university of groningen / faculty of science and engineering / general mathematics

# Sextic CM-fields with Galois group $(C_2)_3 \rtimes C_3$ or $(C_2)_3 \rtimes S_3$

Bachelor's Project Mathematics

July 2020

Student: Lenka Bachoríková

First supervisor: Dr. Pınar Kılıçer

Second assessor: Prof.dr Jaap Top

**Abstract**

In the first two sections of this thesis the theory of number fields and the theory of complex multiplication (CM) is discussed. In the third section, new results are computed, namely the reflex types for two cases. First, where the Galois group of the normal closure of the sextic CM-field $K$ is $(C_2)^3 \rtimes C_3$ and second, where the Galois group of the normal closure of $K$ is $(C_2)^3 \rtimes S_3$. Moreover, in the end of the section explicit examples of sextic CM-fields are found and the reflex fields are computed for some of the examples. This thesis ends with discussion over further research in using the results of this bachelor project.

# Contents

# Preface

A complex multiplication field (CM-field) of degree $2g$ is defined to be a totally imaginary quadratic extension of totally real number field of degree $g$ over $\mathbb{Q}$. For a given CM-field $K$ of degree $g$, one can construct a principally polarized abelian variety (ppav) of dimension $g$ with CM by $K$; this construction is known as the *CM-method*. This connection to algebraic geometry makes these number fields interesting to study. For example, when $g = 1$, these CM-fields are imaginary quadratic fields and the abelian varieties constructed from these fields are CM-elliptic curves, which are commonly used in cryptography.

A CM-type $\Phi$ of a CM-field $K$ of degree $2g$ is a set of $g$ complex embeddings of K such that none of these embeddings are complex conjugate. To every pair $(K, \Phi)$, we can associate a CM-field, called the *reflex field*, $K^r$. The main theorem of CM [10] says that a ppav with CM by $K$ is defined over a finite extension of the $K^r$. One interesting question is to ask when such ppav's are defined over $K^r$, this is known as *CM-class number one problem*. This problem has been solved for $g = 1$, $g = 2$ and partially for $g = 3$.

Let $K$ be a sextic CM-field. Then the Galois group of the normal closure $L$ of $K$ is isomorphic to one of these groups: $C_6$, $D_6$, $(C_2)^3 \rtimes C_3$ or $(C_2)^3 \rtimes S_3$. The CM-class number one problem was solved for the first two cases but it is still open for the latter two cases. The focus of this project will be on the the latter two cases.

The aim is to understand the basics of CM-theory and compute the CM-types $\Phi$ of $K$ and then determine the reflex CM-fields $K^r$ for each $(K, \Phi)$ pair, where the Galois group of $K$ is isomorphic to $(C_2)^3 \rtimes C_3$ or $(C_2)^3 \rtimes S_3$. We will also look at explicit examples of sextic CM-fields for these two cases.

# 1 Number Fields

In this section some basic definitions from field theory and Galois theory are reviewed, and the background on number fields is presented. Most of the definitions are standard and can be found in *Abstract Algebra* by Dummit and Foote [3].

## 1.1 Field extensions

Suppose $K$ and $L$ are fields such that $K \subset L$. We say $L$ is a *field extension* of $K$, and write either $K \subset L$ or $L/K$. Now, let $\alpha \in L$, we say $\alpha$ is *algebraic* over $K$ if there exists a polynomial $f(x) \in K[X]$ with $f(\alpha) = 0$, i.e. $\alpha$ is a root of $f(x)$. Recall that the monic smallest degree polynomial $f(x) \in K[X]$ such that $f(\alpha) = 0$ is called the *minimal polynomial* of $\alpha$ over $K$. If all elements in $L$ are algebraic over $K$, we say $L$ is an *algebraic field extension* over $K$. We write $[L : K]$ for the dimension of $L$ as a $K$-vector space. This dimension is called the *degree* of $L/K$, which can be either *finite*, if $[L : K] < \infty$ or *infinite*, if $[L : K] = \infty$.

Let $K$ be a field and let $f(x) \in K[X]$. A *splitting field* of $K$ is the field $L$ such that

$$L = K(\alpha_1, \ldots, \alpha_n),$$

where $\alpha_i$'s are all the roots of $f(x)$. For any polynomial $f(x) \in K[X]$ a splitting field exists and is defined uniquely up to an isomorphism that acts as identity on $K$, see Theorem 25 and Corollary 28 in §13.4 [3].

Let $K \subset L$ be an algebraic field extension, then $L$ is *normal* over $K$ if every irreducible polynomial in $K[X]$ has all roots in $L$. We say that a polynomial $f(x) \in K[X]$ is *separable* if all its roots in a splitting field are pairwise distinct. An element $\alpha \in L$ is *separable* over $K$ if its minimal polynomial is separable. Finally, an algebraic field extension $K \subset L$ is *separable* if every $\alpha \in L$ is separable over $K$.

For the same field extension, a $K$-*automorphism* of $L$ is an isomorphism of fields such that

$$\begin{aligned} \sigma : L &\longrightarrow L \\ \alpha &\longmapsto \alpha, \quad \forall \alpha \in K, \end{aligned}$$

in other words, $\sigma_{|_K} = \mathrm{id}$. The set of $K$-automorphisms of $L$ forms a group under composition with identity automorphism as the unit element. This holds because the composition of two $K$-automorphisms of $L$ also fixes all the elements in $K$ and is an isomorphism, the inverse of each map exists since they are isomorphisms and associativity is obvious. We denote this group by $\mathrm{Aut}(L/K)$.

**Proposition 1.1.** Let $L$ be a finite extension of the field $K$ and let an element $\alpha \in L$. For each $\sigma \in \mathrm{Aut}(L/K)$ we have that $\sigma(\alpha)$ is a root of the minimal polynomial of $\alpha$ over $K$.

*Proof.* Assume $L$ is a finite extension over $K$ such that $[L : K] = n$ and take $\alpha \in L$. Let us denote the minimal polynomial of $\alpha$ over $K$ by $f(x)$. Then

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

where $a_i \in K$ since $f(x) \in K[X]$. Take $\sigma \in \mathrm{Aut}(L/K)$, then by the fact that $\sigma$ is a field homomorphism and $\sigma_{|_K} = \mathrm{id}$, we get

$$\begin{aligned}\sigma(f(x)) &= \sigma(a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0) \\ &= \sigma(a_n x^n) + \sigma(a_{n-1}x^{n-1}) + \ldots + \sigma(a_1 x) + \sigma(a_0) \\ &= a_n \sigma(x)^n + a_{n-1}\sigma(x)^{n-1} + \ldots + a_\sigma(x) + a_0\end{aligned}$$

and therefore

$$0 = \sigma(f(\alpha)) = a_n \sigma(\alpha)^n + a_{n-1}\sigma(x)^{n-1} + \ldots + a_\sigma(x) + a_0 = f(\sigma\alpha)).$$

This shows that $\sigma(\alpha)$ is a root of $f(x)$. □

**Definition 1.2.** A finite field extension $L/K$ is *Galois* if $L$ is normal and separable over $K$. In this case, the group of automorphisms of $L/K$ is denoted by $\mathrm{Gal}(L/K)$ and it is called the *Galois group* of $L/K$.

## 1.2 Number fields

In this section we will be interested in finite extensions of the field of rational numbers $\mathbb{Q}$ contained in the field of complex numbers $\mathbb{C}$.

**Definition 1.3.** An (algebraic) *number field* $K \subset \mathbb{C}$ is a finite degree field extension of the field of rational numbers $\mathbb{Q}$.

**Proposition 1.4.** Number field extensions are separable.

*Proof.* We begin by proving the following claim: Every non-zero polynomial in $\mathbb{Q}[X]$ is separable if and only if it is relatively prime to its derivative in $\mathbb{Q}[X]$.
Suppose that $f(x)$ is a non-zero separable polynomial in $\mathbb{Q}[X]$ with any root $\alpha \in \mathbb{C}$ such that $f(\alpha) = 0$. Then $f(x) = (x - \alpha)h(x)$, where $h(\alpha) \neq 0$ by the definition of separability. Taking the derivative we get

$$f'(x) = h(x) + (x - \alpha)h'(x).$$

Since $f'(\alpha) = h(\alpha) \neq 0$, so $\alpha$ is not a root of $f'(x)$. This implies that $f(x)$ and $f'(x)$ have no common roots, so they are relatively prime.
Now assume for contraposition that $f(x)$ is not separable. By definition, there exists a repeated root $\alpha$ in $f(x)$, so $f(x) = (x - \alpha)^2 g(x)$ and that implies that

$$f'(x) = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x) = (x - \alpha)(2g(x) - (x - \alpha)g'(x)).$$

So $f(x)$ and $f'(x)$ contain the same root hence they are not relatively prime. This proves the claim.

To finish the proof, we want to show that all irreducible polynomials $f(x)$ in $\mathbb{Q}[X]$ are separable. We will show by contradiction that $(f(x), f'(x)) = 1$. Now assume

that $(f(x), f'(x)) \neq 1$. Then we get $f(x)/f'(x)$, because $f(x)$ is assumed to be irreducible and $f'(x)$ is also in $\mathbb{Q}[X]$. But the degree of $f'(x)$ is lower than that of $f(x)$, so $f'(x) = 0$. Since $\mathrm{char}(\mathbb{Q}) = 0$, every non-constant polynomial in $\mathbb{Q}[X]$ has a non-zero derivative. We get a contradiction, so every irreducible polynomial in $\mathbb{Q}[X]$ is separable. $\square$

**Corollary 1.5.** Every finite normal extension of a number field is Galois.

*Proof.* By Proposition 1.4 it follows that every finite extension of a number field is separable. Then using Definition 1.2, it follows that every normal extension of a number field is Galois. $\square$

**Lemma 1.6.** Let $K$ and $L$ be number fields such that $K$ and $L$ are Galois over $\mathbb{Q}$. Then $KL$ is Galois over $\mathbb{Q}$.

*Proof.* Assume that $K$ and $L$ are number fields Galois over $\mathbb{Q}$. Then $[K : \mathbb{Q}] = n$ and $[L : \mathbb{Q}] = m$ and thus $[KL : \mathbb{Q}] \leq nm$. Since $KL$ is a finite degree extension over $\mathbb{Q}$, it is also a number field and by Proposition 1.4 we have $KL$ is separable over $K$. Now, by definition, $K$ and $L$ are both normal (and separable) over $\mathbb{Q}$ so every irreducible polynomial in $Q[X]$ has all roots in $K$ and $L$ so also in $KL$. This shows that $KL$ is normal, so we proved that $KL$ is Galois over $\mathbb{Q}$. $\square$

**Definition 1.7.** Let $K \subset L$ be an non-normal algebraic field extension. The *normal closure* of $L$ is the smallest field $N$ such that $N/K$ is normal and $L \subset N$.

Note that all normal closures of number fields are Galois. This follows immediately from Corollary 1.5.

In the previous section, we defined algebraic elements. A similar notion exists in number fields.

**Definition 1.8.** Let $K$ be a number field and $\alpha \in \mathbb{C}$, then $\alpha$ is an *algebraic number* if there exists a polynomial in $K[X]$ such that $\alpha$ is a root of that polynomial.

**Lemma 1.9.** If $\alpha, \beta \in \mathbb{C}$ are algebraic over a number field $K$, then there exists an element $\theta$ such that $K(\theta) = K(\alpha, \beta)$.

*Proof.* Let $f_\alpha(x)$ and $g_\beta(x)$ be the minimal polynomials of $\alpha$ and $\beta$ over $K$, respectively. We claim that there is an element $c \in K(\alpha, \beta)$ such that $\theta := \alpha + c\beta$ and $K(\alpha, \beta) = K(\theta)$.

The first inclusion $K(\theta) \subset K(\alpha, \beta)$ is obvious since $\theta = \alpha + c\beta \in K(\alpha, \beta)$. For the second inclusion, we proceed as follows. By Proposition 1.4 we know that all the roots $\alpha_1 := \alpha, \ldots, \alpha_n$ of $f_\alpha(x)$ and $\beta_1 := \beta, \ldots, \beta_m$ of $g_\beta(x)$ are distinct. We choose an element $c \in K(\alpha, \beta)$ so that for all $\alpha_i$ and $\beta_j$ with $i, j > 1$ we have $\alpha + c\beta \neq \alpha_i + c\beta_j$. Note that there are infinitely many elements in $K(\alpha, \beta)$ but only finitely many restriction for $c$, hence such a $c$ exists.

Let $\varphi(x) := f_\alpha(\theta - cx) \in K(\theta)[X]$, then $\varphi(\beta) = f_\alpha(\alpha) = 0$ and $\beta$ is the only common root of $\varphi(x)$ and $g_\beta(x)$ by the choice of $c$. So we get

$$\gcd(\varphi(x), g_\beta(x)) = k(x - \beta) \in K(\theta)[X],$$

where $k$ is such that $k \neq 0$, hence $\beta \in K(\theta)$, thus also $\alpha = \theta - c\beta \in K(\theta)$. This shows that $K(\alpha, \beta) \subset K(\theta)$, so $K(\alpha, \beta) = K(\theta)$. $\square$

**Theorem 1.10. (Primitive Element Theorem)** Let $L/K$ be a number field extension. Then there exists a non-zero element $\theta \in L$ such that $L = K(\theta)$.

*Proof.* Let $L/K$ be a number field extension and let $S$ be a basis of $L$ over $K$, i.e, $S$ is such that $S = \{\alpha_1, \ldots, \alpha_m : \alpha_i \in L\}$ and $L = K(\alpha_1, \ldots, \alpha_m)$. Note that $\#S$ is finite since $L$ is a finite extension over $K$, because they are both number fields. We will use induction on the size of $S$. Assume that $\#S = 1$. Then by definition $L = K(\theta)$. Assume that $\#S = n$ and there exists $\theta \in L$ such that $L = K(\theta)$.

Now let $S = \{\alpha_1, \ldots, \alpha_{n+1} : \alpha_i \in L\}$. So $L = K(\alpha_1, \ldots, \alpha_{n+1})$ but by induction hypothesis there exists $\theta_0 \in L$ such that $L = K(\theta_0, \alpha_{n+1})$. By Lemma 1.9 there exists an element $\theta \in L$ such that $L = K(\theta)$. $\square$

## 1.3 Embeddings

**Definition 1.11.** Let $K$ and $K'$ be two number fields and let $\phi$ be a field homomorphism $\phi : K \hookrightarrow K'$. Then $\phi$ is also called a *field embedding* of $K$ into $K'$. We say that an embedding $\phi : K \hookrightarrow \mathbb{C}$ is a *complex* embedding. A *totally complex* embedding is an embedding of the form $\phi : K \hookrightarrow \mathbb{C} \setminus \mathbb{R}$. A *real* embedding is an embedding such that $\phi : K \hookrightarrow \mathbb{R}$.

Every field homomorphism $\phi : K \hookrightarrow K'$ is injective, because the kernel of a field homomorphism is trivial.

The embedding $\rho$ such that

$$\begin{aligned} \rho : \quad & \mathbb{C} \hookrightarrow \mathbb{C} \\ & a + ib \longmapsto a - ib \end{aligned}$$

where $a$, $b \in \mathbb{R}$ and $i := \sqrt{-1} \in \mathbb{C}$ is an automorphism of $\mathbb{C}$ called *complex conjugation.* Each number field $K$ is a subset of $\mathbb{C}$, so the restriction map $\rho_{|_K} : K \hookrightarrow \mathbb{C}$ is a complex embedding of $K$.

Moreover, totally complex embeddings of a number field $K$ come in conjugate pairs, where we define the *complex conjugate* of a complex embedding $\phi$ of $K$, denoted by $\overline{\phi}$, to be $\overline{\phi} := \rho \circ \phi$. Note that if $\phi$ is a totally complex embedding of $K$, then $\overline{\phi}$ is also a totally complex embedding of $K$.

**Definition 1.12.** A *totally real number field* is a number field $K$ such that all complex embeddings of $K$ are real. Similarly, a *totally imaginary number field* is a number field $K$ such that all complex embeddings of $K$ are totally complex.

Let $K$ be a number field such that $[K : \mathbb{Q}] = n$. By Theorem 1.10 there exists an element $\theta \in \mathbb{C}$ such that $K = \mathbb{Q}(\theta)$. This notation will be used in the following two Lemmas.

**Lemma 1.13.** Any field homomorphism $\phi : K \hookrightarrow \mathbb{C}$ fixes $\mathbb{Q}$.

*Proof.* By the definition of a field homomorphism, it holds that $\phi(\alpha+\beta) = \phi(\alpha)+\phi(\beta)$ and $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$ for any $\alpha, \beta \in K$. Therefore, for any number $a \in \mathbb{Z}$ we have that $\phi(a) = a\phi(1)$ and most importantly, for all $a, b \in \mathbb{Z}$, $b \neq 0$ we have

$$\phi\left(\frac{a}{b}\right) = \phi(a)\phi(b)^{-1} = ab^{-1} = \frac{a}{b},$$

so $\phi_{|_{\mathbb{Q}}} = \mathrm{id}$. □

**Lemma 1.14.** The field homomorphism $\phi : K \hookrightarrow \mathbb{C}$ is uniquely determined by $\phi(\theta)$.

*Proof.* Since we have $K = \mathbb{Q}(\theta)$, every element $\alpha \in K$ can be written as $\alpha = \sum_{i=0}^{n} a_i\theta^i$ for $a_i \in \mathbb{Q}$. Therefore we get

$$\phi(\alpha) = \phi(\sum_{i=0}^{n} a_i\theta^i) = \sum_{i=0}^{n} \phi(a_i)\phi(\theta^i) = \sum_{i=0}^{n} a_i\phi(\theta)^i.$$

Note that $\phi(a_i) = a_i$ by Lemma 1.13. Uniqueness follows from injectivity of $\phi$. □

**Proposition 1.15.** A number field $K$ with $[K : \mathbb{Q}] = n$ has exactly $n$ complex embeddings.

*Proof.* Assume $K$ is a number field such that $[K : \mathbb{Q}] = n$. From Theorem 1.10 we get that there is a $\theta \in K$ such that $\mathbb{Q}(\theta) = K$. Let $f(x)$ be the minimal polynomial of $\theta$ over $K$. By Lemma 1.14 we know that for $\phi$ a complex embedding of $K$, we get $\phi(\theta)$ is a root of $f(x)$. Since $K$ is separable, all roots of $f(x)$ are distinct so each complex embedding maps $\theta$ to a different root of $f(x)$. We can define complex embeddings

$$\begin{aligned} \phi_i : K = \mathbb{Q}(\theta) &\longrightarrow \mathbb{Q}(\theta_i) \subset \mathbb{C} \\ \theta &\longmapsto \theta_i, \end{aligned}$$

where $\theta_1 := \theta, \ldots, \theta_n$ are roots of $f(x)$. Note that $\phi_i$'s are field homomorphisms since

$$\begin{aligned} \phi_i((c_1+\theta c_2)+(d_1+\theta d_2)) &= \phi_i(c_1+d_1+\theta(c_2+d_2)) \\ &= c_1+d_1+\theta_i(c_2+d_2) \\ &= (c_1+\theta_i c_2)+(d_1+\theta_i d_2) \\ &= \phi_i(c_1+\theta c_2)+\phi_i(d_1+\theta d_2) \end{aligned}$$

$$\begin{aligned} \phi_i((c_1+\theta c_2)(d_1+\theta d_2)) &= \phi_i(c_1d_1+c_2d_2+\theta(c_1d_2+c_2d_1)) \\ &= c_1d_1+c_2d_2+\theta_i(c_1d_2+c_2d_1) \\ &= (c_1+\theta_i c_2)(d_1+\theta_i d_2) \\ &= \phi_i(c_1+\theta c_2)\phi_i(d_1+\theta d_2), \end{aligned}$$

for all $c_1, c_2, d_1, d_2 \in \mathbb{Q}$. Moreover, $\phi_i$ forms an isomorphisms since

$$\mathbb{Q}(\theta) \cong \mathbb{Q}[X]/(f) \cong \mathbb{Q}(\theta_i).$$

This shows that $\phi_i$ are complex embeddings of $K$ and there are exactly $n$ of them. □

**Corollary 1.16.** If $K \subset L$ is a number field extension, then every complex embedding of $K$ extends exactly $d := [L : K]$ embeddings of $L$ in $\mathbb{C}$.

*Proof.* This follows from Proposition 1.15 when replacing $\mathbb{Q}, K$ with $K, L$, respectively. $\square$

**Proposition 1.17.** Let $K$ be a number field such that $K/\mathbb{Q}$ is Galois. The complex embeddings of $K$ identify exactly with the elements of $\mathrm{Gal}(K/\mathbb{Q})$.

*Proof.* Let $K \subset \mathbb{C}$ be a normal number field extension over $\mathbb{Q}$ and let $[K : \mathbb{Q}] = n$. By Corollary 1.5, the extension $K/\mathbb{Q}$ is Galois. By Theorem 1.10, there exists $\theta \in \mathbb{C}$ such that $K = \mathbb{Q}(\theta)$. Recall that the elements of the group $\mathrm{Aut}(K/\mathbb{Q})$ (in this case we have $\mathrm{Aut}(K/\mathbb{Q}) = \mathrm{Gal}(K/\mathbb{Q})$) permute the roots of the minimal polynomial of $\theta$ over $\mathbb{Q}$ by Proposition 1.1. Since $K \subset \mathbb{C}$, any automorphism $\sigma \in \mathrm{Aut}(K/\mathbb{Q})$ gives

$$\sigma : K \longrightarrow K \subset \mathbb{C}.$$

So the automorphisms of $K$ give distinct complex embeddings. Moreover, $K/\mathbb{Q}$ is Galois so this implies $\#\,\mathrm{Aut}(K/\mathbb{Q}) = [K : \mathbb{Q}]$. By Proposition 1.15 we can conclude that all the complex embeddings of $K$ arise as automorphisms of $K$. $\square$

Let $K$ be a number field and $L$ the normal closure of $K$. We have that $K = \mathbb{Q}(\theta)$ for some element $\theta \in \mathbb{C}$. Let $\phi : K \hookrightarrow L$ be a field homomorphism, then by Lemma 1.14, the embedding $\phi$ is uniquely determined by the roots of the minimal polynomial of $\theta$ over $\mathbb{Q}$. By Proposition 1.17 we can then identify the complex embeddings of $L$ with the automorphisms of $L$. The embeddings of $K$ into $L \subset \mathbb{C}$ then become

$$\{\phi_{|_K} \in \mathrm{Hom}(K, L) : \phi \in \mathrm{Aut}(L/\mathbb{Q})\}.$$

**Definition 1.18.** Let the notation be as above. Then an automorphism $\phi \in \mathrm{Aut}(L/\mathbb{Q})$ for which $\phi_{|_K} \in \mathrm{Hom}(K, L)$ is called an *extension* of $\phi_{|_K}$.

Assume that $K \subset L$ is an extension of number fields such that the degrees $[K : \mathbb{Q}] = n$ and $[L : K] = d$. By the tower law we have $[L : \mathbb{Q}] = nd$. Following from Proposition 1.15 and Corollary 1.16 there exist exactly $n$ complex embeddings $\phi_i$ of $K$ (note that these are also complex embeddings of $L$ since $K \subset L$) and every complex embedding of $K$ extends exactly $d$ embeddings of $L$ in $\mathbb{C}$.

$$\begin{tikzcd} L \arrow[r, "\phi_L"] & \mathbb{C} \\ K \arrow[u, "\sigma"] \arrow[ur, "\phi=\phi_L\circ\sigma"'] & \end{tikzcd}$$

Figure 1: Extending complex embeddings of $K$ to $L$

Suppose that the field extension $L/K$ is Galois. Let $\phi \in \mathrm{Hom}(K, L)$ then the set

$$\{\phi \circ \sigma \,:\, \sigma \in \mathrm{Gal}(L/K)\}$$

contains $\#\operatorname{Gal}(L/K)$ embeddings of $L$ into $L \subset \mathbb{C}$ and these embeddings are distinct. By Corollary 1.16, we conclude that this is the set of all embeddings in $\operatorname{Hom}(L, L)$ extending $\phi$.

## 1.4 Trace and Norm

Let $K$ be a number field of degree $n$ over $\mathbb{Q}$. The *trace* $\mathrm{T}_K$ and the *norm* $\mathrm{N}_K$ are two maps defined as follows: Let $\phi_1,\ldots,\phi_n$ be the embeddings of $K$ with values in $\mathbb{C}$. For each element $\alpha \in K$ , set

$$\mathrm{T}_K(\alpha) := \sum_{i=1}^{n} \phi_i(\alpha),$$
$$\mathrm{N}_K(\alpha) := \prod_{i=1}^{n} \phi_i(\alpha).$$

Since all $\phi_i$ are embeddings, so they are also field homomorphisms, by definition we have $\phi_i(\alpha+\beta) = \phi_i(\alpha) + \phi_i(\beta)$ and $\phi_i(\alpha\beta) = \phi_i(\alpha)\phi_i(\beta)$. This immediately implies

$$\mathrm{T}_K(\alpha+\beta) = \mathrm{T}_K(\alpha) + T_K(\beta)$$
$$\mathrm{N}_K(\alpha\beta) = \mathrm{N}_K(\alpha)N_K(\beta)$$

for all $\alpha$, $\beta \in K$. Moreover, if $c \in \mathbb{Q}$, by Lemma 1.13 we get

$$\mathrm{T}_K(c\alpha) = c\,\mathrm{T}_K(\alpha) \text{ and } \mathrm{N}_K(c\alpha) = c^n\,\mathrm{N}_K(\alpha).$$

Note that both $\mathrm{T}_K(\alpha)$ and $\mathrm{N}_K(\alpha)$ are coefficients of the minimal polynomial of $\alpha$ over $\mathbb{Q}$, namely $\mathrm{T}_K(\alpha)$ is the second coefficient and $\mathrm{N}_K(\alpha)$ is the last constant term. Then they both must always be rational values. For example, if $K = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Q}$, then we have for any $a$, $b \in \mathbb{Q}$

$$\mathrm{T}_K(a+b\sqrt{d}) = 2a \text{ and } \mathrm{N}_K(a+b\sqrt{d}) = a^2 - db^2,$$

because the only two embeddings of $K$ into $\mathbb{C}$ are identity and complex conjugation.

## 1.5 Ring of integers

**Definition 1.19.** An algebraic number is called an *algebraic integer* whenever it is a root of some *monic irreducible* polynomial with coefficients in $\mathbb{Z}$.

**Theorem 1.20.** The set of algebraic integers in a number field $K$ forms a ring, which has rank $[K : \mathbb{Q}] = n$ over $\mathbb{Z}$ as a $\mathbb{Z}$-module, i.e., it is isomorphic to $\mathbb{Z}^n$ .

*Proof.* The fact that the algebraic integers form a ring follows from Corollary 1 in § 2 [8]. By Corollary on page 22 of [8] it follows that the ring of algebraic integers is a free abelian group of rank $n$, which is the same as it being a $\mathbb{Z}$-module isomorphic to $\mathbb{Z}^n$. □

**Definition 1.21.** The set of all algebraic integers in a number field $K$ is called the *ring of integers* or the *maximal order* and is denoted by $\mathcal{O}_K$.

In order to understand rings of integers better, let us take the trivial number field, namely $K = \mathbb{Q}$. If we take $a \in \mathbb{Q}$ such that it is a root of some monic irreducible polynomial in $\mathbb{Z}[X]$, we get $(x - a) \in \mathbb{Z}[X]$. Hence $a \in \mathbb{Z}$, which implies that $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

Now let $K = \mathbb{Q}(\sqrt{d})$ for some squarefree number $d \in K$. Thus $K$ is a second degree extension over $\mathbb{Q}$. The following proposition shows the possibilities for the ring of integers for different values of $d$.

**Proposition 1.22.** (Example in §7.1, p.229 [3]) Let $d$ be a squarefree integer. The set of algebraic integers in the quadratic field $\mathbb{Q}(\sqrt{d})$ is

$$\mathbb{Z}\left[\sqrt{d}\right] = \left\{a + b\sqrt{d} : a, b \in \mathbb{Z}\right\}, \qquad \text{if } d \equiv 2 \text{ or } 3 \bmod 4,$$

$$\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{\frac{a + b\sqrt{d}}{2} : a, b \in \mathbb{Z} \text{ and } a \equiv b \bmod 2\right\}, \qquad \text{if } d \equiv 1 \bmod 4.$$

**Definition 1.23.** Let $A \subset B$ be an extension of rings. An element $\alpha \in B$ is an *integral* over $A$ if there exists a monic polynomial $f(x) \in A[X]$ such that $f(\alpha) = 0$. If $A$ and $B$ are integral domains, then $B$ is *integrally closed* in $B$ if every element in $B$ that is an integral over $A$ is contained in $A$.

For example, let us take an integral $\alpha \in \mathbb{Q}$. Then the monic polynomial $f(x) \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$. By Gauss Lemma $(x - \alpha) \in \mathbb{Z}[X]$ so also $\alpha \in \mathbb{Z}$. Since both $\mathbb{Z}$ and $\mathbb{Q}$ are integral domains, we have that $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$, where $\mathbb{Q}$ is actually the field of fractions of $\mathbb{Z}$.

**Definition 1.24.** A *Dedekind domain* is an integral domain $R$ such that

1. Every ideal is finitely generated,
2. Every non-zero prime ideal is a maximal ideal,
3. $R$ is integrally closed in its field of fractions

$$Q(R) = \left\{\frac{a}{b} : a, b \in R \text{ and } b \neq 0\right\}.$$

**Theorem 1.25.** (Proposition 14 in §16.3 [3]) The ring of integers $\mathcal{O}_K$ is a Dedekind domain.

## 1.6 Ideals in the ring of integers

Now the attention will turn more towards the ideals in the ring of integers. Let us first recall a couple of notions that will be used in this section. A ring $R$ is called an *integral domain* if for all elements $x$,$y \in R$ such that $xy = 0$, either $x = 0$ or $y = 0$ (or both). The set $I \subset R$ is an *ideal* in $R$ if it satisfies the following conditions:

1. $I$ is a subring of $R$,
2. For all $i \in I$ and $r \in R$, it holds that $ir \in R$.

We say $I$ is a *principal ideal* if $I$ is generated by a single element. An integral domain of which all ideals are principal is called a *principal ideal domain* or simply PID. An ideal $I \neq R$ for which it holds that if $ab \in I$ then either $a \in I$ or $b \in I$ (or both) is called a *prime ideal*. An ideal $M \neq R$ is called *maximal* if it holds that every ideal $J$ of $R$ with $M \subset J \subset R$ is either $J = M$ or $J = R$.

In the next theorem we use the notion of a *unique factorization domain* (UFD). A UFD is an integral domain such that every element can be uniquely factorized to the product of irreducible elements up to a unit. Every PID is actually a UFD (see Theorem 14 in §8.3 [3]) so this theorem states that for Dedekind domains also the opposite inclusion holds.

**Theorem 1.26.** (Corollary 20 of §16.3 [3]) A Dedekind domain is a UFD if and only if it is a PID.

We say that two ideals $\mathfrak{a}$ and $\mathfrak{b}$ in a Dedekind domain $R$ are equivalent if there is a non-zero element $d \in R$ such that $\mathfrak{a} = d\mathfrak{b}$, where $d\mathfrak{b} := \{db : b \in \mathfrak{b}\}$. The ideals that are equivalent to each other form a set called *equivalency class* denoted by

$$[\mathfrak{a}] := \{\mathfrak{b} \subset R : \mathfrak{a} \sim \mathfrak{b} \text{ and } \mathfrak{a}, \mathfrak{b} \text{ are ideals in } R\}.$$

Let $\mathrm{Cl}(R)$ denote the set of all equivalence classes $[\mathfrak{a}]$ of non-zero ideals $\mathfrak{a} \subset R$. With respect to the equivalence relation we define the multiplication of equivalence classes by

$$[\mathfrak{a}][\mathfrak{b}] := [\mathfrak{a}\mathfrak{b}] \tag{1}$$

for ideals $\mathfrak{a}, \mathfrak{b}$ in $R$. Then the following proposition holds.

**Proposition 1.27.** Let $R$ be an integral domain and let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in $R$. Then the following holds:

1. If $c\mathfrak{a}$ is principal for some non-zero $c \in R$ then $\mathfrak{a}$ is principal.
2. The principal ideals in $R$ form an ideal class, which we denote by $[R]$.
3. The set $\mathrm{Cl}(R)$ of ideal classes in $R$ forms a group with respect to multiplication defined in (1) with the identity element $[R]$ if and only if for every ideal $\mathfrak{a}$ there exists an ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b}$ is principal.

*Proof.* We will prove each part of this proposition separately.

1. Assume $c\mathfrak{a} = (\alpha)$ for some non-zero $\alpha \in R$. That means $\alpha = ca$ for some $a \in \mathfrak{a}$. We want to show that $(a) = \mathfrak{a}$.

   Since $a \in \mathfrak{a}$ we get $(a) \subset \mathfrak{a}$. Now take any $b \in \mathfrak{a}$. Then $cb \in c\mathfrak{a} = (\alpha) = (ca)$. Then we can write $cb$ as $cb = kca$ for some non-zero $k \in R$. By commutativity of $R$, it follows that $cb = cka$, so $b = ka \in (a)$. This gives $\mathfrak{a} \subset (a)$ and hence $(a) = \mathfrak{a}$ which means $\mathfrak{a}$ is principal.

2. We need to show that any two principal ideals in $R$ are equivalent and any ideal equivalent to a principal ideal is also principal.

   Let $(\alpha)$ and $(\beta)$ be two principal ideals in $R$. Since $\alpha(\beta) = (\alpha\beta) = (\beta\alpha) = \beta(\alpha)$, we get $(\alpha) \sim (\beta)$. For the second part, let $\mathfrak{a}$ be an ideal in $R$ and $(\gamma)$ be a principal ideal in $R$ such that $(\gamma) \sim \mathfrak{a}$. By definition, $(\gamma) = c\mathfrak{a}$ for some non-zero $c \in R$, so $c\mathfrak{a}$ is principal. By 1, we get that $\mathfrak{a}$ is principal.

3. Assume for every ideal in $R$ there exists an ideal such that their product is a principal ideal. Associativity of ideal class multiplication follows directly from associativity of ideal multiplication. For any class $C$ in $\mathrm{Cl}(R)$ there exists a non-zero ideal $\mathfrak{a}$ such that $C = [\mathfrak{a}]$. So for every $C \in \mathrm{Cl}(R)$ we have

$$[R] \cdot C = [(1) \cdot \mathfrak{a}] = [\mathfrak{a}] = C$$

   for some ideal $\mathfrak{a} \subset R$. To verify that every ideal class has an inverse, let $C$ be any class and $\mathfrak{a} \in C$. By assumption, there exists an ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} \in [R]$. Letting $[\mathfrak{b}]$ be the ideal class of $\mathfrak{b}$, this means $C[\mathfrak{b}] = [R]$, i.e. $[\mathfrak{b}]$ is the inverse of $C$. Hence the ideal classes form a group.

   Now, for the other direction, assume that $\mathrm{Cl}(R)$ forms a group with the identity $[R]$. Let $\mathfrak{a}$ be an ideal in $R$. Then there is a non-zero ideal $\mathfrak{b}$ such that $[\mathfrak{a}][\mathfrak{b}] = [\mathfrak{a}\mathfrak{b}] = [R]$. This implies that $\mathfrak{a}\mathfrak{b}$ is principal.

□

**Lemma 1.28.** (Lemma 2 in §3 [8]) Let $I$ be a proper ideal in a Dedekind domain $R$ with field of fractions $Q(R)$. Then there is an element $\gamma \in Q(R) \setminus R$ such that $\gamma I \subset R$.

**Theorem 1.29.** For every non-zero ideal $\mathfrak{a}$ in a Dedekind domain $R$, there is an ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b}$ is principal.

*Proof.* Let $a \in \mathfrak{a}$ be such that $a \neq 0$ and let $\mathfrak{b} = \{b \in R : b\mathfrak{a} \subset (a)\}$. Then $a \in \mathfrak{b}$ so $\mathfrak{b}$ is a non-zero ideal because if we take any $r \in R$, $ra \in \mathfrak{a}$ for all $a \in \mathfrak{a}$ (by the definition of an ideal) so therefore for every $b \in \mathfrak{b}$ it holds that

$$rb\mathfrak{a} = br\mathfrak{a} \subset b\mathfrak{a} \subset (a)$$

which shows that $rb \in \mathfrak{b}$. Note that this is possible since a Dedekind domain is an integral domain, so it is commutative. By the definition of $\mathfrak{b}$ we get that $\mathfrak{b} \subset (a)$ hence also $\mathfrak{a}\mathfrak{b} \subset (a)$. Consider $A = \frac{1}{a}\mathfrak{a}\mathfrak{b}$. We will show that $A$ is an ideal in $R$.

Take $r \in R$ and $x \in A$. We can write $x = \frac{1}{a}a_1b_1$ for some $a_1 \in \mathfrak{a}$ and $b_1 \in \mathfrak{b}$. By commutativity we get

$$rx = r\frac{1}{a}a_1b_1 = \frac{1}{a}a_1rb_1 = \frac{1}{a}a_1b_2,$$

since again, $b_2\mathfrak{a} = rb_1\mathfrak{a} \subset (a)$ hence $b_2 \in \mathfrak{b}$. Note that since $\mathfrak{a}\mathfrak{b} \subset aR$ then $\frac{1}{a} \in \frac{1}{a}\mathfrak{a}\mathfrak{b} \subset R$.

Now we have two options: If $A = R$ then since $R = (1) = \frac{1}{a}\mathfrak{a}\mathfrak{b}$ this implies $(a) = \mathfrak{a}\mathfrak{b}$, so $\mathfrak{a}\mathfrak{b}$ is principal; In the other case $A$ is a proper ideal and by Lemma 1.28 there is an

element $c \in Q(R) \setminus R$ such that $cA \subset R$. Since $R$ is integrally closed in $Q(R)$, it is enough to show that $c$ is a root of a monic polynomial over $R$ because then $c \in R$ which is a contradiction.

Since $\mathfrak{b} \subset A = \frac{1}{a}\mathfrak{a}\mathfrak{b}$ and $a \in \mathfrak{a}$, we have $c\mathfrak{b} \subset cA \subset R$. By the definition of $\mathfrak{b}$ we get that $c\mathfrak{b} \subset \mathfrak{b}$. Now fix a finite generating set $b_1, \ldots, b_r$ for the ideal $\mathfrak{b}$ (note that $\mathfrak{b}$ is finitely generated ideal because $R$ is a Dedekind domain) and by $c\mathfrak{b} \subset \mathfrak{b}$ we get

$$\begin{aligned} cb_1 &\in \mathfrak{b} \\ cb_2 &\in \mathfrak{b} \\ &\ldots \\ cb_r &\in \mathfrak{b}. \end{aligned}$$

Therefore each $cb_i$ can be written as

$$cb_i = m_{i1}b_1 + m_{i2}b_2 + \ldots + m_{ir}b_r$$

for all $i$. This can also be rewritten in the following form

$$c\begin{bmatrix} b_1 \\ . \\ . \\ . \\ b_r \end{bmatrix} = \begin{bmatrix} m_{11} & . & . & . & m_{1r} \\ . & . & & & . \\ . & & . & & . \\ . & & & . & . \\ m_{r1} & . & . & . & m_{rr} \end{bmatrix} \begin{bmatrix} b_1 \\ . \\ . \\ . \\ b_r \end{bmatrix}.$$

Let $M$ be the $r \times r$ matrix stated above, then via the determinant of $(cI_r - M)$, we obtain a monic polynomial over $R$ having $c$ as a root. This proves theorem. □

**Corollary 1.30.** Let $R$ be a Dedekind domain. Then the set of ideal classes of $R$ denoted by $\mathrm{Cl}(R)$ forms an abelian group with respect to multiplication defined in (1) with identity $[R]$ being the class of principal ideals in $R$.

*Proof.* From Theorem 1.29 we have that for every ideal $\mathfrak{a} \in \mathrm{Cl}(R)$ there exists an ideal $\mathfrak{b} \in \mathrm{Cl}(R)$ such that $\mathfrak{a}\mathfrak{b}$ is principal. Since a Dedekind domain is an integral domain, by the third part of Proposition 1.27 it follows that $\mathrm{Cl}(R)$ forms a group. Moreover, multiplication of ideals is commutative in $R$, hence this group is abelian. □

In particular, by Theorem 1.25, we conclude:

**Corollary 1.31.** Let $K$ be a number field. Then the set of ideal classes of $\mathcal{O}_K$ forms an abelian group with respect to multiplication defined in (1) with identity $[\mathcal{O}_K]$ being the class of principal ideals in $\mathcal{O}_K$.

By Marcus (Chapter 1 and 5 in [8]) the group $\mathrm{Cl}(\mathcal{O}_K)$ is *finite*. This group is called the *ideal class group* and the size of the group is called the *class number*.

**Theorem 1.32.** If $\#\,\mathrm{Cl}(\mathcal{O}_K) = 1$ then $\mathcal{O}_K$ is a PID.

*Proof.* Assume $\#\operatorname{Cl}(\mathcal{O}_K) = 1$, then $\operatorname{Cl}(\mathcal{O}_K) = [\mathcal{O}_K]$. That means that every ideal in $\mathcal{O}_K$ is principal. $\square$

Note that from the previous theorem it follows that if $\mathcal{O}_K$ has class number one then it is also a UFD. By determining the class number one fields we, therefore, determine the ring of integers with UFD property.

The *class number one problem* for number fields of degree $n$ determines a complete list of such fields having class number one. When the number fields are imaginary quadratic, this problem is known as *Gauss class number one* problem which was solved independently by Baker [1], Heegner [4] and Stark [11].

**Theorem 1.33.** ([1, 4, 11]) Let $K$ be an imaginary quadratic number field with the maximal order $\mathcal{O}_K$. Then we have $\#\operatorname{Cl}(\mathcal{O}_K) = 1$ if and only if $K \cong \mathbb{Q}(\sqrt{-d})$, where $d$ is such that $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$.

# 2 CM-fields and CM-types

In this chapter we provide an introduction to the theory of complex multiplication by providing some basic definitions that build upon the theory of number fields. The definitions, theorems, etc. follow from *Complex Multiplication* by Lang [7] and *Complex Multiplication* by Milne [9].

**Definition 2.1.** A *complex multiplication field* also called a *CM-field* $K$ is a totally imaginary quadratic extension of a totally real number field $K_+$. In other words, a CM-field is $K = K_+(\sqrt{r})$, where $r$ is totally negative element in $K_0$.

**Proposition 2.2.** (Characterization of CM-fields by Lang [7]) Either one of the following two conditions characterize a CM-field:

1. $K$ is a totally imaginary quadratic extension of a totally real field.
2. Complex conjugation $\rho$ commutes with every complex embedding of $K$ and $K$ is not real.

**Proposition 2.3.** The normal closure of a CM-field is a CM-field.

*Proof.* Assume that $K$ is a CM-field and $L$ is the normal closure of $K$. By Proposition 2.2 the field $K$ is totally imaginary, meaning that every complex embedding of $K$ is totally complex. We now show that $L$ is also totally imaginary. Assume for contradiction that there is a real embedding $\phi$ of $L$. Then $\phi(a) \in \mathbb{R}$ for all $a \in L$, but we know that $\phi_{|_K}(a') \in \mathbb{C} \setminus \mathbb{R}$ for all $a' \in K \subset L$, hence we get a contradiction, so $L$ is not real.

Now we will show that $\rho$ commutes with every complex embedding of $L$. The degree of $K$ over $\mathbb{Q}$ is finite, so let $[K : \mathbb{Q}] = n$ and by Theorem 1.10 we have that $K = \mathbb{Q}(\theta)$ for some $\theta \in \mathbb{C}$. Now, the minimal polynomial $f(x)$ of $\theta$ over $\mathbb{Q}$ is of the form

$$f(x) = \prod_{i=1}^{n}(x - \theta_i),$$

where $\theta := \theta_1, \ldots, \theta_n$ denote the roots of $f(x)$. We get that there are $n$ fields $\mathbb{Q}(\theta_i)$ which are isomorphic to $K$ by the following isomorphism

$$\begin{aligned} K = \mathbb{Q}(\theta) &\longrightarrow \mathbb{Q}(\theta_i) \\ \theta &\longmapsto \theta_i. \end{aligned}$$

This shows that for all $i$ the field $\mathbb{Q}(\theta_i)$ must be a CM-field. Note that $L = \mathbb{Q}(\theta_1, \ldots, \theta_n)$ since it is the normal closure of $K$. Now the complex conjugation $\rho : \mathbb{C} \to \mathbb{C}$ can be restricted to each of these CM-fields such that by Proposition 2.2 we have that $\rho_{|_{\mathbb{Q}(\theta_i)}}$ commutes with all complex embeddings of $\mathbb{Q}(\theta_i)$ for all $i$. Then any complex embedding $\phi$ of $L$ satisfies $\phi_{|_{\mathbb{Q}(\theta_i)}} \circ \rho = \rho \circ \phi_{|_{\mathbb{Q}(\theta_i)}}$. An arbitrary element $a \in L$ is an element of $\mathbb{Q}(\theta_i)$ for some $0 \leq i \leq n$. Then we have

$$\phi(a) = \phi_{|_{\mathbb{Q}(\theta_i)}}(a)$$

but then we get

$$\rho \circ \phi(a) = \rho \circ \phi_{|_{\mathbb{Q}(\theta_i)}}(a) = \phi_{|_{\mathbb{Q}(\theta_i)}} \circ \rho(a) = \phi \circ \rho(a).$$

This shows that $\rho$ commutes with all complex embeddings of $L$ and hence by Proposition 2.2 the normal closure $L$ of $K$ is a CM-field. $\square$

Let $K$ and $L$ be CM-fields such that $L$ is the normal closure of $K$. Assume that the degree $[K : \mathbb{Q}] = 2g$, so by Proposition 1.15 there are $2g$ complex embeddings of $K$.

**Definition 2.4.** A *CM-type* $\Phi$ of $K$ with values in $L$ is a set of $g$-embeddings of $K$ into $L$ of which no two are complex conjugate of each other.

As we have shown before, complex embeddings come in conjugate pairs. By picking one embedding from each conjugate pair, we construct a CM-type with exactly $g$ embeddings. This also gives $2^g$ possibilities on how to construct a CM-type, so there are exactly $2^g$ CM-types of $K$ with values in $L \subset \mathbb{C}$.

**Definition 2.5.** Let $\Phi$ be a CM-type of $K$ with values in $L$. The CM-type of $L$ *induced* by $\Phi$ is defined as

$$\Phi_L = \{\phi \in \mathrm{Aut}(L) : \phi_{|_K} \in \Phi\}.$$

We say that a CM-type is *primitive* if it is not induced from a CM-type of a strict CM-subfield.

**Definition 2.6.** Let $K$ be a CM-field and let $\Phi$ be a CM-type of $K$. Let $\sigma \in \mathrm{Aut}(K)$ and $\phi$ be an embedding of $K$ into a field $L$. Then we define

$$\Phi\sigma := \{\phi \circ \sigma : \phi \in \Phi\}$$

and

$$\phi\Phi := \{\phi \circ \varphi : \varphi \in \Phi\}.$$

**Proposition 2.7.** (Proposition 1.9 in [9]) Every CM-pair $(K, \Phi)$ is the extension of a unique primitive CM-pair $(K_0, \Phi_0)$ with $K_0 \subset K$. In fact, for any CM-field $L$ containing $K$ such that $L/\mathbb{Q}$ is Galois, $K_0$ is the fixed field of

$$\mathrm{Gal}(L/K_0) = \{\sigma \in \mathrm{Gal}(L/\mathbb{Q}) : \Phi_L \sigma = \Phi_L\},$$

where $\Phi_L$ is the extension of $\Phi$ to $L$.

**Definition 2.8.** Two CM-types $\Phi$ and $\Phi'$ of a CM-field $K$ are *equivalent* if there exists an automorphism $\sigma$ of $K$ such that $\Phi\sigma = \Phi'$.

## 2.1 Reflex types and reflex fields

Let $K$ be a CM-field and let $\Phi$ be a CM-type of $K$ with values in $L$ the normal closure of $K$. The *reflex* $(K^r, \Phi^r)$ of $(K, \Phi)$ is defined as follows. Let $\Phi_L$ be the CM-type of $L$ with values in $L$ induced by $\Phi$. Note that $\Phi_L$ is a set of isomorphisms from $L$ to $L$, so there is a set of inverses of each of these maps, denoted by $\Phi_L^{-1}$.

From §2 of Chapter 1 in [7] it follows that $\Phi_L^{-1}$ is a CM-type of $L$ with values in $L$. By Proposition 2.7, there exists a unique primitive pair $(K^r, \Phi^r)$ that induces $(L, \Phi_L^{-1})$.

**Definition 2.9.** The *reflex type* or *reflex pair* of $(K, \Phi)$ is the pair $(K^r, \Phi^r)$, where $K^r$ is the *reflex field* of $(K, \Phi)$ and $\Phi^r$ is the *reflex CM-type* of $(K, \Phi)$.

**Lemma 2.10.** The CM-type $\Phi^r$ is a primitive CM-type of $K^r$. If we denote the reflex of $(K^r, \Phi^r)$ by $(K^{rr}, \Phi^{rr})$, then $K^{rr}$ is a subfield of $K$ and $\Phi$ is induced by $\Phi^{rr}$. If $\Phi$ is primitive, then we have $K^{rr} = K$ and $\Phi^{rr} = \Phi$.

*Proof.* It follows from the definition that $K^{rr} \subset K$ and $\Phi^{rr}$ induces $\Phi$. Then if $\Phi$ is primitive, there exist no CM-type that would induce $\Phi$, so $\Phi$ must be equal to $\Phi^{rr}$ and hence also $K = K^{rr}$. □

As we know, every normal extension of a number field is Galois. So one can examine the Galois groups of these extensions. The following corollary describes the Galois group of $L/K^r$. This will be useful in constructing the reflex fields in the next section.

**Proposition 2.11.** With the same notation as in Definition 2.9, we have

$$\mathrm{Gal}(L/K^r) = \{\sigma \in \mathrm{Gal}(L/\mathbb{Q}) : \sigma\Phi_L = \Phi_L\}.$$

*Proof.* This follows from Theorem 2.7 and the definition of $K^r$. □

**Proposition 2.12.** Let $K$ be a CM-field and let $\Phi_1$ and $\Phi_2$ be two CM-types of $K$. If $\Phi_1$ and $\Phi_2$ are equivalent, then the reflex fields of $(K, \Phi_1)$ and $(K, \Phi_2)$ are the same.

*Proof.* Assume that $\Phi_1$ and $\Phi_2$ are equivalent CM-types of the CM-field $K$ with values in $L$ the normal closure of $K$. By definition, there exist automorphisms $\sigma, \tau$ of $K$ such that $\Phi_1\sigma = \Phi_2$ and $\Phi_2\tau = \Phi_1$. Note that

$$\begin{aligned}\Phi_1 &= \Phi_2\tau = \Phi_1\sigma\tau,\\ \Phi_2 &= \Phi_1\sigma = \Phi_2\tau\sigma,\end{aligned}$$

so $\tau^{-1} = \sigma$. Now we want to find $K_1^r$ and $K_2^r$, the reflex fields of $(K, \Phi_1)$ and $(K, \Phi_2)$ respectively, using Proposition 2.11.

Take $\varphi \in \mathrm{Gal}(L/K_2^r)$, then $\varphi\Phi_2 = \Phi_2$. Hence $\varphi\Phi_1\sigma = \Phi_1\sigma$ and by multiplying both sides from the right by $\tau$, we get $\varphi\Phi_1 = \Phi_1$. So $\varphi \in \mathrm{Gal}(L/K_1^r)$ hence we find that $\mathrm{Gal}(L/K_2^r) \subset \mathrm{Gal}(L/K_1^r)$. For the other inclusion take $\varphi \in \mathrm{Gal}(L/K_1^r)$, by definition we get $\varphi\Phi_1 = \Phi_1$ which implies $\varphi\Phi_2\tau = \Phi_2\tau$ and again by multiplying both sides with $\sigma$ from the right we obtain $\varphi\Phi_2 = \Phi_2$. We get that $\varphi \in \mathrm{Gal}(L/K_2^r)$ which implies $\mathrm{Gal}(L/K_1^r) \subset \mathrm{Gal}(L/K_2^r)$ and hence $\mathrm{Gal}(L/K_1^r) = \mathrm{Gal}(L/K_2^r)$. We conclude that $K_1^r = K_2^r$. □

**Proposition 2.13.** Let $K$ be a CM-field and let $\Phi$ be a CM-type of $K$. Let $L$ be the normal closure of $K$. Then the reflex type of $(K, \overline{\Phi})$ is $(K^r, \overline{\Phi^r})$.

*Proof.* Since complex conjugation $\rho$ commutes with every embedding of $K$ it follows that $\overline{\Phi} = \Phi \circ \rho|_K$ where $\rho|_K \in \mathrm{Aut}(K/\mathbb{Q})$. Then by Definition 2.8, the CM-types $\Phi$ and $\overline{\Phi}$ are equivalent. By Proposition 2.12, the reflex fields of $\Phi$ and $\overline{\Phi}$ are the same.

Let $(K^r, \Phi^r)$ be the reflex type of $(K, \Phi)$. Then by definition,

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

where $\Phi_L$ is the induced CM-type of $L$ from $\Phi$. From the explanation in Section 1.3 it follows that the induced CM-type of $L$ from $\overline{\Phi}$ is the set

$$\begin{aligned}\overline{\Phi}\,\mathrm{Gal}(L/K) &= \{\rho \circ \phi \circ \sigma \,:\, \phi \in \mathrm{Hom}(K, L) \text{ and } \sigma \in \mathrm{Gal}(L/K)\}\\ &= \{\rho \circ \phi_L \,:\, \phi_L \in \mathrm{Hom}(L, L)\}\\ &= \rho\Phi_L = \overline{\Phi}_L.\end{aligned}$$

Then $\overline{\Phi}_L^{-1} = \{\phi_L^{-1} \circ \rho \,:\, \phi_L \in \mathrm{Hom}(L, L)\} = \overline{\Phi_L^{-1}}$ and we have

$$\begin{aligned}\overline{\Phi}^r &= \{\phi|_{K^r} : \phi \in \overline{\Phi}_L^{-1}\}\\ &= \{\phi|_{K^r} : \phi \in \overline{\Phi_L^{-1}}\}\\ &= \{\phi|_{K^r} : \rho \circ \phi \in \Phi_L^{-1}\}\\ &= \rho\{\phi|_{K^r} : \phi \in \Phi_L^{-1}\}\\ &= \rho\Phi^r.\end{aligned}$$

□

## 2.2 The CM-class group

**Definition 2.14.** The *type norm* of a CM-pair $(K, \Phi)$ is the multiplicative map

$$\begin{aligned} \mathrm{N}_\Phi : K &\longrightarrow K^r \\ x &\longmapsto \prod_{\phi \in \Phi} \phi(x). \end{aligned}$$

By the definition a CM-type $\Phi$ is a set of complex embeddings $\phi$ of $K$ such that $\overline{\phi} \notin \Phi$, so we have that $\Phi$ contains a half of all the complex embeddings of $K$. The other half, namely the complex conjugates of each $\phi \in \Phi$, form another CM-type that we can denote by $\overline{\Phi}$, since it holds that $\overline{\Phi} = \rho \circ \Phi$. Hence by the definition of the norm in Section 1.4 and the type norm, for every $\alpha \in K$ the following holds:

$$\mathrm{N}_\Phi(\alpha)\, \mathrm{N}_{\overline{\Phi}}(\alpha) = \mathrm{N}_\Phi(\alpha)\overline{\mathrm{N}_\Phi(\alpha)} = \mathrm{N}_K(\alpha). \tag{2}$$

By Remark in §3 of Chapter 3 in [7] we know that the map $N_\Phi$ sends ideals to ideals, in particular principal ideals to principal ideals. Namely, if $\mathfrak{a} = (\gamma)$ for some $\gamma \in \mathcal{O}_K$ we have

$$\mathrm{N}_{\Phi^r}(\gamma \mathcal{O}_K) = \mathrm{N}_{\Phi^r}(\gamma)\mathcal{O}_{K^r}.$$

Let $K$ be a CM-field of degree $2g$ and let $\Phi$ be a primitive CM-type of $K$. Let $J(\mathcal{O}_{K^r})$ be the set of ideal classes in $\mathrm{Cl}(\mathcal{O}_{K^r})$ such that there is an ideal representative $\mathfrak{a}$ in each class $C \in \mathrm{Cl}(\mathcal{O}_{K^r})$ satisfying the following: there exists an element $\alpha \in K$ for which we have

$$\mathrm{N}_{\Phi^r}(\mathfrak{a}) = (\alpha) \text{ such that } \alpha\overline{\alpha} \in \mathbb{Q} \text{ for some } \alpha \in K. \tag{3}$$

**Lemma 2.15.** All principal ideals in $\mathcal{O}_{K^r}$ satisfies (3).

*Proof.* Let $\mathfrak{a}$ be a principal ideal in $\mathcal{O}_{K^r}$. Then there exists an element $\gamma \in \mathcal{O}_{K^r}$ such that $\mathfrak{a} = (\gamma)$. Then we have

$$\mathrm{N}_{\Phi^r}(\gamma \mathcal{O}_K) = \mathrm{N}_{\Phi^r}(\gamma)\mathcal{O}_{K^r}.$$

Then by (2), we have

$$\mathrm{N}_\Phi(\gamma)\overline{\mathrm{N}_\Phi(\gamma)} = \mathrm{N}_K(\gamma) \in \mathbb{Q}.$$

□

**Proposition 2.16.** The set $J(\mathcal{O}_{K^r})$ is a subgroup of $\mathrm{Cl}(\mathcal{O}_{K^r})$.

*Proof.* Take the ideal (1) from $[\mathcal{O}_{K^r}]$ the class of principal ideals in $\mathcal{O}_{K^r}$. Then we have that $\mathrm{N}_{\Phi^r}((1)) = 1$ because every complex embedding fixes $\mathbb{Q}$, and moreover $1 \cdot \overline{1} = 1 \in \mathbb{Q}$, we have that the identity element is in $J(\mathcal{O}_{K^r})$.

Let $C_1, C_2$ be two classes in $J(\mathcal{O}_{K^r})$. Then this means that there exist ideals $\mathfrak{a}_1$ and $\mathfrak{a}_2$ in $\mathcal{O}_{K^r}$ such that $C_1 = [\mathfrak{a}_1]$ and $C_2 = [\mathfrak{a}_2]$ satisfying

$$\begin{aligned} &\mathrm{N}_{\Phi^r}(\mathfrak{a}_1) = (\alpha_1) \text{ such that } \alpha_1\overline{\alpha}_1 \in \mathbb{Q} \text{ for some } \alpha_1 \in K, \\ &\mathrm{N}_{\Phi^r}(\mathfrak{a}_2) = (\alpha_2) \text{ such that } \alpha_2\overline{\alpha}_2 \in \mathbb{Q} \text{ for some } \alpha_2 \in K. \end{aligned}$$

Then we have

$$\begin{aligned}
\mathrm{N}_{\Phi^r}(\mathfrak{a}_1\mathfrak{a}_2) &= \prod_{\phi\in\Phi}\phi(\mathfrak{a}_1\mathfrak{a}_2)\\
&= \prod_{\phi\in\Phi}\phi(\mathfrak{a}_1)\prod_{\phi\in\Phi}\phi(\mathfrak{a}_2)\\
&= (\alpha_1)(\alpha_2)\\
&= (\alpha_1\alpha_2)
\end{aligned}$$

and since $\alpha_1\overline{\alpha_1}\in\mathbb{Q}$ and $\alpha_2\overline{\alpha_2}\in\mathbb{Q}$, also their product is in $\mathbb{Q}$.

Finally, let $[\mathfrak{a}]\in J(\mathcal{O}_{K^r})$. Then there exists $\alpha\in K$ such that

$$\mathrm{N}_{\Phi^r}(\mathfrak{a}) = (\alpha) \text{ such that } \alpha\overline{\alpha}\in\mathbb{Q}.$$

Since $\mathrm{Cl}(\mathcal{O}_{K^r})$ is a group then there exists $[\mathfrak{b}]\in\mathrm{Cl}(\mathcal{O}_{K^r})$ such that $[\mathfrak{a}\mathfrak{b}]=[\mathcal{O}_{K^r}]$. Then this means that there is a $\gamma\in\mathcal{O}_{K^r}$ such that $\mathfrak{a}\mathfrak{b}=(\gamma)$. Then we have

$$\mathrm{N}_{\Phi^r}(\gamma\mathcal{O}_{K^r}) = \mathrm{N}_{\Phi^r}(\mathfrak{a}\mathfrak{b}) = \prod_{\phi\in\Phi}\phi(\mathfrak{a})\prod_{\phi\in\Phi}\phi(\mathfrak{b}) = (\alpha)\,\mathrm{N}_{\Phi^r}(\mathfrak{b}).$$

Thus, we have $\mathrm{N}_{\Phi^r}(\mathfrak{b}) = \frac{1}{\alpha}(\xi) = (\frac{1}{\alpha}\xi)$ where $\mathrm{N}_{\Phi^r}(\gamma\mathcal{O}_{K^r}) = (\xi)$ and $\mathrm{N}_{\Phi^r}(\gamma) = \xi\in\mathcal{O}_K$. Moreover, by the property (2), we have $\xi\overline{\xi}\in\mathbb{Q}$. Then we get

$$(\alpha^{-1}\xi)(\overline{\alpha}^{-1}\overline{\xi}) = (\alpha\overline{\alpha})^{-1}\xi\overline{\xi}\in\mathbb{Q}$$

as $\alpha\overline{\alpha}$ and $\xi\overline{\xi}$ in $\mathbb{Q}$. □

By Corollary 1.31, the class group $\mathrm{Cl}(\mathcal{O}_{K^r})$ is an abelian group so $J(\mathcal{O}_{K^r})$ is an abelian subgroup so $J(\mathcal{O}_{K^r})$ is normal and therefore the quotient $\mathrm{Cl}(\mathcal{O}_{K^r})/J(\mathcal{O}_{K^r})$ is a group.

**Definition 2.17.** The quotient group $\mathcal{C}(\mathcal{O}_{K^r}) := \mathrm{Cl}(\mathcal{O}_{K^r})/J(\mathcal{O}_{K^r})$ is called the *CM-class group* of $(K,\Phi)$.

**Remark 2.18.** Since $\mathrm{Cl}(\mathcal{O}_{K^r})$ and $J(\mathcal{O}_{K^r})$ are finite, the group $\mathcal{C}(\mathcal{O}_{K^r})$ is finite.

A generalization of the *Gauss class number one problem* is the *CM-class number one problem.* This problem asks for which CM-fields of degree $2g$ the CM-class group $\mathcal{C}(\mathcal{O}_{K^r})$ is trivial, i.e. when $\#\mathcal{C}(\mathcal{O}_{K^r})=1$ (in this case we say that $(K,\Phi)$ has *CM-class number one*). This problem corresponds to the class number one problem for the imaginary quadratic number fields, that was introduced in the previous section. For quartic CM-fields it was solved by Kılıçer and Streng (2015) [5] but for sextic CM-fields it has only been solved partially by Kılıçer (2016) [6].

**Theorem 2.19.** (Proposition 2.1 in [2]) Let $K$ be a sextic CM-field, and let $G$ be the Galois group of the Galois closure of $K/\mathbb{Q}$. Then $G$ is one of the following groups:

1. $C_2 \times C_3 \cong C_6$
2. $C_2 \times S_3 \cong D_{12}$
3. $(C_2)^3 \rtimes G_+$ with $G_+ \in \{C_3, S_3\}$ where $\rtimes$ denotes the semi-direct product of groups, so $G_+$ is acting by permutations on the three copies of $C_2$.

The CM-class number one problem was solved by Kılıçer for the first two cases. We will therefore restrict ourselves to the third case, for which the CM-class number one problem is still open.

# 3 Sextic CM-fields and their reflex fields

In this section we assume that $K$ is a sextic CM-field with $L$ the normal closure of $K$. In Theorem 2.19 we saw that there are 3 cases for what $\mathrm{Gal}(L/\mathbb{Q})$ can be isomorphic to. In the first case $K = L$, because $K$ is normal over $\mathbb{Q}$ and in the second case, we have $K/\mathbb{Q}$ is not normal but $K$ contains an imaginary quadratic subfield [2]. We will restrict ourselves to the third case, where $K/\mathbb{Q}$ is not normal and $K$ does not contain any imaginary quadratic subfield [2]. The goal of this section is to find the reflex fields and reflex types of $(K, \Phi)$ for every CM-type $\Phi$. For that we will first determine all the complex embeddings of $K$, then all its CM-types which will help us compute the reflex pairs $(K^r, \Phi^r)$ of $(K, \Phi)$.

## 3.1 Sextic CM-fields with Galois group $G = (C_2)^3 \rtimes C_3$

### 3.1.1 The group $G = (C_2)^3 \rtimes C_3$

Let $(C_2)^3 = \langle a, b, c \,:\, a^2 = b^2 = c^2 = 1,\, ab = ba,\, ac = ca,\, bc = cb\rangle$ and similarly let $C_3 = \langle x \,:\, x^3 = 1\rangle$. The group $C_3$ acts on $(C_2)^3$ by

$$x \cdot a = b, \quad x \cdot b = c \quad \text{and} \quad x \cdot c = a.$$

This action induces the following automorphism of $(C_2)^3$

$$\begin{aligned} x : (C_2)^3 &\longrightarrow (C_2)^3 \\ a &\longmapsto b \\ b &\longmapsto c \\ c &\longmapsto a. \end{aligned}$$

Let $\varphi$ be the homomorphism from $C_3$ to $\mathrm{Aut}((C_2)^3)$ sending $x$ to the induced automorphism, i.e,

$$\begin{aligned} \varphi : C_3 &\longrightarrow \mathrm{Aut}((C_2)^3) \\ x &\longmapsto \begin{Bmatrix} a \mapsto b \\ b \mapsto c \\ c \mapsto a \end{Bmatrix}. \end{aligned}$$

By Theorem 10 in §5.5 [3] the set $G$ of ordered pairs $(r, t)$ with $r \in (C_2)^3$ and $t \in C_3$ is a group with respect to the multiplication

$$(r_1, t_1)(r_2, t_2) = (r_1\varphi(t_1)(r_2), t_1t_2). \tag{4}$$

In the group $G$, we have $(1, x)(r, 1)(1, x)^{-1} = (\varphi(x)(r), 1)$ for all $r \in (C_2)^3$. By identifying $(1, x)$ with $x$ and $(r, 1)$ with $r \in \{a, b, c\}$ via isomorphisms $C_3 \to \{(1, t) : t \in C_3\}$ and $(C_2)^3 \to \{(r, 1) : r \in (C_2)^3\}$, respectively, we can present the group $G$ by

$$\begin{aligned} G = \langle a, b, c, x \,:\, & a^2 = b^2 = c^2 = x^3 = 1,\ ab = ba,\ ac = ca,\ bc = cb, \\ & xax^{-1} = b,\ xbx^{-1} = c,\ xcx^{-1} = a\rangle, \\ = \langle a, b, c, x \,:\, & a^2 = b^2 = c^2 = x^3 = 1,\ ab = ba,\ ac = ca,\ bc = cb, \\ & ax = xc,\ bx = xa,\ cx = xb\rangle. \end{aligned}$$

The group $G$ is a non-abelian group of order $\#(C_2)^3 \cdot \#C_3 = 24$. The subgroup $(C_2)^3$ is normal in $G$ since $xax^{-1} = b$, $xbx^{-1} = c$ and $xcx^{-1} = a$. Note that the elements of $G$ are the same elements as of $(C_2)^3 \times C_3$, but the multiplications of elements on $G$ differs from the one in $(C_2)^3 \times C_3$.

**Lemma 3.1.** The center of $G$ is $\langle abc\rangle$.

*Proof.* By the definition, the centre of the group $G$ is

$$Z(G) := \{g \in G : zg = gz\}.$$

First we want to show that 1 and $abc$ commute with every element of $G$. By definition, we know that 1 commutes with every element of $G$, so $1 \in Z(G)$. Now, an element $g \in G$ can be written in the form $g = a^{e_1}b^{e_2}c^{e_3}x^i$, then we have three cases: $i = 0, 1, 2$.

If $i = 0$ then

$$(abc)(a^{e_1}b^{e_2}c^{e_3}) = a^{e_1}b^{e_2}c^{e_3}abc,$$

since $a, b, c$ commute with each other. If $i = 1$ then we get

$$\begin{aligned} (abc)(a^{e_1}b^{e_2}c^{e_3}x) &= a^{e_1}b^{e_2}c^{e_3}abcx \\ &= a^{e_1}b^{e_2}c^{e_3}xcab \\ &= (a^{e_1}b^{e_2}c^{e_3}x)(abc). \end{aligned}$$

And finally, if $i = 2$ then

$$\begin{aligned}(abc)(a^{e_1}b^{e_2}c^{e_3}x^2) &= a^{e_1}b^{e_2}c^{e_3}abcx^2 \\ &= a^{e_1}b^{e_2}c^{e_3}x^2bca \\ &= (a^{e_1}b^{e_2}c^{e_3}x^2)(abc).\end{aligned}$$

Secondly, we will show that no other element than 1 and $abc$ commutes with all elements of $G$. By the definition of $G$ we get $a, b, c, x, ax, bx, cx \notin Z(G)$. Similarly, we know $ax^2 = x^2b$, $bx^2 = x^2c$ and $cx^2 = x^2a$, so also $x^2, ax^2, bx^2, cx^2 \notin Z(G)$. Moreover, we get $ab, bc, ca, abx, bcx, cax, abx^2, bcx^2, cax^2 \notin Z(G)$ since for these elements it holds that $abx^2 = x^2bc$, $bcx^2 = x^2ca$, and $cax^2 = x^2ab$. Finally, $abcx, abcx^2 \notin Z(G)$ since we have $a(abcx) = xba$ and $a(abcx^2) = x^2ca$. From this we can conclude that the center of $G$ is $Z(G) = \langle abc \rangle$. □

**Definition 3.2.** The group $G$ described in this section is called the *semi-direct product* of groups $(C_2)^3$ and $C_3$ with respect to $\varphi$ and is commonly denoted by $G = (C_2)^3 \rtimes_\varphi C_3$. For simplicity, we will be writing $G = (C_2)^3 \rtimes C_3$.

### 3.1.2 Intermediate extensions of $L/\mathbb{Q}$

Assume that $\mathrm{Gal}(L/\mathbb{Q}) \cong (C_2)^3 \rtimes C_3$. Since $\#\,\mathrm{Gal}(L/\mathbb{Q}) = [L : \mathbb{Q}] = 24$, by the tower law, the Galois extension $L/K$ is of degree 4 since $[K : \mathbb{Q}] = 6$ by definition. See the orders of these extensions over $\mathbb{Q}$ in Figure 2.

Let us denote the totally real cubic intermediate field extension $\mathbb{Q} \subset K_+ \subset K$. Let $\delta \in K_+ \setminus \mathbb{Q}$ be a totally positive element such that $K = K_+(\sqrt{-\delta})$ and let

$$\delta_0 := \delta,\ \delta_1 := x(\delta_0),\ \delta_2 := x^2(\delta_0).$$

The extension $N := K_+(\sqrt{-\delta_0}, \sqrt{-\delta_1}, \sqrt{-\delta_2}) = K(\sqrt{-\delta_1}, \sqrt{-\delta_2})$ is a subfield of $L$. Since $\delta_i$'s are distinct, the extension $N/K_+$ is of degree 8. However, since $[L : K_+] = 8$, we get $L = N = K_+(\sqrt{-\delta_0}, \sqrt{-\delta_1}, \sqrt{-\delta_2})$ with

$$1 \to \mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{Gal}(L/K_+) \to \mathrm{Gal}(K_+/\mathbb{Q}) \to 1$$

where $\mathrm{Gal}(K_+/\mathbb{Q}) \cong C_3$ and $\mathrm{Gal}(L/K_+) \cong (C_2)^3$ (Lemma 2.2 in [2]). Recall that $(C_2)^3$ is a normal subgroup of $(C_2)^3 \rtimes C_3$, which by Galois correspondence implies that $K_+/\mathbb{Q}$ is Galois. Hence we get that $\delta_0, \delta_1, \delta_2 \in K_+$.

**Lemma 3.3.** The number fields $K = K_+(\sqrt{-\delta_0})$, $K_+(\sqrt{-\delta_1})$ and $K_+(\sqrt{-\delta_2})$ are isomorphic to each other.

*Proof.* Using the automorphism $x \in G$ we have that

$$\begin{aligned} x^i : K_+(\sqrt{\delta_0}) &\longrightarrow K_+(\sqrt{\delta_i}) \\ \sqrt{-\delta_0} &\longmapsto \sqrt{-\delta_i}. \end{aligned}$$

Note that this is a homomorphism of fields since $K_+(\sqrt{-\delta_i}) \subset L$ and $\mathrm{Aut}(L/\mathbb{Q}) = G$. Since there exists an inverse map

$$\begin{aligned} x^{3-i} : K_+(\sqrt{\delta_{3-i}}) &\longrightarrow K_+(\sqrt{\delta_0}) \\ \sqrt{-\delta_{3-i}} &\longmapsto \sqrt{-\delta_i}, \end{aligned}$$

such that $x^i x^{3-i} = x^3 = 1$, we have that $x^i$ is an isomorphism of fields. Hence

$$(K_+(\sqrt{-\delta_0})) \cong K_+(\sqrt{-\delta_1}) \cong K_+(\sqrt{-\delta_2}).$$

□

$$\begin{tikzcd}
 & & L \arrow[dl, dash, "4"'] \arrow[d, dash, "4"] \arrow[dr, dash, "4"] & & \\
K = K_+(\sqrt{-\delta_0}) \arrow[rr, dash, "\sim"] \arrow[dr, dash, "2"] \arrow[ddr, dash, "6"'] & & K_+(\sqrt{-\delta_1}) \arrow[rr, dash, "\sim"] \arrow[d, dash, "2"] & & K_+(\sqrt{-\delta_2}) \arrow[dl, dash, "2"] \\
 & & K_+ \arrow[d, dash, "3"] & & \\
 & & \mathbb{Q} & &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & & \langle 1 \rangle \arrow[dl, dash, "4"'] \arrow[d, dash, "4"] \arrow[dr, dash, "4"] & & \\
\langle b, c \rangle \arrow[rr, dash, "\sim"] \arrow[dr, dash, "2"] \arrow[ddr, dash, "6"'] & & \langle a, c \rangle \arrow[rr, dash, "\sim"] \arrow[d, dash, "2"] & & \langle a, b \rangle \arrow[dl, dash, "2"] \\
 & & \langle a, b, c \rangle \arrow[d, dash, "3"] & & \\
 & & \langle a, b, c, x \rangle & &
\end{tikzcd}$$

Figure 2: Sublattices of subfields of $L$ and of subgroups of $\mathrm{Gal}(L/\mathbb{Q})$

### 3.1.3 Complex embeddings of $L$

In this section we will find all the complex embeddings of $L$. We know that $L \subset \mathbb{C}$ and $L/\mathbb{Q}$ is Galois so we can identify the complex embeddings of $L$ with the automorphisms of $L$. Let us therefore examine the Galois group of $L/\mathbb{Q}$.

We will now explicitly write the complex embeddings corresponding to the generator automorphisms $a, b, c, x$ of $\mathrm{Gal}(L/\mathbb{Q})$. Note that it is enough to write the images of $\sqrt{-\delta_0}, \sqrt{-\delta_1}, \sqrt{-\delta_2}$, because by Lemma 1.13 every field homomorphism fixes $\mathbb{Q}$ and since $L = K_+(\sqrt{-\delta_0}, \sqrt{-\delta_1}, \sqrt{-\delta_2})$ and $K_+ = \mathbb{Q}(\delta_0, \delta_1, \delta_2)$, by permuting these we automatically permute $\delta_0, \delta_1, \delta_2$. Since $x$ fixes the field $K_+$ we will write the images of $\delta_0, \delta_1, \delta_2$ for this automorphism.

$$\begin{aligned} a : L &\longrightarrow L \subset \mathbb{C} \\ \sqrt{-\delta_0} &\longmapsto -\sqrt{-\delta_0} \\ \sqrt{-\delta_1} &\longmapsto \sqrt{-\delta_1} \\ \sqrt{-\delta_2} &\longmapsto \sqrt{-\delta_2}, \end{aligned} \qquad \begin{aligned} b : L &\longrightarrow L \subset \mathbb{C} \\ \sqrt{-\delta_0} &\longmapsto \sqrt{-\delta_0} \\ \sqrt{-\delta_1} &\longmapsto -\sqrt{-\delta_1} \\ \sqrt{-\delta_2} &\longmapsto \sqrt{-\delta_2}, \end{aligned} \qquad \begin{aligned} c : L &\longrightarrow L \subset \mathbb{C} \\ \sqrt{-\delta_0} &\longmapsto \sqrt{-\delta_0} \\ \sqrt{-\delta_1} &\longmapsto \sqrt{-\delta_1} \\ \sqrt{-\delta_2} &\longmapsto -\sqrt{-\delta_2}, \end{aligned}$$

$$\begin{aligned} x : L &\longrightarrow L \subset \mathbb{C} \\ \delta_0 &\longmapsto \delta_1 \\ \delta_1 &\longmapsto \delta_2 \\ \delta_2 &\longmapsto \delta_0. \end{aligned}$$

The generators $b, c$ are fixing $K$ elementwise, i.e, fixing $\delta_0$, hence we get

$$\mathrm{Gal}(L/K) = \langle b, c \rangle.$$

Since $a, b, c, x$ are the generators of $\mathrm{Gal}(L/\mathbb{Q})$, we get 24 complex embeddings of $L$ by combining these generators. For example, the embedding $ax$ is given as

$$\begin{aligned} ax : \quad & \sqrt{-\delta_0} \longmapsto -\sqrt{-\delta_1}, \\ & \sqrt{-\delta_1} \longmapsto \sqrt{-\delta_2}, \\ & \sqrt{-\delta_2} \longmapsto \sqrt{-\delta_0}. \end{aligned}$$

Note that $ax = xc \neq xa = bx$. The embedding $xa$ looks as follows

$$\begin{aligned} xa : \quad & \sqrt{-\delta_0} \longmapsto \sqrt{-\delta_1}, \\ & \sqrt{-\delta_1} \longmapsto -\sqrt{-\delta_2}, \\ & \sqrt{-\delta_2} \longmapsto \sqrt{-\delta_0}. \end{aligned}$$

**Proposition 3.4.** The element $\rho = abc$ corresponds to complex conjugation on $L$.

*Proof.* By Proposition 2.2, complex conjugation commutes with every embedding of $L$, hence with every element of $\mathrm{Gal}(L/\mathbb{Q})$. So the corresponding automorphism is in the center of $G = \mathrm{Gal}(L/\mathbb{Q})$. Then by Lemma 3.1, we get $\rho = abc$ since complex conjugation is of order 2. □

We denote the complex conjugation by $\rho$ and if $\phi$ is an embedding of $L$ then we denote by the *complex conjugate* of $\phi$ by $\overline{\phi}$, where $\overline{\phi} := \phi \circ \rho$, which is the same as $\rho \circ \phi$.

$$\begin{aligned} \rho : \quad & \sqrt{-\delta_0} \longmapsto -\sqrt{-\delta_0}, \\ & \sqrt{-\delta_1} \longmapsto -\sqrt{-\delta_1}, \\ & \sqrt{-\delta_2} \longmapsto -\sqrt{-\delta_2}. \end{aligned}$$

### 3.1.4 Complex embeddings and CM-types of $K$

In this section we will find all complex embeddings of $K$ and then compute the CM-types of $K$. Since we have $[K : \mathbb{Q}] = 6$, there are 6 complex embeddings of $K$. These embeddings are totally complex since $K$ is a CM-field. Recall that totally complex embeddings come in pairs, so we can denote them by $\varphi_1, \varphi_2, \varphi_3, \overline{\varphi}_1, \overline{\varphi}_2, \overline{\varphi}_3$.

**Proposition 3.5.** The set $S = \{1_{|_K}, x_{|_K}, x^2_{|_K}, \rho_{|_K}, \rho x_{|_K}, \rho x^2_{|_K}\}$ contains all complex embeddings of $K$.

*Proof.* In Section 1.3 we have shown that if $\phi$ is a complex embedding of $K$ and we take $\sigma \in \mathrm{Gal}(L/K)$ we can extend the set of complex embeddings of $K$ to $L$ using $\phi \circ \sigma$. We have that $\mathrm{Gal}(L/K) = \langle b, c\rangle$, so to prove that $S$ contains all complex embeddings of $K$ we will show that $\langle b, c\rangle S = G$.

Take $1 \in \mathrm{Gal}(L/K)$. Since $\rho_{|_K} = a$, then we have

$$1S = 1\{1_{|_K}, x_{|_K}, x^2_{|_K}, \rho_{|_K}, \rho x_{|_K}, \rho x^2_{|_K}\} = \{1, x, x^2, a, ax, ax^2\}.$$

Similarly for $b, c, bc \in \mathrm{Gal}(L/K)$, we get

$$bS = \{b, bx, bx^2, ab, abx, abx^2\},$$

$$cS = \{c, cx, cx^2, ac, acx, acx^2\},$$

and

$$bcS = \{bc, bcx, bcx^2, abc, abcx, abcx^2\}.$$

Adding the elements of these four sets together we obtain all the elements of $G$. We conclude that $\langle b, c\rangle S = G$, so the set $S$ contains all complex embeddings of $K$. □

For simplicity, we will denote the complex embeddings of $K$ as follows

$$\begin{array}{lll} \varphi_1 = 1_{|_K}, & \varphi_2 = x_{|_K} & \varphi_3 = x^2{}_{|_K} \\ \overline{\varphi}_1 = \rho_{|_K}, & \overline{\varphi}_2 = \rho x_{|_K}, & \overline{\varphi}_3 = \rho x^2_{|_K}. \end{array}$$

Now we will construct the CM-types of $K$. Note that in each CM-type there are 3 elements, because it does not contain 2 elements that are complex conjugates of each other. We obtain $2^3 = 8$ CM-types:

$$\{\varphi_1, \varphi_2, \varphi_3\}, \{\overline{\varphi}_1, \varphi_2, \varphi_3\}, \{\varphi_1, \overline{\varphi}_2, \varphi_3\}, \{\varphi_1, \varphi_2, \overline{\varphi}_3\},$$
$$\{\overline{\varphi}_1, \overline{\varphi}_2, \overline{\varphi}_3\}, \{\varphi_1, \overline{\varphi}_2, \overline{\varphi}_3\}, \{\overline{\varphi}_1, \varphi_2, \overline{\varphi}_3\}, \{\overline{\varphi}_1, \overline{\varphi}_2, \varphi_3\}.$$

The following theorem will be used in showing that the only field automorphisms of $K$ are $1_{|_K}$ and $\rho_{|_K}$. This result will be helpful in finding the equivalence of CM-types.

**Theorem 3.6.** (Theorem 9 in §14.2 [3]) Let $K$ be a field and let $G \leq \mathrm{Aut}(K/\mathbb{Q})$ be a subgroup of the group of automorphisms of $K$. Let $F$ be the fixed field $F = K^G$. Then

$$[K : F] = \#G.$$

**Proposition 3.7.** The only field automorphisms of $K$ are $1_{|_K}$ and $\rho_{|_K}$.

*Proof.* We have $[K:\mathbb{Q}]=6$ so the group of automorphisms of $K$ has $\#\operatorname{Aut}(K/\mathbb{Q})\leq 6$. Note that the identity $1_{|_K}$ and the complex conjugation $\rho_{|_K}$ are in $\operatorname{Aut}(K/\mathbb{Q})$, so it has already at least 2 elements. If $\operatorname{Aut}(K/\mathbb{Q})$ is of order 6, then this would imply that $K/\mathbb{Q}$ is Galois, which is a contradiction. We also know that $\#\operatorname{Aut}(K/\mathbb{Q})\neq 3$ or 5, because these subgroups do not contain an element of order 2. So $\#\operatorname{Aut}(K/\mathbb{Q})=2$ or 4.

Now assume $F=K^{\operatorname{Aut}(K/\mathbb{Q})}$ where $\#\operatorname{Aut}(K/\mathbb{Q})=4$. Then also $[F:K]=4$ (using Theorem 3.6) but here we arrive to a contradiction, because $[K:F]=4$ must divide the degree $[K:\mathbb{Q}]=6$ by the tower law, but this does not hold. Hence $\#\operatorname{Aut}(K/\mathbb{Q})=2$, which means the only $K$-automorphisms are $1_{|_K}$ and $\rho_{|_K}$. □

Since the only non-trivial automorphism of $K$ is $\rho_{|_K}$, by Definition 2.8 each CM-type $\Phi$ is only equivalent to its complex conjugate $\overline{\Phi}:=\{\overline{\phi}\,:\,\phi\in\Phi\}$. Thus, we get the following:

$$\begin{aligned}
\Phi_1&=\{\varphi_1,\varphi_2,\varphi_3\}\sim\{\overline{\varphi}_1,\overline{\varphi}_2,\overline{\varphi}_3\}=\overline{\Phi}_1,\\
\Phi_2&=\{\overline{\varphi}_1,\varphi_2,\varphi_3\}\sim\{\varphi_1,\overline{\varphi}_2,\overline{\varphi}_3\}=\overline{\Phi}_2,\\
\Phi_3&=\{\varphi_1,\overline{\varphi}_2,\varphi_3\}\sim\{\overline{\varphi}_1,\varphi_2,\overline{\varphi}_3\}=\overline{\Phi}_3,\\
\Phi_4&=\{\varphi_1,\varphi_2,\overline{\varphi}_3\}\sim\{\overline{\varphi}_1,\overline{\varphi}_2,\varphi_3\}=\overline{\Phi}_4.
\end{aligned}$$

**Proposition 3.8.** All the CM-types mentioned above are primitive.

*Proof.* We want to show that there is no CM-subfield of $K$, which then by definition implies that no CM-type is induced and hence they are all primitive.

Assume for contradiction that there exists an intermediate extension $\mathbb{Q}\subset N\subset K$, such that $N$ is totally imaginary quadratic field over $\mathbb{Q}$, i.e., a CM-subfield of $K$. This implies that $N/\mathbb{Q}$ is Galois because all quadratic field extensions are normal. But as mentioned in Section 3.1.2, $K_+/\mathbb{Q}$ is also Galois. The field $NK_+$ must hence be Galois over $\mathbb{Q}$ by Lemma 1.6 and moreover it is a subfield of $K$ since both $N\subset K$ and $K_+\subset K$.

As $[K_+:\mathbb{Q}]=3$ and $[N:\mathbb{Q}]=2$, we get $[NK_+:\mathbb{Q}]=6$ and that implies $K=NK_+$. However, $K/\mathbb{Q}$ is not Galois over $\mathbb{Q}$ whereas $NK_+$ is, so we get a contradiction. □

### 3.1.5 Reflex fields

Finally, we will find the reflex types $(K^r,\Phi^r)$ of $(K,\Phi)$ for $K$ and each of its CM-types $\Phi$. By Proposition 2.12 and Proposition 2.13 it follows that if $\Phi$ is a CM-type of $K$ with the reflex type $(K^r,\Phi^r)$, then $\overline{\Phi}$ has the reflex type $(K^r,\overline{\Phi^r})$. Hence we only need to consider the following 4 cases:

$$\Phi_1=\{\varphi_1,\varphi_2,\varphi_3\},\ \Phi_2=\{\overline{\varphi}_1,\varphi_2,\varphi_3\},\ \Phi_3=\{\varphi_1,\overline{\varphi}_2,\varphi_3\},\ \Phi_4=\{\varphi_1,\varphi_2,\overline{\varphi}_3\}\tag{5}$$

Take a CM-type $\Phi$ of $K$. In order to find the reflex of $(K,\Phi)$ we will follow the explanation in Section 2.1. We have that $\operatorname{Gal}(L/K)=\langle b,c\rangle=\{1,b,c,bc\}$. Using $\operatorname{Gal}(L/K)$ we can get the set of induced embeddings of $\Phi$ denoted by $\Phi_L$, by computing

$$\Phi_L=\Phi\operatorname{Gal}(L/K).\tag{6}$$

Firstly, finding this set is useful because then by Proposition 2.11 we get $\mathrm{Gal}(L/K^r)$ from which we can determine $K^r$. Secondly, we want to find $\Phi^r$. Since each embedding in $\Phi_L$ is an isomorphism we can determine the set of inverses of the embeddings in $\Phi_L$ denoted by $(\Phi_L)^{-1}$. Finally by computing

$$(\Phi_L)^{-1}(\mathrm{Gal}(L/K^r))^{-1} = (\Phi_L)^{-1}_{|_{K^r}}, \tag{7}$$

which follows from (6), we obtain $\Phi^r = (\Phi_L)^{-1}_{|_{K^r}}$.

**Theorem 3.9.** Let $K$ be a sextic CM-field and let $L$ be the normal closure of $K$ such that $\mathrm{Gal}(L/\mathbb{Q}) = (C_2)^3 \rtimes C_3$. Let $\Phi$ be a CM-type of $K$ with values in $L$. The reflex types of $(K, \Phi)$ are

$$\begin{aligned}
(K_1^r, \Phi_1^r) &= (L^{\langle x\rangle}, \langle b, c\rangle) & (K_5^r, \Phi_5^r) &= (L^{\langle x\rangle}, \rho\langle b, c\rangle)\\
(K_2^r, \Phi_2^r) &= (L^{\langle xac\rangle}, \rho\langle b, c\rangle) & (K_6^r, \Phi_6^r) &= (L^{\langle xac\rangle}, \langle b, c\rangle)\\
(K_3^r, \Phi_3^r) &= (L^{\langle xab\rangle}, \langle b, c\rangle) & (K_7^r, \Phi_7^r) &= (L^{\langle xab\rangle}, \rho\langle b, c\rangle)\\
(K_4^r, \Phi_4^r) &= (L^{\langle xbc\rangle}, \langle b, c\rangle) & (K_8^r, \Phi_8^r) &= (L^{\langle xbc\rangle}, \rho\langle b, c\rangle).
\end{aligned}$$

Moreover, these reflex fields are isomorphic.

*Proof.* We will consider each of the 4 cases mentioned in (5) separately.

**The reflex of $(K, \Phi_1)$**
We first consider $\Phi_1 = \{1_{|_K}, x_{|_K}, x^2_{|_K}\}$. The CM-type induced by $\Phi_1$ on $L$ is

$$\begin{aligned}
\Phi_{1,L} &= \Phi_1\,\mathrm{Gal}(L/K)\\
&= \Phi_1\{1, b, c, bc\}\\
&= \{1, x, x^2, b, xb, x^2b, c, xc, x^2c, bc, xbc, x^2bc\}.
\end{aligned}$$

We will first compute $K_1^r$ using Proposition 2.11. We want to find the elements of $\mathrm{Gal}(L/K_1^r)$, which are the elements $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ such that

$$\sigma\Phi_{1,L} = \Phi_{1,L}. \tag{8}$$

Note that $\sigma$ has to be contained in $\Phi_{1,L}$ since $1 \in \Phi_{1,L}$ so we only check the elements contained in $\Phi_{1,L}$. First we will show that the elements $b, xb, x^2b$ do not satisfy the criterion in (8). We have

$$\begin{aligned}
&bx \in b\Phi_{1,L} \text{ but } bx = xa \notin \Phi_{1,L},\\
&xbx \in xb\Phi_{1,L} \text{ but } xbx = x^2a \notin \Phi_{1,L},\\
&x^2bx \in x^2b\Phi_{1,L} \text{ but } x^2bx = a \notin \Phi_{1,L}.
\end{aligned}$$

Similarly, for the elements $c, xc, x^2c$ we get

$$\begin{aligned}
&cx^2 \in c\Phi_{1,L} \text{ but } cx^2 = x^2a \notin \Phi_{1,L},\\
&xcx^2 \in xc\Phi_{1,L} \text{ but } xcx^2 = a \notin \Phi_{1,L},\\
&x^2cx^2 \in x^2c\Phi_{1,L} \text{ but } x^2cx^2 = xa \notin \Phi_{1,L}.
\end{aligned}$$

Finally, for $bc, xbc, x^2bc$ we have

$$\begin{aligned}
&bcx \in bc\Phi_{1,L} \text{ but } bcx = xab \notin \Phi_{1,L},\\
&xbcx \in xbc\Phi_{1,L} \text{ but } xbcx = x^2ab \notin \Phi_{1,L},\\
&x^2bcx \in x^2bc\Phi_{1,L} \text{ but } x^2bcx = ab \notin \Phi_{1,L}.
\end{aligned}$$

Therefore for any $\sigma \in \{b, xb, x^2b, c, xc, x^2c, bc, xbc, x^2bc\}$ we have that $\sigma\Phi_{1,L} \neq \Phi_{1,L}$, so then $\sigma \notin \mathrm{Gal}(L/K_1^r)$. Now we will show that the elements $1, x, x^2$ do satisfy the criterion in (8). For the element 1 it of course holds that $1\Phi_{1,L} = \Phi_{1,L}$ by the definition of the identity element. Now, for $x, x^2$ we get that

$$x\Phi_{1,L} = \{x, x^2, 1, xb, x^2b, b, xc, x^2c, c, xbc, x^2bc, bc\} = \Phi_{1,L}$$

$$x^2\Phi_{1,L} = \{x^2, 1, x, x^2b, b, xb, x^2c, c, xc, x^2bc, bc, xbc\} = \Phi_{1,L}.$$

We conclude that $\mathrm{Gal}(L/K_1^r) = \langle x \rangle$. Hence $K_1^r = L^{\langle x \rangle}$.

Now we will find the reflex CM-type $\Phi_1^r$ of $(K, \Phi_1)$. For this we need to determine the set of inverse maps in $\Phi_{1,L}$ denoted by $(\Phi_{1,L})^{-1}$ and then find $\Phi_1^r = (\Phi_{1,L})^{-1}_{|K^r}$. We have that

$$(\Phi_{1,L})^{-1} = \{1, x^2, x, b, bx^2, bx, c, cx^2, cx, bc, bcx^2, bcx\}.$$

Since $\langle x \rangle$ fixes $K_1^r$ elementwise and $\Phi_1^r = (\Phi_{1,L})^{-1}_{|K_1^r}$, we get that $\Phi_1^r = \{1, b, c, bc\}$. We obtain the following reflex type of $(K, \Phi_1)$

$$(K^r, \Phi_1^r) = (L^{\langle x \rangle}, \langle b, c \rangle).$$

**The reflex of** $(K, \Phi_2)$

Now we consider $\Phi_2 = \{\rho_{|K}, x_{|K}, x^2_{|K}\}$. Similarly, extending $\Phi_2$ to $L$ gives us the following

$$\begin{aligned}
\Phi_{2,L} &= \Phi_2 \,\mathrm{Gal}(L/K)\\
&= \Phi_2\{1, b, c, bc\}\\
&= \{\rho, x, x^2, \rho b, xb, x^2b, \rho c, xc, x^2c, \rho bc, xbc, x^2bc\}\\
&= \{abc, x, x^2, ac, xb, x^2b, ab, xc, x^2c, a, xbc, x^2bc\}.
\end{aligned}$$

Again, by using Proposition 2.11 we will compute $\mathrm{Gal}(L/K_2^r)$ in order to find the reflex field $K_2^r$ of $(K, \Phi_2)$. Note that since the element $\rho \in \Phi_{2,L}$ and we are searching for all $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\sigma\Phi_{2,L} = \Phi_{2,L}$, we find that $\sigma\rho \in \Phi_{2,L}$ hence $\sigma \in \overline{\Phi}_{2,L}$ where

$$\overline{\Phi}_{2,L} = \{1, xabc, x^2abc, b, xac, x^2ac, c, xab, x^2ab, bc, xa, x^2a\}.$$

We will therefore only consider the elements of $\overline{\Phi}_{2,L}$. We begin with showing that the elements $b, c, bc$ do not satisfy (8), because

$$\begin{aligned}
&bx \in b\Phi_{2,L} \text{ but } bx = ax \notin \Phi_{2,L}\\
&cx^2 \in c\Phi_{2,L} \text{ but } cx^2 = x^2a \notin \Phi_{2,L}\\
&bcx \in bc\Phi_{2,L} \text{ but } bcx = xab \notin \Phi_{2,L}.
\end{aligned}$$

Similarly, for the elements $xabc, x^2abc, x^2ac, xab, xa, x^2a$ we have

$$\begin{aligned}
&xabcx \in xabc\Phi_{2,L} \text{ but } xabcx = x^2abc \notin \Phi_{2,L}\\
&x^2abcx^2 \in x^2abc\Phi_{2,L} \text{ but } x^2abcx^2 = xabc \notin \Phi_{2,L}\\
&x^2acx \in x^2ac\Phi_{2,L} \text{ but } x^2acx = bc \notin \Phi_{2,L}\\
&xabx \in xab\Phi_{2,L} \text{ but } xabx = x^2ac \notin \Phi_{2,L}\\
&xax^2 \in xa\Phi_{2,L} \text{ but } xax^2 = b \notin \Phi_{2,L}\\
&x^2ax \in x^2a\Phi_{2,L} \text{ but } x^2ax = c \notin \Phi_{2,L}.
\end{aligned}$$

Now we will show that $1, xac, x^2ab$ satisfy the criterion in (8). For 1 it holds by definition that $1\Phi_{2,L} = \Phi_{2,L}$. For $xac, x^2ab$ we get that

$$xac\Phi_{2,L} = \{xb, x^2bc, ab, x, x^2c, a, xbc, x^2b, abc, xc, x^2, ac\} = \Phi_{2,L}$$

$$x^2ab\Phi_{2,L} = \{x^2c, ac, xbc, x^2bc, abc, xc, x^2, a, xb, x^2b, ab, x\} = \Phi_{2,L}.$$

Hence we get that $\mathrm{Gal}(L/K^r) = \langle xac\rangle$, so $K_2^r = L^{\langle xac\rangle}$. In order to find the reflex CM-type $\Phi_2^r$ we need to determine $(\Phi_{2,L})^{-1}$ and then $\Phi_2^r = (\Phi_{2,L})^{-1}_{|_{K_2^r}}$. We have that

$$(\Phi_{2,L})^{-1} = \{abc, x^2, x, ac, bx^2, bx, ab, cx^2, cx, a, bcx^2, bcx\}.$$

By Proposition 2.11 we get that $\Phi_2^r = \{abc, ac, ab, a\}$ hence

$$(K_2^r, \Phi_2^r) = (L^{\langle xac\rangle}, \rho\langle b, c\rangle).$$

**The reflex of $(K, \Phi_3)$**

We have $\Phi_3 = \{1_{|_K}, \rho x_{|_K}, x^2_{|_K}\}$. Extending this up to $L$ this gives

$$\begin{aligned}
\Phi_{3,L} &= \Phi_3\,\mathrm{Gal}(L/K)\\
&= \Phi_3\{1, b, c, bc\}\\
&= \{1, \rho x, x^2, b, \rho xb, x^2b, c, \rho xc, x^2c, bc, \rho xbc, x^2bc\}\\
&= \{1, xabc, x^2, b, xac, x^2b, c, xab, x^2c, bc, xa, x^2bc\}.
\end{aligned}$$

We follow the same procedure as before. An element of $\mathrm{Gal}(L/K_3^r)$ is $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\sigma\Phi_{3,L} = \Phi_{3,L}$. Note that $\sigma$ has to be contained in $\Phi_{3,L}$ since $1 \in \Phi_{1,L}$ so we only need to check the elements contained in $\Phi_{3,L}$, such as we did when finding the reflex type of $(K, \Phi_1)$. Now we obtain the following

$$1\Phi_{3,L} = \{1, xabc, x^2, b, xac, x^2b, c, xab, x^2c, bc, xa, x^2bc\} = \Phi_{3,L},$$

$$xab\Phi_{3,L} = \{xab, x^2, bc, xa, x^2, c, xabc, x^2bc, b, xac, x^2c, 1\} = \Phi_{3,L},$$

$$x^2bc\Phi_{3,L} = \{x^2bc, c, xac, x^2c, bc, xabc, x^2b, 1, xa, x^2, b, xab\} = \Phi_{3,L}.$$

This shows that $\mathrm{Gal}(L/K_3^r) = \langle xab \rangle$ so $K_3^r = L^{\langle xab \rangle}$. In order to find $\Phi_3^r$ we determine the set of inverse maps of $\Phi_{3,L}$, where

$$(\Phi_{3,L})^{-1} = \{1, abcx^2, x, b, acx^2, bx, c, abx^2, cx, bc, ax^2, bcx\}.$$

Using Proposition 2.11 we get $\Phi_3^r = \{1, b, c, bc\}$ so therefore the reflex type of $(K, \Phi_3)$ is

$$(K_3^r, \Phi_3^r) = (L^{\langle xab \rangle}, \langle b, c \rangle).$$

**The reflex of** $(K, \Phi_4)$

We consider $\Phi_4 = \{1_{|_K}, x_{|_K}, \rho x^2_{|_K}\}$. Extending this up to $L$ gives

$$\begin{aligned}
\Phi_{4,L} &= \Phi_4 \,\mathrm{Gal}(L/K) \\
&= \Phi_4\{1, b, c, bc\} \\
&= \{1, x, \rho x^2, b, xb, \rho x^2 b, c, xc, \rho x^2 c, bc, xbc, \rho x^2 bc\} \\
&= \{1, x, x^2abc, b, xb, x^2ac, c, xc, x^2ab, bc, xbc, x^2a\}.
\end{aligned}$$

Now we will determine $\mathrm{Gal}(L/K_4^r)$. Again, the elements of $\mathrm{Gal}(L/K_4^r)$ have to be contained in $\Phi_{4,L}$ since $1 \in \Phi_{4,L}$, so we will only check those such as we did when finding the reflex type of $(K, \Phi_1)$ and $(K, \Phi_3)$. We get the following

$$1\Phi_{4,L} = \{1, x, x^2abc, b, xb, x^2ac, c, xc, x^2ab, bc, xbc, x^2a\} = \Phi_{4,L},$$

$$xbc\Phi_{4,L} = \{xbc, x^2ab, b, xc, x^2a, 1, xb, x^2abc, bc, x, x^2ac, c\} = \Phi_{4,L},$$

$$x^2ac\Phi_{4,L} = \{x^2ac, bc, xc, x^2abc, c, xbc, x^2a, b, x, x^2ab, 1, xb\} = \Phi_{4,L}.$$

So $\mathrm{Gal}(L/K_4^r) = \langle xbc \rangle$ and $K_4^r = L^{\langle xbc \rangle}$. In order to find $\Phi_4^r$, we will determine $(\Phi_{4,L})^{-1}$ by finding the inverse of each of the elements in $\Phi_{4,L}$. We obtain

$$(\Phi_{4,L})^{-1} = \{1, x^2, abcx, b, bx^2, acx, c, cx^2, abx, bc, bcx^2, ax\}.$$

Now we get $\Phi_4^r = (\Phi_{4,L})^{-1}_{K_4^r} = \{1, b, c, bc\}$. Hence

$$(K_4^r, \Phi_4^r) = (L^{\langle xbc \rangle}, \langle b, c \rangle).$$

Finally, we will show that the reflex fields that we found are actually isomorphic to each other. Note that $\langle xac\rangle = \langle axa\rangle = \langle a^{-1}xa\rangle = a^{-1}\langle x\rangle a$, so $\langle xac\rangle$ is conjugate to $\langle x\rangle$. Similarly we can show $\langle xab\rangle = b^{-1}\langle x\rangle b$ and $\langle xbc\rangle = c^{-1}\langle x\rangle c$, so also $\langle xab\rangle$ and $\langle xbc\rangle$ are both conjugate to $\langle x\rangle$ as well. Then $L^{\sigma^{-1}\langle x\rangle\sigma}$, where $\sigma \in \{1, a, b, c\}$, is the set of all $\alpha \in L$ such that $\sigma^{-1}x^i\sigma(\alpha) = \alpha$, which is the same as $x^i\sigma(\alpha) = \sigma(\alpha)$. Hence

$$L^{\sigma^{-1}\langle x\rangle\sigma} = \{\alpha \in L : \sigma(\alpha) \in L^{\langle x\rangle}\} = \sigma L^{\langle x\rangle}.$$

Since $\sigma$ is bijective, we conclude that

$$L^{\langle x\rangle} \cong L^{\langle xac\rangle} \cong L^{\langle xab\rangle} \cong L^{\langle xbc\rangle}.$$

□

## 3.2 Sextic CM-fields with Galois group $G = (C_2)^3 \rtimes S_3$

### 3.2.1 The group $G = (C_2)^3 \rtimes S_3$

Let $(C_2)^3 = \langle a, b, c : a^2 = b^2 = c^2 = 1, ab = ba, ac = ca, bc = cb\rangle$ and similarly let $S_3 = \langle x, y : x^3 = y^2 = 1, yxy = x^2\rangle$. The group $S_3$ acts on $(C_2)^3$ by

$$\begin{aligned} x \cdot a &= b, & x \cdot b &= c, & x \cdot c &= a, \\ y \cdot a &= b, & y \cdot b &= a, & y \cdot c &= c. \end{aligned}$$

This action induces the following automorphisms of $(C_2)^3$

$$\begin{aligned} x : (C_2)^3 &\longrightarrow (C_2)^3 & y : (C_2)^3 &\longrightarrow (C_2)^3 \\ a &\longmapsto b & a &\longmapsto b \\ b &\longmapsto c & b &\longmapsto a \\ c &\longmapsto a, & c &\longmapsto c. \end{aligned}$$

Let us now define $\psi$ be the homomorphism from $C_3$ to $\mathrm{Aut}((C_2)^3)$ sending $x$ and $y$ to the induced automorphism, i.e.

$$\begin{aligned} \psi : S_3 &\longrightarrow \mathrm{Aut}((C_2)^3) \\ x &\longmapsto \begin{Bmatrix} a \mapsto b \\ b \mapsto c \\ c \mapsto a \end{Bmatrix} \\ y &\longmapsto \begin{Bmatrix} a \mapsto b \\ b \mapsto a \\ c \mapsto c \end{Bmatrix}. \end{aligned}$$

The set $G$ of ordered pairs $(r, t)$, where $r \in (C_2)^3$ and $t \in S_3$ forms a group under multiplication

$$(r_1, t_1)(r_2, t_2) = (r_1\psi(t_1)(r_2), t_1t_2), \tag{9}$$

which follows by Theorem 10 in §5.5 [3]. Note that by (9) we get

$$(1,t)(r,1)(1,t)^{-1} = (\psi(t)(r),1)$$

for all $r \in \{a,b,c\}$ and $t \in \{x,y\}$. We will identify the element $(1,t)$ with $t \in \langle x,y\rangle$ and similarly $(r,1)$ with $r \in \langle a,b,c\rangle$ via the isomorphisms $S_3 \to \{(1,t) : t \in S_3\}$ and $(C_2)^3 \to \{(r,1) : r \in (C_2)^3\}$, respectively. Hence we can represent $G$ as follows

$$\begin{aligned} G = \langle a,b,c,x,y \,:\, & a^2 = b^2 = c^2 = x^3 = y^2 = 1,\ ab = ba,\ ac = ca,\ bc = cb, \\ & ax = xc,\ bx = xa,\ cx = xb,\ ya = by,\ yb = ay,\ yc = cy, yx = x^2y\rangle. \end{aligned}$$

**Lemma 3.10.** The center of $G$ is $\langle abc\rangle$.

*Proof.* The centre of the group $G$ is defined as

$$Z(G) := \{g \in G : zg = gz\}.$$

By the definition of $G$ above, we already see that $x, xa, xb, xc, y, ya, yb, yx \notin Z(G)$ and from this it follows that any element of the form $xa^{e_1}b^{e_2}c^{e_3}$, $x^2a^{e_1}b^{e_2}c^{e_3}$, $ya^{e_1}b^{e_2}c^{e_3}$, $yxa^{e_1}b^{e_2}c^{e_3}$, $yx^2a^{e_1}b^{e_2}c^{e_3} \notin Z(G)$. Hence we are left with elements of the form $a^{e_1}b^{e_2}c^{e_3}$. Since $ax = xc$, $bx = xa$ and $cx = xb$, we have $a,b,c \notin Z(G)$. Combining these we get that $abx = xca$, $acx = xcb$ and $bcx = xab$ hence $ab, bc, ca \notin Z(G)$.

Now we want to show that 1 and $abc$ do commute with every element of $G$. By definition, 1 commutes with every element of $G$, so $1 \in Z(G)$. Now, every element $g \in G$ can be written of the form $g = x^iy^ja^{e_1}b^{e_2}c^{e_3}$. Note since the elements $a,b,c$ commute with each other, we have $abcx = xabc$ $abcx^2 = x^2abc$ and $abcy = yabc$. From this we obtain the following

$$\begin{aligned} (abc)(x^iy^ja^{e_1}b^{e_2}c^{e_3}) &= x^i(abc)a^{e_1}b^{e_2}c^{e_3} \\ &= x^iy^j(abc)a^{e_1}b^{e_2}c^{e_3} \\ &= x^iy^ja^{e_1}b^{e_2}c^{e_3}(abc). \end{aligned}$$

We conclude that $Z(G) = \langle abc\rangle$. □

Hence it follows that the group $G$ is a non-abelian group of order $\#(C_2)^3 \cdot \#S_3 = 48$. The subgroup $(C_2)^3$ of $G$ is normal in $G$ since $xax^{-1} = b$, $xbx^{-1} = c$, $xcx^{-1} = a$ and $yay^{-1} = b$, $yby^{-1} = a$, $ycy^{-1} = c$.

**Definition 3.11.** The group $G$ described in this section is called the *semi-direct product* of groups $(C_2)^3$ and $S_3$ with respect to $\psi$ and will be denoted by $G = (C_2)^3 \rtimes S_3$.

### 3.2.2 Intermediate extensions of $L/\mathbb{Q}$

Assume that $\mathrm{Gal}(L/\mathbb{Q}) \cong (C_2)^3 \rtimes S_3$. Since $\#\,\mathrm{Gal}(L/\mathbb{Q}) = [L : \mathbb{Q}] = 48$, by the tower law, the Galois extension $L/K$ is of degree 8 since $[K : \mathbb{Q}] = 6$ by definition.

We will denote the totally real cubic intermediate field extension by $\mathbb{Q} \subset K_+ \subset K$. Let $\delta \in K_+ \setminus \mathbb{Q}$ be a totally positive element such that $K = K_+(\sqrt{-\delta})$ and let

$$\begin{aligned}
\delta_0 &:= \delta = y(\delta_1),\\
\delta_1 &:= x(\delta_0) = y(\delta_0),\\
\delta_2 &:= x^2(\delta_0) = y(\delta_2).
\end{aligned}$$

Since $K_+$ is not Galois, we have that $\delta_1, \delta_2 \notin K_+$ but they are contained in the Galois closure of $K_+$ denoted by $L'$. By Lemma 2.2 from [2] we have that $\mathrm{Gal}(L/L') \cong (C_2)^3$ and $\mathrm{Gal}(L'/\mathbb{Q}) \cong S_3$ following from that by Galois correspondence, with

$$1 \to \mathrm{Gal}(L/L') \to \mathrm{Gal}(L'/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q}) \to 1.$$

See the order of these extensions in Figure 3.

$$\begin{tikzcd}
 & & L \arrow[dll, dash, "4"'] \arrow[d, dash, "4"] \arrow[dr, dash, "4"] & \\
L'(\sqrt{-\delta_0}) \arrow[rr, dash, "\sim"] \arrow[d, dash, "2"] \arrow[drr, dash, "2"] & & L'(\sqrt{-\delta_1}) \arrow[r, dash, "\sim"] \arrow[d, dash, "2"] & L'(\sqrt{-\delta_2}) \arrow[dl, dash, "2"] \\
K = K_+(\sqrt{-\delta_0}) \arrow[drr, dash, "2"] \arrow[ddrr, dash, "6"'] & & L' \arrow[d, dash, "2"] & \\
 & & K_+ \arrow[d, dash, "3"] & \\
 & & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & & \langle 1 \rangle \arrow[dll, dash, "4"'] \arrow[d, dash, "4"] \arrow[dr, dash, "4"] & \\
\langle b, c \rangle \arrow[rr, dash, "\sim"] \arrow[d, dash, "2"] \arrow[drr, dash, "2"] & & \langle a, b \rangle \arrow[r, dash, "\sim"] \arrow[d, dash, "2"] & \langle a, c \rangle \arrow[dl, dash, "2"] \\
\langle b, c, x^2y \rangle \arrow[drr, dash, "2"] \arrow[ddrr, dash, "6"'] & & \langle a, b, c \rangle \arrow[d, dash, "2"] & \\
 & & \langle a, b, c, x^2y \rangle \arrow[d, dash, "3"] & \\
 & & \langle a, b, c, x, y \rangle &
\end{tikzcd}$$

Figure 3: Sublattices of subfields of $L$ and of subgroups of $\mathrm{Gal}(L/\mathbb{Q})$

### 3.2.3 Complex embeddings of $L$

In this section we will find all the complex embeddings of $L$. As we already explained, the complex embeddings of $L$ can be identified with the automorphisms of $L$. Let us therefore examine the Galois group of $L/\mathbb{Q}$.

We will now explicitly write the complex embeddings corresponding to the generator automorphisms $a, b, c, x, y$ of $\mathrm{Gal}(L/\mathbb{Q})$. By Lemma 1.13 every field homomorphism fixes $\mathbb{Q}$ and since $L = L'(\sqrt{-\delta_0}, \sqrt{-\delta_1}, \sqrt{-\delta_2})$, by permuting $\sqrt{-\delta_0}, \sqrt{-\delta_1}, \sqrt{-\delta_2}$ we automatically permute $\delta_0, \delta_1, \delta_2$, so it is enough to write the images of $\sqrt{-\delta_0}, \sqrt{-\delta_1}, \sqrt{-\delta_2}$. For $x$ and $y$ we however write the images of $\delta_0, \delta_1, \delta_2$ because these are embeddings of $L'$. Similarly as in Section 3.1.3 we get the following

$$\begin{aligned} a : L &\longrightarrow L \subset \mathbb{C} \\ \sqrt{-\delta_0} &\longmapsto -\sqrt{-\delta_0} \\ \sqrt{-\delta_1} &\longmapsto \sqrt{-\delta_1} \\ \sqrt{-\delta_2} &\longmapsto \sqrt{-\delta_2}, \end{aligned} \qquad \begin{aligned} b : L &\longrightarrow L \subset \mathbb{C} \\ \sqrt{-\delta_0} &\longmapsto \sqrt{-\delta_0} \\ \sqrt{-\delta_1} &\longmapsto -\sqrt{-\delta_1} \\ \sqrt{-\delta_2} &\longmapsto \sqrt{-\delta_2}, \end{aligned} \qquad \begin{aligned} c : L &\longrightarrow L \subset \mathbb{C} \\ \sqrt{-\delta_0} &\longmapsto \sqrt{-\delta_0} \\ \sqrt{-\delta_1} &\longmapsto \sqrt{-\delta_1} \\ \sqrt{-\delta_2} &\longmapsto -\sqrt{-\delta_2}, \end{aligned}$$

$$\begin{aligned} x : L &\longrightarrow L \subset \mathbb{C} \\ \delta_0 &\longmapsto \delta_1, \\ \delta_1 &\longmapsto \delta_2, \\ \delta_2 &\longmapsto \delta_0, \end{aligned} \qquad \begin{aligned} y : L &\longrightarrow L \subset \mathbb{C} \\ \delta_0 &\longmapsto \delta_1 \\ \delta_1 &\longmapsto \delta_0 \\ \delta_2 &\longmapsto \delta_2. \end{aligned}$$

The generators $b, c$ and the element $x^2y$ (which permutes $\sqrt{-\delta_1}$ with $\sqrt{-\delta_2}$) are fixing $K$ elementwise, so we obtain

$$\mathrm{Gal}(L/K) = \langle b, c, x^2y \rangle. \tag{10}$$

Since $a, b, c, x, y$ are the generators of $\mathrm{Gal}(L/\mathbb{Q})$, we get 48 complex embeddings of $L$ by combining these generators.

**Proposition 3.12.** The element $\rho = abc$ corresponds to complex conjugation on $L$.

*Proof.* By Proposition 2.2, complex conjugation commutes with every embedding of $L$, hence with every element of $\mathrm{Gal}(L/\mathbb{Q})$. So the corresponding automorphism to $\rho$ is in the center $Z(G)$ of $G = \mathrm{Gal}(L/\mathbb{Q})$. Then by Lemma 3.10, we get $\rho = abc$ since complex conjugation is of order 2. □

### 3.2.4 Complex embeddings and CM-types of $K$

In this section we will determine all complex embeddings of $K$ and since $[K : \mathbb{Q}] = 6$, there are 6 complex embeddings of $K$. These embeddings are totally complex since $K$ is a CM-field and therefore each of these embeddings has its conjugate pair. We will denote them by $\varphi_1, \varphi_2, \varphi_3, \overline{\varphi}_1, \overline{\varphi}_2, \overline{\varphi}_3$.

**Proposition 3.13.** The set $S = \{1_{|_K}, x_{|_K}, x^2_{|_K}, \rho_{|_K}, \rho x_{|_K}, \rho x^2_{|_K}\}$ contains all complex embeddings of $K$.

*Proof.* By the explanation in Section 1.3 we can take $\phi$ a complex embedding of $K$ and $\sigma \in \mathrm{Gal}(L/K)$ and we can extend the set of complex embeddings of $K$ to $L$ by $\phi \circ \sigma$. We have that $\mathrm{Gal}(L/K) = \langle b, c, x^2y \rangle$, and in order to prove that $S$ contains all complex embeddings of $K$ we will show that $\langle b, c, x^2y \rangle S = G$.

Take $1 \in \mathrm{Gal}(L/K)$. Since $\rho_{|_K} = a$, then we have

$$1S = 1\{1_{|_K}, x_{|_K}, x^2_{|_K}, \rho_{|_K}, \rho x_{|_K}, \rho x^2_{|_K}\} = \{1, x, x^2, a, ax, ax^2\}.$$

Similarly for $b, c, bc \in \mathrm{Gal}(L/K)$, we get

$$bS = \{b, bx, bx^2, ab, abx, abx^2\},$$

$$cS = \{c, cx, cx^2, ac, acx, acx^2\},$$

and

$$bcS = \{bc, bcx, bcx^2, abc, abcx, abcx^2\}.$$

Finally for $x^2y, bx^2y, cx^2y, bcx^2y$ we obtain

$$x^2yS = \{x^2y, xy, y, ax^2y, axy, ay\}$$

$$bx^2yS = \{bx^2y, bxy, by, abx^2y, abxy, aby\}$$

$$cx^2yS = \{cx^2y, cxy, cy, acx^2y, acxy, acy\}$$

$$bcx^2yS = \{bcx^2y, bcxy, bcy, abcx^2y, abcxy, abcy\}.$$

Adding the elements of these sets together we obtain all the elements of $G$. We conclude that $\langle b, c, x^2y\rangle S = G$, so the set $S$ contains all complex embeddings of $K$. □

We will denote the complex embeddings of $K$ as follows

$$\begin{array}{lll} \varphi_1 = 1_{|_K}, & \varphi_2 = x_{|_K} & \varphi_3 = x^2{}_{|_K} \\ \overline{\varphi}_1 = \rho_{|_K}, & \overline{\varphi}_2 = \rho x_{|_K}, & \overline{\varphi}_3 = \rho x^2_{|_K}. \end{array}$$

Each CM-type of $K$ will contain 3 of these embedding, such that two that are conjugate to each other cannot be in the same CM-type. We get the following CM-types:

$$\{\varphi_1, \varphi_2, \varphi_3\}, \{\overline{\varphi}_1, \varphi_2, \varphi_3\}, \{\varphi_1, \overline{\varphi}_2, \varphi_3\}, \{\varphi_1, \varphi_2, \overline{\varphi}_3\},$$
$$\{\overline{\varphi}_1, \overline{\varphi}_2, \overline{\varphi}_3\}, \{\varphi_1, \overline{\varphi}_2, \overline{\varphi}_3\}, \{\overline{\varphi}_1, \varphi_2, \overline{\varphi}_3\}, \{\overline{\varphi}_1, \overline{\varphi}_2, \varphi_3\}.$$

**Proposition 3.14.** The only field automorphisms of $K$ are $1_{|_K}$ and $\rho_{|_K}$.

*Proof.* See the proof of Proposition 3.7. □

Now we want to determine the equivalency of the found CM-types. Since by Proposition 3.14 the only non-trivial automorphism of $K$ is $\rho_{|_K}$, by Definition 2.8 each CM-type $\Phi$ is only equivalent to its complex conjugate $\overline{\Phi} := \{\overline{\phi} : \phi \in \Phi\}$. Thus, we get the following:

$$\Phi_1 = \{\varphi_1, \varphi_2, \varphi_3\} \sim \{\overline{\varphi}_1, \overline{\varphi}_2, \overline{\varphi}_3\} = \overline{\Phi}_1,$$
$$\Phi_2 = \{\overline{\varphi}_1, \varphi_2, \varphi_3\} \sim \{\varphi_1, \overline{\varphi}_2, \overline{\varphi}_3\} = \overline{\Phi}_2,$$
$$\Phi_3 = \{\varphi_1, \overline{\varphi}_2, \varphi_3\} \sim \{\overline{\varphi}_1, \varphi_2, \overline{\varphi}_3\} = \overline{\Phi}_3,$$
$$\Phi_4 = \{\varphi_1, \varphi_2, \overline{\varphi}_3\} \sim \{\overline{\varphi}_1, \overline{\varphi}_2, \varphi_3\} = \overline{\Phi}_4.$$

**Proposition 3.15.** All the CM-types mentioned above are primitive.

*Proof.* We want to show that there is no CM-subfield of $K$, which then by definition implies that no CM-type is induced and hence they are all primitive.

Assume for contradiction that there exists an intermediate extension $\mathbb{Q} \subset N \subset K$, such that $N$ is a totally imaginary quadratic extension over $\mathbb{Q}$, hence a CM-subfield of $K$. And since $K$ is a subfield of $L'(\sqrt{-\delta_0})$ (see Figure 3), we get that $N$ is a subfield of $L'(\sqrt{-\delta_0})$. The extension $N/\mathbb{Q}$ is Galois because all quadratic field extensions are normal. Moreover, since $L'$ is the Galois closure of $K_+$, the extension $L'/\mathbb{Q}$ is Galois, which is a subfield of $L'(\sqrt{-\delta_0})$. Hence the field $NL' \subset L'(\sqrt{-\delta_0})$ is also Galois over $\mathbb{Q}$ by Lemma 1.6. Now, since $[N : \mathbb{Q}] = 2$ and $[L' : \mathbb{Q}] = 6$, then we have two options for the degree of $NL'$ over $\mathbb{Q}$, which is either $[NL' : \mathbb{Q}] = 6$ or 12.

If $[NL' : \mathbb{Q}] = 6$, then $N \subset L'$, but this is not possible since $L'$ is a totally real field so it cannot contain a totally imaginary subfield $N$.

In the other case we have that $[NL' : \mathbb{Q}] = 12$, but then $NL' = L'(\sqrt{-\delta_0})$, where the right hand side is Galois over $\mathbb{Q}$, but the left hand side is not (since it does not contain $\sqrt{-\delta_1}$ and $\sqrt{-\delta_2}$). Therefore, we get a contradiction. We conclude that all the CM-types are primitive. □

### 3.2.5 Reflex fields

In this section we will find the reflex types $(K^r, \Phi^r)$ of $(K, \Phi)$ for $K$ and each of its CM-types $\Phi$. We only need to consider the following 4 cases, because the reflex type of $(K, \overline{\Phi})$ can be concluded after we have found the reflex type of $(K, \Phi)$.

$$\Phi_1 = \{\varphi_1, \varphi_2, \varphi_3\},\ \Phi_2 = \{\overline{\varphi}_1, \varphi_2, \varphi_3\},\ \Phi_3 = \{\varphi_1, \overline{\varphi}_2, \varphi_3\},\ \Phi_4 = \{\varphi_1, \varphi_2, \overline{\varphi}_3\} \tag{11}$$

**Theorem 3.16.** Let $K$ be a sextic CM-field and let $L$ be the normal closure of $K$ such that $\mathrm{Gal}(L/\mathbb{Q}) = (C_2)^3 \rtimes S_3$. Let $\Phi$ be a CM-type of $K$ with values in $L$. The reflex types of $(K, \Phi)$ are

$$\begin{aligned}
(K_1^r, \Phi_1^r) &= (L^{\langle x,y\rangle}, \langle b,c\rangle) & (K_5^r, \Phi_5^r) &= (L^{\langle x,y\rangle}, \rho\langle b,c\rangle)\\
(K_2^r, \Phi_2^r) &= (L^{\langle xac,x^2y\rangle}, \rho\langle b,c\rangle) & (K_6^r, \Phi_6^r) &= (L^{\langle xac,x^2y\rangle}, \langle b,c\rangle)\\
(K_3^r, \Phi_3^r) &= (L^{\langle xab,xy\rangle}, \langle b,c\rangle) & (K_7^r, \Phi_7^r) &= (L^{\langle xab,xy\rangle}, \rho\langle b,c\rangle)\\
(K_4^r, \Phi_4^r) &= (L^{\langle xbc,y\rangle}, \langle b,c\rangle) & (K_8^r, \Phi_8^r) &= (L^{\langle xbc,y\rangle}, \rho\langle b,c\rangle).
\end{aligned}$$

Moreover, these reflex fields are isomorphic.

*Proof.* We will consider each of the 4 cases mentioned in (5) separately.

**The reflex of** $(K, \Phi_1)$

We first consider $\Phi_1 = \{1_{|_K}, x_{|_K}, x^2_{|_K}\}$. The CM-type induced by $\Phi_1$ on $L$ is

$$\begin{aligned}\Phi_{1,L} &= \Phi_1 \operatorname{Gal}(L/K)\\ &= \Phi_1\{1, b, c, bc, x^2y, x^2yb, x^2yc, x^2ybc\}\\ &= \{1, x, x^2, b, xb, x^2b, c, xc, x^2c, bc, xbc, x^2bc, x^2y, y,\\ &\quad xy, x^2yb, yb, xyb, x^2yc, yc, xyc, x^2ybc, ybc, xybc\}.\end{aligned}$$

We will first compute the reflex field $K_1^r$ of $(K, \Phi_1)$ using Proposition 2.11. We want to find the elements of $\operatorname{Gal}(L/K_1^r)$, which are the elements $\sigma \in \operatorname{Gal}(L/\mathbb{Q})$ such that

$$\sigma\Phi_{1,L} = \Phi_{1,L}. \tag{12}$$

Since $1 \in \Phi_{1,L}$, every $\sigma$ satisfying (12) has to be in $\Phi_{1,L}$. We will therefore only consider those elements. We get that

$$\begin{aligned}1\Phi_{1,L} &= \{1, x, x^2, b, xb, x^2b, c, xc, x^2c, bc, xbc, x^2bc, x^2y, y,\\ &\quad xy, x^2yb, yb, xyb, x^2yc, yc, xyc, x^2ybc, ybc, xybc\} = \Phi_{1,L}\\ x\Phi_{1,L} &= \{x, x^2, 1, xb, x^2b, b, xc, x^2c, c, xbc, x^2bc, bc, y, xy,\\ &\quad x^2y, yb, xyb, x^2yb, yc, xyc, x^2yc, ybc, xybc, x^2ybc\} = \Phi_{1,L}\\ x^2\Phi_{1,L} &= \{x^2, 1, x, x^2b, b, xb, x^2c, c, xc, x^2bc, bc, xbc, xy, x^2y,\\ &\quad y, xyb, x^2yb, yb, xyc, x^2yc, yc, xybc, x^2ybc, ybc\} = \Phi_{1,L}\\ y\Phi_{1,L} &= \{y, x^2y, xy, yb, x^2yb, xyb, yc, x^2yc, xyc, ybc, x^2ybc,\\ &\quad xybc, x, 1, x^2, xb, b, x^2b, xc, c, x^2c, xbc, bc, x^2bc\} = \Phi_{1,L}\\ xy\Phi_{1,L} &= \{xy, y, x^2y, xyb, yb, x^2yb, xyc, yc, x^2yc, xybc, ybc,\\ &\quad x^2ybc, x^2, x, 1, x^2b, xb, b, x^2c, xc, c, x^2bc, xbc, bc\} = \Phi_{1,L}\\ x^2y\Phi_{1,L} &= \{x^2y, xy, y, x^2yb, xyb, yb, x^2yc, xyc, yc, x^2ybc, xybc,\\ &\quad ybc, 1, x^2, x, b, x^2b, xb, c, x^2c, xc, bc, x^2bc, xbc\} = \Phi_{1,L}.\end{aligned}$$

We can show that for any other element $\sigma \in \Phi_{1,L}$ apart from $1, x, x^2, y, xy, x^2y$ we have that $\sigma\Phi_{1,L} \neq \Phi_{1,L}$. For example, if $\sigma = x^2yc$, then the element $x^2ycx^2 \in (x^2yc)\Phi_{1,L}$ but since $x^2ycx^2 = ya \notin \Phi_{1,L}$ we have $(x^2yc)\Phi_{1,L} \neq \Phi_{1,L}$. By Proposition 2.11 we conclude that $\operatorname{Gal}(L/K_1^r) = \langle x, y\rangle$ and thus $K_1^r = L^{\langle x,y\rangle}$.

Now we will find the reflex CM-type $\Phi_1^r$ of $(K, \Phi_1)$. For this we need to determine the set of inverse maps in $\Phi_{1,L}$ denoted by $(\Phi_{1,L})^{-1}$ and then find $\Phi_1^r = (\Phi_{1,L})^{-1}_{|_{K_1^r}}$. We have that

$$\begin{aligned}(\Phi_{1,L})^{-1} = \{&1, x^2, x, b, bx^2, bx, c, cx^2, cx, bc, bcx^2, bcx, yx, y,\\ &yx^2, byx, by, byx^2, cyx, cy, cyx^2, bcyx, bcy, bcyx^2\}.\end{aligned}$$

Since $\langle x, y\rangle$ fixes $K_1^r$ elementwise and $\Phi_1^r = (\Phi_{1,L})^{-1}_{|_{K_1^r}}$, we get that $\Phi_1^r = \{1, b, c, bc\}$. We obtain the following reflex type of $(K, \Phi_1)$

$$(K_1^r, \Phi_1^r) = (L^{\langle x,y\rangle}, \langle b, c\rangle).$$

**The reflex of** $(K, \Phi_2)$
Now we consider $\Phi_2 = \{\rho_{|_K}, x_{|_K}, x^2_{|_K}\}$. Similarly, extending $\Phi_2$ to $L$ gives us the following

$$\begin{aligned}\Phi_{2,L} = \{&abc, x, x^2, ac, xb, x^2b, ab, xc, x^2c, a, xbc, x^2bc, x^2yabc,\\ &y, xy, x^2yac, yb, xyb, x^2yab, yc, xyc, x^2ya, ybc, xybc\},\end{aligned}$$

with the set of inverse elements

$$\begin{aligned}(\Phi_{2,L})^{-1} = \{&abc, x^2, x, ac, bx^2, bx, ab, cx^2, cx, a, bcx^2, bcx, abcyx,\\ &y, yx^2, acyx, by, byx^2, abyx, cy, cyx^2, ayx, bcy, bcyx^2\}.\end{aligned}$$

Now we want to find $\mathrm{Gal}(L/K_2^r)$ using Proposition 2.11 Note that since $\rho \in \Phi_{2,L}$ and we are searching for $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\sigma\Phi_{2,L} = \Phi_{2,L}$, we find that $\sigma\rho \in \Phi_{2,L}$ and hence $\sigma \in \overline{\Phi}_{2,L}$.

$$\begin{aligned}1\Phi_{2,L} &= \{abc, x, x^2, ac, xb, x^2b, ab, xc, x^2c, a, xbc, x^2bc, x^2yabc,\\ &\quad y, xy, x^2yac, yb, xyb, x^2yab, yc, xyc, x^2ya, ybc, xybc\} = \Phi_{2,L}\\ xac\Phi_{2,L} &= \{xb, x^2bc, ab, x, x^2c, a, xbc, x^2b, abc, xc, x^2, a, yc, xybc,\\ &\quad x^2yac, ybc, xyc, x^2yabc, y, xyb, x^2ya, yb, xy, x^2yab\} = \Phi_{2,L}\\ x^2ab\Phi_{2,L} &= \{x^2c, ac, xbc, x^2bc, abc, xc, x^2, a, xb, x^2b, ab, x, xyb,\\ &\quad x^2yab, ybc, xy, x^2ya, yc, xybc, x^2yabc, yb, xyc, x^2yac, y\} = \Phi_{2,L}\\ x^2y\Phi_{2,L} &= \{x^2yabc, xy, y, x^2yac, xyb, yb, x^2yab, xyc, yc, x^2ya, xybc,\\ &\quad ybc, abc, x^2, x, ac, x^2b, xb, ab, x^2c, xc, a, x^2bc, xbc\} = \Phi_{2,L}\\ xyac\Phi_{2,L} &= \{xyb, ybc, x^2yab, xy, yc, x^2ya, xybc, yb, x^2yabc, xyc, y,\\ &\quad x^2yac, x^2c, xbc, ac, x^2bc, xc, abc, x^2, xb, a, x^2b, x, ab\} = \Phi_{2,L}\\ yab\Phi_{2,L} &= \{yc, x^2yac, xybc, ybc, x^2yabc, xyc, y, x^2ya, xyb, yb, x^2yab,\\ &\quad xy, xb, ab, x^2bc, x, a, x^2c, xbc, abc, x^2b, xc, ac, x^2\} = \Phi_{2,L}\end{aligned}$$

We conclude that $\mathrm{Gal}(L/K_2^r) = \langle xac, x^2y\rangle$ and thus $K_2^r = L^{\langle acx, x^2y\rangle}$. Since $\langle xac, x^2y\rangle$ fixes $K_2^r$ elementwise and $\Phi_2^r = (\Phi_{2,L})^{-1}_{|_{K_2^r}}$, we get that $\Phi_2^r = \{abc, ca, cb, a\} = \rho\langle b, c\rangle$. We obtain the following reflex type of $(K, \Phi_2)$

$$(K_2^r, \Phi_2^r) = (L^{\langle xac, x^2y\rangle}, \rho\langle b, c\rangle).$$

**The reflex of** $(K, \Phi_3)$

We have $\Phi_3 = \{1_{|_K}, \rho x_{|_K}, x^2_{|_K}\}$. Extending this up to $L$ this gives

$$\begin{aligned}\Phi_{3,L} = \{&1, xabc, x^2, b, xac, x^2b, c, xab, x^2c, bc, xa, x^2bc, x^2y, yabc,\\ &xy, x^2yb, yac, xyb, x^2yc, yab, xyc, x^2ybc, ya, xybc\},\end{aligned}$$

with the set of inverse elements of $\Phi_{3,L}$

$$\begin{aligned}(\Phi_{3,L})^{-1} = \{&1, abcx^2, x, b, acx^2, bx, c, abx^2, cx, bc, ax^2, bcx, yx, abcy,\\ &yx^2, byx, acy, byx^2, cyx, aby, cyx^2, bcyx^2, ay, bcyx^2\}.\end{aligned}$$

We will first find $\mathrm{Gal}(L/K_3^r)$. For the following elements it holds that

$$\begin{aligned}1\Phi_{3,L} &= \{1, xabc, x^2, b, xac, x^2b, c, xab, x^2c, bc, xa, x^2bc, x^2y, yabc,\\ &\quad xy, x^2yb, yac, xyb, x^2yc, yab, xyc, x^2ybc, ya, xybc\} = \Phi_{3,L}\\ xab\Phi_{3,L} &= \{xab, x^2b, bc, xa, x^2, c, xabc, x^2bc, b, xac, x^2c, 1, yac, xyc,\\ &\quad x^2ybc, yabc, xybc, x^2yc, ya, xy, x^2yb, yab, xyb, x^2y\} = \Phi_{3,L}\\ x^2bc\Phi_{3,L} &= \{x^2bc, c, xac, x^2c, bc, xabc, x^2b, 1, xa, x^2, b, xab, xybc,\\ &\quad x^2yb, yab, xyc, x^2y, ya, xyb, x^2ybc, yabc, xy, x^2c, yac\} = \Phi_{3,L}\\ xy\Phi_{3,L} &= \{xy, yabc, x^2y, xyb, yac, x^2yb, xyc, yab, x^2yc, xybc, ya,\\ &\quad x^2ybc, x^2, xabc, 1, x^2b, xac, b, x^2c, xab, c, x^2bc, xa, bc\} = \Phi_{3,L}\\ yab\Phi_{3,L} &= \{yab, x^2yb, xybc, ya, x^2y, xyc, yabc, x^2ybc, xyb, yac, x^2yc,\\ &\quad xy, xac, c, x^2bc, xabc, bc, x^2c, xa, 1, x^2b, xab, b, x^2\} = \Phi_{3,L}\\ x^2ybc\Phi_{3,L} &= \{x^2ybc, xyc, yac, x^2yc, xybc, yabc, x^2yb, xy, ya, x^2y, xyb,\\ &\quad yab, bc, x^2b, xab, c, x^2, xa, b, x^2bc, xabc, 1, x^2c, xac\} = \Phi_{3,L}\end{aligned}$$

Hence we get that $\mathrm{Gal}(L/K_3^r) = \langle xab, xy\rangle$ and thus $K_3^r = L^{\langle xab, xy\rangle}$. Since $\langle xab, xy\rangle$ fixes $K_3^r$ elementwise and $\Phi_3^r = (\Phi_{3,L})^{-1}_{|_{K_3^r}}$, we get that $\Phi_3^r = \{1, b, c, bc\}$. Hence we get the following reflex type of $(K, \Phi_3)$

$$(K_3^r, \Phi_3^r) = (L^{\langle xab, xy\rangle}, \langle b, c\rangle).$$

**The reflex of** $(K, \Phi_4)$

Consider $\Phi_4 = \{1_{|_K}, x_{|_K}, \rho x^2_{|_K}\}$. Extending this up to $L$ this gives

$$\begin{aligned}\Phi_{4,L} = \{&1, x, x^2abc, b, xb, x^2ac, c, xc, x^2ab, bc, xbc, x^2a, x^2y, y,\\ &xyabc, x^2yb, yb, xyac, x^2yc, yc, xyab, x^2ybc, ybc, xya\},\end{aligned}$$

with the set of inverse elements of $\Phi_{4,L}$

$$(\Phi_{4,L})^{-1} = \{1, x^2, abcx, b, bx^2, acx, c, cx^2, abx, bc, bcx^2, ax, yx, y, \\ abcyx^2, byx, by, acyx^2, cyx, cy, abyx^2, bcyx, bcy, ayx^2\}.$$

Now we will find the elements of $\mathrm{Gal}(L/K_4^r)$. We find that

$$\begin{aligned}
1\Phi_{4,L} &= \{1, x, x^2abc, b, xb, x^2ac, c, xc, x^2ab, bc, xbc, x^2a, x^2y, y, \\
&\quad xyabc, x^2yb, yb, xyac, x^2yc, yc, xyab, x^2ybc, ybc, xya\} = \Phi_{4,L} \\
xbc\Phi_{4,L} &= \{xbc, x^2ab, b, xc, x^2a, 1, xb, x^2abc, bc, x, x^2ac, c, ybc, \\
&\quad xyac, x^2yc, yc, xyabc, x^2ybc, yb, xya, x^2y, y, xyac, x^2yb\} = \Phi_{4,L} \\
x^2ac\Phi_{4,L} &= \{x^2ac, bc, xc, x^2abc, c, xbc, x^2a, b, x, x^2ab, 1, xb, xyab, \\
&\quad x^2ybc, yb, xya, x^2yc, y, xyabc, x^2yb, ybc, xyac, x^2y, yc\} = \Phi_{4,L} \\
y\Phi_{4,L} &= \{y, x^2y, xyabc, yb, x^2yb, xyac, yc, x^2yc, xyab, ybc, x^2ybc, \\
&\quad xya, x, 1, x^2abc, xb, b, x^2ac, xc, c, x^2ab, xbc, bc, x^2a\} = \Phi_{4,L} \\
xyac\Phi_{4,L} &= \{xyac, ybc, x^2yc, xyabc, yc, x^2ybc, xya, yb, x^2y, xyab, \\
&\quad y, x^2yb, x^2ab, xbc, b, x^2a, xc, 1, x^2abc, xb, bc, x^2ac, x, c\} = \Phi_{4,L} \\
x^2ybc\Phi_{4,L} &= \{x^2ybc, xyab, yb, x^2yc, xya, y, x^2yb, xyabc, ybc, x^2y, \\
&\quad xyac, yc, bc, x^2ac, xc, c, x^2abc, xbc, b, x^2a, x, 1, x^2ab, xb\} = \Phi_{4,L}.
\end{aligned}$$

Hence we get that $\mathrm{Gal}(L/K_4^r) = \langle xbc, y\rangle$ and thus $K_4^r = L^{\langle xbc,y\rangle}$. Since $\langle xbc, y\rangle$ fixes $K_4^r$ elementwise and $\Phi_4^r = (\Phi_{4,L})^{-1}_{|_{K_4^r}}$, we again have that $\Phi_4^r = \{1, b, c, bc\}$. Hence we get the following reflex type of $(K, \Phi_4)$

$$(K_4^r, \Phi_4^r) = (L^{\langle xbc,y\rangle}, \langle b, c\rangle).$$

Now we will show that the reflex fields are isomorphic. The reflex fields are fixed by the groups $\langle x, y\rangle$, $\langle xac, x^2y\rangle$, $\langle xab, xy\rangle$ and $\langle xbc, y\rangle$ respectively. We will first show that these groups are conjugate. Note that

$$\langle xac, x^2y\rangle = \langle axa, ax^2ya\rangle = a\langle x, y\rangle a = a^{-1}\langle x, y\rangle a,$$

because $ax^2ya = x^2bya = x^2yaa = x^2y$. Hence $\langle xac, x^2y\rangle$ is conjugate to $\langle x, y\rangle$. Similarly we have that

$$\langle xab, xy\rangle = \langle bxb, bxyb\rangle = b^{-1}\langle x, y\rangle b$$

and

$$\langle xbc, y\rangle = \langle cxc, cyc\rangle = c^{-1}\langle x, y\rangle c,$$

so also $\langle xab, xy\rangle$ and $\langle xbc, y\rangle$ are both conjugate to $\langle x, y\rangle$. So we can write any reflex field of $K$ as $L^{\sigma^{-1}\langle x,y\rangle\sigma}$, where $\sigma \in \{1, a, b, c\}$. By definition

$$\begin{aligned} L^{\sigma^{-1}\langle x,y\rangle\sigma} &= \{\alpha \in L : \sigma^{-1}x^i y^j \sigma(\alpha) = \alpha\} \\ &= \{\alpha \in L : x^i y^j \sigma(\alpha) = \sigma(\alpha)\} = \sigma L^{\langle x,y\rangle}. \end{aligned}$$

Since $\sigma$ is an isomorphism, we get

$$L^{\langle x,y\rangle} \cong L^{\langle xac,x^2y\rangle} \cong L^{\langle xab,xy\rangle} \cong L^{\langle xbc,y\rangle}.$$

□

# 4 Explicit examples

In this section we provide some examples of sextic CM-fields and we explicitly compute the reflex fields for some of them. This is done using SageMath.

## 4.1 Examples of sextic CM-fields

Code 1 calculates the sextic CM-fields with minimal polynomial in the form

$$x^6 + Ax^4 + Bx^2 + C$$

such that the Galois group of their normal closure is isomorphic to $(C_2)^3 \rtimes C_3$. We want to find CM-fields with class number one, because these are more interesting for further research.

Code 1: Finding sextic CM-fields with $\mathrm{Gal}(L/\mathbb{Q}) \cong (C_2)^3 \rtimes C_3$

```
R.<X> = PolynomialRing(QQ)
F1.<a,b,c,x> = FreeGroup()
H1 = F1 / [a^2, b^2, c^2, x^3, a*b*a*b, a*c*a*c, b*c*b*c, x*a*x^2*b,
x*b*x^2*c, x*c*x^2*a]
for A in range(1,20):
    for B in range(1,30):
        for C in range(1,30):
            if (X^6 + A*X^4 + B*X^2 + C).is_irreducible():
                K.<a> = NumberField(X^6 + A*X^4 + B*X^2 + C)
                if K.is_CM():
                    L.<b> = K.galois_closure()
                    G = L.galois_group()
                    GG = G.as_finitely_presented_group()
                    if GG.is_isomorphic(H1):
                        if K.class_number() == 1:
                            print(K)
```

For this code we get the following output.

Code 2: Output for Code 1

```
Number Field in a with defining polynomial X^6 + 10*X^4 + 21*X^2 + 11
Number Field in a with defining polynomial X^6 + 12*X^4 + 17*X^2 + 2
Number Field in a with defining polynomial X^6 + 15*X^4 + 14*X^2 + 3
```

Similarly, we can compute some sextic CM-fields with the Galois group of the normal closure isomorphic to $(C_2)^3 \rtimes S_3$, again with class number one. See Code 3.

Code 3: Finding sextic CM-fields with $\mathrm{Gal}(L/\mathbb{Q}) \cong (C_2)^3 \rtimes S_3$

```
R.<X> = PolynomialRing(QQ)
F2.<a,b,c,x,y> = FreeGroup()
H2 = F2 / [a^2, b^2, c^2, x^3, y^2, a*b*a*b, a*c*a*c, b*c*b*c,
x*a*x^2*b, x*b*x^2*c, x*c*x^2*a, y*x*y*x, y*a*y*b, y*b*y*a, y*c*y*c,
x^2*y*x^2*y]
for A in range(1,10):
    for B in range(1,30):
        for C in range(1,30):
            if (X^6 + A*X^4 + B*X^2 + C).is_irreducible():
                K.<a> = NumberField(X^6 + A*X^4 + B*X^2 + C)
                if K.is_CM():
                    L.<b> = K.galois_closure()
                    G = L.galois_group()
                    GG = G.as_finitely_presented_group()
                    if GG.is_isomorphic(H2):
                        if K.class_number() == 1:
                            print(K)
```

For this code we get the following output.

Code 4: Output for Code 3

```
Number Field in a with defining polynomial X^6 + 7*X^4 + 10*X^2 + 2
Number Field in a with defining polynomial X^6 + 8*X^4 + 12*X^2 + 3
Number Field in a with defining polynomial X^6 + 9*X^4 + 14*X^2 + 4
Number Field in a with defining polynomial X^6 + 9*X^4 + 16*X^2 + 2
Number Field in a with defining polynomial X^6 + 9*X^4 + 17*X^2 + 8
Number Field in a with defining polynomial X^6 + 9*X^4 + 19*X^2 + 7
Number Field in a with defining polynomial X^6 + 9*X^4 + 21*X^2 + 8
```

### 4.2 Reflex field computation for $\mathrm{Gal}(L/\mathbb{Q}) \cong (C_2)^3 \rtimes C_3$

Let us take $K$ the CM-field with defining polynomial

$$f(x) = x^6 + 15x^4 + 14x^2 + 3.$$

For this field we have that the Galois group of the normal closure $L$ of $K$ is such that $\mathrm{Gal}(L/\mathbb{Q}) \cong (C_2)^3 \rtimes C_3$ and $K$ has class number one. We use Theorem 3.9 to find the reflex fields of $K$. Using SageMath we compute the fixed fields of the following groups: $\langle x \rangle$, $\langle xab \rangle$, $\langle xac \rangle$, $\langle xbc \rangle$ with the notation from Section 3.1.

First we begin with finding the Galois group of $L$ over $K$, in other words we want to find which elements fix $K$.

Code 5: Computing the reflex fields

```
X = polygen(QQ)
poly = X^6 + 15*X^4 + 14*X^2 + 3
K.<m> = NumberField(poly)
L.<n> = K.galois_closure()
G = L.galois_group()
(r0, s0, t0, u0) = G.gens()
r0.order()
s0.order()
t0.order()
u0.order()
```

The generators of $\mathrm{Gal}(L/\mathbb{Q})$ are of orders 2, 2, 3 and 2 respectively. From the investigation in Section 3.1 we know that $K$ is fixed by a group generated by 2 elements both of order 2. That is why we define number fields $K1$, $K2$ and $K3$.

Code 6: Code for computing the reflex fields

```
G1 = G.subgroup([u0, r0])
G2 = G.subgroup([s0, r0])
G3 = G.subgroup([u0, s0])
K1 = G1.fixed_field()[0]
K2 = G2.fixed_field()[0]
K3 = G3.fixed_field()[0]

K.is_isomorphic(K1)
K.is_isomorphic(K2)
K.is_isomorphic(K3)
```

We now check to which of these number fields is $K$ isomorphic. The output that we get is the following:

False
True
False

Therefore we have that $K \cong K2$ and moreover $\mathrm{Gal}(L/K) = G2 = \langle s0, r0 \rangle$. The next step is to find which elements correspond to the elements $a, b, c, x$ using the notation from Section 3.1. We already know that the order of $t0$ is 3 and and $K_+$ is Galois over $\mathbb{Q}$, hence $t0$ corresponds to $x$. Now we want to find the complex conjugation.

Code 7: Computing the reflex fields

```
r = r0.as_hom()
s = s0.as_hom()
t = t0.as_hom()
u = u0.as_hom()
```

```
embeds = K.embeddings(L)
for phi in embeds:
    print(L(u(phi(m))) == phi(m).conjugate())

s0*t0 == t0*r0
```

Since for each embedding the output is 'True', we get that the element $u0$ corresponds to complex conjugation $abc$. Moreover, since $s0 * t0 == t0 * r0$ also gives 'True', we get that $s0$ corresponds to $c$ and $r0$ to $b$. Therefore we can proceed with defining the subgroups $\langle x \rangle$, $\langle xab \rangle$, $\langle xac \rangle$, and $\langle xbc \rangle$ of $G$ and then finding the fixed fields which by Theorem 3.9 are the reflex fields of $K$.

Code 8: Computing the reflex fields

```
H1 = G.subgroup([t0])          # In our notation <t0> = <x>
H2 = G.subgroup([t0*r0*u0])    # In our notation <t0*u0*r0> = <xac>
H3 = G.subgroup([t0*u0*s0])    # In our notation <t0*u0*s0> = <xab>
H4 = G.subgroup([t0*r0*s0])    # In our notation <t0*r0*s0> = <xbc>
K1r = H1.fixed_field()
K2r = H2.fixed_field()
K3r = H3.fixed_field()
K4r = H4.fixed_field()
```

Finally, we get the following results:

$K_1^r$ is number field with defining polynomial:

$x^8 + 12x^7 + 90x^6 + 432x^5 + 1448x^4 + 3342x^3 + 5196x^2 + 4923x + 2077$

$K_2^r$ is number field with defining polynomial:

$x^8 + 12x^7 + 110x^6 + 612x^5 + 2472x^4 + 6786x^3 + 12758x^2 + 14541x + 7177$

$K_3^r$ is number field with defining polynomial:

$x^8 + 12x^7 + 250x^6 + 1872x^5 + 18048x^4 + 81342x^3 + 418300x^2 + 912675x + 2365111$

$K_4^r$ is number field with defining polynomial:

$x^8 + 12x^7 + 190x^6 + 1332x^5 + 9048x^4 + 35442x^3 + 96550x^2 + 146685x + 119911$

### 4.3 Reflex field computation for $\mathrm{Gal}(L/\mathbb{Q}) \cong (C_2)^3 \rtimes S_3$

Let us now consider $K$ the CM-field with defining polynomial

$$f(x) = x^6 + 7x^4 + 10x^2 + 2.$$

For this field we get that the Galois group of the normal closure $L$ of $K$ is such that $\mathrm{Gal}(L/\mathbb{Q}) \cong (C_2)^3 \rtimes S_3$ and $K$ has class number one. In order to find the reflex fields of $K$, using Theorem 3.16 we need to find the fixed fields by the following subgroups of $\mathrm{Gal}(L/\mathbb{Q})$: $\langle x, y \rangle$, $\langle xac, x^2y \rangle$, $\langle xab, xy \rangle$ and $\langle xbc, y \rangle$ using the notation from Section 3.2.

First we begin with finding which elements fix $K$.

Code 9: Computing the reflex fields

```
X = polygen(QQ)
poly = X^6 + 7*X^4 + 10*X^2 + 2
K.<m> = NumberField(poly)
L.<n> = K.galois_closure()
G = L.galois_group()

(r0, s0, t0, u0, v0) = G.gens()
r0.order()
s0.order()
t0.order()
u0.order()
v0.order()
```

We get that the orders of the generators of $G$ are 3, 2, 2, 2, 2, respectively. Since we know that $\#\,\mathrm{Gal}(L/K) = 8$, we need to try all the following combinations to see which elements fix $K$.

Code 10: Computing the reflex fields

```
G1 = G.subgroup([s0, t0, u0])
G2 = G.subgroup([s0, t0, v0])
G3 = G.subgroup([s0, u0, v0])
G4 = G.subgroup([t0, u0, v0])
K1 = G1.fixed_field()[0]
K2 = G2.fixed_field()[0]
K3 = G3.fixed_field()[0]
K4 = G4.fixed_field()[0]

K1.is_galois()
K2.is_galois()
K3.is_galois()
K4.is_galois()
```

The output for this code is the following:

False
True
False
False

Since $K2$ is Galois over $\mathbb{Q}$ and the only order 8 normal subgroup of $G$ is $\langle a, b, c\rangle$, we have that $\langle s0, t0, v0\rangle = \langle a, b, c\rangle$. That also implies that $\langle r0, u0\rangle = \langle x, y\rangle$.

Next we want to find the complex conjugation and using that we will find what elements correspond to the elements $a, b, c, x, y$.

Code 11: Computing the reflex fields

```
r = r0.as_hom()
s = s0.as_hom()
```

```
t = t0.as_hom()
u = u0.as_hom()
v = v0.as_hom()

embeds = K.embeddings(L)
for phi in embeds:
    print(L(v(phi(m))) == phi(m).conjugate())

t0*r0 == r0*s0*v0                  #ax = xc
s0*t0*r0 == r0*t0                  #bx = xb
s0*v0*r0 == r0*s0*t0               #cx = xa
t0*(r0*u0) == r0*u0*s0*t0          #ay = yb
s0*t0*(r0*u0) == (r0*u0)*t0        #by = ya
s0*v0*(r0*u0) == (r0*u0)*s0*v0     #cy = yc
(r0*u0)*r0 == r0^2*(r0*u0)         #yx = x^2y
```

Since all the outputs say 'True', this shows that $v0$ corresponds to complex conjugation $abc$. Futhermore, we get that $r0 = x$, $s0 = ab$, $t0 = a$ and $u0 = x^2y$.

Code 12: Computing the reflex fields

```
H1 = G.subgroup([r0,r0*u0])            # <x,y>
H2 = G.subgroup([r0*s0*t0*v0,u0])      # <xac,x^2y>
H3 = G.subgroup([r0*s0,r0^2*u0])       # <xab,xy>
H4 = G.subgroup([r0*t0*v0,r0*u0])      # <xbc,y>
K1r = H1.fixed_field()
K2r = H2.fixed_field()
K3r = H3.fixed_field()
K4r = H4.fixed_field()
```

Finally, we get the following results:

$K_1^r$ is number field with defining polynomial:
$x^8 - 408x^7 + 75744x^6 - 7767360x^5 + 480080844x^4 - 18556611408x^3 + 443169154368x^2$
$- 6012645546816x + 35489528179524$
$K_2^r$ is number field with defining polynomial:
$x^8 - 408x^7 + 99072x^6 - 14615424x^5 + 1407513996x^4 - 88174797264x^3 + 3523360622976x^2$
$- 82154208782016x + 879745494828996$
$K_3^r$ is number field with defining polynomial:
$x^8 - 408x^7 + 80928x^6 - 9370944x^5 + 699265548x^4 - 34351844688x^3 + 1095311139264x^2$
$- 20717588448576x + 184356641271492$
$K_4^r$ is number field with defining polynomial:
$x^8 - 408x^7 + 97920x^6 - 13640832x^5 + 1262978892x^4 - 75302469072x^3 + 2803143894912x^2$
$- 62138984096448x + 664976326747716$

# 5 Conclusion

In conclusion, the sextic CM-fields with Galois groups of the normal closure $(C_2)^3 \rtimes C_3$ or $(C_2)^3 \rtimes S_3$ were studied in order to compute the reflex types of these CM-fields. This was done using number theory and complex multiplication theory. The new results that have been computed are stated in Theorem 3.9 for the first case and Theorem 3.16 for the second case.

Furthermore, these computations can be used to compute the CM-class number one problem for the cases 3 and 4 of Theorem 2.19, which is still open for these two cases. Using SageMath we have found sextic CM-fields for these two cases and finally we have explicitly computed the reflex fields for two of these results, namely for the field with the defining polynomial $x^6 + 15x^4 + 14x^2 + 3$ and the field with the defining polynomial $x^6 + 7x^4 + 10x^2 + 2$.

## References


[1] A. Baker. Linear forms in the logarithms of algebraic numbers. I, II, III. *Mathematika*, 13:204–216; ibid. 14 (1967), 102–107; ibid. 14 (1967), 220–228, 1966.

[2] I. Bouw, J. Cooley, K. Lauter, E. Lorenzo García, M. Manes, R. Newton, and E. Ozman. Bad reduction of genus three curves with complex multiplication. In *Women in numbers Europe*, volume 2 of *Assoc. Women Math. Ser.*, pages 109–151. Springer, Cham, 2015.

[3] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[4] K. Heegner. Diophantische Analysis und Modulfunktionen. *Math. Z.*, 56:227–253, 1952.

[5] P. Kılıçer and M. Streng. The CM class number one problem for curves of genus 2. `https://arxiv.org/abs/1511.04869`, 2015.

[6] P. Kılıçer. The CM class number one problem for curves (doctoral dissertation). `https://openaccess.leidenuniv.nl/handle/1887/41145`, 2016.

[7] S. Lang. *Complex multiplication*, volume 255 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1983.

[8] D. A. Marcus. *Number fields*. Universitext. Springer, Cham, 2018. Second edition, With a foreword by Barry Mazur.

[9] J. S. Milne. Complex multiplication. `https://www.jmilne.org/math/CourseNotes/CM.pdf`.

[10] G. Shimura and Y. Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*, volume 6 of *Publications of the Mathematical Society of Japan*. The Mathematical Society of Japan, Tokyo, 1961.

[11] H. M. Stark. A complete determination of the complex quadratic fields of class-number one. *Michigan Math. J.*, 14:1–27, 1967.