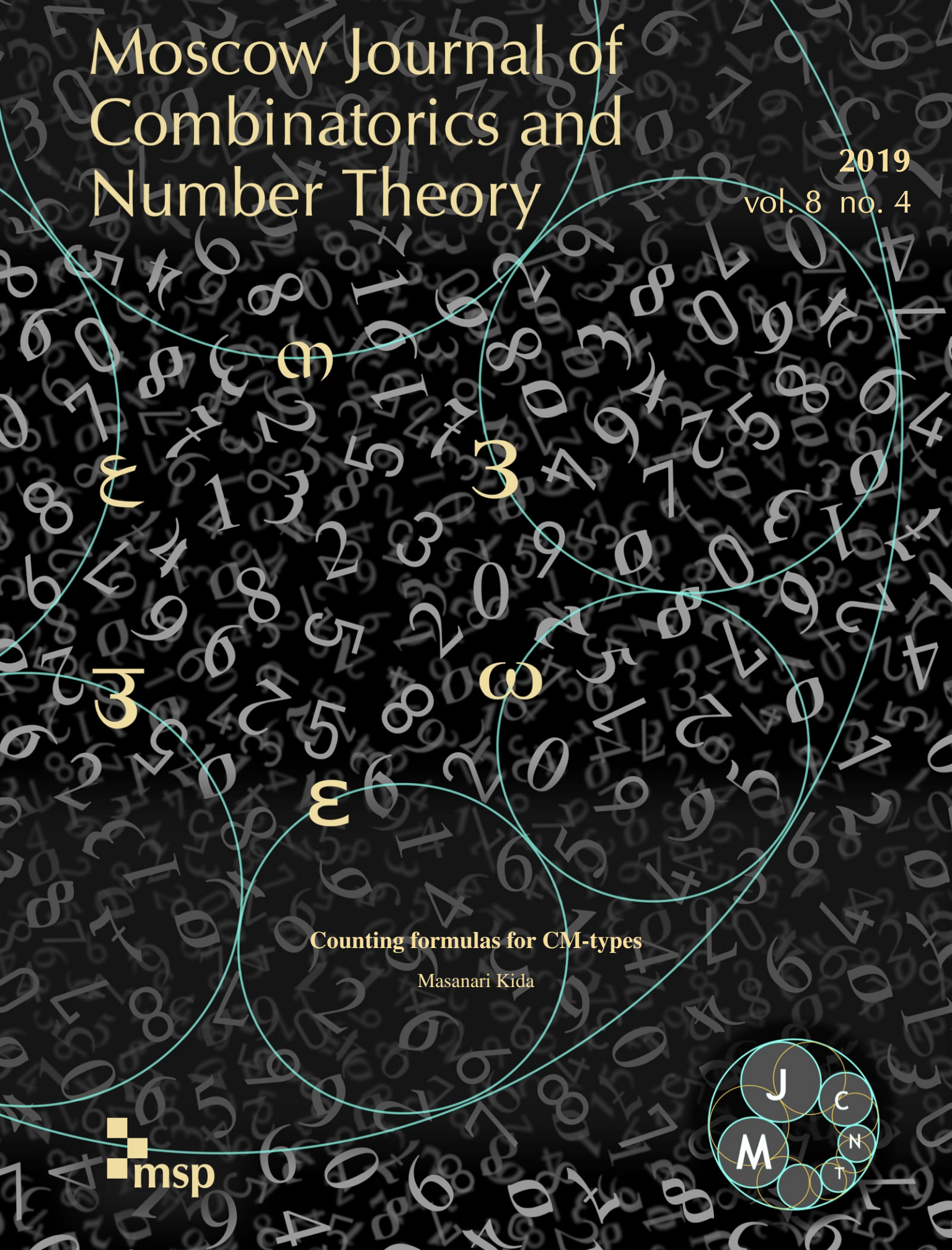
Moscow Journal of Combinatorics and Number Theory

2019
vol. 8 no. 4



Counting formulas for CM-types

Masanari Kida

msp

msp

Moscow Journal of Combinatorics and Number Theory
Vol. 8, No. 4, 2019
dx.doi.org/10.2140/moscow.2019.8.343

Counting formulas for CM-types

Masanari Kida

We prove various counting formulas for CM-types of CM-fields and use them to construct infinite families of degenerate CM-types.

1. Introduction

Let M be a CM-field, which is, by definition, a totally imaginary quadratic extension of a totally real field M^+. Let ρ be a complex conjugation acting on M. Then M^+ is the maximal field fixed by ρ. Let Γ_M be the set of the complex embeddings of M into $\mathbb{C}$. If we denote by $2d$ the degree $[M:\mathbb{Q}]$, then we have $|\Gamma_M| = 2d$. A half set S of Γ_M is called a *CM-type* of M if it satisfies $\Gamma_M = S \sqcup S\rho$ (a disjoint union). Let L be the Galois closure of M over $\mathbb{Q}$ and $G = \mathrm{Gal}(L/\mathbb{Q})$ and $H = \mathrm{Gal}(L/M)$. We have a one-to-one correspondence between Γ_M and the right cosets $H\backslash G$ and ρ lifts to a central involution of G, which we also denote by ρ. We denote the set of the CM-types with respect to (G, H, ρ) by $\mathrm{CM}(G, H, \rho)$.

We define a family $\mathscr{H}$ of subgroups of G by

$$\mathscr{H} = \{H \leq G \mid \rho \notin H\}. \tag{1-1}$$

The fixed field of each $H \in \mathscr{H}$ is a CM-subfield of L; thus, we call such an H a *CM subgroup* of G. The set $\mathscr{H}$ of CM subgroups is a poset by inclusion. If $H \in \mathscr{H}$, we denote by $\pi_H : G \to H\backslash G$ the canonical surjection. Let $\widetilde{S} = \pi_H^{-1}(S)$ be the pullback of S to L. We define two subgroups of G by

$$s(S) = \{g \in G \mid g\widetilde{S} = \widetilde{S}\}, \tag{1-2}$$

$$r(S) = \{g \in G \mid \widetilde{S}g = \widetilde{S}\}. \tag{1-3}$$

It is easy to see that $s(S)$ and $r(S)$ are members of $\mathscr{H}$. A CM-type $S \in \mathrm{CM}(G, H, \rho)$ is called *simple* if $s(S) = H$. If $H' = r(S)$, then

$$S' = \pi_{H'}(\{x^{-1} \mid x \in \widetilde{S}\})$$

is a CM-type of (G, H', ρ) called the *reflex* CM-type of S. We call the group $H' = r(S)$ the *reflex subgroup* of S.

Two CM-types S_1 and S_2 in $\mathrm{CM}(G, H, \rho)$ are *conjugate* if there exists $g \in G$ such that $S_1 = S_2 g$. A conjugacy class of simple CM-types determines an isogeny class of complex abelian varieties with complex multiplication by an order of M.

MSC2010: 11G15, 14K22.
Keywords: CM-types, degenerate CM-types, Hodge conjecture.

The aim of this paper is to prove various counting formulas of the number of CM-types. Our fundamental formula (Theorem 2.4) counts the cardinality of the set

$$\{S \in \mathrm{CM}(G, 1, \rho) \mid s(S) = H \text{ and } r(S) = K\}$$

for given $H, K \in \mathscr{H}$. Other counting formulas we shall prove are those of simple CM-types (Proposition 3.1) and CM-types of (G, H, ρ) with given reflex subgroup (Proposition 3.3) and conjugacy classes of CM-types (Theorem 4.1). These counting formulas enable us to construct degenerate CM-types (Section 5). In fact, we can construct infinite families of degenerate CM-types in Section 6 for nonabelian groups G. Infinite families of degenerate CM-types are previously known by [Greenberg 1980; Dodson 1984].

Throughout this paper, we will use the following purely group-theoretic setting. Let G be a finite group, and ρ a central involution of G fixed once for all. For $H \in \mathscr{H}$ (see (1-1)) we define a subposet $\mathscr{H}_{\geq}(H)$ of $\mathscr{H}$ by

$$\mathscr{H}_{\geq}(H) = \{K \in \mathscr{H} \mid K \geq H\}. \tag{1-4}$$

For $H_1, H_2 \in \mathscr{H}$ satisfying $H_1 \leq H_2$, the Möbius function μ on $\mathscr{H}$ is defined inductively by

$$\mu(H_1, H_1) = 1 \quad \text{and} \quad \mu(H_1, H_2) = -\sum_{H_1 \leq H < H_2} \mu(H_1, H_2). \tag{1-5}$$

2. Fundamental formula

In this section, we prove a counting formula of certain subsets of CM-types. The formula will play a fundamental role throughout the paper. The objects for counting are defined as follows. For $H, K \in \mathscr{H}$, we define

$$\mathscr{X}(H, K) = \{S \in \mathrm{CM}(G, 1, \rho) \mid s(S) = H \text{ and } r(S) = K\}, \tag{2-1}$$

$$\mathscr{X}_{\geq}(H, K) = \{S \in \mathrm{CM}(G, 1, \rho) \mid s(S) \geq H \text{ and } r(S) \geq K\}. \tag{2-2}$$

From these definitions, it readily follows that

$$\mathscr{X}_{\geq}(H, K) = \bigsqcup_{H_1 \in \mathscr{H}_{\geq}(H)} \bigsqcup_{K_1 \in \mathscr{H}_{\geq}(K)} \mathscr{X}(H_1, K_1). \tag{2-3}$$

The following function ε also plays an important role in the rest of this paper.

Definition 2.1. We define a function ε on $\mathscr{H} \times \mathscr{H}$ by

$$\varepsilon(H, K) = \begin{cases} 1 & \text{if } HK^g \not\ni \rho \text{ for all } g \in G, \\ 0 & \text{otherwise,} \end{cases}$$

where $H, K \in \mathscr{H}$ and K^g is the conjugate group gKg^{-1} of K.

We will need the following elementary properties of ε.

Lemma 2.2. *The function ε in Definition 2.1 satisfies the following properties*:

(i) $\varepsilon(H, 1) = \varepsilon(1, H) = 1$ *for all* $H \in \mathscr{H}$.

(ii) *If* $\varepsilon(H, K) = 0$, *then* $\varepsilon(H_1, K_1) = 0$ *for all* $H_1 \geq H$ *and all* $K_1 \geq K$.

(iii) $\varepsilon(H, K) = \varepsilon(K, H)$ *for all* $H, K \in \mathscr{H}$.

(iv) $\varepsilon(H, K) = \varepsilon(H, K^g)$ *for all* $H, K \in \mathscr{H}$ *and for all* $g \in G$.

Proof. (i) This follows from the fact that all $H \in \mathscr{H}$ do not contain ρ.

(ii) If $\rho \in HK^g$ for some g, then $\rho \in HK^g \leq H_1 K_1^g$ for all $H_1 \geq H$ and $K_1 \geq K$.

(iii) If $\rho \in KH^x$ for some $x \in G$, then $\rho = x^{-1}\rho^{-1}x \in HK^{x^{-1}}$ and vice versa.

(iv) If $\varepsilon(H, K) = 0$, then there exist $h \in H,\ k \in K,\ x \in G$ such that $\rho = hxkx^{-1}$. By writing $x = yg$, we have $\rho = hygkg^{-1}y^{-1} \in H(K^g)^y$. Thus we obtain $\varepsilon(H, K^g) = 0$. On the other hand, suppose that $\varepsilon(H, K) = 1$. If $\varepsilon(H, K^g) = 0$ for some $g \in G$, then there exists $y \in G$ such that $\rho \in H(K^g)^y = HK^{gy}$. This is a contradiction. Thus we have $\varepsilon(H, K^g) = 1$ for all $g \in G$. □

Lemma 2.3. *The following formula holds*:

$$|\mathscr{X}_{\geq}(H, K)| = \varepsilon(H, K)2^{\frac{1}{2}|H\backslash G/K|} = \begin{cases} 0 & \text{if } \varepsilon(K, H) = 0, \\ 2^{\frac{1}{2}|H\backslash G/K|} & \text{otherwise.} \end{cases}$$

Proof. Let S be a CM-type in $\mathrm{CM}(G, 1, \rho)$. First note that if $s(S) \geq H$, then the natural projection π_H sends S to the right coset space $H\backslash G$ and S can be written as a union of right cosets of H:

$$S = Hg_1 \sqcup \cdots \sqcup Hg_s \quad (s = [G : H]).$$

Similarly, if $r(S) \geq K$, then a natural map sends S to the left cosets space G/K and, thus, gives a left coset decomposition of S:

$$S = t_1 K \sqcup \cdots \sqcup t_u K \quad (u = [G : K]).$$

Therefore if $S \in \mathscr{X}_{\geq}(N, K)$, then we have a double coset decomposition

$$S = Hx_1 K \sqcup \cdots \sqcup Hx_r K.$$

If $\varepsilon(H, K) = 1$, then both x_i and ρx_i cannot belong to a same double coset $Hx_i K$ simultaneously. Suppose to the contrary that $Hx_i K = H\rho x_i K$. This equality means that there exist $h \in H$ and $k \in K$ such that $x_i = h\rho x_i k$. Since ρ is central in G, this, in turn, implies $\rho = hx_i k x_i^{-1} \in HK^{x_i}$. This is a contradiction. Thus if $\varepsilon(H, K) = 1$, then x_i and ρx_i belong to different double cosets and we have a double coset decomposition of G of the form

$$G = Hx_1 K \sqcup \cdots \sqcup Hx_r K \sqcup H\rho x_1 K \sqcup \cdots \sqcup H\rho x_r K \tag{2-4}$$

and hence we have $2r = |H\backslash G/K|$.

Conversely, if we have the double coset decomposition (2-4), then by choosing one double coset from each pair of cosets $(Hx_i K, H\rho x_i K)$, we can form a CM-type S such that $s(S) \geq N$ and $r(S) \geq K$.

Hence under the assumption $\varepsilon(H, K) = 1$, we have established a one-to-one correspondence between $\mathscr{X}_{\geq}(H, K)$ and the pairwise choice from the double coset decomposition of the form (2-4). We conclude that

$$|\mathscr{X}_{\geq}(N, K)| = 2^{\frac{1}{2}|H\backslash G/K|}$$

if $\varepsilon(H, K) = 1$. On the other hand, if $\varepsilon(H, K) = 0$, then the double coset decomposition of the form (2-4) is obviously impossible. Thus there is no CM-type satisfying the conditions. □

Now we state and prove our fundamental formula.

Theorem 2.4. *The number of elements in $\mathscr{X}(H, K)$ defined by* (2-1) *is given by*

$$|\mathscr{X}(H,K)| = \sum_{H_1 \in \mathscr{H}_{\geq}(H)} \sum_{K_1 \in \mathscr{H}_{\geq}(K)} \varepsilon(H_1,K_1)\mu(H,H_1)\mu(K,K_1)2^{\frac{1}{2}|H_1\backslash G/K_1|}.$$

Proof. We consider a product poset $\mathscr{H} \times \mathscr{H}$ whose partial order is defined by

$$(H_1,K_1) \geq (H_2,K_2) \quad \Longleftrightarrow \quad H_1 \geq H_2 \text{ and } K_1 \geq K_2.$$

Then the identity (2-3) can be rewritten as

$$\mathscr{X}_{\geq}(H,K) = \bigsqcup_{(H_1,K_1)\geq(H,K)} \mathscr{X}(H_1,K_1).$$

The Möbius inversion formula [Rota 1964, Proposition 3] on $\mathscr{H} \times \mathscr{H}$ implies

$$|\mathscr{X}(H,K)| = \sum_{(H_1,K_1)\geq(H,K)} \mu((H,K),(H_1,K_1))|\mathscr{X}_{\geq}(H_1,K_1)|.$$

Since the Möbius function on the product poset is nothing but a product of corresponding Möbius functions [Rota 1964, Proposition 5], we have

$$|\mathscr{X}(H,K)| = \sum_{H_1 \in \mathscr{H}_{\geq}(H)} \sum_{K_1 \in \mathscr{H}_{\geq}(K)} \mu(H,H_1)\mu(K,K_1)|\mathscr{X}_{\geq}(H_1,K_1)|.$$

By Lemma 2.2(ii), neglecting the terms with $\varepsilon(H_1, K_1) = 0$ does not affect the Möbius function. □

By the symmetry of the formula of Theorem 2.4 and that of ε (Lemma 2.2(iii)), we have:

Corollary 2.5. *For any $H, K \in \mathscr{H}$, we have $|\mathscr{X}(H,K)| = |\mathscr{X}(K,H)|$.*

The following corollaries help us to conclude $\mathscr{X}(H, K) = \varnothing$ when H is a normal subgroup of G.

Corollary 2.6. *Let $H, K \in \mathscr{H}$. Suppose that H is a normal subgroup of G:*

(i) *If $H \geq K$, then $\mathscr{X}(H,K) \neq \varnothing$ if and only if $H = K$.*

(ii) *If $HK \gneq K$, then $\mathscr{X}(H,K) = \varnothing$.*

Proof. If H is normal in G, then the double coset decomposition (2-4) agrees with the left coset decomposition by HK. If $H \geq K$ as in (i), then $HK = H$. Hence the result follows. Also if $HK \gneq K$ as in (ii), then the reflex subgroup must be strictly larger than K and $\mathscr{X}(H, K) = \varnothing$. □

Corollary 2.7. *Let $H, K \in \mathscr{H}$. Suppose that both H and K are normal subgroups of G. If $H \neq K$, then*

$$\mathscr{X}(H,K) = \varnothing.$$

In particular, if all CM subgroups of G are normal, then the matrix $(|\mathscr{X}(H,K)|)_{H,K\in\mathscr{H}}$ is diagonal.

Proof. If $H \neq K$, then $HK \gneq K$ holds. Hence by Corollary 2.6(ii), we have $\mathscr{X}(H, K) = \varnothing$. □

If, in particular, all the subgroups of G are normal (such finite groups are called Dedekind groups), then the second assertion of Corollary 2.7 can apply. Dedekind classified such groups: they are of the form $Q_8 \times A$ where A is an abelian group whose 2-Sylow subgroup is elementary. Other than Dedekind groups, nonabelian groups whose CM subgroups with respect to some central involution are all normal include the generalized quaternion groups Q_{2^n} and many others.

Corollary 2.8. *For all $H, K \in \mathscr{H}$ and all $x, y \in G$, we have*

$$|\mathscr{X}(H, K)| = |\mathscr{X}(H^x, K^y)|.$$

Proof. If $\varepsilon(H, K) = 1$, then there is a double coset decomposition of G by H and K given by (2-4). By Lemma 2.2(iv), there also exists a double coset decomposition by H and K^x for all $x \in G$. In fact, it is given by

$$G = Gx^{-1} = Hx_1x^{-1}K^x \sqcup \cdots \sqcup Hx_rx^{-1}K^x \sqcup H\rho x_1x^{-1}K^x \sqcup \cdots \sqcup H\rho x_rx^{-1}K^x.$$

In particular, we have $|\mathscr{X}_{\geq}(H, K)| = |\mathscr{X}_{\geq}(H, K^x)|$. The corollary now follows from Corollary 2.5. □

3. Simple CM-types and reflex CM-types

Let $H \in \mathscr{H}$. In this section, we enumerate simple CM-types in $\mathrm{CM}(G, H, \rho)$ and CM-types in $\mathrm{CM}(G, H, \rho)$ whose reflex subgroup coincides with given $K \in \mathscr{H}$. Although these sets are unions of some $\mathscr{X}(H', K')$'s in Section 2, we can obtain simpler formulas than that can be derived from Theorem 2.4. These formulas will be required to compute the number of conjugacy classes in Section 4.

For that purpose, we define

$$\mathscr{S}(H) = \{S \in \mathrm{CM}(G, 1, \rho) \mid s(S) = H\}, \tag{3-1}$$

$$\mathscr{S}_{\geq}(H) = \{S \in \mathrm{CM}(G, 1, \rho) \mid s(S) \geq H\}, \tag{3-2}$$

$$\mathscr{R}(H) = \{S \in \mathrm{CM}(G, 1, \rho) \mid r(S) = H\}, \tag{3-3}$$

$$\mathscr{R}_{\geq}(H) = \{S \in \mathrm{CM}(G, 1, \rho) \mid r(S) \geq H\}, \tag{3-4}$$

where $s(S)$ and $r(S)$ are defined by (1-2) and (1-3), respectively.

The set $\mathscr{S}(H)$ consists of the pullbacks of the simple CM-types of $\mathrm{CM}(G, H, \rho)$, while $\mathscr{S}_{\geq}(H)$ is the set of the pullbacks of $\mathrm{CM}(G, H, \rho)$.

Proposition 3.1. *The number of the simple CM-types in* $\mathrm{CM}(G, H, \rho)$ *is given by*

$$|\mathscr{S}(H)| = \sum_{N \in \mathscr{H}_{\geq}(H)} \mu(H, N) 2^{\frac{1}{2}|N\backslash G|}.$$

Proof. The following equality obviously holds by definition:

$$\mathscr{S}_{\geq}(H) = \bigsqcup_{N \in \mathscr{H}_{\geq}(H)} \mathscr{S}(N).$$

The cardinality of $\mathscr{S}_{\geq}(H)$ is given by

$$|\mathscr{S}_{\geq}(H)| = |\pi_H^{-1}(\mathrm{CM}(G, H, \rho))| = |\mathrm{CM}(G, H, \rho)| = 2^{\frac{1}{2}|H\backslash G|}.$$

Hence simple Möbius inversion implies our result. □

Corollary 3.2. *The cardinality of $\mathscr{R}(H)$ is the same as that of $\mathscr{S}(H)$:*

$$|\mathscr{R}(H)| = \sum_{N \in \mathscr{H}_{\geq}(H)} \mu(H, N) 2^{\frac{1}{2}|N\backslash G|}.$$

Proof. By the definitions (3-1) and (3-3), it is easy to see that

$$\mathscr{S}(H) = \bigsqcup_{K \in \mathscr{H}} \mathscr{X}(H, K) \quad \text{and} \quad \mathscr{R}(H) = \bigsqcup_{K \in \mathscr{H}} \mathscr{X}(K, H).$$

From Corollary 2.5, the result follows. □

Let $H, K \in \mathscr{H}$. We next count the number of CM-types in $\mathrm{CM}(G, H, \rho)$ whose reflex subgroup is K, namely the cardinality of the set

$$\pi_H(\mathscr{S}_{\geq}(H) \cap \mathscr{R}(K)) = \{S \in \mathrm{CM}(G, H, \rho) \mid r(S) = K\}.$$

Proposition 3.3. *We have the following formula*:

$$|\pi_H(\mathscr{S}_{\geq}(H) \cap \mathscr{R}(K))| = \sum_{N \in \mathscr{H}_{\geq}(K)} \varepsilon(H, N)\mu(K, N)2^{\frac{1}{2}|H \backslash G / N|}.$$

Proof. In the right-hand side of (2-3), we see

$$\begin{aligned} \bigsqcup_{H_1 \in \mathscr{H}_{\geq}(H)} \mathscr{X}(H_1, K_1) &= \{S \in \mathrm{CM}(G, 1, \rho) \mid s(S) \geq H \text{ and } r(S) = K_1\} \\ &= \mathscr{S}_{\geq}(H) \cap \mathscr{R}(K_1) \end{aligned}$$

and thus

$$\mathscr{X}_{\geq}(H, K) = \bigsqcup_{K_1 \in \mathscr{H}_{\geq}(K)} \mathscr{S}_{\geq}(H) \cap \mathscr{R}(K_1).$$

Möbius inversion implies

$$|\mathscr{S}_{\geq}(H) \cap \mathscr{R}(K)| = \sum_{K_1 \in \mathscr{H}_{\geq}(K)} \mu(K, K_1)|\mathscr{X}_{\geq}(H, K_1)|.$$

By Lemma 2.2(ii), the function $\varepsilon(H, N)$ is compatible with the poset structure of $\mathscr{H}_{\geq}(K)$, and we obtain the proposition using Lemma 2.3. □

Corollary 3.4. *We have* $|\mathscr{S}(H) \cap \mathscr{R}_{\geq}(K)| = |\mathscr{S}_{\geq}(K) \cap \mathscr{R}(H)|$.

Proof. By Corollary 2.5, we see that

$$|\mathscr{S}(H) \cap \mathscr{R}_{\geq}(K)| = \sum_{K_1 \in \mathscr{H}_{\geq}(K)} |\mathscr{X}(H, K_1)| = \sum_{K_1 \in \mathscr{H}_{\geq}(K)} |\mathscr{X}(K_1, H)| = |\mathscr{S}_{\geq}(K) \cap \mathscr{R}(H)|. \quad \square$$

For convenience, we summarize the counting formulas obtained up to this section. We arrange the members of $\mathscr{H}$ in a line so that $H_i > H_j$ implies $i > j$ and we form a matrix $X = (|\mathscr{X}(H, K)|)_{H,K \in \mathscr{H}}$. The counting formulas are summarized as follows:

each entry $\lvert\mathscr{X}(H, K)\rvert$	Theorem 2.4
a row sum $\lvert\mathscr{S}(H)\rvert$	Proposition 3.1
a column sum $\lvert\mathscr{R}(K)\rvert$	Corollary 3.2
a row subsum $\lvert\mathscr{S}(H) \cap \mathscr{R}_{\geq}(K)\rvert$	Corollary 3.4
a column subsum $\lvert\mathscr{S}_{\geq}(H) \cap \mathscr{R}(K)\rvert$	Proposition 3.3
a submatrix sum $\lvert\mathscr{X}_{\geq}(H, K)\rvert$	Lemma 2.3

4. Number of conjugacy classes

In this section, we prove a counting formula for the conjugacy classes in $\mathrm{CM}(G, H, \rho)$.

Recall that two CM-types $S, S' \in \mathrm{CM}(G, H, \rho)$ are conjugate if there exists $g \in G$ satisfying $S' = Sg$. Therefore the number of conjugacy classes is the number of the orbits under this group action.

Theorem 4.1. *Let G be a finite group and ρ a central involution of G and H a subgroup of G not containing ρ. The number $c(G, H, \rho)$ of the conjugacy classes in $\mathrm{CM}(G, H, \rho)$ is given by*

$$\begin{aligned} c(G, H, \rho) &= \frac{1}{|G|} \sum_{K \in \mathscr{H}} |K| \, |\mathscr{S}_{\geq}(H) \cap \mathscr{R}(K)| \\ &= \frac{1}{|G|} \sum_{K \in \mathscr{H}} |K| \sum_{N \in \mathscr{H}_{\geq}(K)} \varepsilon(H, N) \mu(K, N) \, 2^{\frac{1}{2}|H \backslash G / N|}. \end{aligned}$$

To prove Theorem 4.1, we need the following proposition.

Proposition 4.2. *For $H, K \in \mathscr{H}$, the number of conjugacy classes in $\mathscr{S}_{\geq}(H) \cap \mathscr{R}(K)$ is*

$$\frac{|K|}{|G|} \, |\mathscr{S}_{\geq}(H) \cap \mathscr{R}(K)|.$$

Proof. If $g \in G$ and $S \in \mathrm{CM}(G, H, \rho)$, then $Sg = S$ holds if and only if $g \in r(S)$. Hence the g-invariant subset of $(\mathscr{S}_{\geq}(H) \cap \mathscr{R}(K))$ is given by

$$\begin{aligned} (\mathscr{S}_{\geq}(H) \cap \mathscr{R}(K))^g &= \{S \in \mathscr{S}_{\geq}(H) \cap \mathscr{R}(K) \mid S = Sg\} \\ &= \begin{cases} \mathscr{S}_{\geq}(H) \cap \mathscr{R}(K) & \text{if } g \in K, \\ \varnothing & \text{otherwise.} \end{cases} \end{aligned}$$

Thus we obtain

$$|(\mathscr{S}_{\geq}(H) \cap \mathscr{R}(K))^g| = \mathrm{ch}_K(g) |\mathscr{S}_{\geq}(H) \cap \mathscr{R}(K)|,$$

where

$$\mathrm{ch}_K(g) = \begin{cases} 1 & \text{if } g \in K, \\ 0 & \text{otherwise} \end{cases}$$

is the characteristic function of K. From the lemma of Burnside and Frobenius [Aigner 2007, Lemma 6.2] it follows that the number of the orbits is then given by

$$\frac{1}{|G|} \sum_{g \in K} \mathrm{ch}_K(g) \, |\mathscr{S}_{\geq}(H) \cap \mathscr{R}(K)| = \frac{|K|}{|G|} \, |\mathscr{S}_{\geq}(H) \cap \mathscr{R}(K)|. \qquad \square$$

Now we can prove the counting formula for the conjugacy classes.

Proof of Theorem 4.1. If two CM-types S and S' are conjugate, then we have $r(S) = r(S')$ by the definition of the conjugacy. Thus the decomposition $\mathrm{CM}(G, H, \rho) = \bigsqcup_{K \in \mathscr{H}} \mathscr{S}_{\geq}(H) \cap \mathscr{R}(K)$ is stable

under this G-action. Hence we have

$$\begin{aligned} c(G,H,\rho) &= \sum_{K\in\mathscr{H}} |\text{the conjugacy classes in } \mathscr{S}_{\geq}(H)\cap\mathscr{R}(K)| \\ &= \sum_{K\in\mathscr{H}} \frac{|K|}{|G|}\,|\mathscr{S}_{\geq}(H)\cap\mathscr{R}(K)| \end{aligned}$$

by Proposition 4.2. This is the first equality of the theorem. The second equality follows readily from Proposition 3.3. This completes the proof of Theorem 4.1. □

Remark 4.3. By Theorem 4.1, we have

$$\begin{aligned} |\mathrm{CM}(G,H,\rho)| &= \sum_{K\in\mathscr{H}} |\mathscr{S}_{\geq}(H)\cap\mathscr{R}(K)| \\ &= \sum_{K\in\mathscr{H}} \frac{|G|}{|K|}\,|\text{the conjugacy classes in } \mathscr{S}_{\geq}(H)\cap\mathscr{R}(K)|. \end{aligned}$$

For each $K\in\mathscr{H}$, we see $[L^K:\mathbb{Q}]=|G|/|K|$, where L^K is the reflex field. Hence the sum of $[L^K:\mathbb{Q}]$ over a representative of the conjugacy classes of $\mathrm{CM}(G,H,\rho)$ is $2^{\frac{1}{2}|H\backslash G|}$. This fact was previously noticed by Dodson [1984, p. 5] and Oishi-Tomiyasu [2010, Lemma 1.4].

5. Construction of degenerate CM-types

For a simple CM-type $S\in\mathrm{CM}(G,H,\rho)$, let $H'=r(S)$ be the reflex subgroup. We define a linear map

$$\Phi_S : \mathbb{Z}[H\backslash G]\to\mathbb{Z}[H'\backslash G]$$

by $x\mapsto\sum_{H'\sigma\in S'} H'\sigma x$, where S' is the reflex CM-type of S. Here we understand that $\mathbb{Z}[H\backslash G]$ is a free left $\mathbb{Z}$-module on $H\backslash G$ and $\mathbb{Z}[H'\backslash G]$ is that on $H'\backslash G$ on which $H\backslash G$ acts from the right. Since the elements of the form $(Hx+Hx\rho)-(Hy+Hy\rho)$ with $x,y\in G$ are contained in the kernel of Φ_S, the rank of Φ_S is less than or equal to $\frac{1}{2}|H\backslash G|+1$. The CM-type S is called *nondegenerate* if the rank is maximal, that is, if $\operatorname{rank}\Phi_S=\frac{1}{2}|H\backslash G|+1$ holds; otherwise it is called *degenerate*. If S is nondegenerate, then the Hodge conjecture is true for CM abelian varieties with CM-type S, whereas, if S is degenerate, then exceptional Hodge cycles exist on a self-product of the CM abelian variety. Hence it is interesting to know how to construct degenerate CM-types. One easy way to construct degenerate simple CM-types S of (G,H,ρ) is to construct CM-types S satisfying $|H'|>|H|$, since we know the rank of Φ_S is less than or equal to $\min\{\frac{1}{2}|H\backslash G|+1,\frac{1}{2}|H'\backslash G|+1\}$ by [Ribet 1980, (3.5)].

We have the following criteria for such CM-types to exist. The first criterion is obvious from the definition of $\mathscr{X}(H,K)$ and Corollary 2.5.

Proposition 5.1. *If $\mathscr{X}(H,K)\neq\varnothing$ for some $H,K\in\mathscr{H}$ such that $|H|\neq|K|$, then there exists a degenerate CM-type in* $\mathrm{CM}(G,H,\rho)$ *or* $\mathrm{CM}(G,K,\rho)$.

Although we have a formula for $\mathscr{X}(H,K)$, it is not immediate how to determine whether $\mathscr{X}(H,K)=\varnothing$ or not. Indeed, there is an example of H such that $\mathscr{X}(H,K)=\varnothing$ for all $K\in\mathscr{H}$ (see Example 6.2).

The following proposition is sometimes useful.

Proposition 5.2. *Let $H \in \mathscr{H}$. Assume that $\varepsilon(H, K) = 0$ for all $K \in \mathscr{H}$ such that $|K| = |H|$. If there exists a simple CM-type in* $\mathrm{CM}(G, H, \rho)$, *then there exists a degenerate CM-type in* $\mathrm{CM}(G, H, \rho)$.

Proof. By the assumptions and Lemma 2.3, it is impossible to have a double coset decomposition by H and K like (2-4). If $H = 1$, then the assumption apparently does not hold and, hence, we may assume $H \neq 1$. Then there exists $N \in \mathscr{H}$ such that $|N| \neq |H|$ and $HN^x \not\supseteq \rho$ for all $x \in G$. For example, we can take $N = 1$. The double coset decomposition of G by H and N is now of the form (2-4). By the assumption of the proposition, the order of $r(S)$ of a simple CM-type S with respect to (G, H, ρ) is different from $|H|$. If $|r(S)| < |H|$, then replacing H by $r(S)$, we obtain a CM-type satisfying $|r(S)| > |H|$. □

In the next section, we will construct infinite families of pairs of finite groups (G, H) satisfying the conditions of Propositions 5.1 and 5.2.

6. Examples

In this section, we use our theorems to give several examples.

The following lemma is useful in explicit computation and interesting in its own right.

Lemma 6.1. *If $H \in \mathscr{H}$ is a normal subgroup of G such that the quotient G/H is isomorphic to either the direct product $C_2 \times C_2$ of cyclic groups of order 2 or the dihedral group D_4 of order 8, then we have*

$$\mathscr{S}(H) = \mathscr{R}(H) = \varnothing.$$

In particular, every CM abelian variety with CM-types in $\mathrm{CM}(G, H, \rho)$ *splits.*

Proof. If H is a normal subgroup, then there is a one-to-one correspondence between $\mathrm{CM}(G, H, \rho)$ and $\mathrm{CM}(G/H, 1, \rho H)$, where the latter ρ is the image of ρ under the natural projection. Therefore it suffices to show that $\mathscr{S}(1) = \mathscr{H}(1) = \varnothing$ for $G = C_2 \times C_2$ or $G = D_4$. For these two groups, the CM subgroups are of order 1 or 2 and the Hasse diagrams of $\mathscr{H}$ are

respectively. By Proposition 3.1, for $G = C_2 \times C_2$ we have $|\mathscr{S}(1)| = 2^2 - 2 \cdot 2 = 0$ and for $G = D_4$ we have $|\mathscr{S}(1)| = 2^4 - 4 \cdot 2^2 = 0$ as desired. The claim for $\mathscr{R}(H)$ follows from Corollary 3.2. □

Schappacher [1977] proved that the converse of Lemma 6.1 also holds.

Example 6.2 (cyclic group C_{2p}). Let p be an odd prime number and $G = C_{2p}$ a cyclic group of order $2p$ generated by x. The element $\rho = x^p$ is a unique central involution in G and we have $\mathscr{H} = \{\langle x^2\rangle, 1\}$. Since all subgroups of G are normal in G, it follows from Corollary 2.7 that if $H \neq K$, then $\mathscr{X}(H, K) = \varnothing$. We have to compute only $|\mathscr{X}(1, 1)|$ and $|\mathscr{X}(\langle x^2\rangle, \langle x^2\rangle)|$. The Möbius function on $\mathscr{H}$ is computed as

$$\mu(1, 1) = 1, \quad \mu(1, \langle x^2\rangle) = -1 \quad \text{and} \quad \mu(\langle x^2\rangle, \langle x^2\rangle) = 0.$$

By Theorem 2.4, we have

$$|\mathscr{X}(1, 1)| = \mu(1, 1)^2 2^p + 2\mu(1, 1)\mu(1, \langle x^2\rangle)2 + \mu(1, \langle x^2\rangle)^2 2 = 2^p - 2,$$
$$|\mathscr{X}(\langle x^2\rangle, \langle x^2\rangle)| = \mu(\langle x^2\rangle, \langle x^2\rangle)2 = 2.$$

The number of conjugacy classes can be computed by Theorem 4.1 and, in this case, it is convenient to use

$$c(G,H,\rho)=\frac{1}{|G|}\sum_{K\in\mathscr{H}}|K||\mathscr{S}_{\geq}(H)\cap\mathscr{R}(K)|=\frac{1}{|G|}\sum_{K\in\mathscr{H}}\sum_{H_1\in\mathscr{H}_{\geq}(H)}|K||\mathscr{X}(H_1,K)|,$$

and we have

$$c(G,\langle x^2\rangle,\rho)=1,\quad c(G,1,\rho)=\frac{2^{p-1}-1}{p}+1.$$

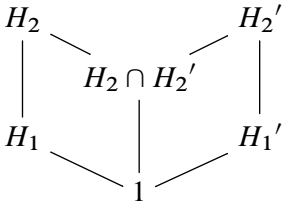
The first term of the right-hand side of the second expression is an integer by Fermat's theorem. In particular, the situation discussed in Section 5 does not occur.

CM-fields over $\mathbb{Q}$ with Galois group C_{2p} can be constructed easily as follows: We choose a prime number q such that $p\parallel(q-1)$. Then the q-th cyclotomic field contains a unique totally real cyclic extension M of degree p over $\mathbb{Q}$. The composite field of M with an imaginary quadratic field gives a desired field.

Example 6.3 (dihedral group D_{2p}). Again let p be an odd prime number. We consider the dihedral group $G=D_{2p}$ of order $4p$, which has a presentation

$$D_{2p}=\langle s,t\mid s^2=1,\ t^{2p}=1,\ sts=t^{2p-1}\rangle.$$

A unique central involution in D_{2p} is $\rho=t^p$. The members of $\mathscr{H}$ are: two nonconjugate subgroups $H_1=\langle st\rangle$, $H_1{}'=\langle st^2\rangle$ of order 2 whose lengths are p and two normal subgroups $H_2=\langle st,t^2\rangle$, $H_2{}'=\langle st^2,t^2\rangle$ of order $2p$ and one normal subgroup $H_2\cap H_2{}'=\langle t^2\rangle$ of order p. The conjugates of H_1 and $H_1{}'$ are, respectively, $H_1^{t^i}$ and $H_1{}'^{t^i}$ $(i=0,1,\dots,p-1)$. The Hasse diagram of $\mathscr{H}$ modulo the conjugacy is



Since $H_1(H_1')^{t^{\frac{1}{2}(p+1)}}\ni st\cdot t^{\frac{1}{2}(p+1)}st^2t^{-\frac{1}{2}(p+1)}=t^p=\rho$, we have the following table of $\varepsilon=\varepsilon_{\mathscr{H}}$:

$H\backslash K$	1	H_1	H_1'	$H_2\cap H_2'$	H_2	H_2'
1	1	1	1	1	1	1
H_1	1	1	0	1	1	0
H_1'	1	0	1	1	0	1
$H_2\cap H_2'$	1	1	1	1	1	1
H_2	1	1	0	1	1	0
H_2'	1	0	1	1	0	1

The Möbius function $\mu(H, K)$ on $\mathscr{H}$ can be computed by the definition (1-5) by noting that both H_1 and H_2 have p conjugate groups:

$H\backslash K$	1	H_1	H_1'	$H_2 \cap H_2'$	H_2	H_2'
1	1	−1	−1	−1	p	p
H_1	0	1	0	0	−1	0
H_1'	0	0	1	0	0	−1
$H_2 \cap H_2'$	0	0	0	1	−1	−1
H_2	0	0	0	0	1	0
H_2'	0	0	0	0	0	1

If $N \in \mathscr{H}$ is normal in G, then $|H_1\backslash G/N| = |H_1 N\backslash G|$, and hence, we have only to compute a double coset decomposition of G by H_1 and H_1:

$$G = H_1H_1 \sqcup H_1tH_1 \sqcup \cdots \sqcup H_1t^pH_1.$$

This yields $|H_1\backslash G/H_1| = p + 1$.

To compute $|\mathscr{X}(1, H_1)|$, it is convenient to use Proposition 3.3. Since H_2 is normal in G, we have $\mathscr{X}(1, H_2) = \varnothing$ by Corollary 2.6. Therefore we obtain

$$\mathscr{S}(1) \cap \mathscr{R}_{\geq}(H_1) = \bigsqcup_{K \in \mathscr{H}_{\geq}(H_1)} \mathscr{X}(1, K) = \mathscr{X}(1, H_1) \sqcup \mathscr{X}(1, H_2) = \mathscr{X}(1, H_1).$$

Using Corollary 3.4 and Proposition 3.3, we compute

$$\begin{aligned}
&|\mathscr{X}(1, H_1)| \\
&\quad = |\mathscr{S}(1) \cap \mathscr{R}_{\geq}(H_1)| = |\mathscr{S}_{\geq}(H_1) \cap \mathscr{R}(1)| \\
&\quad = \sum_{N \in \mathscr{H}_{\geq}(1)} \varepsilon(H_1, N)\mu(1, N)2^{\frac{1}{2}|H_1\backslash G/N|} \\
&\quad = \mu(1,1)2^{\frac{1}{2}|H_1\backslash G|} + p\mu(1, H_1)2^{\frac{1}{2}|H_1\backslash G/H_1|} + \mu(1, H_2 \cap H_2')2^{\frac{1}{2}|H_1\backslash G/H_2\cap H_2'|} + \mu(1, H_2)2^{\frac{1}{2}|H_1\backslash G/H_2|} \\
&\quad = 2^p - p2^{\frac{1}{2}(p+1)} + 2p - 2.
\end{aligned}$$

This quantity is positive if $p \geq 7$. By Proposition 5.1, CM-types contained in this set are simple and degenerate. It is interesting to note that

$$\lim_{p\to\infty} \frac{|\mathscr{X}(1, H_1)|}{|\mathrm{CM}(D_{2p}, 1, \rho)|} = 0.$$

We also compute $\mathscr{X}(H_2 \cap H_2', K)$ for all $K \in \mathscr{H}$. Let $H = H_2 \cap H_2'$ for short. Since H is normal in G, we have $\mathscr{X}(H, K) = \varnothing$ for $K = 1, H_1, H_2$ by Corollary 2.6 and this also holds for $K = H_2$ and H_2' if we combine Corollaries 2.5 and 2.6. Thus only $\mathscr{X}(H, H)$ remains. On the other hand, since $G/H \cong D_4$, we have $\mathscr{S}(H) = \varnothing$ by Lemma 6.1 and, thus, $\mathscr{X}(H, H)$ must be empty. Hence $\mathscr{X}(H_2 \cap H_2', K) = \varnothing$ holds for all $K \in \mathscr{H}$.

Example 6.4 (semidirect product $C_{2^k} \rtimes C_2$). Let k be an integer greater than or equal to 3. In this example, we consider semidirect products $C_{2^k} \rtimes C_2$, where $C_2 = \langle s \rangle$ acts on $C_{2^k} = \langle t \rangle$ by $sts = t^u$. In

this situation, u is one of -1, $2^{k-1}\pm 1$. If $u=-1$, then $C_{2^k}\rtimes C_2\simeq D_{2^k}$ and if $u=2^{k-1}+1$, then the group is isomorphic to the semidihedral group $SD_{2^{k+1}}$ and if $u=2^{k-1}-1$, then the group is called the modular maximal-cyclic group and we denote it by $M_{2^{k+1}}$. A unique central involution of these groups is $\rho=t^{2^{k-1}}$. The CM subgroup posets are

$$\begin{aligned}\mathscr{H}(D_{2^k})&=\{H_1=\langle st\rangle,\ H_2=\langle st^2\rangle\},\\ \mathscr{H}(SD_{2^{k+1}})&=\{H_3=\langle s\rangle\},\\ \mathscr{H}(M_{2^{k+1}})&=\{H_4=\langle s\rangle\}.\end{aligned}$$

The lengths of H_1, H_2, and H_3 are 2^{k-1} and that of H_4 is 2. Since $H_1H_1^{t^{2^{k-2}}}\ni stt^{2^{k-2}}stt^{-2^{k-2}}=\rho$, we have $\varepsilon(H_1,H_1)=0$. Similarly $H_2H_2^{t^{2^{k-2}}}$, $H_3H_3^{t^{-1}}$, and $H_4H_4^t$ contain ρ and we conclude

$$\varepsilon(H_i,H_i)=0\quad(i=1,2,3,4). \tag{6-1}$$

Hence, in particular, $SD_{2^{k+1}}$ and $M_{2^{k+1}}$ satisfy the assumption in Proposition 5.2. On the other hand, we have

$$D_{2^k}=\bigsqcup_{i=1}^{2^{k-2}}(H_1t^iH_2\sqcup H_1t_i\rho H_2) \tag{6-2}$$

and $\varepsilon(H_1,H_2)=1$.

We compute $|\mathscr{X}(1,H_i)|$ by computing $|\mathscr{S}_{\geq}(H_i)\cap\mathscr{R}(1)|$ as in Example 6.3.

For H_1 and H_2, using (6-1) we have

$$\begin{aligned}|\mathscr{X}(1,H_i)|&=\sum_{N\in\mathscr{H}_{\geq}(1)}\varepsilon(H_i,N)\mu(1,N)2^{\frac{1}{2}|H_i\backslash D_{2^k}/N|}\\ &=\varepsilon(H_i,1)\mu(1,1)2^{\frac{1}{2}|H_i\backslash G|}+\sum_x\varepsilon(H_i,H_j^x)\mu(1,H_j^x)2^{\frac{1}{2}|H_i\backslash D_{2^k}/H_j|},\end{aligned}$$

where $i,j\in\{1,2\}$ and $i\neq j$ and the last summation is taken over a transversal of $N_G(H_j)\backslash D_{2^k}$. From Lemma 2.2(iv) and (6-2) it follows

$$|\mathscr{X}(1,H_i)|=2^{2^{k-1}}-2^{k-1}2^{2^{k-2}}=2^{2^{k-1}}-2^{2^{k-2}+k+1}\quad(i=1,2),$$

which is positive if k is greater than 3.

For H_3 and H_4, computation is simpler. In fact, we have

$$|\mathscr{X}(1,H_i)|=\varepsilon(H_i,1)\mu(1,1)2^{\frac{1}{2}|H_i\backslash G|}=2^{2^{k-1}},$$

where G is either $SD_{2^{k+1}}$ or $M_{2^{k+1}}$.

Example 6.5 (wreath product $C_2\wr C_d$). Let H be a CM-subgroup of G and $S\in\mathrm{CM}(G,H,\rho)$. It is generally known that

$$2\log_2|H\backslash G|\leq|r(S)\backslash G|\leq 2^{\frac{1}{2}|H\backslash G|}$$

and that there exists a CM-type S such that $|r(S)\backslash G|=2^{\frac{1}{2}|H\backslash G|}$ holds (see [Ribet 1980, (3.2)]). In this example, we explicitly construct such CM-types when $\frac{1}{2}|H\backslash G|$ is odd.

Let d be an odd integer. We consider the wreath product $G = C_2 \wr C_d$, where C_d acts on d copies of C_2 by permutation. Hence the order of G is $2^d d$. The group G has a presentation

$$G = \langle c_1, \ldots, c_d, r \mid c_1^2 = \cdots c_d^2 = r^d = 1,\ r c_i r^{-1} = c_{i+1}\ (i = 1, \ldots, d)\rangle,$$

where the index i is understood modulo d. It is easy to show that $\rho = c_1 \cdots c_g$ is a central involution (in fact, a unique central involution). We consider the two subgroups of G

$$H = \langle c_2, c_3, \ldots, c_d\rangle, \quad K = \langle r\rangle.$$

They are obviously CM-subgroups of G with respect to ρ and we see $|H| = 2^{d-1}$ and $|K| = d$ and hence $|K\backslash G| = 2d = 2^{\frac{1}{2}|H\backslash G|}$ holds. We shall show $\mathscr{X}(H, K) = 2$.

We first show that H is a maximal CM-subgroup. Suppose that H' is a CM-subgroup such that $H' \gneq H$. If $|H'|$ is a power of 2, then $|H'| = 2^d$ and H' is a 2-Sylow subgroup of G. On the other hand, we know that $C = \langle c_1, \ldots, c_g\rangle$ is a 2-Sylow group, which is normal in G. We thus conclude that $H' = C$ and $\rho \in H'$. This is a contradiction. Therefore there exists an odd prime p dividing $|H'|$ and, by Cauchy's theorem, there exists an element $x \in H'$ of order p. We can write $x = c r^k$ with $c \in H$ and an integer $d > k \geq 1$. We then have $x c_1 x^{-1} = c r^k c_1 r^{-k} c^{-1} = c c_{k+1} c^{-1} \in H$. Here we note that $c_{k+1} \neq c_1$. This implies $c_1 \in x^{-1} H x \subseteq H'$ and then $\rho \in H'$ and we again get a contradiction. Thus we have proved that H is a maximal CM-subgroup and therefore, we have

$$\mathscr{X}(H, K) = \mathscr{S}(H) \cap \mathscr{R}(K) = \mathscr{S}_{\geq}(H) \cap \mathscr{R}(K).$$

We use Proposition 3.3 to enumerate this.

To this end, we have to consider the groups N in $\mathscr{H}_{\geq}(K)$ and compute $|H\backslash G/N|$. We note that the cardinality $|HxK|$ of every double coset of G by H and N is divisible by both $|H|$ and $|K|$ and therefore we have $|HxK| = 2^{d-1}d$ or $2^d d$.

We begin with the case $N = K$. Let $c \in H$ and $r^k \in K$ and suppose that the order of $c r^k \in HK$ is 2. If we write $r^k c r^{-k} = c' \in C$, then we have $c r^k c r^k = c c' r^{2k} = 1$. This implies $2k \equiv 0 \pmod{d}$. We conclude that every element of order 2 in HK is contained in H. In particular, we obtain $\rho \notin HK$ and the double coset decomposition $G = HK \sqcup H\rho K$.

Next we consider $\mathscr{H}_{\geq}(K) \ni N \gneq K$. There exists $c \in N$ of order 2, which is a product of some of $c_2, \ldots, c_g$. Since N is a subgroup, N also contains $r^k c r^{-k}$ for $0 \leq k < d$. At least one of the elements $r^k c r^{-k}$ contains c_1 as a cycle factor. This implies $\rho \in HN$ and we have $G = HN$.

Now it follows from Proposition 3.3 that

$$\mathscr{X}(H, K) = \sum_{N \in \mathscr{H}_{\geq}(K)} \varepsilon(H, N)\mu(K, N) 2^{\frac{1}{2}|H\backslash G/N|} = 2^{\frac{1}{2}|H\backslash G/K|} = 2$$

as desired.

The groups considered in Examples 6.3, 6.4, and 6.5 are all solvable groups. Thus the existence of CM-fields with Galois group isomorphic to these groups is guaranteed by Dodson's theorem [1986, Theorem 1.4]. Many explicit examples with small order are found in the database http://galoisdb.math.upb.de/. In particular, $C_2 \wr C_d$-extensions are constructed by starting from a totally real C_d-extension and using a construction explained in [Shimura 1970, 1.10].

References

[Aigner 2007] M. Aigner, *A course in enumeration*, Graduate Texts in Mathematics **238**, Springer, 2007. MR Zbl

[Dodson 1984] B. Dodson, "The structure of Galois groups of CM-fields", *Trans. Amer. Math. Soc.* **283**:1 (1984), 1–32. MR Zbl

[Dodson 1986] B. Dodson, "Solvable and nonsolvable CM-fields", *Amer. J. Math.* **108**:1 (1986), 75–93. MR Zbl

[Greenberg 1980] R. Greenberg, "On the Jacobian variety of some algebraic curves", *Compositio Math.* **42**:3 (1980), 345–359. MR Zbl

[Oishi-Tomiyasu 2010] R. Oishi-Tomiyasu, "On some algebraic properties of CM-types of CM-fields and their reflexes", *J. Number Theory* **130**:11 (2010), 2442–2466. MR Zbl

[Ribet 1980] K. A. Ribet, "Division fields of abelian varieties with complex multiplication", pp. 75–94 in *Abelian functions and transcendental numbers* (Palaiseau, 1979), Mém. Soc. Math. France (N.S.) **2**, Soc. Math. France, Paris, 1980. MR Zbl

[Rota 1964] G.-C. Rota, "On the foundations of combinatorial theory, I: Theory of Möbius functions", *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete* **2** (1964), 340–368. MR Zbl

[Schappacher 1977] N. Schappacher, "Zur Existenz einfacher abelscher Varietäten mit komplexer Multiplikation", *J. Reine Angew. Math.* **292** (1977), 186–190. MR Zbl

[Shimura 1970] G. Shimura, "On canonical models of arithmetic quotients of bounded symmetric domains", *Ann. of Math.* (2) **91** (1970), 144–222. MR Zbl

Received 14 Mar 2019. Revised 17 May 2019.

MASANARI KIDA:

kida@rs.tus.ac.jp
Department of Mathematics, Faculty of Science Division I, Tokyo University of Science, Tokyo, Japan

Moscow Journal of Combinatorics and Number Theory

msp.org/moscow

EDITORS-IN-CHIEF

Yann Bugeaud — Université de Strasbourg (France), bugeaud@math.unistra.fr
Nikolay Moshchevitin — Lomonosov Moscow State University (Russia), moshchevitin@gmail.com
Andrei Raigorodskii — Moscow Institute of Physics and Technology (Russia), mraigor@yandex.ru
Ilya D. Shkredov — Steklov Mathematical Institute (Russia), ilya.shkredov@gmail.com

EDITORIAL BOARD

Iskander Aliev — Cardiff University (United Kingdom)
Vladimir Dolnikov — Moscow Institute of Physics and Technology (Russia)
Nikolay Dolbilin — Steklov Mathematical Institute (Russia)
Oleg German — Moscow Lomonosov State University (Russia)
Michael Hoffman — United States Naval Academy
Grigory Kabatiansky — Russian Academy of Sciences (Russia)
Roman Karasev — Moscow Institute of Physics and Technology (Russia)
Gyula O. H. Katona — Hungarian Academy of Sciences (Hungary)
Alex V. Kontorovich — Rutgers University (United States)
Maxim Korolev — Steklov Mathematical Institute (Russia)
Christian Krattenthaler — Universität Wien (Austria)
Antanas Laurinčikas — Vilnius University (Lithuania)
Vsevolod Lev — University of Haifa at Oranim (Israel)
János Pach — EPFL Lausanne(Switzerland) and Rényi Institute (Hungary)
Rom Pinchasi — Israel Institute of Technology – Technion (Israel)
Alexander Razborov — Institut de Mathématiques de Luminy (France)
Joël Rivat — Université d'Aix-Marseille (France)
Tanguy Rivoal — Institut Fourier, CNRS (France)
Damien Roy — University of Ottawa (Canada)
Vladislav Salikhov — Bryansk State Technical University (Russia)
Tom Sanders — University of Oxford (United Kingdom)
Alexander A. Sapozhenko — Lomonosov Moscow State University (Russia)
József Solymosi — University of British Columbia (Canada)
Andreas Strömbergsson — Uppsala University (Sweden)
Benjamin Sudakov — University of California, Los Angeles (United States)
Jörg Thuswaldner — University of Leoben (Austria)
Kai-Man Tsang — Hong Kong University (China)
Maryna Viazovska — EPFL Lausanne (Switzerland)
Barak Weiss — Tel Aviv University (Israel)

PRODUCTION

Silvio Levy — (Scientific Editor), production@msp.org

Cover design: Blake Knoll, Alex Scorpan and Silvio Levy

See inside back cover or msp.org/moscow for submission instructions.

The subscription price for 2019 is US $310/year for the electronic version, and $365/year (+$20, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Moscow Journal of Combinatorics and Number Theory (ISSN 2640-7361 electronic, 2220-5438 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

MJCNT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY
mathematical sciences publishers
nonprofit scientific publishing
http://msp.org/
© 2019 Mathematical Sciences Publishers

Moscow Journal of Combinatorics and Number Theory
vol. 8 no. 4 2019