Can. J. Math., Vol. XXXII, No. 2, 1980, pp. 317–330

POLYNOMIAL INVARIANTS OF FINITE LINEAR GROUPS OF DEGREE TWO

W. CARY HUFFMAN

1. Introduction and notation. Recently invariant theory of linear groups has been used to determine the structure of several weight enumerators of codes. Under certain conditions on the code, the weight enumerator is invariant under a finite group of matrices. Once all the polynomial invariants of this group are known, the form of the weight enumerator is restricted and often useful results about the existence and structure of codes can be found. (See [**5**], [**8**], [**14**], and [**15**].) Many of the groups in these applications are of degree 2; in this paper all the invariants of finite 2×2 matrix groups over $\mathbf{C}$ are determined.

We begin with some definitions and theorems. Let $x_1, \ldots, x_n$ be independent variables and $\mathbf{C}[x_1, \ldots, x_n]$ the ring of complex polynomials in $x_1, \ldots, x_n$. Let $A = (\alpha_{ij})$ be an $n \times n$ complex matrix. If $f \in \mathbf{C}[x_1, \ldots, x_n]$, define

$$A \circ f = f\left(\sum_{j=1}^{n} \alpha_{1j}x_j, \ldots, \sum_{j=1}^{n} \alpha_{nj}x_j \right).$$

If B is another $n \times n$ matrix, then $B \circ (A \circ f) = (AB) \circ f$. Let $\mathscr{G}$ be a finite group of $n \times n$ matrices over $\mathbf{C}$ and $\chi: \mathscr{G} \to \mathbf{C}$ a homomorphism. Then f is a *relative invariant of* $\mathscr{G}$ *with respect to* χ if $A \circ f = \chi(A)f$ for all $A \in \mathscr{G}$; if $\chi \equiv 1$, f is an *absolute invariant* of $\mathscr{G}$. We denote by $\mathfrak{M}(\mathscr{G}, \chi)$ the set of all relative invariants of $\mathscr{G}$ with respect to χ. So $\mathfrak{M}(\mathscr{G}, 1)$ is a $\mathbf{C}$-algebra and $\mathfrak{M}(\mathscr{G}, \chi)$ is an $\mathfrak{M}(\mathscr{G}, 1)$-module and a graded Z-module. The object of this paper is to obtain a simple description of $\mathfrak{M}(\mathscr{G}, \chi)$ when $n = 2$. We remark that Burnside [**2**], Blichfeldt [**1**], DuVal [**4**], Klein [**7**], and possibly others completed a simpler version of this problem by describing invariants without regard to the characters χ and examining the groups projectively. Such a separation was necessary in the coding theory applications mentioned previously. Also invariants of groups generated by reflections were studied by Shephard-Todd [**13**] and Stanley [**16**]; recently results were obtained by Riemenschneider [**12**] which deal with absolute invariants of groups of degree 2 containing no reflections. We remark that in this paper any finite group of degree 2 and any linear character χ is covered.

We can write $\mathfrak{M}(\mathscr{G}, \chi) = \bigoplus_{i=0}^{\infty} \mathfrak{M}(\mathscr{G}, \chi)_i$ where

$$\mathfrak{M}(\mathscr{G}, \chi)_i = \{f \in \mathfrak{M}(\mathscr{G}, \chi) | f \text{ is homogeneous of degree } i\}.$$

Received May 27, 1977 and in revised form May 31, 1979.

Let $\varphi(\mathscr{G}, \chi)(\lambda) = \sum_{i=0}^{\infty} \dim_{\mathbf{C}}(\mathfrak{M}(\mathscr{G}, \chi)_i)\lambda^i$ be the *Molien series of* $\mathscr{G}$ *with respect to* χ. Then

THEOREM 1.1. (Molien [**11**]; see [**2**, p. 300] and [**15**])

$$\varphi(\mathscr{G}, \chi)(\lambda) = \frac{1}{|\mathscr{G}|} \sum_{A \in \mathscr{G}} \frac{\bar{\chi}(A)}{\det (I - \lambda A)}$$

where bar denotes complex conjugation.

In our situation we will be able to write $\varphi(\mathscr{G}, \chi)$ in the form

$$\varphi(\mathscr{G}, \chi)(\lambda) = \frac{\sum_{k=1}^{l} \lambda^{b_k}}{(1 - \lambda^{d_1})(1 - \lambda^{d_2})} \text{ for some } l$$

and correspondingly write $\mathfrak{M}(\mathscr{G}, \chi) = \bigoplus_{k=1}^{l} \gamma_k \mathbf{C}[f_1, f_2]$ where f_1, f_2 are algebraically independent and elements of $\mathfrak{M}(\mathscr{G}, 1)_{d_1}$, $\mathfrak{M}(\mathscr{G}, 1)_{d_2}$ and $\gamma_k \in \mathfrak{M}(\mathscr{G}, \chi)_{b_k}$. (See [**6**], [**9**], [**14**], [**15**] for discussion and conjectures regarding the forms of the Molien series and their relationship to the form of $\mathfrak{M}(\mathscr{G}, \chi)$.)

In Section 2, we give generators and characters of the finite groups of degree 2. In Section 3 the invariants for the monomial groups are determined, and in Section 4 the invariants for the primitive groups are given.

2. Groups of degree 2. Let $\mathscr{G}$ be a finite linear group of degree 2 over $\mathbf{C}$. If $\mathscr{H} = N^{-1}\mathscr{G}N$ then $\mathfrak{M}(\mathscr{H}, \chi) = N \circ \mathfrak{M}(\mathscr{G}, \chi^N)$; so we consider $\mathscr{G}$ up to change of basis. As is well known we may assume $\mathscr{G}$ is unitary. Such groups have been enumerated by DuVal [**4**] and Coxeter [**3**] using quaternions. We now give generators for the groups in the form we will need them later as well as the linear characters. It is straightforward to convert, say, Coxeter's list [**3**, Chapter 10] to those listed here. With each lemma we give the groups as in Coxeter's list [**3**] as well as the corresponding projective group in Blichfeldt [**1**]. Z_k is the cyclic group of order k, Z the integers, and $Z(\mathscr{G})$ the center of $\mathscr{G}$.

LEMMA 2.1. (Type 1 of [**3**]; Type A of [**1**]) *Let* $\mathscr{G} = \mathfrak{A}$ *be abelian of exponent* $e = p_1^{a_1} \ldots p_t^{a_t}$ *with* $p_1, \ldots, p_t$ *distinct primes. Let* ϵ *be a primitive* eth *root of* 1. *Then* $\mathfrak{A} \simeq Z_e \times Z_f$ *where* $g = e/f \in Z$. *Also*

i) $\mathfrak{A} = \langle B_1, B_2 \rangle \simeq \langle B_1 \rangle \times \langle B_2 \rangle$ *where*

$$B_1 = \begin{pmatrix} \epsilon^{v_1} & 0 \\ 0 & \epsilon^{v_2} \end{pmatrix} \textit{ and } B_2 = \begin{pmatrix} \epsilon^{g} & 0 \\ 0 & \epsilon^{gd} \end{pmatrix}$$

with

$$v_1 = p_1^{\alpha_1} \ldots p_q^{\alpha_q}, v_2 = jp_s^{\alpha_s} \ldots p_t^{\alpha_t}, q < s, \gcd(j, e) = 1, d = p_{q+1} \ldots \times p_{s-1}.$$

ii) *If* $g = p_1^{r_1} \ldots p_t^{r_t}$, *we may assume* $0 < \alpha_i \leqq r_i$ *for* $i = 1, \ldots, q$ *and* $i = s, \ldots, t$.

https://doi.org/10.4153/CJM-1980-024-6 Published online by Cambridge University Press

iii) *A character* χ *on* $\mathfrak{A}$ *must have values* $\chi(B_1) = \epsilon^{n_1}$ *and* $\chi(B_2) = \epsilon^{gn_2}$ *for some* n_1, n_2. *We may assume* $0 \leqq n_2 < f$ *(which we do in Section* 3).

LEMMA 2.2. (Type 2,3,3′,4 of [**3**]; Type B of [**1**]) *Let* $\mathscr{G}$ *be monomial and nonabelian with diagonal subgroup* $\mathfrak{A} \simeq Z_e \times Z_f$ *of index* 2 *and exponent* $e = p_1^{a_1} \ldots p_t^{a_t}$ *where* $g = e/f = p_1^{r_1} \ldots p_t^{r_t}$. *Let* ϵ *be a primitive* eth *root of* 1. *We may assume* $\mathscr{G} = \langle \mathfrak{A}, F \rangle$ *where* $\mathfrak{A} = \langle A_1, A_2 \rangle \simeq \langle A_1 \rangle \times \langle A_2 \rangle$ *and*

$$A_1 = \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^j \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 0 \\ 0 & \epsilon^g \end{pmatrix}, \quad F = \begin{pmatrix} 0 & 1 \\ \alpha^2 & 0 \end{pmatrix}$$

with $|F| = 2^{b+1}$ *and* α *a primitive* 2^{b+1} *root of* 1. *If* $2|e$, *let* $p_1 = 2$. *We also obtain*

i) *if* $p_1 = 2$, $b \leqq a_1$ *and if* $2 \nmid e$, $b = 0$;

ii) *if* $p_1 = 2$ *and* $r_1 > a_1 - b$ *then* $j \equiv 1 \bmod 2^{r_1-(a_1-b)}$;

iii) $\gcd(j, e) = 1$;

iv) $j^2 \equiv 1 \bmod g$.

v) *Let* $c_1 = \gcd(j - 1, d)$. *A character* χ *on* $\mathscr{G}$ *must have values* $\chi(A_1) = \epsilon^{n_1}$, $\chi(A_2) = \epsilon^{gn_2}$, $\chi(F) = \alpha^{n_3}$ *where*

$$n_1 \equiv (j + 1)n_2 \bmod (e/c_1) \text{ and } n_3 \equiv n_1 + n_2(1 - j) \bmod 2^b.$$

We remark that the first condition on n_1 and n_2 in v) comes from the two facts that $F^{-1}A_1F, F^{-1}A_2F \in \mathfrak{A}$ plus some straightforward calculations involving c_1. The second condition on n_1, n_2, n_3 comes from $F^2 \in \mathfrak{A}$, as does ii).

LEMMA 2.3. (Types 5,6 of [**3**]; Type C of [**1**]) *Let* $\mathscr{G}$ *be primitive and* $\mathscr{G}/Z(\mathscr{G}) \simeq A_4$. *Then* $\mathscr{G}$ *is either*

$$\mathscr{G}_1 = \left\langle Q, A, \begin{pmatrix} \mu & 0 \\ 0 & \mu \end{pmatrix} \right\rangle \text{ or } \mathscr{G}_2 = \left\langle Q, \alpha A, \begin{pmatrix} \mu & 0 \\ 0 & \mu \end{pmatrix} \right\rangle$$

where $A = \dfrac{1}{2}\begin{pmatrix} -1 + i & 1 - i \\ -1 - i & -1 - i \end{pmatrix}$, $Q = \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \right\rangle$ *is the quaternion group of order* 8, μ *is a primitive* dth *root of* 1, *and in* $\mathscr{G}_2$, α *is a primitive* 3^r *root of* 1 $(r \geqq 1)$ *and* $3 \nmid d$. *A character* χ *of* $\mathscr{G}$ *must satisfy* $\chi(\tau) = 1$ *for* $\tau \in Q$, $\chi\begin{pmatrix} \mu & 0 \\ 0 & \mu \end{pmatrix} = \mu^n$ *where* $2|n$ *if* $2|d$, $\chi(A) = 1, \omega$, *or* $\bar{\omega}$ *where* ω *is a primitive cube root of* 1 *if* $\mathscr{G} = \mathscr{G}_1$, *and* $\chi(\alpha A) = \alpha^m$ *if* $\mathscr{G} = \mathscr{G}_2'$.

LEMMA 2.4. (Types 7,8 of [**3**]; Type D of [**1**]) *Let* $\mathscr{G}$ *be primitive and* $\mathscr{G}/Z(\mathscr{G}) \simeq S_4$. *Then* $\mathscr{G}$ *is either*

$$\mathscr{G}_1 = \left\langle Q, A, B, \begin{pmatrix} \nu & 0 \\ 0 & \nu \end{pmatrix} \right\rangle \text{ or } \mathscr{G}_2 = \left\langle Q, A, \beta B, \begin{pmatrix} \nu & 0 \\ 0 & \nu \end{pmatrix} \right\rangle$$

where Q,A *are as in Lemma* 2.3, $B = \dfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ i & -1 \end{pmatrix}$, ν *is a primitive* dth *root of* 1, *and in* $\mathscr{G}_2$, β *is a primitive* 2^r *root of* 1 $(r \geqq 2)$ *and* $2 \nmid d$. *A character* χ *of* $\mathscr{G}$

https://doi.org/10.4153/CJM-1980-024-6 Published online by Cambridge University Press

must satisfy $\chi(\tau) = 1$ *for all* $\tau \in \langle Q, A\rangle$, $\chi\begin{pmatrix}\nu & 0\\ 0 & \nu\end{pmatrix} = \nu^n$ *where* $2|n$ *if* $2|d$, $\chi(B) = \pm 1$ *if* $\mathcal{G} = \mathcal{G}_1$, *and* $\chi(\beta B) = \beta^m$ *where* $2|m$ *if* $\mathcal{G} = \mathcal{G}_2$.

LEMMA 2.5. (Type 9 of [**3**]; Type E of [**1**]) *Let* $\mathcal{G}$ *be primitive and* $\mathcal{G}/Z(\mathcal{G}) \simeq A_5$. *Then* $\mathcal{G} = \mathcal{G}_j$ *for* $j = 1$ *or* 2 *where*

$$\mathcal{G}_j = \left\langle Q, A, C_j, \begin{pmatrix}\mu & 0\\ 0 & \mu\end{pmatrix}\right\rangle, \quad C_j = \begin{pmatrix}\gamma_j & \frac{1}{2}+\delta_j\\ -\frac{1}{2}+\delta_j & -\gamma_j\end{pmatrix},$$

$$\gamma_1 = \delta_2 = i\left(\frac{-1+\sqrt{5}}{4}\right), \gamma_2 = \delta_1 = i\left(\frac{-1-\sqrt{5}}{4}\right),$$

and μ *is a primitive* dth *root of* 1, *using the notation of Lemma* 2.3. *A character* χ *of* $\mathcal{G}$ *must satisfy* $\chi(\tau) = 1$ *for all* $\tau \in \langle Q, A, C_j\rangle$ *and* $\chi\begin{pmatrix}\mu & 0\\ 0 & \mu\end{pmatrix} = \mu^n$ *where* $2|n$ *if* $2|d$.

3. Relative invariants of the monomial groups. Theorems 3.1 and 3.10 give the invariants of the abelian and nonabelian monomial groups.

THEOREM 3.1. *Using the notation of Lemma* 2.1 *let* $m = e/v_1$, $n = ej/v_2$, $f_1 = x^m$, *and* $f_2 = y^n$. *Then there exists an integer* w *such that* $(v_2 - dv_1)w \equiv 1 \bmod fv_1$. *Let*

$$\mathfrak{L} = \{l | l \equiv (n_1 - n_2 v_1)w \bmod fv_1 \text{ and } 0 \leqq l < n\}.$$

If $l \in \mathfrak{L}$, *there exists a unique integer* $k(l)$ *such that* $k(l)v_1 \equiv n_1 - lv_2 \bmod e$ *where* $0 \leqq k(l) < m$. *Let* $\gamma_l = x^{k(l)}y^l$. *Then*

$$\mathfrak{M}(\mathfrak{A}, \chi) = \bigoplus_{l\in\mathfrak{L}} \gamma_l \mathbf{C}[f_1, f_2] \text{ and}$$

$$\varphi(\mathfrak{A}, \chi)(\lambda) = \frac{\sum_{l\in\mathfrak{L}} \lambda^{k(l)+l}}{(1-\lambda^n)(1-\lambda^m)}.$$

Proof. First, w exists because Lemma 2.1 ii) implies $fv_1|e$ and primes dividing e divide precisely one of v_2 and dv_1 giving gcd $(fv_1, v_2 - dv_1) = 1$. If $l \in \mathfrak{L}$, then $l(v_2 - dv_1) \equiv n_1 - n_2 v_1 \bmod fv_1$ which implies $n_1 - lv_2 \equiv 0 \bmod v_1$ and so $k(l)$ exists as $m = e/v_1$; $k(l)$ is unique as $k'v_1 \equiv k(l)v_1 \bmod e$ implies $k' \equiv k(l) \bmod m$.

As $\mathfrak{A}$ is diagonal, every element of $\mathfrak{M}(\mathfrak{A}, \chi)$ is a sum of monomials $x^k y^l \in \mathfrak{M}(\mathfrak{A}, \chi)$. Examining $B_i \circ x^k y^l$, $x^k y^l \in \mathfrak{M}(\mathfrak{A}, \chi)$, if and only if,

(*) $\quad kv_1 + lv_2 \equiv n_1 \bmod e \quad$ and $\quad k + ld \equiv n_2 \bmod f$.

Letting $n_1 = n_2 = 0$, $f_1, f_2 \in \mathfrak{M}(\mathfrak{A}, 1)$ using Lemma 2.1 ii). We are finished if we show that

a) if $l \in \mathfrak{L}$, $\gamma_l \in \mathfrak{M}(\mathfrak{A}, \chi)$;
b) if $x^k y^l \in \mathfrak{M}(\mathfrak{A}, \chi)$, then $x^k y^l \in \sum_{l\in\mathfrak{L}} \gamma_l \mathbf{C}[f_1, f_2]$;
c) $\sum_{l\in\mathfrak{L}} \gamma_l \mathbf{C}[f_1, f_2]$ is a direct sum.

https://doi.org/10.4153/CJM-1980-024-6 Published online by Cambridge University Press

For a) by definition of $k(l)$, $k(l)v_1 + lv_2 \equiv n_1 \bmod e$. As $fv_1|e$,

$$k(l)v_1 + lv_2 \equiv n_1 \bmod fv_1.$$

For $l \in \mathfrak{L}$, $l(v_2 - dv_1) \equiv n_1 - n_2v_1 \bmod dv_1$ whence

$$n_2v_1 - ldv_1 \equiv n_1 - lv_2 \equiv k(l)v_1 \bmod fv_1$$

implying (*). For b) let $l = l_1 + in$ and $k = k_1 + jm$ where $0 \leqq l_1 < n$ and $0 \leqq k_1 < m$. Then

$$x^ky^l = \gamma_{l_1}f_1^jf_2^i \text{ if } l_1 \in \mathfrak{L} \quad \text{and} \quad k_1 = k(l_1).$$

As $fv_1|e$, using (*) we obtain $n_1 - lv_2 + ldv_1 \equiv n_2v_1 \bmod fv_1$ which implies

$$l \equiv (n_1 - n_2v_1)w \bmod fv_1.$$

By Lemma 2.1 ii), $fv_1|n$ implies $l \equiv l_1 \bmod fv_1$ giving $l_1 \in \mathfrak{L}$. Clearly $kv_1 \equiv k_1v_1 \bmod e$ and $lv_2 \equiv l_1v_2 \bmod e$ giving $k_1v_1 \equiv kv_1 \equiv n_1 - lv_2 \equiv n_1 - l_1v_2 \bmod e$ and so $k_1 = k(l_1)$. Finally, for c), as powers of y in $\gamma_l\mathbf{C}[f_1, f_2]$ are congruent to $l \bmod n$, the sum is direct.

For the remainder of this section let $\mathscr{G}$ be as in Lemma 2.2. Clearly polynomials in $\mathfrak{M}(\mathscr{G}, \chi)$ are linear combinations of x^ly^l and $x^ky^l + \beta x^ly^k$ when $k \neq l$.

Lemma 3.2. *We have in the notation of Lemma 2.2.*

i) $\alpha^{2e} = 1$ *and* $\gcd(j,e) = 1$;

ii) $x^ky^l \in \mathfrak{M}(\mathfrak{A}, \chi)$ *if and only if* $k \equiv n_1 - jl \bmod e$ *and* $l \equiv n_2 \bmod f$;

iii) $x^ky^l \in \mathfrak{M}(\mathfrak{A}, \chi)$ *if and only if* $x^ly^k \in \mathfrak{M}(\mathfrak{A}, \chi)$;

iv) *if* $x^ky^l \in \mathfrak{M}(\mathfrak{A}, \chi)$, *then* $n_3 \equiv k + l \bmod 2^b$;

v) $x^ly^l \in \mathfrak{M}(\mathscr{G}, \chi)$ *if and only if* $x^ly^l \in \mathfrak{M}(\mathfrak{A}, \chi)$ *and* $n_3 \equiv 2l \bmod 2^{b+1}$;

vi) *if* $k \neq l$, *then* $x^ky^l + \beta x^ly^k \in \mathfrak{M}(\mathscr{G}, \chi)$ *if and only if* $x^ky^l \in \mathfrak{M}(\mathfrak{A}, \chi)$ *and* $\beta = \alpha^{2l-n_3}$.

Proof. i), ii), v), and vi) follow directly from Lemma 2.2. As $\mathfrak{A}$ is also generated by $\begin{pmatrix}\epsilon^j & 0\\ 0 & \epsilon\end{pmatrix}$ and $\begin{pmatrix}\epsilon^g & 0\\ 0 & 1\end{pmatrix}$, iii) is clear. For iv) we are done if $2 \nmid e$ by Lemma 2.2; so we assume $b \leqq a_1$. By ii) we obtain $k + l \equiv n_1 + (1 - j)l \bmod 2^b$ and $l \equiv n_2 \bmod 2^{a_1 - r_1}$ giving iv) if $b \leqq a_1 - r_1$ by Lemma 2.2 v). If $b > a_1 - r_1$, by Lemma 2.2 ii),

$$1 - j \equiv 0 \bmod 2^{r_1 - (a_1 - b)}$$

which implies $(1 - j)(l - n_2) \equiv 0 \bmod 2^b$ and so

$$k + l \equiv n_1 + (1 - j)n_2 \equiv n_3 \bmod 2^b$$

by Lemma 2.2 v).

Lemma 3.3. *Let m be the minimal positive integer such that* $(1 + j)fm \equiv 0 \bmod e$ *and* $2^b|fm$. *Then*

https://doi.org/10.4153/CJM-1980-024-6 Published online by Cambridge University Press

i) *m exists and $fm|e$ (i.e. $m|g$);*

ii) *if $(1+j)fm' \equiv 0 \bmod e$ and $2^b|fm'$, then $m|m'$;*

iii) *$f_1 = x^e + y^e$ and $f_2 = (xy)^{fm}$ are algebraically independent elements of $\mathfrak{M}(\mathscr{G}, 1)$.*

Proof. The homomorphism ψ: $Z \to Z_e$ given by $x\psi = (1+j)fx \bmod e$ has kernel $\langle m_1 \rangle$ with $e/f \in \langle m_1 \rangle$. The homomorphism θ: $\langle m_1 \rangle \to Z_{2^b}$ given by $x\theta = fx \bmod 2^b$ has kernel $\langle m \rangle$ containing e/f also by Lemma 2.2 i) giving i) and ii). Letting $n_1 = n_2 = n_3 = 0$, $f_1, f_2 \in \mathfrak{M}(\mathscr{G}, 1)$ and iii) follows easily.

From now on we may assume $0 \leqq n_2 < f$; let $d = e/fm$. Let $l(n) = fn + n_2$ and let $k(n)$ be such that $0 \leqq k(n) < e$ where $k(n) \equiv n_1 - jl(n) \bmod e$. Let $\mathscr{I}_1 = \{n | 0 \leqq n < m \text{ and } k(n) > l(n)\}$ and $\mathscr{I}_2 = \{n \in \mathscr{I}_1 | k(n) < fm\}$.

LEMMA 3.4. *Let $0 \leqq n, n^* < m$ with $n \in \mathscr{I}_1$. Assume $k(n) \equiv l(n^*) \bmod fm$, i.e., $k(n) = fmq + l(n^*)$ with $0 \leqq q < d$ (as $0 \leqq l(n^*) < fm$). Then we have*

i) *if $n^* \in \mathscr{I}_1$, then $q > 0$;*

ii) *if $q > 0$, then $k(n^*) = fm(d-q) + l(n)$.*

Proof. By Lemma 3.2 ii) and iii), $l(n) \equiv n_1 - jk(n) \equiv n_1 - jfmq - jl(n^*) \bmod e$. As $k(n^*) \equiv n_1 - jl(n^*) \bmod e$ and $(1+j)fm \equiv 0 \bmod e$,

$$l(n) \equiv k(n^*) + fmq \bmod e.$$

If $q = 0$ as $0 \leqq l(n), k(n^*) < e$, $l(n) = k(n^*)$ and $k(n) = l(n^*)$. As $l(n^*) = k(n) > l(n)$, $n^* > n$. If $n^* \in \mathscr{I}_1$, $l(n) = k(n^*) > l(n^*)$ which implies $n > n^*$, a contradiction giving i). If $q > 0$, then

$$0 \leqq l(n) < fm \leqq fmq + k(n^*) < 2e;$$

as $l(n) \equiv k(n^*) + fmq \bmod e$, $l(n) = fmq + k(n^*) - e$, giving ii).

LEMMA 3.5. *If $0 \leqq n, n' < m$ with $k(n) \equiv k(n') \bmod fm$, then $n = n'$. For each $n \in \mathscr{I}_1$ with $fm \leqq k(n)$ there is a unique $n^* \in \mathscr{I}_1$ such that $k(n) \equiv l(n^*) \bmod fm$. Also $k(n^*) \equiv l(n) \bmod fm$. If $k(n) < fm$ and $n \in \mathscr{I}_1$, then there is no $n^* \in \mathscr{I}_1$ with $k(n) \equiv l(n^*) \bmod fm$.*

Proof. If $k(n) \equiv k(n') \bmod fm$, as $fm|e$, $jl(n) \equiv jl(n') \bmod fm$ whence $l(n) \equiv l(n') \bmod fm$ by Lemma 3.2 i). So $n \equiv n' \bmod m$ and $n = n'$.

If $n \in \mathscr{I}_1$ with $fm \leqq k(n)$ then as $k(n) \equiv n_2 \bmod f$ by Lemma 3.2,

$$k(n) = fmq + fn^* + n_2 \text{ with } 0 \leqq n^* < m \text{ and } 0 < q < d.$$

By Lemma 3.4 ii), $k(n^*) = fm(d-q) + l(n) \geqq fm$ and thus $n^* \in \mathscr{I}_1$. If also for some $0 \leqq n' < m$, $k(n) \equiv l(n') \bmod fm$, then $l(n') \equiv l(n^*) \bmod fm$ and so $n' \equiv n^* \bmod m$ and $n' = n^*$. The last statement follows from Lemma 3.4 i).

Now let

$$A_n(x, y) = x^{k(n)}y^{l(n)} + \alpha^{2l(n)-n_3}x^{l(n)}y^{k(n)} \text{ for } n \in \mathscr{I}_1 \text{ and}$$

$$B_n(x, y) = x^{k(n)}y^{l(n)+e} + \alpha^{2l(n)-n_3}x^{l(n)+e}y^{k(n)} \text{ for } n \in \mathscr{I}_2.$$

By Lemma 3.2 and 3.3 i), $A_n, B_n \in \mathfrak{M}(\mathscr{G}, \chi)$. From now on let $g_{k,l} = x^k y^l + \alpha^{2l-n_3} x^l y^k$.

LEMMA 3.6. *Let* $\mathfrak{N} = \sum \gamma_n \mathbf{C}[f_1, f_2]$ *where* $\{\gamma_n\} = \{A_r | r \in \mathscr{I}_1\} \cup \{B_r | r \in \mathscr{I}_2\}$. *Let* $0 \leqq l < k < e$ *and assume* $g_{k,l} \in \mathfrak{M}(\mathscr{G}, \chi)$. *Then* $l = fmp + l(n)$ *where* $0 \leqq n < m$ *and either* i) $k = fmp + k(n)$ *or* ii) $k = fmp + k(n) - e$. *Also* $g_{k,l} \in \mathfrak{N}$ *and in case* i) $g_{k,l+e} \in \mathfrak{N}$ *and in case* ii) $g_{k+e,l} \in \mathfrak{N}$.

Proof. By Lemma 3.2 ii) $l = fmp + l(n)$ where $0 \leqq n < m$. Also

$$k \equiv n_1 - jl \equiv n_1 - jfmp - jl(n) \equiv k(n) + fmp \bmod e$$

as $(1 + j)fm \equiv 0 \bmod e$ and $k(n) \equiv n_1 - jl(n) \bmod e$. So as $0 \leqq fmp, k(n) < e$, i) or ii) holds.

Assume i) holds. Then $k > l$ implies $k(n) > l(n)$ and $n \in \mathscr{I}_1$. Then

$$g_{k,l} = f_2^{\,p} g_{k(n),l(n)} \in \mathfrak{N}$$

as $\alpha^{2fm} = 1$ since $2^b | fm$. Also

$$g_{k,l+e} = f_2^{\,p} g_{k(n),l(n)+e} \in \mathfrak{N}$$

if $k(n) < fm$. Assume $k(n) \geqq fm$. Let $n^* \in \mathscr{I}_1$ be as in Lemma 3.5. Then by Lemma 3.4, $k(n) = fmq + l(n^*)$ and $k(n^*) = fm(d - q) + l(n)$ which implies $l(n) + e = fmq + k(n^*)$. So

$$g_{k,l+e} = f_2^{\,p} g_{k(n),l(n)+e} = \alpha^{2k(n^*)-n_3} f_2^{\,p+q} g_{k(n^*),l(n^*)} \in \mathfrak{N},$$

the last equality requiring $2l(n^*) + 2k(n^*) \equiv 2n_3 \bmod 2^{b+1}$, which holds by Lemma 3.2 iv).

Assume ii) holds. As $p \leqq d - 1$ and $k \geqq 0$, $k(n) \geqq fm$. So $n \in \mathscr{I}_1$; let $n^* \in \mathscr{I}_1$ be as in Lemma 3.5. Then $k(n) = fmq + l(n^*)$ and $k(n^*) = fm(d - q) + l(n)$ which implies $k = fm(p + q - d) + l(n^*)$ and $l = fm(p + q - d) + k(n^*)$, the former implying $p + q - d \geqq 0$ as $0 \leqq l(n^*) < fm$. So

$$g_{k,l} = \alpha^{2k(n^*)-n_3} f_2^{\,p+q-d} g_{k(n^*),l(n^*)} \in \mathfrak{N}$$

again using $2l(n^*) + 2k(n^*) \equiv 2n_3 \bmod 2^{b+1}$. Also

$$g_{k+e,l} = f_2^{\,p} g_{k(n),l(n)} \in \mathfrak{N},$$

giving the lemma.

Now let $0 \leqq w$ be the minimal integer such that

$$(1 + j)l(w) \equiv n_1 \bmod e \text{ and } n_3 \equiv 2l(w) \bmod 2^{b+1}.$$

Let $0 \leqq v$ be the minimal integer such that $(1 + j)l(v) \equiv n_1 \bmod e$ and $n_3 \not\equiv 2l(v) \bmod 2^{b+1}$. Note that v or w may not exist; define $\mathscr{I}_3$ to be the elements of $\{v, w\}$ which do exist.

LEMMA 3.7. *For* $z \in \mathscr{I}_3$, $0 \leqq z < m$. *If* v_1 *or* w_1 *satisfy the equations defining* v *or* w *respectively, then* $v \equiv v_1 \bmod m$ *and* $w \equiv w_1 \bmod m$.

Proof. Assume $z \geqq m$. Then $(1+j)(l(z-m)) \equiv (1+j)(l(z)-fm) \equiv (1+j)l(z) \equiv n_1 \bmod e$. As $2fm \equiv 0 \bmod 2^{b+1}$, $2l(z) \equiv 2l(z-m) \bmod 2^{b+1}$, contradicting the choice of z.

Now $(1+j)l(w_1) \equiv (1+j)l(w) \bmod e$ which implies $(1+j)f(w_1-w) \equiv 0 \bmod e$; also $2l(w_1) \equiv 2l(w) \bmod 2^{b+1}$ and so $f(w_1-w) \equiv 0 \bmod 2^b$ giving $m|w_1-w$ by Lemma 3.3 ii). As above $(1+j)f(v_1-v) \equiv 0 \bmod e$. By Lemma 3.2,

$$n_3 \equiv 2l(v_1) \equiv 2l(v) \bmod 2^b.$$

As $2l(v_1) = 2^b r + n_3$, $2l(v) = 2^b s + n_3$ and by choice of v, v_1, both r and s are odd. Hence

$$2l(v_1) - 2l(v) = 2f(v_1-v) \equiv 0 \bmod 2^{b+1},$$

again yielding $m|v_1-v$.

Remarks. 1. If $z \in \mathscr{I}_3$, $l(z) = k(z)$.

2. If both v,w exist, then $|v-w| = m/2$ because $0 < 2|v-w| < 2m$ and $2|v-w|$ satisfies the conditions for m.

Now define $C_w(x, y) = (xy)^{l(m)}$ if w exists and

$$C_v(x, y) = x^{l(v)}y^{l(v)+e} + \alpha^{2l(w)-n_3}x^{l(v)+e}y^{l(v)}$$

if v exists. By Lemma 3.2, $C_w, C_v \in \mathfrak{M}(\mathscr{G}, \chi)$.

LEMMA 3.8. *Let* $\mathfrak{M} = \sum \gamma_n \mathbf{C}[f_1, f_2]$ *where* $\{\gamma_n\} = \{A_r|r \in \mathscr{I}_1\} \cup \{B_r|r \in \mathscr{I}_2\} \cup \{C_r|r \in \mathscr{I}_3\}$. *Then the above sum is direct.*

Proof. In $A_r\mathbf{C}[f_1, f_2]$, $B_r\mathbf{C}[f_1, f_2]$, and $C_r\mathbf{C}[f_1, f_2]$ the powers of x are congruent to $k(r)$ and $l(r)$ mod fm. Now $k(w) = l(w) \not\equiv k(v) = l(v) \bmod fm$. Let $n \in \mathscr{I}_1$ and $r \in \mathscr{I}_3$. If $k(n) \equiv k(r) \bmod fm$, $n = r$ by Lemma 3.5, a contradiction. If $l(n) \equiv k(r) \bmod fm$, then $l(n) \equiv l(r) \bmod fm$ and so $n = r$, a contradiction. So by Lemma 3.5, we only need to prove that

i) if $k(n) \geqq fm$ and $n \neq n^*$, then $A_n\mathbf{C}[f_1, f_2] + A_{n^*}\mathbf{C}[f_1, f_2]$ is direct;
ii) if $k(n) < fm$, then $A_n\mathbf{C}[f_1, f_2] + B_n\mathbf{C}[f_1, f_2]$ is direct.

Let $a(x, y) = \sum \alpha_{r,s}f_1^r f_2^s$ and $b(x, y) = \sum \beta_{r,s}f_1^r f_2^s$. To prove i) assume

$$(1) \quad a(x, y)A_n + b(x, y)A_{n^*} = 0.$$

By Lemmas 3.4 and 3.5, $k(n) + l(n) = fm(2q-d) + l(n^*) + k(n^*)$ where $0 < q < d$. Taking homogeneous components of degree z in (1), we obtain

$$(2) \quad 0 = \sum_{\mathscr{S}_1} \alpha_{r,s} f_1^r f_2^s A_n + \sum_{\mathscr{S}_2} \beta_{r,s} f_1^r f_2^s A_{n^*}$$

where $\mathscr{S}_1 = \{(r, s)|rd + 2s + (2q-d) = z_1\}$ and $\mathscr{S}_2 = \{(r, s)|rd + 2s = z_1\}$ when $z_1 = (1/fm)(z - (k(n^*) + l(n^*)))$. The degrees of x in the $\mathscr{S}_1$ sum are congruent to $k(n)$ and $l(n)$ mod fm and in the $\mathscr{S}_2$ sum are congruent to $k(n^*) \equiv l(n) \bmod fm$ and $l(n^*) \equiv k(n) \bmod fm$. Splitting into these two

https://doi.org/10.4153/CJM-1980-024-6 Published online by Cambridge University Press

degrees (as $k(n) \not\equiv l(n) \bmod fm$ since $n \neq n^*$) and letting $y = 1$, we obtain

$$(3) \quad \sum_{\mathscr{S}_1} \alpha_{r,s}(x^e + 1)^r x^{fm(s+q)} + \alpha^{2l(n^*)-n_3} \sum_{\mathscr{S}_2} \beta_{r,s}(x^e + 1)^r x^{fms} = 0$$

$$(4) \quad \alpha^{2l(n)-n_3} \sum_{\mathscr{S}_1} \alpha_{r,s}(x^e + 1)^r x^{fm(s+q)} + \sum_{\mathscr{S}_2} \beta_{r,s}(x^e + 1)^r x^{fm(s+d)} = 0.$$

Combining we obtain

$$(5) \quad \alpha^{2l(n^*)-n_3} \sum_{\mathscr{S}_2} \beta_{r,s}(X^d + 1)^r X^s - \alpha^{2k(n)-n_3} \sum_{\mathscr{S}_2} \beta_{r,s}(X^d + 1)^r X^{s+d} = 0$$

where $x^{fm} = X$. But $(X^d + 1)^r X^s$, $(X^d + 1)^r X^{s+d}$ have degrees $z_1 - s$ and $z_1 - s + d$. Clearly $\beta_{r,s} = 0$ for all $(r, s) \in \mathscr{S}_2$. Similarly using (3), $\alpha_{r,s} = 0$ for all $(r, s) \in \mathscr{S}_2$. We obtain ii) in an analogous manner, the crucial fact needed to obtain two equations being $k(n) \not\equiv l(n) \bmod fm$ since $0 \leqq l(n) < k(n) < fm$.

A straightforward induction yields

LEMMA 3.9. *Let* $\mathscr{S} \subseteq \{(\mu, \nu) | \mu, \nu$ *are nonnegative integers*$\} = \mathscr{T}$. *Assume* $(0, 0) \in \mathscr{S}$ *and either* $(1, 0)$ *or* $(0, 1) \in \mathscr{S}$. *Assume also*

i) $(\mu, \nu), (\mu, \nu + 1) \in \mathscr{S} \Rightarrow (\mu + 1, \nu) \in \mathscr{S}$;

ii) $(\mu, \nu), (\mu + 1, \nu) \in \mathscr{S} \Rightarrow (\mu, \nu + 1) \in \mathscr{S}$;

iii) $(\mu, \nu) \in \mathscr{S} \Rightarrow (\mu + 1, \nu + 1) \in \mathscr{S}$.

Then $\mathscr{S} = \mathscr{T}$.

THEOREM 3.10. $\mathfrak{M}(\mathscr{G}, \chi) = \oplus\, \gamma_n \mathbf{C}[f_1, f_2]$ *where* $\{\gamma_n\} = \{A_n | n \in \mathscr{I}_1\} \cup \{B_n | n \in \mathscr{I}_2\} \cup \{C_n | n \in \mathscr{I}_3\}$.

Proof. As $A_n, B_n, C_n \in \mathfrak{M}(\mathscr{G}, \chi)$ we only need to show $\mathfrak{M}(\mathscr{G}, \chi) \subseteq \mathfrak{M}$ where $\mathfrak{M} = \oplus\, \gamma_n \mathbf{C}[f_1, f_2]$ by Lemma 3.8. Clearly it suffices to show by examining the action of A_1, A_2, F on a polynomial in $\mathfrak{M}(\mathscr{G}, \chi)$ the following:

i) $x^l y^l \in \mathfrak{M}(\mathscr{G}, \chi) \Rightarrow x^l y^l \in \mathfrak{M}$ and

ii) if $k \neq l$, $g_{k,l} \in \mathfrak{M}(\mathscr{G}, \chi) \Rightarrow g_{k,l} \in \mathfrak{M}$.

For i), $l = fmq + l(w)$ by Lemmas 3.2 and 3.7 implying $x^l y^l = C_w f_2^q \in \mathfrak{M}$.

For ii) let $k = \mu^* e + k_1$, $l = \nu^* e + l_1$ with $0 \leqq k_1, l_1 < e$. As

$$g_{k,l} = \alpha^{2l-n_3} g_{l,k}$$

we may assume $l_1 \leqq k_1$. Let

$$\mathscr{S} = \{(\mu, \nu) | g_{\mu e+k_1, \nu e+l_1} \in \mathfrak{M}\}.$$

We are clearly finished if we satisfy the hypotheses of Lemma 3.9. We note that

$$f_1 g_{\mu e+k_1, \nu e+l_1} = g_{(\mu+1)e+k_1, \nu e+l_1} + g_{\mu e+k_1, (\nu+1)e+l_1}$$

using $\alpha^{2e} = 1$ implying i) and ii) of Lemma 3.9. Also

$$f_2{}^d g_{\mu e+k_1, \nu e+l_1} = g_{(\mu+1)e+k_1, (\nu+1)e+l_1}$$

giving iii) of Lemma 3.9.

By Lemma 3.6, if $l_1 < k_1$, $(0, 0) \in \mathscr{S}$ and either $(0, 1) \in \mathscr{S}$ or $(1, 0) \in \mathscr{S}$. If $l_1 = k_1$ and $n_3 \equiv 2l_1 \bmod 2^{b+1}$, by Lemma 3.7, $k_1 = l_1 = fmq + l(w)$. As $g_{l_1, l_1} = 2x^{l_1}y^{l_1} = 2f_2{}^qC_w \in \mathfrak{M}$ using $1 = \alpha^{2l_1 - n_3}$, we obtain $(0, 0) \in \mathscr{S}$. Now as

$$g_{l_1+e, l_1} = f_1x^{l_1}y^{l_1} \in \mathfrak{M},$$

$(1, 0) \in \mathfrak{M}$. Finally if $l_1 = k_1$ and $n_3 \not\equiv 2l_1 \bmod 2^{b+1}$, by Lemma 3.2, $n_3 \equiv 2l_1 \bmod 2^b$, giving $\alpha^{2l_1 - n_3} = -1$. As $g_{l_1, l_1} = 0 \in \mathfrak{M}$, $(0, 0) \in \mathscr{S}$. By Lemma 3.7, $k_1 = l_1 = fmq + l(v)$ which implies $g_{k_1, l_1+e} = f_2{}^qC_v \in \mathfrak{M}$ and $(0, 1) \in \mathscr{S}$.

In all cases Lemma 3.9 holds, completing the proof of the theorem.

Remark. The form for the Molien series in Theorem 3.10 is

$$\varphi(\mathscr{G}, \chi)(\lambda) = \frac{\sum_{n \in \mathscr{I}_1} \lambda^{l(n)+k(n)} + \sum_{n \in \mathscr{I}_2} \lambda^{l(n)+k(n)+e} + \lambda^{2l(w)} + \lambda^{2l(v)+e}}{(1 - \lambda^e)(1 - \lambda^{2fm})}.$$

4. Relative invariants of the primitive groups. In this section we describe the relative invariants of the groups of Lemmas 2.3–2.5. Define the following polynomials:

$$\begin{aligned}
\varphi_4 &= x^4 - 2\sqrt{3}\, i\, x^2y^2 + y^4 \\
\varphi_6 &= x^5y - xy^5 \\
\varphi_8 &= x^8 + 14x^4y^4 + y^8 = \varphi_4\bar{\varphi}_4 \\
\varphi_{12} &= x^{12} - 33(x^8y^4 + x^4y^8) + y^{12} \\
\psi_{12} &= 22\sqrt{5}\varphi_6{}^2 + 5\varphi_{12} \\
\psi_{20} &= 3\varphi_8\varphi_{12} - 38\sqrt{5}\varphi_6{}^2\varphi_8 \\
\psi_{30} &= 6696\varphi_6{}^5 + 225\varphi_6\varphi_8{}^3 - 580\sqrt{5}\varphi_6{}^3\varphi_{12}.
\end{aligned}$$

Also define $\sim$ as the involution in the Galois group of $\mathbf{Q}(i, \sqrt{5})/\mathbf{Q}(i)$ sending $\sqrt{5} \to -\sqrt{5}$ and $-$ is complex conjugation.

We use the notation of Lemmas 2.3, 2.4, 2.5. Let $\mathscr{H}_j = \langle Q, \omega^j A \rangle$ where $\omega = e^{2\pi i/3}$. The characters of $\mathscr{H}_j$ can be determined by $\chi_{i,j}(\omega^j A) = \omega^i$ where $i = 0, 1, 2$. Let $\mathscr{K} = \langle Q, A, B \rangle$. The characters of $\mathscr{K}$ are determined by $\chi_i(B) = (-1)^i$ for $i = 0, 1$. Let $\mathscr{L}_j = \langle Q, A, C_j \rangle$ for $j = 1, 2$. The characters of $\mathscr{L}_j$ are trivial. The groups $\mathscr{H}_j$, $\mathscr{K}$, $\mathscr{L}_j$ are respectively isomorphic to $SL_2(3)$, $GL_2(3)$ and $SL_2(5)$. The following lemma describes the $\mathfrak{M}(\mathscr{G}, \chi)$ for $\mathscr{G} \in \{\mathscr{H}_j, \mathscr{K}, \mathscr{L}_j\}$.

LEMMA 4.1. *The following table is valid:*

Proof. This is a straightforward application of Theorem 1.1. The polynomials φ_4, φ_6, φ_8, φ_{12}, ψ_{12}, ψ_{20}, ψ_{30} have also been obtained by other authors. For instance they are found in Sections 36, 37 of DuVal [4] where they were denoted by $\bar{P}$, S, Q, R, $\sqrt{5}I$, D, T respectively. (DuVal's study first considered the groups projectively (Sections 36, 37) and secondly considered the absolute

$\mathscr{G}$	χ	$\mathfrak{M}(\mathscr{G}, \chi)$	$\varphi(\mathscr{G}, \chi)$
$\mathscr{H}_0$	$\chi_{0,0}$	$\mathbf{C}[\varphi_6, \varphi_8] \oplus \varphi_{12}\mathbf{C}[\varphi_6, \varphi_8]$	$\dfrac{1 + \lambda^{12}}{(1 - \lambda^6)(1 - \lambda^8)}$
$\mathscr{H}_0$	$\chi_{1,0}$	$\bar{\varphi}_4\mathbf{C}[\varphi_6, \varphi_8] \oplus \varphi_4{}^2\mathbf{C}[\varphi_6, \varphi_8]$	$\dfrac{\lambda^4 + \lambda^8}{(1 - \lambda^6)(1 - \lambda^8)}$
$\mathscr{H}_0$	$\chi_{2,0}$	$\varphi_4\mathbf{C}[\varphi_6, \varphi_8] \oplus \bar{\varphi}_4{}^2\mathbf{C}[\varphi_6, \varphi_8]$	
$\mathscr{H}_1$	$\chi_{0,1}$	$\mathbf{C}[\varphi_4, \varphi_6]$	$\dfrac{1}{(1 - \lambda^4)(1 - \lambda^6)}$
$\mathscr{H}_2$	$\chi_{0,2}$	$\mathbf{C}[\bar{\varphi}_4, \varphi_6]$	
$\mathscr{H}_1$	$\chi_{1,1}$	$\bar{\varphi}_4{}^2\mathbf{C}[\varphi_4, \varphi_6]$	$\dfrac{\lambda^8}{(1 - \lambda^4)(1 - \lambda^6)}$
$\mathscr{H}_2$	$\chi_{2,2}$	$\varphi_4{}^2\mathbf{C}[\bar{\varphi}_4, \varphi_6]$	
$\mathscr{H}_1$	$\chi_{2,1}$	$\bar{\varphi}_4\mathbf{C}[\varphi_4, \varphi_6]$	$\dfrac{\lambda^4}{(1 - \lambda^4)(1 - \lambda^6)}$
$\mathscr{H}_2$	$\chi_{1,2}$	$\varphi_4\mathbf{C}[\bar{\varphi}_4, \varphi_6]$	
$\mathscr{K}$	χ_0	$\mathbf{C}[\varphi_6, \varphi_8]$	$\dfrac{1}{(1 - \lambda^6)(1 - \lambda^8)}$
$\mathscr{K}$	χ_1	$\varphi_{12}\mathbf{C}[\varphi_6, \varphi_8]$	$\dfrac{\lambda^{12}}{(1 - \lambda^6)(1 - \lambda^8)}$
$\mathscr{L}_1$	1	$\mathbf{C}[\psi_{12}, \psi_{20}] \oplus \psi_{30}\mathbf{C}[\psi_{12}, \psi_{20}]$	$\dfrac{1 + \lambda^{30}}{(1 - \lambda^{12})(1 - \lambda^{20})}$
$\mathscr{L}_2$	1	$\mathbf{C}[\tilde{\psi}_{12}, \tilde{\psi}_{20}] \oplus \tilde{\psi}_{30}\mathbf{C}[\tilde{\psi}_{12}, \tilde{\psi}_{20}]$	

invariants (Section 39). The present table is thus more extensive because it separates out the relative invariants.)

We now state a theorem giving the invariants of $\mathscr{G}_1$ of Lemma 2.3.

THEOREM 4.2. *Using the notation of Lemma* 2.3, *let* $m_1 = d/\gcd(6, d)$, $m_2 = d/\gcd(8, d)$, *and* $\mathscr{S} = \{(j, k) | 0 \leqq j < m_1, 0 \leqq k < m_2\}$. *Let*

$$\mathscr{I}_t = \{(j, k) \in \mathscr{S} | 6j + 8k + 4t \equiv n \bmod d\} \text{ for } t = 0, 1, 2, 3.$$

Define $\{\gamma_i\}$ *according to the following*

$\chi(A)$	$\{\gamma_i\}$
1	$\{\varphi_6{}^j\varphi_8{}^k \| (j, k) \in \mathscr{I}_0\} \cup \{\varphi_6{}^j\varphi_8{}^k\varphi_{12} \| (j, k) \in \mathscr{I}_3\}$
ω	$\{\varphi_6{}^j\varphi_8{}^k\bar{\varphi}_4 \| (j, k) \in \mathscr{I}_1\} \cup \{\varphi_6{}^j\varphi_8{}^k\varphi_4{}^2 \| (j, k) \in \mathscr{I}_2\}$
$\bar{\omega}$	$\{\varphi_6{}^j\varphi_8{}^k\varphi_4 \| (j, k) \in \mathscr{I}_1\} \cup \{\varphi_6{}^j\varphi_8{}^k\bar{\varphi}_4{}^2 \| (j, k) \in \mathscr{I}_2\}$

Then

$$\mathfrak{M}(\mathscr{G}_1, \chi) = \oplus \gamma_i\mathbf{C}[\varphi_6{}^{m_1}, \varphi_8{}^{m_2}] \text{ and}$$

$$\varphi(\mathscr{G}_1, \chi) = \frac{1}{(1 - \lambda^{6m_1})(1 - \lambda^{8m_2})} \sum \lambda^{d(i)}$$

where $d(i)$ *is the degree of* γ_i.

https://doi.org/10.4153/CJM-1980-024-6 Published online by Cambridge University Press

Proof. By Lemma 4.1, $\sum \gamma_i \mathbf{C}[\varphi_6^{m_1}, \varphi_8^{m_2}]$ is direct and $\varphi_6^{m_1}$, $\varphi_8^{m_2}$ are algebraically independent. We examine $\chi(A) = 1$, the others being similar. By examining $\mathfrak{M}(\mathscr{H}_0, \chi_{0,0})$ of Lemma 4.1, a homogeneous $f = f_1 + f_2$ is in $\mathfrak{M}(\mathscr{G}_1, \chi)$ where $f_1 = \varphi_6^j \varphi_8^k$ and $f_2 = \varphi_{12}\varphi_6^r\varphi_8^s$ if and only if $\begin{pmatrix} \mu & 0 \\ 0 & \mu \end{pmatrix} \circ f_i = \mu^n f_i$ or equivalently $6j + 8k \equiv n \bmod d$ and $6r + 8s + 12 \equiv n \bmod d$. Clearly the result holds.

We now examine $\mathscr{G}_2$ of Lemma 2.3.

THEOREM 4.3. *Using the notation of Lemma* 2.3, *let* $b = 3^r$ *if* $r > 1$ *and* $b = 1$ *if* $r = 1$. *Let* $c = 3^{r-1}$. *Define* $m_1 = db/\gcd(4, db)$, $m_2 = db/\gcd(6, db)$, *and* $\mathscr{S} = \{(j, k) | 0 \leqq j < m_1, 0 \leqq k < m_2\}$. *For* $t = 0, 1, 2$ *define*

$$\mathscr{I}_t = \{(j, k) \in \mathscr{S} | m - (2c + 1)(4j + 6k + 4t) \equiv 2tc \bmod 3^r, n \equiv 4j + 6k + 4t \bmod d\}.$$

Define

$$\{\gamma_i\} = \{\varphi_4^j\varphi_6^k | (j, k) \in \mathscr{I}_0\} \cup \{\varphi_4^j\varphi_6^k\bar{\varphi}_4 | (j, k) \in \mathscr{I}_1\} \cup \{\varphi_4^j\varphi_6^k\bar{\varphi}_4^2 | (j, k) \in \mathscr{I}_2\}.$$

If $\alpha^c = \omega$,

$$\mathfrak{M}(\mathscr{G}_2, \chi) = \oplus \gamma_i \mathbf{C}[\varphi_4^{m_1}, \varphi_6^{m_2}]$$

and if $\alpha^c = \bar{\omega}$,

$$\mathfrak{M}(\mathscr{G}_2, \chi) = \oplus \bar{\gamma}_i \mathbf{C}[\bar{\varphi}_4^{m_1}, \varphi_6^{m_2}].$$

In either case

$$\varphi(\mathscr{G}_2, \chi) = \frac{1}{(1 - \lambda^{4m_1})(1 - \lambda^{6m_2})} \sum \lambda^{d(i)}$$

where $d(i)$ *is the degree of* γ_i.

Proof. We do the case $\alpha^c = \omega$. The sum for $\mathfrak{M}(\mathscr{G}_2, \chi)$ is direct if we show $\mathbf{C}[\varphi_4, \varphi_6] + \bar{\varphi}_4\mathbf{C}[\varphi_4, \varphi_6] + \bar{\varphi}_4^2\mathbf{C}[\varphi_4, \varphi_6]$ is direct. Let $p_i \in \bar{\varphi}_4^i\mathbf{C}[\varphi_4, \varphi_6]$ where $p_0 + p_1 + p_2 = 0$. Applying ωA and $(\omega A)^2$ we obtain $p_0 + \omega^2 p_1 + \omega p_2 = 0$ and $p_0 + \omega p_1 + \omega^2 p_2 = 0$ by Lemma 4.1, yielding $p_i = 0$ for $i = 0, 1, 2$.

By Lemma 4.1, $\varphi_4^{m_1}$, $\varphi_6^{m_2}$ are algebraically independent absolute invariants of $\mathscr{G}_2$. If p is a homogeneous polynomial of degree z, $(\alpha A) \circ p = \alpha^m p$ if and only if $(\omega A) \circ p = \alpha^{m-(2c+1)z} p$ and $\begin{pmatrix} \mu & 0 \\ 0 & \mu \end{pmatrix} \circ p = \mu^n p$ if and only if $z \equiv n \bmod d$. So $p \in \mathfrak{M}(\mathscr{G}_2, \chi)$ if and only if $p \in \mathbf{C}[\varphi_4, \varphi_6]$, $\bar{\varphi}_4\mathbf{C}[\varphi_4, \varphi_6]$, or $\bar{\varphi}_4^2\mathbf{C}[\varphi_4, \varphi_6]$ where $z = 4j + 6k + 4t$ with $t = 0, 1, 2$ respectively and $m - (2c + 1)z \equiv 0, 2c, 4c \bmod 3^r$ respectively and $z \equiv n \bmod d$. The result is now clear.

The next theorem gives corresponding results for the groups of Lemma 2.4; its proof is similar to the previous ones.

THEOREM 4.4. *Using the notation of Lemma 2.4, if $\mathscr{G} = \mathscr{G}_1$ let $b = 1$ and $m = 1$, and if $\mathscr{G} = \mathscr{G}_2$, let $b = 2^r$. Define*

$$m_1 = db/\gcd(6, db),\ m_2 = db/\gcd(8, db),\ \textit{and}\ \mathscr{S} = \{(j, k) | 0 \leqq j < m_1,\ 0 \leqq k < m_2\}.$$

Let

$$\mathscr{I}_t = \{(j, k) \in \mathscr{S} | m - (6j + 8k + 12t) \equiv 0 \bmod b \ \textit{and}\ n \equiv 6j + 8k + 12t \bmod d\}\ \textit{for}\ t = 0, 1.$$

Define $\{\gamma_i\}$ according to the following:

$\mathscr{G}$	$\{\gamma_i\}$
$\mathscr{G}_1$	if $\chi(B) = 1$ $\{\varphi_6{}^j\varphi_8{}^k | (j, k) \in \mathscr{I}_0\}$
$\mathscr{G}_1$	if $\chi(B) = -1$ $\{\varphi_6{}^j\varphi_8{}^k\varphi_{12} | (j, k) \in \mathscr{I}_1\}$
$\mathscr{G}_2$	$\{\varphi_6{}^j\varphi_8{}^k | (j, k) \in \mathscr{I}_0\} \cup \{\varphi_6{}^j\varphi_8{}^k\varphi_{12} | (j, k) \in \mathscr{I}_1\}$

Then

$$\mathfrak{M}(\mathscr{G}, \chi) = \oplus\ \gamma_i \mathbf{C}[\varphi_6{}^{m_1}, \varphi_8{}^{m_2}] \quad \textit{and} \quad \varphi(\mathscr{G}, \chi) = \frac{1}{(1 - \lambda^{6m_1})(1 - \lambda^{8m_2})} \times \sum \lambda^{d(i)}$$

where $d(i)$ is the degree of γ_i.

The final result is for the groups of Lemma 2.5.

THEOREM 4.5. *Using the notation of Lemma 2.5, let*

$$m_1 = d/\gcd(12, d),\ m_2 = d/\gcd(20, d),\ \textit{and}\ \mathscr{S} = \{(j, k) | 0 \leqq j < m_1,\ 0 \leqq k < m_2\}.$$

Define

$$\mathscr{I}_t = \{(j, k) \in \mathscr{S} | 12j + 20k + 30t \equiv n \bmod d\}\ \textit{for}\ t = 0, 1.$$

Let

$$\{\gamma_i\} = \{\psi_{12}{}^j\psi_{20}{}^k | (j, k) \in \mathscr{I}_0\} \cup \{\psi_{12}{}^j\psi_{20}{}^k\psi_{30} | (j, k) \in \mathscr{I}_1\}.$$

Then

$$\mathfrak{M}(\mathscr{G}_1, \chi) = \oplus\ \gamma_i \mathbf{C}[\psi_{12}{}^{m_1}, \psi_{20}{}^{m_2}]\ \textit{and}\ \mathfrak{M}(\mathscr{G}_2, \chi) = \oplus\ \tilde{\gamma}_i \mathbf{C}[\tilde{\psi}_{12}{}^{m_1}, \tilde{\psi}_{20}{}^{m_2}].$$

Also

$$\varphi(\mathscr{G}_j, \chi) = \frac{1}{(1 - \lambda^{12m_1})(1 - \lambda^{20m_2})} \sum \lambda^{d(i)}$$

where $d(i)$ is the degree of γ_i.

We remark that $\mathfrak{M}(\mathscr{G}, 1)$ is a ring and hence $\gamma_i\gamma_j \in \mathfrak{M}(\mathscr{G}, 1)$ when the γ_i's are as in the last four theorems when $\chi \equiv 1$. Expressing $\gamma_i\gamma_j$ in the natural way in $\mathfrak{M}(\mathscr{G}, 1)$ gives a syzygy. All syzygies in this section can be obtained from the following:

$$\bar{\varphi}_4{}^2\bar{\varphi}_4 = \varphi_4{}^3 + 12\sqrt{3}\, i\, \varphi_6{}^2$$
$$(\bar{\varphi}_4{}^2)^2 = \varphi_4{}^3\bar{\varphi}_4 + 12\sqrt{3}\, i\, \varphi_6{}^2\bar{\varphi}_4$$
$$\varphi_{12}{}^2 = \varphi_8{}^3 - 108\varphi_6{}^4$$
$$500\psi_{30}{}^2 = 27\sqrt{5}\,\psi_{12}{}^5 - 3125\sqrt{5}\,\psi_{20}{}^3.$$

These syzygies can also be found in [**4**, Sections 36, 37]. The present author has taken great care to validate the results of this section by hand and with computer.

References

1. H. F. Blichfeldt, *Finite collineation groups* (University of Chicago Press, Chicago, 1917).
2. W. Burnside, *Theory of groups of finite order* (Dover, New York, 1955).
3. H. S. M. Coxeter, *Regular complex polytopes* (Cambridge University Press, 1974).
4. P. DuVal, *Homographies, quaternions and rotations* (Oxford: Oxford University Press, 1964).
5. A. M. Gleason, *Weight polynomials of self-dual codes and the MacWilliams identities*, in: Actes Congrès Internat. Math. 1970, Vol. 3, Gauthiers-Villars, Paris (1971), 211–215.
6. W. C. Huffman and N. J. A. Sloane, *Most primitive groups have messy invariants*, to appear in Adv. in Math.
7. F. Klein, *Lectures on the icosahedron and the solution of equations of the fifth degree* (Dover, New York, 1956).
8. F. J. MacWilliams, C. L. Mallows, and N. J. A. Sloane, *Generalizations of Gleason's theorem on weight enumerators of self-dual codes*, IEEE Trans. Information Theory, IT-*18* (1972), 794–805.
9. C. L. Mallows and N. J. A. Sloane, *On the invariants of a linear group of order* 336, Proc. Camb. Phil. Soc. *74* (1973), 435–440.
10. G. A. Miller, H. F. Blichfeldt, and L. E. Dickson, *Theory and applications of finite groups* (Dover, New York, 1961).
11. T. Molien, *Über die Invarianten der lineare Substitutionsgruppe*, Sitzungsber. König. Preuss. Akad. Wiss. (1897), 1152–1156.
12. O. Riemenschneider, *Die Invarianten der endlichen Untergruppen von* GL(2, **C**), Math Zeit. *153* (1977), 37–50.
13. G. C. Shephard, and J. A. Todd, *Finite unitary reflection groups*, Can. J. Math. *6* (1954), 274–304.
14. N. J. A. Sloane, *Error-correcting codes and invariant theory: new applications of a nineteenth-century technique*, Amer. Math. Monthly *84* (1977), 82–107.
15. ——— *Weight enumerators of codes*, in *Combinatorics* (Proceedings of the NATO Advanced Study Institute, July, 1974), 115–142.
16. R. Stanley, *Relative invariants of finite groups generated by pseudoreflections*, J. Algebra *49* (1977), 134–148.

Loyola University,
Chicago, Illinois