MÖBIUS INVERSION OF SOME CLASSICAL GROUPS AND THEIR APPLICATION TO THE ENUMERATION OF REGULAR HYPERMAPS.

by

M.L.N. Downs

A thesis submitted for the degree of

Doctor of Philosophy

Faculty of Mathematical Studies

University of Southampton.

May 1988

To my dearest Yanna

CONTENTS

ACKNOWLEDGEMENTS

My thanks to the staff of and my colleagues at the faculty, for creating a most pleasant working environment.

My especial thanks to my supervisor, Dr. G.A. Jones, for his open readiness in giving suggestions, help and encouragement throughout the last four years.

My appreciation of and affection to my family for their support in so many ways both material and emotional.

My appreciation at the professional way this treatise has been typed.

Finally my thanks to two institutions, with hopes that both will survive to see more enlightened days. Firstly the S.E.R.C. for giving me financial support, secondly the N.H.S. without the care of which I would not subsequently have been able to complete this thesis.

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

FACULTY OF MATHEMATICAL STUDIES

Doctor of Philosophy

MÖBIUS INVERSION OF SOME CLASSICAL GROUPS AND THEIR APPLICATION TO THE ENUMERATION OF REGULAR HYPERMAPS.

by M.L.N. Downs

For any group Γ abstractly defined by some finite presentation, a method (called Hall's method) is known for calculating the number $d_\Gamma(G)$ of normal subgroups N of Γ for which the quotient group Γ/N is of some preset isomorphism type G. This technique is dependent on the knowledge of the Möbius function μ_G on the subgroup lattice of G. We apply this method by use of the following proposition: if Γ is any group with a finite 2-generator presentation and with relator set R, then $d_\Gamma(G)$ gives the number of regular oriented hypermaps with automorphism group G which satisfy certain well-defined local properties determined by the relators R.

In chapter 1 we review the established theories of Hall's method and of regular hypermaps (including unoriented hypermaps) and discuss their relationship as above.

In chapter 2 the function μ_G is calculated for $G = PSL_2(q)$ or $PGL_2(q)$ for any prime power q (extending an existing result for primes). In chapter 3 these results are applied to explicitly make some enumerations of various specific categories of regular hypermaps. (However some other enumerations are made by a different method, based on trace.)

Chapters 4 and 5 specialise mostly to triangular maps. Chapter 4 examines the local properties of regular oriented triangular maps with automorphism group $G \cong PSL_2(q)$ or $PGL_2(q)$ for some q, in particular how to distinguish two such maps with the same automorphism group. Chapter 5 describes how some of these same maps may be constructed in a different way, each one as the unique triangular imbedding of a graph with vertices defined as the elements of a particular conjugacy class in G.

INTRODUCTION

To start, I give a preview of the description of the basic ideas which form the motivation and foundation of all the subsequent work. This is to give a précis of Chapter 1, in which the group theoretic character of maps is explained (by ideas mostly due to [12])as is the role of Möbius inversion in our calculations (by ideas mostly due to [7]). After this, I summarise the rest of the content in this thesis, chapter by chapter.

An oriented map $\mathcal{M}$ is intuitively thought of as a graph $\mathcal{G}$ where each set of edges incident with a particular vertex v in $\mathcal{G}$ is given a cyclic order. (For our purposes, $|\mathcal{G}|$ is always finite). Clearly to express all these cycles in some single permutation z, this permutation must act on the set Ω of directed edges (which we call darts) of $\mathcal{G}$. To give a unique description of $\mathcal{M}$ then, it is evident that we need only specify a set Ω of darts, and the permutations x and z of Ω, where x is the involution taking each dart to the opposite dart on the same edge. The vertices of $\mathcal{G}$ then can be thought of just as the cycles of z. An isomorphism of maps then is a bijection between the respective sets of darts that preserve both adjacency and cyclic ordering of darts at vertices. A regular map is one for which the automorphism group is transitive on the darts.

As one would expect (though of course it is technically messy to reconcile the topology with the algebraic definition of a map as intimated above), it is possible to represent $\mathcal{M}$ in some oriented surface $, and so we may regard $\mathcal{M}$ as an imbedding of the graph $\mathcal{G}$ in the surface $. In this imbedding, the cycles of the permutations $y:=xz^{-1}$ describe the 'faces of the map' in an obvious way.

The actual definition of a map $\mathcal{M}$ we use specifies Ω, x and y (rather than z). If we no longer constrain the order of x to be two, the resultant broader definition is that for oriented hypermaps. (We also consider unoriented hypermaps, where we specify three permutations of order two acting on a given set Ω).

For oriented hypermaps $\mathcal{H}$ (but with analogous conventions and predicates for regular unoriented hypermaps) we let $G := \langle x,y \rangle$ and label the hypermap $\mathcal{H}$ by the quadruple (G, Ω, x, y). We shall see that if $\mathcal{H}$ is regular then

(i) $G \cong \mathrm{Aut}\mathcal{H}$

(ii) if $\mathcal{H}_1 = (G, \Omega, x_1, y_1)$ is another oriented hypermap defined on the same set Ω of darts, then $\mathcal{H} \cong \mathcal{H}_1$ if and only if there is a group automorphism α of G such that

$$\alpha : x \mapsto x_1 \quad \text{and} \quad \alpha : y \mapsto y_1.$$

In fact for any given finite group G, there is a correspondence between the regular oriented hypermaps with automorphism group G and the classes under AutG of generating pairs (x,y) of elements of G. We endeavour to count these classes.

The technique we use is one of methodical exhaustion, called Möbius inversion. Suppose one has a set S of subsets of another set M for which M itself is an element of S (for example, M could be the group G and S the set of subgroups of G). Then the Möbius function μ associated with S is defined by

$$\mu(M) = 1$$

and all other values $\mu(L)$ for $L \in S$ are defined inductively by

$$\sum_{L \subseteq N \subseteq M} \mu(N) = 0$$

where the summation is over all elements N of S that contain L, as subsets of M. Then it is soon evident that if $\sigma, \varphi : S \to \mathbb{Z}$ are functions such that $\forall N \in S$

$$\sigma(N) = \sum_{L \subseteq N} \varphi(L)$$

then $$\varphi(M) = \sum_{L \in S} \mu(L)\sigma(L) \quad .$$

For example, we have associated for the group G a Möbius function μ defined on the set of subgroups of G. This function depends entirely on the subgroup structure of G; if this is known, μ can be calculated. Now if we let for each subgroup H of G.

$\sigma(H)$ = the total number of pairs of elements in H $= |H|^2$

and $\varphi(H)$ = the number of generating pairs of elements in H

then $$\varphi(G) = \sum_{H \leq G} \mu(H)|H|^2$$

and so we have the number of regular oriented hypermaps with automorphism group G equals

$$\frac{1}{|\mathrm{Aut}G|} \cdot \sum_{H \leq G} \mu(H)|H|^2 \quad .$$

To determine the number of these that are in fact maps we go through the same process except we consider pairs (x,y) of group elements with o(x) = 2; we can further enumerate other different types of oriented hypermap by imposing varying relations that the pairs (x,y) we are counting must satisfy. The philosophy is that the direct calculation of the <u>total</u> number of pairs (x,y) of elements of a group satisfying some specified relations is far easier in general than that just for the <u>generating</u> pairs of the same sort. Once the Möbius function of a group G is known,

Möbius inversion clearly becomes a very powerful tool.

In Chapter 1, I present the ideas and techniques as described above in more detail, in a slightly more general spirit. However the remainder of the work almost exclusively deals with regular hypermaps (both oriented and unoriented) with automorphism group G of isomorphism type $PSL_2(q)$ or $PGL_2(q)$, defined over the finite field GF(q) for some prime power q. In fact the dissertation could be regarded as predominantly being just a study of these groups, 'dressed' in the terminology of maps.

Chapter 2 completely determines the Möbius function for all groups $PSL_2(q)$ and $PGL_2(q)$, q some prime power. It involves an intricate examination of the subgroup structures, and extends a result in [7] for which answers for $PSL_2(p)$ for any prime p are already given.

In Chapter 3 enumerations of certain categories of regular maps and hypermaps with automorphism group G, for G any $PSL_2(q)$ or $PGL_2(q)$, are made. This is done in two sections: the first section follows exactly the method of Möbius inversion as already described, but the enumerations in the second section are done <u>not</u> referring to Möbius inversion (the use of which in the cases dealt with would be inefficient). The latter enumerations count the numbers of hypermaps (G, Ω, x, y) with specified orders for x, y and $z:=y^{-1}x$. They are achieved by developing the results in an existing paper [14] which already explores the pairs of elements (x,y) of G with given values of order for x,y,z with respect to the isomorphism type of the subgroup of G generated by x and y. (It is in this section that the trace of the elements of G, thought of as 2x2 matrices, is first used: trace is often a very useful tool when examining G because of the near correspondence of the sets of elements sharing the same value of trace and the conjugacy classes in G.)

In Chapter 4 we consider the problem, how given two non-isomorphic oriented hypermaps

$$\mathcal{H} := (G, \Omega, x, y)$$

$$\mathcal{H}_1 := (G_1, \Omega_1, x_1, y_1) \qquad \text{with } G_1 \cong G$$

can one find a 'difference' between the two; this amounts to finding a relation satisfied by the pair (x,y) in G not satisfied by the pair (x_1,y_1) in G_1 (alternatively this may be thought of as finding relations that are not mutually shared in two non-equivalent 2-generator presentations for G). For simplicity, I restrict my attention to the most intrinsically interesting subcategory of hypermaps, that of triangular maps $\mathcal{M}$, and endeavour to construct an algorithm which systematically produces, given $\mathcal{M} := (G, \Omega, x, y)$, the relations satisfied by x and y in G. This is effectively done by examining the trace of all the words in x and y. Also I show, given the prime power $q = p^e$, how the set { regular orientable triangular maps (RO Δ Ms) with automorphism group $PSL_2(q)$ or $PGL_2(q)$ } may be characterised by the set of irreducible polynomials of degree e over GF(p). Using this, I discuss how we might identify the ROΔMs $\mathcal{M} = (G, \Omega, x, y)$ with automorphism group G isomorphic to $PSL_2(q)$ or $PGL_2(q)$, for some power q of a fixed prime p, for which a particular relation holds for x and y. Examples are given.

Finally, in Chapter 5, I continue my specialisation to ROΔMs by finding alternative constructions for some of the ROΔMs $\mathcal{M}$ with automorphism group $G \cong PSL_2(q)$ or $PGL_2(q)$, some q. We form the graph $\Psi(G, \ell) := \Psi$ where ℓ is any conjugacy class of elements of G by setting

the vertex set $V(\Psi)$ as the set of elements in ℓ,

the edge set $E(\Psi)$ as exactly those pairs $(u,v) \in \ell^2$ for which $o(uv^2) = o(vu^2) = 2$ in G.

Then we find, if the pair (G,ℓ) satisfies one of

(i) $G \cong PSL_2(p)$ for some prime p, and the elements of ℓ have order p in G

(ii) $G \cong PGL_2(q)$ for any q, and the elements of ℓ have order $(q \mp 1)$,

that Ψ has a unique orientable triangular imbedding and this is a ROΔM with automorphism group isomorphic to G.

CHAPTER 1

PRELIMINARIES

I expound the foundational theory and establish the broad techniques which govern the approach of much of the work in the thesis. I also give many notes which give examples, set a broader context, or explain implications incidental to the central discussion.

1. MÖBIUS INVERSION

Let P be a finite partially ordered set with ordering >. Let σ, φ be functions with domain P, codomain $\mathbb{R}$ such that $\forall p \in P$

$$\sigma(p) = \sum_{q \text{ s.t. } q \leq p} \varphi(q) \quad .$$

Then
$$\varphi(p) = \sum_{q \text{ s.t. } q \leq p} \mu_P(q,p)\, \sigma(q) \qquad (1)$$

where μ_P is a function associated with P (independent of σ or φ)

$$\mu_P: \{\text{ordered pairs } (a,b) \text{ in } P : a \leq b\} \to \mathbb{Z}$$

defined by:

$$\forall a \in P, \quad \mu_P(a,a) = 1$$

then for fixed $a \in P$, $\mu_P(a,b)$ is defined recursively for all $a \neq b$ by

$$\sum_{\substack{x \in P \text{ s.t.} \\ a \leq x < b}} \mu_P(a,x) = 0 \quad .$$

The function μ_P is called the Möbius function of P; the process of finding a single value $\varphi(p)$ in terms of σ and μ_P is called Möbius inversion, and the expression (1) is called the Möbius formula. Its truth is trivially seen by substituting $\sum_{\substack{r \text{ s.t.} \\ r \leq q}} \varphi(r)$ for $\sigma(q)$ for each q in the summation.

This describes Möbius inversion in the broadest applicability of the concept for finite systems (except that the codomain $\mathbb{R}$ of σ , φ may be replaced by any integral domain containing the rationals). We now specialize to lattices.

Definitions

Let P be a poset, let T be a subset of P. Then let

$$M = \{m \in P : m \leqslant t \text{ for every } t \in T\}$$

$$J = \{j \in P : j \geqslant t \text{ for every } t \in T\}.$$

If (M;J) is non-empty and contains a (greatest; least) element (m';j') then (m';j') is called the (meet; join) of T in P. (The last statement is read by taking consistently either the first or second entry in each bracket). If every subset T of P has both a meet and join, then P is a lattice. In particular P must then have a single greatest and a single least element (consider T = P).

Möbius functions of lattices have been examined by combiniatoralists, for example [1]. An elementary general result is

Proposition

If P is a lattice and $p \in P$ then

$$\mu_P(q,p) \neq 0 \Rightarrow q = p \text{ or } q \text{ is the meet of a subset of}$$
$$\{r \in P : r < p \text{ s.t. } \nexists s \in P \text{ s.t. } r < s < p\}.$$

(In fact we may relax condition that P is a lattice, we only need existence in P of meets).

Now the subgroup structure of any group G is a lattice, ordering given

by inclusion, meets by intersections, joins by subgroups generated by unions. So we may talk of finding the Möbius function of G, by considering its subgroup lattice P. But for groups we shall slightly adapt (in fact restrict) the definition of Möbius function; we shall now mean a function μ_G : {subgroups of G} $\to \mathbb{Z}$ given by:

$$\mu_G(H) = \mu_P(H,G) \qquad \forall H \leqslant G \ .$$

(Note that if μ_H is known for every subgroup H of G, then the complete Möbius function of the lattice P is known.)

We have immediately from the proposition:

Corollary

If G is any group, then $\forall H \leqslant G$

$$\mu_G(H) \neq 0 \Rightarrow \Big(H = G \text{ or } H \text{ is the intersection of maximal subgroups of (is 'maxint' in) } G\Big) \ .$$

So in calculating μ_G, we need only consider the lattice of maxint subgroups of G. This observation is crucial to my calculations of μ_G for explicit G.

Most of the research conducted on Möbius inversion has been conducted in the language of lattice theory, results concentrated on classes of lattices satisfying certain strong conditions. The (maxint) subgroup lattice of a group G (especially those with a 'large' simple group as homomorphic image) tends to be complicated without (overall) following a discernible pattern, and then these results seem to be of little use. So then the only way of establishing μ_G is to treat the maxint lattice 'by hand', i.e. calculating $\mu_G(H)$ for $H \leqslant G$ only when $\mu_G(K)$ is known $\forall K \leqslant G$ s.t. $H < K \leqslant G$. If the lattice is known, this of course can always be

done, be it tedious.

Not a great deal of work has been done on the Möbius functions of groups; P. Hall [7] was motivated to consider them by their application in enumerating generating n-tuples of certain types of elements in G (which was in effect also my motivation and will be explained in the next section). Hall (paragraphs 2.7 and 2.8) finds a general expression for μ_G for those groups G whose Sylow subgroups are all self-conjugate (which therefore covers all finite nilpotent groups, by [21] 8.6 and 11.3) ; this general expression is possible by the highly structured nature of these groups. He proceeds to get results for $PSL_2(p)$, for p any prime. A more recent paper is [13], which appeals much more to combinatorial theory: it uses the Burnside ring theory of groups to rediscover the result for nilpotent groups (proposition 2.4). It extends this to deal with all soluble groups (theorem 2.6), but to apply the result for any particular group is already quite involved. The results in [13] depend heavily on the normal subgroup structure of the groups they consider and so their techniques are unlikely to find much applicability for non-cyclic simple groups, with which my research is largely involved. I quote from the paper:

> 'Thus, contrary to the case of soluble groups, the behaviour of the Möbius function of simple groups seems more difficult to understand.'

Example

This example is a trivial calculation of the Möbius function of a simple lattice, but it also may be regarded as a preliminary result for we shall

often make use of it. (It occurs in paragraphs 2.5-2.6 of [7]).

(a) **The Boolean lattice**

Let G be a set of n objects, L the lattice of all 2^n subsets (ordering by inclusion). Let $A,B \in L$ s.t. $A \subseteq B$ and $|A| = a$, $|B| = b$.

Then $k := b - a \geq 0$ and

$$\mu_L(A,B) = (-1)^k .$$

For all $c \in \mathbb{N}$ s.t. $a < c \leq b$, A is contained in exactly $\binom{k}{c-a}$ sets in L of order c and so (using induction on k having fixed A)

$$1 - k + \binom{k}{2} - \binom{k}{3} + \ldots + (-1)^{k-1} k + \mu_L(A,B) = 0$$

and the result is evident by comparing the left-hand side with the binomial expansion of $(1-1)^k$.

(b) Let n be any natural number, and L be the finite lattice of subgroups of C_∞ which contains its subgroup X of index n. Denote

$$\mu_L(X,C_\infty) \text{ by } \mu(n) .$$

The maximal subgroups of C_∞ in L are those with prime index that divide n, and intersections of these have square-free index, hence

$$\mu(n) = 0 \qquad \text{if n has a square divisor .}$$

If n is square-free, L is a Boolean lattice on its prime divisors, and so

$$\mu(n) = (-1)^k$$

where k is the number of prime divisors of n.

Of course we specify

$$\mu(1) = 1$$

We have in fact just recovered (in the context of a lattice) the 'classical' number theoretic Möbius function $\mu : \mathbb{N} \to \mathbb{Z}$ defined by

$$\mu(1) = 1 \quad , \text{ then inductively } \sum_{\substack{\text{divisors } m \\ \text{of } n}} \mu(m) = 0 \quad .$$

This function will appear prominently in our results, and we shall keep to the convention that a function denoted μ without a subscript will represent this classical, rather than any other, Möbius function. I shall also refer to the lattice L as above (or one isomorphic to it) as the number-theoretic lattice on n.

2. APPLICATION OF MÖBIUS INVERSION TO ENUMERATION OF NORMAL SUBGROUPS

In applying Möbius inversion to groups G we are interested in any pair of functions σ, φ on the subgroups of G s.t.

$$\sigma(G) = \sum_{H \leq G} \varphi(H) \quad .$$

The most obvious candidates are number of n-tuples of a certain type in H for σ, and number of generating n-tuples of the same type in H for φ. We now exploit the idea, being more explicit.

The method we describe below is entirely due to Hall [7], and we shall call it Hall's method. The method is for finding the number $d_\Gamma(G)$ of normal subgroups of a finitely presented group Γ with specified quotient type G.

Definition

Let H be any group, and Γ have finite presentation P

$$\Gamma \cong P = \langle X_1, \ldots, X_n : R_1, \ldots, R_m \rangle \quad .$$

Then a P-base of H is a n-tuple of elements of H which satisfy the relations R_1 to R_m and generate H.

Suppose P is fixed. Let

$$\varphi_P(H) = \#\text{ P-bases of } H\ .$$

Then clearly $\varphi_P(H) = \#$ epimorphisms $\rho : \Gamma \to H$ and so is independent of the particular presentation P chosen for Γ, and so the function $\varphi_\Gamma := \varphi_P$ on all groups H is well-defined.

Now

(i) $\exists\ N \lhd \Gamma$ s.t. $\frac{\Gamma}{N} \cong G \iff \exists$ epimorphism $\rho : \Gamma \to G$ with kernel N

(ii) two epimorphisms ρ and ρ' have the kernel N if and only if

$$\rho' = \rho \circ \alpha \qquad \text{where } \alpha \in \mathrm{Aut}G$$

(iii) $\forall$ non-identity epimorphisms ρ and $\alpha \in \mathrm{Aut}G$,

$$\rho \circ \alpha \neq \rho\ .$$

We conclude

$$d_\Gamma(G) = \frac{\varphi_\Gamma(G)}{|\mathrm{Aut}G|}\ .$$

Now let

$\sigma_\Gamma(H) := \#$ n-tuples of elements of H which satisfy R_1 to R_m but do not necessarily generate H (this is also independent of presentation of Γ). I call these n-tuples Γ-strings of H.

Then

$$\sigma_\Gamma(G) = \sum_{H \leq G} \varphi_\Gamma(H)$$

and Möbius inversion gives

$$\varphi_\Gamma(G) = \sum_{H \leq G} \mu_G(H)\, \sigma_\Gamma(H)\ .$$

So if the Möbius function μ_G and $\sigma_\Gamma(H)$ are known $\forall H \leq G$, as well as $|\mathrm{Aut}G|$, then $d_\Gamma(G)$ is determined.

Notes and Examples

1) If G is non-trivial and simple, then the normal subgroups M of Γ s.t. $\frac{\Gamma}{M} \cong G$ (i.e. those groups counted by $d_\Gamma(G)$) are <u>maximal</u> in the normal subgroup lattice of Γ.

2) If Γ is free of rank n, and $M \lhd \Gamma$ s.t.

$$\frac{\Gamma}{M} \cong G \qquad \text{(some group } G\text{)}$$

then M is free of rank $(n-1)|G| + 1$. This is by the Nielsen-Schreier theorem. (See e.g. ~~at~~ p.16 of [10]).

Should we want to enumerate the normal subgroups of Γ of rank m, we could do so if we knew $d_\Gamma(G)$ for all groups G of order $g := \frac{m-1}{n-1}$ (rather ambitious for most values of g!) by summation of these $d_\Gamma(G)$. But of course if g happens to be prime this process becomes somewhat trivial, and in the spirit of an example of Hall's method I prove a result (easily proved by other arguments):

Theorem

If Γ is the free group of rank n, and

$$m = p(n-1) + 1 \quad \text{for some prime } p$$

then the number N of normal subgroups of Γ which are free of rank m is

$$N = \frac{p^n - 1}{p - 1} .$$

Proof

The only group G of order p is the cyclic group C_p. Its Möbius function is

$$\mu_G(C_p) = 1 \quad , \quad \mu_G(I) = -1$$

and $\sigma_\Gamma(C_p) = p^n \quad , \quad \sigma_\Gamma(I) = 1 .$

Möbius inversion gives

$$\varphi_{\Gamma}(C_p) = p^n - 1$$

and $|\mathrm{Aut}C_p| = p - 1$, so

$$N = d_{\Gamma}(C_p) = \frac{p^n - 1}{p - 1} . \quad \square$$

3) If Γ is free of rank n, i.e. we are counting n-tuples of elements in G with no relations, then Hall denoted $d_{\Gamma}(G)$ by $d_n(G)$ and observed that $d_n(G)$ is the greatest number d for which the direct product of d groups isomorphic with G can be generated by n elements. This function (consider group G fixed, vary n and redenote again to $d_G(n)$) is intrinsically related to the growth sequence $g_G(d)$ of G defined by

$g_G(d)$ = the order of the minimum generating set of the direct product G^d for $d \in \mathbb{N}$

and was studied by Wiegold in a series of papers [26-29, 19].

The function d_G determines g_G (and vice-versa), but in practice to calculate g_G for a particular $d \in \mathbb{N}$ using d_G is cumbersome unless we already know close bounds for $g_G(d)$; this is what Wiegold provides. For example, if G is a non-abelian 2-generator simple group, Wiegold [29] identifies $g_G(d)$ to be one of the two integer values $\{m, m + 1\}$ lesser than and nearest to $\log_{|G|} d + 3$; to decide between m and m + 1, calculate $d_G(m)$; if this result yields

$$d_G(m) < d$$

we conclude that $g_G(d) = m + 1$; otherwise $g_G(d) = m$.

4) Another example of Hall's method.

I recover a result (proposition 2.8) in [13] with a neater proof. It can also serve as a check for calculations of Möbius functions of groups.

Proposition

If G is any non-cyclic group, then

$$\sum_{H \leq G} |H| \ \mu_G(H) = 0 \ .$$

Proof

For using Hall's method, let $\Gamma = C_\infty$. Then $\forall H \leqslant G$

$$\sigma_\Gamma(H) = |H| \ ,$$

$$\varphi_\Gamma(H) := \# \text{ generating singletons in } H = 0 \text{ iff } H \text{ is non-cyclic} .$$

The Möbius inversion formula now immediately gives the result.

3. GROUP THEORY OF REGULAR MAPS AND HYPERMAPS

The theory (for maps, and also in a tentative way for hypermaps) is centrally involved in constructing algebraic definitions which correspond to the vague notion of a (hyper)-map being a (hyper)-graph imbedded in a surface $. I deal with the two cases,

(i) the orientable case where we require $ to be orientable.

(ii) the 'non-orientable' case, where there is no such restriction on $ (but $ may still be orientable, however giving different definitions to (i)).

(i) The Orientable Case

Definitions

By an oriented map $\mathcal{M}$ we mean a set Ω with permutations x, y of Ω s.t. both

1) $x^2 = I$ (the identity of S^Ω)

2) $G := gp\langle x,y \rangle$ is transitive on Ω.

We denote $\mathcal{M}$ by the quadruple (G, Ω, x, y).

We call the elements of Ω the darts of $\mathcal{M}$. The cycles of darts of x, y and $z := y^{-1}x$ (i.e. apply the permutation x, then y^{-1}) are called the edges, faces and vertices of $\mathcal{M}$ respectively.

From now on and up to the start of case (ii) I shall often abbreviate 'oriented map' to just 'map'.

A morphism φ from one map $\mathcal{M}_1 := (G_1, \Omega_1, x_1, y_1)$ to another map $\mathcal{M}_2 := (G_2, \Omega_2, x_2, y_2)$ is a pair of functions (σ,τ)

$$\sigma : G_1 \to G_2$$

$$\tau : \Omega_1 \to \Omega_2$$

where σ is the group homomorphism given by

$$\sigma(x_1) = x_2 \qquad \sigma(y_1) = y_2$$

and τ satisfies $\forall g \in G_1, \alpha \in \Omega_1$:

$$\tau(g\alpha) = (\sigma g)(\tau\alpha) \ .$$

(Notice that for an automorphism of a map $\mathcal{M}$ that σ is the identity automorphism of G; I will just denote it τ as appropriate.)

In [12], which gives a comprehensive discourse on the basis of the relationship between groups and maps, a map as defined above is an algebraic map (AM). The paper also defines a structure called a topological map (TM); without going into the intricacies of the definition, it is a connected locally-finite 1-dimensional simplicial complex $\mathcal{G}$ in $\mathbb{R}^3$ imbedded homeomorphically into an orientable surface $\mathcal{S}$. (Strictly speaking we should allow in $\mathcal{G}$ 'loops', i.e. topological circles with a given single point considered as a 0-face. Also we should specify a subset V of the 0-faces

of $\mathcal{G}$; the 0-faces not in V identify 'free edges', i.e. 1-simplices (non-loops) we shall consider as only having one vertex in the underlying graph of $\mathcal{G}$.)

Now given $\mathcal{T} \in$ TM, it can clearly be identified with an algebraic map (G, Ω, x, y), call it AM($\mathcal{T}$), given by (assuming here $\mathcal{T}$ has no loops)

$$\Omega = \{\text{pairs } (e,v) : e \text{ is a 1-simplex in } \mathcal{G},\ v \in V \text{ and } e \cap v = v\}$$

$$x : (e,v) \mapsto \begin{cases} (e,v') & \text{if } v' \in V \\ (e,v) & \text{if } v' \notin V \end{cases}$$

where v' is the 0-face of e other than v.

$$y := z^{-1}x$$

where

$$z : (e,v) \mapsto (e',v)$$

and e' is determined as the 'next' 1-simplex from e following the orientation around v in $. (A slight easy adaption of the definitions of Ω and x is needed to form AM($\mathcal{T}$) if $\mathcal{T}$ has loops).

[12] further showed (given some finiteness conditions) that every $\mathcal{M} \in$ AM is isomorphic to AM($\mathcal{T}$) for some $\mathcal{T} \in$ TM, and that (with the rule of isomorphism for TM as given in that paper):

$$\mathcal{T}_1 \cong \mathcal{T}_2 \text{ in TM} \iff \text{AM}(\mathcal{T}_1) \cong \text{AM}(\mathcal{T}_2) \text{ in AM}.$$

Thus we may sensibly identify $\mathcal{M}$ with the appropriate $\mathcal{T} \in$ TM and define the genus g of $\mathcal{M}$ as that of the surface $ associated with $\mathcal{T}$.

For simplicity I shall restrict my attention from now on to finite maps, i.e. $|\Omega|$ is finite; the last paragraph is then valid. (In fact all the maps relevant to my calculations will be finite.)

We now proceed to isolate a group associated with each map $\mathcal{M}$. So suppose $\mathcal{M} := (G,\Omega,x,y)$ is given.

Let $o(y) = n$ and $\Gamma(n)$ be the free product $C_2 * C_n$, i.e.

$$\Gamma(n) := gp < X,Y : X^2 = Y^n = I > .$$

Then clearly $\exists$ epimorphism $\rho : \Gamma(n) \to G$ given by:

$$\rho : X \mapsto x \quad , \quad \rho : Y \mapsto y$$

and $\mathcal{M}$ determines the group $K \lhd \Gamma(n)$, the kernel of ρ.

However for our purposes it is not so much K that will interest us but the set $\mathcal{L}$ of subgroups of $\Gamma(n)$:

$$\mathcal{L} := \left\{ M_\alpha : \alpha \in \Omega \text{ and } M_\alpha = \rho^{-1}(Fix_G(\alpha)) \right\} \qquad \text{where } Fix_G(\alpha) := \{g \in G : g(\alpha) = \alpha\}.$$

As G is transitive on Ω, the M_α will be mutually conjugate in $\Gamma(n)$; conversely given $M_\alpha \in \mathcal{L}$, all conjugate groups in $\Gamma(n)$ must be the stabilizer under ρ of a dart, and so also be in $\mathcal{L}$. Thus $\mathcal{L}$ is a <u>conjugacy class</u> of subgroups of $\Gamma(n)$. Note that

$$K = \bigcap_{M_\alpha \in \mathcal{L}} M_\alpha \quad , \text{ i.e. the } \underline{\text{core}} \text{ of } \mathcal{L} .$$

We call any $M \in \mathcal{L}$ a <u>map-subgroup</u> of $\mathcal{M}$. The definition I use here is not the same as that found in [12]. In the latter a map subgroup M is a subgroup of the triangle group

$$\Gamma(n,m) := gp < X, Y : X^2 = Y^n = (Y^{-1}X)^m = I >$$

where $m = o(z)$ in G. M is then the inverse image of a stabilizer of a dart under the obvious epimorphism $\Gamma(n,m) \to G$.

Essentially the difference is that in 'my' definition the information

$$o(z) = m$$

is contained in the map subgroup itself, whereas this alternative has the same information in the 'sponsoring' group. The rôle of the two though in describing any particular map is effectively identical.

It is easy to see that any two maps with map-subgroups in the same $\Gamma(n)$ and conjugate in that $\Gamma(n)$ must be isomorphic; also that every subgroup in any $\Gamma(n)$ is a map-subgroup of some map (see [12] p.283-284). Thus $\forall n \in \mathbb{N}$ we have a bijection between

{ conjugacy classes of subgroups of $\Gamma(n)$ s.t. no non-trivial power of Y is contained in their core K }

and

{ maps $\mathcal{M}$ s.t. o(y) = n } .

Now I define regularity for maps:

a map $\mathcal{M}$ is <u>regular</u> if $\mathrm{Aut}(\mathcal{M})$ acts transitively on Ω

and state a result (Theorem 6.3) in [12], reproducing the proof:

Proposition

$\mathcal{M}$ is regular if and only if its map-subgroup M is a normal subgroup of $\Gamma(n)$ for suitable n.

Proof

(i) Let $\mathcal{M}$ be regular, and $g \in \mathrm{Fix}_G(\alpha)$ for some $\alpha \in \Omega$. For any $\tau \in \mathrm{Aut}(\mathcal{M})$,

$\tau(g\alpha) = g(\tau\alpha)$

$\Rightarrow \quad \tau\alpha = g(\tau\alpha)$

$\Rightarrow$ g fixes $\tau\alpha$ and as $\mathrm{Aut}(\mathcal{M})$ is transitive on Ω, g fixes every dart

$\Rightarrow \quad g = I \Rightarrow \mathrm{Fix}_G(\alpha)$ is trivial

$\Rightarrow \quad M = K \trianglelefteq \Gamma(n)$ (K as before)

(ii) Suppose map $\mathcal{M}$ has map-subgroup $M \trianglelefteq \Gamma(n)$. Then $M = K$ and $\mathrm{Fix}_G(\alpha)$ is trivial. Then the permutations $\tau_h : \Omega \to \Omega$ indexed

by the elements h of G given by

$$\tau_h : g\alpha \mapsto gh\,\alpha \qquad (\alpha \text{ some fixed dart}, \forall g \in G)$$

are well-defined and automorphisms of $\mathcal{M}$ (and evidently the only automorphisms of $\mathcal{M}$).

In particular $\forall h \in G$

$$\tau_h : \alpha \to h\alpha$$

and so $\mathrm{Aut}(\mathcal{M})$ acts transitively on Ω. □

Corollary 1

$\mathcal{M}$ is regular $\Leftrightarrow \mathrm{Aut}\,\mathcal{M} \cong G \cong \frac{\Gamma(n)}{M}$

Note

If $\mathcal{M}$ is regular, all the cycles of y (faces) in Ω must in themselves be mutually conjugate in S^{Ω}, and so have equal length = o(y) = n. We say $\mathcal{M}$ is regular with n-gonal faces. Similarly the cycles of z (vertices) will be equal in length (m say), and we say $\mathcal{M}$ has valency m. These of course correspond to the actual properties of the relevant topological map when thought of as a graph imbedded in a surface.

Corollary 2

Let G be any given finite group, let $n \in \mathbb{N}$.

The number of regular oriented maps (ROMs) $\mathcal{M}$ with n-gonal faces s.t. $\mathrm{Aut}\,\mathcal{M} \cong G$ equals the number of torsion-free normal subgroups M of $\Gamma(n)$ s.t. $\frac{\Gamma(n)}{M} \cong G$.

(Clearly if G is non-cyclic and n is prime, the condition 'torsion-free' becomes vacuous.)

In the preceding section we gave a procedure which enables us to calculate this number for the case in parenthesis, this being $d_{\Gamma(n)}(G)$. However the method easily extends to all cases: we simply take σ to be

$$\sigma_{\Gamma(n)}(H) = \#\text{ pairs } (x,y) \text{ in } H \text{ s.t. } o(x) = 2,\ o(y) = n$$

(rather than number of pairs (x,y) in H s.t. $x^2 = y^n = I$), and proceed exactly as before to obtain result $d'_{\Gamma(n)}(G)$ say rather than $d_{\Gamma(n)}(G)$. We need the distinction because the map $\nu_{\Gamma(n)}$ (where the group $\Gamma(n)$ is regarded as acting on itself) may be considered as a universal covering map of n-gonal maps (c.f. p.283 [12]): if we took into account pairs (x,y) of G with o(y) : = d strictly dividing n, we would also be counting quotient maps with d-gonal faces.

Clearly to enumerate <u>all</u> ROMs with automorphism group G we may sum $d'_{\Gamma(n)}(G)$ over all natural numbers n. But it is usually more efficient to use the same sort of techniques to get the result directly as now explained.

The map-subgroup $M \trianglelefteq \Gamma(n)$ is not the only group-theoretic way to represent a map $\mathcal{M}$: = (G, Ω, x, y). For let (for now) Γ be the group

$$\Gamma : = gp < X,Y : X^2 = I >$$

and form the epimorphism $\rho : \Gamma \to G$ by

$$X \mapsto x \quad , \quad Y \mapsto y \ .$$

Then in the same way as before we may associate $\mathcal{M}$ with the conjugacy class $\mathcal{L}$ of subgroups in Γ given by inverse images of stabilizers in G of darts. Regularity again dictates that $\mathcal{L}$ consists of a single normal subgroup of Γ, and vice-versa, and we come to

Theorem

Let $\Gamma = C_2 * C_\infty$, G any group. Then

$$(\#\text{ ROMs } \mathcal{M} \text{ with } \mathrm{Aut}\mathcal{M} \cong G) = d_\Gamma(G) \ .$$

The reasoning can be extended also to count more particular categories of regular maps having given automorphism group G. By this I mean if we had a finite set of words $\{ r_1, \ldots , r_s \}$ for $s \in \mathbb{N}$ in x and y which we required to be identity in G (intuitively interpretated as 'routes' in the map always taking you to the same dart to that from which you started), then the number of such ROMs would equal $d_\Gamma(G)$ where now Γ is the group with presentation

$$< X,Y : X^2 = R_1 = \ldots = R_s = I >$$

and $\forall i = 1, \ldots , s$, R_i is the same word in X and Y as r_i is in x and y. However of course, in general the more complicated the relator set of Γ is, the more difficult it is to calculate $d_\Gamma(G)$ in practice.

Before going on to hypermaps, I include some

Notes

1) The map-subgroups (as I have defined them) of triangular (i.e. o(y) = 3) oriented maps are exactly the subgroups of $\Gamma := C_2 * C_3$ of finite index. But in this case Γ is the much studied modular group $PSL_2(\mathbb{Z})$ (see e.g. [20] chapter 8), and so this case is especially interesting.

   In particular we may ask whether a subgroup of $\Gamma := PSL_2(\mathbb{Z})$ appearing in this context is a congruence subgroup of Γ, i.e. does it contain any principal congruence subgroup of Γ? (One of the latter is defined for each positive integer n as

$$\Gamma_n = \{ \pm A \in \Gamma : A \equiv \pm I \bmod n \} \quad).$$

   For regular maps we are considering normal subgroups of Γ; the

normal congruence subgroups have been classified by [16]. Hence we may sometimes decide the question for the map-subgroup of a given triangular ROM.

2) Unless G is cyclic, a ROM with automorphism group G cannot contain free edges (i.e. x cannot fix any darts). For we showed regularity meant the stabilizer in G of each dart was identity; thus

$$x \text{ fixes a dart} \Rightarrow x \text{ is the identity permutation on } \Omega$$
$$\Rightarrow G = \langle x,y \rangle = \langle y \rangle \quad \square$$

3) $G \leqslant S^{\Omega}$, the symmetric group on the finite set Ω. If G does not have a subgroup of index 2, we have further $G \leqslant A^{\Omega}$, the group of even permutations on Ω. If this is the case for ROM $\mathcal{M}$ with $\mathrm{Aut}(\mathcal{M}) \cong G$, then (for example):

$\mathcal{M}$ has n-gonal faces with n even $\Rightarrow$ $\mathcal{M}$ has an even # faces,

$\mathcal{M}$ has vertices with even valency $\Rightarrow$ $\mathcal{M}$ has an even # vertices.

4) Genus

Suppose an ROM $\mathcal{M}$ is represented as an imbedding in a surface of genus g. Then the valency of each vertex is constant = $o(z) := m$ say, as is the number of edges bounding each face = $o(y) := n$.

Assume also $\mathcal{M}$ has no free edges.

Then:

$$\#\text{ vertices of } \mathcal{M} = \frac{|G|}{m}$$

$$\#\text{ edges of } \mathcal{M} = \frac{|G|}{2}$$

$$\#\text{ faces of } \mathcal{M} \quad = \quad \frac{|G|}{n}$$

and by the Euler-Poincaré characteristic formula

$$2 - 2g \quad = \quad |G| \left(\frac{1}{m} - \frac{1}{2} + \frac{1}{n}\right)$$

$$\Rightarrow \quad g \quad = \quad 1 + \frac{|G|}{2} \cdot \left(\frac{1}{2} - \frac{m+n}{mn}\right)$$

When $\mathcal{M}$ has free edges (and so G is cyclic) the above formula fails because there are now $|G|$ edges, all free, and the associated simplicial complex $\mathcal{C}$ has vertices at the 'free ends' of the free edges not taken account of above. So

$$\#\text{ vertices} = |G| + 1, \ \#\text{ edges} = |G|, \ \#\text{ faces} = 1$$

and $$g = 0 \ .$$

Hypermaps

The philosophy behind hypermaps is to relax the condition we find in the definition of maps that an edge is incident with at most two vertices (this being inherent in requiring $x^2 = I$). For hypermaps, any edge may be incident with any number of vertices (i.e. x is specified, but $x^2 = I$ is relaxed). Note that according to this degree of freedom, maps are themselves hypermaps. The definition is a natural extension to that for (algebraic) maps:

An oriented hypermap (G, Ω, x, y) is a set Ω with permutations x and y of Ω s.t. $G := gp\langle x, y \rangle$ is transitive on Ω.

The cycles in Ω of x, y and $z := (xy)^{-1}$ are the edges, faces and vertices respectively of the hypermap.

The definition for morphism is the natural extension of that given for maps.

Assume from now on $|\Omega|$ finite.

If $\mathcal{H}$ is a hypermap with $o(x) = r$ and $o(y) = n$ I will denote it an (r,n)-hypermap.

Suppose $\mathcal{H}$ is a given (r,n)-hypermap. Let

$$\Gamma(r,n) = gp \langle X, Y : X^r = Y^n = I \rangle$$

and ρ be the epimorphism from $\Gamma(r,n)$ to G determined by

$$X \mapsto x, \quad Y \mapsto y .$$

Then a map-subgroup M of $\mathcal{H}$ is any element of the conjugacy class $\mathcal{L}$ of subgroups of $\Gamma(r,n)$ given by

$$\mathcal{L} = \{ M_\alpha \leq \Gamma(r,n) : \alpha \in \Omega , M_\alpha = \rho^{-1}(Fix_G(\alpha)) \}$$

$\mathcal{L}$ uniquely identifies $\mathcal{H}$.

A regular hypermap $\mathcal{H}$ is one with automorphism group transitive on Ω; exactly as for maps, a hypermap is regular iff its map subgroup M is normal in $\Gamma(r,n)$, and then $\frac{\Gamma(r,n)}{M} \cong$ Aut $\mathcal{H}$. We may enumerate the regular (r,n)-hypermaps with certain automorphism group type G (with known Möbius function) by counting pairs (x,y) s.t. $o(x) = r$, $o(y) = n$ (insisting on orders rather than relations $x^r = y^n = I$) of every subgroup of G, and applying Hall's method.

Similarly we may identify all regular hypermaps with automorphism group G with the set of normal subgroups M s.t. $\frac{\Gamma}{M} \cong G$ where $\Gamma = C_\infty * C_\infty$, the free group of rank 2. (This corresponds to summing the results above for $\Gamma(r,n)$ over $\mathbb{N}^2$). So the number of such hypermaps is $d_\Gamma(G)$ (in the notation of the last section).

Note

It would be nice to associate with a hypermap $\mathcal{H} := (G, \Omega, x, y)$ a (topological) map $\mathcal{M}$ which in some sense faithfully represents $\mathcal{H}$. We can do this by a neat correspondence found by [25], which I state.

First a definition : a map is bipartite if its vertices can be coloured with two colours (with the usual graph-theoretic meaning) such that no two vertices joined by an edge have the same colour. A bipartite map is a map together with such a 2-colouring. Call the colours a and s; note that a map $\mathcal{M}$ which is bipartite has exactly two 2-colourings, the second obtained by 'switching' a and s.

Theorem [25]

$\exists$ bijection ρ from the set of oriented hypermaps onto the set of oriented bipartite maps. For a given hypermap $\mathcal{H}$, ρ maps the vertices, the edges, the darts and the faces of $\mathcal{H}$ onto (respectively) the s-vertices, the a-vertices, the darts incident with the s-vertices and the faces of the map $\rho(\mathcal{H})$.

I will call $\rho(\mathcal{H})$ the bipartite representation of $\mathcal{H}$ and define the genus g of $\mathcal{H}$ to be that of $\rho(\mathcal{H})$. For example, if $\mathcal{H}$ is a regular (r,n)-hypermap with valency (i.e. o(z)) = m then simple use of the Euler-Poincaré formula gives

$$g = 1 + \frac{|\Omega|}{2}\left(1 - \frac{1}{r} - \frac{1}{n} - \frac{1}{m}\right) .$$

Clearly from this we can build up another (essentially identical) topological representation of $\mathcal{H}$, put naively like this: suppose $\rho(\mathcal{H})$ is imbedded in the orientable surface S (of genus g), then 'expand' each vertex

in $ to a face; a resultant face is an 'a-face' or an 's-face' depending on the colour of the associated vertex; forgetting about the original edges of $\rho(\mathcal{H})$ but preserving the faces, we construct a map on $ by specifying that an a-face is incident with a s-face at a single point (a 'new vertex') iff they originate from an adjacent pair of vertices in $\rho(\mathcal{H})$. Otherwise the boundaries of the new faces are mutually disjoint. This construction is always realisable and gives a unique map up to isomorphism.

This new representation $\mathcal{M}$ then has a-faces and s-faces representing edges and vertices of $\mathcal{H}$ respectively, and the remaining faces (f-faces) representing the faces of $\mathcal{H}$; the darts of $\mathcal{H}$ may be associated with the vertices of $\mathcal{M}$ (these being exactly the a-face/s-face incidences). An illustration of such a construction (imbedded in a torus) is given on p.7-8 of [3].

I will call this second representation of $\mathcal{H}$ its topological representation (t.r.). Let $\mathcal{H}$ be an (r,n)-hypermap.

The useful aspect of this t.r. is that any path (connected succession of edges) determines in a natural way a word in x and z : = $(xy)^{-1}$ and vice-versa. In particular if a path w(x,z) takes dart α to itself in $\mathcal{M}$ (i.e. is a loop based at α), then $w(x,z) \in Fix_G(\alpha)$ and the corresponding element w(X,Z) in $\Gamma(r,n)$ is in the map-subgroup M_α. Clearly this works the other way, so such paths characterize M_α : I will exploit this in the next section.

(ii) The case where the (hyper)map may be non-orientable

Given a topological map imbedded in an orientable surface $, we depend on the orientation of $ to decide the cyclic order of the darts in the

permutation y in the associated algebraic map. So if we want to represent algebraicly a topological map imbedded in a non-orientable surface $ we need more 'information' in our model, very vaguely we need to specify next dart around vertex as well as next dart around face in the defining permutations (suggesting we need three of these rather than the two for the orientable case).

What we in fact do (following an idea originally due to Tutte [24]) is consider permutations of oriented darts (face/edge/vertex incidences) rather than darts (edge/vertex incidences). Let the set of the former be Ω'. Then define the following three permutations of Ω':

r_0 takes oriented dart d to the other oriented dart which shares the same edge and face

r_1 takes oriented dart d to the other oriented dart which shares the same vertex and face

r_2 takes oriented dart d to the other oriented dart which shares the same vertex and edge.

We immediately see that for any topological map, be it orientable or non-orientable (according to $), that r_0, r_1, r_2 are naturally determined, $\langle r_0, r_1, r_2 \rangle$ is transitive on Ω' and that

$$(r_0 r_2)^2 = r_i^2 = I \qquad (i = 0, 1, 2) \ .$$

Conversely it can be shown that any abstract transitive permutation group generated by three fixed-point free involutions such that the product of two of them is also of order 2, is an algebraic representation of some unique topological map (see [11]). (If we allow involutions with fixed points, we should also be considering maps with boundary, see [30]).

We use these ideas for maps to motivate our approach to defining hypermaps in general. We know that the set of oriented bipartite maps faithfully represent the set of oriented hypermaps; it seems natural to construct our definition of hypermap in such a way that hypermaps are identified with the elements of the whole set of bipartite maps, orientable or not. Now given a bipartite map we may form its associated 3-face-coloured map $\mathcal{M}$ in the way described before (this second map is certainly orientable if and only if the first is). In $\mathcal{M}$ we may naturally identify (s-face)/(a-face)/(f-face) incidences with the 'ends' of the edges that form the boundaries of the (s-faces). We form involutions r_0, r_1, r_2 on the set Ω' of these ends analogously to before (again the permutation group generated by r_0, r_1, r_2 is clearly transitive on Ω'). These permutations will form the basis of the algebraic definition of the associated hypermap (I shall discuss in the note later the reverse process, i.e. how a bipartite map is associated to any given hypermap, after the definition of the latter is formally given).

Our discussion then prompts the following definitions:

A hypermap $(G, \Omega', r_0, r_1, r_2)$ is a set Ω' together with three permutations r_0, r_1 and r_2 of Ω' s.t. both

(i) $r_0^2 = r_1^2 = r_2^2 = I$

(ii) $G := \text{gp} < r_0, r_1, r_2 >$ is transitive on Ω'.

If $o(r_0r_2) = r$, $o(r_0r_1) = n$ and $o(r_1r_2) = m$, I will say the hypermap $\mathcal{H}$ is of type (r,n,m) : the hypermap is a map iff $r = 2$, it is triangular iff $n = 3$.

The morphisms are defined as usual, in particular the automorphisms are the elements of the centraliser of G in the symmetric group on Ω'; $\mathcal{H}$ is regular iff $Aut(\mathcal{H})$ is transitive on Ω'.

Let $\Gamma = C_2 * C_2 * C_2$, the free product of three cyclic groups of order 2

$$\Gamma := \langle R_0, R_1, R_2 : R_0^2 = R_1^2 = R_2^2 = I \rangle .$$

Define the epimorphism $\rho : \Gamma \to G$ by

$$R_i \mapsto r_i \qquad i = 0, 1, 2 .$$

A map-subgroup M of $\mathcal{H}$ is a subgroup of Γ:

$$M := \rho^{-1}(Fix_G(\alpha)) \qquad \text{for some } \alpha \in \Omega' .$$

M is determined up to conjugacy class in Γ.

Exactly analogous to the oriented case we find that $\mathcal{H}$ is regular if and only if its map-subgroup M is normal in Γ. Also

Theorem

Let G be a given finite group. Then the following are equal:

(i) # regular hypermaps $\mathcal{H}$ with $Aut(\mathcal{H}) \cong G$

(ii) # normal subgroups M of Γ s.t. $\frac{\Gamma}{M} \cong G$

(iii) the value of the expression for $d_\Gamma(G)$ as given on p.7.

Of course this theorem can be specialised, for example

(a) Let $\Lambda := \text{gp} \langle R_0, R_1, R_2 : R_0^2 = R_1^2 = R_2^2 = (R_0R_2)^2 = I \rangle$.

Then

$$\left(\#\text{ regular maps } \mathcal{M} \text{ with } Aut(\mathcal{M}) \cong G\right) = d_\Lambda(G) .$$

Note that if G can be generated by two involutions, some of these maps will be 'degenerate' in that the permutations r_0 and r_2 will be equal, so that the map may be thought of as a single vertex incident with $\frac{|G|}{2}$ free edges.

(b) Let $\Delta := \text{gp} < R_0, R_1, R_2 : R_i^2 (i = 0, 1, 2) = (R_0R_2)^2 = (R_0R_1)^3 = I >$

Then Δ is $PGL_2(\mathbb{Z})$ ([4], section 7.2).

As long as $G \neq I, C_2$, the Klein 4-group or V, the dihedral group of order 6, we have

$\#$(regular triangular maps $\mathcal{M}$ with $\text{Aut}(\mathcal{M}) \cong G) = d_\Delta(G)$.

Note

Suppose we are given the hypermap $\mathcal{H} := (G, \Omega', r_0, r_1, r_2)$. I will associate with it a bipartite map.

Let $\Omega := \Omega' \cup \Omega''$

where Ω'' is any set disjoint from Ω' s.t. $|\Omega''| = |\Omega'|$.

Let s_0 be a bijection $s_0 : \Omega' \to \Omega''$, then s_0 will also denote the permutation of Ω with cycles $(d, s_0(d))$ for each $d \in \Omega'$.

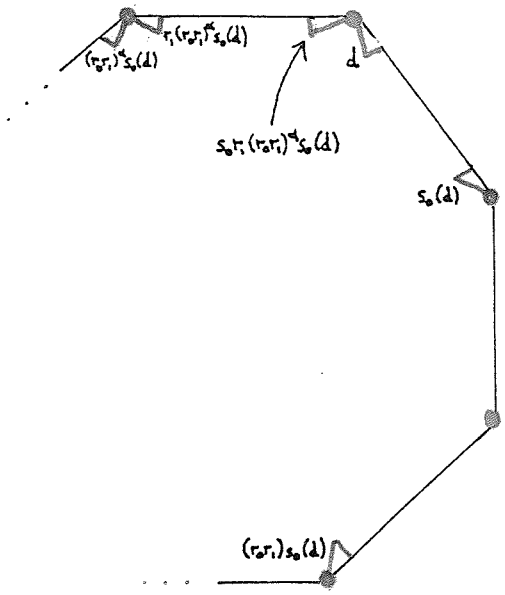
Let $s_1 \in S^\Omega$ be the involution with transpositions

$(d, r_1(d))$ if $d \in \Omega'$

$(d, s_0 r_1 (r_0 r_1)^\alpha s_0(d))$ if $d \in \Omega''$

where $\alpha + 1$ is the least value j s.t. $(r_0 r_1)^j s_0(d) = s_0(d)$.

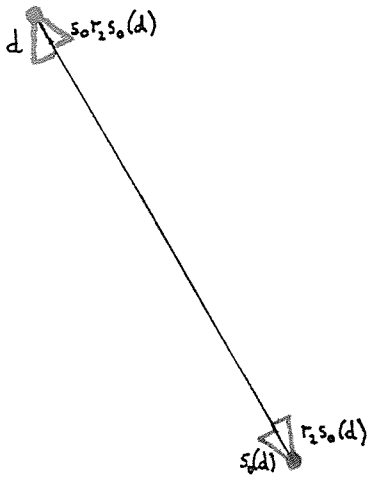
Darts in red lie in Ω''
Darts in green lie in Ω'



Let $s_2 \in S^{\Omega}$ be the involution with transpositions:

$(d, r_2(d))$ if $d \in \Omega'$

$(d, s_0r_2s_0(d))$ if $d \in \Omega''$.



Then clearly $H := \text{gp} \langle s_0, s_1, s_2 \rangle \leq S^{\Omega}$ is transitive on Ω and $(s_0s_2)^2 = I$, so $\mathcal{M} := (H, \Omega, s_0, s_1, s_2)$ defines a map. As $\Omega' \cap \Omega''$ is empty, $\mathcal{M}$ is evidently bipartite; the colouring of $\mathcal{M}$ is determined as:

the vertices corresponding to pairs of cycles of $(r_1 r_2)$ whose elements are in Ω' will be colour s ; in Ω'' will be colour a.

So we have constructed a bipartite map $\mathcal{M}$ from the hypermap $\mathcal{H}$; we gave a procedure earlier to construct a hypermap $\mathcal{H}'$ from $\mathcal{M}$; clearly

$$\mathcal{H} \cong \mathcal{H}'$$

so we have a 1:1 correspondence between bipartite maps and hypermaps as desired. So as for the oriented case we have a bipartite representation (and topological representation) for a hypermap.

We can now define a hypermap as being orientable iff its t.r. is orientable, otherwise it is non-orientable.

However, if a hypermap is orientable, its algebraic definition here as a hypermap is different to that of the oriented hypermap sharing the same bipartite representation (b.r.). In particular the automorphism groups in the two cases need not be isomorphic. For example if a hypermap $\mathcal{H}'$ with orientable b.r. $\mathcal{M}$ is regular, then the oriented hypermap $\mathcal{H}$ with the same b.r. $\mathcal{M}$ will also be regular, but with automorphism group half the order: in fact

$$\mathrm{Aut}(\mathcal{H}) \cong \text{a subgroup of } \mathrm{Aut}(\mathcal{H}') \text{ of index 2.}$$

One consequence of this is that any regular hypermap $\mathcal{H}'$ with $\mathrm{Aut}(\mathcal{H}')$ a group G without a subgroup of index 2 (e.g. a simple group $\neq C_2$) cannot be orientable.

4. Two further notes on the Groups of Maps

1. Type of map-subgroup of an oriented hypermap

For any oriented hypermap $\mathcal{H}$, the characterization of the map-subgroup M_α for any dart α in terms of loops in the surface $ might lead us to expect the fundamental group $\pi_1(\$)$ of $ (and hence genus g) would help determine the isomorphism type of M_α. With this in mind, I specialise to normal torsion-free subgroups of $\Gamma(r,n)$ (alternatively regular (r,n)-hypermaps) with genus g and prove, rather informally:

Theorem

A normal torsion-free subgroup M of finite index μ in $\Gamma(r,n) := C_r * C_n$ is free with rank $1 + (1 - \frac{1}{r} - \frac{1}{n})\mu$.

Proof (all maps, hypermaps referred to are oriented)

Let M be associated with the regular (r,n)-hypermap $\mathcal{H} := (G, \Omega, x, y)$ and this with its topological representation $\mathcal{M}$. Then $|\Omega| = \mu$ and $\mathcal{M}$ is imbedded in the surface $ with genus g,

$$g = 1 + \frac{\mu}{2}(1 - \frac{1}{r} - \frac{1}{n} - \frac{1}{m}) .$$

Let

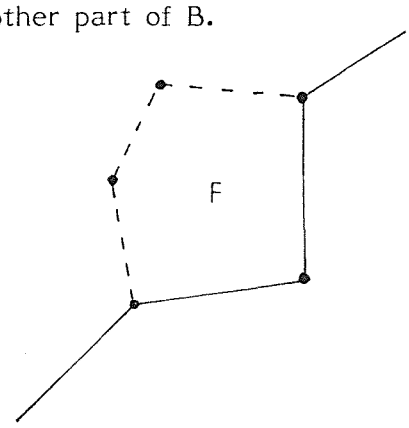
$$\Gamma(r,n) := gp < X, Y : X^r = Y^n = I >$$

and

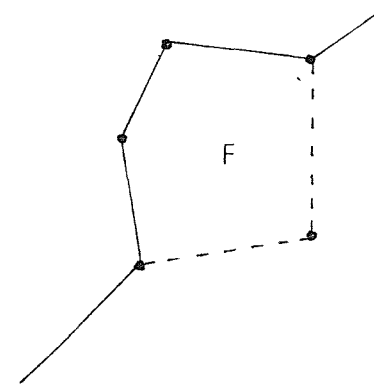
$$Z := (XY)^{-1} .$$

Then note that X and Z generate $\Gamma(r,n)$, so every element of M is expressible as a word in X and Z. A word w(X,Z) in M is free of a set $W = \{w_s(X,Z) \in M : s \in S\}$ for some set S if and only if w cannot be expressed as a product of elements of W (and their inversions) together with insertions or deletions of 'syllables' that are conjugates of X^r and $Y^n = (X^{-1}Z^{-1})^n$. These insertions/deletions only alter the word but not the element of M the word represents. The insertion of one of X^r, X^{-r},

Y^n or Y^{-n} (where the insertion of X^{-r} is the same as deletion of X^r) can always be used to divert a path in $\mathcal{M}$ that at a certain point follows part of a boundary B of either an a- or f-face F, to follow at that point the other part of B.



original path



diverted path

For insertion of X^r or X^{-r}, F will be an a-face of $\mathcal{M}$, for Y^n or Y^{-n} it will be a f-face.

Now isolate $\alpha \in \Omega$ in $\mathcal{M}$, then if w(x,z) is a loop in $\mathcal{M}$, then w(X,Z) is in M. Let the set of vertices of $\mathcal{H}$ be V.

Suppose $\alpha \in$ vertex v, choose for each other vertex u an incident dart β_u and let

$w'_v(x,z) = I$

$w'_u(x,z)$ be any word that takes α to β_u in a non-self-intersecting path for each vertex u (one always exists).

Define for each vertex u, including v,(of which there are $\frac{\mu}{m}$):

$$w_u(x,z) = w'_u(x,z)\, z^m\, w'^{-1}_u(x,z) \ .$$

Then $\forall u \in V$, $w_u(X,Z) \in M$, and these are mutually free. They all rep-

resent trivial loops on $. All other trivial loops in $\mathcal{M}$ correspond (by 'collapse' of faces as inherent above) to some product of these elements (which I now denote c_u).

Now let $w_i(X,Z)$ for $i = 1, \ldots, 2g$ represent the $2g$ non-trivial inequivalent topological simple loops at α in $\mathcal{M}$ (the existence of a loop of each kind is guaranteed by regularity). These loops cannot be obtained from each other by collapse of faces so they are mutually free. Now suppose $w_i'(X,Z)$ corresponds to a topological loop L' equivalent to that L of $w_i(X,Z)$: multiplication by the c_u gives a way of collapsing the s-faces, so we may collapse L' to L and conclude $w_i'(X,Z)$ is a product of $w_i(X,Z)$ with some c_u's as appropriate. Finally from the structure of $\pi_1(\$)$ we know we may assign the $w_i(X,Z)$ as $a_1, b_1, \ldots, a_g, b_g$ s.t.

$$\prod_{j=1}^{g} [a_j, b_j] \text{ is a trivial loop.}$$

In fact we may (w.l.o.g.) let $\prod_{j=1}^{g} [a_j, b_j] = c_v$.

No other combination of the $w_i(X,Z)$ is trivial, so we conclude

$$M \cong gp < a_1, b_1, \ldots, a_g, b_g, \bigcup_{u \in V} c_u : \prod_{j=1}^{g} [a_j, b_j] = c_v >$$

$$= gp < a_1, b_1, \ldots, a_g, b_g, \bigcup_{u \in V} c_u \setminus c_v : - >$$

i.e. M is free of rank $2g + \frac{\mu}{m} - 1$

$$= 2 + \mu(1 - \frac{1}{r} - \frac{1}{n} - \frac{1}{m}) + \frac{\mu}{m} - 1$$

$$= 1 + \mu(1 - \frac{1}{r} - \frac{1}{n}) . \quad \square$$

This result generalises Theorem VIII.7 of [20], which states the formula for $\Gamma(2,3)$, i.e. the classical modular group. The proof I have presented here does not use the Nielsen-Schreier theorem (see p. 8); by considering

combinatorial topological representations of the normal subgroup as I have, I have recovered a non-trivial theorem in combinatorial group theory (c.f. proposition 6.1 in [12] which is the corresponding result using their different defintion of map-subgroup).

2. Groups with signature and Hurwitz groups

The construction of the t.r. of a hypermap is rather naïve when placed against the imbedding theory of groups with signature.

A group with signature Γ with periods $(m_1, \ldots, m_r)$ and quotient space of genus g is a group with abstract definition

$$\Gamma := gp < X_1, \ldots, X_r, a_1, b_1, \ldots, a_g, b_g \mid X_1^{m_1}, \ldots, X_r^{m_r}, (\prod_{i=1}^{r} X_i) \prod_{j=1}^{g} [a_j, b_j] > .$$

Let G be any finite group, φ an epimorphism

$$\varphi : \Gamma \to G$$

such that the orders of X_1 through X_r are preserved. Then a fundamental result is that G acts as a group of automorphisms of a compact Riemann surface \$ of genus γ, where

$$\gamma = 1 + \frac{|G|}{2} \left(2g - 2 + \sum_{i=1}^{r} (1 - \frac{1}{m_i}) \right) .$$

This is the classical Riemann-Hurwitz formula.

In particular if Γ is a triangle group of type (r, n, m), i.e.

$$gp < X, Y : X^r = Y^n = (XY)^m = 1 >$$

then

$$\gamma = 1 + \frac{|G|}{2} (1 - \frac{1}{r} - \frac{1}{n} - \frac{1}{m}) .$$

In fact, given $\Gamma(r, n, m)$, the normal subgroups N s.t.

$$\frac{\Gamma(r, n, m)}{N} \cong G \qquad \text{for given } G$$

naturally give rise to the same regular hypermaps $\mathcal{H}$ of <u>valency m</u> as do the appropriate map-subgroups M of $\Gamma(r, n)$. The imbedding of $\mathcal{H}$ can (more sophisticatedly) be viewed in this light.

(Note: how the classical Riemann-Hurwitz formula appears in the context of the automorphisms of a hypermap and its relationship with its standard setting in the theory of Riemann surfaces is discussed in [15]).

From the above Riemann-Hurwitz formula, given that $G < \mathrm{Aut}(\$)$, $\$$ of genus γ, we may find a bound for $|G|$ by varying the parameters g, r, $m_1 \ldots m_r$; it happens this bound is determined by $g = 0$, $r = 3$, $m_1 = 2$, $m_2 = 3$, $m_3 = 7$. We conclude

$$|G| \leq 84(\gamma - 1)$$

and that this bound is attained by G iff G is the homomorphic image of the triangular group (2, 3, 7). Such a group G is called a <u>Hurwitz group.</u>

Clearly the Möbius function of G if known would be a very powerful tool in deciding whether a particular group G is a Hurwitz group. However, as for any one application of Hall's method, this problem can often be resolved without its direct use: for instance [14], Theorem 8, establishes which $PSL_2(q)$, q a prime power, are Hurwitz groups. But if the relevant Möbius function is known, the working will tend to be more mechanical.

5. Coverings of Riemann Surfaces

Finally, and not pursuing it at all, I give another example where the regular objects C of a certain category $\mathcal{C}$ are in 1:1 correspondence with the normal subgroups M of a certain group Γ, with $\mathrm{Aut}_{\mathcal{C}}(C) \cong \frac{\Gamma}{M}$. Again Hall's method may be used (given the requisite information) to enumerate regular objects of $\mathcal{C}$ with a specified automorphism group type.

The bijection $\mathcal{C} \to M$ in the present case is in essence laid out in [17] (although he doesn't explicitly mention automorphisms). I repeat:

Let $\$$ be a compact Riemann surface of genus g, then the category $\mathcal{C}$ is the set { smooth coverings without boundary $\pi : T \to \$$ for any surface T } . Let $\pi \in \mathcal{C}$, then $\mathrm{Aut}_{\mathcal{C}}\pi$ is the group of covering transformations of π, and π is regular iff $\mathrm{Aut}_{\mathcal{C}}\pi$ is transitive on the set of preimages in T of any point in $\$$. Then the objects of $\mathcal{C}$ correspond to classes of conjugate subgroups of the fundamental group of $\$ \cong \Gamma$ where

$$\Gamma = \mathrm{gp} < a_1, b_1, \ldots, a_g, b_g \mid \prod_{i=1}^{g} [a_i, b_i] = 1 > \quad \text{for } g \geq 1$$

and is trivial for g = 0.

Very similarly to the problem for maps, we may prove the following are equivalent:

i) a covering π is regular

ii) The class of conjugate subgroups of Γ corresponding to π is just a normal subgroup M.

Furthermore, if $M \lhd \Gamma$ corresponds to regular π, then $\mathrm{Aut}\ \pi \cong \Gamma/M$.

So in this respect it will be of interest to know the number $\sigma(G)$ of

solutions for $a_1, b_1, \ldots, a_g, b_g$ (g given) in any group G of the equation:

$$\prod_{i=1}^{g} [a_i, b_i] = I$$

A general answer is available in terms of a summation over the irreducible representations λ of G:

$$\sigma(G) = |G| \sum_{\lambda} \left(\frac{|G|}{f^{(\lambda)}} \right)^{2g-2}$$

where $f^{(\lambda)}$ is the degree of λ.

(The above result is a specialisation of Proposition 1 in [18].)

Then the number $\varphi(G)$ of these solutions generating G is calculated by Möbius inversion, and the number of normal subgroups M of Γ such that $\frac{\Gamma}{M} \cong G$ is ascertained by dividing $\varphi(G)$ by $|\mathrm{Aut}(G)|$.

We note that if $g = 1$, so that Γ is abelian, but G is non-abelian then there can be no epimorphims $\Gamma \to G$ (i.e. there are no coverings of the torus with non-abelian automorphism group). So in this case

$$\varphi(G) = \sum_{H \leq G} \left(\mu_G(H) \cdot |H| \sum_{\lambda} 1 \right) = 0$$

where the 'inner' summation is over the irreducible representations of H. Thus we have for any non-abelian group G:

$$\sum_{H \leq G} \mu_G(H) \cdot |H| \cdot (\#\text{ conjugacy classes of elements in } H) = 0$$

(c.f. proposition on p.10).

CHAPTER 2

In this chapter I will complete the determination of the Möbius function of the linear groups $PSL_2(q)$ and $PGL_2(q)$ over the finite field GF(q) of prime power order q. This is already known (see [7]) for $PSL_2(p)$, p any prime.

$PSL_2(q)$ is the group of 2 x 2 matrices with entries in GF(q) that have determinant 1 and which has $\pm A$ identified for each matrix A. Dickson [5 , chapter XII] analysed its structure, with a full list of subgroups given in §260 of his book.

$PGL_2(q)$ is the group of 2 x 2 matrices with entries in GF(q) that have non-zero determinant quotient by $\left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \ \lambda \in GF(q) \right\}$. If q is a power of two, $q = 2^e$ say, then

$$PGL_2(2^e) \cong PSL_2(2^e) \qquad \text{for any } e \in \mathbb{N}$$

otherwise if q is odd then $PSL_2(q)$ may be regarded as a subgroup of index 2 in $PGL_2(q)$.

As the groups $PSL_2(2^e)$ have structures not quite fitting in with a pattern shared by the other $PSL_2(q)$, the former will be dealt with separately. The schedule will be

Section 1 : $PSL_2(p^e)$, p odd, $e > 1$

Section 2 : $PSL_2(2^e)$, $e > 1$

Section 3 : $PGL_2(p^e)$, p odd.

But first I introduce some definitions and notation (which will carry through to other chapters), and also state two rather trivial (but crucial) general

lemmas, one for subgroup lattices, the second for all lattices.

Definitions

If $H \leq G$, where H, G are groups, then $K \leq G$ is a supergroup of H (in G) iff $H < K$. K is a contributing supergroup iff in addition $\mu_G(K) \neq 0$; K in particular must be maxint (an intersection of maximal subgroups of G, see p. 3). A contributing set of H is any set of supergroups of H that contains all contributing supergroups. A counting set of H means any subset S of a contributing set of H such that

$$\mu_G(H) + \sum_{K \in S} \mu_G(K) = 0 \quad ;$$

having this last definition is useful because very often the 'contributions' (i.e. μ_G value) of certain categories of supergroups cancel, and so these may be ignored.

The following lemma is particularly useful in enumerating supergroups of a certain (isomorphism) type. (The proof is simple and left to the reader.)

Lemma

Let G be any finite group; suppose G has subgroups of type K, and then K has subgroups of type H. Let $\mathcal{H}$, $\mathcal{K}$ be classes under Aut(G) of subgroups in G of type H, K, these classes being of length h, k respectively. Suppose $K \in \mathcal{K}$ contains m groups $H \in \mathcal{H}$. Then

$$\text{the number of supergroups in } \mathcal{K} \text{ of any } H \in \mathcal{H} = \frac{km}{h} .$$

This lemma (I will call it the supergroup lemma) will often be used, usually tacitly. Note also that if $\mathcal{H}$, $\mathcal{K}$ are simply conjugacy classes under G (rather than classes under Aut(G)), an analogous result holds.

I revert for a moment to lattices $\mathcal{L}$ in general, with obvious extensions of definitions.

Lemma

Suppose $\mathcal{L}$ has maximum element G and other element H. There is an 'induced' lattice $\mathcal{L}'$ on any counting set S of H as long as S has a maximum element M. If further $\forall K \in S \setminus \{M\}$ the set $S_K \subseteq S$ where

$$S_K = \{J \in S : K < J \leqslant M\}$$

is a counting set for K in G, then

$$\mu_{\mathcal{L}}(H, G) = \mu_{\mathcal{L}}(M, G) \cdot \mu_{\mathcal{L}'}(H, M) \ .$$

In particular if S is a contributing set of H we <u>always</u> have

$$\mu_{\mathcal{L}}(H, G) = \mu_{\mathcal{L}'}(H, G) \ .$$

I shall call this lemma the <u>sublattice lemma.</u>

Proof

This is by induction on the ordering of $\mathcal{L}$.

Suppose firstly that $H < G$ and $\nexists$ K s.t. $H < K < G$. Then the only counting set S of H is the singleton $\{G\}$, and $\mathcal{L}'$ is the lattice of two elements $\{H, G\}$ with $H < G$, with maximum element $M = G$. Then clearly

$$\mu_{\mathcal{L}}(H, G) = -1 = \mu_{\mathcal{L}'}(H, G) = \mu_{\mathcal{L}}(M, G)\, \mu_{\mathcal{L}'}(H, M) \ .$$

Suppose now that $H < G$ and that the result is true for all K in $\mathcal{L}$ for which $H < K < G$. Then taking $S, \mathcal{L}'$ and M as in the statement,

$$\mu_\ell(H, G) = -\sum_{K \in S} \mu_\ell(K, G)$$

$$= -\mu_\ell(M, G) \cdot \sum_{K \in S} \mu_{\ell'}(K, M) \quad \text{(by inductive supposition)}$$

$$= -\mu_\ell(M, G) \cdot -\mu_{\ell'}(H, M)$$

(Finally when S is a contributing set, we have M = G)

□

Notation

The symbols C_d, D_{2d}, V_q for $d \in \mathbb{N}$, q a prime power, will mean respectively the cyclic group of order d, the dihedral group of order 2d and the elementary abelian group of order q.

The symbol q will always represent the prime p to the power e.

Merely to simplify subscripts I introduce the following functions $r, s : \mathbb{N} \to \mathbb{Q}$ which are defined (given prime p) by:

$$r : f \longmapsto \frac{1}{2}(p^f - 1)$$

$$s : f \longmapsto \frac{1}{2}(p^f + 1).$$

Also the symbol pf as a subscript represents the prime power p^f.

Now specialising more to the present case, I complete giving the notation that will describe the types of subgroups of $PSL_2(q)$ and $PGL_2(q)$.

The elements of $PSL_2(q)$, any odd q, can be regarded as the linear fractional transformations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \longmapsto \frac{az + b}{cz + d} \qquad (\text{recall } ad - bc = 1)$$

with $z \in GF(q) \cup \{\infty\}$; call the latter union the set of marks. It is consideration of this action which largely informs us about the group's structure (although there is an alternative approach identifying trace with conjugacy class, which we shall meet in Chapter 3, section 2).

The $q + 1$ subgroups of $PSL_2(q)$ that are each the stabilizer of a mark are conjugate and are metabelian, a V_q extended by a $C_{r(e)}$ ([5], §250). All subgroups of $PSL_2(q)$ fixing a mark will hence be elementary abelian, cyclic or 'properly' metabelian, i.e. a V_{pf} extended by a C_d for some $p^f \mid q$, $1 < d \mid r(e)$: we denote the latter $M_{f,d}$ (or $M_{q,d}$ for $f = e$).

Similarly $PGL_2(q)$, any q, acts on the set of marks with metabelian stabilizers, this time a V_q extended by a C_{q-1}. Again we denote subgroups of this by $M_{f,d}$ (or $M_{q,d}$ for $f = e$) where $d \mid (q - 1)$ as appropriate.

S_f will denote a group isomorphic to $PSL_2(p^f)$, given prime p.

G_f will denote a group isomorphic to $PGL_2(p^f)$, given prime p.

Finally, S^n will denote the symmetric group on n elements ,

A^n will denote the alternating group on n elements.

I now proceed to discriminate some 'special' V_{pf} and $M_{f,d}$ in G (G some given S_e or G_e over GF(q), $q = p^e$).

If $H \leqslant G$ fixes the mark λ , we sometimes express this by writing $H^{(\lambda)}$.

Now $$V_q^{(\infty)} = \left\{ \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} : \lambda \in GF(q) \right\} .$$

Subgroups $V_{pf}^{(\infty)} \leqslant V_q^{(\infty)}$ for $f \leqslant e$ are given by:

$$V_{pf}^{(\infty)} = \left\{ \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} : \lambda \text{ ranges over a subgroup (of type } V_{pf}) \text{ of the additive group of GF(q)} \right\}.$$

Now suppose H is some V_{pf} or $M_{f,d}$ for $f \leqslant e$. Conjugate H to obtain $H' < M_{q,c(q-1)}^{(\infty)}$ (where $c := (1 ; \frac{1}{2})$ as $G = (G_e ; S_e$ with p odd)).

Then

$$H' \cap V_q^{(\infty)} = \left\{ \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} : \lambda \in A \text{ for some additive subgroup A of type } V_{pf} \text{ in GF(q)} \right\}$$

and I define mult(H) to be the multiplier of A, i.e. the set of elements α in GF(q) s.t. $\alpha A = A$ taken together with the zero element of GF(q). Mult(H) is well-defined, and is a subfield of GF(q).

If for some $f \mid e$ and $H \cong V_{pf}$ or $M_{f,d}$ (some d) we have mult(H) = $GF(p^f)$ (the same f), then I call H special. In all such cases, H will be denoted with an asterisk, H*, if I want to highlight the property.

1. MÖBIUS FUNCTION OF $G := PSL_2(p^e)$, p odd, $e > 1$

First I review the subgroup types of G; for more detail see Dickson [5] chapter12, especially §260.

G clearly has a subgroup S_f for each $f \mid e$ (simply take the matrices with entries in $GF(p^f) \subset GF(q)$); this S_f is its own normalizer except when $\frac{e}{f}$ is even when

$$N_G(S_f) \cong G_f .$$

These subgroups S_f, G_f are the 'linear' subgroups of G.

G is doubly transitive on its marks; the stabilizer of one mark is the metabelian $M_{q,r(e)}$, its normalizer is itself. The stabilizer of any two marks is a $C_{r(e)}$ with

$$N_G(C_{r(e)}) = D_{2r(e)} \ .$$

G also has subgroups $C_{s(e)}$; G may be regarded as a subgroup of S_{2e}, and then these $C_{s(e)}$ are intersections of G with $C_{r(2e)}$ in S_{2e}. Again

$$N_G(C_{s(e)}) = D_{2s(e)} \ .$$

Of the dihedral groups, the Klein-4's V_4 are exceptional in that they alone are subgroups of more than one maximal dihedral group $D_{2r(e)}$ or $D_{2s(e)}$ in G (they are clearly subgroups of exactly three such groups).

G finally has the following 'exceptional' subgroups

A^5 iff $q \equiv \pm 1 \bmod 5$

S^4 iff $q \equiv \pm 1 \bmod 8$

A^4 always.

(Note: $A^5 \cong PSL_2(5)$; $S^4 \cong PGL_2(3)$; $A^4 \cong PSL_2(3)$,

so these can also appear as 'standard' subgroups of G if respectively:

$p = 5$; $p = 3$, e even ; $p = 3$.

In the case $p = 3$, the exceptional and standard A^4's coincide; likewise the S^4's when ~~likewise~~ e is even.)

The above account for all subgroups of G.

The maximal subgroups of G are those of type:

S_f with $\frac{e}{f}$ odd prime

if e even G_k where $k = \frac{e}{2}$

$M_{q,r(e)}$

D_{q-1}

D_{q+1}

and also for $e = 2$, $p \equiv \pm 2 \bmod 5$, an exceptional case dealt with after the more general result, G has maximal subgroups A^5.

My first objective is to distinguish those subgroups of G which could be the intersection of maximal subgroups (are maxint by abuse of notation) from those that are definitely not; the latter automatically have μ_G value 0.

1) Suppose cyclic C_d with $d \mid \frac{1}{2}(q \pm 1)$ and $d > 2$ is maxint. Then C_d evidently must be the intersection of maximal cyclic subgroups (of order $\neq p$ and greater than two) of maximal subgroups of G, i.e. the intersection of groups of type

$C_{s(f)}$, $C_{r(f)}$, with $\frac{e}{f}$ odd prime or $f = e$

if e even $C_{2s(k)}$, $C_{2r(k)}$, where $k = \frac{e}{2}$.

Let $h, g \in \mathbb{N}$, ℓ = h.c.f. $\{h, g\}$, otherwise denoted (h, g). Then

$$(p^h - 1, p^g - 1) = p^\ell - 1$$

$$(p^h + 1, p^g - 1) = \begin{cases} p^\ell + 1 & \text{if } \frac{h}{\ell} \text{ odd and } \frac{g}{\ell} \text{ even} \\ 2 & \text{otherwise} \end{cases}$$

$$(p^h + 1,\ p^g + 1) \quad = \begin{cases} p^{\ell} + 1 & \text{if } \frac{h}{\ell} \text{ odd and } \frac{g}{\ell} \text{ odd} \\ 2 & \text{otherwise} \end{cases}$$

(With the property that maximal cyclic subgroups of G are mutually disjoint apart from the identity in mind) one immediately concludes that

$$d = (p^f + 1) \text{ or } (p^f - 1) \quad \text{with } \frac{e}{f} \text{ even}$$

$$\text{OR} \quad \tfrac{1}{2}(p^f + 1) \text{ or } \tfrac{1}{2}(p^f - 1) \quad \text{with } \frac{e}{f} \text{ odd} .$$

2) Suppose dihedral D_{2d} (for $d \neq p$) is maxint. Then D_{2d} is the intersection of maximal dihedral subgroups of the maximal subgroups of G containing D_{2d}, and considering intersection of cyclic groups as in 1) we obtain

$$d = p^f \pm 1 \quad \text{with } \frac{e}{f} \text{ even}$$

$$\text{or} \quad d = \tfrac{1}{2}(p^f \pm 1) \quad \text{with } \frac{e}{f} \text{ odd} \qquad \text{or} \quad d = 2 .$$

3) First a note:

Note Let α be a primitive element of $GF(p^e)$.

For $f \mid e$, let A_f be an additive subgroup of $GF(p^e)$ of type V_{pf} with multiplier $GF(p^f)$. $\exists$ exactly $\frac{p^e - 1}{p^f - 1} := k$ such A_f (see Dickson §71), each having the form :

$$\alpha^i GF(p^f) \qquad i \in \{1, \ldots, k\}$$

The intersection of any A_g with any A_h is either 0 or is an A_ℓ where $\ell := \text{h.c.f. } \{ h, g \}$.

□

Now suppose V_{pf} is maxint; then it is the intersection of maximal abelian subgroups of maximal subgroups of G and thus of

$$V^*_{p^h} \quad \text{with } \frac{e}{h} \text{ prime or } h = e.$$

But by the note, for any g, h | e,

$$V^*_{p^h} \bigcap V^*_{p^g} = V^*_{p^\ell} \text{ or } I \ .$$

Thus our V_{p^f} is special, and in particular f | e.

4) If $M_{f,d}$ is maxint, it is the intersection of groups of types $M_{h,r(h)}$ for $\frac{e}{h}$ odd prime or h = e, and $M_{h,2r(h)}$ for $h = \frac{e}{2}$ if e even. These groups are in particular special in G.

By the note in 3), $M_{f,d}$ is entitled to be denoted $M^*_{f,d}$ and in particular f | e.

Let c : = (2 ; 1) as $\frac{e}{f}$ is (even ; odd). It is quickly checked by the supergroup lemma that $M_{f,d}$ is contained in a unique $M_{f,cr(f)}$ and all maximal subgroups in G containing $M_{f,d}$ also contain $M_{f,cr(f)}$ so we conclude these two groups are equal.

5) Suppose S_f is maxint. If $\frac{e}{f}$ is even, then its supergroups are exactly a G_f and its respective supergroups in G. Thus $\frac{e}{f}$ is odd.

At this stage, we have 'eliminated' enough subgroups of G (by showing they are not maxint) to make a systematic treatment of the remaining subgroups manageable. We need only deal with the following categories:

i) a) S_f for $\frac{e}{f}$ odd b) G_f for $\frac{e}{f}$ even

ii) a) $M_{f,r(f)}$ for $\frac{e}{f}$ odd b) $M_{f,2r(f)}$ for $\frac{e}{f}$ even

iii) $V^*_{p^f}$

iv) the 'exceptional' subgroups of type A^5, S^4 and A^4

v) a) $D_{2r(f)}$ for $\frac{e}{f}$ odd c) $D_{2.2r(f)}$ for $\frac{e}{f}$ even

b) $D_{2s(f)}$ for $\frac{e}{f}$ odd d) $D_{2.2s(f)}$ for $\frac{e}{f}$ even

vi) a) $C_{r(f)}$ for $\frac{e}{f}$ odd c) $C_{2r(f)}$ for $\frac{e}{f}$ even

b) $C_{s(f)}$ for $\frac{e}{f}$ odd d) $C_{2s(f)}$ for $\frac{e}{f}$ even

vii) V_4

viii) C_2

xi) I

The symbol K will always represent a subgroup of the category being currently considered.

The number of groups in each category (and for each divisor f of e) is given by $|G| / |K|$ except

i) b) & ii) b) , also A^5 and S^4 of iv) : $\frac{2|G|}{|K|}$

iii) $\frac{c|G|}{q(p^f - 1)}$ where c = (2 ; 1) as $\frac{e}{f}$ is (even ; odd)

vi) a), c), d) $\frac{|G|}{q - 1}$ vi) b) $\frac{|G|}{q + 1}$

vii) $\frac{|G|}{12}$

viii) $\frac{|G|}{q \mp 1}$ ($\mp$ as $q \equiv \begin{cases} 1 \\ -1 \end{cases} \mod 4$)

ix) 1

Most conveniently the subgroups of a certain type as listed above all form a single class under AutG, so we will always be able to apply the supergroup lemma.

The ordering i) - ix) of the above categories is such that the supergroups in G of a subgroup in a certain category all lie in the same or in a previous category.

i) a) and b) $K = S_f$ for $\frac{e}{f}$ odd or G_f for $\frac{e}{f}$ even. A contributing set of K is:

a unique S_h $\forall h > f$ s.t. $f|h|e$ and $\frac{e}{h}$ odd

a unique G_h $\forall h > f$ s.t. $f|h|e$ and $\frac{e}{h}$ even .

This contributing set forms a number-theoretic lattice on $\frac{e}{f}$ (see p.6). Immediately, by the sublattice lemma,

$$\mu_G(K) = \mu\left(\frac{e}{f}\right) .$$

ii) a) $K = M_{f,r(f)}$ for $\frac{e}{f}$ odd. A contributing set of K is:

a unique S_h $\forall h$ s.t. $f|h|e$

a unique $M_{h,r(h)}$ $\forall h$ s.t. $f|h|e$, $h > f$.

But the supergroups S_h exactly constitute one S_f and its supergroups;

supposing $f < e$, their total contribution thus is 0. These groups may thus be ignored, leaving us with a counting set, the $M_{h,r(h)}$. The latter form a number-theoretic lattice on $\frac{e}{f}$, with maximal element $M_{q,r(e)}$. But $M_{q,r(e)}$ is a maximal subgroup of G, so

$$\mu_G(M_{q,r(e)}) = -1 \qquad \text{(dealing with case } f = e\text{)}.$$

By the sublattice lemma,

$$\mu_G(K) = -\mu(\tfrac{e}{f}) .$$

b) $K = M_{f,2r(f)}$ for $\frac{e}{f}$ even. A contributing set of K is:

a unique $M_{h,r(h)}$ and S_h $\forall h$ s.t. $f|h|e$ and $\frac{h}{f}$ even

a unique G_h $\forall h$ s.t. $f|h|e$ and $\frac{e}{h}$ even

a unique $M_{h,2r(h)}$ $\forall h > f$ s.t. $f|h|e$ and $\frac{e}{h}$ even

We may ignore the supergroups (as well as itself) of the unique $M_{2f,r(2f)}$ containing K : this leaves

a unique G_h $\forall h$ s.t. $f|h|e$ and $\frac{h}{f}$ odd

a unique $M_{h,2r(h)}$ $\forall h > f$ s.t. $f|h|e$ and $\frac{h}{f}$ odd .

Suppose $f = \frac{e}{2^s}$ where if $2^t || e$ then $s \leq t$.

$$\mu_G(K) + \mu_G(G_f) = 0$$

$$\Rightarrow \mu_G(K) = -\mu(2^s)$$

Now let f be any value less than $\frac{e}{2}$. Then we may discount G_f and its supergroups, leaving the counting set

a unique $M_{h,2r(h)}$ $\quad \forall h > f$ s.t. $f|h|e$ and $\frac{h}{f}$ odd.

Let $2^t || e$, $2^s || f$ and $r = t - s \geq 1$.

Then the counting set forms a number-theoretic lattice on $\frac{e}{2^r f}$ with maximal element $M_{h,2r(h)}$ with $h = \frac{e}{2^r}$. By sublattice lemma

$$\mu_G(K) = -\mu(2^r) \cdot \mu\left(\frac{e}{2^r f}\right) = -\mu\left(\frac{e}{f}\right) .$$

(Note: for $n, m \in \mathbb{N}$, the only instance that

$$\mu(n)\,\mu(m) \neq \mu(nm)$$

is when n and m are both square free and share a prime divisor. We have $2 \nmid \left(\frac{e}{2^r f}\right)$)

iii) $K = V^*_{pf}$. A contributing set of K is

a unique $V^*_{p^h}$ $\quad \forall h > f$ s.t. $f|h|e$

$p^{e-h} M_{h,r(h)}$, $p^{e-h} S_h$ $\quad \forall h$ s.t. $f|h|e$ and $\frac{e}{f}$ odd

$p^{e-h} M_{h,2r(h)}$, $p^{e-h} G_h$ $\quad \forall h$ s.t. $f|h|e$ and $\frac{e}{f}$ even .

The supergroups on the second, also the third, line have cancelling contributions by i) and ii). So we have a counting set, and a number-theoretic lattice on $\frac{e}{f}$, with the abelian supergroups; we have $\mu_G(V_q) = 0$ and so also

$$\mu_G(K) = 0 .$$

iv) Let $q \equiv \pm 1 \bmod 5$, $K \cong A^5$.

Unless $e = 2$, $p \equiv \pm 2 \bmod 5$, $\exists$ a power f of p s.t. $f|e$, $f < e$ and $p^f \equiv \pm 1 \bmod 5$. (I for the time being exclude the exceptional case from consideration: it will be dealt with separately after the main result.) In this case each A^5 is contained in some $S_f < G$; it is quickly established that K has a unique supergroup S_f and that the contributing supergroups of K and this S_f coincide (K can only have linear supergroups): so A^5 cannot be maxint.

Exactly the same sort of reasoning holds for $q \equiv \pm 1 \bmod 8$, $K \cong S^4$; $K \cong A^4$ (as any supergroup A^5 is non-contributing), so in all cases

$$\mu_G(K) = 0 .$$

□

I now identify and label some exceptional cases which occur because of co-incidence of elements of categories vii), viii), ix) (i.e. V_4, C_2, I) with some elements in categories v) and vi).

I) $p = 3$, e even.

Then $C_{2r(1)} \cong C_2$, $D_{2.2r(1)} \cong V_4$

II) $p = 3$, e odd.

Then $C_{r(1)} \cong I$, $D_{2.r(1)} \cong C_2$

$C_{s(1)} \cong C_2$, $D_{2.s(1)} \cong V_4$

III) $p = 5$, e odd.

Then $C_{r(1)} \cong C_2$, $D_{2r(1)} \cong V_4$

In my treatment of categories v) and vi) following, these groups are tacitly excluded and will be dealt with in vii), viii) and ix) as appropriate.

v) **The Dihedral Groups**

Firstly note that $M_{q,r(e)}$ has no dihedral subgroups (except possibly some D_{2p}).

a) K has contributing set:

a unique $D_{2r(h)}$ $\quad \forall h > f$ s.t. $f|h|e$

a unique S_h $\quad \forall h \geq f$ s.t. $f|h|e$

But the supergroups S_h exactly constitute a S_f and its supergroups and so may be ignored (as long as $f \neq e$). This leaves us with a number-theoretic lattice on $\frac{e}{f}$, with maximum element $D_{2r(e)}$ which is a maximal subgroup of G and so has μ_G value -1. Thus

$$\mu_G(K) = -\mu(\tfrac{e}{f})$$

b) The argument and result as for **a)**.

c) K has contributing set given by the following table (all subsequent tables will be headed identically: I will sometimes omit to write the headings down.)

Supergp. Type J	Condns. on h $\forall h$ s.t. $f\|h\|e$ and...	# K in J	# supergps. J of K	$\mu_G(K)$
S_h	$\frac{h}{f}$ even, $\frac{e}{h}$ odd	$\frac{\|J\|}{\|K\|}$	1	$\mu(\frac{e}{f})$
G_h	$\frac{e}{h}$ even	$\frac{\|J\|}{\|K\|}$	2	$\mu(\frac{e}{f})$
$D_{2r(h)}$	$\frac{h}{f}$ even, $\frac{e}{h}$ odd	$\frac{\|J\|}{\|K\|}$	1	$-\mu(\frac{e}{f})$
$D_{2.2r(h)}$	$f < h$ and not both ($\frac{h}{f}$ even, $\frac{e}{h}$ odd)	$\frac{\|J\|}{\|K\|}$	1	?

We may ignore the unique $D_{2r(2f)}$ and its supergroups, leaving

a unique $D_{2.2r(h)}$	$\forall h > f$ s.t. $f\|h\|e$ and $\frac{h}{f}$ odd
two G_h	$\forall h \geq f$ s.t. $f\|h\|e$ and $\frac{h}{f}$ odd

If $2^s|e$ for some $s \geq 1$ and $f = \frac{e}{2^s}$, then

$$\mu_G(K) = -2\ \mu_G(G_f) = -2\,\mu(2^s)$$

otherwise for other values of f we may ignore the supergroups G_h, and an argument identical to that at the end of ii) b) yields

$$\mu_G(K) = -2\mu\left(\frac{e}{f}\right)$$

d) Similar situation and result to above.

vi) **a)** $K = C_{r(f)}$ for $\frac{e}{f}$ odd has 'contributing table':

Type of supergp.				Number
$J =$	S_h	-	$\|J\|/(p^h-1)$	$(p^e-1)/(p^h-1)$	$\mu\left(\frac{e}{h}\right)$
	$M_{h,r(h)}$	-	p^h	$2(p^e-1)/(p^h-1)$	$-\mu\left(\frac{e}{h}\right)$
	$D_{2r(h)}$	-	1	$(p^e-1)/(p^h-1)$	$-\mu\left(\frac{e}{h}\right)$
	$C_{r(h)}$	$h > f$	1	1	?

All supergroups $D_{2r(h)}$ and S_h may be ignored as their contributions cancel. It is then trivial to prove by induction on $n :=$ # prime divisors counting multiplicities of $\frac{e}{f}$ that

$$\mu_G(K) = \frac{2(p^e - 1)}{p^f - 1}\,\mu\left(\frac{e}{f}\right)$$

b) $K = C_{s(f)}$ for $\frac{e}{f}$ odd has contributing table:

Type of supergp.				Number	
$J =$	S_h	-	$\|J\|/(p^h+1)$	$(p^e+1)/(p^h+1)$	$\mu(\frac{e}{h})$
	$D_{2s(h)}$	-	1	"	$-\mu(\frac{e}{h})$
	$C_{s(h)}$	$h > f$	1	1	?

For each h, the (contributions of the) groups $D_{2s(h)}$ and S_h cancel; this means in particular

$$\mu_G(C_{s(e)}) = 0$$

and hence in general

$$\mu_G(K) = 0 \ .$$

c) $K = C_{2r(f)}$ with $\frac{e}{f}$ even. Extracting the unique supergroup of K of type $C_{r(2f)}$ and its supergroups, K has counting set:

Type of supergp.				Number	
$J =$	G_h	$\frac{h}{f}$ odd	$\|J\|/2(p^h-1)$	$(p^e-1)/(p^h-1)$	$\mu(\frac{e}{h})$
	$M_{h,2r(h)}$	$\frac{h}{f}$ odd	p^h	$2(p^e-1)/(p^h-1)$	$-\mu(\frac{e}{h})$
	$D_{2.2r(h)}$	$\frac{h}{f}$ odd	1	$\frac{1}{2}(p^e-1)/(p^h-1)$	$-2\mu(\frac{e}{h})$
	$C_{2r(h)}$	$\frac{h}{f} > 1$ odd	1	1	?

Immediately, $\mu_G(K) = 2\left(\frac{p^e - 1}{p^f - 1}\right)\mu(\frac{e}{f})$.

d) $K = C_{2s(f)}$ with $\frac{e}{f}$ even. Extracting the unique supergroup of K of

type $C_{r(2f)}$ and its supergroups, K has counting set:

Type of supergp.				Number	
J =	G_h	$\frac{h}{f}$ odd	$\|J\|/2(p^h+1)$	$(p^e-1)/(p^h+1)$	$\mu(\frac{e}{h})$
	$D_{2.2s(h)}$	"	1	$(p^e-1)/2(p^h+1)$	$-2\mu(\frac{e}{h})$
	$C_{2s(h)}$	$\frac{h}{f}>1$ odd	1	1	?

Immediately, $\mu_G(K) = 0$.

vii) $\underline{K = V_4}$ –

Firstly, suppose q is not exceptional case I), II) or III). Then K has contributing set:

Type of supergp.				Number	
J =	G_h	$\frac{e}{h}$ even	$\|J\|/6$ *	4	$\mu(\frac{e}{h})$
	S_h	$\frac{e}{h}$ odd	$\|J\|/12$	1	$\mu(\frac{e}{h})$
	$D_{2.2r(h)}$	$\frac{e}{h}$ even	$\|J\|/4$	3	$-2\mu(\frac{e}{h})$
	$D_{2r(h)}$	$\frac{e}{h}$ odd	$\begin{cases}\|J\|/4\\0\end{cases}$	$\begin{cases}3\\0\end{cases}$	$-\mu(\frac{e}{h})$
	$D_{2.2s(h)}$	$\frac{e}{h}$ even	$\|J\|/4$	3	$-2\mu(\frac{e}{h})$
	$D_{2s(h)}$	$\frac{e}{h}$ odd	$\begin{cases}0\\\|J\|/4\end{cases}$	$\begin{cases}0\\3\end{cases}$	$-\mu(\frac{e}{h})$

In the table and subsequently in this chapter unless otherwise indicated,

$$\begin{cases}-\\-\end{cases} \text{ as } q \equiv \begin{cases}1\\-1\end{cases} \mod 4$$

*presumes a result we shall derive in section 3 of this chapter, see p. 71.

We have

$$\mu_G(V_4) + \sum_{e/h \text{ even}} (4 - 6 - 6)\,\mu\left(\frac{e}{h}\right) + \sum_{e/h \text{ odd}} (1 - 3)\,\mu\left(\frac{e}{h}\right) = 0 \quad .$$

But if $e > 1$ and not a power of 2, then

$$\sum_{e/h \text{ even}} \mu\left(\frac{e}{h}\right) = \sum_{e/h \text{ odd}} \mu\left(\frac{e}{h}\right) = 0$$

and so $\mu_G(V_4) = 0$.

However if e is a positive power of 2, 2^r say, then

$$\sum_{e/h \text{ even}} \mu\left(\frac{e}{h}\right) = \sum_{n=1}^{r-1} \mu(2^{r-n}) = \mu(2) = -1$$

$$\sum_{e/h \text{ odd}} \mu\left(\frac{e}{h}\right) = \mu(1) = 1$$

Thus $\mu_G(V_4) + 8 - 2 = 0$

$\Rightarrow \quad \mu_G(V_4) = -6$

Now I consider the exceptional cases:

I) The contributing table of K is as before <u>except</u> it has no supergroups of form $D_{2.2r(1)}$. To compensate the value of $\mu_G(K)$ is <u>decreased by $6\mu(e)$</u> from standard result.

II) Exclude $D_{2.s(1)}$, <u>decrease $\mu_G(K)$ by $3\mu(e)$.</u>

III) Exclude $D_{2r(1)}$, <u>decrease $\mu_G(K)$ by $3\mu(e)$.</u>

viii) <u>$K = C_2$.</u> Firstly suppose q is not exceptional I), II) or III).

Then K has contributing table as on next page.

Supergroup of C_2				Number	$\mu_G \div \mu(\frac{e}{h})$
G_h	$\frac{e}{h}$	even	p^{2h}	$\frac{2(q-1)p^h}{p^{2h}-1}$	1
S_h		odd	$\frac{1}{2}p^h(p^h \pm 1)$	$\frac{q \mp 1}{p^h \mp 1}$	1
$M_{h,2r(h)}$		even	p^h	$\frac{2(q-1)}{p^h-1}$	-1
$M_{h,r(h)}$		odd	$\begin{cases} p^h \\ 0 \end{cases}$	$\begin{cases} 2(q-1)/(p^h-1) \\ 0 \end{cases}$	-1
$D_{2.2r(h)}$		even	p^h	$\frac{1}{2}\frac{(q-1)p^h}{p^h-1}$	-2
$D_{2r(h)}$		odd	$\frac{1}{2}(p^h \pm 1)$	$\frac{1}{2}\frac{(q \mp 1)(p^h \pm 1)}{p^h-1}$	-1
$D_{2.2s(h)}$		even	p^h+2	$\frac{1}{2}\frac{(q-1)(p^h+2)}{p^h+1}$	-2
$D_{2s(h)}$		odd	$\frac{1}{2}(p^h + \begin{cases} 1 \\ 3 \end{cases})$	$\frac{1}{2}\frac{(q \mp 1)(p^h + \begin{cases} 1 \\ 3 \end{cases})}{p^h+1}$	-1
$C_{2r(h)}$		even	1	1	$2\frac{q-1}{p^h-1}$
$C_{r(h)}$		odd	$\begin{cases} 1 \\ 0 \end{cases}$	$\begin{cases} 1 \\ 0 \end{cases}$	$2\frac{q-1}{p^h-1}$
V_4		-	3	$\frac{1}{4}(q \mp 1)$	See vii)

N.B. Where the 'double' signs $\pm$, $\mp$ occur in brackets $(p^k \pm 1)$ or $(p^k \mp 1)$ for some k, one reads the 'top' sign if $q \equiv 1 \bmod 4$, the 'bottom' sign if $q \equiv -1 \bmod 4$. This convention shall be kept subsequently in this chapter.

We obtain (eventually) the result:

If $e > 1$ and not a power of 2, then

$$\mu_G(C_2) = 0 - \tfrac{1}{4}(q \mp 1) \quad \mu_G(V_4) = 0 \ .$$

If $e = 2^r$ with $r \geq 1$, then

$$\mu_G(C_2) = -(q-1) - \tfrac{1}{4}(q-1) \quad \mu_G(V_4)$$

$$= \tfrac{1}{2}(q-1) \ .$$

Now to deal with the exceptional cases:

I) From the table we must exclude the $C_{2r(1)}$ and the $D_{2.2r(1)}$ and compensate for change in $\mu_G(V_4)$.

The total effect is to increase $\mu_G(K)$ by $(q-1)\mu(e)$.

II) We exclude $D_{2.r(1)}$, $D_{2s(1)}$ and compensate for V_4.

Decrease $\mu_G(K)$ by $\tfrac{1}{2}(q+1)\,\mu(e)$.

III) We exclude $C_{r(1)}$, $D_{2r(1)}$ and compensate for V_4.

Increase $\mu_G(K)$ by $\tfrac{1}{2}(q-1)\,\mu(e)$.

ix) The supergroups of I in G are simply the non-trivial subgroups of G; so the contributing table of I neatly summarizes the values of μ_G

except $\mu_G(I)$, the latter however being directly determined by it. On the next two pages, the whole result for μ_G is tabulated. The set-out is slightly different to previous tables and is more explicit.

For the contributing table of I we merely ignore the entries for I; we (eventually) calculate that for the standard case

$$\mu_G(I) = 0 \ .$$

For the exceptional cases I), II) and III) as usual we must make adjustments for the changes of value of $\mu_G(V_4)$ and $\mu_G(C_2)$ as appropriate and also for the omissions of the following group types.

I) $C_{2r(1)}$, $D_{2.2r(1)}$

II) $C_{r(1)}$, $D_{2r(1)}$, $D_{2s(1)}$

III) $C_{r(1)}$, $D_{2r(1)}$

Resulting from this we find:

I) and III) $\mu_G(I) = 0$ II) $\mu_G(I) = |G|\ \mu(e)$

Statement of result

For $G := PSL_2(p^e)$, p odd prime, $e > 1$ and excluding the case $e = 2$, $p \equiv \pm 2 \bmod 5$.

The values of μ_G are as listed below; any subgroup K of G not mentioned has $\mu_G(K) = 0$.

$\forall h$ s.t. $h|e$ and $\frac{e}{h}$ even:

	G_h	$M_{h,2r(h)}$	$D_{2.2r(h)}$	$D_{2.2s(h)}$	$C_{2r(h)}$
Exceptions	-	-	p=3,e even,h=1	-	p=3,e even, h=1
#titled gp.J in G	$\frac{2\|G\|}{\|J\|}$	$\frac{2\|G\|}{\|J\|}$	$\frac{\|G\|}{\|J\|}$	$\frac{\|G\|}{\|J\|}$	$\frac{\|G\|}{q-1}$
$\mu_G(J)$	$\mu(\frac{e}{h})$	$-\mu(\frac{e}{h})$	$-2\mu(\frac{e}{h})$	$-2\mu(\frac{e}{h})$	$\frac{2(q-1)\mu(\frac{e}{h})}{\|J\|}$

$\forall h$ s.t. $h|e$ and $\frac{e}{h}$ odd:

	S_h	$M_{h,r(h)}$	$D_{2r(h)}$	$D_{2s(h)}$	$C_{r(h)}$
Exceptions	-	-	p=3 or 5,e odd,h=1	p=3, e odd, h=1	p=3 or 5, e odd, h=1
#titled gp.J in G	$\frac{\|G\|}{\|J\|}$	$\frac{\|G\|}{\|J\|}$	$\frac{\|G\|}{\|J\|}$	$\frac{\|G\|}{\|J\|}$	$\frac{\|G\|}{q-1}$
$\mu_G(J)$	$\mu(\frac{e}{h})$	$-\mu(\frac{e}{h})$	$-\mu(\frac{e}{h})$	$-\mu(\frac{e}{h})$	$\frac{q-1}{\|J\|}\mu(\frac{e}{h})$

Also:

$\mu_G(V_4) = (-6\ ;\ 0)$ as $(e = 2^r,\ r \geq 1\ ;$ otherwise)

but subtract $6.\mu(e)$ if p = 3, e even

subtract $3.\mu(e)$ if p=3 or 5, e odd.

$\mu_G(C_2) = ((q-1)/2;\ 0)$ as $(e=2^r,\ r \geq 1;$ otherwise)

but subtract $-(q-1)\mu(e)$ if $p = 3$, e even

subtract $+(q+1)\mu(e)/2$ if $p = 3$, e odd

subtract $-(q-1)\mu(e)/2$ if $p = 5$, e odd .

$$\mu_G(I) = 0$$

except

if $p = 3$, e odd when

$$\mu_G(I) = |G|\mu(e) .$$

□

Determination of Result for $G := PSL_2(p^2)$, $p \equiv \pm 2 \bmod 5$

We now have maximal subgroups in G of type A^5; the results for the case $e > 2$ found above carry through except for the subgroups of the A^5's, i.e. the subgroups of G of type A^5, A^4, D_{10}, $D_6 \cong S^3$, V_4, C_5, C_3, C_2 and I.

Thus the values of μ_G are as before apart from the following compensations (entirely due to the lattice structure of the A^5's):

A^5 subtract 1

A^4

$\#A^5$ containing an $A^4 = 2$; thus add 2

For both $K = D_{10}$ or D_6

$\#A^5$ containing a $K = 2$; thus add 2

V_4

$\#A^5$ containing a $V_4 = 2$

$\#A^4$ containing a $V_4 = 1$

Thus $\mu_G(V_4)$ unaltered

C_5 (N.B. $q \equiv -1 \bmod 5 \Rightarrow 5|(q+1)/2$)

$\# A^5$ containing a C_5 = $(q+1)/5$

$\# D_{10}$ containing a C_5 = $(q+1)/10$

Thus $\mu_G(C_5)$ unaltered

C_3 (N.B. q is a square $\Rightarrow q \equiv 1 \bmod 3 \Rightarrow 3|(q-1)/2$)

$\# A^5$ containing a C_3 = $(q-1)/3$

$\# A^4$ containing a C_3 = $(q-1)/3$

$\# D_6$ containing a C_3 = $(q-1)/6$

Thus subtract $2(q-1)/3$

C_2

	A^5	A^4	D_{10}	D_6	V_4
# titled supergp.J	$(q-1)/2$	$(q-1)/4$	$(q-1)/2$	$(q-1)/2$	$(q-1)/4$
Change in $\mu_G(J)$	-1	+2	+2	+2	0

Thus subtract $2(q-1)$

I: Add $2|G|$, concluded from following table (which also summarizes result);

	A^5	A^4	D_{10}	D_6	C_3	C_2
# titled gp.J in G	$\frac{\|G\|}{30}$	$\frac{\|G\|}{12}$	$\frac{\|G\|}{10}$	$\frac{\|G\|}{6}$	$\frac{\|G\|}{q-1}$	$\frac{\|G\|}{q-1}$
Change in $\mu_G(J)$	-1	+2	+2	+2	$\frac{-2(q-1)}{3}$	-2(q-1)

2. MÖBIUS FUNCTION OF G : = $PSL_2(2^e)$, e > 1

I review the subgroups of G (again see Dickson §260). The structure is significantly simpler than the odd prime power case. Most importantly there is less discrimination between groups associated with a divisor h of e for which $\frac{e}{h}$ is odd and those for which $\frac{e}{h}$ is even, due to the fact

$$S_h \cong G_h \qquad \forall h \in \mathbb{N} .$$

So G has subgroups S_h $\forall h$ s.t. $h|e$, and these are their own normaliser in G. The stabilizer of a mark is a metabelian $M_{q,2r(e)}$, which again is its own normaliser. The stabilizer of a pair of marks is a $C_{2r(e)}$ with

$$N_G(C_{2r(e)}) \cong D_{4r(e)} .$$

G also has subgroups $C_{2s(e)}$ with

$$N_G(C_{2s(e)}) \cong D_{4s(e)} \qquad \text{(c.f. odd prime power case)} .$$

G has no other 'exceptional' subgroups.

The maximal subgroups of G are those of type:

S_f with $\frac{e}{f}$ prime

$M_{q,2r(e)}$

$D_{4r(e)}$

$D_{4s(e)}$

Using exactly analogous arguments (involving intersections of maximal subgroups) as used in the corresponding stage in section 1, we may eliminate from consideration many of the subgroups of G. In fact $K \leqslant G$ has $\mu_G(K) = 0$ unless K lies in one of the following categories (for some $f|e$, $f > 1$):

i) S_f

ii) $M_{f,2r(f)}$

iii) $V^*_{p^f}$

iv) (a) $D_{4r(f)}$, $f > 2$ (b) $D_{4s(f)}$ (c) D_6

v) (a) $C_{2r(f)}$, $f > 2$ (b) $C_{2s(f)}$ (c) C_3

vi) C_2

vii) I

The 'small' subgroups D_6, C_3, C_2 are exactly the types if $f = 1$ (and $f = 2$ if e even in iv) a) and v) a)) were allowed in the other categories; then however each would fall into more than one category, and so they must be dealt with separately as above. (In particular the categories above are mutually disjoint.)

The number of groups in the categories above are $|G|/|K|$ except:

iii) $\frac{|G|}{q.2r(f)}$

v) (a), (b) if $\frac{e}{f}$ even , (c) if e even : $\frac{|G|}{4r(e)}$

v)(b) if $\frac{e}{f}$ odd, (c) if e odd: $\frac{|G|}{4s(e)}$

vi) $\frac{|G|}{q}$

vii) 1

All the sets of subgroups in a certain category (for a fixed f) form a single conjugacy class in G, so we may again avail ourselves freely of the supergroup lemma.

I deal with the categories in turn:

i) $\underline{K = S_f}$. Contributing set:

a unique S_h $\forall h > f$ s.t. $f|h|e$

Also $\mu_G(S_e) = \mu_G(G) = 1$. Immediately

$$\mu_G(K) = \mu\left(\frac{e}{f}\right) .$$

ii) $\underline{K = M_{f,2r(f)}}$. Contributing set:

a unique S_h $\forall h$ s.t. $f|h|e$

a unique $M_{h,2r(h)}$ $\forall h > f$ s.t. $f|h|e$

The second line alone forms a counting set.

Now $\mu_G(M_{q,2r(e)}) = -1$.

By the sublattice lemma,

$$\mu_G(K) = -\mu(\tfrac{e}{f}) .$$

iii) $K = V^*_{p^f}$. Contributing set:

$2^{e-h}\, S_h$ $\quad \forall h$ s.t. $f|h|e$

$2^{e-h}\, M_{h,2r(h)}$ $\quad \forall h$ s.t. $f|h|e$

a unique $V^*_{p^h}$ $\quad \forall h > f$ s.t. $f|h|e$

Immediately, $\mu_G(K) = 0$.

iv) a) $K = D_{4r(f)}$, $f > 2$. Contributing set:

a unique S_h $\quad \forall h$ s.t. $f|h|e$

a unique $D_{4r(h)}$ $\quad \forall h > f$ s.t. $f|h|e$

The second line alone forms a counting set (for $f < e$). Also $\mu_G(D_{4r(e)}) = -1$.

$$\mu_G(K) = -\mu(\tfrac{e}{f}) .$$

iv) b) $K = D_{4s(f)}$. Contributing set:

a unique S_h $\quad \forall h$ s.t. $f|h|e$

a unique $D_{4r(h)}$ $\quad \forall h$ s.t. $f|h|e$ and $\frac{h}{f}$ even

a unique $D_{4s(h)}$ $\quad \forall h > f$ s.t. $f|h|e$ and $\frac{h}{f}$ odd

For $f < e$, the S_h may be ignored, leaving us with a number-theoretic lattice on the dihedral supergroups with maximal element M either a $D_{4r(e)}$ or a $D_{4s(e)}$. Thus M is a maximal subgroup of G.

$$\mu_G(M) = -1 \quad .$$

Observing that values $\mu_G(D_{4r(h)})$ are consistent with the result by (a), we conclude

$$\mu_G(K) = -\mu(\tfrac{e}{f}) \quad .$$

(c) $K = D_6$. Contributing set as in (b) for f = 1 except

no S_1

no $D_{4r(2)}$ if e even .

For e odd S_h cancels with $D_{4s(h)}$ $\forall h > 1$. So

$$\mu_G(K) = 0 \quad .$$

For e even S_h cancels with $D_{4r(h)}$ or $D_{4s(h)}$ as appropriate $\forall h > 2$.

Thus

$$\mu_G(K) + \mu_G(S_2) = 0$$

$$\Rightarrow \mu_G(K) = -\mu(\tfrac{e}{2}) \quad .$$

v) (a) $K = C_{2r(f)}$, $f > 2$. Contributing table (with format as that on p.51).

Supergroup				Number	
J =	S_h	-	$\lvert J\rvert /4r(h)$	$(q-1)/(2^h-1)$	$\mu(\frac{e}{h})$
	$M_{h,2r(h)}$	-	2^h	$2(q-1)/(2^h-1)$	$-\mu(\frac{e}{h})$
	$D_{4r(h)}$	-	1	$(q-1)/(2^h-1)$	$-\mu(\frac{e}{h})$
	$C_{2r(h)}$	h > f	1	1	?

The supergroups S_h, $D_{4r(h)}$ cancel; by induction on the number of prime divisors (counting multiplicities) of $\frac{e}{f}$, we conclude

$$\mu_G(K) = \frac{2(q-1)}{2^h-1}\,\mu(\tfrac{e}{h}) \cdot$$

(b) $\underline{K = C_{2s(f)}}$. If $\frac{e}{f}$ is even, K has a unique supergroup $C_{2r(2f)}$; we may discount this $C_{2r(2f)}$ and its supergroups leaving us the counting table:

Supergroup					Number	
J	=	S_h	$\frac{h}{f}$ odd	$\lvert J\rvert/4s(h)$	$(q+1)/(2^h+1)$	$\mu(\frac{e}{h})$
		$D_{4s(h)}$	$\frac{h}{f}$ odd	1	$(q+1)/(2^h+1)$	$-\mu(\frac{e}{h})$
		$C_{2s(h)}$	$\frac{h}{f}>1$ odd	1	1	?

The $D_{4s(h)}$ and the S_h cancel: by trivial induction

$$\mu_G(K) = 0 \cdot$$

(c) $\underline{K = C_3}$.

For e odd. A counting set of C_3 is exactly as in table v) (b) for f = 1, except we exclude the S_1 (otherwise they are counted twice). Thus

$$\mu_G(K) + \frac{(q+1)}{3}\mu_G(D_6) = 0 \quad \Rightarrow \quad \mu_G(K) = 0 \cdot$$

For e even. Now $C_3 = C_{2s(1)} = C_{2r(2)}$. For each even $h \mid e$ s.t. $h > 2$, K has supergroups as in table v) (a) and these cancel; for each odd $h \mid e$ s.t. $h > 1$, K has supergroups as in table v) (b) and these cancel. We are left with the counting set:

$(q-1)/3$ $\quad D_6$

$2(q-1)/3$ $\quad M_{4,3}$

$(q-1)/3$ $\quad S_2$

and we conclude $\mu_G(K) = 2^{\frac{(q-1)}{3}} \mu(\frac{e}{2})$.

vi) $\underline{K = C_2}$. Contributing table:

Supergroup				Number	
J =	S_h	-	$\lvert J\rvert/2^h$	2^{e-h}	$\mu(\frac{e}{h})$
	$M_{h,2r(h)}$	$h > 1$	$\lvert J\rvert/2^h$	2^{e-h}	$-\mu(\frac{e}{h})$
	$D_{4r(h)}$	$h > 2$	$\lvert J\rvert/2$	2^{e-1}	$-\mu(\frac{e}{h})$
	$D_{4s(h)}$	$h > 1$	$\lvert J\rvert/2$	2^{e-1}	$-\mu(\frac{e}{h})$

The supergroups S_h and $M_{h,2r(h)}$ cancel for each $h > 1$, leaving a counting set on the 2^{e-1} $S_1 \cong D_6$ and the supergroups of the bottom two lines.

<u>For e odd:</u> $\mu_G(D_6) = 0$ by iv) (c)

Thus $\mu_G(K) + 2.2^{e-1} \sum_{h|e \text{ s.t. } h>1} -\mu(\frac{e}{h}) = 0$

$\Rightarrow \mu_G(K) = -2^e \mu(e)$ (as $e > 1$) .

<u>For e even:</u> now $\mu_G(D_6) = -\mu(\frac{e}{2})$

$$\mu_G(K) + 2.2^{e-1}\left(\sum_{h>2} -\mu(\frac{e}{h})\right) + 2^{e-1}\mu_G(D_{4.s(2)}) + 2^{e-1}\mu_G(D_6) = 0$$

$$\Rightarrow \quad \mu_G(K) - 2^e\left(\sum_{h>2} \mu(\tfrac{e}{h})\right) - 2^{e-1}\mu(\tfrac{e}{2}) - 2^{e-1}\mu(\tfrac{e}{2}) = 0$$

$$\Rightarrow \quad \mu_G(K) = 2^e \sum_{h>1} \mu(\tfrac{e}{h}) = -2^e\,\mu(e) \ .$$

vii) Again the contributing set for I is given by the statement of result (less the entry for I) below. By straightforward but tedious algebra, it is checked that for both cases e odd and e even that

$$\mu_G(I) = |G|\ \mu(e) \ .$$

Statement of result

For $G := PSL_2(2^e)$, and $e > 1$.

I have already published this particular result in a joint paper with G.A. Jones [6].

The values of μ_G are listed below; any subgroup K of G not mentioned has $\mu_G(K) = 0$.

Isomorphism type of K	$\forall$ h s.t. h|e and ...	Number of subgroups in $G \cong K$	$\mu_G(K)$
S_h	$h > 1$	$\|G\|/\|K\|$	$\mu(\frac{e}{h})$
$M_{h,2r(h)}$	$h > 1$	$\|G\|/\|K\|$	$-\mu(\frac{e}{h})$
$D_{4r(h)}$	$h > 1$	$\|G\|/\|K\|$	$-\mu(\frac{e}{h})$
$D_{4s(h)}$	$h > 1$	$\|G\|/\|K\|$	$-\mu(\frac{e}{h})$
$C_{2r(h)}$	$h > 1$	$\frac{\|G\|}{2(q-1)}$	$\frac{2(q-1)}{2^h-1}\mu(\frac{e}{h})$
C_2	n/a	$\|G\| / q$	$-q\mu(e)$
I	n/a	I	$q(q^2-1)\mu(e)$

3. MÖBIUS FUNCTION OF $G := PGL_2(p^e)$, p odd.

Review of subgroups of G

The structure of G may easily be deduced from that of its subgroup S_e of index 2 (and also from that of the group S_{2e} in which G may be imbedded).

For every divisor h of e, G has subgroups both of type G_h and S_h, with

$$N_G(S_h) \cong G_h \ , \qquad N_G(G_h) = G_h \ .$$

The stabilizer of a mark is a metabelian $M_{q,q-1}$ (again it is its own normalizer in G). The stabilizer of a pair of marks is a $C_{2r(e)}$ with

$$N_G(C_{2r(e)}) \cong D_{4r(e)} \ .$$

G also contains subgroups $C_{2s(e)}$ with

$$N_G(C_{2s(e)}) \cong D_{4s(e)} \ .$$

G finally contains exceptional subgroups type A^5, S^4, A^4 which all occur simply in their rôle of subgroups of the $S_1 < G$ (see p.42), except if $p \equiv \pm 3 \bmod 8$, when G contains a single conjugacy class of $|G|/24$ subgroups of type S^4 which lie in the $G_1 < G$ but not in the S_1.

An important feature of G (as compared to the special linear groups described in section 1) is that both types $C_{r(e)}$, $C_{s(e)}$ of maximal cyclic subgroups have order divisible by 2, giving us two conjugacy classes of involutions, one lying entirely in S_e, the other entirely in $G \setminus S_e$. A $C_2 < G$ with generator in the former class is denoted ${}^aC_2$, the latter ${}^bC_2$. We have

$$\left.\begin{aligned} \#\ {}^{a}C_2 \text{ in } G &= q(q\pm1)/2 \\ \#\ {}^{b}C_2 \text{ in } G &= q(q\mp1)/2 \end{aligned}\right\} \quad \text{as } q \equiv \pm 1 \bmod 4 .$$

The presence of these two classes of involutions obviously is important in any analysis of the dihedral subgroups: in fact it is easy to ascertain:

Lemma (and notation)

G has exactly $|G|/2d$ subgroups of type D_{2d} $\forall\, d > 2$ s.t. $d|(q\pm1)$.

Let $C_d < D_{2d}$.

If $d\,|\,(q\pm1)/2$ (i.e. $d\,|\,r(e)$ or $d\,|\,s(e)$), then these D_{2d} are distributed in two conjugacy classes of order $|G|/4d$, one class consisting of those lying entirely in S_e, the other of those where $D_{2d}\backslash C_d$ lies in $G\backslash S_e$. I denote an element of the first class ${}^{a}D_{2d}$, the second ${}^{b}D_{2d}$.

If $d \nmid (q\pm1)/2$, then the $|G|/2d$ subgroups D_{2d} form a single conjugacy class in G.

□

Of the dihedral subgroups the V_4 are distinguished. This is because if $V_4 < S_e$ (such is denoted ${}^{a}V_4$), then its normaliser is an exceptional subgroup of type S^4; the ${}^{a}V_4$ form a single conjugacy class in G of length $|G|/24$. However if $V_4 \nleq S_e$ (such is denoted ${}^{b}V_4$), then its normaliser is a D_8 (consistent in fact with the lemma for dihedral subgroups in general), and the ${}^{b}V_4$ form a single conjugacy class of length $|G|/8$. In total therefore G contains $|G|/6$ subgroups V_4, a result presumed earlier (p. 55).

Now to start tackling the problem; first I list

The maximal subgroups of G

G_f with $\frac{e}{f}$ prime, $f < e$

S_e

$M_{q,2r(e)}$

$D_{4r(e)}$

$D_{4s(e)}$

Also if $e = 1$, $p \equiv \pm 3 \bmod 8$, $p \neq 3$ (a case henceforth excluded until after the main result; $PGL_2(3) \cong S^4$ excluded too) we have maximal subgroups of type S^4.

The techniques as employed in section 1 at the corresponding stage allow us to say any maxint subgroup of G has one of the types as listed below. The situation now though is still quite complicated. The table displayed has rows labelled i) to x) and two columns (a) and (b), and the entries give twenty categories of groups i)(a) to x)(b) (except some will be empty). A group in an (a) category has least linear supergroup of type S_h for some h, in (b) type G_h. Also f runs through all divisors of e:

	(a)	(b)
i)	S_f	G_f
ii)	$M_{f,r(f)}$	$M_{f,2r(f)}$
iii)	$^aD_{2r(f)}$	$D_{4r(f)}$
iv)	$^aD_{2s(f)}$	$D_{4s(f)}$
v)	$C_{r(f)}$	$C_{2r(f)}$
vi)	$C_{s(f)}$	$C_{2s(f)}$
vii)	V^*_{pf}	

	(a)	(b)
viii)	$^aV_4$	$^bV_4$
ix)	$^aC_2$	$^bC_2$
x)	I	

Definitions and Notes

I shall call the (a) and (b) categories with the same Roman numeral complementary.

We also have a natural subcategorization of each category $\mathcal{C}$ i) to vii), (a) or (b) by divisors f of e; denote this

$$\mathcal{C} = \bigcup \{ \mathcal{C}_f : f|e \}.$$

I shall call the (a) and (b) subcategories with the same Roman numerals and the same divisor subscript f complementary.

Note that the elements ^aK_f of an (a) - subcategory i) to vi) are in 1:1 correspondence with the elements ^bK_f of the complementary subcategory: each ^aK_f can be identified with the unique ^bK_f that contains it with index 2. Such ^aK_f and ^bK_f I call complementary subgroups.

A subcategory i) to vii) is exceptional if it coincides with another subcategory. The only such exceptional cases are:

I) $p = 3$, $f = 1$;

$$C_{s(1)} \cong C_2 ,$$
$$C_{r(1)} \cong I , \quad {}^aD_{2r(1)} \cong C_2 ,$$

$$C_{2r(1)} \cong C_2 \quad , \qquad D_{4r(1)} \cong V_4$$

II) $p = 5$, $f = 1$:

$$C_{r(1)} \cong C_2 \quad , \qquad {}^aD_{2r(1)} \cong V_4$$

These exceptional subcategories shall be tacitly excluded until we tackle the V_4, C_2 and I in their own right.

Each of the subcategories exactly constitute a single conjugacy class of subgroups in G except (possibly) iii)(b) and iv)(b), see lemma p.71. However if $\frac{e}{f}$ is odd, then there are no exceptions, which we see by 2) below is all we need.

We now reduce the calculation by showing in turn:

1) Any $K < G$ in an (a) subcategory i) to vi) for $\frac{e}{f}$ even is not maxint.

2) Any $K < G$ in a (b) subcategory i) to vi) for $\frac{e}{f}$ even is not maxint.

3) If ${}^aK_f$, ${}^bK_f$ are in complementary subcategories for some i) to vi) then

$$\mu_G({}^aK_f) = -\mu_G({}^bK_f) \ .$$

Proofs:

1) Let $K := {}^aK_f$ be a maxint group in a (a) subcategory i) to vi) with divisor f. Then $K < S_e < G$ and so if

$$K = \bigcap_{i \in \Omega} M_i$$

where the M_i, $i \in \Omega$ (Ω just some indexing set), are maximal subgroups of G, then

$$K = \bigcap_{i \in \Omega} (S_e \cap M_i) \ .$$

Clearly if M is any maximal subgroup of G, then $(S_e \cap M)$ is a maximal subgroup of S_e; what the last expression for K then says is that K is maxint in S_e; we use our work in section 1 to conclude $\frac{e}{f}$ is odd.

2) We denote by ${}^bK_f$ any group in any (b) subcategory i) to vi) with divisor f. Suppose $\frac{e}{f}$ is even.

In all cases ${}^bK_f$ has a unique supergroup ${}^aK_{2f}$ in the complementary category. It is straightforward to establish that in any maximal subgroup M of G that contains ${}^bK_f$, ${}^bK_f$ must have a (unique) supergroup ${}^aK'_{2f} \cong {}^aK_{2f}$ (I stress, in M). Necessarily

$${}^aK'_{2f} = {}^aK_{2f}$$

i.e. all maximal subgroups containing ${}^bK_f$ also contain ${}^aK_{2f}$, and the former cannot be maxint.

3) It is trivially established (by supergroup lemma) that ${}^aK_f$ (as in the proposition) has a unique supergroup of type ${}^bK_f$. Also for every (a) subcategory ${}^a\mathcal{C}_h$ s.t. $h > f$, $f|h|e$ we have

$$\#\# \text{ supergroups of } {}^aK_f \text{ in } {}^a\mathcal{C}_h$$

$$= \#\# \text{ supergroups of } {}^aK_f \text{ in the complementary } {}^b\mathcal{C}_h .$$

Notice S_e is maximal in G, so

$$\mu_G(S_e) = -1 = -\mu_G(G_e) \ .$$

The result now follows by induction (on the (a) subcategories ordered as follows:

$$^{a}\mathcal{e}_{h} > {}^{a}\mathcal{e}'_{f}$$

iff either the Roman numeral label of $^{a}\mathcal{e}_{h}$ is greater than that of $^{a}\mathcal{e}'_{f}$

or the Roman numerals are equal and $h < f$).

I now proceed to tackle in turn (for $\frac{e}{f}$ odd on first line):

$$K = G_f;\ M_{f,2r(f)};\ D_{4r(f)};\ D_{4s(f)};\ C_{r(f)};\ C_{s(f)};$$

$$V^*_{pf};\ {}^{a}V_4;\ {}^{b}V_4;\ {}^{a}C_2;\ {}^{b}C_2;\ I$$

i) $K = G_f$

Contributing set:

a unique G_h $\quad \forall\ h > f$ s.t. $f|h|e$

$\mu_G(K) = \mu(\frac{e}{f})$.

ii), iii), iv) $K = K_f := M_{f,2r(f)};\ D_{4r(f)};\ D_{4s(f)}$.

Contributing set:

a unique G_h $\quad \forall h$ s.t. $f|h|e$

a unique K_h $\quad \forall h > f$ s.t. $f|h|e$

The supergroups of the first line may be ignored; K_e is maximal in G;

$$\mu_G(K) = -\mu(\tfrac{e}{f}) .$$

v), vi) $K = C_{r(f)};\ C_{s(f)}$

The contributing table of K in G is exactly the same as the contributing table of K as a subgroup of S_e, see section 1 p.52 - 53 , except the contribution of each supergroup now is the exact negative to what it was before. We conclude

$$\mu_G(C_{r(f)}) = -2\frac{(q-1)}{(p^f-1)}\,\mu(\tfrac{e}{f})$$

$$\mu_G(C_{s(f)}) = 0 .$$

vii) $K = V^*_{pf}$

Contributing set:

$$p^{e-h} \quad G_h,\ S_h,\ M_{h,r(h)},\ M_{h,2r(h)} \qquad \forall\, h \text{ s.t. } f|h|e$$

$$\text{a unique} \quad V^*_{pf} \qquad \forall\, h > f \text{ s.t. } f|h|e$$

The contributions of the supergroups in the top line cancel, we note then $\mu_G(V_q) = 0$ and deduce by induction on the number of prime divisors (counting multiplicities) of $\frac{e}{f}$ that:

$$\mu_G(K) = 0 .$$

viii) (a) and (b)

Recall (also for parts ix), x)) the convention

$$\mp,\ \pm \text{ and } \begin{cases} - \\ - \end{cases} \quad \text{always as } q \equiv \begin{cases} 1 \\ -1 \end{cases} \mod 4$$

unless otherwise stated.

The contributing tables of ${}^aV_4$ and ${}^bV_4$ displayed in one (in which h takes all values s.t. $h|e$ and $\frac{e}{h}$ is odd):

Type J of supergroup	# J containing ${}^aV_4$	Excluding Cases	# J containing ${}^bV_4$	Excluding Cases	$\mu_G(J)$
G_h	1	-	1	-	$\mu(\frac{e}{h})$
S_h	1	-	0	-	$-\mu(\frac{e}{h})$
$D_{4r(h)}$	3	p=3, h=1	1	p=3, h=1	$-\mu(\frac{e}{h})$

Type J of supergroup	#J containing a_{V_4}	Excluding Cases	#J containing b_{V_4}	Excluding Cases	$\mu_G(J)$
${}^aD_{2r(h)}$	$\begin{cases} 3 \\ 0 \end{cases}$	p=3 or 5, h=1	0	-	$\mu(\frac{e}{h})$
$D_{4s(h)}$	3	-	1	-	$-\mu(\frac{e}{h})$
${}^aD_{2s(h)}$	$\begin{cases} 0 \\ 3 \end{cases}$	p=3, h=1	0	-	$\mu(\frac{e}{h})$

We have (excluding the exceptional cases I and II):

$$\mu_G({}^aV_4) = -\sum_{\substack{h \text{ s.t.} \\ e/h \text{ odd}}} (1 - 1 - 3 + \begin{cases} 3 \\ 0 \end{cases} - 3 + \begin{cases} 0 \\ 3 \end{cases}) \mu(\tfrac{e}{h})$$

$$\Rightarrow \mu_G({}^aV_4) = \begin{cases} 3 & \text{if } e = 2^r,\ r \geq 0 \\ 0 & \text{otherwise} \end{cases}$$

Similarly

$$\mu_G({}^bV_4) = \begin{cases} 1 & \text{if } e = 2^r,\ r \geq 0 \\ 0 & \text{otherwise} \end{cases}$$

For p = 3, e odd:

subtract $\mu(e)$ from $\mu_G({}^bV_4)$, do not alter $\mu_G({}^aV_4)$.

For p = 5, e odd:

add $3\mu(e)$ to $\mu_G({}^aV_4)$, do not alter $\mu_G({}^bV_4)$.

ix)(a)

If ${}^aC_2$ has supergroup ${}^bK_h$ in a (b) subcategory i) to vi), then the complementary group ${}^aK_h$ is also a supergroup. Thus the supergroups of ${}^aC_2$ in categories i) to vi) come in complementary pairs, and so their contributions cancel. This leaves a counting set:

$(q \mp 1)/4$ each of ${}^aV_4$ and ${}^bV_4$

so

$$\mu_G({}^aC_2) = \begin{cases} -(q \mp 1) & \text{if } e = 2^r,\ r \geq 0 \\ 0 & \text{otherwise} \end{cases}$$

except if I) $p = 3$, e odd:

the $D_{4s(1)}$ are no longer cancelled by the $D_{2s(1)}$,

compensation is $+ \frac{3(q+1)}{4} \mu(e)$,

$\mu_G({}^bV_4)$ decreased by $\mu(e)$, compensation is $+ \frac{(q+1)}{4} \mu(e)$,

so in total we must add $(q+1)\,\mu(e)$ to $\mu_G({}^aC_2)$

or II) $p = 5$, e odd:

the $D_{4r(1)}$ are no longer cancelled by the $D_{2r(1)}$,

compensation is $+ \frac{3(q-1)}{4} \mu(e)$,

$\mu_G({}^aV_4)$ increased by $3\mu(e)$, compensation is $- \frac{3(q-1)}{4} \mu(e)$,

so $\mu_G({}^aC_4)$ is unaltered.

ix)(b) $K = {}^bC_2$

Contributing table (h takes all values s.t. $h|e$ and $\frac{e}{h}$ is odd):

Type J of supergroup	Exceptional Cases	# supergroups of type J	$\mu_G(J)$
G_h	-	$\frac{q\pm 1}{p^h \pm 1}$	$\mu(\frac{e}{h})$
$M_{h,2r(h)}$	-	$\begin{cases} 0 \\ 2(q-1)/(p^h-1) \end{cases}$	$-\mu(\frac{e}{h})$
$D_{4r(h)}$	I)	$\frac{(q\pm 1)(p^h \mp 1)}{2(p^h-1)}$	$-\mu(\frac{e}{h})$
$D_{4s(h)}$	-	$\frac{(q\pm 1)}{2(p^h+1)}(p^h + \begin{cases} 3) \\ 1 \end{cases}$	$-\mu(\frac{e}{h})$
$C_{2r(h)}$	I)	$\begin{cases} 0 \\ 1 \end{cases}$	$\frac{2(q-1)}{p^h-1}\mu(\frac{e}{h})$

and <u>also</u> ${}^bC_2$ is contained in exactly $(q\pm1)/2$ ${}^bV_4$.

So when <u>$p \equiv 1 \bmod 4$</u>, we calculate :

$$\mu_G({}^bC_2) = \frac{(q+1)}{2} \sum_{\substack{h \text{ s.t.} \\ e/h \text{ odd}}} \mu(\tfrac{e}{h}) = \begin{cases} (q+1)/2 & \text{if } e = 2^r \\ 0 & \text{otherwise} \end{cases}$$

when <u>$p \equiv -1 \bmod 4$</u>

$$\mu_G({}^bC_2) = \frac{(q-1)}{2} \sum_{\substack{h \text{ s.t.} \\ e/h \text{ odd}}} \mu(\tfrac{e}{h})$$

However we also have the exceptional cases:

I) We must compensate for the omission of the $D_{4r(1)}$, $C_{2r(1)}$ and also for the change in $\mu_G({}^bV_4)$. The total compensation is to add $\frac{q-1}{2}\mu(e)$ to $\mu_G({}^bC_2)$.

II) In fact in this instance no compensation is needed and the result is as 'standard'.

x) The contributing set of I is given in the statement of the final result as below by ignoring the entry for I. Apart from the exceptional cases I) and II), the total contribution of all groups in a column headed i) to v) in the table given there always cancel; this leaves a counting set on the V_4 and the C_2 and we calculate: $\mu_G(I) = 0$.

For cases I), II), the appropriate compensations to above give:

I) $\mu_G(I) = -|G| . \mu(e)/2$ II) $\mu_G(I) = -|G| . \mu(e)$

Statement of result

For $G := PGL_2(p^e)$, p odd prime, $e \geq 1$ but excluding the case $e = 1$, $p \equiv \pm 3 \bmod 8$. Let $q = p^e$.

The values of μ_G are as listed below and overleaf; any subgroup K of G not mentioned has $\mu_G(K) = 0$.

$\forall$ h s.t. $h|e$ and $\frac{e}{h}$ odd:

	i)	ii)	iii)	iv)	v)
Type J	G_h	$M_{h,2r(h)}$	$D_{4r(h)}$	$D_{4s(h)}$	$C_{2r(h)}$
Exceptions	-	-	p=3,e odd,h=1	-	p=3,e odd,h=1
# J in G	$\frac{\|G\|}{\|J\|}$	$\frac{\|G\|}{\|J\|}$	$\frac{\|G\|}{\|J\|}$	$\frac{\|G\|}{\|J\|}$	$\frac{\|G\|}{2(q-1)}$
$\mu_G(J)$	$\mu(\frac{e}{h})$	$-\mu(\frac{e}{h})$	$-\mu(\frac{e}{h})$	$-\mu(\frac{e}{h})$	$2\frac{(q-1)}{\|J\|}\mu(\frac{e}{h})$

Again $\forall h$ s.t. $h|e$ and $\frac{e}{h}$ odd :

	i)	ii)	iii)	iv)	v)
Type J	S_h	$M_{h,r(h)}$	${}^aD_{2r(h)}$	${}^aD_{2s(h)}$	$C_{r(h)}$
Exceptions	-	-	p=3,e odd,h=1	p=3 or 5, e odd, h=1	p=3 or 5, e odd, h=1
#J in G	$\frac{\|G\|}{2\|J\|}$	$\frac{\|G\|}{2\|J\|}$	$\frac{\|G\|}{2\|J\|}$	$\frac{\|G\|}{2\|J\|}$	$\frac{\|G\|}{2(q-1)}$
$\mu_G(J)$	$-\mu(\frac{e}{h})$	$\mu(\frac{e}{h})$	$\mu(\frac{e}{h})$	$\mu(\frac{e}{h})$	$-\frac{2(q-1)}{\|J\|}\mu(\frac{e}{h})$

Also G has two conjugacy classes of 4-groups ${}^aV_4$, ${}^bV_4$ of length $|G|/24$ and $|G|/8$ respectively:

$$\mu_G({}^aV_4) = \begin{cases} 3 & \text{if } e = 2^r,\ r \geq 0 \\ 3\mu(e) & \text{if } p = 5,\ e \text{ odd} \\ 0 & \text{otherwise} \end{cases}$$

$$\mu_G({}^bV_4) = \begin{cases} 1 & \text{if } e = 2^r,\ r \geq 0 \\ -\mu(e) & \text{if } p = 3,\ e \text{ odd} \\ 0 & \text{otherwise} \end{cases}$$

Next, G has two conjugacy classes of cyclic groups of order 2, ${}^aC_2$, ${}^bC_2$ which have length $q(q\pm1)/2$ and $q(q \mp 1)/2$ respectively (as $q \equiv \pm 1 \bmod 4$).

$$\mu_G({}^aC_2) = \begin{cases} -(q \mp 1) & \text{if } e = 2^r,\ r \geq 0 \\ (q+1)\mu(e) & \text{if } p = 3,\ e \text{ odd} \\ 0 & \text{otherwise} \end{cases}$$

$$\mu_G({}^bC_2) = \begin{cases} (q\pm 1)/2 & \text{if } e = 2^r,\ r \geqslant 0 \\ (q-1)\mu(e)/2 & \text{if } p = 3,\ e \text{ odd} \\ 0 & \text{otherwise} \end{cases}$$

Finally,

$$\mu_G(I) = \begin{cases} -|G|\,\mu(e)/2 & \text{if } p = 3,\ e \text{ odd} \\ -|G|\,\mu(e) & \text{if } p = 5,\ e \text{ odd} \\ 0 & \text{otherwise} \end{cases}$$

The Case e = 1, p ≡ ± 3 mod 8

Firstly $PGL_2(3)$, i.e. the case q = 3, is standard as before except for ${}^bV_4$, ${}^aC_2$, ${}^bC_2$ where the entries for 'e = 2^r, r ⩾ 0' and 'p = 3, e odd' must be summed. In fact

$$PGL_2(3) \cong S^4$$

and is dealt with explicitly in Hall ([7] §3.63).

For p > 3, though, this case is exceptional in that G : = $PGL_2(p)$ now has maximal subgroups of type S^4. We must therefore make compensations to the values of $\mu_G(K)$ as standard just for those subgroups K < G that lie in a S^4 <G. The subgroups involved are:

Type	Number in G	Number in each S^4	# supergps.S^4
S^4	|G|/24	1	-
A^4	|G|/24	1	1
D_8	|G|/8	3	1
${}^bD_6$	|G|/12	4	2
${}^aV_4$	|G|/24	1	1
${}^bV_4$	|G|/8	3	1

Type	Number in G	Number in each S^4	# supergps.S^4
C_4	$p(p\pm 1)/2$	3	$(p\mp 1)/4$
C_3	$p(p\pm 1)/2$ as $p \equiv \pm 1 \bmod 3$	4	$(p\mp 1)/3$ *
${}^aC_2$	$p(p\pm 1)/2$	3	$(p\mp 1)/4$
${}^bC_2$	$p(p\mp 1)/2$	6	$(p\mp 1)/2$
I	1	1	$\|G\|/24$

*In any number involving C_3's, $\pm$ and $\mp$ are read as $p \equiv \pm 1 \bmod 3$.

I now go through the types of subgroups as listed one by one; I stress that $\mu_G(K)$ is as standard for all subgroups K of G not mentioned. The case p = 5 gives special results: a pair of numbers (n; m) means n for p = 5, m otherwise.

Type	'Standard' μ_G value	Compensation for supergroups ...	Total value of compensation	Actual μ_G value
S^4	0	-	-	-1
A^4	0	one S^4	+1	+1
D_8	-1; 0	one S^4	+1	0; 1
${}^bD_6$	0	two S^4	+2	2
${}^aV_4$	6; 3	one S^4, one A^4, three D_8	-3	3; 0
${}^bV_4$	1	one S^4, one D_8	0	1

Type	Standard μ_G value	Compensation for supergroups ...	Total value of compensation	Actual μ_G value
C_4	2; 0	$(p \mp 1)/4$ each of S^4, D_8	0	2; 0
C_3	0	$(p \mp 1)/3$ each of S^4, A^4		
		$(p \mp 1)/6$ ${}^bD_6$	$-(p \mp 1)/3$	$-(p \mp 1)/3$ as $p \equiv \pm 1 \bmod 3$
${}^aC_2$	$-(p \mp 1)$	$(p \mp 1)/4$ each of S^4, A^4, ${}^aV_4$		
		$3(p \mp 1)/4$ D_8	0	$-(p \mp 1)$
${}^bC_2$	$(p \pm 1)/2$	$(p \pm 1)/2$ of S^4, D_8, ${}^bD_6$	$-(p \pm 1)$	$-(p \pm 1)/2$
I	$-\|G\|$; 0	all of above!	$\|G\|/2$	$-\|G\|/2$; $\|G\|/2$

CHAPTER THREE

This chapter deals with the enumerations of maps and hypermaps. All (oriented or non-oriented) maps or hypermaps referred to are to be assumed regular, with automorphism group $G := PSL_2(q)$ or $PGL_2(q)$ for prime power $q = p^e$ in section 1, and with automorphism group $PSL_2(q)$ in section 2. Also I use the abbreviations:

ROM for regular oriented map

ROΔM for regular oriented triangular map

In section 1 I consider the following categories: maps, triangular maps, hypermaps (for all three taking both the oriented and non-oriented case). The enumerations involved here are in the most part routine, using the methods explained in the preliminary chapter; in particular the results in chapter 2 are used in applying Möbius inversion.

In section 2 I develop an existing exposition [14] of which pairs of elements in G generate G so I can examine the number of regular oriented (a,b)-hypermaps with valency c, for any $(a,b,c) \in \mathbb{N}^3$. This will not involve Möbius inversion. I also deduce some identities between the results as we vary a, b and c.

1 ENUMERATION OF REGULAR HYPERMAPS $\cong$ $PSL_2(q)$ or $PGL_2(q)$

I immediately label six categories of oriented and non-oriented hypermaps as below. As explained in chapter 1, the regular members of each category correspond to the normal subgroups of the sponsor group Γ for that category:

Label of category	Objects in category	Γ
$\mathcal{M}$	Maps	$V_4 * C_2$
$\mathcal{M}^+$	Oriented maps	$C_2 * C_\infty$
$\mathcal{M}_3$	Triangular maps	$PGL_2(\mathbb{Z})$
$\mathcal{M}^+_3$	Oriented triangular maps	$PSL_2(\mathbb{Z})$
$\mathcal{H}$	Hypermaps	$C_2 * C_2 * C_2$
$\mathcal{H}^+$	Oriented hypermaps	$C_\infty * C_\infty$

For each category I enumerate the regular objects with automorphism group G where G is

a) $PSL_2(p^e)$ for p odd prime, $e \geq 1$

b) $PSL_2(2^e)$ for $e \geq 1$

c) $PGL_2(p^e)$ for p odd prime, $e \geq 1$.

This in each case is equivalent to finding the number $d_\Gamma(G)$ of normal subgroups N of Γ such that $\Gamma/N \cong G$. This is done by applying Hall's method, using Möbius inversion on Γ-strings of G as explained in section 1.2. This is generally straightforward (except for triangular maps where $\Gamma \cong PGL_2(\mathbb{Z})$, when enumerating Γ-strings is not immediate), but tedious, especially if one holds in mind all the exceptional cases to the form of the Möbius function μ_G of G. I will go through the whole calculation in only a few instances, and will mostly just state results. As the category $\mathcal{M}_3$ is the most difficult in some respects, but the algebraic part is relatively not too long-winded, I will treat just this category in detail. The scheme I follow is to take each category in turn, and give for each a long result which covers all the groups a), b), c) above 'in one go'. However

before I start I 'process' the method of calculation for the groups (a) to slightly simplify matters.

Processing of method for case a). Let $G := PSL_2(p^e)$ for p odd prime, $e \geq 1$

We start with some notes (1) to 3)) relevant to all G except those with e = 1 or (e = 2 and $p \equiv \pm 2 \bmod 5$), i.e. all G whose μ_G function is given by the main result on p.58-60. I firstly anticipate the form of the expression for $d_\Gamma(G)$ given by Hall's method for each Γ:

$$d_\Gamma(G).|\mathrm{Aut}G| = \sum_{ev} r(p^f)\mu\left(\frac{e}{f}\right) + \sum_{odd} s(p^f)\mu\left(\frac{e}{f}\right) + k + \ell\mu(e)$$

where (and subsequently) $\sum_{ev}$ and $\sum_{odd}$ means summation over all f dividing e s.t. $\frac{e}{f}$ is even and odd respectively. Also, r and s are some polynomials over $\mathbb{Z}$. The $k \in \mathbb{N}$ is the compensation needed if e is a power of two, the $\ell \in \mathbb{N}$ that if (p = 3) or (p = 5, e odd). (See the statement of μ_G). These three notes are concerned with simplifying this form in a general way.

1) The 'even' summation is zero unless e is even: ~~for~~ suppose for the moment 2|e.

$$\text{Let } R := \{ f \in \mathbb{N} : f|e, \tfrac{e}{f} \text{ even and } \mu(\tfrac{e}{f}) \neq 0 \}$$

$$S := \{ f \in \mathbb{N} : f|e, \tfrac{e}{f} \text{ odd and } \mu(\tfrac{e}{f}) \neq 0 \} .$$

Then

$$R := \{ f \in \mathbb{N} : f|e, 2|\tfrac{e}{f} \text{ but } 2^2 \nmid \tfrac{e}{f}, \text{ and } \mu(\tfrac{e}{f}) \neq 0 \}$$

$$= \{ f \in \mathbb{N} : f = h/2 \text{ for some } h \in S \} .$$

By abuse of notation, I write r(f), s(f) instead of $r(p^f)$, $s(p^f)$ for any $f \in \mathbb{N}$. (Remember though that r(f) and s(f) mean something else when used as

subscripts of cyclic or dihedral groups, see p.39. However this should lead to no confusion.) Now if $f \in R$, then

$$r(f)\mu\left(\frac{e}{f}\right) = r(h/2)\,\mu\left(2\frac{e}{h}\right) \qquad \text{where } f = h/2$$

$$= -r(h/2)\mu\left(\frac{e}{h}\right) .$$

Thus $$\sum_{ev.} r(f)\mu\left(\frac{e}{f}\right) = \sum_{odd} -r(f/2)\mu\left(\frac{e}{f}\right) .$$

From now on e may be odd or even. Let $t : S \to \mathbb{Z}$ be defined by

$$t(f) = \begin{cases} s(f) & \text{if e is odd} \\ s(f) - r(f/2) & \text{if e is even} \end{cases}$$

then the form reduces to

$$d_{\Gamma}(G).|AutG| = \sum_{odd} t(f)\mu\left(\frac{e}{f}\right) + k + \ell\mu(e) .$$

2) $$k = \begin{cases} 0 & \text{if e is not a power of 2} \\ k' & \text{if } e = 2^{\alpha}, \text{ independent of the actual } \alpha \in \mathbb{Z}^{+} \end{cases}$$

Define the function $w : S \to \mathbb{Z}$ by

$$w(f) = t(f) + k' .$$

Then for all e (>1 remember),

$$\sum_{odd} t(f)\mu\left(\frac{e}{f}\right) + k = \sum_{odd} w(f)\mu\left(\frac{e}{f}\right)$$

since if e is not a power of 2, then k = 0 and

$$\sum_{odd} k'\mu\left(\frac{e}{f}\right) = 0$$

and if e is a power of 2, then

$$\sum_{\text{odd}} t(f)\,\mu(\tfrac{e}{f}) + k \;=\; t(e) + k'$$

$$= \; w(e)$$

$$= \; \sum_{\text{odd}} w(f)\,\mu(\tfrac{e}{f}) \quad .$$

So we now have

$$d_{\Gamma}(G).|\mathrm{Aut}G| \;=\; \sum_{\text{odd}} w(f)\,\mu(\tfrac{e}{f}) + \ell\mu(e) \quad .$$

3) In this I show the cases (p = 3) and (p = 5 and e odd) need <u>not</u> be regarded as exceptional. I first note a trivial consequence of Fermat's Little Theorem, that if z(x) is any finite polynomial over $\mathbb{Z}$, then for any $n \in \mathbb{Z}$

$z(n^{\alpha}) \equiv 0 \bmod \alpha$ for an infinite number of primes α

if and only if $z(n) = 0$.

Taking up the situation at the end of note 2, given the prime power p^e, we have the function w(f) on the set S of divisors f of e such that $\frac{e}{f}$ is odd. Now w(f) may be regarded as a polynomial expression in p^f if e is odd; in $p^{f/2}$ if e is even. This expression only has two forms (given p), depending only on the parity of e. I take the two cases separately.

<u>e odd:</u> let w(x) be the polynomial over $\mathbb{Z}$ corresponding to the expression of w(f) in p^f. I stress w is independent of e as long as e is odd.

I now let e be any odd prime α. Then

$$d_{\Gamma}(G).|\mathrm{Aut}G| = w(p^{\alpha}) - w(p) - \ell \quad .$$

Let $w(p) + \ell = c$.

Now it is well known [2] that $\mathrm{Aut}G \cong P\Gamma L_2(p^{\alpha})$ and so $|\mathrm{Aut}G| = \alpha p^{\alpha}(p^{2\alpha}-1)$.

This means $\alpha | (w(p^{\alpha}) - c)$ for every odd prime α

$\Rightarrow w(p) - c = 0$

$\Rightarrow \ell = 0$.

e even: let $w(x)$ be the polynomial over $\mathbb{Z}$ corresponding to the expression of $w(f)$ in $p^{f/2}$. Now w is independent of e as long as e is even.

Let $e = 2\alpha$ where α is an odd prime. Then $S = \{2\alpha, 2\}$.

We have

$$d_{\Gamma}(G).|AutG| = w(p^{2\alpha}) - w(p^2) + \ell \ .$$

Let $w(p^2) - \ell = c$.

As before, $w(p^{2\alpha}) - c \equiv 0 \bmod \alpha$ for every odd prime α

$\Rightarrow w(p^2) - c = 0$

$\Rightarrow \ell = 0$.

Conclusion: for all prime powers p^e except the two cases ($e = 1$) and ($e = 2$ and $p \equiv \pm 2 \bmod 5$), the final form of the answers will be

$$d_{\Gamma}(G).|AutG| = \sum_{odd} w(f)\, \mu(\tfrac{e}{f}) \ .$$

where $w(f)$ has one polynomial expression in p^f whenever e is odd, and has another polynomial expression in $p^{f/2}$ whenever e is even.

(A similar final form with a single polynomial expression in p^f for all $e > 1$ may be deduced for $d_{\Gamma}(G)$ when $G \cong PGL_2(q)$ for any q, but this is trivial given just the argument of note 3 here; i.e. the cases ($p = 3$, e odd) and ($p = 5$, e odd) need not be considered exceptional.)

□

Now I start to present the information (just for groups in category a)

still) needed to make the specific calculations. Remember that if, for given Γ, $\sigma_\Gamma(H)$ represents the number of Γ-strings of a group H, then

$$d_\Gamma(G).|\mathrm{Aut}G| = \sum_{H \leq G} \mu_G(H)\, \sigma_\Gamma(H)$$

$$= \sum_{\mathcal{L}} (\#\text{ subgps. of G in } \mathcal{L}\text{, with representative H}).\mu_G(H).\sigma_\Gamma(H)$$

where the latter summation is over classes $\mathcal{L}$ of subgroups of G under AutG. We keep the notion that a subgroup $H \leq G$ is contributing if $\mu_G(H) \neq 0$; we know that if H is contributing, all subgroups of G of type H forms a single class. Thus we have

$$d_\Gamma(G).|\mathrm{Aut}G| = \sum_{\text{type H}} \xi_G(H)\, \sigma_\Gamma(H)$$

where the summation is over types H of subgroups of G and

$$\xi_G(H) = (\#\text{subgroups of G of type H}).\ \mu_G(H)\ .$$

As a summary of the results in section 1 of chapter 2 and to incorporate Hall's results for μ_G when $G := PSL_2(p)$, i.e. e = 1, the table on page 94 gives values of $\xi_G(H)$, where H now denotes a class of subgroups. There will be three cases:

1) The standard case, as described in the preceding notes; the latter two of these suggest that whatever e we may take:

$$\mu_G(V_4) = -6$$

$$\mu_G(C_2) = (q-1)/2$$

$$\mu_G(I) = 0$$

2) Case e = 2, $p \equiv \pm 2 \bmod 5$, as described in section 1 of chapter 2.

3) Case $\underline{e = 1}$, where there are four 'sub-cases' as specified by Hall:

i) $p \equiv \pm 1 \bmod 5$ and $\pm 1 \bmod 8$

ii) $p \equiv \pm 1 \bmod 5$ and $\pm 3 \bmod 8$

iii) $p \equiv \pm 2 \bmod 5$ and $\pm 1 \bmod 8$

iv) $p \equiv \pm 2 \bmod 5$ and $\pm 3 \bmod 8$

(I will completely ignore $PSL_2(3)$ and $PSL_2(5)$ in the table as being 'trivial'. Their Möbius inversion formula are given explicitly in Hall.)

Values of $\xi_G(H)/|G|$

Subgp. Type H for $\frac{e}{f}$ odd	$\frac{e}{f}$ even	Standard Case	Case e=2, $p \equiv \pm 2 \bmod 5$	Case e=1 (i)	(ii)	(iii)	(iv)
S_f	G_f	$\frac{2}{p^f(p^{2f}-1)}\mu(\frac{e}{f})$	⟶				
$M_{f,r(f)}$	$M_{f,2r(f)}$	$\frac{-2}{p^f(p^f-1)}\mu(\frac{e}{f})$	⟶				
$D_{2r(f)}$	$D_{4r(f)}$	$\frac{-1}{(p^f-1)}\mu(\frac{e}{f})$	⟶				
$D_{2s(f)}$	$D_{4s(f)}$	$\frac{-1}{(p^f+1)}\mu(\frac{e}{f})$	⟶				
$C_{r(f)}$	$C_{2r(f)}$	$\frac{2}{(p^f-1)}\mu(\frac{e}{f})$	⟶				
V_4		-1/2	-1/2	0	1/4	0	1/4
C_2		1/2	-3/2	-5/2	-3/2	-1/2	1/2
I		0	2	2	1	0	-1
A^5		0	-1/30	-1/30	-1/30	0	0
S^4		0	0	-1/12	0	-1/12	0
A^4		0	1/6	1/6	1/12	0	-1/12
D_{10}		0	1/5	1/5	1/5	0	0
D_8		0	0	1/4	0	1/4	0
D_6		0	1/3	2/3	1/3	1/3	0
C_3		0	-2/3	-2/3	-1/3	0	1/3

The corresponding table for the cases $G := PGL_2(q)$, any prime power q, may similarly be drawn up, but all the information is adequately displayed in chapter 2. My 'processing' is now complete.

In theory all I need do now is to calculate $\sigma_\Gamma(H)$ for each sponsor group Γ and for relevant subgroup types $H \leq G$; then I may apply the Möbius inversion formula. This however often requires messy (if straightforward) algebraic manipulation; even the statement of σ_Γ is too unwieldly to write down except for our illustrative category $\mathcal{M}_3$. The whole of the next page is taken by the statement of the result for $\mathcal{M}_3$: this is then proved, and afterwards I state the results for the other five categories without proof. (The result for $\mathcal{M}_3$ extends the main theorem in a paper [22] which just identifies the prime powers q for which $PSL_2(q)$ is not a homomorphic image of $PGL_2(\mathbb{Z})$ at all.) Then to round this section off, there will be a few pages of notes on the results in general.

Some notation:

$\sum_f$ means summation over all divisors f of e

d(G) is an abbreviation for $d_\Gamma(G)$ when Γ is specified

so

d(G) = # regular objects in the current category with automorphism group G.

q is always an alternative symbol for the prime power p^e.

$\mathfrak{M}_3$

Table giving d(G) = # regular triangular maps with aut.group G

$G := PSL_2(p^e)$	$G := PGL_2(p^e)$
p = 2 $\frac{1}{e} \cdot \sum_{f} 2^f \mu(\frac{e}{f})$	
p = 3 $\begin{cases} 0 & \text{if } e=2 \text{ or is odd} \\ \frac{1}{2e}\sum_{odd}(3^{f/2}-1)^2\mu(\frac{e}{f}) & e>2 \text{ even} \end{cases}$	$\begin{cases} \frac{1}{e}\sum_{odd}(3^f-1)\mu(\frac{e}{f}) & \text{if e odd} \\ \frac{1}{2e}\sum_{odd}(3^f-1)\mu(\frac{e}{f}) & \text{e even} \end{cases}$
p > 3, e = 1 1 for $p^e = 5$, else $(p-a)/4 - b$ where a=5;3;1;-1 as p≡1;-1;5;-5 mod 12 b=4;2;2;0 as p in sub-case i)-iv)	$(3p-c)/4$ where c=3;5;7;9;11;13;15;17 as p≡1;-1;-7;7;-11;11;5;-5 mod 24
p > 3, e > 1 e odd: $\frac{1}{4e}\sum_{f} p^f \mu(\frac{e}{f})$ e even: $\frac{1}{4e}\sum_{odd}(p^{f/2}-1)(p^{f/2}-3)\mu(\frac{e}{f})$ except subtract 1 if e=2, p≡±2 mod 5	All e: $\frac{3}{4e}\sum_{odd}(p^f-1)\mu(\frac{e}{f})$

Proof

The sponsor group Γ is

$$PGL_2(\mathbb{Z}) := gp\ \langle U,V,W : U^2 = V^2 = W^2 = (UV)^2 = (VW)^3 = I \rangle \ .$$

Then, adapting the strict definition slightly, a (Γ -)string of a group H is a triple (u,v,w) of elements in H such that

$$o(u) = o(v) = o(w) = o(uv) = 2\ ,\ o(vw) = 3$$

and we define $\sigma(H)$ to be the number of strings in H. (We may insist on orders rather than relations because if (u,v,w) is a generating (Γ)-string with the strict meaning in any of the G we consider except $PSL_2(2) \cong D_6$, then none of $\{ u,v,w,uv,vw \}$ can be the identity in G.)

We have

$$|AutG|.d(G) = \sum_{H \leq G} \mu_G(H)\sigma(H)$$

where $|AutG| = \begin{cases} e|G| & \text{as } G \cong \begin{cases} PGL_2(q) & \text{any } q \\ PSL_2(q) & \text{any odd } q \end{cases} \\ 2e|G| \end{cases}$

So we are crucially concerned with calculating $\sigma(H)$ for all contributing groups $H \leq G$. However I give a general method for determining $\sigma(K)$, K <u>any</u> finite group:

Given an involution v in K, then another involution w in K satisfies o(vw) = 3 if and only if $\langle v,w \rangle \cong D_6 \leq K$. Let there be n subgroups D_6 of K containing v. Each of these D_6 'supply' two involutions w: also two distinct such D_6 cannot share the same w, as v and w determine the D_6. Thus there are exactly 2n involutions w for our particular v. By a similar argument, if m is the number of subgroups V_4 of K containing v, the number of involutions u in K such that o(uv) = 2 will be 2m. Clearly the values of

n and m for the original involution v is invariant over the orbit of v under Aut(K), so

$$\sigma(K) = 4\sum_{\ell} |\ell|\ n(\ell)m(\ell)$$

where the summation is over all the orbits ℓ of involutions in K under Aut(K) and $n(\ell)$, $m(\ell)$ are the values of n, m for a representative $v \in \ell$.

Specialising again to subgroups H of G, we know in particular that if H is some S_f or G_f, then H has one or two oribits ℓ of involutions as above, and we know the values of $n(\ell)$ and $m(\ell)$ straightaway in most cases by our analysis of supergroups in chapter 2 (else we may make fresh use of the supergroup lemma p.37).

I now take the different cases separately:

<u>p = 2</u>

For e = 1, the number of generating triples (u,v,w) in $G \cong D_6$ satisfying the relations of Γ is 12, implying d(G) = 2.

For e > 1, consider $\sigma(S_f)$. S_f has one orbit ℓ of involutions v of length $(2^{2f}-1)$ with $n(\ell) = 2^{f-1}$. The normalizer in S_f of each v is an elementary abelian group of order 2^f: I conclude $m(\ell) = (2^f-2)/2$.

Thus

$$\sigma(S_f) = 2(2^{2f}-1)2^{f-1}(2^f-2) = |S_f|(2^f-2)$$

Also trivially, as none of these subgroups contain a V_4,

$$\sigma(M_{f,2r(f)}) = \sigma(D_{4r(f)}) = \sigma(D_{4s(f)}) = \sigma(C_{2r(f)}) = 0$$

so

$$e|G|\ d(G) = \sum_{f} \frac{|G|}{|S_f|}\ |S_f|\ (2^f-2)\mu(\tfrac{e}{f})$$

$$\Rightarrow \quad d(G) = \frac{1}{e} \sum_{f} 2^f \mu\left(\frac{e}{f}\right)$$

which accommodates the case e = 1.

p = 3

This time we have both $\sigma(S_f)$ and $\sigma(G_f)$ to calculate.

First $\sigma(S_f)$: if f is odd, S_f contains no D_6 and immediately $\sigma(S_f) = 0$. Suppose f is even. Then $3^f \equiv 1 \bmod 4$, and S_f contains $3^f(3^f+1)/2$ involutions v. The only D_6 in S_f are contained in the $M_{f,r(f)} < S_f$; considering S_f as a subgroup of index 2 in G_f, then these D_6 are their own normaliser and form a single conjugacy class under G_f. By the supergroup lemma (p. 37), we now find that fixed v is contained in (3^f-1) D_6, supplying $2(3^f-1)$ involutions w; also we know (p.56) v is contained in $(3^f-1)/4$ subgroups V_4, supplying $(3^f-1)/2$ involutions u. Thus

$$\sigma(S_f) = 3^f(3^{2f}-1)(3^f-1)/2 \quad = \quad |S_f|\,(3^f-1) \ .$$

Now $\sigma(G_f)$: G_f has two orbits ℓ and ℓ' of involutions v, for ℓ they all lie in $S_f < G_f$, for ℓ' they all lie in $G_f \setminus S_f$. As f is $\{ \begin{smallmatrix} \text{even} \\ \text{odd} \end{smallmatrix} \}$ we have

$$|\ell| = 3^f(3^f \pm 1)/2 \qquad n(\ell) = \begin{cases} (3^f-1) \\ 0 \end{cases} \qquad m(\ell) = (3^f \mp 1)/2$$

$$|\ell'| = 3^f(3^f \mp 1)/2 \qquad n(\ell') = \begin{cases} 0 \\ (3^f-1) \end{cases} \qquad m(\ell') = (3^f \pm 1)/2$$

and I conclude for all e:

$$\sigma(G_f) = 3^f(3^{2f}-1)(3^f-1) = |G_f|\,(3^f-1) \ .$$

All other contributing subgroups of G (whether $G \cong PSL_2(3^e)$ for some $e > 2$ or $PGL_2(3^e)$ for some e) clearly do not contain both a V_4 and a D_6, so their σ value is zero.

We are ready to apply Möbius inversion.

For $G := PSL_2(3^e)$, e odd, σ is zero on all subgroups and immediately $d(G) = 0$. For $e > 2$ even however (refer to p.94):

$$2e.d(G) = \frac{1}{|G|}\left(\sum_{\text{even}} \xi_G(G_f)\,\sigma_\Gamma(G_f) + \sum_{\text{odd}} \xi_G(S_f)\,\sigma_\Gamma(S_f) \right)$$

$$= 2\sum_{\text{even}} (3^f-1)\mu\left(\frac{e}{f}\right) + \sum_{\text{odd}} (3^f-1)\mu\left(\frac{e}{f}\right)$$

$$= \sum_{\text{odd}} (3^f-2.3^{f/2}+1)\mu\left(\frac{e}{f}\right)$$

The case $e = 2$ is as above except it needs compensation for the subgroups of the maximal subgroups type A^5 in G; as of all the subgroups of A^5 only A^5 itself has non-zero σ value, this being

$$\sigma(A^5) = 120$$

we must add $\xi_G(A^5) \cdot \sigma(A^5) = -4$ to the right hand side which then becomes zero, so $d(G) = 0$.

For $G := PGL_2(3^e)$, e odd, only the subgroups of type G_f for $f|e$ come into the calculation which is then more or less immediate. For e even, both the G_f and the S_f for $\frac{e}{f}$ odd 'contribute':

$$e.d(G) = \frac{1}{|G|}\sum_{\text{odd}} \left(\frac{|G|}{|G_f|}.|G_f|\,(3^f-1) - \frac{|G|}{|G_f|}.|S_f|\,(3^f-1) \right) \mu\left(\frac{e}{f}\right)$$

Calculation of σ for relevant group types for $G := PSL_2(p^e)$ or $PGL_2(p^e)$ with $p > 3$

Note (for our tacit application of the supergroup lemma to calculate values of n) that the set of all D_6 in $H := G_f$ or S_f forms a single class under Aut H of length $|G_f|/12$.

Now S_f has one orbit ℓ of involutions v:

$$|\ell| = p^f(p^f \pm 1)/2 \qquad n(\ell) = (p^f \mp 1)/2 \qquad m(\ell) = (p^f \mp 1)/4$$

and

$$\sigma(S_f) = |S_f|(p^f \mp 1)/2 \qquad \text{as } p^f \equiv \pm 1 \bmod 4$$

G_f has two orbits ℓ, ℓ' of involutions v:

$$|\ell| = p^f(p^f \pm 1)/2 \qquad n(\ell) = (p^f \mp 1)/2 \qquad m(\ell) = (p^f \mp 1)/2$$

$$|\ell'| = p^f(p^f \mp 1)/2 \qquad n(\ell') = (p^f \pm 1)/2 \qquad m(\ell') = (p^f \pm 1)/2$$

and

$$\sigma(G_f) = |G_f|\ (p^f \mp 1)/2 \ + |G_f|\ (p^f \pm 1)/2 \qquad \text{as } p^f \equiv \pm 1 \bmod 4$$

$$\Rightarrow \quad \sigma(G_f) = |G_f|\ p^f \qquad \text{(always)}.$$

Let $H := D_{2k}$ for some $k \in \mathbb{N}$. Then $\sigma(H) = 0$ unless both 2 and 3 divide k. If $6|k$, let

$$D_{2k} := gp\ \langle a,b : a^k = b^2 = (ab)^2 = I \rangle .$$

Then H has two orbits of involutions under $Aut(D_{2k})$:

$$\ell = \{a^{k/2}\}$$

$$\ell' = \{a^i b : i = 1,\ldots,k\}.$$

Now $a^{k/2}$ is in no $D_6 < D_{2k}$.

$\forall\ i \in \{1,\ldots,k\}$, $a^i b$ is in exactly one D_6 and exactly one $V_4 < D_{2k}$.

Thus $\sigma(D_{2k}) = 4k$

and we conclude

$$\sigma(D_{4r(f)}) = \begin{cases} 4(p^f-1), \\ 0 \end{cases} \quad \sigma(D_{4s(f)}) = \begin{cases} 0 \\ 4(p^f+1) \end{cases} \quad \text{as } p^f \equiv \begin{cases} 1 \bmod 3 \\ -1 \bmod 3 \end{cases}$$

$$\sigma(D_{2r(f)}) = \begin{cases} 2(p^f-1) \\ 0 \\ 0 \end{cases}, \quad \sigma(D_{2s(f)}) = \begin{cases} 0 \\ 2(p^f+1) \\ 0 \end{cases} \quad \text{as } p^f \equiv \begin{cases} 1 \bmod 12 \\ -1 \bmod 12 \\ \pm 5 \bmod 12 \end{cases}$$

Also

$$\sigma(A^5) = \sigma(PSL_2(5)) = 120 \qquad \sigma(S^4) = \sigma(PGL_2(3)) = 48$$

It is trivial to see that all remaining relevant group types H have $\sigma(H) = 0$: in particular the only dihedral subgroups that a $M_{f,r(f)}$ or $M_{f,2r(f)}$ can have are of type D_{2p}, so it contains neither a D_6 or a V_4.

We can now finish the proof of the results.

$G := PSL_2(p)$, p odd > 3

Inversion gives:

$$d(G) = \frac{1}{2|G|}\left(\sigma(S_1) - \sigma(D_{2r(1)})\frac{|G|}{(p-1)} - \sigma(D_{2s(1)})\frac{|G|}{(p+1)}\right) - b$$

where

$$-b = \frac{1}{2}\left(-\frac{\sigma(A^5)}{30} - \frac{\sigma(S^4)}{12}; -\frac{\sigma(A^5)}{30}; -\frac{\sigma(S^4)}{12}; 0\right)$$

as p in sub-case i) - iv).

Now $\sigma(S_1)$ depends on the value of p mod 4, $\sigma(D_{2r(1)})$, $\sigma(D_{2s(1)})$ on p mod 12. We obtain:

$$d(G) = \frac{1}{4}(p \mp 1) - \begin{cases} 1 \\ 0 \end{cases} - b$$

$\frac{1}{4}(p \mp 1)$: as $p \equiv \pm 1 \bmod 4$

$\begin{cases} 1 \\ 0 \end{cases}$: as $p \equiv \begin{cases} \pm 1 \bmod 12 \\ \pm 5 \bmod 12 \end{cases}$

$G = PSL_2(p^e)$, $p > 3$, $e > 1$

For e odd, analogously to the case e = 1 but now unconcerned with the compensation term b, we have

$$ed(G) = \sum_{f} \left(\frac{1}{4}(p^f \mp 1) - \begin{Bmatrix} 1 \\ 0 \end{Bmatrix} \right) \cdot \mu\left(\frac{e}{f}\right)$$

($\mp$: as $q \equiv \pm 1 \bmod 4$; $\begin{Bmatrix} 1 \\ 0 \end{Bmatrix}$: as $q \equiv \begin{cases} \pm 1 \bmod 12 \\ \pm 5 \bmod 12 \end{cases}$)

$$= \frac{1}{4} \sum_{f} p^f \mu\left(\frac{e}{f}\right)$$

For e even > 2, necessarily $q \equiv 1 \bmod 12$ and also $p^f \equiv 1 \bmod 12$ whenever $\frac{e}{f}$ odd. We have

$$2ed(G) = \sum_{even} \left(\frac{1}{|S_f|}\sigma(G_f) - \frac{1}{(p^f-1)}\sigma(D_{4r(f)}) - \frac{1}{(p^f+1)}\sigma(D_{4s(f)}) \right) \mu\left(\frac{e}{f}\right)$$

$$+2 \sum_{odd} \left(\frac{1}{4}(p^f-1) - 1 \right) \mu\left(\frac{e}{f}\right)$$

$$= \sum_{even} (2p^f - 4)\mu\left(\frac{e}{f}\right) + \frac{1}{2} \sum_{odd} (p^f - 5)\mu\left(\frac{e}{f}\right)$$

$$\Rightarrow ed(G) = \sum_{odd} \left(-(p^{f/2}-2) + \frac{1}{4}(p^f-5) \right) \mu\left(\frac{e}{f}\right)$$

$$= \frac{1}{4} \sum_{odd} (p^{f/2}-1)(p^{f/2}-3)\, \mu\left(\frac{e}{f}\right)$$

If e = 2, $p \equiv \pm 2 \bmod 5$ we must subtract 2 (as explained in corresponding instance (e = 2) for case p = 3) from the last expression; for e = 2, $p \equiv \pm 1 \bmod 5$ it is unaltered.

$\underline{G := PGL_2(p^e),\ p > 3}$

For $e > 1$,

$$ed(G) = \sum_{odd} \left(\frac{1}{|G_f|}\sigma(G_f) - \frac{1}{|G_f|}\sigma(S_f) - \frac{1}{2(p^f-1)}\sigma(D_{4r(f)}) - \frac{\sigma(D_{4s(f)})}{2(p^f+1)} + \frac{\sigma(D_{2r(f)})}{2(p^f-1)} + \frac{\sigma(D_{2s(f)})}{2(p^f+1)} \right) \mu\left(\frac{e}{f}\right)$$

$$= \sum_{odd} \left(p^f - \frac{1}{4}(p^f \mp 1) - 2 + \begin{Bmatrix} 1 \\ 0 \end{Bmatrix} \right) \mu\left(\frac{e}{f}\right)$$

$\uparrow$ as $q \equiv \pm 1 \bmod 4$; $\uparrow$ as $q \equiv \begin{cases} \pm 1 \bmod 12 \\ \pm 5 \bmod 12 \end{cases}$

$$= \frac{1}{4} \sum_{odd} (3p^f - d)\ \mu\left(\frac{e}{f}\right)$$

where $d = 3;5;7;9$ as $q \equiv 1;-1;5;-5 \bmod 12$

Now as $e > 1$, it does not matter what the actual value of e is, for the purposes of substituting for d an integer giving the right answer we may regard e as being a power of 2, i.e. e is even, $q \equiv 1 \bmod 12$ and $d = 3$. (cf. note 2 on p.89).

For $e = 1$, we must add a compensation $= -48/24 = -2$ for the maximal subgroups of G type S^4 when $p \equiv \pm 3 \bmod 8$. Thus solving congruences we have

$$d(G) = \frac{1}{4}(3p - c)$$

with c as in display of results.

□

$\mathfrak{M}^+_3$ ($\Gamma := C_2 * C_3$)

Table giving d(G) = #ROMs with automorphism group G

$G := PSL_2(p^e)$	$G := PGL_2(p^e)$
p = 2	
$\frac{1}{e}\sum_f (2^f-1)\ \mu(\frac{e}{f})$	
p > 2, e = 1	
1 for p = 3 or 5, else	1 for p = 3, else
(p-a)/2 - b	(p-c)/2
where	where
a = 3;1 as $p \equiv \pm 1;\pm 5 \bmod 12$	c = 1;3;3;5
b = 4;3;2;1 as p in sub-case i)-iv)	as $p \equiv \pm 1;\pm 7;\pm 11;\pm 5 \bmod 24$
p > 2, e > 1	
e odd:	All e:
$\frac{1}{2e}\sum_f p^f\ \mu(\frac{e}{f})$	$\frac{1}{2e}\sum_{odd} (p^f-1)\ \mu(\frac{e}{f})$
e even:	
$\frac{1}{2e}\sum_{odd} (p^{f/2}-1)^2\ \mu(\frac{e}{f})$	
except subtract 1 if ($e=2, p\equiv\pm 2 \bmod 5$)	

$\mathfrak{M}$ $(\Gamma := V_4 * C_2)$

Table giving d(G) = # regular maps with automorphism group G

$G := PSL_2(p^e)$	$G := PGL_2(p^e)$
p = 2 3 for e = 1, else $\frac{1}{e}\sum_{f}(2^f-1)(2^f-2)\,\mu(\frac{e}{f})$	
p > 2, e = 1 3 for p = 5, else $(p^2-ap+b)/8 - c/2$ where a=2;4 as p≡1;-1mod4 b=-3;-9 as p≡1;-1mod4 c=15;9;3;-3 as p in sub-case i)-iv)	3 for p = 3, else $(7p^2-dp+k)/8$ where d=22;20 as p≡1;-1mod4 k=-9;-3;15;21 as p≡-3;3;1;-1mod8
p > 2, e > 1 e odd: $\frac{1}{8e}\sum_{f}p^f(p^f-a)\;\mu(\frac{e}{f})$ e even: $\frac{1}{8e}\sum_{odd}(p^{2f}-10p^f+24p^{f/2}-15)\,\mu(\frac{e}{f})$ except subtract 3 if (e=2,p≡±2mod5 and p > 3)	All e: $\frac{1}{8e}\sum_{odd}(7p^{2f}-dp^f+15)\mu(\frac{e}{f})$ where d = 22;20 as q ≡ 1;-1mod4

$\underline{\mathfrak{M}}^{+}(\Gamma := C_2 * C_\infty)$

Table giving d(G) = # ROMs with automorphism group G

$G := PSL_2(p^e)$	$G := PGL_2(p^e)$
<u>p = 2</u> 2 for e = 1, else $\frac{1}{e}\sum_{f}(2^f-1)(2^f-2)\,\mu(\frac{e}{f})$	
<u>p > 2, e = 1</u> 1;3 for p = 3;5, else $(p^2-3p+a)/4 - b/2$ where a=0;-2 as p≡1;-1mod4 b=15;11;3;-1 as p in sub-case i)-iv)	2 for p = 3, else $(3p^2-9p+c)/4$ where c=6;8;-2;0 as p≡1;-1;-3;3mod8
<u>p > 2, e > 1</u> e odd: $\frac{1}{4e}\sum_{f}p^f(p^f-3)\;\mu(\frac{e}{f})$ e even: $\frac{1}{4e}\sum_{odd}(p^{2f}-7p^f+12p^{f/2}-6)\,\mu(\frac{e}{f})$ except subtract 3 if (e=2,p≡±2mod5, p >3).	All e: $\frac{3}{4e}\sum_{odd}(p^f-1)(p^f-2)\;\mu(\frac{e}{f})$

$\underline{\underline{h}}$ $(\Gamma := C_2 * C_2 * C_2)$

Table giving d(G) = # regular hypermaps with aut.gp. G

$G := PSL_2(p^e)$	$G := PGL_2(p^e)$
$\underline{p = 2}$ 7 for e = 1, else $\frac{1}{2e}\sum_{f} 2^f(2^{2f}-2^f-3)\,\mu(\frac{e}{f})$	
$\underline{p > 2,\ e = 1}$ 19 for p = 5, else $\frac{1}{8}\left(p^3+\begin{cases}2\\-4\end{cases}p^2+\begin{cases}-7\\1\end{cases}p-\begin{cases}8\\14\end{cases}\right)-\frac{c}{2}$ where c=97;71;21;-5 as p in sub-cases i)-iv)	13 for p = 3, else $\frac{1}{8}\left(7p^3-\begin{cases}10\\4\end{cases}p^2-\begin{cases}17\\25\end{cases}p+\begin{cases}20\\26\end{cases}\right)-a$ where a = 0;13 as $p\equiv\pm1;\pm3 \bmod 8$
$\underline{p > 2,\ e > 1}$ e odd: $\frac{1}{8e}\sum_{f} p^f\left(p^{2f}+\begin{cases}2\\-4\end{cases}p^f+\begin{cases}-7\\1\end{cases}\right)\mu(\frac{e}{f})$ e even: $\frac{1}{8e}\sum_{odd}(p^{3f}+2p^{2f}-8p^{3f/2}+p^f+24^{f/2}-20)\,\mu(\frac{e}{f})$ except subtract 19 if $e=2, p\equiv\pm2 \bmod 5, p > 3$	All e: $\frac{1}{8e}\sum_{odd}\left(7p^{3f}-\begin{cases}10\\4\end{cases}p^{2f}-\begin{cases}17\\25\end{cases}p^f+20\right)\mu(\frac{e}{f})$

Note: $\begin{cases}x\\y\end{cases}$ in this table means x for $q\equiv1 \bmod 4$, y for $q\equiv-1 \bmod 4$.

$\underline{\mathcal{H}}^+$ ($\Gamma := C_\infty * C_\infty$)

Table giving d(G) = # regular oriented hypermaps with aut. gp. G

$G := PSL_2(p^e)$	$G := PGL_2(p^e)$
p = 2 3 for e = 1, else $\frac{1}{2e}\sum_{f} 2^f(2^{2f}-2^f-3)\,\mu(\frac{e}{f})$	
p > 2, e = 1 4, 19 for p = 3,5 else $\frac{1}{4}(p+1)(p^2-2p-1) - a$ where a=49,40,11,2 as p in sub-cases i)-iv)	 9 for p = 3, else $\frac{3}{4}(p-1)(p^2-3) - b$ where b=0,9 as $p\equiv\pm1,\pm3 \bmod 8$
p > 2, e > 1 e odd: $\frac{1}{4e}\sum_{f}(p^f+1)(p^{2f}-2p^f-1)\,\mu(\frac{e}{f})$ e even: $\frac{1}{4e}\sum_{odd}(p^{3f}-p^{2f}-4p^{3f/2}+p^f+12p^{f/2}-9)\,\mu(\frac{e}{f})$ except subtract 19 if (e=2,$p\equiv\pm2 \bmod 5$,p > 3)	 All e: $\frac{3}{4e}\sum_{odd}(p^f-1)(p^{2f}-3)\,\mu(\frac{e}{f})$

Notes on the previous results

1. All the results for $G := PSL_2(2^e)$ with any e have already been published in [6]. Also Hall [7] explicitly gave the values of d(G) for $G := PSL_2(p)$, any prime p, for the categories $\mathfrak{M}_3^+$, $\mathfrak{H}$, $\mathfrak{H}^+$.

2. If, in the table covering any of the six categories concerning us, we add a left-hand entry to the corresponding right-hand entry, the sum tends to be of a neater form than that of its two 'components'. I will now be more specific, without being completely general. Suppose we are dealing with the category $\mathfrak{C}$, and that d(G) for $G := PSL_2(2^e)$ with $e > 1$ is given by the expression

$$\frac{1}{e} \sum_{f} w(2^f)\mu\left(\frac{e}{f}\right)$$

where w is a polynomial with integral coefficients.

Suppose also that e is odd, take any prime $p > 2$ and let

$$d(G) = \frac{1}{e} \sum_{f} r(p^f)\mu\left(\frac{e}{f}\right) \qquad \text{for } G := PSL_2(p^e)$$

and

$$d(G) = \frac{1}{e} \sum_{f} s(p^f)\mu\left(\frac{e}{f}\right) \qquad \text{for } G := PGL_2(p^e)$$

where r, s are polynomials with rational coefficients (which are independent of p and e as long as e is odd and p mod 4 is specified).

Then

$$r + s = w + k$$

where k is a rational constant (and may in fact be regarded as 0 for we are free to incorporate the term in any of w, r or s).

For example, for $\mathfrak{C} := \mathfrak{M}_3^+$, we have

i) for $q = 2^e$ with $e > 1$,

$$\#(\text{ROΔM's } \mathcal{M} \text{ with } \mathrm{Aut}(\mathcal{M}) \cong \mathrm{PSL}_2(2^e)) = \frac{1}{e}\sum_{f} 2^f \mu\left(\frac{e}{f}\right)$$

ii) for $q = p^e$, p an odd prime with $e > 1$ odd,

$$\#(\text{ROΔM's } \mathcal{M} \text{ with } \mathrm{Aut}(\mathcal{M}) \cong \mathrm{PSL}_2(q))$$

$$+\#(\text{ROΔM's } \mathcal{M} \text{ with } \mathrm{Aut}(\mathcal{M}) \cong \mathrm{PGL}_2(q)) = \frac{1}{e}\sum_{f} p^f \mu\left(\frac{e}{f}\right) .$$

These particular expressions i) and ii) will interest us in regard of irreducible polynomials as discussed in section 4 of chapter 4.

We can see that the general property is in fact more or less inherent in the form of the Möbius function for the groups involved, should we compare them. I make further observations about these summations in the next note.

3) I partition our categories into three pairs of <u>complementary</u> categories thus

$$\{\mathfrak{M}, \mathfrak{M}^+\} \quad , \quad \{\mathfrak{M}_3, \mathfrak{M}_3^+\} \quad , \quad \{\mathfrak{H}, \mathfrak{H}^+\} .$$

We may easily check from the preceding tables that for any prime power $q \geq 3$ and for any category $\mathfrak{C}$ of our six that

$$\#(\text{regular objects in } \mathfrak{C} \text{ with automorphism group } \mathrm{PSL}_2(q) \underline{\text{ or }} \mathrm{PGL}_2(q))$$
$$= \#(\text{regular objects in the complementary category of } \mathfrak{C} \text{ with automorphism group } \mathrm{PSL}_2(q) \text{ or } \mathrm{PGL}_2(q)) .$$

This of course is no accident: as soon as we translate the equality into strictly group theoretic terms, the result seems natural if not obviously

true. I illustrate with the complementary pair of categories $\mathfrak{M}_3$ and $\mathfrak{M}_3^+$. Fix $q > 3$ and let

$$S := \{ \text{subgroups } N \lhd PSL_2(\mathbb{Z}) \quad \text{s.t.} \quad PSL_2(\mathbb{Z})/N \cong PSL_2(q) \}$$

$$T := \{ \text{subgroups } M \lhd PSL_2(\mathbb{Z}) \quad \text{s.t.} \quad PSL_2(\mathbb{Z})/M \cong PGL_2(q) \}$$

$$U := \{ \text{subgroups } N' \lhd PGL_2(\mathbb{Z}) \quad \text{s.t.} \quad PGL_2(\mathbb{Z})/N' \cong PSL_2(q) \}$$

$$V := \{ \text{subgroups } M' \lhd PGL_2(\mathbb{Z}) \quad \text{s.t.} \quad PGL_2(\mathbb{Z})/M' \cong PGL_2(q) \} .$$

Then the equality reads

$$|S| + |T| = |U| + |V| .$$

I explain how we might deduce this directly.

Take an element N' of U. Then N' is the kernel of an epimorphism

$$\varphi' : PGL_2(\mathbb{Z}) \to PSL_2(q) .$$

Now $PSL_2(\mathbb{Z})$ is a subgroup of $PGL_2(\mathbb{Z})$ of index 2. I restrict φ' to a homomorphism

$$\varphi : PSL_2(\mathbb{Z}) \to PSL_2(q) ,$$

which in fact must be an epimorphism since $PSL_2(q)$ is simple. Let $N \in S$ be the kernel of φ. Then we have associated to each element N' of U an element N of S.

Now take an element M' of V, the kernel of the epimorphism

$$\rho' : PGL_2(\mathbb{Z}) \to PGL_2(q)$$

and restricting ρ' to $PSL_2(\mathbb{Z})$ we have the homomorphism

$$\rho : PSL_2(\mathbb{Z}) \to PGL_2(q) \qquad \text{with kernel K say}$$

whose image must necessarily be either $PGL_2(q)$ or $PSL_2(q) \leq PGL_2(q)$. We have thus associated to each element M' of V an element K of SuT.

Taken together, we have established a function f

$$f : U \cup V \to S \cup T$$

by restriction of epimorphisms. If f is a bijection, our desired equality is automatic; it is in this sense I say the result 'seems natural'. An exactly analogous situation holds for the other two pairs of complementary categories.

Just for the specific case $\{\mathcal{M}_3, \mathcal{M}_3^+\}$ I now go as far as proving that f is one-to-one. This proof also provides the basis for proving that f is also onto.

For fixed q, let $G := PSL_2(q)$, $G' := PGL_2(q)$ and regard $G \leq G'$ (equality only when q is a power of two).

Also let $\Gamma := PSL_2(\mathbb{Z})$, $\Gamma' := PGL_2(\mathbb{Z})$ be given by:

$$\Gamma := gp \langle X, Y : X^2 = Y^3 = I \rangle$$

$$\Gamma' := gp \langle U, V, W : U^2 = V^2 = W^2 = (UV)^2 = (VW)^3 = I \rangle$$

If $N \in S \cup T$, then N is the kernel of a homomorphism $\varphi : \Gamma \to G'$ given by

$$X \mapsto x \qquad Y \mapsto y$$

for some $x, y \in G'$ such that $\langle x,y \rangle \cong G$ or G'.

For the same x, y , consider the solutions (u, v, w) in G' to the system of equations:

$$uv = x, \quad vw = y, \quad o(u) = o(v) = o(w) = 2$$

and for any one of these solutions let N' be the kernel of the homomorphism φ': $\Gamma' \to G'$ given by

$$U \mapsto u \qquad V \mapsto v \qquad W \mapsto w \ .$$

Then clearly $N \lesssim N'$.

This means that if for each N in $(S \cup T)$ a solution (u, v, w) as above exists, then f is onto. If also this solution is in all cases where one exists is unique, then f is one-to-one.

So the problem of proving that f is a bijection reduces to showing that for each generating pair (x, y) in G, and then in G', for which x is an involution and y has order 3, there exists a unique triple of involutions (u, v, w) in G' such that

$$uv = x \quad \text{and} \quad vw = y \ .$$

So take any such pair (x, y) in G' generating either G or G'. Suppose firstly $p \geq 3$.

Let D_x, D_y be the maximal dihedral subgroups of G' that contain x and y respectively in their 'cyclic parts'. Then it is clear (because the 'cyclic parts' of D_x and D_y intersect trivially) that

$$D_x \cap D_y \cong V_4, C_2 \text{ or } I \ .$$

But in fact $D_x \cap D_y \ncong V_4$, else x is an element of D_y and so $\langle x,y \rangle$ cannot be G or G'.

(Note: the case p = 3 is slightly exceptional in that $D_y \cong D_6$, but this need not worry us.)

Suppose now $p = 2$.

Let D_x be the elementary abelian subgroup of G' of type V_q containing x

Let D_y be as before.

Again, just by consideration of the group types of D_x and D_y (remember that the 'cyclic part' of D_y now has no involution), we have

$$D_x \cap D_y \cong C_2 \text{ or } I .$$

Whatever the value of q, D_x and D_y have been constructed such that the involutions v of G' for which there is a solution (u, v, w) as desired are exactly the involutions in $D_x \cap D_y$. Note that v then determines u and w by

$$u = xv \quad , \qquad w = vy \quad .$$

So the number of solutions we have is always 1 or 0, depending on whether $D_x \cap D_y \cong C_2$ or I.

This immediately tells us that f is one-to-one, and to show that f is onto S u T, we need only prove in all cases

$$D_x \cap D_y \cong C_2 \quad .$$

This may be deduced directly from the action of G' on the set of marks (alternatively by judicious use of the supergroup tables of subgroups of G' found in chapter 2). However the details are fiddly; I'll leave them to the reader.

2. FURTHER ENUMERATION OF REGULAR HYPERMAPS $\mathcal{H}$ WITH AUT($\mathcal{H}$) $\cong$ $PSL_2(q)$

There are two major techniques that may be employed to understand the structure and properties of the groups $PSL_2(q)$.

The first is to examine $PSL_2(q)$ by its action on the 'set of marks', i.e.

$$GF(q) \cup \{\infty\}$$

(otherwise denoted by the projective line $PG_1(q)$). It is this technique I have hitherto almost exclusively used.

The second is to form arguments based on the trace of the elements of $G := PSL_2(q)$ when these elements are represented in the standard form of 2 x 2 matrices with entries in GF(q) and determinant 1. (Note though, as the matrices +I and -I are identified in G, that the trace of an element of G is defined only up to plus or minus a certain value in GF(q)). Trace as it happens gives a good description of the conjugacy classes in G (see later) and we can use the algebra of the field GF(q) to deduce many properties of the group.

For a comprehensive analysis of the subgroup lattice of G, we tend to use only the first technique because the action gives a faithful representation preserving <u>all</u> the structure, and this is why in chapter 2 the notion of trace does not occur at all. However it is once the structure is understood that trace is often the most powerful tool in examining further more particular properties. For example using largely the trace, Macbeath in a paper [14] gave a theorem effectively giving a way to calculate the number of torsion-free normal subgroups N of Γ such that $\Gamma/N \cong G$ where Γ is <u>any</u> triangle group (a, b, c); in other words, the number of

regular oriented (a, b)-hypermaps of valency c with automorphism group G (see p. 20). However no such enumerations are expressed explicitly (except for the single case (a, b, c) = (2, 3, 7), of special interest because of the relevance of the triangle group (2, 3, 7) in relation to Hurwitz groups, see p. 32 - 33). In this section I review the paper with the aim of obtaining actual numerical expressions (to compare with some of the results in the previous section). These however will not be quite general. (I shall also indicate later, see p. 129, why I no longer use Möbius inversion in this case.)

For clarity and economy of space, I shall in fact only consider $G := PSL_2(q)$ for q odd > 5; with a few adaptions, similar results may be derived for $PSL_2(q)$ for q even or indeed for $PGL_2(q)$ for q odd.

Firstly it is probably worthwhile just for insight to explain the exact connection between trace and the conjugacy classes of the elements of G. Let $GF(q^2)$ be the field extension of GF(q); let α be a primitive field element of $GF(q^2)$. Then (see Dickson)

$$G < G' := PSL_2(q^2)$$

and all the elements of G are conjugate in G' to an element of one of the following three subgroups of G':

i) $$C_{r(q)} := \left\{ \begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix} : \beta \text{ is a power of } \alpha^{q+1} \text{ in } GF(q^2) \right\}$$

The values of β of course range over $GF(q) < GF(q^2)$. The trace is $(\beta + \beta^{-1}) \in GF(q)$.

ii) $C_{s(q)} := \left\{ \begin{pmatrix} \gamma & 0 \\ 0 & \gamma^{-1} \end{pmatrix} : \gamma \text{ is a power of } \alpha^{q-1} \text{ in } GF(q^2) \right\}$.

The trace of these elements is $(\gamma + \gamma^{-1}) \in GF(q^2)$. As

$$(\gamma + \gamma^{-1})^q = \gamma^{-1} + \gamma$$

we conclude $(\gamma + \gamma^{-1}) \in GF(q)$. (By conjugacy this had to be the case.)

iii) $V_q := \left\{ \begin{pmatrix} 1 & \delta \\ 0 & 1 \end{pmatrix} : \delta \in GF(q) \right\}$

and the trace is ± 2.

Suppose $A \in C_{r(q)} \cup C_{s(q)}$: then the conjugacy class $\ell'(A)$ in G' containing A intersects with $C_{r(q)} \cup C_{s(q)}$ only in A and A^{-1}. Also $\ell'(A) \cap G$ forms a single conjugacy class in G: it is clear from the above that each conjugacy class in G obtained in this way (by varying A) must have a distinct trace. The number of these classes in G is straightforwardly calculated as

$$(q + 1)/2$$

and so each possible value of trace in GF(q) is taken by exactly one of the classes.

However there are two more conjugacy classes in G, the elements of which are the conjugates in G to the elements of $V_q \setminus \{I\}$. (We have already 'accounted for' I). Thus it is only for the value $k = \pm 2$ that we have more than one conjugacy class in G with elements with trace equal to k: in this exceptional case, we have $\{I\}$ and the two classes of elements of order p.

Now given G (i.e. given q) I define the set Ω of non-trivial orders of

elements in G:

$$\Omega := \{ d \in \mathbb{N} : (d = p \text{ or } d \mid (q+1)/2 \text{ or } d \mid (q-1)/2) \text{ and } d > 1 \}.$$

Also let φ denote the classical Eulerian function.

Then, if the function $\varphi' : \Omega \to \mathbb{N}$ is given by the number of values of trace taken by elements of order d in G for each $d \in \Omega$, we have

$$\varphi'(d) = \begin{cases} 1 & \text{if } d = 2 \text{ or } p \\ \varphi(d)/2 & \text{for all other } d \in \Omega \end{cases}$$

Now coming to Macbeath's work, his program is as follows: take all ordered triples (A, B, C) of elements of G such that ABC = I (let's call these the set of G-triples), and then analyse and categorise them so it is known what type of subgroup of G that each G-triple generates. In particular he identifies those G-triples generating the whole of G. The analysis of the G-triples (A, B, C) is done largely through considering two associated triples:

i) the trace-triple (α, β, γ) , where $\alpha = \text{tr } A$, etc.

ii) the order-triple (a, b, c) , where a is the order of A, etc.

(Strictly speaking Macbeath considers triples (A, B, C) of elements in $SL_2(q)$ rather than $PSL_2(q)$; this has the advantage that each element in $SL_2(q)$ has a uniquely defined trace in GF(q), and so the associated trace-triples are simpler to handle. However all his results are easily adapted to describe G-triples as I have defined them by using the natural projective homomorphism from $SL_2(q)$ to $PSL_2(q)$.)

The G-triples generating G are determined by an elimination process,

'discarding' the G-triples that generate some proper subgroup until this has been done for all the proper subgroups of G. This means we need to have a good idea of the form taken by the whole set of G-triples. The framework of the information is contained in the following crucial result in [14]:

i) For every triple $(\alpha, \beta, \gamma) \in (GF(q))^3$ there is a G-triple (A, B, C) which has (α, β, γ) as its trace-triple (where in the latter triple α is read as $\pm\alpha$, etc.).

Let Mat (α, β, γ) be the set of G-triples with trace-triple (α, β, γ). Then the totality of the G-triples in G is given by the union of Mat (α, β, γ) as α, β, γ range freely over the values of trace. We only need to know the conjugacy classes making up each Mat (α, β, γ) to complete our picture.

However we can afford now to specialise more to the G-generating G-triples. Clearly any conjugacy class under $PGL_2(q)$ of such G-triples must have length $|PGL_2(q)|$. I state a result again implicit in [14].

ii) a) Suppose $(\alpha, \beta, \gamma) \neq (\pm 2, \pm 2, \pm 2)$ is a trace-triple of some G-generating G-triple. Then the set of all G-triples (A, B, C) which have associated to them the same trace-triple (α, β, γ) constitutes two conjugacy classes under $PGL_2(q)$ (where we conjugate 'componentwise'), except if any of A, B and C has order 2 when it constitutes just one.

b) For $(\alpha, \beta, \gamma) = (\pm 2, \pm 2, \pm 2)$, associated G-triples may generate subgroups of G of type I, C_p, V_{p^2}; also exactly one conjugacy class of such G-triples have elements generating subgroups of type $PSL_2(p)$ (i.e. G itself if $e = 1$).

With this result known, we need only analyse which are the trace-triple values (α, β, γ) for which the elements of Mat (α, β, γ) do not generate G (in order to understand which G-triples are 'left' and so are G-generating). It is more or less these values (α, β, γ) that Macbeath determined; let me for the moment crudely lump these together as the set S (without for the moment identifying its elements).

I determine to go further by attempting to translate S into terms of order-triples. I explain now the motivation for this, first introducing some notation.

If a, b, c are all elements of Ω, I will denote by Mat(a, b, c) the set of all G-triples with associated order-triple (a, b, c). Also let n(a, b, c) be the number of elements of Mat (a, b, c) that generate G and $d'_{\Gamma}(G)$ be the number of torsion-free normal subgroups N of the triangular group Γ of type V (a, b, c) such that $\Gamma/N \cong G$. What concerns me is the identity

$$n(a, b, c) = |\mathrm{Aut}G| \cdot d'_{\Gamma}(G) \quad .$$

Remember that $|\mathrm{Aut}G| = |PGL_2(q)| \cdot e$ (where $q = p^e$).

Now for any (a, b, c) $\in \Omega^3$, the elements of Mat(a, b, c) have exactly

$$\varphi'(a)\,\varphi'(b)\,\varphi'(c)$$

distinct values of trace-triple.

Suppose exactly s of these values of trace-triple lie in S. Then the previous result (ii) gives

$$\frac{n(a, b, c)}{|PGL_2(q)|} = (1; 2) \cdot (\varphi'(a)\,\varphi'(b)\,\varphi'(c) - s)$$

(where $(1;\ 2)$ means 1 if any of a, b and c equal 2, and means 2 otherwise)

except if $(a, b, c) = (p, p, p)$ when

$$n(p, p, p) = \begin{cases} |PGL_2(q)| & \text{for } e = 1 \\ 0 & \text{for } e > 1 \end{cases}$$

Thus if we know the function $s : \Omega^3 \to \mathbb{N}$ given by

$$s(a, b, c) \mapsto |\ S \cap Tr(a, b, c)|$$

where Tr(a, b, c) is the set of trace-triples taken by elements of Mat (a, b, c), then we know n(a, b, c) for all $(a, b, c) \in \Omega^3$. (Note that s(p, p, p) does not concern us.)

So I endeavour to calculate s. I do this in sections i) - iv), each one dealing with a different category of order-triples. All information I use is to be found in [14].

i) An exceptional order-triple of G is an existing order-triple of G that is a re-arrangement of one of the following:

(2, 2, d) for any $d \in \Omega$

(2, 3, 3) , (3, 3, 3) , (3, 4, 4) , (2, 3, 4) , (2, 5, 5) ,

(5, 5, 5) , (3, 3, 5) , (3, 5, 5) , (2, 3, 5)

Assuming (from now on) that $q > 5$, then any G-triple with an exceptional order-triple (a, b, c) associated to it cannot be G-generating (any such G-triple will in general generate either a dihedral sub-group of G, or one isomorphic to A^4, S^4 or A^5). This is to say

$$s(a, b, c) = \varphi'(a)\,\varphi'(b)\,\varphi'(c)$$

and

$$n(a, b, c) = 0\ .$$

ii) A linear order-triple of G is a triple (a, b, c) $\varepsilon\ \Omega^3$ for which Mat (a, b, c) contains a G-triple with associated trace-triple (α, β, γ) satisfying one of

I) α, β, γ does not generate GF(q)

II) (this is only relevant if e is even). One of $\{\alpha, \beta, \gamma\}$ is contained in $GF(p^{e/2})$ and the two other components independently are either square roots in GF(q) of non-squares in $GF(p^{e/2})$ or are zero.

Every G-triple with a linear order-triple (a, b, c) must generate a subgroup of a proper linear subgroup of G, and so again

$$n(a, b, c) = 0 .$$

But I desire a description of the set of linear order-triples of G independent of trace. It is not hard to see that the following somewhat awkward construction gives exactly the same set.

Let $r : \Omega \to \mathbb{N}$ be given by:

$$r(p) := 1$$

$\forall a \in \Omega \setminus \{p\}$,

$r(a) :=$ the least divisor f of e such that $a \mid (p^f \pm 1)/2$

(Note : any element of G of order a has its trace lying in $GF(p^{r(a)}) \leq$ GF(q) and no smaller subfield.)

Then I define the rank R(a, b, c) of an order-triple (a, b, c) in G as the least common multiple of { r(a), r(b), r(c) } . Thus R(a, b, c) divides e.

I assert the set of linear order-triples of G is given by those (a, b, c) $\epsilon\ \Omega^3$ such that one (or both) of

I) R(a, b, c) is strictly less than e

II) e is even, all three elements of { a, b, c} are independently either p or divide $(p^{e/2}\pm 1)$.

iii) An affine order-triple of G is a triple (a, b, c) $\epsilon\ \Omega^3$ such that Mat(a, b, c) contains a G-triple (A, B, C) for which

$< A, B >$ is commutative .

Suppose (a, b, c) is an affine order-triple that is not also a linear order-triple. Then Tr(a, b, c) intersects S only in the following subset S' of S:

S' : = {trace-triples (α, β, γ) in G : Mat(α, β, γ) contains a G-triple (A, B, C) s.t. $<A, B>$ is commutative } .

(Given $(\alpha, \beta, \gamma) \epsilon$ S', all the elements of Mat(α, β, γ) generate subgroups of G that fix a mark in the action of G on GF(q) $\cup$ $\{\infty\}$.)

Then by definition

$$s(a, b, c) = |\ S \cap Tr(a, b, c)| = |S' \cap Tr(a, b, c)| \geq 1 \ .$$

So we need both to identify in a more numerical way which (a, b, c) $\epsilon\ \Omega^3$ are affine, and then to calculate s(a, b, c) as above.

We do this by considering the different types of maximal commutative subgroups M of G, in particular we consider which order-triples (a, b, c) have solutions (A, B, C) in M to

$o(A) = a, \quad o(B) = b, \quad o(C) = c, \quad ABC = I$

and then the number of such solutions for given (a, b, c). For $M \cong C_{r(q)}$ or $C_{s(q)}$, each of these solutions (A, B, C) (together with its allied solution (A^{-1}, B^{-1}, C^{-1})) corresponds to an element of S'.

I) $M := V_q$

Triples of elements in V_q all have order-triples of one of the following values (or rearrangements):

$(1, 1, 1)$, $(p, p, 1)$, (p, p, p)

Trivially,

$n(1, 1, 1) = n(p, p, 1) = 0$.

(In fact if $1 \in \{a, b, c\}$, all Mat(a, b, c) would be cyclic and immediately $n(a, b, c) = 0$. This is why we could afford to omit 1 (the 'trivial order') in the definition of Ω and tacitly ignore G-triples containing I).

Finally, we already know $n(p, p, p)$.

II) $M := C_{r(q)}$ or $C_{s(q)}$

Consider M as C_m, a cyclic group of order m. Suppose C_m is generated by X. Let a and b divide m.

Then the set E of elements in C_m that are the product of an element of order a and one of order b in C_m is given by

$$E := \{X^w : w = k_1 m/a + k_2 m/b \text{ for some } k_1, k_2 \text{ coprime to } a, b \text{ respectively}\} .$$

We want to examine the orders of elements in E. If we fix $w = k_1 m/a + k_2 m/b$, then it is clear

$$o(X^w) = \frac{ab}{h.c.f.(ab,\ k_1 b + k_2 a)} \quad .$$

Consider more specifically now the affine order-triples with fixed first two components a, b ε Ω , which necessarily must both divide r(q) : = (q-1)/2 or both divide s(q) : = (q+1)/2. These order-triples are exactly the set:

$$\{ (a, b, c) : \text{the set E as defined above for appropriate } C_m \text{ contains an element of order c} \}$$

and for each of them

$$s(a, b, c) = \frac{1}{2} . \#(\text{elements in E of order c}) \ .$$

I shall be more explicit only in two restricted cases (and this is why I earlier said my results were not quite general).

The first case is when <u>a and b are coprime.</u> Then it is simply shown that

$$|E| = \varphi(a)\,\varphi(b) = \varphi(ab)$$

and that every element of E has order ab. So we have:

$$(a, b, c) \ \varepsilon \ \Omega^3 \text{ is an affine order-triple in G} \Leftrightarrow c = ab$$

and

$$s(a, b, ab) = \varphi(ab)/2 = \varphi'(ab)$$

from which we calculate

$$\frac{n(a, b, ab)}{|PGL_2(q)|} = \varphi'(ab)[(1;2).(\varphi'(a)\,\varphi'(b)) - 1]$$

$$= \frac{\varphi(ab)}{2}\left[\frac{\varphi(ab)}{2} - 1\right]$$

I give an example, for a = 2, b = 3 : if the triple (2, 3, 6) is an existing order-triple in G (i.e. if $6 \in \Omega$, or alternatively if 2 and 3 both divide r(q) or both divide s(q)) then

$$n(2, 3, 6) = 0 \quad .$$

This may be interpreted that there can never be a ROΔM of valency 6 with automorphism group G.

The second case is when a = 2 (so I get a complete result for maps if not for hypermaps). The case b odd is covered above, so suppose b is even > 2 (remember (2, 2, c) for any c is exceptional).

$$|E| = \varphi(b)$$

and every element of E has order b if $b \equiv 0 \bmod 4$

has order b/2 if $b \equiv 2 \bmod 4$.

Correspondingly define

$$c_b := \begin{cases} b & \text{if } b \equiv 0 \bmod 4 \\ b/2 & \text{if } b \equiv 2 \bmod 4 \end{cases}$$

Then

$$s(2, b, c_b) = \varphi(b)/2$$

giving (with a little work):

$$\frac{n(2, b, c_b)}{|PGL_2(q)|} = \frac{\varphi(b)}{2}\left[\frac{\varphi(b)}{2} - 1\right]$$

Finally, I should perhaps emphasise that all the relationships I have given for n(a, b, c) for an affine order-triple (a, b, c) are valid only if the same order-triple (a, b, c) is neither exceptional or linear as well.

iv) A G-generating order-triple of G is a triple (a, b, c) $\in \Omega^3$ for which every element of Mat(a, b, c) generates G. The set of these are exactly the triples (a, b, c) $\in \Omega^3$ that are not exceptional, linear, affine or equal to (p, p, p).

By definition

$$s(a, b, c) = 0$$

and

$$\frac{n(a, b, c)}{|PGL_2(q)|} = (1;2).(\varphi'(a)\,\varphi'(b)\,\varphi'(c))$$

$$= \frac{\varphi(a)\varphi(b)\varphi(c)}{4}$$

where φ is the Eulerian function except we from now regard $\varphi(p) = 2$.

I have now completed my examination of the functions s and n on the order-triples of $G := PSL_2(q)$, for a given odd prime power $q = p^e > 5$. Thus for every (a, b, c) $\in \Omega^3$ I have an expression d'(a, b, c) for the number of torsion-free normal subgroups N of the triangular group Γ of type (a, b, c) such that $\Gamma/N \cong G$:

$$d'(a, b, c) = \frac{1}{e} \cdot \frac{n(a, b, c)}{|PGL_2(q)|}$$

(I extend d' to be a function $d' : \mathbb{N}^3 \to \mathbb{N}$ by defining d'(a, b, c) = 0 whenever (a, b, c) $\notin \Omega^3$.)

We know that d'(a, b, c) also represents the number of regular oriented (a, b)-hypermaps of valency c with automorphism group G.

We have obtained entirely explicit expressions for n(a, b, c) only when a and b are coprime or when a = 2 (though it should not be difficult

to extend my analysis of affine order-triples to be quite general). To give a partial résumé, I now state the values of d'(2, b, c) for all pairs (b,c) in Ω^2, in other words I enumerate all ROMs that have b-gonal faces and valency equal to c and have automorphism group isomorphic to G.

Supose (2, b, c) $\in \Omega^3$ is not an exceptional, linear or affine order-triple, then

$$d'(2, b, c) = \frac{1}{4e}\varphi(b)\varphi(c) \qquad \text{(where } \varphi(p) = 2\text{)}.$$

Suppose (2, b, c) = (2, b, 2b) $\in \Omega^3$ for b odd or (2, b, b) $\in \Omega^3$ for b $\equiv 0 \bmod 4$ or (2, b, b/2) $\in \Omega^3$ for b $\equiv 2 \bmod 4$ and $b>2$. If this triple is non-linear (i.e. $b \mid (q\pm1)/2$ but b does not divide $(p^f \pm 1)$ for any proper divisor f of e) then

$$d'(2, b, c) = \frac{\varphi(b)}{4e}[\varphi(b) - 2] .$$

For all other (2, b, c) $\in \Omega^3$,

$$d'(2, b, c) = 0 .$$

I end with some notes.

1) The reader may wonder at my abandonment of the use of Möbius inversion in this section. This is not simply because I believe that he or she will be glad for a rest from the technique by now! The serious reason is that the inversion involved (if we tackled the problem of finding the number of G-generating G-triples with a given order triple-order (a, b, c) by the standard Hall type method) would make the calculation unnecessarily long and clumsy. This is because for most (a, b, c) $\in \Omega^3$, all the elements of Mat(a, b, c) are readily identified either as generating

a subgroup in G lying in a specified class of proper subgroups of G or as generating G itself. This really makes the inversion approach redundant.

2) I refer back to my discussion of affine order-triples (a, b, c) for which a G-triple of Mat(a, b, c) lies in a subgroup of type $C_{r(q)}$ or $C_{s(q)}$ in G.

There, for fixed (a, b) ϵ $(\mathbb{Z}^+)^2$, and for any positive integer m that is a multiple of both a and b, I defined the set E (as a subset of the cyclic group C_m). Well it is clear that both $|E|$ and the number of elements in E of any particular order in C_m have values independent of m (conditional to a|m and b|m).

This means that if for a certain G we have an affine order-triple with first two components equal to (a, b) ϵ $(\mathbb{Z}^+)^2$, then the following are determined entirely by a and b (and no further by G):

I) the set of integers c such that (a, b, c) is an affine order-triple in G.

II) the values of s(a, b, c), and hence the values of e.d'(a, b, c) for the triples in I)

This leads me to the following

Proposition

Fix a triple (a, b, c) of positive integers, and suppose i is the number of distinct odd primes that occur in {a, b, c} (so i = 0, 1, 2 or 3).

Then the number n of different non-zero values that e.d'(a, b, c) takes as we vary $G := PSL_2(q)$ (i.e. vary q over all odd prime powers greater than 5) satisfies

$$n \leq 1 + i \ .$$

Proof

We now know that if (a, b, c) is an affine (non-linear) order-triple in a certain $PSL_2(q')$, then for all $PSL_2(q)$ for which (a, b, c) is also an existing order-triple it will be affine again and will have the same value for e.d'(a, b, c) (or this value could possibly become zero). So in this case n = 1 or 0.

If (a, b, c) is not an affine order-triple in any of the $PSL_2(q)$, then the only non-zero values that d'(a, b, c) can take are given by the expression

$$\frac{\varphi(a)\varphi(b)\varphi(c)}{4e}$$

where φ represents the classical Eulerian function except for any single odd prime p we might chose (strictly speaking, p varies according to q), which we take as $\varphi(p) = 2$. This gives us a maximum of (1 + i) values for e.d'(a, b, c). □

3) Let us fix G (for all this note).

If we take the sum d' for any fixed $(a, b) \in (\mathbb{Z}^+)^2$ as follows:

$$d'(a, b) = \sum_{c \in \mathbb{N}} d'(a, b, c)$$

then d' represents the number of regular oriented (a, b)-hypermaps with automorphism group G. (I have already determined d'(2, 3) explicitly in the previous section, but not d'(a, b) for any other pairs (a, b)).

This summation is messy to actually write down and refine. However, as suggested in the preceding note, the forms of expression for d'(a, b, c) are very limited: this means we can often find useful relations between the values of d' for varying (a, b, c). For example if (a, b, c) and (a, b', c) are both G-generating order-triples in G, then

$$d'(a, b, c) = \frac{\varphi(b)}{\varphi(b')} d'(a, b', c) \quad .$$

Making use of these, we may establish some neat relationships between the different d'(a, b). I concentrate again only on maps, i.e. a = 2, and to give an example show that if $G := PSL_2(p^e)$ for an odd prime p with $e > 2$ then

$$d'(2, 3) = d'(2, p) \quad .$$

I do this by demonstrating that $\forall c \in \mathbb{N}$,

$$d'(2, 3, c) = d'(2, p, c) \quad .$$

Proof

The results are truisms if p = 3, so suppose p > 3 .

Now

(2, 3, c) is exceptional $\iff$ c = 2, 3, 4 or 5

$\implies$ (2, p, c) is linear

(this implication has been manufactured by imposing the condition e > 2).

(2, p, c) is exceptional $\implies$ c = 2, 3, 4 or 5

$\implies$ (2, 3, c) is exceptional

(2, 3, c) is linear $\iff$ (2, p, c) is linear

(2, 3, c) is affine $\implies$ c = 6 and d'(2, 3, 6) = 0

Necessarily (2, p, 6) is linear.

Finally no (2, p, c) can be affine.

The above identifications tell us that

$$d'(2, 3, c) = 0 \quad \text{iff } d'(2, p, c) = 0$$

and that if $d'(2, 3, c) \neq 0$, then both (2, 3, c) and (2, p, c) are G-generating and so

$$d'(2, 3, c) = \frac{1}{2e}\varphi(c) = d'(2, p, c) .$$

Exactly the same sort of arguments give extensions to this result. I will present one such extension now without proof. Remember that for an element $b \neq p$ of Ω that

$$r(b) = \text{the least}^{\text{divisor}} f \text{ of } e \text{ such that } b \mid (p^f \pm 1)/2$$

Theorem

Let $e > 1$ and the prime decomposition of e be

$$e = p_1^{s_1} \cdots p_k^{s_k} .$$

If $b \in \Omega \setminus \{p\}$ has

$$r(b) = p_1^{t_1} \cdots p_k^{t_k} \qquad \text{with } t_i < s_i \quad \forall i = 1, \ldots, k$$

then

$$d'(2, b) = \frac{\varphi(b)}{2} d'(2, p)$$

(with the further condition $e > 2$ needed if $b = 4$ or 5). □

Generalising further (i.e. letting some of the $t_i = s_i$ in the statement of the theorem) is not difficult but the form of the relationships become more involved, so I call a halt here. Note that we can now use our explicit values we have for d'(2,3) to obtain explicit values for d'(2, p) and then for d'(2, b) (for those b covered in the theorem).

CHAPTER FOUR

1. INTRODUCTION (Problems of cycling round a regular map)

The term 'map' obviously (to my mind anyway!) is motivated by thinking of the map as a system of roads (edges) and roundabouts (vertices) on the surface of a planet (with genus ≥ 0). I suppose the map $\mathcal{M}$ (and hence the planet) is oriented. Just for this section, I press the analogy further and suppose B is a bicyclist (ecologist and mathematician) who sets out from home which is situated at the end of a road (the dart α say). B is given a string of directions W for his journey

$$W(x, z) = z^{i_s} x z^{i_{s-1}} x \ldots x z^{i_2} x z^{i_1} \qquad \text{where } s \in \mathbb{N},\ i_1, \ldots, i_s \in \mathbb{Z}$$

where z^{i_1} is the first direction which says 'take the i_1th turning going clockwise round the roundabout you are currently at' (if i_1 is negative, that is to be interpreted to take the $|i_1|$th turning going anti-clockwise). The direction x simply says 'travel to the next roundabout on the road you are on'. What concerns B is will he end up back home again after completing his journey? Or, put the other way, he would like to know which strings of directions W will describe circuits from α; and he wants to know this before setting out!

Now not to make it too chaotic for B, we suppose the map $\mathcal{M}$ is regular. (This makes the 'starting' dart α non-critical). But despite the symmetry, things are still not easy for B. Even if B is given the automorphism type G of $\mathcal{M}$, B cannot determine the circuits because in general there are many regular maps with the same automorphism type. B needs to know a standard presentation (G, Ω, x, y) for $\mathcal{M}$. Letting $z := y^{-1}x$, W is a circuit if and only if $W(x, z) = I$ in G. If B knows the set of circuits for $\mathcal{M}$, then B knows the whole relator set for a 2-generator presentation

of G: if G is a 'complicated' group, this might be quite an achievement. (He would have solved Dehn's word problem for the particular presentation.)

Suppose now $G \cong PSL_2(q)$ or $PGL_2(q)$ for some prime power $q = p^e$ and that $\mathcal{M}$ is a ROΔM (i.e is triangular). Then checking whether $W(x, z) = I$ by brute force (i.e. by matrix multiplication) can be done but is clearly unwieldy. What this chapter does, after setting up the problem (including hypermaps initially) a little more formally, is to describe a far neater program to decide which W are circuits. This is done by finding we may characterize the map $\mathcal{M}$ by G and the minimal polynomial r in $\mathbb{Z}_p$ of $k := tr(z)$. Then an algorithm is constructed by which the value of $tr(W(x,z))$ is given in terms of a polynomial $P(W)$ over $\mathbb{Z}$ in powers of k (these polynomials being independent of q). If r is a factor of either $P(W) + 2$ or $P(W) - 2$ working mod p, then

$$W(x, z) = I \qquad \text{or is of order } p,$$

(and conversely). Finally a simple decision process is described to discriminate between the two cases. So in this way B can fairly easily reassure himself that he'll get back home! And should he want to, he'll be able to generate a circuit in 'his' ROΔM (with automorphism type G) that is not shared by some other ROΔM (whichever one he may choose) with the same automorphism type.

2. ROUTES, CIRCUITS AND PRESENTATIONS

Suppose $\mathcal{M}$ is any oriented map, given algebraically in the standard way as (G, Ω, x, y), and let

$$z := y^{-1}x \quad , \quad d := o(z) \quad .$$

Then there is the obvious (graphical) concept of a path P in $\mathcal{M}$ which is

a (finite) sequence of vertices in $\mathcal{M}$

$$v_0, v_1, v_2, \dots, v_n \qquad \text{for some } n \in \mathbb{N}$$

for which (v_i, v_{i+1}) is an edge for all $i = 0, \dots, n-1$. If the sequence has $(n+1)$ elements, then we say P is of <u>length</u> $(n+1)$.

Now, using the map properties of $\mathcal{M}$ (rather than just the 'weaker' graphical properties), we may represent the path P in a different way: suppose that the dart w is the directed edge from v_1 <u>into</u> v_0, then it is clear that

$$\exists\ s_0, s_1, \dots, s_n \in \mathbb{Z}_d \text{ s.t. } \forall i = 0, \dots, n-1$$

$$w_i := \left(\prod_{j=0}^{i} (xz^{s_j})\right) x\,(w) \text{ is the directed edge from } v_i \text{ to } v_{i+1}\ .$$

I call the word W in x and z given by

$$W(x, z) = xz^{s_{n-1}} x \dots x z^{s_0} x$$

a <u>route</u> which <u>induces the path P at w.</u>

The definition of a route is simply a word W in x and z of the form

$$W(x, z) = z^{t_m} x \dots x z^{t_1} x z^{t_0} \qquad t_m, \dots, t_0 \in \mathbb{Z}\ .$$

An important feature of a route is that, unlike a path, it is defined independently of any map being considered. If we take the route W as above and the map $\mathcal{M} = (G, \Omega, x, y)$, we may take the values of $t_m, \dots, t_0$ modular to d, and W induces a different path in $\mathcal{M}$ at every $w \in \Omega$ in the natural way. However, whatever $\mathcal{M}$ and $w \in \Omega$, the induced path will have length $t_m - 1$. Correspondingly we also say the route W has the

length t_m-1 (i.e. the length is the number of x's in W(x, z)).

So, contextually, we call the word W a route whenever we think of it as inducing paths for certain maps $\mathcal{M}$ at certain darts w of $\mathcal{M}$. But we shall be particularly interested in the instances when for a particular $\mathcal{M}$ and w, W satisfies

$$W(x, z)\,(w) = w \ .$$

Then we say the route W is a <u>circuit</u> at w (in $\mathcal{M}$).

Now I constrain $\mathcal{M}$ to be <u>regular</u>. This means Aut $\mathcal{M} \cong G$. Also if W is a route, and for any dart w of $\mathcal{M}$

$$W(x, z)\,(w) = w$$

then in G,

$$W(x, z) = I \ .$$

In particular

$$W(x, z)\,(w') = w' \qquad \forall w' \in \Omega$$

and I call W just a circuit in $\mathcal{M}$ (with no reference to 'base' dart).

So, given $\mathcal{M}$, we can 'read off' from its topological representation a presentation G($\mathcal{M}$) for the group G:

$$G(\mathcal{M}) := \langle X, Y \mid X^2, W(X, Y) \text{ s.t. } W \text{ is a circuit in } \mathcal{M} \rangle$$

Note that the relator set here is as inefficient as possible in that <u>all</u> the relations are included (of which there are of course an infinite number). For two different regular maps $\mathcal{M}$, $\mathcal{M}'$ with the same automorphism group G, there will be a relation W in the presentation G($\mathcal{M}$) that is

not a relation in the presentation $G(\mathcal{M}')$: this gives us a property for the topological representation of $\mathcal{M}$ not shared by that of $\mathcal{M}'$, the property being 'W is a circuit'.

For an oriented hypermap $\mathcal{H}$, the concepts of path and route are not so natural, but in chapter 1 we saw that $\mathcal{H}$ can be represented by a map $\mathcal{M}$, so the ideas can carry through using $\mathcal{M}$. Despite this, our geometric insight for hypermaps in general tends to be far less concrete than that for maps in particular, and there is little intuitive motive to interpret each algebraic property as a property of some topological representation. However there is always the possibility to exploit the topological properties of the surface of imbedding to give information about $\mathcal{H}$ (or indeed its map subgroup, see p. 29).Just for this it is worthwhile to extend the notion of a route to hypermaps (but we no longer stress that of path); a route is a word W in two letters, and the term is used in the context of testing whether for a particular hypermap $\mathcal{H} := (G, \Omega, x, y)$ with $z := (xy)^{-1}$, and $w \in \Omega$ that

$$W(x, z)\,(w) = w \quad ;$$

if the above holds, W is a circuit in $\mathcal{H}$ at w. If $\mathcal{H}$ is regular, the abstract group given by the presentation

$$G(\mathcal{H}) := \langle X, Z \mid W(X, Z) \text{ s.t. } W \text{ is a circuit in } \mathcal{H} \rangle$$

is isomorphic to G.

Clearly, if H is the set of oriented regular hypermaps $\mathcal{H}$ with automorphism group G, then the set of mutually non-equivalent 2-generator presentations of G is given by

$$\{ G(\mathcal{H}) : \mathcal{H} \in H \}$$

(Exactly the same attitude and comments apply for unoriented maps and hypermaps, but then one is concerned with the presentations of groups with three generators constrained to be involutions. I do not concern myself with this case: all hypermaps referred to henceforth are oriented.)

So if $\mathcal{H} := (G, \Omega, x, y)$ is a regular hypermap, we are interested to find all the words W in two letters such that in G

$$W(x, z) = I$$

as these words exactly form the relator set R of the presentation $G(\mathcal{H})$ for G. For the special case, $\mathcal{H}$ is a ROAM, $G = PSL_2(q)$ or $PGL_2(q)$ for some prime power q, a manageable algorithm that generates the circuits in a systematic way is developed in the next section.

But for now, I suppose we 'know' R. Then we could try to find finite, and then minimal, subsets S of R that constitute a defining set of relations for G. This is something that does not primarily engage us in this chapter, we will be involved mostly in simply finding a relation in one 2-generator presentation for a group G that is not a relation in another 2-generator presentation for the same group G; in other words to find a circuit that occurs in just one of a pair of given regular hypermaps with the same automorphism group. (I will in fact, for simplicity, mostly restrict myself to triangular maps). However, to end this section, I discuss finite presentations a bit further, in the form of a couple of notes.

Note 1

Hall's method, see §1.2 , gives us a method (given a finite group G) for calculating the number N of regular hypermaps with automorphism group G that share a certain set S of prescribed circuits W. Then N is the

number of non-equivalent 2-generator presentations of G for which the relator set R contains S. If $N \geq 2$, S cannot form a defining relator set for G.

Note 2

Here I try to utilise the genus g (supposing that this is greater than 1) of the surface $\$(\mathcal{H})$ of imbedding, in particular to find a finite presentation of G with (2g+2) relations given in terms of circuits representing topologically different simple loops in the imbedding. This is done sketchily and in reference to a note in Chapter 1, p. 29 , where the isomorphic type of the map-subgroup of $\mathcal{H}$ is identified.

So suppose $\mathcal{H} := (G, \Omega, x, y)$ is a regular (r, n, m)-hypermap (that is $o(x) = r$, $o(y) = n$ and $o(z) = m$ where $z := (xy)^{-1}$) and that

$$\Gamma := gp\ \langle X, Y : X^r, Y^n \rangle .$$

Then the map-subgroup M of $\mathcal{H}$ is free of rank $1 + (1 - \frac{1}{r} - \frac{1}{n})|G|$ given by

$$M = gp\ \langle a_1, b_1, \ldots, a_g, b_g, \bigcup_{u \in V} c_u \backslash c_v : - \rangle$$

where $a_1, b_1, \ldots, a_g, b_g$ are words in X and Y such that the same words in x and y are circuits representing the set of simple non-trivial loops of $\$$ (based at vertex v), and where the generators c_u are indexed by the vertex set V and are words in X and Y which are conjugates of Z^m (as explained on p. 30 - 31).

Now each word in X and Y that represents an element in M is a word product of the free generators. Also such a word in X and Y has its exact analogue in x and y as a relation in $G(\mathcal{H})$, and vice-versa. We conclude that the words of the generator set for M as above together with

the relations

$$x^r = I, \qquad y^n = I$$

provide a defining set of relations for $G(\mathcal{H})$. But the words c_u in x and y express conjugates of z^m, which itself describes a trivial simple loop in $ and is dependent on the set of relations $\{ a_1,b_1,\ldots,a_g,b_g,x^r,y^n\}$ (if the genus $g > 1$). Thus

$$G(\mathcal{H}) = \langle x, y : x^r, y^n, a_1, b_1, \ldots , a_g, b_g \rangle$$

which has a relator set of order $2g + 2$

(where $2g = 2 + |G| \left(1 - \frac{1}{r} - \frac{1}{n} - \frac{1}{m}\right)$) .

Note this presentation we have just derived is not necessarily minimal: if w(x, z) is any circuit, then a conjugate word of w(x, z), which also of course is a circuit, need not be topologically equivalent as a loop in $ to w(x, z). So, in this respect, there is a strong possibility of some mutual dependence within the relator set.

3. AN ALGORITHM TO PRODUCE CIRCUITS FOR ANY ROΔM $\mathcal{M}$ WITH AUT $\mathcal{M} \cong PSL_2(q)$ OR $PGL_2(q)$, SOME q

I return to the main problem as I left it in the previous section: suppose $\mathcal{H} := (G, \Omega, x, y)$ is any regular hypermap, for which we know $o(x) = r$, $o(y) = n$ and $o(z) = d$ (where $z := (xy)^{-1}$). Can we find a feasible algorithm to generate those routes W(x,z) which are circuits in $\mathcal{H}$, i.e. for which

$$W(x, z) = I \text{ in } G \ ?$$

Our ability to do this of course depends a lot on the group G (and the form in which it is given to us). But for matrix groups we may always of course use the brute force of matrix multiplication, testing first the

routes of length 1, then the routes of length 2, and so on, to see which ones are circuits.

Fortunately, when I now specialise to $G \cong PSL_2(q)$ or $PGL_2(q)$ for some $q = p^e$, we can be a lot more efficient than this, by use of trace. Instead of having to determine the whole matrix represented by $W(x, z)$, we may simply calculate its trace: if the trace is 2, $W(x, z)$ is either a circuit or is a route of order p in $\mathcal{H}$ (i.e. the route formed by juxtaposing p copies of $W(x, z)$ is a circuit, whereas juxtaposing any fewer copies is not a circuit). However it is fairly easy to construct a decision criterion between the two possibilities that works in every case. But we can do better: whatever the value of the trace of $W(x, z)$, we can use it to calculate the order of $W(x, z)$ as a group element of G; thus we need not 'waste' any calculations (as for each route we consider, we find a circuit).

I now give an example of how these ideas may be put into practice by restricting my attention further to just ROΔMs (so $(r, n) = (2, 3)$). The methods I present here do not necessarily have natural extensions pertinent to hypermaps with associated pair $(r, n) \neq (2, 3)$. Thus the arguments here must be regarded as being special to ROΔMs. However it should not be difficult to adapt them for the other cases, but the process in whole will be more complicated.

So suppose we are given a ROΔM $\mathcal{M} := (G, \Omega, x, y)$ with $G \cong PSL_2(q)$ or $PGL_2(q)$ for some q. I want to generate its circuits.

We in fact do not work in words in x and z (routes) but in words in v and z where

$v := yx$ and $z := y^2x$.

(From now on, whenever I refer to a word, I will mean a word in 2 letters) Noticing that

$$x = y^2xxy^{-1}y^2x = zv^{-1}z$$

$$(\Rightarrow \quad v = zxz)$$

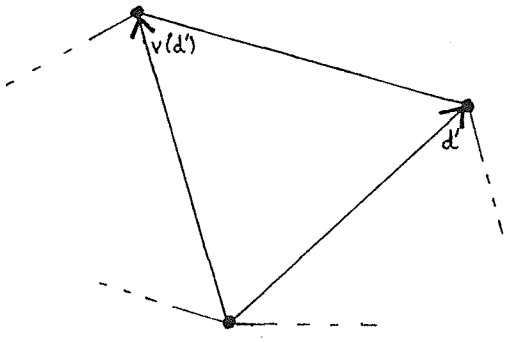
clearly $< v, z > = G$, so this can be done. Whenever we find for a certain word W that

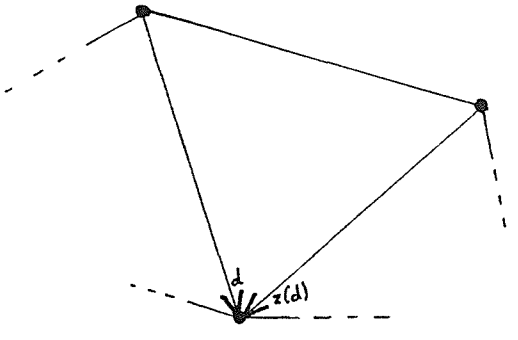
$$W(v, z) = I$$

we need only substitute zxz for each v to obtain the associated circuit, which then will be of length equal to the exponent sum $\exp(W; v)$ of v in W. But we also define another 'measure of size' for $W(v, z)$: the rank $\chi(W)$ of $W(v, z)$ is the total number of letters in the word, i.e. equals

$$\exp(W; v) + \exp(W; z) \ .$$

For insight, notice that the action of v and z by multiplication on the darts of $\mathcal{M}$ can intuitively be thought of as rather like the mechanical actions of a pair of scissors at the tip of the blades and at the joint respectively, but with these two actions working in opposite senses to each other;





Now we shall be talking about trace: I ought to clarify what I mean by this when $G = PGL_2(q)$ for any odd q. What we have to do is choose and fix any non-square β in GF(q). Then for any $g \in G$, we represent g by a pair (plus and minus) of 2 x 2 matrices $\pm M$, where

$$\det(M) = 1 \quad \text{if } g \in PSL_2(q) < PGL_2(q)$$

$$\det(M) = \beta \quad \text{if } g \notin PSL_2(q) .$$

This pair exists and is unique. We set

$$tr(g) = \pm tr(M)$$

One can easily check, whether $G = PSL_2(q)$ or $PGL_2(q)$, that trace is preserved both under taking inverses and taking conjugates. As

$v = yx$ is conjugate to xy which is inverse to $y^2x = z$ we conclude that $tr(v) = tr(z)$, let us say the shared value being $\pm k$, where $k \in GF(q)$.

But our program shall be to calculate in terms of k values of trace of elements of G when these are given simply by words W in v and z; evidently to perform this operation we may fix our values of tr(v) and tr(z) to single values in GF(q) (by fixing the sign of the matrices representing v and z). For instance, we will set

$$\underline{tr(z) = k} \qquad \underline{tr(v) = -k} .$$

Thus we find the one value of trace for W(v, z) which we can then pair with its negative value in GF(q). (In essence what we are doing is defining trace on the set of words in v and z as 1-valued, and trace on the set of elements of G as 2-valued; an element $g \in G$ may be represented by two different words with trace of opposite sign).

In this system of uniquely valued traces tr(W) for words W, we see that trace is still preserved under conjugacy (of words), but now the inverse word W^{-1} satisfies

$$tr(W^{-1}) = \begin{cases} tr(W) & \text{if } \chi(W) \text{ is even} \\ -tr(W) & \text{if } \chi(W) \text{ is odd} \end{cases}$$

From this we easily see that for all words W,

$$tr(W(v, z)) = \pm tr(W(v, z)^{-1}) = \pm tr(W'(z, v))$$

where W' is the word with letters occuring in reverse order to W, and + or - as $\chi(W)$ is even or odd again.

This means that in our efforts to find the value of trace for every word W(v, z), we need only consider those satisfying :

$$\exp(W; v) \leqslant \exp(W; z) \qquad (1)$$

Also we shall soon develop a method to calculate $tr(W^i)$ (for any integer i) given tr(W). (By W^i I mean of course the word formed by juxtaposing i copies of W). So we also need only consider W for which

W is not the juxtaposition of copies of a shorter word. (2)

Thirdly we can partition the set of all words into subsets consisting of the words which are cyclic permutations of letters of each other. Each such subset I call a cycle (of words). Trace is constant under cycle, so we need only consider one word (a 'representative') of any one cycle.

Let $\mathfrak{L}$ be the set of cycles C for which

(1) the words in C satisfy $\exp(W; v) \leqslant \exp(W; z)$

(2) there are no words W in C such that W is the juxtaposition of copies of a shorter word.

Let $\mathcal{W}$ be a set of representatives of the cycles C of ℓ. Then by calculating tr(W) for $W \in \mathcal{W}$ we have effectively dealt with tr(W) for <u>all</u> words W.

As an illustration, the words in v and z as presented below may be regarded (without loss of generality) as the elements of $\mathcal{W}$ of rank less than eight:

χ	Words W(v, z) in $\mathcal{W}$ with rank χ
1	z
2	vz
3	vz^2
4	vz^3, vz^2v
5	vz^4, vz^3v, vz^2vz
6	vz^5, vz^4v, vz^3vz, vz^2vzv, v^3z^3
7	vz^6, vz^5v, vz^4vz, vz^3vz^2, vz^3vzv, vz^2vz^2v, vz^2vzvz, v^3z^4

Now suppose we have determined the trace function on $\mathcal{W}$; we need an algorithm to calculate the order of a word W just from the value of tr(W). (The method shall also show what is the value of $tr(W^i)$, for $i \in \mathbb{N}$, given tr(W)). To proceed we need the following lemmas and corollaries (where $G' := PGL_2(q)$ if G is $PSL_2(q)$ or $PGL_2(q)$, same q, and we regard $G' \geq G$).

<u>Lemma 1</u>

(We regard the word W as the element <u>of G'</u> represented by W(v, z))

Let W be a word.

Let $T_0 = 2$, then for all $j \geq 1$; $T_j = tr(W^j)$.

Then $\forall j \geq 2$,

$$T_j = \begin{cases} T_1 T_{j-1} - T_{j-2} & \text{if } j \text{ is odd or } W \in PSL_2(q) \\ \frac{T}{\beta}_1 T_{j-1} - T_{j-2} & \text{if } j \text{ is even and } W \notin PSL_2(q) \end{cases}$$

Lemma 2

Let W be a word such that tr(W) does not equal +2 or -2. Then the order o(W) of W is given by the smallest natural number n for which T_n(as in the previous lemma) equals +2 or -2.

If $G = PGL_2(q)$ with q odd and $W \notin PSL_2(q) < PGL_2(q)$ then further o(W) is given by the least <u>even</u> natural number n for which $T_n = 2$ or -2.

Lemma 3

Suppose tr(W) = 2. Then W(v, z) = I in G if and only if both

i) tr(W(v, z)z) = tr z = k

ii) tr(W(v, z)v) = tr v = -k .

Similarly if tr(W) = -2, then W(v, z) = -I if and only if both

i) tr(W(v, z)z) = -tr z = -k

ii) tr(W(v, z)v) = -tr v = k .

In both cases, if the conditions are not satisfied, then o(W) = p.

I now give the proofs:

1. I split the proof into two cases

Case 1: $W \in PSL_2(q)$

If $T_1 = \pm 2$, the lemma yields $T_j = \pm 2$ for all j. But $T_1 := tr(W) = \pm 2$ is equivalent to W being either the identity or of order p, which means any power W^j is also identity or of order p, and so $Tr(W^j) = 2$. Thus in this case the lemma is true. We may assume $T_1 \neq \pm 2$.

Let $T_1 = \gamma \neq \pm 2$.

Then due to the correspondence of values of trace $\neq \pm 2$ (where here plus and minus values are identified) with the conjugacy classes of non-identity elements of $PSL_2(q)$ not of order p, we may assume that W is conjugate to the matrix $\begin{pmatrix} \gamma & 1 \\ -1 & 0 \end{pmatrix}$. Because of the invariance of trace under taking conjugates, we may as well let W equal $\begin{pmatrix} \gamma & 1 \\ -1 & 0 \end{pmatrix}$.

For any $j \geq 2$ let

$$W^{j-2} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow T_{j-2} = a + d$$

Then

$$W^{j-1} = \begin{pmatrix} a\gamma - b & a \\ c\gamma - d & c \end{pmatrix} \Rightarrow T_{j-1} = a\gamma - b + c$$

$$W^{j} = \begin{pmatrix} a\gamma^2 - b\gamma - a & a\gamma - b \\ c\gamma^2 - d\gamma - c & c\gamma - d \end{pmatrix} \Rightarrow T_j = \gamma(a\gamma - b + c) - (a + d)$$

The lemma is proved in this case.

<u>Case 2: $W \notin PSL_2(q)$</u> ($\Rightarrow$ q is odd)

The conjugacy classes of elements in $PGL_2(q)$ that lie outside the subgroup $PSL_2(q)$ are characterised by trace. Thus the proof in this case is very similar to that of case 1; if $T_1 = \gamma$ we may take $W = \begin{pmatrix} \gamma & \beta \\ -1 & 0 \end{pmatrix}$ (with no more worrying about confusion between the identity and elements of order p, all these lie in $PSL_2(q)$). We perform analogous matrix multiplications as before (this time keeping tabs of determinants and adjusting by division as appropriate). The remaining results in the lemma are seen to be true. □

2. Suppose $tr(W) \neq \pm 2$ and $tr(W^n) = \pm 2$.

Now $tr(W^n) = \pm 2 \Rightarrow W^n$ is either identity or of order p.

But W^n is of order $p \Rightarrow W^{np} = I$

$$\Rightarrow W^p = I$$

(as G has no elements with order of a multiple of p, except p itself).

$$\Rightarrow tr(W) = \pm 2 \quad \text{⚡}$$

The first statement of the lemma is thus obviously valid.

The second statement of the lemma comes from the first, and from the observation that elements of $PGL_2(q) \setminus PSL_2(q)$ all have even order.

3. Suppose $tr(W) = 2$; we prove the relevant assertion of the lemma (the proof of the other case, $tr(W) = -2$, is exactly similar). The implication one way is evident. To prove the converse, we suppose both:

i) $tr(W(v, z)\, z) = tr\ z$

ii) $tr(W(v, z)v) = tr\ v$

Now if W is not the identity, then W has order p. We suppose this is the case; without loss of generality we may take

$$W(v, z) = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} \qquad \text{for some } \mu \in GF(q) \setminus \{0\}.$$

Let $z = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

Then $W(v, z)z = \begin{pmatrix} a + \mu c & b + \mu d \\ c & d \end{pmatrix}$

and i) implies $c = 0$. In the action of G on marks, this is to say 'z fixes ∞'. Clearly v will have to share this same property. But G is transitive

on the set of marks and $< v, z > = G$. We have a contradiction, and conclude that if W satisfies $tr(W) = 2$ and i), ii) above, it must represent the identity in G.

□

Note

In the preceding lemmas, it is clear that in the case of $G = PGL_2(q)$ (q not a power of 2) we need a way of distinguishing those words W(v,z) that represent elements of G lying in the subgroup $PSL_2(q)$ from those that do not. This is in fact easy: as $G = < v, z >$, and v and z are conjugate to each other, both v and z^{-1} do not lie in $PSL_2(q)$. It is thus exactly those words with even rank that do.

The algorithm we use to find o(W) from the trace tr(W) of a word W is more or less stated in the propositions of Lemmas 1 to 3 themselves. If $tr(W) = \pm 2$, then we can decide whether $W(v, z) = \pm I$ or if $o(W) = p$ by lemma 3; if $tr(W) \neq \pm 2$, then o(W) can be found by repeated application of lemma 1 to find the least j s.t. $T_j = \pm 2$ and then invoking lemma 2.

Note that if $G = PGL_2(q)$ and W is of odd rank (i.e. $W \notin PSL_2(q)$) it is obviously more efficient to find (using lemma 1) the values of trace just of powers of W^2 (rather than W itself).

Also another short-cut that will sometimes be available is if ever $tr(W^j)$ is found to be 0 (or ± 1) and j is the least value for which this is true, then immediately $o(W) = 2j$ (or $3j$).

Finally on this topic, I develop the statement of lemma 1, but this shall be incidental to our purposes. Let us consider just the case $W \in PSL_2(q)$, so that $\forall j \geq 2$

$$T_j = T_1 T_{j-1} - T_{j-2} \ .$$

Now if we leave T_1 as a variable, let us rename it t, then clearly the expression for each T_j is an integral polynomial of degree j in powers of t. For example

$$T_0 = 2 \ , \qquad T_1 = t \ ,$$

$$T_2 = t^2 - 2 \ ,$$

$$T_3 = t(t^2 - 2) - t$$

$$= t^3 - 3t \ .$$

For all j and for each i $(\geq 0$ and $\leq j)$ we define $T_j(i)$ as the coefficient of t^i in the polynomial T_j. For $i > j$, we define $T_j(i)$ as 0. Then clearly $\forall j \geq 2$ and for all i, we have the difference equation:

$$T_j(i) = T_{j-1}(i-1) - T_{j-2}(i)$$

As $T_1(0) = 0$, it is easy to prove by induction that

$$T_j(i) = 0 \qquad \text{whenever } \underline{i + j \text{ is odd}} \ .$$

But if $\underline{(i + j) \text{ is even,}}$ we readily detect 'Pascal triangle characteristics' in the values of $T_j(i)$ which suggest the presence of some binomial coefficient $\binom{n}{r}$, where $\binom{n}{r} := \frac{n!}{r!(n-r)!}$, in any general expression. In fact we find :

$$T_j(i) = \binom{(j+i)/2}{i} \cdot \frac{2j}{j+i} \cdot (-1)^{(j-i)/2}$$

(which can again be checked by induction:

$$T_0(0) = 0 \qquad T_1(1) = 1$$

and all other $T_j(i)$ satisfy the difference equation).

Thus we can calculate T_j for a particular word without necessarily knowing T_{j-1} and T_{j-2}: but as in the algorithms we use we find T_{j-2} and T_{j-1} in any case, this result is only of passing interest.

So far in this section we have specified a set $\mathcal{W}$ of words for which if we know the trace for all $W \in \mathcal{W}$, we have effectively found the set of circuits for $\mathcal{M}$ by using an algorithm for finding the order of a word from its trace. We have seen in passing that the trace of a given power of a word W may be regarded as a polynomial in powers of $tr(W)$; we shall now adopt the same sort of idea to form a second algorithm, to express the trace of any word $W \in \mathcal{W}$ as an integral polynomial in powers of $k := tr(z)$. This gives us a simple form by which our required values of trace may be calculated.

For constructing this, the crucial results are

Lemma 4

$$tr(vz) = \begin{cases} 1 - k^2 & \text{if } G = PSL_2(q) \\ \frac{\beta - k^2}{\beta} & \text{if } G = PGL_2(q),\ q \text{ odd} \end{cases}$$

Lemma 5

Suppose $W \in \mathcal{W}$ and $W(v, z) \neq v, z, vz$ or zv.

Then

i) $W(v, z)$ contains two z's juxtaposed or equals $(zv)^i z$ for some i.

Thus by cycling the letters of W, there exists a word W_1 such that we may take

$$W(v, z) = W_1(v, z)z^2$$

Let $W_2(v, z) = W_1(v, z)z$

Then

ii)
$$\mathrm{tr}W = \begin{cases} k\,\mathrm{tr}(W_2) - \mathrm{tr}(W_1) & \text{if } \begin{cases} G = PSL_2(q) \\ G = PGL_2(q) \text{ and } \chi(W) \text{ odd} \end{cases} \\ \frac{k}{\beta}\,\mathrm{tr}(W_2) - \mathrm{tr}(W_1) & \text{if } G = PGL_2(q) \text{ and } \chi(W) \text{ even} \end{cases}$$

Proof of lemmas

4. We may without loss of generality suppose

$$x = \begin{pmatrix} r & s \\ t & -r \end{pmatrix} \quad \text{where } \det x = -r^2 - st = (1;\beta) \text{ as } G = (PSL_2(q);\ PGL_2(q), q \text{ odd})$$

$$y = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$$

Then we calculate

$$v := -yx = \begin{pmatrix} -r-t & -s+r \\ r & s \end{pmatrix} \qquad z := y^2x = \begin{pmatrix} t & -r \\ -r-t & -s+r \end{pmatrix}$$

Thus $k = t + r - s$ and

$$\mathrm{tr}(vz) = \frac{1}{1;\beta}(-t^2 - 2r^2 - s^2 + 2sr + st - 2rt)$$

$$= \frac{1}{1;\beta}(-k^2 - r^2 - st)$$

$$= \frac{1}{1;\beta}(-k^2 + (1;\beta)) \qquad \square$$

5. i) Suppose $W \in \mathfrak{W}$. Then by definition

$$\exp(W;\ v) \lesssim \exp(W;\ z) .$$

so if two v's are juxtaposed in W then two z's must also be juxtaposed

(or possibly W 'starts' and 'ends' with z, but then w.l.o.g. we make take $z^{-1}Wz$ instead of W). So if W has no z's juxtaposed, it must be of the form

$$v,\ z,\ (vz)^j \quad \text{or} \quad (zv)^j \qquad \text{for some } j \in \mathbb{Z}$$

but again $W \in \mathcal{W}$ constrains $j = 1$.

ii) The proof is similar to that of lemma 1. I deal just with $G = PGL_2(q)$; the case $G = PSL_2(q)$ is analogous and simpler.

Without loss of generality we may let $z = \begin{pmatrix} k & \beta \\ -1 & 0 \end{pmatrix}$

Also let $W_1(v, z) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

with $ad - bc = (1; \beta)$ as $\chi(W) = \chi(W_1) + 2$ is (even; odd).

Then by matrix multiplication,

$$W_2(v, z) = \frac{1}{1;\beta} \begin{pmatrix} ak - b & a\beta \\ ck - d & c\beta \end{pmatrix}$$

and we calculate

$$\begin{aligned} tr(W) &= \frac{1}{\beta}\,(k(ak - b) - a\beta + \beta(ck - d)) \\ &= \frac{k}{\beta}\,(ak + c\beta - b) - (a + d) \\ &= \begin{cases} \frac{k}{\beta}\ tr(W_2) - tr(W_1) & \text{if } \chi(W) \text{ is even} \\ k\,tr(W_2) - tr(W_1) & \text{if } \chi(W) \text{ is odd} \end{cases} \end{aligned}$$

□

By lemmas 4 and 5 it is clear that we can (inductively on rank of words) determine a polynomial P(W) in powers of k giving tr(W) for each $W \in \mathcal{W}$. The polynomial P(W) is of degree $\chi(W)$. As an illustration, the following table gives P(W) for $W \in \mathcal{W}$ (and also a few W <u>not</u> in $\mathcal{W}$) with $\chi(W) \leq 7$, when $G = PSL_2(q)$, any q.

Word W	P(W)	Word W	P(W)
z	k	$*z^6$	$k^6-6k^4+9k^2-2$
$*v$	$-k$	vz^5	$-k^6+5k^4-6k^2+1$
$*z^2$	k^2-2	vz^4v	$k^6-5k^4+7k^2-2$
vz	$-k^2+1$	vz^3vz	$k^6-4k^4+3k^2+1$
$*z^3$	k^3-3k	$*vz^2vz^2$	$k^6-4k^4+4k^2-2$
vz^2	$-k^3+2k$	vz^2vzv	$-k^6+4k^4-4k^2+1$
$*z^4$	k^4-4k^2+2	$*vzvzvz$	$-k^6+3k^4-2$
vz^3	$-k^4+3k^2-1$	v^3z^3	$-k^6+5k^4-7k^2+1$
$*vzvz$	k^4-2k^2-1	$*z^7$	$k^7-7k^5+14k^3-7k$
v^2z^2	k^4-3k^2+2	vz^6	$-k^7+6k^5-10k^3+4k$
$*z^5$	k^5-5k^3+5k	vz^5v	$k^7-6k^5+11k^3-6k$
vz^4	$-k^5+4k^3-3k$	vz^4vz	$k^7-5k^5+6k^3$
vz^3v	k^5-4k^3+4k	vz^3vz^2	$k^7-5k^5+7k^3-3k$
vz^2vz	k^5-3k^3+k	vz^3vzv	$-k^7+5k^5-7k^3+2k$
		vz^2vz^2v	$-k^7+5k^5-8k^3+5k$
		vz^2vzvz	$-k^7+4k^5-3k^3-k$
		v^3z^4	$-k^7+6k^5-11k^3+5k$

The entries marked with an asterisk * denote the words W that do not lie in $\mathcal{W}$ (as set in the table on p.146).

If $G = PGL_2(q)$, the polynomials $P(W)$ are as in the table but with each k^{2n} (any n) replaced by $\frac{k^{2n}}{\beta^n}$, and k^{2n+1} replaced by $\frac{k^{2n+1}}{\beta^n}$.

The table suggests that the coefficient of k^n in $P(W)$ is zero if either

i) n is odd and $\chi(W)$ is even

or ii) n is even and $\chi(W)$ is odd.

This is easily verified by induction.

Finally notice that $P(z^j)$ gives the same polynomial, but in powers of k, as T_j in powers of t on p.151. This means that if in $P(z^i)$ we substitute $P(W)$ for k, then the resulting polynomial will be $P(W^i)$. For example

$$P(z^3) = k^3 - 3k \qquad P(vz) = 1 - k^2$$

$$\Rightarrow P(vzvzvz) = (1 - k^2)^3 - 3(1 - k^2)$$

$$= -k^6 + 3k^4 - 2$$

We are now equipped to come back to our initial objective; to find the circuits of the given ROΔM $\mathcal{M} := (G, \Omega, x, y)$. We firstly calculate k(:=tr(z)) as a value of GF(q). Then for each word $W \in \mathcal{W}$, $tr(W) \in GF(q)$ may be ascertained by substituting the particular value of k for $\mathcal{M}$ in P(W). Our first algorithm then enables us to determine the least natural number n for which W^n is a circuit.

This schedule demonstrates that the set of circuits for $\mathcal{M}$, and hence the relator set of the presentation $G(\mathcal{M})$ for G, is determined entirely by the value of k. This gives us an indirect proof of something already known, that is for fixed G, k determines the ROΔM $\mathcal{M}$ uniquely (see p.120). (However, if $q = p^e$ for some prime p, then the e images of k under

the field automorphisms of GF(q) will determine the same map $\mathcal{M}$ as k, so $\mathcal{M}$ does not conversely determine k). Interestingly this comment, we also already know, does not apply if instead of ROΔMs we consider the set of hypermaps H(r, n) (for fixed r, n ε ℕ both not equal to two) defined by

$$H(r, n) = \{\mathcal{H} : = (G, \Omega, x, y) | o(x) = r, \ o(y) = n\} .$$

If one such hypermap $\mathcal{H}$ satisfies $tr(xy)^{-1} : = k \neq 0$, then there is exactly one other hypermap in H(r, n) which shares this same property. This shows we cannot hope to represent values of trace in terms of polynomials in powers of k for hypermaps in general in quite the same way as for ROΔMs in particular.

The way I have described the program to find the circuits of $\mathcal{M}$ has been termed rather biased to the case when G is defined over a finite field of prime order p. For then one can work entirely in $\mathbb{Z}_p$, and the method is entirely clear. However if $q = p^e$ with $e > 1$, the elements of GF(q) are themselves expressed in terms of polynomials over $\mathbb{Z}_p$. So substituting k into P(W) and then finding expressions for $Tr(W^i)$ will only produce more polynomials over $\mathbb{Z}_p$. How then do we know when $tr(W^i) = \pm 2$? The answer will be in terms of the minimal polynomial of k in GF(q): it shall be explained in the next section.

4. MINIMAL POLYNOMIALS

Before discussing maps again, it is as well to indulge in a revision of some basic finite field theory. First we need a definition; a polynomial over a field F is monic if and only if the coefficient of the term of highest exponent is the multiplicative identity of F.

Suppose we are given the prime power $q = p^e$ and the finite field GF(q). Then I regard $\mathbb{Z}_p$ to be the subfield GF(p) of GF(q). For every element γ of GF(q) there exists a unique monic polynomial r_γ over $\mathbb{Z}_p$ of least degree such that $r_\gamma(\gamma) = 0$. This polynomial r_γ is called the minimal polynomial of γ. For all γ in GF(q), r_γ is irreducible over $\mathbb{Z}_p$; also the degree ∂r_γ of r_γ divides e. Conversely every irreducible monic polynomial r over $\mathbb{Z}_p$ with ∂r dividing e is assumed as the minimal polynomial of some element δ of GF(q), in fact it is assumed by all the elements in the class containing δ under the field automorphisms (but by no other elements of GF(q)).

Now the element γ of GF(q) lies in no proper subfields of GF(q) if and only if $\partial r_\gamma = e$. Thus we may relate the number N(q) of irreducible monic polynomials over $\mathbb{Z}_p$ of degree e with the number n(q) of elements in GF(q) which lie in no proper subfield thus

$$N(q) = \frac{1}{e} n(q) .$$

But to calculate n(q) we may invoke Möbius inversion. Let C_{p^e-1} represent the multiplicative cyclic group of GF(q) and C_{p^f-1} the cyclic subgroup of order (p^f-1) for any $f|e$. Then we establish the Möbius function μ_P on the poset $P := \{C_{p^f-1} : f|e\}$ where ordering is given by inclusion, equivalently $C_{p^f-1} \leq C_{p^h-1}$ iff $f|h$. Evidently

$$\forall f|e, \qquad \mu_P(C_{p^f-1}) = \mu(\tfrac{e}{f}) ,$$

(where μ as usual is the classical Möbius function). Now define $\forall f|e$,

$$\sigma(C_{p^f-1}) = p^f-1$$

$$\varphi(C_{p^f-1}) = \#\text{ elements of } C_{p^f-1} \text{ that do not lie in } C_{p^h-1} \text{ for any proper divisor } h|f .$$

Then $\sigma(C_{p^e-1}) = \sum_{f|e} \varphi(C_{p^f-1})$

$$\Rightarrow \quad n(q) = \varphi(C_{p^e-1}) = \sum_{f|e} \mu_p(C_{p^f-1})\, \sigma(C_{p^f-1})$$

$$= \sum_{f|e} (p^f-1)\, \mu(\tfrac{e}{f})$$

and so $N(q) = \frac{1}{e} \sum_{f|e} (p^f-1)\, \mu(\frac{e}{f})$.

We now come back to maps again, and start by remarking (in reference to the table of enumerations on p.105) that if q is a power of 2 (let us say 2^e), then the number d(G) of ROΔMs with automorphism group G $\cong PSL_2(q)$ satisfies

$$d(G) = \frac{1}{e} \sum_{f|e} (2^f-1)\, \mu(\tfrac{e}{f}) = N(q) .$$

Now all polynomials over GF(2) are monic, so this is paramount to saying that the set $\mathcal{M}_3^+(G)$ of ROΔMs with automorphism group G and the set Ir(q) of irreducible polynomials of degree e over GF(2) have the same cardinality. Can we construct some sort of natural bijection between the two? We in fact use the material of the previous section.

Define the function $\theta : \mathcal{M}_3^+(G) \rightarrow Ir(q)$ as follows

$$\mathcal{M} \mapsto \text{the minimal polynomial of } k := tr(z) .$$

This is well-defined, but we have to justify this on two counts

i) θ is into Ir(q) because $\langle x,z \rangle = G$, and we have seen that the value of trace of every word in x and z is given by some polynomial expression in powers of k and coefficients in $\mathbb{Z}_p$; this means that the values of trace taken by elements of G form a subset of the field generated by

k. But every element of GF(q) is assumed as the trace of some element of G, hence k must generate GF(q), and so the minimal polynomial of k obliges us by belonging to Ir(q).

ii) The map $\mathcal{M}$ of $\mathfrak{M}_3^+(G)$ is represented by any one of e different values of k, these forming an orbit of field elements under the field automorphisms. But the exactly analogous statement obtained by substituting 'The map $\mathcal{M}$ of $\mathfrak{M}_3^+(G)$' by 'The polynomial r in Ir(q)' also holds. Thus θ is consistent.

Certainly θ is one-to-one (see the remarks towards the end of the last section) and we have already noted that

$$|\mathfrak{M}_3^+(G)| = |\mathrm{Ir}(q)|$$

so θ is a bijection.

Now I go on to the odd prime power case. So let $q = p^e$ be odd and extend the definition of Ir(q) thus:

$$\mathrm{Ir}(q) = \{ \text{monic irreducible polynomials over } GF(p) \text{ with degree } e \}$$

and I ask what relationships can we find between Ir(q) and the set $\mathfrak{M}_3^+(G)$ of ROΔMs of automorphism group G when G is in the first case isomorphic to $PSL_2(q)$ and in the second isomorphic to $PGL_2(q)$?

i) Suppose $G \cong PSL_2(q)$ with $e > 1$ and e odd

Then we know

$$|\mathfrak{M}_3^+(G)| = \frac{1}{2e} \sum_{f|e} (p^f - 1)\, \mu\left(\frac{e}{f}\right) = \frac{1}{2} |\mathrm{Ir}(q)| .$$

Now we can identify the elements of Ir(q) in pairs { r, r' } where if

$$r(t) = \sum_{i=0}^{e} a_i t^i \qquad \text{for some } a_0, a_1, \ldots, a_e \in \mathbb{Z}_p$$

then

$$r'(t) = \sum_{i=0}^{e} (-1)^{i+1} a_i t^i \ .$$

I denote this set of pairs Ir'(q). The significance of this set is that if γ is a generating element of GF(q), then the minimal polynomial of γ together with that of $-\gamma$ forms an element of Ir'(q).

Now we define the function $\theta : \mathfrak{M}_3^{+}(G) \to \text{Ir}'(G)$ thus:

$\mathcal{M} \mapsto$ the element of Ir'(q) containing the minimal polynomial of $k := \text{tr}(z)$.

Then θ is clearly well-defined and a bijection. (The essential difference of this to the 'q is even' case is that if the trace $k = \gamma$ represents the ROΔM $\mathcal{M}$, then $k = -\gamma$ will also represent $\mathcal{M}$; when q is even, $-\gamma = \gamma$ and we need not take this into account; but when q is odd, $-\gamma \neq \gamma$, and we have to introduce the set Ir'(q)).

ii) <u>Suppose $G \cong PSL_2(q)$ with $e > 2$ and even</u>

For all elements γ of GF(q), we define $\text{Mat}(0,1,\gamma)$ as the set of triples of matrices (x,y,z) in G satisfying

$$o(x) = 2, \quad o(y) = 3, \quad \text{tr}(z) = \gamma, \quad xyz = I \text{ in } G \ .$$

Then if for some γ and some triple $(x,y,z) \in \text{Mat}(0,1,\gamma)$ we have

$$\langle x,z \rangle = G$$

necessarily γ generates GF(q). However the converse is untrue (unlike the case when e is odd). If γ generates GF(q) then $\text{Mat}(0,1,\gamma)$ is non-empty and any $(x,y,z) \in \text{Mat}(0,1,\gamma)$ satisfies

$$\langle x,z \rangle = G \quad \text{or} \quad \langle x,z \rangle \cong PGL_2(p^{e/2}) \ .$$

So we need to partition the generators of GF(q) into two sets A and B.

A : those γ such that $\langle x,z \rangle \cong PGL_2(p^{e/2})$

This set is given to use by a result on p.28 of [14] (concerning what is termed there as 'irregularity' of trace-triples; c.f. my definition on p.123 of 'linear order-triples').

$$A = \{\gamma \in GF(q) : \gamma \text{ generates } GF(q) \text{ and is a square root of a non-square in the subfield } GF(p^{e/2})\}$$

What is $|A|$? Well clearly the condition put on $\gamma \in GF(q)$ to be an element of A is equivalent to

'γ is a square root of a non-square that generates $GF(p^{e/2})$' .

But it is easy to ascertain that a square of a generator of a finite field is also a generator; additionally, it is certainly true that a square root of a generating square in GF(q) will be generating. We deduce that

$$\begin{aligned} &\#\text{ non-squares that generate } GF(p^{e/2}) \\ &= \frac{1}{2}(\#\text{ generators of } GF(p^{e/2})) \\ &= \frac{1}{2}\sum_{f \mid e/2} (p^{f-1})\ \mu(e/2f) \ . \end{aligned}$$

Then for each non-square generating $GF(p^{e/2})$, there are <u>two</u> square roots lying in GF(q), so

$$|A| = \sum_{f \mid e/2} (p^{f}-1)\ \mu(e/2f) \ .$$

B : those γ such that $\langle x,z \rangle = G$

$$B = \{\gamma \in GF(q) : \gamma \text{ generates } GF(q) \text{ but } \gamma \notin A\}$$

Then

$$|B| = \sum_{f|e} (p^f - 1)\, \mu\left(\frac{e}{f}\right) - |A|$$

$$= \sum_{\substack{f|e \text{ s.t.} \\ e/f \text{ odd}}} (p^{f/2} - 1)^2\, \mu\left(\frac{e}{f}\right)$$

(the last line needs a little straightforward manipulation to justify it, left to the reader).

Now e is even, we define Ir'(q) slightly differently from the case of e odd. Now Ir'(q) is the set of pairs (r,r') in Ir(q) s.t.

if $r(t) = \sum_{i=0}^{e} a_i t^i \qquad a_i \in \mathbb{Z}_p$

then $r'(t) = \sum_{i=0}^{e} (-1)^i a_i t^i$.

Let Ir'(B) be the subset of Ir'(q) that comprises those pairs of minimal polynomials for elements γ and $-\gamma$ of GF(q) that lie in B. (Obviously B is closed under taking negative values and under the action of field automorphisms). Then

$$|Ir'(B)| = \frac{1}{2e} |B| \ .$$

Now define the function $\theta : \mathcal{M}_3^{+}(G) \to Ir'(B)$ by

$\mathcal{M} \mapsto$ the element of Ir'(B) containing the minimal polynomial of $k := tr(z)$.

θ is well-defined and a bijection.

Clearly we should finally like a way of distinguishing an element of Ir(q)

which represents the minimal polynomial of generating elements of GF(q) in B from one which represents elements in A. However this in fact is very simple and more or less self evident:

a generating element γ of GF(q) is <u>in A</u> iff the minimal polynomial r_γ of γ only has terms of even degree, i.e. has the form

$$r_\gamma(t) = \sum_{i=0}^{e/2} \alpha_i t^{2i}$$

for some $\alpha_0, \alpha_1, \ldots, \alpha_{e/2} \in \mathbb{Z}_p$.

iii) <u>Suppose $G \cong PGL_2(q)$, $e > 1$</u>

This case is evidently more complicated, and I shall not attempt here to obtain a characterisation of ROΔMs in $\mathcal{M}_3^+(G)$ by irreducible polynomials as I have done for $\mathcal{M}_3^+(PSL_2(q))$. The difficulty is that (when e is even) we no longer have the property

$$(x,y,z) \in \mathrm{Mat}(0,1,\gamma) \text{ generates } G \Rightarrow \gamma \text{ generates } GF(q).$$

(This is because of the existence of matrices in G with determinant β).

So for the groups $G \cong PSL_2(q)$ (any q) at least we have found a very useful identification for the elements $\mathcal{M}$ of $\mathcal{M}_3^+(G)$ in terms of the minimal polynomial r_k in $\mathbb{Z}_p$ for $k := \mathrm{tr}(z)$. In fact from now on in this chapter I will change how we denote the map $\mathcal{M}$:

$$\mathcal{M} := (G, \Omega, x, y)$$

now becomes

$$\mathcal{M} := (G, r_k).$$

Note that r_k is necessarily an element of Ir(q). Then, to review the situation,

For $G \cong PSL_2(2^e)$

$\forall r \in Ir(q)$, (G,r) represents a map $\mathcal{M}$ and r is unique in $Ir(q)$ by representing $\mathcal{M}$.

For $G \cong PSL_2(p^e)$, p odd, $e > 2$

$\forall r \in Ir(q)$ s.t. r does not only have terms of even degree, (G,r) represents a map $\mathcal{M}$; $\exists$ a second element r' of $Ir(q)$ (for which $(r,r') \in Ir'(q)$) s.t. (G,r') also represents $\mathcal{M}$, but there exist no others.

But we can easily adapt this characterisation of the elements of $\mathfrak{M}_3^+(G)$ to further cover the case when $p > 3$ and $G \cong PSL_2(p^2)$ or $G \cong PSL_2(p)$ (i.e. $e \leq 2$). From our work on exceptional and affine order-triples in the last chapter, it is easily seen that the set $\mathfrak{M}_3^+(G)$ in these cases is as standard to the set $\mathfrak{M}_3^+(PSL_2(p^e))$ for higher exponent e except we must discount those maps where representing G-triples (x,y,z) satisfy (both)

$$(o(z) \nmid p \quad \text{and}) \quad o(z) \leq 6 .$$

Now, from our table on p.155 , and not worrying too much about the sign of trace and whether we take r_k or r'_k in each case, we have:

$$o(z) = 1 \implies k = 2 \iff r_k(t) = t-2$$

However $r_k(t) = t-2 \implies o(z) = 1$ or p

$$o(z) = 2 \iff k = 0 \iff r_k(t) = 0$$

$$o(z) = 3 \iff k = 1 \iff r_k(t) = t-1$$

$$o(z) = 4 \iff (z^2) = 2 \iff k^2-2 = 0$$

$$\iff r_k(t) = \begin{cases} t - \sqrt{2} & \text{if } p \equiv \pm 1 \bmod 8 \\ t^2-2 & \text{if } p \equiv \pm 3 \bmod 8 \end{cases}$$

$\underline{o(z) = 5} \implies k^5-5k^3+5k-2 = 0$ or $k^5-5k^3+5k+2 = 0$

$\implies (k^2+k-1)^2(k-2) = 0$ or $(k^2-k-1)^2(k+2) = 0$

Hence $o(z) = 5 \iff k^2+k-1 = 0$ (for one sign of k).

Now $PSL_2(q)$ has an element of order 5 iff $q \equiv \pm 1 \mod 5$.

Thus k^2+k-1 is reducible iff $p \equiv \pm 1 \mod 5$.

$\underline{o(z) = 6} \iff o(z^3) = 2 \iff k^2-3 = 0$

$$\iff r_k(t) = \begin{cases} t - \sqrt{3} & \text{if } p \equiv \pm 1 \mod 12 \\ t^2 - 3 & \text{if } p \equiv \pm 5 \mod 12 \end{cases}$$

Collecting this information we conclude

$\underline{\text{for } G \cong PSL_2(p^2)}$

Let $S := \{ r \in Ir(p^2) : r$ does not only have terms of even degree$\}$

Then neither $r(t) = t^2-2$

nor $r(t) = t^2-3$

belong to S (even if they are irreducible).

Also if $r(t) = t^2+t-1$

then $r \in S$ iff $p \equiv \pm 2 \mod 5$. In this case there is not a map $\mathcal{M}$ in $\mathfrak{M}_3^+(G)$ given by (G, t^2+t-1), and consequently $|\ \mathfrak{M}_3^+(G)\ |$ is one less than the standard result for exponent $e > 2$.

$\underline{\text{for } G \cong PSL_2(p)}$

$Ir(p) = \{$ polynomials $r_a : r_a(t) = t-a$ for some $a \in \mathbb{Z}_p \setminus \{0\}\}$.

Now (G, r_a) for $r_a \in Ir(p)$ represents a map $\mathcal{M}$ in $\mathfrak{M}_3^+(G)$ except if

$a = \pm 1$

$p \equiv \pm 1 \bmod 8$ and $a = \pm\sqrt{2}$

$p \equiv \pm 1 \bmod 5$ and $(t\pm a)|(t^2+t-1)$

$p \equiv \pm 1 \bmod 12$ and $a = \pm\sqrt{3}$.

(Note that if (G,r_a) does represent a map $\mathcal{M}$ in $\mathfrak{M}_3^+(G)$, then only (G,r_{-a}) represents the same map. From this we may calculate $|\mathfrak{M}_3^+(G)|$ and check that this agrees with our earlier enumeration on p.105).

Finally we have for $p = 3$,

$\mathfrak{M}_3^+(PSL_2(3^2))$ is empty

$\mathfrak{M}_3^+(PSL_2(3)) = \{ (G,t-1) \}$.

Suppose $G = PSL_2(q)$, any q, and $\mathcal{M} := (G,r)$ is any map in $\mathfrak{M}_3^+(G)$. I return to the problem of determining the circuits of $\mathcal{M}$. Suppose k is an element of GF(q) which has the minimal polynomial r. Let z be an element of G with trace k, let $x,y \in G$ satisfy

$o(x) = 2,\ o(y) = 3,\ xyz = I$

and $v := zxz$. Then $\langle v,z \rangle = G$ and we know in terms of a polynomial P(W) with coefficients in $\mathbb{Z}_p$ and in powers of k the value of trace of each word W in v and z when this is considered as an element of G.

For a particular W and P(W) we want firstly to be able to check whether, when we substitute a k appropriate to $\mathcal{M}$,

$P(W) = 2$ or -2.

Let $P_+(W) = P(W)-2$, $P_-(W) = P(W)+2$

then we are in fact checking whether

$P_+(W)$ or $P_-(W)$ is zero .

But a polynomial s over $\mathbb{Z}_p$ yields zero when k is substituted in it if and only if the minimal polynomial r is a factor of s.

Thus P(W) = 2 or -2 (or in other words W(v,z) is the identity or has order p in G) iff $r|P_+(W)$ or $r|P_-(W)$.

By the same token, we can use the decision process as described in Lemma 3 (p.147) to determine, given P(W) = 2 or -2, whether W(v,z) = I or has order p.

In this way we can, for any word W, check if W(v,z) constitutes a circuit in $\mathcal{M}$ or not. This is independent of the z and x chosen.

From the preceding discussion, we may easily deduce the following

Proposition

If $G = PSL_2(p^e)$, and W(v,z) = I in G, then the rank $\chi(W)$ of W is greater than or equal to e.

Proof

The degree of P(W) equals $\chi(W)$ and so the same is true for $P_+(W)$ and $P_-(W)$. For the minimal polynomial of k, which has degree e, to divide $P_+(W)$ or $P_-(W)$, we clearly need

$$\chi(W) \geq e \ .$$

(Clearly in fact this proposition may be extended. Suppose m is a natural

number dividing $\frac{p\pm1}{2}$ or m = p. Then the trace of any element of G with order m will lie in $\mathbb{Z}_p$. Thus if W(v,z) has order m, again $\chi(W) \geq e$).

5. EXAMPLES

In this section I illustrate the ideas of the chapter put in practice, by considering a few simple examples.

Example 1 Examination of $\mathfrak{M}_3^+(G)$ for $G := PSL_2(5^2)$.

First we want to determine the irreducible polynomials over $\mathbb{Z}_5$ of form:

$$r(t) = t^2 + at + b$$

where $a = 1$ or 2 , $b \in \mathbb{Z}_5 \setminus \{0\}$.

(For a, we do not consider a = 0, else r only has terms of even power; we do not consider a = -1 or -2, else we count maps twice).

We find there are exactly four such polynomials and deduce the following inventory of maps in $\mathfrak{M}_3^+(G)$:

$$\mathcal{M}_1 := (G, t^2+t+1)$$

$$\mathcal{M}_2 := (G, t^2+t+2)$$

$$\mathcal{M}_3 := (G, t^2+2t-1)$$

$$\mathcal{M}_4 := (G, t^2+2t-2)$$

Now the valency of each map (i.e. the order of a suitable $z \in G$) must divide $\frac{1}{2}(5^2\pm1)$ and must be greater than six; thus it must be 12 or 13. Defining r_i for i = 1,...,4 as the polynomial describing $\mathcal{M}_i$, we have the valency of $\mathcal{M}_i$ is 12 if and only if $r_i | P(z^6)$. But

$$P(z^6) = k^6-k^4-k^2-2 = (k^2+k+1)(k^2-k+1)(k^2-2)$$

so $\mathcal{M}_1$ has valency 12 whereas $\mathcal{M}_2$, $\mathcal{M}_3$, $\mathcal{M}_4$ all have valency 13.

I set out to distinguish the maps $\mathcal{M}_2$, $\mathcal{M}_3$, $\mathcal{M}_4$ by finding circuits for each one not shared by the other two. I do this not strictly following the algorithms as given in section 3 of this chapter, but in a rather more selective manner working from the known P(W) for words of low rank as listed on p.155.

For $\mathcal{M}_2$

$$k^6+k^4-2k^2+2 = (k^2+k+2)(k^2-k+2)(k^2-2) .$$

But $r_2(t) = t^2+t+2$ is the minimal polynomial of k, so

$$k^6+k^4-2k^2+2 = 0$$

$$\Rightarrow \quad P(vz^3vz) = k^6+k^4-2k^2+1 = -1$$

$$\Rightarrow \quad \underline{o(vz^3vz) = 3}$$

Furthermore, observing that

$$P(vz^3vz) = 1 \Rightarrow k^2(k^4+k^2-2) = k^2(k^2-1)(k^2+2) = 0$$

we can see that $\mathcal{M}_2$ is unique in $\mathfrak{M}_3^+(G)$ in having this circuit.

For $\mathcal{M}_3$

$$k^5+2k^3+k+1 = (k^2+2k-1)(k^2-k+1)(k-1)$$

$$\Rightarrow \quad P(vz^2vz) = k^5+2k^3+k = -1$$

$$\Rightarrow \quad \underline{o(vz^2vz) = 3}$$

Also $P(vz^2vz) = 1 \Rightarrow (k^2-2k-1)(k^2+k+1)(k+1)$ and so $\mathcal{M}_3$ shares this circuit with $\mathcal{M}_1$, but <u>not</u> with $\mathcal{M}_2$, or $\mathcal{M}_4$.

<u>For $\mathcal{M}_4$</u>

$$k^4+2k^2-1 = (k^2+2k-2)(k^2-2k-2)$$

$$\Rightarrow P(vz^3) = -(k^4+2k^2+1) = -2$$

$$\Rightarrow vz^3 = I \quad \text{or} \quad o(vz^3) = 5$$

But $v = z^{-3} \Rightarrow G = \langle v,z \rangle$ is cyclic ※

Thus <u>$o(vz^3) = 5$</u> .

Now $P(vz^3) = 2 \Rightarrow k^4+2k^2-2 = 0$.

It can be checked that (k^4+2k^2-2) is irreducible.

Thus the circuit implicit in $o(vz^3) = 5$ is unique to $\mathcal{M}_4$ in $\mathfrak{M}_3^+(G)$.

<u>Example 2</u> Considering circuits of length less than four.

Recall that initially we thought of a route as being a word in x and z, and the length of the route being the number of x's occuring in that word. The route W(x,z) is a circuit iff

$$W(x,z) = I .$$

Now substituting $x = z^{-1}vz^{-1}$ in W(x,z) we obtain another word W' such that W'(v,z) = I; conversely if W' is any word for which W'(v,z) = I and we substitute v = zxz, the result is a circuit. Evidently we may as well consider W' itself being a circuit, with length equal to exp(W';v).

Now in the next chapter (§2) I shall use some basic properties of G :

$= PSL_2(q)$ for any $q > 3$, to show that once we have taken into account the order $o(z)$ of z (so that in any word, no exponent of z is greater than or equal to $o(z)$) we have :

i) there are no circuits of length 1 or 2

ii) all circuits of length 3 are conjugate as words to $(vz^{-3})^3$, this representing the relation $y^3 = I$.

This has implications for the trace polynomial $P(W)$ for every word $W(v,z)$ with $exp(W;v) \leq 3$, in the following manner. We fix the prime p but now give freedom to the 'group' G to vary over the types $PSL_2(p^e)$ with differing e. (So really G is a function $G : \mathbb{N} \rightarrow \{\text{groups}\}$ given by $G(e) := PSL_2(p^e)$). Then if we take the polynomials $P_+(W)$ and $P_-(W)$ (or indeed any other integral polynomial) and factorise these over $\mathbb{Z}_p$, the irreducible factors r fall into three categories:

I) r is a factor of one of:
$(k\pm1)$, (k^2-2), $(k^2\pm k-1)$, (k^2-3)

II) r is of even degree and only has terms of even power

III) r is neither in category I) or II) .

Only if r is in category III) is the map $\mathcal{M} := (G(\partial r), r)$ defined. If r is so, and if we have as said $exp(W;v) \leq 3$, then clearly we must have in $G(\partial r)$

$$o(W(v,z)) = p$$

rather than

$$W(v,z) = I .$$

If in fact $exp(W;v) = 1$ (and so we may without loss of generality assume

that $W(v,z) = vz^i$ for some $i \in \mathbb{N}$), we may extend essentially the same idea a little further: for we cannot have

i) $o(W) = 2$ unless W is a conjugate of $x = z^{-1}vz^{-1}$

$\Rightarrow W(v,z) = vz^{-2}$

or ii) $o(W) = 3$ unless W is a conjugate of $y = xz^{-1} = z^{-1}vz^{-2}$

$\Rightarrow W(v,z) = vz^{-3}$

and so if r is an irreducible factor of

i) $P(W)$

or ii) $P(W) \pm 1$

such that r is in category III as before, then the pair $(G(\partial r),r)$ determines a map of $\mathcal{M}_3^+(G(\partial r))$ with valency (i+2) for case i) and (i+3) for case ii). An obvious converse also holds.

To illustrate this by an explicit example, let $G(e) = PSL_2(7^e)$ for all natural e, let $W(v,z) = vz^4$ and ask for which $\mathcal{M} \in \bigcup_e \mathcal{M}_3^+(G(e))$ does $o(W) = 3$, i.e. $P(vz^4) = \pm 1$? From the preceding paragraph this is equivalent to finding which $\mathcal{M}$ has valency 7 (and so we are checking our current knowledge that there is just one such map given by $(PSL_2(7), t \pm 2)$).

Now

$$P(vz^4)+1 = -k^5-3k^3-3k+1 = -(k+2)^3(k^2+k-1)$$

$$P(vz^4)-1 = -k^5-3k^3-3k-1 = -(k-2)^3(k^2-k-1)$$

so the only irreducible polynomials r which are factors of $P(vz^4)\pm 1$ and for which $(G(\partial r),r)$ is a map of $\mathcal{M}_3^+(G(\partial r))$ are indeed

$$r(t) = t \pm 2$$

confirming the only map $\mathcal{M}$ is (G(1), $t \pm 2$).

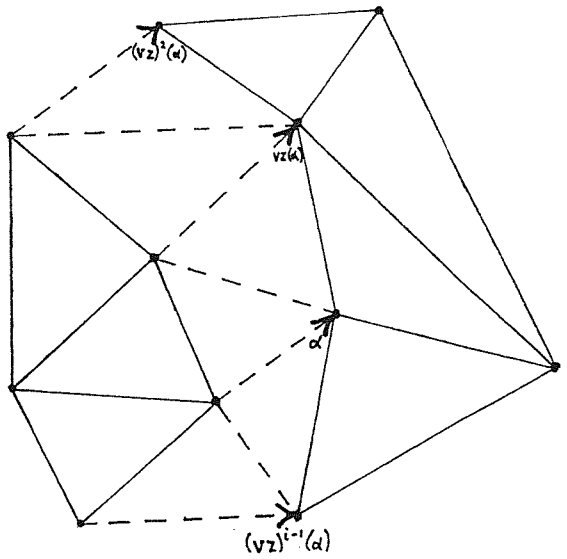
Example 3 The maps with least Petrie polygon length.

A Petrie polygon (P.p.) in any oriented map $\mathcal{M}$ (regular or not, and in spirit even oriented or not, though the algebra to model it in the unoriented case will be different) is a circuit in $\mathcal{M}$ whose path takes the basic zig-zag form. If $\mathcal{M}$ is triangular, then algebraically the P.p. through the dart α of $\mathcal{M}$ is the word W which is the least power i of (vz) such that

$$(vz)^i(\alpha) = \alpha .$$

I shall call 2i the length of the P.p. through α (2i rather than i because, to describe the zig-zag, the route that represents the P.p. is $(xz^{-1}xz)^i$: it is easy to check $xz^{-1}xz = vz$. Then remember that the length of a route is the number of x's it contains.)

For a crude pictorial idea, suppose the diagram below represents part of a triangular oriented map containing the dart α; then the P.p. through α 'follows' the dotted path.



For a regular map of course all the P.p.s will have the same length.

Now I return to ROΔMs $\mathcal{M}$ with automorphism type $PSL_2(q)$ for some $q > 3$. Then because we know there are no circuits W such that $\exp(W;v) < 3$, and all circuits W s.t. $\exp(W;v) = 3$ are conjugates to

$$vz^{-3}vz^{-3}vz^{-3}$$

we conclude that in all cases the P.p. length must be greater or equal to eight. I set myself the question: for which of these maps is the P.p. length exactly eight?

The even case (for q) is quickly dispensed with by the observation that $PSL_2(2^e)$ for any e does not contain elements of order four. So we may suppose $\mathcal{M} := (G,r)$ where $G \cong PSL_2(p^e)$ for some <u>odd</u> prime p, and r is a suitable irreducible polynomial of degree e over $\mathbb{Z}_p$. Then $\mathcal{M}$ has P.p. length 8 iff $(vz)^4 = I$ in G and the latter is so iff r divides P(vzvz).

Now by the table on p.155,

$$P(vzvz) = k^4 - 2k^2 - 1 .$$

We suppose that r (associated with $\mathcal{M}$) is a factor. Straightaway we see $\partial r < 4$, and further if P(vzvz) has a factor of the form (k-a) for some $a \in \mathbb{Z}_p \setminus \{0\}$, it is clear (k+a) is also a factor, so in fact $\partial r < 3$. I consider the two remaining possibilities for ∂r separately.

<u>Case 1</u> <u>$\partial r = 1$</u>

Suppose $r(k) = k-a$ for some $a \in \mathbb{Z}_p \setminus \{0\}$

Then $k^4-2k^2-1 = (k^2-a^2)(k^2+a^{-2})$

$$\Leftrightarrow \quad a^2 - a^{-2} = 2$$

$$\Leftrightarrow \quad a^4 - 2a^2 - 1 = 0$$

$$\Leftrightarrow \quad (a^2 - 1)^2 = 2$$

$$\Leftrightarrow \quad a = \pm\sqrt{\pm\sqrt{2} + 1}$$

In particular the square root of 2 exists in $\mathbb{Z}_p$, so necessarily $p \equiv \pm 1 \bmod 8$; but this is not sufficient to guarantee the existence of a, we also require square roots in $\mathbb{Z}_p$ of $(\sqrt{2} + 1)$ or $(-\sqrt{2} + 1)$, and it is more difficult to determine which primes p fit this constraint. I leave this particular problem as it stands except for the following observation:

$$(\sqrt{2} + 1)(-\sqrt{2} + 1) = -1$$

so if -1 is a square in $\mathbb{Z}_p$, and so $p \equiv 1 \bmod 8$, then both $(\sqrt{2} + 1)$ and $(-\sqrt{2} + 1)$ are squares or both are not: however if -1 is a non-square in $\mathbb{Z}_p$, and so $p \equiv -1 \bmod 8$, then exactly one of $(\sqrt{2} + 1)$ and $(-\sqrt{2} + 1)$ is a square.

Finally we need to check that given $p \equiv \pm 1 \bmod 8$, that the values of a do not assume in $\mathbb{Z}_p$ one of the 'forbidden' values ± 1, $\pm\sqrt{2}$, $\pm\sqrt{3}$ (if these exist), and that (k-a) is not a factor of either $(k^2 \pm k - 1)$. This is very easily done, and I leave it to the reader. (Another easy exercise would be to prove that 7 ~~and 23~~ is the only prime p such that the unique ROΔM with valency p and automorphism group $PSL_2(p)$ has P.p. length 8).

Case 2 $\partial r = 2$

Suppose $r(k) = k^2 + bk + c$ for some $b, c \in \mathbb{Z}_p \setminus \{0\}$.

Then $k^4 - 2k^2 - 1 = (k^2 + bk + c)(k^2 - bk - c^{-1})$

where $c-b^2-c^{-1} = -2$

and $b(c+c^{-1}) = 0$.

The last equation implies $c^2 = -1$, and so necessarily $p \equiv 1 \bmod 4$. Furthermore if we denote one root of -1 by $\sqrt{-1}$ we have

$$b^2 = 2.\sqrt{-1} + 2 \qquad \text{or} \qquad -2.\sqrt{-1} + 2$$

so we require at least one of these to be a square in $\mathbb{Z}_p$. But it is easy to check (by the quadratic formula) that if both are squares then r is reducible (and of course conversely); therefore we require exactly one to be a square. Now

$$(2.\sqrt{-1} + 2)\,(-2.\sqrt{-1} + 2) = 4 + 4 = 8$$

thus this product is a square iff 2 is a square in $\mathbb{Z}_p$, equivalently $p \equiv \pm 1 \bmod 8$. But in this case both $(2.\sqrt{-1} + 2)$ and $(-2.\sqrt{-1} + 2)$ are squares or both are non-squares. Thus we require $p \equiv \pm 3 \bmod 8$ (which guarantees exactly one of our proponents are square as desired), and as also $p \equiv 1 \bmod 4$, we conclude $p \equiv -3 \bmod 8$. Conversely given any such prime, r does exist as specified and

$$P(vzvz) = k^4-2k^2-1 = (k^2+bk+\sqrt{-1})(k^2-bk+\sqrt{-1})$$

so exactly one map is represented.

I now collect our results to present them as a

Theorem

Let $G \cong PSL_2(p^e)$ for any prime power p^e, and let $n(p^e)$ be the number of maps in $\mathcal{M}_3^+(G)$ for which the Petrie polygon length is eight. Then $n(p^e) = 0$ unless:

i) $p \equiv -3 \bmod 8$, $e = 2$ when $n(p^2) = 1$

ii) $p \equiv -1 \bmod 8$, $e = 1$ when $n(p) = 1$

iii) $p \equiv 1 \bmod 8$, $e = 1$ and $(\sqrt{2} + 1)$ is a square in $\mathbb{Z}_p$ when $n(p) = 2$. □

I end with examples to show that for primes $p \equiv 1 \bmod 8$, $(\sqrt{2} + 1)$ can indeed be either a square or a non-square in $\mathbb{Z}_p$. Let $\left(\frac{a}{p}\right)$ for $a \in \mathbb{Z}$ be the classical Legendre symbol.

1) p = 17

$$\sqrt{2} = 6 \Rightarrow (\sqrt{2} + 1) = 7$$

Now by quadratic reciprocity,

$$\left(\frac{7}{17}\right) = \left(\frac{3}{7}\right) = -\left(\frac{1}{3}\right) = -1$$

so $(\sqrt{2} + 1)$ is a non-square in $\mathbb{Z}_{17}$, and $n(17) = 0$.

2) p = 41

$$\sqrt{2} = 17 \Rightarrow (\sqrt{2} + 1) = 18$$

But $10^2 = 18$, so $(\sqrt{2} + 1)$ is square. Also

$$4^2 = 16 = (\sqrt{2} - 1) \Rightarrow \pm\sqrt{-\sqrt{2}+1} = \pm\sqrt{-1}.4 = \pm 9.4 = \pm 5$$

which means

$$P(vzvz) = (k-10)(k+10)(k-5)(k+5)$$

and both the maps $(PSL_2(41), t\text{-}10)$ and $(PSL_2(41), t\text{-}5)$ have Petrie polygon length eight.

CHAPTER FIVE

1. INTRODUCTION

In the previous chapter I had started to restrict my attention to ROΔMs, these being perhaps the most interesting subcategory $\mathcal{M}_3^+$ of all the oriented hypermaps. This specialisation is continued in the present chapter in which I consider some alternative ways for constructing some of the objects in $\mathcal{M}_3^+$ (where as normal we in fact only consider maps with automorphism group G isomorphic to $PSL_2(q)$ or $PGL_2(q)$ for some q: from now on, whenever I use the symbol $\mathcal{M}_3^+$, I in fact will mean just these particular ROΔMs. To stress this I will sometimes write 'restricted' $\mathcal{M}_3^+$).

The original impetus for the work presented here came from coming across in the existing literature [23] a description of some oriented triangular maps. These were strongly related to a rather narrow section of the groups $PSL_2(q)$ and $PGL_2(q)$ and looked likely to be ROΔMs though not presented as such. This motivated an attempt to form actual map isomorphisms between objects in $\mathcal{M}_3^+$ and these 'new' maps. This was successful, and the methods used clearly displayed that the range of application of the construction (of regular maps) is wider than that exploited by Surowski, and in fact involves all the groups $PSL_2(p)$, for some prime p and all the $PGL_2(q)$. (We shall see that maps can be constructed analogously for any other $PSL_2(q)$ for q odd, but this case never results in regular maps.)

Not to tantalise the reader further, I now state the type of construction involved:

Let G be $PSL_2(q)$ or $PGL_2(q)$ for some q, and let ℓ be a conjugacy class

of elements in G. (Let T denote the set of all such pairs (G, ℓ)). Then I define the graph $\Psi(G, \ell)$, abbreviated to Ψ when ambiguity is unlikely, as follows:

the vertex set $V(\Psi)$ is the set of elements in ℓ

the edge set $E(\Psi)$ is given exactly by those pairs $(u, v) \in \ell^2$ for which $o(uv^2) = o(vu^2) = 2$ in G.

Let S be the subset of T which consists of the pairs (G, ℓ) in T that satisfy one of

i) $G = PSL_2(p)$ for some prime p, and the elements of ℓ have order p in G.

ii) $G = PGL_2(q)$ for any q, and the elements of ℓ have order $(q \mp 1)$.

Then the main result of this chapter is that for all pairs (G, ℓ) in S, $\Psi(G, \ell)$ can be imbedded as a ROΔM with automorphism group G.

The reader may feel some consternation in that I have talked of constructing maps whereas the actual construction mentioned is for graphs. The resolution of this apparent anomaly is by introducing the concept of a vertex-transitive triangulation (VTT). As to what exactly a VTT is, I discuss more in the next section, but suffice it to say for the moment that a VTT is a graph with automorphism group transitive on its vertices and with a particularly simple local structure which guarantees it has a unique triangular imbedding (up to taking the mirror-image). Now I shall show in due course that all objects $\mathcal{M}$ of $\mathfrak{M}_3^+$ satisfy both

1) The underlying graph ⊕ of $\mathcal{M}$ is a VTT

2) $\mathcal{M}$ is isomorphic to its mirror-image (i.e. $\mathcal{M}$ is reflexible).

These two facts, taken together, are extremely useful in that if we have just a graph isomorphism between Θ and some other graph Θ' we know that any triangular imbedding of Θ' must in fact be isomorphic to $\mathcal{M}$. This saves having to construct map isomorphisms, which are more unwieldly to handle.

So, to press the point, if I can prove that any graph Θ' is isomorphic to the underlying graph of some $\mathcal{M} \in \mathfrak{M}_3^+$, I may in fact without ambiguity regard the graph Θ' as being isomorphic to the map $\mathcal{M}$.

The idea of VTT's is taken from Surowski's paper (ibid), though he didn't concern himself with regularity as such. Indeed the main purpose of that paper over and above the introduction of the concept itself is to demonstrate that a couple of given categories $\mathfrak{A}$ and $\mathfrak{B}$ of graphs are VTT's:

$\mathfrak{A}$ is the set of $\Psi(G,\ell)$ for the pairs $(G,\ell) \in S$ which satisfy $G = PGL_2(2^e)$ for any $e \geq 3$ and ℓ is any conjugacy class of elements of order 2^e-1 in G.

$\mathfrak{B}$ is the set of graphs $\Lambda(G,\ell)$ where $G = PSL_2(p)$ for any prime p satisfying $16 \mid (p^2-1)$, ℓ is a conjugacy class of elements of order p in G. The vertex set of Λ is ℓ and

$$(u,v) \in \ell^2 \text{ is an edge in } \Lambda \iff o(uv) = 2 \text{ in } G.$$

By considering the regularity of the graphs $\Psi(G, \ell)$ for all pairs (G,ℓ) in S, I will clearly greatly extend the category $\mathfrak{A}$ of VTTs. In the body of the chapter, I will also devote a section, §8, to show the VTT's $\Lambda(G,\ell)$

in $\mathfrak{B}$ are ROΔMs with automorphism group G as well, but in this case the definition for adjacency is more 'tailormade' for the particular types of pairs (G, ℓ) covered and we can't expect to extend this category in the same sort of way as with $\mathfrak{A}$.

Now before I can be more precise about how the isomorphisms needed are actually formed, I need to describe VTTs in more detail which I do in the coming section, §2, which starts with some preamble. After this, there is a short section §3 dealing with the question of reflexibility for the maps in $\mathfrak{M}_3^+$. In §4, then armed with the necessary ammunition, I describe how we proceed.

2. SOME BASIC PROPERTIES OF ROΔMs

(In this section $\mathcal{M}$ will always represent an ROΔM with arbitrary automorphism group G unless otherwise stated. Many of the comments here are of relevance for other categories of regular oriented hypermaps. It will involve, in the language of chapter 4, examining circuits in $\mathcal{M}$ of length less than or equal to three, and interpreting what these represent. It is the circuits of length 3 that are critically related to VTTs.)

Speaking naïvely, the regularity of the maps we are considering would suggest some simplicity in the graphical structure of their topological representations, but the availability of surfaces with genus as high a value as desired tends to counteract this. Here I examine some local (graph-theoretic) properties of $\mathcal{M}$, all of which are concerned with what could be regarded as aspects of basic good behaviour for graphs in general. Each property is translated into terms of relations in G involving a generating pair $(x,y) \in G^2$ which represents $\mathcal{M}$ in the usual way. As

usual, we let:

$$z := y^{-1}x$$

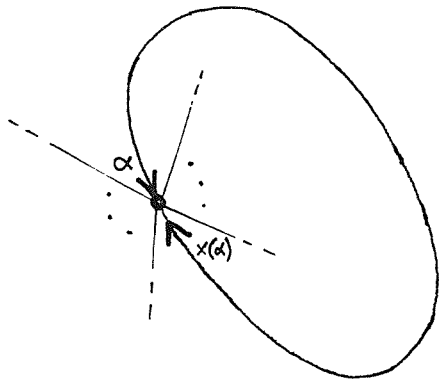
I) Free edges

As already explained in chapter 1 (p.18) $\mathcal{M}$ does not contain free edges unless

$$x = I$$

in which case $G = \langle x,y \rangle$ is cyclic.

II) Loops



We say that $\mathcal{M}$ has a loop if there is a dart α and an integer $i \neq 0$ such that

$$z^i x(\alpha) = \alpha \ .$$

The regularity of $\mathcal{M}$ gives that

$$z^i x = I$$

and so in G,

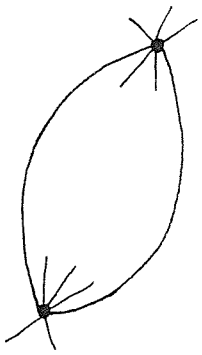
$$\langle x,z \rangle \text{ is cyclic} \ .$$

But $\langle x,y \rangle = \langle x,y^{-1}x \rangle = \langle x,z \rangle = G$.

So if the automorphism group G is not cyclic, $\mathcal{M}$ cannot contain any loops. □

Thus in all but a few very trivial cases, a ROΔM does not contain free edges or loops. Free edges and loops are very often not regarded as legitimate features of a graph, so this is useful. However there is a third type of local structure that can occur in an imbedding which would not normally be allowed in a graph:

III) Multiple Edges



$\mathcal{M}$ has multiple edges if

$$xz^i xz^j = I \qquad \text{for some } i,j \in \mathbb{Z}^+$$

$$\Rightarrow z^i xz^j = x$$

$$\Rightarrow z^i xz^{j+i} xz^j = I$$

$$\Rightarrow (z^{j+i} x)^2 = I$$

$\Rightarrow$ $\langle z^{j+i}, x \rangle$ is dihedral or cyclic in G .

Hence compared with free edges and loops it is harder to decide precisely which ROΔMs contain multiple edges and which are the types of automorphism group G that are thus represented. However for $G := PSL_2(q)$ or $PGL_2(q)$, any $q \geq 3$, suppose $xz^i xz^j = I$. Then $\langle z^{j+i}, x \rangle$ is dihedral or cyclic $\Rightarrow$ $\langle z,x \rangle$ is dihedral or cyclic unless $j = -i$. But

$$xz^i x = z^i$$

$\Rightarrow$ both $z,x \in N_G \langle z^i \rangle$, which is either dihedral or elementary abelian

$\Rightarrow$ $\langle x,z \rangle < G$ ⁂

Also for $q = 2$, the graph underlying the unique ROΔM with automorphism group $PSL_2(2) \cong D_6$ is just a straightforward triangle.

Thus none of the ROΔMs with $G \cong PSL_2(q)$ or $PGL_2(q)$ (for <u>any</u> q) can have multiple edges: this means the underlying graph of each map is in every way a bona-fide graph. □

To recap, we have shown that a certain $\mathcal{M}$ has no loops or free-edges by proving that

$$\forall i \in \mathbb{Z} \ , \qquad z^i x \neq I$$

and that it has no multiple edges by proving

$$\forall i,j \in \mathbb{Z} \ , \qquad z^i x z^j x \neq I \ .$$

We now go further and consider the solutions in G of

$$z^i x z^j x z^k x = I$$

as i,j,k vary independently over the integers.

Note that necessarily we always have

$$zxzxzx = z^{-1}xz^{-1}xz^{-1}x = I \ ,$$

these relations being nothing more than statements that $\mathcal{M}$ is triangular.

However how should we interpret other solutions? This question motivates the following:

IV) Non-simple spans

Definitions

The span $\Theta(v)$ of a vertex v in a graph Θ is the induced graph on the vertices adjacent to v in Θ .

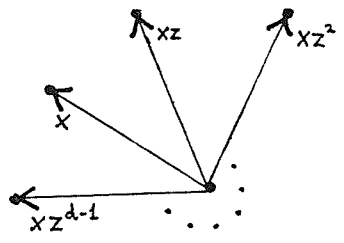
The span $\Theta(v)$ is simple if it is an ordinary n-gon for some positive integer n (where I regard a line-segment as a 2-gon and a point as a 1-gon). If a span is simple and n-gonal then I call it an n-span.

Now for an arbitrary graph, a non-simple span can take many forms: for example it need not be connected. But for the underlying graph Θ of a ROAM $\mathcal{M}$, the type of possible 'violation' causing non-simple spans is more particular:

Suppose Θ has constant valency d. Without loss of generality we may regard a vertex v in Θ as the following set of permutations of darts:

$$\{ I, z, z^2, \ldots , z^{d-1} \}$$

and the following permutations as representing the vertices adjacent to v in Θ : $x, xz, xz^2, \ldots, xz^{d-1}$.

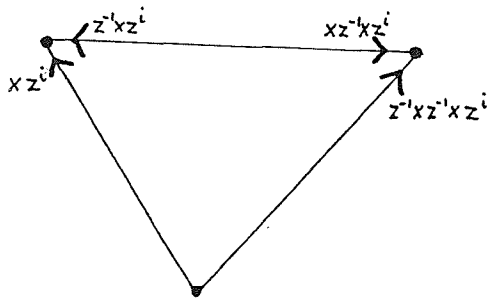


But clearly for each $i \in \{0, \ldots , d-1\}$,

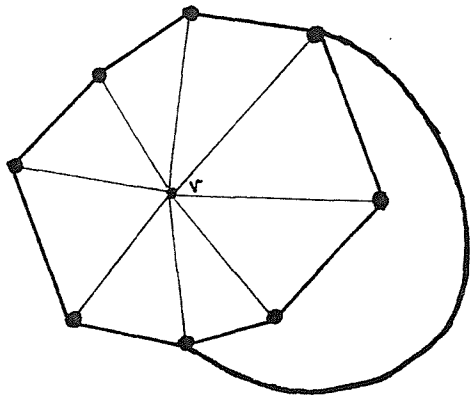
$$xz^i \text{ is adjacent to } xz^{i+1} \text{ in } \Theta$$

for

$$z^{-1}xz^{-1}xz^i = (xz)z^i = xz^{i+1} .$$



Thus the vertices of the span $\Theta(v)$ all lie in an ordinary d-gon in $\Theta(v)$: the only way in which $\Theta(v)$ can be non-simple given this is if an 'additional' edge exists between two of the adjacent vertices. So pictorially we would have this sort of situation:



where the bold vertices and edges form the span of v.

It is easy to see that such a construction occurs in Θ if and only if there exists $(i,j,k) \neq \pm(1,1,1) \in (\mathbb{Z}_d)^3$ such that in $G := \langle x,z \rangle$

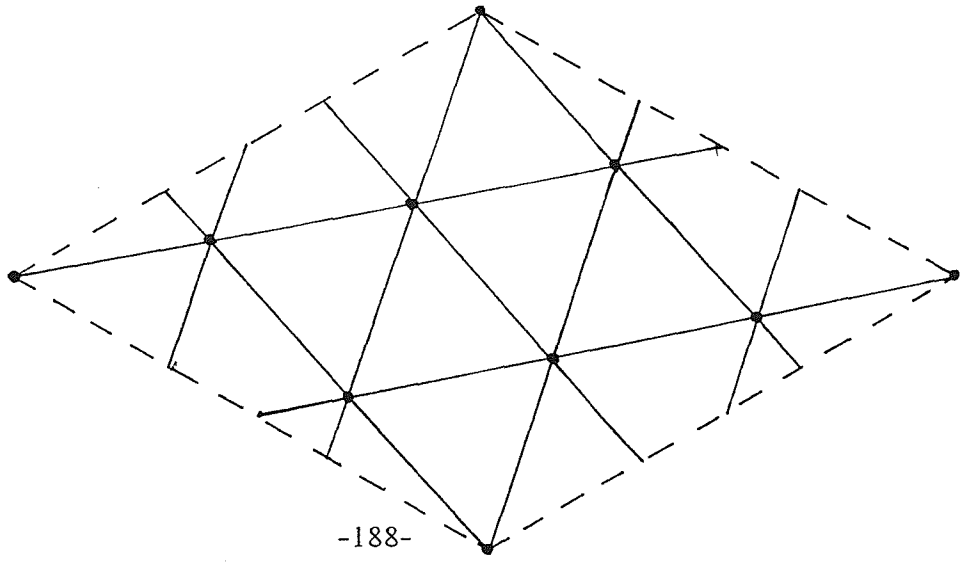
$$z^i x z^j x z^k x = I .$$

I will say that $\mathcal{M}$ has simple or non-simple spans according to whether such a triple (i,j,k) does not or does exist.

(Note that this means, from our previous discourse, that if $\mathcal{M}$ has free-edges, loops or multiple edges, then $\mathcal{M}$ has non-simple spans).

It is this description of spans that I've really been working towards. It interests me primarily in relation to a class of graphs, called vertex-transitive triangulations (VTTs), introduced in [23]. Roughly speaking, they are defined as finite, connected graphs with (simple) n-spans for some $n \geq 4$, with automorphism group transitive on the vertices (and finally with a technical condition to guarantee an orientable imbedding). Trivially, any ROΔM $\mathcal{M}$ is bound to satisfy all these conditions except perhaps that of the n-spans. In other words if $\mathcal{M}$ does have n-spans for some $n \geq 4$, then it is a VTT.

The condition $n \geq 4$ may seem a little artificial, but I adhere to it to be consistent with [23]. Note that the only ROΔM with 2-spans has underlying graph an ordinary triangle and automorphism group isomorphic to $D_6 \cong PSL_2(2)$ and the only ROΔM with 3-spans is a tetrahedron and has automorphism group $A^4 \cong PSL_2(3)$. In addition the term 'vertex-transitive triangulation', also adopted from [23], is perhaps a little unsatisfactory in that perfectly good triangulations exist which are vertex-transitive but certainly do not have simple spans. Consider for example the well-known regular imbedding of the complete graph K_7 in the torus:



Opposite sides of the parallelogram are identified in the usual way.

(Note that the complete graphs are in an obvious sense the graphs with the 'most complicated' spans. It may interest the reader that all regular orientable imbeddings of complete graphs have been analysed in [9].)

But we shall see in due course that the concept of a VTT has merit: the conditions imposed on a VTT clearly ensures a single triangular imbedding of the graph, and it is simply this property which will interest us.

I now show that all $\mathcal{M}$ with automorphism group $G : \cong PSL_2(q)$ or $PGL_2(q)$ (any $q > 3$) must have simple spans, and so are VTTs. I do this by proving the following:

Theorem

In algebraic map language (see p.10 ad.seq.) let

$$\mathcal{M} := (G, \Omega, x, y)$$

be a ROΔM with automorphism group $G : \cong PSL_2(q)$ or $PGL_2(q)$ for any $q > 3$. Also let $z = y^{-1}x$ and $o(z) = d$.

(Necessarily $d > 6$ except for $q = 5$ when there is only the one relevant map, this with $d = 5$; anyway $d \geqslant 4$. See p.129.)

The conclusion is that, in G,

$$z^i x z^j x z^k x = I \Rightarrow i \equiv j \equiv k \equiv \pm 1 \bmod d .$$

Proof

First note that

$$z^i x z^j = x z^{-1} x$$

$$\Rightarrow z^i x z^j = zxz$$

$$\Rightarrow x z^{i-1} x z^{j-1} = I$$

$\Rightarrow$ i = j = 1 (as we know $\mathcal{M}$ has no multiple edges).

Similarly

$$z^i x z^j = xzx$$

$\Rightarrow$ i = j = -1

This means we need only prove

$z^i x z^j x z^k x = I \Rightarrow$ any one of {i,j,k} is 1 or -1 .

We now 'split' the proof, partitioning the maps into 2 classes and considering each separately.

Class 1: those $\mathcal{M}$ with $G \cong PSL_2(p)$, d = p.

W.l.o.g. $x = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ $y = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ $z = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

Then

$$z^i x z^j = \begin{pmatrix} -i & -ij+1 \\ -1 & -j \end{pmatrix} \qquad xz^{-k}x = \begin{pmatrix} -1 & 0 \\ -k & -1 \end{pmatrix}$$

Thus $z^i x z^j x z^k x = I \Rightarrow i = \pm 1$.

Class 2: those $\mathcal{M}$ with i) $G \cong PSL_2(q)$ and $d \mid (q \mp 1)/2$

ii) $G \cong PGL_2(q)$ and $d \mid (q \mp 1)$.

Let α be a primitive element of $GF(q^2)$, the extension of GF(q).

W.l.o.g. we may take $z = \begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix}$

for some power β of α^{q+1} or α^{q-1} in $GF(q^2)$ (such that the order of β in the multiplicative group of $GF(q^2)$ is d).

Suppose $x = \begin{pmatrix} r & s \\ t & w \end{pmatrix}$ $\qquad rw - st = \gamma \in GF(q)$, $w = -r$.

Then

$$z^i x z^j = \begin{pmatrix} r\beta^{i+j} & s\beta^i \\ t\beta^j & w \end{pmatrix} \qquad \text{with determinant } \beta^{j+i}\gamma \ ,$$

$$xz^{-k}x = \begin{pmatrix} r^2\beta^{-k}+st & sr\beta^{-k}+sw \\ tr\beta^{-k}+tw & ts\beta^{-k}+w^2 \end{pmatrix} \qquad \text{with determinant } \beta^{-k}\gamma^2 .$$

Noting that β and γ are both squares in $GF(q^2)$, we have

$$z^i x z^j = xz^{-k}x$$

$$\Rightarrow \beta^{(i+j+k)/2}\gamma^{-1/2}\begin{pmatrix} r^2\beta^{-k}+st & sr\beta^{-k}+sw \\ tr\beta^{-k}+tw & ts\beta^{-k}+w^2 \end{pmatrix} = \begin{pmatrix} r\beta^{i+j} & s\beta^i \\ t\beta^j & w \end{pmatrix} .$$

If we multiply leading diagonals we get:

$$\beta^{(i+j+k)}\gamma^{-1}(r^2\beta^{-k}+st)(ts\beta^{-k}+w^2) = \beta^{i+j}rw$$

$$\Rightarrow \quad (r^2+st\beta^k)(ts\beta^{-k}+w^2) = \gamma rw$$

$$\left(\Rightarrow \quad (\beta^k+\beta^{-k}) = \frac{(2r^2+\gamma)}{r^2} \right) .$$

This last statement allows a maximum of two values for β^k: but we know β and β^{-1} must be solutions, and certainly $\beta \neq \beta^{-1}$. We conclude that k must be plus or minus one, as required. □

3 REFLEXIBILITY OF THE MAPS IN $\mathfrak{M}_3^+$

Given any map $\mathcal{M}$, the mirror-image $\bar{\mathcal{M}}$ of $\mathcal{M}$ is given by reversing the cyclic order of the 'darts' at each vertex. If $\bar{\mathcal{M}}$ is isomorphic to $\mathcal{M}$ as a map, then $\mathcal{M}$ is termed reflexible.

Specialising to $\mathcal{M} \in \mathfrak{M}_3^+$, we know from §2 that the underlying graph Θ of $\mathcal{M}$ is a VTT. If $\mathcal{M}$ is shown to be reflexible, then we know that $\mathcal{M}$ is the only triangular imbedding of Θ. Thus the significance of the

Theorem

All ROΔMs with corresponding map-subgroup $N \lhd \Gamma := C_2 * C_3$ such that $\Gamma/N \cong PSL_2(q)$ or $PGL_2(q)$ (any q) are reflexible. (Remember that the quotient group Γ/N 'gives' the automorphism group of the map, see p. 13-15, so this applies exactly to those maps in our restricted category $\mathfrak{M}_3^+$).

Proof

Let $\Gamma := gp\ \langle X,Y : X^2 = Y^3 = I \rangle$

and let $Z = Y^{-1}X$.

In general, if a ROΔM $\mathcal{M}$ has the map-subgroup $M \lhd \Gamma$ which is the kernel of the epimorphism $\rho : \Gamma \to \mathrm{Aut}\,\mathcal{M}$, then $\bar{\mathcal{M}}$ has the map-subgroup $\bar{M}$, given by the kernel of the following epimorphism $\bar{\rho} : \Gamma \to \mathrm{Aut}\,\mathcal{M}$:

$$\bar{\rho}(X) = \rho(X) \quad , \quad \bar{\rho}(Z) = [\rho(Z)]^{-1}.$$

Let $\rho(X) = x, \rho(Z) = z$. Then

$$\bar{\rho}(X) = x \quad , \quad \bar{\rho}(Z) = z^{-1}.$$

Now take our more particular case M = N, where N is as in the statement of the theorem. Fix the value of q for which $\Gamma/N \cong PSL_2(q)$ or $PGL_2(q)$ and let

$$G := PSL_2(q) \quad , \quad G' := PGL_2(q) \ .$$

Then we may regard Aut $\mathcal{M}$ as being equal to G or G', in particular regard x and z as elements of G'.

Let C_x ,C_z denote the maximal cyclic subgroups of G' containing x and z respectively. Then we have already intimated in a previous problem (p.115) that

$$D_x \cap D_z \cong C_2$$

where D_x,D_z are the maximal dihedral subgroups of G' containing C_x,C_z respectively, except in the case of q being a power of 2 where D_x is the maximal abelian subgroup (of type V_q) containing x. This immediately tells us (as is also proved in lemma 2.8 of [8])that there is an involution x' in G' such that

$$x'x(x')^{-1} = x \qquad \text{and} \qquad x'z^{-1}(x')^{-1} = z$$

which means that $\ker\rho = \ker\bar{\rho}$, i.e. M = $\bar{M}$ and $\mathcal{M} = \bar{\mathcal{M}}$.

4. THE SCHEME OF THE APPROACH LEADING TO THE MAIN RESULT

I now give an explanation of the two stages I shall use in the sections §5 and §6 to construct the desired graph isomorphisms between underlying graphs of the maps in $\mathfrak{M}_3^+$ and the appropriate $\Psi(G,\ell)$, as proposed in §1. Without this overview, the 'drift' of the more technical parts reserved to §5 and §6 might seem obscure.

The first step (§5) is to construct a category R' of maps according to

the following ethos:

Given $\mathcal{M} \in \mathfrak{M}_3^+$, the darts of $\mathcal{M}$ may be regarded as the elements of $G := \mathrm{Aut}(\mathcal{M})$ and the vertices as the cycles in G induced by $z \in G$ when z is multiplied on the left (z is as usual, and is identified up to a conjugacy class in G under $PGL_2(q)$). So typically the set S_v of darts comprising a vertex v will be of the form

$$S_v = \{ g, zg, z^2g, \ldots, z^{d-1}g \}$$

for some $g \in G$, and with $d := o(z)$ in G.

Now let Θ be the underlying graph of $\mathcal{M}$: to give a description of Θ in more standard graphical terms we need to express each dart as an ordered pair of vertices (u,v), in particular this expression for each of the darts in S_v must have the same 'incoming' component v. But there is an obvious way to derive a constant entity from each of the elements of S_v by taking conjugates of z:

$$\forall s \in S_v \ , \qquad s^{-1}zs = g^{-1}zg \ .$$

This begs the question can one, given $\mathcal{M}$, identify the conjugates of z with the vertices of Θ and further construct a graph Θ' isomorphic to Θ by taking the vertex set of Θ' as the elements of the conjugacy class of G containing z and defining adjacency in Θ' in some 'natural' way? If the answer is yes, we may regard Θ' as a VTT, which then has only a mirror-image pair of triangular imeddings: one of these imbeddings is $\mathcal{M}$, which is reflexible, so in fact $\mathcal{M}$ is the only triangular imbedding and in this sense we may regard

$$\Theta' \cong \mathcal{M} \ .$$

In §5 therefore I determine which $\mathcal{M} \in \mathfrak{M}_3^+$ can be recovered in this

sort of way, and call the set of them R'. (What the 'natural' rule of adjacency should be is easy to see, though to write down it is a little technical: I shall leave the statement of it to §5.)

To give a convenient way of describing R', I now introduce the class-triple (G, ℓ,d) associated with each $\mathcal{M} \in \mathfrak{M}_3^+$, where G is the automorphism group type of $\mathcal{M}$, ℓ is the conjugacy class of G containing any z as appropriate to $\mathcal{M}$, and d is the order of z.

Then (we shall see) R' is given exactly by those $\mathcal{M} \in \mathfrak{M}_3^+$ with class-triple (G, ℓ,d) satisfying one of

i) $G = PSL_2(p)$ for any prime p and $d = p$

ii) a) $G = PSL_2(q)$, q odd, and $d = \frac{1}{2}(q \mp 1)$

b) $G = PGL_2(q)$, any q, and $d = (q \mp 1)$.

Now let R be the subset of R' given by those $\mathcal{M} \in \mathfrak{M}_3^+$ satisfying one of just i) or ii) b) as above. Then in section §6 we make use of the newly formed graph $\mathcal{H}'$ by proving that if $\mathcal{M} \in$ R' has class-triple (G, ℓ,d), then the graphs $\mathcal{H}'$ and $\Psi(G, \ell)$ are equal iff further $\mathcal{M} \in$ R.

Hence through the medium of $\mathcal{H}'$ we conclude that for $\mathcal{M} \in$ R

$$\mathcal{H} \cong \Psi(G, \ell) .$$

Remembering again that an isomorphism of VTTs may be regarded as an isomorphism of triangulations, we arrive at the major result of the chapter already mentioned in §1.

Theorem

$\forall (G, \ell) \in S$, $\Psi(G, \ell)$ has a unique imbedding as a triangulation, and this is a ROΔM with automorphism group G.

(In the final section, §9, I review the whole procedure by considering what conditions we need to impose on a pair (G, ℓ) now with G an arbitrary finite group (and $\Psi(G, \ell)$ defined analogously) to be able to come to the same conclusion as in the theorem for $\Psi(G, \ell)$ in general.)

5. ISOMORPHISM BETWEEN Θ AND Θ'

Before we start, please note that I will adopt the convention that

$$\forall g \in G , \quad z^g = g^{-1}zg \ .$$

Let $\mathcal{M}$ be any map in $\mathfrak{M}_3^+$, and suppose that $\mathcal{M}$ has class-triple (G, ℓ, d).

I define two graphs connected with $\mathcal{M}$:

i) Θ (the underlying graph of $\mathcal{M}$)

The vertices $V(\Theta)$ of Θ are the following subsets of G (which partition G):

$$v_g = \{g, zg, z^2g, \ldots, z^{d-1}g\} \qquad \text{for some } g \in G \ .$$

If $h \notin v_g$, then $v_h \neq v_g$ and (v_h, v_g) is an edge in Θ (i.e. is an element of $E(\Theta)$) iff $\exists$ i,j $\in \mathbb{Z}$ mod d s.t.

$$xz^jh = z^{-i}g \ .$$

(Notice that $z^ixz^jhg^{-1} = I \Rightarrow z^{-j}xz^{-i}gh^{-1} = I$, so we have the required symmetry for the edge set).

ii) Θ'

The vertices $V(\Theta')$ of Θ' are the elements of ℓ.

The edges $E(\Theta')$ of Θ' are those pairs $(u',v') \in \ell^2$ which satisfy:

$$\forall h,g \in G \text{ s.t. } u' = z^h \text{ and } v' = z^g, \exists\, i,j \in \mathbb{Z} \bmod d \text{ s.t. } z^i x z^j h g^{-1} = I .$$

(So again we have symmetry for the edge set).

I now make a couple of remarks about the graph Θ' :

Remark 1

$E(\Theta')$ is empty if $\langle z \rangle \neq \langle a \rangle$ where a is a generator of the maximal cyclic group containing z in G. For let $z = a^r$, and $h,g \in G$. Then

$$(z^h, z^g) \in E(\Theta') \Rightarrow z^i x z^j h g^{-1} = I \quad \text{for some } i,j$$

$$\Downarrow$$

$$(z^{ah}, z^{ag}) \in E(\Theta') \Rightarrow z^k x z^\ell a h g^{-1} a^{-1} = I \quad \text{for some } k,\ell$$

Thus

$$z^i x z^j = a^{-1} z^k x z^\ell a$$

$$\Rightarrow a^{ir} x a^{jr} = a^{kr-1} x a^{\ell r+1}$$

$$\Rightarrow x a^{r(i-k)+1} x a^{r(j-\ell)-1} = I .$$

But certainly, as $\langle x,z \rangle = G$ we also have $\langle x,a \rangle = G$ and by the same reasoning by which we concluded that $\mathcal{M}$ has no multiple edges, see p. 184, we have immediately

$$a^{r(i-k)+1} = a^{r(j-\ell)-1} = I$$

$$\Rightarrow r(j-\ell) \equiv 1 \bmod d' \qquad \text{where } d' := o(a)$$

$$\Rightarrow r \text{ is coprime to } d'$$

$$\Rightarrow \langle z \rangle = \langle a \rangle \quad \text{※}$$

Remark 2

If $\langle z \rangle = \langle a \rangle$, the quantifier $\forall$ in the definition of $E(\Theta')$ may be replaced by the quantifier $\exists$. For suppose $(u',v') \in E(\Theta')$.

Then $\exists\, h,g \in G$ s.t. $u' = z^h$, $v' = z^g$ and $z^i x z^j h g^{-1} = I$ for some i,j .

Suppose also h', g' $\in$ G are s.t. $u' = z^{h'}$, $v' = z^{g'}$.

Now $z^{h'} = z^h \Rightarrow z^{h'h^{-1}} = z$

$\Rightarrow h'h^{-1} = z^k$ for some k .

(The only case for which the last implication perhaps needs a word of justification is when o(z) = p; then the centraliser $C_G(z)$ of z in G is of elementary abelian type V_q. But $\langle x,z \rangle$ must generate G, which implies that in fact q = p, and so $C_G(z)$ is indeed cyclic.)

So we have $h' = z^k h$. Similarly $g' = z^\ell g$ for some ℓ.

Thus

$$h'(g')^{-1} = z^k h g^{-1} z^{-\ell} = z^{k-j} x z^{-i-\ell}.$$

□

Now remark 1 tells us that unless z generates a maximal cyclic subgroup of G then Θ' is just a set of unconnected vertices: this does not interest us. So we restrict our attention to those maps $\mathcal{M}$ for which the associated class-triple (G, ℓ, d) satisfies one of:

i) $G = PSL_2(p)$ for any prime p and $d = p$

ii) a) $G = PSL_2(q)$, q odd, and $d = \frac{1}{2}(q \mp 1)$

b) $G = PGL_2(q)$, any q, and $d = (q \mp 1)$

I term the set of such $\mathcal{M}$ the category R' of ROΔMs.

I now prove that for any $\mathcal{M} \in R'$, its two associated graphs Θ and Θ' are isomorphic.

Define the functions $\alpha: V(\Theta) \to V(\Theta')$ and $\beta: E(\Theta) \to E(\Theta')$ by

$$\alpha: v_g \mapsto z^g \qquad \forall g \in G$$

$$\beta: (v_h, v_g) \mapsto (z^h, z^g) \qquad \forall (v_h, v_g) \in E(\Theta).$$

Now α clearly is well-defined and onto. But

$$|V(\Theta)| = |G|/d$$

$$|V(\Theta')| = |\ell| = |G|/d \qquad (\text{as } C_G(z) = \langle z \rangle).$$

Thus α is a bijection.

Also β is well-defined (by remark 2) and is one-to-one (as α is). Clearly β is onto, and so β is a bijection as well.

Thus α (and β) provide a graph ismorphism between Θ and Θ'.

6. THE EQUALITY OF Θ' AND $\Psi(G,\ell)$

Taking up the situation at the end of §5, if we let $\mathcal{M}$ be a map in R' with associated class-triple (G, ℓ, d) then we have defined for $\mathcal{M}$ a graph Θ' isomorphic to the underlying graph of $\mathcal{M}$.

For the same G and ℓ, I define the graph $\Psi(G,\ell) = \Psi$ by

$$V(\Psi) = \ell$$

$$E(\Psi) = \{(u,v) \in \ell^2 : o(uv^2) = o(vu^2) = 2\}.$$

Then Θ' and Ψ have the same vertex set. We show that

$\Theta' = \Psi$

in the following two cases:

i) $G = PSL_2(p)$, $d = p$

ii) $G = PGL_2(q)$, $d = (q \mp 1)$

We do this by proving:

Theorem

Let (G, ℓ, d) satisfy i) or ii) as above. Let $(u,v) \in \ell^2$.

Then (u,v) is an edge in Θ' if and only if (u,v) is an edge in Ψ.

Proof

$(u,v) \in E(\Theta') \Rightarrow u = z^h$, $v = z^g$ for some $h,g \in G$ s.t.

$$z^i x z^j h g^{-1} = I \quad \text{for some } i,j \in \mathbb{Z} \bmod d$$

$$\Rightarrow uv^2 = h^{-1} z h g^{-1} z^2 g = h^{-1}(z h g^{-1} z^2 g h^{-1})h$$

$$= h^{-1}(z^{1-j} x z^2 x z^j)h$$

$$= (z^j h)^{-1}(z x z^2 x)(z^j h)$$

But $zxz^2x = yxy^{-1}$, so

$$uv^2 = (y^{-1} z^j h)^{-1}(x)(y^{-1} z^j h)$$

$$\Rightarrow o(uv^2) = o(x) = 2$$

Exactly analogously, $o(vu^2) = 2$, and hence $(u,v) \in E(\Psi)$.

Now the valency of the vertices of Θ' is d, and so all we need do to prove the inverse implication is to show that there are at most d vertices adjacent to any vertex in Ψ, in other words given any element

v of $\mathfrak{l}$ show that there exist at most d elements u of $\mathfrak{l}$ such that

$$o(uv^2) = 2 .$$

Clearly though, by conjugacy considerations in $\mathfrak{l}$, the graph Ψ has constant valency, so it suffices just to consider one particular v in $\mathfrak{l}$.

I split the remainder of the proof into the two cases i) and ii).

i) $G = PSL_2(p)$ for some prime p and $d = p$.

There are exactly two conjugacy classes, $\mathfrak{l}$ and $\mathfrak{l}'$ say, of elements of order p in G, so strictly we have two graphs

$$\Psi := \Psi(G, \mathfrak{l}) \qquad \Psi' := \Psi(G, \mathfrak{l}')$$

to consider.

However <u>all</u> the elements of G of order p are conjugate under $PGL_2(p)$: by conjugating the vertices of Ψ by an element of $PGL_2(p)\backslash PSL_2(p)$ we obviously have a graph ismorphism giving $\Psi \cong \Psi'$.

Thus we need only examine one of the graphs, take Ψ, and without loss of generality we may let

$$v := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

be an element of $\mathfrak{l}$.

Let $u = \begin{pmatrix} r & s \\ t & w \end{pmatrix}$ be any element of $\mathfrak{l} < G$; this means

1) $rw - st = 1$

2) $r + w = \pm 2$.

We calculate

$$uv^2 = \begin{pmatrix} r & 2r+s \\ t & 2t+w \end{pmatrix}$$

Thus $o(uv^2) = 2$ puts a third condition on u:

3) $r + 2t + w = 0$.

Trivially, if we set $r + w = -2$ in equation 2), we deduce from 1), 2) and 3) that u must be of the form (for some $r \in GF(p)$):

$$u = \begin{pmatrix} r & -r^2-2r-1 \\ 1 & -2-r \end{pmatrix}$$

Similarly, if we set $r + w = 2$ in equation 2), u must have the form:

$$u = \begin{pmatrix} r & r^2-2r+1 \\ -1 & 2-r \end{pmatrix} = \begin{pmatrix} -(-r) & (-r)^2+2(-r)+1 \\ -1 & 2+(-r) \end{pmatrix}$$

But as $\pm I$ are identified in G, u as above has already been accounted for.

Thus there are at most $|GF(p)| = p = d$ elements u of ℓ for which $o(uv^2) = 2$.

ii) $G = PGL_2(q)$, q odd, $d = (q \mp 1)$.

Let α be a primitive element of $GF(q^2)$, the field extension of GF(q). Without loss of generality we may assume that the following element v of $PGL_2(q^2)$ represents ℓ :

$$v = \begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix}$$

(where $\beta = \alpha^k$ and $k = (q+1),(q-1)$ respectively as $d = (q-1), (q+1)$).

Let $u = \begin{pmatrix} r & s \\ t & w \end{pmatrix}$ with 1) $rw - st = \beta$ be another element of ℓ, so in fact

2) $\quad r + w = \pm(\beta + 1)$.

Note that if $d|(q-1)$, we require the components $\{ r, s, t, w \}$ of u to lie in $GF(q) < GF(q^2)$. However if $d|(q+1)$ we require:

$$w = r^q \beta \qquad \text{and} \qquad t = -s^q \beta .$$

Now, $\quad uv^2 = \begin{pmatrix} r\beta^2 & s \\ t\beta^2 & w \end{pmatrix}$ with determinant β^3

so demanding that $o(uv^2) = 2$ imposes the condition

3) $\quad r\beta^2 + w = 0$.

As in the case i) we may take just one sign in the RHS of 2):

$$r + w = \beta + 1$$

Then solving the system of equations 1), 2) and 3) we get

$$r = \frac{1}{\beta - 1} \quad , w = \frac{-\beta^2}{\beta - 1} \quad , \quad st = \frac{-\beta(\beta^2 - \beta + 1)}{(\beta - 1)^2}$$

(It is easy to check that if $d|(q+1)$ then $w = r^q \beta$)

and we conclude that the number of elements u of ℓ such that $o(uv^2) = 2$ is given by the number of solutions for (s, t) above: clearly this is at most d (as required) as long as

$$\beta^2 - \beta + 1 \neq 0 .$$

So I set out to prove the last statement, by contradiction.

Suppose $\beta^2 - \beta + 1 = 0$.

Then $\beta(1-\beta) = 1$

$\Rightarrow \begin{pmatrix} \beta & 0 \\ 0 & 1-\beta \end{pmatrix} \in PSL_2(q)$ and has order 3 (as its trace is 1)

$\Rightarrow \beta^3 = -1$

$\Rightarrow d = q \mp 1 = 6$

$\Rightarrow q = 7$ or 5 .

But we know (p.105) that there are no ROΔMs $\mathcal{M}$ with automorphism group $G = PGL_2(5)$.

Also there exist exactly two ROΔMs $\mathcal{M}$ with $G = PGL_2(7)$, and it can be shown that for both of these that $d = 8$.

Thus, whatever our initial $\mathcal{M}$, a contradiction is acquired. □

Now we have available the graph Θ' isomorphic to the underlying graph of $\mathcal{M} \in \mathfrak{M}_3^+$ with class-triple (G, ℓ, d) (as described in §5) for the case

$$G = PSL_2(q) \quad \text{and} \quad d = \tfrac{1}{2}(q \mp 1)$$

as well as those cases dealt with in the preceding theorem. But in contrast to that theorem, in this instance

$$\Theta' \nmid \Psi(G, \ell) .$$

This will become evident in the next section, in which I consider $\Psi(G, \ell)$ for the remaining $(G, \ell) \in T$.

7. THE GRAPHS $\Psi(G,\ell)$ FOR $(G,\ell) \in T \setminus S$

I remind the reader that

$$T := \{(G,\ell) : G = PSL_2(q) \text{ or } PGL_2(q) \text{ for some } q, \text{ and } \ell \text{ is a conjugacy class in } G\}.$$

For given (G,ℓ) in T, the graph $\Psi(G,\ell) := \Psi$ is given by

$$V(\Psi) = \ell$$

$$E(\Psi) = \{(u,v) \in \ell^2 : o(uv^2) = o(vu^2) = 2 \text{ in } G\}.$$

Also for given (G,ℓ), and supposing G is defined over the finite field GF(q) where $q = p^e$, let

$$G' := PGL_2(q).$$

Then we may regard $G \leq G'$.

We may readily check that the subset S of T defined earlier is alternatively expressed as

$$S := \{(G,\ell) : \text{each element of } \ell \text{ generates a maximal abelian subgroup in } G'\}.$$

We know from the work to date that for all pairs (G,ℓ) in S, $\Psi(G,\ell)$ is a VTT (and further may be regarded as a ROΔM). What can we say for $\Psi(G,\ell)$ when $(G,\ell) \in T \setminus S$?

So fix $(G,\ell) \in T \setminus S$ and let $v \in \ell$.

Suppose that $o(v) = p$. Then analogously to case i) in the proof of the theorem in §6, we may take

$$v := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and then the elements of u of ℓ such that $o(uv^2) = 2$ are given exactly by the matrices of form

$$u = \begin{pmatrix} r & -(r+1)^2 \\ 1 & -2-r \end{pmatrix}$$

where r is any element of GF(q).

Now

$$u^2 = \begin{pmatrix} -2r-1 & 2(r+1)^2 \\ -2 & 2r+3 \end{pmatrix}$$

from which it is easy to check that $o(vu^2) = 2$.

Thus, whatever the value of r, (u,v) is an edge in Ψ : we concude that Ψ has constant valency q.

Now given u adjacent to v, which $u' \in \ell$ are adjacent to both u and v? Let

$$u' = \begin{pmatrix} s & -(s+1)^2 \\ 1 & -2-s \end{pmatrix}$$

for some $s \in GF(q)$.

Then we calculate

$$tr(u'u^2) = 2(s-r)^2 - 2$$

and so u' adjacent to u implies

$$(s-r)^2 - 1 = 0$$

$$\Rightarrow \quad s = r \pm 1 .$$

This means that the subgraph of Ψ induced by the set of vertices adjacent to v, i.e. the span of v, is a collection of p^{e-1} mutually unconnected p-gons. The same comment, by conjugacy, is evidently true for any vertex v of Ψ. Now $(G, \ell) \notin S$ implies $e > 1$, and so Ψ is not a VTT and furthermore cannot be imbedded as a ROΔM.

Suppose now that $d := o(v)$ divides $(q \mp 1)$ (I take just the case $d > 2$). Let C_v be the maximal cyclic subgroup of G' containing v: this will be of order $(q \mp 1)$. Let $a \in G'$ be a generator of C_v.

Now, analogous to case ii) in the proof of the theorem in §6, we may take

$$v := \begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix}$$

where β is the appropriate field element of $GF(q^2)$ with multiplicative order d.

Then all adjacent $u \in \ell$ must have the form

$$u = \begin{pmatrix} (\beta-1)^{-1} & s \\ t & -\beta^2(\beta-1)^{-1} \end{pmatrix}$$

where $st = -\dfrac{\beta(\beta^2-\beta+1)}{(\beta-1)^2}$.

Conversely, all matrices of the said form must represent adjacent vertices in Ψ : it is easily verified that $o(vu^2) = 2$. The only point that needs a little justification is that when $d \mid (q+1)$, we require $t = -s^q\beta$ and so we must have the equation

$$s^{q+1} = \frac{\beta^2-\beta+1}{(\beta-1)^2}$$

having roots for s.

To check that the roots exist we need simply show

$$\left[\frac{\beta^2-\beta+1}{(\beta-1)^2}\right]^{q-1} = I$$

in the multiplicative group $GF(q^2)$.

Now $\beta = \alpha^{i(q-1)}$ for some $i \in \mathbb{N}$, where α is a primitive element of $GF(q^2)$.

Thus

$$\beta^q = \alpha^{i(q^2-q)} = \alpha^{i(1-q)} = \alpha^{-i(q-1)} = \beta^{-1}.$$

So

$$\left[\frac{\beta^2-\beta+1}{(\beta-1)^2}\right]^q = \frac{\beta^{2q}-\beta^q+1}{(\beta^q-1)^2} = \frac{\beta^{-2}-\beta^{-1}+1}{(\beta^{-1}-1)^2}$$

$$= \frac{\beta^2-\beta+1}{(\beta-1)^2} \quad \text{as required.}$$

Thus as long as $d \neq 6$ (and so $(\beta^2-\beta+1 \neq 0)$, Ψ has the constant valency of $q \mp 1$. It is easily ascertained now that if u is one of the vertices adjacent to v, then the set A of all vertices adjacent to v is given by

$$A = \{ a^{-i}ua^i : i = 0,1,\ldots,q \mp 1 \}.$$

So if g is an element of G for which

$$u = g^{-1}vg$$

we have in fact

$$A = \{ a^{-i}g^{-1}vga^i : i = 0,1,\ldots,q \mp 1 \}.$$

Fix $\quad w_1 = a^{-i}g^{-1}vga^i \qquad$ for some $i \in \{0,1,\ldots,q \mp 1\}$

$\quad w_2 = va^{-i}g^{-1}vga^iv^{-1}$.

Then $\quad w_1w_2^2 = a^{-i}g^{-1}vgvg^{-1}v^2ga^iv^{-1}$

which is conjugate in G to

$$v^{-1}g^{-1}vgv^{\pm 1}g^{-1}v^2g \ .$$

But u being adjacent to v in Ψ implies

$$o(vg^{-1}v^2g) = 2$$

$$\Rightarrow \quad vg^{-1}v^2g = g^{-1}v^{-2}gv^{-1}$$

$$\Rightarrow \quad v^{-1}g^{-1}vgv^{\pm 1}g^{-1}v^2g = v^{-1}g^{-1}v^{-1}gv^{-1}$$

and the latter is conjugate to

$$v^{-2}g^{-1}v^{-1}g \ .$$

Thus (again as u is adjacent to v)

$$o(w_1w_2^2) = o(g^{-1}vgv^2) = 2$$

and so w_1 is adjacent to w_2 in Ψ.

This evidently means that the span of v in Ψ contains $(q \mp 1)/d$ polygons with d sides (such that each vertex in the span is contained in exactly one of these polygons). As $(G, \ell) \notin S$, we know that d is a proper divisor of $q \mp 1$, and so we may (again) conclude that Ψ is not a VTT and cannot be imbedded as a ROΔM.

8. TO CONSIDER THE CATEGORY $\mathfrak{B}$ OF VTTs IN RELATION TO $\mathfrak{R}$

Let Λ be a graph in $\mathfrak{B}$. Then there is a prime p with $16|(p^2-1)$ such that $G := PSL_2(p)$, ℓ is a conjugacy class of elements of order p in G and

$$V(\Lambda) = \ell$$

$$E(\Lambda) = \{ (u,v) \in \ell^2 : o(uv) = 2\}.$$

Now in $\mathfrak{R}$ there is exactly one map $\mathcal{M}$ for which the associated graph Ψ has ℓ as the vertex set. However the edge set $E(\Psi)$ is

$$E(\Psi) = \{(u,v) \in \ell^2 : o(uv^2) = 2\}$$

so evidently $\Lambda \neq \Psi$.

However I use this section to demonstrate that Λ is <u>isomorphic</u> as a graph to Ψ, and so (as VTT's) we may regard Λ and Ψ as representing the same map $\mathcal{M}$.

Now it is clear that both the graph Ψ and the graph Λ formed from one conjugacy class of elements of order p in $G = PSL_2(p)$ is isomorphic to the respective analogous graphs formed from the other conjugacy class of elements of order p. Thus we may without loss of generality choose ℓ to be conjugacy class containing the element z of G, where

$$z := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Let x be an involution in G such that

$$\langle x,z \rangle = G \qquad \text{and} \qquad o(xz^{-1}) = 3 .$$

Such an element always exists in G.

I now construct another generating pair of G.

The relevance of the condition $16 \mid (p^2-1)$ is that it guarantees (by the quadratic reciprocity theorem) that square roots of two exist in GF(q), one of which I shall denote by $\sqrt{2}$ (the other is then $-\sqrt{2}$). This means that G contains the involution χ where

$$\chi = \begin{pmatrix} 0 & \sqrt{2}^{-1} \\ -\sqrt{2} & 0 \end{pmatrix}$$

Also, letting $i := \sqrt{2}^{-1}$ we have

$$z^{-i} = \begin{pmatrix} 1 & -\sqrt{2}^{-1} \\ 0 & 1 \end{pmatrix}$$

and of course

$$o(z^{-i}) = o(z) = p .$$

Now, taking the matrix product,

$$\chi z^{-i} = \begin{pmatrix} 0 & \sqrt{2}^{-1} \\ -\sqrt{2} & 1 \end{pmatrix}$$

$$\Rightarrow \quad tr(\chi z^{-i}) = 1$$

$$\Rightarrow \quad o(\chi z^{i}) = 3 .$$

Thus (using the terminology of part 2 of chapter 3) both the G-triples (x, xz^{-1}, z^{-1}) and $(\chi, \chi z^{-i}, z^{-i})$ have associated to them the same trace-triple (0, 1, 2), and by a result in chapter 3 (p.120) we conclude

$$\exists\ c \in PGL_2(p) \text{ s.t.}$$

$$c^{-1}xc = \chi$$

and $$c^{-1}zc = z^{i} .$$

I now define the function $f : G \to G$,

$$\forall g \in G, \qquad f(g) \mapsto c^{-1}gc$$

and from this I form the function $\alpha : \ell \to \ell$ given by

$$\forall g \in G, \qquad \alpha : z^g \mapsto z^{f(g)}.$$

(Note that $\forall j \in \mathbb{Z} \bmod p$,

$$f(z^i g) = z^{ji} f(g)$$
$$\Rightarrow \alpha : z^{z^j g} \mapsto z^{f(g)}$$

and so α is well-defined).

I will show that α provides us with a graph isomorphism between Ψ and Λ.

Firstly, from the trivial observation that $c^{-1}gc$ takes every value in G as g is varied through G, we see that α is onto. Also, for a reason similar to that showing α is well-defined, α is clearly one-to-one. It remains to check that the induced function

$$\beta : E(\Psi) \to \ell^2 \text{ given by } \forall (z^h, z^g) \in E(\Psi),$$

$$\beta(z^h, z^g) \mapsto (\alpha(z^h), \alpha(z^g)) = (z^{f(h)}, z^{f(g)})$$

is in fact into and onto the subset $E(\Lambda)$ of the codomain. (That β is well-defined and one-to-one is automatic from α having the same properties).

Now (by the proof of the theorem in §6) we have an alternative expression for the set $E(\Psi)$:

$$E(\Psi) = \{(u,v) \in \ell^2 : \exists\, h,g \in G \text{ s.t. } (u = z^h,\ v = z^g \text{ and } \exists\, k,\ell \in \mathbb{Z} \bmod p \text{ s.t. } z^k x z^\ell h g^{-1} = I)\}\ .$$

So when we consider $\beta(z^h,z^g)$ for $(z^h,z^g) \in E(\Psi)$ we may assume that

$$z^k x z^\ell h g^{-1} = I \text{ for some } k,\ell \in \mathbb{Z} \bmod p\ .$$

I show that $\beta(z^h,z^g) \in E(\Lambda)$ by proving that

$$o(z^{f(h)}.z^{f(g)}) = 2\ .$$

Now $f(h)(f(g))^{-1} = c^{-1}(hg^{-1})c$

$= c^{-1}(z^{-\ell}xz^{-k})c$

$= z^{-\ell i}\chi z^{-ki}$

and so

$$z^{f(h)}.z^{f(g)} = (f(h))^{-1}\ z\ f(h)(f(g))^{-1}\ zf(g)$$

$$\Rightarrow\quad o(z^{f(h)}.z^{f(g)}) = o(f(g)(f(h))^{-1}\ zf(h)(f(g))^{-1}z)$$

$$= o(z^{ki}\chi z\chi z^{1-ki})$$

$$= o(\chi z\chi z)\ .$$

But, $\chi z = \begin{pmatrix} 0 & \sqrt{2}^{-1} \\ -\sqrt{2} & -\sqrt{2} \end{pmatrix}$

and so

$$(\chi z)^2 = \begin{pmatrix} -1 & -1 \\ 2 & +1 \end{pmatrix}$$

$$\Rightarrow\quad tr(\chi z\chi z) = 0$$

$$\Rightarrow\quad o(z^{f(h)}.z^{f(g)}) = 2 \qquad \text{as required.}$$

Thus we have ascertained that β is <u>into</u> $E(\Lambda)$. But we know that β is one-to-one, so to prove that β is <u>onto</u> $E(\Lambda)$ we need only show that

$$|E(\Psi)| = |E(\Lambda)|.$$

But referring to Surowski's paper, we are told that Λ (like Ψ) has constant valency p, and the above equality is immediate as the two vertex sets are identical.

9. A NOTE CONCERNING OTHER GROUPS G

Of course there is nothing really inherently special to the automorphism groups in the restricted $\mathcal{M}_3^+$ when using the techniques as described in §4 to §7 (the same cannot be said for the argument of §8). It just happens that this category of groups (i.e. $PSL_2(q)$ and $PGL_2(q)$ for all prime powers q) gives some positive results as already shown, and are the groups principally examined in this volume. But one can extend the definition of the graph $\Psi(G,\ell) := \Psi$ to any finite group G and conjugacy class ℓ of G in the expected way:

> The vertex set $V(\Psi)$ of Ψ is given by the elements of ℓ
>
> The edge set $E(\Psi)$ of Ψ is given exactly by those pairs $(u,v) \in \ell^2$ for which $o(uv^2) = o(vu^2) = 2$ in G.

Now one can ask for which pairs (G, ℓ) can we use an analogous method to that we used for our limited case to deduce that $\Psi(G,\ell)$ has a unique triangular imbedding which is a ROΔM (with automorphism group G)? Let us call every pair (G, ℓ) for which we can do this a solution (of the method).

I attempt here to determine the set of solutions by identifying it as consisting exactly of those pairs (G, ℓ) which satisfy some specific group theoretic conditions depending only on G and ℓ. To do this I first write down a sequence of six questions 1) to 6) all of which involve map or

graph properties allied to (G, ℓ), and usefully summarises the different components of the whole argument (which is done mostly at this level). If for particular (G, ℓ) the answer to each question is 'yes', this is sufficient to guarantee the unique imbedding of Ψ as desired. We then translate the map/graph theoretic conditions inherent in these questions into six purely group theoretic conditions on (G, ℓ) which taken together are equivalent. (The appropriate group theoretic conditions resulting from the six map/graph theoretic conditions are already known, or at least are evident, from our previous work).

The six questions involving map and graph properties allied to given (G,ℓ):

1) Does there exist a ROΔM $\mathcal{M}$ such that $\mathcal{M}$ is given by a quadruple (G,Ω,x, y) for which $z := y^{-1}x$ is an element of ℓ?

Assume for the other questions that the answer to 1) is yes, and that $\mathcal{M}$ is any ROΔM satisfying the condition expressed in 1).

2) Is $\mathcal{M}$ uniquely determined?

3) Can the underlying graph $\textcircled{H}$ of $\mathcal{M}$ be described (in terms of an isomorphic graph $\textcircled{H}'$) with the elements of ℓ as the vertex set (as in §5)?

4) Is the answer to 3) yes, and $\Psi = \textcircled{H}'$? (c.f. §6)

5) Is $\textcircled{H}$ a VTT?

6) Is $\mathcal{M}$ reflexible?

The Associated Conditions, on G and ℓ for given (G, ℓ) to be a solution. Let z be any element of ℓ, and $d := o(z) > 6$.

1) There exist a pair (x,y) of elements of G such that

$$\langle x,y \rangle = G \qquad o(x) = 2 \qquad o(y) = 3 \qquad y^{-1}x = z$$

2) The set of pairs (x,y) of G satisfying the conditions in 1) above form a single class under Stab(z) in AutG.

3) The centralizer $C_G(z)$ of z in G must be the cyclic group generated by z (in particular $\langle z \rangle \leqslant G$ must be a maximal cyclic subgroup of G.)

4) There exist at most d elements w in ℓ for which $o(wz^2) = 2$ in G.

5) If x is an involution in G such that $\langle x,z \rangle = G$ with $o(xz^{-1}) = 3$ and if $i,j,k \in \mathbb{Z}_d$, then

$$z^i x z^j x z^k x = I \text{ in } G \Rightarrow i \equiv j \equiv k \equiv \pm 1 \bmod d \ .$$

6) If (x,y) is a pair of elements of G satisfying the conditions in 1) above, then there exists an automorphism α of G such that

$$\alpha : x \longmapsto x \ , \qquad \alpha : z \longmapsto z^{-1} \ .$$

Evidently the above list form quite a formidable set of conditions to check for any given (G, ℓ) and I do not propose here to find more examples that do give solutions. However I note that conditions 2), 5) and 6) are of relevance only to ensure the uniqueness part of the imbedding: if the pair (G, ℓ) satisfies conditions 1), 3) and 4), then Ψ can be imbedded as a ROΔM with automorphism group G but may have other triangular imbeddings.

A final interesting note is that condition 2) in fact is redundant; if for

a particular (G, ℓ) the conditions 1), 3), 4), 5) and 6) hold, then 2) automatically is satisfied. This then may be regarded as a purely group theoretic result. My proposition here may be justified thus:

Suppose there are two ROΔMs $\mathcal{M}$, $\mathcal{M}'$ both with automorphism group G and associated values of z lying in ℓ. Then the answer 'yes' to questions 3) and 4) imply the underlying graphs of $\mathcal{M}$ and $\mathcal{M}'$ are both isomorphic to $\Psi(G, \ell)$ and hence isomorphic to each other: but if for any one of $\mathcal{M}$ or $\mathcal{M}'$ the map is reflexible and its underlying graph is a VTT, there is only one triangular orientable imbedding for the latter and so necessarily $\mathcal{M} \cong \mathcal{M}'$ contrary to our original stipulation. Hence if condition 2) is not satisfied, some other of the conditions must be not satisfied as well.

References

1 Aigner M. Combinatorial Theory (Chapter 4), Berlin Springer, 1979.

2 Carter R.W. Simple Groups of Lie Type (Th. 12.5.1), John Wiley & Sons, 1972.

3 Cori R. Cartes, hypercartes et leurs groupes d'automorphismes, Analyse Appliquée et Informatique n°. 8420, Bordeaux 1, 1984.

4 Coxeter H.S.M. & Moser W.O.J. Generators and Relations for Discrete Groups, Ergebrisse der Math. Neue Folge No 14 (Berlin Springer 1957).

5 Dickson L.E. Linear Groups, Teubner, Leipzig, 1901; reprinted Dover, New York, 1958.

6 Downs M.L.N. & Jones G.A. Enumerating regular objects with a given automorphism group, Discrete Mathematics 64 (1987), 299-302.

7 Hall P. The Eulerian functions of a group, Quart J. Math. (Oxford) 7 (1936), 134-151.

8 Hall W. Automorphisms and Coverings of Klein Surfaces, Ph.D. Thesis, 1977, University of Southampton.

9 James L.D. and Jones G.A. Regular oriented inbeddings of complete graphs, J. Combinatorial Theory B.

10 Johnson D.L. Topics in the Theory of Group Presentations, London Math. Soc. Lecture Note Series 42, C.U.P., 1980.

11 Jones G.A. Graph inbeddings, groups and Riemann surfaces, Algebraic Methods in Graph Theory, Szeged, 1978, Colloq. Math. Soc. Janos Bolyai 25, North-Holland, Amsterdam, 1981.

12 Jones G.A. & Singerman D. Theory of maps on orientable surfaces, Proc. London Math. Soc. (3) 37 (1978), 273-307.

13 Kratzer C. & Thévenaz J. Fonction de Mobius d'un groupe fini et anneau de Burnside, Comment. Math. Helvetici 59 (1984), 425-438.

14 Macbeath A.M. Generators of the linear fractional groups, Proc. Sympos. Pure Math XII (Amer. Math. Soc., Providence, R.I., 1967), 14-32.

15 Machi A. The Riemann-Hurwitz formula for the centraliser of a pair of permutations, Arch. Math. 42 (1984), 280-288.

16 McQuillan D.L. Classification of normal congruence subgroups of the modular group, Am. J. Math. 87 (1965), 285-296.

17 Medryh A.D. On unramified coverings of compact Riemann surfaces, Dokl. Akad. Nauk SSSR 224 (1979); English transl. in Soviet Math. Dokl. 20 (1979), 85-88.

18 Mednyh A.D. On the solution of the Hwwitz problem on the number of nonequivalent coverings over a compact Riemann surfact, Dokl. Akad. Nauk SSSR 261 (1981) No 3; English transl. in Soviet Math. Dokl. 24 (1981), 541-545.

19 Meier D. and Wiegold J. Growth sequences of finite groups V, J. Austral. Math. Soc. (Series A) 31 (1981), 374-375.

20 Newman Integral Matrices, Academic Press, New York, 1972.

21 Rose J.S. A Course on Group Theory, C.U.P., 1978.

22 Singerman D. PSL(2,q) as an image of the extended modular group with application to group actions on surfaces, Proc. of the Edinburgh Math. Soc. (1986) 27.

23 Surowski D.B. Vertex triangulations of compact orientable 2-manifolds, J. of Combinatorial Theory, Series B 39 (1985), 372-375.

24 Tutte W.T. What is a map? New Directions in Graph Theory, Ac. Press, 1973.

25 Walsh T.R.S. Hypermaps versus bipartite graphs, J. Comb. Theory Ser. B 18 (1975), 155-163.

26 Wiegold J. Growth sequences of finite groups, J. Austral. Math. Soc. 17 (1974), 133-141.

27 Wiegold J. Growth sequences of finite groups II, J. Austral. Math. Soc. 20 (1975), 225-229.

28 Wiegold J. Growth sequences of finite groups III, J. Austral. Math. Soc. 25 (Series A) (1978), 142-144.

29 Wiegold J. Growth sequences of finite groups IV, J. Austral. Math. Soc. 29 (Series A) (1980), 14-16.

30 Bryant R.P & Singerman D. Foundations of the theory of maps on surfaces with boundary, Quart. J. Math. Oxford (2), 36, (1985), 17-41.