Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
2023, Volume 29, Number 3, 603–619
DOI: 10.7546/nntdm.2023.29.3.603-619

The group determinants for $\mathbb{Z}_n \times H$

Bishnu Paudel[1] **and Chris Pinner**[2]

[1] Department of Mathematics, Kansas State University
Manhattan KS 66506, United States
e-mail: bpaudel@ksu.edu

[2] Department of Mathematics, Kansas State University
Manhattan KS 66506, United States
e-mail: pinner@math.ksu.edu

Received: 22 March 2023 **Revised:** 4 August 2023
Accepted: 11 August 2023 **Online First:** 25 August 2023

Abstract: Let $\mathbb{Z}_n$ denote the cyclic group of order n. We show how the group determinant for $G = \mathbb{Z}_n \times H$ can be simply written in terms of the group determinant for H. We use this to get a complete description of the integer group determinants for $\mathbb{Z}_2 \times D_8$ where D_8 is the dihedral group of order 8, and $\mathbb{Z}_2 \times Q_8$ where Q_8 is the quaternion group of order 8.
Keywords: Integer group determinant, Dihedral group, Quaternion group.
2020 Mathematics Subject Classification: 11C20, 15B36; Secondary: 11C08, 43A40.

1 Introduction

At the meeting of the American Mathematical Society in Hayward, California, in April 1977, Olga Taussky-Todd [15] asked whether one could characterize the values of the group determinant when the entries are all integers. There was particular interest in the case of $\mathbb{Z}_n$, the cyclic group of order n, where the group determinant corresponds to the $n \times n$ circulant determinant. For a prime p, a complete description was obtained for the cyclic groups $\mathbb{Z}_p$ and $\mathbb{Z}_{2p}$ in [11] and [7], and for D_{2p} and D_{4p} in [8] and [1]. Here D_{2n} denotes the dihedral group of order $2n$. In general though this quickly becomes a hard problem, with only partial results known even for $\mathbb{Z}_{p^2}$ once

$p \geq 7$ (see [12] and [10]). A complete description has though been obtained for all groups of order less than 16 (see [14] and [13]), and for 6 of the 14 groups of order 16, D_{16} and the five Abelian groups $\mathbb{Z}_{16}$, $\mathbb{Z}_2 \times \mathbb{Z}_8$, $\mathbb{Z}_2^4$, $\mathbb{Z}_4^2$ and $\mathbb{Z}_2^2 \times \mathbb{Z}_4$ (see [1,16,18,20,21] and [19]). We write $\mathcal{S}(G)$ for the set of integer group determinants for the group G.

Our goal here is to show how the group determinant for a group of the form $G = \mathbb{Z}_n \times H$ can be straightforwardly related to the group determinants for the group H. We use this to give a complete description for two more non-Abelian groups of order 16, namely $\mathbb{Z}_2 \times D_8$ and $\mathbb{Z}_2 \times Q_8$ where Q_8 is the quaternion group.

Here we shall think of the group determinants as being defined on elements of the group ring $\mathbb{C}[G]$

$$\mathcal{D}_G\left(\sum_{g\in G} a_g g\right) = \det\left(a_{gh^{-1}}\right),$$

although our ultimate interest is of course in the integer group determinants $\mathbb{Z}[G]$. We observe the multiplicative property

$$\mathcal{D}_G(xy) = \mathcal{D}_G(x)\mathcal{D}_G(y), \tag{1.1}$$

using that

$$x = \sum_{g\in G} a_g g, \quad y = \sum_{g\in G} b_g g \;\Rightarrow\; xy = \sum_{g\in G}\left(\sum_{hk=g} a_h b_k\right) g.$$

2 Products with $\mathbb{Z}_n$

We show that when $G = \mathbb{Z}_n \times H$ we can write our integer group G-determinant as a product of n group H-determinants of elements in $\mathbb{Z}[\omega_n][H]$, where $\omega_n := e^{2\pi i/n}$. This is Lemma 1 of [9].

Theorem 2.1. *If $G = \mathbb{Z}_n \times H$ then for any a_{ih} in $\mathbb{C}$*

$$\mathcal{D}_G\left(\sum_{i=0}^{n-1}\sum_{h\in H} a_{ih}(i,h)\right) = \prod_{y^n=1} \mathcal{D}_H\left(\sum_{h\in H}\left(\sum_{i=0}^{n-1} a_{ih} y^i\right) h\right). \tag{2.1}$$

Results of this flavour have been obtained before [17], but here we do not need to assume that H is Abelian.

Proof. One way to see this is to use Frobenius' factorisation [5] of the group determinant in terms of the irreducible, non-isomorphic, representations ρ of G (see for example [2] or [6])

$$\mathcal{D}_G\left(\sum_{g\in G} a_g g\right) = \prod_{\rho} \det\left(\sum_{g\in G} a_g \rho(g)\right)^{\deg(\rho)}.$$

Observe that every representation ρ for H extends to n representations for G

$$\rho_y(i,h) = y^i \rho(h),$$

where y runs through the n-th roots of unity.

More directly we can alternatively follow Newman's proof [11] of the factorization of the group determinant for $G = \mathbb{Z}_n$. Newman observes that the group matrix M for $\sum_{i\in\mathbb{Z}_n} A_i i$, that is the circulant matrix with first row $A_0, A_1, \ldots, A_{n-1}$, takes the form

$$M = A_0 I_n + A_1 P + \cdots + A_{n-1} P^{n-1}, \quad P = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Now P has eigenvalues y, $y^n = 1$, so the matrix M will have the same eigenvectors as P but with eigenvalues

$$A_0 + A_1 y + \cdots + A_{n-1} y^{n-1}, \quad y = 1, \omega_n, \omega_n^2, \ldots, \omega_n^{n-1}. \tag{2.2}$$

Hence the matrix of eigenvectors B will yield a diagonal matrix $B^{-1}MB$ with the values (2.2) down the diagonal.

Now suppose that $H = \{h_1, \ldots, h_m\}$ and order the elements so that the first row of the $G = \mathbb{Z}_n \times H$ group matrix $\mathcal{M}$ for $\sum_{i\in\mathbb{Z}_n, h\in H} a_{ih}(i,h)$ consists of the

$$a_{0h_1}, \ldots, a_{0h_m}, a_{1h_1}, \ldots, a_{1h_m}, \ldots, a_{(n-1)h_1}, \ldots, a_{(n-1)h_m}.$$

Then it is not hard to see that first m rows of our G group matrix $\mathcal{M}$ will consists of $m \times m$ blocks $A_0, A_1, \ldots, A_{n-1}$, where A_i is the group H matrix associated to $\sum_{h\in H} a_{ih}h$, and the subsequent rows the same blocks cyclically permuted.

Hence if we take the $n \times n$ matrix B and replace each entry a_{ij} with the $m \times m$ block $a_{ij}I_m$ we obtain an $nm \times nm$ matrix $\mathcal{B}$, where $\mathcal{B}^{-1}\mathcal{M}\mathcal{B}$ will now be a block matrix with entries the same linear combinations of the blocks A_i as occured for the elements in $B^{-1}MB$; that is blocks (2.2) down the diagonal and zeros elsewhere. The result is then plain. $\square$

Notice that if we start with an integer G group determinant, then we can assemble the n determinants in (2.1) into $\tau(n)$ integers by combining the primitive dth roots of unity, $d \mid n$. If H is Abelian, then these will be integer H group determinants

$$\prod_{\substack{y=\omega_d^j \\ \gcd(j,d)=1}} \mathcal{D}_H\left(\sum_{h\in H}\left(\sum_{i=0}^{n-1} a_{ih}y^i\right)h\right) = \mathcal{D}_H\left(\prod_{\substack{y=\omega_d^j \\ \gcd(j,d)=1}} \sum_{h\in H}\left(\sum_{i=0}^{n-1} a_{ih}y^i\right)h\right), \tag{2.3}$$

since the resulting coefficients will be symmetric expressions in the conjugates and hence in $\mathbb{Z}$. In particular, an integer $G = \mathbb{Z}_n \times H$ group determinant is an integer group H determinant, though this can be seen more directly (if $H = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$, then the G group determinant reduces to a product of an integer polynomial $F(y, x_1, \ldots, x_k)$ over the $n, n_1, \ldots, n_k$th roots of unity and $\prod_{y^n=1} F(y, x_1, \ldots, x_k)$ is just an integer polynomial in one less variable; see also [16, Theorem 1.4]). If H is non-Abelian, then the process (2.3) may leave elements in $\mathbb{Z}[\omega_d][H]$, and we are unable to say that an integer G group determinant must be an integer H group determinant, except for the case when $n = 2$.

3 The group $\mathbb{Z}_2 \times D_8$

Notice that when $n = 2$ we can write an integer $\mathbb{Z}_2 \times H$ group determinant as a product of two integer H group determinants:

$$\mathcal{D}_{\mathbb{Z}_2\times H}\left(\sum_{h\in H} a_h(0,h) + \sum_{h\in H} b_h(1,h)\right) = \mathcal{D}_H\left(\sum_{h\in H}(a_h+b_h)h\right)\mathcal{D}_H\left(\sum_{h\in H}(a_h-b_h)h\right).$$

In the case of $H = D_8 = \langle F, R \mid F^2 = 1, R^4 = 1, RF = FR^3\rangle$ we take the coefficients of the group elements $(0, R^j)$, $(1, R^j)$, $(0, FR^j)$ and $(1, FR^j)$, as the coefficients of x^j in four cubics, f_1, f_2, g_1 and g_2 respectively. The $\mathbb{Z}_2 \times D_8$ determinant, which we will denote $\mathcal{D}(f_1, f_2, g_1, g_2)$, is then the product of two D_8 determinants, which from [8] or [1] can be written

$$\mathcal{D}(f_1, f_2, g_1, g_2) = \mathcal{D}(1)\mathcal{D}(-1), \quad \mathcal{D}(z) = m_1(z)m_2(z)\ell(z)^2, \tag{3.1}$$

where

$$m_1(z) = (f_1(1) + zf_2(1))^2 - (g_1(1) + zg_2(1))^2,$$
$$m_2(z) = (f_1(-1) + zf_2(-1))^2 - (g_1(-1) + zg_2(-1))^2,$$

and

$$\ell(z) = |f_1(i) + zf_2(i)|^2 - |g_1(i) + zg_2(i)|^2. \tag{3.2}$$

We obtain a complete description of the $\mathbb{Z}_2 \times D_8$ integer group determinants.

Theorem 3.1. *For $G = \mathbb{Z}_2 \times D_8$ the set of odd integer group determinants is*

$$A := \{m(m + 16k) \ : \ m, k \in \mathbb{Z}, \ m \text{ odd}\}.$$

The even determinants are the $2^{16}m$, $m \in \mathbb{Z}$.

Notice the set of achieved odd values A consists of all the integers $1 \bmod 16$ and exactly those integers $9 \bmod 16$ which contain a prime $p \equiv \pm 3$ or $\pm 5 \bmod 16$. These are the same as the odd values found in [16] for $\mathbb{Z}_2 \times \mathbb{Z}_8$. In fact $\mathcal{S}(\mathbb{Z}_2 \times D_8) \subsetneq \mathcal{S}(\mathbb{Z}_2 \times \mathbb{Z}_8)$. Sets of this type occur for other 2-groups.

Proposition 3.1. *The odd integer group determinants for $G = \mathbb{Z}_2 \times \mathbb{Z}_{2^n}$ are the*

$$\{m(m + |G|k) \ : \ m, k \in \mathbb{Z}, \ m \text{ odd}\}.$$

The odd integer group determinants for $G = \mathbb{Z}_2^n$ or $\mathbb{Z}_2^n \times \mathbb{Z}_4$ are the $m \equiv 1 \bmod |G|$.

Note, for any group the $m \equiv 1 \bmod |G|$ are in $\mathcal{S}(G)$, with $1 + k|G|$ obtained by taking $a_g = 1 + k$ for the identity and $a_g = k$ for the others.

Proof of Theorem 3.1. **Achieving the values.** We write $H(x) := (x + 1)(x^2 + 1)$.

We achieve the values in A with $m = \pm 1, \pm 9 \bmod 16$ from

$$\mathcal{D}(1 + kH, kH, kH, kH) = 1 + 16k.$$

We get those with $\pm m \equiv 5 \bmod 16$ from $(5+16t)(5+16k)$ achieved with

$$\mathcal{D}(1+x+x^2+(t+k)H, x-x^3+(t-k)H, 1+x+(t+k)H, 1-x^2+(t-k)H)$$

and those with $\pm m \equiv 3 \bmod 16$ from $(3+16t)(3+16k)$ achieved with

$$\mathcal{D}(1+x+(t+k)H, 1+x-x^2-x^3+(t-k)H, 1+x-x^3+(t+k)H, x-x^3+(t-k)H).$$

We achieve the even values $2^{18}m$ using

$$\mathcal{D}(1+x+x^2-mH, 1-x^2-x^3-mH, 1+x-x^3+mH, x+mH),$$

the $2^{17}(2m+1)$ with

$$\mathcal{D}(1+x+x^2+x^3+mH, 1+x+mH, x+mH, 1+x^2-x^3+mH),$$

the $2^{16}(1+4m)$ from

$$\mathcal{D}(1+x+x^2+x^3+mH, 1+x-x^2-x^3+mH, 1+x-x^2-x^3+mH, 1-x+mH),$$

and the $2^{16}(-1+4m)$ from

$$\mathcal{D}(1+x+x^2-mH, 1+x-x^3-mH, 1-x^3-mH, x-x^2-mH).$$

The odd values. We show that any odd determinant must lie in A. We know that any $\mathbb{Z}_2 \times D_8$ determinant must be the product of two D_8 determinants, which we can write

$$\mathcal{D}_1 = m_1 m_2 \ell_1^2, \quad \mathcal{D}_2 = m_3 m_4 \ell_2^2 \tag{3.3}$$

with

$$m_1 = f(1)^2 - g(1)^2, \quad m_2 = f(-1)^2 - g(-1)^2, \quad \ell_1 = |f(i)|^2 - |g(i)|^2,$$

and

$$\begin{aligned} m_3 &= (f(1)+2h(1))^2 - (g(1)+2k(1))^2, \\ m_4 &= (f(-1)+2h(-1))^2 - (g(-1)+2k(-1))^2, \\ \ell_2 &= |f(i)+2h(i)|^2 - |g(i)+2k(i)|^2. \end{aligned}$$

Assume that $\mathcal{D}_1\mathcal{D}_2$ is odd. Switching f and g and replacing f by $-f$ as necessary, we shall assume that $f(1) \equiv 1 \bmod 4$ and $2 \mid g(1)$. The result will follow once we show that

$$\mathcal{D}_1 \equiv \mathcal{D}_2 \pmod{16}.$$

We write

$$h(x) = \sum_{i=0}^{3} a_i (x-1)^i, \quad k(x) = \sum_{i=0}^{3} b_i (x-1)^i, \quad f(x) = \sum_{i=0}^{3} c_i (x-1)^i, \quad g(x) = \sum_{i=0}^{3} d_i (x-1)^i,$$

where $c_0 = 1 \bmod 4$ and $2 \mid d_0$. Now

$$\begin{aligned} m_3 - m_1 &= 4f(1)h(1) + 4h(1)^2 - 4k(1)g(1) - 4k(1)^2 \equiv 4a_0 + 4a_0^2 - 4b_0d_0 - 4b_0^2 \bmod 16, \\ m_4 - m_2 &= 4f(-1)h(-1) + 4h(-1)^2 - 4k(-1)g(-1) - 4k(-1)^2 \\ &\equiv 4(a_0 - 2a_1 - 2a_0c_1) + 4a_0^2 - 4(b_0d_0 - 2b_0d_1) - 4b_0^2 \bmod 16, \end{aligned}$$

and

$$\begin{aligned} \ell_2 - \ell_1 &= (2h(i)\overline{f(i)} + 2\overline{h(i)}f(i) + 4|h(i)|^2) - (2k(i)\overline{g(i)} + 2\overline{k(i)}g(i) + 4|k(i)|^2) \\ &\equiv (4a_0 - 4a_0c_1 - 4a_1 + 4a_0^2) - (-4b_0d_1 + 4b_0^2) \bmod 8 \end{aligned}$$

and

$$\ell_2^2 \equiv \ell_1^2 + 8(a_0 - a_0c_1 - a_1 + a_0^2 + b_0d_1 - b_0^2) \bmod 16.$$

Since $m_1, m_2, \ell_1^2 \equiv 1 \bmod 4$ we get

$$\begin{aligned} \mathcal{D}_1 - \mathcal{D}_2 \equiv{}& 4(a_0 + a_0^2 - b_0d_0 - b_0^2) + 4(a_0 - 2a_1 - 2a_0c_1 + a_0^2 - b_0d_0 + 2b_0d_1 - b_0^2) \\ &+ 8(a_0 - a_0c_1 - a_1 + a_0^2 + b_0d_1 - b_0^2) \equiv 0 \bmod 16. \end{aligned}$$

The even values. We know from [1] that the even D_8 determinants are divisible by 2^8. So any even $\mathbb{Z}_2 \times D_8$ determinant $\mathcal{D}_1\mathcal{D}_2$ must be a multiple of 2^{16}, and all these are achieved. □

Proof of Proposition 3.1. Suppose that H is an abelian 2-group and $G = \mathbb{Z}_2 \times H$. Then by [3, Theorem 2.3] we can write the G-determinant as a product of two H-determinants $\mathcal{D} = \mathcal{D}_1\mathcal{D}_2$ with $\mathcal{D}_2 \equiv \mathcal{D}_1 \bmod |G|$, and

$$\mathcal{S}(\mathbb{Z}_2 \times H) \subseteq \{m(m + k|G|) \;:\; m \in \mathcal{S}(H)\}. \tag{3.4}$$

For $G = \mathbb{Z}_2 \times \mathbb{Z}_t, t = 2^n$, the determinants take the form

$$\mathcal{D}_1 = \prod_{x^t=1} F(x,1),$$
$$\mathcal{D}_2 = \prod_{x^t=1} F(x,-1)$$

for some $F(x,y) = f(x) + yh(x)$, the coefficients of x^i in f and h corresponding to the a_g for $g = (0,i)$ and $(1,i)$ respectively. For an odd positive integer m, taking

$$F(x,y) = \prod_{p^\alpha \| m} \left(\frac{x^p - 1}{x - 1}\right)^\alpha + k(y+1)\left(\frac{x^t - 1}{x - 1}\right)$$

achieves $m(m + k|G|)$.

For $G = \mathbb{Z}_2^n$ all the odd values must be $1 \bmod |G|$ by [4, Lemma 2.1]. For $G_n = \mathbb{Z}_2^n \times \mathbb{Z}_4$ observe when $n = 1$ that $m(m+8k) \equiv m^2 \equiv 1 \bmod 8$, and in general that if $m \equiv 1 \bmod |G_{n-1}|$ then $m(m + |G_n|k) \equiv m^2 \equiv 1 \bmod |G_n|$. □

Interestingly, (3.4) also holds for the non-Abelian groups $H = D_8$ and Q_8.

4 The group $\mathbb{Z}_2 \times Q_8$

A $\mathbb{Z}_2 \times Q_8$ determinant will be a product of two Q_8 determinants, which by [14] can be written in a very similar way to (3.1);

$$\mathcal{D}(f_1, f_2, g_1, g_2) = \mathcal{D}(1)\mathcal{D}(-1), \quad \mathcal{D}(z) = m_1(z)m_2(z)\ell(z)^2, \tag{4.1}$$

with

$$m_1(z) = (f_1(1) + zf_2(1))^2 - (g_1(1) + zg_2(1))^2,$$
$$m_2(z) = (f_1(-1) + zf_2(-1))^2 - (g_1(-1) + zg_2(-1))^2,$$

but now

$$\ell(z) = |f_1(i) + zf_2(i)|^2 + |g_1(i) + zg_2(i)|^2.$$

Writing $Q_8 = \langle A, B : A^4 = 1, B^2 = A^2, AB = BA^{-1}\rangle$, the coefficient of x^i in the cubic f_1, f_2, g_1 and g_2, corresponds to the a_g in the $\mathbb{Z}_2 \times Q_8$ group determinant for $g = (0, A^i), (1, A^i)$, $(0, BA^i)$ and $(1, BA^i)$, respectively.

We obtain a complete description of the $\mathbb{Z}_2 \times Q_8$ integer group determinants.

Theorem 4.1. *When $G = \mathbb{Z}_2 \times Q_8$ the odd integer group determinants are the integers $1 \bmod 16$, plus the integers $9 \bmod 16$ of the form*

$$s_1s_2(\ell_1\ell_2)^2, \quad s_1, s_2 \equiv -3 \bmod 8, \quad \ell_1, \ell_2 \equiv 3 \bmod 4,$$

for some s_1, s_2 in $\mathbb{Z}$ and ℓ_1, ℓ_2 in $\mathbb{N}$, with

$$s_1 \equiv s_2 \bmod 16 \quad \textit{and} \quad \ell_1 \equiv \ell_2 \bmod 8 \tag{4.2}$$

or

$$s_1 \equiv s_2 + 8 \bmod 16 \quad \textit{and} \quad \ell_1 \equiv \ell_2 + 4 \bmod 8. \tag{4.3}$$

The even values are the $2^{18}m$, m in $\mathbb{Z}$, the

$$2^{17}(2m + 1)p^2, \quad m \in \mathbb{Z}, \quad p \equiv 3 \bmod 4,$$

the $2^{16}m$ with $m \equiv 1, 3$ or $5 \bmod 8$, and those with $m \equiv 7 \bmod 8$ of the form

$$2^{16}(8t - 1)\ell^2, \quad t \in \mathbb{Z}, \quad \ell \in \mathbb{N}, \quad \ell \equiv 1 \bmod 4, \ \ell \geq 5, \tag{4.4}$$

or

$$(8t + 3)(8k - 3)2^{16}, \quad t, k \in \mathbb{Z}. \tag{4.5}$$

For the three non-Abelian groups of order 16 whose $\mathcal{S}(G)$ is now known we have:

$$\mathcal{S}(\mathbb{Z}_2 \times Q_8) \subsetneq \mathcal{S}(\mathbb{Z}_2 \times D_8) \subsetneq \mathcal{S}(D_{16}) = \{4m + 1 \ : \ m \in \mathbb{Z}\} \cup \{2^{10}m \ : \ m \in \mathbb{Z}\}.$$

Proof. **Achieving the odd values.** We write $H(x) := (x + 1)(x^2 + 1)$.

We achieve the values $1 \bmod 16$ from

$$\mathcal{D}(1 + kH, kH, kH, kH) = 1 + 16k.$$

To achieve the specified values $9 \bmod 16$ we write the ℓ_i as a sum of four squares. Notice that since they are $3 \bmod 4$, we must have three of them, say, A_i, B_i, C_i, odd and one, D_i, even, with $2 \parallel D_i$ if $\ell_i \equiv 7 \bmod 8$ and $4 \mid D_i$ if $\ell_i \equiv 3 \bmod 8$. Hence with a choice of sign we can write

$$\ell_i = A_i^2 + B_i^2 + C_i^2 + D_i^2, \quad A_i, B_i, C_i \text{ odd}, \quad D_i \text{ even},$$

with

$$A_1 \equiv A_2 \bmod 4, \quad B_1 \equiv B_2 \bmod 4, \quad C_1 \equiv C_2 \bmod 4,$$

and

$$D_1 \equiv D_2 \bmod 4 \quad \text{if} \quad \ell_1 \equiv \ell_2 \bmod 8,$$

and

$$D_1 \equiv D_2 + 2 \pmod 4 \quad \text{if} \quad \ell_1 \equiv \ell_2 + 4 \pmod 8.$$

In the case $\ell_1 \equiv \ell_2 \bmod 8$ we get $(8m-3)(8k-3)(\ell_1\ell_2)^2$, $m \equiv k \bmod 2$, from

$$\begin{aligned}
f_1 &= \frac{1}{4}(D_1+D_2) + \frac{1}{4}(B_1+B_2-2)x - \frac{1}{4}(D_1+D_2)x^2 - \frac{1}{4}(B_1+B_2+2)x^3 + \frac{1}{2}(m+k)H,\\
f_2 &= \frac{1}{4}(D_1-D_2) + \frac{1}{4}(B_1-B_2)x - \frac{1}{4}(D_1-D_2)x^2 - \frac{1}{4}(B_1-B_2)x^3 + \frac{1}{2}(m-k)H,\\
g_1 &= \frac{1}{4}(C_1+C_2-2) + \frac{1}{4}(A_1+A_2-2)x - \frac{1}{4}(C_1+C_2+2)x^2 - \frac{1}{4}(A_1+A_2+2)x^3 + \frac{1}{2}(m+k)H,\\
g_2 &= \frac{1}{4}(C_1-C_2) + \frac{1}{4}(A_1-A_2)x - \frac{1}{4}(C_1-C_2)x^2 - \frac{1}{4}(A_1-A_2)x^3 + \frac{1}{2}(m-k)H.
\end{aligned}$$

In the case $\ell_1 \equiv \ell_2 + 4 \bmod 8$ we get $(8m-3)(5-8k)(\ell_1\ell_2)^2$, $m \equiv k \bmod 2$, from

$$\begin{aligned}
f_1 &= \frac{1}{4}(D_1+D_2-2) + \frac{1}{4}(B_1+B_2-2)x - \frac{1}{4}(D_1+D_2+2)x^2 - \frac{1}{4}(B_1+B_2+2)x^3 + \frac{1}{2}(m+k)H,\\
f_2 &= \frac{1}{4}(D_1-D_2+2) + \frac{1}{4}(B_1-B_2)x - \frac{1}{4}(D_1-D_2-2)x^2 - \frac{1}{4}(B_1-B_2)x^3 + \frac{1}{2}(m-k)H,\\
g_1 &= \frac{1}{4}(C_1+C_2-2) + \frac{1}{4}(A_1+A_2-2)x - \frac{1}{4}(C_1+C_2+2)x^2 - \frac{1}{4}(A_1+A_2+2)x^3 + \frac{1}{2}(m+k)H,\\
g_2 &= \frac{1}{4}(C_1-C_2) + \frac{1}{4}(A_1-A_2)x - \frac{1}{4}(C_1-C_2)x^2 - \frac{1}{4}(A_1-A_2)x^3 + \frac{1}{2}(m-k)H.
\end{aligned}$$

Odd values must be of the stated form. We proceed as in the case of $\mathbb{Z}_2 \times D_8$, with (3.3) becoming

$$\mathcal{D}_1 = m_1 m_2 \ell_1^2, \quad \mathcal{D}_2 = m_3 m_4 \ell_2^2, \tag{4.6}$$

where again

$$\begin{aligned}
m_1 &= f(1)^2 - g(1)^2,\\
m_2 &= f(-1)^2 - g(-1)^2,\\
m_3 &= (f(1)+2h(1))^2 - (g(1)+2k(1))^2,\\
m_4 &= (f(-1)+2h(-1))^2 - (g(-1)+2k(-1))^2,
\end{aligned}$$

but this time

$$\ell_1 = |f(i)|^2 + |g(i)|^2, \;\; \ell_2 = |f(i)+2h(i)|^2 + |g(i)+2k(i)|^2.$$

This does not change $\ell_1 - \ell_2 \bmod 8$, so again we must have $\mathcal{D}_1 \equiv \mathcal{D}_2 \bmod 16$ and $\mathcal{D}_1\mathcal{D}_2$ is 1 or 9 mod 16. The 1 mod 16 are all achievable, so assume $\mathcal{D}_1\mathcal{D}_2 \equiv 9 \bmod 16$. Since all the $m_i \equiv m_1 \bmod 4$, plainly the $\mathcal{D}_i \equiv m_1^2\ell_i^2 \equiv 1 \bmod 4$, so we can assume that $\mathcal{D}_1, \mathcal{D}_2 \equiv -3 \bmod 8$.

Since the $\ell_i^2 \equiv 1 \bmod 8$, we get $m_1m_2, m_3m_4 \equiv -3 \bmod 8$. Since m_1 and m_2 are 1 or $-3 \bmod 8$ we must have one of each, and $2 \parallel g(1)$ and $4 \mid g(-1)$ or vice versa. Hence d_1 must be odd and

$$\ell_1 \equiv (c_0 + c_1)^2 + c_1^2 + (d_0 + d_1)^2 + d_1^2 \equiv 3 \bmod 4.$$

From above we also know that $\ell_1 \equiv \ell_2 \bmod 4$. That is, $\mathcal{D}_1\mathcal{D}_2 = s_1 s_2 (\ell_1 \ell_2)^2$ with $s_1 \equiv s_2 \equiv -3 \bmod 8$ and $\ell_1 \equiv \ell_2 \equiv 3 \bmod 4$. Plainly we have $s_1 s_2 \equiv 9 \bmod 16$ if $s_1 \equiv s_2 \equiv -3$ or $5 \bmod 16$ and $s_1 s_2 \equiv 1 \bmod 16$ if one is -3 and the other $5 \bmod 16$, while $\ell_1 \ell_2 \equiv 1 \bmod 8$ and $(\ell_1 \ell_2)^2 \equiv 1 \bmod 16$ if $\ell_1 \equiv \ell_2 \equiv 3$ or $7 \bmod 8$ and $\ell_1 \ell_2 \equiv -3 \bmod 8$ and $(\ell_1 \ell_2)^2 \equiv 9 \bmod 16$ if one is 3 and the other $7 \bmod 8$. Hence the restrictions (4.2) and (4.3) to get $\mathcal{D}_1\mathcal{D}_2 \equiv 9 \bmod 16$.

Achieving the even values. We obtain the $2^{18}m$, m odd, from

$$f_1 = 1 + x^2 + \frac{1}{2}(m+1)H, \qquad f_2 = \frac{1}{2}(m-1)H,$$
$$g_1 = -(1+x) + \frac{1}{2}(m+1)H, \qquad g_2 = \frac{1}{2}(m-1)H,$$

and the $2^{19}m$ from

$$f_1 = 1 + x + x^2 - mH, \qquad f_2 = -x - x^3 - mH,$$
$$g_1 = x + x^3 + mH, \qquad g_2 = -x^3 + mH.$$

We get the $2^{16}(4m+1)$ from

$$f_1 = 1 + x + x^2 + x^3 + mH, \qquad f_2 = mH,$$
$$g_1 = 1 - x + mH, \qquad g_2 = mH.$$

We get $2^{16}(8t+3)(4s+1)$ from

$$f_1 = 1 + x + x^2 + x^3 + (t+s)H, \qquad f_2 = 1 + x^2 - x^3 + (t-s)H,$$
$$g_1 = (t-s)H, \qquad g_2 = x^3 + (t+s)H,$$

with $s = 0$ giving us the $2^{16}m$, $m \equiv 3 \bmod 8$, and $s = 2k - 1$ the values (4.5). For $\ell \geq 5$ with $\ell \equiv 1 \bmod 4$ we can write $2\ell - 4 \equiv 6 \bmod 8$ as a sum of three squares with two of them odd and the other $2 \bmod 4$:

$$2\ell = (4a+1)^2 + 2^2 + (4c-1)^2 + (4d-2)^2$$

and we can get $2^{16}(4m-1)\ell^2$, and hence (4.4), from

$$f_1 = (1 - x + x^2) + a(1 - x^2) + mH,$$
$$f_2 = -x(1+x) + a(1-x^2) + mH,$$
$$g_1 = -x + (1-x^2)(c+dx) + mH,$$
$$g_2 = -(1+x) + (1-x^2)(c+dx) + mH.$$

For $p \equiv 3 \bmod 4$ we write $2p = A^2 + B^2 + C^2 + D^2$ where, since $2p \equiv 6 \bmod 8$, two of A, B, C, D must be odd and two even, with one of them divisible by 4, the other $2 \bmod 4$. Changing signs as necessary we assume that $A = 1 + 4a$, $B = 4b$, $C = 1 + 4c$, and $D = 2 + 4d$. We achieve $2^{17}(2m + 1)p^2$ with

$$\begin{aligned}
f_1 &= (1 + x)(x^2 + 1) + a(1 - x^2) + bx(1 - x^2) + mH, \\
f_2 &= 1 + (x - 1)(x^2 + 1) + a(1 - x^2) + bx(1 - x^2) + mH, \\
g_1 &= 1 + x + c(1 - x^2) + dx(1 - x^2) + mH, \\
g_2 &= x + c(1 - x^2) + dx(1 - x^2) + mH.
\end{aligned}$$

Even values must be of the stated form. We know if the $\mathbb{Z}_2 \times Q_8$ determinant is even, then both Q_8 determinants are even, and by [14] must each be multiples of 2^8. Hence the even determinants must be multiples of 2^{16}. Note, if the determinant is even we must have $f(1)$ and $g(1)$ the same parity, and all the terms $m_1, m_2, m_3, m_4, \ell_1, \ell_2$ in (4.6) must be even.

The $2^{17} \parallel \mathcal{D}$ are of the stated form. Suppose that we had a determinant $2^{17}m$, m odd, with m not divisible by the square of a prime $3 \bmod 4$. Writing

$$\ell_2 - \ell_1 \equiv 4(a_0c_0 - a_0c_1 - a_1c_0 + a_0^2) + 4(b_0d_0 - b_0d_1 - b_1d_0 + b_0^2) \bmod 8 \tag{4.7}$$

we see that $2 \parallel \ell_1, \ell_2$ or $4 \mid \ell_1, \ell_2$. If $f(1), g(1)$ are both odd then $2^3 \mid m_1, m_2, m_3, m_4$ and we must have $2 \parallel \ell_1, \ell_2$ (else $2^{12+8} \mid \mathcal{D}$). Now if $2^u \parallel f(1)$ and $2^v \parallel g(1)$ with $u, v \geq 1$ then $2^{2\min\{u,v\}} \parallel m_1$ if $u \neq v$, while if $u = v$ we have $2^{2u+3} \mid m_1$. Likewise for m_2, m_3, m_4. To obtain an odd power of two we must therefore have at least one of the m_i with $u = v$. We cannot have two of them (else $2^{5+5+4+4} \mid \mathcal{D}$). Again we can assume that $2 \parallel \ell_1, \ell_2$ (otherwise $2^{5+6+8} \mid \mathcal{D}$). Since ℓ_1 and ℓ_2 do not contain any primes $3 \bmod 4$ we have $\ell_1 \equiv \ell_2 \equiv 2 \bmod 8$ and (4.7) gives

$$a_0c_0 - a_0c_1 - a_1c_0 + a_0^2 + b_0d_0 - b_0d_1 - b_1d_0 + b_0^2 \equiv 0 \bmod 2. \tag{4.8}$$

Suppose first that $f(1)$, $g(1)$ are odd. Since c_0 and d_0 are odd, (4.8) becomes

$$-a_0c_1 - b_0d_1 \equiv a_1 + b_1 \bmod 2. \tag{4.9}$$

To get power 17, rearranging if necessary to make the highest power on m_1, we must have $2^4 \parallel m_1$, $2^3 \parallel m_2, m_3, m_4$. That is, $m_1 \equiv 0 \bmod 16$, and $m_2 \equiv m_3 \equiv m_4 \equiv 8 \bmod 16$. From

$$m_1 = c_0^2 - d_0^2 \equiv 0 \bmod 16, \quad m_3 = (c_0 + 2a_0)^2 - (d_0 + 2b_0)^2 \equiv 8 \bmod 16$$

we get

$$a_0c_0 + a_0^2 - b_0^2 - b_0d_0 \equiv 2 \bmod 4. \tag{4.10}$$

From

$$\begin{aligned}
m_4 &\equiv (c_0 - 2c_1 + 4c_2 + 2a_0 - 4a_1)^2 - (d_0 - 2d_1 + 4d_2 + 2b_0 - 4b_1)^2 \bmod 16 \\
&\equiv m_2 + 4a_0^2 + 4(a_0c_0 - 2a_0c_1 - 2a_1c_0) - 4b_0^2 - 4(d_0b_0 - 2d_1b_0 - 2d_0b_1) \bmod 16,
\end{aligned}$$

we get

$$a_0^2 + a_0c_0 - b_0^2 - b_0d_0 - 2(a_0c_1 + a_1 - d_1b_0 - b_1) \equiv 0 \bmod 4.$$

Applying (4.9), this becomes $a_0^2 + a_0c_0 - b_0^2 - b_0d_0 \equiv 0 \bmod 4$, contradicting (4.10).

Now suppose that $2^u \parallel f(1), g(1)$, $u \geq 1$. Since c_0 and d_0 are even, (4.8) becomes

$$-a_0c_1 + a_0^2 - b_0d_1 + b_0^2 \equiv 0 \bmod 2. \tag{4.11}$$

Notice we cannot have c_1, d_1 both odd or both even, else

$$\ell_1 = |c_0 - c_1 + ic_1 + 2\alpha|^2 + |d_0 - d_1 + id_1 + 2\beta|^2 \equiv 2c_1^2 + 2d_1^2 \bmod 4$$

would be divisible by 4.

We cannot have a_0, b_0 both odd, else (4.11) becomes $c_1 + d_1 \equiv 0 \bmod 2$, contradicting c_1, d_1 having opposite parity. If $u = 1$ we can rule out a_0, b_0 both even, else $2 \parallel f(1)+2h(1) = c_0+2a_0$, $g(1) + 2k(1) = d_0 + 2b_0$ (we ruled out m_1 and m_3 both having $u = v$). If $u \geq 2$ we cannot have a_0, b_0 both even, else 4 divides both terms, $2^4 \mid m_3$, $2^7 \mid m_1$ and $2^{7+2+4+2+4} \mid D$. So a_0, b_0 like c_1, d_1 have opposite parity. From

$$f(-1) + 2h(-1) \equiv c_0 - 2c_1 + 2a_0 \bmod 4, \quad g(-1) + 2k(-1) = d_0 - 2d_1 + 2b_0 \bmod 4$$

we cannot have $a_0 \equiv c_1 \bmod 2$ and $b_0 \equiv d_1 \bmod 2$, else if $u = 1$ we would have a single 2 dividing both (ruled out) and if $u = 2$ we would have 4 dividing both and $2^4 \mid m_4$, $2^7 \mid m_1$. Hence we must have $a_0 \equiv d_1$, $b_0 \equiv c_1 \bmod 2$ and (4.11) becomes $a_0^2 + b_0^2 \equiv 0 \bmod 2$, contradicting that a_0, b_0 have opposite parity.

The $2^{16} \parallel \mathcal{D}$ are of the stated form. Suppose now that we have $\mathcal{D} = 2^{16}m$, with $m \equiv -1 \bmod 8$, that is not of the form (4.4) or (4.5). Note, $\ell_1\ell_2$ does not contain a prime $p \equiv 1 \bmod 4$ or two primes $p_1, p_2 \equiv 3 \bmod 4$ (else it will be type (4.4) with $\ell = p$ or p_1p_2), and $\mathcal{D}$ has no factor $\pm 3 \bmod 8$ (else it will be type (4.5)).

If $2^2 \mid \ell_1$ or ℓ_2 then $2^2 \parallel \ell_1, \ell_2$ and $2^2 \parallel m_1, m_2, m_3, m_4$ and $f(1), g(1)$ are even. Now $m_1/4 = (f(1)/2)^2 - (g(1)/2)^2 \equiv \pm 1 \bmod 8$ and likewise for $m_2/4, m_3/4$ and $m_4/4$, with their product $-1 \bmod 8$. Switching f and g as necessary and rearranging, we can assume $m_1/4 \equiv -1 \bmod 8$ and $m_2/4, m_3/4, m_4/4 \equiv 1 \bmod 8$. That is $4 \mid f(1)/2$ and $f(1)/2 + h(1)$, $f(-1)/2, f(-1)/2 + h(-1)$ are all odd. From the first two $h(1)$ is odd, from the second two, $h(-1)$ is even, but $h(1)$ and $h(-1)$ must have the same parity. Hence we can assume that $2 \parallel \ell_1, \ell_2$, moreover that $\ell_1 = \ell_2 = 2$, or one is 2 and the other $2p$ for some prime $p = 3 \bmod 4$.

If $f(1) = c_0$ and $g(1) = d_0$ are odd, then plainly $2^3 \parallel m_1, m_2, m_3, m_4$. We rule out one of ℓ_1, ℓ_2 being $2 \bmod 8$ and the other $6 \bmod 8$. In this case (4.7) becomes

$$1 \equiv -a_0c_1 - a_1 - b_0d_1 - b_1 \bmod 2. \tag{4.12}$$

But the difference of

$$m_4 \equiv (c_0 - 2c_1 + 4c_2 + 2a_0 - 4a_1)^2 - (d_0 - 2d_1 + 4d_2 + 2b_0 - 4b_1)^2 \equiv 8 \bmod 16$$

and

$$m_2 \equiv (c_0 - 2c_1 + 4c_2)^2 - (d_0 - 2d_1 + 4d_2)^2 \equiv 8 \bmod 16$$

gives

$$4(a_0^2 + a_0c_0 - b_0^2 - b_0d_0) - 8(a_1c_0 + a_0c_1 - b_1d_0 - b_0d_1) \equiv 0 \bmod 16,$$

where

$$4(a_0^2 + a_0c_0 - b_0^2 - b_0d_0) = m_3 - m_1 \equiv 0 \bmod 16,$$

and $a_1 + a_0c_1 - b_1 - b_0d_1 \equiv 0 \bmod 2$, contradicting (4.12). This just leaves us with the case $\ell_1 = \ell_2 = 2$ considered in the lemma below.

Suppose $f(1) = c_0 = 2c$, $g(1) = d_0 = 2d$ are even. If c and d have opposite parity then $2^2 \parallel m_1$, if both are odd then $2^5 \mid m_1$ and if $c = 2c'', d = 2d''$ then $2^4 \parallel m_1$ if c'' and d'' have opposite parity and $2^6 \mid m_1$ otherwise. Moreover if c and d have the same parity and 2^2 divides

$$m_1/4 = c^2 - d^2,$$

then 2^4 must also divide at least one of the other m_i. To see this observe that if a_0 and b_0 have the same parity then 2^2 divides

$$m_3/4 = (c + a_0)^2 - (d + b_0)^2, \tag{4.13}$$

if c_1 and d_1 have the same parity then 2^2 divides

$$m_2/4 \equiv (c - c_1 + 2c_2)^2 - (d - d_1 + 2d_2)^2 \bmod 8, \tag{4.14}$$

and if both a_0 and b_0, and c_1 and d_1 have opposite parity, then $a_0 - c_1$ and $b_0 - d_1$ have the same parity and 2^2 divides

$$m_4/4 \equiv (c - c_1 + 2c_2 + a_0 - 2a_1)^2 - (d - d_1 + 2d_2 + b_0 - 2b_1)^2 \bmod 8. \tag{4.15}$$

Hence, rearranging as necessary, we can assume that $2^4 \parallel m_1$ and one other m_i, and $2^2 \parallel m_i$ for the other two m_i. In particular $c_0 = 4c'$ and $d_0 = 4d'$ with c', d' of opposite parity. Suppose now that one of ℓ_1, ℓ_2 is $2 \bmod 8$ and the other $6 \bmod 8$, so that (4.7) becomes

$$1 \equiv -a_0c_1 + a_0^2 - b_0d_1 + b_0^2 \bmod 2. \tag{4.16}$$

Notice that this rules out a_0, b_0 both even or c_1, d_1 both odd. We can rule out a_0, b_0 both odd, else $2^3 \mid m_3/4$ in (4.13), and c_1, d_1 both even else

$$\ell_1 = |4c' + c_1(i-1) + 2i\alpha|^2 + |4d' + d_1(i-1) + 2i\beta|^2 \equiv 0 \bmod 4.$$

Hence $a_0 - c_1$ and $b_0 - d_1$ have the same parity, but cannot be odd, else $2^3 \mid m_4/4$ in (4.15). Hence $c_1 \equiv a_0 \bmod 2$ and $d_1 \equiv b_0 \bmod 2$, violating (4.16). This just leaves the case $\ell_1 = \ell_2 = 2$ dealt with in the next lemma. □

Lemma 4.1. *All* $\mathbb{Z}_2 \times Q_8$ *determinants* $2^{16}m$ *with* $m \equiv 7 \bmod 8$ *and* $\ell_1 = \ell_2 = 2$ *in* (4.6) *must be of the form* (4.5).

Proof. Suppose that $\mathcal{D} = 2^{16}m$, where $\ell_1 = \ell_2 = 2$, and all the factors of m are $\pm 1 \bmod 8$. We show that $m \equiv 1 \bmod 8$. Hence any with $m \equiv -1 \bmod 8$ must have a factor $\pm 3 \bmod 8$ and be of the form (4.5).

Case 1: $f(1)$ and $g(1)$ are even. Since $|f(i)|^2$ and $|g(i)|^2$ are both even, we must have one of them 2 and the other 0. Switching f and g and replacing $f(x)$ by $\pm f(\pm x)$ as necessary, we can assume that $f(i) = 1 + i$ and $g(i) = 0$. Hence we can write

$$f(x) = 1 + x + (x^2 + 1)v(x), \quad g(x) = (x^2 + 1)u(x).$$

Note 2^2 divides $|g(i)+2k(i)|^2$, so this term must also be zero, while $f(i)+2h(i)=\varepsilon+\delta i$ with $\delta,\varepsilon=\pm1$, and

$$\begin{aligned}f(x)+2h(x)&=\varepsilon+\delta x+(x^2+1)(v(x)+2h_1(x)),\\ g(x)+2k(x)&=(x^2+1)(u(x)+2k_1(x)).\end{aligned}$$

Hence

$$\begin{aligned}m_1/4&=(1+v(1))^2-u(1)^2,\\ m_2/4&=v(-1)^2-u(-1)^2,\\ m_3/4&=\left(\frac{1}{2}(\varepsilon+\delta)+v(1)+2h_1(1)\right)^2-(u(1)+2k_1(1))^2,\\ m_4/4&=\left(\frac{1}{2}(\varepsilon-\delta)+v(-1)+2h_1(-1)\right)^2-(u(-1)+2k_1(-1))^2.\end{aligned}$$

Note, one of $1+v(1)$ and $v(-1)$ must be odd, and hence $u(1),u(-1)$ must be even (else $2^3\mid m_1/4$ or $m_2/4$).

(i) **Suppose that $v(1)$ is odd.** Since $m_2/4\not\equiv-3 \bmod 8$ we must have $m_2/4\equiv 1 \bmod 8$, $4\mid u(-1)$, and

$$\frac{m_1}{2^4}=\left(\frac{1+v(1)}{2}\right)^2-\left(\frac{u(1)}{2}\right)^2.$$

If $\delta=-\varepsilon$ then $m_3/4\equiv 1 \bmod 8$, $4\mid(u(1)+2k_1(1))$, and

$$\frac{m_4}{2^4}=\left(\frac{\varepsilon+v(-1)}{2}+h_1(-1)\right)^2-\left(\frac{u(-1)}{2}+k_1(-1)\right)^2.$$

If $2\mid u(1)/2$ then $2\mid k_1(1)$, $2\mid(u(-1)/2+k_1(-1))$, and $m_1/2^4, m_4/2^4\equiv 1 \bmod 8$. If $2\nmid u(1)/2$ then $2\nmid k_1(1)$, $2\nmid(u(-1)/2+k_1(-1))$, and $m_1/2^4, m_4/2^4\equiv -1 \bmod 8$. In both cases $m_1m_2m_3m_4/2^{12}\equiv 1 \bmod 8$.

If $\delta=\varepsilon$ we have $m_4/4\equiv 1 \bmod 8$, $4\mid(u(-1)+2k_1(-1))$, $2\mid k_1(-1),k_1(1)$ and

$$\frac{m_3}{2^4}=\left(\frac{\varepsilon+v(1)}{2}+h_1(1)\right)^2-\left(\frac{u(1)}{2}+k_1(1)\right)^2.$$

If $2\mid u(1)/2$ then $m_1/2^4, m_3/2^4\equiv 1 \bmod 8$ and if $2\nmid u(1)/2$ both are $-1 \bmod 8$. Again $m_1m_2m_3m_4/2^{12}\equiv 1 \bmod 8$.

(ii) **Suppose that $v(1)$ is even.** In this case $m_1/4\equiv 1 \bmod 8$, $4\mid u(1)$ and

$$\frac{m_2}{2^4}=\left(\frac{v(-1)}{2}\right)^2-\left(\frac{u(-1)}{2}\right)^2.$$

If $\delta=-\varepsilon$ then $m_4/4\equiv 1 \bmod 8$, $4\mid(u(-1)+2k_1(-1))$, and

$$\frac{m_3}{2^4}=\left(\frac{v(1)}{2}+h_1(1)\right)^2-\left(\frac{u(1)}{2}+k_1(1)\right)^2.$$

If $2 \mid u(-1)/2$ then $m_2/2^4 \equiv 1 \bmod 8$ and $2 \mid k_1(-1)$, $2 \mid (u(1)/2 + k_1(1))$ and $m_3/2^4 \equiv 1 \bmod 8$. If $2 \nmid u(-1)/2$ then $m_2/2^4 \equiv -1 \bmod 8$, $2 \nmid k_1(-1)$, $2 \nmid (u(1)/2 + k_1(1))$ and $m_3/2^4 \equiv -1 \bmod 8$. Again, $m_1m_2m_3m_4/2^{12} \equiv 1 \bmod 8$.

If $\delta = \varepsilon$ then $m_3/4 \equiv 1 \bmod 8$, $4 \mid (u(1) + 2k_1(1))$, $2 \mid k_1(1), k_1(-1)$ and

$$\frac{m_4}{2^4} = \left(\frac{v(-1)}{2} + h_1(-1)\right)^2 - \left(\frac{u(-1)}{2} + k_1(-1)\right)^2.$$

If $2 \mid u(-1)/2$ then $m_2/2^4, m_4/2^4 \equiv 1 \bmod 8$. If $2 \nmid u(-1)/2$ then $m_2/2^4, m_4/2^4 \equiv -1 \bmod 8$. In both cases $m_1m_2m_3m_4/2^{12} \equiv 1 \bmod 8$.

In conclusion, there are no cases where $\mathcal{D}/2^{16} = m_1m_2m_3m_4/2^{12} \equiv -1 \bmod 8$.

Case 2: $f(1)$ and $g(1)$ are odd. In this case we have $2^3 \parallel m_1, m_2, m_3, m_4$. From $\ell_1 = \ell_2 = 2$ we must have $f(i), g(i), f(i) + 2h(i), g(i) + 2k(i) = \pm 1$ or $\pm i$. Multiplying the f and h or the g and k through by ± 1 or $\pm x$ we can assume that $f(i) = 1$ and $g(i) = 1$ and

$$f(x) = 1 + (x^2 + 1)v(x), \quad g(x) = 1 + (x^2 + 1)u(x).$$

Clearly we must have $f(i) + 2h(i), g(i) + 2k(i) = \pm 1$ and

$$f(x) + 2h(x) = \varepsilon + (x^2 + 1)(v(x) + 2h_1(x)), \quad g(x) + 2k(x) = \delta + (x^2 + 1)(u(x) + 2k_1(x))$$

for some $\varepsilon, \delta = \pm 1$. Hence

$$\frac{m_1}{4} = (1 + u(1) + v(1))(v(1) - u(1)),$$
$$\frac{m_3}{4} = \left(\frac{\varepsilon + \delta}{2} + v(1) + u(1) + 2h_1(1) + 2k_1(1)\right)\left(\frac{\varepsilon - \delta}{2} + v(1) - u(1) + 2h_1(1) - 2k_1(1)\right).$$

Similarly for $m_2/4$ and $m_4/4$ with $u(-1), v(-1), h_1(-1), k_1(-1)$ in place of $u(1), v(1), h_1(1)$, $k_1(1)$.

(i) **Suppose that $u(1) + v(1)$ is even.** In this case $m_1/8 = \alpha_1\alpha_2$ with

$$\alpha_1 = 1 + u(1) + v(1), \quad \alpha_2 = \frac{1}{2}(v(1) - u(1))$$

When $\delta = -\varepsilon$ we have $m_3/8 = \lambda_1\lambda_2$, with

$$\lambda_1 = \frac{1}{2}(v(1) + u(1)) + h_1(1) + k_1(1),$$
$$\lambda_2 = \varepsilon + v(1) - u(1) + 2h_1(1) - 2k_1(1).$$

Recall that by assumption all these factors are $\pm 1 \bmod 8$. Since

$$\lambda_1 = \varepsilon\alpha_2 + \frac{1}{2}(1 - \varepsilon)v(1) + \frac{1}{2}(1 + \varepsilon)u(1) + h_1(1) + k_1(1),$$

we have $2 \mid \frac{1}{2}(1 - \varepsilon)v(1) + \frac{1}{2}(1 + \varepsilon)u(1) + h_1(1) + k_1(1)$ and

$$\lambda_2 = \varepsilon\alpha_1 + (1 - \varepsilon)v(1) - (1 + \varepsilon)u(1) + 2h_1(1) - 2k_1(1) \equiv \varepsilon\alpha_1 \bmod 4.$$

Hence $\lambda_2 \equiv \varepsilon\alpha_1 \bmod 8$ and $4 \mid \frac{1}{2}(1-\varepsilon)v(1) - \frac{1}{2}(1+\varepsilon)u(1) + h_1(1) - k_1(1)$. So

$$\lambda_1\lambda_2 \equiv (\varepsilon\alpha_2 + (1+\varepsilon)u(1) + 2k_1(1))\varepsilon\alpha_1 \equiv \alpha_1\alpha_2 + (1+\varepsilon)u(1) + 2k_1(1) \bmod 4,$$

and $m_3/8 \equiv m_1/8 \bmod 4$, and $m_1m_3/2^6 \equiv 1 \bmod 8$, iff $2 \mid \frac{1}{2}(1+\varepsilon)u(1) + k_1(1)$. Clearly $2 \mid \frac{1}{2}(1+\varepsilon)u(1)+k_1(1)$ iff $2 \mid \frac{1}{2}(1+\varepsilon)u(-1)+k_1(-1)$, giving $m_1m_3/2^6 \equiv m_2m_4/2^6 \bmod 8$, and $m = m_1m_2m_3m_4/2^{12} \equiv 1 \bmod 8$.

Similarly, when $\delta = \varepsilon$ we have

$$\lambda_1 = \frac{1}{2}(v(1) - u(1)) + h_1(1) - k_1(1),$$
$$\lambda_2 = \varepsilon + v(1) + u(1) + 2h_1(1) + 2k_1(1).$$

Since

$$\lambda_1 = \varepsilon\alpha_2 + \frac{1}{2}(1-\varepsilon)v(1) - \frac{1}{2}(1-\varepsilon)u(1) + h_1(1) - k_1(1),$$

we have $2 \mid \frac{1}{2}(1-\varepsilon)v(1) - \frac{1}{2}(1-\varepsilon)u(1) + h_1(1) - k_1(1)$, and

$$\lambda_2 = \varepsilon\alpha_1 + (1-\varepsilon)v(1) + (1-\varepsilon)u(1) + 2h_1(1) + 2k_1(1) \equiv \varepsilon\alpha_1 \bmod 4.$$

So $\lambda_2 \equiv \varepsilon\alpha_1 \bmod 8$, $4 \mid \frac{1}{2}(1-\varepsilon)v(1) + \frac{1}{2}(1-\varepsilon)u(1) + h_1(1) + k_1(1)$ and

$$\lambda_1\lambda_2 \equiv (\varepsilon\alpha_2 - (1-\varepsilon)u(1) - 2k_1(1))\varepsilon\alpha_1 \equiv \alpha_1\alpha_2 - (1-\varepsilon)u(1) - 2k_1(1) \bmod 4,$$

giving $m_1m_3/2^6 \equiv 1 \bmod 8$, iff $2 \mid \frac{1}{2}(1-\varepsilon)u(1) + k_1(1)$. Again $m \equiv 1 \bmod 8$.

(ii) **Suppose that $u(1) + v(1)$ is odd.** In this case

$$\alpha_1 = v(1) - u(1), \quad \alpha_2 = \frac{1}{2}(1 + u(1) + v(1)).$$

When $\delta = -\varepsilon$ we have

$$\lambda_1 = \frac{1}{2}(\varepsilon + v(1) - u(1)) + h_1(1) - k_1(1),$$
$$\lambda_2 = v(1) + u(1) + 2h_1(1) + 2k_1(1).$$

So

$$\lambda_1 = \varepsilon\alpha_2 + \frac{1}{2}(1-\varepsilon)v(1) - \frac{1}{2}(1+\varepsilon)u(1) + h_1(1) - k_1(1),$$

and $2 \mid \frac{1}{2}(1-\varepsilon)v(1) - \frac{1}{2}(1+\varepsilon)u(1) + h_1(1) - k_1(1)$, giving

$$\lambda_2 = \varepsilon\alpha_1 + (1-\varepsilon)v(1) + (1+\varepsilon)u(1) + 2h_1(1) + 2k_1(1) \equiv \varepsilon\alpha_1 \bmod 4.$$

Hence $\lambda_2 \equiv \varepsilon\alpha_1 \bmod 8$, $4 \mid \frac{1}{2}(1-\varepsilon)v(1) + \frac{1}{2}(1+\varepsilon)u(1) + h_1(1) + k_1(1)$ and

$$\lambda_1\lambda_2 \equiv (\varepsilon\alpha_2 - (1+\varepsilon)u(1) - 2k_1(1))\varepsilon\alpha_1 \equiv \alpha_1\alpha_2 - (1+\varepsilon)u(1) - 2k_1(1) \bmod 4.$$

Thus $m_1m_3/2^6 \equiv 1 \bmod 8$ iff $2 \mid \frac{1}{2}(1+\varepsilon)u(1) + k_1(1)$. Again $m \equiv 1 \bmod 8$.

When $\delta = \varepsilon$ we have

$$\lambda_1 = \frac{1}{2}(\varepsilon + v(1) + u(1)) + h_1(1) + k_1(1),$$
$$\lambda_2 = v(1) - u(1) + 2h_1(1) - 2k_1(1).$$

Hence

$$\lambda_1 = \varepsilon\alpha_2 + \frac{1}{2}(1-\varepsilon)v(1) + \frac{1}{2}(1-\varepsilon)u(1) + h_1(1) + k_1(1),$$

and $2 \mid \frac{1}{2}(1-\varepsilon)v(1) + \frac{1}{2}(1-\varepsilon)u(1) + h_1(1) + k_1(1)$, giving

$$\lambda_2 = \varepsilon\alpha_1 - (1-\varepsilon)u(1) + (1-\varepsilon)v(1) + 2h_1(1) - 2k_1(1) \equiv \varepsilon\alpha_1 \bmod 4.$$

So $\lambda_2 \equiv \varepsilon\alpha_1 \bmod 8$, $4 \mid \frac{1}{2}(1-\varepsilon)v(1) - \frac{1}{2}(1-\varepsilon)u(1) + h_1(1) - k_1(1)$, and

$$\lambda_1\lambda_2 \equiv (\varepsilon\alpha_2 + (1-\varepsilon)u(1) + 2k_1(1))\varepsilon\alpha_1 \equiv \alpha_1\alpha_2 + (1-\varepsilon)u(1) + 2k_1(1) \bmod 4.$$

Hence $m_1m_3/2^6 \equiv 1 \bmod 8$ iff $2 \mid \frac{1}{2}(1-\varepsilon)u(1) + k_1(1)$. Again $m \equiv 1 \bmod 8$. □

Acknowledgements

The authors are grateful to one of the referees for pointing out existing results in [8] and [9] as well as catching some typos.

References

[1] Boerkoel, T., & Pinner, C. (2018). Minimal group determinants and the Lind–Lehmer problem for dihedral groups. *Acta Arithmetica*, 186(4), 377–395.

[2] Conrad, K. (1998). The origin of representation theory. *L'Enseignement Mathématique*, 44(3–4), 361–392.

[3] DeSilva, D., Mossinghoff, M., Pigno, V., & Pinner, C. (2019). The Lind–Lehmer constant for certain p-groups. *Mathematics of Computation*, 88(316), 949–972.

[4] DeSilva, D., & Pinner, C. G. (2014). The Lind–Lehmer constant for $\mathbb{Z}_p^n$. *Proceedings of the American Mathematical Society*, 142, 1935–1941.

[5] Frobenius, F. G. (1968). Über die Primefactoren der Gruppendeterminante. *Gesammelte Ahhand-lungen, Band III*. Springer, New York, pp. 38–77. MR0235974.

[6] Johnson, K. W. (2019). *Group Matrices Group Determinants and Representation Theory*. Lecture Notes in Mathematics 2233, Springer, Cham.

[7] Laquer, H. T. (1980). Values of circulants with integer entries. *A Collection of Manuscripts Related to the Fibonacci Sequence*. Fibonacci Association, Santa Clara, pp. 212–217. MR0624127.

[8] Mahoney, M. K. (1982). Determinants of integral group matrices for some nonabelian 2-generator groups. *Linear and Multilinear Algebra*, 11(2), 189–201.

[9] Mahoney, M. K., & Newman, M. (1980). Determinants of abelian group matrices. *Linear and Multilinear Algebra*, 9(2), 121–132.

[10] Mossinghoff, M., & Pinner, C. (2023). Prime power order circulant determinants. *Illinois Journal of Mathematics*, 67(2), 333–362.

[11] Newman, M. (1980). On a problem suggested by Olga Taussky-Todd. *Illinois Journal of Mathematics*, 24, 156–158.

[12] Newman, M. (1980). Determinants of circulants of prime power order. *Linear Multilinear Algebra*, 9(3), 187–191. MR0601702.

[13] Paudel, B., & Pinner, C. (2022). Integer circulant determinants of order 15. *Integers*, 22, Article A4.

[14] Pinner, C., & Smyth, C. (2020). Integer group determinants for small groups. *The Ramanujan Journal*, 51(2), 421–453.

[15] Taussky-Todd, O. (1977). Integral group matrices. *Notices of the American Mathematical Society*, 24(3), A-345. (Abstract no. 746-A15, 746th Meeting, Hayward, CA, Apr. 22–23, 1977).

[16] Yamaguchi, N., & Yamaguchi, Y. (2022). *Generalized Dedekind's theorem and its application to integer group determinants*. arXiv: 2203.14420v2 [math.RT].

[17] Yamaguchi, N., & Yamaguchi, Y. (2023). Remark on Laquer's theorem for circulant determinants. *International Journal of Group Theory*, 12(4), 265–269.

[18] Yamaguchi, Y., & Yamaguchi, N. (2022). *Integer group determinants for* C_4^2. arXiv: 2211.01597 [math.NT].

[19] Yamaguchi, Y., & Yamaguchi, N. (2022). *Integer group determinants for abelian groups of order* 16, arXiv: 2211.14761 [math.NT].

[20] Yamaguchi, Y., & Yamaguchi, N. (2023). Integer group determinants for C_2^4. *The Ramanujan Journal*, DOI: 10.1007/s11139-023-00727-z.

[21] Yamaguchi, Y., & Yamaguchi, N. (2023). Integer circulant determinants of order 16. *The Ramanujan Journal*, 61, 1283–1294.