PUBLICATIONS MATHÉMATIQUES DE L'I.H.É.S.

LEONARD CHASTKOFSKY
WALTER FEIT

On the projective characters in characteristic 2 of the groups $Suz(2^m)$ and $Sp_4(2^n)$

Publications mathématiques de l'I.H.É.S., tome 51 (1980), p. 9-35
<http://www.numdam.org/item?id=PMIHES_1980__51__9_0>

© Publications mathématiques de l'I.H.É.S., 1980, tous droits réservés.

L'accès aux archives de la revue « Publications mathématiques de l'I.H.É.S. » (http://www.ihes.fr/IHES/Publications/Publications.html) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

ON THE PROJECTIVE CHARACTERS IN CHARACTERISTIC 2 OF THE GROUPS $\mathrm{Suz}(2^m)$ AND $\mathrm{Sp}_4(2^n)$

by LEONARD CHASTKOFSKY (1) *and* WALTER FEIT (1)

1. Introduction.

The purpose of this paper is to obtain an explicit formula for the first Cartan invariant in characteristic 2 of the groups $\mathrm{Suz}(2^m)$ and $\mathrm{Sp}_4(2^n)$. Formulas for the degrees of the projective indecomposable characters for these groups are also obtained.

We need to introduce some notation before stating some of these results. This notation will be used throughout the paper.

$$G = G_m = \begin{cases} \mathrm{Sp}_4(2^{m/2}) & \text{if } m \text{ is even} \\ \mathrm{Suz}(2^m) & \text{if } m \text{ is odd.} \end{cases}$$

$$q = q_m = \begin{cases} 2^{m/2} & \text{if } m \text{ is even} \\ 2^m & \text{if } m \text{ is odd.} \end{cases}$$

Thus $G_m = \mathrm{Sp}_4(q)$ or $\mathrm{Suz}(q)$ according to whether m is even or odd. The S_2-group of G_m has order 2^{2m} in either case.

We write $\varphi_\varnothing = \varphi_\varnothing^{(m)}$ for the trivial irreducible Brauer character for the prime $p = 2$ of G_m, $\Phi_\varnothing = \Phi_\varnothing^{(m)}$ for the corresponding projective indecomposable character and $c_{\varnothing\varnothing} = c_{\varnothing\varnothing}^{(m)}$ for the corresponding Cartan invariant.

Define

$$T_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Then T_n is the n-th Lucas number and

$$T_{n+2} = T_{n+1} + T_n \quad \text{for} \quad n \geq 0.$$

Let $\quad U_n = \alpha^n + \beta^n + \gamma^n, \quad$ where $\quad (x-\alpha)(x-\beta)(x-\gamma) = x^3 - 3x^2 - x + 5.$

(1) The first author was supported by the Canada Council and the second author was partially supported by NSF contract GP-33591. Both authors with to express their thanks to the I.H.E.S. for their hospitality during the spring of 1977 when part of this work was done.

Then $$U_{n+3}=3U_{n+2}+U_{n+1}-5U_n \quad \text{for} \quad n\geq 0,$$
$$U_0=3, \quad U_1=3, \quad U_2=11.$$

Theorem A.

$$\Phi_{\varnothing}^{(m)}(1)=2^{2m}(2^{2m}-T_m 2^m+(-1)^m).$$

A proof of Theorem A is given in Section 6. It is a simple consequence of Theorem (6.3). As an immediate consequence of Theorem A one gets

Corollary A.

$$\Phi_{\varnothing}^{(2m)}(1)=2^{2m}(2^{2m}+T_m 2^m+(-1)^m)\Phi_{\varnothing}^{(m)}(1).$$

The formula in Corollary A is somehow related to the fact that G_m is the twisted form of G_{2m}. It would of course be very desirable to find a more conceptual proof of this result which explains this relationship between $\Phi_{\varnothing}^{(m)}$ and $\Phi_{\varnothing}^{(2m)}$.

Section 7 contains formulas for the degrees of the other projective indecomposable characters of G_m.

Theorem B.

$$c_{\varnothing\varnothing}^{(m)}=2^{3m}+2^{2m}+2^m+(-1)^m 2^{m+1}+2^m U_m-2^{m+1}(2^m+1)T_m.$$

The following consequence of Theorem B is easily verified.

Corollary B.

If $m\geq 3$ then $c_{\varnothing\varnothing}^{(m)}>2^{2m}$. Furthermore

$$\lim_{m\to\infty}\frac{c_{\varnothing\varnothing}^{(m)}}{2^{3m}}=1.$$

The proof of Theorem B is much more difficult than the proof of Theorem A. The nature of the expression for $c_{\varnothing\varnothing}^{(m)}$, in particular the existence of a term which involves U_m, would seem to indicate that one should not expect to find a proof which does not involve a cubic recursion.

The appearance of the polynomial $f(x)=x^3-3x^2-x+5$ in connection with Theorem B is rather mysterious. The discriminant of $f(x)$ is 148 and the roots of $f(x)$ are approximately 2.6753, 1.5392, −1.2145. [*Added in proof.* — J.-P. Serre has pointed out that 148 is the smallest discriminant of a totally real number field with S_3 as a Galois group!]

The results of Section 6 show that in some sense the following statement is true. As the structure of the irreducible Brauer character gets more complicated so the structure of the corresponding indecomposable character gets simpler. For instance the Steinberg character is the most complicated irreducible Brauer character and the simplest projective character. Thus in Theorems A and B we are studying the most complicated projective indecomposable character $\Phi_{\varnothing}$. As an example of this phenomenon we show in Section 6 that certain Cartan invariants are easily computed.

The degrees of the indecomposable projective characters in characteristic p of $SL_2(p^n)$ were found by Srinivasan [7]. The work of Jeyakumar [5] and Humphreys [4] makes it possible to get a great deal of information about the structure of projective modules for $SL_2(p^n)$, and in particular to get information about the Cartan matrix for these groups. In [1], Alperin gave a complete description of the Cartan matrix for $SL_2(2^n)$. Aside from the groups $SL_2(p^n)$, very little information is known about the projective characters of finite groups of Lie type. The results in this paper are apparently the first in which $\Phi_{\emptyset}(1)$ or $c_{\emptyset\emptyset}$ has been computed for an infinite number of groups of Lie type other than $SL_2(p^n)$.

In [6] Landrock computed the Cartan matrix for the prime $p=2$ of G_3, the smallest Suzuki group. He noticed in particular that $c_{\emptyset\emptyset}^{(3)}=160>|G_3|_2=64$. This result contradicts an old conjecture of Brauer which asserted that the Cartan invariants of a group are bounded by the order of a Sylow subgroup. It is clear from Corollary B that Landrock's result is not an accident. In fact the conjecture was off by an order of magnitude.

Motivated partly by trying to understand Landrock's result, the second author suggested to the first author early in 1976 that he study the projective characters of the Suzuki groups for the prime $p=2$. Later during that year the first author succeeded in proving Theorems A and B in case m is odd, i.e. in case G_m is a Suzuki group. The argument used was similar to the one in this paper, though the graph used was more complicated than the one introduced in Section 3. Shortly thereafter the first author realized that a similar (even simpler) argument should apply to the symplectic groups G_{2n}. In fact it turned out that the simpler argument applied in all cases. Furthermore by treating the groups G_m for m even and m odd simultaneously, various parts of the argument were further simplified, and the induction on m needed in the proof of Theorem B was made considerably less cumbersome. It is this work which is the content of the present paper.

Analogous arguments can be used to study projective characters of the groups $SL_3(2^m)$ and $SU_3(2^m)$. In a forthcoming paper we will prove a result analogous to Theorem A for these groups and also derive some information concerning the first Cartan invariant $c_{\emptyset\emptyset}$.

2. Notation.

We write $\mathbf{F}_q$ for the field of cardinality q, $\mathbf{K}$ for the algebraic closure of $\mathbf{F}_q$, σ for the Frobenius automorphism of $\mathbf{K}$ or $\mathbf{F}_q$. Thus if $a\in\mathbf{K}$ then $a^\sigma=a^2$.

Let $G=G_m$, $q=q_m$ have the same meaning as in the introduction. Let $G_\infty=Sp_4(\mathbf{K})$. Let σ also denote the automorphism of G_∞ or G_m induced by the Frobenius automorphism.

Let τ denote the graph automorphism of G_∞. See ([2], Section (12.3)) for a detailed description of this automorphism. Then $\tau^2=\sigma$ on G_∞. Furthermore

$G_{2n+1} = \mathrm{Suz}(2^{2n+1})$ is the subgroup of $G_{2(2n+1)} = \mathrm{Sp}_4(2^{2n+1})$ consisting of all elements fixed by τ^{2n+1}.

Let $G = G_\infty$ or G_m. If M is a $\mathbf{K}[G]$ module and θ is an automorphism of G, let M^θ denote the module obtained by letting $g \in G$ act on M^θ as g^θ acts on M. If G is finite and φ is the Brauer character afforded by M, let φ^θ denote the Brauer character afforded by M^θ.

Let $S = S_m = \mathbf{Z}/m\mathbf{Z}$. For each subset $I \subseteq S$, let $I' = S - I$ and let $|I|$ denote the cardinality of I. If m is even let $E = \{2, 4, 6, \ldots, m\} \subseteq S$.

1 or 1_H denotes the trivial character or Brauer character of any finite group H.

$\Gamma = \Gamma_m$ is the Steinberg character of G_m.

If α, β are complex valued class functions defined on the finite group H let

$$(\alpha, \beta) = (\alpha, \beta)_H = \frac{1}{|H|} \sum_{x \in H} \alpha(x) \overline{\beta(x)}.$$

Define $||\alpha||^2 = (\alpha, \alpha)$.

If θ is a Brauer character of G_m then (Γ, θ) is defined since Γ vanishes on all 2-singular elements of G_m.

If φ is an irreducible Brauer character of G_m then it is well known that

$$(\Gamma, \varphi) = 0 \quad \text{for} \quad \varphi \neq \Gamma, \qquad ||\Gamma||^2 = 1.$$

3. The Brauer Characters of G_m.

Lemma (3.1). — *Let* M *be the* 4*-dimensional* $\mathbf{K}[G_\infty]$ *module underlying the natural representation of* $G_\infty = \mathrm{Sp}_4(\mathbf{K})$. *Let* g *be a semi-simple element in* G_∞. *Then the characteristic values of* g *on* M *are* $\alpha, \alpha^{-1}, \beta, \beta^{-1}$ *for some* $\alpha, \beta \in \mathbf{K}$ *and the characteristic values of* g *on* M^τ *are* $\alpha\beta, (\alpha\beta)^{-1}, \alpha\beta^{-1}, \alpha^{-1}\beta$.

Proof. — Let a be a short root and b a long root in the root system B_2. The results of ([2], Chapter 11) imply that

$$x_a(t) = \begin{pmatrix} 1 & t & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -t \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad x_b(t) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & t & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Furthermore $x_{-a}(t)$, $x_{-b}(t)$ is the transpose of $x_a(t)$, $x_b(t)$ respectively.

By definition $n_a(t) = x_a(t)x_{-a}(-t^{-1})x_a(t)$ and $h_a(t) = n_a(t)n_a(-1)$. Similarly $n_b(t) = x_b(t)x_{-b}(-t^{-1})x_b(t)$ and $h_b(t) = n_b(t)n_b(-1)$. This yields that

$$h_a(t) = \begin{pmatrix} t & 0 & 0 & 0 \\ 0 & t^{-1} & 0 & 0 \\ 0 & 0 & t & 0 \\ 0 & 0 & 0 & t^{-1} \end{pmatrix}, \qquad h_b(t) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -t & 0 & 0 \\ 0 & 0 & -t^{-1} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

By ([2], (12.3.3))

$$\tau:\ h_a(t)\mapsto h_b(t^2)$$
$$h_b(t)\mapsto h_a(t).$$

Thus $\tau: h_a(t)h_b(u)\mapsto h_a(u)h_b(t^2)$. The result now follows by setting $\alpha=t$ and $\beta=t^{-1}u$.

Fix the integer m. Let $G=G_m$ and let φ denote the Brauer character of G afforded by the natural 4-dimensional $\mathbf{K}[G]$ module. For any integer i, let $\varphi_i=\varphi^{\tau^i}$. If m is odd, then $\varphi_m=\varphi_0=\varphi$ by definition. If m is even, then $\varphi_m=\varphi_0=\varphi$, since $\tau^2=\sigma$. Thus in any case we may define $\varphi_i=\varphi^{\tau^i}$ for $i\in S$.

For any subset $I\subseteq S$ define

$$\varphi_I=\prod_{i\in I}\varphi_i.$$

Theorem **(3.2)**. — *Let* $G=G_m$. *Then* $\{\varphi_I \mid I\subseteq S\}$ *is the set of all irreducible Brauer characters of* G. *Furthermore* $\varphi_\varnothing=1$ *and* $\varphi_S=\Gamma$ *in the Steinberg character of* G.

Proof. — In case m is odd and $G=\mathrm{Suz}(2^m)$ this is proved in ([8], section 12), since $\tau=\sigma^{(m+1)/2}$. Suppose that $m=2$ and $G=\mathrm{Sp}_4(2)\simeq S_6$ (the symmetric group on 6 letters). Then there are 4 semi-simple conjugate classes C_1, C_2, C_3, C_4 of orders 1, 3, 3, 5 respectively. The following table is easily computed by using Lemma (3.1).

	C_1	C_2	C_3	C_4
1	1	1	1	1
φ	4	-2	1	-1
φ^τ	4	1	-2	-1
$\varphi\varphi^\tau$	16	-2	-2	1

Thus $\varphi\varphi^\tau$ is the Steinberg character of G_2 and so is irreducible. The result now follows from the tensor product theorem. See [8].

Corollary **(3.3)**. — *Let* $G=G_m$. *Then every irreducible Brauer character of* G *is real valued.*

Proof. — Immediate from Lemma (3.1) and Theorem (3.2).

Theorem **(3.4)**. — *Let* $G=G_m$. *Let* $i\in S$. *Then*

$$\varphi_i^2=4+2\varphi_{i+1}+\varphi_{i+2}.$$

Proof. — This is a direct consequence of Lemma (3.1) since a Brauer character is determined by its values on semi-simple elements.

Let $G=G_m$. If $I\subseteq S$ let Φ_I denote the projective indecomposable character of G which corresponds to φ_I. Then $\varphi_S=\Phi_S=\Gamma$ and $(\Phi_I,\varphi_J)=\delta_{IJ}$ for $I, J\subseteq S$.

The next result will not be used directly in this paper but it indicates that the results in this section capture all the essential properties in some sense of the ring of Brauer characters of G_m.

Theorem **(3.5)**. — *Let* $G = G_m$ *and let* R(G) *denote the ring of Brauer characters of* G *(or equivalently the Grothendieck ring of* G*). Then* R(G) *is isomorphic to the commutative* **Z**-*algebra which is generated by elements* x_i, $i \in S$ *that satisfy*

$$x_i^2 = 4 + 2x_{i+1} + x_{i+2}.$$

Proof. — Let A denote the **Z**-algebra defined in the statement. By Theorem (3.4) there exists an epimorphism $f: A \to R(G)$. By Theorem (3.2) R(G) has rank 2^m as a **Z**-module. Since A is generated as a **Z**-module by the elements $\prod_{i \in I} x_i$ as I ranges over all subsets of S it follows that A has **Z**-rank at most 2^m. This implies that f is an isomorphism.

4. The Graph $\mathfrak{G}$.

Let $m \geq 2$. We associate a directed graph $\mathfrak{G} = \mathfrak{G}_m$ to the group $G = G_m$ as follows.

The vertices are labelled by the elements of S. There is an edge from i to j if and only if $j = i+1$ or $i+2$. An edge $i \to i+1$ is a *short edge*. An edge $i \to i+2$ is a *long edge*. By abuse of notation we will frequently identify S with the set of vertices of $\mathfrak{G}$.

Two vertices $i, j \in S$ are *adjacent* if $|i-j| = 1$.

By Theorem (3.4) there is an edge from i to j if and only if φ_j is a constituent of φ_i^2. This is the reason that the structure of $\mathfrak{G}$ is relevant to the study of the ring of Brauer characters of G.

The graph $\mathfrak{G}$ is most easily visualized by choosing m points on the unit circle and labelling them 1, 2, ..., m in a clockwise direction. The edges are then the arcs from i to $i+1$ and i to $i+2$ for $1 \leq i \leq m$. (Of course $m+i$ is identified with i.)

A *path* $\mathfrak{P}$ is a set of vertices $i_0, \ldots, i_k$ and edges $i_{j-1} \to i_j$ for $1 \leq j \leq k$ such that $i_s \neq i_t$ for $s \neq t$ except possibly for $\{s, t\} = \{0, k\}$. The set of all vertices in $\mathfrak{P}$ is the *support* of $\mathfrak{P}$.

The path $1 \to 2 \to \ldots \to m \to 1$ will be denoted by $\mathfrak{C}$.

A path $\mathfrak{P}$ is *closed* if $\mathfrak{P}$ contains at least one edge and for any ordered pair of distinct vertices i, j in $\mathfrak{P}$ there exists a path from i to j contained in $\mathfrak{P}$.

A subset I of S is *circular* if it is the union of pairwise disjoint subsets, each of which is the support of a closed path.

Lemma **(4.1)**. — *Let* $I \subseteq S$.

(i) I *is circular if and only if no two elements in* I′ *are adjacent.*

(ii) *If* $J \subseteq I$ *and* J *is circular then* I *is circular.*

(iii) *If* I *is circular then* $|\mathrm{I}|\geq m/2$.

(iv) *If* I *and* I′ *are both circular then* m *is even and* $\mathrm{I}=\mathrm{E}$ *or* E′.

Proof. — (i) Clear by definition.

(ii) and (iii) are immediate consequences of (i).

(iv) If I and I′ are both circular then, by (iii), $|\mathrm{I}|\geq m/2$ and $|\mathrm{I}'|\geq m/2$. Thus $|\mathrm{I}|=|\mathrm{I}'|=m/2$ and so m is even. The result now follows from (i).

Lemma **(4.2)**. — *Suppose that* $\mathfrak{P}$ *is a path whose support contains the vertices* i, $i+1$, $i+2$. *If* $i\rightarrow i+2$ *is an edge in* $\mathfrak{P}$ *then* m *is odd,* S *is the support of* $\mathfrak{P}$ *and* $\mathfrak{P}$ *is the path*

$$1\rightarrow 3\rightarrow 5\rightarrow \dots \rightarrow m-1\rightarrow 1.$$

Proof. — The edge $i+1\rightarrow i+3$ must be in $\mathfrak{P}$. Thus by induction it follows that for any j the edges $j\rightarrow j+2$ and $j+1\rightarrow j+3$ must be in $\mathfrak{P}$. Hence the support of $\mathfrak{P}$ is S and $\mathfrak{P}$ contains no short edges. Since $\mathfrak{P}$ is a path, m cannot be even and the result follows.

Lemma **(4.3)**. — *Suppose that* I *is circular and* $\mathrm{I}\neq\mathrm{S}$.

(i) I *is not the union of at least two pairwise disjoint subsets, each of which is the support of a closed path.*

(ii) *There is a unique path with support* I.

(iii) *The number of long edges in* $\mathfrak{P}$ *is* $|\mathrm{I}'|$.

Proof. — (i) Immediate by Lemma (4.1) (iii).

(ii), (iii). Let $0\leq i_0\leq\dots\leq i_k\leq m-1$, where $\mathrm{I}=\{i_t|0\leq t\leq k\}$. If $\mathfrak{P}$ is not the path $i_0\rightarrow i_1\rightarrow\dots\rightarrow i_k$ then there must exist vertices i, $i+1$, $i+2\in\mathrm{I}$ and an edge $i\rightarrow i+2$ contrary to Lemma (4.2). This proves (ii). Statement (iii) follows from the fact that the number of long edges in $\mathfrak{P}$ is clearly $|\mathrm{I}'|$, the number of elements not in I.

Lemma **(4.4)**. — (i) *Suppose that* m *is even. Then* S *is the support of the unique path* $\mathfrak{C}$. *Furthermore* $\mathrm{S}=\mathrm{E}\cup\mathrm{E}'$ *and* E, E′ *are each the support of a unique path, and this path has no short edges.*

(ii) *Suppose that* m *is odd. Then* S *is the support of* $\mathfrak{C}$ *and of the path*

$$1\rightarrow 3\rightarrow 5\rightarrow \dots \rightarrow m-1\rightarrow 1$$

and no others. Furthermore S *is not the union of two pairwise disjoint circular sets.*

Proof. — If S is the support of a path other than $\mathfrak{C}$ then there must be an edge $i\rightarrow i+2$ in this path. Hence by Lemma (4.2) m is odd and the other path is the required one. If S is the union of two pairwise disjoint circular sets then by Lemma (4.1) m is even and the result follows immediately.

Theorem **(4.5).** — *Let* $\varnothing \neq \mathrm{I} \subseteq \mathrm{S}$.

(i) φ_{I} *is a constituent of* φ_{I}^2 *if and only if* I *is circular.*

(ii) *If* I *is circular and* $\mathrm{I} \neq \mathrm{S}$ *then the multiplicity of* φ_{I} *as a constituent of* φ_{I}^2 *is* $2^m 4^{-|\mathrm{I}'|} = 2^{-m} 4^{|\mathrm{I}|}$.

(iii) *The multiplicity of* $\varphi_{\mathrm{S}} = \Gamma$ *as a constituent of* Γ^2 *is* $2^m + 1$.

Proof. — By Theorem (3.4) $\varphi_{\mathrm{I}}^2 = \prod_{i \in \mathrm{I}} (4 + 2\varphi_{i+1} + \varphi_{i+2})$. Let θ be a term in the expansion of φ_{I}^2. Then θ is an integer times a product of at most $|\mathrm{I}|$ characters φ_j. Thus if θ is a multiple of φ_{I}, then $\theta = 2^n \prod_{i \in \mathrm{I}} \varphi_{i+\varepsilon(i)}$, where $\varepsilon(i) = 1$ or 2 for each i and n is the number of values $i \in \mathrm{I}$ with $\varepsilon(i) = 1$. Since θ is a multiple of φ_{I} it also follows that $\{i + \varepsilon(i) \mid i \in \mathrm{I}\} = \mathrm{I}$. Hence $i \to i + \varepsilon(i)$ defines a disjoint union of closed paths with support I and n is the number of short edges in these paths. This in particular implies that (i) holds.

If $\mathrm{I} \neq \mathrm{S}$ then, by Lemma (4.3), there is a unique path $\mathfrak{P}$ with support I and the number of long edges is $|\mathrm{I}'|$. Thus the number of short edges is $|\mathrm{I}| - |\mathrm{I}'| = m - 2|\mathrm{I}'|$. This proves (ii).

If $\mathrm{I} = \mathrm{S}$. Then by Lemma (4.4) it follows that in any case there are two such terms θ and the multiplicity of φ_{S} in φ_{S}^2 is $2^m + 1$ as required to prove (iii).

5. Some Inner Products.

The following result is of basic importance for the rest of this paper.

Lemma **(5.1).** — *Let* I, J *be subsets of* S. *Then*

$$(\Gamma\varphi_{\mathrm{I}}, \varphi_{\mathrm{J}}) = (\Gamma, \varphi_{\mathrm{I}}\varphi_{\mathrm{J}}) = (\Gamma, \varphi_{\mathrm{I}\cup\mathrm{J}-\mathrm{I}\cap\mathrm{J}}\varphi_{\mathrm{I}\cap\mathrm{J}}^2).$$

Furthermore

$$\begin{aligned}
(\Gamma\varphi_{\mathrm{I}}, \varphi_{\mathrm{J}}) &= 0 && \textit{if } \mathrm{I}\cup\mathrm{J} \neq \mathrm{S}.\\
&= 1 && \textit{if } \mathrm{I}\cup\mathrm{J} = \mathrm{S},\ \mathrm{I}\cap\mathrm{J} = \varnothing, \text{ i.e. } \mathrm{J} = \mathrm{I}'.\\
&= 0 && \textit{if } \mathrm{I}\cup\mathrm{J} = \mathrm{S},\ \mathrm{I}\cap\mathrm{J} \neq \varnothing,\ \mathrm{I}\cap\mathrm{J} \textit{ is not circular.}\\
&= 2^m 4^{-|(\mathrm{I}\cap\mathrm{J})'|} && \textit{if } \mathrm{I}\cup\mathrm{J} = \mathrm{S},\ \mathrm{I}\cap\mathrm{J} \neq \mathrm{S},\ \mathrm{I}\cap\mathrm{J} \textit{ is circular.}\\
&= 2^m + 1 && \textit{if } \mathrm{I} = \mathrm{J} = \mathrm{S}.
\end{aligned}$$

Proof. — The first equation follows from Corollary (3.3). Thus we need only compute $(\Gamma, \varphi_{\mathrm{I}\cup\mathrm{J}-\mathrm{I}\cap\mathrm{J}}\varphi_{\mathrm{I}\cap\mathrm{J}}^2)$.

Suppose that $\mathrm{I}\cap\mathrm{J} = \varnothing$. Then $(\Gamma, \varphi_{\mathrm{I}\cup\mathrm{J}}) = \delta_{\mathrm{S},\mathrm{I}\cup\mathrm{J}}$ and the result is proved.

Suppose that $\mathrm{I}\cap\mathrm{J} \neq \varnothing$. By Theorem (3.4) $\varphi_{\mathrm{I}\cap\mathrm{J}}^2 = \prod_{i \in \mathrm{I}\cap\mathrm{J}} (4 + 2\varphi_{i+1} + \varphi_{i+2})$. Let θ be a term in the expansion of $\varphi_{\mathrm{I}\cap\mathrm{J}}^2$ such that $(\Gamma, \varphi_{\mathrm{I}\cup\mathrm{J}-\mathrm{I}\cap\mathrm{J}}\theta) \neq 0$. Then θ is an integer times a product of k characters φ_j with $k \leq |\mathrm{I}\cap\mathrm{J}|$. By the choice of θ it follows that $k + |\mathrm{I}\cup\mathrm{J} - \mathrm{I}\cap\mathrm{J}| = m$. Hence $|\mathrm{I}\cup\mathrm{J}| = m$ and $|\mathrm{I}\cap\mathrm{J}| = k$. Thus in particular $\mathrm{I}\cup\mathrm{J} = \mathrm{S}$.

Hence θ is a multiple of $\varphi_{I\cap J}$. Furthermore $(\Gamma, \varphi_{I\cup J-I\cap J}\varphi^2_{I\cap J})$ is equal to the multiplicity of $\varphi_{I\cap J}$ as a constituent of $\varphi^2_{I\cap J}$. The result now follows from Theorem (4.5).

Corollary **(5.2).** — *Let* $I \subseteq S$. *Then*

$$\begin{aligned}(\Gamma^2, \varphi_I) &= 1 && \text{if } I = \emptyset.\\ &= 0 && \text{if } I \neq \emptyset,\ I \text{ is not circular.}\\ &= 2^m 4^{-|I'|} && \text{if } I \neq S,\ I \text{ is circular.}\\ &= 2^m + 1 && \text{if } I = S.\end{aligned}$$

Proof. — Let $J = S$ in Lemma (5.1).

Corollary **(5.3).** — *Suppose that m is even. Then*

$$(\Gamma^2, \varphi_E) = (\Gamma^2, \varphi_{E'}) = 1.$$

Proof. — Let $I = E$ or E' in Corollary (5.2).

6. Projective Indecomposable Characters.

Lemma **(6.1).** — *Let* $K \subseteq S$. *Then*

$$\Phi_K = \Gamma\varphi_{K'} - \sum_{\substack{K \subseteq J \\ J-K \text{ circular}}} (\Gamma^2, \varphi_{J-K})\Phi_J.$$

Proof. — Since $\Gamma\varphi_{K'}$ is a projective character it follows from the orthogonality relations that $\Gamma\varphi_{K'} = \sum_J (\Gamma\varphi_{K'}, \varphi_J)\Phi_J$. If $(\Gamma\varphi_{K'}, \varphi_J) \neq 0$ then $K' \cup J = S$ by Lemma (5.1) and so $K \subseteq J$. Furthermore

$$(\Gamma\varphi_{K'}, \varphi_J) = (\Gamma, \varphi_{K'}\varphi_J) = (\Gamma, \varphi_{K'\cup J}\varphi_{K'\cap J}) = (\Gamma, \Gamma\varphi_{K'}\varphi_J) = (\Gamma^2, \varphi_{J-K}).$$

Thus by Lemma (5.1)

$$\Gamma\varphi_{K'} = \sum_{K\subseteq J} (\Gamma^2, \varphi_{J-K})\Phi_J = \Phi_K + \sum_{K \subsetneqq J} (\Gamma^2, \varphi_{J-K})\Phi_J.$$

By Lemma (5.1) $(\Gamma^2, \varphi_{J-K}) = 0$ unless $J-K$ is circular.

Lemma **(6.2).** — *Suppose that* J *is circular. Then* $\Phi_J = \Gamma\varphi_{J'}$ *except when m is even and* $J = E$ *or* E'. *In the latter case* $\Phi_J = \Gamma\varphi_{J'} - \Gamma$.

Proof. — If J' is not circular then Lemma (4.1) (ii) implies that $I-J$ is not circular for any set I with $J \subseteq I \subseteq S$. Thus $(\Gamma^2, \varphi_{I-J}) = 0$ by Lemma (5.1) for $J \subsetneqq I \subseteq S$. Hence $\Phi_J = \Gamma\varphi_{J'}$ by Lemma (6.1).

Suppose that J' is circular. Then m is even and $J = E$ or E'. If $J \subseteq I \subseteq S$ and $I-J$ is circular then $I = S$. Hence by Lemma (5.1) $(\Gamma^2, \varphi_{I-J}) = 0$ for $J \subsetneqq I \subsetneqq S$. By Corollary (5.3) $(\Gamma^2, \varphi_{S-J}) = 1$. The result follows from Lemma (6.1).

Theorem **(6.3)**. — *Let* $K \subseteq S$.

(i) *If* m *is odd or* $K \neq \emptyset$ *then*

$$\Phi_K = \Gamma\varphi_{K'} - \sum_{\substack{K \subseteq J \\ J-K \text{ circular}}} (\Gamma^2, \varphi_{J-K})\Gamma\varphi_{J'}.$$

(ii) *If* m *is even then*

$$\Phi_\emptyset = \Gamma^2 - \sum_{J \text{ circular}} (\Gamma^2, \varphi_J)\Gamma\varphi_{J'} + 2\Gamma.$$

Proof. — If $J-K$ is circular then J is circular by Lemma (4.1) (ii). Thus Lemma (6.2) implies that either $\Gamma\varphi_{J'} = \Phi_J$ or m is even $J = E$ or E' and $\Phi_J = \Gamma\varphi_{J'} - \Gamma$. If $J = E$ or E' and $J - K$ is circular then $K = \emptyset$ by Lemma (4.1) (iii) and $(\Gamma^2, \varphi_J) = 1$ by Corollary (5.3). The result now follows from Lemma (6.1).

It is now easy to prove Theorem A.

Proof of Theorem A. — By Theorem (6.3) and Corollary (5.2)

$$\Phi_\emptyset = \Gamma^2 - \sum_{J \text{ circular}} 2^m 4^{-|J'|}\Gamma\varphi_{J'} + (-1)^m\Gamma.$$

Since $\varphi_{J'}(1) = 4^{|J'|}$ it follows that

$$\Phi_\emptyset(1) = \Gamma(1)(2^{2m} - 2^m \sum_{J \text{ circular}} 1 + (-1)^m).$$

By the Corollary in the Appendix the number of circular subsets of S is T_m. This completes the proof.

The next result shows, as mentioned in the introduction, that certain Cartan invariants are easily computed.

Theorem **(6.4)**. — *Suppose that* $m > 2$. *Let* $i, j \in S$. *Then* $c_{\{i\}', \{j\}'} = 4\delta_{ij}$.

Proof. — Since $\{i\}'$ and $\{j\}'$ are both circular it follows from Lemma (6.2) that $\Phi_{\{i\}'} = \Gamma\varphi_i$ and $\Phi_{\{j\}'} = \Gamma\varphi_j$. Thus if $i \neq j$ then Lemma (5.1) implies that

$$c_{\{i\}', \{j\}'} = (\Gamma\varphi_i, \Gamma\varphi_j) = (\Gamma^2, \varphi_i\varphi_j) = 0.$$

Since $\varphi_i^2 = 4 + 2\varphi_{i+1} + \varphi_{i+2}$ it follows from Lemma (5.1) that

$$c_{\{i\}', \{i\}'} = (\Gamma\varphi_i, \Gamma\varphi_i) = (\Gamma^2, \varphi_i^2) = (\Gamma^2, 4 + 2\varphi_{i+1} + \varphi_{i+2}) = 4.$$

7. Degrees of Projective Indecomposable Characters.

In this section we will compute $\Phi_K(1)$ for $\emptyset \neq K \subseteq S$.

If $I \subseteq S$ then a *component* of I is a nonempty subset A of I which is the support of a path with only short edges and is maximal with respect to this property. Thus if $|I'| \leq 1$ then I is the only component of I. If $i, j \in I'$, $i, i+1 \neq j$ and if

$$A = \{i + s \mid s = 1, \ldots, (j-i) - 1\} \subseteq I,$$

then A is a component of I; and conversely, if $|I'| > 1$, every component is of this form. Clearly no two distinct components of I intersect and I is the union of its components.

Let K be a nonempty set in S and let $|K|=k>0$. Then $K=\{i_1, \ldots, i_k\}$ with $0\leq i_1<\ldots<i_k\leq m-1$. For $1\leq s\leq k$ let

$$A_s=\{j\,|\,i_s<j<i_{s+1}\}, \quad 1\leq s\leq k-1$$
$$A_k=\{j\,|\,0\leq j<i_1 \text{ or } i_k<j\leq m-1\}.$$

Thus the nonempty sets A_s are the components of K'. Let $a_s=|A_s|$ for all s. Then

$$|K'|=m-k=a_1+\ldots+a_k.$$

The set $\{a_1, \ldots, a_k\}$ is called the *type* of K.

Lemma **(7.1)**. — *Let* K *be a set of type* $\{a_1, \ldots, a_k\}$. *Then* K' *is circular if and only if* $a_s\neq 0$ *for all* s.

Proof. — By Lemma (4.1) (i), K' is not circular if and only if K contains a pair of adjacent elements. This is clearly the case if and only if $a_s=0$ for some s.

Define

$$F_n=\frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

Thus F_n is the n-th Fibonacci number. Observe in particular that $F_0=0$.

Theorem **(7.2)**. — *Let* $\emptyset\neq K\subseteq S$. *Let* $\{a_1, \ldots, a_k\}$ *be the type of* K. *Then*

$$\Phi_K(1)=2^{3m-2k}\left(2^m-\prod_{s=1}^{k}F_{a_s}\right).$$

Proof. — Let X be the set of all sets J with $K\subseteq J\subseteq S$ and $J-K$ circular. If $J\in X$ then Corollary (5.2) implies that

$$(\Gamma^2, \varphi_{J-K})=2^m 4^{-|(J-K)'|}=2^m 4^{-(m-|J|+k)}=2^{m-2k}4^{-m+|J|}.$$

Thus, by Theorem (6.3),

$$\Phi_K(1)=\Gamma(1)\left(4^{m-k}-2^{m-2k}\sum_{J\in X}4^{-m+|J|}4^{m-|J|}\right)$$
$$=2^{2m}(2^{2m-2k}-2^{m-2k}|X|)=2^{3m-2k}(2^m-|X|).$$

Thus it suffices to show that $|X|=\prod_{s=1}^{k}F_{a_s}$.

If K' is not circular then by Lemma (4.1) (ii) $X=\emptyset$ and so $|X|=0$. By Lemma (7.1) $a_s=0$ for some s and so $\prod_{s=1}^{k}F_{a_s}=0$. The result holds in this case.

Suppose that K' is circular. Let $K=\{i_1, \ldots, i_k\}$ with $0\leq i_1<\ldots<i_k\leq m-1$. Let A_s be defined as above and choose the notation so that $a_s=|A_s|$ for each s. A set J is in X if and only if J satisfies the following two conditions:

(i) J contains the end points i_s+1, $i_{s+1}-1$ of A_s for each s.

(ii) J does not omit adjacent points of any set A_s.

By the Corollary in the Appendix the number of such subsets of A_s is F_{a_s}. Thus $|X| = \prod_{s=1}^{k} F_{a_s}$ as required.

Corollary **(7.3)**. — *If* $m \geq 4$ *there exist subsets* I, J *of* S *such that* $\varphi_I(1) = \varphi_J(1)$ *but* $\Phi_I(1) \neq \Phi_J(1)$.

Proof. — As an example let $I = \{1, 2\}$ and $J = \{1, 3\}$. Then $\varphi_I(1) = \varphi_J(1) = 4^2$. Since I is of type $\{0, m-2\}$ and J is of type $\{1, m-3\}$ it follows from Theorem (7.2) that $\Phi_I(1) = 2^{4m-4}$ and

$$\Phi_J(1) = 2^{4m-4} - 2^{3m-4} F_{m-3} < \Phi_I(1).$$

8. Some More Inner Products

This section contains the computations of some inner products which are needed for the proof of Theorem B.

Lemma **(8.1)**. — *Suppose that* $G = \mathrm{Suz}(q)$. *If* θ *is a class function on the set of all* $2'$*-elements of* G *then*

$$(\Gamma^3, \theta) = (\Gamma, \theta) + (q+1)\theta(1).$$

Proof. — If x is a $2'$-element in G, $x \neq 1$ then $\Gamma(x) = \pm 1$. See for instance [9] or [10]. Thus $(\Gamma^3 - \Gamma)(x) = 0$ for $x \in G$, $x \neq 1$. Therefore

$$(\Gamma^3 - \Gamma, \theta) = \frac{1}{|G|}\{\Gamma^3(1) - \Gamma(1)\}\theta(1) = \frac{(q^6 - q^2)\theta(1)}{(q^2+1)q^2(q-1)} = (q+1)\theta(1)$$

as required.

Throughout the rest of this section $G = \mathrm{Sp}_4(q)$ and the following notation is used.

H is a cyclic subgroup of G of order $q^2 - 1$. Thus every cyclic subgroup of G of order $q^2 - 1$ is conjugate to exactly one of the groups H, H^τ. See [3].

H^+ is the subgroup of H of order $q+1$.

H^- is the subgroup of H of order $q-1$.

Lemma **(8.2)**

$$\begin{aligned} \Gamma(x) &= -q \quad \textit{if} \quad x \in H^+ - \{1\} \\ &= q \quad \textit{if} \quad x \in H^- - \{1\} \\ &= -1 \quad \textit{if} \quad x \in H - H^+ \cup H^-. \end{aligned}$$

Proof. — See [3].

Lemma **(8.3)**. — $1_H^G + 1_{H^\tau}^G = 2(\Gamma^2 - \Gamma)$.

Proof. — See [3].

Lemma **(8.4)**. — *There exist linear characters* η, ζ *on* H^+, H^- *respectively such that if* $\varphi=\varphi_1$ *then*

$$\varphi_{H^+}=2+\eta+\eta^{-1},\qquad \varphi_{H^+\tau}=2(\eta+\eta^{-1}).$$
$$\varphi_{H^-}=2+\zeta+\zeta^{-1},\qquad \varphi_{H^-\tau}=2(\zeta+\zeta^{-1}).$$

Proof. — See [3].

Lemma **(8.5)**. — *Suppose that* $I\subseteq S$ *and* I' *is circular. Then*

$$(1_{H^-},(\varphi_I)_{H^-})=(1_{H^+},(\varphi_I)_{H^+})\quad \textit{if}\quad I\neq E \textit{ or } E'$$
$$(1_{H^-},(\varphi_E+\varphi_{E'})_{H^-})=(1_{H^+},(\varphi_E+\varphi_{E'})_{H^+})+2(q+1).$$

Proof. — By Lemma (8.4)

$$(\varphi_I)_{H^-}=\prod_{i\in E\cap I}2(\zeta^{2^i}+\zeta^{-2^i})\prod_{i\in E'\cap I}(2+\zeta^{2^i}+\zeta^{-2^i}),$$
$$(\varphi_I)_{H^+}=\prod_{i\in E\cap I}2(\eta^{2^i}+\eta^{-2^i})\prod_{i\in E'\cap I}(2+\eta^{2^i}+\eta^{-2^i}).$$

Since $0\leq i\leq m-1$ it follows that $\sum_i\pm 2^i\not\equiv 0 \pmod{q+1}$ and $\sum_i\pm 2^i\equiv 0 \pmod{q-1}$ can only hold for $\pm(1+2+\ldots 2^{m-1})=\pm(q-1)$. Hence $(1_{H^+},(\varphi_I)_{H^+})=2^{|I\cap E'|}$ and if $I\neq E$ or E', then $(1_{H^-},(\varphi_I)_{H^-})=2^{|I\cap E'|}$. Furthermore $(1_{H^-},(\varphi_E)_{H^-})=2q$ and $(1_{H^-},(\varphi_{E'})_{H^-})=2$. This yields the result.

Lemma **(8.6)**. — (i) $(\Gamma^2,\Gamma^2)=q^6+q^4+2q^2+2q+1$.

(ii) $(\Gamma^2,\Gamma\varphi_E)=(\Gamma^2,\Gamma\varphi_{E'})=q^2(q^2+1)+(q+1)$.

(iii) *If* I' *is circular and* $I\neq E$ *or* E', *then* $(\Gamma^2,\Gamma\varphi_I)=4^{|I|}(q^2+1)$.

Proof. — Let $I\subseteq S$. By Lemma (8.3),

(8.7)
$$(\Gamma^2,\Gamma\varphi_I)=(\Gamma^2-\Gamma,\Gamma\varphi_I)+(\Gamma-1,\Gamma\varphi_I)+(\Gamma,\varphi_I)$$
$$=(\Gamma^2-\Gamma,(\Gamma+1)\varphi_I)+(\Gamma,\varphi_I)=\frac{1}{2}(1_H^G+1_{H^\tau}^G,(\Gamma+1)\varphi_I)+(\Gamma,\varphi_I).$$

By Frobenius reciprocity

$$(1_H^G+1_{H^\tau}^G,(\Gamma+1)\varphi_I)=((\Gamma+1)_H,(\varphi_I)_H)+((\Gamma+1)_{H^\tau},(\varphi_I)_{H^\tau})$$
$$=((\Gamma+1)_H,(\varphi_I+\varphi_I^\tau)_H).$$

Thus Lemmas (8.2) and (8.4) imply that

$$(1_H^G+1_{H^\tau}^G,(\Gamma+1)\varphi_I)=\frac{1}{q^2-1}\Big((q^4+1)2.4^{|I|}+(q+1)\sum_{x\in H^--\{1\}}(\varphi_I(x)+\varphi_I^\tau(x))$$
$$+(-q+1)\sum_{x\in H^+-\{1\}}(\varphi_I(x)+\varphi_I^\tau(x))\Big)$$
$$=\frac{1}{q^2-1}(q^4-1)2.4^{|I|}+(1_{H^-},(\varphi_I+\varphi_I^\tau)_{H^-})$$
$$-(1_{H^+},(\varphi_I+\varphi_I^\tau)_{H^+}).$$

Therefore (8.7) implies that

(8.8) $$(\Gamma^2, \Gamma\varphi_I)=(q^2+1)4^{|I|}+(\Gamma, \varphi_I)+\frac{1}{2}((1_{H^-}, (\varphi_I+\varphi_I^\tau)_{H^-})-(1_{H^+}, (\varphi_I+\varphi_I^\tau)_{H^+}))$$

(i) If $I=S$ then $\varphi_I=\Gamma$. Lemma (8.2) implies that

$$\begin{aligned}(1_{H^-}, 2\Gamma_{H^-})-(1_{H^+}, 2\Gamma_{H^+})&=\frac{2}{q-1}(q^4+(q-2)q)-\frac{2}{q+1}(q^4-q^2)\\&=2(q^3+q^2+2q-q^3+q^2)=2(2q^2+2q).\end{aligned}$$

Since $(\Gamma, \Gamma)=1$ and $|I|=m$ the result follows in this case from (8.8).

(ii) Since $\varphi_E^\tau=\varphi_{E'}$, Lemma (8.5) and (8.8) yield that if $I=E$ or E' then

$$(\Gamma^2, \Gamma\varphi_I)=(q^2+1)2^m+q+1=(q^2+1)q^2+q+1.$$

(iii) By (8.8) and Lemma (8.5) $(\Gamma^2, \Gamma\varphi_I)=(q^2+1)4^{|I|}$ as required.

9. Some Preliminary Computations for $c_{\varnothing\varnothing}$.

Define

$$\Theta=\sum_{\varnothing\neq J\neq S}(\Gamma^2, \varphi_J)\Gamma\varphi_{J'}.$$

By Lemma (5.2) and Theorem (6.3)

$$\Phi_\varnothing=\Gamma^2-(2^m-(-1)^m)\Gamma-\Theta,$$

and $$\Theta=\sum_{\substack{J\text{ circular}\\ J\neq S}}2^m4^{-|J'|}\Gamma\varphi_{J'}.$$

Thus

(9.1) $$c_{\varnothing\varnothing}=||\Gamma^2-(2^m-(-1)^m)\Gamma||^2-2(\Gamma^2-(2^m-(-1)^m)\Gamma, \Theta)+||\Theta||^2.$$

Lemma **(9.2)**. — *Suppose that m is odd. Then*

(i) $||\Gamma^2-(2^m-(-1)^m)\Gamma||^2=q^3-2q$

(ii) $(\Gamma^2-(2^m-(-1)^m)\Gamma, \Theta)=q(q+1)T_m-q(q+1)$.

Proof. — (i) By Lemma (8.1)

$$(\Gamma^2, \Gamma^2)=(\Gamma^3, \Gamma)=1+(q+1)q^2=q^3+q^2+1.$$

Thus by Corollary (5.2)

$$\begin{aligned}||\Gamma^2-(2^m-(-1)^m)\Gamma||^2&=||\Gamma^2||^2-2(q+1)(\Gamma^2, \Gamma)+(q+1)^2||\Gamma||^2\\&=q^3+q^2+1-2(q+1)^2+(q+1)^2=q^3-2q.\end{aligned}$$

(ii) Since J and J' are never both circular it follows that $(\Gamma, \Theta)=0$. Thus

$$(\Gamma^2-(2^m-(-1)^m)\Gamma, \Theta)=(\Gamma^2, \Theta)=\sum_{\substack{J\text{ circular}\\ J\neq S}}2^m4^{-|J'|}(\Gamma^2, \Gamma\varphi_{J'}).$$

By Lemma (8.1)

$$(\Gamma^2, \Gamma\varphi_{J'}) = (\Gamma^3, \varphi_{J'}) = (\Gamma, \varphi_{J'}) + (q+1)4^{|J'|}.$$

Hence
$$(\Gamma^2, \Theta) = q(q+1) \sum_{\substack{J \text{ circular} \\ J \neq S}} 1 = q(q+1)(T_m - 1)$$

by the Corollary in the Appendix. This implies the result.

Lemma **(9.3)**. — *Suppose that m is even. Then*

(i) $\|\Gamma^2 - (2^m - (-1)^m)\Gamma\|^2 = q^6 + 2q + 4$

(ii) $(\Gamma^2 - (2^m - (-1)^m)\Gamma, \Theta) = q^2(q^2+1)T_m - q^4 - 3q^2 + 2q + 4.$

Proof. — (i) By Lemma (8.6) (i) and Corollary (5.2)

$$\begin{aligned}\|\Gamma^2 - (2^m - (-1)^m)\Gamma\|^2 &= \|\Gamma^2\|^2 - 2(q^2-1)(\Gamma^2, \Gamma) + (q^2-1)^2 \\ &= q^6 + q^4 + 2q^2 + 2q + 1 \\ &\quad - 2(q^2-1)(q^2+1) + (q^2-1)^2.\end{aligned}$$

(ii) J and J′ are circular if and only if J = E or E′. Thus by Corollary (5.2)

$$(\Gamma, \Theta) = (\Gamma, \Gamma\varphi_E) + (\Gamma, \Gamma\varphi_{E'}) = 2.$$

By Lemma (8.6) (ii) and (iii) and the Corollary in the Appendix

$$\begin{aligned}(\Gamma^2, \Theta) &= \sum_{\substack{J \text{ circular} \\ J \neq S}} 2^m 4^{-|J'|} 4^{|J'|}(q^2+1) + 2(q+1) \\ &= q^2(q^2+1) \sum_{\substack{J \text{ circular} \\ J \neq S}} 1 + 2(q+1) = q^2(q^2+1)(T_m - 1) + 2(q+1).\end{aligned}$$

Thus
$$\begin{aligned}(\Gamma^2 - (2^m - (-1)^m)\Gamma, \Theta) &= (\Gamma^2 - (q^2-1)\Gamma, \Theta) \\ &= q^2(q^2+1)(T_m - 1) + 2(q+1) - 2(q^2-1).\end{aligned}$$

This yields the result

Lemma **(9.4)**. — *To prove Theorem B it suffices to prove the following statements.*

(i) *If m is odd then*

$$\|\Theta\|^2 = qU_m - q^2 - q.$$

(ii) *If m is even then*

$$\|\Theta\|^2 = q^2 U_m - q^4 - 3q^2 + 2q + 4.$$

The result follows directly from (9.1) and Lemmas (9.2) and (9.3).

10. The computation of $c_{\varnothing\varnothing}$ continued.

Define

(10.1)
$$Y = Y_m = \sum_{\substack{I \cap J \neq \varnothing \\ I, J \neq S}} (\Gamma^2, \varphi_{I'})(\Gamma^2, \varphi_{J'})(\Gamma^2, \varphi_I \varphi_J)$$

(10.2)
$$Z = Z_m = \sum_{\substack{I \cap J = \varnothing \\ I, J \neq \varnothing, S}} (\Gamma^2, \varphi_{I'})(\Gamma^2, \varphi_{J'})(\Gamma^2, \varphi_{I \cup J}).$$

By definition $||\Theta||=Y+Z$. This section contains the computation of Z. The much more difficult question of computing Y is the content of the rest of this paper. We begin with a combinatorial result.

Lemma **(10.3)**. — *Let* K *be a circular set with* $|K'|>0$. *The number of ordered pairs* (I, J) *of subsets of* S *with* I′, J′ *circular,* $I\cap J=\emptyset$ *and* $I\cup J=K$ *is* $2^{|K'|}$.

Proof. — Since no two elements of K′ are adjacent, K has $|K'|$ components. No two elements of I or J can be adjacent. Hence for each component of K the placement of some vertex in either I or J determines the placement of all the other vertices in that component, they must alternately belong to I and J. Thus there are 2 ways of placing the elements of a component in I or J. Thus there are $2^{|K'|}$ ways of choosing the pair (I, J) as required.

Lemma **(10.4)**. — *Suppose that* I′, J′, $I\cup J$ *are circular and* $I\cap J=\emptyset$. *Then one of the following occurs.*

(i) I′, J′, $I\cup J\neq S$ *and*

$$(\Gamma^2, \varphi_{I'})(\Gamma^2, \varphi_{J'})(\Gamma^2, \varphi_{I\cup J})=2^m$$

(ii) *m is even. Either* $I'=S$ *and* $J=E$ *or* E′ *or* $I=E$ *or* E′ *and* $J=S$; *or* $I=J'=E$ *or* E′. *Furthermore*

$$(\Gamma^2, \varphi_{I'})(\Gamma^2, \varphi_{J'})(\Gamma^2, \varphi_{I\cup J})=2^m+1.$$

Proof. — If $I'=S$ then J and J′ are both circular and so *m* is even and $J=E$ or E′. Similarly if $J'=S$ then $I=E$ or E′. If $I\cup J=S$ then since $|I|$, $|J|\leq m/2$ it follows that $|I|=|J|=m/2$. Thus *m* is even and $I=J'=E$ or E′.

(i) Since $I\cap J=\emptyset$ it follows that $|I\cup J|=|I|+|J|$. Thus by Corollary (5.2)

$$(\Gamma^2, \varphi_{I'})(\Gamma^2, \varphi_{J'})(\Gamma^2, \varphi_{I\cup J})=2^{3m}4^{-(|I|+|J|+m-|I\cup J|)}=2^{3m}4^{-m}=2^m$$

(ii) In each of the three cases $\{I', J', I\cup J\}=\{E, E', S\}$. Thus by Corollary (5.2) the expression is

$$(\Gamma^2, \varphi_E)(\Gamma^2, \varphi_{E'})(\Gamma^2, \varphi_S)=2^m+1.$$

Lemma **(10.5)**. — (i) *If m is odd* $Z=q(q-2)$.

(ii) *If m is even* $Z=q^4-2q^2+2$.

Proof. — For any circular set K define

$$X(K)=\{(I, J)\,|\,I', J' \text{ circular}, I\cup J=K, I\cap K=\emptyset, I, J\neq \emptyset, S\}.$$

If $K\neq S$ then Lemmas (10.3) and (10.4) imply that

$$\textbf{(10.6)}\qquad \sum_{(I, J)\in X(K)}(\Gamma^2, \varphi_{I'})(\Gamma^2, \varphi_{J'})(\Gamma^2, \varphi_K)=2^m 2^{|K'|}.$$

(i) If m is odd then Lemma (10.4) and (10.6) imply that

$$Z = \sum_{\substack{K \text{ circular} \\ K \neq S}} 2^m 2^{|K'|} = 2^m \sum_{K \text{ circular}} 2^{|K'|} - 2^m = 2^m(2^m - 2) = q(q-2)$$

by the Corollary in the Appendix.

(ii) If K is circular and $(I, J) \in X(K)$ with $I = \emptyset$ or $J = \emptyset$ then Lemma (10.4) implies that $K = E$ or E' and there are exactly 4 such pairs. Thus by (10.6), Lemma (10.4) and the Corollary in the Appendix

$$Z = \sum_{(I, J) \in X(S)} (\Gamma^2, \varphi_I)(\Gamma^2, \varphi_J)(\Gamma^2, \varphi_S) + \sum_{\substack{K \text{ circular} \\ K \neq S}} 2^m 2^{|K'|} - 4 . 2^m$$

$$= 2(2^m + 1) + 2^{2m} - 4 . 2^m = 2^{2m} - 2 . 2^m + 2 = q^4 - 2q^2 + 2$$

as required.

Lemma **(10.7)**. — *To prove Theorem B it suffices to prove the following statements.*

(i) *If m is odd then*

$$Y_m = qU_m - 2q^2 + q.$$

(ii) *If m is even then*

$$Y_m = q^2 U_m - 2q^4 - q^2 + 2q + 2.$$

Proof. — Clear by Lemmas (9.4) and (10.5).

11. Configurations in $\mathfrak{G}$.

A *configuration* $\mathfrak{Q}$ in $\mathfrak{G}$ is a set of edges and vertices of $\mathfrak{G}$ such that for each edge in $\mathfrak{Q}$, the vertices at both end points are also in $\mathfrak{Q}$. Edges may occur more than once. An edge which occurs n times is said to have *multiplicity* n.

For example, any subset of S or any union of paths is a configuration.

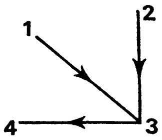
If $\mathfrak{Q}$ is a configuration let $s(\mathfrak{Q})$ denote the number of short edges in $\mathfrak{Q}$ and let $\ell(\mathfrak{Q})$ denote the number of long edges in $\mathfrak{Q}$. Define $e(\mathfrak{Q}) = s(\mathfrak{Q}) + \ell(\mathfrak{Q})$. Thus $e(\mathfrak{Q})$ is the total number of edges in $\mathfrak{Q}$.

If $I, J \subseteq S$ and $K \subseteq S$ such that φ_K is a term in $\varphi_I \varphi_J$ when it is expanded by using Theorem (3.4) then we will associate a configuration $\mathfrak{Q}$ to this situation as follows: if at some point in the expansion we take the φ_j term in φ_i^2 then we place the edge $i \to j$ into $\mathfrak{Q}$ together with the vertices i, j. If we take the $\varphi_\emptyset$ term then we simply place the vertex i in $\mathfrak{Q}$. If this occurs n times then the edge $i \to j$ has multiplicity n in $\mathfrak{Q}$. We will say that $\mathfrak{Q}$ is *associated to the pair* $\{I, J\}$ *and results in* K. A configuration $\mathfrak{Q}$ is *associated to the pair* $\{I, J\}$ if it is associated to the pair I, J and results in some K.

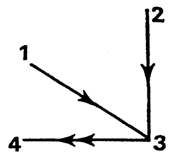
Let $\mathfrak{Q}$ be a configuration associated to $\{I, J\}$. We wish to define partial configurations $\mathfrak{Q}_n$. $\mathfrak{Q}$ results in some set K. Let $\mathfrak{Q}_0$ be the empty configuration. For $n > 0$ let $\mathfrak{Q}_n$ consist of $\mathfrak{Q}_{n-1}$ together with the vertices and edges in $\mathfrak{Q}$ obtained by expanding every φ_i^2 which had not been expanded at the previous step. Clearly $\mathfrak{Q}=\mathfrak{Q}_n$ for sufficiently large n.

Thus in particular $\mathfrak{Q}_1$ arises from all the expansions of φ_i^2 with $i \in \mathrm{I} \cap \mathrm{J}$. In particular $\mathfrak{Q}=\mathfrak{Q}_0$ is the empty configuration if $\mathrm{I} \cap \mathrm{J} = \varnothing$.

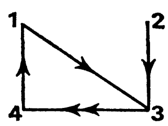
As an example let $m=5$, $\mathrm{I}=\mathrm{J}=\{1, 2, 3\}$ and $\mathrm{K}=\{1\}$. As a first step take the φ_3 term in both φ_1^2 and φ_2^2 and the φ_4 term in φ_3^2. Then $\mathfrak{Q}_1$ is



As a second step take the φ_4 term in φ_3^2. Then $\mathfrak{Q}_2$ is



where the double arrow indicates an edge of multiplicity 2. Finally take the φ_1 term in φ_4^2 to get $\mathfrak{Q}=\mathfrak{Q}_3$ which is



Lemma (**II.1**). — *Suppose that* I' *and* J' *are circular with* $\mathrm{I} \cap \mathrm{J} \neq \varnothing$. *Let* $\mathfrak{Q}$ *be a configuration associated with* $\{\mathrm{I}, \mathrm{J}\}$. *Then* none *of the following four statements occur.*

(i) *Two distinct edges enter the same vertex in* $\mathfrak{Q}$.

(ii) *An edge occurs with multiplicity at least* 2 *in* $\mathfrak{Q}$.

(iii) *Two edges emerge from the same vertex in* $\mathfrak{Q}$.

(iv) *For some* i, *both* $i \to i+2$ *and* $i+1 \to i+3$ *occur in* $\mathfrak{Q}$.

Furthermore $\mathfrak{Q}$ *is a union of paths no two of which have a common edge, the first vertex of each one being in* $\mathrm{I} \cap \mathrm{J}$, *and every other vertex, except perhaps the last in* $(\mathrm{I} \cup \mathrm{J}) - (\mathrm{I} \cap \mathrm{J})$.

Proof. — Let $\mathfrak{Q}_n$ be defined as above for $n = 0, 1, \ldots$ There are three ways in which an edge can emerge from a vertex i in $\mathfrak{Q}_n$:

(a) i is the first vertex of a path in $\mathfrak{Q}_n$.

(b) i is the end point of an edge in $\mathfrak{Q}_{n-1}$ and $i \in (\mathrm{I} \cup \mathrm{J}) - (\mathrm{I} \cap \mathrm{J})$.

(c) i is the end point of two edges in $\mathfrak{Q}_{n-1}$.

We will now prove by induction on n that $\mathfrak{Q}_n$ satisfies the conclusions of the Lemma for all n. If $n=0$, $\mathfrak{Q}_n$ is empty and the result is trivial. Suppose now that the result has been proved for $\mathfrak{Q}_t$ with $t < n$.

If (ii) or (iii) occurs in $\mathfrak{Q}_n$ then either (i) or (ii) must occur in $\mathfrak{Q}_{n-1}$ which is not the case. Thus neither (ii) nor (iii) occurs in $\mathfrak{Q}_n$. Since (i) does not occur in $\mathfrak{Q}_{n-1}$, the possibility *(c)* for having an edge emerge from a vertex does not occur in $\mathfrak{Q}_n$.

Suppose that (i) occurs in $\mathfrak{Q}_n$. Then for some i, $i \to i+2$ and $i+1 \to i+2$ are both edges in $\mathfrak{Q}_n$. Since (ii) and (iii) do not occur and the possibility *(c)* does not occur in $\mathfrak{Q}_n$ it follows that two paths in $\mathfrak{Q}_n$ can have at most one vertex in common, and this must be the last one in each path. Thus if (i) or (iv) occurs there exist two paths of one of the following forms:

$$\begin{matrix} j \to j+2 \dots \\ \dots j-1 \to j+1 \dots \end{matrix} \quad \text{or} \quad \begin{matrix} j \to j+1 \dots \\ \dots j-1 \to j+1 \dots \end{matrix}$$

Since $\mathfrak{Q}_{n-1}$ satisfies the conclusions of the Lemma it follows that $j \in I \cap J$ and $j-1 \in I \cup J$. Thus either I or J contains a pair of adjacent edges contrary to the fact that I′ and J′ are circular. Thus (i) and (iv) do not occur in $\mathfrak{Q}_n$. The last statement is an immediate consequence.

Corollary (**11.2**). — *Suppose that* I′ *and* J′ *are circular with* $I \cap J \neq \emptyset$. *Let* $K \neq \emptyset$ *and let* $\mathfrak{Q}$ *be the configuration associated to* $\{I, J\}$ *which results in* K. *Then*

$$K \cap ((I \cup J) - (I \cap J)) = K \cap \{j \mid j \text{ is not the end point of an edge in } \mathfrak{Q}\}.$$

Proof. — Suppose that $j \in K$. If j is not the end point of an edge in $\mathfrak{Q}$ then clearly $j \in I \cup J$ and $j \notin I \cap J$ as φ_K is a component of $\varphi_I \varphi_J$. If j is the end point of an edge then this edge is unique by Lemma (11.1). Since φ_K is a component of $\varphi_I \varphi_J$ this now implies that either $j \in I \cap J$ or $j \notin I \cup J$ by Lemma (11.1). This proves the result.

Lemma (**11.3**). — *Suppose that* I′ *and* J′ *are circular with* $I \cap J \neq \emptyset$. *Let* $K \subseteq S$ *and let* $\mathfrak{Q}$ *be the configuration associated to* $\{I, J\}$ *which results in* K. *Suppose that* K *is circular. Then the following hold.*

(i) *If* $\mathfrak{P}$ *is a maximal path in* $\mathfrak{Q}$ *which is not closed then either* $\mathfrak{P}$ *consists of one vertex and no edges or* $\mathfrak{P}$ *is of the form* $i \to i+1$ *for some* i.

(ii) $K \cap [I \cup J - I \cap J] = \emptyset$. *Thus every element in* K *is the end point of an edge in* $\mathfrak{Q}$.

(iii) $I = J = E$ *or* E′ *and* $K = E$ *or* E′.

Proof. — (i) Suppose that $\mathfrak{P}$ contains at least two vertices and let i be the first vertex in $\mathfrak{P}$. By Lemma (11.1), $i \in I \cap J$. Thus $i+1, i-1 \notin I \cup J$ as I′ and J′ are circular. By Corollary (11.2) $i \notin K$. Hence $i+1 \in K$ as K is circular and so $i+1$ is the end point of an edge by Corollary (11.2). Since $i+1 \notin I \cup J$ it follows from Lemma (10.1) that $i+1$ is the last vertex in $\mathfrak{P}$. This completes the proof.

(ii) Suppose that $i \in K \cap ((I \cup J) - (I \cap J))$. By Lemma (11.1) and Corollary (11.2), i is neither the beginning or end point of an edge in $\mathfrak{Q}$. Since I′, J′ are circular, neither $i+1$ or $i-1$ is in $I \cap J$. Since K is circular $i+\varepsilon \in K$ for $\varepsilon = 1$ or 2.

Suppose that $i+\varepsilon \notin (I \cup J) - (I \cap J)$. Then by Corollary (11.2), $i+\varepsilon$ is the end point of an edge in $\mathfrak{Q}$. If $i+\varepsilon \in I \cap J$ then $\varepsilon = 2$ and the edge $i+1 \to i+2$ occurs in $\mathfrak{Q}$. Since I′ and J′ are circular $i+1 \notin I \cup J$ contrary to Lemma (11.1).

If $i+\varepsilon \notin I \cup J$ then either $i+1 \to i+2$ or $i-1 \to i+1$ occurs in $\mathfrak{Q}$. Since $i+\varepsilon$ is the end of a nonclosed path by Lemma (11.1) it follows from (i) and Lemma (11.1) that $i+1$ or $i-1 \in I \cap J$ contrary to what has been shown above.

Therefore $i+\varepsilon \in (I \cup J)-(I \cap J)$. If $\varepsilon = 2$ then $i+1 \notin I \cap J$ as I′ and J′ are circular. Thus if this argument is iterated it implies that no element of S is in $I \cap J$ contrary to hypothesis. The second statement follows from Corollary (11.2).

(iii) Let $i \in I \cap J$. We consider 2 cases.

Case (a). — The edge $i \to i+1$ occurs in $\mathfrak{Q}$. As $i+1 \notin I \cup J$ it follows from Lemma (11.1) that $i+2$ is not the end point of an edge in $\mathfrak{Q}$. Thus $i+2 \notin K$ by (ii), and so $i+3 \in K$. Hence $i+2 \in I \cap J$ and the edge $i+2 \to i+3$ occurs in $\mathfrak{Q}$. If this argument is iterated it shows that m is even and $\mathfrak{Q}$ consists of either the edges $2j \to 2j+1$ or the edges $2j-1 \to 2j$. This implies that $I = J = K' = E$ or E′.

Case (b). — The edge $i \to i+2$ occurs in $\mathfrak{Q}$. Since $i-1 \notin I \cup J$ it follows that $i+1$ is not the end point of an edge in $\mathfrak{Q}$. Thus $i+1 \notin K$ by (ii) and so $i \in K$. Thus $i-2 \in I \cup J$ and $i-2 \to i$ is in $\mathfrak{Q}$. If this argument is iterated it shows that m is even and $\mathfrak{Q}$ consists of either the edges $2j \to 2(j+1)$ or the edges $2j-1 \to 2(j+1)-1$. This implies that $I = J = K = E$ or E′.

Lemma **(11.4)**. — *Suppose that m is even. Let* $I = E$ *or* E′. *Then* φ_I *occurs with multiplicity* 1 *as a constituent of* φ_I^2 *and* $\varphi_{I'}$ *occurs with multiplicity* $2^{m/2} = q$ *as a constituent of* φ_I^2.

Proof. — By Theorem (3.4)

$$\varphi_I^2 = \prod_{i \in I} (4 + 2\varphi_{i+1} + \varphi_{i+2}) = 2^{m/2} \prod_{i \in I} \varphi_{i+1} + \prod_{i \in I} \varphi_{i+2} + \theta = q\varphi_{I'} + \varphi_I + \theta,$$

where θ is a sum of terms, each of which is a product of at most $m/2$ characters φ_i, and none of which is φ_I or $\varphi_{I'}$.

Suppose that I′ and J′ are circular with $I \cap J \neq \emptyset$. A configuration $\mathfrak{Q}$ is *acceptable for* $\{I, J\}$ if it is associated with $\{I, J\}$ and results in $\emptyset$. A configuration $\mathfrak{Q}$ is *acceptable* if it is acceptable for some pair $\{I, J\}$ with I′ and J′ circular, and $I \cap J \neq \emptyset$.

Lemma **(11.5)**. — *Suppose that* $\mathfrak{Q}$ *is acceptable for* $\{I, J\}$, *where* $I \cap J \neq \emptyset$, I′ *and* J′ *are circular. Then* $\mathfrak{Q}$ *is a disjoint union of nonclosed paths, the first vertex of each being in* $I \cap J$ *and every other vertex in* $(I \cup J)-(I \cap J)$. *Every element in* $I \cup J$ *is a vertex in* $\mathfrak{Q}$.

Proof. — This is an immediate consequence of Lemma (11.1).

Lemma **(11.6)**. — *Suppose that* I′ *and* J′ *are circular with* $I \cap J \neq \emptyset$. *There is at most one configuration* $\mathfrak{Q}$ *which is acceptable for* $\{I, J\}$.

Proof. — Elements of $I \cap J$ must be first vertices of the maximal paths in $\mathfrak{Q}$ and all the remaining vertices are the elements in $(I \cup J) - (I \cap J)$. If i is a vertex in $\mathfrak{Q}$ such that both $i+1$ and $i+2$ are in $(I \cup J) - (I \cap J)$ then by Lemma (11.1) (ii) $i \to i+1 \to i+2$ must occur in $\mathfrak{Q}$. Thus the paths of $\mathfrak{Q}$ are completely determined.

Lemma **(11.7)**. — *A configuration $\mathfrak{Q}$ is acceptable if and only if $\mathfrak{Q}$ is non-empty and a disjoint union of paths such that the following hold.*

(i) *The first edge of every path which contains an edge is of the form* $i \to i+2$.

(ii) *If i and $i+1$ are both vertices of $\mathfrak{Q}$ then* $i \to i+1$ *occurs in $\mathfrak{Q}$.*

Furthermore if $\mathfrak{Q}$ satisfies these conditions then the number of ordered pairs (I, J) *such that $\mathfrak{Q}$ is acceptable for* $\{I, J\}$ *is* $2^{\ell(\mathfrak{Q})}$.

Proof. — Suppose that $\mathfrak{Q}$ is acceptable for $\{I, J\}$. If i is the first vertex of a path in $\mathfrak{Q}$ then $i \in I \cap J$ and so $i+1 \notin I \cup J$ as I' and J' are circular. Thus the path either consists of i or contains $i \to i+2$. Condition (ii) follows from Lemma (11.1) (iv). Since $I \cap J \neq \emptyset$ it follows that $\mathfrak{Q}$ is nonempty.

Conversely suppose that (i) and (ii) are satisfied. We will construct all possible ordered pairs (I, J) such that $\mathfrak{Q}$ is acceptable for $\{I, J\}$. By definition $I \cap J$ is the set of all first vertices of maximal paths in $\mathfrak{Q}$. Suppose that i is in I (J respectively). If $i \to i+1$ is in $\mathfrak{Q}$ then $i+1$ is in J (I respectively). If $i \to i+2$ is in $\mathfrak{Q}$ then we can place $i+2$ in either I or J. In this way we construct $2^{\ell(\mathfrak{Q})}$ ordered pairs (I, J). Because of condition (ii) adjacent vertices cannot belong to distinct paths and so neither I nor J contains adjacent vertices. Thus I' and J' are circular. Since $\mathfrak{Q}$ is non-empty, $I \cap J \neq \emptyset$. This construction clearly yields all ordered pairs (I, J) such that $\mathfrak{Q}$ is acceptable for $\{I, J\}$.

Suppose that $\mathfrak{Q}$ is an acceptable configuration. Let $e = e(\mathfrak{Q})$. Let $v = v(\mathfrak{Q})$ be the number of vertices in $\mathfrak{Q}$ and let $p = p(\mathfrak{Q})$ be the number of maximal paths in $\mathfrak{Q}$. Define

(11.8) $$W(\mathfrak{Q}) = 2^{2m-2v+e}.$$

Let $$W = W_m = \sum_{\mathfrak{Q} \text{ acceptable}} W(\mathfrak{Q}).$$

Lemma **(11.9)**. — *To prove Theorem B it suffices to prove that*

$$W_m = \sum_{\mathfrak{Q} \text{ acceptable}} W(\mathfrak{Q}) = 2^m U_m - 2^{2m+1} + (-1)^{m-1} 2^m.$$

Proof. — If $\mathfrak{Q}$ is acceptable for $\{I, J\}$, where I', J' are circular and $I \cap J \neq \emptyset$ then by Lemma (11.7) $|I| + |J| = p + v$. Thus by Corollary (5.2)

$$(\Gamma^2, \varphi_{I'})(\Gamma^2, \varphi_{J'}) = 2^{m-2|I|} 2^{m-2|J|} = 2^{2(m-p-v)}.$$

Except in case $I = J = E$ or E' it follows from Lemmas (11.3) and (11.6) that $(\Gamma^2, \varphi_I \varphi_J) = 2^{s(\mathfrak{Q})} 4^p$. By Lemmas (11.3) and (11.4)

$$(\Gamma^2, \varphi_E^2) = (\Gamma^2, \varphi_{E'}^2) = 2^{s(\mathfrak{Q})} 4^p + (2^{m/2} + 1).$$

Thus if m is odd then by Lemma (11.7)

$$Y_m = \sum_{\mathfrak{Q} \text{ acceptable}} 2^{\ell(\mathfrak{Q})} 2^{2(m-p-v)} 2^{s(\mathfrak{Q})} 4^p = \sum_{\mathfrak{Q} \text{ acceptable}} W(\mathfrak{Q})$$

since $\ell(\mathfrak{Q}) + s(\mathfrak{Q}) = e$. The result follows from Lemma (10.7).

If m is even then by Lemma (11.7)

$$Y_m = \sum_{\mathfrak{Q} \text{ acceptable}} 2^{\ell(\mathfrak{Q})} 2^{m-p-v} 2^{s(\mathfrak{Q})} 4^p + 2(2^{m/2}+1) = \sum_{\mathfrak{Q} \text{ acceptable}} W(\mathfrak{Q}) + 2(q+1).$$

Thus the result also follows in this case by Lemma (10.7).

12. The computation of $c_{\emptyset\emptyset}$ completed.

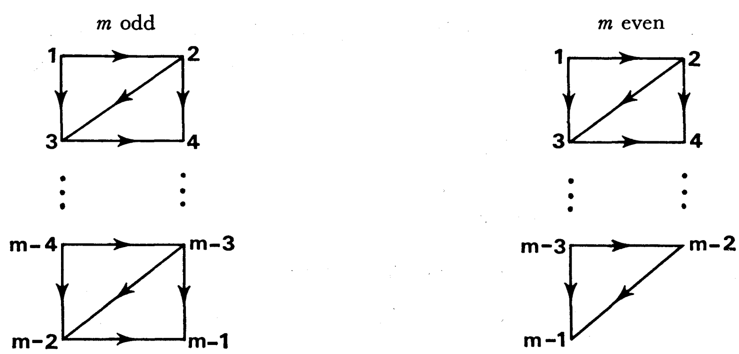
Let $\mathfrak{G}'_m$ denote the graph obtained by deleting the vertex m and all edges on which it lies together with the edge $m-1 \to 1$ from $\mathfrak{G}_m$.

Let $\mathfrak{G}''_m$ denote the graph obtained from $\mathfrak{G}'_m$ by deleting the vertex $m-1$ and all edges on which it lies from $\mathfrak{G}'_m$.

If $\mathfrak{Q}$ is an acceptable configuration containing 1 as the first vertex of one of its maximal paths then by Lemma (11.7), neither the vertex m nor the path $m-1 \to 1$ occurs in $\mathfrak{Q}$. Thus every vertex and edge in $\mathfrak{Q}$ is in $\mathfrak{G}'_m$.

Lemma (**12.1**). — *There is a graph isomorphism from $\mathfrak{G}''_m$ onto $\mathfrak{G}'_{m-1}$ which sends short edges onto short edges and long edges onto long edges. Thus an acceptable configuration $\mathfrak{Q}$ in $\mathfrak{G}'_m$ with 1 as first vertex of one of its maximal paths can be considered as a configuration in $\mathfrak{G}'_{m-1}$ and so in $\mathfrak{G}_{m-1}$.*

Proof. — The graph $\mathfrak{G}'_m$ looks as follows:



The result is now obvious.

Let $\mathfrak{X}_{p,m}$ be the set of all acceptable configurations $\mathfrak{Q}$ which have exactly p maximal paths such that 1 is the first vertex of one of these paths. We will partition $\mathfrak{X}_{p,m}$ into three subsets.

Let $\mathfrak{A}_{p,m} \subseteq \mathfrak{X}_{p,m}$ consist of all configurations $\mathfrak{Q}$ which do not contain $m-1$ as a vertex.

Let $\mathfrak{B}_{p,m} \subseteq \mathfrak{X}_{p,m}$ consist of all $\mathfrak{Q}$ such that $m-1$ is a first vertex in some path.

Let $\mathfrak{C}_{p,m} \subseteq \mathfrak{X}_{p,m}$ consist of all $\mathfrak{Q}$ such that $m-1$ is a vertex in $\mathfrak{Q}$ but is not the first vertex of any path in $\mathfrak{Q}$.

Define

$$A_{p,m} = \sum_{\mathfrak{Q} \text{ in } \mathfrak{A}_{p,m}} W(\mathfrak{Q}),$$

$$B_{p,m} = \sum_{\mathfrak{Q} \text{ in } \mathfrak{B}_{p,m}} W(\mathfrak{Q}),$$

$$C_{p,m} = \sum_{\mathfrak{Q} \text{ in } \mathfrak{C}_{p,m}} W(\mathfrak{Q}).$$

Therefore

$$\sum_{\mathfrak{Q} \text{ in } \mathfrak{X}_{p,m}} W(\mathfrak{Q}) = A_{p,m} + B_{p,m} + C_{p,m}. \tag{12.2}$$

For each acceptable configuration in $\mathfrak{G}_m$ we can specify an arbitrary element of S, instead of 1, which is to occur as a first vertex of some path, and so obtain m acceptable configurations in this way. However each configuration which contains p maximal paths is then counted p times. Therefore by (12.2)

$$W_m = \sum_{\mathfrak{Q} \text{ acceptable}} W(Q) = \sum_p \frac{m}{p} (A_{p,m} + B_{p,m} + C_{p,m}). \tag{12.3}$$

We will now compute $A_{p,m}$, $B_{p,m}$, $C_{p,m}$ by induction and so evaluate W_m.

(i) If $\mathfrak{Q}$ is in $\mathfrak{A}_{p,m}$, let $\hat{\mathfrak{Q}}$ be the same configuration as $\mathfrak{Q}$ but considered as a configuration in $\mathfrak{G}'_{m-1}$. By (11.8) $W(\mathfrak{Q}) = 4W(\hat{\mathfrak{Q}})$. Each configuration in $\mathfrak{X}_{p,m-1}$ arises in this way from a unique one in $\mathfrak{A}_{p,m}$. Hence

$$A_{p,m} = 4(A_{p,m-1} + B_{p,m-1} + C_{p,m-1}). \tag{12.4}$$

(ii) If $\mathfrak{Q}$ is in $\mathfrak{B}_{p,m}$, let $\hat{\mathfrak{Q}}$ denote the configuration in $\mathfrak{G}'_{m-1}$ obtained from $\mathfrak{Q}$ by deleting the vertex $m-1$ (there are no edges in $\mathfrak{Q}$ with $m-1$ as a vertex). Since $m-2$ is not in $\mathfrak{Q}$, $\hat{\mathfrak{Q}}$ is in $\mathfrak{A}_{p-1,m-1}$ and every configuration in $\mathfrak{A}_{p-1,m-1}$ arises in this way from a unique $\mathfrak{Q}$ in $\mathfrak{B}_{p,m}$. We have

$$v(\mathfrak{Q}) = 1 + v(\hat{\mathfrak{Q}}), \quad e(Q) = e(\hat{\mathfrak{Q}}).$$

Thus by (11.8) $W(\mathfrak{Q}) = W(\hat{\mathfrak{Q}})$ and so

$$B_{p,m} = A_{p-1,m-1}. \tag{12.5}$$

(iii) If $\mathfrak{Q}$ is in $\mathfrak{C}_{p,m}$, let $\hat{\mathfrak{Q}}$ be the configuration obtained by deleting the vertex $m-1$ and any edge with $m-1$ as end point. Such an edge is either $m-2 \rightarrow m-1$ or $m-3 \rightarrow m-1$.

If $m-2 \rightarrow m-1$ is in $\mathfrak{Q}$ then $m-2$ is not the first vertex in any maximal path in $\mathfrak{Q}$ and $\hat{\mathfrak{Q}}$ is in $\mathfrak{C}_{p,m-1}$. In this case

$$v(\mathfrak{Q}) = 1 + v(\hat{\mathfrak{Q}}), \quad e(\mathfrak{Q}) = 1 + e(\hat{\mathfrak{Q}})$$

and so $W(\mathfrak{Q})=2W(\hat{\mathfrak{Q}})$ by (11.8). Every configuration in $\mathfrak{C}_{p,m-1}$ arises in this way from a unique $\mathfrak{Q}$ in $\mathfrak{C}_{p,m}$.

If $m-3\rightarrow m-1$ occurs in $\mathfrak{Q}$, then the vertex $m-2$ is not in $\mathfrak{Q}$ and so $\hat{\mathfrak{Q}}$ is in $\mathfrak{B}_{p,m-2}\cup\mathfrak{C}_{p,m-2}$. Every such $\hat{\mathfrak{Q}}$ arises in a unique way from such a $\mathfrak{Q}$ in $\mathfrak{C}_{p,m}$. In this case

$$v(\mathfrak{Q})=1+v(\hat{\mathfrak{Q}}),\qquad e(\mathfrak{Q})=1+e(\hat{\mathfrak{Q}})$$

and so by (11.8) $W(\mathfrak{Q})=8W(\hat{\mathfrak{Q}})$. Therefore

(12.6) $$C_{p,m}=2C_{p,m-1}+8(B_{p,m-2}+C_{p,m-2}).$$

Equations (12.4) and (12.5) hold for $m\geq 3$ and (12.6) holds for $m\geq 4$. Observe that $A_{p,2}=C_{p,2}=C_{p,3}=0$ for all p while $B_{p,2}=0$ for all $p\neq 1$ and $B_{1,2}=4$.

Define

$$f(x,y)=\sum_{m\geq 2}\sum_{p\geq 0}A_{p,m}x^py^m$$

$$g(x,y)=\sum_{m\geq 2}\sum_{p\geq 0}B_{p,m}x^py^m$$

$$h(x,y)=\sum_{m\geq 2}\sum_{p\geq 0}C_{p,m}x^py^m.$$

Equations (12.4) to (12.6) yield the following statements

$$f=4y(f+g+h)$$
$$g=xyf+B_{1,2}xy^2=xyf+4xy^2$$
$$h=8y^2g+(8y^2+2y)h.$$

If g is eliminated from these linear equations we get that

$$(4xy^2+4y-1)f+4yh=-16xy^3$$
$$8xy^3f+(8y^2+2y-1)h=-32xy^4.$$

This in turn implies that

(12.7) $$f(x,y)=\frac{-16xy^3(2y-1)}{x(8y^3-4y^2)+32y^3-6y+1}.$$

By (12.3) and (12.4)

(12.8) $$W_m=\frac{1}{4}\sum_p\frac{m}{p}A_{p,m+1}.$$

Let $F(y)=\int_0^1\frac{f(x,y)}{4xy}\,dx$. Then (12.8) implies that

(12.9) $$F'(y)=\sum_{m\geq 1}W_my^{m-1}$$

Computing $F(y)$ we find

$$F(y)=\int_0^1 \frac{-4y^2(2y-1)}{x(8y^3-4y^2)+32y^3-6y+1}\,dx$$
$$=-\log(40y^3-4y^2-6y+1)+\log(32y^3-6y+1).$$

Thus

(12.10) $$F'(y)=\frac{-(120y^2-8y-6)}{40y^3-4y^2-6y+1}+\frac{(96y^2-6)}{32y^3-6y+1}.$$

Let $H(y)=\frac{1}{2}F'(y/2)$. Then (12.9) implies that

(12.11) $$H(y)=\sum_{m\geq 1} 2^{-m}W_m y^{m-1}.$$

By (12.10)

$$H(y)=\frac{-15y^2+2y+3}{5y^3-y^2-3y+1}+\frac{12y^3-3}{4y^3-3y+1}.$$

Hence if α, β, γ are the roots of x^3-3x^2-x+5 as in Section 1, it follows that

$$H(y)=\frac{\alpha}{1-\alpha y}+\frac{\beta}{1-\beta y}+\frac{\gamma}{1-\gamma y}+\frac{1}{1+y}-\frac{4}{1-2y}.$$

Hence the coefficient of y^{m-1} in $H(y)$ is

$$\alpha^m+\beta^m+\gamma^m+(-1)^{m-1}-2^{m+1}.$$

Hence (12.11) yields that

$$W_m=2^m(\alpha^m+\beta^m+\gamma^m+(-1)^{m-1}-2^{m+1})=2^m(U_m+(-1)^{m-1}-2^{m+1}).$$

By Lemma (11.9) this completes the proof of Theorem B.

APPENDIX

This Appendix contains some combinatorial results which are needed in this paper.

Lemma. — *Let* $c > 0$. *Let* X_{m+2} *(resp.* Y_m*) be the sum* $\Sigma c^{|K|}$, *where* K *ranges over all subsets of* m *points arranged on a line (resp. circle) such that no points are adjacent. Then*

$$X_m = \frac{1}{\sqrt{1+4c}}\left(\left(\frac{1+\sqrt{1+4c}}{2}\right)^m - \left(\frac{1-\sqrt{1+4c}}{2}\right)^m\right), \quad \textit{for} \quad m \geq 3,$$

$$Y_m = \left(\frac{1+\sqrt{1+4c}}{2}\right)^m + \left(\frac{1-\sqrt{1+4c}}{2}\right)^m \quad \textit{for} \quad m \geq 1.$$

Proof. — A subset of the line or circle is admissible if no two points are adjacent.

Let x_m (resp. y_m) denote the right hand side of the first (resp. second) equation in the statement. Direct computation shows that

$$X_3 = x_3 = 1 + c, \qquad X_4 = x_4 = 1 + 2c$$
$$Y_1 = y_1 = 1, \qquad Y_2 = y_2 = 1 + 2c.$$

It can furthermore be verified directly that $X_m = x_m$ and $Y_m = y_m$ for small values of m so that it may be assumed that m is sufficiently large so that all quantities are defined.

The removal of an end point from the line with m points leaves a line with $m - 1$ points. The sum over the admissible subsets which do not contain this end point is X_{m+1}, while the sum over the admissible subsets which contain this end point is cX_m. Thus $X_{m+2} = X_{m+1} + cX_m$. It is easily verified that $x_{m+2} = x_{m+1} + cx_m$. Thus $X_m = x_m$ for all $m \geq 3$.

The removal of a fixed point from the circle with $m + 2$ points leaves a line with $m + 1$ points. Thus the sum over the admissible subsets which do not contain this point is X_{m+1} and the sum over the admissible subsets which do contain this points is cX_{m-1}. Therefore

$$Y_{m+2} = X_{m+1} + cX_{m-1} = X_m + cX_{m-1} + cX_{m-2} + c^2X_{m-3} = Y_{m+1} + cY_m.$$

Since $y_{m+2} = y_{m+1} + cy_m$, it follows that $Y_m = y_m$ for $m \geq 1$.

Corollary. — (i) *The number of subsets of* m *points arranged on a line which contains no adjacent points is* $F_m = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^m - \left(\frac{1-\sqrt{5}}{2}\right)^m\right)$.

(ii) *The number of circular subsets of* S *is* $T_m = \left(\frac{1+\sqrt{5}}{2}\right)^m + \left(\frac{1-\sqrt{5}}{2}\right)^m$.

(iii) $\sum_{\substack{K \text{ circular} \\ |K'| \neq 0}} 2^{|K'|}$ *is* 2^m *for* m *even and* $2^m - 2$ *for* m *odd.*

Proof. — (i) Let $c = 1$ for X_{m+2}.

(ii) Let $c = 1$ for Y_m.

(iii) Let $c = 2$ for Y_m.

REFERENCES

[1] J. L. Alperin, *Projective modules for* $SL(2, 2^n)$ (to appear).

[2] R. W. Carter, *Simple groups of Lie type*, London, John Wiley & Sons, 1972.

[3] H. Enomoto, The characters of the finite symplectic groups $Sp(4, q)$, $q = 2^f$, *Osaka J. Math.*, **9** (1972), 75-94.

[4] J. E. Humphreys, Projective modules for $SL_2(q)$, *J. of Algebra*, **25** (1973), 513-518.

[5] A. V. Jeyakumar, Principal indecomposable representations for the group $SL(2, q)$, *J. of Algebra*, **30** (1974), 444-458.

[6] P. Landrock, A counterexample to a conjecture on the Cartan invariants of a group algebra, *Bull. London Math. Soc.*, **5** (1973), 223-224.

[7] B. Srinivasan, On the modular characters of the special linear group $SL(2, p^n)$, *Proc. London Math. Soc.*, **14** (1964), 101-114.

[8] R. Steinberg, Representations of algebraic groups, *Nagoya Math. J.*, **22** (1963), 33-56.

[9] —, Endomorphisms of linear algebraic groups, *Memoirs A.M.S.*, **80** (1968).

[10] M. Suzuki, On a class of doubly transitive groups, *Ann. of Math.* (2), **75** (1962), 105-145.

Department of Mathematics,
Yale University,
Box 2155, Yale Station,
New Haven, Connecticut 06520.

Manuscrit reçu le 28 juillet 1978.