  | 73  | 1                | 1         | 1       | 73,              | 47, | 388  |
| 101, | 33, | 45  | 101 | 5   | 3                | 1         | 2       | 5,               | 66, | 909  |
| 109, | 17, | 45  | 109 | 5   | 1                | 1         | 1       | 5,               | 21, | 109  |
| 113, | 33, | 18  | 113 | 2   | 3                | 1         | 2       | 8,               | 66, | 1017 |
| 137, | 35, | 272 | 137 | 17  | 1                | 1         | 1       | 17,              | 47, | 548  |
| 149, | 13, | 5   | 149 | 5   | 1                | 1         | 1       | 5,               | 26, | 149  |
| 157, | 25, | 117 | 157 | 13  | 1                | 1         | 1       | 13,              | 41, | 157  |
| 172, | 34, | 117 | 43  | 13  | 1                | 1         | 2       | 13,              | 17, | 43   |
| 181, | 41, | 13  | 181 | 13  | 1                | 1         | 1       | 13,              | 29, | 181  |
| 233, | 19, | 32  | 233 | 2   | 1                | 1         | 1       | 8,               | 38, | 233  |
| 236, | 32, | 20  | 59  | 5   | 1                | 1         | 2       | 5,               | 16, | 59   |
| 257, | 23, | 68  | 257 | 17  | 1                | 3         | 1       | 17,              | 46, | 257  |
| 269, | 17, | 5   | 269 | 5   | 1                | 1         | 1       | 5,               | 34, | 269  |
| 281, | 17, | 2   | 281 | 2   | 1                | 1         | 1       | 8,               | 34, | 281  |
| 389, | 37, | 245 | 389 | 5   | 1                | 1         | 1       | 5,               | 41, | 389  |

The fields are  $K = \mathbb{Q}[X]/(X^4 + AX^2 + B)$  with  $d_{K_+} = D$ . Their reflex fields are  $K^r \cong \mathbb{Q}(\sqrt{-\pi s_1 \cdots s_u})$  where  $\pi$  is totally positive of norm  $p$  inside the ring of integers of  $K_+^r = \mathbb{Q}(\sqrt{q})$ . The class number of  $K_+$  is  $h_{K_+}$  and the class number of  $K$  is  $h_{K_+} h_K^*$ . The reflex field  $K^r$  is also given by the  $D, A$  and  $B$  in the final column

By Proposition 4.1, we have  $K_+ = \mathbb{Q}(\sqrt{p})$ , where  $p$  is a prime with  $p \not\equiv 3 \pmod{4}$ . There are  $t_K$  ramified primes in  $K/K_+$ , and the ones that are distinct from  $(\sqrt{p})$  are inert in  $K_+/\mathbb{Q}$ , by Proposition 4.1. Let  $S$  be the set of prime numbers generating these inert prime ideals and let  $s_1, s_2, \dots, s_u$  be the elements of  $\{s \in S : s \text{ or } \text{ord}_{(s)}(\beta) \text{ is odd}\}$ .

We then have  $u \in \{t_K - 1, t_K - 2\}$ .

Since  $p \not\equiv 3 \pmod{4}$ , by the genus theory for quadratic fields, we have  $N_{K_+/\mathbb{Q}}(\epsilon) = -1$  where  $\epsilon$  is the fundamental unit of  $\mathcal{O}_{K_+}$ . Take  $\epsilon > 0$  so that  $\epsilon\sqrt{p} \gg 0$ .

Take  $\alpha = s_1 \cdots s_u$  if  $\text{ord}_{(\sqrt{p})}(\beta)$  is even, and take  $\alpha = \epsilon s_1 \cdots s_u \sqrt{p}$  otherwise.

Then exactly as in the proof of Claim 1 in the proof of Proposition 3.19, we have  $\alpha/\beta \in (K_+^\times)^2$ , hence  $K = K_+(\sqrt{-\alpha})$ .

In the case  $\alpha = s_1 \cdots s_u$ , we get a biquadratic field, contradiction. Therefore, we have  $\alpha = \epsilon s_1 \cdots s_u \sqrt{p}$  and  $K = K_+(\sqrt{-\alpha}) = \mathbb{Q}(\sqrt{-\alpha})$ . □

The next step is to bound the conductor and the relative class number.

**Theorem 4.3** (Louboutin [36], Theorem 5) *Let  $K$  be a cyclic quartic CM field of conductor  $f_K$  and discriminant  $d_K$ . Then we have*

$$h_K^* \geq \frac{2}{3e\pi^2} \left( 1 - \frac{4\pi e^{1/2}}{d_K^{1/4}} \right) \frac{f_K}{(\log(f_K) + 0.05)^2}. \tag{4.1}$$

Most of what is stated in the following two results are also observed in [7].

**Lemma 4.4** *Let  $K$  be a cyclic PQ1 field. In the notation of Proposition 4.2, if  $u = t_K - 2$ , then let  $s_{t_K-1} = 2$ . Then we have*

$$f_K \geq p s_1 \cdots s_{t_K-1} \quad \text{and} \quad d_K \geq 5f_K^2.$$



*Proof* By Propositions 11.9 and 11.10 in Chapter VII of [37], we have  $f_K^2 = d_K/d_{K^+}$ , hence  $d_K = f_K^2 d_{K^+} \geq 5f_K^2$ . Moreover, the conductor  $f_K$  is divisible by the ramified primes, hence  $f_K \geq ps_1 \cdots s_{t_K-1}$ .  $\square$

**Lemma 4.5** For real numbers  $D \geq 1$  and non-negative integers  $t$ , let

$$\ell(D) = \frac{2}{3e\pi^2} \left( 1 - \frac{4\pi e^{1/2}}{5D^{1/2}} \right) \frac{D}{(\log(D) + 0.05)^2} \quad \text{and} \quad g(t) = 2^{-t+1} \ell(\Delta_t) \quad (4.2)$$

where  $\Delta_t$  is the product of the first  $t$  prime numbers. Then  $\ell(D)$  increases monotonically for  $D \geq 1$  and  $g(t)$  increases monotonically for  $t \geq 0$ .

*Proof* We checked monotonicity of  $f$  and  $g$  in the same way as in Lemma 3.10.  $\square$

**Proposition 4.6** For every cyclic PQ1 field  $K$ , we have  $h_K^* \leq 2^5$  and  $f_K < 2 \cdot 10^5$ .

*Proof* Lemma 4.4 gives  $d_K \geq 5f_K^2$ . As the factor  $(1 - 4\pi e^{1/2} d_K^{-1/4})$  in (4.1) increases with  $d_K$ , Theorem 4.3 gives  $h_K^* \geq \ell(f_K)$ . By Lemma 4.4, we have  $f_K \geq ps_1 \cdots s_{t_K-1}$ . Let  $\Delta_t$  be the product of the first  $t$  primes. As  $f$  is monotonically increasing, we get  $h_K^* \geq \ell(\Delta_{t_K})$ . By Proposition 3.1, we have  $h_K^* = 2^{t_K-1}$ , so we obtain  $1 \geq g(t_K)$ . As  $g(t)$  is monotonically increasing with  $t \geq 0$  and we have  $g(7) > 1$ , we get  $t_K \leq 6$ . So we get  $h_K^* \leq 2^5$ .

Moreover, we compute  $\ell(2 \cdot 10^5) > 2^5$ , and therefore we get  $f_K < 2 \cdot 10^5$ .

---

#### Algorithm 4 Computing all cyclic PQ1 fields

---

**Input:** Nothing.

**Output:** All cyclic PQ1 fields.

Step 1. For each prime number  $p \leq 2 \cdot 10^5$  with  $p \not\equiv 3 \pmod{4}$ , iterate over all tuples  $s_1 < s_2 < \cdots < s_u$  of primes such that

- (i)  $0 \leq u \leq 5$ ,
- (ii)  $s_1, \dots, s_u$  are inert in  $\mathbb{Q}(\sqrt{p})$ ,
- (iii)  $ps_1 s_2 \cdots s_u \leq 2 \cdot 10^5$ .

Step 2. For each such tuple, take a fundamental unit  $\epsilon$  in  $\mathbb{Q}(\sqrt{p})$  such that  $\epsilon\sqrt{p} \gg 0$ , and construct  $K = \mathbb{Q}(\sqrt{-\epsilon s_1 \cdots s_u \sqrt{p}})$ .

Step 3. Test whether the CM field  $K$  has CM class number one, using Algorithm 3 for  $K^r = K$ . If so, output  $K$ .

---

*Proof* Propositions 4.2 and 4.6 show that every cyclic PQ1 field is listed. Algorithm 3 eliminates exactly the incorrect fields.  $\square$

We implemented the algorithm in SageMath [29, 31, 34] and obtained the list of the CM fields in Table 4. The implementation is available online at [35]. This computation took less than 2 core-hours.

This proves the cyclic case of our main result:

**Theorem 4.7** There exist exactly 20 isomorphism classes of cyclic quartic CM fields with CM class number one. The fields are exactly those listed in Table 4.

**Table 4** Table of fields referenced in Theorem 4.7

| $D$ | $A$  | $B$   | $f_K$                 | $\rho$ | $s_1 \cdots s_u$ | $h_{K_+}$ | $h_K^*$ |
|-----|------|-------|-----------------------|--------|------------------|-----------|---------|
| 5,  | 5,   | 5     | 5                     | 5      | 1                | 1         | 1       |
| 5,  | 10,  | 20    | $2^3 \cdot 5$         | 5      | 2                | 1         | 2       |
| 5,  | 15,  | 45    | $2^2 \cdot 3 \cdot 5$ | 5      | 3                | 1         | 4       |
| 5,  | 30,  | 180   | $2^3 \cdot 3 \cdot 5$ | 5      | $2 \cdot 3$      | 1         | 4       |
| 5,  | 35,  | 245   | $2^2 \cdot 5 \cdot 7$ | 5      | $2 \cdot 7$      | 1         | 4       |
| 5,  | 65,  | 845   | $5 \cdot 13$          | 5      | 13               | 1         | 2       |
| 5,  | 85,  | 1445  | $5 \cdot 17$          | 5      | 17               | 1         | 2       |
| 5,  | 105, | 2205  | $3 \cdot 5 \cdot 7$   | 5      | $3 \cdot 7$      | 1         | 4       |
| 8,  | 4,   | 2     | $2^4$                 | 2      | 1                | 1         | 1       |
| 8,  | 12,  | 18    | $2^4 \cdot 3$         | 2      | 3                | 1         | 2       |
| 8,  | 20,  | 50    | $2^4 \cdot 5$         | 2      | 5                | 1         | 2       |
| 13, | 13,  | 13    | 13                    | 13     | 1                | 1         | 1       |
| 13, | 26,  | 52    | $2^3 \cdot 13$        | 13     | 2                | 1         | 2       |
| 13, | 65,  | 325   | $5 \cdot 13$          | 13     | 5                | 1         | 2       |
| 17, | 119, | 3332  | $7 \cdot 17$          | 17     | 7                | 1         | 2       |
| 17, | 255, | 15300 | $3 \cdot 5 \cdot 17$  | 17     | $3 \cdot 5$      | 1         | 4       |
| 29, | 29,  | 29    | 29                    | 29     | 1                | 1         | 1       |
| 37, | 37,  | 333   | 37                    | 37     | 1                | 1         | 1       |
| 53, | 53,  | 53    | 53                    | 53     | 1                | 1         | 1       |
| 61, | 61,  | 549   | 61                    | 61     | 1                | 1         | 1       |

The fields are  $K = \mathbb{Q}[X]/(X^4 + AX^2 + B) \cong \mathbb{Q}(\sqrt{-\epsilon s_1 \cdots s_u \sqrt{p}})$ , where  $\epsilon$  is any totally positive unit in the maximal order of the real quadratic field  $K_+ = \mathbb{Q}(\sqrt{p})$  of discriminant  $D$ . The conductor of  $K$  is  $f_K$ , the class number of  $K_+$  is  $h_{K_+}$  and the class number of  $K$  is  $h_{K_+} h_K^*$

### 5 Consequences for curves of genus two with CM

In this section we derive Theorems 5.6–5.8 from the main results.

In order to study a curve  $C$  over a field  $k$  of characteristic 0 (by which we mean a smooth, projective, geometrically irreducible curve), we will work with its *Jacobian*  $A = J(C)$ , which is an abelian variety variety of dimension equal to the genus of  $C$ ; for details we refer to [38]. The Jacobian satisfies  $J(C)(\bar{k}) \cong \text{Pic}^0(C_{\bar{k}})$  and if  $k \subset \mathbb{C}$ , then  $J(C)(\mathbb{C}) \cong \mathbb{C}^g / \Lambda$  for the period lattice  $\Lambda$  of  $C$ .

An abelian variety  $A$  over a field  $k$  of characteristic 0 has *complex multiplication (CM)* if there exists an embedding  $\theta : K \rightarrow \text{End}(A_{\bar{k}}) \otimes \mathbb{Q}$  for a CM field  $K$  of dimension  $2 \cdot \dim(A)$ . In this case, we also say that  $A$  (or  $C$ ) has CM by  $K$  or that it has CM by the order  $\theta^{-1}(\text{End}(A_{\bar{k}})) \subset K$ .

Given  $A$  with CM by  $K$  via an embedding  $\theta$ , we obtain a CM-type  $\Phi$  of  $K$  with values in  $\bar{k}$  as follows. Let  $\text{Tgt}_0(A)$  be the tangent space of  $A$  over  $\bar{k}$  at 0. Let  $\Phi$  be the set of homomorphisms  $K \rightarrow \bar{k}$  occurring in the diagonalisation of the representation  $K \rightarrow \text{End}_{\bar{k}}(\text{Tgt}_0(A_{\bar{k}})) : \alpha \mapsto D(\theta(\alpha))$ . Then  $\Phi$  is a CM type of  $K$ , and we say that  $(A, \theta)$  is of type  $(K, \Phi)$ .

Our goal in this section is to state the following result and show how it follows from standard references.

**Proposition 5.1** *Let  $K$  be a quartic CM field and  $\Phi$  a CM type of  $K$ . Let  $C$  be a curve of genus 2 over  $K^r$  such that  $J(C)_{\mathbb{C}}$  has CM by an order  $\mathcal{O}$  in  $K$  of type  $\Phi$ . If  $J(C)_{\mathbb{C}}$  is simple or  $\text{End}(J(C)_{\mathbb{C}}) \cong \mathcal{O}$ , then  $K$  is a PQ1 field.*

A polarized abelian variety of type  $(K, \Phi)$  is a triple  $P = (A, \theta, \varphi)$  formed by an abelian variety  $(A, \theta)$  of type  $(K, \Phi)$  and a polarization  $\varphi$  of  $A$  such that  $\theta(K)$  is stable under the Rosati involution of  $\text{End}(A_{\bar{k}}) \otimes \mathbb{Q}$  determined by  $\varphi$ . For more details see Shimura–Taniyama [19, Chap. 14].

**Theorem 5.2** (Shimura–Taniyama) *Let  $P = (A, \theta, \varphi)$  be a polarized abelian variety over a field  $k$  and of type  $(K, \Phi)$ . Then the following are equivalent.*

- (i) *The abelian variety  $A$  is absolutely simple, i.e., not isogenous over  $\bar{k}$  to a product of abelian varieties of lower dimension.*
- (ii) *The endomorphism ring  $\text{End}(A_{\bar{k}})$  is an integral domain of rank  $2g$ .*
- (iii) *The CM type  $(K, \Phi)$  is primitive.*

*Proof* This follows e.g. from [20, I.3.3 and I.3.5].  $\square$

The field of moduli of a polarized abelian variety  $(A, \varphi)$  over a field  $k$  of characteristic zero is the unique field  $k_0 \subset k$  with the following property [19, I.4.2, Theorem 2]: for all embeddings  $\sigma : k \rightarrow \bar{k}$ , we have

$$(A, \varphi) \cong (\sigma A, \sigma \varphi) \iff \sigma|_{k_0} = \text{id}_{k_0}.$$

The first main theorem of complex multiplication tells us that  $k_0 \cdot K^r$  is a class field over  $K^r$  as follows.

**Theorem 5.3** (Shimura–Taniyama) *Let  $P = (A, \theta, \varphi)$  be a polarized abelian variety of primitive type  $(K, \Phi)$  with CM by an order in  $K$ . Let  $k_0$  be the field of moduli of  $(A, \varphi)$ . Then  $k_0 \cdot K^r$  contains the unramified class field over  $K^r$  corresponding to the ideal group  $I_0(\Phi^r)$  of (2.1).*

*Proof* In the case of CM by the maximal order  $\mathcal{O}_K$ , this is [19, Main Theorem 1 in §15.3], which in fact gives equality of the fields. In general, this follows from [19, Main Theorem 3 in §17.3].  $\square$

**Corollary 5.4** *Let  $(K, \Phi)$  be a primitive CM type and let  $C$  be a curve over  $\mathbb{C}$  with CM of type  $(K, \Phi)$  by an order in  $K$ . If  $C$  has a model over  $K^r$ , then the quotient  $I_{K^r}/I_0(\Phi^r)$  is trivial.*

*Proof* If  $C$  has a model over  $K^r$  then the field of moduli of the Jacobian  $J(C)$  is contained in  $K^r$ . Hence by Theorem 5.3, we have  $I_0(\Phi^r) = I_{K^r}$ .  $\square$

**Remark 5.5** In the case of CM by the maximal order, the converse to Corollary 5.4 is true as well and follows from Milne [39, 40]. See also Bouyer–Streng [9, Theorem 5.3].

*Proof of Proposition 5.1* If  $J(C)_{\mathbb{C}}$  is simple or  $\text{End}(J(C)_{\mathbb{C}}) \cong \mathcal{O}$ , then the CM type is primitive by Theorem 5.2. In particular, the result follows from Corollary 5.4.  $\square$

We now prove the following consequences of the main theorems.

**Theorem 5.6** *There exist exactly 21 curves  $C/\mathbb{Q}$  of genus 2 up to  $\bar{\mathbb{Q}}$ -isomorphism such that  $\text{End}(J(C)_{\bar{\mathbb{Q}}})$  is an order in a quartic number field. The fields and 19 of the curves are those given in van Wamelen [8]. The other two curves are  $y^2 = x^6 - 4x^5 + 10x^3 - 6x - 1$  and  $y^2 = 4x^5 + 40x^4 - 40x^3 + 20x^2 + 20x + 3$ , which are given in Theorem 14 of Bisson–Streng [10].*

*Proof* For such a curve  $C$ , let  $\mathcal{O} = \text{End}(J(C)_{\overline{\mathbb{Q}}})$  and  $K = \mathcal{O} \otimes \mathbb{Q}$ . Then  $K$  is a CM field by [20, Theorem 1.1.3] and is PQ1 by Proposition 5.1. Moreover, Proposition 5.17 in Shimura [41] shows that  $K/\mathbb{Q}$  is Galois, so it is cyclic and hence Theorem 4.7 gives all possibilities for  $K$ .

Bouyer–Streng [9] prove that the 19 curves in [8] are exactly the curves with  $\mathcal{O} = \mathcal{O}_K$  for these fields  $K$  and Bisson–Streng [10] prove that the two curves in the statement are exactly the curves with  $\mathcal{O} \subsetneq \mathcal{O}_K$  that can be defined over  $\mathbb{Q}$ . □

**Theorem 5.7** *There are exactly 231 curves of genus 2 over  $\overline{\mathbb{Q}}$  up to isomorphism, such that  $\text{End}(J(C)_{\overline{\mathbb{Q}}})$  is the ring of integers of a quartic CM field  $K$  and  $C$  has field of moduli contained in the reflex field. The corresponding CM fields  $K$  are those of Tables 3 and 4, and the curves are those of [9, Tables 1a, 1b, 2b, and 2c].*

**Theorem 5.8** *There are exactly 301 curves of genus 2 over  $\overline{\mathbb{Q}}$  up to isomorphism, such that  $\text{End}(J(C)_{\overline{\mathbb{Q}}})$  is an order in a quartic CM field  $K$  and  $C$  has field of moduli contained in the reflex field. The corresponding CM fields  $K$  are those of Tables 3 and 4.*

*Proof of Theorems 5.7 and 5.8* By Proposition 5.1, the CM field  $K$  is PQ1. Theorems 3.26 and 4.7 give exactly the fields.

The main result of Bouyer–Streng [9] is the complete list of curves with endomorphism ring  $\mathcal{O}_K$  for those fields. There are 19 defined over  $\mathbb{Q}$  in Table 1A, and the rest have a quadratic field of moduli  $K_0^r$ . Of the latter, only one representative of the  $\text{Gal}(K_0^r/\mathbb{Q})$ -orbit of these moduli is given in [9], hence the  $12+58+36 = 106$  entries in Tables 1B, 2B, and 2C of [9] represent  $2 \cdot 106 = 212$  moduli points over  $\mathbb{Q}$ . In total, this gives  $19 + 212 = 231$ , which proves Theorem 5.7.

Now that we know all PQ1 fields we use the methods of Bisson–Streng [10, Theorem 4] to find all non-maximal orders of CM class number one and their principally polarized lattices. We made the SageMath script for this calculation available online at [35]. It yields 70 isomorphism classes of lattices, each corresponding to an isomorphism class of curves (including the two listed in Theorem 5.6). Together with the 231 curves in Theorem 5.7, this gives 301 curves, which proves Theorem 5.8. □

*Remark 5.9* Of the 301 curves of Theorem 5.8, exactly 68 do not appear in Theorems 5.6 and 5.7. These curves have CM by non-maximal orders.

We computed numerical approximations of the values of the Igusa invariants of the curves and rounded them to conjecturally correct values in  $K_0^r$ . Models of the curves can be computed from the Igusa invariants using the methods of [9, 42, 43]. The Igusa invariants and some curve models are available at the same link as the calculation.

Proving correctness of these numerical values goes beyond the scope of this article, but might be possible using [44], [10, last page of Sect. 6.1.5], [45]. It is not needed for the proof of Theorem 5.8

**Acknowledgements**

This paper is based on Chapter 2 of the PhD thesis of the first author, completed at Universiteit Leiden and Université de Bordeaux, and supervised by Andreas Enge, Peter Stevenhagen, and the second author. The authors wish to thank Maarten Derickx and Florian Hess for the helpful discussions and the anonymous referee for various helpful suggestions.

**Data availability** Various computations referred to in the paper were implemented by the authors in SageMath. The corresponding scripts are publicly available at <https://bitbucket.org/pkilocer/cm-class-number-one-genus-2>.

#### Author details

<sup>1</sup>Bernoulli Institute for Mathematics, Computer Science and Artificial Intelligence, University of Groningen, Nijenborgh 9, 9747 AG Goningen, The Netherlands, <sup>2</sup>Mathematical Institute, Leiden University, 9512, Leiden 2300 RA, The Netherlands.

Received: 8 April 2022 Accepted: 18 November 2022

Published online: 17 January 2023

#### References

- Heegner, K.: Diophantische analysis und Modulfunktionen. *Math. Z.* **56**, 227–253 (1952)
- Baker, A.: Linear forms in the logarithms of algebraic numbers. I. *Mathematika* **13**, 204–216 (1966)
- Stark, H.M.: A complete determination of the complex quadratic fields of class-number one. *Mich. Math. J.* **14**, 1–27 (1967)
- Uchida, K.: Imaginary abelian number fields with class number one. *Tohoku Math. J.* **2**(24), 487–499 (1972). <https://doi.org/10.2748/tmj/1178241490>
- Setzer, B.: The determination of all imaginary, quartic, abelian number fields with class number 1. *Math. Comput.* **35**(152), 1383–1386 (1980). <https://doi.org/10.2307/2006404>
- Louboutin, S., Okazaki, R.: Determination of all non-normal quartic CM-fields and of all non-abelian normal octic CM-fields with class number one. *Acta Arith.* **67**(1), 47–62 (1994). <https://doi.org/10.4064/aa-67-1-47-62>
- Murabayashi, N., Umegaki, A.: Determination of all  $\mathbb{Q}$ -rational CM-points in the moduli space of principally polarized abelian surfaces. *Sūrikaiseikikenkyūsho Kōkyūroku* **1160**, 169–176 (2000)
- van Wamelen, P.: Examples of genus two CM curves defined over the rationals. *Math. Comput.* **68**(225), 307–320 (1999). <https://doi.org/10.1090/S0025-5718-99-01020-0>
- Bouyer, F., Streng, M.: Examples of CM curves of genus two defined over the reflex field. *LMS J. Comput. Math.* **18**(1), 507–538 (2015). <https://doi.org/10.1112/S1461157015000121>. [arXiv:1307.0486](https://arxiv.org/abs/1307.0486)
- Bisson, G., Streng, M.: On polarised class groups of orders in quartic CM-fields. *Math. Res. Lett.* **24**(2), 247–270 (2017). [arXiv:1302.3756](https://arxiv.org/abs/1302.3756)
- Gélin, A., Howe, E.W., Ritzenthaler, C.: Principally polarized squares of elliptic curves with field of moduli equal to  $\mathbb{Q}$ . In: *Proceedings of the Thirteenth Algorithmic Number Theory Symposium*. Open Book Ser., vol. **2**, pp. 257–274. Math. Sci. Publ., Berkeley (2019)
- Narbonne, F.: Polarized products of elliptic curves with complex multiplication and field of moduli  $\mathbb{Q}$ . preprint, [arXiv:2203.11982](https://arxiv.org/abs/2203.11982) (2022)
- Louboutin, S.: Explicit lower bounds for residues at  $s = 1$  of Dedekind zeta functions and relative class numbers of CM-fields. *Trans. Am. Math. Soc.* **355**(8), 3079–3098 (2003). <https://doi.org/10.1090/S0002-9947-03-03313-0>
- Murabayashi, N.: The field of moduli of abelian surfaces with complex multiplication. *J. Reine Angew. Math.* **470**, 1–26 (1996). <https://doi.org/10.1515/crll.1996.470.1>
- Park, Y.-H., Kwon, S.-H.: Determination of all non-quadratic imaginary cyclic number fields of 2-power degree with relative class number  $\leq 20$ . *Acta Arith.* **83**(3), 211–223 (1998). <https://doi.org/10.4064/aa-83-3-211-223>
- Kılıçer, P.: The CM class number one problem for curves. PhD thesis, Université de Bordeaux and Leiden University (2016). <https://openaccess.leidenuniv.nl/handle/1887/41145>
- Kılıçer, P., Labrande, H., Lercier, R., Ritzenthaler, C., Sijtsing, J., Streng, M.: Plane quartics over  $\mathbb{Q}$  with complex multiplication. *Acta Arith.* **185**(2), 127–156 (2018). <https://doi.org/10.4064/aa170227-16-3>
- Somoza, A.: Inverse jacobian and related topics for certain superelliptic curves. PhD thesis, UPC Barcelona and Leiden University (2019). <https://scholarlypublications.universiteitleiden.nl/handle/1887/70564>
- Shimura, G., Taniyama, Y.: Complex Multiplication of Abelian Varieties and Its Applications to Number Theory. *Publications of the Mathematical Society of Japan*, vol. **6**, p. 159. The Mathematical Society of Japan, Tokyo (1961)
- Lang, S.: Complex Multiplication. *Grundlehren der Mathematischen Wissenschaften*, vol. 255, p. 184. Springer, New York (1983). <https://doi.org/10.1007/978-1-4612-5485-0>
- Louboutin, S.: On the class number one problem for nonnormal quartic CM-fields. *Tohoku Math. J.* **46**(1), 1–12 (1994). <https://doi.org/10.2748/tmj/1178225798>
- Shimura, G.: On abelian varieties with complex multiplication. *Proc. Lond. Math. Soc.* **34**(1), 65–86 (1977)
- Streng, M.: Complex multiplication on abelian surfaces. PhD thesis, Leiden University (2010). <https://openaccess.leidenuniv.nl/handle/1887/15572>
- Uchida, K.: Relative class numbers of normal CM-fields. *Tohoku Math. J.* **2**(25), 347–353 (1973). <https://doi.org/10.2748/tmj/1178241335>
- Washington, L.C.: *Introduction to Cyclotomic Fields* Graduate Texts in Mathematics, vol. 83, p. 389. Springer, New York (1982). <https://doi.org/10.1007/978-1-4684-0133-2>
- Techebichef, M.: Mémoire sur les nombres premiers. *J. Mathématiques Pures et Appliquées*, 366–390 (1852)
- Goren, E.Z., Lauter, K.E.: Genus 2 curves with complex multiplication. *Int. Math. Res. Not. IMRN* **5**, 1068–1142 (2012)
- Cohen, H.: *Advanced Topics in Computational Number Theory*. Graduate Texts in Mathematics, vol. 193, p. 578. Springer, New York (2000). <https://doi.org/10.1007/978-1-4419-8489-0>
- The Sage Developers: SageMath, the Sage Mathematics Software System (Version 9.1). (2020). <http://www.sagemath.org>
- Streng, M.: An explicit version of Shimura’s reciprocity law for Siegel modular functions. preprint, [arXiv:1201.0020](https://arxiv.org/abs/1201.0020) (2012)
- Streng, M.: RECIPI—REpository of Complex multiPlication sage code. <https://bitbucket.org/mstreng/recip> (2014)

32. Bach, E.: Explicit bounds for primality testing and related problems. *Math. Comput.* **55**(191), 355–380 (1990). <https://doi.org/10.2307/2008811>
33. Kohel, D., et al.: ECHIDNA algorithms for algebra and geometry experimentation. <https://www.i2m.univ-amu.fr/perso/david.kohel/dbs/index.html>
34. PARI: PARI/GP Computer Algebra System (Version 2.11.2). (2020)
35. Kiliçer, P., Streng, M.: CM class number one (genus 2). SageMath code, <https://bitbucket.org/pkiler/cm-class-number-one-genus-2>
36. Louboutin, S.: CM-fields with cyclic ideal class groups of 2-power orders. *J. Number Theory* **67**(1), 1–10 (1997). <https://doi.org/10.1006/jnth.1997.2179>
37. Neukirch, J.: Algebraic Number Theory. Grundlehren der Mathematischen Wissenschaften, vol. 322, p. 571. Springer, New York (1999). <https://doi.org/10.1007/978-3-662-03983-0>. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. <https://doi.org/10.1007/978-3-662-03983-0>
38. Milne, J.S.: Jacobian varieties. In: *Arithmetic Geometry* (Storrs, Conn., 1984), pp. 167–212. Springer, New York (1986)
39. Milne, J.S.: Abelian varieties defined over their fields of moduli. I. *Bull. Lond. Math. Soc.* **4**, 370–372 (1972)
40. Milne, J.S.: Correction: “Abelian varieties defined over their fields of moduli. I”. *Bull. Lond. Math. Soc.* **6**, 145–146 (1974)
41. Shimura, G.: Introduction to the Arithmetic Theory of Automorphic Functions. Publications of the Mathematical Society of Japan, vol. 11, p. 271. Princeton University Press, Princeton (1994). Reprint of the 1971 original, Kanô Memorial Lectures, 1
42. Mestre, J.-F.: Construction de courbes de genre 2 à partir de leurs modules. In: *Effective Methods in Algebraic Geometry* (Castiglione, 1990). *Progr. Math.*, vol. 94, pp. 313–334. Birkhäuser Boston, Boston (1991)
43. Bouyer, F., Streng, M.: Reduction of binary forms. SageMath code, <https://bitbucket.org/mstreng/reduce/src/master/>
44. Lauter, K., Viray, B.: An arithmetic intersection formula for denominators of Igusa class polynomials. *Am. J. Math.* **137**(2), 497–533 (2015). <https://doi.org/10.1353/ajm.2015.0010>
45. Costa, E., Mascot, N., Sijsling, J., Voight, J.: Rigorous computation of the endomorphism ring of a Jacobian. *Math. Comput.* **88**(317), 1303–1339 (2019). <https://doi.org/10.1090/mcom/3373>

## Publisher’s Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.