INTEGER GROUP DETERMINANTS FOR SMALL GROUPS

CHRISTOPHER PINNER AND CHRISTOPHER SMYTH

Abstract. For every group of order at most 14 we determine the values taken by its group determinant when its variables are integers.

1. Introduction

For a finite group $G = \{g_1, \dots, g_n\}$ of order n, we assign a variable x_g for each element $g \in G$ and define its *group determinant* $\mathscr{D}_G(x_{g_1}, \dots, x_{g_n})$ to be the determinant of the $n \times n$ matrix whose (i,j)th entry is $x_{g_i g_j^{-1}}$. In the case of the cyclic group of order n, the group determinant becomes an $n \times n$ *circulant determinant*, where each row is obtained from the previous one by a cyclic shift one step to the right. At the meeting of the American Mathematical Society in Hayward, California, in April 1977, Olga Taussky-Todd asked which integers could be obtained as an $n \times n$ circulant determinant when the entries are all integers. Of course we can ask for a complete description of the group determinants over the integers for any group G, not just for the cyclic groups. Thus our problem is to determine the set

$$\mathcal{S}(G) = \{\mathscr{D}_G(x_{g_1}, \dots, x_{g_n}) \,:\, x_{g_1}, \dots, x_{g_n} \in \mathbb{Z}\}.$$

For the additive cyclic group $\mathbb{Z}_n$ of order n, Laquer [14] and Newman [20, 21] gave divisibility conditions on the integers that can be group determinants, as well as sets of achievable values; for example any integer coprime to n or a multiple of n^2 will be a group determinant, if m is a determinant then so is $-m$, and if $p \mid m$ and $p^\alpha \parallel n$ then $p^{\alpha+1} \mid m$. Conditions like these enabled them to obtain a complete description of the values for certain cyclic groups. For example Laquer [14] and Newman [20] showed that for a prime p

$$\mathcal{S}(\mathbb{Z}_p) = \{p^a m_p \,:\, a = 0, a \geq 2\}, \tag{1.1}$$

while for p an odd prime, Laquer [14] showed that

$$\mathcal{S}(\mathbb{Z}_{2p}) = \{2^a p^b m_{2p} \,:\, a = 0, a \geq 2, \;\; b = 0, b \geq 2\}. \tag{1.2}$$

Newman [21] determined $\mathcal{S}(\mathbb{Z}_9)$ as

$$\mathcal{S}(\mathbb{Z}_9) = \{3^a m_3 \,:\, a = 0, a \geq 3\}, \tag{1.3}$$

with upper and lower set inclusions for general $\mathbb{Z}_{p^2}$. In the above, and henceforth, m_t denotes an arbitrary integer coprime to t.

Date: August 12, 2018.

2010 *Mathematics Subject Classification.* Primary: 11R06, 15B36; Secondary: 11B83, 11C08, 11C20, 11G50, 11R09, 11T22, 43A40.

Key words and phrases. Lind-Lehmer constant, Mahler measure, group determinant, dihedral group, dicyclic group, circulant determinant.

For a polynomial $F(x_1,\dots,x_r)$ in $\mathbb{Z}[x_1,\dots,x_r]$, the traditional logarithmic Mahler measure $m(F)$ can be defined by

$$m(F) = \log M(F) = \int_0^1 \cdots \int_0^1 \log|F(e^{2\pi i x_1},\dots,e^{2\pi i x_r})| dx_1 \cdots dx_r.$$

In 2005 Lind [18] viewed the traditional Mahler measure as a measure on the circle group $(\mathbb{R}/\mathbb{Z})^r$ and generalised the concept to an arbitrary compact abelian group. In particular for a finite group

$$G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r} \tag{1.4}$$

one can define the logarithmic measure of an $F(x_1,\dots,x_r)$ in $\mathbb{Z}[x_1,\dots,x_r]$ relative to G to be

$$m_G(f) = \frac{1}{|G|}\log|M_G(F)|,$$

where

$$M_G(F) = \prod_{j_1=1}^{n_1} \cdots \prod_{j_r=1}^{n_r} F(\omega_{n_1}^{j_1},\dots,\omega_{n_r}^{j_r}), \qquad \omega_n := e^{2\pi i/n}.$$

Curiously, the Lind variant of the Mahler measure for $\mathbb{Z}_n$ had essentially appeared in a 1916 paper of Pierce [22], and also in the famous paper of Lehmer [16], in the form $\Delta_n := \prod_{i=1}^r(\alpha_i^n - 1) = (-1)^{rn} M_{\mathbb{Z}_n}(F)$, for a monic integer one-variable polynomial F with roots $\alpha_1,\dots,\alpha_r$.

As observed by Dedekind, the group of characters $\hat{G}$ of a finite abelian group G can be used to factor its group determinant as

$$\mathscr{D}_G(x_{g_1},\dots,x_{g_n}) = \prod_{\chi\in\hat{G}} \left(\chi(g_1)x_{g_1} + \cdots + \chi(g_n)x_{g_n}\right). \tag{1.5}$$

On making the characters explicit, it is readily seen that for a group G of the form (1.4) we have

$$\mathscr{D}_G(a_{g_1},\dots,a_{g_n}) = M_G(F), \tag{1.6}$$

where

$$F(x_1,\dots,x_r) = \sum_{g=(t_1,\dots t_r)\in G} a_g x_1^{t_1}\cdots x_r^{t_r}, \tag{1.7}$$

a connection observed by Vipismakul [26] in his thesis. Of course any polynomial in $\mathbb{Z}[x_1,\dots,x_r]$ can be reduced to (1.7) by working in the ring

$$\mathbb{Z}[x_1,\dots,x_r]/\langle x_1^{n_1}-1,\dots,x_r^{n_r}-1\rangle. \tag{1.8}$$

Throughout the paper, the variables in such integer polynomial rings will be assumed to commute when the associated group is abelian, but not, as for instance in (1.11) or (2.1) below, when the associated group in non-abelian. We are really defining measures on the elements of the group ring $\mathbb{Z}[G]$.

Kaiblinger [13] used the Lind measure approach to obtain

$$\mathcal{S}(\mathbb{Z}_4) = \{2^a m_2 \,:\, a=0, a\geq 4\} \tag{1.9}$$

and

$$\mathcal{S}(\mathbb{Z}_8) = \{2^a m_2 \,:\, a=0, a\geq 5\}, \tag{1.10}$$

with upper and lower set inclusions for the other $\mathbb{Z}_{2^k}$. Defining $\lambda(G)$ to be the smallest non-trivial determinant value

$$\lambda(G) := \min\{|s| \,:\, s \in \mathcal{S}(G),\ s \neq 0, \pm 1\},$$

Kaiblinger [12] obtained $\lambda(\mathbb{Z}_n)$ when $420 \nmid n$; this was extended to all n with $892371480 \nmid n$ by Pigno and Pinner [23]. Values of $\lambda(G)$ for non-cyclic abelian G were considered in [9, 10, 24, 4].

As explored in Boerkoel and Pinner [3], the connection (1.6) between Lind measures and group determinants suggests a way to extend the concept of Lind measure to non-abelian finite groups, and to measures on (not necessarily commutative) polynomial rings modulo appropriate group relations. See Dasbach and Lalín[7] for another approach. As observed by Frobenius, see for example [11, 5], the counterpart to (1.5) for a non-abelian group will involve non-linear factors and the set of irreducible representations for G, which, although no longer a group, we still denote by $\hat{G}$. Specifically,

$$\mathscr{D}_G(x_{g_1}, \ldots, x_{g_n}) = \prod_{\rho \in \hat{G}} \det\left(\sum_{g \in G} x_g \rho(g)\right)^{\deg(\rho)}.$$

For example, for the dihedral group $G = D_{2n}$ of order $2n$, one can define the measure $M_G(F)$ of an F in

$$\mathbb{Z}[x,y]/\langle x^n - 1, y^2 - 1, xy - yx^{-1}\rangle, \tag{1.11}$$

reduced to the form

$$F(x) = f(x) + yg(x), \quad f(x) = \sum_{j=0}^{n-1} a_j x^j, \quad g(x) = \sum_{j=0}^{n-1} b_j x^j,$$

by

$$M_G(F) = \mathscr{D}_G(a_0, \ldots, a_{n-1}, b_0, \ldots, b_{n-1}).$$

This was shown in [3, Section 3] to equal

$$M_{\mathbb{Z}_n}\left(f(x)f(x^{-1}) - g(x)g(x^{-1})\right), \tag{1.12}$$

and was used in [3] to determine $\mathcal{S}(D_{2p})$ for p an odd prime as

$$\mathcal{S}(D_{2p}) = \{2^a p^b m_{2p} \,:\, a = 0, a \geq 2,\ \ b = 0, b \geq 3\}, \tag{1.13}$$

(which includes S_3 under the guise of D_6). Also

$$\mathcal{S}(D_{4p}) = \mathcal{S}_{\text{odd}}(D_{4p}) \cup \mathcal{S}_{\text{even}}(D_{4p}),$$

where

$$\mathcal{S}_{\text{odd}}(D_{4p}) = \{m \equiv 1 \bmod 4 \,:\, p \nmid m, p^3 \mid m\}. \tag{1.14}$$

and

$$\mathcal{S}_{\text{even}}(D_{4p}) = \{2^a p^b m_{2p} \,:\, a = 4, a \geq 6,\ \ b = 0, b \geq 3\}. \tag{1.15}$$

For $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, viewed as D_4 :

$$\mathcal{S}(\mathbb{Z}_2 \times \mathbb{Z}_2) = \{4m+1,\ \ 2^4(2m+1),\ \ 2^6 m \,:\, m \in \mathbb{Z}\}, \tag{1.16}$$

for $G = D_8$:

$$\mathcal{S}(D_8) = \{4m+1,\ \ 2^8 m \,:\, m \in \mathbb{Z}\}, \tag{1.17}$$

for $G = D_{16}$:

$$\mathcal{S}(D_{16}) = \{4m+1,\ \ 2^{10}m\ :\ m \in \mathbb{Z}\}, \tag{1.18}$$

with upper and lower set inclusions for the other D_{2^k}. For $G = D_{2p^2}$ when $p = 3, 5$ or 7:

$$\mathcal{S}(D_{2p^2}) = \{2^a p^b m_{2p}\ :\ a = 0, a \geq 2,\ \ b = 0, b \geq 5\}.$$

Also, the value of $\lambda(D_k)$ was determined for $k < 3.79 \times 10^{47}$ in [3].

Many of the small groups are of one of the above forms. Indeed for the groups of order at most 14 this just leaves out the groups $G = Q_8, \mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2^3$, $\mathbb{Z}_3 \times \mathbb{Z}_3$, A_4, Q_{12}, $\mathbb{Z}_{12}$ and $\mathbb{Z}_6 \times \mathbb{Z}_2$, where Q_{4n} denotes the dicyclic group of order $4n$. Our goal here is to determine $\mathcal{S}(G)$ for these remaining groups G. As we shall see, for example for $G = \mathbb{Z}_6 \times \mathbb{Z}_2$, these can become complicated very quickly, so developing a general theory for dealing with all finite groups is probably not feasible. While it is known [11] that the group determinant polynomial, $\mathscr{D}_G(x_{g_1}, \ldots, x_{g_n})$, determines the group, it remains unknown as to whether $\mathcal{S}(G)$ also determines the group.

We shall make frequent use of the multiplication property

$$\mathscr{D}_G(a_{g_1}, \ldots, a_{g_n})\mathscr{D}_G(b_{g_1}, \ldots, b_{g_n}) = \mathscr{D}_G(c_{g_1}, \ldots, c_{g_n}),\ \ c_g := \sum_{uv=g} a_u b_v, \tag{1.19}$$

corresponding to multiplication $\left(\sum_{g\in G} a_g g\right)\left(\sum_{g\in G} b_g g\right) = \sum_{g\in G} c_g g$ in $\mathbb{Z}[G]$ (or multiplication and reduction of polynomials subject to the relations). Thus $\mathcal{S}(G)$ is a semigroup.

We shall work interchangeably with the group determinants $\mathscr{D}_G(x_{g_1}, \ldots, x_{g_n})$ and the polynomial measures $M_G(F)$. We begin by expressing the group determinant for the dicyclic group Q_{4n} as a $\mathbb{Z}_{2n}$ Lind measure of an associated polynomial.

2. Dicyclic Groups

We write the dicyclic group of order $4n$ in the form

$$Q_{4n} = \langle a, b\ :\ a^{2n} = 1, b^2 = a^n, ab = ba^{-1}\rangle,$$

and order the elements $1, a, a^2, \ldots, a^{2n-1}, b, ba, \ldots, ba^{2n-1}$.

Our polynomial measures will be defined on

$$\mathbb{Z}[x, y]/\langle x^{2n} - 1, y^2 - x^n, xy - yx^{2n-1}\rangle, \tag{2.1}$$

where we can assume that F in $\mathbb{Z}[x, y]$ has been reduced to the form

$$F(x, y) = f(x) + yg(x), \qquad f(x) = \sum_{j=0}^{2n-1} a_j x^j, \quad g(x) = \sum_{j=0}^{2n-1} b_j x^j. \tag{2.2}$$

For $n = 1$, see (1.9). The case $n = 2$ gives us the classical quaternion group

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}, \quad i^2 = j^2 = k^2 = ijk = -1,$$

under the correspondence $(1, a, a^2, a^3, b, ba, ba^2, ba^3) = (1, i, -1-i, j, -k, -j, k)$.

Our determinant $\mathscr{D}_{Q_{4n}}(a_0, \ldots, a_{2n-1}, b_0, \ldots, b_{2n-1})$ will have four linear factors, corresponding to the characters $\chi(a) = 1$ and $\chi(b) = \pm 1$, and $\chi(a) = -1$ with $\chi(b) = \pm 1$ if n is even and $\chi(b) = \pm i$ if n is odd,

$$\Big(f(1) + g(1)\Big)\Big(f(1) - g(1)\Big)\Big(f(-1) + g(-1)\Big)\Big(f(-1) - g(-1)\Big), \quad n \text{ even},$$
$$\Big(f(1) + g(1)\Big)\Big(f(1) - g(1)\Big)\Big(f(-1) + ig(-1)\Big)\Big(f(-1) - ig(-1)\Big), \quad n \text{ odd}.$$

For the remaining complex $2n$th roots of unity $\omega = \omega_{2n}^j$, $1 \le j \le n-1$, (complex conjugates give the same factors) we have $n-1$ two-dimensional representations

$$\rho(a) = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}, \quad \rho(b) = \begin{pmatrix} 0 & \omega^n \\ 1 & 0 \end{pmatrix},$$

leading to the squares of $n-1$ quadratic factors

$$\begin{aligned} \det\left(\rho\left(\sum_{j=0}^{2n-1} a_j a^j + \sum_{j=0}^{2n-1} b_j b a^j\right)\right) &= \det\begin{pmatrix} f(\omega) & \omega^n g(\omega^{-1}) \\ g(\omega) & f(\omega^{-1}) \end{pmatrix} \\ &= f(\omega)f(\omega^{-1}) - \omega^n g(\omega)g(\omega^{-1}). \end{aligned}$$

Hence we can write

$$\mathscr{D}_{Q_{4n}}(a_0, \dots, a_{2n-1}, b_0, \dots, b_{2n-1}) = \prod_{j=0}^{2n-1} (f(\omega_{2n}^j)f(\omega_{2n}^{-j}) - \omega_{2n}^{jn} g(\omega_{2n}^j)g(\omega_{2n}^{-j}).$$

We take this to be the dicyclic measure of an $F(x,y)$ in $\mathbb{Z}[x,y]$, reduced to the form (2.2),

$$M_{Q_{4n}}(F) = M_{\mathbb{Z}_{2n}}\Big(f(x)f(x^{-1}) - x^n g(x)g(x^{-1})\Big). \tag{2.3}$$

We observe for future reference that

$$\begin{aligned} &M_{\mathbb{Z}_{2n}}\Big(g(x)g(x^{-1}) - x^n f(x)f(x^{-1})\Big) \\ &\qquad = (-1)^n M_{\mathbb{Z}_{2n}}\Big(f(x)f(x^{-1}) - x^n g(x)g(x^{-1})\Big), \end{aligned} \tag{2.4}$$

so that $\mathcal{S}(Q_{4n}) = -\mathcal{S}(Q_{4n})$ when n is odd.

3. Groups of order 8

In this section we determine $\mathcal{S}(G)$ for the five groups of order eight: $G = \mathbb{Z}_8$, D_8, Q_8, $\mathbb{Z}_4 \times \mathbb{Z}_2$ and $\mathbb{Z}_2^3$.

As mentioned in the introduction, $\mathcal{S}(G)$ is already known for $G = \mathbb{Z}_8$ and D_8, namely

$$\mathcal{S}(\mathbb{Z}_8) = \{2m+1 \text{ and } 32m \,:\, m \in \mathbb{Z}\}$$

and

$$\mathcal{S}(D_8) = \{4m+1 \text{ and } 2^8 m \,:\, m \in \mathbb{Z}\}.$$

For the groups $G = D_8, Q_8$ and $\mathbb{Z}_4 \times \mathbb{Z}_2$, the group determinants correspond to Lind-Mahler measures on the two-variable polynomials $F(x,y) \in \mathbb{Z}[x,y]$ reduced to

$$F(x,y) = f(x) + yg(x), \text{ where } f(x) = \sum_{j=0}^{3} a_j x^j, \;\; g(x) = \sum_{j=0}^{3} b_j x^j. \tag{3.1}$$

These are given in terms of Lind-Mahler measures of cyclic groups by (1.12) for D_8, by (2.3) for Q_8, and by

$$M_{\mathbb{Z}_4 \times \mathbb{Z}_2}(F) = M_{\mathbb{Z}_4}(f(x) + g(x)) \cdot M_{\mathbb{Z}_4}(f(x) - g(x)) \tag{3.2}$$

for $\mathbb{Z}_4 \times \mathbb{Z}_2$.

For $G = \mathbb{Z}_2^3$ the determinants correspond to measures of polynomials in $\mathbb{Z}[x, y, z]$, reducible mod $\langle x^2 - 1, y^2 - 1, z^2 - 1\rangle$ to

$$F(x, y, z) = \sum_{i,j,k\in\{0,1\}} a_{i,j,k} x^i y^j z^k \in \mathbb{Z}[x, y, z], \quad M_G(F) = \prod_{x,y,z=\pm 1} F(x, y, z).$$

Theorem 3.1. *We have*

$$\mathcal{S}(\mathbb{Z}_4 \times \mathbb{Z}_2) = \{8m + 1 \text{ and } 2^8 m \,:\, m \in \mathbb{Z}\},$$

$$\mathcal{S}(Q_8) = \mathcal{S}(\mathbb{Z}_4 \times \mathbb{Z}_2) \cup \{(8m - 3)p^2 \,:\, m \in \mathbb{Z},\ p \equiv 3 \bmod 4 \text{ prime}\},$$

and

$$\mathcal{S}(\mathbb{Z}_2^3) = \{8m + 1 \text{ and } 2^8(4m + 1) \text{ and } 2^{12} m \,:\, m \in \mathbb{Z}\}.$$

Note that

$$\mathcal{S}(\mathbb{Z}_2^3) \subsetneq \mathcal{S}(\mathbb{Z}_4 \times \mathbb{Z}_2) \subsetneq \mathcal{S}(Q_8) \subsetneq \mathcal{S}(D_8) \subsetneq \mathcal{S}(\mathbb{Z}_8).$$

The Theorem immediately gives us the minimum non-trivial measure for the groups of order 8.

Corollary 3.2. *We have*

$$\lambda(\mathbb{Z}_4 \times \mathbb{Z}_2) = \lambda(\mathbb{Z}_2^3) = \lambda(Q_8) = 7 \text{ and } \lambda(D_8) = \lambda(\mathbb{Z}_8) = 3.$$

4. The Alternating Group A_4

Taking the two generators

$$\alpha = (123), \quad \beta = (12)(34),$$

we order the elements $(g_1, g_2, \ldots, g_{12})$ of A_4 as

$$\begin{aligned}&(1, (12)(34), (13)(24), (14)(23), (123), (243), (142), (134), (132), (143), (234), (124))\\ &\quad = (1, \beta, \alpha^2\beta\alpha, \alpha\beta\alpha^2, \alpha, \beta\alpha, \alpha^2\beta\alpha^2, \alpha\beta, \alpha^2, \beta\alpha^2, \alpha^2\beta, \alpha\beta\alpha).\end{aligned}$$

Now A_4 has four irreducible representations: three linear ones χ_0, χ_1, χ_2 where $\chi(\beta) = 1$ and $\chi(\alpha) = 1, \omega$ or ω^2 respectively with $\omega := e^{2\pi i/3}$, and one, ρ, of degree 3. This latter representation comes from isometries of the regular tetrahedron (vertices $1, 2, 3, 4$) relative to the three axes passing through the centres of opposite pairs of sides. Explicitly,

$$\rho(\alpha) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \qquad \text{and} \qquad \rho(\beta) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

generating the representation:

$$\rho(\alpha^2\beta\alpha) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho(\alpha\beta\alpha^2) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad \rho(\beta\alpha) = \begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix},$$

$$\rho(\alpha^2\beta\alpha^2) = \begin{pmatrix} 0 & 0 & -1 \\ -1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \rho(\alpha\beta) = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}, \quad \rho(\alpha^2) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

$$\rho(\beta\alpha^2) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0 \end{pmatrix}, \quad \rho(\alpha^2\beta) = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}, \quad \rho(\alpha\beta\alpha) = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{pmatrix}.$$

Writing $x = \sum_i a_i g_i$ in $\mathbb{Z}[G]$, then for $G = A_4$ the group determinant takes the form

$$\mathscr{D}_G(a_1, a_2, \ldots, a_{12}) = l_0 l_1 l_2 D^3$$

where, putting

$$a := a_1 + a_2 + a_3 + a_4, \quad b := a_5 + a_6 + a_7 + a_8 \quad \text{and} \quad c := a_9 + a_{10} + a_{11} + a_{12},$$

we have

$$l_0 = \chi_0(x) = a+b+c, \quad l_1 = \chi_1(x) = a+b\omega+c\omega^2, \quad l_2 = \chi_2(x) = a+b\omega^2+c\omega, \tag{4.1}$$

and

$$D = \det(\rho(x)) = \det \begin{pmatrix} a_1+a_2-a_3-a_4 & a_9+a_{10}-a_{11}-a_{12} & a_5+a_6-a_7-a_8 \\ a_5-a_6-a_7+a_8 & a_1-a_2-a_3+a_4 & a_9-a_{10}-a_{11}+a_{12} \\ a_9-a_{10}+a_{11}-a_{12} & a_5-a_6+a_7-a_8 & a_1-a_2+a_3-a_4 \end{pmatrix}. \tag{4.2}$$

We can regard $\mathscr{D}_G(a_1, a_2, \ldots, a_{12})$ as the Lind measure $M_G(F)$ of the generic polynomial

$$\begin{aligned} F(x,y) = a_1 + a_2 y + a_3 x^2 yx + a_4 xyx^2 + a_5 x + a_6 yx + a_7 x^2 yx^2 \\ + a_8 xy + a_9 x^2 + a_{10} yx^2 + a_{11} x^2 y + a_{12} xyx, \end{aligned}$$

in $\mathbb{Z}[x, y]$ with non-commutative multiplication, and reduction according to the relations

$$x^3 = 1, \quad y^2 = 1, \quad yxy = x^2 yx^2 \quad \text{and} \quad yx^2 y = xyx.$$

Theorem 4.1. *We have* $\mathcal{S}(A_4) = \mathcal{S}(A_4)_{\text{even}} \cup \mathcal{S}(A_4)_{\text{odd}}$, *where*

$$\mathcal{S}(A_4)_{\text{even}} = \{2^a 3^b m_6 \,:\, a = 4, a \geq 8,\ b = 0, b \geq 2\}$$

and

$$\mathcal{S}(A_4)_{\text{odd}} = \{m \equiv 1 \bmod 4 \,:\, 3 \nmid m, 3^2 \mid m\}.$$

5. Groups of Order 12

There are five groups of order twelve: $\mathbb{Z}_{12}$, $\mathbb{Z}_6 \times \mathbb{Z}_2$, D_{12}, Q_{12} and A_4 (dealt with in the previous section).

From [3] we know that $\mathcal{S}(D_{12}) = \mathcal{S}(D_{12})_{\text{even}} \cup \mathcal{S}(D_{12})_{\text{odd}}$, where

$$\mathcal{S}(D_{12})_{\text{even}} = \{2^a 3^b m_6 \,:\, a = 4, a \geq 6, \ \ b = 0, b \geq 3\}$$

and

$$\mathcal{S}(D_{12})_{\text{odd}} = \{m \equiv 1 \bmod 4 \,:\, 3 \nmid m, 3^3 \mid m\}.$$

For the groups $G = Q_{12}$, D_{12} and $\mathbb{Z}_6 \times \mathbb{Z}_2$ we work with measures of polynomials

$$F(x,y) = f(x) + yg(x) \in \mathbb{Z}[x,y], \quad f(x) = \sum_{j=0}^{5} a_j x^j, \ \ g(x) = \sum_{j=0}^{5} b_j x^j. \tag{5.1}$$

These are given in terms of Lind-Mahler measures of cyclic groups by (2.3) for Q_{12}, by (1.12) for D_{12}, and by

$$M_{\mathbb{Z}_6 \times \mathbb{Z}_2}(F) = M_{\mathbb{Z}_6}(f(x) + g(x)) \cdot M_{\mathbb{Z}_6}(f(x) - g(x)). \tag{5.2}$$

Theorem 5.1. *The set $\mathcal{S}(Q_{12})$ consists of integers M of the following forms:*

$$2^a 3^b m_6 \ : \ a = 0, 4, a \geq 6, \quad b = 0, b \geq 3, \tag{5.3}$$

$$2^5 3^b m_6 \ : \ b = 4, b \geq 6, \tag{5.4}$$

$$2^5 3^b m_6 k \ : \ b = 0, 3, 5, \tag{5.5}$$

where, in (5.5), k can be a prime $p \equiv 5 \bmod 12$ and also the square of a prime $p \equiv 5 \bmod 6$.

For $G = \mathbb{Z}_6 \times \mathbb{Z}_2$ and $\mathbb{Z}_{12}$ we need to partition the primes $p \equiv 1 \bmod 12$ into two sets

$$\mathcal{P}_1 := \{p \equiv 1 \bmod 12 \ : \ p = (6k+2)^2 + (6t+3)^2 \text{ for some } k, t \in \mathbb{Z}\},$$

$$\mathcal{P}_2 := \{p \equiv 1 \bmod 12 \ : \ p = (6k)^2 + (6t+1)^2 \text{ for some } k, t \in \mathbb{Z}\}. \tag{5.6}$$

These sets are disjoint by the uniqueness of representation of primes $\equiv 1 \bmod 4$ as a sum of two squares. They are probably not describable by a simple congruence; see Cox [6] for a class field theory approach to distinguishing which primes are of the form $x^2 + 36y^2$.

Theorem 5.2. *The set $\mathcal{S}(\mathbb{Z}_6 \times \mathbb{Z}_2)$ consists of integers M of the following forms:*

(a) The integers M with $3^3 \mid M$ that take the form

$$3^3(4m-1), \quad 2^4 \cdot 3^3(2m-1), \quad 2^6 \cdot 3^3 m.$$

(b) The integers M with $3^2 \parallel M$ that take the form

$$3^2(4m-1)p, \quad 2^4 \cdot 3^2(2m-1)p, \quad 2^6 \cdot 3^2 mp,$$

for some prime $p \equiv 7 \bmod 12$, or

$$2^8 \cdot 3^2(4m-1) \quad \text{or} \quad 2^{10} \cdot 3^2(4m-1) \quad \text{or} \quad 2^{12} \cdot 3^2(2m-1) \quad \text{or} \quad 2^{14} \cdot 3^2 m.$$

(c) The integers M coprime to 3 of the form

$$12m+1, \quad 2^4(6m+1), \quad 2^6(3m+1),$$

or

$$(12m+5)k, \quad -2^4(6m+1)k, \quad -2^6(3m+1)k, \tag{5.7}$$

where $k = p$ for some prime $p \equiv 1 \bmod 12$ in $\mathcal{P}_1$, or $k = p^2$ for some $p \equiv 5 \bmod 12$, or $k = p_1 p_2$ for some primes $p_1, p_2 \equiv 7 \bmod 12$, or

$$2^8(12m+5), \quad 2^8(12m+5)p, \quad 2^{10}(12m+5), \quad 2^{10}(12m+5)p,$$

for some $p \equiv 7 \bmod 12$, or

$$-2^{12}(6m+1), \quad -2^{14}(3m+1).$$

In each case m runs through all the integers.

Note that in $\mathcal{S}(\mathbb{Z}_6 \times \mathbb{Z}_2)$ there are no integers M with $3 \parallel M$.

For the group $G = \mathbb{Z}_{12}$, we work with measures on polynomials $F(x) = \sum_{j=0}^{11} a_j x^j$.

Theorem 5.3. *Let $G = \mathbb{Z}_{12}$. We separate $\mathcal{S}(\mathbb{Z}_{12})$ into its odd and even integer values:*

(a) The odd integers coprime to 3 take any value m_6.
The odd multiples of 3 take the form $9m_6p$ for primes $p \equiv 5$ and $7 \bmod 12$, and p in $\mathcal{P}_1$, and $27m_2$.

(b) The even integers divisible by 3 take the form $2^4 \cdot 3^2 m$ for all integers m.
The even integers coprime to 3 take the forms $2^4 m_6$, and $2^5 m_6 p$ for some prime $p \equiv 5$ and 7 mod 12, and p in $\mathcal{P}_1$, and $2^6 m_3$.

Again, in this theorem there are no values M with $3 \parallel M$.

The Lind-Lehmer constant (the minimal non-trivial measure) is readily determined for the groups of order 12:

Corollary 5.4. *We have*

$$\lambda(D_{12}) = \lambda(Q_{12}) = \lambda(\mathbb{Z}_{12}) = \lambda(A_4) = 5, \quad \lambda(\mathbb{Z}_6 \times \mathbb{Z}_2) = 11.$$

6. The remaining group $\mathbb{Z}_3 \times \mathbb{Z}_3$

Theorem 6.1. *We have $\mathcal{S}(\mathbb{Z}_3 \times \mathbb{Z}_3) = \{9m \pm 1 : m \in \mathbb{Z}\} \cup \{3^6 m : m \in \mathbb{Z}\}$.*

7. Proofs for Section 3

Proof of Theorem 3.1. We first prove the result for $G = Q_8$ and $\mathbb{Z}_4 \times \mathbb{Z}_2$. Since it requires no extra work we also include D_8, although it is already covered in [3]. We assume that $F(x, y)$ is of the form (3.1). We begin by comparing the form of the Lind measure for these three groups. In all three cases we have the same four linear factors in $\mathbb{Z}[a_0, a_1, a_2, a_3, b_0, b_1, b_2, b_3]$, namely

$$\begin{aligned}
\ell_1 &:= F(1,1) = (a_0 + a_2) + (a_1 + a_3) + (b_0 + b_2) + (b_1 + b_3),\\
\ell_2 &:= F(1,-1) = (a_0 + a_2) + (a_1 + a_3) - (b_0 + b_2) - (b_1 + b_3),\\
\ell_3 &:= F(-1,1) = (a_0 + a_2) - (a_1 + a_3) + (b_0 + b_2) - (b_1 + b_3),\\
\ell_4 &:= F(-1,-1) = (a_0 + a_2) - (a_1 + a_3) - (b_0 - b_2) + (b_1 + b_3).
\end{aligned}$$

The remaining factors are quadratics in $\mathbb{Z}[a_0, a_1, a_2, a_3, b_0, b_1, b_2, b_3]$:

$$\begin{aligned}
\mathscr{D}_{Q_8}(a_0, a_1, a_2, a_3, b_0, b_1, b_2, b_3) &= \ell_1\ell_2\ell_3\ell_4 q_1^2,\\
\mathscr{D}_{D_8}(a_0, a_1, a_2, a_3, b_0, b_1, b_2, b_3) &= \ell_1\ell_2\ell_3\ell_4 q_2^2,\\
\mathscr{D}_{\mathbb{Z}_4\times\mathbb{Z}_2}(a_0, a_1, a_2, a_3, b_0, b_1, b_2, b_3) &= \ell_1\ell_2\ell_3\ell_4 q_3 q_4,
\end{aligned}$$

where

$$\begin{aligned}
q_1 &:= |f(i)|^2 + |g(i)|^2 = (a_0 - a_2)^2 + (a_1 - a_3)^2 + (b_0 - b_2)^2 + (b_1 - b_3)^2,\\
q_2 &:= |f(i)|^2 - |g(i)|^2 = (a_0 - a_2)^2 + (a_1 - a_3)^2 - (b_0 - b_2)^2 - (b_1 - b_3)^2,\\
q_3 &:= |f(i) + g(i)|^2 = ((a_0 - a_2) + (b_0 - b_2))^2 + ((a_1 - a_3) + (b_1 - b_3))^2,\\
q_4 &:= |f(i) - g(i)|^2 = ((a_0 - a_2) - (b_0 - b_2))^2 + ((a_1 - a_3) - (b_1 - b_3))^2.
\end{aligned}$$

Thus for $G = Q_8$, D_8 or $\mathbb{Z}_4 \times \mathbb{Z}_2$ we have

$$\mathscr{D}_G(m+1, m, m, m, m, m, m, m) = 8m+1,$$
$$\mathscr{D}_G(k+2, k, k, k, k, k, k, k) = 2^8(4k+1),$$
$$\mathscr{D}_G(k-1, k+1, k-1, k+1, k+1, k+1, k, k) = -2^8(4k+1),$$
$$\mathscr{D}_G(k+1, k, k+1, k, k-1, k-1, k, k) = 2^8(2k).$$

Equivalently, writing these as polynomial measures we have

$$M_G\left(1 + m\frac{x^4-1}{x-1} + ym\frac{x^4-1}{x-1}\right) = 8m+1,$$
$$M_G\left(2 + k\frac{x^4-1}{x-1} + yk\frac{x^4-1}{x-1}\right) = 2^8(4k+1),$$
$$M_G\left((x^2+1)(x-1) + k\frac{x^4-1}{x-1} + y\left((x+1) + k\frac{x^4-1}{x-1}\right)\right) = -2^8(4k+1),$$
$$M_G\left((x^2+1) + k\frac{x^4-1}{x-1} + y\left(-(x+1) + k\frac{x^4-1}{x-1}\right)\right) = 2^8(2k).$$

Writing $p \equiv 3 \bmod 4$ as $p = a^2+b^2+c^2+d^2$ with a even, b, c, d odd, then

$$(a_0, a_1, a_2, a_3) = \left(m + \frac{a}{2}, m + \frac{(b-1)}{2}, m - \frac{a}{2}, m - \frac{(b+1)}{2}\right),$$
$$(b_0, b_1, b_2, b_3) = \left(m + \frac{(c-1)}{2}, m + \frac{(d-1)}{2}, m - \frac{(c+1)}{2}, m - \frac{(d+1)}{2}\right),$$

has $\mathscr{D}_{Q_8}(a_0, a_1, a_2, a_3, b_0, b_1, b_2, b_3) = (8m-3)p^2$, while

$$\mathscr{D}_{D_8}(m, m, m, m-1, m, m, m-1, m-1) = 8m-3.$$

It remains to show that a determinant $\mathscr{D}_G$ takes one of the stated forms. Suppose first that $\mathscr{D}_G$ is even. Since the $\ell_j \equiv \ell_1 \bmod 2$ and the $q_i \equiv \ell_1^2 \bmod 2$ we know that the ℓ_j and q_j are all even. If $(a_0 - a_2)$, $(a_1 - a_3)$, $(b_0 - b_2)$, $(b_1 - b_3)$ are all even or all odd then in all cases $4 \mid q_j$ and $2 \mid \ell_j$ and $2^8 \mid \mathscr{D}_G$. So suppose two of them are even and two odd. Hence two of $(a_0 + a_2)$, $(a_1 + a_3)$, $(b_0 + b_2)$, $(b_1 + b_3)$ are even and two odd. Call these A, B, C, D, in any order, then

$$\ell_1\ell_2\ell_3\ell_4 = ((A+B)^2 - (C+D)^2)((A-B)^2 - (C-D)^2).$$

Hence if A, C are odd and B, D even then $(A \pm B)^2 - (C \pm D)^2 \equiv 1 - 1 = 0 \bmod 8$, so $2^6 \mid \ell_1\ell_2\ell_3\ell_4$ and $2 \mid q_j$, and $2^8 \mid \mathscr{D}_G$.

Suppose that $\mathscr{D}_G$ is odd. So either one or three of the $(a_0 - a_2)$, $(a_1 - a_3)$, $(b_0 - b_2)$, $(b_1 - b_3)$, will be odd (and hence one or three of the corresponding A, B, C, D, will odd). Suppose that A is odd and B is even and C, D have the same parity. Plainly $q_1^2, q_2^2 \equiv 1 \bmod 8$ and

$$q_4 = q_3 - 4(a_0 - a_2)(b_0 - b_2) - 4(a_1 - a_3)(b_1 - b_3).$$

So if three of A, B, C, D are even then $q_4 \equiv q_3 \bmod 8$ and $q_3q_4 \equiv q_3^2 \equiv 1 \bmod 8$, while if three are odd we have $q_4 \equiv q_3 + 4 \bmod 8$ and $q_3q_4 \equiv q_3^2 - 4 \equiv -3 \bmod 8$. Similarly

$$\begin{aligned}(A-B)^2 - (C-D)^2 &= (A+B)^2 - (C+D)^2 - 4AB + 4CD \\ &\equiv (A+B)^2 - (C+D)^2 + 4CD \bmod 8.\end{aligned}$$

Hence if C, D are even we have $\ell_1\ell_2\ell_3\ell_4 \equiv ((A+B)^2-(C+D)^2)^2 \equiv 1 \bmod 8$ and $\mathscr{D}_G \equiv 1 \bmod 8$. If C, D are odd then $\ell_1\ell_2\ell_3\ell_4 \equiv ((A+B)^2-(C+D)^2)^2 - 4 \equiv -3 \bmod 8$, and $\mathscr{D}_G \equiv 1 \bmod 8$ for $G = \mathbb{Z}_4 \times \mathbb{Z}_2$, and $\mathscr{D}_G \equiv -3 \bmod 8$ for $G = Q_8$ or D_8, with $q_1 \equiv 3 \bmod 4$ for $G = Q_8$ (and so divisible by at least one $p \equiv 3 \bmod 4$). This completes the proof for $G = Q_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ and D_8.

Next, for $G = \mathbb{Z}_2^3$ we have $M_G(F) = \prod_{x,y,z=\pm 1} F(x,y,z)$.

We can achieve anything of the form $8m+1$, $2^8(4m+1)$ or $2^{12}m$ using

$$M_G\left(1 + m(1+x)(1+y)(1+z)\right) = 8m+1,$$
$$M_G\left(2 + m(1+x)(1+y)(1+z)\right) = 2^8(4m+1),$$
$$M_G\left(3 + z + k(1+x)(1+y)(1+z)\right) = 2^{12}(2k+1),$$
$$M_G\left(x+y+z-3 + (1-x)(1-y)(1-z) + k(1+x)(1+y)(1+z)\right) = 2^{12}(2k),$$

so it just remains to check that any $M_G(F)$ is of one of these forms.

We write $F(x,y) = f(x,y) + zg(x,y)$, with $f(x,y)$ and $g(x,y)$ in $\mathbb{Z}[x,y]$ of the form

$$f(x.y) = b(0,0) + b(1,0)x + b(0,1)y + b(1,1)xy,$$
$$g(x.y) = a(0,0) + a(1,0)x + a(0,1)y + a(1,1)xy,$$

so that

$$M_G(F) = \prod_{x,y=\pm 1} f(x,y)^2 - g(x,y)^2.$$

Notice that the $f(\pm 1, \pm 1) \equiv f(1,1) \bmod 2$, and $g(\pm 1, \pm 1) \equiv g(1,1) \bmod 2$, and $M_G(F) \equiv (f(1,1) - g(1,1))^4 \bmod 2$ is even if $f(1,1)$ and $g(1,1)$ have the same parity and odd otherwise.

Suppose first that $M_G(F)$ is odd. Reversing the roles of $f(x,y)$ and $g(x,y)$ as necessary we suppose that the $f(\pm 1, \pm 1)$ are all odd and the $g(\pm 1, \pm 1)$ all even. Then mod 8 we have

$$M_G(F) \equiv \prod_{x,y=\pm 1} (1 - g(x,y)^2) \equiv 1 - \sum_{x,y=\pm 1} g(x,y)^2 \equiv 1 - \left(\sum_{x,y=\pm 1} g(x,y)\right)^2.$$

But

$$\sum_{x,y=\pm 1} g(x,y) = 4a(0,0),$$

and so $M_G(F) \equiv 1 \bmod 8$.

Suppose that $M_G(F)$ is even. If the $f(\pm 1, \pm 1)$ and $g(\pm 1, \pm 1)$ are all odd then the $f(x,y)^2 - g(x,y)^2 \equiv 1 - 1 = 0 \bmod 8$ for each of the four factors and $2^{12} \mid M_G(F)$. So suppose that they are all even and

$$M_G(F) = 2^8 \prod_{x,y=\pm 1} (f(x,y)/2)^2 - (g(x,y)/2)^2.$$

If any of the $f(x,y)/2$ and $g(x,y)/2$ have the same parity then 4 divides that factor. Moreover, since $\sum_{x,y=\pm 1} (f(x,y)/2 - g(x,y)/2) = 2b(0,0) - 2a(0,0)$ is even, we must have an even number of such factors, and $2^{12} \mid M_G(F)$. So assume that they have opposite parity for all $x, y = \pm 1$, with $(f(x,y)/2)^2 - (g(x,y)/2)^2$ equalling 1 mod 4 if $g(x,y)/2$ is even and -1 mod 4 if $g(x,y)/2$ is odd. But the

$\sum_{x,y=\pm 1} g(x,y)/2 = 2a(0,0)$ is even, so we must have an even number of -1's and $\prod_{x,y=\pm 1}(f(x,y)/2)^2 - (g(x,y)/2)^2 \equiv 1 \bmod 4$. □

8. Proof of Theorem 4.1

Suppose that 3 divides

$$\mathscr{D}_G(a_1,\dots,a_{12}) = l_0 l_1 l_2 D^3$$

with l_0, l_1, l_2 and D as in (4.1) and (4.2). If $3 \mid l_0 l_1 l_2$ then 3 divides l_0 or $l_1 l_2$ and, from the congruence

$$l_1 l_2 \equiv l_0^2 \bmod 3,$$

must divide both, and $3^2 \mid \mathscr{D}_G(a_1,\dots,a_{12})$. If $3 \mid D$ then plainly $3^3 \mid \mathscr{D}_G(a_1,\dots,a_{12})$. Hence $3 \mid \mathscr{D}_G(a_1,\dots,a_{12})$ implies that $3^2 \mid \mathscr{D}_G(a_1,\dots,a_{12})$.

It is easy to see that $D \equiv \det \begin{pmatrix} a & c & b \\ b & a & c \\ c & b & a \end{pmatrix} \bmod 2$, the circulant determinant equalling $l_0 l_1 l_2$, the $\mathbb{Z}_3$ measure of $a + bx + cx^2$, but in fact expanding we have the stronger congruence

$$D \equiv l_0 l_1 l_2 \bmod 4.$$

From this we see that any odd determinant must have $l_0 l_1 l_2$ odd and

$$\mathscr{D}_G(a_1,\dots,a_{12}) \equiv (l_0 l_1 l_2)^4 \equiv 1 \bmod 4.$$

If the determinant is even then 2 divides $l_0 l_1 l_2$ or D and from the congruence must divide both. Moreover if $2 \parallel l_0 l_1 l_2$ then $2 \parallel D$ and $2^4 \parallel \mathscr{D}_G(a_1,\dots,a_{12})$, while if $2^2 \mid l_0 l_1 l_2$ then $2^2 \mid D$ and $2^8 \mid \mathscr{D}_G(a_1,\dots,a_{12})$.

Hence the determinants must be of the stated form. It remains to show that we can achieve all these. From

$$\mathscr{D}_G(1,1,0,0,0,0,0,0,1,0,0,0) = 9,$$
$$\mathscr{D}_G(1,1,-1,0,0,0,0,0,0,0,0,0) = -27,$$

and multiplication we can obtain any $\pm 3^b$ with $b \geq 2$ which is 1 mod 4.

For the powers of 2 we have

$$\mathscr{D}_G(0,0,0,0,1,0,0,0,1,0,0,0) = 2^4,$$
$$\mathscr{D}_G(1,-1,0,0,1,0,0,0,1,0,0,0) = -2^4,$$

and

$$\mathscr{D}_G(k+2,k,k,k,k+1,k,k,k,k+1,k,k,k) = 2^8(1+3k),$$
$$\mathscr{D}_G(k+2,k+1,k-1,k,k+1,k,k,k,k+1,k,k,k) = -2^8(1+3k),$$

with $k = 0, -1, 1, -3$ giving $\pm 2^8, \pm 2^9, \pm 2^{10}, \pm 2^{11}$. Multiplication of these gives all $\pm 2^a$ with $a = 4$ or $a \geq 8$.

The $m \equiv 1 \bmod 4$ with $(m,6) = 1$ can be obtained with

$$\mathscr{D}_G(k+1,k,k,k,k,k,k,k,k,k,k,k) = 1 + 12k,$$
$$\mathscr{D}_G(k+1,k,k,k,k+1,k+1,k,k,k+1,k+1,k,k) = 5 + 12k.$$

Multiplication of these produces all the forms in Theorem 4.1. □

9. Proofs for Section 5

We write ω for the primitive cube root of unity $\omega_3 = e^{2\pi i/3}$, and observe that ωi is a primitive 12th root of unity.

We shall need some results on factoring in $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ and $\mathbb{Z}[\omega_{12}] = \mathbb{Z}[\omega i] = \mathbb{Z}[\omega, i]$. Note that (see for example [27, Chapter 11]) all these rings are UFDs, with the primes splitting in $\mathbb{Z}[i]$ being 2 and those $p \equiv 1 \bmod 4$ and in $\mathbb{Z}[\omega]$ being 3 and those primes p with $\left(\frac{-3}{p}\right) = 1$, namely $p \equiv 1$ or $7 \bmod 12$. The primes $p \equiv 1 \bmod 12$ split in both $\mathbb{Z}[\omega]$ and $\mathbb{Z}[i]$, being a product of 4 primes in $\mathbb{Z}[\omega, i]$. We write N_1 and N_2 for the norms for $\mathbb{Z}[\omega]$ and $\mathbb{Z}[\omega, i]$, so that

$$N_1(H(\omega)) = H(\omega)H(\omega^2) = |H(\omega)|^2,$$
$$N_2(H(\omega, i)) = H(\omega, i)H(\omega^2, i)H(\omega, -i)H(\omega^2, -i).$$

Lemma 9.1. *If α in $\mathbb{Z}[\omega]$ has $3 \nmid N_1(\alpha)$ then one of $\pm\alpha$ takes the form*

$$-1 + (A + B\omega)(1 - \omega), \quad A, B \in \mathbb{Z},$$

while if $\gcd(N_1(\alpha), 6) = 1$ then exactly one of $\pm\alpha, \pm\alpha\omega, \pm\alpha\omega^2$ takes the form

$$-1 + 2(A + B\omega)(1 - \omega), \quad A, B \in \mathbb{Z}.$$

Proof. Suppose that $3 \nmid N_1(\alpha)$. Writing $\alpha = a + b(1 - \omega)$ we have $3 \nmid a$, else $3 \mid N_1(\alpha) = a^2 + 3ab + 3b^2$. Replacing α by $-\alpha$ as necessary we can assume that $a \equiv -1 \bmod 3$ and, writing $a = -1 + 3k$, $3 = (1 - \omega)(2 + \omega)$ we get

$$\alpha = -1 + (A + B\omega)(1 - \omega).$$

Suppose also that $2 \nmid N_1(\alpha)$. We can't have A even and B odd, else

$$\alpha = 2w + (A + (B - 1)\omega)(1 - \omega) \;\Rightarrow\; 2 \mid N_1(\alpha).$$

If A, B are both odd we take

$$\alpha\omega = -1 + ((1 - B) + (A - B)\omega)(1 - \omega),$$

and if A is odd and B even we can take

$$\alpha\omega^2 = -1 + ((B - A + 1) + (1 - A)\omega)(1 - \omega).$$

With A, B even the $\alpha\omega^j$ cycle through the three possible parity combinations. □

In (5.6) we partitioned the primes $p \equiv 1 \bmod 12$ into two sets $\mathcal{P}_1$ and $\mathcal{P}_2$.

Lemma 9.2. *If $p \equiv 7 \bmod 12$ then $p = N_1(\alpha)$ for an*

$$\alpha = -1 + 2(1 - \omega)(2A + 1 + B\omega), \quad A, B \in \mathbb{Z},$$

with B even (also one with B odd).

If $p \equiv 1 \bmod 12$ then $p = N_1(\alpha)$ for an

$$\alpha = -1 + 2(1 - \omega)(2A + B\omega), \quad A, B \in \mathbb{Z}, \tag{9.1}$$

with B even when $p \in \mathcal{P}_2$ and B odd when $p \in \mathcal{P}_1$.

If $p \equiv 1 \bmod 12$ then $p = N_2(\alpha_1)$ for some

$$\alpha_1 = -1 + (2A + 2B\omega)(1 - \omega) + i\left(2 + (C + 2D\omega)(1 - \omega)\right), \quad A, B, C, D \in \mathbb{Z}, \tag{9.2}$$

with C even when $p \in \mathcal{P}_1$ and C odd when p is in $\mathcal{P}_2$. Also $p = N_2(\alpha_2)$ for some

$$\alpha_2 = (A + 1 + 2B\omega)(1 - \omega) + i\left(1 + (C + D\omega)(1 - \omega)\right), \quad A, B, C, D \in \mathbb{Z}, \tag{9.3}$$

with A, C and D all even when $p \in \mathcal{P}_1$ and all odd when $p \in \mathcal{P}_2$.

Proof. As above for $p \equiv 7 \bmod 12$ we can take $\alpha = -1 + 2(a+b\omega)(1-\omega)$. Note that a must be odd, since otherwise $\alpha \equiv -1 + 2b\omega(1-\omega) \equiv -1 + 2b \bmod 4$ and $N(\alpha) \equiv 1 \bmod 4$. If b is also odd then we can replace α by its conjugate $-1 + 2(a+b\omega^2)(1-\omega^2) = -1 + 2(1-\omega)(a + (a-b)\omega)$ with $(a-b)$ even.

Supposing $p \equiv 1 \bmod 12$, then $p = N_2(\alpha)$ for some $\alpha = (a + b(1-\omega)) + i(c + d(1-\omega))$. We can't have $3 \mid a$ and $3 \mid c$, else $3 \mid N(\alpha)$ and we can assume that $3 \nmid ac$ else we replace α by

$$(1+i\omega)\alpha = (a - c - 3d) + (1-\omega)(b + c + 2d) + i(a + c + 3b + (1-\omega)(d - a - 2b)).$$

Replacing α by $-\alpha$ or $\pm i\alpha$ we can assume that $a, c \equiv 2 \bmod 3$ and writing $3 = (1-\omega)(2+\omega)$ we can write

$$\alpha = -1 + (1-\omega)(A + B\omega) + i\left(2 + (1-\omega)(C + D\omega)\right).$$

It remains to show that we can take A, B, D all even. We work first with A, B. We have

$$\omega(-1 + (A+B\omega)(1-\omega)) = -1 + (1 - B + (A-B)\omega)(1-\omega),$$
$$\omega^2(-1 + (A+B\omega)(1-\omega)) = -1 + (B - A + 1 + (1-A)\omega)(1-\omega),$$

so if A, B are both odd we can replace α by $\omega\alpha$ and if A is odd and B even by $\omega^2\alpha$. If A is even and B odd we write

$$-1 + (A+B\omega)(1-\omega) = 2 + (1-\omega)(A - 2 + (B-1)\omega).$$

Notice this does not occur if C, D are both even else $2 \mid \alpha$, so replacing α by a conjugate of $-i\alpha$ we reverse the roles of the A, B and C, D and then work to make the new A, B both even noting that the process keeps C, D even:

$$\omega(2 + (C+D\omega)(1-\omega)) = 2 + (-D - 2 + (C-D)\omega)(1-\omega),$$
$$\omega^2(2 + (C+D\omega)(1-\omega)) = 2 + (D - C - 2 + (-C-2)\omega)(1-\omega).$$

So suppose that A and B are even (replacing them by $2A$ and $2B$). We can't have C even, D odd else $\alpha \equiv -1 + i \bmod 2$ and $2 \mid N(\alpha)$. If C and D are both odd then we can replace α by its conjugate

$$\begin{aligned} &-1 + 2(A + B\omega^2)(1-\omega^2) + i\left(2 + (C + D\omega^2)(1-\omega^2)\right) \\ &\quad = -1 + 2(A + (A-B)\omega)(1-\omega) + i\left(2 + (C + (C-D)\omega)(1-\omega)\right), \end{aligned}$$

so we can assume that D is also even. Replacing D by $2D$ and observing that

$$\alpha = -1 + 2(A + B\omega)(1-\omega) + i(2 + (C + 2D\omega)(1-\omega)),$$
$$\alpha' = -1 + 2(A + B\omega^2)(1-\omega^2) + i(2 + (C + 2D\omega^2)(1-\omega^2),$$

have $\alpha\alpha' = -3\delta + i\rho$, with

$$\delta = 1 + C^2 + 2A + 2C - 2CD + 4D^2 - 4(A^2 - AB + B^2),$$
$$\rho = -4 - 3C + 6(2A + 2AC + 4BD - BC - 2AD),$$

plainly C even leads to $2 \mid \rho$ and a $\mathcal{P}_1$ representation of p and if C is odd $2 \mid \delta$ and p must be in $\mathcal{P}_2$. With

$$\alpha_1 = -1 + (2A + 2B\omega)(1-\omega) + i\left(2 + (C + 2D\omega)(1-\omega)\right)$$

we take $\alpha_2 = (\omega^2 + i)\alpha_1 = \delta_2 + i\rho_2$ where

$$\delta_2 = ((2B - 2A - C - 1) - (2A + 2D)\omega)\,(1 - \omega),$$
$$\rho_2 = 1 + ((2A + 2D - C - 2) + (2B - C - 2)\omega)\,(1 - \omega),$$

and the second form (9.3) is plain. Observe that

$$\alpha = -1 + 2(A + B\omega)(1 - \omega) + i(2 + (C + 2D\omega)(1 - \omega)),$$
$$\alpha'' = -1 + 2(A + B\omega)(1 - \omega) - i(2 + (C + 2D\omega)(1 - \omega)),$$

has

$$\alpha\alpha'' = 5 + C^2(1 - \omega)^2 + 4(1 - \omega)v(\omega),$$

where $v(\omega)$ is an integer polynomial in ω. When p is in $\mathcal{P}_1$ and C is even

$$\alpha\alpha'' = -1 + 2(1 - \omega)\Big(2 + \omega + 2(C/2)^2(1 - \omega) + 2v(\omega)\Big),$$

giving (9.1) with B odd, while when p is in $\mathcal{P}_2$ and C is odd

$$\omega\alpha\alpha'' = -1 + 4(1 - \omega)\left(\frac{1}{4}(C^2 - 1) + \frac{1}{2}(C^2 + 1)\omega + \omega v(\omega)\right),$$

giving (9.1) with B even. □

We write

$$h(x) := \frac{x^6 - 1}{x - 1} = \sum_{j=0}^{5} x^j, \quad h(1) = 6,\ h(-1) = h(\pm\omega) = h(\pm w^2) = 0.$$

Proof of Theorem 5.1. As before, we let m_t (e.g., m_2, m_6) denote an arbitrary integer coprime to t. From the formula (2.3) we know that $\mathcal{S}(Q_{12})$ consists of measures $M := M(F) := M_{Q_{12}}(F)$ of the form

$$M = ab(cd)^2, \tag{9.4}$$

where, if $F(x, y) = f(x) + yg(x)$,

$$a := f(1)^2 - g(1)^2,\ b := f(-1)^2 + g(-1)^2,$$
$$c := |f(\omega)|^2 - |g(\omega)|^2,\ d := |f(-\omega)|^2 + |g(-\omega)|^2.$$

The proof proceeds by a series of steps, followed by their proofs:

Step 1. We have $c \equiv a \bmod 3$, $d \equiv b \bmod 3$ and

$$3 \nmid M \quad \text{or} \quad 3^3 \mid M. \tag{9.5}$$

Since $\omega \equiv 1 \bmod (1 - \omega)$ in $\mathbb{Z}[\omega]$ and a and c are integers we have $c \equiv a \bmod 3$. Likewise $d \equiv b \bmod 3$. So $cd \equiv ab \bmod 3$ and $M \equiv (ab)^3 \bmod 3$. Hence $3 \mid M$ iff $3 \mid ab$ and $3 \mid cd$, proving Step 1.

Step 2. All odd integers of the forms $M = m_6$ and $M = 3^3 m_2$ belong to $\mathcal{S}(Q_{12})$.

From Step 1 we know that all odd M are of one of these two forms. Conversely, we obtain all odd integers that are 1 mod 4 satisfying (9.5) as follows:

$$M\,(1 + t\,h(x) + yt\,h(x)) = 1 + 12t, \tag{9.6}$$

$$M\left(1 + x(x^3 + 1) + t\,h(x) + y\left((1 + x^3) + t\,h(x)\right)\right) = 5 + 12t, \tag{9.7}$$

$$M\left(1 + t\,h(x) + y\left((1 + x^3) + t\,h(x)\right)\right) = -3^3(1 + 4t). \tag{9.8}$$

Swapping f and g in (2.3) changes the sign, by (2.4), so that these identities give us all odd integers satisfying (9.5).

This deals with the odd measures, so we can assume that M is even from now on. In particular, at least one of ab and cd is even.

Step 3. We have $c \equiv d \bmod 2$, $f(1) \equiv f(-1) \bmod 2$, $g(1) \equiv g(-1) \bmod 2$, and ab even iff $f(1) \equiv g(1) \bmod 2$.

Step 4. We have $2^4 \mid M$, and $2^5 \parallel M$ possible only when c and d are both odd, and $f(-1), g(-1)$ are both odd, or both even with $f(-1)/2$, $g(-1)/2$ both odd.

If cd is even, then from $d \equiv c \bmod 2$ we have that $2^4 \parallel (cd)^2$ or $2^6 \mid (cd)^2$. If $f(1)$ and $g(1)$ are both odd then $2^3 \mid a$ and $2 \parallel b$. If both are even then, writing

$$f(1) = 2\alpha_1, \quad f(-1) = 2\alpha_2, \quad g(1) = 2\beta_1, \quad g(-1) = 2\beta_2,$$

we get $a = 4(\alpha_1^2 - \beta_1^2)$ and $b = 4(\alpha_2^2 + \beta_2^2)$. Hence $2^4 \mid ab$, and we get $2^4 \mid M$, with $2^5 \parallel M$ only as specified.

Step 5. All M with $2^4 \parallel M$ with property (9.5) are possible.

This is seen using

$$M\left(1 + x^2 + t\,h(x) + yt\,h(x)\right) = 2^4(1+6t),$$
$$M\left((1+x^2) + t\,h(x) + y\left((1+x^2)(1+x^3) + t\,h(x)\right)\right) = -3^3 2^4(1+2t),$$

recalling that we can use (2.4) to change the sign on the first of these.

Step 6. All M with $2^6 \mid M$ with property (9.5) are possible.

This is seen using (2.4) and

$$M\left((1 + x + x^2 + x^4) + t\,h(x) + yt\,h(x)\right) = 2^6(1+3t),$$
$$M\left((1+x^2) + t\,h(x) + y\left(-(1+x^3) + t\,h(x)\right)\right) = 2^6 3^3 t.$$

So the even measures with $2^4 \parallel M$ or $2^6 \mid M$ are as claimed.

For the rest of the proof we can assume that $2^5 \parallel M$ and that $3^\beta \parallel M$. We know that $\beta = 0$ or $\beta \geq 3$.

Step 7. If $\beta = 4$ or $\beta \geq 6$ then $M = 2^5 3^\beta m_6$.

We get $2^5 3^4$ and $2^5 3^6$ from

$$M\left((1 - x - x^5) + h(x) + y\left((x^4 + x^2 + 1) + (x^2 - 1)(x+1)^\delta\right)\right) = 2^5 3^{4+2\delta}.$$

Hence, multiplying by an odd measure, we can obtain any $2^5 3^\beta m_6$ with $\beta = 4$ or $\beta \geq 6$.

This just leaves $\beta = 0, 3$ or 5, which we can now assume holds.

Step 8. We have $3 \nmid b$.

For if $3 \mid b = f(-1)^2 + g(-1)^2$ then $3 \mid f(-1), g(-1)$ with $(f(-1)/3)^2 + (g(-1)/3)^2$ coprime to 3 or a multiple of 3^2, giving $3^2 \parallel b$ or $3^4 \mid b$. Then also, from Step 1, $d \equiv b \equiv 0 \bmod 3$, with d contributing an even power of 3 to bd^2, so that $3^4 \parallel bd^2$ or $3^6 \mid bd^2$. Also, from $a \equiv c \bmod 3$ we have either $3 \nmid a$ or $3^3 \mid ac^2$. Hence $3^4 \parallel M$ or $3^6 \mid M$, contrary to assumption.

Step 9. If $3 \mid f(-1)g(-1)$ then $p \mid M$ for some prime $p \equiv 5 \bmod 12$.

Supposing first that $3 \mid f(-1)g(-1)$, then from Step 4 we have a factor of M of the form

$$f(-1)^2 + g(-1)^2 \text{ or } (f(-1)/2)^2 + (g(-1)/2)^2 = A^2 + (3B)^2 = 2k$$

with k odd and $2k \equiv 1 \bmod 3$. Thus $k \equiv 2 \bmod 3$ is an odd sum of two squares, so must contain an odd power of a prime $p \equiv 2 \bmod 3$ which must be a sum of two squares, and hence $p \equiv 5 \bmod 12$. Conversely suppose that we have a prime $p \equiv 5 \bmod 12$ then $2p$ is a sum of two squares $2p = a^2 + b^2$ where a and b must be odd and one of them a multiple of 3, $2p = (1+6A)^2 + (3+6B)^2$.

Step 10. Conversely every $2^5 p$ with $p \equiv 5 \bmod 12$ is an M.

This is because if $2p = (1+6A)^2 + (3+6B)^2$ then

$$M\left(-1 - Ah(-x) + h(x) + y\left(x^4 + x^2 + 1 + Bh(-x)\right)\right) = 2^5 p.$$

Step 11. If $3 \nmid f(-1)g(-1)$ then $p^2 \mid M$ for some prime $p \equiv 5 \bmod 6$.

For if $3 \nmid f(-1)g(-1)$ then

$$d = |f(-\omega)|^2 + |g(-\omega)|^2 \equiv f(-1)^2 + g(-1)^2 \equiv 2 \bmod 3$$

is odd. Hence this term must be divisible by a prime $p \equiv 5 \bmod 6$ and M by p^2.

Step 12. Conversely every such $2^5 p^2$ with $p \equiv 5 \bmod 6$ is an M.

We can write a $p \equiv 5 \bmod 6$ as a sum of two norms of elements in $\mathbb{Z}[w]$, $p = N_1(\alpha) + N_1(\gamma)$; we can do this since any integer not of the form $9^k(9n+6)$ can be represented by $x^2+xy+y^2+z^2$ – see Dickson [8] (in fact $x^2+xy+y^2+z^2+zw+w^2$ should represents all integers [2]). Moreover since p is odd one of the norms must be even and hence an element in $2\mathbb{Z}[w]$ and we can write $p = N_1(\alpha) + 4N_1(\beta)$ with $N_1(\alpha), N_1(\beta) \equiv 1 \bmod 3$. By Lemma 9.1 we can assume that $\alpha = -1 + 2(1-\omega)(A + B\omega)$ and $\beta = -1 + (C + D\omega)(1-\omega)$. We take

$$f(x) = -1 - (A - Bx)(x^3 - 1)(1 + x) + h(x)$$
$$g(x) = (x^2 + x + 1) - (C - 1 - Dx)(x^3 - 1)(1 + x).$$

Then $f(1)^2 - g(1)^2 = 2^4$, $f(-1)^2 + g(-1)^2 = 2$, $|f(\omega)|^2 - |g(\omega)|^2 = 1$, $|f(-\omega)|^2 + |g(-\omega)|^2 = N_1(\alpha) + N_1(2\beta) = p$ and $M_G(f(x) + yg(x)) = 2^5 p^2$.

Step 13. Any $2^5 3^\beta k m_6$, with $k = p$, $p \equiv 5 \bmod 12$, or $k = p^2$, $p \equiv 5 \bmod 6$ and $\beta = 0$ or $\beta \geq 3$ is an M.

Hence we can get any $2^5 k$, where $k = p$, $p \equiv 5 \bmod 12$, or $k = p^2$, $p \equiv 5 \bmod 6$, and by multiplicativity any $2^5 3^\beta k m_6$, with $\beta = 0$ or $\beta \geq 3$. □

We remark that the evaluation of $\mathcal{S}(D_{12})$, already known from [3], can be modelled on the first six steps of the above proof for Q_{12}. In place of (9.4), for $G = D_{12}$ formula (1.12) gives $M = ab_1(cd_1)^2$, with $b_1 := f(-1)^2 - g(-1)^2$ and $d_1 := |f(-\omega)|^2 - |g(-\omega)|^2$. Step 1 of the proof also holds for $G = D_{12}$, because $d_1 \equiv b_1 \bmod 3$. Step 2 also follows using the identities (9.6), (9.7) and (9.8). For D_{12} swapping f and g is not necessary because odd $M \equiv (acd_1)^2 \equiv 1 \bmod 4$. In Step 3 we still have $c \equiv d_1 \bmod 2$. In Step 4 we also have $2^3 \mid b_1$ when $f(1)$ and $g(1)$ are both odd and $b_1 = 4(\alpha_2^2 - \beta_2^2)$, when both are even, giving $2^4 \parallel ab_1$ or $2^6 \mid ab_1$,

and so $2^4 \parallel M$ or $2^6 \mid M$. For Steps 5 and 6, we use the same four identities, but, without (2.4) to change signs, we need the two extra identities

$$M\left((1+x^2)(1+x(x^3+1)) + t\,h(x) + y\left((1+x^3)(1+x^2) + t\,h(x)\right)\right) = 2^4(5+6t),$$
$$M\left((1-x) + t\,h(x) + y\left((1+x^2)(1+x^3) + t\,h(x)\right)\right) = -2^6(1+3t),$$

to complete the proof.

Proof of Theorem 5.2. Suppose that $G = \mathbb{Z}_6 \times \mathbb{Z}_2$. From (5.2) we have

$$M_G(F) = ab_1e_1e_2e_3e_4,$$

for the integers

$$a := f(1)^2 - g(1)^2, \quad b_1 := f(-1)^2 - g(-1)^2,$$
$$e_1 := |f(\omega) + g(\omega)|^2, \ \ e_2 := |f(\omega) - g(\omega)|^2, \quad e_1e_2 = N_1(f(\omega)^2 - g(\omega)^2),$$
$$e_3 := |f(-\omega) + g(-\omega)|^2, \ \ e_4 := |f(-\omega) - g(-\omega)|^2, \quad e_3e_4 = N_1(f(-\omega)^2 - g(-\omega)^2).$$

Since $f(\omega) \equiv f(\omega^2) \equiv f(1) \bmod (1-\omega)$ etc. in $\mathbb{Z}[\omega]$, we readily see that $e_1e_2 \equiv a^2 \bmod 3$ and $e_3e_4 \equiv b_1^2 \bmod 3$ in $\mathbb{Z}$. Hence we cannot have $3 \parallel ab_1e_1e_2e_3e_4$ and

$$3^\alpha \parallel M_G(F) \Rightarrow \alpha = 0 \text{ or } \alpha \geq 2. \tag{9.9}$$

Moreover $3^2 \parallel M_G(F)$ implies that $3 \parallel ab_1$ and $3 \parallel e_1e_2e_3e_4$.

Since $f(-x) = f(x) + 2u_1(x)$ we readily see that all the $e_i \equiv e_1 \bmod 2$. Moreover considering factorisation in $\mathbb{Z}[\omega]$, or by checking that $2 \mid N_1(A+B\omega) = A^2 - AB + B^2$ only when $2 \mid A, B$, we see that a norm of an element in $\mathbb{Z}[\omega]$ is divisible by an even power of 2. Hence

$$2^\beta \parallel e_1e_2e_3e_4 \Rightarrow \beta = 2t, \ t = 0 \text{ or } t \geq 4.$$

From the proof of Theorem 5.1, and the comments on D_{12} after it, we have that

$$2^\beta \parallel ab_1 \Rightarrow \beta = 0, 4 \text{ or } \beta \geq 6.$$

Hence we certainly have

$$2^\beta \parallel M_G(F) \Rightarrow \beta = 0, 4 \text{ or } \beta \geq 6. \tag{9.10}$$

Similarly, since $f(-x)^2 = f(x)^2 + 4u_2(x)$ we get $b_1 \equiv a \bmod 4$ and $e_3e_4 \equiv e_1e_2 \bmod 4$ and if ab_1 is odd then $ab_1 \equiv a^2 \equiv 1 \bmod 4$ and if $e_1e_2e_3e_4$ is odd then it is $1 \bmod 4$. In particular

$$M_G(F) \text{ odd } \Rightarrow M_G(F) \equiv 1 \bmod 4. \tag{9.11}$$

Case (a) We begin with the multiples of 27. We can achieve all odd multiples satisfying (9.11) using (9.8), and all even multiples satisfying (9.10) with

$$M_G\left((x^2+1)(x^3+1) + kh(x) + y\left((x^2+1) + k\,h(x)\right)\right) = -2^4 3^3(1+2k),$$
$$M_G\left(1 + m\,h(x) + y\left((1-x-x^5) + m\,h(x)\right)\right) = -2^6 3^3 m.$$

Case (b) Suppose next that $3^2 \parallel M_G(F)$. Consider first the case $e := e_1e_2e_3e_4$ odd. From the above discussion we know that $e \equiv 1 \bmod 4$ and $3 \parallel e$. So $e/3 \equiv 3 \bmod 4$, and must be divisible by an odd power of a prime $p \equiv 3 \bmod 4$ with $p \neq 3$. Since e is a norm in $\mathbb{Z}[\omega]$ we must have $p \equiv 7 \bmod 12$. Conversely suppose that $p \equiv 7 \bmod 12$. By Lemma 9.2 we have $p = N_1(\alpha_1)$ with $\alpha_1 = 1 - 2\omega + 4(A + B\omega)(1-\omega)$. Take

$$f(x) = (x+1) - (A - Bx)(x^3-1)(x+1) + m\,h(x),$$
$$g(x) = x - (A - Bx)(x^3-1)(x+1) + m\,h(x).$$

Then $a = 3(1+4m)$, $b_1 = -1$, $e_1e_2 = |f(\omega)^2 - g(\omega)^2|^2 = |\omega - \omega^2|^2 = 3$, $e_3 = N_1(\alpha_1) = p$, and $e_4 = 1$, giving $M_G(F) = -9(1+4m)p$, and hence all the odd multiples of $9p$ satisfying (9.11). Likewise

$$f(x) = (x+1) - (A - Bx)(x^3-1)(x+1) + (m-1)\,h(x),$$
$$g(x) = (x^2+1) - (A - Bx)(x^3-1)(x+1) - m\,h(x),$$

has $a = 12(1-2m)$, $b_1 = -4$, $e_1e_2 = N_1(\omega - \omega^2) = 3$, $e_3 = N_1(\alpha_1)$ and $e_4 = 1$, and $M_G(F) = 9 \cdot 2^4(2m-1)p$, while

$$f(x) = (x+1) + (x^4+x^2+1) - (A - Bx)(x^3-1)(x+1) + (m-1)\,h(x),$$
$$g(x) = x - (A - Bx)(x^3-1)(x+1) + m\,h(x).$$

has $a = -24m$, $b_1 = 8$, $e_1e_2 = 3$, $e_3e_4 = p$, and $M_G(F) = -3^2 \cdot 2^6 mp$. Hence we can achieve all the even multiples of $9p$ satisfying (9.10).

Suppose now that $3^2 \parallel M_G(F)$ with $e = e_1e_2e_3e_4$ even, then $2^{8+2t} \parallel e$ and $3 \parallel e$. We can suppose that $M_G(F)$ is not divisible by a prime $p \equiv 7 \bmod 12$, since we already have all such multiples of these. Hence the odd powers of primes, other than 3, dividing e are all 1 mod 4 and hence $e2^{-8-2t}3^{-1}$ is 1 mod 4. Also the odd ab_1 are 1 mod 4 and the evens are odd multiples of 2^4 or multiples of 2^6. Thus either $M_G(F) = 2^8 m$ or $2^{10}m$ with $m \equiv -1 \bmod 4$, or $2^{12} \parallel M_G(F)$ or $2^{14} \mid M_G(F)$. We can achieve all these:

$$f(x) = 2(x^2+1) - (x^4+x^2+1) + m\,h(x),$$
$$g(x) = (x^3+1) + m\,h(x).$$

has $a = -3(1+4m)$, $b_1 = 1$, $e_1e_2 = N_1(4\omega^2 - 4) = 2^4 \cdot 3$, $e_3e_4 = N_1(4\omega^2) = 2^4$ and $M_G(F) = -3^2 \cdot 2^8(1+4m)$, while

$$f(x) = (1-x^2) - 2(x^3+1) + (m+1)\,h(x),$$
$$g(x) = -x^4 + x^2(x^3+1) + m\,h(x),$$

has $a = 3(1+4m)$, $b_1 = -1$, $e_1 = N_1(2(\omega^2-1)) = 2^2 \cdot 3$, $e_2 = N_1(4\omega) = 2^4$, $e_3 = N_1(2) = 2^2$, $e_4 = N_1(-2\omega^2) = 2^2$, and $M_G(F) = -3^2 \cdot 2^{10}(1+4m)$.

Taking

$$f(x) = 2(x^2+1) - h(-x) + m\,h(x),$$
$$g(x) = (x^3+1) + m\,h(x),$$

has $a = 12(1+2m)$, $b_1 = 4$, $e_1e_2 = N_1(4\omega^2 - 4) = 2^4 \cdot 3$, $e_3e_4 = N_1(4\omega^2) = 2^4$, and $M_G(F) = 3^2 \cdot 2^{12}(1+2m)$. Similarly

$$f(x) = 2(x^2+1) - (x^4+x^2+1) + m\,h(x),$$
$$g(x) = (x^3+1) - (x^4+x^2+1) + m\,h(x),$$

has $a = 24m$, $b_1 = -8$, $e_1e_2 = 2^4 \cdot 3$, $e_3e_4 = 2^4$, and $M_G(F) = -3^2 \cdot 2^{14}m$.

Case (c) Finally we deal with the measures coprime to 3. We achieve any value 1 mod 12 with (9.6). We can also get all multiples of 2^6 when the multiple is 1 mod 3, and all such odd multiples of 2^4:

$$M_G\left((x^2+1) + m\,h(x) + y\,m\,h(x)\right) = 2^4(6m+1),$$
$$M_G\left((x^4+x^2+1) + m\,h(x) + y\,(1 + m\,h(x))\right) = 2^6(3m+1).$$

Since odd measures are 1 mod 4 and even measures are divisible by exactly 2^4 or at least 2^6 this leaves the measures 5 mod 12 or $-2^4(6m+1)$ or $-2^6(3m+1)$.

Suppose that $p \equiv 1 \bmod 12$ is in $\mathcal{P}_1$ then, by Lemma 9.2, $p = N_1(\alpha)$ for some

$$\alpha = -1 - 2\omega(1-\omega) + 4(A+B\omega)(1-\omega). \tag{9.12}$$

Alternatively, if $p = 12t+5$ then $\alpha = -1-2\omega(1-\omega)+4((2t+1)+(t+1)\omega)(1-\omega)$ and $p^2 = N_1(\alpha)$ for an α of the form (9.12). If $p_1, p_2 \equiv 7 \bmod 12$ then, by Lemma 9.2, $p_1p_2 = N_1(\alpha)$ for some

$$\begin{aligned}\alpha &= \big(-1+2(1-\omega)+4(1-\omega)K_1(\omega)\big)\big(1+2(1-\omega)(1+\omega)+4(1-\omega)K_2(\omega)\big)\\ &= -1-2\omega(1-\omega)+4(1-\omega)K_3(\omega),\end{aligned}$$

which is also of the form (9.12). Hence for $k = p$ with p in $\mathcal{P}_1$ or $k = p^2$ with $p \equiv 5 \bmod 12$ or $k = p_1p_2$ with $p_1, p_2 \equiv 7 \bmod 12$ we can write $k = N_1(\alpha)$ for an α of the form (9.12) and taking

$$\begin{aligned}f(x) &= x(x^2+x+1) - (A-Bx)(x^3-1)(1+x) + m\,h(x),\\ g(x) &= x(x+1) - (A-Bx)(x^3-1)(1+x) + m\,h(x),\end{aligned}$$

or

$$\begin{aligned}f(x) &= x^2(1-x^3) - (A-Bx)(x^3-1)(1+x) + m\,h(x),\\ g(x) &= x(x+1) - (A-Bx)(x^3-1)(1+x) + m\,h(x),\end{aligned}$$

or

$$\begin{aligned}f(x) &= x(x^2+x+1) - (A-Bx)(x^3-1)(1+x) + m\,h(x),\\ g(x) &= x(x+1) - (x^4+x^2+1) - (A-Bx)(x^3-1)(1+x) - m\,h(x),\end{aligned}$$

we have $e_1e_2 = N_1(-1) = 1$, $e_3 = N_1(\alpha) = k$, $e_4 = N_1(-1) = 1$ with,

$$(a, b_1) = (5+12m, 1), \quad (-2^2(6m+1), 2^2), \quad \text{and} \quad (2^3(3m+1), -2^3),$$

respectively, and $M_G(F) = (5+12m)k$, $-2^4(6m+1)k$ and $-2^6(3m+1)k$.

So we can achieve the (5.7) and need just consider cases that do not contain the square of a prime 5 mod 12 or two primes 7 mod 12 or a prime in $\mathcal{P}_1$. Suppose first that $e = e_1e_2e_3e_4$ is odd, then since it is 1 mod 4, it must contain only primes from $\mathcal{P}_2$ and squares of primes 11 mod 12. Since $e \equiv 1 \bmod 3$, to get a measure 2 mod 3 we must have one of $a = f(1)^2 - g(1)^2$, $b_1 = f(-1)^2 - g(-1)^2 \equiv 1 \bmod 3$ and the other $-1 \bmod 3$. Replacing $\pm x$, $\pm f$, $\pm g$ we can assume that $f(1) \equiv 1 \bmod 3$, $g(1) \equiv 0 \bmod 3$, $f(-1) \equiv 0 \bmod 3$, $g(-1) \equiv 1 \bmod 3$. Since $f(\pm\omega) \equiv f(\pm 1) \bmod (1-\omega)$, $g(\pm\omega) \equiv g(\pm 1) \bmod (1-\omega)$, we can write

$$\begin{aligned}f(\omega) + g(\omega) &= 1 + (1-\omega)(A_1 + B_1\omega),\\ f(\omega) - g(\omega) &= 1 + (1-\omega)(A_2 + B_2\omega),\\ f(-\omega) + g(-\omega) &= 1 + (1-\omega)(A_3 + B_3\omega),\\ f(-\omega) - g(-\omega) &= -1 + (1-\omega)(A_4 + B_4\omega),\end{aligned}$$

and since $f(-\omega) \equiv f(\omega) \bmod 2$ and $g(-\omega) \equiv g(\omega) \bmod 2$ and 2 is prime we readily see that the A_i have the same parity and the B_i all have the same parity. Multiplying by x or x^2 as necessary we can assume that A_1 and B_1 are both even and hence all the A_i and B_i are all even. All the primes in $\mathcal{P}_2$ or 11 mod 12 factor in $\mathbb{Z}[\omega]$ into $1+4(A+B\omega)(1-\omega)$ times a unit, and (however we factor) an expression of this type with A_i, B_i even will have A_i, B_i both a multiple of 4. Hence $g(\omega) \equiv 0$

mod 2 and $g(-\omega) \equiv 1 \bmod 2$ contradicting $g(\omega) \equiv g(-\omega) \bmod 2$, so we have no extra measures. This leaves e even and hence $2^{8+2\ell_1} \parallel e$ and $2^{\ell_2} \parallel ab_1$ with $\ell_1 = 0, 4$ or $\ell_1 \geq 6$ and hence $2^t \parallel M_G(F)$ with $t = 8, 10, 12$ or $t \geq 14$. We can get all the multiples of 2^{12} and 2^{14}:

$$f(x) = (x^2 + x + 1) + m\, h(x),$$
$$g(x) = (x^2 - x + 1) + m\, h(x),$$

and

$$f(x) = (x^2 + x + 1) - (x^4 + x^2 + 1) + m\, h(x),$$
$$g(x) = (x^2 - x + 1) - (x^4 + x^2 + 1) - m\, h(x),$$

have $e_1e_2 = N_1(-4\omega^2) = 2^4$, $e_3e_4 = N_1(4\omega^2) = 2^4$ with, respectively,

$$a = 2^3(1 + 3m),\ \ b_1 = -2^3 \quad \text{and} \quad a = -2^2(1 + 6m),\ b_1 = 2^2,$$

giving $M_G(F) = -2^{14}(3m + 1)$ and $-2^{12}(6m + 1)$.

For $t = 8$, 10 we have $ab_1 \equiv 1 \bmod 4$. If e does not contain a prime 7 mod 12 then $e = 2^{\ell_2}n'$ with $\ell_2 = 8$ or 10 and $n' \equiv 1 \bmod 4$ and $M_G(F) = 2^8 n$ or $2^{10}n$ with $n \equiv 1 \bmod 4$, and all these 2 mod 3 are obtainable:

$$f(x) = (x^2 + x + 1) + m\, h(x),$$
$$g(x) = (x^3 + 1) + m\, h(x),$$

has $e_1e_2 = N_1(-2^2) = 2^4$, $e_3 = e_4 = N_1(-2\omega) = 2^2$, $a = (5 + 12m)$, $b_1 = 1$, and

$$f(x) = -1 - 2x^3 - m\, h(x),$$
$$g(x) = -1 + (x^2 + x + 1) + m\, h(x),$$

has $e_1e_2 = N_1(2^3) = 2^6$, $e_3 = N_1(-2\omega) = 2^2$, $e_4 = N_1(2 + 2\omega) = 2^2$ with $a = (5 + 12m)$, $b_1 = 1$, giving $M_G(F) = 2^8(5 + 12m)$ and $2^{10}(5 + 12m)$ respectively.

If e contains a prime $p \equiv 7 \bmod 12$ (since it has at most one the remaining odd primes are in $\mathcal{P}_2$ or squares of primes 11 mod 12) we have $M_G(F) = 2^4 pn$ or $2^6 pn$ with $n \equiv 1 \bmod 4$ and all are again achievable. We write

$$p = N_1(1 + 2(A + B\omega)(1 - \omega)), \quad k(x) := -x(A - Bx)(x^3 - 1)(1 + x),$$

then adding $k(x)$ to both $f(x)$ and $g(x)$ in the previous two examples, instead of $e_3 = N_1(-2\omega)$ we have $e_3 = N_1(-2\omega - 4w(A + B\omega)(1 - \omega)) = 2^2 p$, with the other values remaining unchanged, and $M_G(F) = 2^8(5 + 12m)p$ and $2^{10}(5 + 12m)p$. □

Proof of Theorem 5.3. We can write

$$F(x) = f(x^2) + xg(x^2) \in \mathbb{Z}[x], \quad f(x) = \sum_{j=0}^{5} a_j x^j,\ \ g(x) = \sum_{j=0}^{5} b_j x^j$$

so that

$$M_G(F) = \prod_{j=0}^{11} F(\omega_{12}^j) = abs_1s_2$$

where, as before $a = f(1)^2 - g(1)^2$, $b = f(-1)^2 + g(-1)^2$, and

$$s_1 := N_1(f(\omega)^2 - \omega g(\omega)^2),\ \ s_2 := N_1(f(-\omega)^2 + \omega g(-\omega)^2).$$

Observe that $s_1 \equiv a^2 \bmod 3$ and $s_2 \equiv b^2 \bmod 3$, so either $3 \nmid M_G(F)$ or $3^2 \mid M_G(F)$.

Case (i) Suppose that $M_G(F)$ is odd. Note that $M_G(x) = -1$ giving us both $\pm m$ for measures m. For the odd values we can get any integer coprime to 6 using $M_G\left(1 + m\,k(x)\right) = 1 + 12m$ and

$$M_G\left(\frac{x^5-1}{x-1} + m\,k(x)\right) = 5 + 12m, \quad k(x) := \frac{x^{12}-1}{x-1},$$

and any odd multiple of 27 with

$$M_G\left(1 + x^3 + x^6 + t\,k(x)\right) = 3^3(1+4t).$$

This leaves $9m$, $2, 3 \nmid m$. Moreover we cannot have $3 \mid b$ unless $3 \mid f(-1), g(-1)$ and $3^2 \mid b$ and $3^3 \mid M_G(F)$. So we assume that $3 \nmid s_2 b$ and $3 \parallel a$, $3 \parallel s_1$.

Suppose first that $3 \nmid f(-1)g(-1)$. Then $b \equiv 2 \bmod 3$ and hence is divisible by an odd power of some prime $p \equiv 2 \bmod 3$ which must itself be a sum of two squares, and $p \equiv 5 \bmod 12$. Conversely suppose that $p \equiv 5 \bmod 12$ then p is a sum of two squares both must $\pm 1 \bmod 3$ with one even and one odd. So changing signs as necessary $p = (6A+1)^2 + (6B+2)^2$. Taking

$$\begin{aligned} f(x) =& (x^2+1) - B(x^4+x^2+1)(x-1) + m\,h(x), \\ g(x) =& 1 - A(x^4+x^2+1)(x-1) + m\,h(x), \end{aligned}$$

we have $a = 3(1+4m)$, $b = (6B+2)^2 + (6A+1)^2 = p$, $s_1 = N_1(\omega^2 - \omega) = 3$, $s_2 = N_1(\omega^2+\omega) = 1$ and $M_G(F) = 9p(1+4m)$.

Suppose now that $3 \mid f(-1)g(-1)$. Writing

$$\begin{aligned} &u := |f(\omega)|^2 + |g(\omega)|^2, \quad v := \omega f(\omega)g(\omega^2) + \omega^2 f(\omega^2)g(\omega), \\ &\alpha := |f(-\omega)|^2 - |g(-\omega)|^2, \quad \beta := \omega f(-\omega)g(-\omega^2) + \omega^2 f(-\omega^2)g(-\omega), \end{aligned} \tag{9.13}$$

then u, v, α, β are integers with

$$\begin{aligned} (f(\omega) + \omega^2 g(\omega))(f(\omega^2) + \omega g(\omega^2)) &= u + v, \\ (f(\omega) - \omega^2 g(\omega))(f(\omega^2) - \omega g(\omega^2)) &= u - v, \\ (f(-\omega) + i\omega^2 g(-\omega))(f(-w^2) + i\omega g(-\omega^2)) &= \alpha + i\beta, \\ (f(-\omega) - i\omega^2 g(-\omega))(f(-\omega^2) - i\omega g(-\omega^2)) &= \alpha - i\beta, \end{aligned}$$

and

$$s_1 = (u+v)(u-v) = u^2 - v^2, \quad s_2 = (\alpha + i\beta)(\alpha - i\beta) = \alpha^2 + \beta^2.$$

Writing $f(-\omega) = f(\omega) + 2h_1(\omega)$, $f(\omega) = f(1) + (1-\omega)h_2(\omega)$, $f(-\omega) = f(-1) + (1-\omega)h_3(\omega)$ etc. and observing that since $3 \parallel a$ we must have $3 \nmid f(1)g(1)$, we readily get

$$\begin{gathered} u \equiv f(1)^2 + g(1)^2 \equiv 2 \bmod 3, \quad \alpha \equiv f(-1)^2 - g(-1)^2 \equiv \pm 1 \bmod 3, \\ u \equiv \alpha \bmod 2, \quad v \equiv \beta \bmod 2, \\ v \equiv 2f(1)g(1) \equiv \pm 1 \bmod 3, \quad \beta \equiv 2f(-1)g(-1) \equiv 0 \bmod 3. \end{gathered}$$

Suppose first that u is odd. Then v is even and $s_1 = u^2 - v^2 \equiv 1 \bmod 4$. Hence, in addition to the single prime 3, s_1 must contains an odd power of a prime $p \equiv 3 \bmod 4$. Since it is a norm in $\mathbb{Z}[\omega]$, the prime must be 1 or 7 mod 12 and so $p \equiv 7 \bmod 12$. From Lemma 9.2 we have $p = N_1(\alpha) = N_1(-\alpha\omega)$ where $\alpha = -1 + 2(1-\omega)(2A + 1 + 2B\omega)$ and

$$-\alpha\omega = 1 - \omega^2 + 4(\omega^2 + A(\omega^2 - \omega) + B(1-\omega^2)) = 1 - \omega^2 + 4(C + D\omega)$$

for some integers C, D. Taking

$$f(x) = x^3 + 1 + (C + Dx)(1 - x)(x^3 + 1) + m\, h(x),$$
$$g(x) = x + x(C + Dx)(1 - x)(x^3 + 1) + m\, h(x),$$

gives $a = 3(1 + 4m)$, $b = 1$, $s_2 = N_1(1) = 1$ and $f(\omega) - \omega^2 g(\omega) = 1$ with

$$f(\omega) + \omega^2 g(\omega) = 3 + 4(1 - \omega)(C + D\omega) = (1 - \omega)(-\alpha\omega),$$

and $s_1 = 3p$. Suppose next that u is even, so $\alpha \equiv \pm 1 \bmod 3$ is even and β is an odd multiple of 3. Since we have produced all multiples of primes 5 or 7 mod 12 we suppose that all the primes dividing $s_2 = \alpha^2 + \beta^2$ are 1 or 11 mod 12. Since α and β are both non-zero we have a non-trivial factorisation in $\mathbb{Z}[i]$ and s_2 must contain at least one prime $p \equiv 1 \bmod 12$. Moreover we can't have all these primes in $\mathcal{P}_2$, since

$$(6k + (6t + 1)i)(6k' \pm (6t' + 1)i) = 6k'' \mp 1 + 6t''i$$

all the possible factorisations of such an n in $\mathbb{Z}[i]$ would produce an $\alpha + i\beta$ of the form $6t \pm (6k + 1)i$ not $(6t + 2) + (6k + 3)i$, so at least one of the primes is in $\mathcal{P}_1$. Conversely suppose that $p \equiv 1 \bmod 12$ is in $\mathcal{P}_1$. Then by Lemma 9.2 we can write $p = N_2(\alpha_2)$ with

$$\alpha_2 = (1 + 2A + 2B\omega)(1 - \omega) + i\,(1 + 2(C + D\omega)(1 - \omega))\,.$$

We take

$$f(x) = 1 + x - (A - Bx)(1 + x)(x^3 - 1) + m\, h(x),$$
$$g(x) = x - x(C - Dx)(1 + x)(x^3 - 1) + m\, h(x),$$

which gives $a = 3(1 + 4m)$, $b = 1$, $s_1 = N_1(w - 1) = 3$ and

$$f(-\omega) = (1 - \omega)(1 + 2A + 2B\omega), \quad -w^2 g(-\omega) = 1 + (1 - \omega)(2C + 2D\omega),$$

and $s_2 = N_2(f(-\omega) - iw^2 g(-\omega)) = p$ and $M_G(F) = 9(1 + 4m)p$.

Case (ii) Suppose that $M_G(F)$ is even. Observe, as in the proof of Theorem 5.1, that ab is odd or a multiple of 2^4 and since $s_1 \equiv s_2 \bmod 2$, with a norm of a $\xi + \eta w$ even only when it is a power of 4 we have $s_1 s_2$ is odd or an odd multiple of 2^4 or a multiple of 2^6. We can achieve all odd multiples of 2^4 and all multiples of 2^6 that are coprime to 3, and multiples of 2^4 divisible by 3^2.

$$M_G\left(1 + x^4 + m\, k(x)\right) = 2^4(1 + 6m),$$
$$M_G\left((1 + x^4)^2 - \ h(-x^2) + m\, k(x)\right) = 2^6(1 + 3m),$$
$$M_G\left(1 - x + m\, k(x)\right) = 2^4 3^2 m.$$

That just leaves $2^5 m$ with $(m, 6) = 1$. Suppose first that $3 \mid f(-1)g(-1)$. As in the discussion in Theorem 5.1 we must have $f(-1)^2 + g(-1)^2 = 2n$ or $8n$, with here $n \equiv 2 \bmod 3$ odd. Hence n is divisible by an odd power of an odd prime $p \equiv 2 \bmod 3$ and since p factors in $\mathbb{Z}[i]$ must also be 1 mod 4 and $p \equiv 5 \bmod 12$. Conversely suppose that $p \equiv 5 \bmod 12$. Then $2p$ is a sum of two squares $2p = r^2 + s^2$. Since it is 1 mod 3, replacing r by $-r$ as necessary, we can assume that $3 \mid s$ and $r \equiv 1 \bmod 3$ and $2p = (1 - 3A)^2 + (3B)^2$. The choice

$$f(x) = (x^2 + 1) + A(x - 1)(x^4 + x^2 + 1) + m\, h(x),$$
$$g(x) = Bx(x - 1)(x^4 + x^2 + 1) + m\, h(x),$$

has $a = 4(1+6m)$, $s_1 = s_2 = N_1^2(1+\omega^2) = 1$, $b = (2-6A)^2 + (6B)^2 = 8p$, and $M_G(F) = 32(1+6m)p$.

Suppose that $3 \nmid f(-1)g(-1)$. Defining u, v and α, β as in (9.13) and observing that since $3 \nmid a$ we must have $3 \mid f(1)$ or $g(1)$ but not both, we readily get

$$u \equiv f(1)^2 + g(1)^2 \equiv 1 \bmod 3, \quad \alpha \equiv f(-1)^2 - g(-1)^2 \equiv 0 \bmod 3,$$

$$u \equiv \alpha \bmod 2, \quad v \equiv \beta \bmod 2,$$

$$v \equiv 2f(1)g(1) \equiv 0 \bmod 3, \quad \beta \equiv 2f(-1)g(-1) \equiv \pm 1 \bmod 3.$$

Suppose first that u is even. Since $2 \nmid s_1 = u^2 - v^2$ we get v is odd and $s_1 \equiv 3 \bmod 4$ is a positive integer so must be divisible by an odd power of a prime $p \equiv 3 \bmod 4$. Since n is the norm of an element of $\mathbb{Z}[\omega]$ which is a UFD the prime p must split in $\mathbb{Z}[\omega]$ and so $p \equiv 7 \bmod 12$. Conversely suppose that $p \equiv 7 \bmod 12$. Then we can, by Lemma 9.2, write $p = N_1(\alpha)$ with $\alpha = -1 + 2(2A + 1 + 2B\omega)(1-\omega)$. We take

$$f(x) = (x^2+1) + (A+Bx)(x^3+1)(1-x) + m\,h(x),$$
$$g(x) = x(1-x) + x(A+Bx)(x^3+1)(1-x) + m\,h(x),$$

then $a = 4(1+6m)$, $b = 8$, $s_2 = N_1(\omega^2+\omega) = 1$, with

$$f(\omega) + \omega^2 g(\omega) = -1 + 2(2A+1+2B\omega)(1-\omega), \quad f(\omega) - \omega^2 g(\omega) = -1,$$

and $s_1 = N_1(\alpha) = p$ and $M_G(F) = 32(6m+1)p$.

Suppose that u is odd. Then α is an odd multiple of 3 and $\beta \equiv \pm 1 \bmod 3$ is even. We have already obtained all multiples of primes 5 or 7 mod 12 so we can assume that $s_2 = \alpha^2 + \beta^2$ contains only primes 1 or 11 mod 12, but the primes 11 mod 12 do not split in $\mathbb{Z}[i]$ so we can not obtain a factorisation of s_2 with α and β both non-zero from just those primes. Thus s_2 contains at least one prime $p \equiv 1 \bmod 12$ with at least one of these in $\mathcal{P}_1$. Conversely suppose that p is in $\mathcal{P}_1$. By Lemma 9.2 there is an

$$\alpha_1 = -1 + 2(A+B\omega)(1-\omega) + i(2 + 2(C+D\omega)(1-\omega)).$$

with $p = N_2(\alpha_1)$, and

$$f(x) = x^2(x^2+1) - (A-Bx)(x^3-1)(1+x) + m\,h(x),$$
$$g(x) = x(x^3-1) + (C-Dx)x(x^3-1)(1+x) + m\,h(x),$$

has $a = 4(1+6m)$, $b = 8$, $s_1 = N_1(1) = 1$, with

$$f(-\omega) + i\omega^2 g(-\omega) = -1 + 2(A+B\omega)(1-\omega) + i\,(2 + 2(C+D\omega)(1-\omega)) = \alpha_1,$$

so that $s_2 = N_2(\alpha_1) = p$ and $M_G(F) = 32(6m+1)p$. □

10. Proof of Theorem 6.1

Note that $M_G(-F) = -M_G(F)$, so we take both signs for each value. In [9] it was shown that the measures for $\mathbb{Z}_p \times \mathbb{Z}_p$ coprime to p are exactly the $(p-1)$st roots of unity mod p^2. For $p = 3$ these are ± 1 mod 9 achieved with

$$M_G(\pm 1 + m(x^2+x+1)(y^2+y+1)) = 9m \pm 1.$$

For the multiples of 3 we note, writing $\omega = e^{2\pi i/3}$, that in $\mathbb{Z}[\omega]$

$$F(\omega^i, \omega^j) \equiv F(1,1) \bmod (1-\omega),$$

in particular if $3 \mid M_G(F)$ then $3 \mid F(1,1)$ and $(1-\omega) \mid F(\omega^i, \omega^j)$ in $\mathbb{Z}[\omega]$ for all i, j, and $3(1-\omega)^8 \mid M_G(F)$ and $3^5 \mid M_G(F)$. In fact more is true. We write our polynomial in the form

$$\begin{aligned} F(x,y) = (A_0 + A_1(x-1) + A_2(x-1)^2) \\ + (B_0 + B_1(x-1) + B_2(x-1)^2)(y-1) \\ + (C_0 + C_1(x-1) + C_2(x-1)^2)(y-1)^2. \end{aligned}$$

If $3 \mid F(1,1)$ we have $3 \mid A_0$ and hence

$$F(\omega^i, \omega^j) \equiv A_1(\omega^i - 1) + B_0(\omega^j - 1) \bmod (1-\omega)^2.$$

If $3 \mid A_1$ or $3 \mid B_0$ we have $(1-\omega)^2 \mid F(x,y)$ for $(x,y) = (1,\omega), (1,\omega^2)$ or $(\omega,1), (\omega^2,1)$ and we gain an additional 3. Similarly if $A_1 \equiv B_0 \bmod 3$ we have $(1-\omega)^2 \mid F(x,y)$ for $(x,y) = (\omega^2,\omega), (\omega,\omega^2)$ and if $A_1 \equiv -B_0 \bmod 3$ we have $(1-\omega)^2 \mid F(x,y)$ for $(x,y) = (\omega,\omega), (\omega^2,\omega^2)$. Hence we must have $3^6 \mid M_G(F)$.

Noting that $M_G(-F) = -M_G(F)$ we can obtain all multiples of 3^6 using

$$M_G(1 + 2x + m(x^2+x+1)(y^2+y+1)) = 3^6(1+3m),$$
$$M_G(1 + 2x - x(y^2+y+1) + m(x^2+x+1)(y^2+y+1)) = 3^7 m. \quad \square$$

Acknowledgement

We are very grateful to the reviewer for reading the manuscript so carefully, and for suggesting numerous minor improvements. The second author also thanks the University of Edinburgh for the invitation to visit, and the Edinburgh Mathematical Society for its financial support.

References

[1] T. M. Apostol, *Resultants of cyclotomic polynomials*, Proc. Amer. Math. Soc. **24** (1970), 457-462.
[2] M. Bhargava and J. Hanke, *Universal quadratic forms and the 290-theorem,* preprint.
[3] T. Boerkoel and C. Pinner, *Minimal group determinants and the Lind-Lehmer problem for dihedral groups*, arXiv:1802.07336 [math.NT].
[4] S. Clem and C. Pinner, *The Lind Lehmer constant for 3-groups*, to appear Integers.
[5] K. Conrad, *The origin of representation theory*, Enseign. Math. (2) **44** (1998), no. 3-4, 361-392.
[6] D. A. Cox, Primes of the form $x^2 + ny^2$, Fermat, Class Field Theory and Complex Multiplication, John Wiley, 1989.
[7] O. Dasbach and M. Lalín, *Mahler measure under variations of the base group,* Forum Math. **21** (2009), 621-637.
[8] L.E. Dickson, *Quatenary quadratic forms representing all integers*, Amer. J. Math. **49** (1927), 39–56.
[9] D. De Silva and C. Pinner, *The Lind-Lehmer constant for $\mathbb{Z}_p^n$*, Proc. Amer. Math. Soc. **142** (2014), no. 6, 1935–1941.
[10] D. De Silva, M. Mossinghoff, V. Pigno and C. Pinner, *The Lind-Lehmer constant for certain p-groups*, to appear Math. Comp.
[11] E. Formanek and D. Sibley, *The group determinant determines the group*, Proc. Amer. Math. Soc. **112** (1991), 649-656.
[12] N. Kaiblinger, *On the Lehmer constant of finite cyclic groups*, Acta Arith. **142** (2010), no. 1, 79-84.
[13] N. Kaiblinger, *Progress on Olga Taussky-Todd's circulant problem*, Ramanujan J. **28** (2012), no. 1, 45-60.
[14] H. Laquer, *Values of circulants with integer entries*, in A Collection of Manuscripts Related to the Fibonacci Sequence, pp. 212-217. Fibonacci Assoc., Santa Clara (1980)

[15] S. Lang, Cyclotomic Fields I and II, Graduate Texts in Mathematics 121, Springer-Verlag 1990.
[16] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. Math. (2) **34** (1933), no. 3, 461–479.
[17] E. T. Lehmer, *A numerical function applied to cyclotomy*, Bull. Amer. Math. Soc. **36** (1930), 291-298.
[18] D. Lind, *Lehmer's problem for compact abelian groups*, Proc. Amer. Math. Soc. **133** (2005), no. 5, 1411–1416.
[19] M. Mossinghoff, V. Pigno, and C. Pinner, *The Lind-Lehmer constant for* $\mathbb{Z}_2^r \times \mathbb{Z}_4^s$, to appear Mosc. J. Comb. Number Theory, arXiv:1805.05450 [math.NT].
[20] M. Newman, *On a problem suggested by Olga Taussky-Todd*, Ill. J. Math. **24** (1980), 156–158.
[21] M. Newman, *Determinants of circulants of prime power order*, Linear and Multilinear Algebra **9** (1980), 187–191.
[22] Tracy A. Pierce, The numerical factors of the arithmetic forms $\prod_{i=1}^{n}(1 \pm \alpha_i^m)$, Ann. of Math. (2) **18** (1916), no. 2, 53–64.
[23] V. Pigno and C. Pinner, *The Lind-Lehmer constant for cyclic groups of order less than* $892,371,480$, Ramanujan J. **33** (2014), no. 2, 295–300.
[24] C. Pinner and W. Vipismakul, *The Lind-Lehmer constant for* $\mathbb{Z}_m \times \mathbb{Z}_p^n$, Integers **16** (2016), #A46, 12pp.
[25] J.-P. Serre, Linear Representations of Finite Groups, Graduate Texts in Mathematics 42, Springer-Verlag 1977.
[26] W. Vipismakul, *The stabilizer of the group determinant and bounds for Lehmer's conjecture on finite abelian groups*, Ph. D. Thesis, University of Texas at Austin, 2013.
[27] L. Washington, Introduction to Cyclotomic Fields, GTM 83, Springer-Verlag, NY 1982.

Department of Mathematics, Kansas State University, Manhattan, KS 66506, USA
E-mail address: pinner@math.ksu.edu

School of Mathematics and Maxwell Institute for Mathematical Sciences, University of Edinburgh, Edinburgh EH9 3FD, Scotland, UK
E-mail address: c.smyth@ed.ac.uk