Generalized Dedekind's theorem and its application to integer group determinants

Naoya Yamaguchi and Yuka Yamaguchi

June 26, 2023

Abstract

In this paper, we give a refinement of a generalized Dedekind's theorem. In addition, we show that all possible values of integer group determinants of any group are also possible values of integer group determinants of its any abelian subgroup. By applying the refinement of a generalized Dedekind's theorem, we determine all possible values of integer group determinants of the direct product group of the cyclic group of order 8 and the cyclic group of order 2.

1 Introduction

For a finite group G, let x_g be an indeterminate for each $g \in G$ and let $\mathbb{Z}[x_g]$ be the multivariate polynomial ring in x_g over $\mathbb{Z}$. The group matrix $M_G(x_g)$ and the group determinant $\Theta_G(x_g)$ of G were defined by Dedekind as follows:

$$M_G(x_g) := \left(x_{gh^{-1}}\right)_{g,h \in G}, \quad \Theta_G(x_g) := \det M_G(x_g) \in \mathbb{Z}[x_g].$$

When the elements of G are reordered arbitrarily, the group matrix M formed according to this reordering is of the form $M = P^{-1} M_G(x_g) P$, where P is an appropriate permutation matrix. Thus, $\Theta_G(x_g)$ is invariant under any reordering of the elements of G. For a finite group G, let $\widehat{G}$ be a complete set of representatives of the equivalence classes of irreducible representations of G over $\mathbb{C}$. Around 1880, for the case that G is abelian, Dedekind gave the irreducible factorization of $\Theta_G(x_g)$ over $\mathbb{C}$: *Let G be a finite abelian group. Then*

$$\Theta_G(x_g) = \prod_{\chi \in \widehat{G}} \sum_{g \in G} \chi(g) x_g.$$

This is called Dedekind's theorem. In 1896, Frobenius [3] gave the irreducible factorization of $\Theta_G(x_g)$ over $\mathbb{C}$ for any finite group: *Let G be a finite group. Then*

$$\Theta_G(x_g) = \prod_{\varphi \in \widehat{G}} \det\left(\sum_{g \in G} \varphi(g) x_g\right)^{\deg \varphi}.$$

This is the most well known generalization of Dedekind's theorem. This generalization is obtained from the decomposition of the regular representation L of G as a direct sum of irreducible representations and the expression $M_G(x_g) = \sum_{g \in G} x_g L(g)$. Frobenius created the character theory of finite groups in the process of obtaining the irreducible factorization. For the history on the theory, see, e.g., [2, 4, 5, 6, 20]. On the other hand, another generalization of Dedekind's theorem was given in [21]: *Let G be a finite abelian group and let H be a subgroup of G. For every $h \in H$, there exists a homogeneous polynomial $A_h \in \mathbb{C}[x_g]$ satisfying $\deg A_h = |G/H|$ and*

$$\Theta_G(x_g) = \prod_{\chi \in \widehat{H}} \sum_{h \in H} \chi(h) A_h = \Theta_H(A_h). \tag{1}$$

If $H = G$, then we can take $A_h = x_h$ for each $h \in H$. This generalization shows that the group determinant of an abelian group can be written by the group determinant of any subgroup. Let $\mathrm{C}_n = \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}$ be the cyclic group of order n. The matrix $M_{\mathrm{C}_n}(x_g)$ is similar to the circulant matrix of order n. That is, the circulant determinant is a special case of the group determinant. For the circulant determinant, Laquer [12, Theorem 2] gave the following factorization in 1980: *Let $n = rs$, where r and s are relatively prime, and let $x_j := x_{\overline{j-1}}$ for any $1 \leq j \leq n$. Then*

$$\Theta_{\mathrm{C}_n}(x_j) = \prod_{l=0}^{s-1} \Theta_{\mathrm{C}_r}\left(y_j^l\right), \quad y_j^l := \sum_{k=0}^{s-1} \zeta_s^{l(kr+j-1)} x_{kr+j},$$

where ζ_s is a primitive s-th root of unity. We call this theorem Laquer's theorem. In recently, Laquer's theorem was generalized as follows [24, Theorem 1.1]: *Let $G = H \times K$ be a direct product of finite abelian groups. Then we have*

$$\Theta_G(x_g) = \prod_{\chi \in \widehat{K}} \Theta_H(y_h^\chi), \quad y_h^\chi = \sum_{k \in K} \chi(k) x_{hk}. \tag{2}$$

In this paper, we give a refinement of (1), which is a generalization of (2).

Theorem 1.1. *Let G be a finite abelian group, let H be a subgroup of G and let*

$$\widehat{G}_H := \left\{\chi \in \widehat{G} \mid \chi(h) = 1,\ h \in H\right\}, \quad G = \bigsqcup_{t \in T} tH, \quad \widehat{G} = \bigsqcup_{\chi \in X} \chi \widehat{G}_H.$$

Then we have

$$\Theta_G(x_g) = \prod_{\chi \in X} \Theta_{G/H}(y_{tH}^\chi) = \Theta_H(z_h),$$

where

$$y_{tH}^\chi := \sum_{h \in H} \chi(th) x_{th}, \quad z_h := \frac{1}{|H|} \sum_{\chi \in X} \chi(h^{-1}) \Theta_{G/H}(y_{tH}^\chi).$$

For any $f(x_g) \in \mathbb{Z}[x_g]$, we denote by $f(x_g)_h$ the sum of all monomials $cx_{g_1}x_{g_2}\cdots x_{g_k}$ in $f(x_g)$ satisfying $g_1g_2\cdots g_k = h$. The following theorem gives another expression for z_h in Theorem **1.1**. When calculating z_h, the expression for z_h in the following theorem might be more useful than one in Theorem **1.1** (see Example **2.3**).

Theorem 1.2. *Let $y_{tH} := \sum_{h \in H} x_{th}$. Then we have*

$$z_h = \Theta_{G/H}(y_{tH})_h \in \mathbb{Z}[x_g].$$

Theorem **1.1** is a refinement of (1) since $\{\chi|_H \mid \chi \in X\} = \widehat{H}$ holds and we can take $A_h = z_h$ in (1). Note that for a finite abelian group G and any subgroup K, there exists a subgroup H of G satisfying $K \cong G/H$. That is, Theorem **1.1** implies that $\Theta_G(x_g)$ can also be expressed as a product of the group determinants of any subgroup. Thus, Theorem **1.1** derives (2). We apply Theorems **1.1** and **1.2** to the study of the integer group determinant.

A group determinant called an integer group determinant when its variables are integers. For a finite group G, let

$$S(G) := \{\Theta_G(x_g) \mid x_g \in \mathbb{Z}\}.$$

It immediately follows from $M_G(x_g) = \sum_{g \in G} x_g L(g)$ that $S(G)$ is a monoid. Determining $S(G)$ is an open problem. For the $G = \mathrm{C}_n$ cases, determining $S(G)$ is called Olga Taussky-Todd's circulant problem since Olga Taussky-Todd suggested it at the meeting of the American Mathematical Society in Hayward, California [14]. Even Olga Taussky-Todd's circulant problem remains as an open problem.

For $S(\mathrm{C}_n)$, the following relation is known [10, Lemma 3.6]: *Let $n, q \geq 1$. If $q \mid n$, then*

$$S(\mathrm{C}_n) \subset S(\mathrm{C}_q). \tag{3}$$

From Theorems **1.1** and **1.2**, we obtain a generalization of (3).

Corollary 1.3. *Let G be a finite abelian group and let H be a subgroup of G. Then*

$$S(G) \subset S(H).$$

Corollary **1.3** is generalized as follows.

Theorem 1.4. *Let G be a finite group and let H be an abelian subgroup of G. Then*

$$\left\{\alpha^{[G:H]} \mid \alpha \in S(H)\right\} \subset S(G) \subset S(H),$$

where $[G : H]$ is the index of H in G.

For some types of groups, the problem was solved in [1, 10, 12, 13, 14, 15, 18, 19, 25, 28]. As a result, for every group G of order at most 15, $S(G)$ is determined (see [15, 19]). For the groups of order 16, the complete descriptions of $S(G)$ were obtained for D_{16} [1, Theorem 5.3], C_{16} [25] and C_2^4 [28], where D_n denotes the dihedral group of order n.

Laquer [12] determined $S(\mathrm{C}_{2p})$, where p is an odd prime, by using Laquer's theorem which provides an expression for the integer circulant determinant of C_{2p} as a product of two integer circulant determinants of C_p. In [28], $S(\mathrm{C}_2^4)$ is determined by using (2) which provides an expression for the integer group determinant of C_2^n as a product of two integer group determinants of C_2^{n-1}. We can generalize these approaches by using Theorem **1.1** to determine $S(G)$ for any abelian groups. There are fourteen groups of order 16 up to isomorphism [7, 30], and five of them are abelian. The unsolved abelian groups of order 16 are $\mathrm{C}_8 \times \mathrm{C}_2$, C_4^2 and $\mathrm{C}_4 \times \mathrm{C}_2^2$. By applying Theorem **1.1**, we determine $S(\mathrm{C}_8 \times \mathrm{C}_2)$.

Theorem 1.5. *Let* $A := \{(8k-3)(8l-3) \mid k, l \in \mathbb{Z},\ k \equiv l \pmod 2\} \subsetneq \{16m - 7 \mid m \in \mathbb{Z}\}$. *Then we have*

$$\begin{aligned} S\left(\mathrm{C}_8 \times \mathrm{C}_2\right) = &\left\{16m+1,\ m',\ 2^{10}(2m+1),\ 2^{12}m \mid m \in \mathbb{Z},\ m' \in A\right\} \\ &\cup \left\{2^{11}p(2m+1) \mid p = a^2+b^2 \equiv 1,\ a+b \equiv \pm 3 \pmod 8,\ m \in \mathbb{Z}\right\} \\ &\cup \left\{2^{11}p(2m+1) \mid p \equiv -3 \pmod 8,\ m \in \mathbb{Z}\right\} \\ &\cup \left\{2^{11}p^2(2m+1) \mid p \equiv 3 \pmod 8,\ m \in \mathbb{Z}\right\}, \end{aligned}$$

where p *denotes a prime.*

The remaining two abelian groups could also be solved by using Theorem **1.1**. (While this paper under review, it have been solved in [26, 29]. Also, as for non-abelian groups of order 16, $\mathrm{D}_8 \times \mathrm{C}_2$, $\mathrm{Q}_8 \times \mathrm{C}_2$ [16, Theorems 3.1 and 4.1], Q_{16} [17] and $\mathrm{C}_2^2 \rtimes \mathrm{C}_4$ [27] have been solved, where Q_n denotes the generalized quaternion group of order n.)

Pinner and Smyth [19, p.427] noted the following inclusion relations for all groups of order 8:

$$S(\mathrm{C}_2^3) \subsetneq S(\mathrm{C}_4 \times \mathrm{C}_2) \subsetneq S(\mathrm{Q}_8) \subsetneq S(\mathrm{D}_8) \subsetneq S(\mathrm{C}_8).$$

From preceding results and Theorem **1.5**, we have

$$S(\mathrm{C}_2^4) \subsetneq S(\mathrm{C}_8 \times \mathrm{C}_2) \subsetneq S(\mathrm{D}_{16}) \subsetneq S(\mathrm{C}_{16}).$$

Determining the integer group determinants aims to investigate the structure of a group by means of the group determinant. It is expected that individual new results will help us understand more about groups.

This paper is organized as follows. In Section **2**, we prove Theorems **1.1** and **1.2**. In Sections **3** and **4**, we prove Theorems **1.4** and **1.5**, respectively.

2 Proofs of Theorems 1.1 and 1.2

For a finite group G, let x_g be an indeterminate for each $g \in G$, let $\mathbb{C}[x_g]$ be the multivariate polynomial ring in x_g over $\mathbb{C}$, let $\mathbb{C}G$ the group algebra of G over $\mathbb{C}$, and let $\mathbb{C}[x_g]G := \mathbb{C}[x_g] \otimes \mathbb{C}G = \left\{\sum_{g \in G} A_g g \mid A_g \in \mathbb{C}[x_g]\right\}$ be the group algebra of G over $\mathbb{C}[x_g]$. Also, for a finite abelian group G and a subgroup H of G, let

$$\widehat{G}_H := \left\{\chi \in \widehat{G} \mid \chi(h) = 1,\ h \in H\right\}.$$

It is easily verified that $\widehat{G}_H = \left\{\varphi \circ \pi \mid \varphi \in \widehat{G/H}\right\}$, where $\pi : G \to G/H$ is the canonical homomorphism. To prove Theorem **1.1**, we use the following lemma.

Lemma 2.1 ([21, Lemma 3.6])**.** *Let G be a finite abelian group and H be a subgroup of G. For every $h \in H$, there exists a homogeneous polynomial $A_h \in \mathbb{C}[x_g]$ satisfying* $\deg A_h = |G/H|$ *and*

$$\prod_{\chi \in \widehat{G}_H} \sum_{g \in G} \chi(g) x_g g = \sum_{h \in H} A_h h \in \mathbb{C}[x_g]H.$$

If $H = G$, then we can take $A_h = x_h$ for each $h \in H$.

Proof of Theorem **1.1***.* From Dedekind's theorem, we have

$$\begin{aligned}
\Theta_G(x_g) &= \prod_{\chi \in \widehat{G}} \sum_{g \in G} \chi(g) x_g \\
&= \prod_{\chi \in X} \prod_{\chi' \in \widehat{G}_H} \sum_{t \in T} \sum_{h \in H} (\chi\chi')(th) x_{th} \\
&= \prod_{\chi \in X} \prod_{\chi' \in \widehat{G}_H} \sum_{t \in T} \chi'(t) \sum_{h \in H} \chi(th) x_{th} \\
&= \prod_{\chi \in X} \prod_{\chi' \in \widehat{G/H}} \sum_{tH \in G/H} \chi'(tH) y^{\chi}_{tH} \\
&= \prod_{\chi \in X} \Theta_{G/H}(y^{\chi}_{tH}).
\end{aligned}$$

Next, we show that for any $\chi \in X$, there exists $A_h \in \mathbb{C}[x_g]$ satisfying

$$\Theta_{G/H}(y^{\chi}_{tH}) = \sum_{h \in H} \chi(h) A_h.$$

For any $\chi \in X$, let $F_\chi \colon \mathbb{C}[x_g]G \to \mathbb{C}[x_g]G$ be the $\mathbb{C}[x_g]$-algebra homomorphism defined by $F_\chi(g) = \chi(g)g$. Then, from Lemma **2.1**, there exists $A_h \in \mathbb{C}[x_g]$ satisfying

$$\begin{aligned}
\sum_{h \in H} \chi(h) A_h h &= F_\chi\left(\sum_{h \in H} A_h h\right) \\
&= F_\chi\left(\prod_{\chi' \in \widehat{G}_H} \sum_{g \in G} \chi'(g) x_g g\right) \\
&= F_\chi\left(\prod_{\chi' \in \widehat{G}_H} \sum_{t \in T} \sum_{h \in H} \chi'(t) x_{th} th\right) \\
&= \prod_{\chi' \in \widehat{G}_H} \sum_{t \in T} \sum_{h \in H} \chi'(t) \chi(th) x_{th} th.
\end{aligned}$$

Let $F\colon \mathbb{C}[x_g]G \to \mathbb{C}[x_g]$ be the $\mathbb{C}[x_g]$-algebra homomorphism defined by $F(g) = 1$. Applying F to the both sides of the above, we have

$$\sum_{h\in H} \chi(h)A_h = \prod_{\chi'\in \widehat{G}_H} \sum_{t\in T} \sum_{h\in H} \chi'(t)\chi(th)x_{th} = \prod_{\chi'\in \widehat{G/H}} \sum_{tH\in G/H} \chi'(tH)y^{\chi}_{tH} = \Theta_{G/H}(y^{\chi}_{tH}).$$

From the above, it follows that there exists $A_h \in \mathbb{C}[x_g]$ satisfying

$$\Theta_G(x_g) = \prod_{\chi\in X} \Theta_{G/H}(y^{\chi}_{tH}) = \prod_{\chi\in X} \sum_{h\in H} \chi(h)A_h = \prod_{\chi\in \widehat{H}} \sum_{h\in H} \chi(h)A_h = \Theta_H(A_h). \tag{4}$$

Finally, we show that A_h in (4) is expressed as

$$A_h = \frac{1}{|H|} \sum_{\chi\in X} \chi(h^{-1})\Theta_{G/H}(y^{\chi}_{tH})$$

for any $h \in H$. From orthogonality relations for characters, for any $h \in H$, we have

$$\begin{aligned}
\sum_{\chi\in X} \chi(h^{-1})\Theta_{G/H}(y^{\chi}_{tH}) &= \sum_{\chi\in X} \chi(h^{-1}) \sum_{h'\in H} \chi(h')A_{h'} \\
&= \sum_{\chi\in X} \sum_{h'\in H} \chi(h^{-1}h')A_{h'} \\
&= \sum_{h'\in H} \sum_{\chi\in \widehat{H}} \chi(h^{-1}h')A_{h'} \\
&= |H|A_h.
\end{aligned}$$

□

Remark 2.2. *From the proof of Theorem* **1.1**, *A_h in Lemma* **2.1** *equals to z_h in Theorem* **1.1**.

Proof of Theorem **1.2**. From Lemma **2.1** and Remark **2.2**, we have

$$\sum_{h\in H} z_h h = \prod_{\chi\in \widehat{G}_H} \sum_{g\in G} \chi(g)x_g g = \prod_{\chi\in \widehat{G/H}} \sum_{g\in G} \chi(gH)x_g g = \prod_{\chi\in \widehat{G/H}} \sum_{tH\in G/H} \sum_{h'\in H} \chi(tH)x_{th'}th'.$$

Therefore, we have

$$z_h = \left(\prod_{\chi\in \widehat{G/H}} \sum_{tH\in G/H} \chi(tH) \sum_{h'\in H} x_{th'} \right)_h = \Theta_{G/H}(y_{tH})_h \in \mathbb{Z}[x_g].$$

□

From Theorems **1.1** and **1.2**, we can take $z_h \in \mathbb{Z}[x_g]$ satisfying $\Theta_G(x_g) = \Theta_H(z_h)$. Thus, Corollary **1.3** is obtained.

Example 2.3. *Using Theorems* **1.1** *and* **1.2**, *we calculate* $\Theta_{\mathrm{C}_4}(x_g)$. *Let* $G = \mathrm{C}_4$ *and* $H = \{\overline{0}, \overline{2}\}$. *Then,* $G/H = \{\overline{0}H, \overline{1}H\}$. *We write* $x_{\overline{i}}$ *as* x_i *for any* $0 \leq i \leq 3$. *From Theorem* **1.2**, *we have*

$$z_{\overline{0}} = \Theta_{G/H}(y_{tH})_{\overline{0}} = x_0^2 + x_2^2 - 2x_1x_3, \quad z_{\overline{2}} = \Theta_{G/H}(y_{tH})_{\overline{2}} = 2x_0x_2 - x_1^2 - x_3^2$$

since $y_{\overline{0}H} = x_0 + x_2$, $y_{\overline{1}H} = x_1 + x_3$ *and*

$$\Theta_{G/H}(y_{tH}) = y_{\overline{0}H}^2 - y_{\overline{1}H}^2 = \left(x_0^2 + 2x_0x_2 + x_2^2\right) - \left(x_1^2 + 2x_1x_3 + x_3^2\right).$$

Therefore, from Theorem **1.1**, *we have*

$$\Theta_G(x_g) = \Theta_H(z_h) = z_{\overline{0}}^2 - z_{\overline{2}}^2 = \left(x_0^2 + x_2^2 - 2x_1x_3\right)^2 - \left(2x_0x_2 - x_1^2 - x_3^2\right)^2.$$

3 Proof of Theorem 1.4

The lower bound in Theorem **1.4** is derived from [23, Lemma 3.2]. Also, the upper bound immediately follows from the following lemma essentially provided in [22, Theorem 1.4].

Lemma 3.1. *Let* G *be a finite group and let* H *be an abelian subgroup of* G. *Then, there exists a homogeneous polynomial* $A_h \in \mathbb{Z}[x_g]$ *satisfying* $\deg A_h = [G : H]$ *and*

$$\Theta_G(x_g) = \Theta_H(A_h),$$

where $[G : H]$ *is the index of* H *in* G.

The proof in [22] is not concise. We give a brief proof of Lemma **3.1**. For the purpose, we use the following identity [9, p. 82, Theorem 2.6]; see also [8, 11]: *Given the block matrix* M *of the form*

$$\begin{pmatrix} M_{11} & M_{12} & \cdots & M_{1n} \\ M_{21} & M_{22} & \cdots & M_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ M_{n1} & M_{n2} & \cdots & M_{nn} \end{pmatrix},$$

where the matrices M_{ij} *are pairwise commuting of size* $m \times m$ *then*

$$\det M = \det\left(\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) M_{1\sigma(1)} M_{2\sigma(2)} \cdots M_{n\sigma(n)}\right).$$

Proof of Lemma **3.1**. Let $G = \{g_1, g_2, \ldots, g_{mn}\}$, let $H = \{h_1, h_2, \ldots, h_m\}$ and let $G = t_1H \sqcup t_2H \sqcup \cdots \sqcup t_nH$, where $g_i = t_kh_l \in G$ with $i = (k-1)m + l$ for $1 \leq k \leq n$ and $1 \leq l \leq m$. Then, the group matrix $\left(x_{g_ig_j^{-1}}\right)_{1 \leq i,j \leq mn}$ of G can be expressed as the block matrix:

$$\left(x_{g_ig_j^{-1}}\right)_{1 \leq i,j \leq mn} = (M_{kl})_{1 \leq k,l \leq n},$$

where M_{kl} is the matrix obtained by replacing each $x_{h_i h_j^{-1}}$ in the group matrix $\left(x_{h_i h_j^{-1}}\right)_{1\leq i,j\leq m}$ of H to $x_{(t_k h_i)(t_l h_j)^{-1}}$. That is, $M_{kl} = \left(x_{(t_k h_i)(t_l h_j)^{-1}}\right)_{1\leq i,j\leq m}$. Since H is abelian, M_{kl} are pairwise commuting. Therefore, there exists $A_h \in \mathbb{Z}[x_g]$ satisfying

$$\Theta_G(x_g) = \det\left(x_{g_i g_j^{-1}}\right)_{1\leq i,j\leq mn} = \det\left(\sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) M_{1\sigma(1)} M_{2\sigma(2)} \cdots M_{n\sigma(n)}\right) = \Theta_H(A_h)$$

since $\sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) M_{1\sigma(1)} M_{2\sigma(2)} \cdots M_{n\sigma(n)}$ is also of the form of a group matrix of H. □

4 Proof of Theorem 1.5

In this section, by applying Theorem **1.1**, we determine $S(\mathrm{C}_8 \times \mathrm{C}_2)$.

4.1 Relations with group determinants of subgroups

We denote the variable $x_{\overline{i}}$ by x_i for any $\overline{i} \in \mathrm{C}_n$ and let $D_n(x_0, x_1, \ldots, x_{n-1}) := \Theta_{\mathrm{C}_n}(x_g)$. Also, for any $g = (\overline{r}, \overline{s}) \in \mathrm{C}_8 \times \mathrm{C}_2$ with $r \in \{0, 1, \ldots, 7\}$ and $s \in \{0, 1\}$, we denote the variable y_g by y_j, where $j := r + 8s$, and let $D_{8\times 2}(y_0, y_1, \ldots, y_{15}) := \Theta_{\mathrm{C}_8\times\mathrm{C}_2}(y_g)$. From the $G = \mathrm{C}_8 \times \mathrm{C}_2$ and $H = \left\{(\overline{0}, \overline{0}), (\overline{0}, \overline{1})\right\}$ case of Theorem **1.1**, we have

$$D_{8\times 2}(y_0, \ldots, y_{15}) = D_8(y_0 + y_8, \ldots, y_7 + y_{15}) D_8(y_0 - y_8, \ldots, y_7 - y_{15}).$$

Let ζ_n be a primitive n-th root of unity. From the $G = \mathrm{C}_8$ and $H = \left\{\overline{0}, \overline{4}\right\}$ case of Theorem **1.1**, we have

$$\begin{aligned} D_8(x_0, x_1, \ldots, x_7) &= D_4(x_0 + x_4, x_1 + x_5, x_2 + x_6, x_3 + x_7) \\ &\quad \times D_4(x_0 - x_4, \zeta_8(x_1 - x_5), \zeta_8^2(x_2 - x_6), \zeta_8^3(x_3 - x_7)). \end{aligned}$$

From the $G = \mathrm{C}_4$ and $H = \left\{\overline{0}, \overline{2}\right\}$ case of Theorem **1.1**, we have

$$\begin{aligned} D_4(x_0, x_1, x_2, x_3) &= D_2(x_0 + x_2, x_1 + x_3) D_2(x_0 - x_2, \zeta_4(x_1 - x_3)) \\ &= D_2(x_0^2 + x_2^2 - 2x_1x_3, -x_1^2 - x_3^2 + 2x_0x_2). \end{aligned}$$

Let $\widetilde{D}_4(x_0, x_1, x_2, x_3) := D_4(x_0, \zeta_8 x_1, \zeta_8^2 x_2, \zeta_8^3 x_3)$. Then we have the following lemma.

Lemma 4.1. *The following hold:*

(1) $D_4(x_0, x_1, x_2, x_3) = \{(x_0 + x_2)^2 - (x_1 + x_3)^2\}\{(x_0 - x_2)^2 + (x_1 - x_3)^2\}$;

(2) $\widetilde{D}_4(x_0, x_1, x_2, x_3) = (x_0^2 - x_2^2 + 2x_1x_3)^2 + (x_1^2 - x_3^2 - 2x_0x_2)^2$.

Lemma **4.1** (2) shows that $\widetilde{D}_4(x_0, x_1, x_2, x_3) \in \mathbb{Z}$ holds for any $x_0, x_1, x_2, x_3 \in \mathbb{Z}$. Throughout this paper, we assume that $a_0, a_1, \ldots, a_{15} \in \mathbb{Z}$, and for any $0 \leq i \leq 3$, put

$$b_i := (a_i + a_{i+8}) + (a_{i+4} + a_{i+12}), \qquad c_i := (a_i + a_{i+8}) - (a_{i+4} + a_{i+12}),$$
$$d_i := (a_i - a_{i+8}) + (a_{i+4} - a_{i+12}), \qquad e_i := (a_i - a_{i+8}) - (a_{i+4} - a_{i+12}).$$

Also, let $\boldsymbol{a} := (a_0, a_1, \ldots, a_{15})$ and let

$$\boldsymbol{b} := (b_0, b_1, b_2, b_3), \quad \boldsymbol{c} := (c_0, c_1, c_2, c_3), \quad \boldsymbol{d} := (d_0, d_1, d_2, d_3), \quad \boldsymbol{e} := (e_0, e_1, e_2, e_3).$$

The following relations will be frequently used in this paper:

$$\begin{aligned} D_{8\times 2}(\boldsymbol{a}) &= D_8(a_0 + a_8, a_1 + a_9, \ldots, a_7 + a_{15}) D_8(a_0 - a_8, a_1 - a_9, \ldots, a_7 - a_{15}) \\ &= D_4(\boldsymbol{b}) \widetilde{D}_4(\boldsymbol{c}) D_4(\boldsymbol{d}) \widetilde{D}_4(\boldsymbol{e}). \end{aligned}$$

Remark 4.2. *For any $0 \leq i \leq 3$, the following hold:*

(1) $b_i \equiv c_i \equiv d_i \equiv e_i \pmod 2$*;*

(2) $b_i + c_i + d_i + e_i \equiv 0 \pmod 4$*.*

Lemma 4.3. *We have $D_{8\times 2}(\boldsymbol{a}) \equiv D_4(\boldsymbol{b}) \equiv \widetilde{D}_4(\boldsymbol{c}) \equiv D_4(\boldsymbol{d}) \equiv \widetilde{D}_4(\boldsymbol{e}) \pmod 2$.*

Proof. From Lemma **4.1**, we have $D_4(x_0, x_1, x_2, x_3) \equiv x_0 + x_1 + x_2 + x_3 \equiv \widetilde{D}_4(x_0, x_1, x_2, x_3) \pmod 2$. Therefore, from Remark **4.2** (1), the lemma is proved. □

4.2 Impossible odd numbers

Let $\mathbb{Z}_{\text{odd}}$ be the set of all odd numbers and $A := \{(8k-3)(8l-3) \mid k, l \in \mathbb{Z},\ k \equiv l \pmod 2\}$.

Lemma 4.4. *We have $S(\mathrm{C}_8 \times \mathrm{C}_2) \cap \mathbb{Z}_{\text{odd}} \subset \{16m + 1 \mid m \in \mathbb{Z}\} \cup A$.*

To prove Lemma **4.4**, we use the following three lemmas.

Lemma 4.5. *We have*

$$\begin{aligned} &D_4(\boldsymbol{b}) \widetilde{D}_4(\boldsymbol{c}) D_4(\boldsymbol{d}) \widetilde{D}_4(\boldsymbol{e}) \\ &\quad = D_4(b_1, b_2, b_3, b_0) \widetilde{D}_4(c_1, c_2, c_3, -c_0) D_4(d_1, d_2, d_3, d_0) \widetilde{D}_4(e_1, e_2, e_3, -e_0) \\ &\quad = D_4(b_2, b_3, b_0, b_1) \widetilde{D}_4(c_2, c_3, -c_0, -c_1) D_4(d_2, d_3, d_0, d_1) \widetilde{D}_4(e_2, e_3, -e_0, -e_1) \\ &\quad = D_4(b_3, b_0, b_1, b_2) \widetilde{D}_4(c_3, -c_0, -c_1, -c_2) D_4(d_3, d_0, d_1, d_2) \widetilde{D}_4(e_3, -e_0, -e_1, -e_2). \end{aligned}$$

Proof. From Lemma **4.1**, we have

$$D_4(x_0, x_1, x_2, x_3) = -D_4(x_1, x_2, x_3, x_0), \quad \widetilde{D}_4(x_0, x_1, x_2, x_3) = \widetilde{D}_4(x_1, x_2, x_3, -x_0).$$

Therefore, the lemma is proved. □

Lemma 4.6. *For any $k, l, m, n \in \mathbb{Z}$, the following hold:*

(1) $D_4(2k+1, 2l, 2m, 2n) \equiv 8m+1 \pmod{16}$;

(2) $\widetilde{D}_4(2k+1, 2l, 2m, 2n) \equiv 8m+1 \pmod{16}$.

Proof. Let $D := D_4(2k+1, 2l, 2m, 2n)$ and $\widetilde{D} := \widetilde{D}_4(2k+1, 2l, 2m, 2n)$. Then we have

$$\begin{aligned} D &= \left\{4(k+m)^2 + 4(k+m) + 1 - 4(l+n)^2\right\}\left\{4(k-m)^2 + 4(k-m) + 1 + 4(l-n)^2\right\} \\ &\equiv 8m+1 \pmod{16}, \\ \widetilde{D} &= \left\{4k(k+1) + 1 - 4m^2 + 8ln\right\}^2 + \left\{4l^2 - 4n^2 - 8km - 4m\right\}^2 \\ &\equiv 8m+1 \pmod{16}. \end{aligned}$$

□

Lemma 4.7. *For any $k, l, m, n \in \mathbb{Z}$, the following hold:*

(1) $D_4(2k, 2l+1, 2m+1, 2n+1) \equiv 8(k+l+n) - 3 \pmod{16}$;

(2) $\widetilde{D}_4(2k, 2l+1, 2m+1, 2n+1) \equiv 8(k+l+n) + 1 \pmod{16}$.

Proof. Let $D := D_4(2k, 2l+1, 2m+1, 2n+1)$ and $\widetilde{D} := \widetilde{D}_4(2k, 2l+1, 2m+1, 2n+1)$. Then,

$$\begin{aligned} D &= \left\{4(k+m)^2 + 4(k+m) + 1 - 4(l+n+1)^2\right\}\left\{4(k-m)^2 - 4(k-m) + 1 + 4(l-n)^2\right\} \\ &\equiv 8(k+l+n) - 3 \pmod{16}, \\ \widetilde{D} &= \left\{4k^2 - 4m(m+1) + 8ln + 4l + 4n + 1\right\}^2 + \{4l(l+1) - 4n(n+1) - 8km - 4k\}^2 \\ &\equiv 8(k+l+n) + 1 \pmod{16}. \end{aligned}$$

□

Proof of Lemma **4.4**. Let $D_{8\times 2}(\boldsymbol{a}) = D_4(\boldsymbol{b})\widetilde{D}_4(\boldsymbol{c})D_4(\boldsymbol{d})\widetilde{D}_4(\boldsymbol{e}) \in \mathbb{Z}_{\mathrm{odd}}$. Then, $b_0 + b_2 \not\equiv b_1 + b_3 \pmod{2}$ holds since $D_4(\boldsymbol{b})$ is odd. We prove the following:

(i) If exactly three of b_0, b_1, b_2, b_3 are even, then $D_{8\times 2}(\boldsymbol{a}) \in \{16m+1 \mid m \in \mathbb{Z}\}$;

(ii) If exactly one of b_0, b_1, b_2, b_3 is even, then $D_{8\times 2}(\boldsymbol{a}) \in A$.

First, we prove (i). If $\boldsymbol{b} \equiv (1,0,0,0) \pmod{2}$, then there exist $m_i \in \mathbb{Z}$ satisfying $b_2 = 2m_0$, $c_2 = 2m_1$, $d_2 = 2m_2$, $e_2 = 2m_3$ and $\sum_{i=0}^{3} m_i \equiv 0 \pmod{2}$ from Remark **4.2**. Therefore, from Lemma **4.6**, $D_{8\times 2}(\boldsymbol{a}) \equiv \prod_{i=0}^{3}(8m_i + 1) \equiv 8\sum_{i=0}^{3} m_i + 1 \equiv 1 \pmod{16}$. From this and Lemma **4.5**, the remaining three cases are also proved. Next, we prove (ii). If $\boldsymbol{b} \equiv (0,1,1,1) \pmod{2}$, then there exist $k_i, l_i, n_i \in \mathbb{Z}$ satisfying $(b_0, b_1, b_3) = (2k_0, 2l_0+1, 2n_0+1)$, $(c_0, c_1, c_3) = (2k_1, 2l_1+1, 2n_1+1)$, $(d_0, d_1, d_3) = (2k_2, 2l_2+1, 2n_2+1)$, $(e_0, e_1, e_3) = (2k_3, 2l_3+1, 2n_3+1)$ and $\sum_{i=0}^{3} k_i \equiv \sum_{i=0}^{3} l_i \equiv \sum_{i=0}^{3} n_i \equiv 0 \pmod{2}$ from Remark **4.2**. Therefore, from Lemma **4.7**, we have $D_4(\boldsymbol{b})\widetilde{D}_4(\boldsymbol{c}) \equiv (8r_0 - 3)(8r_1 + 1) \equiv 8r_0 + 8r_1 - 3 \pmod{16}$ and $D_4(\boldsymbol{d})\widetilde{D}_4(\boldsymbol{e}) \equiv (8r_2 - 3)(8r_3 + 1) \equiv 8r_2 + 8r_3 - 3 \pmod{16}$, where $r_i := k_i + l_i + n_i$. Thus, there exist $s_0, s_1 \in \mathbb{Z}$ satisfying $D_4(\boldsymbol{b})\widetilde{D}_4(\boldsymbol{c}) = 16s_0 + 8r_0 + 8r_1 - 3$, $D_4(\boldsymbol{d})\widetilde{D}_4(\boldsymbol{e}) = 16s_1 + 8r_2 + 8r_3 - 3$. Let $k := 2s_0 + r_0 + r_1$ and $l := 2s_1 + r_2 + r_3$. Then $D_{8\times 2}(\boldsymbol{a}) = (8k-3)(8l-3) \in A$ since $k \equiv l \pmod{2}$ holds from $\sum_{i=0}^{3} r_i \equiv 0 \pmod{2}$. From this and Lemma **4.5**, the remaining three cases are also proved. □

4.3 Impossible even numbers

We will use Kaiblinger's [10, Theorem 1.1] results $S(\mathrm{C}_4) = \mathbb{Z}_{\mathrm{odd}} \cup 2^4\mathbb{Z}$ and $S(\mathrm{C}_8) = \mathbb{Z}_{\mathrm{odd}} \cup 2^5\mathbb{Z}$.

Lemma 4.8. *We have* $S(\mathrm{C}_8 \times \mathrm{C}_2) \cap 2\mathbb{Z} \subset 2^{10}\mathbb{Z}$.

Proof. Let $D_{8\times2}(\boldsymbol{a}) = D_8(a_0 + a_8, \ldots, a_7 + a_{15})D_8(a_0 - a_8, \ldots, a_7 - a_{15}) \in 2\mathbb{Z}$. Since $D_8(a_0 + a_8, \ldots, a_7 + a_{15}) \equiv D_8(a_0 - a_8, \ldots, a_7 - a_{15}) \pmod 2$ holds from $a_i + a_{i+8} \equiv a_i - a_{i+8} \pmod 2$, we have $D_8(a_0 + a_8, \ldots, a_7 + a_{15}), D_8(a_0 - a_8, \ldots, a_7 - a_{15}) \in S(\mathrm{C}_8) \cap 2\mathbb{Z} = 2^5\mathbb{Z}$. Therefore, $D_{8\times2}(\boldsymbol{a}) \in 2^{10}\mathbb{Z}$. □

Lemma 4.9. *Let* $p_i = a_i^2 + b_i^2 \equiv 1 \pmod 8$ *be a prime with* $a_i \pm b_i \in \{8m \pm 1 \mid m \in \mathbb{Z}\}$ *for each* $1 \leq i \leq r$*, let* $p_{r+1}, \ldots, p_{r+s} \equiv -1 \pmod 8$ *be primes, let* $q_1, \ldots, q_t \equiv 3 \pmod 8$ *be distinct primes, and let* $k_1, \ldots, k_{r+s}$ *be non-negative integers. Then*

$$2^{11}p_1^{k_1} \cdots p_r^{k_r} p_{r+1}^{k_{r+1}} \cdots p_{r+s}^{k_{r+s}} Q \notin S(\mathrm{C}_8 \times \mathrm{C}_2)$$

for any $Q \in \{\pm1,\ \pm q_1 \cdots q_t\}$.

Let

$$\alpha_0 := (b_0 + b_2)^2 - (b_1 + b_3)^2, \qquad \alpha_1 := (b_0 - b_2)^2 + (b_1 - b_3)^2,$$
$$\alpha_2 := (d_0 + d_2)^2 - (d_1 + d_3)^2, \qquad \alpha_3 := (d_0 - d_2)^2 + (d_1 - d_3)^2,$$
$$\beta := (c_0^2 - c_2^2 + 2c_1c_3) - \zeta_4(c_1^2 - c_3^2 - 2c_0c_2), \qquad \gamma := (e_0^2 - e_2^2 + 2e_1e_3) - \zeta_4(e_1^2 - e_3^2 - 2e_0e_2).$$

Then we have $\alpha_0\alpha_1 = D_4(\boldsymbol{b})$, $\alpha_2\alpha_3 = D_4(\boldsymbol{d})$, $\beta\overline{\beta} = \widetilde{D}_4(\boldsymbol{c})$, $\gamma\overline{\gamma} = \widetilde{D}_4(\boldsymbol{e})$, where $\overline{x}$ denotes the complex conjugate of $x \in \mathbb{C}$. To prove Lemma **4.9**, we use the following remark and two lemmas.

Remark 4.10. *From Remark* **4.2** (1) *and*

$$\alpha_1 \in 2\mathbb{Z}_{\mathrm{odd}} \iff b_0 + b_2 \equiv b_1 + b_3 \equiv 1 \pmod 2,$$
$$\alpha_3 \in 2\mathbb{Z}_{\mathrm{odd}} \iff d_0 + d_2 \equiv d_1 + d_3 \equiv 1 \pmod 2,$$
$$\beta\overline{\beta} \in 2\mathbb{Z}_{\mathrm{odd}} \iff c_0 + c_2 \equiv c_1 + c_3 \equiv 1 \pmod 2,$$
$$\gamma\overline{\gamma} \in 2\mathbb{Z}_{\mathrm{odd}} \iff e_0 + e_2 \equiv e_1 + e_3 \equiv 1 \pmod 2,$$

we have $\alpha_1 \in 2\mathbb{Z}_{\mathrm{odd}} \iff \alpha_3 \in 2\mathbb{Z}_{\mathrm{odd}} \iff \beta\overline{\beta} \in 2\mathbb{Z}_{\mathrm{odd}} \iff \gamma\overline{\gamma} \in 2\mathbb{Z}_{\mathrm{odd}}$.

Lemma 4.11. *If* $D_{8\times2}(\boldsymbol{a}) \in 2^{11}\mathbb{Z}_{\mathrm{odd}}$*, then we have* $(\alpha_i, \alpha_j) \in 2^3\mathbb{Z}_{\mathrm{odd}} \times 2^4\mathbb{Z}_{\mathrm{odd}}$ *and* α_1, α_3, $\beta\overline{\beta}$, $\gamma\overline{\gamma} \in 2\mathbb{Z}_{\mathrm{odd}}$*, where* $\{i, j\} = \{0, 2\}$.

Proof. Let $D_{8\times2}(\boldsymbol{a}) = \alpha_0\alpha_1\alpha_2\alpha_3\beta\overline{\beta}\gamma\overline{\gamma} \in 2^{11}\mathbb{Z}_{\mathrm{odd}}$. Then, from Lemma **4.3**, $\alpha_0\alpha_1 \equiv \alpha_2\alpha_3 \equiv \beta\overline{\beta} \equiv \gamma\overline{\gamma} \equiv 0 \pmod 2$ holds. In particular, $\alpha_0\alpha_1, \alpha_2\alpha_3 \in S(\mathrm{C}_4) \cap 2\mathbb{Z} = 2^4\mathbb{Z}$. From this and Remark **4.10**, we have $\beta\overline{\beta}, \gamma\overline{\gamma} \in 2\mathbb{Z}_{\mathrm{odd}}$. Therefore, $\alpha_1, \alpha_3 \in 2\mathbb{Z}_{\mathrm{odd}}$. □

Lemma 4.12. *Let* $b_0 + b_2 \equiv b_1 + b_3 \equiv 1 \pmod 2$*. Then the following hold:*

(1) $\alpha_0 \equiv \alpha_1 + 4(b_0b_2 + b_1b_3) - 2 \pmod{16}$;

(2) $\alpha_2 \equiv \alpha_3 + 4(d_0d_2 + d_1d_3) - 2 \pmod{16}$;

(3) $\mathrm{Re}(\beta) \equiv (-1)^{c_2} + 2(c_0c_2 + c_1c_3) \pmod{8}$;

(4) $\mathrm{Re}(\gamma) \equiv (-1)^{e_2} + 2(e_0e_2 + e_1e_3) \pmod{8}$;

(5) $(b_0b_2 + b_1b_3) + (c_0c_2 + c_1c_3) + (d_0d_2 + d_1d_3) + (e_0e_2 + e_1e_3) \equiv 0 \pmod{4}$.

Proof. We obtain (1) from $\alpha_0 = \alpha_1 + 4(b_0b_2 + b_1b_3) - 2(b_1 + b_3)^2$. In the same way, we can obtain (2). We obtain (3) from $\mathrm{Re}(\beta) = (c_0 - c_2)^2 - 2c_2^2 + 2(c_0c_2 + c_1c_3)$. In the same way, we can obtain (4). We prove (5). There are four cases:

$$\boldsymbol{b} \equiv (0,0,1,1),\ (0,1,1,0),\ (1,1,0,0) \text{ or } (1,0,0,1) \pmod{2}.$$

If $\boldsymbol{b} \equiv (0,0,1,1) \pmod{2}$, then

$$\begin{aligned}(b_0b_2 + b_1b_3) &+ (c_0c_2 + c_1c_3) + (d_0d_2 + d_1d_3) + (e_0e_2 + e_1e_3)\\ &\equiv (b_0 + b_1) + (c_0 + c_1) + (d_0 + d_1) + (e_0 + e_1)\\ &\equiv 0 \pmod{4}\end{aligned}$$

from Remark **4.2**. In the same way, the remaining three cases can also be proved. □

Proof of Lemma **4.9**. We prove by contradiction. Assume that there exist $a_0, a_1, \ldots, a_{15} \in \mathbb{Z}$ satisfying $D_{8\times 2}(\boldsymbol{a}) = \alpha_0\alpha_1\alpha_2\alpha_3\beta\overline{\beta}\gamma\overline{\gamma} = 2^{11}p_1^{k_1}\cdots p_r^{k_r}p_{r+1}^{k_{r+1}}\cdots p_{r+s}^{k_{r+s}}Q$, where Q is ± 1 or $\pm q_1\cdots q_t$. Since α_1, α_3, $\beta\overline{\beta}$ and $\gamma\overline{\gamma}$ are integers expressible in the form $x^2 + y^2$, in the prime factorization of them, every prime of the form $4k+3$ occurs an even number of times. From this fact and Lemma **4.11**, there exist $l_f, m_f, n_f, u_f, v_f \geq 0$ satisfying

$$\begin{aligned}\alpha_i &= 2^3p_1^{k_1-l_1-w_1}\cdots p_r^{k_r-l_r-w_r}p_{r+1}^{k_{r+1}-l_{r+1}-2w_{r+1}}\cdots p_{r+s}^{k_{r+s}-l_{r+s}-2w_{r+s}}Q_1,\\ \alpha_j &= 2^4p_1^{l_1}\cdots p_r^{l_r}p_{r+1}^{l_{r+1}}\cdots p_{r+s}^{l_{r+s}}Q_2,\\ \alpha_1 &= 2p_1^{m_1}\cdots p_r^{m_r}p_{r+1}^{2m_{r+1}}\cdots p_{r+s}^{2m_{r+s}},\\ \alpha_3 &= 2p_1^{n_1}\cdots p_r^{n_r}p_{r+1}^{2n_{r+1}}\cdots p_{r+s}^{2n_{r+s}},\\ \beta\overline{\beta} &= 2p_1^{u_1}\cdots p_r^{u_r}p_{r+1}^{2u_{r+1}}\cdots p_{r+s}^{2u_{r+s}},\\ \gamma\overline{\gamma} &= 2p_1^{v_1}\cdots p_r^{v_r}p_{r+1}^{2v_r+1}\cdots p_{r+s}^{2v_{r+s}},\end{aligned}$$

where $\{i,j\} = \{0,2\}$, $w_f := m_f + n_f + u_f + v_f$ and $Q_1Q_2 = Q$. From the above, we have $\alpha_i \equiv 8, \alpha_j \equiv 0, \alpha_1 \equiv \alpha_3 \equiv 2 \pmod{16}$. Therefore, from Lemma **4.12** (1) and (2),

$$(b_0b_2 + b_1b_3, d_0d_2 + d_1d_3) \equiv (2,0) \text{ or } (0,2) \pmod{4}.$$

Note that $c_0c_2 + c_1c_3 \equiv e_0e_2 + e_1e_3 \equiv 0 \pmod{2}$ since $b_0 + b_2 \equiv b_1 + b_3 \equiv 1 \pmod{2}$. From [25, Lemma 4.8], we have $\mathrm{Re}(\beta), \mathrm{Re}(\gamma) \in \{8m \pm 1 \mid m \in \mathbb{Z}\}$. From this and Lemma **4.12** (3) and (4), it follows that $c_0c_2 + c_1c_3 \equiv e_0e_2 + e_1e_3 \equiv 0 \pmod{4}$. Therefore, we have

$$(b_0b_2 + b_1b_3) + (c_0c_2 + c_1c_3) + (d_0d_2 + d_1d_3) + (e_0e_2 + e_1e_3) \equiv 2 \pmod{4}.$$

This contradicts Lemma **4.12** (5). □

4.4 Possible numbers

Lemmas **4.4**, **4.8** and **4.9** imply that $S(\mathrm{C}_8 \times \mathrm{C}_2)$ does not include every integer that is not mentioned in Lemmas **4.13** and **4.14**.

Lemma 4.13. *For any $m, n \in \mathbb{Z}$, the following are elements of $S(\mathrm{C}_8 \times \mathrm{C}_2)$:*

(1) $16m + 1$;

(2) $(16m - 3)(16n - 3)$;

(3) $(16m + 5)(16n + 5)$;

(4) $2^{10}(2m + 1)$;

(5) $2^{12}(2m + 1)$;

(6) $2^{12}(2m)$.

Lemma 4.14. *The following hold:*

(1) *Suppose that p is a prime with $p \equiv -3 \pmod 8$, then $2^{11}p(2m + 1) \in S(\mathrm{C}_8 \times \mathrm{C}_2)$;*

(2) *Suppose that p is a prime with $p \equiv 3 \pmod 8$, then $2^{11}p^2(2m + 1) \in S(\mathrm{C}_8 \times \mathrm{C}_2)$;*

(3) *Suppose that p is a prime with $p = a^2 + b^2 \equiv 1 \pmod 8$ and $a + b \equiv \pm 3 \pmod 8$, then $2^{11}p(2m + 1) \in S(\mathrm{C}_8 \times \mathrm{C}_2)$.*

Proof of Lemma **4.13**. We obtain (1) from $D_{8\times 2}(m + 1, m, \ldots, m) = 16m + 1$. From

$$\begin{aligned}
&D_{8\times 2}(\overbrace{m + n, \ldots, m + n}^{5}, m + n - 1, m + n - 1, m + n - 1, m - n, \ldots, m - n)\\
&\quad = (16m - 3)(16n - 3),\\
&D_{8\times 2}(\overbrace{m + n + 1, \ldots, m + n + 1}^{5}, m + n, m + n, m + n, m - n, \ldots, m - n)\\
&\quad = (16m + 5)(16n + 5),
\end{aligned}$$

we obtain (2) and (3), respectively. We obtain (4) from

$$\begin{aligned}
&D_{8\times 2}(m + 1, m + 1, m + 1, m, m, m, m + 1, m, \ldots, m) = 2^{10}(4m + 1),\\
&D_{8\times 2}(\overbrace{m, \ldots, m}^{6}, m + 1, m - 1, m, m, m - 1, m, m - 1, m - 1, m, m - 1) = 2^{10}(4m - 1).
\end{aligned}$$

We obtain (5) from $D_{8\times 2}(m + 2, m, \overbrace{m + 1, \ldots, m + 1}^{6}, m, \ldots, m) = 2^{12}(2m + 1)$. From

$$\begin{aligned}
&D_{8\times 2}(m + 1, m, m, m + 1, m + 1, m, m + 1, m, m - 1, m - 1, m, m - 1, m, m, m - 1, m)\\
&\quad = 2^{12}(2m),
\end{aligned}$$

we obtain (6). $\square$

To prove Lemma **4.14**, we use the following lemma.

Lemma 4.15 ([25, Proof of Theorem 5.1])**.** *The following hold:*

(1) *Suppose that* $p \equiv -3 \pmod 8$ *is a prime, then there exist* $k, l \in \mathbb{Z}$ *satisfying*

$$2p = (8k+3)^2 + (8l+1)^2;$$

(2) *Suppose that* $p \equiv 3 \pmod 8$ *is a prime, then there exist* $k, l \in \mathbb{Z}$ *satisfying*

$$p = (4k-1)^2 + 2(4l-1)^2;$$

(3) *Suppose that* $p = a^2 + b^2 \equiv 1 \pmod 8$ *is a prime with* $a + b \equiv \pm 3 \pmod 8$*, then there exist* $k, l, m, n \in \mathbb{Z}$ *satisfying*

$$\begin{aligned} 2p = &\left\{(4k-1)^2 - (4m-2)^2 + 2(2l-1)(4n)\right\}^2 \\ &+ \left\{(2l-1)^2 - (4n)^2 - 2(4k-1)(4m-2)\right\}^2. \end{aligned}$$

Proof of Lemma **4.14**. First, we prove (1). Let

$$\begin{aligned} &a_0 = k+m+2, && a_1 = l+m+1, && a_2 = -k+m, && a_3 = -l+m+1, \\ &a_4 = k+m+1, && a_5 = l+m, && a_6 = -k+m+1, && a_7 = -l+m, \\ &a_8 = k-m, && a_9 = l-m, && a_{10} = -k-m, && a_{11} = -l-m-1, \\ &a_{12} = k-m, && a_{13} = l-m, && a_{14} = -k-m-1, && a_{15} = -l-m. \end{aligned}$$

Then $D_{8\times 2}(\boldsymbol{a}) = 2^{10}\left\{(8k+3)^2 + (8l+1)^2\right\}(2m+1)$. Therefore, from Lemma **4.15** (1), we obtain (1). We prove (2). Let

$$\begin{aligned} &a_0 = k+l+m, && a_1 = k-l+m, && a_2 = -l+m+1, && a_3 = -l+m+1, \\ &a_4 = -k-l+m+2, && a_5 = -k+l+m+1, && a_6 = l+m+1, && a_7 = l+m, \\ &a_8 = k+l-m, && a_9 = k-l-m, && a_{10} = -l-m, && a_{11} = -l-m, \\ &a_{12} = -k-l-m, && a_{13} = -k+l-m-1, && a_{14} = l-m-1, && a_{15} = l-m \end{aligned}$$

and $s := 4k-1$, $t := 4l-1$. Then $D_{8\times 2}(\boldsymbol{a}) = 2^{11}(s^2+2t^2)^2(2m+1)$. Therefore, (2) is proved from Lemma **4.15** (2). We prove (3). Let $l' := \frac{l}{2}$ if l is even; $\frac{l-1}{2}$ if l is odd and

$$\begin{aligned} &a_0 = k+r+1, && a_1 = l'+r, && a_2 = m+r, && a_3 = n+r, \\ &a_4 = -k+r+1, && a_5 = -l'+r+\frac{(-1)^l+1}{2}, && a_6 = -m+r+2, && a_7 = -n+r+1, \\ &a_8 = k-r-1, && a_9 = l'-r, && a_{10} = m-r, && a_{11} = n-r, \\ &a_{12} = -k-r, && a_{13} = -l'-r+\frac{(-1)^l-1}{2}, && a_{14} = -m-r, && a_{15} = -n-r-1. \end{aligned}$$

Then $D_{8\times 2}(\boldsymbol{a}) = 2^{10}\widetilde{D}_4(4k-1, 2l-1, 4m-2, 4n)(2r+1)$. Therefore, (3) is proved from Lemma **4.15** (3). □

From Lemmas **4.4**, **4.8**, **4.9**, **4.13** and **4.14**, Theorem **1.5** is proved.

References

[1] Ton Boerkoel and Christopher Pinner. Minimal group determinants and the Lind-Lehmer problem for dihedral groups. *Acta Arith.*, 186(4):377–395, 2018.

[2] Keith Conrad. The origin of representation theory. *Enseign. Math. (2)*, 44(3-4):361–392, 1998.

[3] Ferdinand Georg Frobenius. Über die Primfactoren der Gruppendeterminante. *Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin*, pages 1343–1382, 1896. Reprinted in *Gesammelte Abhandlungen, Band III.* Springer-Verlag Berlin Heidelberg, New York, 1968, pages 38–77.

[4] Thomas Hawkins. The origins of the theory of group characters. *Arch. History Exact Sci.*, 7(2):142–170, 1971.

[5] Thomas Hawkins. Hypercomplex numbers, lie groups, and the creation of group representation theory. *Arch. History Exact Sci.*, 8(4):243–287, 1972.

[6] Thomas Hawkins. New light on Frobenius' creation of the theory of group characters. *Arch. History Exact Sci.*, 12:217–243, 1974.

[7] Otto Hölder. Die Gruppen der Ordnungen p^3, pq^2, pqr, p^4. *Math. Ann.*, 43(2-3):301–412, 1893.

[8] M. H. Ingraham. A note on determinants. *Bull. Amer. Math. Soc.*, 43(8):579–580, 1937.

[9] K.W. Johnson. *Group Matrices, Group Determinants and Representation Theory: The Mathematical Legacy of Frobenius.* Lecture Notes in Mathematics. Springer International Publishing, 2019.

[10] Norbert Kaiblinger. Progress on Olga Taussky-Todd's circulant problem. *Ramanujan J.*, 28(1):45–60, 2012.

[11] Istvan Kovacs, Daniel S. Silver, and Susan G. Williams. Determinants of commuting-block matrices. *Amer. Math. Monthly*, 106(10):950–952, 1999.

[12] H. Turner Laquer. Values of circulants with integer entries. In *A collection of manuscripts related to the Fibonacci sequence*, pages 212–217. Fibonacci Assoc., Santa Clara, Calif., 1980.

[13] Morris Newman. Determinants of circulants of prime power order. *Linear and Multilinear Algebra*, 9(3):187–191, 1980.

[14] Morris Newman. On a problem suggested by Olga Taussky-Todd. *Illinois J. Math.*, 24(1):156–158, 1980.

[15] Bishnu Paudel and Chris Pinner. Integer circulant determinants of order 15. *Integers*, 22:Paper No. A4, 21, 2022.

[16] Bishnu Paudel and Christopher Pinner. The group determinants for $\mathbb{Z}_n \times H$, 2022. arXiv:2211.09930v3 [math.NT].

[17] Bishnu Paudel and Christopher Pinner. The integer group determinants for Q_{16}, 2023. arXiv:2302.11688v1 [math.NT].

[18] Christopher Pinner. The integer group determinants for the symmetric group of degree four. *Rocky Mountain J. Math.*, 49(4):1293–1305, 2019.

[19] Christopher Pinner and Christopher Smyth. Integer group determinants for small groups. *Ramanujan J.*, 51(2):421–453, 2020.

[20] B. L. van der Waerden. *A history of algebra*. Springer-Verlag, Berlin, 1985. From al-Khwārizmī to Emmy Noether.

[21] Naoya Yamaguchi. An extension and a generalization of Dedekind's theorem. *Int. J. Group Theory*, 6(3):5–11, 2017.

[22] Naoya Yamaguchi. Study-type determinants and their properties. *Cogent Math. Stat.*, 6(1):Art. ID 1683131, 19, 2019.

[23] Naoya Yamaguchi and Yuka Yamaguchi. Generalized group determinant gives a necessary and sufficient condition for a subset of a finite group to be a subgroup. *Comm. Algebra*, 49(4):1805–1811, 2021.

[24] Naoya Yamaguchi and Yuka Yamaguchi. Remark on Laquer's theorem for circulant determinants. *International Journal of Group Theory*, 12(4):265–269, 2023.

[25] Yuka Yamaguchi and Naoya Yamaguchi. Integer circulant determinants of order 16. *Ramanujan J.*, 2022. Advance online publication, https://doi.org/10.1007/s11139-022-00599-9.

[26] Yuka Yamaguchi and Naoya Yamaguchi. Integer group determinants for abelian groups of order 16, 2022. arXiv:2211.14761v1 [math.NT].

[27] Yuka Yamaguchi and Naoya Yamaguchi. Integer group determinants for $\mathrm{C}_2^2 \rtimes \mathrm{C}_4$, 2023. arXiv:2303.08489v2 [math.NT].

[28] Yuka Yamaguchi and Naoya Yamaguchi. Integer group determinants for C_2^4. *Ramanujan J.*, 2023. Advance online publication, https://doi.org/10.1007/s11139-023-00727-z.

[29] Yuka Yamaguchi and Naoya Yamaguchi. Integer group determinants for C_4^2, 2023. arXiv:2211.01597v2 [math.NT].

[30] J. W. A. Young. On the Determination of Groups Whose Order is a Power of a Prime. *Amer. J. Math.*, 15(2):124–178, 1893.

Faculty of Education, University of Miyazaki, 1-1 Gakuen Kibanadai-nishi, Miyazaki 889-2192, Japan
Email address, Naoya Yamaguchi: n-yamaguchi@cc.miyazaki-u.ac.jp
Email address, Yuka Yamaguchi: y-yamaguchi@cc.miyazaki-u.ac.jp