Inverse Jacobian and related topics for certain superelliptic curves

Somoza Henares, A.

CM cyclic plane quintic curves defined over $\mathbb{Q}$

4

In this chapter we give a complete list of CM-fields whose ring of integers occurs as the endomorphism ring over $\mathbb{C}$ of the Jacobian of a CPQ curve defined over $\mathbb{Q}$ with complex multiplication (CM). We do so by extending the methods for genus 2 and 3 due to Kılıçer [12], see also [15].

In Section 4.1 we define what a polarized abelian variety (or a curve) with complex multiplication is as a particular case of the polarized abelian varieties with m-CM-type that we defined in Chapter 3.

In Section 4.2 we define what the CM class number of a CM-field is, and its relation with the field of moduli of the polarized abelian variety. We also show as a direct consequence of Theorem 4.3.1 in Kılıçer [12] that the list of heuristic models of maximal CM Picard curves over $\mathbb{Q}$ in Section 1.5 is complete.

Finally, in Section 4.3 we focus on the case of CPQ curves, and prove that the fields appearing in the list in Section 2.3 are the only possible CM-fields by which a CPQ curve defined over $\mathbb{Q}$ can have maximal CM over $\mathbb{C}$.

4.1 CM-types

Let K be a CM-field. Throughout this chapter we refer to 1-CM-types as just *CM-types*, that is, sets $\Phi \subseteq \mathrm{Hom}(K, \mathbb{C})$ such that for every complex conjugate pair of homomorphisms $\phi, \overline{\phi}$, exactly one belongs to Φ. For details, see Shimura [42, Chapter II].

Definition 4.1.1. Let k be a proper CM-subfield of K with CM-type Φ_k. The CM-type of K *induced by* Φ_k is

$$\Phi = \{\phi \in \mathrm{Hom}(K, \mathbb{C}) : \phi|_k \in \Phi_k\}.$$

A CM-type Φ of K is *primitive* if it is not induced by any CM-type of any proper CM-subfield.

Definition 4.1.2. The *reflex field* K^r of a CM-type (K, Φ) is

$$K^r = \mathbb{Q}\left(\left\{\sum_{\phi\in\Phi} \phi(x) : x \in K\right\}\right) \subseteq \mathbb{C}.$$

Let now L be the normal closure of the extension $K/\mathbb{Q}$ and let Φ_0 be the CM-type of L induced by Φ. If we take $N \subseteq \mathbb{C}$ the unique subfield of $\mathbb{C}$ isomorphic to L, then we can see the elements in Φ_0 as homomorphisms (hence isomorphisms) from L to N. In this setting we define the *reflex CM-type*.

Definition 4.1.3. The *reflex CM-type* Φ^r of a CM-type (K, Φ) is

$$\Phi^r = \{\phi^{-1}|_{K^r} : \phi \in \Phi_0\}.$$

The CM-type (K^r, Φ^r) is called the *reflex* of (K, Φ).

Lemma 4.1.4 (Shimura, see [42, pg. 63])**.** Let (K, Φ) be a primitive CM-type. Then the reflex type of its reflex type (K^r, Φ^r) coincides with (K, Φ).

Definition 4.1.5. The *type norm* of a CM-type (K, Φ) is the multiplicative map

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

In this context, following Definition 3.1.1 we obtain that a *polarized abelian variety with complex multiplication* (CM) by (K, Φ) is a triple (X, λ, ι) where:

- ▷ X is an abelian variety over $\mathbb{C}$ of dimension g,
- ▷ λ is a polarization of X, and
- ▷ ι is a ring homomorphism $\iota : K \hookrightarrow \mathrm{End}(X) \otimes \mathbb{Q}$ such that:
  - the analytic representation $\rho_a \circ \iota$ is equivalent to the representation $\rho_\Phi = \mathrm{diag}(\phi_1, \ldots, \phi_g)$, and
  - the Rosati involution on $\mathrm{End}(X) \otimes \mathbb{Q}$ with respect to the polarization λ extends the complex conjugation on K via ι.

We say that it has *CM by an order* $\mathcal{O} \subseteq K$ if $\iota^{-1}(\mathrm{End}(X)) = \mathcal{O}$.

Lemma 4.1.6 (Theorem 1.3.5 in Lang [19])**.** A polarized abelian variety with CM-type (K, Φ) is absolutely simple if and only if Φ is primitive. □

In Sections 1.5 and 2.3 we defined a maximal CM Picard curve (respectively CPQ curve) to be a Picard curve (resp. CPQ curve) such that its Jacobian has endomorphism ring isomorphic to the maximal order of some sextic field K

(resp. a degree-12 field). The following result shows that then its Jacobian is a principally polarized abelian varieties with complex multiplication.

Proposition 4.1.7. If C is a maximal CM Picard curve (respectively CPQ curve), then there exist a primitive CM-type (K, Φ) and an embedding $\iota : K \to \mathrm{End}(J(C)) \otimes \mathbb{Q}$ such that $(J(C), \lambda_C, \iota)$ is a principally polarized abelian variety with CM by $\mathcal{O}_K$.

Proof. Assume C is a maximal CM Picard (respectively CPQ) curve. Then there exists a sextic (resp. degree-12) field K that satisfies $\mathrm{End}(J(C)) \cong \mathcal{O}_K$. In particular, the field K contains a primitive third root of unity $\zeta_3 \in K$ (resp. a primitive fifth root of unity $\zeta_5 \in K$), which corresponds via the isomorphism to the automorphism ρ_*.

We define $\iota : K \to \mathrm{End}(J(C) \otimes \mathbb{Q}$ to be the extension of the ring isomorphism $\mathcal{O}_K \to \mathrm{End}(J(C))$ and Φ to be a CM-type such that $\rho_a \circ \iota$ is equivalent to ρ_Φ.

As $J(C)$ is absolutely simple, by Lemma 4.1.6, the CM-type Φ is primitive. Moreover, the field K is a CM-field and the Rosati involution on $\mathrm{End}(J(C)) \otimes \mathbb{Q}$ with respect to λ_C extends the complex conjugation on K via ι, see for example Lemma 1.3.5.4 in Chai-Conrad-Oort [4]. □

In the case of (1-)CM-types, the moduli space $\mathcal{H}_{\mathbf{r},\mathbf{s}}$ contains only one point, thus one can find the corresponding period matrix following the construction due to Shimura that we gave in Section 3.2. For example, given a CM-type (K, Φ), Van Wamelen's method lists all pairs $(\mathcal{M}, T) \in \Upsilon(\Phi)$ as defined in Section 3.1 and then computes all the period matrices of principally polarized abelian varieties with complex multiplication by $\mathcal{O}_K$ following the construction in Section 3.2, see [51] for details.

If we apply Van Wamelen's method to a primitive CM-type (K, Φ) where K is a sextic CM-field containing a primitive third root of unity $\zeta_3 \in K$, then we obtain a list of period matrices corresponding to principally polarized abelian threefolds with CM by $\mathcal{O}_K$ with a order-3 automorphism $\iota(\zeta_3)$. Hence by Proposition 1.4.1 they correspond to Jacobians of Picard curves. Obtaining the rational representation of $\iota(\zeta_3)$ with Van Wamelen's is then a matter of keeping track of the changes of basis throughout the algorithm.

4.2 The CM class number

In this section we introduce the concept of the *field of moduli* of a polarized abelian variety, which is closely related to the field of definition, and we see how it relates to the CM-field in the case of polarized abelian varieties with CM.

Theorem 4.2.1 (Shimura, see [41, pp. 130–131])**.** Let (X, λ) be a polarized abelian variety over $\mathbb{C}$, let K be a number field and let $\iota : \mathcal{O}_K \to \mathrm{End}(X)$ be an embedding. There exists a unique field $k \subseteq \mathbb{C}$ such that for every $\sigma \in \mathrm{Aut}(\mathbb{C})$, the restriction of σ to k is the identity if and only if there exists an isomorphism $f : X \to {}^{\sigma}X$ that satisfies $f^{\vee} \circ {}^{\sigma}\lambda \circ f = \lambda$ and $f \circ \iota(a) = {}^{\sigma}\iota(a) \circ f$ for all $a \in \mathcal{O}_K$. □

The field k in Theorem 4.2.1 is called the *field of moduli* of (X, λ, ι).

In particular, if a polarized abelian variety (X, λ, ι) is defined over $\mathbb{Q}$, then its field of moduli is $\mathbb{Q}$. The following results give conditions on the field of moduli for polarized abelian varieties with CM.

Proposition 4.2.2 (Shimura [41, Proposition 5.17])**.** Let (K, Φ) and (K^r, Φ^r) be respectively a primitive CM-type and its reflex. Let (X, λ, ι) be a polarized abelian variety of CM-type (K, Φ). Let F be a subfield of K, $\iota|_F$ be the restriction of λ to F and M_F be the field of moduli of $(X, \lambda, \iota|_F)$. Then the following assertions hold:

(1) the field $M_F K^r$ is the field of moduli of (X, λ, ι),
(2) the reflex field K^r is normal over $M_F \cap K^r$,
(3) the field $M_F K^r$ is normal over M_F, and
(4) the group $\mathrm{Gal}(M_F K^r / M_F)$ is isomorphic to a subgroup of $\mathrm{Aut}(K/F)$.

Theorem 4.2.3 (Shimura-Taniyama [43, Main theorem 1])**.** Let (K, Φ) be a primitive CM-type and let (K^r, Φ^r) be its reflex CM-type. Let (X, λ, ι) be a polarized abelian variety of type (K, Φ) with CM by $\mathcal{O}_K$, and let M be the field of moduli of $(X, \lambda, \iota|_{\mathbb{Q}})$. Then MK^r is the unramified class field over K^r corresponding to the ideal group

$$I_0(\Phi^r) := \{\mathfrak{b} \in I_{K^r} : \exists \alpha \in K^{\times} \text{ such that } N_{\Phi^r}(\mathfrak{b}) = (\alpha),\ N_{K/\mathbb{Q}}(\mathfrak{b}) = \alpha\overline{\alpha}\}. \quad \square$$

Observe that if M is a subfield of K^r, then $I_{K^r}/I_0(\Phi^r)$ is trivial. In this context, the quotient $I_{K^r}/I_0(\Phi^r)$ is called the *CM class group* of (K, Φ) and when it is trivial we say that K has *CM class number one*.

Proposition 4.2.4. Let (X, λ) be an absolutely simple polarized abelian variety defined over $\mathbb{Q}$ with CM by $\mathcal{O}_K$. Then K has CM class number one and is normal over $\mathbb{Q}$.

Proof. Since (X, λ) is defined over $\mathbb{Q}$ we have $M_{\mathbb{Q}} = \mathbb{Q}$, by Proposition 4.2.2.(2), the field K^r is normal over $\mathbb{Q}$. We also have that, by Proposition 4.2.2.(4), the group $\mathrm{Gal}(K^r/\mathbb{Q})$ is isomorphic to a subgroup of $\mathrm{Aut}(K/\mathbb{Q})$, hence we obtain

$$[K^r : \mathbb{Q}] = \#\,\mathrm{Gal}(K^r/\mathbb{Q}) \leq \#\,\mathrm{Aut}(K/\mathbb{Q}) = [K : \mathbb{Q}].$$

By Lemma 4.1.6, since X is absolutely simple we have that its CM-type Φ is primitive, so by Lemma 4.1.4 we get $K^{rr} = K$, and since K^r is normal we

	$p(x)$	h_K	h_K^*
(1)	$x^3 - 3x - 1$	1	1
(2)	$x^3 - x^2 - 2x + 1$	1	1
(3)	$x^3 - x^2 - 4x - 1$	1	1
(4)	$x^3 + x^2 - 10x - 8$	1	1
(5)	$x^3 - x^2 - 14x - 8$	1	1
(6)	$x^3 - 21x - 28$	3	1
(7)	$x^3 - 21x + 35$	3	1
(8)	$x^3 - 39x + 26$	3	1
(13)	$x^3 - 61x - 183$	4	4
(14)	$x^3 - x^2 - 22x - 5$	4	4

Table 4.1: List of CM class number one sextic CM-fields K containing a primitive third root of unity $\zeta_3 \in K$. We write $K = K_0(\zeta_3)$ for K_0 the splitting field of $p(x)$, and indicate the class number h_K of K and its relative class number $h_K^* := h_K/h_{K_0}$. The number in the first column indicates which curves in Section 1.5 are heuristic models for the Picard curves with maximal CM by K.

obtain that K^{rr} is isomorphic to a subfield of K^r. Altogether it gives us that K is isomorphic to K^r and therefore K is normal over $\mathbb{Q}$.

Lastly, by Proposition 4.2.2.(1) we have that the field of moduli of (X, λ, ι) is K^r, so it follows that K has CM class number one. □

Proposition 4.2.4 characterizes the CM-fields whose maximal order may occur as the endomorphism ring of a polarized abelian variety with CM.

Kılıçer studies in [12] the CM class number one fields that correspond to principally polarized abelian varieties of dimension 2 and 3. In particular, Table 3.1 in [12] includes a complete list of CM-fields whose ring of integers is the endomorphism ring of the Jacobian of a Picard curve.

Corollary 4.2.5 (See also Theorem 4.3.1 in Kılıçer [12])**.** Let C be a Picard curve defined over $\mathbb{Q}$ with CM by $\mathcal{O}_K$ for a sextic CM-field K. The field K is isomorphic to $K_0(\zeta_3)$, where ζ_3 is a primitive third root of unity and K_0 is the splitting field of a polynomial $p(x)$ from Table 4.1.

Proof. Let C be a Picard curve with CM by the ring of integers of a sextic CM-field K. Recall that C has an automorphism given by $\rho(x, y) = (x, z_3 y)$ that induces an automorphism ρ_* in the Jacobian. It follows that the field K contains a primitive third root of unity, and thus $k = \mathbb{Q}(\zeta_3)$ is a quadratic CM-subfield

whose discriminant has absolute value 3. The list in Table 4.1 contains all CM class number one cyclic sextic CM-fields of Table 3.1 in [12] with $d_k = 3$. □

It follows that the list in Section 1.5 contains heuristic models for all Picard curves with maximal CM that have a model over $\mathbb{Q}$. In the cases (13) and (14) we also list heuristic models defined over K_0 for three other Picard curves, which by Theorem 4.3.1 in Kılıçer [12] exist and have field of moduli K_0.

Remark 4.2.6. Park and Kwon [34, Table 3] give a complete list of all imaginary abelian sextic number fields K with class number $h_K \leq 11$. In particular, those with an imaginary quadratic subfield of conductor 3 contain a third root of unity, and thus occur as CM-fields of Picard curves.

Table 3 in [34] includes four fields with CM class number bigger than 1, for which we also applied Van Wamelen's method and obtained heuristic models for the corresponding Picard curves with maximal CM, see cases (9)–(12) in Section 1.5.

4.3 CM class number one fields for CPQ curves

The goal for this section is to give a result analogous to Corollary 4.2.5 in the case of CPQ curves, that is, we want to find all fields whose maximal order may occur as the endomorphism ring over $\mathbb{C}$ of the Jacobian of a CPQ curve with CM and defined over $\mathbb{Q}$.

By Proposition 4.2.4 we only need to look for CM class number one CM-fields that are Galois over $\mathbb{Q}$. We will prove the following result.

Theorem 4.3.1. Let C be a CPQ curve defined over $\mathbb{Q}$ with CM by the ring of integers of a degree-12 CM-field K. Then the field K is isomorphic to $K_0(\zeta_5)$, where ζ_5 is a primitive fifth root of unity and K_0 is the splitting field of a polynomial $p(x)$ from Table 4.2.

We start by listing the possible Galois groups of degree-12 Galois number fields containing a primitive fifth root of unity. Then we give a sufficient condition for such a field to have CM class number one and finally we study the necessary conditions for that to happen for each occurring Galois group.

Proposition 4.3.2. Let n be a positive integer, and consider the group given by the presentation

$$Q_{4n} = \langle s, t : s^{2n} = 1, s^n = t^2, sts = t \rangle.$$

The group Q_{4n} has order $4n$.

Proof. See pp. 347–348 in [36]. □

	$p(x)$	h_K	h_K^*
(1)	$x^3 - x^2 - 2x + 1$	1	1
(2)	$x^3 - 3x - 1$	1	1
(3)	$x^3 - x^2 - 4x - 1$	4	4
(4)	$x^3 - 12x - 14$	4	4

Table 4.2: List of CM class number one CM-fields K of degree 12 containing a primitive fifth root of unity $\zeta_5 \in K$. We write $K = F(\zeta_5)$ for F the splitting field of $p(x)$, and indicate the class number h_K of K and its relative class number $h_K^* := h_K/h_{K^+}$. The number in the first column indicates which curve in Section 2.3 is an heuristic model for the CPQ curve defined over $\mathbb{Q}$ with maximal CM by K over $\mathbb{C}$.

A group isomorphic to Q_{4n} as defined in Proposition 4.3.2 is called a *dicyclic group of order* $4n$.

Definition 4.3.3. Let N and H be two groups, and let $\varphi : H \to \mathrm{Aut}(N)$ be a group homomorphism. *The semidirect product* $N \rtimes H$ *of* N *and* H *with respect to* φ is the Cartesian product $N \times H$ together with the operation

$$(n, h)(n', h') = (n\varphi(h)(n'), hh').$$

Proposition 4.3.4. If K is a degree-12 Galois number field containing a quartic cyclic number field k, then the Galois group of K is a cyclic or dicyclic group of order 12.

Proof. Let $G = \mathrm{Gal}(K/\mathbb{Q})$, and let $H = \mathrm{Gal}(K/k)$, which has order 3. We have

$$G/H \simeq \mathrm{Gal}(k/\mathbb{Q}) = C_4,$$

and by the Schur-Zassenhaus theorem, we obtain

$$G = H \rtimes G/H \simeq C_3 \rtimes C_4.$$

Let g and h be generators of C_3 and C_4 respectively. Since C_3 has two possible automorphisms, the trivial one and the one given by $g \mapsto g^2$, the group homomorphisms in $\mathrm{Hom}(C_4, \mathrm{Aut}(C_3))$ are

$$\begin{aligned} \varphi_1 : C_4 &\to \mathrm{Aut}(C_3) \\ h &\mapsto (g \mapsto g), \end{aligned} \qquad \text{and} \qquad \begin{aligned} \varphi_2 : C_4 &\to \mathrm{Aut}(C_3) \\ h &\mapsto (g \mapsto g^2). \end{aligned}$$

We obtain that the semidirect product of C_4 and C_3 with respect to φ_1 is actually the direct product, and thus a cyclic group of order 12.

Consider now the semidirect product of C_4 and C_3 with respect to φ_2. Let $s = (g, h^2) \in C_3 \times C_4$ and $t = (1, h) \in C_3 \times C_4$. Note that $s^2 = (g^2, 1)$ has order 3 and t has order 4. Moreover they satisfy

$$s^3 = (g, h^2)(g, h^2)(g, h^2) = (g^2, 1)(g, h^2) = (1, h^2) = (1, h)(1, h) = t^2,$$

thus we obtain $s^6 = t^4 = 1$; and also

$$sts = (g, h^2)(1, h)(g, h^2) = (g, h^3)(g, h^2) = (1, h) = t.$$

We conclude that the semidirect product of C_4 and C_3 with respect to φ_2 is a dicyclic group of order 12. □

As we proved in Proposition 3.3.1, the Jacobians of CPQ curves have 3-CM-type $\mathfrak{Z} = (\mathbb{Q}(\zeta_5), (\phi_1, \phi_2), (3, 2), (0, 1))$, where $\phi_k : K \to \mathbb{C}$ maps ζ_5 to $z_5^k = \exp(2\pi ik/5)$. This has to be taken into account when considering possible CM-types for the Jacobian of a CPQ curve, since it introduces some restrictions.

Definition 4.3.5. Let k be a proper CM-subfield of a CM-field K. We say that a CM-type (K, Φ) *restricts to* an m-CM-type (k, Ψ) if the fields satisfy $m = [K : k]$ and for every $\psi \in \mathrm{Hom}(k, \mathbb{C})$ we have

$$\mathrm{mult}_\Psi(\psi) = \#\{\phi \in \Phi : \phi|_k = \psi\}.$$

Definition 4.3.6. We say that a CM-type (K, Φ) is *CPQ-compatible* if K is a degree-12 CM-field containing a primitive fifth root of unity $\zeta_5 \in K$ such that Φ restricts to the m-CM-type $\mathfrak{Z}$ on the subfield $\mathbb{Q}(\zeta_5) \subseteq K$.

Corollary 4.3.7. If K Galois over $\mathbb{Q}$ and (K, Φ) is a CPQ-compatible CM-type, then the CM-type Φ is primitive.

Proof. If (K, Φ) is a CPQ-compatible CM-type, then K contains a fifth root of unity $\zeta_5 \in K$. It follows that the subfield $k = \mathbb{Q}(\zeta_5) \subseteq K$ is a cyclic quartic number field and since by assumption K is Galois over $\mathbb{Q}$, it follows that it is cyclic or dicyclic. In particular, in either case the only proper CM-subfield of K is $k = \mathbb{Q}(\zeta_5)$, see Figures 4.1 and 4.2. If Φ was induced, its restriction to k without multiplicity would be a CM-type of k. However, since (K, Φ) is CPQ-compatible, the restriction of Φ to k is the 3-CM-type $\mathfrak{Z}$, which is not a CM-type when considered without multiplicity. □

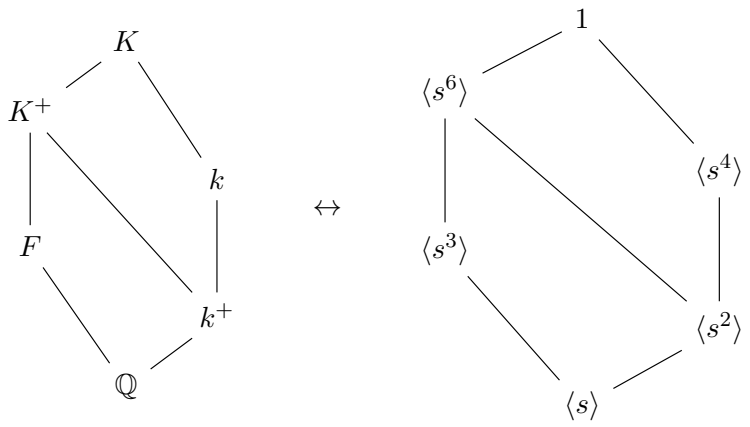


Figure 4.1: Lattices of subfields and subgroups for a cyclic field K of degree 12.

4.3.1 Sufficient condition for CM class number one

Let K be a CM-field with maximal totally real subfield K^+. In this section we give a sufficient condition for a CPQ-compatible CM-type (K, Φ) to have CM class number one. We denote the *class number* of K by h_K and define its *relative class number* $h_K^* := h_K/h_{K^+}$.

We will prove the following result.

Proposition 4.3.8. Let K be a Galois degree-12 CM-field containing a primitive fifth root of unity $\zeta_5 \in K$, let K^+ be its maximal totally real subfield and let Φ be a primitive CM-type. Let t_K be the number of primes in K^+ that ramify in K.

If the relative class number of K is $h_K^* = 2^{t_K-1}$, then K has CM class number one.

To prove this proposition we start with a result by Kılıçer that given a CM-field K with group of roots of unity W_K and *Hasse unit index* $Q_K := [\mathcal{O}_K^\times : W_K\mathcal{O}_{K^+}^\times] = 1$, writes the relative class number h_K^* in terms of t_K and the index $[I_K : I_K^H P_K]$ for $H = \mathrm{Gal}(K/K^+)$. Then we prove that this applies to our case because our CM-fields have $Q_K = 1$, and finally we prove that if we have $I_K = I_K^H P_K$, then the CM-field has CM class number one.

Lemma 4.3.9 (Lemma 2.2.2 in Kılıçer [12])**.** Let K be a CM-field with maximal totally real subfield K^+, and let t_K be the number of primes in K^+ that ramify in K. If the Hasse unit index Q_K of K is one, then we have

$$h_K^* = 2^{t_K-1}[I_K : I_K^H P_K].$$

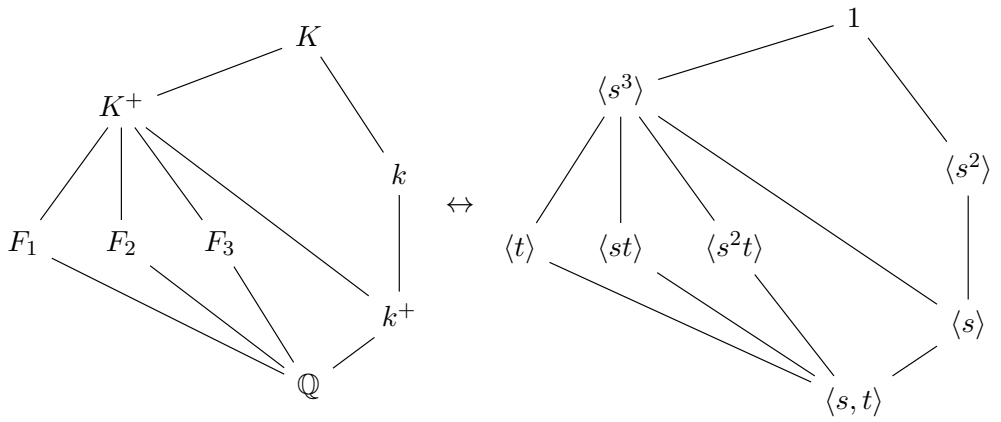


Figure 4.2: Lattices of subfields and subgroups for a dicyclic field K of degree 12.

□

Lemma 4.3.10. Let K be a degree-12 CM-field containing a primitive fifth root of unity $\zeta_5 \in K$, let K^+ be its maximal totally real subfield and let t_K be the number of primes in K^+ that ramify in K. The relative class number of K is

$$h_K^* = 2^{t_K - 1}[I_K : I_K^H P_K].$$

Proof. Louboutin, Okazaki and Olivier [22] state in Theorem 5(i) that two CM-fields $k \subseteq K$ for which $[K : k]$ is odd have the same Hasse unit index.

In the case at hand, we have by assumption $\mathbb{Q}(\zeta_5) \subseteq K$ with $[K : \mathbb{Q}(\zeta_5)] = 3$, and thus we obtain $Q_K = Q_{\mathbb{Q}(\zeta_5)}$. One computes that the Hasse unit index for $\mathbb{Q}(\zeta_5)$ is $Q_{\mathbb{Q}(\zeta_5)} = 1$. Then the result follows from Lemma 4.3.9. □

Proof of Proposition 4.3.8. Since K is Galois over $\mathbb{Q}$ and the CM-type is primitive, we identify the CM-field K with its reflex field K^r via an isomorphism and assume $h_K^* = 2^{t_K - 1}$. By Lemma 4.3.10 we have that $I_K = I_K^H P_K$.

For any $\mathfrak{b} \in I_{K^+}$ we have $N_{\Phi^r}(\mathfrak{b}) = (N_{K^+/\mathbb{Q}}(\mathfrak{b}))$, where $N_{K^+/\mathbb{Q}}(\mathfrak{b}) \in \mathbb{Q}^\times$, hence we obtain the inclusion $I_{K^+} P_K \subseteq I_0(\Phi^r)$. Considering the exact sequence

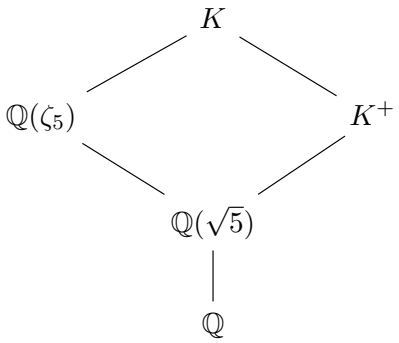
$$1 \to I_{K^+} \to I_K^H \to \bigoplus_{\mathfrak{p} \text{ prime of } K^+} \mathbb{Z}/e_{K/K^+}(\mathfrak{p})\mathbb{Z} \to 1$$

we see that the elements in I_K^H / I_{K^+} are represented by the products of primes in K that are ramified in K/K^+. For any such prime $\mathfrak{P}$, let $\mathfrak{p} = \mathfrak{P} \cap K^+$ and

$p\mathbb{Z} = \mathfrak{P} \cap \mathbb{Q}$. We obtain

$$N_{\Phi^r}(\mathfrak{P})^2 = N_{\Phi^r}(\mathfrak{p}\mathcal{O}_K) = N_{K^+/\mathbb{Q}}(\mathfrak{p})\mathcal{O}_K, \tag{4.1}$$

where $N_{K^+/\mathbb{Q}}(\mathfrak{p}) = p^{f_{K^+/\mathbb{Q}}(\mathfrak{p})}$. We have the subfield lattice



hence the rational prime p over which $\mathfrak{P}$ lies is ramified in $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ (see also Proposition 4.8(ii) in [20, II]), so we conclude that $p = 5$ and by (4.1) we get

$$N_{\Phi^r}(\mathfrak{P}) = \sqrt{N_{K^+/\mathbb{Q}}(\mathfrak{p})\mathcal{O}_K} = (\pi), \text{ where } \pi = \begin{cases} \sqrt{5} & \text{for } f_{K^+/\mathbb{Q}}(\mathfrak{p}) = 1, \\ 5 & \text{for } f_{K^+/\mathbb{Q}}(\mathfrak{p}) = 2, \\ 5\sqrt{5} & \text{for } f_{K^+/\mathbb{Q}}(\mathfrak{p}) = 3, \\ 5^3 & \text{for } f_{K^+/\mathbb{Q}}(\mathfrak{p}) = 6, \end{cases}$$

where indeed in all cases we have $N_{K/\mathbb{Q}}(\mathfrak{P}) = \pi\overline{\pi}$. We conclude

$$I_K = I_K^H P_K \subseteq I_0(\Phi^r)$$

and the statement follows. □

In the following sections we prove the converse result for the different Galois group possibilities.

4.3.2 Cyclic degree-12 CM-fields

Throughout this section, we assume K to be a cyclic degree-12 CM-field containing a primitive fifth root of unity $\zeta_5 \in K$ and denote its maximal totally real subfield by K^+.

We will prove that if K has CM class number one, then its relative class number h_K^* is $2^{t_K - 1}$. To do so we show that there is a unique CPQ-compatible CM-type up to the choice of an isomorphism between K and its reflex field K^r. That way we can use a concrete CM-type to prove that we have $I_K = I_K^H P_K$ using the type norm (see Definition 4.1.5).

Proposition 4.3.11. Let (K, Φ) be a cyclic CPQ-compatible CM-type for a primitive fifth root of unity $\zeta_5 \in K$ and let s be a generator of $\mathrm{Gal}(K/\mathbb{Q})$ that maps ζ_5 to ζ_5^2. There is an embedding $\sigma : K \hookrightarrow \mathbb{C}$ such that if we identify K with its reflex field K^r via σ, then Φ is $\{\mathrm{id}, s, s^3, s^4, s^5, s^8\}$. The reflex CM-type Φ^r is $\{\mathrm{id}, s^4, s^7, s^8, s^9, s^{11}\}$.

Proof. Let s be a generator of $\mathrm{Gal}(K/\mathbb{Q})$ that satisfies $s(\zeta_5) = \zeta_5^2$. The image of ζ_5 by the k-th power of s is $\zeta_5^{2^k}$ and thus it only depends on the class of k modulo 4.

If we consider an embedding $\sigma : K \to \mathbb{C}$ that satisfies $\sigma(\zeta_5) = z_5$, then there is a set $N \subseteq \mathbb{Z}/12\mathbb{Z}$ such that the CM-type consists of embeddings of the form $\sigma \circ s^k$ for $k \in N$. Since Φ restricts to the 3-CM-type $\mathfrak{Z}$, the subset N contains all $k \in \mathbb{Z}/12\mathbb{Z}$ that satisfy $k \equiv 0 \pmod 4$, one that satisfies $k \equiv 3 \pmod 4$ and two that satisfy $k \equiv 1 \pmod 4$.

Moreover, by definition, the CM-type Φ does not contain a complex conjugate pair, so the value $k \in N$ with $k \equiv 3 \pmod 4$ determines the those with $k \equiv 1 \pmod 4$. Therefore there are three possible index sets:

$$N_i = \{0, 4, 8, 3 + 4i, 1 + 4i, 5 + 4i\}, \quad i \in \{0, 1, 2\}.$$

It follows that, if we identify K with its reflex field K^r with the embedding $\sigma \circ s^{-4i}$, then we get Φ as in the statement of the proposition. Finally, since K is normal and Φ is primitive, the reflex CM-type is therefore $\Phi^r = \{\mathrm{id}, s^4, s^7, s^8, s^9, s^{11}\}$. □

Notation 4.3.12. For an arbitrary field F, an ideal $\mathfrak{b} \subseteq F$ and g an automorphism of F, we denote by ${}^g\mathfrak{b}$ the image by g of $\mathfrak{b}$, so we have ${}^{gr}\mathfrak{b} = {}^g({}^r\mathfrak{b})$. We extend this notation to the group ring $\mathbb{Z}[\mathrm{Aut}(F)]$.

Proposition 4.3.13. Let (K, Φ) be a cyclic CPQ-compatible CM-type, let K^+ be the maximal totally real subfield of K and let t_K be the number of primes in K^+ that ramify in K. If K has CM class number one, then the relative class number of K is $h_K^* = 2^{t_K - 1}$.

Proof. Let (K, Φ) be a cyclic CPQ-compatible CM-type. It follows from Lemma 4.3.10 that the relative class number is $h_K^* = 2^{t_K-1}[I_K : I_K^H P_K]$, so we only need to prove $[I_K : I_K^H P_K] = 1$ when K has CM class number one, that is, when we have $I_0(\Phi^r) = I_{K^r}$.

We will start by proving that for any $\mathfrak{b} \in I_K$ the fractional ideal ${}^{1-s^6}\mathfrak{b}$ is principal and generated by an element $\alpha \in K^\times$ that satisfies $\alpha\overline{\alpha} = 1$. Then we will use Hilbert's Theorem 90 to prove that the ideal $\mathfrak{b}$ is in $I_K^H P_K$.

Let $\zeta_5 \in K$ be the primitive fifth root of unity for which the CM-type (K, Φ) is CPQ-compatible, and let $k = \mathbb{Q}(\zeta_5)$. Identify K with its reflex field K^r via

the embedding given in Proposition 4.3.11, so we have $\Phi = \{\mathrm{id}, s, s^3, s^4, s^5, s^8\}$ for s a generator of $\mathrm{Gal}(K/\mathbb{Q})$ that maps ζ_5 to ζ_5^2. For any $\mathfrak{b} \in I_K$ we can check by writing it out that we obtain

$$N_{\Phi^r}({}^{-1+s+s^5-s^6}\mathfrak{b})/N_{K/k}({}^{s-s^3}\mathfrak{b}) = {}^{1-s^6}\mathfrak{b}.$$

By assumption we have $I_0(\Phi^r) = I_{K^r}$, so the ideal $N_{\Phi^r}({}^{-1+s+s^5-s^6}\mathfrak{b})$ is generated by an element $\beta \in K^\times$ with $\beta\overline{\beta} = N_{K/\mathbb{Q}}({}^{-1+s+s^5-s^6}\mathfrak{b}) = 1$.

The ideal $N_{K/k}({}^{s-s^3}\mathfrak{b}) \in I_k$ is also principal, since it is a fractional ideal of the class number one field k. Choose a generator $\gamma \in k^\times$. By cancellation, it satisfies

$$(\gamma\overline{\gamma}) = N_{K/k}({}^{s-s^3}\mathfrak{b})\overline{N_{K/k}({}^{s-s^3}\mathfrak{b})} = (1).$$

But since we have seen that all totally positive units in k^+ are norms of elements of $\mathcal{O}_k^\times$ (see Lemma 3.4.14), we change γ so that it satisfies $\gamma\overline{\gamma} = 1$.

Altogether we have that ${}^{1-s^6}\mathfrak{b}$ is a principal ideal generated by an element $\alpha = (\beta/\gamma)$ such that $\alpha\overline{\alpha} = 1$. It follows from Hilbert's Theorem 90 [10] that there exists an element $\delta \in K^\times$ with $\alpha = \overline{\delta}\delta^{-1}$. In consequence, we obtain $\delta\mathfrak{b} = \overline{\delta\mathfrak{b}} \in I_K^H$ so we write $\mathfrak{b} = \overline{\delta\mathfrak{b}}\left(\frac{1}{\delta}\right) \in I_K^H P_K$ and thus we obtain the equality $I_K = I_K^H P_K$. □

4.3.3 Dicyclic degree-12 CM-fields

In this section we consider the remaining case, that is, we assume that K is a degree-12 CM-field containing a fifth root of unity and whose Galois group is a dicyclic group of order 12. In particular there are elements $s, t \in \mathrm{Gal}(K/\mathbb{Q})$ that satisfy $\mathrm{Gal}(K/\mathbb{Q}) = \langle s, t : s^6 = 1, s^3 = t^2, sts = t\rangle$.

We will prove also in this case that if the field K has relative class number $h_K^* = 2^{t_K - 1}$, then it also has CM class number one.

To do so we follow the same strategy as in Section 4.3.2. First we determine the unique CPQ-compatible CM-type Φ up to the choice of an embedding $\sigma : K \hookrightarrow \mathbb{C}$ and then we use that to prove $I_K = I_K^H P_K$ using the type norm of the reflex type Φ^r.

Lemma 4.3.14. If (K, Φ) is a dicyclic CPQ-compatible CM-type for a primitive fifth root of unity $\zeta_5 \in K$, then there exist generators s and t of $\mathrm{Gal}(K/\mathbb{Q})$ that map ζ_5 to ζ_5^4 and ζ_5^2 respectively, and satisfy the relations $ts = s^5t$, $t^2 = s^3$ and $s^6 = 1$.

Proof. Let $s, t \in \mathrm{Gal}(K/\mathbb{Q})$ satisfy $\mathrm{Gal}(K/\mathbb{Q}) = \langle s, t : s^6 = 1, s^3 = t^2, sts = t\rangle$.

The automorphism s maps ζ_5 to ζ_5^4 because it has order 2 in $\langle s, t\rangle/\langle s^2\rangle$ (see Figure 4.2) and the map given by $\zeta_5 \mapsto \zeta_5^4$ is the only order-2 element in $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$.

Analogously, the automorphism t has order 4 in $\langle s,t\rangle/\langle s^2\rangle$ so, changing t to t^{-1} if necessary, we get that it maps ζ_5 to ζ_5^2. □

Proposition 4.3.15. Let (K,Φ) be a dicyclic CPQ-compatible CM-type for a primitive fifth root of unity $\zeta_5 \in K$ and let s and t be generators of $\mathrm{Gal}(K/\mathbb{Q})$ as in Lemma 4.3.14. Then there is an embedding $\sigma : K \hookrightarrow \mathbb{C}$ such that if we identify K with its reflex field K^r via σ, then Φ is $\{\mathrm{id}, s^2, s^4, t, st, s^2t\}$. Moreover, the reflex CM-type Φ^r is $\{\mathrm{id}, s^2, s^4, s^3t, s^4t, s^5t\}$.

Proof. Let s and t be generators of $\mathrm{Gal}(K/\mathbb{Q})$ as in Lemma 4.3.14. We can write the Galois group of K as

$$\mathrm{Gal}(K/\mathbb{Q}) = \{s^it^j : 0 \le i \le 5, j \in \{0,1\}\}$$

together with the relations $ts = s^5t$, $t^2 = s^3$ and $s^6 = 1$.

If we consider an embedding $\sigma : K \to \mathbb{C}$ that satisfies $\sigma(\zeta_5) = z_5$, then there exists a subset $P \subseteq \mathrm{Gal}(K/\mathbb{Q})$ such that the CM-type consists of embeddings of the form $\sigma \circ s^it^j$ for $s^it^j \in P$. Since Φ restricts to the 3-CM-type $\mathfrak{Z}$, the subset P contains all automorphism that map ζ_5 to itself, one that maps ζ_5 to ζ_5^3 and two that map ζ_5 to ζ_5^2.

Moreover, by definition, the CM-type does not contain a complex conjugate pair, so the automorphism in P mapping ζ_5 to ζ_5^3 determines those mapping ζ_5 to ζ_5^2.

Since the group $\langle s^2\rangle$ fixes $\mathbb{Q}(\zeta_5)$ (see Figure 4.2) we get $\langle s^2\rangle \subseteq P$. Furthermore, the automorphism t maps ζ_5 to ζ_5^2 and s^3 is the complex conjugation in K, hence only one automorphism in the subgroup $\langle s^2\rangle s^3t = \langle s^2\rangle st$ is in P, and it determines the remaining two automorphisms.

Altogether, we obtain that there are 3 possible subsets $P \subseteq \mathrm{Gal}(K/\mathbb{Q})$:

$$P_i = \{\mathrm{id}, s^2, s^4, s^{2i}t, s^{1+2i}t, s^{2+2i}t\}, \quad i \in \{0,1,2\}.$$

It follows that, if we identify K with its reflex field K^r via the embedding $\sigma \circ s^{-2i}$, then we get that Φ is P_0. Lastly, since K is normal and Φ is primitive by Remark 4.3.7, we can compute the reflex CM-type $\Phi^r = \{\mathrm{id}, s^2, s^4, s^3t, s^4t, s^5t\}$. □

Proposition 4.3.16. Let (K,Φ) be a dicyclic CPQ-compatible CM-type, let K^+ be its maximal totally real subfield and let t_K be the number of primes in K^+ that ramify in K. If K has CM class number one, then the relative class number of K is $h_K^* = 2^{t_K-1}$.

Proof. Let (K,Φ) be a dicyclic CPQ-compatible CM-type. It follows from Lemma 4.3.10 that the relative class number is $h_K^* = 2^{t_K-1}[I_K : I_K^H P_K]$, so

we only need to prove $[I_K : I_K^H P_K] = 1$ when the CM-field K has CM class number one, that is, when we have $I_0(\Phi^r) = I_{K^r}$.

We will start by proving that for any $\mathfrak{b} \in I_K$ the fractional ideal ${}^{1-s^3}\mathfrak{b}$ is principal and generated by an element $\alpha \in K^\times$ that satisfies $\alpha\overline{\alpha} = 1$. Then we can use Hilbert's Theorem 90 to prove that the ideal $\mathfrak{b}$ is in $I_K^H P_K$.

Let $\zeta_5 \in K$ be the primitive fifth root of unity for which (K, Φ) is CPQ-compatible, and let $k = \mathbb{Q}(\zeta_5)$. Identify K with its reflex field K^r via the embedding given in Proposition 4.3.15, so we have $\Phi = \{\mathrm{id}, s^2, s^4, t, st, s^2t\}$ for s and t generators of $\mathrm{Gal}(K/\mathbb{Q})$ as in Lemma 4.3.14. For any ideal $\mathfrak{b} \in I_K$ we can check by writing it out that we obtain

$$N_{\Phi^r}({}^{t-s^5t}\mathfrak{b})/N_{K/k}({}^{t-st}\mathfrak{b}) = {}^{1-s^3}\mathfrak{b}.$$

By an argument analogous to the one in the proof of Proposition 4.3.13, there exists $\alpha \in K^\times$ that satisfies ${}^{1-s^3}\mathfrak{b} = (\alpha)$ and $\alpha\overline{\alpha} = 1$, hence, by Hilbert's Theorem 90 [10], there exists an element $\delta \in K^\times$ with $\alpha = \overline{\delta}\delta^{-1}$. In consequence, $\mathfrak{b} = \overline{\delta\mathfrak{b}}\left(\frac{1}{\delta}\right) \in I_K^H P_K$ and thus $I_K = I_K^H P_K$. □

4.3.4 Final results

The following theorem summarizes all the results above.

Theorem 4.3.17. Let (K, Φ) be a Galois CPQ-compatible CM-type for a primitive fifth root of unity $\zeta_5 \in K$, let K^+ be the maximal totally real subfield of K and let Φ be a primitive CM-type. Let t_K be the number of primes in K^+ that ramify in K. The relative class number h_K^* of K is 2^{t_K-1} if and only if K has CM class number one.

Proof. One implication corresponds to Proposition 4.3.8. For the converse, note that by Proposition 4.3.4 the field K has a cyclic or dicyclic Galois group. Then, Propositions 4.3.13 and 4.3.16 are enough to prove the statement. □

With this result we can now prove Theorem 4.3.1.

Proof of Theorem 4.3.1. By Theorem 4.3.17, the field K has CM class number one if and only if its relative class number is $h_K^* = 2^{t_K-1}$ where t_K is the number of primes in the maximal totally real subfield K^+ that ramify in K. But since $\sqrt{5}$ is the only ramified prime in $\mathbb{Q}(\zeta_5)/\mathbb{Q}(\sqrt{5})$, all ramified primes in K/K^+ lie above 5 (see Proposition 4.8(ii) in [20, II]) and we get $t_K \leq 3$, hence we obtain $h_K^* \leq 4$.

Recall that by Proposition 4.3.4 the field K has a cyclic or dicyclic Galois group, so we look at each case separately.

On the one hand, Chang and Kwon [5] list all imaginary cyclic number fields of even degree with relative class number (with respect to their maximal totally

real subfields) less than or equal to 4, see [5, Table I]. In particular, we are interested in those that are degree-12 CM-fields containing a quartic field with conductor 5, that is, containing $\mathbb{Q}(\zeta_5)$, which are the fields (1)–(3) in Table 4.2.

On the other hand, Louboutin and Park [23] prove that the minimum relative class number of dicyclic CM-fields is 4, and list all such CM-fields (see Theorem 1 in [23]). In particular, we are again interested in those degree-12 CM-fields containing a quartic field with conductor 5, that is, containing $\mathbb{Q}(\zeta_5)$, which is exactly case (4) in Table 4.2. □

Using the methods due to Kılıçer [12, Chapter 4] and Theorem 3.5.3, one can prove that if Conjecture 3.5.1 holds, then for every field K in Table 4.2 there exists a unique CPQ curve with maximal CM by K and defined over $\mathbb{Q}$.

The curves in Section 2.3 are heuristic models for those curves, which we obtained by applying Algorithm 2.2.6 to the period matrices obtained through Van Wamelen's method, see Section 4.1 for details.