COMBINATORIAL FORMULAS, INVARIANTS AND STRUCTURES ASSOCIATED WITH PRIMITIVE PERMUTATION REPRESENTATIONS OF PSL(2,q) AND PGL(2,q)

BY

IRERI NTHIGA KAMUTI

A thesis submitted for the degree of

Doctor of Philosophy

Faculty of Mathematical Studies

University of Southampton

June 1992.

CONTENTS

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

FACULTY OF MATHEMATICAL STUDIES

PURE MATHEMATICS

Doctor of Philosophy

COMBINATORIAL FORMULAS, INVARIANTS AND STRUCTURES ASSOCIATED WITH PRIMITIVE PERMUTATION REPRESENTATIONS OF PSL(2,q) AND PGL(2,q)

BY Ireri Nthiga Kamuti.

This thesis describes various aspects of primitive permutation representations of the groups PSL(2,q) and PGL(2,q). The disjoint cycle structures, ranks, cycle index formulas and the subdegrees of these representations are computed. A method is devised for constructing some suborbital graphs of PSL(2,q) and PGL(2,q) on the cosets of their maximal dihedral subgroups of orders q-1 and 2(q-1) respectively. Some graph theoretic properties such as the girth and diameter are discussed for some of these graphs. A general form of the intersection matrix of PGL(2,q) on the cosets of its maximal dihedral subgroup of order 2(q-1) relative to the suborbit of length 2(q-1) is given. The number of triangles on every edge of the suborbital graph corresponding to this intersection matrix is shown to be q-1.

INTRODUCTION

In this thesis we exploit the knowledge of the well-known subgroup structure of the groups PSL(2,q) and PGL(2,q) to study some important combinatorial formulas, invariants and structures associated with their primitive permutation representations. Our discussion will be mainly on the disjoint cycle structures, ranks, cycle index formulas, suborbital graphs and intersection matrices associated with some of these representations.

This thesis is divided into four chapters.

In chapter 1 we compute the disjoint cycle structures, ranks and cycle index formulas for the primitive permutation representations of PSL(2,q) and PGL(2,q).

In chapter 2 we compute the subdegrees of all primitive permutation representations of PSL(2,q) and PGL(2,q) (confirming and extending the results in [3] and [7]). Though various methods are used here, the most prominent one is based on [14] which uses the table of marks. The ranks computed in chapter 1 are also confirmed in this chapter.

In chapter 3 we devise a method for constructing some of the suborbital graphs of PSL(2,q) and PGL(2,q) on the cosets of their maximal dihedral subgroups of orders q-1 and 2(q-1) respectively. This method gives an alternative way of constructing the Coxeter graph given in [5]. Some graph theoretic properties such as the girth and diameter are found for some of the graphs discussed in this chapter.

In chapter 4 a general form of the intersection matrix of PGL(2,q) on the cosets of its maximal dihedral subgroup of order 2(q-1) relative to the suborbit of length 2(q-1) is given. The number of triangles on every edge of the suborbital graph corresponding to this intersection matrix is shown to be q-1.

CHAPTER 1

PRIMITIVE PERMUTATION REPRESENTATIONS OF PSL(2,q) AND PGL(2,q) AND THEIR CORRESPONDING CYCLE INDICES

The only well-known cycle index formulas are for the following five groups: S_n, A_n, D_n, C_n and I_n (the identity permutation on n elements) (see Harary [9], p.184). The main aim of this chapter is to derive the cycle index formulas for the primitive permutation representations of PSL(2,q) and PGL(2,q), $q=p^f$ where p is prime.

In section 1.1 we give definitions and results needed in the rest of the chapter.

The disjoint cycle structures and ranks of all primitive permutation representations of PSL(2,q) and PGL(2,q) are computed in sections 1.2 and 1.3.

In section 1.4 we illustrate by giving examples how to compute the cycle index formulas of primitive permutation representations of PSL(2,q) and PGL(2,q) by using the results in sections 1.2 and 1.3.

1.1 Group actions and cycle indices

Definition 1.1.1 Let (G_1,X_1) and (G_2,X_2) be finite permutation groups (i.e G_i acts on X_i). To say that $(G_1, X_1) \cong (G_2, X_2)$ (permutation isomorphism) means that there exists a group isomorphism $\phi : G_1 \to G_2$ and a bijection $\theta : X_1 \to X_2$ so that

$\theta(gx) = \phi g(\theta x)$ for all $g \in G_1, x \in X_1$ or $\theta g = \phi g \theta$ for all $g \in G_1$.

In other words the diagram

$$\begin{tikzcd} X_1 \arrow[r, "g"] \arrow[d, "\theta"'] & X_1 \arrow[d, "\theta"] \\ X_2 \arrow[r, "\phi g"'] & X_2 \end{tikzcd}$$

is commutative for all $g \in G_1$.

An important special case is when $G_1 = G_2$ and ϕ is the identity map. Then the condition is $\theta g = g \theta$ for all $g \in G$, and the definition determines the notion of <u>equivalent actions</u> of G on the two sets X_1 and X_2.

An important well known example follows:

<u>Theorem 1.1.2</u> Let G act transitively on the set X. Let $x \in X$

and let H = $stab_G(x)$. Then the action of G on X is equivalent to action by multiplication on the set of (right) cosets of H in G.

(See Rose [18], p.76)

Notation

From now on, $\pi(g)$ and C^g will denote the number of fixed points and the conjugacy class of $g \in G$ respectively.

The following two results will be of great use later in the chapter.

Theorem 1.1.3 Let G be a finite transitive permutation group acting on the right cosets of its subgroup H. If $g \in G$ and $|G:H|=n$,

then

$$\frac{\pi(g)}{n} = \frac{|C^g \cap H|}{|C^g|}.$$

Proof An elememt of $g \in G$ fixes a coset

$$\begin{aligned} Hs \quad &\Leftrightarrow Hsg = Hs \\ &\Leftrightarrow sgs^{-1} \in H \\ &\Leftrightarrow sgs^{-1} \in H \cap C^g. \end{aligned}$$

Since H is the subgroup of G which fixes one coset, that is H itself, then every subgroup of G fixing a coset is conjugate to H. Hence $|H \cap C^g| = |yHy^{-1} \cap C^g|$, for every $g \in G$. The number of ordered pairs (y,z) with $z \in yHy^{-1} \cap C^g$ is $n|H||H \cap C^g|$.

But if z $\in C^g$, then $\pi(z)=\pi(g)$, so that there are $\pi(g)$ cosets for which z $\in yHy^{-1}$. Therefore, the number of ordered pairs (y,z) satisfying this condition is $\pi(g)|H||C^g|$.

Hence

$$\pi(g)|H||C^g| = n|H||H \cap C^g| \ . \ \square$$

If a finite group G acts on a set X with n elements, each g $\in$ G corresponds to a permutation σ of X, which can be written uniquely as a product of disjoint cycles. If σ has α_1 cycles of length 1, α_2 cycles of length 2,....., α_n cycles of length n, we will say that σ and hence g has <u>cycle type</u> $(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

<u>Lemma 1.1.4</u> Let g be a permutation with cycle type $(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Then

(a) the number $\pi(g^l)$ of 1-cycles in g^l is $\sum_{i|l} i\alpha_i$.

(b) $\alpha_l = \frac{1}{l}\sum_{i|l} \pi(g^{l/i})\mu(i)$, where μ is the Mobius function

(see Hardy and Wright [10], p.234 for the definition of

$\mu)$.

<u>Proof</u> (a) Suppose $\theta_1\theta_2......$, is a disjoint cycle decomposition of g, then

$$g^{l} = (\theta_1\theta_2.....)^{l} = \theta_1^{l}\theta_2^{l}...... .$$

Let θ be any i-cycle in g, then θ^{l} is a product of (i,l) $\frac{i}{(i,l)}$-*cycles* and it contains a 1-cycle if and only if $i|l$. In this case we have i 1-cycles. The result follows when we sum over all the cycles of various lengths i such that $i|l$.

(b) Let $f(l) = \pi(g^{l})$.

From (a), $f(l) = \sum_{i|l} i\alpha_i = \sum_{i|l} h(i)$, *where we define* $h(i) = i\alpha_i$.

By using the Möbius Inversion Formula (see Hardy and Wright [10], Theorem 266),

we get

$$l\alpha_l = g(l) = \sum_{i|l} f(i)\mu(l/i) = \sum_{i|l} f(\frac{l}{i})\mu(i) = \sum_{i|l} \pi(g^{l/i})\mu(i) \quad . \square$$

<u>Definition 1.1.5</u> If a finite group G acts on X, $|X|=n$ and $g\epsilon G$ has cycle type $(\alpha_1, \alpha_2,....,\alpha_n)$ we define the <u>monomial</u> of g to be

$$mon(g) = t_1^{\alpha_1} t_2^{\alpha_2} \ldots . t_n^{\alpha_n} ,$$

where t_1, t_2, ...,t_n are n distinct (commuting) indeterminates.

Definition 1.1.6 The cycle index of the action of G on X is the polynomial (say over the rational field $\mathbb{Q}$) in t_1, t_2, ...,t_n given by

$$\mathcal{Z}(G) = Z_{G,X}(t_1, t_2, \ldots, t_n) = \frac{1}{|G|} \sum \{ mon(g) : g \in G \} .$$

Note that if G has conjugacy classes K_1, K_2,....,K_m, with $g_i \in K_i$ for all i, then

$$\mathcal{Z}(G) = \frac{1}{|G|} \sum_{i=1}^{m} |K_i| mon(g_i) .$$

Definition 1.1.7 If G is a finite group acting on a finite set X, we define the orbit of $x \in X$ to be

$$Orb_G(x) = \{gx | g \in G\}.$$

The number of G-orbits is normally found using the following well-known formula.

Theorem 1.1.8 (Cauchy - Frobenius Formula) Let G be a group acting on a finite set X. The number of G-orbits in X is

$$\frac{1}{|G|} \sum_{g \in G} \pi(g) .$$

(see Krishnamurthy [15], Theorem 1.4.)

If G_x is the stabilizer of $x \in X$, the number of G_x-orbits on X is called the rank r of G. Later in the chapter we shall use the Cauchy - Frobenius Formula to calculate the ranks of PSL(2,q) and PGL(2,q) on the cosets of their maximal subgroups.

Let (G,X) be a finite permutation group and we denote by $X^{(2)}$ the set of 2-element subsets of X. If g is a permutation in (G,X), we may want to know the disjoint cycle structure of the permutation g' induced by g on $X^{(2)}$.

We shall briefly sketch the technique (we call it the pair group action) for obtaining the disjoint cycle structure of g';

for a detailed treatment and examples one can refer to Harary [8], chap. 5.

Let $mon(g) = t_1^{\alpha_1} t_2^{\alpha_2} \ldots\ldots t_n^{\alpha_n}$, our aim is to find mon(g')

from which the disjoint cycle structure of g' can straightforwardly be obtained. To do this, there are two separate contributions from g to the corresponding term of mon(g') which we need to consider:

(i) From pairs of points, both lying in a common cycle of g.

(ii) From pairs of points, one in each of two different cycles of g.

It is convenient to divide the first contributions into:

(a) those pairs from the odd cycles and (b) those pairs from even cycles.

(i) (a) Let $\theta = (1\ 2\ 3 \ldots\ldots 2m+1)$ be an odd cycle in g, then the permutation θ' in $(G,X^{(2)})$ induced by θ is as follows:

$$123\ldots 2m+1 \rightarrow \left\{ \begin{array}{l} \{1,2\}\rightarrow\{2,3\}\rightarrow\{3,4\}\rightarrow\ldots\ldots\rightarrow\{2m+1,1\} \\ \{1,3\}\rightarrow\{2,4\}\rightarrow\{3,5\}\rightarrow\ldots\ldots\rightarrow\{2m,1\}\rightarrow\{2m+1,2\} \\ \{1,4\}\rightarrow\{2,5\}\rightarrow\{3,6\}\rightarrow\ldots\ldots\rightarrow\{2m-1,1\}\rightarrow\{2m,2\}\rightarrow\{2m+1,3\} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \{1,m\}\rightarrow\{2,m+1\}\rightarrow\ldots\ldots\rightarrow\{m+3,1\}\rightarrow\ldots\ldots\rightarrow\{2m+1,m-1\} \\ \{1,m+1\}\rightarrow\{2,m+2\}\rightarrow\ldots\ldots\rightarrow\{m+2,1\}\rightarrow\ldots\ldots\rightarrow\{2m+1,m\} \end{array} \right.$$

Hence $t_{2m+1}\rightarrow s_{2m+1}^{m}$.

So if we have α_{2m+1} cycles of length 2m+1 in g, the pairs of points lying in the common cycles contribute:

$$t_{2m+1}^{\alpha_{2m+1}} \rightarrow s_{2m+1}^{m\alpha_{2m+1}} \qquad (1.1.1)$$

for odd cycles.

(i) (b) If $\theta = (1\ 2\ 3\ \ldots .\ 2m)$, then we get θ' as follows:

$$
(1\,2\,3\ldots 2m) \rightarrow \begin{cases}
\{1,2\}\rightarrow\{2,3\}\rightarrow\{3,4\}\rightarrow\ldots\ldots\rightarrow\{2m,1\} \\
\{1,3\}\rightarrow\{2,4\}\rightarrow\{3,5\}\rightarrow\ldots\ldots\rightarrow\{2m-1,1\}\rightarrow\{2m,2\} \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\{1,m-1\}\rightarrow\{2,m\}\rightarrow\ldots\ldots\rightarrow\{m+3,1\}\rightarrow\ldots\ldots\rightarrow\{2m,m-2\} \\
\{1,m\}\rightarrow\{2,m+1\}\rightarrow\ldots\ldots\rightarrow\{m+2,1\}\rightarrow\ldots\ldots\rightarrow\{2m,m-1\} \\
\{1,1+m\}\rightarrow\{2,m+2\}\rightarrow\ldots\ldots\ldots\ldots\ldots\ldots\rightarrow\{m,2m\}
\end{cases}
$$

Hence $t_{2m} \rightarrow s_m s_{2m}^{m-1}$.

So if α_{2m} is the number of cycles of length 2m in g, the pairs of points lying in common cycles contribute:

$$t_{2m}^{\alpha_{2m}} \rightarrow (s_m s_{2m}^{m-1})^{\alpha_{2m}} \qquad (1.1.2)$$

for even cycles.

(ii) Consider two distinct cycles of length a and b in (G,X). If x belongs to an a-cycle θ_a of g and y belongs to a b-cycle θ_b of g, then the least positive integer β, for which $g^\beta x=x$ and also $g^\beta y=y$, is [a,b], the lcm of a and b. So the element {x,y} belongs to an [a,b]-cycle of g'. The number of such [a,b]-cycles contributed by g on $\theta_a x \theta_b$ to g' is the total number of pairs in $\theta_a x \theta_b$ divided by [a,b], the length of each cycle. This number is therefore

$$\frac{ab}{[a,b]} = (a,b) \ ,$$

the gcd of a and b.

In particular when a = b = ℓ, the contribution by g on $\Theta_a X \Theta_b$ to g' is ℓ cycles of length ℓ. Thus when $a \neq b$, we have

$$t_a^{\alpha_a} t_b^{\alpha_b} \rightarrow s_{[a,b]}^{\alpha_a \alpha_b (a,b)} \ , \tag{1.1.3}$$

and when a = b = ℓ,

$$t_\ell^{\alpha_\ell} \rightarrow s_\ell^{\ell \binom{\alpha_\ell}{2}} \ , \tag{1.1.4}$$

Now we simply need to multiply the right-sides of (1.1.1) - (1.1.4) over all applicable cases. Collecting the like terms and simplifying gives mon(g') and hence the disjoint cycle structure of g'.

Before we start discussing the next section, we first give some definitions and notation which we shall carry through to the other chapters.

The PGL(2,q) group over the finite field GF(q) of prime power order q is a group consisting of linear fractional transformations of the form

$$x \to \frac{ax+b}{cx+d} \ ,$$

with $x \in PG(1,q)$, $a, b, c, d \in GF(q)$, where $ad-bc \neq 0$.

PGL(2,q) is 3-transitive on PG(1,q) of degree q+1 and order $q(q^2-1)$.

The PSL(2,q) is a subgroup of PGL(2,q) with ad - bc = 1. It is simple for q > 3. It is also 2-transitive on PG(1,q) of degree q+1 and order $\frac{q(q^2-1)}{k}$, where k=(q-1,2).

If q is a power of 2, then

$$PGL(2,q) \cong PSL(2,q).$$

As we shall see later, in both PSL(2,q) and PGL(2,q) only the identity has more than two fixed points and both groups are partitioned by their non-identity elements into three parts (excluding the identity), namely;

(i) those permutations with precisely <u>one</u> fixed point on PG(1,q) (the <u>parabolic elements</u>),

(ii) those permutations with precisely <u>two</u> fixed points (the <u>hyperbolic elements</u>),

(iii) those permutations with no fixed points (<u>elliptic elements</u>).

Notation

We shall denote the sets of parabolic, hyperbolic and elliptic elements by the symbols τ_1, τ_2 and τ_0 respectively. The symbols C_n, D_{2n} and P_q for $n \in \mathbb{N}$,q a prime power, will mean respectively the cyclic group of order n, the dihedral group of order 2n and the elementary abelian group of order q.

The symbol q will always represent the prime p to the power f. For an arbitrary $m|f$, the symbol e will represent the prime p to the power m. Also merely for simplification, we introduce the following functions $w,z:\mathbb{N} \to \mathbb{Q}$ which are defined by:

$$w:n \to \frac{1}{n}(p^f-1),$$
$$z:n \to \frac{1}{n}(p^f+1).$$

With the help of the above simplifications, we now give some more notation that will describe some subgroups of PSL(2,q) and PGL(2,q). From now onwards we shall take k to be (2,w(1)).

The z(1) Frobenius groups in PSL(2,q) that are each the stabilizer of a point are semi-direct products of a P_q by a $C_{w(k)}$ (see Dickson [6], § 250). Any subgroup of these which is a 'proper' semi-direct product will be denoted by $S_{e,n}$, (i.e $S_{e,n} = P_e \rtimes C_n$, where $1 \le n|w(k)$) or by $S_{q,n}$ if m=f.

Similarly PGL(2,q) has Frobenius stabilizers $P_q \rtimes C_{w(1)}$. We shall also denote subgroups of this by $S_{e,n}$ (or $S_{q,n}$ for m=f) where $n|w(1)$.

1.2 Primitive permutation representations of G = PSL(2,q)

We shall first have a brief look at the subgroup structure of G; for more details see Dickson [6], chap. 12 or Huppert [13], chap. 2, §8 for more modern and standard terminology.

Theorem 1.2.1 (a) The elementary abelian subgroup P_q of G is a Sylow p-subgroup isomorphic to the additive group of GF(q).

(b) The elements of P_q have a common fixed point, and each non-identity element of P_q has only this fixed point.

(c) G has precisely z(1) Sylow p-subgroups.

(d) Each pair of distinct conjugates of P_q intersect only at the identity.

(see Huppert [13], p.191.)

The normalizer of P_q is $S_{q,w(k)}$.

Theorem 1.2.2 (a) The subgroup of G which fixes 0 and ∞ is a cyclic group $C_{w(k)}$.

(b) Each pair of distinct conjugates of $C_{w(k)}$ intersect only at the identity.

(c) For each u with $I \neq u \in C_{w(k)}$, $N_G(\langle u \rangle)$ is a dihedral group of order 2w(k).

(see Huppert [13], p.192.)

Theorem 1.2.3 (a) G has a cyclic subgroup $C_{z(k)}$.

(b) If $I \neq s \in C_{z(k)}$, then $N_G(\langle s \rangle)$ is a dihedral group of order $2z(k)$.

(c) Each pair of distinct conjugates of $C_{z(k)}$ intersect only at the identity.

(d) If $I \neq s \in C_{z(k)}$, then s has no fixed points on PG(1,q).

(see Huppert [13], p.192.)

By using the notation introduced earlier on, the normalizers of $C_{w(k)}$ and $C_{z(k)}$ become $D_{2w(k)}$ and $D_{2z(k)}$ respectively.

We now state a theorem which gives a partition of G into sets each of which contains elements with a precise number of fixed points. The notation used in the theorem should not be confused with the notation C^g introduced earlier on. By $C^g_{w(k)}$ for example, we mean conjugation of $C_{w(k)}$ by $g \in G$.

Theorem 1.2.4 Let $\mathcal{P}$ be the following set of subgroups of G;

$$\mathcal{P} = \left\{ P_q^g,\ C_{w(k)}^g,\ C_{z(k)}^g \,\middle|\, g \in G \right\} .$$

Then each non-identity element of G is contained in exactly one group in $\mathcal{P}$. (Thus the set $\mathcal{P}$ forms a partition of G).

(b) Let $\pi(g)$ be the number of fixed points of $g \in G$ on PG(1,q).

Now if we recall that

$$\tau_i = \{g | g \in G,\ \pi(g) = i\} \ ;$$

then

$$\tau_0 = \bigcup_{g\in G} (C_{z(k)} - I)^g, \ \tau_1 = \bigcup_{g\in G} (P_q - I)^g, \ \tau_2 = \bigcup_{g\in G} (C_{w(k)} - I)^g \ .$$

(see Huppert [13], p.193.)

<u>Lemma 1.2.5</u> If g is elliptic or hyperbolic of order greater than 2, or if g is parabolic, then its centralizer in G consists of all elliptic (resp. hyperbolic, parabolic) elements with the same fixed point set, together with the identity element. On the other hand, if g is elliptic or hyperbolic of order 2, then its centralizer is a dihedral group of order 2z(k) or 2w(k) respectively.

(see Dickson [6], § 224.)

<u>Lemma 1.2.6</u> Let $d_\omega = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \in C_{w(k)}$; *if* $g^{-1} d_\omega g = d_\rho$ for some

$g \in G$ and $\omega \neq \pm 1$, then $\rho = \omega$ or $\rho = \omega^{-1}$ and $g \in D_{2w(k)}$.

(see Suzuki [20], Lemma 6.4.)

<u>Lemma 1.2.7</u> The w(1) non-identity elements of the Sylow p-subgroup P_q of G are all conjugate if p=2, but are separated into two sets of w(2) conjugate elements if p > 2.

(see Dickson [6], § 241.)

Lemma 1.2.8 The p-1 non-identity elements of a cyclic subgroup C_p of G belong half to one set of conjugacy classes and half to the other if $p > 2$ and f is odd but all belong to the same set if

$p > 2$ and f is even or $p=2$.

(see Dickson [6], § 241.)

A subgroup H of G is maximal if it is isomorphic to one of the following types of groups satisfying the given conditions:

1) $S_{q,w(k)}$;

2) $D_{2w(k)}$ (exceptions occur when q=3,5,7,9,11);

3) $D_{2z(k)}$ (exceptions occur when q=2,7,9);

4) Alternating group A_4, when $q=p > 3$ and $q\equiv 3,13,27,37 \pmod{40}$;

5) Alternating group A_5, when $q=5^n$ or 4^n where n is prime, or $q=p$ and $q=\pm 1 \bmod 5$, or $q=p^2$ where $p > 2$ and $q\equiv -1 \bmod 5$;

6) Symmetric group S_4, when $q=p$ and $q\equiv\pm 1 \bmod 8$;

7) PSL(2,e) when f/m is an odd prime number;

8) PGL(2,e) when f/m=2.

(see Suzuki [20], p.417.)

Furthermore we have one conjugacy class of subgroups isomorphic to H in 1), 2), 3), 4) (if $q\equiv\pm 3 \bmod 8$), 5) (when $q=4^n$ or 5^n where n is prime), 7) and two conjugacy classes in 4) (if $q\equiv\pm 1 \bmod 8$), 5) (when $q=p$ and $q\equiv\pm 1 \bmod 5$ or $q=p^2$, $p > 2$ and $q\equiv 1 \bmod 5$), 6) and 8), conjugate in PGL(2,q) (see Dickson [6], § 260). Hence we have (up to equivalence) one permutation representation on the cosets of H.

Next we compute the disjoint cycle structures of G and its rank on the right cosets of H in the order given in the list above. (Although our main aim is to work with maximal subgroups H of G, where possible we shall generalize our results to include cases where H is not maximal.)

Our computations will be carried out by each time taking an element g of order d in G from τ_1, τ_2 and τ_0 respectively.
(i.e $d=p$, $d|w(k)$ and $d|z(k)$ respectively.)

1) Representation on the cosets of $H \cong S_{q,w(k)}$

From Theorem 1.1.2, the action of G on the cosets of H is equivalent to its natural action on PG(1,q) of degree z(1).

From Theorems 1.2.1 - 1.2.4, we have the following results:

Table 1.2.1

	(I)		(II)		(III)
	τ_1		τ_2		τ_0
Cycle lengths of g'	1	p	1	d	d
No. of cycles	1	p^{f-1}	2	w(d)	z(d)

Where for example in the second column we mean $g \in \tau_1$ induces a permutation g' with one 1-cycle and p^{f-1} p-cycles.

Since G is 2-transitive on PG(1,q), its rank in this case is 2.

2) Representation on the cosets of $H \cong D_{2w(k)}$

Since H is the stabilizer of an unordered pair $\{\beta,\lambda\} \subseteq PG(1,q)$ and G is 2-transitive on PG(1,q), by Theorem 1.1.2 we can obtain the disjoint cycle structures of the elements of G on the cosets of H by considering its action on unordered pairs of PG(1,q).

The method we shall use here is based on the results on the pair group action introduced earlier. Before we start, it is important to specify the column (headed by τ_i, i=0,1,2) in Table 1.2.1 in which permutations g' with even cycle lengths lie (any of the other two columns will have permutations of odd lengths only). Hence three cases must be distinguished: (a) p=2 (b) $q\equiv 1 \bmod 4$ (c) $q\equiv -1 \bmod 4$.

If $g \in \tau_2$ or τ_0; in cases (b) and (c) we have to differentiate between the cases $2|d$ and $2\nmid d$. We will work out case (b) with $g \in \tau_2$ and $2|d$ fully; for the other cases we only give the results.

Now if $g \in \tau_2$, $q\equiv 1 \bmod 4$ and $2|d$; from the results in Table 1.2.1, g contains two 1-cycles and w(d) d-cycles. By using the results on the pair group action, we get the contributions as follows:

By (1.1.1), the two trivial cycles contribute:

$$t_1^2 \rightarrow s_1^{\circ}. \tag{1.2.1}$$

By (1.1.2), the w(d) non-trivial cycles contribute:

$$t_d^{w(d)} \rightarrow s_{\frac{1}{2}d}^{w(d)} s_d^{w(2d)(d-2)}. \qquad (1.2.2)$$

By (1.1.3), contributions from the non-trivial cycles are:

$$t_1^2 t_d^{w(d)} \rightarrow s_d^{2w(d)}. \qquad (1.2.3)$$

By (1.1.4), the contribution from the two trivial cycles is:

$$t_1^2 \rightarrow s_1^1. \qquad (1.2.4)$$

Again by (1.1.4), contributions fron the non-trivial cycles are:

$$t_d^{w(d)} \rightarrow s_d^{w(2d)(w(1)-d)}. \qquad (1.2.5)$$

Combining (1.2.1) - (1.2.5) we get

$$mon(g') = s_1 s_{\frac{1}{2}d}^{w(d)} s_d^{w(2d)z(1)} .$$

(i.e g' contains one 1-cycle, w(d) ½d-cycles and w(2d)z(1) d-cycles). We can similarly obtain the results for the other cases.

Summary of the results.

(I) $g \in \tau_1$

In case (a), g' contains 2^{f-1} 1-cycles and 4^{f-1} p-cycles.

In case (b) and (c), g' contains $z(2)p^{f-1}$ p-cycles.

Results for $g \in \tau_2$ and τ_0 are displayed in the table below:

Table 1.2.2

	(II)			(III)	
	τ_2			τ_0	
CYCLE LENGTHS OF g'	1	½d	d	½d	d
NO. OF CYCLES: Case (a)	1	0	w(2d)z(1)	0	qz(2d)
Cases (b) and (c) with					
d even	1	w(d)	w(2d)z(1)	z(d)	w(2d)z(1)
d odd	1	0	w(2d)(q+2)	0	qz(2d)

Note that the above table has been compressed to save space. This though does not hinder us from getting the information the table was intended for (i.e the disjoint cycle structure of g' for the cases listed earlier). For example if we take case (c) where $q \equiv -1 \bmod 4$ and $g \in \tau_0$, all we have to note is that d can either be even or odd. Now from column (III) we get; for d even, g' contains z(d) d/2-cycles and w(2d)z(1) d-cycles; and for d odd, g' contains qz(2d) d-cycles.

By using the Cauchy - Frobenius formula, we calculate the rank r of G as follows:

Case (a)

From the results given above, elements of H have fixed points as follows:

The identity fixes $qz(2)$ cosets. We also have $w(1)$ elements of order two each fixing 2^{f-1} cosets and $q-2$ elements of order greater than two each fixing one coset. Hence

$$r = \frac{1}{2w(1)}[qz(2) + w(1)2^{f-1} + (q-2)] = 2^{f-1} + 1 .$$

<u>Case (b)</u>

$$r = \frac{1}{w(1)}[qz(2) + (z(2))^2 + \frac{q-5}{2}] = \frac{3}{4}(q+3) .$$

<u>Case (c)</u>

$$r = \frac{1}{w(1)}[qz(2) + w(2)z(2) + w(2)] = \frac{3q+7}{4} .$$

In parts 3) -8) we compute the cycle structure of g' using an approach different from the one used previously. Our first objective will be to determine $|C^g|$ and $|C^g \cap H|$. We easily obtain $|C^g|$ by using Theorems 1.2.1 - 1.2.3 and Lemmas 1.2.5 and 1.2.7. If no $h \in H$ with $|h|=d$ (order of g) exists, then $|C^g \cap H|=0$; if such an h exists, this intersection can be obtained using Theorems 1.2.1 - 1.2.3, Lemmas 1.2.5 - 1.2.8 and the knowledge of conjugacy classes of H which we shall discuss as we go along. We use Theorem 1.1.3 to calculate $\pi(g)$. Once $\pi(g)$ is known, the numbers α_i will be determined using Lemma 1.1.4(b) and some quite straightforward arguments. <u>Remark 1.2.1</u> We notice from Lemma 1.1.4(b) that g' contains a cycle of length i if there exists $h \in H$ with $d/(d,i) = |h|$ (i.e if $\pi(g^i)=0$, then $\alpha_i=0$).

The way we arrive at various cases in each of the parts needs a mention; bearing in mind conditions given earlier for H to be maximal, we search for the conditions on q giving all the possible distributions of non-identity elements of H over the three partitions (τ_i, i=0,1,2) of G, then eliminate those possibilities where H does not exist or H is not maximal.

3) Representation on the cosets of $H \cong D_{2z(k)}$.

Let $C_{z(k)}$ be the maximal cyclic subgroup of H. The z(k) involutions in $H \backslash C_{z(k)}$ are all conjugate in H if $q \equiv 1 \bmod 4$ or $p=2$. If $q \equiv -1 \bmod 4$ these involutions lie in two conjugacy classes of z(4) elements.

Let $\langle s \rangle = C_{z(k)}$, then the conjugacy class of s^j, $j \in \mathbb{N}$ in H is $\{s^j, s^{-j}\}$. In particular H contains a singleton conjugacy class containing an involution in $C_{z(k)}$ if and only if $q \equiv -1 \bmod 4$.

Involutions in G form a single conjugacy class containing

$$\begin{cases} qz(2) & if\ q = 1 \bmod 4 \\ qw(2) & if\ q = -1 \bmod 4 \\ w(1)z(1) & if\ p = 2 \end{cases}$$

elements.

If d (order of g) is 2, then

$$|C^g \cap H| = \begin{cases} z(k) & \text{if } p = 2 \text{ or } q \equiv 1 \bmod 4 \\ \frac{q+3}{2} & \text{if } q \equiv -1 \bmod 4. \end{cases}$$

From Theorem 1.2.3 and the information given above, if d>2, then

$$|C^g \cap H| = \begin{cases} 2 & \text{if } g \in \tau_0 \\ 0 & \text{otherwise.} \end{cases}$$

The involutions in H lie in one of the τ_i (i=0,1,2), giving us 3 cases to consider:

(a) when p=2 (b) when q≡ 1 mod 4 (c) when q≡ -1 mod 4.

The table below gives the values of π(g).

Table 1.2.3

	$\lvert C^g \rvert$	$\lvert C^g \cap H \rvert$	$\pi(g)$
(I) $g \in \tau_1$: Case (a)	w(1)z(1)	z(1)	2^{f-1}
Case (b) and (c)	w(2)z(1)	0	0
(II) $g \in \tau_2$: Case (a) Case (b) with d≠2 Case (c)	qz(1)	0	0
Case (b) with d=2	qz(2)	z(2)	w(2)
(III) $g \in \tau_0$: Case (a) Case (c) with d≠2 Case (b)	qw(1)	2	1
Case (c) with d=2	qw(2)	(q+3)/2	(q+3)/2

We may now proceed to calculate in detail the cycle lengths of the element g' corresponding to g in this representation.

(I) $g \in \tau_1$

Case (a)

From Table 1.2.3, $\pi(g)=2^{f-1}$. It is quite straightforward that the only non-trivial cycles g' has are the $2^{f-1}(2^{f-1}-1)$ 2-cycles.

Case (b) and (c)

Here d=p and for $1 \le l < p$, $|g^l| = p$.

From Table 1.2.3, $\pi(g^l)=0$. Hence from Remark 1.2.1, $\alpha_l=0$.

We also have

$$\begin{aligned} \alpha_p &= \frac{1}{p}\pi(g^p) \\ &= qw(2p) . \end{aligned}$$

(II) $g \in \tau_2$

Case (a)

If $1 \le l < d$, we deduce from Table 1.2.3 that $\pi(g^l) = 0$.

Hence from Remark 1.2.1, $\alpha_l = 0$.

Now

$$\begin{aligned} \alpha_d &= \frac{1}{d}\pi(g^d) \\ &= 2w(2d) . \end{aligned}$$

Case (b)

(i) If $1 \le l < d$, $2|d$, from Table 1.2.3 we have

$$\pi(g^{l}) = \begin{cases} w(2) & if\ l = \dfrac{d}{2} \\ 0 & otherwise. \end{cases}$$

Hence if $l \neq d/2$, $\alpha_l=0$

and

$$\alpha_{\frac{d}{2}} = \frac{2}{d}\pi(g^{\frac{d}{2}})$$
$$= w(d) \quad .$$

We also have

$$\alpha_d = \frac{1}{d}[\pi(g^{d}) - \pi(g^{\frac{d}{2}})]$$
$$= w(2d)\,(w(1))\,.$$

(ii) If $2 \nmid d$, for $1 \leq l < d$, $\pi(g^l)=0$ and therefore $\alpha_l=0$.

If $l=d$ then

$$\alpha_d = \frac{1}{d}\pi(g^{d})$$
$$= qw(2d)\,.$$

<u>Case (c)</u>

As in b(ii) above, g' contains only the qw(2d) d-cycles.

(III) $g \in \mathcal{T}_0$

Case (a)

From Table 1.2.3, $\pi(g^l)=1$ for $1 \leq l < d$. Hence for $1 < l < d$,

$$\left.\begin{aligned}\alpha_l &= \frac{1}{l}\sum_{i|l}\mu(i)\\ &= 0\end{aligned}\right\} \tag{1.2.6}$$

We also have

$$\left.\begin{aligned}\alpha_d &= \frac{1}{d}[\pi(g^d) + \sum_{i|d}\mu(i) - \mu(1)]\\ &= \frac{1}{d}[\pi(g^d) - \mu(1)]\\ &= (q-2)z(2d)\end{aligned}\right\} \tag{1.2.7}$$

Case (b)

Since $\pi(g^l)=1$ for $1 \leq l < d$, then for $1 < l < d$, $\alpha_l=0$ (cf. (1.2.6)).

Now

$\alpha_d=(q-2)z(2d)$ (cf. (1.2.7)).

Case (c)

(i) For $1 \leq l < d$, $2|d$, we have

$$\pi(g^l) = \begin{cases}\frac{q+3}{2} & \text{if } l=\frac{d}{2}\\ 1 & \text{otherwise.}\end{cases}$$

So if $1 < l < d$ and $l \neq d/2$, then, $\alpha_l=0$ (cf. (1.2.6)).
If $l=d/2$, then

$$\begin{aligned}\alpha_{d/2} &= \frac{2}{d}[\pi(g^{\frac{d}{2}})+\sum_{i|\frac{d}{2}}\mu(i)-\mu(1)] \\ &= \frac{2}{d}[\frac{q+3}{2}-1] \\ &= z(d).\end{aligned}$$

We also have

$$\begin{aligned}\alpha_d &= \frac{1}{d}[\pi(g^d)-\pi(g^{\frac{d}{2}})+\sum_{i|d}\mu(i)-\mu(1)+1] \\ &= \frac{1}{d}[\pi(g^d)-\pi(g^{\frac{d}{2}})] \\ &= (q-3)z(2d).\end{aligned}$$

(ii) If $2\nmid d$, then for $1 \leq l < d$, $\pi(g^l)=1$. Now g' contains one 1-cycle and $(q-2)z(2d)$ d-cycles (cf. (1.2.6) and (1.2.7)).

<u>Summary of the results</u>

(I) <u>$g \in \tau_1$</u>

In case (a), g' contains 2^{f-1} 1-cycles and $2^{f-1}(2^{f-1}-1)$ p-cycles.

In cases (b) and (c), g' contains $p^{f-1}w(2)$ p-cycles.

Results for $g \in \tau_2$ and τ_0 are displayed in the table below:

Table 1.2.4

	(II)		(III)		
	τ_2		τ_0		
CYCLE LENGTHS OF g'	½d	d	1	½d	d
NO. OF CYCLES					
Case (a)	0	qw(2d)	1	0	(q-2)z(2d)
Case (b) and (c) with d even	w(d)	w(2d)w(1)	1	z(d)	(q-3)z(2d)
d odd	0	qw(2d)	1	0	(q-2)z(2d)

Rank of G

Case (a) $$r = \frac{1}{2z(1)}\left[qw(2) + \frac{q}{2}z(1) + q\right] = 2^{f-1}.$$

Case (b) $$r = \frac{1}{z(1)}\left[qw(2) + w(2)z(2) + w(2)\right] = 3w(4).$$

Case (c) $$r = \frac{1}{z(1)}\left[qw(2) + \left(\frac{q+3}{2}\right)^2 + \frac{q-3}{2}\right] = 3z(4).$$

In parts 4) - 6) arguments similar to those used in part 3) continue to be used. But after having dealt with part 3) in detail, we will only deal with some isolated cases in the remaining parts before listing the results.

<u>4) Representation on the cosets of $H \cong A_4$</u>

There are subgroups H isomorphic to A_4 if and only if p > 2 or p=2 and f≡0 mod 2. Together with the identity element, H contains 3 conjugate elements of order 2 and 8 elements of order 3 which lie in 2 mutually inverse conjugacy classes of 4 elements.

The conjugacy classes of involutions in G were discussed in the previous part. It is easily noticed that for d=2,

$$|C^g \cap H| = 3.$$

If p=3, G contains w(1)z(1) elements of order 3. By Lemma 1.2.7, these elements form two conjugacy classes of w(2)z(1) elements. These classes are self-inverse or mutually inverse as f is even or odd.

If p≠3, from Theorems 1.2.2, 1.2.3 and Lemma 1.2.5, there is a single conjugacy class of elements of order 3 in G containing $q(q+\epsilon)$ elements, where

$$\epsilon = \begin{cases} 1 & if \quad q \equiv 1 \mod 3 \\ -1 & if \quad q \equiv -1 \mod 3 \end{cases}.$$

Therefore we have

$$|C^g \cap H| = \begin{cases} 8 \quad 0 \; if \; p=3 & f \; even \\ 4 \quad if \; p=3 & f \; odd \\ 8 \quad if \; p \neq 3. \end{cases}$$

Now excluding the cases p=2 or 3 when H is not maximal, we have the following four cases to consider:

(a) $q\equiv 5 \mod 12$

(b) $q\equiv 7 \mod 12$

(c) $q\equiv 1 \mod 12$

(d) $q\equiv -1 \mod 12$.

Values for $\pi(g)$ in all the four cases are given in the table below.

Table 1.2.5

	$\lvert C^g\rvert$	$\lvert C^g\cap H\rvert$	$\pi(g)$
(I) $g\in\tau_1$ Cases (a) -(d)	$w(2)w(1)$	0	0
(II) $g\in\tau_2$ Cases (a) and (c) with d=2 Cases (a)-(d), $d\neq 2,3$ Cases (b) and (c), d=3	 $qz(2)$ $qz(1)$ $qz(1)$	 3 0 8	 $w(4)$ 0 $w(3)$
(III) $g\in\tau_0$ Cases (a) and (d) with d=3 Cases (a)-(d), $d\neq 2,3$ Cases (b) and (d), d=2	 $qw(1)$ $qw(1)$ $qw(2)$	 8 0 3	 $z(3)$ 0 $z(4)$

Perhaps the best case to consider in order to illustrate how the numbers α_i come about is case (c) with $g\in\tau_2$. This case splits into the following four subcases:

(i) $2|d$, $3\nmid d$ (ii) $3|d$, $2\nmid d$ (iii) $2, 3|d$ (iv) $2, 3\nmid d$.

We shall only work out subcase (iii).

If $1 \leq \iota < d$, then from Table 1.2.5,

$$\pi(g^{\iota}) = \begin{cases} w(4) & if\ \iota = \frac{d}{2} \\ w(3) & if\ \iota = \frac{d}{3},\ \frac{2d}{3} \\ 0 & if\ \iota \neq \frac{d}{2},\ \frac{d}{3},\ \frac{2d}{3}. \end{cases}$$

Note that there are $\Phi(3)=2$ (Φ the Euler Φ-function) distinct l,

$1 \leq l < d$ such that $|g^l|=3$, namely $d/3$ and $2d/3$.

From Remark 1.2.1, $e_l=0$ for $l \neq d/2, d/3, 2d/3$.

If $l = d/2$, then

$$\alpha_{\frac{d}{2}} = \frac{2}{d}\pi(g^{\frac{d}{2}}) = w(2d) .$$

If $l = d/3$, then

$$\alpha_{\frac{d}{3}} = \frac{3}{d}\pi(g^{\frac{d}{3}}) = w(d) .$$

If $l = 2d/3$, then

$$\alpha_{\frac{2d}{3}} = \frac{3}{2d}[\pi(g^{\frac{2d}{3}}) - \pi(g^{\frac{d}{3}})] = 0 .$$

Lastly,

$$\alpha_d = \frac{1}{d}[\pi(g^d) - \pi(g^{\frac{d}{2}}) - \pi(g^{\frac{d}{3}})] = (q^2 + q - 14)w(24d) .$$

Summary of the results.

(I) $g \in \tau_1$

In all the four cases g' contains qw(24p)z(1) p-cycles.

Results for $g \in \tau_2$ and τ_0 are displayed in the table below:

Table 1.2.6

	(II)			(III)		
	τ_2			τ_0		
CYCLES LENGTHS OF g'	$\frac{1}{3}d$	$\frac{1}{2}d$	d	$\frac{1}{3}d$	$\frac{1}{2}d$	d
NO. OF CYCLES Cases (a)-(d) with						
$2 \mid d, 3 \nmid d$	0	$w(2d)$	$(q+3)(q-2)w(24d)$	0	$z(2d)$	$(q-3)(q+2)z(24d)$
$3 \mid d, 2 \nmid d$	$w(d)$	0	$(q^2+q-8)w(24d)$	$z(d)$	0	$(q^2-q-8)z(24d)$
$2,3 \mid d$	$w(d)$	$w(2d)$	$(q^2+q-14)w(24d)$	$z(d)$	$z(2d)$	$(q^2-q-14)z(24d)$
$2,3 \nmid d$	0	0	$qw(24d)z(1)$	0	0	$qw(24d)z(1)$

Rank of G

Case(a)

$$r = \frac{1}{12}[qw(24)z(1) + 3w(4) + 8z(3)]$$
$$= \frac{q^3 + 81q + 46}{288}.$$

Case(b)

$$r = \frac{1}{12}[qw(24)z(1) + 8w(3) + 3z(4)]$$
$$= \frac{q^3 + 81q - 46}{288}.$$

Case(c)

$$r = \frac{1}{12}[qw(24)z(1) + 3w(4) + 8w(3)]$$
$$= (q^2 + q + 82)w(288).$$

Case(d)

$$r = \frac{1}{12}[qw(24)z(1) + 8z(3) + 3z(4)]$$
$$= (q^2 - q + 82)z(288).$$

5) Representation on the cosets of $H \cong A_5$

G contains subgroups H isomorphic to the alternating group A_5 precisely when p=5 or $q \equiv \pm 1$ mod 5. Together with the identity element, H contains 24 elements of order 5 forming 2 conjugacy classes of 12 elements which are transposed by squaring, 20 conjugate elements of order 3 and 15 conjugate elements of order 2.

From the discussion we had in part 3) on the conjugacy classes of elements of order 2 in G, it is readily noticed that

$$|H \cap C^g| = 15.$$

Conjugacy classes of elements of order 3 in G were discussed in part 4). If d=3, we can easily deduce that

$$|H \cap C^g| = \begin{cases} 20 & 0 \ \mathit{if}\ p=3 \text{ and } f \text{ even} \\ 20 & \mathit{if}\ p \neq 3. \end{cases}$$

Note that the case when p=3 and f odd does not occur because we can never have $q \equiv \pm 1 \bmod 5$.

There exists elements of order 5 in G if and only if p=5 or $q \equiv \pm 1 \bmod 5$. If p=5, there are w(1)z(1) elements of order 5. By Lemma 1.2.7, these elements form two self-inverse conjugacy classes containing w(2)z(1) elements. Squaring preserves or transposes these classes as f is even or odd. If $q \equiv \pm 1 \bmod 5$; from Theorems 1.2.2 and 1.2.3 and Lemma 1.2.5, there are two self-inverse conjugacy classes of $q(q+\delta)$ elements, where

$$\delta = \begin{cases} 1 & \mathit{if}\ q \equiv 1 \bmod 5 \\ -1 & \mathit{if}\ q \equiv -1 \bmod 5; \end{cases}$$

squaring transposes the two classes.

From the information given above, the two conjugacy classes of elements of order 5 in H lie in the same conjugacy class in G if and only if p=5 and f is even. Moreover, if d is 5, then

$$|H \cap C^g| = \begin{cases} 24 \text{ or } 0 & \text{if } p=5,\ f \text{ even} \\ 12 & \text{if } p=5,\ f \text{ odd or } q \equiv \pm 1 \bmod 5. \end{cases}$$

We now have the following cases to consider:

(a) $p=2$, $q\equiv 4 \bmod 15$

(b) $p=2$, $q\equiv 1 \bmod 15$

(c) $p=3$, $q\equiv 9 \bmod 20$

(In fact here H is only maximal when $f=2$, but in this case we generalize to include $f\equiv 2 \bmod 4$)

(d) $p=5$, $q\equiv 5 \bmod 12$

(e) $q\equiv 29 \bmod 60$

(f) $q\equiv 19 \bmod 60$

(g) $q\equiv 11 \bmod 60$

(h) $q\equiv 49 \bmod 60$

(i) $q\equiv 41 \bmod 60$

(j) $q\equiv 31 \bmod 60$

(k) $q\equiv 1 \bmod 60$

(l) $q\equiv -1 \bmod 60$.

Values for $\pi(g)$ are presented in the table below:

Table 1.2.7

	$\|C^g\|$	$\|C^g{}_{nH}\|$	$\pi(g)$
(I) $g\epsilon\tau_1$			
Cases(a) and (b)	w(1)z(1)	15	2^{f-2}
Case (c)	w(2)z(1)	20 or 0	3^{f-1} or 0
Case (d)	w(2)z(1)	12	5^{f-1}
Cases(e)-(l)	w(2)z(1)	0	0
(II) $g\epsilon\tau_2$			
Cases(a) and (b) with d=3	qz(1)	20	w(3)
Case (a); d=5	qz(1)	12	w(5)
Cases(a)-(l), $d\neq 2,3,5$	qz(1)	0	0
Cases (c),(d), (e),(h),(i), (k); d=2	qz(2)	15	w(4)
Cases (f),(h) (j),(k);d=3	qz(1)	20	w(6)
Cases (g),(i), (j),(k),;d=5	qz(1)	12	w(10)
(III) $g\epsilon\tau_0$			
Case (a);d=5	qw(1)	12	z(5)
Cases(a)-(l), $d\neq 2,3,5$	qw(1)	0	0
Cases (f),(g), (j),(l);d=2	qw(2)	15	z(4)
Cases (d),(e) (g),(i),(l);d=3	qw(1)	20	z(6)
Cases (c),(e), (f),(h),(l);d=5	qw(1)	12	z(10)

Here we give case (k) with $g\epsilon\tau_2$ as an example of how we obtain the numbers α_i. We have the following subcases:

(i) $2|d$, $(3,5\nmid d)$ (ii) $3|d$, $(2,5\nmid d)$ (iii) $5|d$, $(2,3\nmid d)$

(iv) $2,3|d$ $(5\nmid d)$ (v) $2,5|d$ $(3\nmid d)$ (vi) $3,5|d$ $(2\nmid d)$ (vii) $2,3,5|d$

(viii) $2,3,5\nmid d$.

We will only work out subcase (vii).

Using the arguments similar to those in part 4), it can be shown that $\alpha_{1/2d} = \alpha_{1/3d} = w(2d)$ and $\alpha_{2/5d} = 0$.

There are $\Phi(5) = 4$ distinct ι, $1 \leq \iota < d$ such that $\pi(g^{\iota})=5$,

namely d/5, 2d/5, 3d/5 and 4d/5. Now by using arguments similar to those in part 4), the following results are immediate,

$$\alpha_{\frac{1}{5}d} = w(2d),$$
$$\alpha_{\frac{2}{5}d} = \alpha_{\frac{3}{5}d} = \alpha_{\frac{4}{5}d} = 0 \quad \text{and } \alpha_d = (q^2+q-62)w(120d).$$

For any ι, $1 \leq \iota < d$ different from the ones above, $\alpha_{\iota}=0$.

<u>Summary of the results</u>

<u>(I) $g\epsilon\tau_1$</u>

In cases (a) and (b), g' contains 2^{f-1} 1-cycles and

$\frac{1}{120}q(q^2-16)$ p-cycles. In case (c), g' contains 3^{f-1} 1-cycles

and $\frac{1}{360}q(q^2-41)$ p-cycles or only qw(360p)z(1) p-cycles.

In case (d), g' contains 5^{f-1} 1-cycles and $\frac{1}{600}q(q^2-25)$

p-cycles. In cases (e)-(ℓ), g' contains qw(120p)z(1) p cycles.
Results for $g\epsilon\tau_2$ and τ_0 are displayed in the table below:

Table 1.2.8

(II)

	τ_2			
CYCLE LENGTH OF g	d/5	d/3	d/2	d
NO. OF CYCLES				
<u>Case (a) and (b)</u>				
$3 \mid d,\ 5 \nmid d$	0	w(d)	0	(q+5)(q-4)w(60d)
$5 \mid d,\ 3 \nmid d$	w(2d)	0	0	(q+4)(q-3)w(60d)
$3,5 \mid d$	w(2d)	w(d)	0	(q^2-q-32)w(60d)
$3,5 \nmid d$	0	0	0	qw(60d)z(1)
<u>Case (c)</u>				
$2 \mid d,\ 5 \nmid d$	0	0	w(2d)	(q+6)(q-5)w(120d)
$5 \mid d,\ 2 \nmid d$	0	0	0	0
$2,5 \nmid d$	0	0	0	qw(120d)z(1)
<u>Case (d)</u>				
$2 \mid d,\ 3 \nmid d$	0	0	w(2d)	(q+6)(q-5)w(120d)
$3 \mid d,\ 2 \nmid d$	0	0	0	0
$2,3 \nmid d$	0	0	0	qw(120d)z(1)
<u>Cases (e)-(l)</u>				
$2 \mid d, 3,5 \nmid d$	0	0	w(2d)	(q+6)(q-5)w(120d)
$3 \mid d, 2,5 \nmid d$	0	w(2d)	0	(q+5)(q-4)w(120d)
$5 \mid d, 2,3 \nmid d$	w(2d)	0	0	(q+4)(q-3)w(120d)
$2,3 \mid d, 5 \nmid d$	0	w(2d)	w(2d)	(q^2+q-50)w(120d)
$2,5 \mid d, 3 \nmid d$	w(2d)	0	w(2d)	(q+7)(q-6)w(120d)
$3,5 \mid d, 2 \nmid d$	w(2d)	w(2d)	0	(q^2+q-32)w(120d)
$2,3,5 \mid d$	w(2d)	w(2d)	w(2d)	(q^2+q-62)w(120d)
$2,3,5 \nmid d$	0	0	0	qw(120d)z(1)

(III)

	τ_0			
CYCLE LENGTH OF g'	d/5	d/3	d/2	d
NO. OF CYCLES				
<u>Case (a) and (b)</u>				
$3 \mid d,\ 5 \nmid d$	0	0	0	0
$5 \mid d,\ 3 \nmid d$	0	0	0	(q-4)(q+3)z(60d)
$3,5 \mid d$	0	0	0	0
$3,5 \nmid d$	0	0	0	qw(60d)z(1)
<u>Case (c)</u>				
$2 \mid d,\ 5 \nmid d$	0	0	0	0
$5 \mid d,\ 2 \nmid d$	z(2d)	0	0	(q+3)(q-4)z(120d)
$2,5 \nmid d$	0	0	0	qw(120d)z(1)
<u>Case (d)</u>				
$2 \mid d,\ 3 \nmid d$	0	0	0	0
$3 \mid d,\ 2 \nmid d$	0	z(2d)	0	(q-5)(q+4)z(120d)
$2,3 \nmid d$	0	0	0	qw(120d)z(1)
<u>Case (e)-(l)</u>				
$2 \mid d, 3,5 \nmid d$	0	0	z(2d)	(q+5)(q-6)z(120d)
$3 \mid d, 2,5 \nmid d$	0	z(2d)	0	(q-5)(q+4)z(120d)
$5 \mid d, 2,3 \nmid d$	z(2d)	0	0	(q-4)(q+3)z(120d)
$2,3 \mid d, 5 \nmid d$	0	z(2d)	z(2d)	(q^2-q-50)z(120d)
$2,5 \mid d, 3 \nmid d$	z(2d)	0	z(2d)	(q+6)(q-7)z(120d)
$3,5 \mid d, 2 \nmid d$	z(2d)	z(2d)	0	(q^2-q-32)z(120d)
$2,3,5 \mid d$	z(2d)	z(2d)	z(2d)	(q^2-q-62)z(120d)
$2,3,5 \nmid d$	0	0	0	qw(120d)z(1)

Rank of G

Case (a)

$$r = \frac{1}{60}\left[qw(60)\,z(1) + 15\frac{q}{4} + 20w(3) + 24z(5)\right]$$
$$= \frac{q^3 + 912q - 112}{3600}.$$

Case (b)

$$r = \frac{1}{60}\left[qw(60)\,z(1) + 15\frac{q}{4} + 20w(3) + 24w(5)\right]$$
$$= \frac{q^3 + 912q - 688}{3600}.$$

Case (c)

$$r = \frac{1}{60}\left[qw(120)\,z(1) + 15w(4) + 203^{f-1} + 24z(10)\right]$$
$$= \frac{q^3 + 1537q - 162}{7200}.$$

Case (d)

$$r = \frac{1}{60}\left[qw(120)\,z(1) + 24\frac{q}{5} + 15w(4) + 20z(6)\right]$$
$$= \frac{q^3 + 1425q - 50}{7200}.$$

Case (e)

$$r = \frac{1}{60}[qw(120)z(1) + 15w(4) + 20z(6) + 24z(10)]$$
$$= \frac{q^3 + 1137q + 238}{7200}.$$

Case (f)

$$r = \frac{1}{60}[qw(120)z(1) + 20w(6) + 15z(4) + 24z(10)]$$
$$= \frac{q^3 + 1137q + 338}{7200}.$$

Case (g)

$$r = \frac{1}{60}[qw(120)z(1) + 24w(10) + 15z(4) + 20z(6)]$$
$$= \frac{q^3 + 1137q + 562}{7200}.$$

Case (h)

$$r = \frac{1}{60}[qw(120)z(1) + 15w(4) + 20w(6) + 24z(10)]$$
$$= \frac{q^3 + 1137q - 562}{7200}.$$

Case (i)

$$r = \frac{1}{60}[qw(120)z(1) + 15w(4) + 24w(10) + 20z(6)]$$
$$= \frac{q^3 + 1137q - 338}{7200}.$$

Case (j)

$$r = \frac{1}{60}[qw(120)z(1) + 20w(6) + 24w(10) + 15z(4)]$$
$$= \frac{q^3 + 1137q - 238}{7200}.$$

Case (k)

$$r = \frac{1}{60}[qw(120)z(1) + 15w(4) + 20w(6) + 24w(10)]$$
$$= \frac{q^3 + 1137q - 1138}{7200}.$$

Case (l)

$$r = \frac{1}{60}[qw(120)z(1) + 15z(4) + 20z(6) + 24z(10)]$$
$$= \frac{q^3 + 1137q + 1138}{7200}.$$

6) Representation on the cosets of $H \cong S_4$.

G contains subgroups H isomorphic to S_4 if and only if $q \equiv \pm 1 \bmod 8$. Let us now examine the conjugacy classes of elements of H.

Cycle structure	Number of them	Order
(1)	1	1
(ab)	6	2
(ab)(cd)	3	2
(abc)	8	3
(abcd)	6	4

It is well known that two permutations are conjugate in the symmetric group S_n if and only if they have the same cycle structure. Hence the table above gives the conjugacy classes of H.

The conjugacy classes of elements of order 2 and 3 in G were described in the previous parts. There are nine involutions in H, so for d=2 we have

$$|C^g \cap H| = 9.$$

If d=3 we have

$$|C^g \cap H| = \begin{cases} 8 \text{ or } 0 & \text{if } p=3 \\ 8 & \text{if } p>3. \end{cases}$$

G contains elements of order 4 if and only if $q \equiv \pm 1 \bmod 8$. These elements form a single class of $q(q+\delta)$ elements where

$$\delta = \begin{cases} 1 & q \equiv 1 \bmod 8 \\ -1 & q \equiv -1 \bmod 8. \end{cases}$$

So we have, for d=4,

$$|C^g \cap H| = 6.$$

Note that when p=3, H is not maximal in PSL(2,q). So this case will not be considered.

We have the following cases to consider:

(a) $q \equiv 17 \mod 24$

(b) $q \equiv 7 \mod 24$

(c) $q \equiv 1 \mod 24$

(d) $q \equiv -1 \mod 24$.

Below is the table of values of $\pi(g)$:

Table 1.2.9.

	$\lvert C^g\rvert$	$\lvert C^g \cap H\rvert$	$\pi(g)$
(I) $g \in \tau_1$ Case (a)-(d)	w(2)z(1)	0	0
(II) $g \in \tau_2$			
Cases (a) and (c) with d=2	qz(2)	9	3w(8)
Cases (a) and (c) with d=4	qz(1)	6	w(8)
Cases (b) and (c) with d=3	qz(1)	8	w(6)
Cases (a)-(d), $d \neq 2,3,4$	qz(1)	0	0
(III) $g \in \tau_0$			
Cases (a) and (d) with d=3	qw(1)	8	z(6)
Cases (b) and (d) with d=2	qw(2)	9	3z(8)
Cases (b) and (d) with d=4	qw(1)	6	z(8)
Cases (a)-(d), $d \neq 2,3,4$	qz(1)	0	0

We shall give case (c) with $g \in \tau_2$ and $3,4 \mid d$ as an example of how we obtain the numbers α_i. If $1 \le \ell < d$, then from Table 1.2.9,

$$\pi(g^{\ell}) = \begin{cases} 3w(8) & if\ \ell = \frac{d}{2} \\ w(8) & if\ \ell = \frac{d}{4},\ 3\frac{d}{4} \\ w(6) & if\ \ell = \frac{d}{3},\ 2\frac{d}{3} \\ 0 & Otherwise. \end{cases}$$

Now it can be shown that

$$\alpha_{\frac{d}{2}} = \alpha_{\frac{d}{3}} = \alpha_{\frac{d}{4}} = w(2d) \quad \text{and} \quad \alpha_{2\frac{d}{3}} = \alpha_{3\frac{d}{4}} = 0.$$

If $l \neq \frac{d}{2}, \frac{d}{3}, 2\frac{d}{3}, 3\frac{d}{4}$, *then* $\alpha_l = 0$.

Finally

$$\alpha_d = \frac{1}{d}[\pi(g^d) - \pi(g^{\frac{d}{2}}) - \pi(g^{\frac{d}{3}})]$$
$$= (q^2 + q - 26)w(48d).$$

<u>Summary of the results.</u>

<u>(I) $g \epsilon \tau_1$</u>

In all the four cases, g' contains qw(48p)z(1) p-cycles.

Results for $g \epsilon \tau_2$ and τ_0 are displayed in the table below:

<u>Table 1.2.10</u>

	(II)				(III)			
	τ_2				τ_0			
CYCLE OF LENGTHS g'	d/4	d/3	d/2	d	d/4	d/3	d/2	d
No. OF CYCLES <u>Cases (a) - (d)</u>								
$3 \mid d,\ 2 \nmid d$	0	w(2d)	0	$(q^2+q-8)w(48d)$	0	z(2d)	0	$(q^2-q-8)z(48d)$
$2 \mid d, 3, 4 \nmid d$	0	0	3w(4d)	$(q^2+q-18)w(48d)$	0	0	3z(4d)	$(q^2-q-18)z(48d)$
$4 \mid d, 3 \nmid d$	w(2d)	0	w(2d)	$(q^2+q-18)w(48d)$	z(2d)	0	z(2d)	$(q^2-q-18)z(48d)$
$2,3 \mid d, 4 \nmid d$	0	w(2d)	3w(4d)	$(q^2+q-26)w(48d)$	0	z(2d)	3z(4d)	$(q^2-q-26)z(48d)$
$3,4 \mid d$	w(2d)	w(2d)	w(2d)	$(q^2+q-26)w(48d)$	z(2d)	z(2d)	z(2d)	$(q^2-q-26)z(48d)$
$3,4 \nmid d$	0	0	0	qw(48d)z(1)	0	0	0	qw(48d)z(1)

Rank of G.

Case (a)

$$r = \frac{1}{24}[qw(48)z(1) + 27w(8) + 6w(8) + 8z(6)]$$
$$= \frac{q^3 + 261q - 134}{1152}.$$

Case (b)

$$r = \frac{1}{24}[qw(48)z(1) + 8w(6) + 27z(8) + 6z(8)]$$
$$= \frac{q^3 + 261q + 134}{1152}.$$

Case (c)

$$r = \frac{1}{24}[qw(48)z(1) + 27w(8) + 6w(8) + 8w(6)]$$
$$= \frac{q^3 + 261q - 262}{1152}.$$

Case (d)

$$r = \frac{1}{24}[qw(48)z(1) + 27z(8) + 6z(8) + 8z(6)]$$
$$= \frac{q^3 + 261q + 262}{1152}.$$

7) Representation on the cosets of $H \cong PSL(2,e)$, f/m an odd prime.

G contains subgroups H isomorphic to PSL(2,e) where $e=p^m$ if and only if m divides f. So far we know quite a lot about the structure of G and hence that of H to enable us to tackle the problem. Throughout this section, we take $q=e^h$, where h is an odd prime number.

(I) $g \epsilon \tau_1$

By Lemma 1.2.7, $|C^g|=w(k)z(1)$.

It is readily noticed that $|C^g \cap H| = \frac{1}{k}(e^2 - 1)$.

By Theorem 1.1.3, $\pi(g) = e^{h-1}$.

For $1 \leq l < p$, $|g^l|=p$ and hence $\pi(g^l) = e^{h-1}$.

Clearly $\alpha_l=0$ for $1 < l < p$.

Now

$$\alpha_p = \frac{qw(e(e^2-1)) - e^{h-1}}{p} = \frac{e^{h-1}(e^{2h}-e^2)}{p(e^2-1)} .$$

(II) $g \epsilon \tau_2$

Let x and y be elements of order w(k) and $\frac{e-1}{k}$ in τ_2

respectively. Supposing both x and y have the same fixed point set, then $C_{w(k)} = \langle x\rangle \supseteq \langle y\rangle = \langle x^{w(e-1)}\rangle = C_{\frac{1}{k}(e-1)}$.

Now let $g\in\tau_2$ with $|g|=d$. Up to conjugation by an element in G, we may assume that $g\in C_{w(k)}$. So $g=x^n$ for some $n\in\mathbb{N}$. If $\langle x^n\rangle = \langle x^u\rangle$, where u is the least positive power of x in this cyclic group, x^n and x^u have the same cycle structure on PG(1,q). Hence up to disjoint cycle decomposition we may assume $g=x^u$.

Now let $\langle x^u\rangle \cap \langle y\rangle = \langle x^j\rangle$, where j is the least positive power of x in this cyclic group (i.e the lcm of u and w(e-1)).

By Lemma 1.2.5 $|C^g| = \begin{cases} qz(2) & \text{if } d=2 \\ qz(1) & \text{if } d>2. \end{cases}$

We also have

$$|C^g \cap H| = \begin{cases} \frac{1}{2}e(e+1) & \text{if } u=j,\ d=2 \\ e(e+1) & \text{if } u=j,\ d>2 \\ 0 & \text{otherwise.} \end{cases}$$

So by Theorem 1.1.3,

$$\pi(g) = \begin{cases} w(e-1) & \text{if } u=j \\ 0 & \text{otherwise.} \end{cases}$$

Now if $j\neq w(k)$ and for $1 < l < d$, $\langle x^j\rangle \supseteq \langle g^l\rangle = \langle x^{ul}\rangle$ if and only if

$j|u\ell$. Thus

$$\pi(g^{\ell}) = \begin{cases} w(e-1) & \text{if } j|u\ell \\ 0 & \text{otherwise} \end{cases}$$

and if $i|\ell$, then

$$\pi(g^{\frac{\ell}{i}}) = \begin{cases} w(e-1) & \text{if } j|\frac{u\ell}{i} \\ 0 & \text{otherwise.} \end{cases} \quad . \qquad (1.2.8)$$

By the Remark 1.2.1, $\alpha_\ell=0$ if $j\nmid u\ell$.

Now suppose $j|u\ell$, we have

$$\begin{aligned}
\alpha_\ell &= \frac{1}{\ell}\sum_{i|\ell}\pi(g^{\ell|i})\,\mu(i) \\
&= \frac{1}{\ell}\sum_{i|\frac{u\ell}{j}}\pi(x^{\frac{u\ell}{i}})\,\mu(i) \qquad \text{--(by (1.2.8),} \\
&\qquad \text{the fact that } j|\frac{u\ell}{i} \Rightarrow i|\frac{u\ell}{j}) \\
&= \frac{1}{\ell}w(e-1)\sum_{i|\frac{u\ell}{j}}\mu(i) \\
&= \begin{cases} w(\ell[e-1]), & \text{if } \frac{u\ell}{j}=1 \\ 0 & \text{otherwise.} \end{cases}
\end{aligned}$$

If $j\neq w(k)$, then

$$\alpha_d = \frac{1}{d}[\pi(g^d) + w(e-1)\sum_{i|\frac{ud}{j}} \mu(i) - w(e-1)\mu(1)]$$
$$= \frac{1}{d}[e^{h-1}\frac{(e^{2h}-1)}{e^2-1} - w(e-1)]$$
$$= w(de(e^2-1))(e^{2h} + e^h - e^2 - e).$$

If j=w(k), then

$$\alpha_d = \frac{e^{h-1}(e^{2h}-1)}{d(e^2-1)} .$$

(III) $g \epsilon \tau_0$

Let x and y be elements of order z(k) and $\frac{e+1}{k}$ in τ_0 respectively. Suppose $C_{z(k)} = \langle x\rangle \supseteq \langle y\rangle = \langle x^{z(e+1)}\rangle = C_{\frac{1}{k}(e+1)}$.

If $g \epsilon \tau_0$ with $|g|=d$, we may assume that $g \epsilon C_{z(k)}$. So $g=x^n$ for some $n \epsilon \mathbb{N}$. Now let u be the least positive power of x such that $\langle x^n\rangle = \langle x^u\rangle$, and as we had before, take $g = x^u$. Let $\langle x^u\rangle \cap \langle y\rangle = \langle x^j\rangle$, where $j=[u, z(e+1)]$.

Now arguments same as those in (II) above give us:

$$\pi(g) = \begin{cases} z(e+1) & if\ u=j \\ 0 & otherwise. \end{cases}$$

For $1 < l < d$,

$$e_l = \begin{cases} z(l(e+1)) & \text{if } \frac{ul}{j} = 1 \\ 0 & \text{otherwise.} \end{cases}$$

If $j \neq z(k)$, then

$$\alpha_d = z(de(e^2-1))(e^{2h}-e^h-e^2+e) \ .$$

If $j = z(k)$, then

$$\alpha_d = \frac{e^{h-1}(e^{2h-1})}{d(e^2-1)} \ .$$

<u>Summary of the results.</u>

<u>(I) $g \in \tau_1$</u>

In all cases g' contains e^{h-1} 1-cycles and $\dfrac{e^{h-1}(e^{2h}-e^2)}{p(e^2-1)}$

p-cycles.

Results for $g \in \tau_2$ and τ_0 are displayed in the table below:

Table 1.2.11

	(II)		(III)	
	τ_2		τ_0	
CYCLE LENGTHS OF g'	l	d	l	d
No. OF CYCLES j≠w(k) or z(k), ul/j=1 j=w(k) or z(k)	 w(l(e-1)) 0	 * ***	 z(l(e+1)) 0	 ** ***

where, * represents $w(de(e^2-1))(e^{2h}+e^h-e^2-e)$;

** represents $z(de(e^2-1))(e^{2h}-e^h-e^2+e)$;

*** represents $\dfrac{e^{h-1}(e^{2h}-1)}{d(e^2-1)}$; and $1 \le i < d$.

Rank of G

(a) When e is even,

$$
\begin{aligned}
r &= \frac{1}{e(e^2-1)}\Big[e^{h-1}\frac{(e^{2h}-1)}{e^2-1}+(e^2-1)e^{h-1} \\
&\quad +e(e-2)(e+1)w(2(e-1))+e^2(e-1)z(2(e+1))\Big] \\
&= \frac{e^{3h-2}+e^{h+3}-e^{h+1}-3e^h-e^2+2e+1}{(e^2-1)^2}.
\end{aligned}
$$

(b) When e is odd,

$$
\begin{aligned}
r &= \frac{2}{e(e^2-1)}\Big[e^{h-1}\frac{(e^{2h}-1)}{e^2-1}+(e^2-1)e^{h-1} \\
&\quad +e(e-3)(e+1)w(4(e-1))+e(e^2-1)z(4(e+1))\Big] \\
&= \frac{2e^{3h-2}+e^{h+3}-e^{h+1}-6e^h-e^2+4e+1}{(e^2-1)^2}.
\end{aligned}
$$

8) Representation on the cosets of H≅PGL(2,e), f/m=2

An important feature of H (as compared to the PSL(2,e)) is that H contains maximal cyclic subgroups C_{e-1} and C_{e+1}, the former consisting of hyperbolic elements with the same fixed point set while the latter consists of fixed-points-free non-identity elements. We refer to the latter as a Singer cycle in H. A fixed point-free element in H belongs to a unique Singer cycle; any two Singer cycles are conjugate under an element in H. The same can be said about maximal cyclic subgroups C_{e-1}, that is any hyperbolic element belongs to a unique maximal cyclic subgroup C_{e-1} in H and any two of these are conjugate.

Since 2 divides $e\pm1$ when p is odd, H has two conjugacy classes of involutions; one lying entirely in PSL(2,e), the other in H\PSL(2,e).

We now have the following results:

Lemma 1.2.9

$$\left.\begin{array}{l} \text{The number of } C_2 \text{ in } PSL(2,q) \text{ is } \dfrac{e(e\pm1)}{2} \\ \text{The number of } C_2 \text{ in } H\backslash PSL(2,e) \text{ is } \dfrac{e(e\mp1)}{2} \end{array}\right\} \text{as } e \equiv \pm1 \bmod 4 .$$

We now compute the disjoint cycle structures of elements of G on the cosets of H. Here we take $q=e^2$.

(I) $g\epsilon\tau_1$.

(a) When e is even

By Lemma 1.2.7, $|C^g|=W(1)z(1)$ and $|C^g\cap H|=W(1)$.

By Theorem 1.1.3, $\pi(g)=e$.

Clearly g has to be an involution. Now g' contains the 2-cycles as the only non-trivial cycles.

We easily obtain, $\alpha_2 = \dfrac{e^3}{2}$.

(b) <u>When e is odd</u>

$|C^g|=w(2)z(1)$ and $|C^g \cap H|=w(1)$ or 0.

Now

$$\pi(g)=e \text{ or } 0.$$

Clearly

$$\alpha_p=ew(2p) \text{ or } ez(2p).$$

<u>(II) $g\epsilon\tau_2$</u>

Since $e+1|w(1)$, any elliptic element in H is hyperbolic in G. Elliptics in distinct maximal cyclic subgroups C_{e+1} in H are in distinct maximal cyclic subgroups $C_{w(1)}$ in G. Hyperbolics in H remain Hyperbolics in G.

Now we have:

(a) <u>When e is even</u>

$|C^g|=qz(1)$ and $|C^g \cap H|=e(e+1)$, $e(e-1)$ or 0. So that $\pi(g)=e+1$, $e-1$ or 0.

Now let x, y, s be elements of G with the same fixed point set such that $\langle x\rangle=C_{w(1)}$, $\langle y\rangle=C_{e-1}$ and $\langle s\rangle=C_{e+1}$. Up to conjugation by an element of G, we may assume that $g=x^n$, $n\epsilon N$. Let u be the least positive power of x such that $\langle x^n\rangle=\langle x^u\rangle$. Now up to disjoint cycle decomposition, we may assume that $g=x^u$.

Now suppose $\langle x^u\rangle \cap \langle y\rangle=\langle x^j\rangle$ and $\langle x^u\rangle \cap \langle s\rangle=\langle x^v\rangle$, where $j=[u,e+1]$ and $v=[u,e-1]$. We have

$$|C^g \cap H| = \begin{cases} e(e+1) & \text{if } u=j \\ e(e-1) & \text{if } u=v \\ 0 & \text{otherwise.} \end{cases}$$

Hence

$$\pi(g) = \begin{cases} e+1 & \text{if } u = j \\ e-1 & \text{if } u = v \\ 0 & \text{otherwise.} \end{cases}$$

If v=w(1) and j≠w(1), then as we had in part 7), there exists an ℓ, $1 \leq \ell < d$ such that $u\ell/j=1$ and

$$\alpha_\ell = \frac{e+1}{\ell}$$
$$\alpha_d = \frac{e^3-1}{d}.$$

If j=w(1) and v≠w(1), we find in the same way as before that there exists $1 \leq h < d$ such that $uh/v=1$ and

$$\alpha_h = \frac{e-1}{h},$$
$$\alpha_d = \frac{e^3+1}{d}.$$

If v,j ≠w(1), then there exists ℓ and h, $1 \leq \ell, h < d$ such that

$\dfrac{u\ell}{j} = \dfrac{h}{v} = 1$ and

$$\alpha_l = \frac{e+1}{l},$$
$$\alpha_h = \frac{e-1}{h},$$
$$\alpha_d = ew(d).$$

Note that the case v=j=w(1) does not occur since $d|w(1)$ implies d has factors in one or both e-1 and e+1.

(b) <u>When e is odd</u>

With u as we had in (a), j and v become [u,e+1/2] and [u,e-1/2] respectively. We now have

$$|C^g| = \begin{cases} qw(2) & \text{if } d=2 \\ qw(1) & \text{if } d>2 \end{cases}$$

and

$$|C^g \cap H| = \begin{cases} e(e+1) & \text{if } d>2, u=j \\ e(e-1) & \text{if } d>2, u=v \\ 2q & \text{if } d=2, u=j=v=w(4) \\ 0 & \text{otherwise.} \end{cases}$$

Hence

$$\pi(g) = \begin{cases} \dfrac{e+1}{2} & \text{if } d>2, u=j \\ \dfrac{e-1}{2} & \text{if } d>2, u=v \\ e & \text{if } d=2, u=j=v=w(4) \\ 0 & \text{otherwise.} \end{cases}$$

If d=2, then u=j=v=w(4),

$$\alpha_1 = e$$

and

$$\alpha_2 = ew(4).$$

If d>2, $j \neq w(2)$, v=w(2), we have

$$\alpha_\ell = \frac{e+1}{2\ell}, \quad where \ \frac{u\ell}{j} = 1$$

and

$$\alpha_d = \frac{e^3-1}{2d}.$$

Similarly if d>2, $v \neq w(2)$, j=w(2), we have

$$\alpha_h = \frac{e-1}{2h}, \qquad \frac{uh}{v} = 1$$

and

$$\alpha_d = \frac{e^3+1}{2d}.$$

If d>2, v,j $\neq w(2)$, we have the following 3 cases:

(i) j < w(4), v = w(4) (ii) v < w(4), j = w(4),

(iii) j,v < w(4).

Now the cycle lengths of g' are as follows:

(i) $\alpha_{\ell} = \frac{e+1}{2\ell}$, where $\frac{u\ell}{j} = 1$; $\alpha_{d/2} = \frac{e-1}{d}$; and $\alpha_d = ew(2d)$.

(ii) $\alpha_h = \frac{e-1}{2h}$, where $\frac{uh}{v} = 1$; $\alpha_{d/2} = \frac{e+1}{d}$; and $\alpha_d = ew(2d)$.

(iii)
$$\alpha_{\ell} = \frac{e+1}{2\ell}, \text{ where } \frac{u\ell}{j} = 1;$$
$$\alpha_h = \frac{e-1}{2h}, \text{ where } \frac{uh}{v} = 1;$$
$$\alpha_{\frac{d}{2}} = 0; \text{ and } \alpha_d = ew(2d).$$

Again here the case v=j=w(2) does not arise.

<u>(III) $g\epsilon\tau_0$</u>

From the discussion we had in the opening pages of this part, we notice that $|C^g \cap H|=0$. Clearly g' contains only the ez(2d) d-cycles.

<u>Summary of the results.</u>

<u>(I) $g\epsilon\tau_1$</u>

If e is even, g' contains e 1-cycles and $\frac{e^3}{2}$ 2-cycles.

If e is odd, g'contains e 1-cycles and ew(2p) p-cycles, or ez(2p) p-cycles.

(II) $g \in \tau_2$

If e is odd, d=2, u=v=j=w(4), g' contains e 1-cycles and ew(4) 2-cycles.

Results for all the other cases are given in the table below.

(III) $g \in \tau_0$

Always g' contains ez(2d) d-cycles.

Table 1.2.12

	(II)			
	τ_2			
CYCLE LENGTHS OF g'	l	h	$d/2$	d
No. OF CYCLES				
e even				
$v=w(1), j\neq w(1), ul/j=1$	$(e+1)/l$	0	0	$(e^3-1)/d$
$j=w(1), v\neq w(1), ul/v=1$	0	$(e-1)/h$	0	$(e^3+1)/d$
$v, j\neq w(1), ul/j=uh/v=1$	$(e+1)/l$	$(e-1)/h$	0	$ew(d)$
e odd				
$d>2, j\neq w(2), v=w(2), ul/j=1$	$(e+1)/2l$	0	0	$(e^3-1)/2d$
$d>2, v\neq w(2), j=w(2), uh/v=1$	0	$(e-1)/2h$	0	$(e^3+1)/2d$
$d>2, j<d/2, v=d/2, ul/j=1$	$(e+1)/2l$	0	$(e-1)/d$	$ew(2d)$
$d>2, v<d/2, j=d/2, uh/v=1$	0	$(e-1)/2h$	$(e+1)/d$	$ew(2d)$
$d>2, v, j<d/2, ul/j=uh/v=1$	$(e+1)/2l$	$(e-1)/2h$	0	$ew(2d)$

Rank of G

e even

$$r = \frac{1}{ew(1)}\left[ew(1) + \frac{e}{2}(e+1)^2(e-2) + \frac{q}{2}(e-1)^2 + ez(1)\right]$$
$$= e+1.$$

e odd

$$r = \frac{1}{ew(1)}\left[qz(2) + e^3 + ew(1) + e\left(\frac{e+1}{2}\right)^2(e-3) + \frac{e}{4}(e-1)^3\right]$$
$$= \frac{e+3}{2}.$$

1.3 Primitive permutation representations of G=PGL(2,q)

As we noted in section 1.1; when q is even, PGL(2,q) $\cong$ PSL(2,q). Since this case was dealt with in section 1.2, throughout this section q is taken to be odd.

We start by having a brief look at the

Finite subgroups of G.

The structure of G can easily be deduced from that of its subgroup PSL(2,q) of index 2 (and from that of the group PSL($2,q^2$) in which G may be imbedded). G has the following types of finite subgroups (see [23]):

(i) cyclic groups C_n, where $n|q\pm1$;

(ii) elementary abelian p-groups, P_e;

(iii) dihedral groups D_{2n}, where $n|q\pm1$;

(iv) semi-direct products $S_{e,n}=P_e \rtimes C_n$, $n|w(1)$;

(v) the alternating groups A_4 and A_5;

(vi) the symmetric groups S_4;

(vii) PSL(2,e) and PGL(2,e).

The subgroups A_4, A_5, S_4 all occur in G simply in their role of subgroups of PSL(2,q) (see § 1.2), except if $q\equiv\pm3$ mod 8 when G contains a single conjugacy class of $|G|/24$ subgroups of type S_4 which does not lie in PSL(2,q).

G contains subgroups $C_{w(1)}$ and $C_{z(1)}$ (see part 8) of § 1.2) whose normalizers are $D_{2w(1)}$ and $D_{2z(1)}$ respectively.

The non-identity elements of a Sylow p-subgroup P_q of G have a unique fixed point and each pair of distinct conjugates

of P_q intersect trivially. The normalizer of P_q in G is the stabilizer of a point $S_{q,w(1)} = P_q \rtimes C_{w(1)}$.
If we define $\tau_i = \{g | g \in G, \pi(g)=i\}$, each non-identity element of G is seen to lie in one set of the partition

$$\tau_0 = \bigcup_{g\in G}(C_{z(1)} - I)^g, \quad \tau_1 = \bigcup_{g\in G}(P_q - I)^g, \quad \tau_2 = \bigcup_{g\in G}(C_{w(1)} - I)^g$$

of G.

From the list of subgroups of G given above, a subgroup H of G is seen to be maximal if it is isomorphic to one of the following groups:

1) the stabilizer of a point $S_{q,w(1)}$;
2) the dihedral group $D_{2w(1)}$;
3) the dihedral group $D_{2z(1)}$;
4) the symmetric group S_4 when $q=p\neq 3$, $q\equiv\pm 3 \bmod 8$;
5) PSL(2,q);
6) PGL(2,e), f/m a prime number.

G contains a single conjugacy class of each of the maximal subgroups given above. Except for the case when $H\cong PSL(2,q)$ when the length of the conjugacy class of H is $|G|/2|H|$, all the other conjugacy classes are of length $|G|/|H|$.

We now compute the disjoint cycle structures of elements of G and the rank of G on the right cosets of each of its maximal subgroups H. As we did in section 1.2, we shall each time be taking an element g of order d in G from the sets τ_1,

τ_2 and τ_0 respectively.

1) Representation on the cosets of $H \cong S_{q,w(1)}$

By Theorem 1.1.2, the action of G on the cosets of H is equivalent to its natural action on PG(1,q) of degree z(1).

The disjoint cycle structure of g' is as we have below:

Table 1.3.1

	τ_1		τ_2		τ_0
CYCLE LENGTHS OF g'	1	p	1	d	d
NO. OF CYCLES	1	p^{f-1}	2	w(d)	z(d)

Since G is triply transitive on PG(1,q), its rank is 2.

2) Representation on the cosets of $H \cong D_{2w(1)}$

By using the results on the pair group action in section 1.1, the disjoint cycle structure of g' is as follows:

(I) $g \in \tau_1$ In all cases g' contains $z(2)p^{f-1}$ p-cycles.

Table 1.3.2

	(II) τ_2			(III) τ_0	
CYCLE LENGTHS OF g'	1	½d	d	½d	d
NO. OF CYCLES					
d even	1	w(d)	w(2d)z(1)	z(d)	w(2d)z(1)
d odd	1	0	w(2d)z(1)	0	qz(2d)

By using the Cauchy-Frobenius Formula, we calculate the rank(r) of G as follows:

From Table 1.3.2, elements of H have fixed points as follows:

The identity fixes qz(2) cosets.

There are q involutions each fixing z(2) cosets and q-3 elements of order greater than two each fixing a single coset.

Hence

$$r = \frac{1}{2w(1)}[qz(2) + qz(2) + (q-3)] = \frac{q+3}{2}.$$

3) Representation on the cosets of $H \cong D_{2z(1)}$

Let $C_{z(1)}$ be the maximal cyclic subgroup of H. The z(1) involutions in $H\backslash C_{z(1)}$ lie in two conjugacy classes of z(2) elements in H; one lying entirely in PSL(2,q), the other entirely in G\PSL(2,q). If $\langle s\rangle = C_{z(1)}$, then the conjugacy class containing s^j, $j \in N$ in H is $\{s^j, s^{-j}\}$. In particular H contains a singleton conjugacy class containing an involution in $C_{z(1)}$.

The conjugacy classes of involutions in G were discussed in part 8) of section 1.2. If d > 2, then $|C^g|$ in G is

$$\begin{cases} qz(1) & if\ g \in \tau_2 \\ qw(1) & if\ g \in \tau_0 \\ w(1)z(1) & if\ g \in \tau_1 \end{cases}$$

and $|C^g \cap C_{z(1)}|$ is

$$\begin{cases} 0 & if\ g \in \tau_2 \text{ or } \tau_1 \\ 2 & if\ g \in \tau_0. \end{cases}$$

Now from the information given above, we have:

If d=2, then

$$|C^g \cap H| = \begin{cases} z(2) & \text{if } g \in \tau_2 \\ \dfrac{q+3}{2} & \text{if } g \in \tau_0 \\ 0 & \text{if } g \in \tau_1. \end{cases}$$

If d > 2, then

$$|C^g \cap H| = \begin{cases} 0 & \text{if } g \in \tau_2 \text{ or } \tau_1 \\ 2 & \text{if } g \in \tau_0. \end{cases}$$

The table giving the values of $\pi(g)$ is as follows:

Table 1.3.3

	$\lvert C^g\rvert$	$\lvert C^g \cap H\rvert$	$\pi(g)$
(I) $g \in \tau_1$	$w(1)z(1)$	0	0
(II) $g \in \tau_1$, d=2 d≠2	$qz(2)$ $qz(1)$	$z(2)$ 0	$w(2)$ 0
(III) $g \in \tau_0$, d=2	$qw(2)$	$\frac{q+3}{2}$	$\frac{q+3}{2}$
d≠2	$qw(1)$	2	1

By using arguments similar to those in parts 3) - 8) of section 1.2, the disjoint cycle structure of g' is as follows:

(I) $g \in \tau_1$ In all cases g' contains $w(2)p^{f-1}$ p-cycles.

Table 1.3.4

	(II)		(III)		
	τ_2		τ_0		
CYCLE LENGTHS OF g'	d/2	d	1	d/2	d
NO. OF CYCLES d even	w(d)	w(2d)w(1)	1	z(d)	(q-3)z(2d)
d odd	0	qw(2d)	1	0	(q-2)z(2d)

Rank of G

$$
\begin{aligned}
r &= \frac{1}{2z(1)}\left[qw(2) + w(2)z(2) + \left(\frac{q+3}{2}\right)^2 + w(1)\right] \\
&= z(2).
\end{aligned}
$$

4) Representation on the cosets of $H \cong S_4$

G contains subgroups H isomorphic to S_4 if and only if $q\equiv\pm1$ mod 8 or $q\equiv\pm3$ mod 8, in which case there is a single conjugacy class of length $|G|/24$. If $q\equiv\pm1$ mod 8, this conjugacy class splits into two classes of equal lengths in PSL(2,q) (see § 1.2). If $q\equiv\pm3$ mod 8, PSL(2,q) does not contain a subgroup isomorphic S_4.

Since H is not maximal when $q\equiv\pm1$ mod 8, our discussion will be on the case when $p\neq3$, $q\equiv\pm3$ mod 8.

Conjugacy classes of elements of H were discussed in part 6) of section 1.2.

Conjugacy classes of involutions of G were discussed in part 8) of section 1.2.

If p=3 there is a single conjugacy class of elements of order 3 in G containing G/q elements. If $p \neq 3$, there is a single conjugacy class containing $q(q+\delta)$ elements of order 3, where

$$\delta = \begin{cases} 1 & if\ q \equiv 1 \bmod 3 \\ -1 & if\ q \equiv -1 \bmod 3. \end{cases}$$

G contains elements of order 4 if and only if $q \equiv \pm 1 \bmod 4$, in which case they form a single conjugacy class of $q(q+\epsilon)$ elements, where

$$\epsilon = \begin{cases} 1 & if\ q \equiv 1 \bmod 4 \\ -1 & if\ q \equiv -1 \bmod 4. \end{cases}$$

From the information given above, we have:

If d=2 and $q \equiv 1 \bmod 4$, then

$$| C^g \cap H | = \begin{cases} 3 & if\ g \in \tau_2 \\ 6 & if\ g \in \tau_0. \end{cases}$$

If d=2 and $q \equiv -1 \bmod 4$, then

$$| C^g \cap H | = \begin{cases} 6 & if\ g \in \tau_2 \\ 3 & if\ g \in \tau_0. \end{cases}$$

If d=3, then

$$| C^g \cap H | = 8.$$

If d=4, then

$$| C^g \cap H | = 6 .$$

Now the following are the cases to consider:

(a) $q \equiv 7 \bmod 12$ and $q \equiv \pm 3 \bmod 8$

(b) $q \equiv 5 \bmod 12$ and $q \equiv \pm 3 \bmod 8$

(c) $q \equiv 1 \bmod 12$ and $q \equiv \pm 3 \bmod 8$

(d) $q \equiv -1 \bmod 12$ and $q \equiv \pm 3 \bmod 8$.

Values for $\pi(g)$ are presented in the table below:

Table 1.3.5

	$\lvert C^g \rvert$	$\lvert C^g \cap H \rvert$	$\pi(g)$
(I) $g \in T_1$	$w(1)z(1)$	0	0
(II) $g \in T_2$			
Cases (a) and (d), d=2	$qz(2)$	6	$w(2)$
Cases (a) and (c), d=3	$qz(1)$	8	$w(3)$
Cases (b) and (c), d=2	$qz(2)$	3	$w(4)$
Cases (b) and (c), d=4	$qz(1)$	6	$w(4)$
Cases (a)-(d), $d \neq 2,3,4$	$qz(1)$	0	0
(III) $g \in T_0$			
Cases (a) and (d), d=2	$qw(2)$	3	$z(4)$
Cases (b) and (c), d=2	$qw(2)$	6	$z(2)$
Cases (b) and (d), d=3	$qw(1)$	8	$z(3)$
Cases (a) and (d), d=4	$qw(1)$	6	$z(4)$
Cases (a)-(d), $d \neq 2,3,4$	$qw(1)$	0	0

By using arguments similar to those in parts 3) - 8) of section 1.2, the disjoint cycle structure of g' is as follows:

(I) $g \in \tau_1$ In all cases g' contains $qw(24p)z(1)$ p-cycles.

Table 1.3.6

	(II)				(III)			
	τ_2				τ_0			
CYCLE LENGTHS OF g'	d/4	d/3	d/2	d	d/4	d/3	d/2	d
NO. OF CYCLES								
Cases (a) and (d)								
$2 \mid d,\ 3,\ 4 \nmid d$	0	0	$w(d)$	$(q-3)(q+4)w(24d)$	0	0	$z(2d)$	$(q-3)(q+2)z(24d)$
$3 \mid d,\ 2 \nmid d$	0	$w(d)$	0	$(q^2+q-8)w(24d)$	0	$z(d)$	0	$(q^2-q-8)z(24d)$
$4 \mid d,\ 3 \nmid d$	0	0	0	0	$z(d)$	0	0	$(q-3)(q+2)z(24d)$
$2,\ 3, \mid d, 4 \nmid d$	0	$w(d)$	$w(d)$	$(q+5)(q-4)w(24d)$	0	$z(d)$	$z(2d)$	$(q^2-q-14)z(24d)$
$3,\ 4 \mid d$	0	0	0	0	$z(d)$	$z(d)$	0	$(q^2-q-14)z(24d)$
$2,\ 3 \nmid d$	0	0	0	$qw(24d)z(1)$	0	0	0	$qw(24d)z(1)$
Cases (b) and (c)								
$2 \mid d,\ 3,\ 4 \nmid d$	0	0	$w(2d)$	$(q+3)(q-2)w(24d)$	0	0	$z(d)$	$(q+3)(q-4)z(24d)$
$3 \mid d,\ 2 \nmid d$	0	$w(d)$	0	$(q^2+q-8)w(24d)$	0	$z(d)$	0	$(q^2-q-8)z(24d)$
$4 \mid d,\ 3 \nmid d$	$w(d)$	0	0	$(q+3)(q-2)w(24d)$	0	0	0	0
$2,\ 3, \mid d, 4 \nmid d$	0	$w(d)$	$w(2d)$	$(q^2+q-14)w(24d)$	0	$z(d)$	$z(d)$	$(q+4)(q-5)z(24d)$
$3,\ 4 \mid d$	$w(d)$	$w(d)$	0	$(q^2+q-14)w(24d)$	0	0	0	0
$2,\ 3 \nmid d$	0	0	0	$qw(24d)z(1)$	0	0	0	$qw(24d)z(1)$

Rank of G

Case (a)

$$r = \frac{1}{24}[qw(24)z(1) + 6w(2) + 8w(3) + 3z(4) + 6z(4)]$$
$$= \frac{q^3 + 189q - 82}{576}.$$

Case (b)

$$r = \frac{1}{24}[qw(24)z(1) + 3w(4) + 6w(4) + 6z(2) + 8z(3)]$$
$$= \frac{q^3 + 189q + 82}{576}.$$

Case (c)

$$r = \frac{1}{24}[qw(24)z(1) + 3w(4) + 6w(4) + 8w(3) + 6z(2)]$$
$$= \frac{q^3 + 189q - 46}{576}.$$

Case (d)

$$r = \frac{1}{24}[qw(24)z(1) + 6w(2) + 3z(4) + 6z(4) + 8z(3)]$$
$$= \frac{q^3 + 189q + 46}{576}.$$

5) Representation on the cosets of $H \cong PSL(2,q)$

Since $|G:H|=2$, then (i) g' is the identity if $g \in H$ (ii) g' is a cycle of length 2 if $g \in G\backslash H$. The rank of G is 2.

6) Representation on the cosets of $H \cong PGL(2,e)$, f/m an odd prime

G contains subgroups H isomorphic to PGL(2,e) if and only if $m|f$. We shall take $q = e^h$, where h is a prime.

(I) $g \in \tau_1$

We have $|C^g| = w(1)z(1)$ and $|C^g \cap H| = e^2 - 1$.

Hence

$$\pi(g) = e^{h-1}.$$

Clearly a non-trivial cycle in g' is of length p.

Hence

$$\alpha_p = \frac{e^{h-1}(e^{2h}-e^2)}{p(e^2-1)}.$$

(II) $g \in \tau_2$

Let x and y be elements of τ_2 with the same fixed point set and orders w(1) and e-1 respectively.

Let $g = x^u$ and $\langle x^u \rangle \cap \langle y \rangle = \langle x^j \rangle$, where u and j are taken as in the corresponding stage of part 7) of section 1.2.

We have

$$|C^g| = \begin{cases} qz(2) & \text{if } d=2 \\ qz(1) & \text{if } d>2 \end{cases}$$

and

$$|C^g \cap H| = \begin{cases} \dfrac{e(e+1)}{2} & \text{if } u=j,\ d=2 \\ e(e+1) & \text{if } u=j,\ d>2 \\ 0 & \text{otherwise.} \end{cases}$$

Hence

$$\pi(g) = \begin{cases} w(e-1) & \text{if } u=j \\ 0 & \text{otherwise.} \end{cases}$$

Arguments similar to the ones in part 7) of section 1.2 give us:

For $1 \leq l < d$ and $j \neq w(1)$, g' contains cycles of lengths l and d with,

$$\alpha_l = w(l(e-1)), \text{ where } ul/j=1$$

and

$$\alpha_d = w(de(e^2-1))(e^{2h}+e^h-e^2-e).$$

If $j=w(1)$, then g' contains only the d-cycles with,

$$\alpha_d = \frac{e^{h-1}(e^{2h}-1)}{d(e^2-1)}.$$

(III) $g \in \tau_0$

Let x and y be elements of order z(1) and e+1 in τ_0 respectively. Suppose $C_{z(1)} = \langle x\rangle \supseteq \langle y\rangle = C_{e+1}$.

Let $g = x^u$ and $\langle x^u\rangle \cap \langle y\rangle = \langle x^j\rangle$, where u and j are taken as in the corresponding stage of part 7) of section 1.2.

Now arguments similar to the ones in part 7) of section 1.2 give us:

For $1 \leq l < d$ and $j \neq z(1)$, g' contains cycles of lengths l and d with,

$$\alpha_l = z(l(e+1)), \text{ where } ul/j=1$$

and

$$\alpha_d = z(de(e^2-1))(e^{2h}-e^h-e^2+e).$$

If $j=z(1)$, then g' contains only the d-cycles with,

$$\alpha_d = \frac{e^{h-1}(e^{2h}-1)}{d(e^2-1)}.$$

Summary of the results.

(I) $g \in \tau_1$

Always g' contains e^{h-1} 1-cycles and $\frac{e^{h-1}(e^{2h}-e^2)}{p(e^2-1)}$ p-cycles.

Results for $g \in \tau_2$ and $g \in \tau_0$ are displayed in the table below:

Table 1.3.7

	(II)		(III)	
	τ_2		τ_0	
CYCLE OF LENGTHS OF g'	l	d	l	d
NO. OF CYCLES				
$j \neq w(1)$ or $z(1)$, $ul/j=1$	$w(l(e-1))$	*	$z(l(e+1))$	**
$j=w(1)$ or $z(1)$	0	***	0	***

where, * represents $w(de(e^2-1))(e^{2h}+e^h-e^2-e)$,

** represents $z(de(e^2-1))(e^{2h}-e^h-e^2+e)$,

*** represents $\frac{e^{h-1}(e^{2h}-1)}{d(e^2-1)}$

and $1 \leq l < d$.

Rank of G

$$r = \frac{1}{e(e^2-1)}\left[\frac{e^{h-1}(e^{2h}-1)}{e^2-1} + e^{h-1}(e^2-1) + e(e-2)(e+1)w(2(e-1))\right.$$
$$\left. + \frac{e^2}{2}(e-1)z(e+1)\right]$$
$$= \frac{e^{3h-2} + e^{h+3} - e^{h+1} - 3e^{h} - e^2 + 2e+1}{(e^2-1)^2}.$$

1.4 The explicit cycle index formulas for primitive permutation representations of G = PSL (2,q) or PGL(2,q).

After having computed the disjoint cycle structures for elements of PSL(2,q) and PGL(2,q) for any primitive permutation representation of these two groups (see sections 1.2 and 1.3), the problem of finding the cycle index formulas for these representations becomes quite straightforward.

In this section we shall sketch some general formulas for the cycle indices of these representations and then give the cycle indices of

1) representation of PSL(2,q) on the cosets of $S_{q,w(k)}$ in part 1) of section 1.2,
2) representation of PSL(2,q) on the cosets of A_4 in part 4) of section 1.2,
3) representation of PGL(2,q) on the cosets of

PGL(2,e) in part 6) of section 1.3

as examples. Computation of cycle index formulas for the other representations is very similar.

We start by giving a simple result by Redfield [17].

<u>Theorem 1.4.1</u> The cycle index of the regular representation of the cylic group C_n is given by

$$\mathfrak{Z}(C_n) = \frac{1}{n} \sum_{d|n} \phi(d)\ t_d^{n/d},$$

where ϕ is the Euler ϕ-function.

In what follows, t_1, t_2,.... are distinct (commuting) indeterminates and as we had before, for any $g \in G$, g' will represent the permutation induced by g in a given permutation representation of G.

<u>Theorem 1.4.2</u> The cycle index of G = PGL(2,q) on the cosets of its maximal subgroup H is

$$\mathfrak{Z}(G) = \frac{1}{|G|}\ [t_1^{|G|/|H|} + (q^2-1)\ mon(x') + qz(2) \sum [mon(g')\ |g \in C_{w(1)} \setminus I] + qw(2) \sum [mon(g')\ |\ g \in C_{z(1)} \setminus I]],$$

where $x \in \tau_1$.

<u>Proof</u>

The identity contributes $t_1^{|G|/|H|}$ to the sum of the monomials.

All the q^2-1 parabolics lie in the same conjugacy class. Hence they all have the same monomial. Thus the parabolics contribute $(q^2-1)\mathrm{mon}(x')$, $x \in \tau_1$ to the sum of the monomials.

Each $g \in \tau_2$ is contained in a unique cyclic group $C_{w(1)}$ and there are in total qz(2) conjugates of $C_{w(1)}$. Hence the contribution by elements of τ_2 to the total sum of monomials is $qz(2) \sum [mon(g') \mid g \in C_{w(1)} \setminus I]$.

Each $g \in \tau_0$ is contained in a unique cyclic group $C_{z(1)}$ and there are in total qw(2) conjugates of $C_{z(1)}$. Hence the contribution by elements of τ_0 to sum of monomials is

$$qw(2) \sum [mon(g') \mid g \in C_{z(1)} \setminus I] \ .$$

Now adding all the contributions and dividing by the order of G we get the result. □

<u>Theorem 1.4.3</u> The cycle index of G = PSL(2,q), q odd, on the cosets of its maximal subgroup H is one of the following:

$$\begin{aligned}(a)\ \mathfrak{Z}(G) = \frac{1}{|G|}\ [\, & t_1^{|G|/|H|} + (q^2-1)\,mon(x') \\ & + qz(2) \sum [mon(g') \mid g \in C_{w(2)} \setminus I] \\ & + qw(2) \sum [mon(g') \mid g \in C_{z(2)} \setminus I]\,],\end{aligned}$$

if H has two conjugacy classes of elements of order p in G, or if H contains no elements of order p; where x ϵ τ_1.

$$(b)\quad \mathfrak{Z}(G) = \frac{1}{|G|}\ [t_1^{|G|/|H|} + \frac{1}{2}(q^2-1)\,mon(x_1') + \frac{1}{2}(q^2-1)\,mon(x_2') + $$
$$+\ qw(2)\sum [mon(g')\,|g \in C_{z(2)}\setminus I] + qz(2)\sum [mon(g')\,|g\in C_{w(2)}\setminus I]]$$

if H has a single conjugacy class of elements of order p in G; where x_1 and x_2 are parabolics each from one of the two conjugacy classes containing the parabolics in G.

Proof

In principle the proof is similar to that of Theorem 1.4.2 except that unlike in Theorem 1.4.2, the q^2-1 parabolics lie in two conjugacy classes of the same length in G.

(a) If H has two conjugacy classes of elements of order p in G, these conjugacy classes are of equal lengths as is evident from section 1.2. Hence the q^2-1 parabolics have the same number of fixed points in this representation. It can also be clearly noticed that the q^2-1 parabolics have the same monomial. If H has no element of order p, then the q^2-1 parabolics in G have no fixed points in this representation. It can also be shown that the parabolics have the same monomial. Hence in both cases we get formula (a).

(b) If H has a single conjugacy class of elements of order p in G, then all the elements of order p in H lie in one of the two conjugacy classes of parabolics in G. Hence in this representation half of the parabolic elements have fixed points (same number), while the other half have none. Evidently we have two different types of monomials with half of the parabolics sharing each, hence formula (b). □

Examples

1) Cycle index of $G = PSL(2,q)$ on the cosets of $S_{q,w(k)}$

From Theorems 1.4.1, 1.4.2, 1.4.3(a) and the results in Table 1.2.1 we have:

Contribution to the sum of monomials by the identity element is $t_1^{z(1)}$.

Contribution by elements of τ_1 is $(q^2-1)\, t_1\, t_p^{p^{f-1}}$.

Contribution by elements of τ_2 is $q\, z(2) \sum_{1 \neq d | w(k)} \phi(d)\ t_1^2\ t_d^{w(d)}$.

Contribution by elements of τ_0 is $qw(2) \sum_{1 \neq d | z(k)} \phi(d)\, t_d^{z(d)}$.

Now adding all the above contributions and dividing by $|G|$ we have,

$$\mathcal{Z}(G) = \frac{1}{|G|}\Big[t_1^{z(1)} + (q^2-1)\, t_1 t_p^{p^{f-1}} + qz(2) \sum_{1 \neq d | w(k)} \phi(d)\ t_1^2\ t_d^{w(d)} + qw(2) \sum_{1 \neq d | z(k)} \phi(d)\, t_d^{z(d)}\Big].$$

2) Cycle index of G = PSL(2,q) on the cosets of A_4 with q≡1 mod 12.

From Theorems 1.4.1, 1.4.3(a) and the results in part 4) of section 1.2, we have:

Contribution to the sum of monomials by the identity element is $t_1^{qw(24)z(1)}$.

Contribution by elements of τ_1 is $(q^2-1)\, t_p^{qw(24p)z(1)}$.

We have four different types of monomials for elements of τ_2,

(i) $t_{d/2}^{w(2d)} \quad t_d^{(q+3)(q-2)w(24d)} \qquad if \quad 3\nmid d, \quad 2|d|w(2)$

(ii) $t_{d/3}^{w(d)} \quad t_d^{(q^2+q-8)w(24d)} \qquad if \quad 2\nmid d, \quad 3|d|w(2)$

(iii) $t_{d/2}^{w(2d)} \; t_{d/3}^{w(d)} \quad t_d^{(q^2+q-14)w(24d)} \qquad if \quad 2,3|d|w(2)$

(iv) $t_d^{q\,w(24d)z(1)} \qquad if \qquad 2,3 \nmid d|w(2) \;, \; d \neq 1.$

Hence elements of τ_2 contribute

$$qz(2)\Big[\sum_{\substack{2|d|w(2)\\(3\nmid d)}} \phi(d)\, t_{d/2}^{w(2d)}\ t_d^{(q+3)(q-2)\ w(2d)} + \sum_{\substack{3|d|w(2)\\(2\nmid d)}} \phi(d)\ t_{d/3}^{w(d)}\, t_d^{(q^2+q-8)\,w(24d)} + \sum_{2,3|d|w(2)} \phi(d)\ t_{d/2}^{w(2d)}\, t_{d/3}^{w(d)}\, t_d^{(q^2+q-14)\,w(24d)} + \sum_{\substack{2,3\nmid d\\ d\neq 1}} \phi(d)\, t_d^{qw(24d)\,z(1)}\Big].$$

We also have four different types of monomials for elements of τ_0

(i) $t_{d/2}^{z(2d)}\ t_d^{(q-3)(q+2)\,z(24d)}$ *if* $3\nmid d,\ 2|d|z(2)$

(ii) $t_{d/3}^{z(d)}\ t_d^{(q^2-q-8)\,z(24d)}$ *if* $2\nmid d,\ 3|d|z(2)$

(iii) $t_{d/3}^{z(2d)}\ t_{d/2}^{z(2d)}\ t_d^{(q^2-q-14)\,z(24d)}$ *if* $2,3|d|z(2)$

(iv) $t_d^{q\ w(24d)\,z(1)}$ *if* $2,3\nmid d|z(2), d\neq 1$.

Hence elements of τ_0 contribute

$$qw(2)\,[\sum_{\substack{2|d|z(2)\\(3\nmid z(2))}} \phi(d)\, t_{d/2}^{z(2d)}\; t_d^{(q-3)(q+2)\; z(24d)}$$
$$+ \sum_{\substack{3|d|z(2)\\(2\nmid d)}} \phi(d)\; t_{d/3}^{z(d)}\, t_d^{(q^2-q-8)\,z(24d)}$$
$$+ \sum_{2,3|d|z(2)} \phi(d)\; t_{d/3}^{z(d)}\, t_{d/2}^{z(2d)}\, t_d^{(q^2-q-14)\,z(24d)} + \sum_{\substack{2,3\nmid d\\(d\neq 1)}} t_d^{qw(24d)\,z(1)}\,]\,.$$

Adding all the above contributions and dividing by $|G|$ we get,

$$\mathcal{Z}(G) = \frac{1}{|G|}\,[qw(24)\,z(1) + (q^2-1)\,t_p^{qw(24p)\,z(1)}$$
$$+ qz(2) \sum_{\substack{2|d|w(2)\\(3\nmid d)}} \phi(d)\, t_{d/2}^{w(2d)}\; t_d^{(q+3)(q-2)\; w(24d)}$$
$$+ qz(2) \sum_{\substack{3|d|w(2)\\(2\nmid d)}} \phi(d)\; t_{d/3}^{w(d)}\, t_d^{(q^2+q-8)\,w(24d)}$$
$$+ qz(2) \sum_{2,3|d|w(2)} \phi(d)\; t_{d/2}^{w(2d)}\, t_{d/3}^{w(d)}\, t_d^{(q^2+q-14)\,w(24d)}$$
$$+ qz(2) \sum_{\substack{2,3\nmid d|w(2)\\(d\neq 1)}} \phi(d)\, t_d^{qw(24d)\,z(1)}$$
$$+ qw(2) \sum_{\substack{2|d|z(2)\\(3\nmid d)}} \phi(d)\, t_{d/2}^{z(2d)}\, t_d^{(q-3)(q+2)\,z(24d)}$$
$$+ qw(2) \sum_{\substack{3|d|z(2)\\2\nmid d}} \phi(d)\, t_{d/3}^{z(d)}\, t_d^{(q^2-q-8)\,z(24d)}$$
$$+ \sum_{2,3|d|z(2)} \phi(d)\, t_{d/3}^{z(d)}\, t_{d/2}^{z(2d)}\, t_d^{(q^2-q-14)\,z(24d)}$$
$$+ \sum_{\substack{2,3\nmid d\\(d\neq 1)}} t_d^{qw(24d)\,z(1)}\,]\,.$$

3) Cycle index of G = PGL(2,q) on the cosets of PGL(2,e)

From Theorems 1.4.1, 1.4.2 and the results in part 6) of section 1.3, we have:

Contribution to the sum of monomials by the identity element is $t_1^{\frac{|G|}{|H|}}$.

Contribution by the elements of τ_1 is $(q^2-1)\, t_1^{e^{h-1}}\, t_p^{e^{h-1}\frac{(e^{2h}-e^2)}{p(e^2-1)}}$.

With ℓ, u, j and d as in part 6) (II) of section 1.3, we have two different types monomials for elements of τ_2,

(i) $t_{\ell}^{w(\ell(e-1))}\, t_d^{w(de(e^2-1))(e^{2h}+e^{h}-e^2-e)}$, where $\frac{u\ell}{j}=1$;

(ii) $t_d^{e^{h-1}\frac{(e^{2h}-1)}{d(e^2-1)}}$, $j=w(1)$.

The hyperbolics with the first type of monomial have their orders divisible by a factor ($\neq 1$) of e-1.

The contribution by elements of τ_2 is

$$qz(2)\,\Big[\sum_{\substack{j|d|w(1)\\(u\ell=j\neq w(1))}} \Phi(d)\, t_{\ell}^{w(\ell(e-1))}\, t_d^{w(de(e^2-1))(e^{2h}+e^{h}-e^2-e)} + \sum_{\substack{d|w(1)\\(j=w(1))}} \Phi(d)\, t_d^{\frac{e^{h-1}(e^{2h}-1)}{d(e^2-1)}}\Big].$$

With ℓ, u, j and d as in part 6) (III) of section 1.3, we have two different types of monomials for elements of τ_0,

(i) $t_{\ell}^{z(\ell(e+1))}\, t_d^{z(de(e^2-1))(e^{2h}-e^{h}-e^2+e)}$, where $\frac{u\ell}{j}=1$;

(ii) $t_d^{e^{h-1}\frac{(e^{2h}-1)}{d(e^2-1)}}$, $j=z(1)$.

The elliptics with the first type of monomial have their orders divisible by a factor ($\neq 1$) of e+1.

The contribution by elements of τ_0 is

$$qw(2)\,\Big[\sum_{\substack{j|d|z(1)\\(u\ell=j\neq w(1))}} \Phi(d)\, t_{\ell}^{z(\ell(e+1))}\, t_d^{z(de(e^2-1))(e^{2h}-e^{h}-e^2+e)} + \sum_{\substack{d|z(1)\\(j=z(1))}} \Phi(d)\, t_d^{\frac{e^{h-1}(e^{2h}-1)}{d(e^2-1)}}\Big].$$

Now adding all the above contributions and dividing by $|G|$, we have

$$\zeta(G) = \frac{1}{|G|}\Big[t_1^{\frac{|G|}{|H|}} + (q^2-1)\, t_1^{e^{h-1}}\, t_p^{e^{h-1}\frac{(e^{2h}-e^2)}{p(e^2-1)}}$$

$$+ qz(2) \sum_{\substack{j \mid d \mid w(1) \\ (u\ell = j \neq w(1))}} \Phi(d)\, t_\ell^{w(\ell(e-1))}\, t_d^{w(de(e^2-1))(e^{2h}+e^{h}-e^2-e)}$$

$$+ qz(2) \sum_{\substack{d \mid w(1) \\ (j = w(1))}} \Phi(d)\, t_d^{e^{h-1}\frac{(e^{2h}-1)}{d(e^2-1)}}$$

$$+ qw(2) \sum_{\substack{j \mid d \mid z(1) \\ (u\ell = j \neq z(1))}} \Phi(d)\, t_\ell^{z(\ell(e+1)}\, t_d^{z(de(e^2-1))(e^{2h}-e^{h}-e^2+e)}$$

$$+ qw(2) \sum_{\substack{d \mid z(1) \\ (j = z(1))}} \Phi(d)\, t_d^{\frac{e^{h-1}(e^{2h}-1)}{d(e^2-1)}} \Big].$$

CHAPTER 2

THE SUBDEGREES OF THE PRIMITIVE PERMUTATION REPRESENTATIONS OF PSL(2,q) AND PGL(2,q)

In this chapter we compute the subdegrees of the primitive permutation representations PSL (2,q) and PGL (2,q) and confirm the results on the ranks computed in chapter 1. The subdegrees of the primitive permutation representations of PSL (2,q) have previously been computed by Tchuda [21] in his Ph.D thesis (in Russian) as we learnt recently from Faradžev and Ivanov [7]. In [7], Faradžev and Ivanov have given the subdegrees of the representations of PSL(2,q) on the cosets of PSL(2,e), f/m an odd prime; PGL(2,e), f/m =2 and (see also Bon and Cohen [3]) PGL(2,q) on the cosets of its maximal dihedral subgroups.

As the work by Tchuda [21] is not readily available, we shall work out the subdegrees of the primitive permutation representations of PSL(2,q) in details except for the representations on the cosets of PSL(2,e), f/m an odd prime and PGL(2,e), f/m=2 for which we shall only quote the results given by Faradžev and Ivanov [7]. We also extend these calculations to the primitive representations of PGL(2,q).

The subdegrees of PSL(2,q) and PGL(2,q) on the cosets of their maximal dihedral subgroups will be computed using the results in chapter 1. A full description of the suborbits of PSL(2,q) and PGL(2,q) on the cosets of their maximal subgroups $D_{2w(k)}$ and $D_{2w(1)}$ respectively will be given. In all the other primitive representations of PSL(2,q) and PGL(2,q) (except PSL(2,q) on the cosets of A_4) we shall use the method proposed in [14].

In section 2.1 we give some definitions and notation (which we shall carry through to other chapters), and review the results in [14] on the computation of the subdegrees of transitive permutation groups using the table of marks.

In sections 2.2 and 2.3 we compute the subdegrees of primitive permutation representations of PSL(2,q) and PGL(2,q). (However where possible we generalize our results to include some imprimitive permutation representations).

2.1 Computing the subdegrees of transitive permutation groups using the table of marks

Let G be transitive on X and let G_x be the stabilizer in G of a point $x \in X$. The orbits $\Delta_0 = \{x\}, \Delta_1, \Delta_2, \ldots, \Delta_{r-1}$ of G_x on X are known as the <u>suborbits</u> of G. The rank of G in this case is r. The sizes $n_i = |\Delta_i|$ $(i=0,1,\ldots,r-1)$, often called the 'lengths' of the suborbits, are known as the <u>subdegrees</u> of G. It is worthwhile noting that both r and the cardinalities of the suborbits Δ_i $(i=0,1,\ldots,r-1)$ are independent of the choice of $x \in X$. We can choose the numbering so that $n_0 = 1 \leq n_1 \leq \ldots\ldots \leq n_{r-1}$.

<u>Definition 2.1.1</u> Let Δ be an orbit of G_x on X. Define $\Delta^* = \{gx \mid g \in G, x \in g\Delta\}$, then Δ^* is also an orbit of

G_x and is called the G_x-orbit (or the G-suborbit) paired with Δ.

Clearly $|\Delta|=|\Delta^*|$. If $\Delta^*=\Delta$, then Δ is called a self-paired orbit of G_x.

We now introduce the concept of the marks of a group; give some general properties of the table of marks and review the results in [14] on the computation of the subdegrees of transitive permutation groups using the table of marks.

Two definitions of the mark of a group appear in literature.

Burnside's definition of the mark (see Burnside [4], §180) translated into more familiar language states:

Definition 2.1.2 For any two subgroups A and B of a group G, the mark of A in the representation of G on the cosets of B is the number m(A, B, G) of the cosets of B that are fixed by every permutation in A.

Whites's definition of the mark (see White [24]) is as follows:

Definition 2.1.3 For any two subgroups A and B of a group G, the mark of A in the representation of G on the cosets of B is defined as the number

$$m(A,B,G) = \frac{1}{|B|}\sum_{g\in G}\chi(g^{-1}Ag \subset B),$$

Where $\chi\ (statement) = \begin{cases} 1 & \textit{if statement is true} \\ 0 & \textit{otherwise.} \end{cases}$

Before we prove the equivalence of the two definitions, we need the following:

Lemma 2.1.4 Let H_1 and H_2 be conjugate subgroups of G. The number of $g \in G$ such that $g^{-1}H_1g = H_2$ is $|N_G(H_1)|$.

Proof This is a trivial consequence of the fact that $\{g \mid g^{-1}H_1g=H_2\}$ is a coset of $N_G(H_1)$. □

Theorem 2.1.5 Let A and B be subgroups of G. If $\gamma(A)$ is the number of conjugates of A (by elements of G) contained in B, then in the permutation representation of G on $G/_B$,

$$\pi(A) = \frac{|G:B|\gamma(A)}{|C^A|},$$

where $\pi(A)$ = the number of cosets of B fixed by A and $C^A = \{gAg^{-1} \mid g \in G\}$.

Proof See the proof of Theorem 1.1.3.

□

Lemma 2.1.6 Definitions 2.1.2 and 2.1.3 are equivalent.

Proof If we start with White's definition of the mark,

$$
\begin{aligned}
m(A,B,G) &= \frac{1}{|B|}\sum_{g\in G}\chi(g^{-1}Ag \subset B)\\
&= \frac{1}{|B|}\,|N_G(A)|\,\gamma(A) \text{ (by Lemma 2.1.4} \qquad \text{Theorem 2.1.5)}\\
&= \frac{|G|}{|B|}\,\frac{N_G(A)}{|G|}\,\gamma(A)\\
&= \frac{|G:\ B|\gamma(A)}{|C^A|}\\
&= \pi(A) \text{ (by Theorem 2.1.5)}. \square
\end{aligned}
$$

One immediate fact we establish about marks is:

<u>Lemma 2.1.7</u> If $B \le G$ and A_1, A_2 are conjugate subgroups of G, then $m(A_1,B,G) = m(A_2,B,G)$.

By Theorem 1.1.2, the action of G on X is equivalent to its action on the cosets of $H = G_x$, while that of H on Δ_i $(i=0,1,..,r-1)$ is equivalent to its action on the set of cosets of some subgroup $F \le H$.

Let $\{H_1, H_2, \ldots, H_t\}$ be a complete set of representatives of all distinct conjugacy classes of subgroups of H in G, ordered such that $|H_1| \le |H_2| \le \ldots \le |H_t| = |H|$.
Form a matrix $M = (m_{ij})$, where $m_{ij} = m(H_j, H_i, G)$.

We call matrix M the <u>table of marks</u> of H. A useful fact about matrix M is the following:

Lemma 2.1.8 The matrix M is lower triangular with diagonal entries at least 1.

Proof Trivially $m_{ij} = 0$ if $i < j$ and ≥ 1 if $i = j$.

□

If we denote by Q_i the number of suborbits Δ_j on which the action of H is equivalent to its action on the cosets of H_i $(i=1,2,\ldots t)$, by computing all the Q_i we get the subdegrees of (G,X). Hence we have

Theorem 2.1.9 The numbers Q_j satisfy the system of linear equations

$$\sum_{i=j}^{t} Q_i \, m(H_j, H_i, H) = m(H_j, H, G) \quad \text{for each} \quad j = 1, \ldots, t.$$

(See [14].)

Lemma 2.1.10 If $m(H_j,H,G) = 1$ for some j, $1<j<t$, then $Q_j = 0$.

(See [14].)

Lemma 2.1.11 Let $F \leq H \leq G$ and $\{F_1, F_2, \ldots F_n\}$ be a complete set of conjugacy class representatives of subgroups of H that are conjugate to F in G, then

$$m(F, H, G) = \sum_{i=1}^{n} |N_G(F_i) : N_H(F_i)|.$$

In particular when n = 1, then F is conjugate in H to all subgroups F' that are contained in H and conjugate to F in G, and

$$m(F,H,G) = |N_G(F):N_H(F)|.$$

(See [14].)

2.2 The subdegrees of the primitive permutation representations of G = PSL(2,q)

We shall work with maximal subgroups of G in the order given in Chap. 1, §1.2. But before we begin, we first discuss the normalizers of some subgroups of G. For more details see Dickson [6], chap. 12.

The normalizers of some subgroups of G were given in Theorems 1.2.1, 1.2.2 and 1.2.3. From Lemma 1.2.5, the normalizer of an involution in G is $D_{2(q\pm1)}$, when p is odd and P_q when p is even.

The subgroup PSL (2,e) of G is its own normalizer except when f/m is even, in which case N_G(PSL(2,e) = PGL(2,e).

<u>Lemma 2.2.1</u> Let C_p be a cyclic subgroup of order p in G. Then

$$|N_G(C_p)| = \begin{cases} \frac{1}{2}q(p-1) & p \text{ odd, } f \text{ odd} \\ q(p-1) & p \text{ odd, } f \text{ even} \\ q & p=2. \end{cases}$$

(*See Dickson*[6], §249.)

<u>Lemma 2.2.2</u> Let C_d, (d coprime to p) be a cyclic subgroup of order d in G. Then

$$N_G(C_d) = \begin{cases} D_{q\pm1} & p \text{ odd} \\ D_{2(q\pm1)} & p=2, \end{cases}$$

$\pm$ sign as $d|q\pm1$.

(*See Dickson*[6], §246.)

<u>Lemma 2.2.3</u> Let $d > 2$ be a divisor of $\frac{1}{k}(q\pm1)$ and δ be the quotient. Then

$$N_G(D_{2d}) = \begin{cases} D_{2d} & \text{if } \delta \text{ is odd} \\ D_{4d} & \text{if } \delta \text{ is even.} \end{cases}$$

(*See Dickson*[6], §246.)

Lemma 2.2.4 $N_G(S_{q,w(k)}) = S_{q,w(k)}$.

Proof This is obvious since $S_{q,w(k)}$ is maximal in G (See p.18). □

We now proceed to compute the subdegrees of G.

1) The subdegrees of G on the cosets of $H \cong S_{q,w(k)}$

since the rank of G is 2, its subdegrees are:
One suborbit of length 1 and one suborbit of length q.

2) The subdegrees of G on the cosets of $H \cong D_{2w(k)}$

Here we take H to be the normalizer of the cyclic maximal subgroup <u> fixing 0 and ∞. As in part 2) of section 1.2, we may view this representation as the action of G on unordered pairs of points of PG(1,q).

Before we start computing the subdegrees of G, we give some simple results which we shall use later.

lemma 2.2.5 If -1 is a square mod p $(p\neq 2)$, then

$p\equiv 1 \bmod 4$.

Proof Let $x \in GF(p)$. $-1 = x^2 \Leftrightarrow x$ has order $4 \Leftrightarrow |x| \mid |GF(p)^*| = p-1 \Leftrightarrow p\equiv 1 \bmod 4$. □

Lemma 2.2.6 1 and -1 lie in the same cycle in u if and only if if $q\equiv 1 \bmod 4$.

Proof Let β be a primitive root of GF(q) and take u to be

$\begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix}$. The cycle containing 1 in u consists of all even

powers of β that is all non-zero squares in GF(q). Hence from Lemma 2.2.5, the lemma follows. □

Corollary 2.2.7 Let $x \in GF(q)$ then x and -x belong to the same cycle in u if and only if $q \equiv 1 \bmod 4$. □

To get the <u> orbits in this representation we shall use the results on the pair group action (see p.9). The subdegrees of G are the lengths of the H-Orbits in this representation. Each of these H-orbits is a union of <u>-orbits under some involution in H\<u>.

The following three cases must be distinguished:

(I) $q \equiv 1 \bmod 4$ (II) $q \equiv -1 \bmod 4$ (III) $p=2$

(I) $q \equiv 1 \bmod 4$

In the natural action, u contains two 1-cycles (one containing 0 and the other ∞) and two non-trivial cycles (one consisting of residues and the other consisting of non-residues). Any $g \in H\backslash\langle u\rangle$ fixes two points both from a non-trivial common cycle in u. Evidently , non-trivial cycles in g are 2-cycles containing (0∞) and pairs of points from a common cycle in u.

Now we classify H-orbits in this representation.

(a) Orbits of H formed by pairs of points lying in a common cycle in u.

(i) No pairs can be formed from a trivial cycle in u.

(ii) The pairs from non-trivial cycles give two <u> - orbits each of length w(4) consisting of points $\{x,-x\}$ in either of the two non - trivial cycles of u (x residue or non-residue), and $\frac{q-5}{2}$ <u> - orbits each of length w(2) and

consisting of pairs

$\{x,y\}$ ($y \neq x$, $-x$; x,y both residues or both non-residues).

Now to classify the above <u>-orbits into H-orbits, we simply have to note that for any <u>-orbit Δ with a

representative $\{x,y\}$, there exists a reflection g with (xy) as one of its cycles and for $1 \leq i \leq w(2)$, $u^i g(\{x,y\}) \in \Delta$. So any reflection $g \in H\backslash\langle u\rangle$ preserves the <u>-orbits. Hence the <u>-orbits and the H-orbits are the same.

(b) Orbits of H formed by pairs of points lying in different cycles of u of equal lengths.

(i) The two trivial cycles of u contribute a pair $\{0,\infty\}$ and this forms a <u>-orbit by itself. Since $\{0,\infty\}$ is fixed by H, $\{0,\infty\}$ forms an H-orbit by itself.

(ii) The <u>-orbits formed from pairs of points from different non-trivial cycles of u are w(2), each of length w(2).

We have $(w(2))^2$ pairs in this category each with the identity as the stabilizer. Hence H permutes these pairs semiregularly, so all H-orbits have length $|H| = w(1)$, and the number of them is $\frac{(w(2))^2}{|H|} = w(4)$. Hence there are $w(4)$

H-orbits each of length $w(1)$.

(c) Orbits of H formed by pairs of points lying in different cycles of u of unequal lengths.

In this case we have four $\langle u \rangle$-orbits each of length $w(2)$. Pairs of points in these $\langle u \rangle$-orbits intersect with $\{0,\infty\}$ in a singleton. If $x \neq 0$ is a residue and y a non-residue in GF(q), the pairs $\{0,x\}$, $\{\infty,x\}$, $\{0,y\}$, $\{\infty,y\}$ lie in different $\langle u \rangle$-orbits.

The pairs $\{0,x\}$ and $\{\infty,x\}$ respectively $\{0,y\}$ and $\{\infty,y\}$ lie in the same H-orbit. Hence in this case we have two H-orbits each of length $w(1)$.

Now gathering all the above contributions together we find the rank of G to be $\frac{3(q+3)}{4}$. The subdegrees are:

Table 2.2.1

Suborbit length	1	w(4)	w(2)	w(1)
No. of suborbit	1	2	$\frac{q-5}{2}$	$\frac{q+7}{4}$

(II) $q\equiv -1 \bmod 4$

In this case also, in the natural action, u contains two 1-cycles (one containing 0 and the other ∞) and two non-trivial cycles (one consisting of residues and the other consisting of non-residues).

Any $g \in H\backslash\langle u\rangle$ has no fixed point in PG(1,q). Cycles in g are involutions (0∞) and pairs of points from different non-trivial cycles of u.

Now we classify H-orbits in this representation.

(a) Orbits of H formed by pairs of points lying in a common cycle in u.

(i) No pairs can be formed from a trivial cycle in u.

(ii) From the two non-trivial cycles of u we get $\frac{q-3}{2}$

$\langle u\rangle$-orbits, each of length w(2).

We have $2\binom{w(2)}{2} = w(4)(q-3)$ pairs in this category each

with the identity as the stabilizer. Hence there are

$$\frac{w(4)(q-3)}{|H|} = \frac{q-3}{4}$$

H-orbits, each of length $|H| = w(1)$.

(b) Orbits of H formed by pairs of points in different cycles of u of equal lengths.

(i) The two trivial u - cycles contribute a pair $\{0,\infty\}$ which is both a <u> and an H-orbit.

(ii) From two non-trivial cycles of u we get w(2) <u>-orbits, each of length w(2).

An argument similar to that in case (I) (a) (ii) shows <u>-orbits and H- orbits to be the same.

(c) Orbits of H formed by pairs of points lying in different cycles of u of unequal lengths.

For $x \neq 0$ a residue and y a non-residue in GF(q), the four pairs $\{0,x\}$, $\{\infty,x\}$, $\{0,y\}$, $\{\infty,y\}$ lie in different <u>-orbits.

It is easily noticed that $\{0,x\}$ and $\{\infty,y\}$, respectively $\{\infty,x\}$ and $\{0,y\}$ lie in the same H-orbit.

Hence we have two H-orbits, each of length w(1). Now gathering all the above contributions together we find the rank of g to be $\frac{3q+7}{4}$. The subdegrees are:

Table 2.2.2

Suborbit length	1	w(2)	w(1)
No. of suborbits	1	w(2)	$\frac{q+5}{4}$

(III) $p = 2$

Here u contains two 1-cycles and one w(1)-cycle. We now classify H-orbits in this representation.

(a) Orbits of H formed by pairs of points lying in a common cycle in u.

(i) No pairs can be formed from a trivial cycle.

(ii) From the single non-trivial cycle of u we get $\frac{q-2}{2}$ <u>-orbits, each of length w(1).

An argument similar to that in case (I) (a) (ii) shows <u>-orbits and H-orbits to be the same.

(b) Orbits of H formed by pairs of points lying in different cycles of u of equal lengths.

The two trivial cycles of u contribute a pair $\{0,\infty\}$ which is an H-orbit by itself.

(c) Orbits of H formed by pairs of points in different cycles of u of unequal lengths.

Here we have two <u>-orbits, each of length w(1). The pairs $\{0,1\}$ and $\{\infty,1\}$ are in different <u>-orbits but in the same H-orbit. Hence the contribution to the total number of H-orbits in this case is 1 <u>-orbit of length 2(q-1).

Now gathering all the above contributions together we find that G has rank $\frac{q+2}{2}$. The subdegrees are:

Table 2.2.3

suborbit length	1	$w(1)$	$2(q-1)$
No. of suborbits	1	$\frac{q-2}{2}$	1

The results in (III) can also be got either by the method used by Faradžev and Ivanov [7] or by one used by Bon and Cohen [3].

3) The Subdegrees of G on the cosets of $H \cong D_{2z(k)}$

In this part $\langle s\rangle$ is the maximal cyclic subgroup of H with $|\langle s\rangle| = z(k)$.

We shall compute the subdegrees of G in this representation under the following three cases:

(I) $q \equiv 1 \bmod 4$ (II) $q \equiv -1 \bmod 4$ (III) $p = 2$

(I) $q \equiv 1 \bmod 4$

From Table 1.2.4, $\langle s\rangle$ decomposes the cosets of H into one $\langle s\rangle$-orbit of length 1 and $q-2$ $\langle s\rangle$-orbits, each of length $z(2)$. So the total number of the $\langle s\rangle$-orbits are $1 + (q-2) = w(1) > 3w(4)$ (the rank of G on P.30).

Hence some H-orbits are a union of more than one $\langle s\rangle$-orbit. By the Orbit-Stabilizer Theorem, the maximum length an H-orbit can have is $z(1)$. So the maximum number of $\langle s\rangle$-orbits an H-orbit can have is 2.

Now let x be the number of H-orbits of length z(1).

Then

$$1+(q-2)-2x+x = 3w(4)$$
$$\Leftrightarrow q-1-x = 3w(4)$$
$$\Leftrightarrow x = w(4).$$

Hence we have

Table 2.2.4

Suborbit length	1	z(2)	z(1)
No. of suborbits	1	$\frac{q-3}{2}$	w(4)

(II) $q \equiv -1 \bmod 4$

From Table 1.2.4, <s> decomposes the cosets of H into one <s>-orbit of length 1, two <s>-orbits each of length z(4), and q-3 <s>-orbits each of length z(2). So the total number of <s>-orbits are $1+2+q-3 \geq 3z(4)$ (the rank of G on p.30). The above inequality is strict if $q > 3$. Therefore some $g \in H\backslash$<s> will transpose certain pairs of <s>-orbits of length z(2) when $q > 3$. Now let x be the number of H-orbits of length z(1). Then

$$1 + 2 + (q-3) - 2x + x = 3z(4)$$
$$\leftrightarrow x = \frac{1}{4}(q-3),$$

Hence we have

Table 2.2.5

Suborbit length	1	z(4)	z(2)	z(1)
No. of suborbits	1	2	½ $(q - 3)$	$\frac{1}{4}(q-3)$

(III) p = 2

From Table 1.2.4, <s> decomposes the cosets of H into one <s>-orbit of length 1 and ½(q-2) <s>-orbits of length z(1) each. On p.30 we found the rank of G to be q/2, which is equal to the sum of the <s>-orbits in this representation. Hence the <s>-orbits and the H-orbits are the same.
Hence we have

Table 2.2.6

Suborbit length	1	z(1)
No. of suborbits	1	$\frac{1}{2}(q-2)$

We can also obtain the results in this part either by the method used by Faradžev and Ivanov [7] or by the one used by

Bon and Cohen [3].

4) The subdegrees of G on the cosets of $H \cong A_4$

Our computations will be carried under four cases as given in part 4) of section 1.2. Note that $N_G(V_4)$ is A_4 if $q \equiv \pm 3 \bmod 8$ and S_4 if $q \equiv \pm 1 \bmod 8$. Since $A_4 < S_4 < G$ in the latter case, it will not be considered in our calculations. Throughout this part, we denote $g^{-1}Hg$ ($g \in G$) by H^g.

a) $q \equiv 5 \bmod 12$

When G acts on G/H, the stabilizer of a coset Hg ($g \in G$) is H^g. If we restrict to the action of H on G/H, the stabilizer of a coset becomes $H \cap H^g$.

Let $F = H \cap H^g$, then F could be: H, V_4, C_3(4 subgroups), C_2(3 subgroups), 1.

i) $F = H \Leftrightarrow H \cap H^g = H \Leftrightarrow g \in N_G(H) = H$, therefore there exist 12 such elements g forming the coset $Hg = H$. Thus 1 suborbit (trivial) has $F = H$.

ii) $F \geq V_4 \Leftrightarrow H \cap H^g \geq V_4 \Leftrightarrow V_4^{g^{-1}} \leq H \Leftrightarrow g^{-1} \in N_G(V_4) = H.$

Thus there exist 12 elements g with $F \geq V_4$; these are the 12 elements g with $F = H$. Therefore no suborbit has $F = V_4$.

(iii) There exist 4 subgroups C_3 in H, all conjugate in G.

For any $C \leq H$ isomorphic to C_3, $F \geq C \Leftrightarrow C^{g^{-1}} \leq H$. For a

particular $C \cong C_3$, $N_G(C) = |D_{q+1}| = q+1$. So for any $C \cong C_3$, there are 4(q+1) elements g such that $C^{g^{-1}} \leq H$, therefore there are

4(q+1) elements g with $F \geq C$. Of these 12 have $F = H$. Therefore for any $C \cong C_3$, there exist 4(q-2) elements g with $F \cong C$. Hence for each $C \cong C_3$ the 4(q-2) elements g form ⅓(q-2) cosets of H. Therefore for the 4 subgroups C_3 there are

$\frac{4}{3}(q-2)$ cosets with $F \cong C_3$, forming $\frac{1}{3}(q-2)$ suborbits,

each of length $|H:C_3| = 4$.

(iv) There exist 3 subgroups C_2 in H, all conjugate in G. For

any $C \leq H$ isomorphic to C_2, $F \geq C \Leftrightarrow C^{g^{-1}} \leq H$. For a particular

subgroup $C \cong C_2$, the number of elements g normalizing C is $|N_G(C)| = |D_{q-1}| = q-1$. So for any $C \cong C_2$, there exist 3(q-1)

elements g with $H \geq C^{g^{-1}}$, therefore there exist 3(q-1)

elements g with $F \geq C$. Of these, 12 have $F = H$ or V_4. Therefore for any $C \cong C_2$ there exist 3(q-5) elements g with $F \cong C$. Hence for each $C \cong C_2$ the 3(q-5) elements g form ¼(q-5) cosets of H. Hence for the 3 subgroups C_2, there are

$\frac{3}{4}(q-5)$ cosets with $F \cong C_2$ forming ⅛(q-5) suborbits, each of

length $|H:C_2| = 6$.

All the other elements g must have F = 1, giving rise to regular suborbits of length $|H| = 12$. Cases (i), (ii), (iii) and (iv) account for 1, 0, $\frac{4}{3}(q-2)$ and $\frac{3}{4}(q-5)$ cosets respectively.

So the remaining

$$\frac{q(q^2-1)}{24} - \left(1+\frac{4}{3}(q-2)+\frac{3}{4}(q-5)\right) = \frac{q^3-51q+130}{24}$$

Cosets form $\frac{q^3-51q+130}{288}$ suborbits of length 12.

Thus we have:

Table 2.2.7

Suborbit length	1	4	6	12
No of suborbits	1	$\frac{q-2}{3}$	$\frac{q-5}{8}$	$\frac{q^3-51q+130}{288}$
No of cosets	1	$\frac{4(q-2)}{3}$	$\frac{3(q-5)}{4}$	$\frac{q^3-51q+130}{24}$

The rank (r) of G is $\frac{q^3+81q+46}{288}$.

Similarly for cases (b), (c) and (d) we get:

(b) $q \equiv 7 \bmod 12$

Table 2.2.8

F	A_4	V_4	C_3	C_2	I
$N_G(F)$	A_4	A_4	D_{q-1}	D_{q+1}	G
No. of cosets with stab =F	1	0	$\frac{4(q-4)}{3}$	$\frac{3(q-3)}{4}$	*
No. of suborbits	1	0	$\frac{q-4}{3}$	$\frac{q-3}{8}$	**
Suborbit length	1	-	4	6	12

where $*= \dfrac{q^3-51q+158}{24}$ and $**= \dfrac{q^3-51q+158}{288}$.

$r=\dfrac{q^3+81q-46}{288}$.

(c) $q \equiv 1 \bmod 12$

Table 2.2.9

F	A_4	V_4	C_3	C_2	I
$N_G(F)$	A_4	A_4	D_{q-1}	D_{q-1}	G
No. of cosets with stab=F	1	0	$\frac{4(q-4)}{3}$	$\frac{3(q-5)}{4}$	*
No. of suborbits	1	0	$\frac{q-4}{3}$	$\frac{q-5}{8}$	**
Suborbit length	1	-	4	6	12

where $* = \dfrac{q^3-51q+194}{24}$ and $** = \dfrac{q^3-51q+194}{288}$,

$$r = \frac{(q-1)(q^2+q+82)}{288} ,$$

(d) $q \equiv -1 \bmod 12$

Table 2.2.10

F	A_4	V_4	C_3	C_2	I
$N_G(F)$	A_4	A_4	D_{q+1}	D_{q+1}	G
No. of cosets with stab=F	1	0	$\frac{4(q-2)}{3}$	$\frac{3(q-3)}{4}$	*
No. of suborbits	1	0	$\frac{q-2}{3}$	$\frac{q-3}{8}$	**
Suborbit length	1	-	4	6	12

where $*= \frac{q^3-51q+94}{24}$ and $**= \frac{q^3-51q+94}{288}$,

$r = \frac{(q+1)(q^2-q+82)}{288}$.

5) The subdegrees of G on the cosets of $H \cong A_5$

The following are all the subgroups of H: H, 5 conjugate subgroups isomorphic A_4, 6 conjugate subgroups isomorphic D_{10}, 10 conjugate subgroups isomorphic D_6, 6 conjugate subgroups isomorphic to C_5, 5 conjugate subgroups isomorphic to V_4, 10 conjugate subgroups isormophic C_3, 15 conjugate subgroups isomorphic to C_2, 1.

Table of marks for H

Table 2.2.11

	1	C_2	C_3	V_4	C_5	D_6	D_{10}	A_4	H
1	60	0	0	0	0	0	0	0	0
C_2	30	2	0	0	0	0	0	0	0
C_3	20	0	2	0	0	0	0	0	0
V_4	15	3	0	3	0	0	0	0	0
C_5	12	0	0	0	2	0	0	0	0
D_6	10	2	1	0	0	1	0	0	0
D_{10}	6	2	0	0	1	0	1	0	0
A_4	5	1	2	1	0	0	0	1	0
H	1	1	1	1	1	1	1	1	1

Our computations will be carried under cases (a) - (l) listed on p.37. But in cases (c) - (l) (where p is odd), we have to distinguish between the case (i) when $q \equiv \pm 3 \bmod 8$ and case (ii) when $q \equiv \pm 1 \bmod 8$. This is because $N_G(V_4) = A_4$ and $N_G(A_4) = A_4$ in the former case, while $N_G(V_4) = S_4$ and $N_G(A_4) = S_4$ in the latter case. Now after adding some extra conditions to the cases we had before, removing those which are either superflous or impossible, then simplifying we get the following cases:

(a) $p = 2$, $q \equiv 4 \bmod 15$

(b) $p = 2$, $q \equiv 1 \bmod 15$

(c) $p = 3$, $q \equiv 9 \bmod 40$

(d) $p = 5$, f odd

(e) (i) $p \equiv 29 \bmod 120$, f odd

(ii) $p \equiv 89 \mod 120$, f odd

(f) (i) $p \equiv 19 \mod 120$, f odd

(ii) $p \equiv 79 \mod 120$, f odd

(g) (i) $p \equiv 11 \mod 120$, f odd

(ii) $p \equiv 71 \mod 120$, f odd

(h) (i) $p \equiv 109 \mod 120$, f odd

(ii) $p \equiv 49 \mod 120$, f odd or $p \equiv 23$ or $47 \mod 120$, $f \equiv 2 \mod 4$

(i) (i) $p \equiv 101 \mod 120$, f odd

(ii) $p \equiv 41 \mod 120$, f odd

(j) (i) $p \equiv 91 \mod 120$, f odd

(ii) $p \equiv 31 \mod 120$, f odd

(k) (i) $p \equiv 61 \mod 120$, f odd

(ii) $p \equiv 1 \mod 120$, f odd or $p \equiv \pm 1 \mod 5$, $f \equiv 2 \mod 4$ or $p \equiv \pm 2 \mod 5$, $f \equiv 0 \mod 4$

(ℓ) (i) $p \equiv 59 \mod 120$, f odd

(ii) $p \equiv -1 \mod 120$, f odd

From now on, if $F \leq H$, we shall use the abbreviation $m(F)$ for $m(F,H,G)$. The table below gives the values of $m(F)$ for all the cases (a) - (ℓ) listed above.

Table 2.2.12

F	m(F)
1	$q(q^2-1)/_{60}$ in cases (a) and (b). $q(q^2-1)/_{120}$ in cases (c) - (l).
C_2	$q/_4$ in cases (a) and (b). $\frac{q\pm1}{4}$ in cases (c) - (l), ± as $q \equiv \pm 1 \bmod 4$.
C_3	$(q-1)/_3$ in case (a) and b. $q/_3$ in case (c). $\frac{q\pm1}{6}$ in cases (d) - (l), ± as $q \equiv \pm 1 \bmod 6$.
V_4	$q/_4$ in cases (a) and (b). 2 if $q \equiv \pm 1 \bmod 8$ and 1 if $q \equiv \pm 3 \bmod 8$ in cases (c) -(l).
C_5	$(q \pm 1)/_5$ in cases (a) and (b), ± as $q \equiv \pm 1 \bmod 5$. $q/_5$ in case (d). $(q \pm 1)/_{10}$ in cases (c) and (e)-(l), ± as $q \equiv \pm1 \bmod 10$.
D_6	1 in cases (a) - (f) and (i) - (j). 2 in cases (g), (h), (k) and (l).
D_{10}	1 in cases (a) - (e) and (g), (h), (i). 2 in cases (f), (i), (k), and (l).
A_4	1 in cases (a) and (b). 2 if $q \equiv \pm1 \bmod 8$ and 1 if $q \equiv \pm3 \bmod 8$ in cases (c) - (l).
H	1 in cases (a) - (l).

Now let

$\underset{\sim}{N} = \left(m(1), m(C_2), m(C_3), m(V_4), m(C_5), m(D_6), m(D_{10}), m(A_4), m(H) \right)$,

$\underset{\sim}{Q} = \left(Q_1,\ Q_2, \ldots\ldots Q_9 \right)$ and M the matrix of table of marks given in Table 2.2.11. We now have $\boldsymbol{M}^{\boldsymbol{T}}\ \underset{\sim}{\boldsymbol{Q}}^{\boldsymbol{T}} = \underset{\sim}{\boldsymbol{N}}^{\boldsymbol{T}}$, *ie*

$$\begin{pmatrix} 60 & 30 & 20 & 15 & 12 & 10 & 6 & 5 & 1 \\ 0 & 2 & 0 & 3 & 0 & 2 & 2 & 1 & 1 \\ 0 & 0 & 2 & 0 & 0 & 1 & 0 & 2 & 1 \\ 0 & 0 & 0 & 3 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 2 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} Q_1 \\ Q_2 \\ Q_3 \\ Q_4 \\ Q_5 \\ Q_6 \\ Q_7 \\ Q_8 \\ Q_9 \end{pmatrix} = \begin{pmatrix} m(1) \\ m(C_2) \\ m(C_3) \\ m(V_4) \\ m(C_5) \\ m(D_6) \\ m(D_{10}) \\ m(A_4) \\ m(H) \end{pmatrix} \qquad \text{----(2.2.13)}$$

Substituting the values of m(F) given in Table 2.2.12 on the right hand side of (2.2.13) for each of the cases (a) - (l) and solving for the system of linear equations (2.2.13) we obtain $\underset{\sim}{Q}$ and hence the subdegrees of G in each of the cases as follows:

<u>Case (a)</u>

$$\underset{\sim}{Q} = \left(\frac{q^3-348q+1328}{3600},\ 0,\ \frac{q-4}{6},\ \frac{q-4}{12},\ \frac{q-4}{10}, 0, 0, 0, 1 \right).$$

Hence we have

Table 2.2.14

Suborbit length	No. of suborbits
1	1
12	$\frac{q-4}{10}$
15	$\frac{q-4}{12}$
20	$\frac{q-4}{6}$
60	$\frac{q^3-348q+1328}{3600}$

Therefore

$$r = \frac{q^3 + 912q - 112}{3600}.$$

Case (b)

$$\underset{\sim}{Q} = \left(\frac{q^3-348q+1472}{3600},\ 0,\ \frac{q-4}{6},\ \frac{q-4}{12},\ \frac{q-6}{10},0,0,0,1\right).$$

Hence we have

Table 2.2.15

Suborbit length	1	12	15	20	60
No. of suborbits	1	$\frac{q-6}{10}$	$\frac{q-6}{12}$	$\frac{q-4}{6}$	$\frac{q^3-348q+1472}{3600}$

Therefore

$$r = \frac{q^3 + 912q - 688}{3600}.$$

Case (c)

$$\underset{\sim}{Q} = \left(\frac{q^3-923q+7578}{7200}, \frac{q-9}{8}, \frac{q-9}{6}, 0, \frac{q-9}{20}, 0, 0, 1, 1\right).$$

Hence we have

Table 2.2.16

Suborbit length	1	5	12	20	30	60
No. of suborbits	1	1	$\frac{q-9}{20}$	$\frac{q-9}{6}$	$\frac{q-9}{8}$	$\frac{q^3-923q+7578}{7200}$

Therefore

$$r = \frac{q^3 + 1537q - 162}{7200}.$$

Case (d)

$$\underset{\sim}{Q} = \left(\frac{q^3-795q+3850}{7200}, \frac{q-5}{8}, \frac{q-5}{12}, 0, \frac{q-5}{10}, 0, 0, 0, 1\right).$$

Hence we have

Table 2.2.17

Suborbit length	1	12	20	30	60
No. of suborbits	1	$\frac{q-5}{10}$	$\frac{q-5}{12}$	$\frac{q-5}{8}$	$\frac{q^3-795q+3850}{7200}$

Therefore

$$r = \frac{q^3 + 1425q - 50}{7200}.$$

Case (e)(i)

$$\underset{\sim}{Q} = \left(\frac{q^3-723q+3778}{7200}, \frac{q-5}{8}, \frac{q-5}{12}, 0, \frac{q-9}{20}, 0, 0, 0, 1\right).$$

Hence we have

Table 2.2.18

Suborbit length	1	12	20	30	60
No. of Suborbits	1	$\frac{q-9}{20}$	$\frac{q-5}{12}$	$\frac{q-5}{8}$	$\frac{q^3-723q+3778}{7200}$

Therefore

$$r = \frac{q^3+1137q+238}{7200}.$$

Case (e) (ii)

$$\underset{\sim}{Q} = \left(\frac{q^3-723q+7378}{7200}, \frac{q-9}{8}, \frac{q-17}{12}, 0, \frac{q-9}{20}, 0, 0, 1, 1\right).$$

Hence we have

Table 2.2.19

Suborbit length	1	5	12	20	30	60
No. of suborbits	1	1	$\frac{q-9}{20}$	$\frac{q-17}{12}$	$\frac{q-9}{8}$	$\frac{q^3-723q+7378}{7200}$

Therefore

$$r = \frac{q^3+1137q+238}{7200}.$$

Case (f)(i)

$$\underset{\sim}{Q} = \left(\frac{q^3-723q+6878}{7200}, \frac{q-11}{8}, \frac{q-7}{12}, 0, \frac{q-19}{20}, 0, 1, 0, 1\right).$$

Hence we have

Table 2.2.20

Suborbit length	1	6	12	20	30	60
No. of Suborbits	1	1	$\frac{q-19}{20}$	$\frac{q-7}{12}$	$\frac{q-11}{8}$	$\frac{q^3-723q+6878}{7200}$

Therefore

$$r = \frac{q^3 + 1137q + 338}{7200}.$$

Case (f)(ii)

$$\underset{\sim}{Q} = \left(\frac{q^3 - 723q + 10478}{7200}, \frac{q-15}{8}, \frac{q-19}{12}, 0, \frac{q-19}{20}, 0, 1, 1, 1\right).$$

Hence we have

Table 2.2.21

Suborbit length	1	5	6	12	20	30	60
No. of Suborbits	1	1	1	$\frac{q-19}{20}$	$\frac{q-19}{12}$	$\frac{q-15}{8}$	$\frac{q^3-723q+10478}{7200}$

Therefore

$$r = \frac{q^3 + 1137q + 338}{7200}.$$

Case (q) (i)

$$\underset{\sim}{Q} = \left(\frac{q^3 - 723q + 6622}{7200}, \frac{q-11}{8}, \frac{q-11}{12}, 0, \frac{q-11}{20}, 1, 0, 0, 1\right).$$

Hence we have

Table 2.2.22

Suborbit length	1	10	12	20	30	60
No. of suborbits	1	1	$\frac{q-11}{20}$	$\frac{q-11}{12}$	$\frac{q-11}{8}$	*

where $* = \dfrac{q^3 - 723q + 6622}{7200}$.

Therefore

$$r = \frac{q^3 + 1137q + 562}{7200}.$$

Case (q) (ii)

$$\underset{\sim}{Q} = \left(\frac{q^3-723q+10222}{7200}, \frac{q-15}{8}, \frac{q-23}{12}, 0, \frac{q-11}{20}, 1, 0, 1, 1\right).$$

Hence we have

Table 2.2.23

Suborbit length	1	5	10	12	20	30	60
No. of suborbits	1	1	1	$\frac{q-11}{20}$	$\frac{q-23}{12}$	$\frac{q-15}{8}$	*

$$\text{where } * = \frac{q^3-723q+10222}{7200}.$$

Therefore

$$r = \frac{q^3+1137q+562}{7200}.$$

Case (h) (i)

$$\underset{\sim}{Q} = \left(\frac{q^3-723q+7778}{7200}, \frac{q-13}{8}, \frac{q-13}{12}, 0, \frac{q-9}{20}, 1, 0, 0, 1\right).$$

Hence we have

Table 2.2.24

Suborbit length	1	10	12	20	30	60
No. of suborbits	1	1	$\frac{q-9}{20}$	$\frac{q-13}{12}$	$\frac{q-13}{8}$	*

$$\text{where } * = \frac{q^3-723q+7778}{7200}.$$

Therefore

$$r = \frac{q^3+1137q-562}{7200}.$$

Case (h) (ii)

$$\underset{\sim}{Q} = \left(\frac{q^3-723q+11378}{7200}, \frac{q-17}{8}, \frac{q-25}{12}, 0, \frac{q-9}{20}, 1, 0, 1, 1 \right) .$$

Hence we have

Table 2.2.25

Suborbit length	No. of suborbits
1	1
5	1
10	1
12	$\frac{q-9}{20}$
20	$\frac{q-25}{12}$
30	$\frac{q-17}{8}$
60	$\frac{q^3-723q+11378}{7200}$

Therefore

$$r = \frac{q^3+1137q-562}{7200} .$$

Case (i) (i)

$$\underset{\sim}{Q} = \left(\frac{q^3-723q+7522}{7200}, \frac{q-13}{8}, \frac{q-5}{12}, 0, \frac{q-21}{20}, 0, 1, 0, 1 \right) .$$

Hence we have

Table 2.2.26

Suborbit length	1	6	12	20	30	60
No. of suborbits	1	1	$\frac{q-21}{20}$	$\frac{q-5}{12}$	$\frac{q-13}{8}$	*

where $*= \dfrac{q^3-723q+7522}{7200}$.

Therefore

$$r = \frac{q^3+1137q-338}{7200}.$$

Case (i) (ii)

$$\underset{\sim}{Q} = \left(\frac{q^3-723q+11122}{7200}, \frac{q-17}{8}, \frac{q-17}{12}, 0, \frac{q-21}{20}, 0, 1, 1, 1\right).$$

Hence we have

Table 2.2.27

Suborbit length	1	5	6	12	20	30	60
No. of suborbits	1	1	1	$\frac{q-21}{20}$	$\frac{q-17}{12}$	$\frac{q-17}{8}$	*

where $*= \dfrac{q^3-723q+11122}{7200}$.

Therefore

$$r = \frac{q^3+1137q-338}{7200}.$$

Case (j) (i)

$$\underset{\sim}{Q} = \left(\frac{q^3-723q+3422}{7200}, \frac{q-3}{8}, \frac{q-7}{12}, 0, \frac{q-11}{20}, 0, 0, 0, 1\right).$$

Hence we have

Table 2.2.28

Suborbit length	1	12	20	30	60
No. of suborbits	1	$\frac{q-11}{20}$	$\frac{q-7}{12}$	$\frac{q-3}{8}$	*

where $* = \frac{q^3-723q+3422}{7200}$.

Therefore

$$r = \frac{q^3+1137q-238}{7200}.$$

Case (j) (ii)

$$\underset{\sim}{Q} = \left(\frac{q^3-723q+7022}{7200}, \frac{q-7}{8}, \frac{q-19}{12}, 0, \frac{q-11}{20}, 0, 0, 1, 1\right).$$

Hence we have

Table 2.2.29

Suborbit length	1	5	12	20	30	60
No. of suborbits	1	1	$\frac{q-11}{20}$	$\frac{q-19}{12}$	$\frac{q-7}{8}$	*

$$\text{where}*= \frac{q^3-723q+7022}{7200}$$

Therefore

$$r = \frac{q^3+1137q-238}{7200}.$$

<u>Case (k) (i)</u>

$$\underset{\sim}{Q} = \left(\frac{q^3-723q+1522}{7200}, \frac{q-21}{8}, \frac{q-13}{12}, 0, \frac{q-21}{20}, 1, 1, 0, 1\right).$$

Hence we have

<u>Table 2.2.30</u>

Suborbit length	1	6	10	12	20	30	60
No. of suborbits	1	1	1	$\frac{q-21}{20}$	$\frac{q-13}{12}$	$\frac{q-13}{8}$	*

$$\text{where } *= \frac{q^3-723q+1522}{7200},$$

Therefore

$$r = \frac{q^3+1137q-1138}{7200}.$$

<u>Case (k) (ii)</u>

$$\underset{\sim}{Q} = \left(\frac{q^3-723q+15122}{7200}, \frac{q-25}{8}, \frac{q-25}{12}, 0, \frac{q-21}{20}, 1, 1, 1, 1\right).$$

Hence we have

Table 2.2.31

Suborbit length	1	5	6	10	12	20	30	60
No. of suborbits	1	1	1	1	$\frac{q-21}{20}$	$\frac{q-25}{12}$	$\frac{q-25}{8}$	*

$$\text{where } * = \frac{q^3-723q+15122}{7200}$$

Therefore

$$r = \frac{q^3+1137q-1138}{7200}.$$

Case (l) (i)

$$\underset{\sim}{Q} = \left(\frac{q^3-723q+10078}{7200}, \frac{q-19}{8}, \frac{q-11}{12}, 0, \frac{q-19}{20}, 1, 1, 0, 1\right).$$

Hence we have

Table 2.2.32

Suborbit length	1	6	10	12	20	30	60
No. of suborbits	1	1	1	$\frac{q-19}{20}$	$\frac{q-11}{12}$	$\frac{q-19}{8}$	*

$$\text{where } * = \frac{q^3-723q+10078}{7200}.$$

Therefore

$$r = \frac{q^3+1137q+1138}{7200}.$$

Case l (ii)

$$\underset{\sim}{Q} = \left(\frac{q^3-723q+13678}{7200}, \frac{q-23}{8}, \frac{q-23}{12}, 0, \frac{q-19}{20}, 1, 1, 1, 1 \right).$$

Hence we have

Table 2.2.33

Suborbit length	1	5	6	10	12	20	30	60
No. of suborbits	1	1	1	1	$\frac{q-19}{20}$	$\frac{q-23}{12}$	$\frac{q-23}{8}$	*

where $* = \dfrac{q^3-723q+13678}{7200}$.

Therefore

$$r = \frac{q^3+1137q+1138}{7200}.$$

6) The subdegrees of G on the cosets of $H \simeq S_4$

The following are all the subgroups of H:

(i) H

(ii) A_4, which is a normal subgroup.

(iii) A conjugacy class of 3 subgroups of order 8, isomorphic to D_8.

(iv) A conjugacy class of 4 subgroups of order 6, isomorphic to D_6.

(v) A normal subgroup of order 4, isomorphic to $C_2 \times C_2$ which we shall denote by $V_4^{(1)}$.

(vi) A conjugacy class of 3 subgroups of order 4 isomorphic to $C_2 \times C_2$. We denote a subgroup of this type by $V_4^{(3)}$.

(vii) A conjugacy class of 3 cyclic subgroups of order 4, C_4.

(viii) A conjugacy class of 4 subgroups of order 3, C_3.

(ix) A conjugacy class of 6 subgroups of order 2 not contained in A_4. We denote a subgroup of this type by $C_2^{(6)}$.

(x) A conjugacy class of 3 subgroups of order 2 contained in A_4. We denote a subgroup of this type by $C_2^{(3)}$.

(xi) I.

Table of marks of H

Table 2.2.34

	1	$C_2^{(6)}$	$C_2^{(3)}$	C_3	C_4	$V_4^{(1)}$	$V_4^{(3)}$	D_6	D_8	A_4	H
1	24	0	0	0	0	0	0	0	0	0	0
$C_2^{(6)}$	12	2	0	0	0	0	0	0	0	0	0
$C_2^{(3)}$	12	0	4	0	0	0	0	0	0	0	0
C_3	8	0	0	2	0	0	0	0	0	0	0
C_4	6	0	2	0	2	0	0	0	0	0	0
$V_4^{(1)}$	6	0	6	0	0	6	0	0	0	0	0
$V_4^{(3)}$	6	2	2	0	0	0	2	0	0	0	0
D_6	4	2	0	1	0	0	0	1	0	0	0
D_8	3	1	3	0	1	3	1	0	1	0	0
A_4	2	0	2	2	0	2	0	0	0	2	0
H	1	1	1	1	1	1	1	1	1	1	1

By Theorem 2.2.3, the value of $m(D_8)$ is either 1 or 2 depending on whether $\delta = \frac{q\pm 1}{8}$ is odd or even.

Each subgroup of type $V_4^{(3)}$ is contained in a unique subgroup of type D_8 in H and $V_4^{(1)}$ is the intersection of the 3 subgroups of type D_8 in H. For $q \equiv \pm 1 \bmod 8$, G contains two sets each of $|G|/_{24}$ conjugate Klein 4-groups V_4. Now from Theorem 2.2.3, it is easy to ascertain:

Lemma 2.2.8 The Klein 4-groups V_4 in H are in the same conjugacy class in G if and only if δ is even.

Our computations will be carried under the cases (a) - (d) listed on p. 45. Let F be a representative of a conjugacy class in H, the table below gives the values of m(F) for all the cases (a) - (d).

Table 2.2.35

F	m(F)
1	$\frac{q(q^2-1)}{48}$ in all the cases (a) - (d).
$C_2^{(6)}$	$\frac{3(q-1)}{8}$ in cases (a) and (c).
	$\frac{3(q+1)}{8}$ in cases (b) and (d).
$C_2^{(3)}$	$\frac{3(q-1)}{8}$ in cases (a) and (c).
	$\frac{3(q+1)}{8}$ in cases (b) and (d).
C_3	$\frac{q+1}{6}$ in cases (a) and (c).
	$\frac{q-1}{6}$ in cases (b) and (d).
C_4	$\frac{q-1}{8}$ in cases (a) and (c).
	$\frac{q+1}{8}$ in cases (b) and (d).
$V_4^{(1)}$	$\begin{cases} 4 \textit{ if } \delta \textit{ is even} \\ 3 \textit{ if } \delta \textit{ is odd.} \end{cases}$
$V_4^{(3)}$	$\begin{cases} 4 \textit{ if } \delta \textit{ is even} \\ 1 \textit{ if } \delta \textit{ is odd.} \end{cases}$
D_6	1 in cases (a) and (b). 2 in cases (c) and (d).
D_8	$\begin{cases} 1 \textit{ if } \delta \textit{ is odd} \\ 2 \textit{ if } \delta \textit{ is even.} \end{cases}$
A_4	1 in all the cases (a) - (d).
H	1 in all the cases (a) - (d).

Now let

$$\underset{\sim}{N}=(m(1),m(C_2^{(6)}),m(C_2^{(3)}),m(C_3),m(C_4),m(V_4^{(1)}),$$
$$m(V_4^{(3)}),m(D_6),m(D_8),m(A_4),m(H)),$$

$\underset{\sim}{Q} = (Q_1, Q_2, \ldots, Q_{11})$ and M the matrix of table of marks given in Table 2.2.34. Solving for the values of Q_i in the system of linear equations $M^T\underset{\sim}{Q}^T = \underset{\sim}{N}^T$.

We get:

<u>Case (a) (i)</u> When δ is even

$$\underset{\sim}{Q} = \left(\frac{q^3-195q+1858}{1152}, \frac{3q-35}{16}, \frac{q-17}{16}, \frac{q-5}{12}, \frac{q-17}{16}, 0,1,0,1,0,1\right).$$

Hence we have

<u>Table 2.2.36</u>

F	H	D_8	$\mathcal{C}$	C_4	C_3	$\mathcal{A}$	$\mathcal{B}$	1
No. of suborbits with stab =F	1	1	1	$\frac{q-17}{16}$	$\frac{q-5}{12}$	$\frac{q-17}{16}$	*	**
Suborbit length	1	3	6	6	8	12	12	24

where $\mathcal{A} = C_2^{(6)}$, $\mathcal{B} = C_2^{(3)}$, $\mathcal{C} = V_4^{(1)}$, $* = \frac{3q-35}{16}$ and

$$**= \frac{q^3-195q+1858}{1152},$$

Therefore

$$r = \frac{q^3+261q-134}{1152}.$$

(ii) When δ is odd

$$\underset{\sim}{Q} = \left(\frac{q^3-195q+1282}{1152}, \frac{3(q-9)}{16}, \frac{q-9}{16}, \frac{q-5}{12}, \frac{q-9}{16}, 0, 1, 0, 0, 0, 1\right).$$

Hence we have

Table 2.2.37

F	H	$\mathcal{C}$	C_4	C_3	$\mathcal{B}$	$\mathcal{A}$	1
No. of suborbits with stab = F	1	1	$\frac{q-9}{16}$	$\frac{q-5}{12}$	$\frac{q-9}{16}$	*	**
Suborbit length	1	6	6	8	12	12	24

where $\mathcal{A} = C_2^{(6)}$, $\mathcal{B} = C_2^{(3)}$, $\mathcal{C} = V_4^{(1)}$, $* = \frac{3(q-9)}{16}$

and $** = \frac{q^3-195q+1282}{1152}$.

Therefore

$$r = \frac{q^3+261q-134}{1152}.$$

Case (b) (i) When δ is even

$$\underset{\sim}{Q} = \left(\frac{q^3-195q+1598}{1152}, \frac{3q-29}{16}, \frac{q-15}{16}, \frac{q-7}{12}, \frac{q-15}{16}, 0,1,0,1,0,1\right).$$

Hence we have

Table 2.2.38

F	H	D_8	$\mathcal{C}$	C_4	C_3	$\mathcal{B}$	$\mathcal{A}$	1
No. of suborbits with stab.= F	1	1	1	α	β	γ	σ	μ
Suborbit length	1	3	6	6	8	12	12	24

where $\mathcal{D} = V_4^{(3)}$, $\mathcal{B}= C_2^{(3)}$, $\mathcal{A}= C_2^{(6)}$, $\alpha= \frac{q-5}{16}$, $\beta= \frac{q-7}{12}$,

$\gamma= \frac{q-15}{16}$, $\sigma= \frac{3q-29}{16}$, $\mu= \frac{q^3-195q+1598}{1152}$.

Therefore

$$r = \frac{q^3+261q+134}{1152}.$$

(ii) When δ is odd

$$\underset{\sim}{Q} = \left(\frac{q^3-195q+1022}{1152}, \frac{3(q-7)}{16}, \frac{q-7}{16}, \frac{q-7}{12}, \frac{q-7}{16}, 0,1,0,0,0,1\right).$$

Hence we have

Table 2.2.39

F	H	$\mathcal{D}$	C_4	C_3	$\mathcal{B}$	$\mathcal{A}$	1
No. of suborbits with stab.=F	1	1	$\frac{q-7}{16}$	$\frac{q-7}{12}$	$\frac{q-7}{16}$	*	**
Suborbit length	1	6	6	8	12	12	24

where $\mathcal{D} = V_4^{(3)}$, $\mathcal{B} = C_2^{(3)}$, $\mathcal{A} = C_2^{(6)}$, $* = \frac{3(q-7)}{16}$ and

$$** = \frac{q^3-195q+1022}{1152}.$$

Therefore

$$r = \frac{q^3+261q+134}{1152}.$$

<u>Case (c) (i)</u> When δ is even

$$\underset{\sim}{Q} = \left(\frac{q^3-195q+2498}{1152}, \frac{3(q-17)}{16}, \frac{q-17}{16}, \frac{q-13}{12}, \frac{q-17}{16}, 0, 1, 1, 1, 0, 1\right).$$

Hence we have

Table 2.2.40

F	H	D_8	D_6	$\mathcal{D}$	C_4	C_3	$\mathcal{B}$	$\mathcal{A}$	1
No. of suborbits with stab. =F	1	1	1	1	σ	α	β	γ	μ
Suborbit length	1	3	4	6	6	8	12	12	24

where $\mathcal{D} = V_4^{(3)}$, $\mathcal{B} = C_2^{(3)}$, $\mathcal{A} = C_2^{(6)}$, $\sigma = \dfrac{q-1}{8}$, $\alpha = \dfrac{q-13}{12}$,

$\beta = \dfrac{q-17}{16}$, $\gamma = \dfrac{3(q-17)}{16}$ and $\mu = \dfrac{q^3-195q+2498}{1152}$.

Therefore

$$r = \frac{q^3+261q-262}{1152}.$$

(ii) When δ is odd

$$\underset{\sim}{Q} = \left(\frac{q^3-195q+1922}{1152}, \frac{3q-43}{16}, \frac{q-9}{16}, \frac{q-13}{12}, \frac{q-9}{16}, 0,1,1,0,0,1\right).$$

Hence we have

Table 2.2.41

F	H	D_6	$\mathcal{D}$	C_4	C_3	$\mathcal{B}$	$\mathcal{A}$	1
No. of suborbits with stab. = F	1	1	1	$\frac{q-9}{16}$	$\frac{q-13}{12}$	α	β	γ
Suborbit length	1	4	6	6	8	12	12	24

where $\mathcal{D} = V_4^{(3)}$, $\mathcal{B} = C_2^{(3)}$, $\mathcal{A} = C_2^{(6)}$, $\alpha = \dfrac{q-9}{16}$, $\beta = \dfrac{3q-43}{16}$ and

$$\gamma = \frac{q^3-195q+1922}{1152}.$$

Therefore

$$r = \frac{q^3+261q-262}{1152}.$$

Case (d) (i) When δ is even

$$\underset{\sim}{Q} = \left(\frac{q^3-195q+2110}{1152}, \frac{3(q-15)}{16}, \frac{q-15}{16}, \frac{q-11}{12}, \frac{q-15}{16}, 0, 1, 1, 1, 0, 1\right).$$

Hence we have

Table 2.2.42

F	H	D_8	D_6	$\mathcal{D}$	C_4	C_3	$\mathcal{B}$	$\mathcal{A}$	1
No. of suborbits with stab.=F	1	1	1	1	α	β	α	σ	μ
Suborbit length	1	3	4	6	6	8	12	12	24

where $\mathcal{D} = V_4^{(3)}$, $\mathcal{B} = C_2^{(3)}$, $\mathcal{A} = C_2^{(6)}$, $\alpha = \dfrac{q-15}{16}$, $\beta = \dfrac{q-11}{12}$,

$\sigma = \dfrac{3(q-15)}{16}$ and $\mu = \dfrac{q^3-195q+2110}{1152}$.

Therefore

$$r = \frac{q^3+261q+262}{1152}.$$

(ii) When δ is odd

$$\underset{\sim}{Q} = \left(\frac{q^3-195q+1534}{1152}, \frac{3q-37}{16}, \frac{q-7}{16}, \frac{q-11}{12}, \frac{q-7}{16}, 0,1,1,0,0,1\right).$$

Hence we have

Table 2.2.43

F	H	D_6	$\mathcal{D}$	C_4	C_3	$\mathcal{B}$	$\mathcal{A}$	1
No. of suborbits with stab.=F	1	1	1	σ	α	σ	γ	μ
Suborbit length	1	4	6	6	8	12	12	24

where $\mathcal{D} = V_4^{(3)}$, $\mathcal{B} = C_2^{(3)}$, $\mathcal{A} = C_2^{(6)}$, $\sigma = \dfrac{q-7}{16}$, $\alpha = \dfrac{q-11}{12}$,

$\gamma = \dfrac{3q-37}{16}$, and $\mu = \dfrac{q^3-195q+2110}{1152}$.

Therefore

$$r = \frac{q^3+261q+262}{1152}.$$

7) The subdegrees of G on the cosets of H ≅ PSL(2,e), f/m an odd prime

Firstly let $q = e^h$. The subdegrees of the representation of G on the coset of H are given by Faradžev and Ivanov [7] as follows:

Table 2.2.44

Suborbit Length	1	$\dfrac{e^2-1}{\mu}$	$e(e-1)$	$e(e+1)$	$\dfrac{e(e^2-1)}{\mu}$
No. of suborbits	1	$\mu\alpha$	β	γ	$\mu\sigma$

Where

$$\mu = (2, e-1),$$

$$\alpha = \frac{e^{h-1}-1}{e-1},$$

$$\beta = \frac{e^{h}-e}{2(e+1)},$$

$$\gamma = \frac{e^{h}-e}{2(e-1)},$$

$$\sigma = \frac{e^{3h-2}-e^{h-2}(e^4+e^3+2e^2-e)+(e^3+e^2+e-1)}{(e^2-1)^2}.$$

Hence

$$r = \frac{e^{3h-2}+e^{h+3}-e^{h+1}-3e^{h}-e^2+2e+1}{(e^2-1)^2} \quad \textit{if } p=2$$

or $$\frac{2e^{3h-2}+e^{h+3}-e^{h+1}-6e^{h}-e^2+4e+1}{(e^2-1)^2} \quad \textit{if } p > 2.$$

8) The subdegrees of G on the cosets of H ≅ PGL(2,e), f/m=2

Let $q = e^2$. The subdegrees of the representation of G on the cosets of H are given by Faradžev and Ivanov [7] as follows:

Table 2.2.45

When p=2.

Suborbit length	1	e^2-1	$e(e-1)$	$e(e+1)$
No. of suborbits	1	1	$\frac{1}{2}(e-2)$	$\frac{1}{2}e$

Table 2.2.46

When $p > 2$

Suborbit length	1	$\frac{1}{2}e(e-\epsilon)$	e^2-1	$e(e-1)$	$e(e+1)$
No. of suborbits	1	1	1	$\frac{1}{4}(e-4-\epsilon)$	$\frac{1}{4}(e-2+\epsilon)$

Where $e \equiv \epsilon \bmod 4$, $\epsilon = \pm 1$

Hence

$r = e + 1$ if $p = 2$

or $\frac{1}{2}(e + 3)$ if $P > 2$.

2.3 The subdegrees of the primitive permutation representations of G= PGL (2,q)

We start by briefly looking at normalizers of some subgroups of G.

By the fact that G is imbedded in PSL $(2,q^2)$ and the review of subgroups of PSL(2,q) given by Dickson [6] §260, we deduce:

(a) For every divisor m of f, G has subgroups PGL (2,e) and PSL (2,e), with $N_G(PSL(2,e)) \cong PGL(2,e)$, $N_G(PGL(2,e)) \cong PGL(2,e)$.

(b) The subgroup $S_{q,w(1)}$ is its own normalizer in G.
In fact this is easily realized from the fact that $S_{q,w(1)}$ is a maximal subgroup of G (see p. 62).

(c) For the subgroups S_4, A_5 and A_4 (see p. 61 for the conditions of their existence); S_4 and A_5 are their own normalizers, while the normalizer of A_4 in G is S_4.

(d) Denote by ${}^{a}C_2$ and ${}^{b}C_2$ a C_2 in PSL (2,q) and a $C_2 \not< PSL(2,q)$

respectively (see Lemma 1.2.9). The presence of these two conjugacy classes of involutions leads us to the conclusion that there are two conjugacy classes of subgroups isomorphic to V_4. If $V_4 < PSL(2,q)$ (we denote such by ${}^{a}V_4$), it has S_4 as its normalizer. However if $V_4 \not< PSL(2,q)$ (we denote such by ${}^{b}V_4$), its normalizer is D_8.

We now compute the subdegrees of G on the cosets of each of its maximal subgroup H given on p.62.

<u>1) The subdegrees of G on the cosets of</u> $H \cong S_{q,w(1)}$

This is the natural representation of G on PG (1,q) of degree z(1). Since the rank is two, the subdegrees are:1 suborbit of length 1 and 1 suborbit of length q.

<u>2) The subdegrees of G on the cosets of</u> $H \cong D_{2w(1)}$

Let <u> be the cyclic maximal subgroup of order w(1) in the dihedral subgroup H of G fixing $\{0,\infty\}$. In the natural action, u contains two 1-cycles (one containing 0 and the other ∞) and one
w(1)-cycle.

In this representation, we obtain the H-orbits, hence the subdegrees of G as follows:

(a) Orbits of H formed by pairs of points lying in a common cycle in u:

(i) No pairs can be formed from a trivial cycle in u.

(ii) The pairs from the non-trivial cycle of u give one <u>-orbit of length w(2) and $\frac{1}{2}(q-3)$ <u>-orbits of length w(1). An argument similar to that in Case I (a) (ii) of part 2) of §2.2 shows the <u>-orbits and the H-orbits to be the same.

(b) Orbits of H formed by pairs of points lying in different cycles of u of equal lengths:

The two trivial cycles of u contribute a pair $\{0,\infty\}$ which is an H-orbit by itself.

(c) Orbits of H formed by pairs of points in different cycles of u of unequal lengths:

We have two <u>-orbits each of length w(1) with representatives $\{0,1\}$ and $\{\infty,1\}$. Any involution in H with a cycle (0∞) and fixing 1 and any other element in GF (q) unites the two <u>-orbits to an H-orbit.

Gathering the above contributions together we find the rank of G to be $\frac{1}{2}(q+3)$.

The subdegrees are:

Table 2.3.1

Suborbit length	1	w(2)	w(1)	2w(1)
No. of suborbits	1	1	$\frac{1}{2}(q-3)$	1

We can also obtain the results in this part either by the method used by Faradzev and Ivanov [7] or by the one used by Bon and Cohen [3].

3) The subdegrees of G on the cosets of H $\cong D_{2z(1)}$

Let <s> be the cyclic maximal subgroup of order z(1) in H. In this representaion <s> decomposes the cosets of H into one
<s>-orbit of length 1, one <s>-orbit of length z(2) and $\frac{1}{2}(q-3)$ <s>-orbits of length z(1) (see Table 1.3.4). On p.66 we found the rank of G to be z(2), which is equal to the number of <s>-orbits in this representation. Hence the <s>-orbits and the H-orbits are the same.

The table below gives the subdegrees of G.

Table 2.3.2

Suborbit length	1	z(2)	z(1)
No. of suborbits	1	1	½(q-3)

We can also obtain the results in this part either by the method used by Faradžev and Ivanov [7] or by the one used by Bon and Cohen [3].

4) The subdegrees of G on the cosets of $H \cong S_4$

Table 2.2.34 on p.126 is the table of marks for H. Our computations will be carried under the cases (a) - (d) listed on p.68. As before let F be a representative of a conjugacy class in H. The table below gives the values of m(F) for all the cases (a) - (d).

<u>Table 2.3.3</u>

F	m (F)
1	$q(q^2-1)/_{24}$ in all the cases (a) - (d).
$C_2^{(6)}$	$\frac{q-1}{2}$ in cases (a) and (d)
	$\frac{q+1}{2}$ in cases (b) and (c).
$C_2^{(3)}$	$\frac{q+1}{4}$ in cases (a) and (d).
	$\frac{q-1}{4}$ in cases (b) and (c).
C_3	$\frac{q-1}{3}$ in cases (a) and (c).
	$\frac{q+1}{3}$ in cases (b) and (d).
C_4	$\frac{q+1}{4}$ in cases (a) and (d).
	$\frac{q-1}{4}$ in cases (c) and (b).
$V_4^{(1)}$	1 in all the cases (a) - (d).
$V_4^{(3)}$	1 in all the cases (a) - (d).
D_6	2 in all the cases (a) - (d).
D_8	1 in all the cases (a) - (d).
A_4	1 in all the cases (a) - (d).
H	1 in all the cases (a) - (d).

Now let $\underset{\sim}{N}$ and $\underset{\sim}{Q}$ be the vectors given on p. 128 and M the matrix of table of marks for H. As before, solving for the values of Q_i in the system of linear equations

$$M^T \underset{\sim}{Q}^T = \underset{\sim}{N}^T ,$$

we get

<u>Case (a)</u>

$$\underset{\sim}{Q} = \left(\frac{q^3-123q+662}{576}, \frac{q-7}{4}, 0, \frac{q-7}{6}, \frac{q-3}{8}, 0, 0, 1, 0, 0, 1\right).$$

Hence we have

<u>Table 2.3.4</u>

F	H	D_6	C_4	C_3	A	1
No. of suborbits with stab. = F	1	1	$\frac{q-3}{8}$	$\frac{q-7}{6}$	α	β
Suborbit length	1	4	6	8	12	24

where $A = C_2^{(6)}$, $\alpha = \frac{q-7}{4}$ and $\beta = \frac{q^3-123q+662}{576}$.

Therefore

$$r = \frac{q^3+189q-82}{576}.$$

<u>Case (b)</u>

$$\underset{\sim}{Q} = \left(\frac{q^3-123q+490}{576}, \frac{q-5}{4}, 0, \frac{q-5}{6}, \frac{q-5}{8}, 0, 0, 1, 0, 0, 1\right).$$

Hence we have

Table 2.3.5

F	H	D_6	C_4	C_3	A	1
No. of suborbits with stab. = F	1	1	$\frac{q-5}{8}$	$\frac{q-5}{6}$	α	β
Suborbit length	1	4	6	8	12	24

where $A = C_2^{(6)}$, $\alpha = \frac{q-5}{4}$ and $\beta = \frac{q^3-123q+490}{576}$.

Therefore

$$r = \frac{q^3+189q+82}{576}.$$

Case (c)

$$\underset{\sim}{Q} = \left(\frac{q^3-123q+554}{576}, \frac{q-5}{4}, 0, \frac{q-7}{6}, \frac{q-5}{8}, 0,0,1,0,0,1\right).$$

Hence we have

Table 2.3.6

F	H	D_6	C_4	C_3	A	1
No. of suborbits with stab. = F	1	1	$\frac{q-5}{8}$	$\frac{q-7}{6}$	α	β
Suborbit length	1	4	6	8	12	24

where $A = C_2^{(6)}$, $\alpha = \frac{q-5}{4}$ and $\beta = \frac{q^3-123q+554}{576}$,

Therefore

$$r = \frac{q^3+189q-46}{576}.$$

<u>Case (d)</u>

$$\underset{\sim}{Q} = \left(\frac{q^3-123q+598}{576}, \frac{q-7}{4}, 0, \frac{q-5}{6}, \frac{q-3}{8}, 0, 0, 1, 0, 0, 1\right).$$

Hence we have

<u>Table 2.3.7</u>

F	H	D_6	C_4	C_3	A	1
No. of suborbits with stab. = F	1	1	$\frac{q-3}{8}$	$\frac{q-5}{6}$	α	β
Suborbit length	1	4	6	8	12	24

where $A = C_2^{(6)}$, $\alpha = \frac{q-7}{4}$ and $\beta = \frac{q^3-123q+598}{576}$.

Therefore

$$r = \frac{q^3+189q+46}{576}.$$

<u>5) The subdegrees of G on the cosets of</u> H ≅ PSL(2,q)

Since the degree of G is 2, its subdegrees are: two suborbits, each of length 1.

6) The subdegrees of G on the cosets of H ≅ PGL(2,e), f/m an odd prime

Throughout this part $q = e^h$, h an odd prime. Our first objective will be to determine those subgroups F of H which are isomorphic to $H \cap H^g$ for some $g \in G$.

(a) Suppose that $H \cap H^g$ is isomorphic to C_n with $n|e\pm1$. Then C_n must be the intersection of two maximal cyclic subgroups of H and H^g of the same order $e\pm1$. In G, two cyclic subgroups of the same order are either equal or intersect trivially. Hence $n = e\pm1$ or 1.

(b) Suppose $H \cap H^g \cong D_{2n}(n\neq p)$. Then D_{2n} is the intersection of maximal dihedral subgroups of H and H^g containing D_{2n}. Considering intersections of cyclic subgroups as in (a), we conclude that $n = e\pm1, 2$ or 1.

(c) If $H \cap H^g \cong P_{p^l}(l|m)$, then it is the intersection of maximal elementary abelian p-subgroups of H and H^g; these intersect trivially in G, so $P_{p^l} = P_e$ or 1.

(d) If $H \cap H^g = S_{p^l,n}$ then it is the intersection of maximal subgroups of type $S_{e,e-1}$ in H and H^g.

From (a) and (c), we find that $S_{p^l,n} = S_{e,e-1}$ or 1.

We are now left with the following list of representatives of distinct conjugacy classes of H which may possibly arise as intersections $F = H \cap H^g(g\in G)$:

(i) 1 (ii) ${}^aC_2$ (iii) ${}^bC_2$ (iv) ${}^aV_4$ (v) ${}^bV_4$ (vi) C_{e-1} (vii) C_{e+1} (viii) A_4 (ix) A_5 (x) S_4 (xi) P_e (xii) $D_{2(e-1)}$ (xiii) $D_{2(e+1)}$ (xiv) $S_{e,e-1}$ (xv) $PSL(2,p^l)$ (xvi) $PGL(2,p^l)$

Before doing a further elimination, we calculate m(F) for the subgroups in the list above.

In the remaining portion of this part, $\pm, \mp, \beta = \begin{cases} 0 \\ 2 \end{cases}$ and

$\theta = \begin{cases} 2 \\ 0 \end{cases}$ are read as $e \equiv \pm1 \mod 4$.

Table 2.3.8

F	$\|N_G(F)\|$	$\|N_H(F)\|$	m(F)
1	$q(q^2-1)$	$e(e^2-1)$	$\frac{q(q^2-1)}{e(e^2-1)}$
a_{C_2}	$2(q\mp1)$	$2(e\mp1)$	$\frac{q \mp 1}{e \mp 1}$
b_{C_2}	$2(q\pm1)$	$2(e\pm1)$	$\frac{q \pm 1}{e \pm 1}$
a_{V_4}	24	24	1
b_{V_4}	8	8	1
C_{e-1}	$2(q-1)$	$2(e-1)$	$\frac{q-1}{e-1}$
C_{e+1}	$2(q+1)$	$2(e+1)$	$\frac{q+1}{e+1}$
A_4	24	24	1
A_5	60	60	1
S_4	24	24	1
P_e	q(e-1)	e(e-1)	e^{h-1}
$D_{2(e-1)}$	$2(e-1)$	$2(e-1)$	1
$D_{2(e+1)}$	$2(e+1)$	$2(e+1)$	1
$S_{e,e-1}$	$e(e-1)$	$e(e-1)$	1
$PSL(2,p^l)$	$P^l(P^{2l}-1)$	$P^l(P^{2l}-1)$	1
$PGL(2,p^l)$	$P^l(P^{2l}-1)$	$P^l(P^{2l}-1)$	1

By Lemma 2.1.10, we can eliminate all the subgroups F (except F = H) with m(F) = 1. The conjugacy class representatives of the remaining subgroups are enough for the purpose of computing the subdegrees of G.

Table 2.3.9

Table of marks

	1	$\mathcal{A}$	$\mathcal{B}$	$\mathcal{C}$	$\mathcal{D}$	$\mathcal{E}$	H
1	α	0	0	0	0	0	0
$\mathcal{A}$	β	ω	0	0	0	0	0
$\mathcal{B}$	β	0	λ	0	0	0	0
$\mathcal{C}$	σ	θ	β	2	0	0	0
$\mathcal{D}$	π	β	θ	0	2	0	0
$\mathcal{E}$	μ	0	0	0	0	γ	0
H	1	1	1	1	1	1	1

where $\mathcal{A} = a_{C_2}$, $\mathcal{B} = b_{C_2}$, $\mathcal{C} = C_{e-1}$, $\mathcal{D} = C_{e+1}$, $\mathcal{E} = P_e$ $\alpha = e(e^2-1)$, $\beta = e(e^2-1)/_2$, $\gamma = e-1$, $\sigma = e(e+1)$, $\pi = e(e-1)$, $\mu = (e^2-1)$, $\omega = (e\mp 1)$ and $\lambda = (e\pm 1)$.

Now let $\underset{\sim}{N} = \left(m(1), m({}^aC_2), m({}^bC_2), m(C_{e-1}), m(C_{e+1}), m(P_e), m(H) \right)$ (for the entries of $\underset{\sim}{N}$, see Table 2.3.8), $\underset{\sim}{Q} = (Q_1, Q_2, \ldots, Q_7)$ and M the matrix of table of marks given in Table 2.3.9. Solving for the values of Q_i in the system of linear equations $M^T \underset{\sim}{Q}^T = \underset{\sim}{N}^T$,

We get

$$\underset{\sim}{Q} = \left(\frac{e^{3h-2} - e^{h+2} - e^{h+1} - 2e^{h} + e^{h-1} + e^3 + e^2 + e - 1}{(e^2-1)^2},\ 0,\ 0,\ \frac{e^h - e}{2(e-1)}, \frac{e^h - e}{2(e+1)}, \frac{e^h - e}{e(e-1)}, 1 \right).$$

for both $e \equiv 1 \bmod 4$ and $e \equiv -1 \bmod 4$.

Hence we have

Table 2.3.10

Suborbit length	1	e^2-1	$e(e-1)$	$e(e+1)$	$e(e^2-1)$
No. of Suborbits	1	$\frac{e^h-e}{e(e-1)}$	$\frac{e^h-e}{2(e+1)}$	$\frac{e^h-e}{2(e-1)}$	$\frac{e^{3h-2}-e^{h+2}-e^{h+1}-2e^h+e^{h-1}+e^3+e^2+e-1}{(e^2-1)^2}$

Therefore

$$r = \frac{e^{3h-2}+e^{h+3}-e^{h+1}-3e^h-e^2+2e+1}{(e^2-1)^2} \; .$$

CHAPTER 3

SUBORBITAL GRAPHS CORRESPONDING TO PRIMITIVE PERMUTATION REPRESENTATIONS OF PSL (2,q) AND PGL (2,q)

After having calculated the subdegrees of the primitive permutation representations of the groups PSL (2,q) and PGL (2,q) (see chap 2), the next natural and indeed quite an interesting problem is that of constructing and finding the properties of the suborbital graph corresponding to a given suborbit. This problem is obviously quite complicated and we cannot expect a straightforward answer which covers all the suborbits of a given group.

For groups PSL (2,q) and PGL(2,q), Faradžev and Ivanov [7] have classified the suborbital graphs which are distance-transitive through the approach of determining the distance-transitive representations of these groups.

This chapter is divided into four sections. In section 3.1 we give some notation, definitions and results which will be used in the remainder of the chapter.

In section 3.2 we discuss the suborbits of PSL(2,q) formed by pairs of points of PG(1,q) intersecting $\{0,\infty\}$ in a singleton and give a construction of their corresponding suborbital graphs when PSL(2,q) acts on the cosets of the dihedral subgroup $D_{w(1)}$ fixing $\{0,\infty\}$.

In section 3.3 we give a construction of the suborbital graph of PGL(2,q) corresponding to the suborbit of length 2w(1) when PGL(2,q) acts on the cosets of the dihedral subgroup $D_{2w(1)}$ fixing $\{0,\infty\}$.

In section 3.4 we discuss the suborbits of PGL(2,q) of lengths less than 2w(1) and give a construction of their corresponding suborbital graphs when PGL(2,q) acts on the cosets of the dihedral subgroup $D_{2w(1)}$ fixing $\{0,\infty\}$.

3.1. Suborbital graphs

This section gives background material of the results to be proved later in the chapter. A detailed treatment of the results to be found in this section may be obtained from Sims [19] or Neumann [16].

Let G be a transitive permutation group acting on a set X. Then G acts on X x X by $g(x,y) = (gx,gy)$, $g \in G$, $x,y \in X$. If $0 \subseteq X \times X$ is a G-orbit, then for any $x \in X$, $\Delta = \{ y \in X | (x,y) \in 0 \}$ is a G_x-orbit on X. Conversely if $\Delta \subseteq X$ is a G_x-orbit, then $0=\{(gx,gy) \mid g \in G, y \in \Delta\}$ is a G-orbit on X x X. We say Δ corresponds to 0.

Lemma 3.1.1 Let G be a transitive permutation group acting on X.

Then there are bijections $(\leftrightarrow)$ between:

(a) the set of orbits of G_x on X, for fixed $x \in X$;

(b) the set of orbits of G on $X \times X$;

(c) the set of double cosets $G_x g G_x$, $g \in G$, for fixed $x \in X$.

<u>Proof</u> Since G is transitive on X, by Theorem 1.1.2 the action of G on X is equivalent to action by right multiplication on the right cosets $G_x g$, the G_x-orbit containing $G_x g$ has the form $G_x g G_x$, so $(a) \leftrightarrow (c)$.

Given a G-orbit $\mathcal{O} \subseteq X \times X$, let $\Delta = \{y \in X \mid (x,y) \in \mathcal{O}\}$ for a fixed $x \in X$; one easily checks that Δ is a G_x-orbit. Conversely, given a G_x-orbit $\Delta \subseteq X$, define

$0 = \{(gx, gy) \mid g \in G, y \in \Delta\}$, a G-orbit in $X \times X$.

Then $\Delta \leftrightarrow 0$ gives $(a) \leftrightarrow (b)$. $\square$

The G_x-orbits on X are called <u>suborbits</u> (see §2.1) and

G-orbits on $X \times X$ are called <u>suborbitals.</u>

Let $0_i \subseteq X \times X$, $i = 0, 1, ---, r-1$, be a suborbital. Then

we form a graph Γ_i, by taking X as the set of vertices of Γ_i and by including a directed edge from x to y ($x, y \in X$) if and only if $(x,y) \in O_i$. Thus each suborbital O_i determines a <u>suborbital graph</u> Γ_i.

Now $O_i^* = \{(x,y) \mid (y,x) \in O_i\}$ is a G-orbit. Let Γ_i^* be the suborbital graph corresponding to the suborbital O_i^*. Let the suborbit Δ_i $(i=0,1,---,r-1)$ correspond to the suborbital O_i.

Then Γ_i is <u>undirected</u> if Δ_i is self-paired (because directed edges arise in pairs which are to be amalgamated into a single undirected edge), and Γ_i is directed if Δ_i is not self-paired.

<u>Theorem 3.1.2</u> Let Γ be any suborbital graph for a transitive group G on X. Then $G \leq \text{Aut } \Gamma$, and G is transitive on the vertices of Γ. If Γ is directed then G is transitive on directed edges. If Γ is undirected then G is transitive on ordered pairs of adjacent vertices.

(See Sims [19].)

A graph is said to be <u>connected</u> if for any two points x and y, there is a path from x to y.

<u>Theorem 3.1.3</u> Let G be transitive on X. Then G is primitive if and only if each suborbital graph Γ_i, i=1,2,....,r-1 is

connected.

(See Sims [19].)

3.2 The suborbits of $G = PSL(2,q)$ formed by pairs of points of $PG(1,q)$ intersecting $\{0,\infty\}$ in a singleton when G acts on the cosets of the dihedral subgroup $D_{w(1)}$ and their corresponding suborbital graphs

We recall from parts 2) of § 2.2 that these are the two

suborbits of G formed by pairs of points of u (where <u> is the maximal cyclic subgroup of the dihedral group $D_{w(1)}$ lying in different cycles of unequal lengths in u.

Notation

When $q \equiv 1 \bmod 4$ we shall denote by O_a the suborbital $\{\{0,a\},\{\infty,a\} \mid a$ is a square in $GF(q)$, $a \neq 0\}$ and by O_b the suborbital $\{\{0,b\},\{\infty,b\} \mid b$ is not a square in $GF(q)\}$ and by Δ_a and Γ_a and by Δ_b and Γ_b their corresponding suborbits and suborbital graphs respectively.

When $q \equiv -1 \bmod 4$, we shall denote by O_a^b the suborbital

$\{\{0,a\},\{\infty,b\} \mid a$ is a square in $GF(q)$, $a \neq 0$, b not a square in $GF(q)\}$, by O_b^a the suborbital $\{\{0,b\},\{\infty,a\} \mid a$ is a square in

$GF(q)$, $a \neq 0$, b not a square in $GF(q)\}$ and by Δ_a^b and Γ_a^b and by Δ_b^a and Γ_b^a their corresponding suborbits and suborbital graphs respectively.

<u>Theorem 3.2.1</u> When $q \equiv 1 \bmod 4$, Γ_a and Γ_b are self-paired.

<u>Proof</u> Γ_a: By Lemma 2.2.6, $\{0,1\}$ and $\{0,-1\} \in \Delta_a$.

$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ maps $\{0,\infty\}$ to $\{0,1\}$ and $\{0,-1\}$ to $\{0,\infty\}$. Hence Γ_a is self-paired.

Γ_b: By corollary 2.2.7 $\{0,b\}$, $\{0,-b^{-1}\} \in \Delta_b$.

$\begin{pmatrix} b^{-1} & 0 \\ -1 & b \end{pmatrix}$ maps $\{0,\infty\}$ to $\{0,-b^{-1}\}$ and $\{0,b\}$ to $\{0,\infty\}$.

Hence Γ_b is self-paired. □

<u>Theorem 3.2.2</u> When $q \equiv -1 \bmod 4$, Γ_a^b and Γ_b^a are paired.

<u>Proof</u> Take $\{\infty,1\} \in \Delta_b^a$ and $g=\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$. Then $g(\{\infty,1\})=\{0,\infty\}$ and $g(\{0,\infty\})=\{0,1\} \in \Delta_a^b$.

Hence Γ_a^b and Γ_b^a are paired. $\square$

Given a pair $\{v,h\}$, $v,h \in GF(q)$ $(v \neq h)$; since $PSL(2,q)$ is doubly transitive, there exists a $g \in PSL(2,q)$ such that $g(\infty) = v$ and $g(0) = h$. Our aim here is to express g in terms of v and h and later give a construction for the graphs $\Gamma_a, \Gamma_b, \Gamma_b^a$ and Γ_a^b .

We represent v as $\frac{v}{1}$ and h as $\frac{x}{y}$, where

$$x = h(v-h)^{-1}$$

and

$$y = (v-h)^{-1}.$$

We immediately have,

$$g = \begin{pmatrix} v & h(v-h)^{-1} \\ 1 & (v-h)^{-1} \end{pmatrix} \in PSL(2,q) \text{ ----- } (3.2.1) .$$

If one of v,h, is ∞, put $v = \infty$. Now g becomes

$$\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \text{ -------- } (3.2.2) .$$

Asuming $q \equiv 1 \mod 4$, the following theorem gives a construction for Γ_a .

Theorem 3.2.3 $(\{v,h\}, \{c,d\})$ is in Γ_a for each of the following cases, and only for these

(a) $v,h \neq\infty$, c[or d] = v and d[or c] $=(va+h(v-h)^{-1})(a+(v-h)^{-1})^{-1}$,

(b) $v,h \neq\infty$, c[or d] = h and d[or c] $=(va+h(v-h)^{-1})(a+(v-h)^{-1})^{-1}$,

(c) c[or d] = v = ∞ and d[or c] = a+h

(d) v = ∞, c[or d] = h, and d[or c] = a+h.

Proof (a) Since $(\{\infty,0\}, \{\infty,a\})$ is in Γ_a if $(\{v,h\}, \{c,d\})$ is in Γ_a, there exists $g \in PSL(2,q)$ which sends ∞ to v and o to h. From (3.2.1), we can choose g to be

$$\begin{pmatrix} v & h(v-h)^{-1} \\ 1 & (v-h)^{-1} \end{pmatrix} .$$

Now $g(\{\infty, a\}) = (\{c, d\}) \Rightarrow g(\infty) = c$ [or d] $\Rightarrow v=c$ [or d]

and

$$\begin{pmatrix} v & h(v-h)^{-1} \\ 1 & (v-h)^{-1} \end{pmatrix} \begin{pmatrix} a \\ 1 \end{pmatrix} = \begin{pmatrix} va + h(v-h)^{-1} \\ a + (v-h)^{-1} \end{pmatrix} \Rightarrow$$

d[or c] = $(va+h(v-h)^{-1})(a+(v-h)^{-1})^{-1}$, so (a) holds. Since $(\{\infty,0\}, \{0,a\})$ is in Γ_a, we similarly obtain (b).

If one of v,h is ∞ and taking $v = \infty$, by (3.2.2) we take g to be $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$.

Now repeating the arguments in (a) we obtain (c) and (d). □.

Replacing the a in Theorem 3.2.3 with b we get a construction for Γ_b.

<u>Theorem 3.2.4</u>

When $q \equiv -1 \bmod 4$, $(\{v,h\}, \{c,d\})$ is in Γ_b^a for each of the following cases, and only for these

(a) $v,h \neq \infty$, c[or d] = v and d[or c] $=(va+h(v-h)^{-1})(a+(v-h)^{-1})^{-1}$,

(b) $v,h \neq \infty$, c[or d] = h and d[or c] $=(vb+h(v-h)^{-1})(b+(v-h)^{-1})^{-1}$,

(c) c[or d] = $v = \infty$ and d [or c]= a+h

(d) $v = \infty$, c[or d] = h, and d [or c]= b+h.

<u>Proof</u> We use arguments similar to those in Theorem 3.2.3. □

The construction for Γ_a^b follows from Theorem 3.2.4 after interchanging a and b.

Examples

1. $G = PSL(2,3)$

$u = (0)\ (\infty)\ (1)\ (2)$

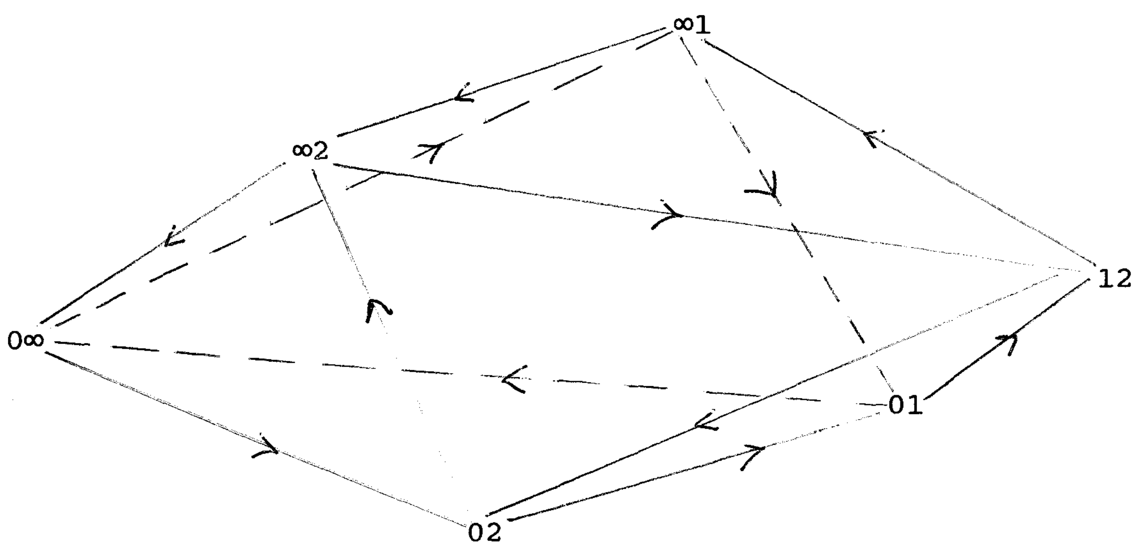
The following are the suborbits of G with each column containing pair of points in the same suborbit.

	$\{\infty, 1\}$	$\{\infty, 2\}$	
$\{0, \infty\}$	$\{0, 2\}$	$\{0, 1\}$	$\{1, 2\}$

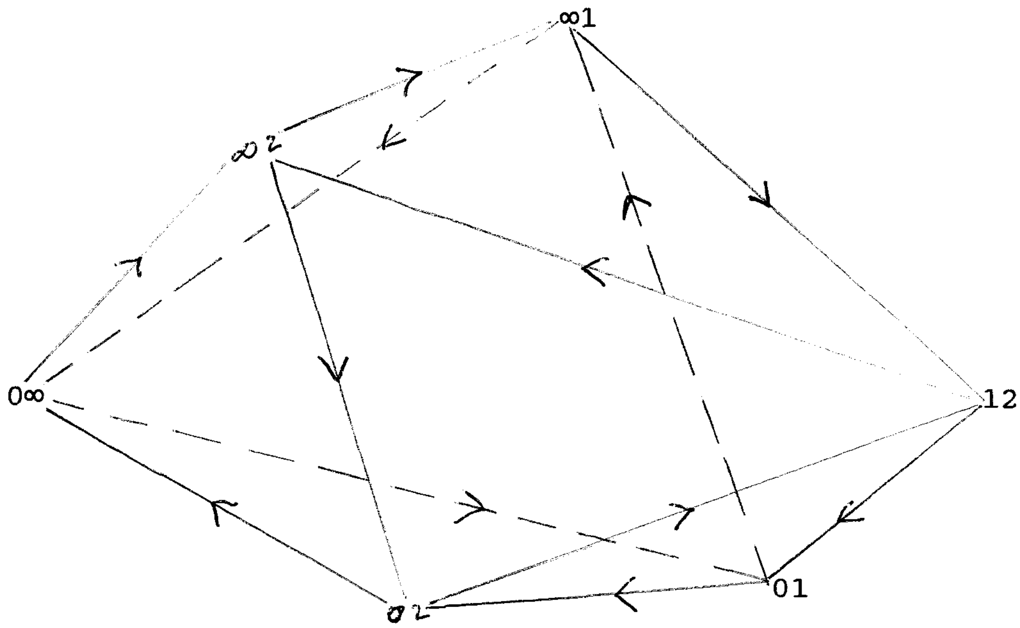
We draw the graphs with unordered pairs $\{a, b\}$ abbreviated to

ab .

Suborbital graph Γ_b^a



Suborbital graph Γ_a^b



Γ_b^a and Γ_a^b are octahedral graphs.

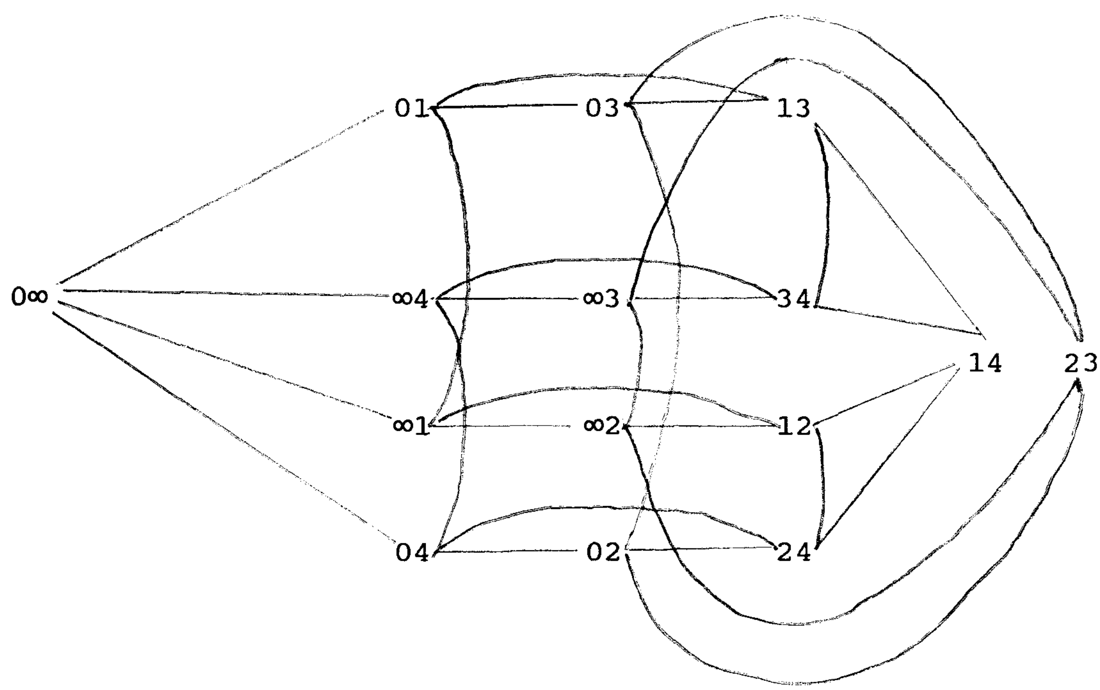
2. $G = PSL(2,5)$

$$u = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} = (o)\,(\infty)\,(14)\,(23)$$

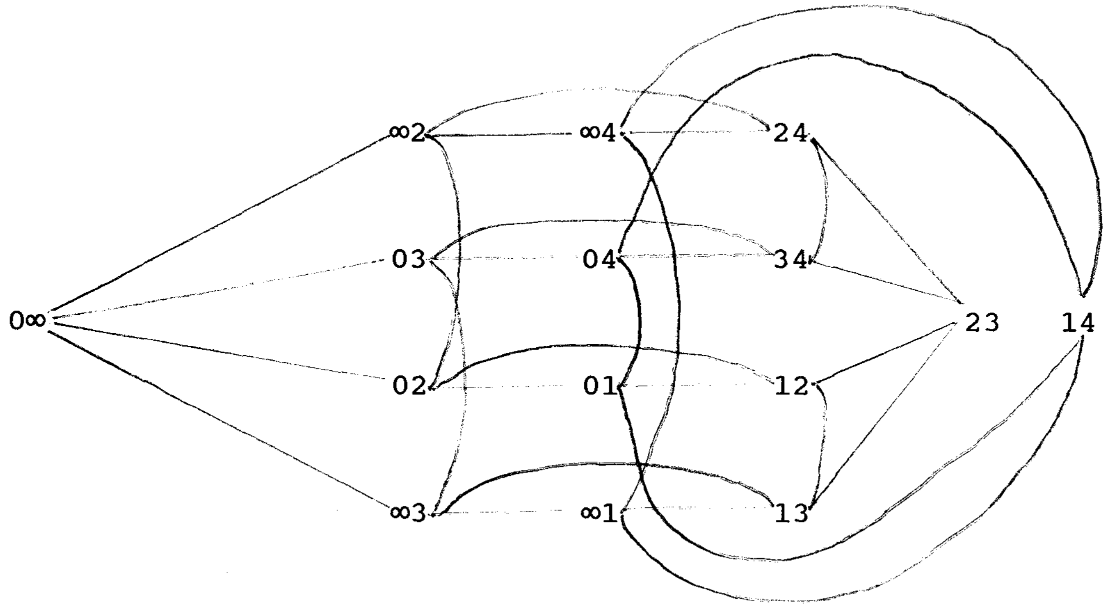
The following are the suborbits of G:

	{0,1}	{0,2}	{1,3}		
{0,∞}	{0,4}	{0,3}	{3,4}	{1,4}	{2,3}
	{∞,1}	{∞,2}	{1,2}		
	{∞,4}	{∞,3}	{1,3}		

Suborbital graph Γ_a



Suborbital graph Γ_b



Lemma 3.2.5 The suborbital graphs $\Gamma_a, \Gamma_b, \Gamma_b^a$ and Γ_a^b all have girth 3.

Proof Γ_a: Since $\{\infty,1\}$, $\{0,1\} \in \Delta_a$ in Γ_a, $\{0,\infty\}$ is adjacent to $\{\infty,1\}$ and $\{0,1\}$. By Lemma 2.2.6 and Theorem 3.2.3 (d) and taking $\{v,h\}$ to be $\{\infty,1\}$ and a to be -1, we find that $(\{0,1\}, \{\infty,1\})$ is an edge in Γ_a, giving a triangle.

Γ_b: Since $\{\infty,b\}$, $\{0,b\} \in \Delta_b$, in Γ_b $\{0,\infty\}$ is adjacent to $\{\infty,b\}$ and $\{0,b\}$. Taking $\{v,h\}$ to be $\{\infty,b\}$ and substituting -b for a in Theorem 3.2.3 (d); by Corollary 2.2.7 and Theorem 3.2.3 (d), $(\{\infty,b\}, \{0,b\})$ is an edge in Γ_b, giving a triangle.

Γ_b^a : $(\{0,\infty\},\{\infty,1\})$ is an edge in Γ_b^a .

By Theorem 3.2.4 (d), $(\{\infty,1\}, \{0,1\})$ is also an edge in Γ_b^a .

Since $\{0,1\}$ is in Δ_a^b, $(\{0,\infty\},\{0,1\})$ is an edge in Γ_a^b . Now we know that Γ_b^a and Γ_a^b are paired and therefore $(\{0,1\},\{0,\infty\})$ is an edge in Γ_b^a , giving us a triangle.

Γ_a^b : Since Γ_b^a and Γ_a^b are paired , Γ_b^a has girth 3 $\leftrightarrow \Gamma_a^b$ has girth 3. $\square$

<u>Theorem 3.2.6</u> $\Gamma_a \cup \Gamma_b$ has diameter 2.

<u>Proof</u> $(\{a,b\}, \{c,d\})$ is an edge in $\Gamma_a \cup \Gamma_b$ if and only if $|\{a,b\} \cap \{c,d\}| = 1$. If $\{x,y\}$ and $\{v,h\}$ are any two vertices not forming an edge in $\Gamma_a \cup \Gamma_b$, then

$d(\{x,y\}, \{v,h\}) \leq d(\{x,y\}, \{y,v\}) + d(\{y,v\}, \{v,h\}) = 2$

Hence $d(\{x,y\}, \{v,h\}) = 2$. $\square$

Let X be a finite set. The <u>Johnson graph</u> of the m-sets in X has vertex set $\binom{X}{m}$, the collection of m-subsets of X. Two vertices x,y are adjacent whenever $x \cap y$ has cardinality m-1.

When X is some unspecified n-set we denote the graph by J(n,m). $\Gamma_a \cup \Gamma_b$ is in the family of graphs J(n,2), usually called the <u>triangular graphs</u> (see Higman [12]).

<u>Theorem 3.2.7</u> Γ_a and Γ_b are isomorphic.

<u>Proof</u> Let β be a generator of $GF(q)^*$ and

$$\begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix} = (0)(\infty)\,((a_1\ a_2\ ---\ a_{w(2)})(b_1\ b_2\ ---\ b_{w(2)})\ ,$$

where a_i and b_i are squares and non-squares in $GF(q)^*$ respectively.

$$\text{Let}\quad \gamma = \begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix} = (0)(\infty)\,(a_1 b_1 a_2 b_2\ ---\ a_{w(2)}\ \ b_{w(2)})\ .$$

From Theorem 3.2.6, we have immediately

$\gamma : \Gamma_a \to \Gamma_b$ is an isomorphism defined by $\gamma(a_i) = b_i$. □

<u>3.3 The suborbital graph Γ of G = PGL(2,q) corresponding to the suborbit of length 2w(1) when G acts on the coset of the dihedral subgroup</u> $D_{2w(1)}$.

The suborbit under consideration is the only suborbit of length 2w(1) and therefore it must be self-paired (see part 2) of

§ 2.3).

Since G is doubly transitive; given a pair $\{v,h\}$, $v \neq h$, v, $h \in PG(1,q)$, there exists $g \in G$ such that $g(\infty) = v$ and $g(0) = h$.

For v, $h \neq \infty$, g can be chosen to be $\begin{pmatrix} v & h \\ 1 & 1 \end{pmatrix}$. If either v or h is ∞, then we can choose g to be $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} v & 1 \\ 1 & 0 \end{pmatrix}$ respectively. Now let β be a generator of $GF(q)^*$; using the ideas above, we construct the suborbital graph Γ as follows:

<u>Theorem 3.3.1</u> $(\{v,h\}, \{c,d\})$ is an edge in Γ for each of the following cases, and only for these

(a) $v,h \neq \infty$, $v = c$[or d] and d[or c] $= (v\beta^i + h)(\beta^i + 1)^{-1}$,

(b) $v,h \neq \infty$, $h = c$[or d] and d[or c] $= (v\beta^i + h)(\beta^i + 1)^{-1}$,

(c) $v = \infty$, $v = c$[or d] and d[or c] $= \beta^i + h$,

(d) $v = \infty$, $h = c$[or d] and d[or c] $= \beta^i + h$,

(e) $h = \infty$, $v = c$[or d] and d[or c] $= (v\beta^i + 1)\beta^{-i}$,

(f) $h = \infty$, $h = c$[or d] and d[or c] $= (v\beta^i + 1)\beta^{-i}$,

where $1 \leq i \leq w(1)$.

<u>Proof</u> See the proof of Theorem 3.2.3. □

We note that $\Gamma = \Gamma_a \cup \Gamma_b$ (see Theorem 3.2.6) is the Johnson graph $J(n,2)$.

It was shown by Higman [12] that the full automorphism group of the Johnson graph $J(n,2)$ is S_n when $n > 4$.

From Lemma 3.2.5, the girth of Γ is 3; in fact it can straightfordwardly be seen that if $\{x,y\},\{y,v\}$ and $\{x,v\}$, $v \neq x,y$ are vertices of Γ, they form a circuit of length 3.

3.4 Suborbital graphs Γ of $G = PGL(2,q)$ corresponding to the suborbits of lengths less than $2w(1)$ when G acts on the cosets of the dihedral subgroup $D_{2w(1)}$

Let Δ be a suborbit of length less than $2w(1)$. Then Δ has a representative $\{1,x\}$ for some $x \in GF(q)^*$.

Lemma 3.4.1 If $\{1,x\} \in \Delta$, then $\{1,x^{-1}\} \in \Delta$.

Proof $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in D_{2w(1)}$ maps $\{1,x\}$ to $\{1,x^{-1}\}$. □

Lemma 3.4.2 If $\{1,x\} \in \Delta$, then $\{-1,-x\} \in \Delta$.

Proof $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in D_{2w(1)}$ maps $\{1,x\}$ to $\{-1,-x\}$. □

Lemma 3.4.3 Δ is self-paired.

Proof The transformation $\begin{pmatrix} -1 & x \\ 1 & -1 \end{pmatrix}$ takes $\{1,x\}$ to $\{0,\infty\}$ and $\{0,\infty\}$ to $\{-x,-1\}$. Hence by Lemma 3.4.2 Δ is self-paired. □

Let β be a generator of $GF(q)^*$ and as before let $\{1,x\}$ be a representative of the suborbit Δ. The elements in this suborbit are of the form $\{\beta^i, x\beta^i\}$, where $1 \le i \le w(1)$.

By arguments similar to those in Theorem 3.2.3, we have:

<u>Theorem 3.4.4</u> $(\{v,h\},\{c,d\})$ is an edge in Γ for each of the following cases, and only for these

(a) $c[\text{or } d]=(v\beta^i + h)(\beta^i + 1)^{-1}$ and $d[\text{or } c]=(vx\beta^i + h)(x\beta^i +1)^{-1}$,

(b) $v = \infty$, $c[\text{or } d] = \beta^i + h$ and $d[\text{or } c] = x\beta^i + h$,

(c) $h = \infty$, $c[\text{or } d] =\beta^{-i}(v\beta^i + 1)$ and $d[\text{or } c] = (x\beta^i)^{-1}(vx\beta^i + 1)$.

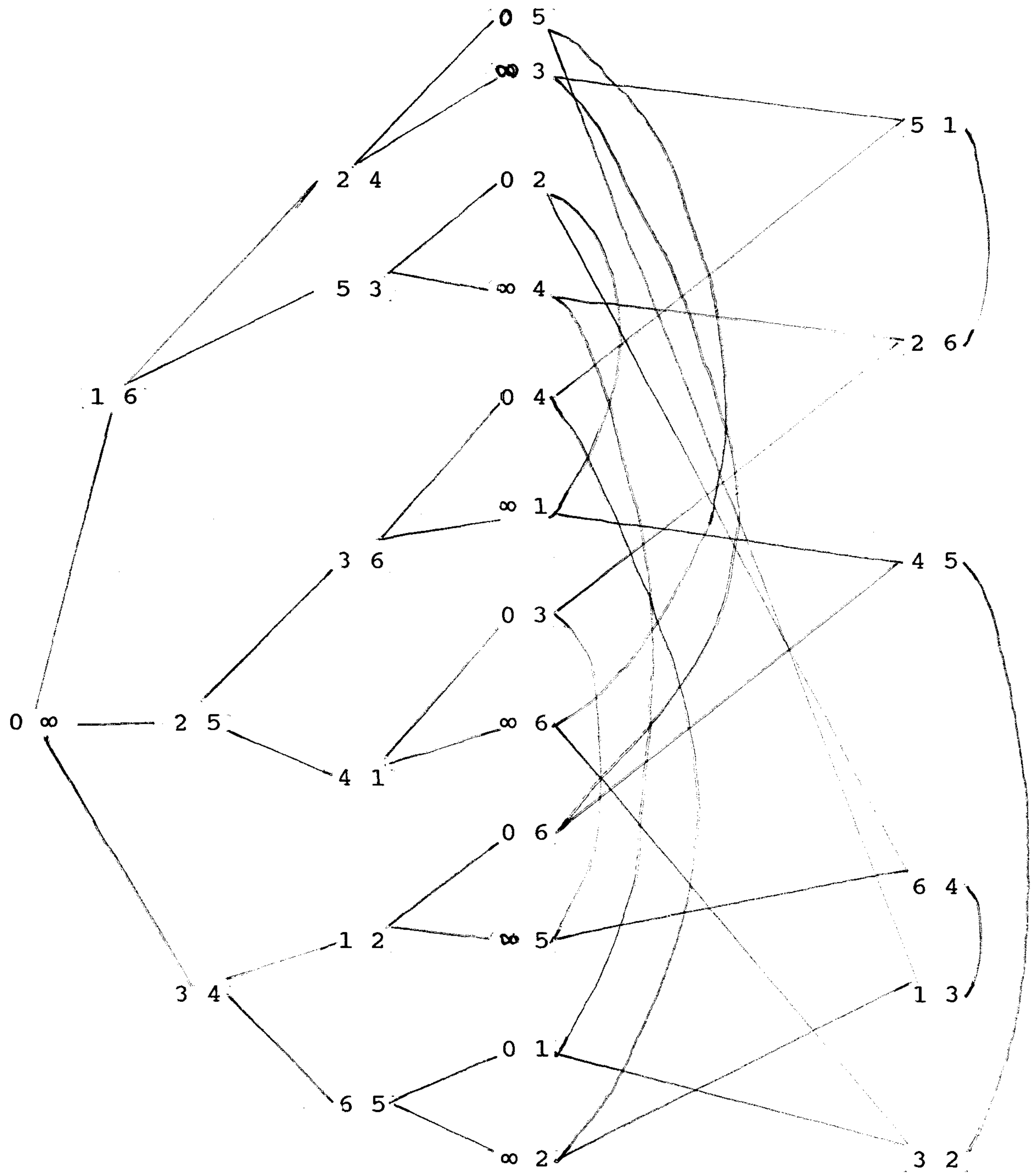
<u>Theorem 3.4.5</u> If $x \neq -1$, diam $\Gamma \le 4$ and if $x = -1$, diam $\Gamma \le 6$.

(See Bon and Cohen [3].)

As an example, we use Theorem 3.4.4 to construct the suborbital graph of PGL(2,7) with $\{1,-1\}$ as a representative of Δ.

$\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} = (0)(\infty)\ (132645)$ generates the maximal cyclic subgroup

of D_{12}.



This graph was described by Tutte [22] and he ascribed it to H.S.M. Coxeter. The graph has been studied in details by Biggs [2]. For other description of this graph, one may refer to

Biggs and Smith [1]. This graph is among the twelve trivalent graphs whose automorphism groups act transitively on pairs of vertices at each particular distance apart (trivalent distance-transitive graphs) (see Biggs and Smith [1]). This graph is also among the list of the four trivalent distance-transitive graphs whose automorphism groups act primitively on their vertices (see Biggs [1]). In [1], Biggs has shown that like the famous Petersen graph, the Coxeter graph only just fails to be Hamiltonian.

Other suborbital graphs of projective linear groups which have been studied extensively are the Biggs-Smith graph and Perkel graph corresponding to a suborbit of PSL(2,17) and PSL(2,19) with S_4 and A_5 as the stabilizers respectively. Bon and Cohen [3] have shown these graphs to be distance-transitive.

CHAPTER 4

INTERSECTION MATRICES FOR G = PGL (2,q)

This chapter is divided into two sections. In section 4.1 we give some notation, definitions and results to be used later in the chapter. In section 4.2 we find the general form of the intersection matrix of G relative to the suborbit of length 2w(1) when G acts on the cosets of its dihedral subgroup $D_{2w(1)}$ fixing $\{0,\infty\}$.

4.1 intersection matrices for finite permutation groups

In this section we shall briefly consider the matrix M of intersection numbers of a suborbit Δ of a group G on a finite set X. For detailed treatment we refer the reader to Higman [11]. For the most part we adhere to the notation of that paper. We also mention briefly the algebra spanned by the adjacency matrices corresponding to suborbital graphs of G on X and the connection between the intersection numbers and the multiplication constants defined by Neumann [16] p. 106.

Let G be a finite group acting on a finite set X and $\Delta_{\ell}(a)$ be the ℓ^{th} G_a-orbit for $a \in X$ and for a given arrangement of the G_a-orbits.

The G_b-orbits are also arranged such that if $b \in X$ and g(a) = b, then $g(\Delta_{\ell}(a)) = \Delta_{\ell}(g(a)) = \Delta_{\ell}(b)$.

The intersection numbers relative to a suborbit $\Delta_{\ell}(a)$ are defined by

$$\mu_{ij}^{\ell} = |\Delta_{\ell}(b) \cap \Delta_i(a)| \qquad [b \in \Delta_j(a)] .$$

If the rank of G is r, then the r x r matrix $M_{\ell} = \left(\mu_{ij}^{(\ell)}\right)_{i,j}$ is called the <u>intersection matrix</u> of $\Delta_{\ell}(a)$. If $|\Delta_i| = n_i$ and as we had before $\Delta_i^* = \Delta_{i*}$ is the suborbit paired with Δ_i ; Higman [11] showed that

Theorem 4.1.1 (a) $\mu_{io}^{(l)} = \begin{cases} n_i \ if \ i = l, \\ 0 \ if \ i \neq l. \end{cases}$

(b) $\mu_{oj}^{(l)} = \begin{cases} 1 \ if \ j = l^*, \\ 0 \ if \ j \neq l^*. \end{cases}$

(c) $n_j\mu_{ij}^{(l)} = n_i\mu_{ji}^{(l^*)}$ and $n_i\mu_{l^*i}^{(j)} = n_j\mu_{i^*j}^{(l)} = n_l\mu_{j^*l}^{(i)}$.

Theorem 4.1.2 M_l has column-sum n_l, and $M_lL = n_lL$ where L is transpose of the vector $(n_0, n_1, \ldots, n_{r-1})$.

Now let the orbits of a stabilizer

G_a on X be $\Delta_0, \Delta_1, \ldots, \Delta_{r-1}$ and the corresponding orbits of G on

X x X be 0_0, 0_1, $0_2, \ldots, 0_{r-1}$.

We define the corresponding adjacency matrices B_0, $B_1, \ldots, B_{r-1}$ to be n x n matrices where $n = |X|$ with rows and columns indexed by X, where $(B_i)_{x,y} = \begin{cases} 1 \ if \ (x,y) \in 0_i, \\ 0 \ if \ (x,y) \notin 0_i. \end{cases}$

If we identify G with a group of permutation matrices P_g in the usual way:

$P_g = (g_{x,y})$ where

$g_{x,y} = \begin{cases} 1 \ if \ g(x) = y, \\ 0 \ if \ g(x) \neq y, \end{cases}$

we have

<u>Lemma 4.1.3</u> The set $\{B_0, B_1, \ldots\ldots, B_{r-1}\}$ is a basis for the space V of all matrices over C commuting with every element of G.

(see Neumann [16], Lemma 5.)

<u>Corollary 4.1.4</u> The space V spanned by the adjacency matrices $B_0, B_1, \ldots\ldots, B_{r-1}$ is an algebra. That is, there exist integers $a_{ijl} \geq 0$ such that $B_i B_j = \sum_{l=0}^{r-1} a_{ijl} B_l$.

If O_i, O_j are suborbitals, with suborbital graphs Γ_i, Γ_j and adjacency matrices B_i, B_j, the constant a_{ijl} (see corollary 4.1.4) is the number of triangles 

based on a given pair$(x,y) \in O_l$ where the edges labelled i,j,l belong to Γ_i, Γ_j, Γ_l. The non-negative integers a_{ijl} are called the <u>multiplication constants</u>. The multiplication constant a_{ijl} is the same as the intersection number $\mu_{il}^{(j^*)}$

(see Neumann 16, p.106).

4.2 Intersection matrices for $G = PGL(2,q)$ on the cosets of $D_{2w(1)}$

In this section we shall find the general form of the intersection matrix of G on $D_{2w(1)}$ relative to the suborbit of length 2w(1) for q both odd and even. Some multiplication constants can easily be got from this intersection matrix according to the discussion we had in section 4.1. In particular the number of triangles on every edge of the suborbital graph corresponding to this intersection matrix is found.

The suborbits of G on $D_{2w(1)}$ were discussed in length in section 2.3. In what follows we assume the knowledge of that section. In section 3.3 and 3.4 all these suborbits were shown to be self-paired.

We start by considering the case when q is odd.

Throughout the suborbits of G are assumed to have the following arrangement:-

$$\Delta_0 = \{0, \infty\}, \Delta_1, \Delta_2, \ldots, \Delta_{\frac{q-3}{q}}, \Delta_{w(2)}, \Delta_{z(2)},$$

Where

$$|\Delta_1| = |\Delta_2| = \ldots . = |\Delta_{\frac{q-3}{2}}| = w(1),$$

$$|\Delta_{w(2)}| = w(2) \quad \text{and} \quad |\Delta_{z(2)}| = 2w(1).$$

Let β be a generator of $GF(q)^*$; we can then take

$u = \begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix}$, which in disjoint cycle decomposition form is

$(0)(\infty)(1\ \beta\ \beta^2 \ldots \beta^{q-2})$, to be a generator of the maximal cyclic subgroup of $D_{2w(1)}$.

The suborbits $\Delta_i, 1 \le i \le w(2)$ are arranged in such a way that Δ_i has a representative $\{1, \beta^i\}$, while $\{1, 0\}$ is a representative of $\Delta_{z(2)}$.

We now compute the intersection matrix $M_{z(2)}$. We compute the intersection numbers in several steps:

<u>(i) The intersection numbers $\mu^{z(2)}_{i,\ell}$ and $\mu^{z(2)}_{i,z(2)}$, Where</u>

<u>$\ell \neq z(2)$, $i \neq w(2), z(2)$</u>

$$\Delta_i\{0,\infty\} = \Big\{ \{1,\beta^i\},\{\beta,\beta^{i+1}\},\{\beta^2,\beta^{i+2}\},\{\beta^3,\beta^{i+3}\},\ldots$$
$$\ldots,\{\beta^{q-2-i},\beta^{q-2}\},\{\beta^{q-1-i},1\},\{\beta^{q-i},\beta\},\{\beta^{q-i+1},\beta^2\}\ldots$$
$$\ldots\{\beta^{q-2},\beta^{i-1}\}\Big\} \qquad \text{------}(4.2.1)$$

$$\Delta_{z(2)}\{1,\beta^{l}\} = \{\{1,0\},\{1,\infty\},\{\beta^{l},0\},\{\beta^{l},\infty\},\{\bigcup_{j\neq 0,l}\{1,\beta^{j}\}\},\{\bigcup_{j\neq 0,l}\{\beta^{l},\beta^{j}\}\}\}$$

--------- (4.2.2)

$$\Delta_{z(2)}\{1,0\} = \{\{\bigcup_{j\neq 0}\{1,\beta^{j}\}\},\{\bigcup_{j\neq 0}\{0,\beta^{j}\}\},\{0,\infty\},\{1,\infty\}\} \quad - (4.2.3).$$

(a) If $i=l$, (4.2.1) and (4.2.2) intersect at $\{\beta^{q-1-i},1\}$ and $\{\beta^{l},\ \beta^{2l}\}$.

Hence $\mu_{i,i}^{(z(2))} = 2$.

(b) If $i\neq l$, (4.21) and (4.22) intersect at

$$\left\{\{1,\beta^{i}\},\{\beta^{q-1-i},1\},\{\beta^{l},\beta^{i+l}\},\{\beta^{q-i+l-1},\beta^{l}\}\right\}.$$

Hence

$$\mu_{i,l}^{(z(2))} = 4.$$

(c) (4.2.1) and (4.2.3) intersect at $\{1,\beta^{i}\}$ and $\{\beta^{q-1-i},1\}$.

Hence

$$\mu_{i,z(2)}^{(z(2))} = 2.$$

(ii) The intersection numbers $\mu^{z(2)}_{w(2),l}$, $l \neq z(2)$ and $\mu^{z(2)}_{w(2),z(2)}$.

$$\Delta_{w(2)}\{0,\infty\} = \left\{\{1,\beta^{w(2)}\},\{\beta,\beta^{z(2)}\},\{\beta^2,\beta^{(q+3)/2}\},\ldots,\{\beta^{(q-3)/2},\beta^{q-2}\}\right\}$$

----------(4.2.4).

(d) If $l=w(2)$, (4.2.2) and (4.2.4) have empty intersection.

Hence

$$\mu^{(z(2))}_{w(2),w(2)} = 0 .$$

(e) If $l \neq w(2)$, (4.2.2) and (4.2.4) intersect at $\{1,\beta^{w(2)}\}$ and $\{\beta^l,\beta^{(q-1+2l)/2}\}$.

Hence

$$\mu^{(z(2))}_{w(2),l} = 2 .$$

(f) (4.2.3) and (4.2.4) intersect at $\{1,\beta^{w(2)}\}$.

Hence $\mu^{(z(2))}_{w(2),z(2)} = 1$.

(iii) intersection numbers $\mu^{(z(2))}_{z(2),l}$

$$\Delta_{z(2)}\{0,\infty\} = \left\{\{\cup\{0,\beta^i\}\},\{\cup\{\infty,\beta^j\}\}\right\} \text{ ---- } (4.2.5)$$

(g) If $l=z(2)$, then (4.2.2) and (4.2.5) intersect at $\left\{\{1,\infty\},\{\cup_{j\neq 0}\{0,\beta^j\}\}\right\}$.

Hence $\mu^{(z(2))}_{z(2),z(2)} = w(1)$.

(h) If $\iota \neq z(2)$, then (4.2.2) and (4.2.5) intersect at $\{\{1,0\},\{1,\infty\},\{\beta^{\iota},0\},\{\beta^{\iota},\infty\}\}$.

Hence $\mu^{(z(2))}_{z(2),1} = 4$. .

Combining Theorem 4.1.1 (a) and (b) with (a) - (h) above we have

<u>Theorem 4.2.1</u> The intersection matrix $M_{z(2)}$ when q is odd is of the form

$$\begin{pmatrix} 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 \\ 0 & 2 & 4 & 4 & \cdots & 4 & 4 & 2 \\ 0 & 4 & 2 & 4 & \cdots & 4 & 4 & 2 \\ \cdot & \cdot & \cdot & \cdot & \cdots & \cdot & \cdot & \cdot \\ 0 & 4 & 4 & 4 & \cdots & 2 & 4 & 2 \\ 0 & 2 & 2 & 2 & \cdots & 2 & 0 & 1 \\ 2w(1) & 4 & 4 & 4 & \cdots & 4 & 4 & w(1) \end{pmatrix}$$

<u>Examples</u>

(1) <u>When q=3</u>

$$M_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 4 & 4 & 2 \end{pmatrix}$$

(2) <u>When q=5</u>

$$M_3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 2 & 4 & 2 \\ 0 & 2 & 0 & 1 \\ 8 & 4 & 4 & 4 \end{pmatrix}$$

(3) <u>When q=7</u>

$$M_4 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 2 & 4 & 4 & 2 \\ 0 & 4 & 2 & 4 & 2 \\ 0 & 2 & 2 & 0 & 1 \\ 12 & 4 & 4 & 4 & 6 \end{pmatrix}$$

Next we consider the case when q is even.

The arrangements of the suborbits of G is taken as follows:-

$\Delta_0 = \{0, \infty\}, \Delta_1, \ldots\ldots, \Delta_{\frac{q-2}{2}}, \Delta_{\frac{q}{2}},$

where $|\Delta_1| = |\Delta_2| = \ldots\ldots = |\Delta_{\frac{q-2}{2}}| = w(1)$, $|\Delta_{\frac{q}{2}}| = 2w(1)$ and for

a generator β of $GF(q)^*$, Δ_i has a representative $\{1,\beta^i\}$ for

$1 \le i \le \frac{q-2}{2}$, while $\{1,0\}$ is a representative for the suborbit $\Delta_{\frac{q}{2}}$.

We now compute the intersection matrix $M_{\frac{q}{2}}$.

As in the previous case, $\Delta_i\{0,\infty\}$, $\Delta_{\frac{q}{2}}\{1,\beta^{l}\}$, $\Delta_{\frac{q}{2}}\{1,0\}$, and $\Delta_{\frac{q}{2}}\{0,\infty\}$ can easily be found. Arguments similar to those used before give us

<u>Theorem 4.2.2</u> The intersecting Matrix $M_{q/2}$

is of the form

$$\begin{pmatrix}
0 & 0 & 0 & 0 & \ldots\ldots\ldots\ldots & 0 & 0 & 1 \\
0 & 2 & 4 & 4 & \ldots\ldots\ldots\ldots & 4 & 4 & 2 \\
0 & 4 & 2 & 4 & \ldots\ldots\ldots\ldots & 4 & 4 & 2 \\
0 & 4 & 4 & 2 & \ldots\ldots\ldots\ldots & 4 & 4 & 2 \\
. & . & . & . & \ldots\ldots\ldots\ldots & . & . & . \\
0 & 4 & 4 & 4 & \ldots\ldots\ldots\ldots & 4 & 2 & 2 \\
2w(1) & 4 & 4 & 4 & \ldots\ldots\ldots\ldots & 4 & 4 & w(1)
\end{pmatrix}$$

Since in general the multiplication constant a_{ijl} is the same as the intersection number $\mu_{i\ell}^{(j^*)}$, from Theorems 4.1.1 and 4.2.1 we can easily get the multiplication constants $a_{iz(2)\ell}$, $a_{z(2)j\ell}$ and $a_{ijz(2)}$ for $0 \leq i,j,\ell \leq z(2)$. Similarly Theorems 4.1.1 and 4.2.2 give us multiplication constants $a_{i\frac{q}{2}\ell}$, $a_{\frac{q}{2}j\ell}$ and $a_{ij\frac{q}{2}}$ for $0 \leq i,j,\ell \leq \frac{q}{2}$.

In particular if $\tau_{z(2)}$ and $\tau_{\frac{q}{2}}$ are the suborbital graphs corresponding to the intersection matrices $M_{z(2)}$ and $M_{\frac{q}{2}}$ respectively, we have

<u>Lemma 4.2.3</u> The number of triangles on every edge of $\tau_{z(2)}$ and $\tau_{\frac{q}{2}}$ is w(1).

<u>Proof</u>

The number of triangles on each edge in the graphs $\tau_{z(2)}$ and $\tau_{\frac{q}{2}}$

are the multiplication constants $a_{z(2)z(2)z(2)}$ and $a_{\frac{q}{2}\frac{q}{2}\frac{q}{2}}$ which we find from Theorems 4.2.1 and 4.2.2 to be w(1). □

REFERENCES

1. Biggs N. L. and Smith D. H., On trivalent graphs, Bull. London Math. Soc. 1971(3) 155-158.

2. Biggs N. L., Three remarkable graphs, Canad J. Math. 1973(25) 397-411.

3. Bon J. V. and Cohen A. M., Linear groups and distance - transitive graphs, Enrop. J. Combinatorics 1989(10) 399-411.

4. Burnside W., Theory of groups of finite order (2nd ed.) Cambridge University Press, 1911: reprinted Dover, New York 1955.

5. Coxeter H. S. M., My graph, Proc. London Math. Soc. 1983(46) 117-136.

6. Dickson L. E., Linear groups with an exposition of the Galois field theory, Teubner, Leipzig, 1901, reprinted Dover, New York, 1958.

7. Faradžev I. A. and Ivanov. A. A., Distance - transitive representations of groups G with $PSL(2,q) \trianglelefteq G \leq P\Gamma L(2,q)$,Europ. J. Combinatorics (1990) 11 347-356.

8. Harary F., A seminar on graph theory, Holt, Rinehart and Winston, New York, 1967.

9. ____________, Graph theory, Addison - Wesley, Reading MA, 1969.

10. Hardy G. H. and Wright E. M., An introduction to the theory of numbers, Oxford University Press, 1938.

11. Higman D. G., Intersection matrices for finite permutation groups, J. Algebra 1967 (6) 22-42.

12. ____________, Characterization of families of rank 3 permutation groups by subdegrees I. Arch, Math. 1970 (21) 151-156.

13. Huppert B., Endliche Gruppen I, Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer, Berlin 1967.

14. Ivanov A. A., Klin M. K., Tsaranov S. V., and Shpektorov S. V., On the problem of computing the subdegrees of transitive permutation groups, Sov. Math. Surv. 1983 (38) 123-124.

15. Krishnamurthy V. Combinatorics, theory and applications, Ellis Horwood, Chichester, 1986.

16. Neumann P. M., Finite permutation groups, Edge - coloured graphs and matrices, Topics in group theory and computation, edited by M. P. J. Curran, Academic Press, London, 1977.

17. Redfield J. H., The theory of group-reduced distributions, Amer. J. Math. 1927 (49) 433-455.

18. Rose J. S. A course on group theory, Cambridge University Press 1978.

19. Sims C. C., Graphs and finite permutation groups, Math. Z. 1967 (95) 76-86.

20. Suzuki M., Group theory I, Springer Berlin, 1982.

21. Tchuda F. L., Combinatorial-geometric characterizations of some primitive representations of the groups PSL(n,q) for n=2,3, Ph.D. thesis, Kiev, 1986 in Russian.

22. Tutte W. T., A non-Hamiltonian graph, Canad. Math. Bull. 1960 (3) 1-5.

23. Valentini R. C. and Madan M., A Haupsatz of L. E. Dickson and Artin-Schreier extensions, J, Reine Angew. Math. 318 (1980) 156-177

24. White D. E., Counting patterns with a given automorphism group, proc. of Amer. Math. Soc., 1975 (47) 41-44