university of groningen / faculty of science and engineering

# Classifying CM-fields of degree 8 and their applications

Bachelor's Project Mathematics

July 2023

Student: Jeroen van Haastert

First supervisor: Dr. P. Kılıçer

Second assessor: Prof. J.S. Müller

# Abstract

The first chapter of this bachelor thesis covers basic results about number fields and complex multiplication fields (CM-fields). In chapter 2, it is discussed that equivalent $\rho$-structures yield equivalent results in regards to primitive CM-types and reflex fields. Chapter 3 contains the full classification of intermediate CM-fields, primitive CM-types and reflex fields for all Galois CM-fields of degree 8 and all possible $\rho$-structures. The next chapter covers a complete classification of all $\rho$-structures of abelian Galois groups of finite degree. Lastly, the obtained theory and results on CM-fields are put in practice by showing that the Jacobian $J(C)$ is simple when $C$ is given by $\eta^2 = (s+2)(s^8 - 8s^6 + 20s^4 - 16s^2 + 2)$ or by the family of curves $y^m = x^d + 1$ with $m > d$ primes such that $m \equiv -1 \pmod{d}$.

# Contents

# Preface

Complex Multiplication fields (CM-fields) are defined to be totally imaginary fields that result from a degree 2 extension over a totally real field. The theory of CM originated from the study of abelian varieties. An abelian variety, $A$, is called simple if it is not isogenous to the product of lower dimension abelian varieties over an algebraically closed field; i.e. $A$ is simple if it does not allow for an embedding of an abelian variety of lower dimension.

If a field $K$ of degree $2g$ over $\mathbb{Q}$, embeds in the endomorphism algebra of an abelian variety $A$ with dimension $g$, then it is known that the field $K$ must be a CM-field. If this holds, we say that $A$ has CM by $K$. Through the complex representation of the endomorphism algebra, we can associate a CM-type $\Phi$ to $A$, where $\Phi$ consists of a set of $g$ embedding $\phi\colon K \to \mathbb{C}$, such that no two embeddings are complex conjugate to each other.

A CM-type $\Phi = \{\phi_1, \phi_2, \ldots, \phi_n\}$ of a CM-field $K$ can be induced from a CM-type $\Phi'$ on a field $K' \subseteq K$ if $\{\phi_1|_{K'}, \ldots, \phi_n|_{K'}\} = \Phi'$. If there exists no CM-type $\Phi'$ that induces $\Phi$, we call $\Phi$ primitive. It holds that the abelian variety $A$ is simple if and only if the associated CM-type $\Phi$ is primitive.

The study of CM is connected to projective smooth curves, through the Jacobian $J(C)$, which is an abelian variety. The Jacobians of curves are of interest in cryptography, and thus CM-fields play a crucial role in the study of these Jacobians.

# 1 Preliminaries

## 1.1 Basic Galois theory

We start by recalling the notions of Galois theory. In particular, we are interested in number fields, which are fields that are finite extensions of the rational numbers.

**Definition 1.1.1.** A *number field* $K$ is a field resulting from a finite field extension of $\mathbb{Q}$. Thus $\mathbb{Q} \subseteq K$ and $K$ has finite dimension when considered as vector space over $\mathbb{Q}$.

Number fields have certain desirable properties. In particular, the characteristic of number fields is 0.

**Lemma 1.1.2.** The characteristic of number fields is 0. In particular, if $K$ and $L$ are number fields, then $L/K$ is separable. □

Given that for any number field $K$ we have that $[K : \mathbb{Q}]$ is finite, and $K/\mathbb{Q}$ is separable, we can apply the primitive element theorem.

**Lemma 1.1.3.** Let $K$ be a number field, then there exists $\theta \in K$ such that $K = \mathbb{Q}(\theta)$. □

Let $p(x)$ denote the minimal polynomial of $\theta$. Then $p(x)$ has degree $n := [\mathbb{Q}(\theta) : \mathbb{Q}]$. Any field homomorphism of $\mathbb{Q}(\theta)$ is completely determined by the image of $\theta$. Moreover, the field homomorphism must send $\theta$ to one of the *algebraic conjugates* of $\theta$, which are the $n$ roots of $p(x)$.

**Definition 1.1.4.** A field extension $L$ over $K$ is said to be *normal* if any irreducible polynomial in $K[X]$ with at least one root in $L$ has all roots in $L$.

**Definition 1.1.5.** Field extensions that are both separable and normal are called *Galois extensions*. Note that any number field that is normal over $\mathbb{Q}$ is also Galois over $\mathbb{Q}$.

**Definition 1.1.6.** Let $K$ be a number field. The *Galois closure* of $K$, denoted by $K^{\mathrm{cl}}$, is the smallest field extensions such that $K^{\mathrm{cl}}$ is Galois over $\mathbb{Q}$. Upon writing $K = \mathbb{Q}(\theta)$, we have that $K^{\mathrm{cl}}$ is obtained by adding the conjugates of $\theta$ to $K$.

If $L/K$ is Galois, we may associate the Galois group with the extension $L/K$, subgroups of the Galois group correspond one to one with intermediate fields of $L$.

**Definition 1.1.7.** Let $L/K$ be a Galois extension. The group of automorphisms of $L$ fixing $K$ is called the *Galois group* and denoted by $\mathrm{Gal}(L/K)$.

**Theorem 1.1.8.** Let $L/K$ be a Galois extension and denote $G = \mathrm{Gal}(L/K)$ as the Galois group. We have that $[L : K] = |G|$. Furthermore we have,

- Let $H \subseteq G$ be a subgroup of $G$. Define $L^H$ to be the set of elements fixed by the automorphisms in $H$. Then $L^H$ is a subfield of $L$ with $[L : L^H] = |H|$;
- Let $L' \subseteq L$. Then the set of automorphisms of $L$ fixing $L'$ is a subgroup of $G$. □

We conclude that if $L/K$ is Galois, then there is a one-to-one correspondence between the subgroups of $\mathrm{Gal}(L/K)$ and the intermediate fields of $L$.

## 1.2 Embeddings

In the first part of this thesis, we are interested in determining CM-types for certain fields. In short, CM-types are sets of embeddings of a CM-field. We start by defining embeddings.

**Definition 1.2.1.** A *complex embedding* of a number field $K$ is a (injective) homomorphism $\phi\colon K \hookrightarrow \mathbb{C}$. Note that injectivity is not a necessary condition as field homomorphisms are always injective. We write $\Sigma_K$ to be the set of all embeddings of $K$ into $\mathbb{C}$.

**Definition 1.2.2.** Let $\phi$ be a complex embedding, we distinguish between 2 types of embeddings.

- An embedding $\phi \in \Sigma_K$ is a *real embedding* if $\phi(K) \subset \mathbb{R}$;
- An embedding $\phi \in \Sigma_K$ is a *complex embedding* if $\phi(K) \not\subset \mathbb{R}$, i.e. if $\phi$ takes complex values for some $x \in K$.

Using embeddings, we can define totally real and totally complex fields.

**Definition 1.2.3.**

- A number field $K$ is *totally real* if every complex embedding $\phi \in \Sigma_K$ is a real embedding.
- A number field $K$ is *totally complex* if every complex embedding $\phi \in \Sigma_K$ is a complex embedding.

Let $K$ be a number field and write $K = \mathbb{Q}(\theta)$. Then the number of embeddings is determined by the number of conjugates of $\theta$.

**Proposition 1.2.4.** Let $K$ be a number field, then there are $[K : \mathbb{Q}]$ distinct complex embeddings. Furthermore, each complex embedding $\phi \in \Sigma_K$ is such that $\phi(K) \subset K^{\mathrm{cl}}$.

*Proof.* Write $K = \mathbb{Q}(\theta)$ for some $\theta \in K$, and let $p(x) = \sum_{i=1}^{n} a_i x^i$ be the minimal polynomial of $\theta$. Recall that complex embeddings are field homomorphisms and thus

$$0 = \phi(0) = \phi(p(\theta)) = \phi(\Sigma_{i=1}^{n} a_i \theta^i) = \Sigma_{i=1}^{n} a_i \phi(\theta)^i.$$

This shows that complex embeddings permute the roots of the minimal polynomial of $\theta$. Since $p(x)$ is the minimal polynomial of field extension with degree $[\mathbb{Q}(\theta) : \mathbb{Q}] = n$, we get that $p(x)$ has $n$ distinct roots $\theta_1, \theta_2, \ldots, \theta_n$.

Define $\phi_i\colon \mathbb{Q}(\theta) \to \mathbb{C}$ by $\phi_i(\theta) = \theta_i$. It is straightforward to check that each $\phi_i$ forms an embedding. Thus there are $[K : \mathbb{Q}] = n$ distinct embeddings of $K$ into $\mathbb{C}$.

Lastly we show $\phi_i(K) \subset K^{\mathrm{cl}}$. Let $x \in \phi_i(\mathbb{Q}(\theta))$. Then $x$ is of the form

$$x = \phi_i\left(\sum_{j=1}^{n} c_j \theta^j\right) = \sum_{j=1}^{n} c_i \theta_i^j \in K^{\mathrm{cl}},$$

as $K^{\mathrm{cl}}$ contains all conjugates $\theta_1, \ldots, \theta_n$ of $\theta$. □

If $K$ is Galois over $\mathbb{Q}$, then it is easy to see if $K$ is a totally real field.

**Lemma 1.2.5.** Let $K$ be a number field that is Galois over $\mathbb{Q}$ and write $K = \mathbb{Q}(\theta)$. If $\theta \in \mathbb{R}$, then $\mathbb{Q}(\theta)$ is totally real.

*Proof.* Since $\mathbb{Q}(\theta)$ is Galois over $\mathbb{Q}$, the algebraic conjugates of $\theta$ must be contained in $\mathbb{Q}(\theta)$. Given that $\theta \in \mathbb{R}$, we have that $\mathbb{Q}(\theta) \subset \mathbb{R}$ and thus for all conjugates of $\theta$, denoted by $\theta_i$, it must hold that $\theta_i \in \mathbb{R}$. Let $\phi_i$ denote the embedding that is determined by sending $\theta$ to $\theta_i$. Then $\phi(\mathbb{Q}(\theta)) = \mathbb{Q}(\theta_i) \subset \mathbb{R}$ so that each $\phi_i$ is a real embedding and hence $\mathbb{Q}(\theta)$ is totally real. □

**Remark 1.2.6.** We have just seen that the image of each complex embedding of $K$ is contained in $K^{\mathrm{cl}}$. This leads to the idea that we can also consider the complex embeddings of $K$ into another field $L$, where $K^{\mathrm{cl}} \subseteq L$. Note that if $K^{\mathrm{cl}} \subseteq L$, then there are still $[K : \mathbb{Q}]$ embeddings of $K$ into $L$ as each complex embedding also gives an embedding in $L$. We formally introduce embeddings of $K$ into $L$.

**Definition 1.2.7.** Let $K$ and $L$ be fields such that $K \subset L$. Let $\phi \colon K \to L$ be a homomorphism of fields. Then $\phi$ is an embedding of $K$ with values in $L$.

**Remark 1.2.8.** If we say $\phi$ is an embedding of $K$ without specifying the range of $\phi$, we assume that $\phi \colon K \to K^{\mathrm{cl}}$.

Automorphisms of a field $K$ are in particular also embeddings of $K$. Thus, if $K$ is Galois over $\mathbb{Q}$, then each element in the Galois group yields an embedding.

**Theorem 1.2.9.** Let $K$ be a Galois number field over $\mathbb{Q}$. Then the embeddings (when viewing the embeddings as $\phi : K \to K^{\mathrm{cl}} = K$) agree with the elements in the Galois group.

*Proof.* For all $\phi_i \in \Sigma_K$ we have $\phi_i(K) \subset K^{\mathrm{cl}} = K$ (Proposition 1.2.4). Thus each $\phi_i$ maps $K$ to a subset of $K$. Furthermore, from the fact that $\mathbb{Q}(\theta) \cong \mathbb{Q}(\theta_i)$, we have that $\phi_i$ is an isomorphism and thus in particular an automorphism. Hereby it follows that $\phi_i \in \mathrm{Gal}(K/\mathbb{Q})$ and thus $\Sigma_K \subset \mathrm{Gal}(K/\mathbb{Q})$. Furthermore, since

$$n = |\Sigma_K| = [K : \mathbb{Q}] = |\mathrm{Gal}(K/\mathbb{Q})|,$$

we have that $\Sigma_K = \mathrm{Gal}(K/\mathbb{Q})$. □

**Remark 1.2.10.** Note that the embeddings only agree with the Galois group when restricting the image to $K$. This is allowed as Proposition 1.2.4, together with the above proof shows that $\phi(K) = K$. Throughout this thesis, all fields, unless stated otherwise, are Galois over $\mathbb{Q}$. Thus we will treat the embeddings as automorphisms and vice versa.

## 1.3 CM-fields

Complex multiplication fields (CM-fields) are a special type of number field.

**Definition 1.3.1.** A *CM-field* is a totally complex number field $K$ of degree $2g$ such that $K$ is a degree 2 extension of a totally real field $K_0$ of degree $g$.

Thus CM-fields are fields of the form $K_0(\sqrt{-r})$ where $0 << r \in K_0$ and $K_0$ is a real number field.

An equivalent definition is given in [Lan83].

**Proposition 1.3.2.** Let $K$ be a number field. The following 2 statements are equivalent;

1. $K$ is a CM-field;
2. The restriction of complex conjugation to $K$, denoted by $\rho$, is nontrivial and commutes with all embeddings of $K$.

This second condition is useful for proving the following corollaries.

**Corollary 1.3.3.** Let $K$ be a CM-field with intermediate field $K'$. Then $K'$ is either totally real or a CM-field.

*Proof.* For sake of contradiction, assume $K$ is a CM-field with intermediate field $K'$ where $K'$ is neither real nor a CM-field. Then there must exist an embedding $\phi' \in \Sigma_{K'}$ such that complex conjugation restricted to $K'$ does not commute with $\phi'$. However, now define $\phi$ to be an embedding of $K$ such that $\phi|_{K'} = \phi'$. Then $\phi \in \Sigma_K$ is an embedding that does not commute with complex conjugation, a contradiction. □

**Corollary 1.3.4.** Let $K$ be a CM-field that is Galois over $\mathbb{Q}$. From Theorem 1.2.9, we have that the elements in $\text{Gal}(K/\mathbb{Q})$ are also embeddings and thus $\rho$ is an order 2 element in the center of $\text{Gal}(K/\mathbb{Q})$.

**Corollary 1.3.5.** Let $\phi$ be an embedding of a CM-field $K$, and denote with $\rho$ complex conjugation restricted to $K$. Then $\bar{\phi} = \rho \circ \phi$ is also an embedding as $\rho$ is an automorphism of $K$.

Since CM-fields do not allow for totally real embeddings, $\phi$ and $\bar{\phi}$ are distinct. This means that embeddings of CM-fields always come in (complex) conjugate pairs.

**Definition 1.3.6.** Let $K$ be a CM-field of degree $2n$, write $\phi_1, \bar{\phi}_1, \phi_2, \bar{\phi}_2, \dots \phi_n, \bar{\phi}_n$ as the $2n$ embeddings. A CM-type is the pair $(K, \Phi)$ such that $\Phi = \{\phi_1, \phi_2, \dots \phi_n\}$ where each $\phi_i$ is chosen between $\phi$ or $\bar{\phi}$; i.e. non of the embeddings $\phi \in \Phi$ can be conjugate to each other.

Note that there are in total $2^n$ distinct CM-types as for each $i$, where $1 \leq i \leq n$, we have to choose between either $\phi_i$ or $\bar{\phi}_i$.

Just like the automorphisms can act on different embeddings, automorphisms can also act on CM-types, and take one CM-type to another CM-type.

**Definition 1.3.7.** Let $K$ be a CM-field, $\Phi := \{\phi_1, \phi_2, \ldots, \phi_n\}$ a CM-type and $\sigma \in \mathrm{Aut}(K)$. We define

$$\Phi\sigma := \{\phi_1 \circ \sigma, \phi_2 \circ \sigma, \ldots, \phi_n \circ \sigma\}.$$

Furthermore, if $K$ is Galois, we define $\sigma\Phi$ as

$$\sigma\Phi := \{\sigma \circ \phi_1, \sigma \circ \phi_2, \ldots, \sigma \circ \phi_n\}.$$

**Proposition 1.3.8.** Let $K$ be a CM-field, $\sigma \in \mathrm{Aut}(K)$ and let $\Phi$ be a CM-type of $K$. Then $\Phi\sigma$ is a CM-type as well. If $K$ is Galois over $\mathbb{Q}$, then $\sigma\Phi$ is also a CM-type.

*Proof.* Note that both $\sigma$ and $\phi_i \in \Phi$ are field homomorphisms so that $\phi_i \circ \sigma$ is a field homomorphism from $K \to K^{\mathrm{cl}}$ and thus an embedding of $K$. Therefore, to show that $\Phi\sigma$ is a CM-type of $K$, we need to show that $\phi_i\sigma$ and $\phi_j\sigma$ cannot be conjugates of each other.

$$\rho(\phi_i\sigma) = \phi_j\sigma \implies \rho\phi_i\sigma = \phi_j\sigma \implies \rho\phi_i = \phi_j.$$

This is a contradiction as CM-type do not contain conjugate embeddings. Thus $\Phi\sigma$ is a CM-type of $K$. Similar reasoning shows that $\sigma\Phi$ is a CM-type, where we use that $K$ is a Galois field to ensure $\sigma\phi$ is well-defined. □

**Definition 1.3.9.** Two CM-types $\Phi$ and $\Phi'$ of $K$ are called *equivalent* if there exist automorphism $\sigma \in \mathrm{Aut}(K)$ such that $\Phi\sigma = \Phi'$.

**Example 1.3.10.** For this example, we look at $K = \mathbb{Q}(\sqrt{2}, i)$. Note that $K$ is a CM-field as it is an imaginary quadratic extionsion of the field $\mathbb{Q}(\sqrt{2})$. We have $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and that elements in the $K$ are of the form $x = x_1 + x_2\sqrt{2} + x_2 i + x_3\sqrt{-2}$. Since $K$ is Galois over $\mathbb{Q}$, we have that the embeddings are given by the field automorphisms (see Theorem 1.2.9). Thus the embeddings are given by

$$\begin{cases} \phi_1(x) = x_1 + x_2\sqrt{2} + x_3 i + x_4\sqrt{-2}; \\ \bar{\phi}_1(x) = x_1 + x_2\sqrt{2} - x_3 i - x_4\sqrt{-2}; \\ \phi_2(x) = x_1 - x_2\sqrt{2} + x_3 i - x_4\sqrt{-2}; \\ \bar{\phi}_2(x) = x_1 - x_2\sqrt{2} - x_3 i + x_4\sqrt{-2}. \end{cases}$$

Now the $2^2 = 4$ CM-types are given by

$$\begin{cases} \Phi_1 = \{\phi_1, \phi_2\}; \\ \Phi_2 = \{\bar{\phi}_1, \phi_2\}; \\ \Phi_3 = \{\phi_1, \bar{\phi}_2\}; \\ \Phi_4 = \{\bar{\phi}_1, \bar{\phi}_2\}. \end{cases}$$

Since $\phi_2$ is also a field automorphism (again by Theorem 1.2.9), we can compute

$$\Phi_3\phi_2 = \{\phi_1 \circ \phi_2, \bar{\phi}_2 \circ \phi_2\} = \{\phi_2, \bar{\phi}_1\} = \Phi_2.$$

Thus we indeed see that acting on the CM-types by an automorphism of $K$ takes CM-types to other CM-types. In this case $\Phi_3\phi_2 = \Phi_2$ and thus $\Phi_3$ and $\Phi_2$ are equivalent types.

**Example 1.3.11.** For a second example, we look at the number field $K \coloneqq \mathbb{Q}(\zeta_{16})$, where $\zeta_{16}$ denotes the 16th root of unity. Note that $K$ is a CM-field as by Lemma 1.2.5 we have that $\mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})$ is a totally real subfield of $K$ with $[K : \mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})] = 2$. Thus $K$ is an imaginary quadratic extension of a totally real field and hence a CM-field.

We know that $\mathbb{Q}(\zeta_{16})$ is a cyclotomic field, and thus in particular a Galois field over $\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}_{16})^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_4$. Thus by Theorem 1.2.9, the embeddings of $K$ are given by the elements in the Galois group. As usual, the automorphisms in this group are uniquely determined by where they send a primitive element, in this case $\zeta_{16}$.

$$\begin{cases} \phi_1 : \zeta_{16} \to \zeta_{16} \implies \bar{\phi}_1 : \zeta_{16} \to \zeta_{16}^{-1}; \\ \phi_2 : \zeta_{16} \to \zeta_{16}^{3} \implies \bar{\phi}_2 : \zeta_{16} \to \zeta_{16}^{-3}; \\ \phi_3 : \zeta_{16} \to \zeta_{16}^{5} \implies \bar{\phi}_3 : \zeta_{16} \to \zeta_{16}^{-5}; \\ \phi_4 : \zeta_{16} \to \zeta_{16}^{7} \implies \bar{\phi}_4 : \zeta_{16} \to \zeta_{16}^{-7}. \end{cases}$$

Now the $2^4 = 16$ CM-types are given by sets of four embeddings in such a way that no two embeddings are complex conjugates. Two examples of CM-types are

$$\Phi_1 \coloneqq \{\phi_1, \phi_2, \phi_3, \phi_4\} \quad \text{and} \quad \Phi_2 \coloneqq \{\phi_1, \bar{\phi}_2, \bar{\phi}_3, \phi_4\}.$$

Since $\bar{\phi}_2 \in \mathrm{Gal}(K/\mathbb{Q})$ is an automorphism of $K$, we should have that $\Phi_1\bar{\phi}_2$ is another CM-type. Indeed note that

$$\Phi_1\bar{\phi}_2 = \{\phi_1 \circ \bar{\phi}_2, \phi_2 \circ \bar{\phi}_2, \phi_3 \circ \bar{\phi}_2, \phi_4 \circ \bar{\phi}_2\} = \{\bar{\phi}_2, \phi_4, \phi_1, \bar{\phi}_3\} = \Phi_2.$$

This also shows that $\Phi_1$ and $\Phi_2$ are equivalent CM-types.

**Definition 1.3.12.** Let $\Phi$ be a CM-type of $K$ where the embeddings in $\Phi$ take values in $L$, where $L$ is Galois over $\mathbb{Q}$. A CM-type of $L$ is *induced* by $\Phi$, denoted by $\Phi_L$, if

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

A CM-type is called *primitive* if it is not induced by a CM-type of a strict CM-subfield.

**Example 1.3.13.** Like Example 1.3.10, set $K \coloneqq \mathbb{Q}(\sqrt{2}, i)$, $K_1 \coloneqq \mathbb{Q}(i)$ and $K_2 \coloneqq \mathbb{Q}(\sqrt{-2})$, so that $K_1, K_2$ are the CM-subfields of $K$. Recall that the embeddings of $K$ are given by

$$\begin{cases} \phi_1(x) = x_1 + x_2\sqrt{2} + x_3 i + x_4\sqrt{-2}; \\ \bar{\phi}_1(x) = x_1 + x_2\sqrt{2} - x_3 i - x_4\sqrt{-2}; \\ \phi_2(x) = x_1 - x_2\sqrt{2} + x_3 i - x_4\sqrt{-2}; \\ \bar{\phi}_2(x) = x_1 - x_2\sqrt{2} - x_3 i + x_4\sqrt{-2}. \end{cases}$$

And a similar computation shows that the embeddings in $K_1$ are given by

$$\begin{cases} \phi_1'(x) = x_1 + x_2 i; \\ \bar{\phi}_1'(x) = x_1 - x_2 i. \end{cases}$$

Whereas the embeddings of $K_2$ are given by

$$\begin{cases} \phi_2'(x) = x_1 + x_2\sqrt{-2}; \\ \bar{\phi}_2'(x) = x_1 - x_2\sqrt{-2}. \end{cases}$$

Now, the four CM-types of $K$ are given by $\{\phi_1, \phi_2\}, \{\phi_1, \bar{\phi}_2\}, \{\bar{\phi}_1, \phi_2\}$ and $\{\bar{\phi}_1, \bar{\phi}_2\}$, whereas the CM-types of $K_1$ are given by $\{\phi_1'\}$ and $\{\bar{\phi}_1'\}$ and on $K_2$ by $\{\phi_2'\}$ and $\{\bar{\phi}_2'\}$.

Note that the restriction of the embeddings $\phi_1, \phi_2 \in \Sigma_K$ to $K_1$ give the embedding $\phi_1' \in \Sigma_{K_1}$ whereas $\bar{\phi}_1, \bar{\phi}_2$ restricted to $K_1$ give the embedding $\bar{\phi}_1' \in \Sigma_{K_1}$.

Similarly, the restriction of the embeddings $\phi_1, \bar{\phi}_2 \in \Sigma_K$ to $K_2$ give the embedding $\phi_2' \in \Sigma_{K_2}$ whereas $\bar{\phi}_1, \phi_2$ restricted to $K_2$ give the embedding $\bar{\phi}_2' \in \Sigma_{K_2}$. This shows that

- The CM-type $\{\phi_1, \phi_2\}$ of $L$ is induced by the CM-type $\{\phi_1'\}$ of $K_1$;
- The CM-type $\{\bar{\phi}_1, \phi_2\}$ of $L$ is induced by the CM-type $\{\bar{\phi}_2'\}$ of $K_2$;
- The CM-type $\{\phi_1, \bar{\phi}_2\}$ of $L$ is induced by the CM-type $\{\phi_2'\}$ of $K_2$;
- The CM-type $\{\bar{\phi}_1, \bar{\phi}_2\}$ of $L$ is induced by the CM-type $\{\bar{\phi}_1'\}$ of $K_1$.

Thus we see that in this example, none of the CM-types of $K$ are primitive as each CM-type is induced from a CM-type of the strict CM-subfields $K_1$ or $K_2$.

**Example 1.3.14.** Similar to Example 1.3.11, we take $K = \mathbb{Q}(\zeta_{16})$, and set $K_1 = \mathbb{Q}(\sqrt{-2})$. Note that we have $(\zeta_{16}^4)((\zeta_{16} - \zeta_{16}^{-1})^2 - 2) = \sqrt{-2}$ so that $K_1$ is a CM-subfield of $K$.

Since $K_1$ is a Galois CM-field, the embeddings are given by the elements in $\mathrm{Gal}(K_1/\mathbb{Q})$. Note that elements $x \in K_1$ can be written as $x = x_1 + x_2\sqrt{-2}$ so that we can write the embeddings as follows:

$$\begin{cases} \phi'(x) = x_1 + x_2\sqrt{-2}; \\ \bar{\phi}'(x) = x_1 - x_2\sqrt{-2}. \end{cases}$$

Thus the 2 CM-types of $K_1$ are given by $\{\phi'\}$ and by $\{\bar{\phi}'\}$. In this example, we show that the CM-type $\Phi_1 := \{\phi_1, \phi_2, \bar{\phi}_3, \bar{\phi}_4\}$ (embeddings as in Example 1.3.11) is induced by the CM-type $\{\phi'\}$ on $K_1$, while $\{\bar{\phi}_1, \bar{\phi}_2, \phi_3, \phi_4\}$ is induced by $\{\bar{\phi}'\}$. For this, we need to compute how the embeddings are restricted to $K_1$.

$$\begin{aligned} \phi_k(\sqrt{-2}) &= (\phi_k(\zeta_{16}))^4(\phi_k(\zeta_{16}) - \phi_k(\zeta_{16}^{-1}))^2 - \phi_k(2)) \\ &= (\zeta_{16}^{2k+1})^4((\zeta_{16}^{2k+1} - \zeta_{16}^{-2k-1})^2 - 2) \\ &= (-1)^k\sqrt{-2}(\cos(k\pi/2) - \sin(k\pi/2)) \\ &= \begin{cases} \sqrt{-2} \text{ when } k = 0, 1 \\ -\sqrt{-2} \text{ when } k = 2, 3. \end{cases} \end{aligned}$$

This shows that the embeddings $\phi_1, \phi_2, \bar{\phi}_3$ and $\bar{\phi}_4$ restricted to $K_1$ fix $\sqrt{-2}$ and thus agree with $\phi'$, whereas $\bar{\phi}_1, \bar{\phi}_2, \phi_3$ and $\phi_4$ restricted to $K_1$ send $\sqrt{-2}$ to $-\sqrt{-2}$ and hence restrict to $\bar{\phi}'$.

We conclude that the CM-type $\{\phi_1, \phi_2, \bar{\phi}_3, \bar{\phi}_4\}$ is induced by $\{\phi'\}$ while $\{\bar{\phi}_1, \bar{\phi}_2, \phi_3, \phi_4\}$ is induced by $\{\bar{\phi}'\}$.

In practice, one is mostly interested in finding which CM-types are primitive. This is usually not done via computations similar to above, but instead by making use of the following result.

**Theorem 1.3.15.** [Mil, Proposition 1.9] Each CM-pair $(K, \Phi)$ is induced by a unique primitive CM-pair $(K', \Phi')$ where $K' \subseteq K$.

Furthermore, denote with $\Phi_{K^{\mathrm{cl}}}$ the CM-type of $K^{\mathrm{cl}}$ that is induced by $\Phi$. Then we have that $K'$ is given by the fixed field of

$$\mathrm{Gal}(K^{\mathrm{cl}}/K') = \{\sigma \in \mathrm{Gal}(K^{\mathrm{cl}}/\mathbb{Q}) \mid \Phi_{K^{\mathrm{cl}}}\sigma = \Phi_{K^{\mathrm{cl}}}\}.$$

□

**Remark 1.3.16.** In the case that $K$ is Galois, the theorem becomes significantly easier to use as it translates into: Let $\Phi$ be a CM-type of the Galois field $K$. Then $\Phi$ is induced by a primitive CM-type of the field fixed by

$$\mathrm{Gal}(K/K') = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \Phi\sigma = \Phi\}.$$

In particular, Theorem 1.2.9 also tells us that the automorphisms are given by the embeddings, thus we may use both to check primitivity of $\Phi$.

**Example 1.3.17.** We use Theorem 1.3.15 to verify the result in Example 1.3.14; i.e. we show that $\{\phi_1, \phi_2, \bar{\phi}_3, \bar{\phi}_4\}$ is induced by a CM-type of the CM-subfield $\mathbb{Q}(\sqrt{-2})$. By computing $\Phi\sigma$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, we find that

$$\{\phi_1, \phi_2, \bar{\phi}_3, \bar{\phi}_4\}\sigma = \{\phi_1, \phi_2, \bar{\phi}_3, \bar{\phi}_4\} \iff \sigma \in \{\phi_1, \phi_2, \bar{\phi}_3, \bar{\phi}_4\}.$$

Thus from Theorem 1.3.15, we know that $\{\phi_1, \phi_2, \bar{\phi}_3, \bar{\phi}_4\}$ is induced by a CM-type of the field fixed by $H \coloneqq \{\phi_1, \phi_2, \bar{\phi}_3, \bar{\phi}_4\}$. This field has degree $[\mathrm{Gal}(K/\mathbb{Q}) : H] = 2$ over $\mathbb{Q}$, by the Galois correspondence. Furthermore, from Example 1.3.14, we know that the automorphisms $\{\phi_1, \phi_2, \bar{\phi}_3, \bar{\phi}_4\}$ all send $\sqrt{-2} \to \sqrt{-2}$ and thus the fixed field of $\{\phi_1, \phi_2, \bar{\phi}_3, \bar{\phi}_4\}$ is $\mathbb{Q}(\sqrt{-2})$. Which again shows that $\{\phi_1, \phi_2, \bar{\phi}_3, \bar{\phi}_4\}$ is induced by a CM-type of the CM-subfield $\mathbb{Q}(\sqrt{-2})$.

**Remark 1.3.18.** In a more concrete sense, as in the case above, using Theorem 1.3.15 is straightforward. However, in the case of more abstract Galois groups, it is not always clear which element represent complex conjugation. From Theorem 1.3.4, we know that $\rho$ must be represented by an order 2 element in the center of the Galois group. However, this may not always yield a unique element to represent complex conjugation. Furthermore, different choices of complex conjugation can (but often will not) lead to different primitive CM-types.

**Example 1.3.19.** In this example, we again take $K = \mathbb{Q}(\sqrt{2}, i)$. We know $K$ is Galois with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, thus the embeddings are given by the automorphisms in the Galois group (see Theorem 1.2.9). To specify the 4 CM-types, we need to know which of these automorphisms are complex conjugate to each other. For this we first have to choose an element in the Galois group that represents complex conjugation. From Theorem 1.3.2, we have that complex conjugation, denoted by $\rho$, is an element of order 2 in the center of the Galois group. This leaves us with 3 choices for $\rho$, as given below. We will analyse the primitive CM-types for the first 2 choices of complex conjugation.

$$\rho_1 \coloneqq (1, 0),\ \rho_2 \coloneqq (0, 1) \text{ and } \rho_3 \coloneqq (1, 1).$$

**Fixing conjugation as $(1,0)$:**
If we fix complex conjugation $\rho_1 = (1,0)$, then we have the embeddings

$$\phi_1 = (0,0),\ \phi_2 = (0,1) \implies \bar{\phi}_1 = (1,0),\ \bar{\phi}_2 = (1,1).$$

Thus the $2^2 = 4$ CM-types of $K$ are given by

$$\{\phi_1, \phi_2\},\ \{\phi_1, \bar{\phi}_2\},\ \{\bar{\phi}_1, \phi_2\} \text{ and } \{\bar{\phi}_1, \bar{\phi}_2\}.$$

To use Theorem 1.3.15, we need to find the automorphisms $\sigma \in \mathbb{Z}_2 \times \mathbb{Z}_2$ for which we have $\Phi\sigma = \Phi$. For the CM-type $\{\phi_1, \phi_2\}$, we note that

$$\begin{cases} \{\phi_1, \phi_2\}(0,0) = \{(0,0)+(0,0), (0,1)+(0,0)\} = \{\phi_1, \phi_2\}; \\ \{\phi_1, \phi_2\}(0,1) = \{(0,0)+(0,1), (0,1)+(0,1)\} = \{\phi_2, \phi_1\}; \\ \{\phi_1, \phi_2\}(1,0) = \{(0,0)+(1,0), (0,1)+(1,0)\} = \{\bar{\phi}_1, \bar{\phi}_2\}; \\ \{\phi_1, \phi_2\}(1,1) = \{(0,0)+(1,1), (0,1)+(1,1)\} = \{\bar{\phi}_2, \bar{\phi}_1\}. \end{cases}$$

Thus the automorphisms fixing $\{\phi_1, \phi_2\}$ are given by $\{(0,0), (0,1)\}$, hence $\{\phi_1, \phi_2\}$ is induced by a type on the field fixed by $\langle(0,1)\rangle$. Similar computations show that

- The CM-type $\{\phi_1, \phi_2\}$ is induced by a CM-type of the field $K^{\langle(0,1)\rangle}$;
- The CM-type $\{\phi_1, \bar{\phi}_2\}$ is induced by a CM-type of the field $K^{\langle(1,1)\rangle}$;
- The CM-type $\{\bar{\phi}_1, \phi_2\}$ is induced by a CM-type of the field $K^{\langle(1,1)\rangle}$;
- The CM-type $\{\bar{\phi}_1, \bar{\phi}_2\}$ is induced by a CM-type of the field $K^{\langle(0,1)\rangle}$.

Note that upon writing $K = \mathbb{Q}(i, \sqrt{2})$ as in Example 1.3.13 and identifying

$$\begin{cases} (0,0) = x_1 + x_2\sqrt{2} + x_3 i + x_4\sqrt{-2}; \\ (1,0) = x_1 + x_2\sqrt{2} - x_3 i - x_4\sqrt{-2}; \\ (0,1) = x_1 - x_2\sqrt{2} + x_3 i - x_4\sqrt{-2}; \\ (1,1) = x_1 - x_2\sqrt{2} - x_3 i + x_4\sqrt{-2}, \end{cases}$$

shows that the results agree with Example 1.3.13, since

$$K^{\langle(0,1)\rangle} = \mathbb{Q}(i) \text{ and } K^{\langle(1,1)\rangle} = \mathbb{Q}(\sqrt{-2}).$$

**Fixing conjugation as $(0,1)$:**
Next, we claim that choosing $\rho_2 = (0,1)$ yields the same results. Instead of running through the same computations, we use a more general approach that relies on the fact that there exists an automorphism $f$ of $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ such that $f(\rho_1) = \rho_2$. Intuitively, such an automorphism relables $\rho_1 = (1,0)$ into $\rho_2 = (0,1)$ without affecting the structure of the group. First note that $f$ as defined below is indeed an automorphism of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

$$f(0,0) = (0,0),\ f(1,0) = (0,1),\ f(0,1) = (1,0) \text{ and } f(1,1) = (1,1).$$

Since $K$ is Galois, we use Theorem 1.2.9 to give that we may apply the automorphism $f$ on the embeddings too.

$$f(\phi_1) = f(0,0) = (0,0),\ f(\phi_2) = (1,0) \implies f(\bar{\phi}_1) = (0,1),\ f(\bar{\phi}_2) = f(1,1) = (1,1).$$

Here, the conjugate pairs $\phi_i$ and $\bar{\phi}_i$ are conjugate with respect to $\rho_1 = (1, 0)$. While $f(\phi_i)$ and $f(\bar{\phi}_i)$ are conjugate with respect to $\rho_2 = (0, 1)$.

We write $f(\Phi)$ to denote $\{f(\phi_1), f(\phi_2)\}$. Then note that

$$\Phi\sigma = \Phi \iff f(\Phi\sigma) = f(\Phi) \iff f(\Phi) \circ f(\sigma) = f(\Phi).$$

This shows that $f(\sigma)$ fixes $f(\Phi)$ precisely when $\sigma$ fixes $\Phi$. This leads to the following:

$$\Phi \text{ is induced by } (K^H, \Phi') \implies f(\Phi) \text{ is induced by } K^{f(H)}.$$

This shows that $f(\Phi)$ is a primitive CM-type of the same field as the primitive CM-type $\Phi$ up to relabeling the elements in $\mathrm{Gal}(K/\mathbb{Q})$. This idea is formally proven in Section 2.

### 1.3.1 Reflex fields

Let $K$ be a CM-field and let $\Phi$ be a CM-type of $K$. Let $\Phi_{K^{\mathrm{cl}}}$ denote a CM-type of $K^{\mathrm{cl}}$ induced by $\Phi$. Since $K^{\mathrm{cl}}$ is Galois over $\mathbb{Q}$, the embeddings in the CM-type $\Phi_{K^{\mathrm{cl}}}$ are each automorphisms of $K^{\mathrm{cl}}$ and thus each have inverses (Theorem 1.2.9). Denote the CM-type containing this set of inverses with $\Phi^{-1}_{K^{\mathrm{cl}}}$. The unique primitive CM-pair $(K^r, \Phi^r)$ that induces $\Phi^{-1}_{K^{\mathrm{cl}}}$ is called the reflex pair of $(K, \Phi)$.

**Definition 1.3.20.** Let $K$ be a CM field with CM-type $\Phi$. Then the reflex pair $(K^r, \Phi^r)$ is the unique primitive CM-pair that induces $\Phi^{-1}_{K^{\mathrm{cl}}}$ as defined above.

We can also take the reflex of the reflex.

**Lemma 1.3.21.** Let $(K, \Phi)$ be a CM-type, we have that $K^{rr} \subset K$ and that $\Phi^{rr}$ induces $\Phi$. If $\Phi$ is primitive, then $K^{rr} = K$ and $\Phi^{rr} = \Phi$.

*Proof.* Note that the extension of $\Phi^r$ to $K^{\mathrm{cl}}$ is given by $\Phi^{-1}_{K^{\mathrm{cl}}}$. Then taking the inverse embeddings gives us $\Phi_{K^{\mathrm{cl}}}$. By definition, $\Phi^{rr}$ is now given by the primitive CM-type that induces $\Phi_{K^{\mathrm{cl}}}$. This shows that $\Phi^{rr}$ also induces $\Phi$ and thus $K^{rr} \subset K$.

If $\Phi$ is primitive, the only CM-type inducing $\Phi$ is given by $\Phi$ itself. In this case, we may conclude $\Phi^{rr} = \Phi$ and $K^{rr} = K$. □

**Theorem 1.3.22.** Let $(K, \Phi)$ be a CM-pair. The reflex field $K^r$ is the fixed field of

$$\mathrm{Gal}(K^{\mathrm{cl}}/K^r) = \{\sigma \in \mathrm{Gal}(K^{\mathrm{cl}}/\mathbb{Q}) \mid \sigma\Phi_{K^{\mathrm{cl}}} = \Phi_{K^{\mathrm{cl}}}\}.$$

*Proof.* By definition of the reflex field, we know that $K^r$ is given by the unique primitive pair $(K^r, \Phi^r)$ that induces $\Phi^{-1}_{K^{\mathrm{cl}}}$. By Theorem 1.3.15, this field is fixed by $\tau \in \mathrm{Gal}(K^{\mathrm{cl}}/\mathbb{Q})$ such that $\Phi^{-1}_{K^{\mathrm{cl}}}\tau = \Phi^{-1}_{K^{\mathrm{cl}}}$; i.e. we have $\{\phi_1^{-1} \circ \tau, \phi_2^{-1} \circ \tau, \ldots, \phi_n^{-1} \circ \tau\} = \{\phi_1^{-1}, \phi_2^{-1}, \ldots, \phi_n^{-1}\}$. Write $\tau = (\tau^{-1})^{-1}$ so that $\phi_i^{-1} \circ \tau = \phi_i^{-1} \circ (\tau^{-1})^{-1} = (\tau^{-1} \circ \phi)^{-1}$. Setting $\sigma = \tau^{-1}$ yields that $\{(\sigma \circ \phi_1)^{-1}, \ldots, (\sigma \circ \phi_n)^{-1}\} = \{(\phi_1)^{-1}, \ldots, (\phi_n)^{-1}\}$. Lastly, make the observation that $(\sigma\phi_i)^{-1} = (\phi_j)^{-1} \iff \sigma\phi_i = \phi_j$ which finishes the results as we may get rid of the inverses. □

**Remark 1.3.23.** If $K$ is a Galois CM-field over $\mathbb{Q}$, then Theorem 1.3.22 shows that the reflex field of $K$ is given by the fixed field of

$$\mathrm{Gal}(K/K^r) = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \sigma\Phi = \Phi\}.$$

**Corollary 1.3.24.** Reflex fields are CM-fields.

*Proof.* From Theorem 1.3.22, we know that the reflex field $K^r$ of $(K, \Phi)$ is given by the fixed field of $\sigma \in \mathrm{Gal}(K^{\mathrm{cl}}/\mathbb{Q})$ such that $\sigma\Phi_{K^{\mathrm{cl}}} = \Phi_{K^{\mathrm{cl}}}$. Note that $\rho$ cannot fix $\Phi_{K^{\mathrm{cl}}}$ as it conjugates all embeddings, thus $K^r$ is not fixed by complex conjugation and hence cannot be a totally real field. By Theorem 1.3.3, we conclude that $K^r$ is a CM-field. □

### 1.3.2 Equivalent CM-types

Recall that two CM-types $\Phi_1$ and $\Phi_2$ of $K$ are equivalent if there exists an automorphism of $K$ such that $\Phi_1\sigma = \Phi_2$. We will show that equivalent CM-types form a partition of the set of CM-types of $K$.

**Lemma 1.3.25.** Let $K$ be a CM-field that is Galois over $\mathbb{Q}$ with $G \coloneqq \mathrm{Gal}(K/\mathbb{Q})$ and CM-types $X = \{\Phi_i\}$. Then $G$ acts on $X$ from both the left and the right via $a_1, a_2 \colon X \times G \to X$ defined as $a_1(\Phi, \sigma) = \Phi\sigma$ and $a_2(\Phi, \sigma) = \sigma\Phi$ respectively.

*Proof.* From Proposition 1.3.8, note that $a_1(\Phi, \sigma) \in X$ and $a_2(\Phi, \sigma) \in X$. Furthermore, it can be checked that $a_1$ and $a_2$ satisfy the definition of an action. □

**Lemma 1.3.26.** Let $K$ be a Galois CM-field and $\Phi$ a CM-type. The equivalent CM-types are given by the orbit of $\Phi$ of the right action as defined in Lemma 1.3.25.

*Proof.* The equivalent CM-types of $\Phi$ are given by $\{\Phi\sigma \mid \sigma \in \mathrm{Gal}(K/\mathbb{Q})\}$. Note that this is the definition of the orbit of action $a_1$ as defined in Lemma 1.3.25. □

**Remark 1.3.27.** Since $G$ defines an action on the set of CM-types $X = \{\Phi_i\}$, we have that the orbits give a partition on the set of CM-types. Thus being equivalent CM-types defines an equivalence relation.

**Theorem 1.3.28.** Let $K$ be a Galois CM-field with a CM-type $\Phi$ and $|\mathrm{Gal}(K/\mathbb{Q})| = 2n$. Then $\Phi$ is primitive if and only if $\Phi$ has $2n$ equivalent CM-types.

*Proof.* The CM-type $\Phi$ has $2n$ equivalent CM-types precisely when $|\mathrm{Orb}(\Phi)| = 2n$. By the orbit stabilizer theorem, we have $\mathrm{Stab}(\Phi) = |\mathrm{Gal}(K/\mathbb{Q})|/|\mathrm{Orb}(\Phi)| = 1$. Thus there is only one element $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\Phi\sigma = \Phi$, hence Theorem 1.3.15 tells us that $\Phi$ is primitive. □

**Remark 1.3.29.** Note that the above definitions and proofs also hold when $K$ is not Galois, but then we have to replace $\Phi$ by a CM-type $\Phi_{K^{\mathrm{cl}}}$ where $\Phi_{K^{\mathrm{cl}}}$ is induced by $\Phi$.

**Theorem 1.3.30.** Let $K$ be a CM-field that is Galois over $\mathbb{Q}$ with CM-types $\Phi_1$ and $\Phi_2$, which are induced by $(K'_1, \Phi'_1)$ and $(K'_2, \Phi'_2)$ respectively. If $\Phi_1$ and $\Phi_2$ are equivalent, then $K'_1 = K'_2$.

*Proof.* Let $\Phi_1$ and $\Phi_2$ be equivalent CM-types and write $\Phi_1\tau = \Phi_2$ for some $\tau \in \mathrm{Aut}(K)$. By Theorem 1.3.15, we know that $K'_1$ is the fixed field of $\{\sigma \in \mathrm{Gal}(K^{\mathrm{cl}}/\mathbb{Q}) \mid \Phi_1\sigma = \Phi_1\}$. In particular, we have

$$\begin{aligned}\{\sigma \in \mathrm{Gal}(K^{\mathrm{cl}}/\mathbb{Q}) \mid \Phi_1\sigma = \Phi_1\} &= \{\sigma \in \mathrm{Gal}(K^{\mathrm{cl}}/\mathbb{Q}) \mid \Phi_1\sigma\tau = \Phi_1\tau\} \\ &= \{\sigma \in \mathrm{Gal}(K^{\mathrm{cl}}/\mathbb{Q}) \mid \Phi_1\tau\sigma = \Phi_1\tau\} \\ &= \{\sigma \in \mathrm{Gal}(K^{\mathrm{cl}}/\mathbb{Q}) \mid \Phi_2\sigma = \Phi_2\}.\end{aligned}$$

The second equality holds since $\{\sigma\tau \mid \sigma \in \mathrm{Gal}(K^{\mathrm{cl}}/\mathbb{Q})\} = \{\tau\sigma \mid \sigma \in \mathrm{Gal}(K^{\mathrm{cl}}/\mathbb{Q})\}$. This shows that $K'_1 = K'_2$ as the fields are fixed by the same automorphisms. □

**Corollary 1.3.31.** Let $\Phi$ and $\Phi'$ be equivalent CM-types, then $\Phi$ is primitive if and only if $\Phi'$ is primitive.

**Theorem 1.3.32.** Let $K$ be a CM-field with reflex pairs $(K_1^r, \Phi_1)$ and $(K_2^r, \Phi_2)$. If $\Phi_1$ and $\Phi_2$ are equivalent, then $K_1^r = K_2^r$.

*Proof.* Let $\Phi_1$ and $\Phi_2$ be equivalent CM-types and write $\Phi_1\tau = \Phi_2$ for some $\tau \in \mathrm{Aut}(K)$. By Theorem 1.3.22, we know that $K_1^r$ is the fixed field of $\{\sigma \in \mathrm{Gal}(K^{\mathrm{cl}}/\mathbb{Q}) \mid \sigma\Phi_1 = \Phi_1\}$.

$$\begin{aligned}\{\sigma \in \mathrm{Gal}(K^{\mathrm{cl}}/\mathbb{Q}) \mid \sigma\Phi_1 = \Phi_1\} &= \{\sigma \in \mathrm{Gal}(K^{\mathrm{cl}}/\mathbb{Q}) \mid \sigma\Phi_1\tau = \Phi_1\tau\} \\ &= \{\sigma \in \mathrm{Gal}(K^{\mathrm{cl}}/\mathbb{Q}) \mid \sigma\Phi_2 = \Phi_2\}.\end{aligned}$$

This shows that $K_1^r$ and $K_2^r$ are fixed by the same automorphisms and thus $K_1^r = K_2^r$. □

### 1.3.3 Reflex fields for abelian Galois groups

In the case that $K$ is a Galois CM-field with abelian Galois group, we can relate the reflex fields with the primitivity of a CM-type $\Phi$. This will be highlighted in this section.

**Theorem 1.3.33.** Let $K$ be a CM-field that is Galois over $\mathbb{Q}$ with abelian Galois group. Assume that $(K, \Phi)$ is a CM-pair induced by $(K', \Phi')$ with reflex field $K^r$. Then $K' = K^r$.

*Proof.* From Theorems 1.3.15 and 1.3.22, we have

$$\mathrm{Gal}(K/K') = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \Phi\sigma = \Phi\} = \{\sigma \in \mathrm{Gal} \mid \sigma\Phi = \Phi\} = (K/\mathbb{Q})\} = \mathrm{Gal}(K/K^r).$$

Here we use that $\sigma\Phi = \Phi\sigma$ since $\mathrm{Gal}(K/\mathbb{Q})$ is abelian. Thus we conclude $K^r = K'$. □

**Corollary 1.3.34.** Let $K$ be a CM-field that is Galois over $\mathbb{Q}$ with abelian Galois group, together with primitive CM-type $\Phi$ which has reflex $K^r$. Then $K^r = K$. □

# 2 Equivalent actions and $\rho$-structures

Our aim is to classify all primitive CM-types and reflex fields of Galois CM-fields of degree 8. For this, we take the same course of action as in the example of the degree 4 Galois CM-field in Example 1.3.19.

1. Fix a group $G$ of order 8;
2. Fix an element of order 2 in the center of $G$ to represent complex conjugation;
3. Determine the primitive CM-types and reflex fields using Theorems 1.3.15 and 1.3.22.

This process will be repeated over all possible groups of order 8 and all possible choices of complex conjugation.

**Theorem 2.0.1.** There are five groups of order 8. The groups together with possible representatives for $\rho$ are given below.

- $D_4 = \langle a, b \mid a^4 = b^2 = e, ab = ba^{-1} \rangle$ where $\rho = a^2$;
- $Q_8 = \langle i, j, k \mid i^2 = j^2 = ijk = -1 \rangle$ where $\rho = -1$;
- $\mathbb{Z}_8$ where $\rho = \bar{4}$;
- $\mathbb{Z}_2 \times \mathbb{Z}_4$ where $\rho \in \{(1,0), (0,2), (1,2)\}$;
- $(\mathbb{Z}_2)^3$ where $\rho \in \{(1,0,0), (0,1,0), (0,0,1), (1,1,0), (1,0,1), (0,1,1), (1,1,1)\}$. □

As one can see, the analysis for the groups $D_4, Q_8$ and $\mathbb{Z}_8$ can be done quick as there is a unique element of order 2 in the center of the group. However, the groups $\mathbb{Z}_2 \times \mathbb{Z}_4$ and $(\mathbb{Z}_2)^3$ require more work. To reduce the casework, we introduce the notion of $\rho$-equivalence.

As explained in Example 1.3.19, $\rho$-equivalence encapsulates the idea that if 2 elements of order 2 in the center of the group can be interchanged using a group automorphism, then they must lead to the same primitive CM-types and reflex fields. This idea can be formalized via the notion of equivalent orbits.

**Definition 2.0.2.** Let $G_1 \cong G_2$ via isomorphism $f$. Moreover, let $X_1$ and $X_2$ be sets with bijection $\psi \colon X_1 \to X_2$. Assume that $G_1, G_2$ act on $X_1, X_2$ via $a_1, a_2$ respectively. If $\psi(a_1(g,x)) = a_2(f(g), \psi(x))$, then the $a_1$ and $a_2$ are called *equivalent actions.*

Equivalent actions have, up to relabeling the elements by automorphism $f$ and bijection $\psi$, the same orbits and stabilizer.

**Theorem 2.0.3.** Let $G_1 \cong G_2$ be groups acting on $X_1, X_2$ via equivalent actions $a_1, a_2$ respectively. Let $x_0 \in X_1$ be arbitrary. Then $\mathrm{Orb}(\psi(x_0)) = \{\psi(x) \mid x \in \mathrm{Orb}(x_0)\}$.

*Proof.* The orbit of $\psi(x_0) \in X_2$ is given by $\mathrm{Orb}(\psi(x_0)) = \{a_2(g, \psi(x_0)) \mid g \in G_2\}$. Since we have $G_1 \cong G_2$ via isomorphism $f$, we may write each $g \in G_2$ as $f(g')$ for some element $g' \in G_1$. Thus we find $\mathrm{Orb}(\psi(x_0)) = \{a_2(f(g'), \psi(x_0)) \mid g' \in G_2\}$. Using the definition of equivalent orbits, we get $\mathrm{Orb}(\psi(x_0)) = \{\psi(a_1(g', x_0) \mid g' \in G_2\}$, which shows that $\mathrm{Orb}(\psi(x_0)) = \{\psi(x) \mid x \in \mathrm{Orb}(x_0)\}$. □

**Theorem 2.0.4.** Let $G_1 \cong G_2$ be groups acting on $X_1, X_2$ via equivalent actions $a_1, a_2$ respectively. Let $x_0 \in X_1$ be arbitrary, then $\operatorname{Stab}(\psi(x_0)) = \{f(g) \mid g \in \operatorname{Stab}(x_0)\}$.

*Proof.* The stabilizer of $\psi(x_0)$ is given by $\operatorname{Stab}(\psi(x_0)) = \{g \in G_2 \mid a_2(g, \psi(x_0)) = \psi(x_0)\}$. Since $G_1 \cong G_2$ via isomorphism $\phi$, we have that for each $g \in G_2$, we may assign $g' \in G_1$ such that $f(g') = g$. Thus we get $\operatorname{Stab}(\psi(x_0)) = \{f(g') \in G_2 \mid a_2(f(g'), \psi(x_0)) = \psi(x_0)\} = \{g' \in G_1 \mid \psi(a_1(g', x_0)) = \psi(x_0)\}$ where the last equality follows from the definition of equivalent actions. Lastly, note that we may get rid of $\psi$ as it is a bijection to find that $\operatorname{Stab}(\psi(x_0)) = \{f(g') \mid g' \in \operatorname{Stab}(x_0)\}$ as desired. □

**Remark 2.0.5.** Note that neither the definition of equivalent orbits nor the two results following rely on specifying whether $a_1$ and $a_2$ are left or right orbits.

**Definition 2.0.6.** Let $G$ be a group and $\rho_1$, $\rho_2$ be elements of order 2 in the center of $G$. The elements $\rho_1$ and $\rho_2$ are said to be *$\rho$-equivalent* if there exists $f \in \operatorname{Aut}(G)$ such that $f(\rho_1) = \rho_2$.

Equivalence classes formed under being $\rho$-equivalence are called a *$\rho$-structures*.

**Theorem 2.0.7.** Let $G_1 \cong G_2$ be Galois groups of Galois CM-fields $K_1$ and $K_2$ respectively. Let $\rho_1 \in G_1$ and $\rho_2 \in G_2$ represent complex conjugation and assume $f\colon G_1 \to G_2$ is an isomorphism such that $f(\rho_1) = \rho_2$. Since $K_1$ is Galois, the embeddings in $\Phi$ are elements in the Galois group $G_1$ (Theorem 1.2.9). Write $\Phi = \{g_1, g_2, \ldots, g_n\}$ where $g_i \in G_1$, then

$$f(\Phi) \coloneqq \{f(g_1), f(g_2), \ldots, f(g_n)\},$$

is a CM-type of the field $K_2$.

*Proof.* Note that $\Phi$ is a CM-type of $K_1$ so that no two embeddings differ by complex conjugation; i.e. we have $g_i \neq \rho_1 g_j$ for all $g_i, g_j \in \Phi$. Then $f(\Phi) = \{f(g_1), f(g_2), \ldots, f(g_n)\}$ is a set of $n$ embeddings of $K_2$. Furthermore, we have

$$g_i \neq \rho_1 g_j \implies f(g_i) \neq f(\rho_1 g_j) \implies f(g_i) \neq \rho_2 f(g_j),$$

so that no two embeddings of $K_2$ differ by complex conjugation. This shows that $f(\Phi)$ is a CM-type of $K_2$. □

**Corollary 2.0.8.** With the same notation as in Theorem 2.0.7, we additionally write $\{\Phi_i\}$ to be the collection of the $2^n$ distinct CM-types of $K_1$. Then $\{f(\Phi_i)\}$ is the collection of $2^n$ distinct CM-types of $K_2$.

*Proof.* This follows from Theorem 2.0.7 along with the fact that $f$ is an isomorphism. □

Next, we show that equivalent CM-types give equivalent orbits when groups $G_1, G_2$ are taken to be the Galois groups of fields $K_1, K_2$ and $X_1, X_2$ are taken to be the set of CM-types.

**Theorem 2.0.9.** Let $G_1 \cong G_2$ be Galois groups of CM-fields $K_1$ and $K_2$ respectively. Let $\rho_1 \in G_1$ and $\rho_2 \in G_2$ represent complex conjugation and assume $f\colon G_1 \to G_2$ is an isomorphism such that $f(\rho_1) = \rho_2$. Set $X_1 = \{\Phi_i\}$ and $X_2 = \{f(\Phi_i)\}$. Define the left action as $a_1\colon G_1 \times X_1 \to X_1$ as $a_1(\sigma, \Phi) = \sigma\Phi$ and $a_2\colon G_2 \times X_2 \to X_2$ as $a_2(\tau, f(\Phi)) = \tau(f(\Phi))$. Then $a_1$ and $a_2$ are equivalent actions.

*Proof.* We note that $f(a_1(g, \Phi)) = f(g \circ \Phi) = f(g) \circ f(\Phi) = a_2(f(g), f(\Phi))$ so that $a_1$ and $a_2$ are equivalent actions by defining $\psi\colon X_1 \to X_2$ as $\psi(\Phi) = f(\Phi)$, where Theorem 2.0.7 guarantees that this is a bijection of sets. □

**Corollary 2.0.10.** With notation as in Theorem 2.0.9, defining $a_1, a_2$ as right actions instead according to $a_1(\sigma, \Phi\} = \Phi\sigma$ and $a_2(\tau, f(\Phi)) = f(\Phi)\tau$. Then $a_1$ and $a_2$ are also equivalent actions. □

By Theorems 1.3.15 and 1.3.22, primitivity and reflex fields of $\Phi$ are determined by the fixed points of the right and left action of $G$ on $\Phi$ respectively. Thus we can use the newly obtained results on equivalence of these action of $G$ on $\Phi$ to relate the CM-types, primitivity, and reflex fields under choices of complex conjugation in the same $\rho$-structure.

**Theorem 2.0.11.** Let $K_1, K_2$ be two Galois CM-fields with $G \cong \mathrm{Gal}(K_1/\mathbb{Q}) \cong \mathrm{Gal}(K_2/\mathbb{Q})$. Assume that $\rho_1 \in G$ represents complex conjugation for $K_1$ and $\rho_2 \in G$ represent complex conjugation for $K_2$. If $\rho_1$ and $\rho_2$ are $\rho$-equivalent via an automorphism $f$ of $G$, then the following holds.

1. Let $K_1'$ and $K_2'$ be subfields of $K_1, K_2$ respectively, with $f(\mathrm{Gal}(K/K_1')) = \mathrm{Gal}(K/K_2')$. Then $K_1'$ is a CM-subfield if and only if $K_2'$ is a CM-subfield;
2. If $\{\Phi_i\}$ is the collection of CM-types for $K_1$, then $\{f(\Phi_i)\}$ is the collection of CM-types for $K_2$;
3. Let $(K_1, \Phi)$ be induced by primitive pair $(K_1^{H_1}, \Phi')$, then $(K_2, f(\Phi))$ is induced by primitive pair $(K_2^{f(H_1)}, f(\Phi'))$;
4. If $(K_1, \Phi)$ has the reflex pair $(K_1^r, \Phi^r) = (K_1^{H_1}, \Phi^r)$, then $(K_2, f(\Phi))$ has the reflex pair $(K_2^{f(H_1)}, f(\Phi^r))$.

*Proof.* (1) Let $K_1'$ and $K_2'$ be subfields of $K_1, K_2$ respectively, so that $f(\mathrm{Gal}(K/K_1')) = \mathrm{Gal}(K/K_2')$. Recall that a subfield of a CM-field is either totally real or a CM-field so that subfield $K_1'$ is a CM-field $\iff \rho_1 \notin \mathrm{Gal}(K/K_1') \iff f(\rho_1) \notin f(\mathrm{Gal}(K/K_1')) \iff \rho_2 \notin \mathrm{Gal}(K/K_2') \iff K_2'$ is a CM-field.

(2) This is Theorem 2.0.8.

(3) We know $(K_1, \Phi)$ is induced by $K_1^{H_1}$ where $H_1 = \{\sigma \in G \mid \Phi\sigma = \Phi\}$, thus $H_1 = \mathrm{Stab}(\Phi)$. By Theorems 2.0.9 and 2.0.4, we know that $\mathrm{Stab}(f(\Phi)) = \{f(g) \mid g \in \mathrm{Stab}(\Phi)\} = f(H_1)$ Thus $(K_2, f(\Phi))$ is induced from $K_2^{f(H_1)}$. Lastly, since $\Phi'$ induces $\Phi$, we have that $f(\Phi')$ induces $f(\Phi)$.

(4) Same proof as (3), using the left action instead of the right action. □

# 3 The results for the order $8$ groups

## 3.1 The group $\mathbb{Z}_2 \times \mathbb{Z}_4$

The first group of order 8 we consider is the group $\mathbb{Z}_2 \times \mathbb{Z}_4$. The analysis of this group is particularly interesting as there are three representatives for $\rho$, which together give two $\rho$-structures. In this section, we work out the primitive CM-types and reflex fields for $\mathbb{Z}_2 \times \mathbb{Z}_4$ for the two $\rho$-structures. Moreover, examples of fields attaining both $\rho$-structures are given.

We start with determining the elements that can represent complex conjugation. Note that $\mathbb{Z}_2 \times \mathbb{Z}_4$ contains three elements of order 2 in the center, these are

$$\rho_1 \coloneqq (1,0),\ \rho_2 \coloneqq (0,2) \text{ and } \rho_3 \coloneqq (1,2).$$

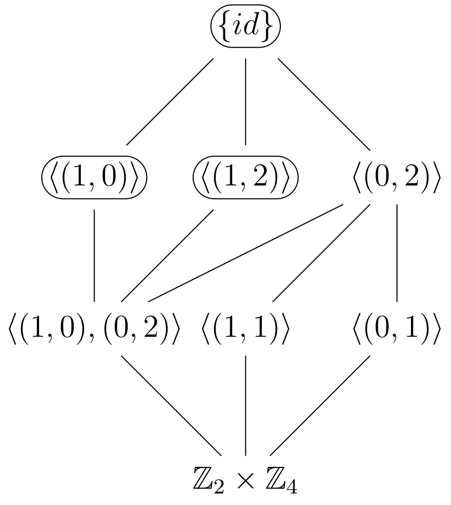
### 3.1.1 The subgroup lattice

In light of giving a complete overview of the problem, we compute the subgroup lattice for each choice of complex conjugation. For this, observe that the subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_4$ are given by

- Order 2: $\langle(1,0)\rangle, \langle(0,2)\rangle$ and $\langle(1,2)\rangle$;
- Order 4: $\langle(0,1)\rangle, \langle(1,1)\rangle$ and $\langle(1,0),(0,2)\rangle$.

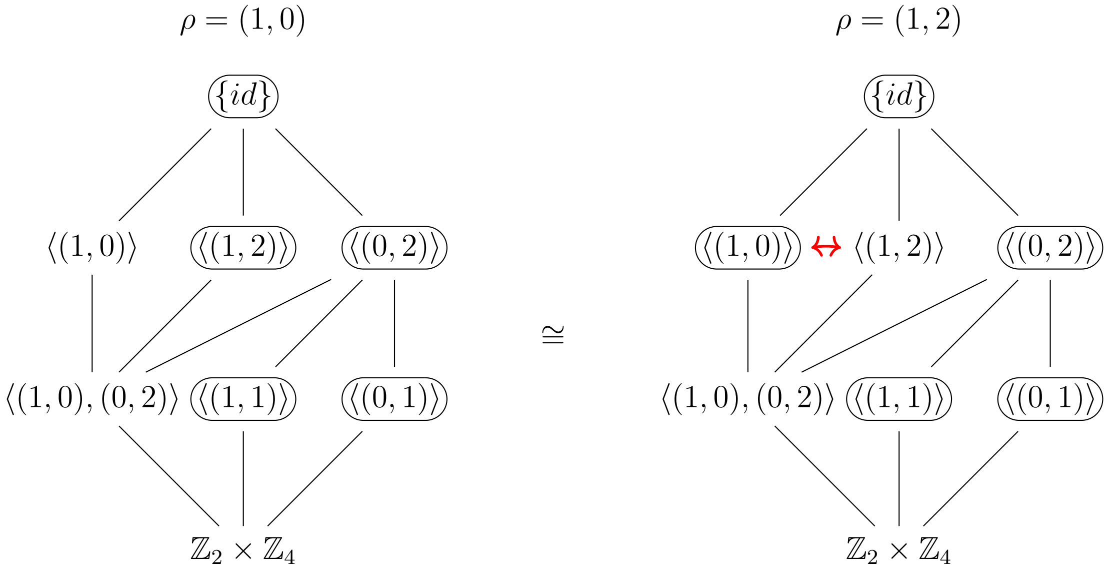
Then the subgroup lattice is given by

$\rho_2 = (0,2)$



By the Galois correspondence, these subgroups correspond to intermediate fields fixed by the elements in the Galois group. In particular, subfields of CM-fields are either totally real or CM-fields (Theorem 1.3.3). This means that the subgroups containing complex conjugation, given by $\rho_2 = (0,2)$ correspond to totally real fields, while the subgroups not containing complex conjugation correspond to CM-subfields, which are indicated by a box.

Drawing the subgroup lattice, but choosing $\rho_1 = (1,0)$ and $\rho_3 = (1,2)$ for complex conjugation gives the following diagram, where the CM-intermediate fields are in almost the same location.



However, recall that the way we draw the subgroup lattice is to some extent arbitrary. In this case, we can swap the groups in the right lattice without affecting the subgroup structure. This interchange of subgroups puts the intermediate CM-fields in exactly the same location in the subgroup lattice. This intuitively justifies that the CM-subfields in both cases are in some sense equivalent. We use $\rho$-structures to make this formal.

**Lemma 3.1.1.** The group $\mathbb{Z}_2 \times \mathbb{Z}_4$ has two $\rho$-structures with representatives $\rho_1 = (1,0)$ and $\rho_2 = (0,2)$. The element $\rho_3 = (1,2)$ is in the same $\rho$-structure as $\rho_1$.

*Proof.* Define $f\colon \mathbb{Z}_2 \times \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_4$ by $f(1,0) = (1,2)$ and $f(0,1) = (0,1)$. It can be shown that $f$ is a group automorphism such that $f(\rho_1) = \rho_3$. Hence, $\rho_1$ and $\rho_3$ lie in the same $\rho$-structure.

We claim there is no automorphism $g$ such that $g(\rho_1) = \rho_2$. Indeed, assume such an automorphism exists, then $2g^{-1}(0,1) = (1,0)$, but $(1,0)$ cannot be written this way. □

Observe that applying automorphism $f$ to the subgroups in the subgroup lattice places the CM-group $\langle(1,2)\rangle$ into the location $f(\langle(1,2)\rangle) = \langle(1,0)\rangle$. It can be checked that $f$ fixes all other subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_4$. This shows that $f$ changes the subgroups according to the red arrow in Diagram 3.1.1. This verifies (1) in Theorem 2.0.11.

### 3.1.2 The CM-types in the case $\rho_2 = (0,2)$

Next, we compute the CM-types of fields with Galois group $\mathbb{Z}_2 \times \mathbb{Z}_4$ for both $\rho$-structures and highlight which CM-types are primitive. We will also compute the reflex fields.

First, fix $\rho_2 = (0, 2)$. The embeddings are given by the elements in the Galois group.

$$\phi_1 = (0, 0),\ \phi_2 = (0, 1),\ \phi_3 = (1, 0),\ \phi_4 = (1, 1),$$

as none of these four embeddings differ by $\rho_2 = (0, 2)$. The conjugated embeddings are

$$\bar{\phi}_1 = (0, 2),\ \bar{\phi}_2 = (0, 3),\ \bar{\phi}_3 = (1, 2),\ \bar{\phi}_4 = (1, 3).$$

By definition of CM-types, the $2^4 = 16$ CM-types are given by choosing one embedding out of each pair $\{\phi_i, \bar{\phi}_i\}$ for $1 \leq i \leq 4$.

Next, we compute which CM-types are equivalent by computing for which $\sigma \in \mathbb{Z}_2 \times \mathbb{Z}_4$, we have $\Phi\sigma = \Phi$. The calculations are explicitly shown for $\Phi = \{\phi_1, \phi_2, \phi_3, \phi_4\}$.

$$\begin{aligned}
\{(0,0),(0,1),(1,0),(1,1)\} \circ (0,0) &= \{(0,0),(0,1),(1,0),(1,1)\} = \{\phi_1, \phi_2, \phi_3, \phi_4\};\\
\{(0,0),(0,1),(1,0),(1,1)\} \circ (0,1) &= \{(0,1),(0,2),(1,1),(1,2)\} = \{\phi_2, \bar{\phi}_1, \phi_4, \bar{\phi}_3\};\\
\{(0,0),(0,1),(1,0),(1,1)\} \circ (0,2) &= \{(0,2),(0,3),(1,2),(1,3)\} = \{\bar{\phi}_1, \bar{\phi}_2, \bar{\phi}_3, \bar{\phi}_4\};\\
\{(0,0),(0,1),(1,0),(1,1)\} \circ (0,3) &= \{(0,3),(0,0),(1,3),(1,0)\} = \{\bar{\phi}_2, \phi_1, \bar{\phi}_4, \phi_3\};\\
\{(0,0),(0,1),(1,0),(1,1)\} \circ (1,0) &= \{(1,0),(1,1),(0,0),(0,1)\} = \{\phi_3, \phi_4, \phi_1, \phi_2\};\\
\{(0,0),(0,1),(1,0),(1,1)\} \circ (1,1) &= \{(1,1),(1,2),(0,1),(0,2)\} = \{\phi_4, \bar{\phi}_3, \phi_2, \bar{\phi}_1\};\\
\{(0,0),(0,1),(1,0),(1,1)\} \circ (1,2) &= \{(1,2),(1,3),(0,2),(0,3)\} = \{\bar{\phi}_3, \bar{\phi}_4, \bar{\phi}_1, \bar{\phi}_2\};\\
\{(0,0),(0,1),(1,0),(1,1)\} \circ (1,3) &= \{(1,3),(1,0),(0,3),(0,0)\} = \{\bar{\phi}_4, \phi_3, \bar{\phi}_2, \phi_1\}.
\end{aligned}$$

And thus we find that the CM-types equivalent to $\{\phi_1, \phi_2, \phi_3, \phi_4\}$ are

$$[\{\phi_1, \phi_2, \phi_3, \phi_4\}] = \{\{\phi_1, \phi_2, \phi_3, \phi_4\}, \{\bar{\phi}_1, \phi_2, \bar{\phi}_3, \phi_4\}, \{\bar{\phi}_1, \bar{\phi}_2, \bar{\phi}_3, \bar{\phi}_4\}, \{\phi_1, \bar{\phi}_2, \phi_3, \bar{\phi}_4\}\}.$$

Similar computations show that we have the following equivalence classes:

$$\begin{aligned}
[\{\phi_1, \phi_2, \phi_3, \phi_4\}] &= \{\{\phi_1, \phi_2, \phi_3, \phi_4\}, \{\bar{\phi}_1, \phi_2, \bar{\phi}_3, \phi_4\}, \{\bar{\phi}_1, \bar{\phi}_2, \bar{\phi}_3, \bar{\phi}_4\}, \{\phi_1, \bar{\phi}_2, \phi_3, \bar{\phi}_4\}\};\\
[\{\bar{\phi}_1, \bar{\phi}_2, \phi_3, \phi_4\}] &= \{\{\bar{\phi}_1, \bar{\phi}_2, \phi_3, \phi_4\}, \{\phi_1, \bar{\phi}_2, \bar{\phi}_3, \phi_4\}, \{\phi_1, \phi_2, \bar{\phi}_3, \bar{\phi}_4\}, \{\bar{\phi}_1, \phi_2, \phi_3, \bar{\phi}_4\}\};\\
[\{\bar{\phi}_1, \phi_2, \phi_3, \phi_4\}] &= \{\{\bar{\phi}_1, \phi_2, \phi_3, \phi_4\}, \{\bar{\phi}_1, \bar{\phi}_2, \bar{\phi}_3, \phi_4\}, \{\phi_1, \bar{\phi}_2, \bar{\phi}_3, \bar{\phi}_4\}, \{\phi_1, \phi_2, \phi_3, \bar{\phi}_4\}\\
&\qquad \{\phi_1, \phi_2, \bar{\phi}_3, \phi_4\}, \{\bar{\phi}_1, \phi_2, \bar{\phi}_3, \bar{\phi}_4\}, \{\bar{\phi}_1, \bar{\phi}_2, \phi_3, \bar{\phi}_4\}, \{\phi_1, \bar{\phi}_2, \phi_3, \phi_4\}\}.
\end{aligned}$$

### 3.1.3 The reflex fields in the case $\rho_2 = (0, 2)$

We are interested in finding the reflex fields for all 16 CM-type. From Theorem 1.3.22, we know that the fixed field of $\{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \sigma\Phi = \Phi\}$ is the reflex field of $(K, \Phi)$. Theorem 1.3.32 shows that each equivalence class leads to the same reflex field $K^r$. Thus we compute which $\sigma \in \mathbb{Z}_2 \times \mathbb{Z}_4$ fix $\Phi$ for the three representatives of the equivalence classes.

- For $\Phi_1 = \{\phi_1, \phi_2, \phi_3, \phi_4\}$, we compute that $\sigma\Phi_1 = \Phi_1 \iff \sigma \in \{(0, 0), (1, 0)\}$. Thus we find that $\Phi_1$ has reflex $K^r = K^{\langle(1,0)\rangle}$.
- For $\Phi_2 = \{\bar{\phi}_1, \bar{\phi}_2, \phi_3, \phi_4\}$, we compute that $\sigma\Phi_2 = \Phi_2 \iff \sigma \in \{(0, 0), (1, 2)\}$. Thus we have that $\Phi_2$ has reflex $K^r = K^{\langle(1,2)\rangle}$.
- Note that $\Phi_3 = \{\bar{\phi}_1, \phi_2, \phi_3, \phi_4\}$ has 8 equivalent CM-types and thus is primitive by Theorem 1.3.28. From Theorem 1.3.34, we have that $K^r = K$.

Comparing this result to the Diagram 3.1.1, we find that each CM-subfield is a reflex field for some CM-type of $K$.

### 3.1.4 The primitive CM-types in the case $\rho_2 = (0, 2)$

From Theorem 1.3.28, we know that $\Phi$ is primitive if and only if it has 8 equivalent CM-types, which shows that $\{\bar{\phi}_1, \phi_2, \phi_3, \phi_4\}$ is primitive. Furthermore, Theorem 1.3.30, shows that all 8 CM-types in the equivalence class of $\{\bar{\phi}_1, \phi_2, \phi_3, \phi_4\}$ are primitive. Lastly, Theorem 1.3.33 shows that $\Phi_1$ is induced by a CM-type of the field $K^{\langle(1,0)\rangle}$ and $\Phi_2$ is induced by a CM-type of the field $K^{\langle(1,2)\rangle}$.

### 3.1.5 The CM-types in the case $\rho_1 = (1, 0)$

Here, we study the second $\rho$-structure, that is the case for $\rho_1 = (1, 0)$ and $\rho_3 = (1, 2)$. From Theorem 2.0.11, we get that the results for $\rho_3 = (1, 2)$ are identical (up to relabeling of the Galois group) to the results of $\rho_1 = (1, 0)$. Thus only computations for $\rho_1 = (1, 0)$ are shown.

When complex conjugation is given by $(1, 0)$, the four embeddings that do not differ by complex conjugation, together with their conjugate embeddings are given by

$$\phi_i = (0, i) \implies \bar{\phi}_i = (1, i) \text{ where } 1 \leq i \leq 4.$$

Computing the equivalent CM-types in the same manner as in Section 3.1.2, we find that the equivalent CM-types are given by

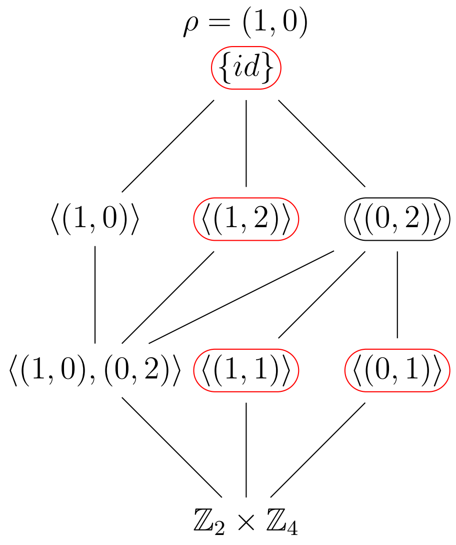
$$\begin{aligned}
[\{\phi_1, \phi_2, \phi_3, \phi_4\}] &= \{\{\phi_1, \phi_2, \phi_3, \phi_4\}, \{\bar{\phi}_1, \bar{\phi}_2, \bar{\phi}_3, \bar{\phi}_4\}\}; \\
[\{\bar{\phi}_1, \phi_2, \bar{\phi}_3, \phi_4\}] &= \{\{\bar{\phi}_1, \phi_2, \bar{\phi}_3, \phi_4\}, \{\phi_1, \bar{\phi}_2, \phi_3, \bar{\phi}_4\}\}; \\
[\{\bar{\phi}_1, \bar{\phi}_2, \phi_3, \phi_4\}] &= \{\{\bar{\phi}_1, \bar{\phi}_2, \phi_3, \phi_4\}, \{\phi_1, \bar{\phi}_2, \bar{\phi}_3, \phi_4\}, \{\phi_1, \phi_2, \bar{\phi}_3, \bar{\phi}_4\}, \{\bar{\phi}_1, \phi_2, \phi_3, \bar{\phi}_4\}\}; \\
[\{\bar{\phi}_1, \phi_2, \phi_3, \phi_4\}] &= \{\{\bar{\phi}_1, \phi_2, \phi_3, \phi_4\}, \{\phi_1, \bar{\phi}_2, \phi_3, \phi_4\}, \{\phi_1, \phi_2, \bar{\phi}_3, \phi_4\}, \{\phi_1, \phi_2, \phi_3, \bar{\phi}_4\} \\
&\qquad \{\phi_1, \bar{\phi}_2, \bar{\phi}_3, \bar{\phi}_4\}, \{\bar{\phi}_1, \phi_2, \bar{\phi}_3, \bar{\phi}_4\}, \{\bar{\phi}_1, \bar{\phi}_2, \phi_3, \bar{\phi}_4\}, \{\bar{\phi}_1, \bar{\phi}_2, \bar{\phi}_3, \phi_4\}\}.
\end{aligned}$$

### 3.1.6 The reflex fields in the case $\rho_1 = (1, 0)$

The reflex fields are given by the fixed points of the action of the Galois group on the left, these can easily be computed in the same manner as in Section 3.1.3 to find that the above equivalence classes have the following reflex fields

- $\Phi_1 \coloneqq \{\phi_1, \phi_2, \phi_3, \phi_4\}$ has associated reflex field $K^r = K^{\langle(0,1)\rangle}$;
- $\Phi_2 \coloneqq \{\bar{\phi}_1, \phi_2, \bar{\phi}_3, \phi_4\}$ has associated reflex field $K^r = K^{\langle(1,1)\rangle}$;
- $\Phi_3 \coloneqq \{\bar{\phi}_1, \bar{\phi}_2, \phi_3, \phi_4\}$ has associated reflex field $K^r = K^{\langle(1,2)\rangle}$;
- $\Phi_4 \coloneqq \{\bar{\phi}_1, \phi_2, \phi_3, \phi_4\}$ has associated reflex field $K^r = K$.

Comparing this result to the subgroup lattice of $\rho_1 = (1, 0)$, we find that not every CM-field corresponds to a reflex field. In the lattice below, the CM-fields are circled in red if they are reflex fields of some CM-type of $K$, and boxed in black if not.



### 3.1.7 The primitive CM-types in the case $\rho_1 = (1,0)$

Theorem 1.3.28 tells us that the 8 CM-types in the equivalence class of $\{\bar{\phi}_1, \phi_2, \phi_3, \phi_4\} = \Phi_4$ are primitive. Furthermore, Theorem 1.3.33 shows that $\Phi_1$ is induced from a CM-field of $K^{\langle(0,1)\rangle}$, $\Phi_2$ is induced from $K^{\langle(1,1)\rangle}$ and lastly $\Phi_3$ is induced from $K^{\langle(1,2)\rangle}$.

### 3.1.8 An example

In this section, we will find two Galois CM-fields $K$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_4$ one of which attains the results regarding CM-subfields, primitivity of CM-types and reflex fields according to the case $\rho_2 = (0,2)$ and the other one according to the case $\rho_1 = (1,0)$.

The fields we will look at is the field $K_1 \coloneqq \mathbb{Q}(\zeta_{16})$ and $K_2$ the splitting field of the polynomial $p(x) \coloneqq x^8 + 8x^6 + 20x^4 + 16x^2 + 1$.

Note that $K_1$ is a cyclotomic field and thus has Galois group $(\mathbb{Z}_{16})^\times = \mathbb{Z}_2 \times \mathbb{Z}_4$. Furthermore $K_1$ is a CM-field as $\mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1}) \subset \mathbb{Q}(\zeta_{16})$ is a totally real subfield such that we have $[\mathbb{Q}(\zeta_{16}) : \mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})] = 2$.

Showing that $K_2$, the splitting field of $p = x^8 + 8x^6 + 20x^4 + 16x^2 + 1$, is a CM-field and has Galois group $\mathbb{Z}_2 \times \mathbb{Z}_4$ requires a bit more work and will be done via the following observations.

1. Note that $p$ is irreducible: Indeed, we have that $p(x-1) = x^8 - 8x^7 - 36x^6 - 104x^5 + 210x^4 - 296x^3 + 284x^2 - 168x + 46$ is an Eisenstein polynomial for the prime 2.

2. The roots of $f$ are given by $x = \pm i\sqrt{2 \pm \sqrt{2 \pm \sqrt{3}}}$: To see this, we write the polynomial $p(x) = (x^4 + 4x^2)^2 + 4(x^4 + 4x^2) + 1$. Repeated application of the quadratic formula yields

$$p(x) = 0 \iff x = \pm i\sqrt{2 \pm \sqrt{2 \pm \sqrt{3}}}.$$

3. Set $\alpha := i\sqrt{2+\sqrt{2+\sqrt{3}}}$, we have that $K_2 = \mathbb{Q}(\alpha)$ is the splitting field of $p(x)$. Note that $\sqrt{2+\sqrt{3}}, \sqrt{3}, \sqrt{2} \in \mathbb{Q}(\alpha)$ and $1/(\sqrt{2+\sqrt{3}}) = \sqrt{2-\sqrt{3}} \in \mathbb{Q}(\alpha)$. Also

   - $\sqrt{2-\sqrt{3}}/\alpha = i\sqrt{2-\sqrt{2+\sqrt{3}}} \in \mathbb{Q}(\alpha)$;
   - $(\sqrt{2}+\sqrt{3})/\alpha = i\sqrt{2+\sqrt{2-\sqrt{3}}} \in \mathbb{Q}(\alpha)$;
   - $(1+\sqrt{2})/\alpha = i\sqrt{2-\sqrt{2-\sqrt{3}}} \in \mathbb{Q}(\alpha)$.

   Thus $\mathbb{Q}(\alpha)$ contains all roots of $p(x)$ and hence is the splitting field of $p(x)$.

4. We have $G = \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.

   Define $\beta = i\sqrt{2-\sqrt{2+\sqrt{3}}}$, $\gamma = i\sqrt{2+\sqrt{2-\sqrt{3}}}$, $\delta = i\sqrt{2-\sqrt{2-\sqrt{3}}}$.

   Next, define $\sigma \in G$ to be the automorphism that sends $\alpha \to \beta$. Then we have that $\sigma(\alpha^2) = \beta^2$ which is equivalent to $\sigma(-\sqrt{2+\sqrt{3}}) = \sqrt{2+\sqrt{3}}$. Rewriting the nested square root gives $\sigma((1+\sqrt{3})/-\sqrt{2}) = (1+\sqrt{3})/\sqrt{2})$. And thus regarding $\sigma$ as an automorphism of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, we see $\sigma$ sends $\sqrt{3} \to \sqrt{3}$ and $\sqrt{2} \to -\sqrt{2}$. Since $\alpha\beta = (1-\sqrt{3})/\sqrt{2}$, we conclude that $\sigma(\alpha\beta) = -\alpha\beta$. From this, it follows that $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = \beta\sigma(\beta) = -\alpha\beta \implies \sigma(\beta) = -\alpha$ and thus $\sigma$ has order 4.

   Let us define $\tau \in G$ to be the automorphism that sends $\beta \to \gamma$. Then we have that $\tau(\beta^2) = \gamma^2$ which is equivalent to $\tau((1+\sqrt{3})/\sqrt{2}) = (1-\sqrt{3})/\sqrt{2}$, so that $\tau$ restricted to $\mathbb{Q}(\sqrt{2,\sqrt{3}})$ can be identified with sending $\sqrt{2} \to \sqrt{2}$ and $\sqrt{3} \to -\sqrt{3}$. Now $\tau(\beta\gamma) = \tau(1-\sqrt{2}) = 1-\sqrt{2} = \beta\gamma$. Thus we conclude that $\tau(\gamma) = \beta$ and $\tau$ has order 2. Moreover, $\sigma^2 \neq \tau$ since $\tau(\alpha^2) = 2+\tau((\sqrt{3}+1)/\sqrt{2}) = 2+(1-\sqrt{3})/\sqrt{2} \neq \beta^2$.

   Lastly, we show $\sigma\tau = \tau\sigma$. For this we first show $\tau(\beta) = -\delta$ and $\sigma(-\delta) = \gamma$. Note that $\tau(\alpha\beta) = \tau((\sqrt{3}-1)/\sqrt{2}) = -(1+\sqrt{3})/\sqrt{2} = -\gamma\delta$. From this, we can conclude that $\tau(\alpha)\tau(\beta) = \tau(\alpha)\gamma = -\gamma\delta \implies \tau(\alpha) = -\delta$. Furthermore, $\sigma(\alpha\delta) = \sigma(1+\sqrt{2}) = 1-\sqrt{2} = -\beta\gamma$. From this we get $\sigma(\alpha\delta) = \sigma(\alpha)\sigma(\delta) = \sigma(\delta)\beta = -\beta\gamma \implies \sigma(\delta) = -\gamma$. Thus, $(\sigma\tau)(\alpha) = \sigma(-\delta) = \gamma$ and $(\tau\sigma)(\alpha) = \tau(\beta) = \gamma$. Hence $\sigma$ and $\tau$ commute.

   By the previous observations, we have that $|\mathrm{Gal}(\mathbb{Q}(\alpha))| = 8$. Since $\tau \neq \sigma^2$, we conclude that $|\langle\tau, \sigma\rangle| = 8$. Furthermore, $\sigma$ and $\tau$ commute, giving us the following representation: $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{\sigma, \tau \mid \sigma^4 = \tau^2 = id, \tau\sigma = \sigma\tau\}$, which is isomorphi to $\mathbb{Z}_2 \times \mathbb{Z}_4$ as desired.

5. Lastly, we claim $K_2$ is a CM-field. Indeed observe that $\mathbb{Q}(\sqrt{2+\sqrt{3}}) \subset K_2$ is a totally real field and that $[K_2 : \mathbb{Q}(\sqrt{2+\sqrt{3}})] = 2$.

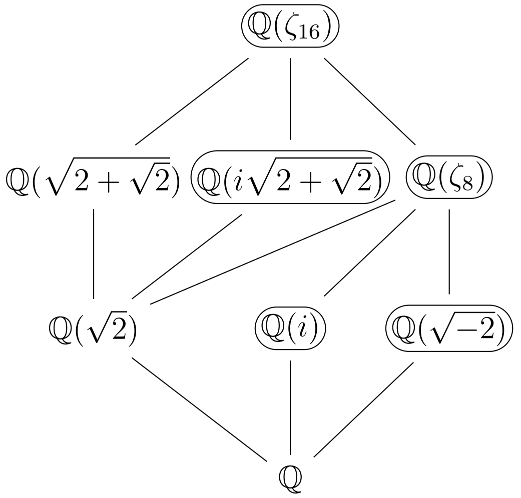
We computed that both $\mathbb{Q}(\zeta_{16})$ and $\mathbb{Q}(\sqrt{2+\sqrt{2+\sqrt{3}}})$ are CM-fields and have the same Galois group $\mathbb{Z}_2 \times \mathbb{Z}_4$ over $\mathbb{Q}$, we now compute the intermediate field lattices and indicate the CM-subfields with boxes as before.

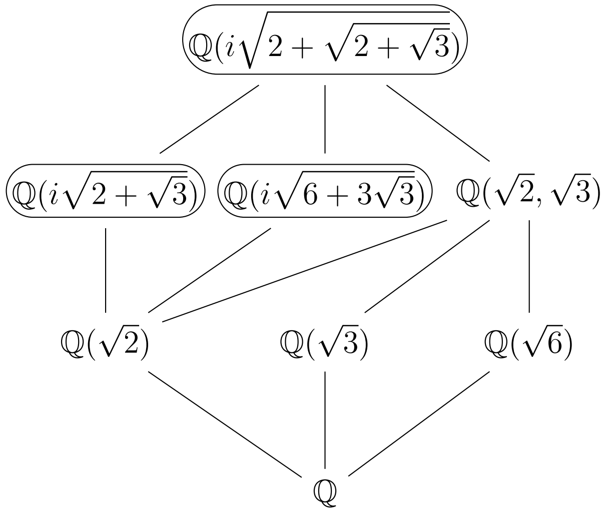
For $K_1 = \mathbb{Q}(\zeta_{16})$, we observe that $\zeta_{16}^4 = i$, thus $\mathbb{Q}(i)$ is a subfield. Similarly $\zeta_{16}^2 + \zeta_{16}^{-2} = \sqrt{2}$ and $\zeta_{16}^2 + \zeta_{16}^6 = \sqrt{-2}$ give us the intermediate fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$. As there are 3 subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_4$ with index 2, we know we have found all fields of degree 2 over $\mathbb{Q}$.

Next, $\mathbb{Q}(\zeta_8)$ is the first intermediate field of degree 4 over $\mathbb{Q}$. The other two degree 4 extensions are given by $\zeta_{16} + \zeta_{16}^{-1} = \sqrt{2+\sqrt{2}}$ and $\zeta_{16}^3 + \zeta_{16}^5 = i\sqrt{2+\sqrt{2}}$ to give us that $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ and $\mathbb{Q}(i\sqrt{2+\sqrt{2}})$ respectively. We have $\mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2}) \subset \mathbb{Q}(\zeta_8)$ which shows what intermediate fields go on which places in the field lattice.

Similar computations for $K_2 = \mathbb{Q}(i\sqrt{2+\sqrt{2+\sqrt{3}}})$ give the subfields $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{6})$ as fields of degree 2 over $\mathbb{Q}$.

The degree 4 fields are given by $\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}(i\sqrt{2+\sqrt{3}})$ and $\mathbb{Q}(i\sqrt{6+3\sqrt{3}})$. Constructing the intermediate field lattice for both cases leads to




$\mathbb{Q}(i\sqrt{2+\sqrt{2+\sqrt{3}}})$
$\mathbb{Q}(i\sqrt{2+\sqrt{3}})$
$\mathbb{Q}(i\sqrt{6+3\sqrt{3}})$
$\mathbb{Q}(\sqrt{2}, \sqrt{3})$
$\mathbb{Q}(\sqrt{2})$
$\mathbb{Q}(\sqrt{3})$
$\mathbb{Q}(\sqrt{6})$
$\mathbb{Q}$

Thus we see that the field $K_1 = \mathbb{Q}(\zeta_{16})$ corresponds to the case where $\rho_2 = (0, 2)$ is complex conjugation whereas the field $K_2$ corresponds to the case where $\rho_1 = (1, 0)$ (or $\rho_3 = (1, 2)$) corresponds to complex conjugation.

## 3.2 The cyclic group $\mathbb{Z}_8$

Next, we look at the cyclic group $\mathbb{Z}_8$. Since $\mathbb{Z}_8$ is cyclic, there can only be one element of order 2, in this case this is the element $\rho := 4 \in \mathbb{Z}_8$. Since there is only one element that can represent complex conjugation, there will only be one $\rho$-structure, meaning that the analysis for this case will go much quicker.

### 3.2.1 The subgroup lattice

Again, we first compute the subgroup lattice, and indicate which intermediate fields can be CM-fields. Note that the only subgroups of $\mathbb{Z}_8$ are given by $\langle 4 \rangle$ of order 2 and $\langle 2 \rangle$ of order 4. Thus the subgroup lattice looks as follows.

$$\begin{tikzcd}
\boxed{\{id\}} \arrow[d, dash] \\
\mathbb{Z}_2 \arrow[d, dash] \\
\mathbb{Z}_4 \arrow[d, dash] \\
\mathbb{Z}_8
\end{tikzcd}$$

Every subgroup of $\mathbb{Z}_8$ contains the element $4 \in \mathbb{Z}_8$, which corresponds to complex conjugation. Thus every subfield of a CM-field $K$ with Galois group $\mathbb{Z}_8$ is fixed by complex conjugation and therefore cannot be a CM-field. Thus $K$ has no CM-subfields.

### 3.2.2 The CM-types

Recall that $\rho = 4 \in \mathbb{Z}_8$. Thus the 4 embeddings that do not differ by complex conjugation can be given by

$$\phi_1 = 0,\ \phi_2 = 1,\ \phi_3 = 2,\ \phi_4 = 3,$$

which gives that the conjugate embeddings must be

$$\bar{\phi}_1 = 4,\ \bar{\phi}_2 = 5,\ \bar{\phi}_3 = 6,\ \bar{\phi}_4 = 7.$$

Now, the $2^4 = 16$ CM-types are given by choosing one embedding out of each pair $\phi_i, \bar{\phi}_i$ for $1 \leq i \leq 4$. The equivalent CM-types can be computed in the same manner as Section 1.3.9 to yield

$$\begin{aligned}
[\{\phi_1,\phi_2,\phi_3,\phi_4\}] = \{&\{\phi_1,\phi_2,\phi_3,\phi_4\},\{\bar{\phi}_1,\phi_2,\phi_3,\phi_4\},\{\bar{\phi}_1,\bar{\phi}_2,\phi_3,\phi_4\},\{\bar{\phi}_1,\bar{\phi}_2,\bar{\phi}_3,\phi_4\}\\
&\{\bar{\phi}_1,\bar{\phi}_2,\bar{\phi}_3,\bar{\phi}_4\},\{\phi_1,\bar{\phi}_2,\bar{\phi}_3,\bar{\phi}_4\},\{\phi_1,\phi_2,\bar{\phi}_3,\bar{\phi}_4\},\{\phi_1,\phi_2,\phi_3,\bar{\phi}_4\}\};\\
[\{\phi_1,\bar{\phi}_2,\phi_3,\phi_4\}] = \{&\{\phi_1,\bar{\phi}_2,\phi_3,\phi_4\},\{\bar{\phi}_1,\phi_2,\bar{\phi}_3,\phi_4\},\{\bar{\phi}_1,\bar{\phi}_2,\phi_3,\bar{\phi}_4\},\{\phi_1,\bar{\phi}_2,\bar{\phi}_3,\phi_4\}\\
&\{\bar{\phi}_1,\phi_2,\bar{\phi}_3,\bar{\phi}_4\},\{\phi_1,\bar{\phi}_2,\phi_3,\bar{\phi}_4\},\{\phi_1,\phi_2,\bar{\phi}_3,\phi_4\},\{\bar{\phi}_1,\phi_2,\phi_3,\bar{\phi}_4\}\}.
\end{aligned}$$

### 3.2.3 The reflex fields

From Theorem 1.3.24, we know that reflex fields are CM-fields. From the definition of the reflex fields, we also know that $K^r \subseteq K^{\mathrm{cl}}$. Since $K$ is Galois, we have $K^r \subseteq K$. There are no strict CM-subfields of $K$, and thus we have $K^r = K$.

### 3.2.4 The primitive CM-types

All CM-types are primitive as there are no intermediate CM-fields that can induce any of the CM-types.

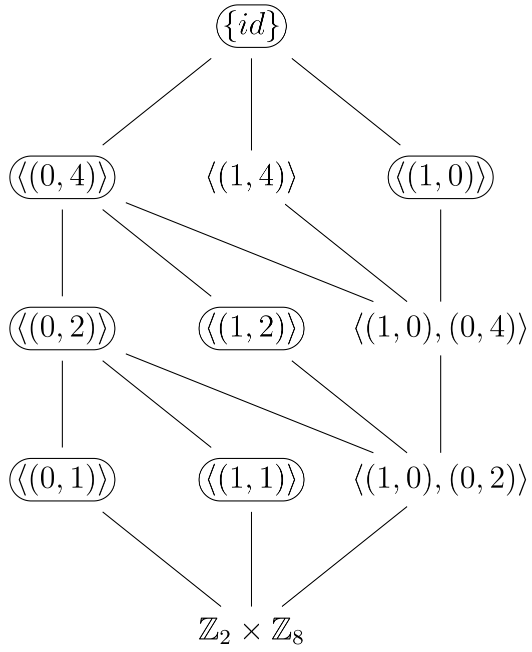
This can also be reasoned through Theorem 1.3.33 as each reflex field is given by $K^r = K$ and thus all CM-types are induced from the field $K$ itself; i.e. they are primitive.

### 3.2.5 An example

We further elucidate this case by giving an explicit example. For this we look at the CM-field $K \coloneqq \mathbb{Q}(\zeta_{32})$. We have $G \coloneqq \mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}_{32})^{\times}$. Since the Galois group is abelian, any intermediate field will also be Galois over $\mathbb{Q}$. The field $K$ itself is of degree 16 over $\mathbb{Q}$, but the idea of looking at this field is that it might contain a CM-subfield of degree 8 with desired Galois group. It turns out that this is indeed the case. To show this, we can construct the intermediate field and subgroup lattice of $\mathbb{Q}(\zeta_{32})$ and $\mathbb{Z}_2 \times \mathbb{Z}_8$ respectively. First we start with the subgroups. We notice that we have the following subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_8$

- Order 8: $\langle(0,1)\rangle$, $\langle(1,1)\rangle$ and $\langle(1,0),(0,2)\rangle$;
- Order 4: $\langle(0,2)\rangle$, $\langle(1,2)\rangle$ and $\langle(1,0),(0,4)\rangle$;
- Order 2: $\langle(1,0)\rangle$, $\langle(0,4)\rangle$ and $\langle(1,4)\rangle$.

This gives us the following subgroup lattice

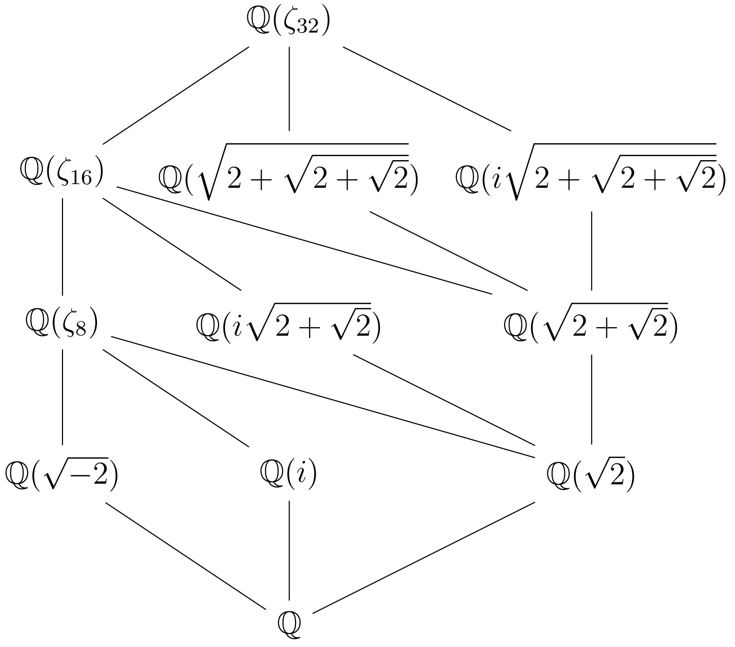


We can choose the element $\rho \coloneqq (1,4) \in \mathbb{Z}_2 \times \mathbb{Z}_8$ to be conjugation as $(1,4)$ is an element of order 2 in the center of $G$. In the above subgroup lattice, all groups that do not contain the element $(1,4)$ are circled as these subgroups are not fixed by complex conjugation and thus by Theorem 1.3.3 are CM-subfields. In particular, the field $K^{\langle(1,0)\rangle}$ must be a CM-field.

We compute the Galois group of this field. Since $G$ is abelian, we have that $\langle(1,0)\rangle$ is a normal subgroup of $G$. Thus we get that $\mathrm{Gal}(K^{\langle(1,0)\rangle}) = G/\langle(1,0)\rangle \cong \mathbb{Z}_8$. Here the last equality follows from the first homomorphism theorem by taking $f\colon G \to \mathbb{Z}_8$ to be $f(a,b) = b$.

Thus we have shown the existence of a CM-field with Galois group $\mathbb{Z}_8$. For completeness of this example, we will fill out the subfield diagram as well, in order to find this field explicitely. For this, note that $\mathbb{Q}(\zeta_{16})$ is a subfield $\mathbb{Q}(\zeta_{32})$, and that the subgroup lattice of $\mathbb{Q}(\zeta_{16})$ was computed in Diagram 3.1.8. This allows us to fill in the majority of the lattice already.

Note that $\mathbb{Q}(\zeta_{32} + \zeta_{32}^{-1}) = \mathbb{Q}(\sqrt{2+\sqrt{2+\sqrt{2}}})$ and $\mathbb{Q}(\zeta_{32}^7 + \zeta_{32}^9) = \mathbb{Q}(i\sqrt{2+\sqrt{2+\sqrt{2}}})$ are both subfields of $\mathbb{Q}(\zeta_{32})$ of degree 8 over $\mathbb{Q}$. We can fill in the subfield lattice by noting that both $\mathbb{Q}(i\sqrt{2+\sqrt{2+\sqrt{2}}})$ and $\mathbb{Q}(\zeta_{16})$ are CM-fields and must be associated with groups of order 2 that do not contain complex conjugation. Putting these observations together yields the following intermediate field lattice.


$\mathbb{Q}(\zeta_{32})$
$\mathbb{Q}(\zeta_{16})$
$\mathbb{Q}(\sqrt{2+\sqrt{2+\sqrt{2}}})$
$\mathbb{Q}(i\sqrt{2+\sqrt{2+\sqrt{2}}})$
$\mathbb{Q}(\zeta_8)$
$\mathbb{Q}(i\sqrt{2+\sqrt{2}})$
$\mathbb{Q}(\sqrt{2+\sqrt{2}})$
$\mathbb{Q}(\sqrt{-2})$
$\mathbb{Q}(i)$
$\mathbb{Q}(\sqrt{2})$
$\mathbb{Q}$

This shows that $\mathbb{Q}(i\sqrt{2+\sqrt{2+\sqrt{2}}})$ is a Galois CM-field of degree 8 with Galois group $\mathbb{Z}_8$, as desired.

## 3.3 The quaternions

### 3.3.1 The subgroup lattice

The quaternions, denoted by $Q_8$, is the next Galois group of order 8 that we look at. The quaternion group is given by $\langle 1, i, j, k \mid i^2 = j^2 = k^2 = ijk = -1 \rangle$. The quaternions have the following subgroups

- Order 4: $\langle i \rangle = \{1, -1, i, -i\}$, $\langle j \rangle = \{1, -1, j, -j\}$, $\langle k \rangle = \{1, -1, k, -k\}$;
- Order 2: $\langle -1 \rangle = \{-1, 1\}$.

Furthermore, $-1 \in Q_8$ is the only element of order 2 in the center of $Q_8$ and hence the element associated with complex conjugation. The subgroup lattice is given below.

$$\begin{tikzcd}
& \boxed{\{id\}} \arrow[d, dash] & \\
& \langle -1 \rangle \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle i \rangle \arrow[dr, dash] & \langle j \rangle \arrow[d, dash] & \langle k \rangle \arrow[dl, dash] \\
& Q_8 &
\end{tikzcd}$$

Note that every non-trivial subgroup of $Q_8$ contains $-1$, the element associated to complex conjugation. Thus each subfield is fixed by complex conjugation and thus cannot be CM-fields. We conclude that a Galois CM-field $K$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong Q_8$ cannot have intermediate CM-fields.

### 3.3.2 The reflex fields

From Theorem 1.3.24, we know that reflex fields are CM-fields. Recall $K^r \subset K^{\mathrm{cl}} = K$. Given that there are no intermediate CM-fields, we must have $K^r = K$ for all CM-types $\Phi$.

### 3.3.3 The primitive CM-types

Each CM-type is primitive, as there are no intermediate CM-fields that can induce a CM-types.

### 3.3.4 An example

We again compute an explicit example of a CM-field with Galois group isomorphic to $Q_8$. For this, we define $\alpha := i\sqrt{(2+\sqrt{2})(3+\sqrt{3})}$. We claim that $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) \cong Q_8$ and that $\mathbb{Q}(\alpha)$ is a CM-field. Verifying that $\mathbb{Q}(\alpha)$ is a CM-field is done quickly by noticing that we have $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\alpha)$ and thus $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ is a totally real subfield of $\mathbb{Q}(\alpha)$. Furthermore we have $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2}+\sqrt{3})] = 2$ and thus $\mathbb{Q}(\alpha)$ is a CM-field by definition. Next, we compute $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ in the same manner as in Section 3.1.8. The computations are summarized below.

1. We have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2}+\sqrt{3})][\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4 \cdot 2 = 8$.
2. The minimal polynomial of $\alpha$ is given by $f = x^8 - 24x^6 + 24x^4 - 288x^2 + 144$ and is irreducible by the fact that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 8$.

3. The roots of $f$ are given by $\pm\sqrt{(2\pm\sqrt{2})(3\pm\sqrt{3})}$, and we have

   - $\sqrt{(2-\sqrt{2})(3+\sqrt{3})} = \sqrt{2}(3+\sqrt{3})/\alpha \in \mathbb{Q}(\alpha)$;
   - $\sqrt{(2+\sqrt{2})(3-\sqrt{3})} = \sqrt{6}(2+\sqrt{2})/\alpha \in \mathbb{Q}(\alpha)$;
   - $\sqrt{(2-\sqrt{2})(3-\sqrt{3})} = 2\sqrt{3}/\alpha \in \mathbb{Q}(\alpha)$.

4. To show that $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) \cong Q_8$, we define the other roots of $f$ as follows

$$\beta = \sqrt{(2-\sqrt{2})(3+\sqrt{3})},\ \gamma = \sqrt{(2+\sqrt{2})(3-\sqrt{3})},\ \delta = \sqrt{(2-\sqrt{2})(3-\sqrt{3})}$$

   Since the Galois group acts transitively on the roots we can define $\sigma, \tau \in \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ as $\sigma(\alpha) = \beta$ and $\tau(\alpha) = \gamma$. We get $\sigma(\alpha\beta) = -\alpha\beta$ and thus $\sigma \in G$ is an element of order 4. Through similar reasoning, one can check that $\tau \in G$ also has order 4. We hence find $\sigma^2(\alpha) = -\alpha = \tau^2(\alpha)$.

   Lastly $\sigma\tau(\alpha) = -\delta$ and $\tau\sigma(\alpha) = \delta$. Combining everything yields the following relations:

$$\sigma^2 = \tau^2 = -id,\ \sigma\tau = \tau\sigma^3$$

   Thus by identifying $\sigma$ with $i$, $\tau$ with $j$ and $\sigma\tau$ with $k$, we get the following relations: $i^2 = j^2 = k^2 = ijk = -1$. This shows that $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) \cong Q_8$ as desired.

Now we determine the intermediate fields. From the subgroup lattice, we know there are three intermediate fields of degree 2 over $\mathbb{Q}$. These are given by $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{6})$. Furthermore, there is only one subfield of order 4 over $\mathbb{Q}$. which is given by $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Placing these in the intermediate field lattice gives

$$\begin{tikzcd}
 & \mathbb{Q}(\alpha) \arrow[d, dash] & \\
 & \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{3}) \arrow[d, dash] & \mathbb{Q}(\sqrt{6}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Indeed, we see that non of the intermediate fields are themselves CM-fields, as corresponds with the subgroup lattice as seen in Diagram 3.3.1.

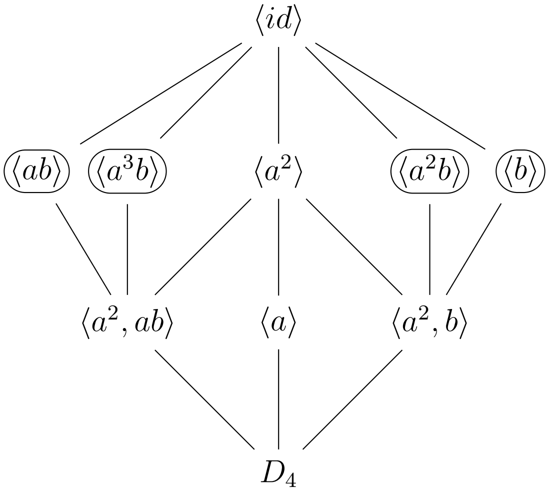
## 3.4 The dihedral group $D_4$

### 3.4.1 The subgroup lattice

Next we look at the case when the Galois group of a field is isomorphic to $D_4$. We know that $D_4$ is given by $D_4 = \langle a, b |\ a^4 = b^2 = 1, ab = ba^{-1}\rangle$. Furthermore, the subgroups are given by

- Order 4: $\langle a^2, ab\rangle = \{1, a^2, ab, a^3b\}$, $\langle a\rangle = \{1, a, a^2, a^3\}$, $\langle a^2, b\rangle = \{1, a^2, b, a^2b\}$.
- Order 2: $\langle a^2\rangle$, $\langle b\rangle$, $\langle ab\rangle$, $\langle a^2b\rangle$, $\langle a^3b\rangle$.

Next, we note that $a^2 \in D_4$ is the only element of order 2 that commutes with all other elements. Thus this is the element that must be associated with complex conjugation. Drawing the subgroup lattice gives



The subgroups $\langle b\rangle, \langle ab\rangle, \langle a^2b\rangle, \langle a^3b\rangle$ all correspond to intermediate CM-fields as these are the groups that do not contain complex conjugation.

### 3.4.2 The CM-types

To list the CM-types, we fix $\rho = a^2$ as only option for complex conjugation and we define

$$\phi_1 = e,\ \phi_2 = a,\ \phi_3 = b,\ \phi_4 = ba \implies \bar{\phi}_1 = a^2,\ \bar{\phi}_2 = a^3,\ \bar{\phi}_3 = a^2b,\ \bar{\phi}_4 = ba^3$$

To compute the equivalent CM-types, we compute the orbit of each CM-type under composition on the right by elements of the Galois group, where equivalent CM-types lie in the same orbit. The results are given below.

- $[\{\phi_1, \phi_2, \phi_3, \phi_4\}] = \{\{\phi_1, \phi_2, \phi_3, \phi_4\}, \{\bar{\phi}_1, \phi_2, \bar{\phi}_3, \phi_4\}, \{\bar{\phi}_1, \bar{\phi}_2, \bar{\phi}_3, \bar{\phi}_4\}, \{\phi_1, \bar{\phi}_2, \phi_3, \bar{\phi}_4\}\}$
- $[\{\phi_1, \bar{\phi}_2, \bar{\phi}_3, \phi_4\}] = \{\{\phi_1, \bar{\phi}_2, \bar{\phi}_3, \phi_4\}, \{\phi_1, \phi_2, \bar{\phi}_3, \bar{\phi}_4\}, \{\bar{\phi}_1, \phi_2, \phi_3, \bar{\phi}_4\}, \{\bar{\phi}_1, \bar{\phi}_2, \phi_3, \phi_4\}\}$
- $[\{\phi_1, \phi_2, \phi_3, \bar{\phi}_4\}] = \{\{\phi_1, \phi_2, \phi_3, \bar{\phi}_4\}, \{\bar{\phi}_1, \phi_2, \phi_3, \phi_4\}, \{\bar{\phi}_1, \bar{\phi}_2, \bar{\phi}_3, \phi_4\}, \{\phi_1, \bar{\phi}_2, \bar{\phi}_3, \bar{\phi}_4\}\}$
- $[\{\phi_1, \bar{\phi}_2, \phi_3, \phi_4\}] = \{\{\phi_1, \bar{\phi}_2, \phi_3, \phi_4\}, \{\phi_1, \phi_2, \bar{\phi}_3, \phi_4\}, \{\bar{\phi}_1, \phi_2, \bar{\phi}_3, \bar{\phi}_4\}, \{\bar{\phi}_1, \bar{\phi}_2, \phi_3, \bar{\phi}_4\}\}$

### 3.4.3 The reflex fields

From Theorem 1.3.22, we know that the reflex field of a CM-type $\Phi$ is given by the fixed field of $\{\sigma \mid \sigma\Phi = \Phi\}$. Furthermore, Theorem 1.3.32 shows that we only have to do these computations for the four representatives of each equivalence class. These computations can be easily bruteforced, but can also be executed efficiently by means of the following observations.

1. The types in each equivalence class have the same reflex field, thus we look for elements $\sigma \in \mathrm{Gal}(K/\mathbb{Q}) = D_4$ such that for each CM-type $\Phi$ in the equivalence class, we have $\sigma\Phi = \Phi$.
2. A CM-type $\Phi$ in which $\phi_1 = e \in D_4$ is present, can only be fixed by embeddings in $\Phi$ as $e$ must be sent to some other embedding in the CM-type.
3. Each equivalence class has exactly 2 CM-types in which $\phi_1 = e$ is present, name these types $\Phi_1$ and $\Phi_2$. Thus the $\sigma \in D_4$ fixing the CM-types in these orbits must be an embedding in both $\Phi_1$ and $\Phi_2$.

This last point can in practice be used for finding the reflex fields efficiently. For example in the first equivalence class $\{\{\phi_1, \phi_2, \phi_3, \phi_4\}, \{\bar{\phi}_1, \phi_2, \bar{\phi}_3, \phi_4\}, \{\bar{\phi}_1, \bar{\phi}_2, \bar{\phi}_3, \bar{\phi}_4\}, \{\phi_1, \bar{\phi}_2, \phi_3, \bar{\phi}_4\}\}$, we see that $\Phi_1 = \{\phi_1, \phi_2, \phi_3, \phi_4\}$ and $\Phi_2 = \{\phi_1, \bar{\phi}_2, \phi_3, \bar{\phi}_4\}\}$. Thus $\Phi_1$ and $\Phi_2$ can only be fixed simultaneously by $\phi_1 = e \in D_4$ and $\phi_3 = b \in D_4$, as these are the only 2 embeddings present in both $\Phi_1$ and $\Phi_2$. Hence we see that $\{\phi_1, \phi_2, \phi_3, \phi_4\}$ is induced from the field $K^{\langle b \rangle}$. Repeating this procedure for the other CM-types yields

- CM-types equivalent to $\{\phi_1, \phi_2, \phi_3, \phi_4\}$ have $K^r = K^{\langle b \rangle}$ as reflex field;
- CM-types equivalent to $\{\phi_1, \bar{\phi}_2, \bar{\phi}_3, \phi_4\}$ have $K^r = K^{\langle a^2 b \rangle}$ as reflex field;
- CM-types equivalent to $\{\phi_1, \phi_2, \phi_3, \bar{\phi}_4\}$ have $K^r = K^{\langle ba^3 \rangle}$ as reflex field;
- CM-types equivalent to $\{\phi_1, \bar{\phi}_2, \phi_3, \phi_4\}$ have $K^r = K^{\langle ba \rangle}$ as reflex field.

### 3.4.4 The primitive CM-types

By Theorem 1.3.28, we know that $\Phi$ is primitive if and only if $\Phi$ has eight elements per equivalence class. Given that each equivalence class has four elements, there are no primitive CM-types.

### 3.4.5 An example

Using a database such as lmfdb.org, we find that the splitting field of

$$p(x) := x^8 + 16x^6 + 75x^4 + 88x^2 + 1,$$

is a CM-field with Galois group isomorphic to $D_4$.

## 3.5 The group $(\mathbb{Z}_2)^3$

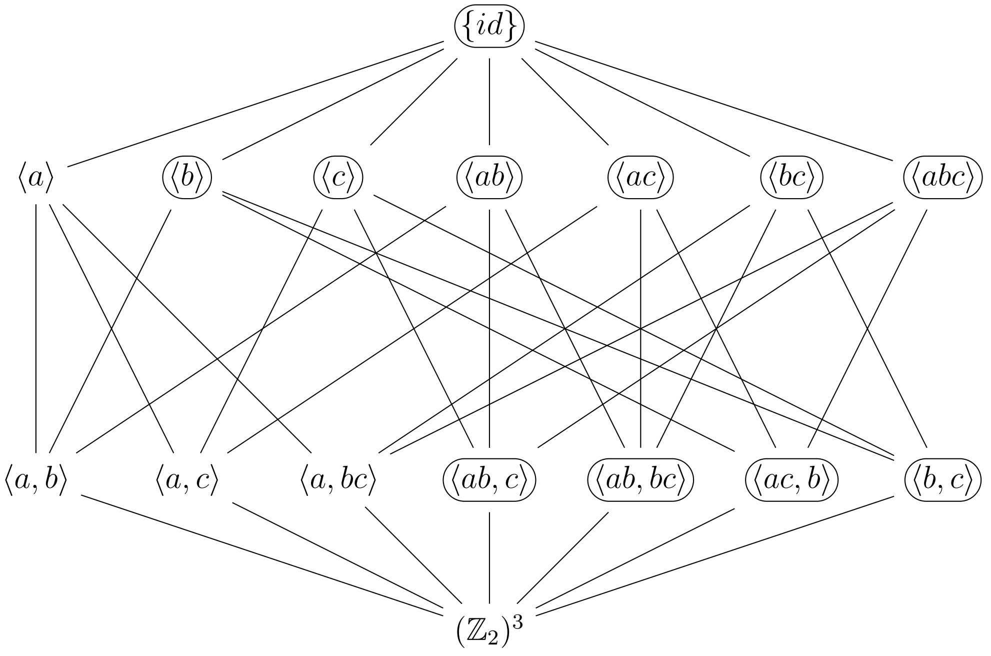
The last case we study is $G \cong (\mathbb{Z}_2)^3$. Here we notice that there are seven elements of order 2 in the center of $G$, however, we claim that there is only one $\rho$-structure. Before showing this, we first compute the subgroup lattice. For notational reasons, we write $(\mathbb{Z}_2)^3$ in representation notation, that is

$$(\mathbb{Z}_2)^3 = \{a, b, c \mid a^2 = b^2 = c^2 = 1, ab = ba, ac = ca, bc = cb\}.$$

Using this notation, one can identify the subgroups

- Order 4: $\langle a, b\rangle$, $\langle a, c\rangle$, $\langle a, bc\rangle$, $\langle ab, c\rangle$, $\langle ab, bc\rangle$, $\langle ac, b\rangle$, $\langle b, c\rangle$;
- Order 2: $\langle a\rangle$, $\langle b\rangle$, $\langle c\rangle$, $\langle ab\rangle$, $\langle ac\rangle$, $\langle bc\rangle$, $\langle abc\rangle$.

Computing the subgroup lattice yields



In the above lattice, the element $a$ was chosen to represent complex conjugation. However, we can also choose $b, c, ab, ac, bc$ or $abc$. However, we claim these seven choices for $\rho$ all lie in the same $\rho$-structure so that they result in identical reflex fields and primitive CM-types.

### 3.5.1 The $\rho$-structures

To show that all CM-types lie in the same $\rho$-structure, we make use of the following lemma.

**Lemma 3.5.1** ([HR06]). The automorphism group of groups of the form $G \cong \mathbb{Z}_p^n$ is given by $\mathrm{Aut}(\mathbb{Z}_{p^n}) \cong GL(n, \mathbb{Z}_p))$, where $GL(n, \mathbb{Z}_p)$ denotes $n \times n$ invertible matrices with entries in the field $\mathbb{Z}_p$ and transforms vectors $(x_1, x_2, x_3 \dots x_n) \in \mathbb{Z}_p^n$. □

**Theorem 3.5.2.** Let $G \cong (\mathbb{Z}_2)^3$, then $G$ has a unique $\rho$-structure.

*Proof.* Let $\rho_1, \rho_2 \in G$ be arbitrary order 2 elements of $G$. Since $\rho_1$ is order 2 we have that $\rho_1$ is not identically 0 and thus for each $\rho_2 \in G$, there exists a matrix $A$ with entries in $\mathbb{Z}_2$ such that $A\rho_1 = \rho_2$. Furthermore, since $\rho_2$ is not identically 0, we must have that $A$ is invertible. Thus by Lemma 3.5.1, we have that $A$ is an automorphism. Hence there is only one $\rho$-structure. $\square$

### 3.5.2 The CM-types

To find the CM-types, we first fix an element that represents complex conjugation. Since there is only one $\rho$-structure, it does not matter which order 2 element represents complex conjugation. We set $\rho = a$ to represent complex conjugation. This yields the embeddings

$$\phi_1 = id,\ \phi_2 = b,\ \phi_3 = c,\ \phi_4 = bc,$$

with conjugated embeddings given by

$$\bar{\phi}_1 = a,\ \bar{\phi}_2 = ab,\ \bar{\phi}_3 = ac,\ \bar{\phi}_4 = abc.$$

The equivalence classes are computed to be as follows:

$$\begin{aligned}
[\{\phi_1, \phi_2, \phi_3, \phi_4\}] =& \{\{\phi_1, \phi_2, \phi_3, \phi_4\}, \{\bar{\phi}_1, \bar{\phi}_2, \bar{\phi}_3, \bar{\phi}_4\}\};\\
[\{\bar{\phi}_1, \phi_2, \bar{\phi}_3, \phi_4\}] =& \{\{\bar{\phi}_1, \phi_2, \bar{\phi}_3, \phi_4\}, \{\phi_1, \bar{\phi}_2, \phi_3, \bar{\phi}_4\}\};\\
[\{\bar{\phi}_1, \bar{\phi}_2, \phi_3, \phi_4\}] =& \{\{\bar{\phi}_1, \bar{\phi}_2, \phi_3, \phi_4\}, \{\phi_1, \bar{\phi}_2, \bar{\phi}_3, \phi_4\}, \{\phi_1, \phi_2, \bar{\phi}_3, \bar{\phi}_4\}, \{\bar{\phi}_1, \phi_2, \phi_3, \bar{\phi}_4\}\};\\
[\{\bar{\phi}_1, \phi_2, \phi_3, \phi_4\}] =& \{\{\bar{\phi}_1, \phi_2, \phi_3, \phi_4\}, \{\phi_1, \bar{\phi}_2, \phi_3, \phi_4\}, \{\phi_1, \phi_2, \bar{\phi}_3, \phi_4\}, \{\phi_1, \phi_2, \phi_3, \bar{\phi}_4\}\\
& \{\phi_1, \bar{\phi}_2, \bar{\phi}_3, \bar{\phi}_4\}, \{\bar{\phi}_1, \phi_2, \bar{\phi}_3, \bar{\phi}_4\}, \{\bar{\phi}_1, \bar{\phi}_2, \phi_3, \bar{\phi}_4\}, \{\bar{\phi}_1, \bar{\phi}_2, \bar{\phi}_3, \phi_4\}\}.
\end{aligned}$$

### 3.5.3 The reflex fields

The different reflex fields are computed to be

- The CM-type $\{\phi_1, \phi_2, \phi_3, \phi_4\}$ has reflex field $K^r = K^{\langle b,c\rangle}$;
- The CM-type $\{\bar{\phi}_1, \phi_2, \bar{\phi}_3, \phi_4\}$ has reflex field $K^r = K^{\langle ac,b\rangle}$;
- The CM-type $\{\bar{\phi}_1, \bar{\phi}_2, \phi_3, \phi_4\}$ has reflex field $K^r = K^{\langle ac\rangle}$;
- The CM-type $\{\bar{\phi}_1, \phi_2, \phi_3, \phi_4\}$ has reflex field $K^r = K^{id}$.

### 3.5.4 The primitive CM-types

We use Theorem 1.3.34 to find that the CM-subfield that induces a CM-type $\Phi$ is given by the reflex field of $\Phi$. In particular, the CM-types equivalent to $\{\bar{\phi}_1, \phi_2, \phi_3, \phi_4\}$ are primitive. The other CM-types are induced.

### 3.5.5 An example

In this case, we can easily find an example as we can take the field $\mathbb{Q}(\sqrt{2}, \sqrt{3}, i)$. Note that this field is the splitting field of the minimal polynomial of $\alpha := \sqrt{2} + \sqrt{3} + i$ which is given by $p(x) = x^8 - 16x^6 + 88x^4 + 192x^2 + 144$.

The roots of this polynomial are given by $\pm\sqrt{2} \pm \sqrt{3} \pm i$. One can check that $\mathbb{Q}(\alpha)$ contains all algebraic conjugates of $\alpha$ and thus is Galois over $\mathbb{Q}$. Furthermore, it is easily checked that $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) \cong (\mathbb{Z}_2)^3$ as each automorphism in $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ is determined by choosing between sending $\sqrt{2} \to \pm\sqrt{2}$, $\sqrt{3} \to \pm\sqrt{3}$ and $i \to \pm i$.

Lastly note that $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2}, \sqrt{3})] = 2$. The field $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{(3)})$ is a totally real field, which follows from Lemma 1.2.5, and $\mathbb{Q}(\alpha)$ does not have real embeddings. Therefore, $\mathbb{Q}(\alpha)$ is a CM-field.

# 4 Generalization $\rho$-structure abelian groups

The objective of this section is to determine the distinct $\rho$-structures for arbitrary finite abelian groups. For this, we recall that two order 2 elements $\rho$ and $\rho'$ in the center of $G$ represent the same $\rho$-structure if there exists an automorphism $\psi \in \mathrm{Aut}(G)$ such that $\psi(\rho) = \rho'$. To start the analysis, we introduce basic results on automorphisms of finite abelian groups.

## 4.1 Prerequisites

The first step in classifying the $\rho$-structures for finite abelian groups is classifying finite abelian groups themselves. This can be done through the primary structure theorem.

**Proposition 4.1.1.** Define $H_p \cong (\mathbb{Z}_{p^{e_1}})^{n_1} \times (\mathbb{Z}_{p^{e_2}})^{n_2} \times \cdots \times (\mathbb{Z}_{p^{e_n}})^{n_m}$, for some prime $p$, where $n_i, e_i$ are natural numbers, such that $e_1 < e_2 < \cdots < e_m$. Then any finite abelian group can be written as a product of groups $H_{p_i}$, where each $p_i$ is a distinct prime.

**Remark 4.1.2.** Observe that abelian Galois groups corresponding to CM-fields have even degree, thus $H_2$ must be present in the primary decomposition of $G$.

For $\rho$-structures, only the automorphisms evaluated at elements of order 2 are taken into account. This implies that we only take into account the part of the automorphism that acts on elements of order 2.

**Prerequisite 4.1.3.** Let $G$ be a finite abelian group such that $G \cong G_1 \times G_2$. If $|G_1|$ and $|G_2|$ are relatively prime, then $\mathrm{Aut}(G) \cong \mathrm{Aut}(G_1) \times \mathrm{Aut}(G_2)$. In particular, when decomposing $G$ according to the primary structure theorem, we note that

$$\mathrm{Aut}(G) \cong \mathrm{Aut}(H_{p_1}) \times \mathrm{Aut}(H_{p_2}) \times \cdots \times \mathrm{Aut}(H_{p_k}).$$

We use the above result to show that an automorphism of $G$ sending $\rho \to \rho'$ exists if and only if there exists an automorphism sending $\rho_1 \to \rho_1'$, where $\rho_1$ denotes the part of $\rho$ that lives in $H_2$. More formally this is stated as follows.

**Lemma 4.1.4.** Let $G \cong H_2 \times H_{p_2} \times \cdots \times H_{p_k}$, where each $p_i$ is a prime larger than 2. Let $\rho \in G$ be an element of order 2 and $\psi \in \mathrm{Aut}(G)$. Write $\rho = (\rho_1, \rho_2, \ldots, \rho_k)$, such that $\rho_i \in H_{p_i}$ and write $\psi = (\psi_1, \psi_2, \ldots, \psi_k) \in \mathrm{Aut}(H_2) \times \mathrm{Aut}(H_{p_2}) \times \cdots \times \mathrm{Aut}(H_{p_k})$. Then $\psi(\rho) = (\psi_1(\rho_1), 0, 0, \ldots, 0) \in G$.

*Proof.* Let $\rho \in G \cong H_2 \times H_{p_2} \times \cdots \times H_{p_k}$ be an element of order 2. Write $\rho = (\rho_1, \rho_2, \ldots, \rho_k)$ where each $\rho_i \in H_{p_i}$. Note that $2\rho = 0 \in G$ so that $2\rho_i = 0 \in H_{p_i}$. Since the order of elements must divide the order of the group, we have that $\rho_i = 0 \in H_{p_i}$, except for $\rho_1$, which follows from the fact that $|H_{p_i}|$ is a multiple of $p_i$ and thus only $|H_2|$ is a multiple of 2. Thus $\rho = (\rho_1, 0, 0, \ldots, 0) \in G$ and $\psi(\rho) = (\psi_1(\rho_1), \psi_2(0), \ldots, \psi_k(0)) = (\psi_1(\rho_1), 0, \ldots, 0)$, as desired. □

**Corollary 4.1.5.** With $G$ as above, write $\rho = (\rho_1, 0, 0, \dots, 0)$ and $\rho' = (\rho'_1, 0, 0, \dots, 0)$ where $\rho_1, \rho'_1 \in H_2$ so that $\rho, \rho'$ are the most general order 2 elements in $G$. The above lemma gives us that $\exists \psi \in \mathrm{Aut}(G)$ such that $\psi(\rho) = \rho' \iff \exists \psi_1 \in H_2$ such that $\psi_1(\rho_1) = \rho'_1$.

**Remark 4.1.6.** This shows that we only need to take the automorphisms of $H_2$ into account when computing the $\rho$-structures. We make the observation that for two arbitrary order 2 elements $\rho, \rho' \in G$, there exist an automorphism $\psi \in \mathrm{Aut}(G) \iff \rho'$ is in the orbit of $\rho$ when $\mathrm{Aut}(G)$ acts on the set of order 2 elements of $G$. This hints at the fact that the number of $\rho$-structures is equal to the number of distinct orbits. We formalize this idea in the following lemma.

**Lemma 4.1.7.** Let $G \cong H_2 \times H_{p_2} \times \cdots \times H_{p_k}$ and let $\mathrm{Aut}(H_2)$ act on the set of order 2 elements $\rho_1 \in H_2$ according to $\psi \cdot \rho_1 \coloneqq \psi(\rho_1)$. Then the number of $\rho$-structures equals the number of orbits of this action.

*Proof.* We first proof the statement that $\rho$ and $\rho'$ represent the same $\rho$-structure if and only if $\rho$ and $\rho'$ lie in the same orbit when the action is as defined above. Indeed by definition $\rho$ and $\rho'$ define the same $\rho$-structure if and only if there exist $\psi \in G$ such that $\psi(\rho) = \rho'$. Furthermore, Theorem 4.1.5 shows that we have $\exists \psi \in \mathrm{Aut}(G)$ such that $\psi(\rho) = \rho' \iff \exists \psi_1 \in \mathrm{Aut}(H_2)$ such that $\psi_1(\rho_1) = \rho'_1$, which is true if and only if $\rho'_1$ lies in the orbit of $\rho_1$.

Since $\rho$ and $\rho'$ represent the same $\rho$-structure if and only if they lie in the same orbit, we immediately conclude that the number of $\rho$-structures equals the number of orbits of the action of $\mathrm{Aut}(H_2)$ on order 2 elements in $H_2$. □

The prerequisites imply that the course of action that will be taken comes down to computing the number of orbits of $\mathrm{Aut}(H_2)$ on the set of order 2 elements in $H_2$. To do this, we look at two cases where we restrict the structure of $H_2$ to make the analysis easier. Only in Section 4.3 do we compute the $\rho$-structures for the most general form of $H_2$.

One of these restrictions has to do with groups of the form $(\mathbb{Z}_2)^n$. Recall that the automorphism group of is given by the following result (Theorem 3.5.1).

**Prerequisite 4.1.8.** The automorphism group of groups of the form $G \cong \mathbb{Z}_p^n$ is given by $\mathrm{Aut}(\mathbb{Z}_{p^n}) \cong GL(n, \mathbb{Z}_p))$, where $GL(n, \mathbb{Z}_p)$ denotes $n \times n$ invertible matrices with entries in the field $\mathbb{Z}_p$ and transforms vectors $(x_1, x_2, \dots, x_n) \in \mathbb{Z}_p^n$.

## 4.2 Two weaker results

The 2 restrictions of $H_2$ that we analyze first are given by the following cases.

1. $H_2 \cong (\mathbb{Z}_2)^n$ i.e. $e_1 = 1$ and $n_1 = n$ in the primary decomposition theorem;
2. $H_2 \cong \mathbb{Z}_{2^{e_1}} \times \mathbb{Z}_{2^{e_2}} \times \cdots \times \mathbb{Z}_{2^{e_m}}$ with $e_1 < e_2 < \cdots < e_m$ i.e. when each $n_i = 1$ in the primary decomposition theorem.

### 4.2.1 The first weak result

Fix $H_2 \cong (\mathbb{Z}_2)^n$ such that the most general finite abelian group with this $H_2$ in the primary decomposition is given by $G \cong (\mathbb{Z}_2)^n \times H_{p_2} \times \cdots \times H_{p_k}$. The following result holds.

**Theorem 4.2.1.** Let $G \cong H_2 \times H_{p_2} \times \cdots \times H_{p_k}$, where $H_2 \cong (\mathbb{Z}_2)^n$. Then $G$ has a unique $\rho$-structure.

*Proof.* Let $G$ be an abelian group such that $G \cong H_2 \times H_{p_2} \times \cdots \times H_{p_k}$, where $H_2 \cong (\mathbb{Z}_2)^n$. As per Remark 4.1.5, we only need to find the orbits of the action of $\mathrm{Aut}(H_2)$ on the order 2 elements in $H_2$. Define $\rho = (c_1, c_2, \ldots, c_n)$ and $\rho' = (c_1', c_2', \ldots, c_n')$ where each $c_i, c_i' \in 0, 1$ as most general order 2 element in $(\mathbb{Z}_2)^n$. Since $\rho$ and $\rho'$ are vectors with entries in $\mathbb{Z}_2$ and not identically zero, we know from linear algebra that there exists an invertible matrix $B$ with entries in $\mathbb{Z}_2$ such that $B\rho = \rho'$. Thus $B \in GL(n, \mathbb{Z}_2) = \mathrm{Aut}(H_2)$ by Proposition 4.1.8. Therefore, arbitrary order 2 elements $\rho, \rho' \in H_2$ lie in the same orbit. □

**Remark 4.2.2.** Note that the group $(\mathbb{Z}_2)^3$ is of the form as described in Theorem 4.2.1. This shows that $(\mathbb{Z}_2)^3$ has a unique $\rho$-structure as agrees with in Section 3.5.

### 4.2.2 Computing Aut($H_2$)

To find all possible $\rho$-structures of any abelian group, we need to find the automorphism group of $H_2$ in the most broad definition of $H_2$. Luckily, the automorphism groups of finite abelian groups are fully classified and can be computed using a method described in [HR06]. Below, we summarize this method and apply it to find the automorphism group of $\mathbb{Z}_2 \times \mathbb{Z}_4$ and show that the outcome reconciles with the result obtained in Section 3.1.

**The method:**
Write $H_p \cong (\mathbb{Z}_{p^{e_1}})^{n_1} \times (\mathbb{Z}_{p^{e_2}})^{n_2} \times \ldots \times (\mathbb{Z}_{p^{e_m}})^{n_m}$ for a fixed prime $p$ and $e_i, n_i \in \mathbb{N}$, such that $e_1 < e_2 < \cdots < e_m$. We denote with $R_p$ block matrices of the form.

$$A = \begin{bmatrix} B_{11} & B_{12} & B_{13} & \ldots & B_{1m} \\ p^{e_2-e_1}B_{21} & B_{22} & B_{33} & \ldots & B_{2m} \\ p^{e_3-e_1}B_{31} & p^{e_3-e_2}B_{32} & B_{33} & \ldots & B_{3m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p^{e_m-e_1}B_{m1} & p^{e_m-e_2}B_{m2} & p^{e_m-e_3}B_{m3} & \ldots & B_{mm} \end{bmatrix} \text{ where } B_{ij} \in \mathbb{Z}^{n_i \times n_j}.$$

In [HR06], it was shown that $R_p$ forms a ring under standard matrix multiplication and addition. Define $\psi\colon R_p \to \mathrm{End}(H_p)$ by $\psi(A)(\bar{h}_1, \bar{h}_2, \ldots, \bar{h}_n)^T = \pi(A(h_1, h_2, \ldots, h_n)^T)$, where $(\bar{h}_1, \ldots, \bar{h}_n) \in H_p$ and $\pi$ is the projection of $\mathbb{Z}^n$ onto $H_p$. Then $\psi$ is a surjective ring homomorphism. We denote $\pi = (\pi_1, \pi_2 \ldots, \pi_m)$ where $\pi_i$ is given by reducing modulo $p^{e_i}$ such that $\pi$ indeed forms the projection onto $H_p$.

Lastly, it was shown that $\psi(A)$ is an automorphism $\iff$ $A$ (modulo $p$) is in $GL(n, \mathbb{Z}_p)$.

**Remark 4.2.3.** Note that the definitions of $H_p$ and the matrices $A \in R_p$ are different in the above described method than in [HR06]. The notation used above is more useful for describing $\rho$-structures, and we will proof that both definitions are indeed equivalent.

*Proof.* We note that the notation used in [HR06] for $H_p = \mathbb{Z}_{p^{e_1}} \times \mathbb{Z}_{p^{e_2}} \times \cdots \times \mathbb{Z}_{p^{e_n}}$ where the $e_i$'s are integers and $e_1 \leq e_2 \leq \cdots \leq e_n$ instead of writing $H_2 = (\mathbb{Z}_{2^{e_1}})^{n_1} \times \cdots \times (\mathbb{Z}_{2^{e_m}})^{n_m}$. Furthermore, they define $R_p$ to contain matrices of the form

$$R_p = \{(a_{ij}) \in \mathbb{Z}^{n \times n} : p^{e_i - e_j} \mid a_{ij} \text{ for all } i, j \text{ satisfying } 1 \leq i \leq j \leq n\}$$

We show that $R_p$ as defined in the method 4.2.2 is the same as the above definition by use of 4 steps.

1. Let $H_p \cong \mathbb{Z}_{p^{e_1}} \times \mathbb{Z}_{p^{e_2}} \times \cdots \times \mathbb{Z}_{p^{e_n}}$ Where $e_1 \leq e_2 \leq \cdots \leq e_n$. It directly follows from the definition given in [HR06], that $A$ is of the form

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ p^{e_2-e_1}a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ p^{e_3-e_1}a_{31} & p^{e_3-e_2}a_{32} & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p^{e_n-e_1}a_{n1} & p^{e_n-e_2}a_{n2} & p^{e_n-e_3}a_{n3} & \cdots & a_{nn} \end{bmatrix} \text{ where } a_{ij} \in \mathbb{Z}.$$

2. Now we group together $\mathbb{Z}_{p^{e_i}}$ and $\mathbb{Z}_{p^{e_j}}$ whenever $e_i = e_j$. This gives the following result $H_p \cong \mathbb{Z}_{p^{e_1}} \times \mathbb{Z}_{p^{e_2}} \times \cdots \times \mathbb{Z}_{p^{e_n}} = (\mathbb{Z}_{p^{e_1}})^{n_1} \times (\mathbb{Z}_{p^{e_{k_2}}})^{n_2} \times \cdots \times (\mathbb{Z}_{p^{e_{k_m}}})^{n_m}$ where each $k_j$ is given by $1+\sum_{i=1}^{j} n_i$. Note that after this grouping, we have strict inequality between each $e_{k_j}$, that is to say we get $e_1 < e_{k_1} < \cdots < e_{k_m}$.

3. Now we note that for the entries $b_{lq}$ where $k_i \leq l < k_{i+1}$ and $k_j \leq q < k_{j+1}$ with $i < j$, i.e. strict upper triangular part, we have by the definition of $R_p$ in [HR06] that each $b_{lq} \in \mathbb{Z}$. Hence we can define the submatrix $B_{k_i k_j} = (b_{lq}) \in \mathbb{Z}^{n_i \times n_j}$.

   For the entries $b_{lq}$ where $k_i \leq l < k_{i+1}$ and $k_i \leq q < k_{i+1}$ (i.e. $i = j$), we have by the definition of $R_p$ in [HR06] that each $b_{lq} \in \mathbb{Z}$ as for the entries $b_{lq}$ with $l > q$, we get $b_{lq} \in \mathbb{Z}$ and for $l \leq q$, we get $p^{e_l - e_q} = p^0 = 1 \mid b_{lq}$ and thus also $b_{lq} \in \mathbb{Z}$. Hence we can define the submatrix $B_{k_i k_j} = (b_{lq}) \in \mathbb{Z}^{n_i \times n_i}$.

   For the entries $b_{lq}$ where $k_i \leq l < k_{i+1}$ and $k_j \leq q < k_{j+1}$ with $i > j$, we have by the definition of $R_p$ in [HR06] that for each $b_{lq}$, we have that $p^{e_l - e_q} \mid b_{lq}$. Recall that we have that $e_l = e_{k_i}$ and $e_q = e_{k_j}$ for each $l$ and $q$ in the range $k_i \leq l < k_{i+1}$ and $k_j \leq q < k_{j+1}$. Thus we get $p^{e_l - e_q} \mid b_{lq} \iff b_{lq} = p^{e_{k_i} - e_{k_j}} b'_{lq}$ where $b'_{lq} \in \mathbb{Z}$. Thus we can define submatrix $B_{k_i k_j} = p^{e_{k_i} - e_{k_j}}(b'_{lq}) \in (p^{e_{k_i} - k_j}\mathbb{Z})^{n_i \times n_j}$.

4. Note that in the above definition of submatrices, we can use a change of variables to rename $k_i$ to be $i$ and $k_j$ to be $j$. Under this new definition, we find that we have $H_p \cong (\mathbb{Z}_{p^{e_1}})^{n_1} \times (\mathbb{Z}_{p^{e_2}})^{n_2} \times \cdots \times (\mathbb{Z}_{p^{e_m}})^{n_m}$ and careful considerations of the

dimensions of the block matrices indeed shows that we can now write the matrices inside $R_p$ as block matrices of the form.

$$A = \begin{bmatrix} B_{11} & B_{12} & B_{13} & \dots & B_{1m} \\ p^{e_2-e_1}B_{21} & B_{22} & B_{33} & \dots & B_{2m} \\ p^{e_3-e_1}B_{31} & p^{e_3-e_2}B_{32} & B_{33} & \dots & B_{3m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p^{e_m-e_1}B_{m1} & p^{e_m-e_2}B_{m2} & p^{e_m-e_3}B_{m3} & \dots & B_{mm} \end{bmatrix} \text{ where } B_{ij} \in \mathbb{Z}^{n_i \times n_j}.$$

This coincides with the definition given in the method 4.2.2 and thus these definitions for matrices in $R_p$ are equivalent. Thus the above method gives a valid way to compute all automorphisms.

□

**Example 4.2.4.** We illustrate the proof by an example: Let $H_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_8 \times \mathbb{Z}_8$. According to the definition given in [HR06], we have that matrices in $R_2$ are of the form

$$A = \begin{bmatrix} b_{11} & b_{12} & b_{13} & b_{14} & b_{15} \\ 2^{1-1}b_{21} & b_{22} & b_{23} & b_{24} & b_{25} \\ 2^{2-1}b_{31} & 2^{2-1}b_{32} & b_{33} & b_{34} & b_{35} \\ 2^{3-1}b_{41} & 2^{3-1}b_{42} & 2^{3-2}b_{43} & b_{44} & b_{45} \\ 2^{3-1}b_{51} & 2^{3-1}b_{52} & 2^{3-2}b_{53} & 2^{3-3}b_{54} & b_{55} \end{bmatrix} \text{ where } b_{ij} \in \mathbb{Z}.$$

Rewriting $H_2$ by grouping $\mathbb{Z}_{2^{e_i}}$ with $\mathbb{Z}_{2^{e_j}}$ whenever $e_i = e_j$ gives $H_2 \cong (\mathbb{Z}_2)^2 \times \mathbb{Z}_4 \times (\mathbb{Z}_8)^2$. In the notation of the proof, we find that $n_1 = 2, n_2 = 1, n_3 = 2$ and $k_1 = 1, k_2 = 3, k_3 = 4$. Thus, when considering $A$ as a block matrix, $A$ has 9 submatrices $B_{k_ik_j}$. For example, note $B_{k_2k_1} = \begin{bmatrix} 2b_{31} & 2b_{32} \end{bmatrix}$, which is indeed $n_2 \times n_1 = 1 \times 2$ and $B_{k_3k_1} = \begin{bmatrix} 4b_{41} & 4b_{42} \\ 4b51 & 4b_{52} \end{bmatrix}$. Computing the other block matrices gives the following result for $A$.

$$A = \begin{bmatrix} B_{11} & B_{12} & B_{13} \\ 2B_{21} & B_{22} & B_{23} \\ 4B_{31} & 2B_{32} & B_{33} \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} & | & b_{13} & | & b_{14} & b_{15} \\ b_{21} & b_{22} & | & b_{23} & | & b_{24} & b_{25} \\ -- & -- & + & -- & + & -- & -- \\ 2b_{31} & 2b_{32} & | & b_{33} & | & b_{34} & b_{35} \\ -- & -- & + & -- & + & -- & -- \\ 4b_{41} & 4b_{42} & | & 2b_{43} & | & b_{44} & b_{45} \\ 4b_{51} & 4b_{52} & | & 2b_{53} & | & b_{54} & b_{55} \end{bmatrix}.$$

This indeed coincides with the matrix given by the definition in Section 4.2.2.

**Example 4.2.5.** Now we can use this new theory to recover the fact that we got 2 $\rho$-structures in the case $G = \mathbb{Z}_2 \times \mathbb{Z}_4$. For this, we note that $\mathbb{Z}_2 \times \mathbb{Z}_4$ corresponds to the values $p = 2, e_1 = 1, e_2 = 2$ and $n_1 = n_2 = 1$. Thus we find the following matrices $A$ that make up $R_2$,

$$A = \begin{bmatrix} b_{11} & b_{12} \\ 2b_{21} & b_{22} \end{bmatrix}.$$

Contrary to computing a matrix representation for $\psi(A)$ first and crossing out the ones where $A \notin GL(2,\mathbb{Z}_2)$, it is faster to reduce $A$ modulo 2 first and find a condition on the entries to make $A$ invertible as this drastically reduces the possible options for $\psi(A)$. Reducing $A$ modulo 2 yields the following 8 options.

$$\begin{bmatrix}0 & 0\\0 & 0\end{bmatrix}, \begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}, \begin{bmatrix}0 & 1\\0 & 0\end{bmatrix}, \begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}1 & 1\\0 & 0\end{bmatrix}, \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}0 & 1\\0 & 1\end{bmatrix}, \begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}.$$

Out of which, only 2 matrices are invertible, these matrices are given by

$$\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}.$$

Thus now we know that all automorphisms are given by $\psi(A)$ such that $A$ reduced modulo 2 gives the above cases. By slight abuse of notation, we will write the automorphisms corresponding to $\psi(A)$ as matrices that are deduced from $A$ by reducing the first row of $A$ modulo $p^{e_1} = 2$ and the second row of $A$ modulo $p^{e_2} = 4$. This new matrix agrees with the operation of $\psi(A)$ on elements in $\mathbb{Z}_2 \times \mathbb{Z}_4$ as the elements in the first row of $A$ end up only in the first entry of $\psi(A)(\vec{h})$ and thus will be reduced modulo 2 when projected onto $\mathbb{Z}_2 \times \mathbb{Z}_4$. Entries in the second row of $A$ only end up in $\pi_2$, and are thus reduced modulo 4. therefore, we may represent the automorphism $\psi(A)$ in this manner. Writing out the possible cases yield the following options for $\psi(A)$:

$$\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\0 & 3\end{bmatrix}, \begin{bmatrix}1 & 1\\0 & 3\end{bmatrix}, \begin{bmatrix}1 & 0\\2 & 1\end{bmatrix}, \begin{bmatrix}1 & 1\\2 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\2 & 3\end{bmatrix}, \begin{bmatrix}1 & 1\\2 & 3\end{bmatrix}.$$

From here we obtain the $\rho$-structures by taking arbitrary $\rho$ and $\rho'$ as order two elements, and seeing if for any of the above matrices, we have $A\rho = \rho'$. Note that this effectively comes down to computing the orbit of $\rho$ and checking whether this contains $\rho'$.

Recall that the three order 2 elements of $G \cong \mathbb{Z}_2 \times \mathbb{Z}_4$ were given by $\rho_1 = (1,0), \rho_2 = (0,2)$ and $\rho_3 = (1,2)$. We note that the orbit of $\rho_1$ is given by $\{(1,0),(1,2)\}$ and the orbit of $\rho_2 = (0,2)$ is given by $\{(0,2)\}$. Thus we find that there indeed exists an automorphism interchanging $\rho_1$ and $\rho_3$, but $\rho_2$ can not be changed to either $\rho_1$ or $\rho_3$ under automorphisms. Thus we find two different $\rho$-structures, which is consistent with the result in Lemma 3.1.1.

### 4.2.3 The second weak result

With the full characterization of the automorphisms of $H_2$, we can tackle the problem of finding all distinct $\rho$-structures. However, in spite of the fact that the result is rather satisfying, the notation involved in the proof gets cumbersome. To make ourselves more comfortable with the notation involved, we first solve in the case where we have the restriction $H_2 \cong \mathbb{Z}_{2^{e_1}} \times \cdots \times \mathbb{Z}_{2^{e_m}}$, where $e_1 < e_2 < \cdots < e_m$. Motivation behind this choice of $H_2$ comes from the fact that in this specific case, each block matrix inside $A \in R_2$ is of dimension $1 \times 1$. Furthermore, reducing $A$ (modulo 2) gives a triangular matrix, which makes finding conditions on invertibility more manageable. We formalize the above notion as follows.

**Theorem 4.2.6.** Let $H_2 \cong \mathbb{Z}_{2^{e_1}} \times \mathbb{Z}_{2^{e_2}} \times \cdots \times \mathbb{Z}_{2^{e_m}}$, where $e_1 < e_2 < \cdots < e_m$. Then $H_2$ has precisely $m$ different $\rho$-structures.

*Proof.* We note that any matrix $A \in R_2$ is given by

$$A = \begin{bmatrix} b_{11} & b_{12} & b_{13} & \dots & b_{1m} \\ 2^{e_2-e_1}b_{21} & b_{22} & b_{23} & \dots & b_{2m} \\ 2^{e_3-e_1}b_{31} & 2^{e_3-e_2}b_{32} & b_{33} & \dots & b_{3m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 2^{e_m-e_1}b_{m1} & 2^{e_m-e_2}b_{m2} & 2^{e_m-e_3}b_{m3} & \dots & b_{mm} \end{bmatrix} \text{ where } b_{ij} \in \mathbb{Z}.$$

Note that the submatrices are integers as each submatrix $B_{ij} \in \mathbb{Z}^{n_i \times n_j} = \mathbb{Z}^{1\times 1}$. Furthermore, observe that reducing modulo 2 gives the following upper triangular matrix:

$$A \text{ (modulo 2) } = \begin{bmatrix} \bar{b}_{11} & \bar{b}_{12} & \bar{b}_{13} & \dots & \bar{b}_{1m} \\ \bar{0} & \bar{b}_{22} & \bar{b}_{33} & \dots & \bar{b}_{2m} \\ \bar{0} & \bar{0} & \bar{b}_{33} & \dots & \bar{b}_{3m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \bar{0} & \bar{0} & \bar{0} & \dots & \bar{b}_{mm} \end{bmatrix}.$$

We know that $A \in GL(m, \mathbb{Z}_2))$ if and only if $b_{ii} \equiv 1$ (modulo 2) for all diagonal entries.

Next we compute $\psi(A)(\rho)$ under the condition that $b_{ii} \equiv 1 \pmod 2$. For this, we note that the most general order 2 element in $H_2$ is given by $\rho = (c_1 2^{e_1-1}, c_2 2^{e_2-1}, \dots, c_m 2^{e_m-1})$ where $c_i \in \{0, 1\}$. This ensures that $2\rho = 0 \in H_2$. This way of writing the order 2 element $\rho$ will be common practice through-out this section.

Then we get that $\psi(A)(\rho)$ is given by

$$\begin{aligned} \psi(A)(\rho) &= \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1m} & \\ 2^{e_2-e_1}b_{21} & b_{22} & b_{23} & \dots & b_{2m} \\ \vdots & \vdots & \ddots & \vdots & \\ 2^{e_m-e_1}b_{m1} & 2^{e_m-e_2}b_{m2} & \dots & b_{mm} & \end{bmatrix} \begin{bmatrix} c_1 2^{e_1-1} \\ c_2 2^{e_2-1} \\ \vdots \\ c_m 2^{e_m-1} \end{bmatrix} \\ &= \begin{bmatrix} \pi_1(b_{11}c_1 2^{e_1-1}) & + & \pi_1(b_{12}c_2 2^{e_2-1}) & + \cdots + & \pi_1(b_{1m}c_m 2^{e_m-1}) \\ \pi_2(b_{21}c_1 2^{e_2-1}) & + & \pi_2(b_{22}c_2 2^{e_2-1}) & + \cdots + & \pi_2(b_{2m}c_m 2^{e_m-1}) \\ \vdots & & \vdots & & \vdots \\ \pi_m(b_{m1}c_1 2^{e_m-1} & + & \pi_m(b_{m2}c_2 2^{e_m-1}) & + \cdots + & \pi_m(b_{mm}c_m 2^{e_m-1}) \end{bmatrix}. \end{aligned}$$

Where we used the additive property $\pi_i(x+y) = \pi_i(x) + \pi_i(y)$ which follows from the fact that $\pi_i$ is defined to be reduction modulo $2^{e_i}$.

Before explicitly computing the orbits, we make the observation that for $i < j$, we have that $c_j 2^{e_j-1} \equiv 0$ (modulo $2^{e_i}$), and thus $\pi_i(b_{ij}c_j 2^{e_j-1}) = \bar{0} \in \mathbb{Z}_{2^{e_i}}$. This reduces many entries in the above vector to 0.

Now we compute the number of orbits as follows: First we notice that order 2 elements of the form $\rho^{(j)} := (0, \dots, 0, 2^{e_j-1}, 0 \dots, 0)$ under automorphism $\psi$ must be send to elements of the from $\psi(A)(\rho^{(j)}) = \rho'$ in which the $j^{\text{th}}$ coordinate cannot be zero. This can most easily be seen from writing out $\psi(A)(\rho^{(j)})$ and setting $c_i = \delta_{ij}$ ($\delta_{ij}$ denotes the Kronecker delta).

$$\psi(A)(\rho^{(j)}) = \begin{bmatrix} \pi_1(b_{1j}2^{e_j-1}) \\ \pi_2(b_{2j}2^{e_j-1}) \\ \pi_3(b_{3j}2^{e_j-1}) \\ \vdots \\ \pi_m(b_{mj}2^{e_j-1}) \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ \pi_j(b_{jj}2^{e_j-1}) \\ \vdots \\ \pi_m(b_{mj}2^{e_j-1}) \end{bmatrix}.$$

Furthermore, recall that we have that $b_{jj} \equiv 1$ (modulo 2), which gives us the result that $\pi_j(b_{jj}2^{e_j-1}) = 2^{e_j-1} \neq 0$ (modulo $2^{e_j}$). Thus, the $j^{\text{th}}$ coordinate of $\psi(A)(\rho^{(j)}) = \rho'$ is not 0 which also shows that there are at least $m$ orbits as each $\rho^{(j)}$ must lie in a distinct orbit.

To prove that there are at most $m$ orbits of the order 2 elements, we let $\rho^{(j)}$ be as defined above and let $\rho'^{(j)} = (0, 0, \dots, 0, 2^{e_j-1}, c_{j+1}2^{e_{j+1}-1}, \dots, c_m 2^{e_m-1})$, where each $c_i \in \{0, 1\}$. We will show that $\rho'^{(j)}$ is in the orbit of $\rho^{(j)}$. Indeed, recall that

$$\psi(A)(\rho^{(j)}) = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ \pi_j(2^{e_j-1}) \\ \pi_{j+1}(b_{j+1j}2^{e_j-1}) \\ \vdots \\ \pi_m(b_{mj}2^{e_j-1}) \end{bmatrix}.$$

Note that for $i > j$ we can indeed make $\pi_i(b_{ij}2^{e_i-1}) = 0$ or $2^{e_i-1}$ by either fixing $b_{ij} \cong 0$ or $b_{ij} \cong 1$ (modulo 2). This shows that with correct choice of matrix $A$, we can indeed obtain $\psi(A)(\rho^{(j)})$ to be any element of the form $\rho'^{(j)}$. Therefore, $\rho'^{(j)}$ lies in the orbit of $\rho^{(j)}$. Furthermore, we note that any order 2 element is of the form $\rho'^{(j)}$ for some $1 \leq j \leq m$. This shows that there are at most $m$ orbits.

Thus we conclude there are exactly $m$ orbits and thus $m$ distinct $\rho$-structures as was claimed. □

We illustrate this proof by following the same steps in a specific example.

**Example 4.2.7.** We look at $H_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{16}$. Thus we take $e_1 = 1, e_2 = 2, e_3 = 4$ and $n_1 = n_2 = n_3 = 1$ so that $H_2$ is such that the above proof applies and we should find three distinct $\rho$-structures. We start by computing $A \in R_2$ and reducing $A$ (mod 2) to find the upper triangular matrix

$$A = \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ 2b_{21} & b_{22} & b_{23} \\ 8b_{31} & 4b_{32} & b_{33} \end{bmatrix} \implies A \text{ (mod 2)} = \begin{bmatrix} \bar{b}_{11} & \bar{b}_{12} & \bar{b}_{13} \\ \bar{0} & \bar{b}_{22} & \bar{b}_{23} \\ \bar{0} & \bar{0} & \bar{b}_{33} \end{bmatrix}.$$

Thus $A$ (mod 2) is invertible precisely when $b_{11} \equiv b_{22} \equiv b_{33} \equiv 1 \pmod 2$, thus we will write $b_{11} = 2b'_{11} + 1, b_{22} = 2b'_{22} + 1$ and $b_{33} = 2b'_{33} + 1$ to denote this.

We continue by computing matrix representations of $\psi(A)$ using the same abuse of notation as before

$$\bar{A} = \begin{bmatrix} 1 & 0 & 0 \\ 2b_{21} & 2b'_{22} + 1 & 0 \\ 8b_{31} & 4b_{32} & 2b'_{33} + 1 \end{bmatrix} \begin{array}{l} \leftarrow \text{reduced modulo } 2^1; \\ \leftarrow \text{reduced modulo } 2^2; \\ \leftarrow \text{reduced modulo } 2^4. \end{array}$$

Now we can compute all possible matrices $A$ of the above form and check the orbits of the order 2 elements to find that

- The orbit of $(1, 0, 0)$ is given by $\{(1, 0, 0), (1, 2, 0), (1, 0, 8), (1, 2, 8)\}$.
- The orbit of $(0, 2, 0)$ is given by $\{(0, 2, 0), (0, 2, 8)\}$.
- The orbit of $(0, 0, 8)$ is given by $\{(0, 0, 8)\}$.

Note that each order 2 element is in exactly one of these orbits and thus we conclude that there must be exactly 3 orbits and hence 3 $\rho$-structures.

## 4.3 The $\rho$-structures for finite abelian groups

The proof for the most general form of $H_2$ takes a similar approach to the proof of Theorem 4.2.6. However, when loosening the restriction $n_1 = n_2 = \cdots = n_m = 1$, we find that the submatrices of $A \in R_2$ now have dimension $n_i \times n_j$ rather than $1 \times 1$. This makes the consequent analysis more hazardous, but in essence, the proof does not change.

**Theorem 4.3.1.** Let $H_2 \cong (\mathbb{Z}_{2^{e_1}})^{n_1} \times (\mathbb{Z}_{2^{e_2}})^{n_2} \times \cdots \times (\mathbb{Z}_{2^{e_n}})^{n_m}$, where $e_1 < e_2 < \cdots < e_n$ and $e_i, n_i \in \mathbb{N}$. Then $H_2$ has $m$ different $\rho$-structures.

*Proof.* We note that any matrix $A \in R_2$ is given by

$$A = \begin{bmatrix} B_{11} & B_{12} & B_{13} & \dots & B_{1m} \\ 2^{e_2 - e_1} B_{21} & B_{22} & B_{33} & \dots & B_{2m} \\ 2^{e_3 - e_1} B_{31} & 2^{e_3 - e_2} B_{32} & B_{33} & \dots & B_{3m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 2^{e_m - e_1} B_{m1} & 2^{e_m - e_2} B_{m2} & 2^{e_m - e_3} B_{m3} & \dots & B_{mm} \end{bmatrix} \text{ where } B_{ij} \in \mathbb{N}^{e_i \times e_j}.$$

Furthermore, observe that reducing modulo 2 gives the following block-upper triangular matrix

$$A \text{ (modulo 2) } = \begin{bmatrix} \bar{B}_{11} & \bar{B}_{12} & \bar{B}_{13} & \dots & \bar{B}_{1m} \\ \bar{0} & \bar{B}_{22} & \bar{B}_{33} & \dots & \bar{B}_{2m} \\ \bar{0} & \bar{0} & \bar{B}_{33} & \dots & \bar{B}_{3m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \bar{0} & \bar{0} & \bar{0} & \dots & \bar{B}_{mm} \end{bmatrix},$$

where $\bar{B}_{ij}$ denotes that the entries of $B_{ij}$ have been taken modulo 2. Furthermore, we know that this matrix is invertible (i.e. in $GL(n,2)$) if and only if $\bar{B}_{ii}$ is invertible for every block matrix on the diagonal.

Next, we compute $\psi(A)(\rho)$ under the condition that $B_{ii}$ (modulo 2) is invertible. For this note that the most general order 2 element in $H_2$ is given by $\rho = (\rho_1, \rho_2, \rho_3, \ldots, \rho_m)$ where each $\rho_i = 2^{e_i-1} \cdot (c_1^i, c_2^i, c_3^i, \ldots, c_{e_i}^i)$ where $c_j^i \in \{0,1\}$. In other words $\rho_i$ is a vector with $e_i$ entries such that each entry is either 0 or $2^{e_i-1}$, this ensures that $2\rho_i = 0$ (modulo $2^{e_i}$).

Thus similarly as before, we find that $\psi(A)(\rho)$ is given by

$$\psi(A)(\rho) \begin{bmatrix} \pi_1(B_{11}\rho_1) & + & \pi_1(B_{12}\rho_2) & + \cdots + & \pi_1(B_{1m}\rho_m) \\ \pi_2(2^{e_2-e_1}B_{21}\rho_1) & + & \pi_2(B_{22}\rho_2) & + \cdots + & \pi_2(B_{2m}\rho_m) \\ \vdots & & \vdots & & \vdots \\ \pi_m(2^{e_m-e_1}B_{m1}\rho_1) & + & \pi_2(2^{e_m-e_2}B_{m2}\rho_2) & + \cdots + & \pi_2(B_{mm}\rho_m) \end{bmatrix}.$$

Again, we compute the number of orbits in the same manner as before. First we notice that order 2 elements of the form $\rho^{(j)} := (\rho_1, \rho_2, \ldots, \rho_m) = (0, 0, \ldots, 0, \rho_j, 0, \ldots, 0)$, with $\rho_j := (2^{e_j-1}, 0, \ldots, 0)$ must be send to $\psi(A)(\rho^{(j)}) = \rho'_1, \rho'_2, \ldots, \rho'_m$. In which $\rho'_j$ cannot be identically zero.

This claim follows from the observation that for $i < j$, we have $\rho_j \equiv 0$ (modulo $2^{e_i}$), and thus $\pi_i(B_{ij}\rho_j) = \bar{0} \in \mathbb{Z}_{2^{e_i}}$. Which allows us to compute $\psi(A)(\rho^{(j)})$ explicitly:

$$\psi(A)(\rho^{(j)}) = \begin{bmatrix} \pi_1(B_{1j}\rho_j) \\ \pi_2(B_{2j}\rho_j) \\ \pi_3(B_{3j}\rho_j) \\ \vdots \\ \pi_m(B_{mj}\rho_j) \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ \pi_j(B_{jj}\rho_j) \\ \vdots \\ \pi_m(B_{mj}\rho_j) \end{bmatrix}.$$

Recall that $B_{jj}$ is invertible modulo 2 and that $\rho_j = (2^{e_j-1}, 0, \ldots, 0)$ Thus we note that $\pi_j(B_{jj}\rho_j)$ cannot be identically 0, as claimed. Again, this gives at least $m$ orbits as each $\rho^{(j)}$ must lie in a distinct orbit.

To prove that there are at most $m$ orbits of the order 2 elements, we let $\rho^{(j)}$ be as defined above and let $\rho'^{(j)} = (\rho'_1, \rho'_2, \ldots, \rho'_m)$, where $\rho'_1, \ldots, \rho'_{j-1}$ are identically 0, $\rho'_j$ is not identically 0 and $\rho_{j+1}, \ldots, \rho_m$ are free to choose (in the sense that $\rho_i = 2^{e_i-1} \cdot (c_1^i, c_2^i, \ldots, c_{e_i}^i)$, the most general order 2 element in $\mathbb{Z}_{2^{e_i}}$). We will show that $\rho'$ is in the orbit of $\rho^{(j)}$.

$$\psi(A)(\rho^{(j)}) = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ \pi_j(B_{jj}\rho_j) \\ \pi_{j+1}(2^{e_{j+1}-e_j}B_{j+1j}\rho_j) \\ \vdots \\ \pi_m(2^{e_m-e_j}B_{mj}\rho_j) \end{bmatrix}.$$

We need to show that $\pi_j(B_{jj}\rho_j)$ can attain any $\rho'_j$ that is not identically 0. Indeed basic linear algebra shows that this is possible as the only restriction placed on $B_{jj}$ is being invertible (modulo 2).

Furthermore, we have to show that $\pi_k(2^{e_k-e_j}B_{kj}\rho_j)$ can attain any $\rho'_k$. For this simply write $\rho'_k = (c_1 2^{e_k-1} c_2 2^{e_k-1}, \ldots, c_{n_k} 2^{e_k-1})$. Then fix $B_{kj}$ to be a matrix with $(c_1, c_2, \ldots, c_{n_k})$ as first column. Then $\pi_k(2^{e_k-e_j}B_{kj}\rho_j) = \pi_k(2^{e_k-1}B_{kj}(1,0,\ldots,0)) = \rho'_k$. Thus we can indeed find such a matrix $B_{kj}$.

This shows that the orbit of $\rho^{(j)}$ contains all order 2 elements $\rho'^{(j)} = (\rho'_1, \rho'_2, \ldots, \rho'_m)$, where $\rho'_1, \ldots, \rho'_{j-1}$ are identically 0, $\rho'_j$ is not identically 0 and $\rho_{j+1}, \ldots, \rho_m$ are free. Furthermore, we note that any order 2 element is of the form $\rho^{(j)}$ for some $1 \leq j \leq m$. This shows that there are at most $m$ orbits.

Thus we conclude there are exactly $m$ orbits and thus $m$ distinct $\rho$-structures. □

**Corollary 4.3.2.** Let $G$ be any finite abelian group of even order and write the group as $G = H_2 \times H_{p_1} \times \cdots \times H_{p_k}$, where $H_2 \cong (\mathbb{Z}_{2^{e_1}})^{n_1} \times \cdots \times (\mathbb{Z}_{2^{e_m}})^{n_m}$. Then $G$ has exactly $m$ distinct $\rho$-structures, where for each $1 \leq j \leq m$, $\rho^{(j)}$ as defined in the proof of Theorem 4.3 is a representative of the $m$ different $\rho$-structures.

*Proof.* This follows immediately from Theorem 4.3 together with Lemma 4.1.7. □

# 5 Superelliptic curves with simple CM-Jacobians

## 5.1 An introduction to curves

In this section, we will apply the theory of CM-fields and CM-types to algebraic curves. Curves, typically denoted by $C$, are equations of the form $f(x, y) = 0$ were $f(x, y)$ is a polynomial in 2 variables. The equation is usually seen over a field of characteristic 0, and in this section are taken over $\mathbb{Q}$. This means that the points $(x, y)$ that satisfy the curve $C$ will be of the form $(x, y) \in \mathbb{Q}^{\mathrm{al}} \times \mathbb{Q}^{\mathrm{al}}$.

We will specifically apply the theory to superelliptic curves, which are equations of the form $y^m = f(x)$, where $f(x)$ is a polynomial of degree $d$. Note that superelliptic curves are generalizations of elliptic curves. That is, taking $m = 2$ and $d = 3$ yields elliptic curves. Furthermore $d \geq 5$ and $m = 2$ are known as hyperelliptic curves. The theory in this section is based on [Sil09] and to a lesser extent on [MZW96].

**Definition 5.1.1.** Let $K$ be a field of characteristic 0 (throughout the paper taken to be $\mathbb{Q}$) and $K^{\mathrm{al}}$ its algebraic closure. A *curve* is an equation of the form

$$f(x, y) = 0,$$

for some polynomial $f(x, y) \in K[x, y]$. The curve $C$ is defined to be all points that satisfy the equation; i.e. we have $C = \{(x, y) \in K^{\mathrm{al}} \times K^{\mathrm{al}} \mid f(x, y) = 0\}$.

We define certain special types of curves: *Superelliptic curves* are equations which take the form $y^m = f(x)$ where $f(x) \in K[x]$ has degree $d$ and $m \in \mathbb{Z}_{\geq 2}$. In the case of superelliptic curves, we assume $\gcd(m, d) = 1$ and that $f$ does not contain repeated roots.

If $m = 2$ and $d = 3$, $C$ is called an *elliptic curve.* If $m = 2$ and $d \geq 5$, then $C$ is *hyperelliptic.*

**Definition 5.1.2.** A curve is said to be *non-singular* if no points on the curve $C$ simultaneously satisfy $\frac{\partial f}{\partial x} = 0$ and $\frac{\partial f}{\partial y} = 0$.

**Remark 5.1.3.** To make a group out of an elliptic curve, we add a point at infinity, denoted by $P_\infty$. For general curves, a similar procedure is taken. However, similar to elliptic curves, we require the point at infinity to be non-singular. A given curve $C$ is not be required to be non-singular at infinity, but we need $C$ to be non-singular everywhere including the point at infinity under a suitable change of coordinates.

For superelliptic curves $C\colon y^m = f(x)$, it turns out that such a change of coordinates always exists if $f(x)$ has no repeated roots and $m, d$ are coprime; this is the reason why Definition 5.1.1 contains these assumptions. For more details, please refer to [Tow93].

Throughout this section, any curve is assumed to be a smooth projective curve; i.e. all points, including the point at infinity are assumed to be non-singular (or at least there is a suitable change of coordinates attaining this requirement, as we usually do not write curves in the coordinates where they are non-singular at infinity, as these can be inconvenient to write down).

### 5.1.1 Divisors

**Remark 5.1.4.** Elliptic curves are usually studied by means of their group structure. Recall that points on elliptic curves form a group when applying to chord-tangent group law. For this, one requires that the line through distinct points $P$ and $Q$ on the elliptic curve must intersect the curve in a unique third point. This condition is not met for general curves and thus one cannot define a group law on the points of arbitrary curves in this manner. There is a way to use curves to define a group; this is done through the Jacobian. In Section 5.1.4, we define the Jacobian, but before doing so, we need to define notions such as the divisor of a rational function, which is the aim of this section. A more thorough investigation can be found in [Mil86b].

**Definition 5.1.5.** Let $C$ be a curve over $K$ given by $f(x, y) = 0$ and define the polynomial quotient rings

$$K[C] = K[x, y]/(f(x, y));$$
$$K^{\mathrm{al}}[C] = K^{\mathrm{al}}[x, y]/(f(x, y)).$$

The *function fields* of $C$, denoted by $K(C)$ and $K^{\mathrm{al}}(C)$ are the fields of fractions of $K[C]$ and $K^{\mathrm{al}}[C]$ respectively.

**Definition 5.1.6.** A *divisor* $D$ is a formal sum of points on a curve $C$ of the form

$$D = \sum_{P \in C} m_P P, \text{ where } m_P \in \mathbb{Z},$$

such that only a finite number of $m_P$'s are non-zero.

The *degree* of $D$ is the sum of the $m_P$'s, i.e. $\deg(D) = \Sigma_{P \in C} m_P$. The *order* of a divisor at a point $P$ is the value $m_P$, denoted by $\mathrm{ord}_P(D) = m_P$.

The set of all divisors, denoted by $\mathbf{D}$, is an abelian group, under the operation

$$\sum_{P \in C} m_P P + \sum_{P \in C} n_P P = \sum_{P \in C} (m_P + n_P) P.$$

Let $\mathbf{D}^0$ denote the set of divisors of degree 0. Then $\mathbf{D}^0$ is a subgroup of $\mathbf{D}$.

Next, the notion of order of a rational function at a point is introduced.

**Definition 5.1.7.** Let $P \in C$ be a point on curve $C$, then $K^{\mathrm{al}}[C]_P$ denotes the ring of all rational functions that are defined at $p$; i.e. have a denominator that is non-zero at $P$.

**Lemma 5.1.8.** *The ring $K^{\mathrm{al}}[C]_P$ is a discrete valuation ring for each $P \in C$ and thus has a unique maximal ideal, $\mathbf{m}_P$, generated by some $t \in C$ called a uniformizer.*

*Proof.* This is shown in Section II.1 of [Sil09]. □

**Definition 5.1.9.** Let $f \in K^{\mathrm{al}}[C]$ and $P \in C$. Then the *order* of $f$ at $P$, denoted by $\mathrm{ord}_P(f)$ is given by $d$ such that $f = ut^d$, where $u$ is a unit and $t$ is a uniformizer as given in Lemma 5.1.8; i.e. $d$ is the largest integer such that $f \in \mathbf{m}_P^d$.

We extend this definition to rational functions in $K^{\text{al}}(C)$ in the following manner.

**Definition 5.1.10.** Let $U \in K^{\text{al}}(C)$ be a rational function and let us write $R = G/H$ for $G, H \in K^{\text{al}}[C]$. The *order* of $R$ at $P$, given as $\text{ord}_P(R)$, is defined as $\text{ord}_P(G) - \text{ord}_P(H)$.

Rational functions $R = G/H$ with polynomials $G, H \in K^{\text{al}}[C]$ are such that the polynomials are of finite degree and thus have a finite number of zeros. In particular that means that the order of $R$ at $P$ is nonzero at only finitely many places. This leads to the following definition.

**Definition 5.1.11.** Let $R \in K^{\text{al}}(C)$, with $R \neq 0$ be a rational function. Then the *divisor* of $R$ is

$$\text{div}(R) = \sum_{P \in C} \text{ord}_P(R)P.$$

Since $\text{ord}_P(R)$ is nonzero in only finitely many places, we have that $\text{div}(R) \in \mathbf{D}$.

Divisors of the form $\text{div}(R) = \sum_{P \in C} \text{ord}_P(R)P$ are called *principal.* The set of all principal divisors is denoted by $\mathbf{P}$.

**Theorem 5.1.12.** *Let $R \in K^{\text{al}}(C)$ be an arbitrary rational function. Then $\text{div}(R) \in \mathbf{D}^0$, i.e. we have that $\sum_{P \in C} \text{ord}_P(R) = 0$. Furthermore, $\mathbf{P}$ is a subgroup of $\mathbf{D}^0$.*

*Proof.* This is Section II.3 of [Sil09]. □

Using Definition 5.1.10, the order at the point $P_\infty$ is also defined. However, in practice it is easier to compute the order at infinity using the above theorem as the only pole of polynomials is at infinity and thus the order of this pole must ‘cancel out’ the sum of the orders of all the zeros. This is illustrated in the following example.

**Example 5.1.13.** Let $C\colon y^2 = x^{17} + x$, and $P = (x_0, y_0)$ where $x_0 \in K^{\text{al}}$ and $y_0$ is given by $y_0 = +\sqrt{x_0^{17} + x_0}$. Note that the unique maximal ideal of $K^{\text{al}}[C]_P$ must be given by all rational functions that are 0 at $P$ (In a DVR $R$, the unique maximal ideal is given by $R/R^\times$, thus $\mathbf{m}_P$ is the rational functions that are 0 at $P$). We get $\mathbf{m}_P = (x - x_0, y - y_0) = (x - x_0)$, where the last equality follows from the fact that $\mathbf{m}_P$ is generated by a single element.

Given that $\mathbf{m}_P$ has only one factor of $x - x_0$, we conlcude that $\text{ord}_P(x - x_0) = 1$. Similarly, it can be shown that $P_1 \coloneqq (x_0, -y_0)$ also gives $\text{ord}_{P_1}(x - x_0) = 1$. Lastly, if $P_2 = (x', y')$ where $x' \neq x_0$, then we have $\text{ord}_{P_2}(x - x_0) = 0$. Thus $\text{div}(x - x_0) = (P) + (P_1) - rP_\infty$. We know $x - x_0$ is a rational function and thus $\deg(x - x_0) = 0$, which gives us $r = 2$.

This concludes the discussion of the divisor of rational functions over function fields of curves.

### 5.1.2 The regular differentials

Regular differentials form an important component of the study of curves. In this section, we introduce regular differentials and show examples on how to compute them for various curves.

**Definition 5.1.14.** Let $C$ be a curve. The space of *differentials* on $C$ is denoted by $\Omega_C$ and is a vector space over $K^{\text{al}}$ generated by symbols of the form $dg$ for $g \in K^{\text{al}}(C)$. Elements in the space $\Omega_C$ are subject to the standard differentiation rules

1. $d(f+g) = df + dg$;
2. $d(fg) = fdg + gdf$;
3. $d(\alpha) = 0 \, \forall \alpha \in K^{\text{al}}$.

**Example 5.1.15.** Let $C$ be given by $y = x$, so that $dy = dx$. Using these 2 relations, we can eliminate $y$ and $dy$ from all elements $fdg \in \Omega_C$. Thus we get that all elements in $\Omega_C$ are of the form $f(x)dx$ for some $f \in K(x)$.

Next, we define the order of differentials. The standard definition of order/divisors of differentials uses uniformizers much in the same way as the definition for order of the rational functions. However, the order of the differentials can be related to divisors of rational functions as is shown in [Sil09, Proposition 3.4]. We take this proposition as definition.

**Theorem 5.1.16.** Let $f, g \in K^{\text{al}}(C)$ and $P \in C$ such that $g(P) = 0$. Then we have

$$\operatorname{ord}_P(fdg) = \operatorname{ord}_P(f) + \operatorname{ord}_P(g) - 1.$$

□

**Definition 5.1.17.** Let $\omega \in \Omega_C$ be a differential of a curve $C$. Then the *divisor of* $\omega$ is

$$\sum_{P \in C} \operatorname{ord}_P(\omega)(P) \in \operatorname{div}(C).$$

The differential $\omega$ is called *regular* if $\operatorname{ord}_P(\omega) \geq 0$ for all $P \in C$.

**Example 5.1.18.** Let $C$ be given by $y^2 = x^{17} + x$. Write $x_i$ with $1 \leq i \leq 17$ for the 17 roots of $x^{17} + x$, so that $(x_i, 0) \in C$. We have that $d(x - x_i) = dx - dx_i = dx$ so that we may use Theorem 5.1.16 to compute $\operatorname{ord}_{(x_i,0)}(d(x - x_i)) = \operatorname{ord}_{(x_i,0)}(x - x_i) - 1 = 2 - 1 = 1$. For points of the form $P = (p_1, p_2)$ with $p_2 \neq 0$, we have that $\operatorname{ord}_{(p_1,p_2)}(d(x - p_1)) = \operatorname{ord}_{(p_1,p_2)}(x - p_1) - 1 = 1 - 1 = 0$. Lastly, at the point $P_\infty$, we must take $1/x$ as uniformizer. Thus we find $\operatorname{ord}_{P_\infty}(dx) = \operatorname{ord}_{P_\infty}(-1/x^2 d(1/x)) = \operatorname{ord}_{P_\infty}(-1/x^2) + \operatorname{ord}_{P_\infty}(1/x) - 1 = -3$.

Similarly, we compute $\operatorname{ord}_{(x_i,0)}(y) = 1$ and $\operatorname{ord}_{(p_1,p_2)}(y) = 0$. Lastly, since $y$ is a rational function, we use Theorem 5.1.12 to find that the point $P_\infty$ is such that $\operatorname{ord}_{P_\infty}(y) = -17$.

Thus we get that $\operatorname{div}(dx) = (x_1, 0) + (x_2, 0) + \cdots + (x_{17}, 0) - 3(P_\infty)$ and $\operatorname{div}(y) = (x_1, 0) + (x_2, 0) + \cdots + (x_{17}, 0) - 17(P_\infty)$. In particular this means that $\operatorname{div}(dx/y) = 14(P_\infty)$ and thus $\omega_0 := dx/y$ is a regular differential.

**Theorem 5.1.19.** The space of regular differentials, $\{\omega \in \Omega_C \mid \omega \text{ is regular}\}$, is a vector space over $K^{\text{al}}$. The dimension of this vector space is called the *genus* of $C$, denoted by $g$.

*Proof.* This can be found in [Sil09, Corollary 5.5 in Section II.5]. □

### 5.1.3 The Riemann-Hurwitz formula

In practice, one cannot compute the genus of a curve $C$ using the definition, as it is impractical to prove that a given set of differentials indeed spans the space of differentials. The Riemann-Hurwitz formula gives the genus $g$ in terms of the rammification points of a curve $C$. This section covers the necessary theory to describe the theorem. Note that the theory of this section is aimed at superelliptic curves.

**Remark 5.1.20.** Let $C$ be a superelliptic curve given by $y^m = f(x)$. Denote with $\pi$ a projection of $C$ onto $\mathbb{P}^1$, that is, $\pi(x, y) = x \in \mathbb{P}^1$. This yields a covering of $\mathbb{P}^1$ of degree $m$ in the sense that almost every point $f(x) \in \mathbb{P}^1$ has $m$ distinct preimages. The finite points where there are less than $m$ associated values are exactly the points where $f(x) = 0$ as here $y^m = f(x) = 0 \implies y = 0$ and thus there is only one value of $y$ associated to this value of $x$. We call these points ramification points or branching points. The point at infinity can also be a ramification point, the idea behind the ramification at infinity is explained below.

Write $C$ as $y^m = \Pi_{i=1}^{d}(x - \alpha_i)$, where we assume $d < m$. Projecting to $\mathbb{P}^1$ gives $\Pi(x - \alpha_i)$. To see what happens at infinity, we make the change of coordinates given by $x \to 1/X$. This gives $\Pi\frac{(1/\alpha_i - 1/X)}{(X\alpha_i)}$.

Next assume that $d = cm - k$ where $1 \leq k < m$. We make a change of variables $Y = yx^c$ to obtain $\Pi(\alpha_i)Y^m = X^k\Pi(1/\alpha_i - X)$. Since we set $x = 1/X$ and $d < m$, the point at infinity is given by $X = 0$. At $X = 0$, the curve is ramified exactly when $k \neq 0$ as this gives us that at $X = 0$, the only value for $Y$ is given by $Y = 0$. If $k = 0$, we find that at $X = 0$, there are $m$ choices for $Y$, and thus the curve is unramified at $X = 0$. Hence we find that superelliptic curves of the form $y^m = f(x)$ are ramified at infinity exactly when $d$ is not a multiple of $m$. If $m > d$, a similar reasoning can be given to find that $C$ is ramified at $P_\infty$ when $m$ is not a multiple of $d$. Given that our definition of superelliptic curves requires that $\gcd(d, m) = 1$, all superelliptic curves are ramified at infinity.

We will take this intuition behind our definition of ramification. Please note that this is not the standard definition of ramification points, but rather a corollary of theory that can be found in [Koo91].

**Definition 5.1.21.** Let superelliptic curve $C$ be given by $y^m = f(x)$ where $f(x)$ has degree $d$. Then the finite *ramification points* of $C$ are given by the $d$ (distinct) points $(x_i, 0)$ where $f(x_i) = 0$. The point $P_\infty$ is always a ramification point.

The ramification index is an integer associated to each ramification point. The standard definition is rather cumbersome, but the assumption that $f(x)$ can have no repeated roots and $\gcd(d, m) = 1$, fixes the possible values for the ramification index, as is discussed in [Koo91]. We take this result as definition.

**Definition 5.1.22.** Let $C$ be a superelliptic curve given by $y^m = f(x)$. Then each ramification point $P$ has ramification index $m$, denoted by $e_P$.

The ramification points and ramification index is used in the Riemann-Hurwitz theorem.

**Theorem 5.1.23.** Let $y^m = f(x)$ be a superelliptic curve. The genus $g$ of $C$ is given by

$$2g - 2 = -2m + \sum_{P \in C} (e_p - 1).$$

*Proof.* See [Sil09, Theorem 5.9]. □

**Example 5.1.24.** From Definition 5.1.21, it follows that the ramification points of the curve $y^2 = x^{17} + x$ are given by the points $(0, x_i)$ where $1 \leq i \leq 17$ and $x_i \in K^{\text{al}}$ is such that $x_i^{17} + x_i = 0$. The point $P_\infty$ is also a ramification point and each ramification point has ramification index $m = 2$ (see Definition 5.1.22). Thus by the Riemann-Hurwitz formula, we find that $2g - 2 = -2 \cdot 2 + 18 \implies 2g = 16 \implies g = 8$.

**Example 5.1.25.** The ramification points of $y^5 = x^3 + 1$ are given by the points $(0, x_i)$ where $1 \leq i \leq 3$ and $x_i$ is such that $x_i^3 + 1 = 0$. $P_\infty$ is also a ramification point and all points have ramification index $m = 5$. The genus is then given by $2g - 2 = -2 \cdot 5 + 16 \implies g = 4$.

**Remark 5.1.26.** In Theorem 5.1.19, it was discussed that the regular differentials form a vector space over $K^{\text{al}}$ of dimension $g$. Thus we can use the above result to note that the curve $C \colon y^2 = x^{17} + x$ has 8 linearly independent regular differentials and that the curve $C \colon y^5 = x^3 + 1$ has 4.

**Example 5.1.27.** This theorem allows us to find a basis for the regular differentials of superelliptic curves. We return to the curve $C$ given by $y^2 = x^{17} + x$. In Example 5.1.18, we found that $\omega_0 = dx/y$ is a regular differential. We claim that $\omega_i = x^i dx/y$ for $0 \leq i \leq g - 1$ forms a basis for $\mathcal{L}(K_C)$. For this, note that $\operatorname{div}(x) = 2(0,0) - 2(P_\infty)$. Hence we find

$$\operatorname{div}(\omega_i) = \operatorname{div}(x^i dx/y) = i(0, q_1) + i(0, q_2) + (14 - 2i)(P_\infty),$$

which is holomorphic exactly when $i \geq 0$ and $14 - 2i \geq 0 \implies 0 \leq i \leq g - 1 = 7$. Thus we found 8 regular differentials. To show that these 8 differentials are linearly independent over $K^{\text{al}}$, we note that

$$\sum c_i \omega_i = 0 \iff \sum c_i x^i dx/y = 0 \iff dx/y \sum c_i x^i = 0 \iff \sum c_i x^i = 0.$$

Thus each $c_i$ must be 0 and we find that the 8 differentials are linearly independent and thus must form a basis for $\mathcal{L}(K_C)$.

**Example 5.1.28.** Let $C$ be given by the curve $y^5 = x^3 + 1$, and let $x_i$ be the three zeros of $f(x) = x^3 + 1$. Denote by $Q_i$ the points $(x, y) = (x_i, 0) \in C$. Then denote by $P_i$ the five points given by $(0, \zeta_5^i) \in C$.

First, we compute $\operatorname{div}(dx)$. For this, note that

$$\operatorname{ord}_{P_i}(dx) = \operatorname{ord}_{P_i}(d(x - x_i)) = \operatorname{ord}_{P_i}(x - x_i) - 1 = 5 - 1 = 4.$$

Similar computations show that for other finite points $P$, we have $\operatorname{ord}_P(dx) = 0$ and for the point at infinity, we get $\operatorname{ord}_{P_\infty}(dx) = -6$. Thus we find

$$\operatorname{div}(dx) = 4(Q_1) + 4(Q_2) + 4(Q_3) - 6(P_\infty).$$

Further computations show that

$$\begin{aligned}\operatorname{div}(x) &= (P_1)+(P_2)+(P_3)+(P_4)+(P_5)-5(P_\infty);\\ \operatorname{div}(y) &= (Q_1)+(Q_2)+(Q_3)-3(P_\infty).\end{aligned}$$

In Example 5.1.24, we computed that the genus of $C$ was 4. Thus there must be 4 linearly independent (over $\mathbb{Q}^{\mathrm{al}}$) regular differentials. We can compute these by making educated guesses of combinations of the above divisors to find that the regular differentials are

- $\operatorname{div}(dx/y^2) = \operatorname{div}(dx) - 2\operatorname{div}(y) = 2(Q_1)+2(Q_2)+2(Q_3)$;
- $\operatorname{div}(dx/y^3) = \operatorname{div}(dx) - 3\operatorname{div}(y) = (Q_1)+(Q_2)+(Q_3)+3(P_\infty)$;
- $\operatorname{div}(dx/y^4) = \operatorname{div}(dx) - 4\operatorname{div}(y) = 6(P_\infty)$;
- $\operatorname{div}(xdx/y^4) = \operatorname{div}(x)+\operatorname{div}(dx)+4\operatorname{div}(y) = (P_1)+(P_2)+(P_3)+(P_4)+(P_5)+(P_\infty)$.

Similar computations to Example 5.1.27 shows that these regular differentials are linearly independent and thus must form a basis for $\mathcal{L}(K_C)$.

### 5.1.4 The Jacobian of curves

In this section, we introduce the Jacobian of a superelliptic curve. Recall that the Jacobian is a generalization of the group structure for elliptic curves and thus is a group. However, the Jacobian contains more structure, making it an abelian variety. The definition of an abelian variety is out of the scope of this thesis, but an introduction can be found in [Mil86a].

**Definition 5.1.29.** The Jacobian of a curve $C$, denoted by $J(C)$, is an abelian variety such that $J(C) = \mathbf{D}^0/\mathbf{P}$.

**Theorem 5.1.30.** [Mil86b, Proposition 2.1] The dimension of $J(C)$ is equal to the genus of $C$.

**Definition 5.1.31.** A Jacobian $J(C)$ is called *simple* if it is not isogenous to the product of abelian varieties over an algebraically closed field.

**Remark 5.1.32.** The Jacobian of a curve $C$ is always an abelian variety. Hence if $J(C)$ is simple, then there does not exists a lower genus curve $C'$ such that $J(C')$ embeds in $J(C)$. However, keep in mind that not every abelian variety can be written as the Jacobian of a curve.

**Definition 5.1.33.** An *endomorphism* of $J(C)$ is a morphism of varieties respecting the group structure of $J(C)$. The set of all endomorphisms of $J(C)$ is denoted by $\operatorname{End}(J(C))$ and forms a ring.

**Remark 5.1.34.** In particular, the endomorphism $n\colon J(C) \to J(C)$ which is defined as $n([\sum a_i P_i]) = [\sum n \cdot a_i(P_i)]$ is an endomorphism for all $n \in \mathbb{Z}$ and thus $\mathbb{Z} \subseteq \operatorname{End}(J(C))$.

**Definition 5.1.35.** The *endomorphism algebra* of $J(C)$ is given by $\operatorname{End}(J(C)) \otimes \mathbb{Q}$ and is denoted by $\operatorname{End}_0(J(C))$.

We can relate an automorphism of $C$ to a cyclotomic field present in the endomorphism algebra of $J(C)$ as follows.

**Theorem 5.1.36.** Let $C$ be a curve with an automorphism $\zeta\colon C \to C$ of order $r$. Then we have that $\mathbb{Q}(\zeta_r) \subset \mathrm{End}_0(J(C))$.

*Proof.* We first relate the automorphisms of $C$ to the endomorphisms of $J(C)$. Define $G = \mathrm{Aut}(C)$ to be the automorphism group of the curve $C$. Then an automorphism $h \in G$ induces an endomorphism $[h] \in \mathrm{End}(J(C))$ by

$$h\colon J(C) \to J(C),\ h([\sum a_i P_i]) \to [\sum a_i h(P_i)].$$

Furthermore, if $h_1, h_2 \in G$ then $m[h_1] + n[h_2]$ is an endomorphism on $J(C)$ defined by

$$\left[\sum a_i P_i\right] \mapsto \left[m \sum a_i h_1(P_i) + n \sum a_i h_2(P_i)\right],$$

and similarly $[h_1] \cdot [h_2]$ is an endomorphism on $J(C)$ defined by

$$\left[\sum a_i P_i\right] \mapsto \left[m \sum a_i h_1 \cdot h_2(P_i)\right].$$

This gives an embedding from the group ring $\mathbb{Z}[G] \coloneqq \{\sum m_i[h_i] \mid h_i \in G\}$ into $\mathrm{End}(J(C))$; i.e. we have $\mathbb{Z}[G] \hookrightarrow \mathrm{End}(J(C))$. Tensoring both $\mathbb{Z}$-modules with $\mathbb{Q}$ yields the following embedding $\mathbb{Q}[G] \hookrightarrow \mathrm{End}_0(J(C))$. Note that we assumed that there exists an automorphism $\zeta\colon C \to C$ with order $r$. It can be easily checked that $\mathbb{Q}[\zeta] = \mathbb{Q}(\zeta_r)$ and thus

$$\mathbb{Q}(\zeta_r) \cong \mathbb{Q}[\zeta] \subset \mathbb{Q}[G] \hookrightarrow \mathrm{End}_0(J(C)),$$

shows that the cyclotomic field $\mathbb{Q}(\zeta_r)$ embeds into $\mathrm{End}_0(J(C))$. □

The last notion we introduce is the notion of a CM-Jacobian.

**Theorem 5.1.37.** [Lan83, Theorem 3.1] Let $J(C)$ be the Jacobian of some curve $C$ with genus $g$. If a field $K$ of degree $2g$ embeds in $\mathrm{End}_0(J(C))$, then $K$ is a CM-field.

**Definition 5.1.38.** Let $C$ be a curve of genus $g$. Let $K$ be a CM-field of degree $2g$ over $\mathbb{Q}$. We say that $J(C)$ has CM by $K$ if there is an embedding $K \hookrightarrow \mathrm{End}_0(J(C))$. In this case, we call $J(C)$ a *CM-Jacobian*.

**Remark 5.1.39.** It follows from Theorems 5.1.36 and 5.1.37, that a curve $C$ with genus $g$ containing an automorphism of degree $n$ such that $|(\mathbb{Z}_n)^\times| = 2g$, then $J(C)$ has CM by $\mathbb{Q}(\zeta_n)$.

## 5.2 Finding simple CM-Jacobians

In this section, we find Jacobians with simple CM-jacobians. In [TTV91], a method is given to show that $J(C)$ is simple.

**Remark 5.2.1.** As explained in Chapter 1 of [Lan83] if the Jacobian $J(C)$ of a genus $g$ curve $C$ has CM by a CM-field $K$ then the *complex representation* of $\mathrm{End}_0(J(C))$ is a $\mathbb{C}$ vector space of dimension $g$ and is isomorphic to the direct sum of a CM-type $\Phi$ of $K$. We say that $J(C)$ is of type $(K, \Phi)$.

Using the method in [TTV91] we read the CM-type of the CM Jacobians of some explicit curves via the action of the automorphisms of $C$ on the regular differentials of $C$.

Lastly, the main reason why we are interested in CM-Jacobians is that Jacobians of this form have an easy to check equivalent criteria of being simple.

**Theorem 5.2.2.** [Lan83, Theorem 3.5] A Jacobian $J(C)$ is of type $(K, \Phi)$ is simple if and only if $\Phi$ is primitive.

**Remark 5.2.3.** Putting everything together, we show that the Jacobian of a curve $C$ is simple by means of the following steps.

1. Find (if possible) an automorphism $\zeta$ of $C$ of order $n$ such that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 2g$;
2. Compute the regular differentials $\{\omega_1, \dots, \omega_g\}$ of $C$;
3. Compute $\Phi \coloneqq \{\phi_i \colon \zeta_{2g} \mapsto \zeta({\omega_i}^i)\}$;
4. Check that $\Phi$ gives a CM-type of the field $\mathbb{Q}(\zeta_{2g})$;
5. Check if $\Phi$ is primitive.

### 5.2.1 The first example

We will illustrate this method by applying it to the curve $C$ given by $y^5 = x^3 + 1$. Note that $\zeta \colon C \to C$ given by $\zeta(x, y) = (\zeta_3 x, \zeta_5 y)$ is an automorphism of $C$. Furthermore, note that $\langle\zeta\rangle \cong \mathbb{Z}_{15}$ so that $\mathbb{Q}(\zeta_{15})$ embeds in the endomorphism algebra of $J(C)$. In particular, note that $[\mathbb{Q}(\zeta_{15}) : \mathbb{Q}] = 8$ and recall that $g = 4$ is the genus of $C$ (see Example 5.1.24) so that we find a field of sufficiently large and thus $J(C)$ is a CM-Jacobian. We will show that $J(C)$ is of primitive CM-type $(\mathbb{Q}(\zeta_{15}), \Phi)$ and hence use Theorem 5.2.2 to conclude that $J(C)$ is simple.

The regular differentials of $C$ were computed in Example 5.1.28, and are given by

$$\omega_1 = dx/y^2,\ \omega_2 = dx/y^3,\ \omega_3 = dx/y^4 \text{ and } \omega_4 = xdx/y^4.$$

The action of the automorphism $\zeta$ on the regular differentials is then given by

- $\zeta(\omega_1) = d(\zeta_3 x)/(\zeta_5 y)^2 = \zeta_3 \zeta_5^3 \omega_1 = \zeta_{15}^{14}\omega_1$;
- $\zeta(\omega_2) = d(\zeta_3 x)/(\zeta_5 y)^3 = \zeta_3 \zeta_5^2 \omega_2 = \zeta_{15}^{11}\omega_2$;
- $\zeta(\omega_3) = d(\zeta_3 x)/(\zeta_5 y)^4 = \zeta_3 \zeta_5 \omega_3 = \zeta_{15}^{8}\omega_3$;
- $\zeta(\omega_4) = \zeta_3 x d(\zeta_3 x)/(\zeta_5 y)^4 = \zeta_3^2 \zeta_5 \omega_4 = \zeta_{15}^{13}\omega_4$.

As described in Remark 5.2.3, we define the embeddings $\phi_i(\zeta_{15}) = \zeta(\omega_i)$. This results in the following four homomorphisms, which give embeddings of $\mathbb{Q}(\zeta_{15})$. Furthermore, since $\mathbb{Q}(\zeta_{15})$ is Galois over $\mathbb{Q}$, we may associate these embeddings with elements of the Galois group, as follows from Theorem 1.2.9.

- $\phi_1(\zeta_{15}) = \zeta_{15}^{14} \implies 14 \in (\mathbb{Z}_{15})^\times$;
- $\phi_2(\zeta_{15}) = \zeta_{15}^{11} \implies 11 \in (\mathbb{Z}_{15})^\times$;
- $\phi_3(\zeta_{15}) = \zeta_{15}^{8} \implies 8 \in (\mathbb{Z}_{15})^\times$;
- $\phi_4(\zeta_{15}) = \zeta_{15}^{13} \implies 13 \in (\mathbb{Z}_{15})^\times$.

This gives the set of embeddings $\Phi := \{14, 11, 8, 13\}$. We check that $\Phi$ indeed gives a CM-type. Note that $|(\mathbb{Z}_{15})^\times| = 8$, hence $\Phi$ is a CM-type when we show that $\Phi$ contains no conjugate embeddings. Complex conjugation is given by the element $14 = -1 \in (\mathbb{Z}_{15})^\times$ and none of the embeddings in $\{14, 11, 8, 13\}$ differ by multiplication by $-1$, thus $\Phi$ is a CM-type.

Lastly, we claim that $\Phi$ is primitive. For this, note that $(\mathbb{Z}_{15})^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_4$ via the isomorphism $f\colon (\mathbb{Z}_{15})^\times \to \mathbb{Z}_2 \times \mathbb{Z}_4$ such that $f(14) = (1, 0)$ and $f(2) = (0, 1)$. By applying the automorphism to $\Phi$, we find that $\Phi$ is given by the CM-type $\{(1, 0), (1, 2), (0, 3), (1, 1)\}$ on the CM-field $\mathbb{Z}_2 \times \mathbb{Z}_4$ with $\rho = (1, 0)$. By defining the embeddings as in Section 3.1.5, gives that $\Phi = \{\phi_1, \bar{\phi}_2, \bar{\phi}_3, \bar{\phi}_4\}$, which is primitive as claimed in Section 3.1.7.

This shows that Jacobian of the curve $y^5 = x^3 + 1$ is simple. □

### 5.2.2 The second example

Next, we look at the curve $C$ given by $y^2 = x^{17} + x$. As will be shown, the Jacobian of $C$ decomposes as it allows for an embedding of the Jacobian of a genus 4 curve. Moreover, we will show that the Jacobian of the curve of genus 4 is simple. This example is more involved than Example 5.2.1, and thus we first have to introduce some additional results about the Jacobian. In particular, we find specific divisors that represent the equivalence classes of Jacobians of hyperelliptic curves. We also introduce a corollary of Torelli's theorem.

**Definition 5.2.4.** Let $C$ be a hyperelliptic curve. A divisor $D$ is called a *reduced divisor* if the following holds

- $D$ is of the form $D = \sum m_i(P_i) - \left(\sum m_i\right)(P_\infty)$ where each $m_i \geq 0$;
- Each point $P_i \in \text{Supp}(D)$ is finite and $P_i \in \text{Supp}(D) \implies \tilde{P}_i \notin \text{Supp}(D)$ unless we have $P_i = \tilde{P}_i$ in which case $m_i = 1$;
- $\sum m_i \leq g$ where $g$ is the genus of a curve $C$.

Here, $\text{Supp}(D)$ denotes the points $P_i \in C$ where $\text{ord}_{P_i}(D) \neq 0$ and if $P = (x_0, y_0)$, then we denote $\tilde{P}_i = (x_0, -y_0)$.

**Theorem 5.2.5.** [MZW96, Theorem 47] Let $C$ be a hyperelliptic curve, then each equivalence class in $J(C)$ is represented by a unique reduced divisor. □

For this second example, we also need to relate the automorphisms of a curve $C$ to the automorphisms of the Jacobian $J(C)$. This can be done through a corollary of Torelli's theorem.

**Theorem 5.2.6.** Let $C$ be a superelliptic curve, then

$$\mathrm{Aut}(C) \cong \begin{cases} \mathrm{Aut}(J(C)) & \text{if } C \text{ is hyperelliptic;} \\ \mathrm{Aut}(J(C)) \times \mathbb{Z}_2 & \text{if } C \text{ is not hyperelliptic.} \end{cases}$$

*Proof.* This is a direct consequence of Torelli's theorem, of which the proof is beyond the scope of the thesis but can be found in [LS01, Theorem 3]. □

**Definition 5.2.7.** Let $C$ be a curve and $\tau$ an automorphism of $C$. Then $C/\langle\tau\rangle$ is the set of points on the curve $C$ that are fixed by the automorphisms in the group $\langle\tau\rangle$.

**Example 5.2.8.** Take $y^2 = x^{17} + x$ and let $\tau\colon C \to C$ be given by $\tau(x, y) = (1/x, y/x^9)$ be an automorphism of $C$. Since $\tau^2 = id$, we have that $C/\langle\tau\rangle$ is precisely given by the points of $C$ fixed under $\tau$. We claim that $C' = C/\langle\tau\rangle$ is also a hyperelliptic curve.

**Lemma 5.2.9.** Let $C$ be given by $y^2 = x^{17} + x$ and $\tau(x, y) = (1/x, y/x^9)$ be an automorphism of $C$. Then $C' = C/\langle\tau\rangle$ is a hyperelliptic curve.

*Proof.* To show this, note that $\tau(y/x^4) = y/x^5$ and $\tau(y/x^5) = y/x^4$. Therefore we find that $\tau$ fixes $y/x^5 + y/x^4 = y(1 + 1/x)/x^4 := \eta$. Next, note that

$$\begin{aligned} \eta^2 &= y^2(1 + 2/x + 1/x^2)/x^8 \\ &= (x^{17} + x)(1 + 2/x + 1/x^2)/x^8 \\ &= x^9 + x^{-9} + 2x^8 + 2x^{-8} + x^7 + x^{-7}. \end{aligned}$$

Furthermore, note that $\tau$ fixes $x + 1/x$ so that we can substitute $s = x + 1/x$ to get

$$\eta^2 = (s + 2)(s^8 - 8s^6 + 20s^4 - 16s^2 + 2).$$

This can be readily verified to be a hyperelliptic curve $C'$ with genus 4 and is fixed by $\tau$.

Furthermore, we have that $J(C')$ embeds into $J(C)$. This follows directly from the fact that every reduced divisor of $J(C')$ also satisfies the criteria of being a reduced divisor in $J(C)$. In particular, this means that the Jacobian $J(C)$ is not simple as it allows for an embedding of the Jacobian of a smaller genus curve $C'$. □

We find that the Jacobian of $y^2 = x^{17}+x$ is not simple, however, we claim that the Jacobian of $C'$ defined by $\eta^2 = (s + 2)(s^8 - 8s^6 + 20s^4 - 16s^2 + 2)$ is simple.

**Theorem 5.2.10.** Let $C'$ be the curve given by $\eta^2 = (s + 2)(s^8 - 8s^6 + 20s^4 - 16s^2 + 2)$, then $J(C')$ is simple.

*Proof.* For this, observe that $\zeta\colon C \to C$ given by $\zeta(x,y) = (\zeta_{32}^2 x, \zeta_{32} y)$ is an automorphism of $C$. We claim that $\zeta - \zeta^{-1}$ is an automorphism of $C'$. To conclude this, we follow the same argument as in [TTV91] and show that $\zeta - \zeta^{-1}$ preserves the regular differentials that are fixed under $\tau$. For this, we first show that $\tau$ and $\zeta - \zeta^{-1}$ commute.

$$\begin{aligned}(\tau \circ \zeta)(x,y) &= \tau(\zeta_{32}^2 x, \zeta_{32} y)\\ &= (1/(\zeta_{32}^2 x), \zeta_{32} y/(\zeta_{32}^{18} x^9))\\ &= (\zeta_{32}^{30}/x, \zeta_{32}^{15} y/x^9)\\ &= \zeta^{15} \circ \tau.\end{aligned}$$

We conclude, $\tau \circ \zeta = \zeta^{15} \circ \tau$. Therefore we find

$$\tau \circ (\zeta - \zeta^{-1}) = \tau \circ \zeta - \tau \circ \zeta^{-1} = \zeta^{15} \circ \tau - \zeta^{-15}\tau = (-\zeta^{-1} + \zeta)\tau,$$

and thus $\zeta - \zeta^{-1}$ commutes with $\tau$.

Next, we show that $\zeta - \zeta^{-1}$ preserves the regular differentials fixed by $\tau$. For this, let $\omega_j$ be a differential fixed by $\tau$. Since $\tau$ and $\zeta - \zeta^{-1}$ commute, we get

$$\tau \circ (\zeta - \zeta^{-1})(\omega_j) = (\zeta - \zeta^{-1}) \circ \tau(\omega_j) = (\zeta - \zeta^{-1})(\omega_j),$$

and thus $\tau$ fixes $(\zeta - \zeta^{-1})(\omega_j)$.

From Example 5.1.28, it follows that a basis for the regular differentials for $C$ was given by $\omega_i = x^i dx/y$ for $0 \leq i \leq 7$. We have that

$$\tau\left(x^t \frac{dx}{y}\right) = \frac{x^{9-t} d(1/x)}{y} = -x^{7-t}\frac{dx}{y}.$$

This shows that the invariant regular differentials under $\tau$ are given by

$$\omega_1 = (1 - x^7)\frac{dx}{y},\ \omega_2 = (x - x^6)\frac{dx}{y},\ \omega_3 = (x^2 - x^5)\frac{dx}{y},\ \omega_4 = (x^3 - x^4)\frac{dx}{y}.$$

Thus we have found that these regular differentials are the regular differentials of $C'$. Similar to Example 5.2.1, we compute the action of $\zeta - \zeta^{-1}$ on these regular differentials and check that we obtain a CM-type. If this CM-type is primitive, then $J(C')$ is simple.

We compute the action of $\zeta - \zeta^{-1}$ on the differential fixed by $\tau$.

$$\zeta\left(x^t \frac{dx}{y}\right) = \frac{\zeta_{32}^{2t} x^t d(\zeta_{32}^2 x)}{\zeta_{32} y} = \zeta_{32}^{2t+1} x^t \frac{dx}{y}.$$

Using this, we find

- $(\zeta - \zeta^{-1})\omega_0 = (\zeta_{32} - \zeta_{32}^{-1})\omega_0;$

- $(\zeta - \zeta^{-1})\omega_1 = (\zeta_{32}^3 - \zeta_{32}^{-3})\omega_1$;
- $(\zeta - \zeta^{-1})\omega_2 = (\zeta_{32}^5 - \zeta_{32}^{-5})\omega_2$;
- $(\zeta - \zeta^{-1})\omega_3 = (\zeta_{32}^7 - \zeta_{32}^{-7})\omega_3$.

We again define $\phi_i(\zeta_{32} - \zeta_{32}^{-1}) = \zeta(\omega_i) = \zeta_{32}^{2i-1} - \zeta_{32}^{-2i+1}$. We can compute that the minimal polynomial of $\zeta_{32} - \zeta_{32}^{-1}$ is given by $p(x) = x^8 - 8x^6 + 20x^4 - 16x^2 + 2$ and that the other roots of this polynomial are given by $\zeta_{32}^{2i-1} - \zeta_{32}^{-2i+1}$ with complex conjugates $-\zeta_{32}^{2i-1} + \zeta_{32}^{-2i+1}$. Thus, the functions $\phi_i$ define embeddings of the CM-field $\mathbb{Q}(\zeta_{32} - \zeta_{32}^{-1})$. We concretely write out the embeddings as follows

- $\phi_1(\zeta_{32} - \zeta_{32}^{-1}) = \zeta_{32} - \zeta_{32}^{-1} \implies \bar{\phi}_1(\zeta_{32} - \zeta_{32}^{-1}) = -\zeta_{32} + \zeta_{32}^{-1}$;
- $\phi_2(\zeta_{32} - \zeta_{32}^{-1}) = \zeta_{32}^3 - \zeta_{32}^{-3} \implies \bar{\phi}_2(\zeta_{32} - \zeta_{32}^{-1}) = -\zeta_{32}^3 + \zeta_{32}^{-3}$;
- $\phi_3(\zeta_{32} - \zeta_{32}^{-1}) = \zeta_{32}^5 - \zeta_{32}^{-5} \implies \bar{\phi}_3(\zeta_{32} - \zeta_{32}^{-1}) = -\zeta_{32}^5 + \zeta_{32}^{-5}$;
- $\phi_4(\zeta_{32} - \zeta_{32}^{-1}) = \zeta_{32}^7 - \zeta_{32}^{-7} \implies \bar{\phi}_4(\zeta_{32} - \zeta_{32}^{-1}) = -\zeta_{32}^7 + \zeta_{32}^{-7}$.

This shows that the action of $\zeta$ on the regular differentials yields the set of embeddings $\{\phi_1, \phi_2, \phi_3, \phi_4\}$, which is indeed a CM-type. Next we compute the Galois group of the field $\mathbb{Q}(\zeta_{32} - \zeta_{32}^{-1})$. For this, note that $\zeta_{32} - \zeta_{32}^{-1} = \zeta_{32} + \zeta_{32}^{15}$ is fixed by $\zeta_{32}$ and $\zeta_{32}^{15}$. This shows that $\mathrm{Gal}(\mathbb{Q}(\zeta_{32} - \zeta_{32}^{-1})/\mathbb{Q}) \cong (\mathbb{Z}_{32})^\times / \langle 15 \rangle \cong \mathbb{Z}_8$. From Section 3.2.4, we know that all CM-types of a field with Galois group $\mathbb{Z}_8$ are primitive, in particular $\{\phi_1, \phi_2, \phi_3, \phi_4\}$ is primitive and thus $J(C')$ is simple. □

## 5.3 Generalizing this example

### 5.3.1 The curve $y^m = x^d + 1$

In this last section, we will generalize the proof of the fact that the Jacobian of the superelliptic curve $y^5 = x^3 + 1$ is simple. The generalized curve we look at is given by $C_{d,m}$ defined as $y^m = x^d + 1$, where $m > d$ are primes and $m \equiv -1 \pmod{d}$. Note that $y^5 = x^3 + 1$ is indeed of this form as $5 \equiv -1 \pmod{3}$. We follow the same steps to prove that the Jacobian of superelliptic curves of the form $C_{d,m}$ is simple. For this, we first need to find an automorphism of the curve.

**Lemma 5.3.1.** Let $C_{d,m}$ be given as above, then $\zeta\colon C \to C$ given by $(x, y) \to (\zeta_d x, \zeta_m y)$ is an automorphism of $C$. □

**Lemma 5.3.2.** The curve $C_{d,m}$ has genus $g = (d-1)(m-1)/2$.

*Proof.* Note that projecting the $x$-coordinate of $C_{d,m}$ to $\mathbb{P}^1$ yields an $m$-folded covering with ramification points $Q_i = (x_i, 0)$ (with $1 \leq i \leq d$) where $x_i$ is such that $x_i^d + 1 = 0$. Furthermore, the projection is ramified at infinity as follows from Definition 5.1.21. At all $d+1$ ramification points, the ramification index is $m$, which follows from Definition 5.1.22. Thus by the Riemann-Hurwitz formula, $C_{d,m}$ has genus

$$2g - 2 = -2m + (d+1)(m-1) \implies g = (d-1)(m-1)/2.$$

### 5.3.2 The regular differentials

In this section, we compute the regular differentials of $C_{d,m}$. The final result is given in Theorem 5.3.12. In the following paragraphs, we follow the thought process which lead to finding the regular differentials, for which we first introduce the following notation.

**Definition 5.3.3.** Let $C_{d,m}$ be given by $y^m = x^d + 1$. Then $Q_i$ and $P_i$ are the points

$$Q_i = (x_i, 0) \text{ where } x_i^d + 1 = 0 \text{ for } 1 \leq i \leq d, \quad P_j = (0, \zeta_m^j) \text{ for } 1 \leq j \leq m.$$

**Lemma 5.3.4.** The divisors of $dx, x$ and $y$ on the curve $C_{d,m}$ are given by

$$\begin{aligned} \operatorname{div}(dx) &= -(m+1)(P_\infty) + (m-1)(D_Q); \\ \operatorname{div}(x) &= -m(P_\infty) + (D_P); \\ \operatorname{div}(y) &= -d(P_\infty) + (D_Q). \end{aligned}$$

Here $Q$ and $P$ denote the sum of points

$$(D_Q) = \Sigma_{i=1}^d (Q_i) \quad \text{and} \quad (D_P) = \Sigma_{i=1}^m (P_i).$$

*Proof.* This follows from identical computations as seen in Example 5.1.28. □

**Remark 5.3.5.** We claim that a basis for the space of regular differentials can be made by combinations of the functions $dx, x$ and $y$. An educated guess for the form of these regular differentials, based on the regular differentials computed for $y^5 = x^3 + 1$, is given by $\omega_{s,t} = x^s dx/y^t$. We will show that the correct restrictions on the pairs $(s, t)$ indeed give that the $\omega_{s,t}$ form a basis for the space of regular differentials.

**Definition 5.3.6.** Recall that $m \equiv -1 \pmod{d}$, so that we can write $m = dk - 1$. Throughout this section, the integer $k$ is defined by $k = (m+1)/d$. In particular, note that $k$ is the inverse of $d$ modulo $m$.

**Lemma 5.3.7.** Let $k$ be as above. Then $dx/y^k$ is a regular differential of $C_{d,m}$.

*Proof.* We have

$$\begin{aligned} \operatorname{div}(dx/y^k) &= \operatorname{div}(dx) - k\operatorname{div}(y) \\ &= -(m+1)(P_\infty) + (m-1)(D_Q) + dk(P_\infty) - k(D_Q) \\ &= -(m+1)(P_\infty) + (m-1)(D_Q) + (m+1)(P_\infty) - k(D_Q) \\ &= (m-k-1)(D_Q). \end{aligned}$$

Since $k < m$, we have that $(m-k-1) \geq 0$ and thus $dx/y^k$ is regular. □

It turns out that we can slightly generalize the above computation to find that $dx/y^t$ is also a regular differential for the correct choice of $t$.

**Lemma 5.3.8.** Let $t \in \mathbb{Z}$ with $k \leq t \leq m-1$. Then $dx/y^t$ is a regular differential of $C_{d,m}$.

*Proof.* We compute that

$$\begin{aligned} \operatorname{div}(dx/y^t) &= \operatorname{div}(dx) - t\operatorname{div}(y) \\ &= (-m-1+dt)(P_\infty) + (m-1-t)(D_Q). \end{aligned}$$

Since we assumed $k \leq t$, we have that $m+1 = dk \leq dt$. Thus $-m-1+dt \geq 0$. Furthermore, we assumed that $t \leq m-1$ so that $m-1-t \geq 0$. Hence $dx/y^t$ is a regular differential of $C_{d,m}$. □

**Remark 5.3.9.** From Lemma 5.3.2, we have that the genus of $C_{d,m}$ is $g = (d-1)(m-1)/2$. We know that there are $(d-1)(m-1)/2$ linearly independent regular differentials. Note that there are 'only' $m-k$ integer values $t$ that satisfy $k \leq t \leq m-1$. Thus, we are still short by a considerable amount of regular differentials.

We will show that $\omega_{s,t} = x^{s-1}dx/y^t$ are regular differentials, as long as $1 \leq s \leq d-1$ and $sk \leq t \leq m-1$. For this, first note that these bounds are well-defined as

$$1 \leq s \leq d-1 \implies sk \leq (d-1)k \leq m-k+1 \leq m-1.$$

therefore, the values $1 \leq s \leq d-1$ allow us to bound $t$ as $sk \leq t \leq m-1$.

**Lemma 5.3.10.** Write $\omega_{s,t} = x^{s-1}dx/y^t$ where $1 \leq s \leq d-1$ and $sk \leq t \leq m-1$. Then $\omega_{s,t}$ is a regular differential of $C_{d,m}$.

*Proof.* Again, we compute $\operatorname{div}(\omega_{s,t})$ to find

$$\begin{aligned} \operatorname{div}(\omega_{s,t}) &= \operatorname{div}(x^{s-1}dx/y^t) \\ &= (s-1)\operatorname{div}(x) + \operatorname{div}(dx) - t\operatorname{div}(y) \\ &= (-m-1-(s-1)m+dt)(P_\infty) + (m-1-t)(D_Q) + (s-1)(D_P) \\ &= (dt-sm-1)(P_\infty) + (m-1-t)(D_Q) + (s-1)(D_P). \end{aligned}$$

Note that $dt-sm-1 = dt-s(dk-1)-1 = dt-skd+s-1 \geq dt-dt+s-1 \geq 0$. Furthermore, we assumed that $m-1-t \geq 0$. This concludes that $\omega_{s,t}$ is a regular differential. □

We claim that the differentials $\omega_{s,t} = x^{s-1}dx/y^t$ under the restrictions $1 \leq s \leq d-1$ and $sk \leq t \leq m-1$ form a basis for the space of regular differentials.

**Lemma 5.3.11.** The set $\{x^{s-1}dx/y^t \mid 1 \leq s \leq d-1 \text{ and } sk \leq t \leq m-1\}$ forms a basis for the space of regular differentials of $C_{d,m}$.

*Proof.* It suffices to show that there are $g = (d-1)(m-1)/2$ regular differentials in the set $\{\omega_{s,t}\}$ and that this set of regular differentials is linearly independent over $K^{\text{al}}$. First we show the linear independence. Take an arbitrary linear combination of the regular differentials

$$\sum c_i\omega_{s,t} = 0 \iff dx/y^m \sum c_i x^s y^{m-t} = 0 \iff \sum c_i x^s y^{m-t} = 0 \iff c_i = 0.$$

Here, the last step follows from the fact $\sum c_i x^s y^{m-t}$ is a polynomial in $x, y$ where the powers of $x, y$ are such that $1 \leq s \leq d-1$ and $1 \leq m-t \leq m-1$. Therefore, we may never replace $y^t$ with (a power of) $x^d+1$ or $x^s$ with (a power of) $y^m-1$. Since each term in the sum has a unique power for $x$ and $y$, we have that all $c_i$ must be 0.

We count the number of differentials by iterating over $s$. There are $m-k$ differentials when $s=1$, since the corresponding restriction on $t$ is given by $k \leq t \leq m-1$. Similarly, if we fix $s=i$, then $t$ must satisfy $ik \leq t \leq m-1$ and thus there are $m-ik$ possibilities for $\omega_{s,t}$ whenever $s=i$. Given that $s$ takes values $1 \leq s \leq d-1$, we have that the total number of differentials equals

$$\begin{aligned}\Sigma_{i=1}^{d-1}(m-ik) &= (d-1)m - k(d(d-1)/2)\\ &= (d-1)m - (m+1)(d-1)/2)\\ &= (2dm - 2m - dm - d + m + 1)/2\\ &= (d-1)(m-1)/2.\end{aligned}$$

This shows that we have found the $g = (d-1)(m-1)/2$ differentials that form a basis for the space of regular differentials. □

This finishes the proof of the final result on the regular differentials, which is stated below for the sake of completeness.

**Theorem 5.3.12.** Let $m > d$ be primes such that $m \equiv -1 \pmod{d}$. Define $k = (m+1)/d$ and let $s \in \mathbb{Z}$ such that $1 \leq s \leq d-1$. Define $t \in \mathbb{Z}$ such that $sk \leq t \leq m-1$. Then the differentials of the form $x^{s-1}dx/y^t$ form a basis for the space of regular differentials of the curve $y^m = x^d + 1$. □

**Example 5.3.13.** We use the above theory to find the regular differentials of the superelliptic curve $y^5 = x^3 + 1$. Note that $5 = 2 \cdot 3 - 1$ so that we have $k = 2, m = 5, d = 3$. Thus we have that $1 \leq s \leq d-1 \implies 1 \leq s \leq 2$. Furthermore, $sk \leq t \leq m-1 \implies 2s \leq t \leq 4$. Thus $s = 1 \implies 2 \leq t \leq 4$ and $s = 2 \implies t = 4$. This gives rise to the following pairs for $(s,t) : \{(1,2),(1,3),(1,4),(2,4)\}$. Recall that $\omega_{s,t} = x^{s-1}dx/y^t$ so that the differentials are given by $dx/y^2, dx/y^3, dx/y^4$ and $xdx/y^4$, which agrees with Example 5.1.28.

### 5.3.3 The CM-type

From the method in [TTV91], we have that automorphism $\zeta$ applied to the regular differentials $\omega_{s,t}$ yields a CM-type of the CM-field $K = \mathbb{Q}(\zeta_{dm})$ which has degree $2g$ over $\mathbb{Q}$. In this section, we will show that the action of automorphism $\zeta$ on the differentials $\omega_{s,t}$ gives a primitive CM-type of the field $K$. First note that $K$ is Galois over $\mathbb{Q}$ with Galois group $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}_{dm})^\times$. Thus the embeddings of $K$ are given by the elements in the Galois group (Theorem 1.2.9), which will be used throughout this section.

**Lemma 5.3.14.** The action of $\zeta$ on the regular differentials $\omega_{s,t}$ yields the set of embeddings

$$\Phi := \{ms - dt \mid 1 \leq s \leq d-1, ks \leq t \leq m-1\} \subset (\mathbb{Z}_{dm})^\times.$$

*Proof.* We compute $\zeta(\omega_{s,t})$ below:

$$\zeta(\omega_{s,t}) = \zeta(x^{s-1}dx/y^t) = \zeta_d^s\zeta_m^{-t}x^{s-1}dx/y^t = \zeta_d^s\zeta_m^{-t}\omega_{s,t}$$

Next, note that $\zeta_d^s\zeta_m^{-t} = \zeta_{dm}^{sm-dt}$, which in turn corresponds to the element $sm-dt \in (\mathbb{Z}_{dm})^\times$. Thus, the set of embeddings is given by

$$\{ms - dt \mid 1 \leq s \leq d-1, ks \leq t \leq m-1\}.$$

□

**Lemma 5.3.15.** The set $\Phi = \{ms - dt \mid 1 \leq s \leq d-1, ks \leq t \leq m-1\}$ forms a CM-type of the CM-field $K = \mathbb{Q}(\zeta_{dm})$.

*Proof.* To show this, we first show that $\Phi \subset \mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}_{dm})^\times$. Note that

$$ms - dt \in (\mathbb{Z}_{dm})^\times \iff \gcd(ms-dt, dm) = 1 \iff$$
$$\begin{cases} \gcd(ms-dt, d) = 1 \\ \gcd(ms-dt, m) = 1 \end{cases} \iff \begin{cases} s \text{ is not a multiple of } d; \\ t \text{ is not a multiple of } m. \end{cases}$$

Given that $1 \leq s \leq d-1$ and $k \leq t \leq m-1$, the last statement is trivially true, which shows that $ms - dt \in (\zeta_{dm})^\times$.

Next, recall that there are $(m-1)(d-1)/2$ differentials $\omega_{s,t}$. We also claim that there are $(m-1)(d-1)/2$ distinct values for $ms - dt$.

$$ms - dt = ms' - dt' \iff m(s-s') = d(t-t').$$

Since $d, m$ are primes, we must have that $s-s'$ is a multiple of $d$. Given that $1 \leq s, s' \leq d-1$, this is only possible if $s - s' = 0$ which shows $s = s'$. A similar argument shows $t = t'$. Thus, distinct regular differentials correspond to distinct embeddings and this shows that the set of $(d-1)(m-1)/2$ regular differentials correspond to $(d-1)(m-1)/2$ distinct embeddings in $(\mathbb{Z}_{dm})^\times$. Furthermore, we have $|(\mathbb{Z}_{dm})^\times| = (d-1)(m-1)$. Thus $\Phi$ contains exactly half of the embeddings of $K$ and hence is a CM-type upon showing that these embeddings are non-conjugate.

Two embeddings in $\Phi$ being conjugate is equivalent to $ms - dt \equiv -(ms' - dt') \pmod{dm}$. Aiming for contradiction, we write $sm - dt = cdm - s'm + dt'$ for some $c \in \mathbb{Z}$. This gives us that $(s+s')m + cdm = d(t+t')$. Since the right hand side of the equation is a multiple of $d$, the left hand side must be so as well. Since $d, m$ are primes, we have that $s + s'$ is a multiple of $d$. Given that $1 \leq s, s' \leq d-1$, we thus have that $s + s' = d$. A similar argument shows that $t + t' = m$. Given that $sk \leq t \leq m-1$ and $s'k \leq t' \leq m-1$, we have that $m + 1 = dk = (s+s')k \leq t + t'$. However, this contradicts that $t + t' = m$. This shows that the embeddings in $\Phi$ is non-conjugate. In particular, $\Phi$ is a CM-type of the field $\mathbb{Q}(\zeta_{dm})$. □

### 5.3.4 CM-type $\Phi$ is primitive

In this section, we show that the CM-type $\Phi = \{ms - dt \mid 1 \leq s \leq d-1, ks \leq t \leq m-1\}$ is a primitive CM-type of the field $K = \mathbb{Q}(\zeta_{dm})$.

**Remark 5.3.16.** To show this efficiently, we first notice that $K = \mathbb{Q}(\zeta_{dm})$ is Galois over $\mathbb{Q}$ so that the embeddings are given by the automorphisms in the Galois group $(\mathbb{Z}_{dm})^\times$. Then we note that choosing $(s,t) = (1,k)$ corresponds to $ms - dt = m - dk = -1 \in \Phi$. We can look at the conjugated CM-type $\bar{\Phi} = \Phi \circ (-1)$ so that $1 \in \bar{\Phi}$. Any automorphism fixing $\bar{\Phi}$ must send 1 to some other embedding in $\bar{\Phi}$, thus this automorphism must be given by one of the embeddings in $\bar{\Phi}$. This will be used to show that $\bar{\Phi}$ is primitive. Since $\bar{\Phi}$ and $\Phi$ are equivalent CM-types, this will also show that $\Phi$ is primitive.

**Lemma 5.3.17.** The CM-type $\bar{\Phi} = \{dt - ms \mid 1 \leq s \leq d-1, ks \leq t \leq m-1\}$ is primitive.

*Proof.* Aiming for contradiction, we assume $\bar{\Phi}$ is not primitive, then $\bar{\Phi} \circ \sigma = \bar{\Phi}$ for some non-trivial automorphism $\sigma$. By the explanation in Remark 5.3.16, we must have $\sigma \in \bar{\Phi}$. Thus we write $\sigma = (dt - sm)$. If $\sigma$ fixes $\bar{\Phi}$, we must have for all embeddings $(dt' - s'm) \in \bar{\Phi}$ that $(dt - sm)(dt' - s'm) \in \bar{\Phi}$. i.e. we have $(dt - sm)(dt' - s'm) \equiv (dt^* - s^*m) \pmod{dm}$ for some $dt^* - s^*m \in \bar{\Phi}$. We first simplify this equation.

$$\begin{aligned} & (dt - sm)(dt' - s'm) \equiv dt^* - s^*m \pmod{dm} \\ \iff & d^2tt' + ss'm^2 \equiv dt^* - s^*m \pmod{dm} \\ \iff & ss' \equiv s^* \pmod{d} \text{ and } dtt' \equiv t^* \pmod{m} \end{aligned}$$

Recall that the last set of equations must hold for all embeddings in $\bar{\Phi}$, i.e. if $\bar{\Phi}$ were not primitive, there must be a pair $(s,t)$ such that for all $(s',t')$ we have that there is a pair $(s^*,t^*)$ that solves

$$\begin{cases} ss' \equiv s^* \pmod{d} \\ dtt' \equiv t^* \pmod{m}. \end{cases}$$

Moreover, recall that the following restrictions hold

$$1 \leq s, s', s^* \leq d-1 \text{ and } sk \leq t \leq m-1,\ s'k \leq t' \leq m-1,\ s^*k \leq t^* \leq m-1.$$

We will show that this is not possible.

For this, we split the proof in two cases. We first assume $s \neq 1$. Since $d$ is a prime, we know that $s \in (\mathbb{Z}_d)^\times$ and thus can choose $s'$ such $s' \equiv -s^{-1} \pmod{d}$. In particular, note that $s \neq 1 \implies s' \neq d-1$. This choice of $s'$ gives that $s^* \equiv -1 \pmod{d}$. Since we have $1 \leq s^* \leq d-1$, we find that $s^* = d-1$.

From the bound $s^*k \leq t^* \leq m-1$, we find that $(d-1)k = m-k+1 \leq t^* \leq m-1$. We thus write $t^* = m-k+j$ where $1 \leq j \leq k-1$. Next, note that $s'k \leq (d-2)k = m-2k+1$ implies that $t' = m-k$ is a valid choice for $t'$ (i.e. this choice does not violate the bound $s'k \leq t \leq m-1$). Plugging these values into $dtt' \equiv t^*$ (mod $m$) yields

$$\begin{aligned} dtt' \equiv t^* &\iff dt(m-k) \equiv m-k+j \pmod{m} \\ &\iff -dkt \equiv -k+j \pmod{m} \\ &\iff -(m+1)t \equiv -k+j \pmod{m} \\ &\iff t \equiv k-j \pmod{m} \end{aligned}$$

This is a contradiction since $0 \leq k-j < k$ and $k \leq t \leq m-1$. Thus we conclude that if $\Phi$ is primitive, then the automorphism fixing $\bar{\Phi}$ must be given by $dt - sm$ where $s = 1$.

Next, we check the case when $s = 1$. Here we first set $s' = 1$, so that $ss' \equiv s^*$ (mod $d$) implies that $s^* \equiv 1$ (mod $d$). Given that $1 \leq s^* \leq d-1$, we conclude $s^* = 1$. In particular, this means that $k \leq t, t', t^* \leq m-1$ since $s = s' = s^* = 1$. Given that $m$ is a prime and that $d, t$ are not multiples of $m$, we see that $dt \in (\mathbb{Z}_m)^\times$. Let $a \in (\mathbb{Z}_m)^\times$ be such that $(dt)a \equiv 1$ (mod $m$). If $k \leq a \leq m-1$, then set $t' = a$ so that $dtt' \equiv 1$ (mod $m$). Again, since $k \leq t^* \leq m-1$, this is a contradiction.

Next assume $a = 2, 3, \ldots, k-1$. In this case, we cannot set $t' = a$ as we must have that $k \leq t' \leq m-1$. However, now set $t' = a \cdot \lceil k/a \rceil$ (note: $k \leq a \cdot \lceil k/a \rceil < 2k \leq m-1$ so that this value for $t'$ is allowed). Thus, we have $dtt' = dta \cdot \lceil k/a \rceil \equiv \lceil k/a \rceil$ (mod $m$). Hence, in particular, $dtt' \equiv t^* \implies t^* \equiv \lceil k/a \rceil$ (mod $m$). Since $a \geq 2$, we have that $\lceil k/a \rceil < k$ which is a contradiction as $k \leq t^* \leq m-1$.

Lastly, if $a = 1$, then $dta \equiv 1$ (mod $m$) $\iff$ $dt \equiv 1$ (mod $m$) $\iff$ $t = k$. This shows that the only automorphism that can fix $\bar{\Phi}$ is given by $(s, t) = (1, k)$, which corresponds to $dt - ms = dk - m = 1$, which trivially fixes $\bar{\Phi}$. Thus we conclude that $\bar{\Phi}$ is primitive. In particular, $\Phi$ is primitive and $J(C_{d,m})$ is simple. □

**Corollary 5.3.18.** The Jacobian of $y^m = x^d + 1$ where $m > d$ are primes such that $m \equiv -1$ (mod $d$) is simple.

**Remark 5.3.19.** It is expected that the condition that $m \equiv -1$ (mod $d$) is not necessary. This condition was imposed to make the computations in the proof shorter and more tangible, but is not necessary from any fundamental point of view. As an example, consider the curve $C$ given by $y^7 = x^3 + 1$. Note that $7 \not\equiv -1$ (mod 3), but the curve $C$ has simple Jacobian, as is shown below.

Note that $\zeta(x, y) = (\zeta_3 x, \zeta_7 y)$ is an automorphism of $C$, and that the genus of $C$ is $g = 6$. It can be computed that a basis for the space of regular differentials is given by

$$\omega_1 = dx/y^3,\ \omega_2 = dx/y^4,\ \omega_3 = dx/y^5,\ \omega_4 = dx/y^6,\ \omega_5 = xdx/y^5,\ \omega_6 = x^2dx/y^6.$$

Note that we have that $\mathbb{Q}(\zeta_{21})$ is present in the endomorphism ring of $J(C)$. Furthermore, $\zeta(\omega_i)$ corresponds to a CM-type of $\mathbb{Q}(\zeta_{21})$. One can compute that this CM-type is given by $\Phi = \{19, 16, 13, 10, 20, 17\} \subset (\mathbb{Z}_{21})^\times$. One can check that this CM-type is only fixed by $1 \in (\mathbb{Z}_{21})^\times$ and is thus primitive. We conclude that $J(C)$ is primitive.

# Conclusion

We find that the Jacobian $J(C)$ is simple for the hyperelliptic curve $C$ that is given by $\eta^2 = (s+2)(s^8 - 8s^6 + 20s^4 - 16s^2 + 2)$ and for the family of superelliptic curves $C$ given by $y^m = x^d + 1$ where $m > d$ are primes and $m \equiv -1 \pmod{d}$. It is expected that further computations can show that the condition $m \equiv -1 \pmod{d}$ is not necessary; i.e. that the curve $y^m = x^d + 1$ has simple Jacobian for all primes $m > d$.

The simple Jacobian of the curve $\eta^2 = (s+2)(s^8 - 8s^6 + 20s^4 - 16s^2 + 2)$ has CM by the field $\mathbb{Q}(\zeta_{32} - \zeta_{32}^{-1})$, which has Galois group $\mathrm{Gal}(\zeta_{32} - \zeta_{32}^{-1}/\mathbb{Q}) \cong \mathbb{Z}_8$. The Jacobian of the curve $y^5 = x^3 + 1$ had CM via the field $\mathbb{Q}(\zeta_{15})$, for which $\mathrm{Gal}(\mathbb{Q}(\zeta_{15})/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_4$. A natural question that arises is: Can a simple Jacobian have CM by a Galois CM-field $K$ where $\mathrm{Gal}(K/\mathbb{Q})$ is any of the studied groups of order 8?

The answer is not always: In our classification, we found that CM-fields $K$ with Galois group $D_4$ have no primitive CM-types, and thus a Jacobian with CM by $K$ cannot be simple. However, as is seen in the classification, fields with Galois group $Q_8$ and $(\mathbb{Z}_2)^3$ both have primitive CM-types and thus could allow for simple Jacobians. It would be an interesting exercise to find simple Jacobians that have CM by a field with Galois group $Q_8$ or $(\mathbb{Z}_2)^3$, or to find a decomposable Jacobian that has CM by a field with Galois group $D_4$.

# 6 References

[HR06] Christopher J. Hillar and Darren Rhea. Automorphisms of finite abelian groups, 2006.

[Koo91] Ja Kyung Koo. On holomorphic differentials of some algebraic function field of one variable over c. *Bulletin of the Australian Mathematical Society*, 43(3):399–405, 1991.

[Lan83] S. Lang. *Complex Multiplication.* Grundleheren der math. Wiss,255. Springer-Verlag, 1983.

[LS01] Kristin Lauter and Jean-Pierre Serre. Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields, 2001.

[Mil] J.S. Milne. Complex multiplication.

[Mil86a] J. S. Milne. *Abelian Varieties*, pages 103–150. Springer New York, New York, NY, 1986.

[Mil86b] James S. Milne. Jacobian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 167–212. Springer, New York, 1986.

[Mos23] O. Mos. Dikke dijen, 2023.

[MZW96] A. Menezes, R. Zuccherato, and Y.H. Wu. *An Elementary Introduction to Hyperelliptic Curves.* CORR Report. Faculty of Mathematics, University of Waterloo, 1996.

[Sil09] Joseph H Silverman. *The Arithmetic of Elliptic Curves.* Graduate texts in mathematics. Springer, Dordrecht, 2009.

[Tow93] C.W. Towse. *Weierstrass Points on Cyclic Covers of the Projective Line.* Brown University, 1993.

[TTV91] Walter Tautz, Jaap Top, and Alain Verberkmoes. Explicit hyperelliptic curves with real multiplication and permutation polynomials. *Canadian Journal of Mathematics*, 43(5):1055–1064, 1991.