UNIVERSITY OF SOUTHAMPTON

FACULTY OF MATHEMATICAL STUDIES

AUTOMORPHISMS OF THE MODULAR AND EXTENDED MODULAR GROUPS

by

JOHN STEWART THORNTON

A thesis submitted for the degree of Doctor of Philosophy

November 1983

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

FACULTY OF MATHEMATICAL STUDIES

MATHEMATICS

Doctor of Philosophy

AUTOMORPHISMS OF THE MODULAR AND EXTENDED MODULAR GROUPS

by John Stewart Thornton

The groups of 2×2 integral matrices $GL(2, \mathbb{Z})$ and $SL(2, \mathbb{Z})$ and their related projective groups $PGL(2, \mathbb{Z})$ and $PSL(2, \mathbb{Z})$ have been used and studied for over a century, but little work has been done on their automorphism groups. Hua and Reiner in the early 1950's gave generators for all these automorphism groups (not only for 2×2, but also for $n \times n$ matrix groups) showing, in particular, that the groups $PGL(n, \mathbb{Z})$ have only inner automorphisms. We show that in fact $n = 2$ is an exception, having outer automorphisms too, and we give presentations for the automorphism groups of $GL(2, \mathbb{Z})$, $SL(2, \mathbb{Z})$, $PGL(2, \mathbb{Z})$ and $PSL(2, \mathbb{Z})$, showing the close relationships between them.

A complete list is given of the conjugacy classes of $PSL(2, \mathbb{Z})$ and $PGL(2, \mathbb{Z})$, and it is seen that most are not invariant under the automorphisms of their groups.

Congruence subgroups of $PGL(2, \mathbb{Z})$ and $PSL(2, \mathbb{Z})$ are studied, and we show that most are not characteristic in $PGL(2, \mathbb{Z})$. In fact only a finite number are characteristic, demonstrating that their definition is essentially number-theoretic rather than group theoretic.

By considering the theory of maps on surfaces we find a geometric interpretation for the outer automorphisms of $PGL(2, \mathbb{Z})$. We show that the outer automorphism group of $PGL(2, \mathbb{Z})$ acts on the class of trivalent maps to interchange faces and Petrie polygons.

ACKNOWLEDGEMENTS

I should like to express my gratitude to my supervisor Dr. G.A. Jones for all the help and guidance given to me during the course of this research. I also wish to thank my adviser Dr. D. Singerman for his help and encouragement.

My thanks go to Mrs. Hazel Paul for her quick and careful typing of this thesis.

I am indebted to the Science and Engineering Research Council for their financial support while I undertook this work.

CONTENTS

	Page No.
ABSTRACT	i
ACKNOWLEDGEMENTS	ii
CONTENTS	iii
CHAPTER I	1
I.1 Introduction	1
I.2 Preliminaries	4
CHAPTER II	
II.1 Aut(PSL)	8
II.2 Aut(SL)	
II.3 Aut(PGL)	18
II.4 Aut(GL)	30
CHAPTER III	36
III.1 Conjugacy Classes in PSL	36
III.2 The Effect of Aut(PSL) on the Conjugacy Classes of PSL	44
III.3 Conjugacy Classes in PGL	48
III.4 The Effect of Aut(PGL) on the Conjugacy Classes of PGL	52
CHAPTER IV	58
IV.1 Preliminaries	59
IV.2 Congruence Subgroups and Quotients	60

CONTENTS (Continued)

	Page No.
IV.3 Normal Subgroups of Direct Products	63
IV.4 Normal Structure of $Q(p^e)$	64
IV.5 Subgroups of N(12)	66
IV.6 Proof of Theorem 1	68
IV.7 Proof of Corollary 2	81
CHAPTER V	83
V.1 Algebraic Maps	83
V.2 Automorphisms of G	87
V.3 Operations on Maps	88
V.4 Trivalent and Triangular Maps	90
APPENDIX	94
REFERENCES	97

CHAPTER I

I.1 Introduction

The groups we are mainly concerned with in this work are the modular group and the extended modular group. We define $GL(2, \mathbb{Z})$ and $SL(2, \mathbb{Z})$ as the groups of 2×2 matrices, with integer coefficients, whose determinants are ± 1 in the former case, and 1 in the latter. Thus $SL(2, \mathbb{Z})$ is a subgroup of index 2 in $GL(2, \mathbb{Z})$. Each of these groups has centre $\{\pm I\}$ (I is the 2×2 identity matrix), and factoring them by their centres gives the modular group

$$PSL(2, \mathbb{Z}) = SL(2, \mathbb{Z})/\{\pm I\}$$

and the extended modular group

$$PGL(2, \mathbb{Z}) = GL(2, \mathbb{Z})/\{\pm I\} .$$

Again $PSL(2, \mathbb{Z})$ is a subgroup of index 2 in $PGL(2, \mathbb{Z})$.

It is well known that $PSL(2, \mathbb{Z})$ is isomorphic to the group Γ of linear fractional transformations

$$\tau : z \mapsto \frac{az+b}{cz+d} \qquad (1)$$

where a,b,c,d are any integers satisfying $ad-bc = 1$. Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then τ corresponds to $\{M,-M\}$. The group Γ is

also referred to as the modular group, and we use Γ and $PSL(2, \mathbb{Z})$ interchangeably. Thus Γ may also be studied geometrically, by considering its action on the upper half-plane $\mathcal{U}$, taking z to be a complex number with positive imaginary part. The transformation τ is then classified as hyperbolic, parabolic, or elliptic according as it has two real fixed points, one real fixed point, or one fixed point in $\mathcal{U}$.

We can also define an action of the extended modular group on $\mathcal{U}$ by

$$\tau : z \mapsto \frac{az+b}{cz+d} \qquad \text{if} \quad ad-bc = 1,$$

$$\tau : z \mapsto \frac{a\bar{z}+b}{c\bar{z}+d} \qquad \text{if} \quad ad-bc = -1 .$$

In the former case τ is orientation-preserving, and in the latter it is orientation-reversing.

Interest in the modular group arose out of its connection with number theory. "Many of the great advances in analytic number theory have come through a detailed study of this group and its subgroups. The connection arises via the elliptic modular functions and forms, such as the Dedekind eta function or the theta functions. These functions are invariant or semi invariant with respect to the linear transformations (1) and are the generating functions of numerous number-theoretic functions of great interest, such as the partition function, and the function that counts the number of representatives of an integer by some integral positive definite quadratic form". (Newman [16, page 138]).

In this connection the congruence subgroups are of particular importance, so it is interesting to consider whether they are purely number-theoretic in definition, or whether they have some group-theoretic definition. It is therefore important to consider their behaviour under automorphisms, so we devote Chapter II to obtaining the automorphism groups of the four integral matrix groups mentioned at the beginning.

We obtain the automorphism group of $PSL(2, \mathbb{Z})$ by methods that are essentially combinatorial, and show that it can be considered as $PGL(2, \mathbb{Z})$ acting by conjugation on $PSL(2, \mathbb{Z})$. From this we derive the automorphism group of $PGL(2, \mathbb{Z})$ by considering the elements of $Aut(PGL(2, \mathbb{Z}))$ which restrict to elements of $Aut(PSL(2, \mathbb{Z}))$, and showing that these form a subgroup of index 2 in $Aut(PGL(2, \mathbb{Z}))$. The automorphism groups of $SL(2, \mathbb{Z})$ and $GL(2, \mathbb{Z})$ are obtained by similar methods.

In Chapter III we use combinatorial methods to give a list of the conjugacy classes of elements of both $PSL(2, \mathbb{Z})$ and $PGL(2, \mathbb{Z})$, and we consider the effects of their automorphism groups on them, showing which classes are invariant.

In Chapter IV we use group-theoretic methods to study the congruence subgroups of $PSL(2, \mathbb{Z})$ and $PGL(2, \mathbb{Z})$ - subgroups defined by congruence relations on the entries of the matrices. The principal congruence subgroups of level n of $PSL(2, \mathbb{Z})$, denoted by $\Gamma(n)$, consist of all those matrices congruent modulo n to the identity matrix. A subgroup C of $PGL(2, \mathbb{Z})$ is a congruence subgroup if it contains $\Gamma(n)$ for some n. We show that a congruence subgroup is characteristic in $PGL(2, \mathbb{Z})$ only if it contains $\Gamma(600)$, and hence that the number of characteristic congruence subgroups is finite. Therefore the congruence subgroups must be considered to be number-theoretic or geometric in their nature, rather than group-theoretic.

This being the case, it is unlikely that any number-theoretic interpretation can be found for the outer automorphisms of $PGL(2, \mathbb{Z})$, but a geometric interpretation can be found in the theory of maps on surfaces. It has been shown that there are just six invertible operations on maps (see [10] and [19]), forming a group isomorphic to S_3. In Chapter V we show that these arise naturally in algebraic map theory, being induced by the outer automorphism group of a certain group G. In particular, we show that the outer automorphism group of $PGL(2, \mathbb{Z})$ - shown in Chapter III to have order 2 - acts on the class of trivalent maps to interchange faces and Petrie polygons.

I.2 Preliminaries

Many of the elementary properties of the modular group are given by Newman [16, Chapter VIII] and the reader is referred to that book, but one result of fundamental importance will be stated here, namely that Γ is the free product of cyclic groups $\{x\}$, $\{y\}$ of orders 2 and 3 :

$$\Gamma = \{x\} * \{y\} .$$

We define

$$X = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

and for all $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, define $m = \{M, -M\}$ (so $x = \{X, -X\}$ etc.).

Then $PSL(2, \mathbb{Z})$ is generated by x and y (Newman, [16]), and $PGL(2, \mathbb{Z})$ is generated by x, y, and a. These are the generators

that we use most of the time. However, if we define

$$V = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad W = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

then it will sometimes be found useful to use v and w as generators of $PSL(2, \mathbb{Z})$ [16] . Let us also define

$$R_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad R_2 = \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}, \quad R_3 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

then r_1, r_2, r_3 are useful as generators of $PGL(2, \mathbb{Z})$ (Coxeter and Moser [3, page 85]).

Following Poincaré we can regard the upper half-plane $\mathcal{U}$ as a conformal representation of the hyperbolic plane, in which case $r_1, r_2,$ and r_3 (which all have determinant -1) can be considered as reflections. Since these generate $PGL(2, \mathbb{Z})$ it follows that $PSL(2, \mathbb{Z})$ (all of whose elements are orientation-preserving) is the subgroup consisting of products of an even number of the generators r_1, r_2, r_3 .

Considering now the fixed points of the linear fractional transformation of $\mathcal{U}$,

$$z = \frac{az+b}{cz+d}$$

implies that $cz^2 + (d-a)z - b = 0$. The discriminant of this equation is $(d+a)^2 - 4$, so a transformation is hyperbolic, parabolic, or elliptic according as $|a+d|$ is greater than, equal to , or less than 2 . But $a+d$ is the trace of M so we call $m = \{M,-M\} \in PSL(2, \mathbb{Z})$

hyperbolic, parabolic, or elliptic according as $|\text{trace } M|$ is greater than, equal to, or less than 2 .

The matrices we are considering are all 2×2 , and usually over the ring of integers, so that in these cases we drop the $(2, \mathbb{Z})$ and refer simply to SL, PSL and so on. If the ring is $\mathbb{Z}_n$ then we write PSL(2, n) and so on.

In Chapter II we use capital letters for matrices in GL, SL, and lower case letters for their images in PGL, PSL, as we have already been doing. (Thus if $M \in GL$ then $m = \{M,-M\} \in PGL$.) For an automorphism induced by conjugation we use the corresponding Greek letter, so conjugation of m by x is denoted by

$$x^{-1}mx = m\xi .$$

In subsequent chapters however, we are looking exclusively at PSL and PGL , and it is convenient to drop the preceding convention. Therefore in these chapters we write $\pm M$ or just M rather than m , but no confusion should arise. This means that trace $M = \pm(a+d)$, but again we usually refer to trace M as $|a+d|$.

Presentations for groups will be given using either relations or relators in the form

$$\langle \text{ generators : relations or relators} \rangle .$$

Thus, for example

$$\Gamma = \langle x,y : x^2 = y^3 = 1 \rangle$$

or

$$\Gamma = \langle x,y : x^2,y^3 \rangle .$$

Finally, conjugation of a by b is denoted sometimes by a^b, that is,

$$a^b = b^{-1}ab .$$

CHAPTER II

An important step in studying the structure of any group is to determine its automorphism group. In this chapter we calculate the automorphism groups of PSL, SL, PGL, and GL. Schreier [17] gives the automorphisms of PSL, but gives only a sketchy proof. Hua and Reiner give generators only for all the automorphism groups of $SL(n, \mathbb{Z})$, $GL(n, \mathbb{Z})$ [5] and $PSL(n, \mathbb{Z})$, $PGL(n, \mathbb{Z})$ [6].

Starting with PSL, its generators x and y must be sent by any automorphism to elements of orders 2 and 3 respectively, and these are known so we can find all possible automorphisms. We give generators and find relations between them and so give a presentation for Aut(PSL). The groups SL, PGL, and GL are closely related to PSL and we expect their automorphism groups to be closely related to Aut(PSL). We develop presentations for Aut(SL), Aut(PGL), and Aut(GL) in such a way that the connections between them and Aut(PSL) become clear.

The main subject of our study is PSL, but this is a subgroup of PGL, and the effect of Aut(PGL) on PSL is of some interest, and will be considered in subsequent chapters.

II.1 Aut(PSL)

$$PSL = \langle x,y : x^2 = y^3 = 1 \rangle \quad .$$

Suppose $\theta \in Aut(PSL)$. We need look only at the effect of θ on the generators x and y. Suppose $x\theta = u$ and $y\theta = v$. Since θ is an isomorphism, u and v have the same orders as x and y respectively, i.e. u has order 2, v has order 3; and as

$u,v \in PSL$, we know [16,p.142] that u must be conjugate to x and v must be conjugate to y or to y^{-1} , say

$$u = g^{-1}xg \ , \ v = h^{-1}y^{\varepsilon}h \quad , \ g,h \in PSL, \ \varepsilon = \pm 1 \ .$$

By composing θ with the inner automorphism i_g^{-1} we get another automorphism

$$\theta \circ i_g^{-1} : x \mapsto x$$

$$y \mapsto (hg^{-1})^{-1} \, y^{\varepsilon} (hg^{-1})$$

so we may assume that for some $k \in PSL$,

$$\theta : x \mapsto x$$

$$y \mapsto k^{-1}y^{\varepsilon}k \ , \quad \varepsilon = \pm 1 \qquad (1)$$

We ask, then: for which elements k does $\{x, k^{-1}y^{\varepsilon}k\}$ generate PSL? Equivalently, we can ask : for which elements $k \in PSL$ does there exist a word W in x and $k^{-1}y^{\varepsilon}k$ such that

$$y = W(x, \, k^{-1}y^{\varepsilon}k) \ ?$$

Suppose there exists such a word, then for some $n \in \mathbb{N}$,

$$y = x^{\alpha}k^{-1}y^{e_1}kxk^{-1}y^{e_2}kx....xk^{-1}y^{e_n}kx^{\beta} \qquad (2)$$

where

$$e_i = \pm 1$$

and

$$\alpha,\beta = 0 \text{ or } 1 \ .$$

We may write k as a reduced, non-empty, word in x and y . The right hand side of (2) must 'collapse' to y , and can do so only by adjacent letters cancelling by the rules $x^2 = y^3 = 1$. In particular,

the internal x's must disappear, and so each must cancel with another x. Now each internal x is flanked by k on the left and k^{-1} on the right. If $k = k'x$ (k' also reduced and $L(k') = L(k)-1$, where $L(k)$ means the length of k; i.e. if k as a reduced word ends in x) then

$$kxk^{-1} = (k'x)x\left(x(k')^{-1}\right)$$

$$= k'x(k')^{-1} ,$$

and since k', or otherwise k, ends in y it is clear that we cannot get rid of the x's in this way. The only possibility left therefore is that the internal x's can come together. This necessitates that the intervening $k^{-1}y^{e_i}k = 1$, which is impossible. We conclude that $n = 1$. Thus

$$y = x^{\alpha}k^{-1}y^{e_1}kx^{\beta} .$$

Since we must lose the x's that are (possibly) on the ends, it is easy to see that either

$$\alpha = \beta = 1 \quad \text{and} \quad k = \ldots\ldots y^{\pm 1}x$$

or

$$\alpha = \beta = 0 \quad \text{and} \quad k = \ldots\ldots y^{\pm 1}$$

so that either

$$y = (kx)^{-1}\, y^{e_1}(kx) \quad \text{with} \quad k = \ldots\ldots y^{\pm 1}x$$

or

$$y = k^{-1}\, y^{e_1}k \qquad \text{with} \quad k = \ldots\ldots y^{\pm 1} .$$

Now y is not conjugate to y^{-1}, so $e_1 = \varepsilon e_1' = +1$, and

$$y = (kx)^{-1}\, y(kx) \quad \text{with} \quad k = \ldots y^{\pm 1}x \qquad (a)$$

or

$$y = k^{-1}yk \qquad \text{with} \quad k = \ldots\ldots y^{\pm 1} \qquad (b).$$

If $y = t^{-1}yt$ then t belongs to the centralizer $C_{PSL}(y)$ of y in PSL, but $C_{PSL}(y)$ is just $\langle y : y^3 = 1\rangle$, and it follows that in case (a) $kx = y$ or y^{-1} so that $k = y^{\pm 1}x$, and in case (b) $k = y^{\pm 1}$.

Referring back to (1) now, case (b) gives

$$\theta = \theta_b : x \mapsto x$$

$$y \mapsto y^{\varepsilon} \quad , \quad \varepsilon = \pm 1$$

and case (a) gives

$$\theta = \theta_a : x \mapsto x$$

$$y \mapsto xy^{\varepsilon}x \quad , \quad \varepsilon = \pm 1 \, ,$$

but this is just θ_b composed with i_x, i.e.

$$\theta_a = \theta_b \circ i_x \, ,$$

and gives us nothing new.

Putting $\varepsilon = 1$ in θ_b gives us just the identity automorphism, and putting $\varepsilon = -1$ in θ_b gives the automorphism

$$\alpha : x \mapsto x$$

$$y \mapsto y^{-1}$$

Therefore every automorphism of PSL has the form

$$i_g \qquad (g \in PSL)$$

or

$$\alpha \circ i_g \qquad (g \in PSL) \quad .$$

Now $\{i_g : g \in PSL\} \cong PSL/Z(PSL) = PSL$, and $\alpha \notin \{i_g\}$; but $\alpha^2 = 1 \in \{i_g\}$, so

$Aut(PSL) = \{i_g : g \in PSL\} \cup \alpha\{i_g : g \in PSL\}$, and $\{i_g\} = Inn(PSL) \trianglelefteq Aut(PSL)$ with $Aut(PSL)/Inn(PSL) \cong C_2$. In fact $Aut(PSL)$ is a split extension of $Inn(PSL)$ by $\langle\alpha\rangle \cong C_2$. Let $\xi = i_x$ and let $\eta = i_y$ (so that for $g \in PSL$, $g\xi = x^{-1}gx$ and $g\eta = y^{-1}gy$), then since $\{i_g : g \in PSL\} \cong PSL$, it has presentation

$$\langle \xi, \eta \ : \ \xi^2 = \eta^3 = 1 \rangle \quad .$$

In order to find a presentation for $Aut(PSL)$ we calculate $\alpha^{-1}\xi\alpha$ and $\alpha^{-1}\eta\alpha$.

$$\alpha^{-1}\xi\alpha : x \mapsto x \quad = x\xi$$

$$y \mapsto x^{-1}yx = y\xi \ , \quad \text{so} \quad \alpha^{-1}\xi\alpha = \xi \ ;$$

$$\alpha^{-1}\eta\alpha : x \mapsto yxy^{-1} = x\eta^{-1}$$

$$y \mapsto y \quad = y\eta^{-1} \ , \ \text{so} \quad \alpha^{-1}\eta\alpha = \eta^{-1} \quad .$$

We know that $\alpha^2 = 1$, hence we have

Theorem 1

A presentation for Aut(PSL) *is*

$$\langle \xi,\eta,\alpha : \xi^2 = \eta^3 = \alpha^2 = 1 \ , \ \xi^\alpha = \xi, \ \eta^\alpha = \eta^{-1} \rangle \ .$$

Consider now $a = \{A, -A\}$ (see Chapter I.2). The determinant of A is -1, so $a \in PGL \setminus PSL$. It is easy to check that $a^2 = 1$ and that $a^{-1}xa = x$ and $a^{-1}ya = y^{-1}$, so that a acts by conjugation on x and y exactly as α does. Thus Aut(PSL) is isomorphic to the group G generated by $x,y,$ and a. Since $a \notin PSL$, $G > PSL$.

Let M be a product of X's, Y's and A's. Since $\det(X) = \det(Y) = 1$ and $\det(A) = -1$, M has determinant ± 1, and so either $m = M, -M \in PSL$ or $ma \in PSL$; hence $G : PSL = 2$.

Now $PGL > PSL$ with index 2, and $a \in PGL \setminus PSL$, so $G = PGL$, and we have

Theorem 2

$$Aut(PSL) \cong PGL \ .$$

We can think of Aut(PSL) as being PGL acting by conjugation on PSL.

It follows that a presentation for PGL is

$$\langle x,y,a : x^2 = y^3 = a^2 = 1 \ , \ axa = x, \ aya = y^{-1} \rangle \ .$$

II.2 Aut(SL)

The centre $Z(G)$ of any group G must be invariant under its automorphism group $Aut(G)$. Consequently $G/Z(G)$ is invariant under

automorphisms of G, and so any automorphism $\theta \in \mathrm{Aut}(G)$ induces an autormorphism θ' on $G/Z(G)$: if $g,h \in G$ and $h = g\theta$, then

$$\theta' : Z(G)g \mapsto Z(G)g\theta = Z(G)h$$

is the automorphism induced on $G/Z(G)$ by θ.

In the case of SL, $Z(SL) = \{\pm I\}$ and $SL/\{\pm I\} = PSL$, so if $\theta \in \mathrm{Aut}(SL)$, the automorphism induced on PSL is

$$\theta' : \{M, -M\} \mapsto \{M\theta, -M\theta\} .$$

Let ψ denote the homomorphism $\mathrm{Aut}(SL) \to \mathrm{Aut}(PSL)$ defined by $\theta \mapsto \theta'$ as above. Now we know $\mathrm{Aut}(PSL)$ so we know all the θ' (we show later that ψ is an epimorphism) and we therefore look for non-trivial $\theta \in \mathrm{Aut}(SL)$ which induce the trivial $\theta' \in \mathrm{Aut}(PSL)$; in other words, we look for the kernel of ψ. Thus we require $M\theta = \pm M$ for all $M \in SL$. Now θ is a homomorphism, so we know its action on SL if we know its action on the generators of SL. A presentation for SL is

$$\langle X,Y : X^4 = Y^6 = I, X^2 = Y^3 \rangle .$$

As before, $X = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$, and it can easily be seen that $X^2 = Y^3 = -I$. Since SL has two generators, there are four possible actions of θ :

$$X \mapsto X \ , \ Y \mapsto Y \qquad \text{(the identity)} \ ,$$

$$\theta_X : X \mapsto X \ , \ Y \mapsto -Y \ ,$$

$$\theta_Y : X \mapsto -X, \ Y \mapsto Y \ ,$$

$$\theta_X \circ \theta_Y : X \mapsto -X, \ Y \mapsto -Y \ ,$$

Now $(-Y)X^2 = Y$ and $(-X)^3 = X$, so both $\{X, -Y\}$ and $\{-X, Y\}$ generate SL ; but $Y^3 = -I$, $(-Y)^3 = I$, so θ_X is not an automorphism. (It is not a homomorphism, for if it were then we would have $I = (-Y)^3 = (Y\theta_X)^3 = (Y^3)\theta_X = (-I)\theta_X = (X^2)\theta_X = (X\theta_X)^2 = X^2 = -I$, which is not so.) However, $X^2 = (-X)^2 = -I$, so θ_Y is a homomorphism. It has finite order and so is a monomorphism, and hence an automorphism. It follows that $\theta_X \circ \theta_Y$ is not an automorphism, for if it were then so also would be $(\theta_X \circ \theta_Y) \circ \theta_Y = \theta_X$, which we have seen is not. Put $\beta = \theta_Y$, so

$$\beta : X \mapsto -X \ , \ Y \mapsto Y \ .$$

Since $X^2 = -I$, $(-X)X = I$ so $-X = X^{-1}$; thus

$$\beta : X \mapsto X^{-1} \ , \ Y \mapsto Y \ .$$

Clearly $\beta^2 = 1$, so $\ker\psi = \langle\beta\rangle \cong C_2$, where $\psi : \mathrm{Aut(SL)} \to \mathrm{Aut(PSL)}$ is defined as above.

From Theorem 1 we have

$$\mathrm{Aut}(PSL) = \langle \xi, \eta, \alpha : \xi^2 = \eta^3 = \alpha^2 = 1 \ , \ \xi^\alpha = \xi, \ \eta^\alpha = \eta^{-1} \rangle \ ,$$

where

$$\xi : m \mapsto x^{-1}mx \qquad (m \in PSL) \ ,$$

$$\eta : m \mapsto y^{-1}my \qquad (m \in PSL) \ ,$$

$$\alpha : x \mapsto x \ , \ y \mapsto y^{-1} \ ,$$

and from Theorem 2, $\mathrm{Aut}(PSL) \cong PGL$.

Now for any group G , if $\psi : G \to H$ is an epimorphism and if $K \leqslant G$ then $\psi(K) = H$ if and only if $G = \ker(\psi).K$. In the case where G is $\mathrm{Aut}(SL)$ and ψ is defined as above, we know $\mathrm{Ker}(\psi)$ so we can find $\mathrm{Aut}(SL)$ if ψ is an epimorphism and if we can find a subgroup $K \leqslant \mathrm{Aut}(SL)$ satisfying $\psi(K) = \mathrm{Aut}(PSL)$.

Lemma 1

ψ is an epimorphism.

Proof

SL is a normal subgroup of GL , so GL acts on SL by conjugation, and this action has kernel $= C_{GL}(SL) = \{\pm I\}$. Any conjugation is an automorphism of SL , so $GL/\{\pm I\} = PGL \leqslant \mathrm{Aut}(SL)$. When calculating $\mathrm{Aut}(PSL)$ we saw that $\psi(PGL) = \mathrm{Aut}(PSL)$, and since $\mathrm{Aut}(SL) \geqslant PGL$ it follows that $\psi(\mathrm{Aut}(SL)) = \mathrm{Aut}(PSL)$, so that ψ is an epimorphism as required.

This also shows that we can take K to be PGL, and so we have:

Corollary 1

$$\mathrm{Aut}(SL) \cong PGL \cdot \langle \beta \rangle \ .$$

Now $\langle \beta \rangle = \ker(\psi)$ so $\langle \beta \rangle \lhd \mathrm{Aut}(SL)$, but also $\langle \beta \rangle \cong C_2$ so β is a central element of $\mathrm{Aut}(SL)$.

Lemma 2

$$PGL \cap \langle \beta \rangle = \{1\}$$

Proof

If β is conjugation by an element of PGL then $\exists\, B \in GL$ such that

$$B^{-1}XB = X^{-1} \qquad (a)$$

and

$$B^{-1}YB = Y \qquad (b)$$

Condition (b) shows that B commutes with Y and so either B must be $\pm$ the identity (which is impossible because of condition (a)) or B and Y are $\pm$ powers of the same element. Since Y has finite order and generates the largest cyclic subgroup containing it, this is equivalent to B being a power of Y. Thus (a) gives the relation $Y^{-n}XY^{n}X = I$ for some n with $Y^{n} \neq I$; but no such relation

exists in SL . Therefore $GL \cap \langle\beta\rangle = \{1\}$. Thus

$$\mathrm{Aut}(SL) \cong PGL \times \langle\beta\rangle \cong \mathrm{Aut}(PSL) \times C_2 ,$$

and we have

Theorem 2

A presentation for Aut(SL) *is*

$$\langle \xi,\eta,\alpha,\beta : \xi^2 = \eta^3 = \alpha^2 = \beta^2 = 1 ,\ \xi^\alpha = \xi,\ \eta^\alpha = \eta^{-1},\xi^\beta = \xi,\ \eta^\beta = \eta,\alpha^\beta = \alpha \rangle .$$

II.3 Aut(PGL)

Hua and Reiner in [6] claim that under any automorphism of PGL(n, $\mathbb{Z}$) , PSL(n, $\mathbb{Z}$) is invariant. That this is so for $n \geq 3$ but not for $n = 2$ is mentioned by Dyer [4] . In our development of Aut(PGL) this fact arises naturally, and indicates how Aut(PGL) is an extension of Aut(PSL) .

We shall make use of the following standard argument.

For any finitely generated group G , let $N = \cap \{K \trianglelefteq G : |G:K| = p\}$ for some fixed prime p (and assume that at least one such K exists). Then $K \trianglelefteq G \Rightarrow N \trianglelefteq G$. Also $G/K \cong C_p \Rightarrow G/K$ abelian $\Rightarrow K \geq G' \Rightarrow N \geq G' \Rightarrow G/N$ is abelian. For all $g \in G$, $g^p \in K \Rightarrow g^p \in N \Rightarrow G/N$ has exponent p . Thus G/N is an elementary abelian p-group (i.e. a product of C_p's , since G is finitely generated). If $M \trianglelefteq G$ satisfies $G/M = C_p \times C_p \times \ldots$ then M

is an intersection of some normal subgroups of index p, so $M \geq N$. Conversely, if $M \geq N$ then G/M is an image of G/N, hence abelian of exponent dividing p, so G/M is an elementary abelian p-group (or the trivial group).

Thus N is the least normal subgroup with G/N an elementary abelian p-group, or equivalently, G/N is the largest homomorphic image isomorphic to $C_p \times C_p \times \ldots$. In particular, normal subgroups N_i with $G/N_i \cong C_p$ correspond to maximal subgroups N_i/N of G/N.

We have

$$PGL = \langle x,y,a : x^2, y^3, a^2, a^{-1}xax, a^{-1}yay \rangle \qquad (*)$$

with PSL a (normal) subgroup of index 2 in PGL. Each $\gamma \in Aut(PGL)$ must send PSL to a subgroup of index 2 - either itself or an isomorphic subgroup - so to find the structure of $Aut(PGL)$ it would be useful to know all the subgroups of PGL of index 2 and how $Aut(PGL)$ permutes them.

Let $N_1, N_2, N_3, \ldots$ be all the subgroups of index 2 in PGL, and let $N = N_1 \cap N_2 \cap N_3 \cap \ldots$. By the above argument PGL/N is the largest homomorphic image isomorphic to $C_2 \times C_2 \times \ldots$. Therefore to find all the N_i's we find the largest factor group of PGL which is a product of C_2's, and then to each subgroup of index 2 will correspond one of the N_i's.

To obtain this factor group we add relations as necessary to the presentation (*) to turn (*) into the presentation of a product

of C_2's . Every element of a product of C_2's has order dividing 2 , so we need the relator y^2 . The presentation (*) then becomes

$$\langle x,y,a : x^2, y^3, y^2, a^2, a^{-1}xax, a^{-1}yay\rangle$$

$$= \langle x,a : x^2, a^2, a^{-1}xax\rangle$$

$$\cong C_2 \times C_2 ,$$

since

$$y^3 = y^2 = 1 \Rightarrow y = y^3y^{-2} = 1 .$$

We obtained this by adding the minimum of relations, so it must be the largest factor group which is a product of C_2's . It has three subgroups of index 2 , namely $\langle x\rangle$, $\langle a\rangle$, and $\langle ax\rangle$ - so PGL has three subgroups of index 2 . These can be realised as the kernels of homomorphisms $PGL \to C_2$. The above indicates that we have a homomorphism

$$\theta : PGL \to \text{Klein's 4-group} = \langle \bar{x},\bar{a} : (\bar{x})^2, (\bar{a})^2, (\bar{\bar{a}\bar{x}})^2\rangle ,$$

$$\theta : x \mapsto \bar{x} , a \mapsto \bar{a} , y \mapsto 1 ,$$

and we can map Klein's 4-group onto $C_2 = \langle t\rangle$ in three ways:

$$\theta_1 : \bar{x} \mapsto t , \bar{a} \mapsto 1 ,$$

$$\theta_2 : \bar{x} \mapsto 1 , \bar{a} \mapsto t ,$$

$$\theta_3 : \bar{x} \mapsto t , \bar{a} \mapsto t .$$

Taking the compositions $\theta \circ \theta_i$ we get the homomorphisms

$$\phi_i : PGL \to C_2 \qquad (i = 1,2,3)$$

given by

$$\phi_1 : x \mapsto t \ , \ a \mapsto 1 \ , \ y \mapsto 1 \ ,$$

$$\phi_2 : a \mapsto t \ , \ x \mapsto 1 \ , \ y \mapsto 1 \ ,$$

$$\phi_3 : x \mapsto t \ , \ a \mapsto t \ , \ y \mapsto 1 \ .$$

We now have $N_i = \ker\phi_i$, $i = 1,2,3$. We can obtain presentations for these by the Reidemeister-Schreier process, for which we need coset representatives. We choose them as follows:

$$\phi_1 : x \mapsto t \Rightarrow x \notin N_1 \ ;$$

choose $\{1,x\}$ as coset representatives

$$\phi_2 : a \mapsto t \Rightarrow a \notin N_2 \ ;$$

choose $\{1,a\}$ as coset representatives

$$\phi_3 : x \mapsto t \Rightarrow x \notin N_3 \ ;$$

choose $\{1,x\}$ as coset representatives.

These sets of representatives trivially form Schreier systems.

We now compute presentations for the three subgroups of index 2, using the Reidemeister-Schreier process with the notation of [12, p.94] . The s-symbols s_{M,A_λ} are the generators of the subgroup H (N_i in this case); M is a coset representative , a_λ is a generator of the group G in question (i.e. PGL) . For $g \in G$, $\bar{g}$ is the coset representative of g . A rewriting process where $\tau(g)$ is g rewritten in terms of the s-symbols is denoted by τ (so that g is rewritten as $\tau(g)$) ; and the symbol '$\approx$' means " is freely equivalent to".

Presentation for N_1

S-symbols:

$$S_{1,x},\ S_{1,y},\ S_{1,a},\ S_{x,x},\ S_{x,y},\ S_{x,a} .$$

S-symbols *satisfying* $Ma_\lambda \approx \overline{Ma}_\lambda$

(which are both generators and relators of N_1 , and which can therefore be discarded): $S_{1,x}$.

S-symbols *not satisfying* $Ma_\lambda \approx \overline{Ma}_\lambda$

(non-trivial generators for N_1) :

$$S_{1,y} = y\overline{y^{-1}} = y1^{-1} = y$$

$$S_{1,a} = a\overline{a^{-1}} = a1^{-1} = a$$

$$S_{x,x} = x^2\overline{x^{2^{-1}}} = x^2 1^{-1} = x^2$$

$$S_{x,y} = xy\overline{xy^{-1}} = xyx^{-1}$$

$$S_{x,a} = xax\overline{a^{-1}} = xax^{-1}$$

Relators:

(i) $\tau(1.x^2.1^{-1}) = \tau(x^2) = S_{x,x}$

(ii) $\tau(x.x^2.x^{-1}) \approx \tau(x^2)$

(iii) $\tau(1.y^3.1^{-1}) = \tau(y^3) = S_{1,y}{}^3$

(iv) $\tau(x.y^3\,x^{-1}) \approx \tau\left((xyx^{-1})^3\right) = S_{x,y}{}^3$

(v) $\tau(1.a^2.1^{-1}) = \tau(a^2) = S_{1,a}{}^2$

(vi) $\tau(x.a^2.x^{-1}) \approx \tau\left((xax^{-1})^2\right) = S_{x,a}{}^2$

(vii) $\tau(1.a^{-1}xax^{-1}.1^{-1}) = \tau(a^{-1}xax^{-1}) = S_{1,a}{}^{-1}.S_{x,a}$

(viii) $\tau(x.a^{-1}xax^{-1}.x^{-1}) \approx \tau(xa^{-1}x^{-1}.x^2.a.x^{-2}) = S_{x,a}{}^{-1}.S_{x,x}.S_{1,a}.S_{x,x}{}^{-1}$

(ix) $\tau(1.a^{-1}yay.1^{-1}) = \tau(a^{-1}yay) = S_{1,a}{}^{-1}.S_{1,y}.S_{1,a}.S_{1,y}$

$$(x) \qquad \tau(x.a^{-1}yay.x^{-1}) \simeq \tau(xa^{-1}x^{-1}.xyx^{-1}.xax^{-1}.xyx^{-1})$$
$$= S_{x,a}^{-1}.S_{x,y}.S_{x,a}.S_{x,y}$$

We now eliminate what generators and relators we can. Relator (i) implies $S_{x,x} = 1$ so eliminate $S_{x,x}$. Relator (vii) implies $S_{1,a} = S_{x,a}$, so eliminate $S_{x,a}$ and (vi). Using (i) and (vii), (viii) becomes $S_{1,a}^{-1}.1.S_{1,a}.1$, so (viii) is redundant. Relator (ii) is also redundant, so we now have generators

$$S_{1,y}\ ,\ S_{1,a}\ ,\ S_{x,y}$$

with relators

$$S_{1,y}^{3},\quad S_{x,y}^{3},\quad S_{1,a}^{3},\quad S_{1,a}^{-1}.S_{1,y}.S_{1,a}.S_{1,y}\ ,\ S_{1,a}^{-1}.S_{x,y}.S_{1,a}.S_{x,y}$$

Writing $f = S_{x,y} = xyx^{-1}$, and using $S_{1,y} = y$, $S_{1,a} = a$ we have

$$N_1 = \langle y,f,a : y^3,\ f^3,\ a^2,\ a^{-1}yay,\ a^{-1}faf \rangle .$$

Presentation for N_2

By its construction $N_2 = \ker(\phi_2)$, and $x,y \in \ker(\phi_2)$ so $PSL \leq N_2$. However, PSL and N_2 each have index 2 in PGL, and so

$$N_2 = PSL = \langle x,y : x^2,\ y^3 \rangle .$$

This is confirmed by the Reidemeister-Schreier process.

Presentation for N_3

Omitting the calculations, which are entirely similar to those for N_1, we have, on putting $g = ax$,

$$N_3 = \langle g,y : g^2, y^3 \rangle \ .$$

We now have presentations for the three subgroups of index 2 in PGL. Clearly N_2 is isomorphic to N_3, so two questions arise. Firstly is there some $\gamma \in \mathrm{Aut(PGL)}$ such that $N_2\gamma = N_3$? Secondly, is N_1 isomorphic to N_2 and N_3? We answer the second question first.

Lemma 3

N_1 *is not isomorphic to* N_2

Proof

If G' denotes the commutator subgroup of any group G, then $G \cong H$ implies $G/G' \cong H/H'$. It follows that $G/G' \ncong H/H'$ implies $G \ncong H$. Given a presentation for G we obtain a presentation for G/G' by making the presentation abelian. We do this for N_1 and N_2.

$$N_1 = \langle y,f,a : y^3, f^3, a^2, a^{-1}yay, a^{-1}faf \rangle$$

so

$$N_1/N_1' = \langle y,f,a : y^3, f^3, a^2, a^{-1}yay, a^{-1}faf, a^{-1}yay^{-1}, a^{-1}faf^{-1}, y^{-1}fyf^{-1} \rangle$$

$$= \langle a : a^2 \rangle \cong C_2 \ .$$

$$N_2 = \langle x,y : x^2,y^3 \rangle$$

so

$$N_2/N_2' = \langle x,y : x^2,y^3,x^{-1}yxy^{-1} \rangle \cong C_2 \times C_3 .$$

Hence N_1 is not isomorphic to N_2 .

We return to the first question, and show that the obvious candidate is indeed an automorphism of PGL. Recalling that N_2 is generated by $\{x,y\}$ and N_3 is generated by $\{ax,y\}$, define γ on the generators of PGL by

$$\gamma : y \mapsto y,\ a \mapsto a,\ x \mapsto ax .$$

Lemma 4

γ extends to an automorphism of PGL, *sending* N_2 *to* N_3 .

Proof.

Firstly, the image of each relator is a relator -

$$\gamma(x^2) = (ax)^2 = axax = a^{-1}xax ,$$

$$\gamma(y^3) = y^3 ,$$

$$\gamma(a^2) = a^2 ,$$

$$\gamma(a^{-1}xax) = a^{-1}(ax)a(ax) = xa^2x = x^2 ,$$

$$\gamma(a^{-1}yay) = a^{-1}yay$$

So γ extends to a homomorphism. Secondly $\gamma^2 = 1$ implies γ has an inverse, namely γ itself, and so is an isomorphism, as required. Clearly $\gamma : N_2 \to N_3$.

We can deduce from this that Aut(PGL) has a subgroup of index 2 which leaves N_2 invariant.

Definition

Let $\overline{\text{Aut}}(\text{PGL})$ denote this subgroup.

It is natural, now, to ask : what is $\overline{\text{Aut}}(\text{PGL})$?

Recall that $N_2 = \text{PSL}$ and that Aut(PSL) is PGL acting by conjugation. Now $\text{Inn}(\text{PGL}) \cong \text{PGL}/Z(\text{PGL}) = \text{PGL}/\{I\} = \text{PGL}$, so that Aut(PGL) contains a subgroup $\big(\text{Inn}(\text{PGL})\big)$, isomorphic to Aut(PSL), which leaves PSL invariant (because $\text{PSL} \lhd \text{PGL}$) and acts on PSL as Aut(PSL) ; and it follows that $\text{Inn}(\text{PGL}) \leq \overline{\text{Aut}}(\text{PGL})$. We show that $\text{Inn}(\text{PGL}) = \overline{\text{Aut}}(\text{PGL})$ by showing that the action of $\theta \in \overline{\text{Aut}}(\text{PGL})$ on PSL determines uniquely its action on $\text{PGL} \setminus \text{PSL}$, and hence $\theta \in \text{Inn}(\text{PGL})$.

Let $\beta, \gamma \in \overline{\text{Aut}}(\text{PGL})$ be such that $\beta\big|_{\text{PSL}} = \gamma\big|_{\text{PSL}}$; then $\beta\gamma^{-1}\big|_{\text{PSL}} = 1$. Put $\theta = \beta\gamma^{-1}$ then θ fixes PSL pointwise, so

$$x\theta = x,\ y\theta = y,\ a\theta = b$$

for some $b \in \text{PGL}$. Since θ is an automorphism, b satisfies the same relations as a , namely

$$b^2 = 1, \quad b^{-1}xb = x, \quad b^{-1}yb = y^{-1} .$$

The second two relations show that b acts by conjugation as an automorphism of PSL , fixing x and inverting y . We must have $b \in PGL \setminus PSL$ because $b = a\theta, a$ leaves PSL invariant, and $a \in PGL \setminus PSL$, so $b = ag$ where $g \in PSL$. We now replace b by ag in the second two relations, giving

$$g^{-1}a^{-1}xag = x , \quad g^{-1}a^{-1}yag = y^{-1} .$$

Since $a^{-1}xa = x$ and $a^{-1}ya = y^{-1}$ (from the relations for PGL), these become

$$g^{-1}xg = x , \; g^{-1}y^{-1}g = y^{-1} ;$$

or equivalently

$$g^{-1}xg = x , \quad g^{-1}yg = y \quad .$$

Thus g commutes with both generators of PSL , hence $g \in Z(PSL) = \{I\}$, so $g = 1$. Working back, $g = 1 \Rightarrow a = b \Rightarrow \theta = 1 \Rightarrow \beta = \gamma$.

Now if $\beta \in \overline{Aut}(PGL)$ then because $Aut(PSL) = PGL = Inn(PGL) \leq \overline{Aut}(PGL)$, β induces a $\gamma \in Aut(PSL)$. But we have seen that $\beta\big|_{PSL} = \gamma\big|_{PSL}$ implies $\beta = \gamma \in Inn(PGL)$, so $\overline{Aut}(PGL) \leq Inn(PGL)$, and hence,

Lemma 5

$$\overline{\mathrm{Aut}}(\mathrm{PGL}) = \mathrm{Inn}(\mathrm{PGL}) \quad .$$

Thus we have

$$\overline{\mathrm{Aut}}(\mathrm{PGL}) = \left\langle \xi, \eta, \alpha : \xi^2,\ \eta^3,\ \alpha^2,\ \alpha^{-1}\xi\alpha\xi,\ \alpha^{-1}\eta\alpha\eta \right\rangle$$

where for $g \in \mathrm{PGL}$,

$$g\xi = x^{-1}gx \quad ,$$

$$g\eta = y^{-1}gy \quad ,$$

$$g\alpha = a^{-1}ga \quad .$$

We also have

$$\mathrm{Aut}(\mathrm{PGL}) = \overline{\mathrm{Aut}}(\mathrm{PGL}) \cup \overline{\mathrm{Aut}}(\mathrm{PGL}).\gamma$$

where $\gamma \in \mathrm{Aut}(\mathrm{PGL})$ is defined by

$$x\gamma = ax \quad ,$$

$$y\gamma = y \quad ,$$

$$a\gamma = a \quad ;$$

and $\gamma^2 = 1$ so $\gamma = \gamma^{-1}$.

To give a presentation for Aut(PGL) we need relations between γ and the other three generators of Aut(PGL).

$$\gamma^{-1}\xi\gamma : x \overset{\gamma^{-1}}{\mapsto} ax \overset{\xi}{\mapsto} xa \overset{\gamma}{\mapsto} x \quad \left(=(ax)^{-1}x(ax)\right) ,$$

$$y \mapsto y \mapsto x^{-1}yx \mapsto (ax)^{-1}y(ax) ,$$

$$a \mapsto a \mapsto x^{-1}ax \mapsto (ax)^{-1}a(ax) ;$$

therefore $\gamma^{-1}\xi\gamma = \alpha\xi$. By similar calculations we obtain $\gamma^{-1}\eta\gamma = \eta$ and $\gamma^{-1}\alpha\gamma = \alpha$, so using the notation $\gamma^{-1}\eta\gamma = \eta^{\gamma}$ etc., we have

Theorem 3

A presentation for Aut(PGL) *is*

$$\left\langle \xi,\eta,\alpha,\gamma : \xi^2 = \eta^3 = \alpha^2 = \gamma^2 = 1, \xi^{\alpha} = \xi, \quad \eta^{\alpha} = \eta^{-1}, \ \xi^{\gamma} = \alpha\xi, \ \eta^{\gamma} = \eta, \ \alpha^{\gamma} = \alpha \right\rangle$$

II.4 Aut(GL)

A presentation for GL is

$$\left\langle X, Y, A : X^4 = Y^6 = A^2 = 1, X^A = X^{-1}, Y^A = Y^{-1}, X^2 = Y^3 \right\rangle ;$$

where

$$X = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} , \quad Y = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} , \quad A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

We know $Aut(PGL)$, so we use the same arguments to try to obtain $Aut(GL)$ from $Aut(PGL)$ as we used to obtain $Aut(SL)$ from $Aut(PSL)$.

$Z(GL) = \{\pm I\}$ and $GL/\{\pm I\} = PGL$, so if $\theta \in Aut(GL)$ and $M \in GL$, θ induces an automorphism θ' on PGL , namely

$$\{M, -M\}\theta = \{M\theta, -M\theta\}$$

Let ψ denote the homomorphism $Aut(GL) \to Aut(PGL)$ defined by $\theta \mapsto \theta'$ as above. We look for the kernel of ψ , hence we look for $\theta \in Aut(GL)$ satisfying $\{M, -M\} = \{M\theta, -M\theta\}$; or equivalently, $M\theta = \pm M$. We need only to consider the action of θ on the generators X, Y, and A of GL ; and then, since θ is a homomorphism, we know its action on all of GL .

Define

$$\theta_X : X \mapsto -X,\ Y \mapsto Y,\ A \mapsto A ,$$

$$\theta_Y : X \mapsto X,\ Y \mapsto -Y,\ A \mapsto A ,$$

$$\theta_A : X \mapsto X,\ Y \mapsto Y,\ A \mapsto -A ,$$

on the generators of GL , then if they extend to autmorphisms of GL , all $\theta \in \ker\psi$ can be obtained as compositions of these θ_M's ($M \in \{X,Y,A\}$) .

Now θ_Y does not extend to an automorphism; for Y has order 6 but $-Y$ has order 3, so the relation $X^2 = Y^3$ of GL is not preserved. However, it is easy to check that θ_A and θ_X preserve the relations of GL, and because their unique homomorphic extensions to GL have finite order, they are bijections, and so are automorphisms of GL. Thus $\ker(\psi) = \{1, \theta_X, \theta_A, \theta_X o \theta_A\}$. (Note that $\theta_A o \theta_X = \theta_X o \theta_A$, and that, for example, $\theta_Y \circ \theta_X$ is not an automorphism; for if it were, then so too would be $(\theta_Y \circ \theta_X) \circ \theta_X^{-1} = \theta_Y$, which is not.) Now $-X = X^{-1}$, so let $\beta = \theta_X$, then

$$\beta : X \mapsto X^{-1}, Y \mapsto Y, A \mapsto A .$$

(c.f. II.2, where for Aut(SL) we defined $\beta : X \mapsto X^{-1}$, $Y \mapsto Y$). Also $-A = X^2 A$, so let $\delta = \theta_A$, then

$$\delta : X \mapsto X, Y \mapsto Y, A \mapsto X^2 A .$$

The autmorphisms β and δ clearly satisfy the relations

$$\beta^2 = \delta^2 = 1, \beta\delta = \delta\beta .$$

Following the argument used for Aut(SL), we would like now to show that $\psi : \mathrm{Aut}(GL) \to \mathrm{Aut}(PGL)$ is an epimorphism. Unfortunately it isn't. To see this, consider $\gamma \in \mathrm{Aut}(PGL)$ defined, as before, by $\gamma : x \mapsto ax, y \mapsto y, a \mapsto a$. If $\gamma = \bar{\gamma}\psi$ for some $\bar{\gamma} \in \mathrm{Aut}(GL)$ then $\bar{\gamma} : A \mapsto \pm A$, $X \mapsto \pm AX$ (the $\pm$'s being independent), but X has order 4, AX and $-AX$ each have order 2 - impossible if $\bar{\gamma} \in \mathrm{Aut}(GL)$.

However, all is not lost. This suggests that if we redefine ψ with the codomain $\mathrm{Aut}(PSL)$ instead of $\mathrm{Aut}(PGL)$ then we might have an epimorphism. Before we can do this, though, we must show that PSL is invariant under $(\mathrm{Aut}(GL))\psi$. (Recall that PGL contains two isomorphic copies of PSL, and that the outer autmorphisms of PGL interchange them.) Now $(\mathrm{Aut}(GL))\psi$ is a subgroup of $\mathrm{Aut}(PGL)$ containing $\mathrm{Inn}(PGL)$ (because every element of PGL 'lifts' to an element of GL which then induces the required inner automorphism) but not containing γ, as we have just seen. But $\mathrm{Inn}(PGL)$ is a maximal subgroup of $\mathrm{Aut}(PGL)$ (it has index 2), so $(\mathrm{Aut}(GL))\psi = \mathrm{Inn}(PGL)$. Since $PSL \lhd PGL$, PSL is invariant under $\mathrm{Inn}(PGL)$, and therefore under $(\mathrm{Aut}(GL))\psi$, as required. Also, $\mathrm{Inn}(PGL) = \mathrm{Aut}(PSL)$ so under ψ, $\mathrm{Aut}(GL)$ induces the full automorphism group of PSL, and $\psi : \mathrm{Aut}(GL) \to \mathrm{Aut}(PSL)$ is an epimorphism.

We need now to find the kernel of this new ψ. We saw that the kernel of $\psi : \mathrm{Aut}(GL) \to \mathrm{Aut}(PGL)$ is $\langle \beta, \delta \rangle$. Now $\psi : \mathrm{Aut}(GL) \to \mathrm{Aut}(PGL)$ is not an epimorphism, but has image $\mathrm{Inn}(PGL) = \mathrm{Aut}(PSL)$ so we can regard it as $\psi : \mathrm{Aut}(GL) \to \mathrm{Aut}(PSL)$, and the kernel will be the same as before.

Now

$$\mathrm{Inn}(GL)\psi = \mathrm{Aut}(PSL) \cong PGL ,$$

and

$$\ker(\psi) = \langle \beta, \delta : \beta^2, \delta^2, (\beta\delta)^2 \rangle \cong C_2 \times C_2$$

so

$$\mathrm{Aut}(GL) = \mathrm{Inn}(GL) \cdot \ker(\psi)$$

$$\cong PGL \cdot (C_2 \times C_2) .$$

Theorem 4

$$\mathrm{Aut}(GL) \cong PGL \times C_2 \times C_2 \ .$$

Proof

We have to show that the above product is a direct product. Firstly we show that $\mathrm{Inn}(GL) \cap \langle \beta, \delta \rangle = \{1\}$ by showing that β, δ, and $\beta\delta \notin \mathrm{Inn}(GL)$.

Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL$. For $\beta, \delta,$ or $\beta\delta$ to be represented by conjugation by M , we require that respectively $A^M = A$ while $X^M = -X$, $A^M = -A$ while $X^M = X$, or $A^M = -A$ while $X^M = -X$; and in all cases we want $Y^M = Y$. By calculation we find that

$$M^{-1}AM = A \Rightarrow \begin{cases} & a = d = \pm 1 \ , \ b = c = 0 \Rightarrow M = \pm I \\ \text{or} & \\ & a = d = 0 \ , \quad b = c = \pm 1 \Rightarrow M = \pm A \ . \end{cases}$$

The latter case gives $M^{-1}XM = -X$, but it also gives $M^{-1}YM = Y^{-1} \neq Y$, so M does not represent β . Similarly we find that

$$M^{-1}AM = -A \Rightarrow \begin{cases} & a = -d = \pm 1 \ , \ b = c = 0 \Rightarrow M = \pm AX \ , \\ \text{or} & \\ & a = d = 0 \ , \ b = -c = \pm 1 \Rightarrow M = \pm X \ , \end{cases}$$

but in neither case do we have $M^{-1}YM = Y$, so M does not represent either δ or $\beta\delta$. It follows that

$$\mathrm{Inn}(GL) \cap \langle \beta, \delta \rangle = \{1\}$$

Secondly we show that the elements of $\langle \beta, \delta \rangle$ commute with all the elements of $\mathrm{Inn}(GL)$.

For any group G , $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$, so in particular $\mathrm{Inn}(GL) \trianglelefteq \mathrm{Aut}(GL)$. Also, $\langle \beta, \delta \rangle = \ker(\psi)$ and so $\langle \beta, \delta \rangle \trianglelefteq \mathrm{Aut}(GL)$. We have seen that $\mathrm{Inn}(GL) \cap \langle \beta, \delta \rangle = \{1\}$, and it follows that $\mathrm{Inn}(GL)$ and $\langle \beta, \delta \rangle$ commute.

We have shown therefore, that

$$\mathrm{Aut}(GL) \cong PGL \times C_2 \times C_2 \ ,$$

as required. Specifically, with the generators as defined below, a presentation for $\mathrm{Aut}(GL)$ is

$$\langle \xi, \eta, \alpha : \xi^2, \eta^3, \alpha^2, \xi^{\alpha} = \xi, \eta^{\alpha} = \eta^{-1} \rangle \times \langle \beta, \delta : \beta^2, \delta^2, (\beta\delta)^2 \rangle$$

where for $L \in GL$,

$$L\xi = X^{-1}LX \ ,$$

$$L\eta = Y^{-1}LY \ ,$$

$$L\alpha = A^{-1}LA \ ,$$

and β and δ are defined by

$$X\beta = X^{-1} \ , \quad Y\beta = Y \ , \quad A\beta = A \ ;$$

$$X\delta = X \ , \quad Y\delta = Y \ , \quad A\delta = X^2A \ .$$

CHAPTER III

III.1 Conjugacy Classes in PSL .

In this section we give a complete classification of the conjugacy classes of PSL , including methods for determining to which class any element of PSL belongs. We treat elements of PSL and PGL as matrices, in both this chapter and the next. (See Chapter I.2).

An important result, easily verified by calculation, is

Proposition 1

Conjugate elements have the same trace.

This is a necessary, but usually not a sufficient condition for two elements of PSL to be conjugate.

Another important result is as follows. Let E,F be elements of PSL , let $X = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $Y = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$ as before, and let E(X,Y) , F(X,Y) be reduced words in X and Y for E,F respectively. Now reduce E(X,Y) and F(X,Y) cyclically to produce C_E and C_F . Then

Proposition 2

E *and* F *are conjugate if and only if* C_E *is a cyclic permutation of* C_F .

The 'if' part is easy to see because cyclic reduction and cyclic permutation can be achieved by conjugation. We shall use '$\sim$' to denote equivalence under conjugation.

Example

Cyclic permutation : $Y^2XYX \sim Y(Y^2XYX)Y^{-1} = XYXY^{-1} = XYXY^2$.

Cyclic reduction : $Y^2XY \sim Y(Y^2XY)Y^{-1} = X$.

In order to implement this result we give a method for expressing an element of PSL as a word in the generators X and Y . Let E be an element of PSL. Consider the first column of E . Our aim is to reduce the entries in this column to 1 and 0 by means of repeatedly subtracting the row containing the smaller in magnitude from the row containing the larger in magnitude (or adding; whichever is appropriate). Let $V = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $W = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$; then this process is equivalent to premultiplying E by either a power of V , which adds the bottom row to the top, or a power of W , which adds the top row to the bottom. The procedure will be quite clear from examples without the need to formulate it precisely. We then change the word thus obtained in V and W to a word in X and Y by using:

$$V = XY^2 \ , \ W = XY \ .$$

Example 1

$$\begin{pmatrix} 12 & -17 \\ 5 & -7 \end{pmatrix} = (V^2V^{-2}) \begin{pmatrix} 12 & -17 \\ 5 & -7 \end{pmatrix} = V^2 \begin{pmatrix} 2 & -3 \\ 5 & -7 \end{pmatrix}$$

$$= V^2W^2 \begin{pmatrix} 2 & -3 \\ 1 & -1 \end{pmatrix}$$

$$= V^2W^2V \begin{pmatrix} 1 & -2 \\ 1 & -1 \end{pmatrix}$$

$$= V^2W^2VW \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$$

$$= V^2W^2VWV^{-2}$$

$$= (XY^2)^2(XY)^2(XY^2)(XY)(XY^2)^{-2}$$

$$= XY^2XY^2XYXYXY^2XYYXYX$$

$$= XY^2XY^2XYXYXY^2XY^2XYX$$

(reduced word),

$$\sim XYXYXY^2XY$$

(cyclically reduced word).

Note that the process must terminate in a finite number of steps because the magnitude of the maximum modulus in the first column is reduced at every step.

However, for elliptic and parabolic elements there exist much simpler methods for determining the conjugacy class to which each belongs.

Elliptic Elements

It is well known that every elliptic element (i.e. having trace $= 0$ or ± 1) is conjugate to just one of X, Y, Y^{-1} [16, p.142]. Since the trace is preserved under conjugation, all elements with

trace = 0 are conjugate to X, and hence to one another. All elements with trace ± 1 are conjugate to one of Y, Y^{-1}.

Let $C = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then

$$C^{-1}YC = \begin{pmatrix} * & b^2+db+d^2 \\ * & * \end{pmatrix} \text{ with trace } = +1 ,$$

$$C^{-1}Y^{-1}C = \begin{pmatrix} * & -(b^2+db+d^2) \\ * & * \end{pmatrix} \text{ with trace } = +1 ;$$

and $b^2 + bd + d^2 > 0$. (This is clear if $bd > 0$; if $bd < 0$ then $-bd > 0$ and $b^2 + bd + d^2 = (b+d)^2 - bd = (b+d)^2 + (-bd) > 0$.)

Thus if $D = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ is elliptic we have:-

$$\beta(\alpha+\delta) > 0 \implies D \sim Y^{+1} ,$$

$$\beta(\alpha+\delta) < 0 \implies D \sim Y^{-1} ,$$

$$\beta(\alpha+\delta) = 0 \implies D \sim X .$$

It is worth noting that because the three expressions are homogeneous of degree 2, it is irrelevant whether one uses $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ or $-\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ for D.

Parabolic Elements

It is also well known that every parabolic element P (i.e. having trace $= \pm 2$, and $\neq I$) is conjugate to one of

$$V^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \text{ or } V^{-n} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} , \quad n \in \mathbb{N} .$$

Considering the standard form of a parabolic element -

$$P = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} 1-abm & a^2m \\ -b^2m & 1+abm \end{pmatrix} = \begin{pmatrix} -a & y \\ -b & x \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & -y \\ b & -a \end{pmatrix}$$

(where, considered as a Möbius transformation of the upper half-plane, P fixes $\frac{a}{b}$ with amplitude $|m|$) - it can be seen that

$$n = \text{h.c.f.}(\beta,\gamma)$$

(with the convention that h.c.f. $(k,0) = k$) and that

$$\beta(\alpha+\delta) > 0 \quad \left(\text{or } \gamma(\alpha+\delta) < 0 \text{ if } \beta = 0\right) \implies P \sim V^{+n} ,$$

$$\beta(\alpha+\delta) < 0 \quad \left(\text{or } \gamma(\alpha+\delta) > 0 \text{ if } \beta = 0\right) \implies P \sim V^{-n} .$$

This gives us complete knowledge of the conjugacy classes of elliptic and parabolic elements, so we now turn our attention to the hyperbolic elements of PSL (i.e. those having $|\text{trace}| \geq 3$). The following treatment of hyperbolic elements covers also parabolic elements and does so naturally and for no extra effort, so we consider them again.

Hyperbolic and Parabolic Elements

We start with the following useful result:

Theorem 1

If trace $E \neq 0$ *or* ± 1 *and* $E \neq I$ *then* E *is conjugate to a cyclically reduced word which starts with* X *and ends with* Y *or* Y^2.

Proof

Let C_E be a cyclically reduced word derived from E and let $\bar{L}(C_E)$ be the length of C_E ; so that in Example 1 above, $\bar{L}(C_E) = 8$. (It would seem more consistent if we wrote Y^{-1} instead of Y^2 since we would like Y^2 to have length 1; but later we want W^n to have length n - hence the bars on the L's in this notation to distinguish the different concepts of length.)

If E is conjugate to one of X, Y, Y^2 then $\bar{L}(C_E) = 1$, but since trace $E \neq 0, \pm 1$ this is not the case, so we must have $\bar{L}(C_E) > 1$. Now C_E cannot both start and end with X or a power of Y since it is cyclically reduced. Thus it must either start with X and end with Y or Y^2 , which is what we would like; or it must end with X and start with Y or Y^2 , in which case conjugating by Y or Y^2 respectively will bring it to the required form.

Replacing XY^2 by V and XY by W in C_E we have immediately

Corollary 1

If trace $E \neq 0, \pm 1$, *and* $E \neq I$ *then* E *is conjugate to a cyclically reduced word* C_E *in the generators* V *and* W *in which every exponent is positive.*

Since all the entries in V and W are non-negative (0 or 1 in fact), this gives us also

Corollary 2

If trace $E \neq 0, \pm 1$ *and* $E \neq I$ *then* E *is conjugate to an element* C_E *whose every entry is non-negative.*

Example

In Example 1 above,

$$C_E = XYXYXY^2XY$$
$$= W^2VW = \begin{pmatrix} 2 & 1 \\ 5 & 3 \end{pmatrix} .$$

For any given t, there are only finitely many matrices with trace t and with all entries non-negative, and hence we deduce the classical result [Newman, 16] that there are only finitely many conjugacy classes of elements of PSL with trace $\pm t$.

We now develop our next result, a complete list of conjugacy classes of PSL, taking our inspiration from Corollary 1.

Definition 1

Let $L(C_E)$ denote the length of C_E written as a word in the generators V and W.

Example

$$L(W^3) = L(W^2V) = L(WVW) = 3 .$$

Note that, in view of Corollary 1, $L(C_E)$ is defined only for E with trace ≥ 2 ; and when it is defined it is equal to $\frac{1}{2}\bar{L}(C_E)$ (as defined for the proof of Theorem 1).

Definition 2

Let $\mathcal{W}_L$ denote the set of all words in V and W (positive powers only) with length L ; thus $\mathcal{W}_L$ contains 2^L elements.

Now $\mathcal{W}_L$ contains many conjugate elements, because if C belongs to $\mathcal{W}_L$ then every cyclic permutation of C also belongs to $\mathcal{W}_L$, and all these are conjugate. On the other hand, they are conjugate to no others, as can be seen by rewriting them in the generators X,Y (using $V = XY^2$, $W = XY$) and applying Proposition 2. Therefore we form another set by choosing just one of the cyclic permutations. This can be done at random (accepting the axiom of choice) or by some system such as the following : choose that which starts with the highest power of V , and if this still leaves a choice, that which is followed by the highest power of W , and so on.

Example

Choose $V^2W^3V^2W$ rather than, say, $V^2WV^2W^3$ or VW^3V^2WV .

Definition 3

Let $\mathcal{C}_L$ denote this set.

Drawing together the various strands we now have

Theorem 2

$$\left\{I, X, Y, Y^{-1}\right\} \cup \left(\bigcup_{L=1}^{\infty} C_L \right)$$

is a complete set of representations (with no redundant elements) of the conjugacy classes of the modular group.

Definition 4

Let $C(PSL)$ denote this set.

We can list the elements of $C(PSL)$ by length, but it is more natural, as we see in the next section, to list them by trace. Such a list can be obtained from a list according to length by using the easily proved result that if a word representing a hyperbolic element has trace t then its length is less than t. See the Appendix for lists of conjugacy classes by length and by trace.

III.2 The Effect of Aut(PSL) *on the Conjugacy Classes of* PSL

We saw in Section II.1 that Aut(PSL) acts on PSL exactly as PGL acting by conjugation. Thus to study the effect of Aut(PSL) on the conjugacy classes of PSL we can look at the effect of conjugation by elements of PGL. It is sufficient to look at the action of the generators of PGL, namely X, Y and A. Now X and Y belong to PSL, so from their very definition the conjugacy classes must be invariant under conjugation by X and Y, i.e.

under the automorphisms ξ and η of Aut(PSL). This leaves only the action of the automorphism α to consider.

We look first at the action of α on the parabolic and hyperbolic conjugacy classes. This gives a reason for grouping these classes by trace rather than by length, for in view of Proposition 1, α must permute the classes within the sets of equal trace.

By calculation we find that

$$A^{-1}V^nA = W^n$$

and

$$A^{-1}W^mA = V^m ,$$

so that

$$V^n\alpha = W^n$$

and

$$W^m\alpha = V^m ,$$

Because α is a homomorphism, this immediately extends to

$$(V^{n_1}W^{n_2}V^{n_3}W^{n_4}\ldots)\alpha = (V^{n_1}\alpha)(W^{n_2}\alpha)(V^{n_3}\alpha)(W^{n_4}\alpha)\ldots$$

$$= W^{n_1}V^{n_2}W^{n_3}V^{n_4}\ \ldots\ .$$

Examples

$$(V^2W^2)\alpha = W^2V^2 \sim V^2W^2$$

$$(VWVW)\alpha = WVWV \sim VWVW$$

$$(V^5W)\alpha = W^5V \sim VW^5 \not\sim V^5W$$

$$(VW^3VW)\alpha = WV^3WV \sim V^3WVW \not\sim VW^3VW\ .$$

The question which naturally arises is, for $C \in \bigcup_{L=1}^{\infty} C_L$, when is $C\alpha \sim C$? Or in other words, when is the conjugacy class represented by C invariant under α ? Clearly this is when $C\alpha$ is a cyclic permutation of C , as in the first two examples.

Theorem 3

$C \sim C\alpha$ *if and only if* $C = B\bar{B}B\bar{B}\ldots B\bar{B}$, *where* B *is a word in* V, W *and* $\bar{B}$ *is the same word in* W, V *(that is,* $\bar{B} = B\alpha$) .

Proof

Clearly if C is of this form then $C\alpha = \bar{B}B\bar{B}B\ldots\bar{B}B \sim C$.

Assume now that $C \sim C\alpha$. Write

$$C = V^{e_1}W^{e_2}V^{e_3}\ldots V^{e_{r-1}}W^{e_r} .$$

Then

$$C\alpha = W^{e_1}V^{e_2}W^{e_3}\ldots W^{e_{r-1}}V^{e_r} .$$

Since $C \sim C\alpha$, for some minimal i (≥ 1 and odd) we have $e_1 = e_{i+1}$, $e_2 = e_{i+2}$,... (suffixes read mod r) so that

$$(V^{e_1}W^{e_2}\ldots V^{e_i})\alpha = W^{e_{i+1}}V^{e_{i+2}}\ldots W^{e_{2i}} ,$$

$$(W^{e_{i+1}}V^{e_{i+2}}\ldots W^{e_{2i}})\alpha = V^{e_{2i+i}}W^{e_{2i+1}}\ldots V^{e_{3i}} ,$$

and so on. Putting $V^{e_1}W^{e_2}\ldots V^{e_i} = B$ and writing $\bar{B}$ for $B\alpha$ we have

$$C = B\bar{B}B\bar{B}\ldots .$$

Now firstly $i|r$, for otherwise $r = mi + n$ with $1 \leq n < i$, and then

$$e_1 = e_{i+1-n} \ , \ e_2 = e_{i+2-n} \ , \ldots .$$

contradicting the minimality of i .

Secondly $2i|r$, because C must end with W^{e_r} , and so must end in $\bar{B}$, not B . Hence

$$C = B\bar{B}B\bar{B}...B\bar{B} \ .$$

as required.

It can be shown that the proportion of words in C_L satisfying $C\alpha \sim C$ tends to 0 as $L \to \infty$; thus in 'most' cases $C\alpha \not\sim C$, and in these cases α interchanges the conjugacy classes represented by C and $C\alpha$. In other words 'most' conjugacy classes occur as one of a distinct pair $\{C, C\alpha\}$.

The classes not yet considered are those represented by I, X, Y, and Y^{-1} . The presentation of PGL shows that

$$A^{-1}XA = X$$

and

$$A^{-1}YA = Y^{-1} \ ,$$

so together with the results for the parabolic and hyperbolic conjugacy classes, we have

Theorem 4

The conjugacy classes of PSL *are invariant under* $\xi,\eta \in$ Aut(PSL) *and are acted on as follows by* $\alpha \in$ Aut(PSL) :

$$I\alpha = I$$

elliptic elements : $X\alpha = X$, $Y\alpha = Y^{-1}$, $Y^{-1}\alpha = Y$,

parabolic elements : $V^n\alpha = W^n$, $W^n\alpha = V^n$,

hyperbolic elements : If C is hyperbolic then C is invariant under α if and only if $C\alpha$ is a cyclic permutation of C ; otherwise C and $C\alpha$ are distinct and are interchanged by α.

III.3 Conjugacy Classes in PGL

In this section we construct a set of conjugacy class representations for PGL similar to that which is constructed for PSL in Section III.1 (see Theorem 2 and Definition 4).

In PSL each element is uniquely expressed as a word in the generators of PSL : X and Y . When we move into PGL this uniqueness of expression is lost. For example,

$$XAY^2XYA = XYAXYA = XYXY^2 .$$

To overcome this problem we make the following

Definition 5

$E \in$ PSL $\lhd$ PGL is said to be in normal form if E is written as a reduced word in X and Y alone ; or, as appropriate, in V and W alone.

Now if $E \in PGL\backslash PSL$ then E can be uniquely expressed as FA where $F \in PSL$ and $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ as usual. Thus :

Definition 6

$E \in PGL\backslash PSL$ is said to be in normal form if E is written as FA where $F \in PSL$ is in normal form. When F is cyclically reduced, we write $F = M_E$.

Given $E \in PSL$ as a matrix we have a procedure (described in Section III.1) for expressing E in normal form. If $E \in PGL\backslash PSL$ then write $E = EA.A$, and $EA \in PSL$ so we apply that procedure to EA to obtain E in normal form. From now on assume all elements of PGL to be in normal form unless otherwise indicated.

Much of the theory we developed for the conjugacy classes of PSL now follows with only slight modification for PGL . First we note that if $E, F \in PGL$ are conjugate then, since $PSL \lhd PGL$, either $E, F \in PSL$ or $E, F \in PGL\backslash PSL$, thus conjugacy classes in PGL are contained either entirely in PSL or entirely in $PGL\backslash PSL$. Those contained in PSL are easily determined : they are $[C] \cup [C\alpha]$ where $C \in \mathcal{C}(PSL)$ (see Definition 4) and $[C]$ is the conjugacy class in PSL represented by C . For suppose $D \sim C$, (that is, conjugate in PGL) then $D = M^{-1}CM$ for some $M \in PGL$. If $M \in PSL$ then $D \in [C]$. If $M \in PGL\backslash PSL$ then $M = LA$ for some $L \in PSL$, and $D = (A^{-1}L^{-1})\, C(LA) = A^{-1}(L^{-1}CL)A \sim A^{-1}CA = C\alpha$, i.e. $D \in [C\alpha]$. Therefore the conjugacy class in PGL containing C is just $[C] \cup [C\alpha]$.

From the pair $\{C, C\alpha\}$ choose one, and for convenience suppose it is C . We make the following

Definition 7

Let $C(PGL)$ denote the set of all chosen C's , $C \in C(PSL)$.

It is clear that $C(PGL)$ is a complete set (with no redundancies) of representations of the conjugacy classes of PGL lying inside PSL.

We now turn our attention to the conjugacy classes in $PGL \setminus PSL$. Assume that $E \in PGL \setminus PSL$, so $E = FA$ where $F \in PSL$ is in normal form. First we cyclically reduce E ,transferring letters from the front to the back by conjugation, and normalizing at each stage using $AX = XA$, $AY = Y^2A$.

Example

$$E = XY^2XYXA \sim Y^2XYXAX = Y^2XYX.XA = Y^2XYA$$

$$\sim XYAY^2 = XY.YA = XY^2A$$

$$= M_E A \ .$$

Now E will be cyclically reduced when M_E (assumed for the moment to have $\bar{L}(M_E) > 1$) is a word beginning with X and ending with a power of Y , or vice versa. In the latter case one further cyclic permutation will bring M_E to the convenient former form. Without repeating a lot of detail, this gives us a result corresponding to Corollary 1 :

Theorem 5

If $\bar{L}(M_E) > 1$ *(that is,* $M_E \neq I, X, Y, Y^2$*) then* E *is conjugate to* MA *, where* $M \in W_L$ *for some* L .

Thus,with the obvious notation,

Corollary 3

All conjugacy classes in PGL\PSL *are represented in* $\{I, X, Y, Y^2\}A \cup (\bigcup_{L=1}^{\infty} W_L A)$.

Of course, most are represented many times, as was the case with PSL , so now we perform a similar trick to eliminate repetitions (see Definitions 2 and 3). As before, for each $E \in \bigcup_{L=1}^{\infty} W_L A$ we take all normalized cyclic permutations of E , and since these are all conjugate to each other we choose just one, call it D , as a representative (we can do this by applying the rule given just before Definition 3 to all the F's , where $E \sim FA \in W_L A$) . Form another set consisting of the chosen representatives D , where $D = CA$ and $C \in W_L$.

Definition 8

Let $\mathcal{D}_L$ denote this set.

Note that $\mathcal{D}_L \neq C_L A$.

So far, the 'factoring out' of cyclic permutations we have performed ensures that for $D, E \in \mathcal{D}_L$, D, E are not conjugate by any element of PSL . In fact they are not conjugate by any element of PGL ; for suppose they are , then for some $F \in$ PGL\PSL , $E = F^{-1}DF$. But we can write $F = DB$ where $B \in$ PSL , whence $E = (B^{-1}D^{-1})D(DB) = B^{-1}DB$ and E is conjugate to D by $B \in$ PSL , a contradiction.

Applying normalized cyclic permutations and the above considerations to the set $\{A, XA, YA, Y^2A\}$ reduces it to $\{A, XA, YA\}$ as a set of conjugacy class representations , so we now have

Theorem 6

$\{A, XA, YA\} \cup \left(\bigcup_{L=1}^{\infty} \mathcal{D}_L\right)$ *is a complete set of representatives (with no redundant elements) of the conjugacy classes of* PGL *contained in* PGL\PSL .

Definition 9

Let $\mathcal{D}$(PGL) denote this set.

This, together with Definition 7 gives us

Theorem 7

$\mathcal{C}$(PGL) $\cup$ $\mathcal{D}$(PGL) *is a complete set of representatives of the conjugacy classes of* PGL .

III. 4 The Effect of Aut(PGL) *on the Conjugacy Classes of* PGL

Aut(PGL) is generated by ξ, η, α, and γ (see Section II.3). However, the first three automorphisms represent conjugation by X, Y , and A respectively, so these will leave each conjugacy class invariant. This leaves only the action of the outer automorphism γ to consider. Recall that γ sends PSL to $N_3 = \langle AX, Y \rangle$. Let $\Gamma^* = PSL \cap N_3 = \langle Y, XYX \rangle$. Now $\Gamma^* \neq PSL$ because $X \notin \Gamma^*$; but $X, Y \in \Gamma^* \cup \Gamma^*X$ so $PSL = \Gamma^* \cup \Gamma^*X$ and $[PSL:\Gamma^*] = 2$; hence $[PGL : \Gamma^*] = 4$. It is easy to check that the cosets in PGL of Γ^* are

$$\Gamma^*, \ \Gamma^*X \ , \ \Gamma^*AX \ , \ \Gamma^*A$$

and that Γ^* and Γ^*A are invariant under γ , while Γ^*X and Γ^*AX are interchanged by γ.

Now $\Gamma^* \lhd PGL$, so conjugacy classes of PGL are contained either entirely within Γ^* or entirely without Γ^* . But similarly every conjugacy class of PGL lies entirely within PSL or entirely without PSL , and by similar arguments we conclude that every conjugacy class of PGL lies entirely within one of the four cosets of Γ^* . This gives us three cases to consider, according as $[C]$ - the conjugacy class represented by C where $C \in \mathcal{C}(PGL) \cup \mathcal{D}(PGL)$ - lies in Γ^* , $\Gamma^*X \cup \Gamma^*AX$, or $\Gamma^* A$.

Case 1 : $[C] \subset \Gamma^*X \cup \Gamma^*AX$

Since γ interchanges Γ^*X and Γ^*AX , $[C]$ must lie in one of Γ^*X, Γ^*AX and $[C]\gamma = [C\gamma]$ must lie in the other, hence we cannot have $[C\gamma] = [C]$, and the effect of γ is to interchange all pairs $([C], [C\gamma])$. The elements C belonging to $\Gamma^*X \cup \Gamma^*AX$ may be characterized as those for which the exponent sum of the X's is odd. Equivalently, assuming $C \in \mathcal{C}(PGL) \cup \mathcal{D}(PGL)$ to be written in normal form, they are X, XA , and all C such that L(C) - the length of C - is odd. Those which end in A belong to Γ^*AX , the others to Γ^*X .

Definition 10 :

For $C \in PSL$, L(C) was defined in Definition 1. For $C \in PGL \backslash PSL$ write C in normal form as $M_C A$, then define $L(C) = L(M_C)$.

Case 2 : $[C] \subset \Gamma^*$

Γ^* is invariant under γ , so in this case we have the possibility that $[C] = [C\gamma]$. The $C \in \Gamma^*$ may be characterized as $1, Y$, and those having even length and not ending in A . Now $1\gamma = 1$ and

$Y\gamma = Y$, so $[1]$ and $[Y]$ are invariant under γ . To investigate the rest, we may assume that they are written in normal form as words of even length in V and W .

Recall that

$$X\gamma = AX \ , \ Y\gamma = Y \ , \ A\gamma = A$$

so that

$$V\gamma = AV \ , \ W\gamma = AW \ .$$

We adopt the notation

$$\bar{V} = AVA = W \ , \ \bar{W} = AWA = V \ ,$$

so that if

$$C = T_1 T_2 \ldots . T_n$$

where each T_i is V or W and n is even, then

$$C\gamma = AT_1 AT_2 \ldots . AT_n$$

$$= \bar{T}_1 T_2 \bar{T}_3 T_4 \ldots . \bar{T}_{n-1} T_n \ .$$

Suppose $C\gamma \sim C$, then for some $M \in PGL$,

$$C = M^{-1} C\gamma M \ .$$

If $M \in PSL$ then $M^{-1} C\gamma M$ reduces to a cyclic permutation of $C\gamma$, so C is equal to a cyclic permutation of $C\gamma$. If $M \notin PSL$ then $M = AL$ where $L \in PSL$, and then

$$C = L^{-1} AC\gamma AL$$

$$= L^{-1} (AC\gamma A) L$$

$$= L^{-1} (C\gamma\alpha) L$$

and $L \in PSL$ so C is equal to a cyclic permutation of $C\gamma\alpha$. Now

$$C\alpha = ACA = AT_1 \ldots T_n A$$

$$= AT_1A.AT_2A \ldots AT_nA$$

$$= \bar{T}_1\bar{T}_2 \ldots \bar{T}_n$$

and clearly $\bar{\bar{T}}_i = T_i$, so

$$C\gamma\alpha = T_1\bar{T}_2T_3\bar{T}_4 \ldots T_{n-1}\bar{T}_n$$

Thus for some m,

$$T_1T_2 \ldots T_n = \begin{cases} T_{m+1}\bar{T}_{m+2}T_{m+3}\bar{T}_{m+4} \ldots T_{m-1}\bar{T}_m \\ \text{or} \\ \bar{T}_{m+1}T_{m+2}\bar{T}_{m+3}T_{m+4} \ldots \bar{T}_{m-1}T_m \end{cases}$$

and we have to consider two cases separately : m even and m odd.

Case 2(a) : m even

Firstly, if C is a cyclic permutation of $C\gamma$ then

$$C = T_1T_2 \ldots T_n = \bar{T}_{m+1}T_{m+2}\bar{T}_{m+3}T_{m+4} \ldots T_n\bar{T}_1 \ldots \bar{T}_{m-1}T_m \qquad (1)$$

and, reading suffixes modulo n if necessary, we have

$$T_1 \ldots T_m = \bar{T}_{m+1}T_{m+2} \ldots \bar{T}_{2m-1}T_{2m},$$

$$T_{m+1} \ldots T_{2m} = \bar{T}_{2m+1}T_{2m+2} \ldots \bar{T}_{3m-1}T_{3m},$$

$$T_{2m+1} \ldots T_{3m} = \bar{T}_{3m+1}T_{3m+2} \ldots \bar{T}_{4m-1}T_{4m}, \quad \text{etc.}$$

Thus if we write $B = T_1 \ldots T_m$ we can deduce

$$T_{m+1} \cdots T_{2m} = B\gamma \ ,$$

$$T_{2m+1} \cdots T_{3m} = B \ ,$$

$$T_{3m+1} \cdots T_{4m} = B\gamma \ , \quad \text{etc.}$$

From (1) we see that C ends with $B\gamma$, and so

$$C = B.B\gamma.B.B\gamma \ \ldots \ B.B\gamma \ .$$

(It should not be inferred that the final sequence of $B.B\gamma$'s necessarily coincides with the initial sequence of $B.B\gamma$'s (that is, that $2m|n$) either in this case or in the other, similar cases.)

Secondly, if C is a cyclic permutation of $C\gamma\alpha$ then

$$C = T_1T_2 \cdots T_n = T_{m+1}\bar{T}_{m+2}T_{m+3}\bar{T}_{m+4} \cdots \bar{T}_nT_1 \cdots T_{m-1}\bar{T}_m \quad (2)$$

and we obtain

$$T_1 \cdots T_m = T_{m+1}\bar{T}_{m+2} \cdots T_{2m-1}\bar{T}_{2m} \ , \text{ etc.}$$

Again, writing $B = T_1 \ldots T_m$ we deduce

$$T_{m+1} \cdots T_{2m} = B\gamma\alpha \ ,$$

$$T_{2m+1} \cdots T_{3m} = B \ ,$$

$$T_{3m+1} \cdots T_{4m} = B\gamma\alpha \ , \quad \text{etc.},$$

and we see from (2) that C ends in $B\gamma\alpha$, and so

$$C = B.B\gamma\alpha.B.B\gamma\alpha \ \ldots \ B.B\gamma\alpha \ .$$

Case 2(b), m odd, is similar, as are cases 3(a) and 3(b) dealing with $[C] \subset \Gamma^*A$, except that in case 3(a) (corresponding to (c) and (d) in the following theorem) the pattern with which C ends is found to be different from that with which it begins, so that C must contain two interlocking patterns. Omitting the proofs we have:

Theorem 8

A necessary condition for $C \in \mathcal{C}(PGL) \cup \mathcal{D}(PGL)$ *to satisfy* $[C] = [C\gamma]$ *is that*

$$C \in \{1, Y, A, YA\}$$

or C *is of one of the following forms:*

(a)	$B.B\gamma.B.B\gamma \ \ldots \ B.B\gamma$	$C \in \Gamma^*$	m *even*
(b)	$B.B\gamma\alpha \ B.B\gamma\alpha \ \ldots \ B.B\gamma\alpha$		
(c)	$B.B\gamma.B.B\gamma \ \ldots \ B\gamma\alpha.A$	$C \in \Gamma^*A$	
(d)	$B.B\gamma\alpha.B.B\gamma\alpha \ \ldots \ B\gamma.A$		
(e)	$J.J \ \ldots \ J$	$C \in \Gamma^*$	m *odd*
(f)	$K.K \ \ldots \ K$		
(g)	$J.J \ \ldots \ J.B.B\gamma.A$	$C \in \Gamma^*A$	
(h)	$K.K \ \ldots \ K.B.B\gamma\alpha.A$		

where for some m , $B = T_1T_2 \ldots T_m$ ($T_i = V$ *or* W) *and*

$J = B.B\gamma.B\alpha.B\gamma\alpha$, $K = B.B\gamma\alpha.B\alpha.B\gamma$.

In all but cases (c) and (d) examples are easily found.

CHAPTER IV

The congruence subgroups of PSL and of PGL consist of those elements whose matrix-entries satisfy various congruence relations, so their definitions depend heavily on the traditional representation of PGL by projective transformations. The aim of this chapter is to investigate to what extent these congruence subgroups are invariant under the automorphism groups of PSL and PGL. If they are invariant, they can be regarded as features of the abstract groups PSL and PGL; whereas if they are not invariant, then their definitions depend essentially on the projective representation of PGL, so we must regard them as number-theoretic or geometric, rather than group-theoretic, in character.

There is no difficulty with PSL , since Aut PSL can be identified with PGL acting by conjugation on PSL (Chapter II.1). Now the congruence subgroups of PSL are those containing some principal congruence subgroup $\Gamma(n)$, consisting of the elements of PSL $(= \Gamma)$ congruent to $\pm I \mod n$, where $n \in \mathbb{N}$. Since $\Gamma(n)$ is normal in PGL for each n , it follows that Aut PSL preserves the class of congruence subgroups of PSL. In particular, the principal congruence subgroups are all characteristic in PSL.

The situation for PGL is quite different. In 1952 Hua and Reiner [6] determined the automorphism groups of various projective groups, and they asserted that PSL is a characteristic subgroup of PGL, and that all automorphisms of PGL are inner. If true, these assertions would solve our problem, but as pointed out in Chapter II.3 they are false: the outer automorphism group Out PGL of PGL has order 2, being generated by an automorphism γ which does not leave PSL invariant.

We show that, with only finitely many exceptions, γ maps congruence subgroups to noncongruence subgroups, and in particular, we see that only finitely many congruence subgroups are characteristic in PGL, in contrast with the situation in PSL.

In view of this, it is hardly surprising that there seems to be no straightforward number-theoretic interpretation of γ. Nevertheless, γ does have a realization in the theory of maps on surfaces, which we consider in the next chapter.

IV.1 Preliminaries

We record here the presentations of Γ = PSL and PGL :

$$\Gamma = \langle x, y : x^2 = y^3 = 1 \rangle ,$$

$$PGL = \langle x, y, a : x^2 = y^3 = a^2 = 1 , x^a = x, y^a = y^{-1} \rangle .$$

The following results follow easily from these presentations.

Proposition 1.

(i) $PGL^{ab} \cong C_2 \times C_2$,

(ii) $PGL' = \langle y \rangle^{PGL} = \langle y, y^x : y^3 = (y^x)^3 = 1 \rangle \cong C_3 * C_3$,

(iii) $(PGL')^{ab} \cong C_3 \times C_3$

(iv) $PGL'' \cong C_\infty * C_\infty * C_\infty * C_\infty$.

The fourth of these follows from Newman [16, Theorem VIII,7]. We can take as a basis $[y, y^x]$, $[y^{-1}, y^x]$, $[y, (y^x)^{-1}]$, $[y^{-1}, (y^x)^{-1}]$. Notice that $PGL' = \Gamma^* (= \Gamma \cap \Gamma\gamma)$, so the elements of PGL' are just those words in x and y for which x has even exponent-sum; for example $v^k = (xy^2)^k$ belongs to PGL' if and only if k is even.

We have $v\gamma = av = \pm\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, and the following result is easily verified by induction. Let $f = v\gamma$.

Proposition 2

For each $k \geq 1$, $f^k = (v\gamma)^k = \begin{pmatrix} f_{k-1} & f_k \\ f_k & f_{k+1} \end{pmatrix}$ where (f_k) is the Fibonacci sequence given by $f_0 = 0$, $f_1 = 1$, $f_k = f_{k-1} + f_{k-2}$.

Since $\det(v\gamma) = -1$, $(v\gamma)^k \in \Gamma$ if and only if k is even. Later we shall need to calculate $v^k\gamma = (v\gamma)^k = f^k$ for various k, so we record here part of the Fibonacci sequence in both $\mathbb{Z}$ and $\mathbb{Z}_{125}$.

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17...
f_k	0	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610	987	1597...
$f_k \bmod 125$	0	1	1	2	3	5	8	13	21	34	55	89	19	-17	2	-15	-13	-28...

IV.2 Congruence Subgroups and Quotients

Let $P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ represent a typical element of PGL. For each integer $n \geq 1$, we define:

$$M(n) = \{P \in \mathrm{PGL} : a \equiv d,\ b \equiv c \equiv 0 \mod n\},$$

$$N(n) = M(n) \cap \Gamma$$

$$= \{P \in \Gamma : a \equiv d,\ b \equiv c \equiv 0 \mod n\},$$

and $\Gamma(n) = \{P \in \Gamma : a \equiv d \equiv \pm 1,\ b \equiv c \equiv 0 \mod n\}$.

These are normal subgroups of PGL, satisfying

$$M(n) \geq N(n) \geq \Gamma(n).$$

They are sometimes called the principal congruence subgroups of level n, though this term is usually reserved for $\Gamma(n)$. Clearly $M(1) = \mathrm{PGL}$ and $N(1) = \Gamma(1) = \Gamma$.

Notice that if $P \in M(n)$, then

$$\pm 1 = \det P \equiv a^2 \bmod n ,$$

and it follows easily that

$$|M(n) : N(n)| = \begin{cases} 2 & \text{if } -1 \text{ is a square mod } n , \\ 1 & \text{otherwise} . \end{cases}$$

In particular, $M(n) = N(n)$ if n is divisible by 4 or by a prime $p \equiv 3 \bmod 4$.

Similarly if $P \in N(n)$ then $1 = \det P \equiv a^2 \bmod n$, so that $p^2 \equiv \begin{pmatrix} a^2 & 0 \\ 0 & a^2 \end{pmatrix} \equiv I \bmod n$, and it follows that $N(n)/\Gamma(n) \cong \{a \in \mathbb{Z}_n : a^2 = 1\}/\{\pm 1\}$, an elementary abelian 2-group of rank $\pi(n) - \delta$, where $\pi(n)$ is the number of distinct primes dividing n, and

$$\delta = \begin{cases} 0 & \text{if } 8 | n \text{ or } n = 1 , \\ 2 & \text{if } 2 \| n \text{ and } n \neq 2 , \\ 1 & \text{otherwise.} \end{cases}$$

In particular, $N(n) = \Gamma(n)$ if n is $1, 2, 4, 6$ or an odd prime power; whereas, for example, $|N(12):\Gamma(12)| = 2$, $|N(60): \Gamma(60)| = |N(300): \Gamma(300)| = 4$ and $|N(600) : \Gamma(600)| = 8$.

We have $N(n) \leq N(m)$ if and only if $m | n$, with a similar result for $M(n)$ and $\Gamma(n)$. In particular, if n is even then

$$N(n) \leq N(2) = \Gamma(2) = \langle v^2 \rangle^{PGL} \leq PGL' = \Gamma^* ,$$

whereas if n is odd then $v^n \in N(n) \setminus (\Gamma^* \cap N(n))$. We define

$$N^*(n) = N(n) \cap \Gamma^* ,$$

a normal subgroup of PGL satisfying

$$\left|N(n) : N^*(n)\right| = \begin{cases} 1 & \text{if } n \text{ is even} , \\ 2 & \text{if } n \text{ is odd} . \end{cases}$$

We define

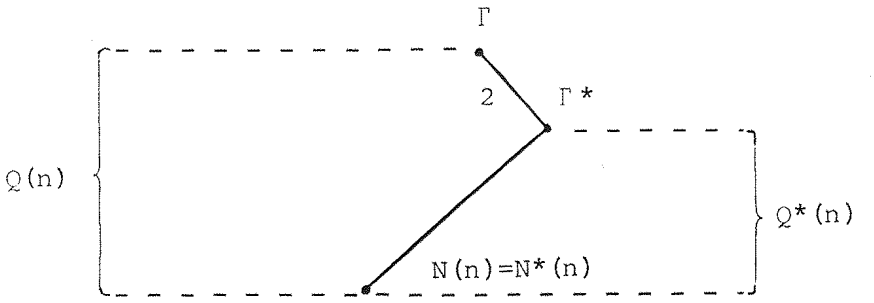
$$Q(n) = \Gamma/N(n)$$

and

$$Q^*(n) = \Gamma^*/N^*(n)$$

so that $Q^*(n) \cong Q(n)$ for n odd, whereas $Q^*(n)$ is a subgroup of index 2 in $Q(n)$ for n even.

n even



n odd

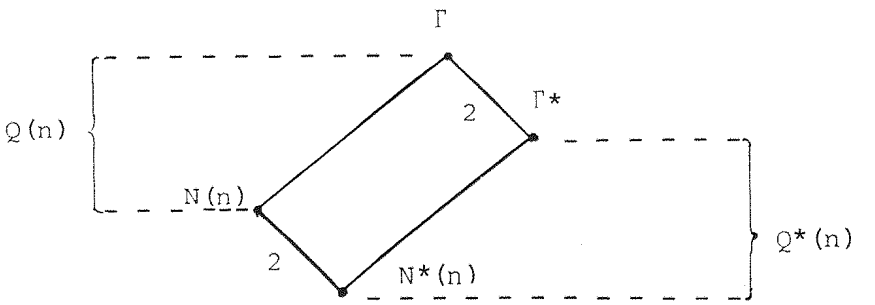


Figure 1.

Newman [16] shows that $N(m)N(n) = N((m,n))$ and $N(m) \cap N(n) = N([m,n])$, from which it follows that

$$Q(n) = \bigtimes_{p^e \| n} N(n/p^e)/N(n)$$

$$\cong \bigtimes_{p^e \| n} \Gamma/N(p^e) = \bigtimes_{p^e \| n} Q(p^e) ,$$

and similarly,

$$Q^*(n) \cong \bigtimes_{p^e \| n} Q^*(p^e) ,$$

where p^e ranges over all the maximal prime powers dividing n.

IV.3 Normal Subgroups of Direct Products

These decompositions reduce the study of the groups $Q(n)$ and $Q^*(n)$ to the case $n = p^e$. In particular, we can find the normal subgroups of $Q(n)$ and $Q^*(n)$ by using the following results due to McQuillan [13].

Proposition 3

Let $N \trianglelefteq G = G_1 \times G_2$, let $F_i = N \cap G_i$ and let N_i be the projection of N onto G_i, for $i = 1, 2$. Then $F_i \trianglelefteq G_i$, $N_i/F_i \leq Z(G_i/F_i)$, and $N_1/F_1 \cong N_2/F_2$.

Corollary 1

Suppose that for all homomorphic images $\bar{G}_i$ of G_i, $i = 1,2$, $Z(\bar{G}_1) \geq A_1 \cong A_2 \leq Z(\bar{G}_2)$ implies that A_1 and A_2 are trivial.

Then each normal subgroup N of $G_1 \times G_2$ has the form $N = N_1 \times N_2$ where $N_i \trianglelefteq G_i$ for $i = 1, 2$.

Proof

Putting $\bar{G}_i = G_i/F_i$ and $A_i = N_i/F_i$ in Proposition 3, we see that N_i/F_i is trivial, so $N_i = F_i$ for $i = 1, 2$. Since $F_1 \times F_2 \leq N \leq N_1 \times N_2$, we must have $N = N_1 \times N_2$, with $N_i \trianglelefteq G_i$, since $N \trianglelefteq G$.

Notice that for finite groups G_i, the hypothesis of Corollary 1 is equivalent to $\left(|Z(\bar{G}_1)|, |Z(\bar{G}_2)|\right) = 1$ for all images $\bar{G}_i$ of G_i.

To apply these results to $Q(n)$ and $Q^*(n)$ we need to know the normal structure of $Q(p^e)$ and $Q^*(p^e)$.

IV.4 Normal Structure of $Q(p^e)$

For any prime p, $Q(p^e)$ has normal subgroups

$$Q(p^e) = Q_0(p^e) \triangleright Q_1(p^e) \triangleright \ldots \triangleright Q_e(p^e) = 1 ,$$

where

$$Q_i(p^e) = N(p^i)/N(p^e) \qquad \text{for } i = 0,1,2,\ldots,e.$$

Then

$$Q_0(p^e)/Q_1(p^e) \cong \Gamma/N(p) = PSL(2, p) ,$$

which is simple for $p > 3$; and for $i > 0$ and $p \geq 3$ we have

$$Q_i(p^e)/Q_{i+1}(p^e) \cong C_p \times C_p \times C_p .$$

Now for $p \geq 3$, $Q(p^e) = PSL(2, p^e)$, and $Q(2^e) \cong PSL(2,2^e)/C_2$ for $e > 2$, so we can use the results of McQuillan [13, 14] to find the normal structure of $Q(p^e)$.

For $p > 3$, the subgroups $Q_i(p^e)$ are the only normal subgroups of $Q(p^e)$, so they are all characteristic in $Q(p^e)$.

If $p = 3$ then $Q(3^e)$ has one extra normal subgroup $R(3^e)$, corresponding to the fact that $Q_o(3^e)/Q_1(3^e) \cong PSL(2, 3) \cong A_4$ is not simple. We have a chief series

$$Q(3^e) = Q_o(3^e) \triangleright R(3^e) \triangleright Q_1(3^e) \triangleright Q_2(3^e) \triangleright \ldots \triangleright Q_e(3^e) = 1,$$

with $Q_o(3^e)/R(3^e) \cong C_3$, $R(3^e)/Q_1(3^e) \cong C_2 \times C_2$, and all other chief factors isomorphic to $C_3 \times C_3 \times C_3$. Again, all normal subgroups are characteristic. We define R to be the inverse image of $R(3^e)$ in Γ, so that $R = \langle x \rangle^{PGL}$ is the unique normal subgroup of index 3 in Γ .

If $p = 2$ then $Q_o(2^e)/Q_1(2^e) \cong PSL(2,2) \cong S_3$ is not simple. We have

$$Q(2^e) = Q_o(2^e) \triangleright Q^*(2^e) \triangleright Q_1(2^e) \triangleright Q_2(2^e) \triangleright \ldots \triangleright Q_e(2^e) = 1 ,$$

where

$$Q_o(2^e)/Q^*(2^e) \cong C_2 \ , \ Q^*(2^e)/Q_1(2^e) \cong C_3 \ ,$$

$Q_1(2^e)/Q_2(2^e) \cong Q_2(2^e)/Q_3(2^e) \cong C_2 \times C_2$, and $Q_i(2^e)/Q_{i+1}(2^e) \cong C_2 \times C_2 \times C_2$ for $2 < i < e$. In general there may be other normal subgroups of $Q(2^e)$, but they are all contained in $Q_2(2^e)$. Thus $Q^*(2^e)$, $Q_1(2^e)$, and $Q_2(2^e)$ are characteristic in $Q(2^e)$, and indeed in $Q^*(2^e)$. It will be useful to note that $Q(2^e)/Q_2(2^e) \cong Q(4) \cong S_4$ and $Q^*(2^e)/Q_2(2^e) \cong Q^*(4) \cong A_4$.

Notice that the centre of $Q(p^e)$ is trivial, except when $p = 2$ and $e \geq 4$ in which case it has order 2, generated by $\begin{pmatrix} 1+2^{e-2} & 2^{e-1} \\ 2^{e-1} & 1-2^{e-2} \end{pmatrix}$. For $p > 3$, $Q(p^e)$ is perfect, whereas it is soluble for $p \leq 3$.

IV.5 Subgroups of N(12)

It will be useful for us to know the normal and the characteristic subgroups of PGL containing N(12). Now N(3), the normal closure $\langle v^3 \rangle^{PGL}$ of $v^3 = (xy^2)^3$, is mapped by γ to $\langle (av)^3 \rangle^{PGL}$ - a subgroup of index $|PGL : N(3)| = 24$ in PGL. In the extended octahedral group $PGL/N(4) = PGL/\langle v^4 \rangle^{PGL} \cong S_4 \times C_2$, $(av)^3$ represents the central involution, so $\langle (av)^3, v^4 \rangle^{PGL}$ has index $|S_4| = 24$ also, and hence coincides with its subgroup $\langle (av)^3 \rangle^{PGL} = N(3)\gamma$. Thus $\Gamma \cap N(3)\gamma = N(4)$, so $N(3).N(3)\gamma$ contains $N(3)N(4) = \Gamma$, properly since $(av)^3 \notin \Gamma$, giving $N(3).N(3)\gamma = PGL$. We have

$$N(3) \cap N(3)\gamma = N(3) \cap \Gamma \cap N(3)\gamma = N(3) \cap N(4) = N(12),$$

so

$$\begin{aligned} PGL/N(12) &= \big(N(3)/N(12)\big) \times \big(N(3)\gamma/N(12)\big) \\ &\cong \big(PGL/N(3)\gamma\big) \times \big(PGL/N(3)\big) \\ &\cong S_4 \times S_4 \end{aligned}$$

with γ acting by transposing the direct factors.

We can use Proposition 3 to find the normal subgroups of $S_4 \times S_4$, and hence those of PGL containing N(12). There are 17, consisting of 16 of the form AB where $N(3) \trianglerighteq A \geq N(12)$ and $N(3)\gamma \trianglerighteq B \geq N(12)$, and one other, which we call Γ_o (the N_1 of II.3), of index 2 in PGL.

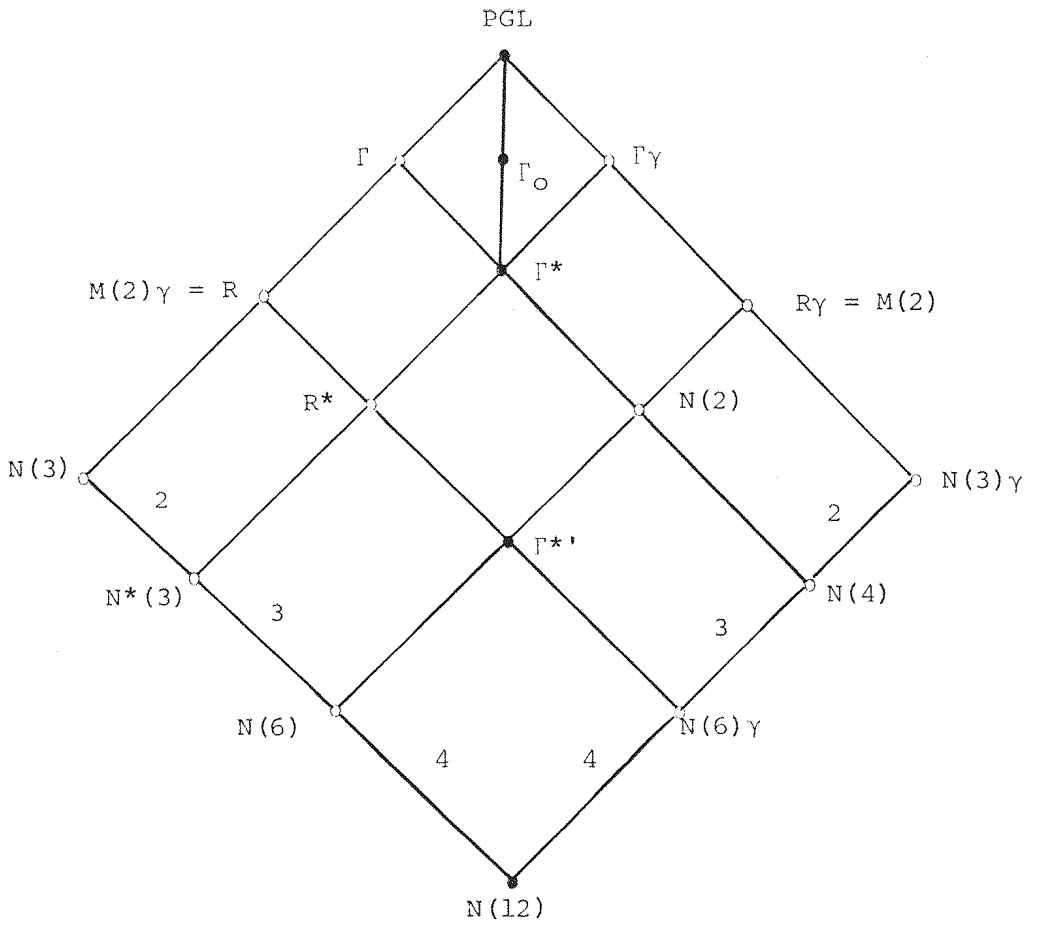


Figure 2.

Since γ transposes the two direct factors of PGL/N(12), just 5 of these 17 normal subgroups are γ-invariant and hence characteristic in PGL ; namely PGL, Γ_o , Γ^*, $\Gamma^{*'}$, and N(12).

We shall see shortly (Lemma 1) that $M(5^c)$ is characteristic in PGL only for c = 0, 1, and 2. We now state our main results.

Theorem 1.

$PGL \trianglerighteq K \gtrsim N(n)$ *for some* n *if and only if* $K = L \cap M(5^c)$ *where* $L = PGL, \Gamma_0, \Gamma^*, \Gamma^{*\prime}$, *or* $N(12)$ *and* $c = 0, 1,$ *or* 2. *There are* 15 *such groups* K *all containing* $N(12) \cap M(5^2) = N(300)$.

Corollary 2.

Let C be a congruence subgroup of PGL such that C^γ is also a congruence subgroup; then $C \gtrsim \Gamma(600)$.

Thus, with only finitely many exceptions, γ maps congruence subgroups to non-congruence subgroups. In particular, only finitely many congruence subgroups are characteristic in PGL.

IV.6 Proof of Theorem 1.

The main part of the proof consists of determining all characteristic subgroups K of PGL containing some $N(n)$ and contained in Γ (or equivalently, in Γ^*); this done, we then remove the restriction $K \lesssim \Gamma$. The reason for imposing the condition $\Gamma \gtrsim K \gtrsim N(n)$, rather than the more natural $PGL \gtrsim K \gtrsim \Gamma(n)$, is that the normal structure of $Q(n)$ is more easily described (IV.3 and IV.4) than that of $PGL/\Gamma(n)$. We shall exploit this as follows.

For any K such that $\Gamma \gtrsim K \gtrsim N(n)$, we define $\bar{K} = K/N(n)$. (Usually n will be chosen to be minimal with respect to $K \gtrsim N(n)$.) Thus $\bar{K} \lesssim \Gamma/N(n) = Q(n)$, and if $K \not\trianglelefteq \Gamma$ (e.g. if $K \trianglelefteq PGL$) then $\bar{K}$ must be a normal subgroup of $Q(n)$ as described earlier in this chapter so limiting the possibilities for K. A second general argument we shall use is the following.

For any $K \trianglelefteq \Gamma^*$ (in particular any characteristic subgroup of PGL contained in Γ) we define $\tilde{K} = \Gamma^*/K$. Now if K is characteristic in PGL, then γ induces an automorphism of $\tilde{K}$, so if N is any normal subgroup of PGL such that $\Gamma^* \geq N \geq K$ and $N/K \trianglelefteq \tilde{K}$, then γ leaves N/K and hence N invariant, giving $N \trianglelefteq$ PGL. We shall use this argument repeatedly to obtain proofs by contradiction, choosing N to be a normal subgroup known not to be γ-invariant, and thus proving that certain groups K are not characteristic in PGL.

Lemma 1

(i) Let $\Gamma^* > K \geq N^*(p^e)$ *for some prime* p, *then* $K \trianglelefteq$ PGL *if and only if* $p = 5$ *and* $K = N^*(5)$ *or* $N^*(5^2)$.

(ii) $M(5^e) \trianglelefteq$ PGL *if and only if* $e = 0, 1,$ *or* 2.

(N.B. $M(5^0) = M(1) =$ PGL, $N^*(5^0) = \Gamma^*$; both characteristic in PGL).

Proof

(i) Let PGL $\trianglerighteq K$; then

$K/N^*(p^e)$ is a proper normal subgroup of $\Gamma^*/N^*(p^e) \cong Q^*(p^e)$, so the possibilities for K are given by IV.4. In particular, if $p \geq 5$ then $K = N^*(p^c)$ for some $c \leq e$.

First let $p > 5$. If $K \trianglelefteq$ PGL then γ acts on $\tilde{K} = \Gamma^*/K \cong Q(p^c)$; and all normal subgroups of this are characteristic, so γ leaves $N^*(p)$ invariant, that is, $N^*(p) \trianglelefteq$ PGL. Now $N^*(p)$ contains v^{2p}, and hence contains $(v^{2p})_\gamma = f^{2p}$, so $f^2 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ has order p in $\Gamma/N(p) = Q(p) =$ PSL(2, p). However, it follows from Sylow's Theorems that the elements of order p in PSL(2, p) are the parabolic elements,

and these have trace ± 2, so $\pm 2 \equiv \pm 3 \mod p$, which is impossible for $p > 5$.

Next let $p = 5$, so $K = N^*(5^c)$ for some c. If $c \geq 3$ then, because all normal subgroups of $Q(5^c)$ are characteristic, we have $N^*(5^3) \trianglelefteq$ PGL. By direct calculation, we see that the element $g = (xv^4xv^{63})^2$ lies in $N^*(5^3)$. Now $g\gamma = (axf^4axf^{63})^2 \equiv \begin{pmatrix} -49 & 0 \\ 25 & 51 \end{pmatrix} \mod 5^3$. [For example, Table 1 gives $f^{16} \mod 5^3$, from which we obtain $f^{63} = (f^{16})^4.f^{-1}$, and hence $g\gamma \mod 5^3$.] Thus $g\gamma \notin N^*(5^3)$, so $N^*(5^3) \not\trianglelefteq$ PGL and hence $N^*(5^c) \not\trianglelefteq$ PGL for $c \geq 3$. (In fact, since $g\gamma \notin M(5^3)$, we have also shown that $M(5^c) \not\trianglelefteq$ PGL for $c \geq 3$, giving the "only if" part of (ii).)

Campbell and Robertson [2] show that $N(5^2) = \langle h \rangle^\Gamma$, where $h = (xv^4xv^{13})^2 v^{25}$. (Their theorem is stated only for odd prime levels, but, as they point out, their presentations are also valid for any odd level.) Now $h\gamma = (axf^4axf^{13})^2 f^{25} \equiv \begin{pmatrix} 7 & 0 \\ 0 & 7 \end{pmatrix} \mod 5^2$, so $h\gamma \in M(5^2)$ and hence $N(5^2)\gamma \leq M(5^2)$. Both $N(5^2)$ and $N(5^2)\gamma$ have index 2 in $M(5^2)$, and they are distinct since $h\gamma$, having determinant -1, cannot lie in $N(5^2)$. Thus $M(5^2)$ is generated by $N(5^2)$ and $N(5^2)\gamma$, and is therefore characteristic in PGL; similarly $N^*(5^2) \cap N(5^2)\gamma \trianglelefteq$ PGL, and since $PGL/M(5^2) \cong \Gamma^*/N^*(5^2) \cong Q(5^2)$, with $M(5)$ and $N^*(5)$ the inverse images of the characteristic subgroup $Q_1(5)$ of $Q(5^2)$, it follows that $M(5)$ and $N^*(5)$ are characteristic in PGL, and (ii) is proved.

The argument for $p = 3$ is similar to that for $p > 5$, the only extra possibility being that $K = R^*$. However, $R^* = R \cap \Gamma^* = R \cap PGL' = \Gamma' = \langle [x, y] \rangle^{PGL}$ is mapped by γ to $\langle [ax, y] \rangle^{PGL} = \langle (xy)^2 \rangle^{PGL} = N(2) \neq R^*$, so $R^* \not\trianglelefteq$ PGL.

Finally, let $p = 2$, so that $N^*(2^e) = N(2^e)$. Then $\bar{K} = K/N(2^e)$ is a normal subgroup of $\Gamma/N(2^e) = Q(2^e)$, properly contained in $\Gamma^*/N(2^e) = Q^*(2^e)$, so it follows from IV.4 that $\bar{K} \leq Q_1(2^e)$ and hence $K \leq N(2)$. Now $N(2)/N(2^e)$ is a 2-group, and hence so is its homomorphic image $N(2)/K$. Since $N(2)$ is a normal subgroup of index 3 in Γ^*, it follows that $N(2)/K$, being normal and of index 3 in $\tilde{K} = \Gamma^*/K$, is the unique Sylow 2-subgroup of $\tilde{K}$, and hence is characteristic in $\tilde{K}$. This shows that $N(2)$ is characteristic in PGL, whereas (in the case $p = 3$) we have seen that γ transposes $N(2)$ and R^* : a contradiction which completes the proof.

From now on we assume that $K \trianglelefteq$ PGL, $\Gamma^* \geq K \geq N(n)$ and that n is minimal with respect to this property. We put $n = \ell m$, where $\ell = 2^a 3^b$ and $(m, 6) = 1$. Since $v^n \in N(n) \leq \Gamma^*$, n is even, so $a \geq 1$.

Lemma 2

$K \leq N^*(m)$.

Proof

$\bar{K} = K/N(n) \leq \Gamma^*/N(n) = Q^*(n) = \big(N^*(m)/N(n)\big) \times \big(N(\ell)/N(n)\big) \cong Q^*(\ell) \times Q(m)$, where $Q(m)$ is a direct product of groups $Q(p^e)$ for primes $p \geq 5$; hence the normal subgroups of $N(\ell)/N(n)$ are the groups $N(\ell m')/N(n)$, where $m' \mid m$, with quotients $N(\ell)/N(\ell m') \cong Q(m')$ which is centreless, so Corollary 1 implies $\bar{K} = \bar{K}_1 \times \bar{K}_2$ where $\bar{K}_1 = \big(K \cap N^*(m)\big)/N(n)$ $\cong KN(\ell)/N(\ell) \leq Q^*(\ell)$, and $\bar{K}_2 = \big(K \cap N(\ell)\big)/N(n) = N(\ell m')/N(n)$ $\cong N^*(m')/N^*(m) \leq Q(m)$. Thus $\bar{K} \geq \bar{K}_1$, so $K \geq N(\ell m') \geq N(n)$, and by the minimality of n this implies that $\ell m' = n$, so $m' = m$, $\bar{K}_2 = 1$, and $K \leq N^*(m') = N^*(m)$. See Figure 3.

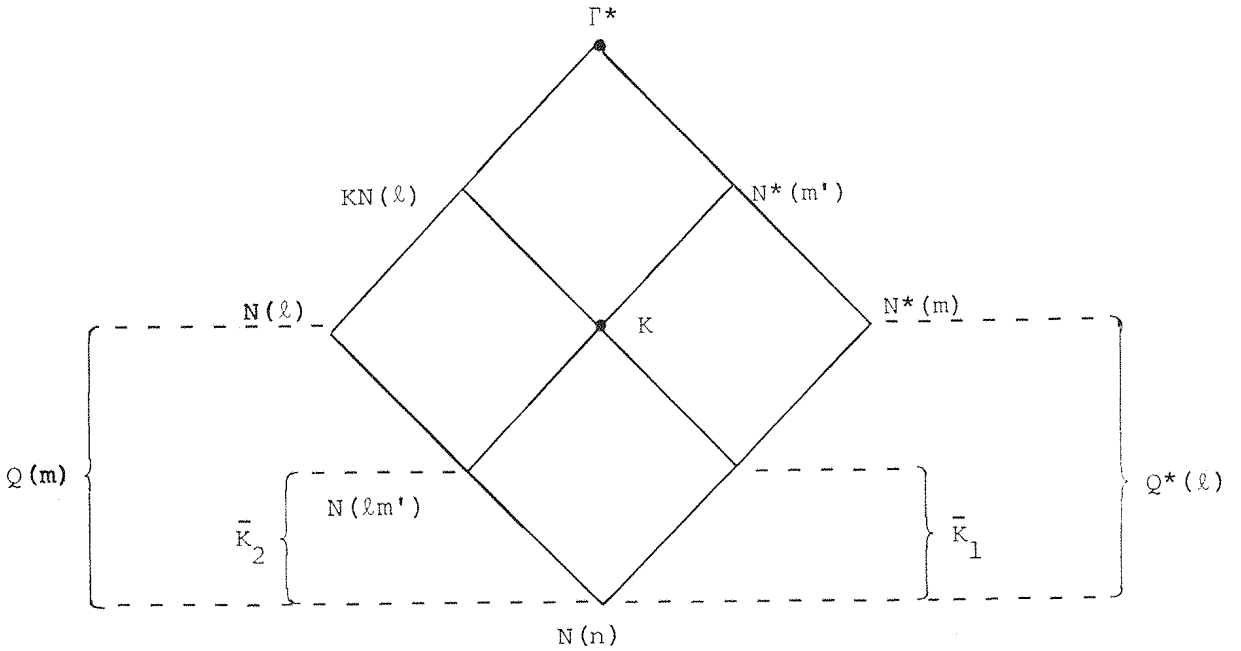


Figure 3

Lemma 3

$m = 5^c$ *for some* $c \geq 0$.

Proof

Suppose not, say $p^e \| m$ for some prime $p > 5$, $e \geq 1$. Let $q = n/p^e$. By Lemma 2, $K \leq N^*(m) \leq N^*(p^e)$, so $\tilde{K} = \tilde{K}_p \times \tilde{K}_q$ where we define $\tilde{K}_p = KN(q)/K \cong \Gamma^*/N^*(p^e) \cong Q(p^e)$, and $\tilde{K}_q = N^*(p^e)/K \cong \Gamma^*/KN(q)$, which is homomorphic image of $\Gamma^*/N(q) \cong Q^*(q)$. Since $(p,q) = 1$ and $p \neq 2, 3$; $Q(p^e)$ and $Q^*(q)$ have no composition factors in common, and hence neither have $\tilde{K}_p$ and $\tilde{K}_q$, so they are both characteristic in $\tilde{K}$. In particular, this implies that $N^*(p^e) \trianglelefteq$ PGL, contradicting Lemma 1. See Figure 4.

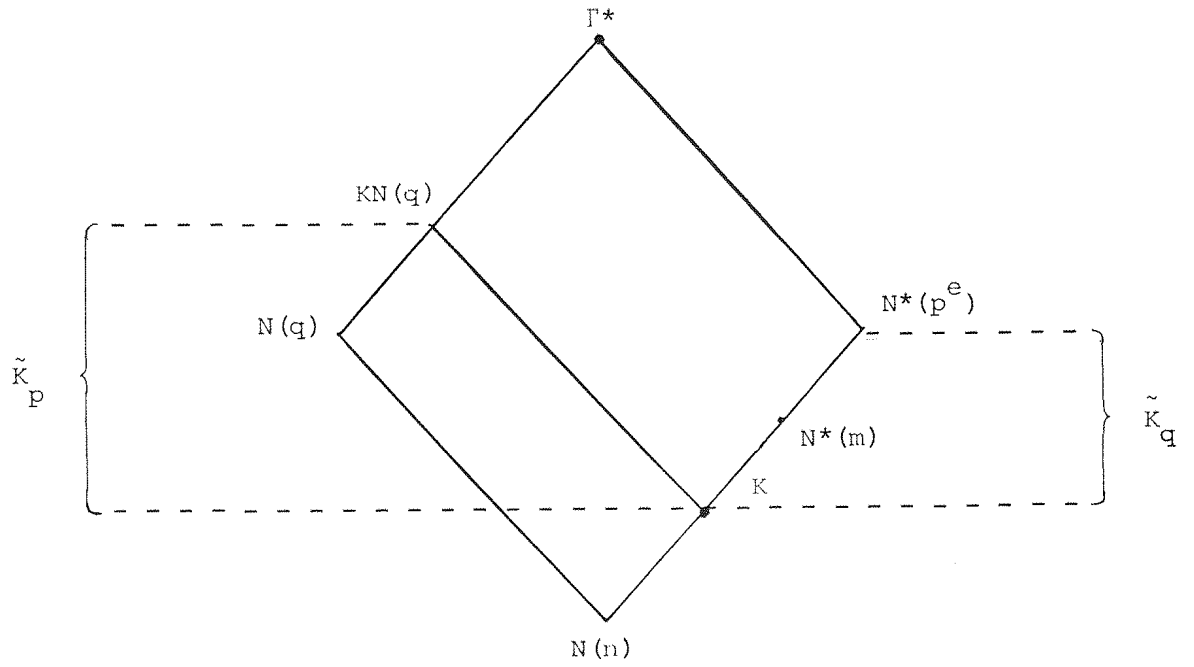


Figure 4.

Lemma 4

$K = L \cap N^*(5^c)$ *where* $\Gamma^* \geq L \geq N(\ell)$, $L \trianglelefteq PGL$, *and* $c = 0, 1,$ *or* 2 .

Proof

Lemma 2 gives $K \leq N^*(m)$, and Lemma 3 gives $m = 5^c$ for some c, so $N(n) \leq K \leq N^*(5^c)$. Putting $L = KN(\ell)$ we have $K = L \cap N^*(5^c)$ with $N(\ell) \leq L \leq PGL$. Then $\tilde{K} = \tilde{K}_5 \times \tilde{K}_\ell$, where we define $\tilde{K}_5 = L/K \cong PGL/N^*(5^c) \cong Q(5^c)$ which is perfect and centreless, and $\tilde{K}_\ell = N^*(5^c)/K \cong \Gamma^*/L$ which is soluble (being a homomorphic image of $\Gamma^*/N(\ell) \cong Q^*(2^a) \times Q(3^b)$). Thus $\tilde{K}_5$ is the last term of the derived series of $\tilde{K}$, and is therefore characteristic in $\tilde{K}$, so $L \trianglelefteq PGL$. Since $\tilde{K}_5$ is centreless, its centraliser in $\tilde{K}$ is $\tilde{K}_\ell$ which is therefore also characteristic in $\tilde{K}$; thus $N^*(5^c) \trianglelefteq PGL$, so $c = 0, 1,$ or 2 by Lemma 1. See Figure 5.

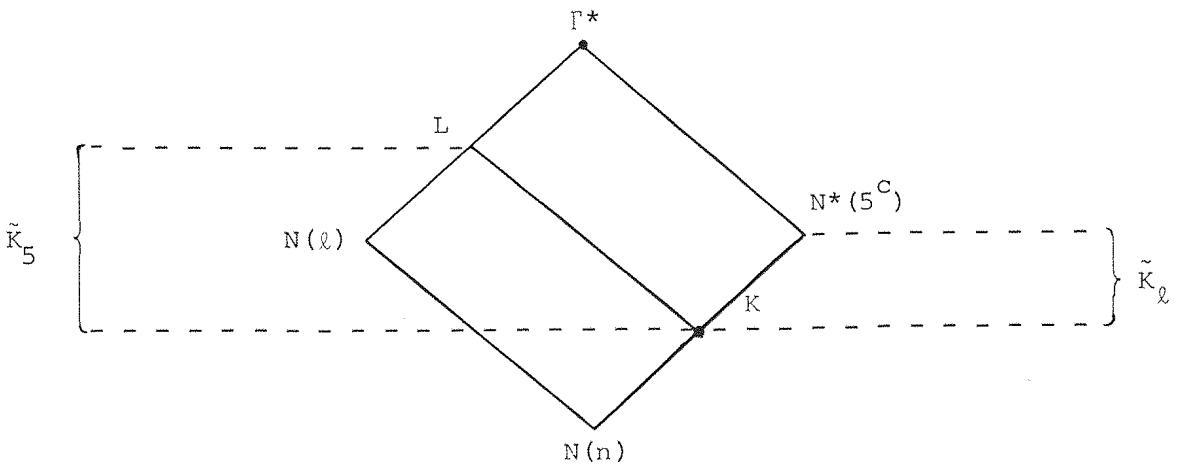


Figure 5

This means that, in order to determine K, it is sufficient to determine all possible subgroups L satisfying the conclusion of Lemma 4, and then intersect these with $N^*(5^c)$ for $c \leq 2$. In other words, replacing L by K we can assume that $n = \ell = 2^a 3^b$.

Let us assume that $K < \Gamma^*$, so that $b > 0$ by Lemma 1. Then $\bar{K}$ is a proper normal subgroup of $Q^*(n) = \Gamma^*/N(n) = \big(N^*(3^b)/N(n)\big) \times \big(N(2^a)/N(n)\big) \cong Q^*(2^a) \times Q(3^b)$. Now all quotient groups of $Q(3^b)$, except $Q(3^b)/R(3^b) \cong C_3$, are centreless, so the only quotients of $Q^*(2^a)$ and $Q(3^b)$ with non trivial isomorphic central subgroups are $Q^*(2^a)/Q_1(2^a)$ and $Q(3^b)/R(3^b)$, both isomorphic to C_3. Hence Proposition 3 implies that either

(i) $Q^*(n) \rhd \bar{K} \rhd Q_1(2^a) \times R(3^b)$ (both indices = 3), or

(ii) $\bar{K} = \bar{K}_2 \times \bar{K}_3$ where $\bar{K}_2 = \big(K \cap N^*(3^b)\big)/N(n) \cong KN(2^a)/N(2^a) \lhd Q^*(2^a)$ and $\bar{K}_3 = \big(K \cap N(2^a)\big)/N(n) \cong KN(3^b)/N(3^b) \lhd Q(3^b)$.

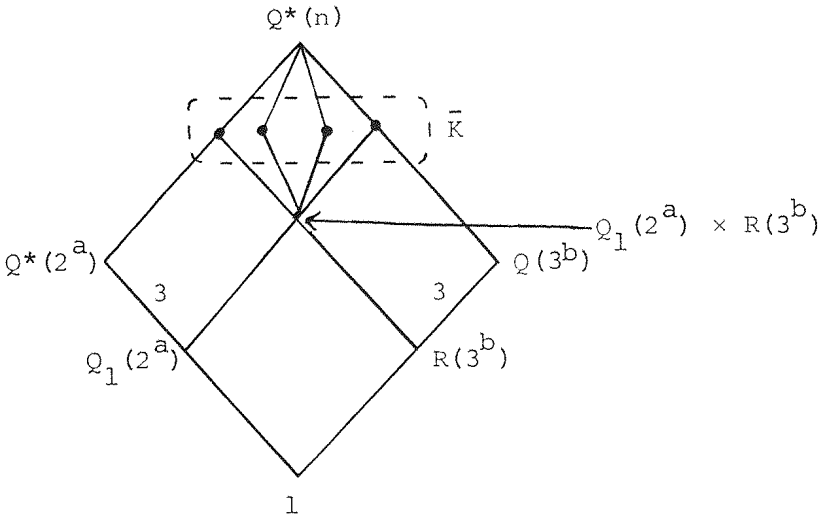


Figure 6 : Case (i)

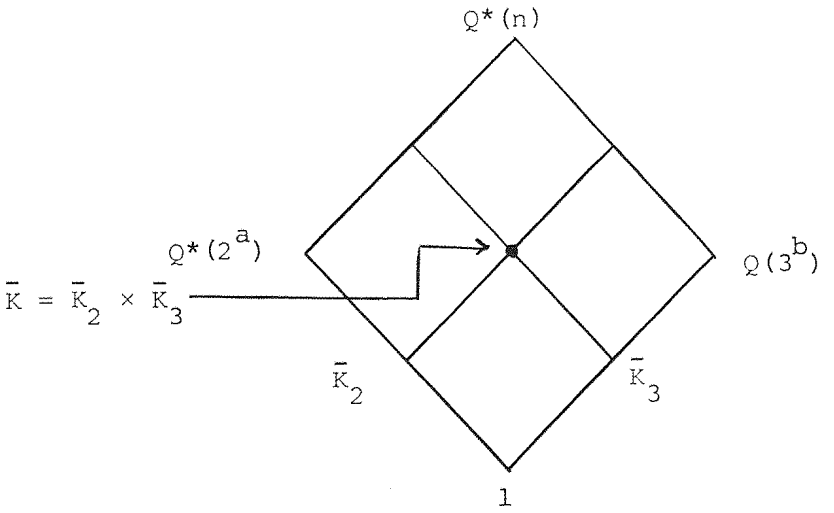


Figure 7 : Case (ii)

Case (i)

We have $\Gamma^* \triangleright K \triangleright N(2) \cap R^* = \Gamma^{*\prime}$ and by Proposition 1 (ii) and (iii) there are just 4 such subgroups K, generated by $\Gamma^{*\prime}$ together with y, $y^x.y = (xy)^2$, $(y^x)^{-1}y = [x, y]$, and y^x respectively. Now x (acting by conjugation) transposes the first and fourth of these, while γ transposes the second and third ($N(2)$ and R^* respectively),

so none of them is characteristic in PGL. Thus Case (i) does not arise.

Case (ii)

The minimality of n implies that $\bar{K}_3 \neq Q_i(3^b)$ for any $i < b$, so the only remaining proper normal subgroups $\bar{K}_3 \trianglelefteq Q(3^b)$ are

(iia) $\bar{K}_3 = R(3^b)$, and

(iib) $\bar{K}_3 = Q_b(3^b)$, that is, $\bar{K} = \bar{K}_2 \trianglelefteq Q^*(2^a)$.

In either case, we define $\tilde{K}_2 = KN^*(3^b)/K \cong \Gamma^*/KN(2^a)$ and $\tilde{K}_3 = KN(2^a)/K \cong \Gamma^*/KN^*(3^b)$, homomorphic images of $Q^*(2^a)$ and $Q(3^b)$ respectively, with $\tilde{K} = \tilde{K}_2 \times \tilde{K}_3$. Note that $\bar{K} = \bar{K}_2 \times \bar{K}_3$ with $\bar{K}_2 \trianglelefteq Q^*(2^a)$, $Q^*(2^a)/\bar{K}_2 \cong \tilde{K}_2$, and $\bar{K}_3 \trianglelefteq Q(3^b)$, $Q(3^b)/\bar{K}_3 \cong \tilde{K}_3$.

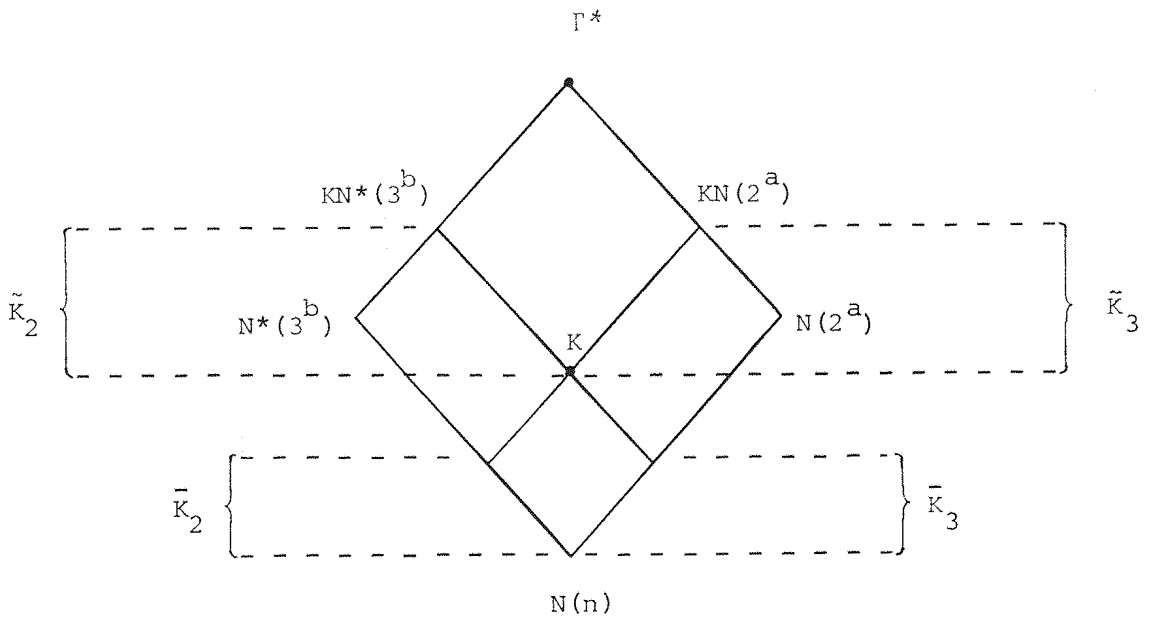


Figure 8

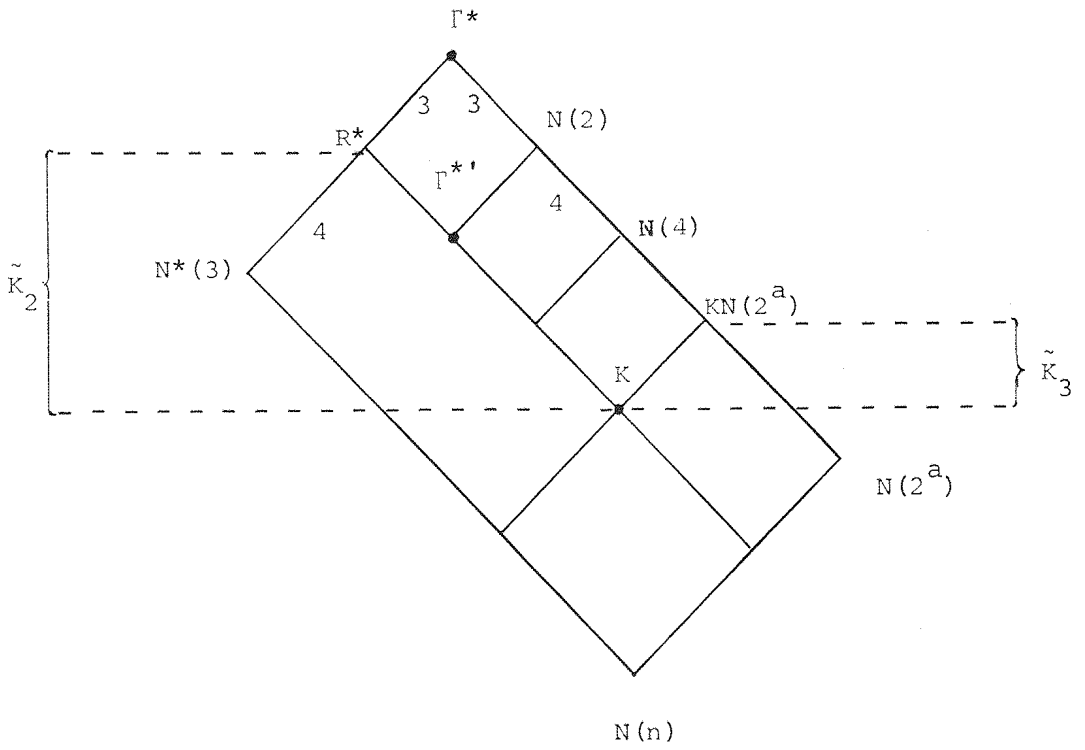


Figure 9

Case (iia)

We have $K = R^* \cap KN(2^a) \geq N(2^a.3)$, so $b = 1$ by the minimality of n. In case (i) we saw that $K \neq R^*$, so $KN(2^a) < \Gamma^*$. Now $\bar{K}_2 = KN(2^a)/N(2^a)$ is a normal subgroup of $Q(2^a)$, properly contained in $Q^*(2^a)$ and hence contained in $Q_1(2^a)$, so that $K \leq N(2)$ and hence $K \leq N(2) \cap R^* = \Gamma^{*\prime}$. Suppose that $K < \Gamma^{*\prime}$, then $KN(2^a) < N(2)$, so (from the normal structure of $Q(2^a)$) $KN(2^a) \leq N(4)$. Now $\tilde{K} = \tilde{K}_2 \times \tilde{K}_3$ where we define $K_2 = R^*/K \cong \Gamma^*/KN(2^a)$ and $\tilde{K}_3 = KN(2^a)/K \cong \Gamma^*/R^* \cong C_3$. Since $\tilde{K}_2$ has order 3.2^i for some i and maps onto $\Gamma^*/N(4) = Q^*(4) \cong A_4$, its centre has order coprime to 3. Thus $\tilde{K}_3 = O_3(Z(\tilde{K}))$, so $\tilde{K}_3$ is characteristic in $\tilde{K}$, and $KN(2^a)$ is characteristic in PGL. Since $\Gamma^* > KN(2^a) \geq N(2^a)$, this contradicts Lemma 1 (applied to $KN(2^a)$). Thus case (iia) leads only to $K = \Gamma^{*\prime}$, which we know to be characteristic in PGL.

Case (iib)

We have $\bar{K}_3 = 1$, so $N^*(3^b) \geq K \geq N(n)$. As in case (iia), $\bar{K}_2$ is a normal subgroup of $Q(2^a)$, contained in $Q^*(2^a)$, so it is either $Q^*(2^a)$, $Q_1(2^a)$, or a subgroup of $Q_2(2^a)$. If $\bar{K}_2 = Q^*(2^a)$, we have $KN(2^a) = \Gamma^*$, so $K = N^*(3^b)$, contradicting Lemma 1. If $\bar{K}_2 = Q_1(2^a)$, we have $KN(2^a) = N(2)$, so $K = N(2) \cap N^*(3^b) = N(2.3^b)$ and $n = 2.3^b$; then $\tilde{K}_2 = N^*(3^b)/K \cong C_3$, while $\tilde{K}_3 = N(2)/K \cong \Gamma^*/N^*(3^b) \cong Q(3^b)$ is centreless, so $\tilde{K}_2 = Z(\tilde{K}) \trianglelefteq \tilde{K}$; thus $N^*(3^b) \trianglelefteq PGL$, again contradicting Lemma 1.

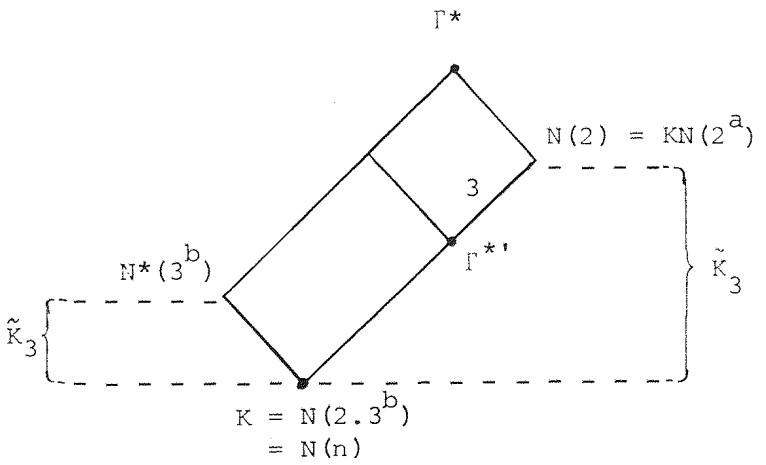


Figure 10

Finally, if $\bar{K}_2 \leq Q_2(2^a)$ then $KN(2^a) \leq N(4)$, that is, $K \leq N(4) \cap N^*(3^b) = N(4.3^b)$, so $a \geq 2$.

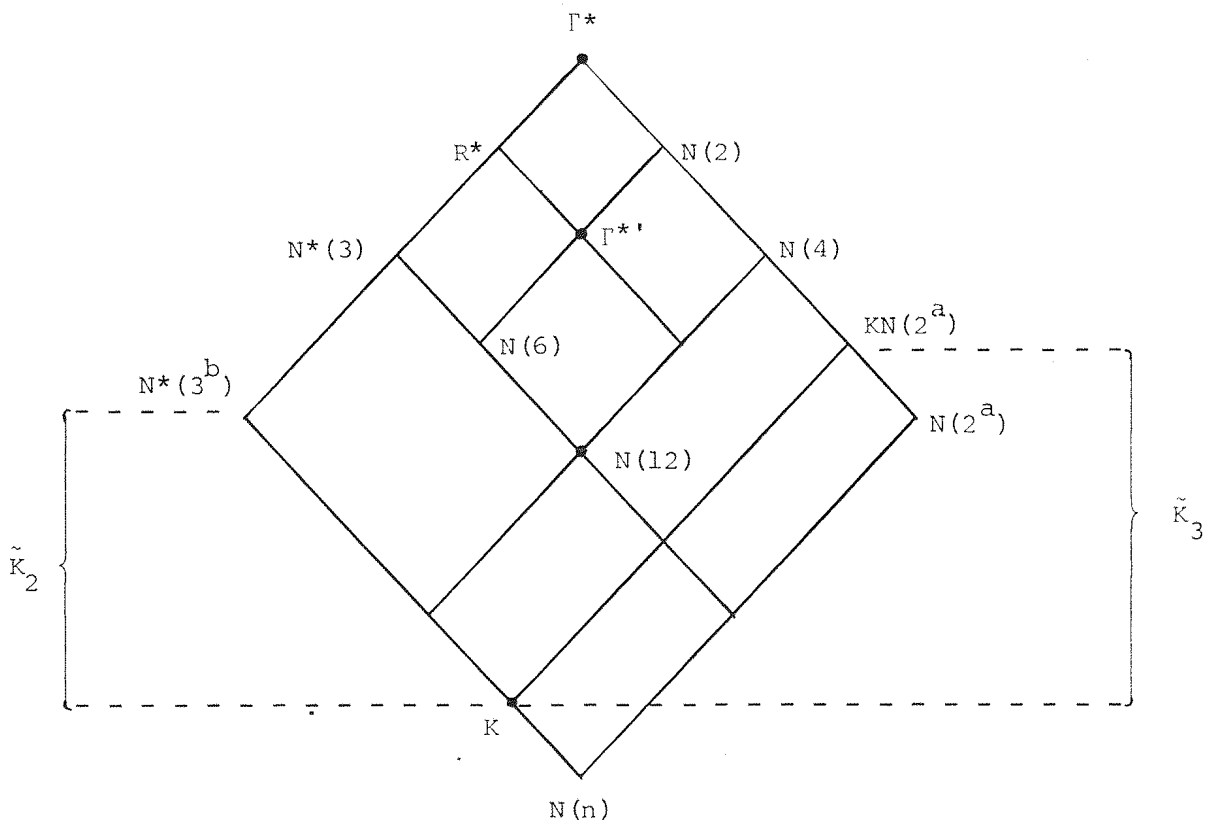


Figure 11

We have $\tilde{K}_2 = N^*(3^b)/K \cong \Gamma^*/KN(2^a)$ and $\tilde{K}_3 = KN(2^a)K \cong \Gamma^*/N^*(3^b) \cong Q(3^b)$. In each case, $\tilde{K}_i$ is soluble and $|\tilde{K}_i^{ab}|$ has prime order (= 3), so $\tilde{K}_i$ is directly indecomposable. Moreover, $Z(\tilde{K}_3) = 1$, while $Z(\tilde{K}_2)$ is a 2-group (possibly trivial) since $\tilde{K}_2$ maps onto $Q^*(4) \cong A_4$. Thus $\left(|\tilde{K}_i^{ab}|, |Z(\tilde{K}_j)|\right) = 1$ for $i \neq j$, so by a standard argument [7, Satz, I. 12.6], the direct decomposition $\tilde{K} = \tilde{K}_2 \times \tilde{K}_3$ is unique. Now if $\tilde{K}_2 \neq \tilde{K}_3$ then each $\tilde{K}_i$ is characteristic in $\tilde{K}$, giving $N^*(3^b) \trianglelefteq PGL$, against Lemma 1. Thus $\tilde{K}_2 \cong \tilde{K}_3 \cong Q(3^b)$. Now $3 \mid |\tilde{K}_2| = |Q(3^b)|$, so $b = 1$, giving $|\tilde{K}_2| = |\tilde{K}_3| = 12$, and $|\tilde{K}| = 144$. Since $K \leq N(4.3^b) = N(12)$, with $|\Gamma^* : K| = 144 = |\Gamma^* : N(12)|$, we have $K = N(12)$.

We have now proved

Lemma 5

If $K \trianglelefteq \mathrm{PGL}$ *and* $\Gamma^* \geq K \geq N(\ell)$ *where* $\ell = 2^a.3^b$, *then* $L = \Gamma^*, \Gamma^{*\prime}$ *or* $N(12)$.

Combining this with Lemma 4, we have

Corollary 3

If $K \trianglelefteq \Gamma^*$ and $\Gamma^* \geq K \geq N(n)$, then $K = L \cap M(5^c)$ where $L = \Gamma^*, \Gamma^{*\prime}$ or $N(12)$ and $c = 0, 1,$ or 2. In particular $K \geq N(300)$.

We now remove the restriction that $K \leq \Gamma^*$, and restate

Theorem 1

$\mathrm{PGL} \trianglerighteq K \geq N(n)$ *for some* n *if and only if* $K = L \cap M(5^c)$, *where* $L = \mathrm{PGL}, \Gamma_o, \Gamma^*, \Gamma^{*\prime}$, *or* $N(12)$ *and* $c = 0, 1,$ or 2. *In particular,* $K \geq N(300)$.

Proof

Suppose that $\mathrm{PGL} \trianglerighteq K \geq N(n)$, and define $K^* = K \cap \Gamma^*$. Then $K^* \trianglelefteq \mathrm{PGL}$, and $\Gamma^* \geq K^* \geq N(2n)$ since $\Gamma^* \geq N(2)$, so Corollary 3 implies that $K^* \geq N(300)$. Thus $K \geq N(300)$, so $K/N(300)$ is a normal subgroup of $\mathrm{PGL}/N(300)$. Now $\mathrm{PGL}/N(300) \cong S_4 \times S_4 \times Q(5^2)$, and we can use Proposition 3 to find all $(4^2 + 1) \times 3 = 51$ normal subgroups of this. Since γ acts by transposing the two factors S_4, we see that the only γ-invariant normal subgroups are those corresponding to the 15 groups K in Theorem 1.

Conversely, we have seen that each of the specified groups L and $M(5^C)$ is characteristic in PGL, and hence so is each of the 15 groups $L \cap M(5^C)$.

IV.7 Proof of Corollary 2

We restate the result here:

Corollary 2

Let C be a congruence subgroup of PGL such that $C\gamma$ is also a congruence subgroup; then $C \geq \Gamma(600)$.

Proof

If C and $C\gamma$ are congruence subgroups then they each contain $\Gamma(n)$ for some common value of n. Being normal in PGL, $\Gamma(n)$ is contained in the core $C^O = \bigcap_{g \in PGL} C^g$ of C, and similarly in the core $(C\gamma)^O$ of $C\gamma$, and hence in the normal subgroup $K = C^O \cap (C\gamma)^O$ of PGL. Now $(C^O)\gamma = (C\gamma)^O$, so K is γ-invariant and hence characteristic in PGL.

For any subgroup $H \trianglelefteq PGL$, let $H^+ = \{h \in PGL : h^2 \in H$ and $[h, g] \in H$ for all $g \in PGL\}$; then H^+/H consists of the central involutions in PGL/H, together with the identity, so if H is characteristic in PGL then so is H^+. For any $H \trianglelefteq PGL$, let $H^- = H^2.[H, PGL]$ be the subgroup generated by all h^2 and $[h, g]$ for $h \in H$, $g \in PGL$, so that $(H^+)^- \leq H \leq (H^-)^+$.

Now $PGL \trianglerighteq K \geq \Gamma(n)$, and since the elements of $N(n)/\Gamma(n)$ are congruent mod n to scalar matrices of order 1 or 2 , we have $N(n) \leq \Gamma(n)^{+}$ and hence $PGL \trianglerighteq K^{+} \geq N(n)$. Thus K^{+} must be one of the 15 groups listed in Theorem 1, and in particular K^{+} contains $N(300)$, so putting $N = N(300)$, K contains N^{-}.

Since $v^{300} = \begin{pmatrix} 1 & 300 \\ 0 & 1 \end{pmatrix} \in N$, and since N/N^{-} has exponent 2, we have $v^{600} \in N^{-} \leq K$. Now the parabolic elements $g \in \Gamma$ are just the conjugates of the powers of v , so $g^{600} \in K$ for every such g since $K \trianglelefteq PGL$. Since K is a congruence subgroup, Wohlfahrt's Theorem [20] gives $K \geq \Gamma(600)$, and hence $C \geq \Gamma(600)$.

CHAPTER V

There is a well-known duality for maps on surfaces, interchanging vertices and faces, so that a map M of type (m, n) is transformed into its dual map M^* of type (n, m) while retaining certain important features such as its automorphism group. Recently topological descriptions have been given for other similar operations on maps, firstly by Wilson [19] for regular and reflexible maps, and later by Lins [10] for all maps; they each exhibit four more invertible operations which, together with the above duality and the identity operation, form a group isomorphic to S_3. In this chapter we show that these operations arise naturally in algebraic map theory : maps may be regarded as transitive permutation representations of a certain group G, and the outer automorphism group

$$\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G) \cong S_3$$

permutes these representations, inducing the six operations on maps. There are no other invertible operations on the class of maps, though certain subclasses (such as maps of given valency) may admit other invertible operations induced by outer automorphisms of homomorphic images of G. Several consequences follow easily from this algebraic interpretation of operations on maps, for example the fact that each finite map M has a finite reflexible cover $\hat{M}$ which is invariant under all six operations.

V.1 Algebraic Maps

First we shall briefly outline the algebraic theory of maps developed in [1], [8], [9] and [18]. To each map M we

associate a set Ω of blades ; wherever an edge e meets a vertex v , we draw on the surface a pair of blades, one on each side of e . We define three permutations of Ω as follows : t (the transverse reflection) transposes each such pair of blades, ℓ (the longitudinal reflection) sends each blade to the blade at the other end of e and on the same side of e , and r (the rotary reflection) transposes pairs of blades with a vertex and face in common; Fig. 1 . illustrates the effect of these permutations on a blade β .

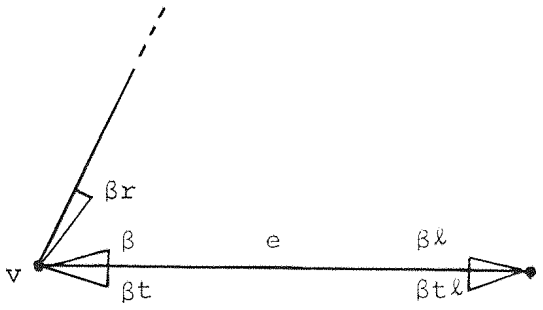


Figure 1

(These definitions require some slight modifications, allowing t, ℓ, r, or $t\ell$ to have fixed-points on Ω, when M is on a surface with boundary or when the underlying graph of M has free edges. Since these modifications do not alter our subsequent arguments, and since most interest is directed towards maps which do not have these features, we shall not explore these possibilities further; the interested reader can refer to [1] for details.)

Clearly these permutations satisfy the relations:

$$t^2 = \ell^2 = r^2 = (t\ell)^2 = 1 ,$$

and by the connectedness of M they generate a transitive group of permutations of Ω, so we have a transitive permutation representation $\pi : G \to S^{\Omega}$ of the group

$$G = \langle t, \ell, r : t^2 = \ell^2 = r^2 = (t\ell)^2 = 1 \rangle \qquad (1)$$

Conversely, given a transitive permutation representation $\pi : G \to S^{\Omega}$ of G, we can reconstruct the map M : we define the vertices, edges, and faces of M to be the orbits in Ω of the dihedral subgroups $\langle t, r\rangle$, $\langle t, \ell\rangle$, and $\langle \ell, r\rangle$ of G, with incidence corresponding to non-empty intersection of orbits. (A more sophisticated appraoch, described in [1] and [8], is to represent G as the automorphism group of a certain tessellation on a Riemann surface, and to take M to be the quotient of this tessellation by a suitable subgroup M of G.)

This gives a bijection between maps and transitive permutation representations of G (or more strictly between isomorphism classes in each category), and it allows us to apply group theory to map-theoretic problems. Each map M determines a permutation representation π which is isomorphic to the action of G (by right multiplication) on the cosets Mg of a subgroup $M \leq G$; this subgroup M, the map-subgroup associated with M, is the stabiliser in G of an element of Ω, and is uniquely determined up to conjugacy. Then map coverings $M_1 \to M_2$ correspond to inclusions $M_1 \leq M_2$, and the autmorphism group $\mathrm{Aut}(M)$ can be realised as the action of $N_G(M)/M$ on the cosets of M, where $N_G(M)$ is the normaliser of M in G, acting by left multiplication.

We can think of the elements of G as representing "paths" in maps : for example, Fig. 2 shows that rt and $r\ell$ represent rotations about vertices and faces, while $rt\ell$ is the basic "zig" (or "zag") out of which Petrie polygons are formed [3, 5.2 and 8.5]. It is reasonable to expect that any operation on maps (such as duality) should induce a permutation of the set of all such paths, preserving compositions, in the way that duality interchanges the orbits of $\langle rt\rangle$ and $\langle r\ell\rangle$; in

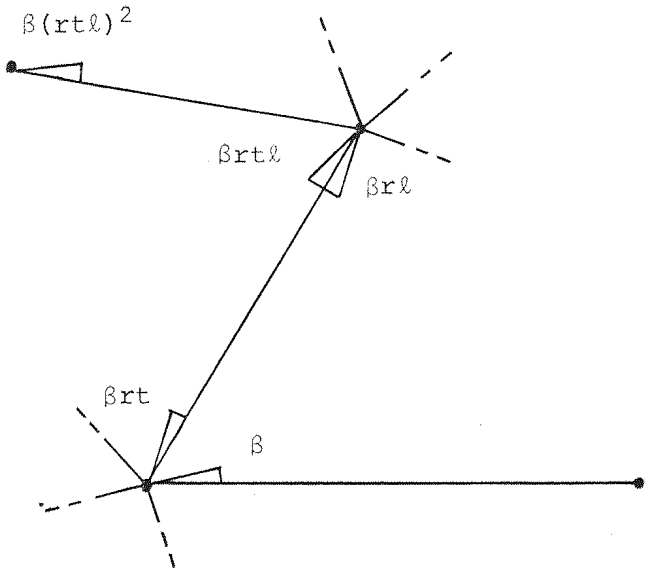


Figure 2

other words, it should induce an automorphism of G. Conversely, any automorphism θ of G induces such an operation on maps : if M is the map, with map-subgroup M, associated with a permutation representation $\pi : G \to S^{\Omega}$, then we define M^{θ} to be the map with map-subgroup M^{θ}, associated with the representation $\theta^{-1} \circ \pi : G \to S^{\Omega}$ of G. Since the automorphism group $\mathrm{Aut}(G)$ preserves inclusions and normalisers of subgroups, the induced operations will preserve coverings and automorphism groups of maps. Each inner automorphism θ of G sends M to a conjugate map-subgroup, so that $M^{\theta} = M$; thus the inner automorphism group $\mathrm{Inn}(G)$ acts trivially on maps, so we have an induced action of the outer automorphism group

$$\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$$

We shall therefore determine the outer automorphisms of G, and then consider the operations on maps resulting from them.

V.2 Automorphisms of G

It is clear from the presentation (1) that G is a free product $G = K * C$, where

$$K = \langle t, \ell : t^2 = \ell^2 = (t\ell)^2 = 1 \rangle$$

is a Klein four-group, and

$$C = \langle r : r^2 = 1 \rangle$$

is a cyclic group of order 2.

Theorem 1

Aut(G) *is a split extension of a normal subgroup* $\mathrm{Inn}(G) \cong G$ *by a complement* $S \cong S_3$ *which fixes* r *and permutes* $\{t, \ell, t\ell\}$ *transitively.*

Proof

As is the case for any group, Inn(G) is a normal subgroup of Aut(G), and since G has trivial centre (like any proper free product) we have $\mathrm{Inn}(G) \cong G/Z(G) = G$. The six permutations of $\{t, \ell, t\ell\}$ extend to automorphisms of K, and hence induce automorphisms of G, leaving r fixed and forming a subgroup $S \cong S_3$ of Aut(G). Since no two of t, ℓ, and $t\ell$ are conjugate in G we have $\mathrm{Inn}(G) \cap S = 1$, so to prove the theorem it is sufficient to show that $\mathrm{Aut}(G) = \mathrm{Inn}(G).S$.

The rest of the proof is analogous to Theorem 1, Chapter II, using the fact that G is a free product, and we shall omit it.

Corollary 1

Out(G) *is isomorphic to* S_3 , *the six cosets of* Inn(G) *in* Aut(G) *being represented by the elements of* S.

V.3 Operations on Maps

It follows from Corollary 1 that there are at most six distinct operations on maps; they are induced by the elements of S , and hence form a group Σ which is a homomorphic image of S. As shown by Wilson [19] , the cube gives rise to six non-isomorphic maps under these operations, that is, it lies in an orbit of Σ of length 6, so there are exactly six operations, and so

$$\Sigma \cong S \cong S_3 .$$

(However, some orbits have length properly dividing 6 : for example the tetrahedron, being self-dual but not invariant under all six operations, must lie in an orbit of length 3.)

We shall now identify the operations in Σ with those described by Wilson [19] and Lins [10] . For ease of notation we will use the same symbol for an automorphism in S and the operation in Σ it induces. First we recall that the vertices, edges, and faces of a map correspond to the orbits of the subgroups $\langle t, r\rangle$, $\langle t, \ell\rangle$, and $\langle r, \ell\rangle$ on Ω ; similarly, Fig. 2 shows that the orbits of $\langle r, t\ell\rangle$ correspond to the Petrie polygons.

Let τ and θ be the automorphisms in S induced by the transposition (t, ℓ) and the 3-cycle $(t, \ell, t\ell)$ of the involutions in K, so that the corresponding operations generate Σ. Table 1 shows the six operations, the corresponding permutations of $\{t, \ell, t\ell\}$, the effect each operation has on vertices, faces, and Petrie polygons (abbreviated to v, f, and p), and the notations used by Wilson and Lins for these operations. (Note that whereas we have composed mappings from left to right, Wilson does so from right to left; thus our operation $\theta = (\theta\tau)\tau$ corresponds to his DP rather than PD.)

Operation	Permutation	Effect	Wilson	Lins
1	1	1	I	M
τ	(t, ℓ)	(v, f)	D	D_M
$\theta\tau$	$(\ell, t\ell)$	(f, p)	P	$M^{\sim}$
$\tau\theta$	$(t, t\ell)$	(v, p)	PDP	P_M
θ	$(t, \ell, t\ell)$	(v, f, p)	DP	$P^{\sim}$
θ^{-1}	$(\ell, t, t\ell)$	(f, v, p)	PD	$D^{\sim}$

Table 1.

For example, the automorphism τ transposes the subgroups $\langle t, r\rangle$ and $\langle \ell, r\rangle$, and leaves $K = \langle t, \ell\rangle$ and $\langle r, t\ell\rangle$ invariant; hence the operation τ transposes the sets of vertices and faces,

leaving edges and Petrie polygons invariant, so M^T is the dual M^* of M. As can be seen from Table 1 , the operations in Σ induce all six permutations of the sets of vertices, faces, and Petrie polygons, while leaving the set of edges invariant (since S leaves K invariant).

V.4 Trivalent and Triangular Maps

The extended modular group PGL has a presentation

$$\langle t, \ell, r : t^2 = \ell^2 = r^2 = (t\ell)^2 = (tr)^3 = 1 \rangle \qquad (2)$$

where t , ℓ , and r are the elements

$$\pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} , \pm \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} , \pm \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix} \qquad (3)$$

of PGL , that is, a, ax, ay in our previous notation (c.f. Chapter I.2). Since (2) is obtained by adding the relation $(tr)^3 = 1$ to the presentation (1) for **G**, it follows that PGL plays the same role in relation to the class of trivalent maps (by which we mean those in which all valencies divide 3) as G plays in relation to all maps; specifically, trivalent maps can be identified with transitive permutation representations of PGL, and operations on this class of maps correspond to outer automorphisms of PGL.

As we saw in Chapter II.3, $\mathrm{Out}(\mathrm{PGL}) \cong C_2$; in fact, $\mathrm{Aut}(\mathrm{PGL})$ is a split extension of $\mathrm{Inn}(\mathrm{PGL}) \cong \mathrm{PGL}$ by a cyclic group $\langle \gamma \rangle$ of

of order 2, where γ is the automorphism which fixes t and r and sends ℓ to $t\ell$.

Thus γ induces the unique non-identity operation on the class of trivalent maps; it transposes faces and Petrie polygons, while leaving the underlying graph invariant, and it corresponds, via the obvious epimorphism $G \to PGL$, to the similar operation $\theta\tau$ (Wilson's Petrie operation P) on the class of all maps.

For example, let M be the cube; thus the map-subgroup M of PGL associated with M is the normal closure of $(\ell r)^4$, or equivalently the principle congruence subgroup of PGL of level 4, the kernel of the reduction mod(4) : $PGL(2, \mathbb{Z}) \to PGL(2, \mathbb{Z}_4)$. Then $M^\gamma = M^{\theta\tau} = P(M)$ is a trivalent orientable map of genus 1 with four hexagonal faces (the Petrie polygons of M), for which the map subgroup M^γ is the normal closure of $(t\ell r)^4$, i.e. $\Gamma(4)$. M^γ can be obtained from Figure 3 by identifying pairs of edges as indicated by their numbering.

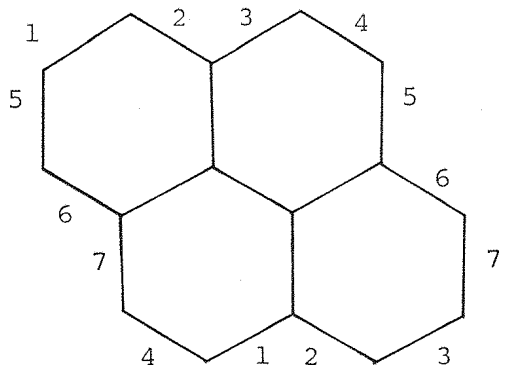


Figure 3

By renaming the generators (3) of PGL as ℓ, t, r (in that order), so that $(\ell r)^3 = 1$, or equivalently by taking dual maps, we

can also regard PGL as representing all triangular maps, and γ as the unique non-identity operation on this class, corresponding to Wilson's "opposite" operation opp = PDP and Lins' "phial" operation P_M, which transposes vertices and Petrie polygons.

For example, let M be the octahedron (which is the dual of the cube) so the map-subgroup M of PGL associated with M is $\Gamma(4)$ again, the normal closure of $(tr)^4$; and $M^\gamma = M^{\tau\theta}$ is a triangular orientable map of genus 1 with 4 vertices (the Petrie polygons of M), for which the map-subgroup M^γ is the normal closure of $(\ell tr)^4$. M^γ can be obtained from Figure 4 by identifying similarly numbered edges.

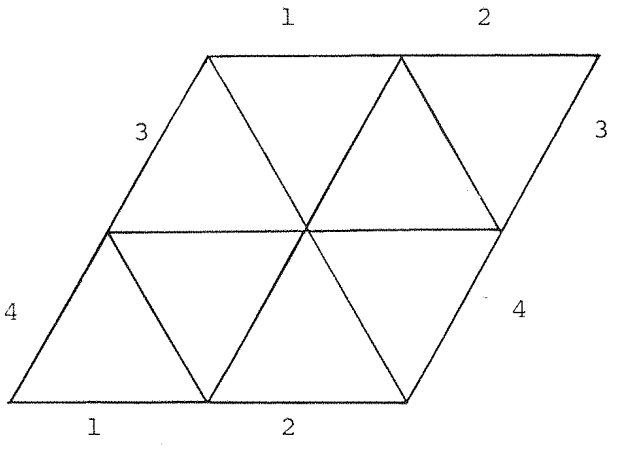


Figure 4.

As another example, let M be the isosahedron. This time M^γ is non-orientable triangular map of genus 6, and the map-subgroups of PGL associated with M and M are the normal closures of $(tr)^5$ and $(\ell tr)^5$, i.e. $\Gamma(5)$ and $\Gamma(5)\gamma$. To construct the map M^γ take $\bar{M}$ to be K_6 (the complete graph on 6 vertices) embedded in the

projective plane. See Figure 5 where the edges should be identified according to their arrows.

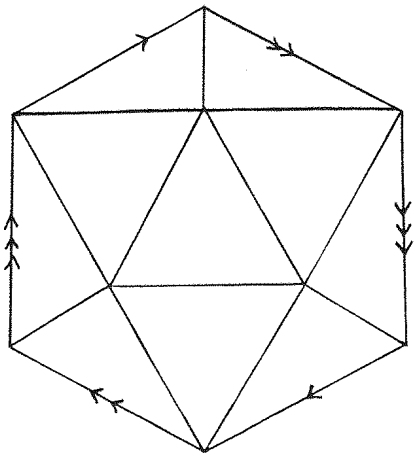


Figure 5. $\bar{M}$

Form a 2-sheeted branched covering M' of $\bar{M}$ with branch points at each of the 6 vertices of $\bar{M}$, so each (5-valent) vertex of $\bar{M}$ lifts to a 10-valent vertex of M', while each edge on face of $\bar{M}$ lifts to 2 of the same on M'. Then $M' = M^{\gamma}$.

Both M and M^{γ} are double coverings of $\bar{M}$ (M unbranched) and the map-subgroup corresponding to $\bar{M}$ is $M(5)$. We know that $M(5) < PGL$, so $(\bar{M})^{\gamma} = \bar{M}$.

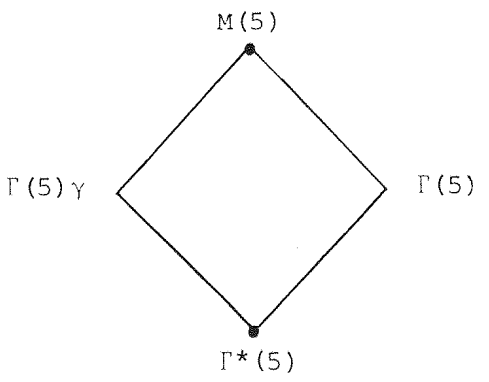


Figure 6.

APPENDIX

Table 1 gives the sets C_L for $L = 1$ to 8, together with the trace of each element. Table 2 gives a list of the conjugacy classes of hyperbolic elements by trace, up to trace = 18.

TABLE 1

C_1	trace	C_2	trace
		V^2	2
V	2	VW	3
W	2	W^2	2

C_3	trace	C_4	trace
V^3	2	V^4	2
V^2W	4	V^3W	5
VW^2	4	V^2W^2	6
W^3	2	VW^3	5
		$VWVW$	7
		W^4	2

C_5	trace
V^5	2
V^4W	6
V^3W^2	8
V^2W^3	8
V^2WVW	10
VW^4	6
VW^2VW	10
W^5	2

Table 1 Continued

C_6	trace	C_7	trace	C_8	trace
v^6	2	v^7	2	v^8	2
v^5w	7	v^6w	8	v^7w	9
v^4w^2	10	v^5w^2	12	v^6w^2	14
v^3w^3	11	v^4w^3	14	v^5w^3	17
v^3wvw	13	v^4wvw	16	v^5wvw	19
v^2w^4	10	v^3w^4	14	v^4w^4	18
v^2w^2vw	15	v^3w^2vw	20	v^4w^2vw	25
v^2wv^2w	14	v^3wv^2w	18	v^4wv^2w	22
v^2wvw^2	15	v^3wvw^2	20	v^4wvw^2	25
vw^5	7	v^2w^5	12	v^3w^5	17
vw^3vw	13	v^2w^3vw	20	v^3w^3vw	27
vw^2vw^2	14	$v^2w^2v^2w$	22	$v^3w^2v^2w$	29
$vwvwvw$	18	$v^2w^2vw^2$	22	$v^3w^2vw^2$	30
w^6	2	v^2wvw^3	20	v^3wv^3w	23
		v^2wvwvw	26	$v^3wv^2w^2$	29
		vw^6	8	v^3wvw^3	27
		vw^4vw	16	v^3wvwvw	34
		vw^3vw^2	18	v^2w^6	14
		vw^2vwvw	26	v^2w^4vw	25
		w^7	2	$v^2w^3v^2w$	30
				$v^2w^3vw^2$	29
				$v^2w^2v^2w^2$	34
				$v^2w^2vw^3$	29
				v^2w^2vwvw	39
				v^2wvw^4	25
				v^2wv^2wvw	37
				v^2wvw^2vw	38
				v^2wvwvw^2	39
				vw^7	9
				vw^5vw	19
				vw^4vw^2	22
				vw^3vw^3	23
				vw^3vwvw	34
				vw^2vw^2vw	37
				$vwvwvwvw$	47
				w^8	2

TABLE 2

t=3 vw	t=9 v^7w vw^7	t=13 v^3wvw vw^3vw $v^{11}w$ vw^{11}	t=16 v^4wvw vw^4vw v^7w^2 v^2w^7 $v^{14}w$ vw^{14}
t=4 v^2w vw^2	t=10 v^2wvw vw^2vw v^4w^2 v^2w^4 v^8w $v\,w^8$	t=14 v^2wv^2w vw^2vw^2 v^4w^3 v^3w^4 v^6w^2 v^2w^6 $v^{12}w$ vw^{12}	t=17 v^5w^3 v^3w^5 $v^{15}w$ vw^{15}
t=5 v^3w vw^3	t=11 v^3w^3 v^9w vw^9		
t=6 v^2w^2 v^4w vw^4			t=18 $vwvwvw$ v^3wv^2w vw^3vw^2 v^4w^4 v^8w^2 v^2w^8 $v^{16}w$ vw^{16}
t=7 $vwvw$ v^5w vw^5	t=12 v^5w^2 v^2w^5 $v^{10}w$ vw^{10}	t=15 v^2w^2vw v^2wvw^2 $v^{13}w$ vw^{13}	
t=8 v^3w^2 v^2w^3 v^6w vw^6			

TABLE 3

Trace	*Number of Conjugacy Classes*
0	1
1	2
2	∞
3	1
4	2
5	2
6	3
7	3
8	4
9	2
10	6
11	3
12	4
13	4
14	8
15	4
16	6
17	4
18	8

REFERENCES

[1] BRYANT, R.P. and SINGERMAN, D. *Foundations of the Theory of Maps on Surfaces with Boundary*. Quarterly Journal of Mathematics, Oxford. To appear.

[2] CAMPBELL, C.M. and ROBERTSON, E.F. *A Deficiency Zero Presentation for* SL(2, p). Bulletin of the London Mathematical Society, 12 (1980) pp. 17-20.

[3] COXETER, H.S.M. and MOSER, W.O.J. *Generators and Relations for Discrete Groups* (4^{th} Edition). Springer-Verlag, Berlin, Heidelberg, and New York, 1980.

[4] DYER, Joan L. *Automorphism Sequences of Integer Unimodular Groups*. Illinois Journal of Mathematics, 22 (1978). pp. 1-30.

[5] HUA, L.K. and REINER, I. *Automorphisms of the Unimodular Group*. Transactions of the American Mathematical Society, 71 (1951) pp. 331-348.

[6] HUA, L.K. and REINER, I. *Automorphisms of the Projective Unimodular Group*. Transactions of the American Mathematical Society, 72 (1952) pp.467-473.

[7] HUPPERT, B. *Endliche Gruppen I*. Springer, Berlin 1967.

[8] JONES, G.A. *Graph Imbeddings, Groups, and Riemann Surfaces*. Colloq. Math. Soc. János Bolyai 25, Algebraic Methods in Graph Theory, Szeged, 1978 (L. Lovász and V.T. Sós, Eds.) North-Holland, Amsterdam, 1981.

[9] JONES, G.A. and SINGERMAN, D. *Theory of Maps on Orientable Surfaces*. Proceedings of the London Mathematical Society (3) 37 (1978) pp. 273-307.

[10] LINS, S. *Graph-encoded Maps*. Journal of Combinatorial Theory (B) 32 (1982) pp. 171-181.

[11] LYNDON, R.C. and Schupp, P.E. *Combinatorial Group Theory*. Springer-Verlag, Berlin, Heidelberg, and New York, 1977.

[12] MAGNUS, W., KARRASS, A. and SOLITAR, S. *Combinatorial Group Theory : Presentations of Groups in Terms of Generators and Relations*. New York, 1966.

[13] McQUILLAN, D.L. *Classification of Normal Subgroups of the Modular Group*. American Journal of Mathematics 87 (1965) pp. 285-296.

[14] McQUILLAN, D.L. *Some Results on the Linear Fractional Group*. Illinois Journal of Mathematics 10 (1966) pp. 24-38.

[15] NEWMAN, M. *Normal Congruence Subgroups of the Modular Group*. American Journal of Mathematics 85 (1963) pp. 419-427.

[16] NEWMAN, M. *Integral Matrices*. Academic Press, New York and London, 1972.

[17] SCHREIER, O. *Über die Gruppen* $A^aB^b = 1$. Abhandlungen aus dem Mathematishen Seminar der Hamburgischen Universität, 3 (1924) pp. 167-9.

[18] TUTTE, W.T. *What is a Map?* New Directions in the Theory of Graphs (F. Harary, Ed.). Academic Press, New York and London, 1973.

[19] WILSON, S.E. *Operators over Regular Maps.* Pacific Journal of Mathematics, 81 (1979), pp. 559-568.

[20] WOHLFAHRT, K. *An Extension of F. Klein's Level Concept.* Illinois Journal of Mathematics 8, (1964), pp. 529-535.