

Mathematical Proceedings of the Cambridge Philosophical Society

<http://journals.cambridge.org/PSP>

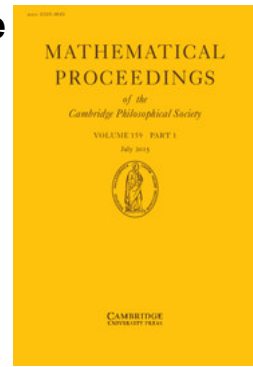
Additional services for *Mathematical Proceedings of the Cambridge Philosophical Society*:

Email alerts: [Click here](#)

Subscriptions: [Click here](#)

Commercial reprints: [Click here](#)

Terms of use : [Click here](#)



On the invariants of a linear group of order 336

C. L. Mallows and N. J. A. Sloane

Mathematical Proceedings of the Cambridge Philosophical Society / Volume 74 / Issue 03 / November 1973,
pp 435 - 440

DOI: 10.1017/S0305004100077161, Published online: 24 October 2008

Link to this article: http://journals.cambridge.org/abstract_S0305004100077161

How to cite this article:

C. L. Mallows and N. J. A. Sloane (1973). On the invariants of a linear group of order 336. *Mathematical Proceedings of the Cambridge Philosophical Society*, 74, pp 435-440 doi:10.1017/S0305004100077161

Request Permissions : [Click here](#)

On the invariants of a linear group of order 336

BY C. L. MALLOWS AND N. J. A. SLOANE

Bell Laboratories, Murray Hill, New Jersey

(Received 2 April 1973)

Abstract. The polynomial invariants of a certain classical linear group of order 336 arise naturally in studying error-correcting codes over GF(7). An incomplete description of these invariants was given by Maschke in 1893. With the aid of the Poincaré series for this group, found by Edge in 1947, we complete Maschke's work by giving a unique representation for the invariants in terms of 12 basic invariants. A conjecture is made concerning the relationship between the Poincaré series and the degrees of the basic invariants for any linear group. A partial answer to this conjecture, due to E. C. Dade, is given.

1. *Introduction.* Let \mathcal{G} be the group of order 336 generated by

$$\begin{pmatrix} 1 & & & \\ & \omega & & \\ & & \omega^4 & \\ & & & \omega^2 \end{pmatrix} \quad \text{and} \quad \frac{1}{\sqrt{-7}} \begin{pmatrix} 1 & 2 & 2 & 2 \\ 1 & \omega + \omega^6 & \omega^2 + \omega^5 & \omega^3 + \omega^4 \\ 1 & \omega^2 + \omega^5 & \omega^3 + \omega^4 & \omega + \omega^6 \\ 1 & \omega^3 + \omega^4 & \omega + \omega^6 & \omega^2 + \omega^5 \end{pmatrix},$$

where $\omega = e^{\frac{2\pi i}{7}}$; thus \mathcal{G} is the complex four-dimensional representation of $SL(2, 7)$. This group has a long and interesting history: almost 100 years ago Klein (10) studied \mathcal{G} in his investigation of the simple group $PSL(2, 7)$. In 1896 Maschke (12), continuing the work of Brioschi (3), gave an apparently complete description of the polynomial invariants of \mathcal{G} and of the syzygies relating them. However, as we shall see, there are omissions in this work. The papers of Baker in 1935 (2) and Edge in 1947 (7) give a great deal of geometric information about the two groups, and other references to the vast literature on these groups can be found there.

Finally, in 1972 (11) the group \mathcal{G} has arisen in studying error-correcting codes. In order to extend a theorem of Gleason (8) to self-dual codes over GF(7), the invariants of \mathcal{G} are required.

The main result of this paper is a complete description of the invariants of \mathcal{G} , Theorem 1, filling in the omissions in Maschke's work.

In order to do this, we use a result of Molien (13) giving a generating function (sometimes called the Poincaré series (1)) for the number of invariants of a given degree. In all the groups we have considered there is a particularly simple relationship between the form of the Poincaré series and the degrees of the basic invariants, and we conjecture that this relationship holds for any finite group (section 2). A weaker version of this conjecture has been established by Professor E. C. Dade (6), and we give his results in section 4.

2. *Invariants.* Let G be any finite group of $n \times n$ matrices over the complex numbers C , and let $R = C[x_1, \dots, x_n]$. An invariant of G is a polynomial $f \in R$ which is unchanged by the action of G , i.e. satisfies

$$f\left(\sum_{i=1}^n a_{1i}x_i, \dots, \sum_{i=1}^n a_{ni}x_i\right) = f(x_1, \dots, x_n)$$

for all $A = (a_{ij}) \in G$. The set of all invariants of G forms a ring \mathcal{R} .

Let c_d be the number of linearly independent homogeneous invariants of degree d . In 1897 Molien showed that a generating function for c_d is given by

$$\Phi(\lambda) = \sum_{d=0}^{\infty} c_d \lambda^d = \frac{1}{|G|} \sum_{A \in G} \frac{1}{\det(I - \lambda A)}, \tag{1}$$

((13); (5), p. 300). This is sometimes called the Poincaré series for $G(1)$.

Our aim is to find n algebraically independent homogeneous invariants $\theta_1, \dots, \theta_n$, and a further set of $k \geq 1$ homogeneous invariants $\gamma_1 = 1, \gamma_2, \dots, \gamma_k$, such that the ring of invariants \mathcal{R} can be written as a direct sum

$$\mathcal{R} = \bigoplus_{i=1}^k S\gamma_i, \tag{2}$$

where $S = C[\theta_1, \dots, \theta_n]$.

Two consequences of equation (2) are as follows.

(a) Any homogeneous invariant f of degree d can be written in a *unique* way as

$$f = \sum c(a_1, \dots, a_n, r) \theta_1^{a_1} \dots \theta_n^{a_n} \gamma_r, \tag{3}$$

where the sum is over all (a_1, \dots, a_n, r) such that $a_i = 0, 1, \dots, r = 1, \dots, k$, and

$$a_1 \deg \theta_1 + \dots + a_n \deg \theta_n + \deg \gamma_r = d,$$

and the coefficients $c(a_1, \dots, a_n, r)$ are in C .

(b) There are $\frac{1}{2}k(k+1)$ syzygies expressing $\gamma_i \gamma_j$ for $1 \leq i, j \leq k$ in the form (3).

If d_i, b_i are the degrees of θ_i, γ_i , this implies that the number of linearly independent homogeneous invariants of degree d is the number of solutions of

$$a_1 d_1 + \dots + a_n d_n + b_r = d,$$

for which $a_i = 0, 1, 2, \dots$, and $r = 1, 2, \dots, k$; i.e. is the coefficient of λ^d in the expansion of

$$\frac{\sum_{r=1}^k \lambda^{b_r}}{\sum_{i=1}^n (1 - \lambda^{d_i})}, \tag{4}$$

which must therefore be $\Phi(\lambda)$. Thus the Poincaré series can be written down immediately from the degrees of the basic invariants.

We conjecture that the converse to the latter statement holds also:

Conjecture. Whenever the Poincaré series for G can be put† in the form of (4), then a matching set of basic invariants can be found, consisting of n algebraically independent homogeneous invariants $\theta_1, \dots, \theta_n$ of degrees d_1, \dots, d_n , and k homogeneous invariants $\gamma_1, \dots, \gamma_k$ of degrees b_1, \dots, b_k , such that (2) holds.

† By cancelling common factors and/or by multiplying numerator and denominator by the same polynomial.

The conjecture is known to be true for finite unitary groups generated by reflexions(14), and has been verified for a number of other groups. One special case, for the group \mathcal{G} , will be seen in the next section.

Professor E. C. Dade has communicated to us(6) a proof of a weaker version of this conjecture. His theorem, which we give in section 4, shows that the Poincaré series of any finite group *can* always be put into the form of (4), and a matching set of invariants found. But the question of whether this holds *whenever* the Poincaré series has the form of (4) remains open.

3. *Invariants of \mathcal{G} .* The Poincaré series (1) for \mathcal{G} was determined by Edge in (7); his expression may be rearranged to give

$$\Phi(\lambda) = \frac{1 + \lambda^8 + \lambda^{10} + \lambda^{12} + \lambda^{16} + \lambda^{18} + \lambda^{20} + \lambda^{28}}{(1 - \lambda^4)(1 - \lambda^6)(1 - \lambda^8)(1 - \lambda^{14})}, \tag{5}$$

which has the form of (4), and so, according to the conjecture, suggests the degrees of the basic invariants. We show that basic invariants can indeed be found with these degrees.

THEOREM 1. *\mathcal{G} has a set of 12 basic invariants, consisting of 4 algebraically independent invariants $\Phi_4, \Phi_6, \Gamma_8, \Phi_{14}$ of degrees 4, 6, 8, 14, and a further set of 8 invariants*

$$\gamma_1 = 1, \gamma_2, \dots, \gamma_8$$

of degrees 0, 8, 10, 12, 16, 18, 20, 28, such that the ring \mathcal{R} of invariants of \mathcal{G} is the direct sum

$$\mathcal{R} = \bigoplus_{i=1}^8 S\gamma_i, \tag{6}$$

where $S = C[\Phi_4, \Phi_6, \Gamma_8, \Phi_{14}]$. There are 36 syzygies expressing the products $\gamma_i\gamma_j$ in terms of the basic invariants in the form (3).

Proof. Maschke in (12) gave 7 invariants and 3 syzygies relating them. To complete his work it is necessary to choose the 12 basic invariants correctly in terms of his 7, and to find the 36 syzygies. Since the number of invariants of any degree d will then equal the coefficient of λ^d in (5), we will indeed have established (6).

The invariants are defined in terms of x_1 and the following functions of x_2, x_3, x_4 :

$$\begin{aligned} x_2x_3x_4 &= a, \\ x_2^2x_3 + x_3^2x_4 + x_4^2x_2 &= b, \\ x_2^2x_3^3 + x_3^2x_4^3 + x_4^2x_2^3 &= c, \\ x_2x_3^5 + x_3x_4^5 + x_4x_2^5 + a^2 &= d, \\ x_2^7 + x_3^7 + x_4^7 + 7ab &= e. \end{aligned}$$

The four algebraically independent basic invariants will be taken to be (in Maschke's notation):

$$\begin{aligned} \Phi_4 &= 2x_1^4 + 6ax_1 + b, \\ \Phi_6 &= 8x_1^6 - 20ax_1^3 - 10bx_1^2 - 10cx_1 - 14a^2 - d, \\ \Gamma_8 &= x_1^8 + 14ax_1^5 - 7bx_1^4 + 14cx_1^3 - 7dx_1^2 + ex_1, \end{aligned}$$

$$\begin{aligned}\Phi_{14} = & 48x_1^{14} + 168ax_1^{11} + 308bx_1^{10} - 1596cx_1^9 + 126(42a^2 + 11d)x_1^8 - 8(37e + 490ab)x_1^7 \\ & + 196(12ac + 5b^2)x_1^6 + 196(15ad - 13bc)x_1^5 + 14(182c^2 - 86ae - 7bd)x_1^4 \\ & + 28(11be - 42cd)x_1^3 + 14(21d^2 - 16ce)x_1^2 + 14dex_1 - e^2.\end{aligned}$$

(Maschke incorrectly gave the coefficient of $a^2x_1^8$ in Φ_{14} as 63.21 instead of 126.42.)
Then the other 8 basic invariants are:

$$\begin{aligned}\gamma_1 &= 1, \\ \gamma_2 &= x_1^3 - 2ax_1^5 + bx_1^4 + 2cx_1^3 + (6a^2 + d)x_1^2 + 2abx_1 + ac, \\ \gamma_3 &= -8x_1^{10} - 20ax_1^7 + 14bx_1^6 + 14cx_1^5 + 7(16a^2 - d)x_1^4 + (42ab - e)x_1^3 + 7(b^2 + 3ac)x_1^2 \\ &\quad + 7(7a^3 + bc)x_1 + ae, \\ \gamma_4 &= 26x_1^{12} + 202ax_1^9 - 33bx_1^8 + 120cx_1^7 + 14(13a^2 + d)x_1^6 + (378ab - 23e)x_1^5 \\ &\quad + 7(35ac - 2b^2)x_1^4 + 14(49a^3 - 10ad + 5bc)x_1^3 + 2a(10e + 49ab)x_1^2 \\ &\quad + (49a^2c + 49ab^2 - 7cd + 2be)x_1 + ce, \\ \gamma_5 &= \gamma_2^2, \quad \gamma_6 = \gamma_2\gamma_3, \quad \gamma_7 = \gamma_2\gamma_4 \quad \text{and} \quad \gamma_8 = \gamma_2^2\gamma_4.\end{aligned}$$

(Our $\gamma_2, \gamma_3, \gamma_4$ are Maschke's $\Phi_8, \Phi_{10}, \Phi_{12}$.)

There are 5 syzygies from which all the others can be obtained. The first three of these were given by Maschke, but the last two were not. The five are:

$$\begin{aligned}27\gamma_2^3 = & (-7\Phi_4^5 - 13\Phi_4^3\Gamma_8 - 7\Phi_4^2\Phi_6^2 + 2\Phi_4\Gamma_8^2 + \Phi_6^2\Gamma_8) + (-14\Phi_4^3 + 29\Phi_4\Gamma_8)\gamma_2 \\ & - 27\Phi_4\Phi_6\gamma_3 + (7\Phi_4^2 - \Gamma_8)\gamma_4 + 189\Phi_4\gamma_2^2 - 27\gamma_2\gamma_4,\end{aligned}\tag{7}$$

$$\gamma_3\gamma_4 = \Phi_6\Gamma_8(\Gamma_8 - 7\Phi_4^2) - (7\Phi_6\Gamma_8 + \Phi_{14})\gamma_2 - 7\Phi_4\Gamma_8\gamma_3,\tag{8}$$

$$\begin{aligned}\gamma_4^2 = & (\Phi_4\Phi_6\Phi_{14} + 7\Phi_4\Gamma_8(\Phi_4^3 + \Phi_6^2) + 13\Phi_4^2\Gamma_8^2 - \Gamma_8^3) + (210\Phi_4^2\Gamma_8 - 22\Gamma_8^2)\gamma_2 \\ & + (6\Phi_6\Gamma_8 + \Phi_{14})\gamma_3 - 6\Phi_4\Gamma_8\gamma_4 + 7\Gamma_8\gamma_2^2 - 7\Phi_4\gamma_3^2,\end{aligned}\tag{9}$$

$$\begin{aligned}5103\gamma_2^3 = & -(49\Phi_4^5 + 91\Phi_4^4\Gamma_8 + 49\Phi_4^3\Phi_6^2 - 41\Phi_4^2\Gamma_8^2 + \Phi_4\Phi_6(27\Phi_{14} + 722\Phi_6\Gamma_8) - 27\Gamma_8^3) \\ & + (91\Phi_4^4 - 3982\Phi_4^2\Gamma_8 + 189\Phi_4\Phi_6^2 + 1323\Gamma_8^2)\gamma_2 \\ & - 27(7\Phi_4^2\Phi_6 + \Phi_{14} + 33\Phi_6\Gamma_8)\gamma_3 + (76\Phi_4^3 + 20\Phi_4\Gamma_8 + 27\Phi_6^2)\gamma_4 \\ & + 27(63\Phi_4^2 + 587\Gamma_8)\gamma_2^2 + 729\Phi_6\gamma_2\gamma_3 - 324\Phi_4\gamma_2\gamma_4,\end{aligned}\tag{10}$$

$$\begin{aligned}189\gamma_2^2\gamma_3 = & -(7\Phi_4^5\Phi_6 + \Phi_4^3(\Phi_{14} - 29\Phi_6\Gamma_8) + 7\Phi_4^2\Phi_6^3 + 2\Phi_4\Gamma_8(\Phi_{14} + 23\Phi_6\Gamma_8) \\ & + \Phi_6^2(\Phi_{14} + 6\Phi_6\Gamma_8)) - (14\Phi_4^2\Phi_6 - 5\Phi_{14} + 125\Phi_6\Gamma_8)\Phi_4\gamma_2 \\ & + (7\Phi_4^4 + 90\Phi_4^2\Gamma_8 - 20\Phi_4\Phi_6^2 + 27\Gamma_8^2)\gamma_3 + (7\Phi_4^2\Phi_6 + \Phi_{14} + 33\Phi_6\Gamma_8)\gamma_4 \\ & + 189\Phi_4\Phi_6\gamma_2^2 + (14\Phi_4^2 + 594\Gamma_8)\gamma_2\gamma_3 - 27\Phi_6\gamma_2\gamma_4.\end{aligned}\tag{11}$$

We verified (7)–(9) and found (10), (11) with the help of the ALTRAN computer program for manipulating rational functions (4), (9).

The 36 syzygies can now be found from equations (7)–(11). Of course $\gamma_1\gamma_i = \gamma_i$ for all i . The first few of the others, arranged by increasing degree, are:

$$\begin{aligned} \gamma_2^2 &= \gamma_5, & \gamma_2\gamma_3 &= \gamma_6, & \gamma_2\gamma_4 &= \gamma_7, \\ \gamma_3^2 &: \text{eqn. (7)}, & \gamma_3\gamma_4 &: \text{eqn. (8)}, \\ \gamma_2\gamma_5 &= \gamma_2^3: \text{eqn. (10)}, & \gamma_4^2 &: \text{eqns (9), (7)}, \\ \gamma_2\gamma_6 &= \gamma_2^2\gamma_3 = \gamma_3\gamma_5: \text{eqn. (11)}, \\ \gamma_2\gamma_7 &= \gamma_2^2\gamma_4 = \gamma_8, \end{aligned}$$

$\gamma_3\gamma_6 = \gamma_2\gamma_3^2$: this is expressed by equation (7) in terms of $\gamma_2^2, \gamma_2\gamma_3, \gamma_2\gamma_4, \gamma_3^2, \gamma_2^2\gamma_4$, which have already appeared on this list, and so on. We leave to the reader the easy verification that all 36 syzygies can be obtained in this way. This completes the proof.

4. *Decomposition of the ring of invariants.* In this section we state Dade’s theorems on the decomposition of the ring of invariants \mathcal{R} of a finite group G of $n \times n$ matrices over C .

THEOREM 2. (E. C. Dade (6).) *Suppose $\{\theta_1, \dots, \theta_n\}$ is a set of n homogeneous polynomials in $R = C[x_1, \dots, x_n]$, algebraically independent over C . Let $S = C[\theta_1, \dots, \theta_n]$ and suppose R is integral over the subalgebra S . Then there exist homogeneous $\eta_1, \dots, \eta_k \in R$ such that*

$$R = \bigoplus_{i=1}^k S\eta_i.$$

COROLLARY. *There exists an integer l , a set of n homogeneous, algebraically independent invariants $\{\theta_1, \dots, \theta_n\} \subset \mathcal{R}$, of degree l , and a set of homogeneous invariants $\{\gamma_1, \dots, \gamma_k\} \subset \mathcal{R}$, such that*

$$\mathcal{R} = \bigoplus_{i=1}^k S\gamma_i,$$

where $S = C[\theta_1, \dots, \theta_n]$. The Poincaré series for G is

$$\Phi(\lambda) = \frac{\sum_{i=1}^k \lambda^{\deg \gamma_i}}{(1 - \lambda^l)^n}.$$

Notice that this result does not provide a complete resolution of our conjecture, the status of which is still unclear.

We should like to thank W. L. Edge for his helpful comments on the first version of this paper, E. C. Dade for supplying a proof of Theorem 2 and its corollary, and R. P. Kurshan for many fruitful discussions.

REFERENCES

- (1) ATIYAH, M. F. and MACDONALD, I. G. *Introduction to commutative algebra* (Reading, Massachusetts, Addison-Wesley, 1969), p. 116.
- (2) BAKER, H. F. Note introductory of the study of Klein's group of order 168. *Proc. Cambridge Philos. Soc.* **31**, (1935), 468–481.
- (3) BRIOSCHI, F. Über die Jacobi'sche Modulargleichung vom achten Grade. *Math. Ann.* **15** (1879), 241–250.
- (4) BROWN, W. S. *ALTRAN user's manual* (Bell Laboratories, Murray Hill, New Jersey, 1971).
- (5) BURNSIDE, W. *Theory of groups of finite order*, 2nd ed. (1911), republished by Dover Publications, New York, 1955.
- (6) DADE, E. C. Written communication, 23 April 1972.
- (7) EDGE, W. L. The Klein group in three dimensions. *Acta Math.* **79** (1947), 153–223.
- (8) GLEASON, A. M. Weight polynomials of self-dual codes and the MacWilliams identities. *Actes, Congrès intern. Math.*, 1970 (Gauthier-Villars, 1971), tome 3, pp. 211–215.
- (9) HALL, A. D. JR. The ALTRAN system for rational function manipulation – A survey. *Comm. ACM* **14** (1971), 517–521.
- (10) KLEIN, F. Über die Auflösung gewisser Gleichungen vom seibenten und achten Grade. *Math. Ann.* **15** (1879), 25–82.
- (11) MACWILLIAMS, F. J., MALLOWS, C. L. and SLOANE, N. J. A. Generalizations of Gleason's theorem on weight enumerators of self-dual codes. *IEEE Trans. Information Theory* **IT-18** (1972), 794–805.
- (12) MASCHKE, H. The invariants of a group of 2.168 linear quaternary substitutions. *International Mathematical Congress 1893* (New York, Macmillan, 1896), pp. 175–186.
- (13) MOLIEN, T. Über die Invarianten der linearen Substitutions-gruppen. *Sitz. König. Preuss. Akad. Wiss.* (1897), 1152–1156.
- (14) SHEPHARD, G. C. and TODD, J. A. Finite unitary reflection groups. *Canad. J. Math.* **6** (1954), 274–304.