UNIVERSITY OF SOUTHAMPTON

NORMAL SUBGROUPS OF HECKE GROUPS

by

İsmail Naci Cangül

Doctor of Philosophy

Faculty of Mathematical Studies

December 1993

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

FACULTY OF MATHEMATICAL STUDIES

Doctor of Philosophy

NORMAL SUBGROUPS OF HECKE GROUPS

by *İsmail Naci Cangül*

The Hecke group $H(\lambda_q)$ is the discrete subgroup of $PSL(2,\mathbf{R})$ generated by $R(z) = -1/z$ and $T(z) = z + \lambda_q$ for $\lambda_q = 2cos\pi/q$. In this thesis we investigate normal subgroups of these Hecke groups.

The most important Hecke group is the modular group obtained for $q = 3$. There are many results in the literature concerning normal subgroups of the modular group. We are interested in generalizing these to other Hecke groups $H(\lambda_q)$.

Jones and Singerman, [Jo–Si,1], determined a 1:1 correspondence between normal subgroups of certain triangle groups, including Hecke groups, and regular maps. We study normal subgroups of $H(\lambda_q)$ by means of this correspondence and obtain results about normal subgroups of $H(\lambda_q)$ using the known regular maps. This is especially useful when $g = 0$ or 1, as all regular maps with these genera are classified (see [Co–Mo,1] or [Jo–Si,1]).

We obtain fairly complete information about the normal subgroups of $H(\lambda_4)$, $H(\lambda_5)$ and $H(\lambda_6)$ of low index and obtain some other results for other values of q. In particular we investigate principal congruence subgroups of $H(\lambda_q)$ for prime powers q.

CONTENTS

ACKNOWLEDGEMENTS

I am extremely grateful to Dr. David Singerman who supervised me during the preparation of this thesis. His professional guidance and friendly encouragement have been invaluable.

My thanks to my advisor Dr. Gareth A. Jones for his help on many occasions and to Prof. Stewart A. Robertson and Prof. Martin J. Dunwoody for their moral support.

I wish to thank Prof. Turgut Başkan and Prof. Caroline Series for giving me a background in discrete group theory and encouraging me to further studies.

I would like to thank other academic and secreterial staff for their help and invaluable friendship.

Special thanks to my wife, Oya, for her unfailing patience and moral support, particularly during the writing of this thesis.

Finally I would like to express my sincere gratitude to my parents, my brother and my sister, my relatives and friends who prayed for my success during my study.

INTRODUCTION

In "Über die Bestimmung Dirichletcher Reichen durch ihre Funktionalgleichungen", Erich Hecke introduced the groups H(λ) generated by two linear fractional transformations

$$R(z) := -\frac{1}{z} \quad and \quad T(z) := z + \lambda, \tag{1}$$

where λ is a fixed positive real number. R and T have matrix representations

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad and \quad \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \tag{2}$$

respectively. Let $S = R.T$.

These groups are useful in the study of Dirichlet series only when H(λ) is properly discontinuous, i.e. a Fuchsian group. E. Hecke, in [He,1], showed that when $\lambda \geq 2$ and real, or when

$$\lambda = \lambda_q = 2cos\frac{\pi}{q} \tag{3}$$

where q is an integer ≥ 3, when $\lambda < 2$, the set

$$F_\lambda = \{z \in \mathcal{U} : |\, Re\ z \,| < \lambda/2, |\, z \,| > 1\} \tag{4}$$

is a fundamental region for the group H(λ), and also that F_λ fails to be a fundamental region for all other $\lambda > 0$ (see Chapter 1 for more details). It follows from this that H(λ) is Fuchsian if and only if $\lambda = \lambda_q$ or $\lambda > 2$ is real. In these two cases H(λ) is called a Hecke group. Because of its interest, we shall deal in this thesis with the case $\lambda < 2$ and denote the group obtained by H(λ_q). Then the Hecke group H(λ_q) is the discrete subgroup of $PSL(2,\mathbf{R})$ generated by R and T, where $T(z) := z + \lambda_q$.

The Hecke groups $\mathrm{H}(\lambda_q)$ are included in a more general class $\mathrm{H}(\lambda_p, \lambda_q)$ generated by

$$R'(z) := -\frac{1}{z-\lambda_p} \quad and \quad T'(z) := z + \lambda_p + \lambda_q, \tag{5}$$

where $2 \leq p \leq q < \infty$, $p+q > 4$. In fact

$$H(\lambda_q) = H(\lambda_2, \lambda_q). \tag{6}$$

It is known that $\mathrm{H}(\lambda_p, \lambda_q)$ is the free product of a cyclic group of order p and one of order q (see [Lh–Ne,1]). In Chapter 2 we prove this result for Hecke groups, geometrically, and find that $\mathrm{H}(\lambda_q)$ is the free product of cyclic groups of orders two and q.

The most important and worked Hecke group is the *modular group* $\mathrm{H}(\lambda_3)$. In this case $\lambda_3 = 2cos\,\pi/3 = 1$ and hence the underlying field for this group is $\mathbf{Q}(1) = \mathbf{Q}$, i.e. all coefficients of the elements of $\mathrm{H}(\lambda_3)$ are rational integers.

In the literature, the symbols Γ and $\Gamma(1)$ are used to denote the modular group. In this thesis we shall use Γ and $\mathrm{H}(\lambda_3)$ for this purpose.

There are many results in the literature concerning Γ. Some of them can easily be generalized to all Hecke groups with only a few differences.However most results, especially number theoretical ones, can only be generalized to $\mathrm{H}(\lambda_p)$, where p is a prime. For example, when power subgroups $\mathrm{H}^m(\lambda_q)$ are considered, the situation in the $\mathrm{H}(\lambda_p)$ case is similar to the modular group case. Indeed, as we shall see in Chapter 6, $\mathrm{H}(\lambda_p)$ has only three power subgroups $\mathrm{H}(\lambda_p)$, $\mathrm{H}^2(\lambda_p)$ and $\mathrm{H}^p(\lambda_p)$ like the modular group. Finally there are some results which are only true for the modular group and do not hold for the other Hecke groups. The main reason for this is that the underlying field $\mathbf{Q}(\lambda_q)$ for $q > 3$ is clearly more complicated, being a simple extension of $\mathbf{Q}$, than $\mathbf{Q}$, and therefore the coefficients of elements of $H(\lambda_q)$, $q > 3$, are more complex than integers, which are the coefficients of elements of Γ. As a result of this, all calculations are more complicated than they are in the modular group case.

The next two most important Hecke groups are those for $q = 4$ and 6. In these cases $\lambda_q = \sqrt{2}$ and $\sqrt{3}$, respectively. Therefore the underlying fields are $\mathbf{Q}(\sqrt{2})$ and $\mathbf{Q}(\sqrt{3})$, i.e. quadratic extensions of the field $\mathbf{Q}$ of rationals.

We are also going to work with $H(\lambda_5)$ seperately, since in this case, the underlying field is again a quadratic extension of $\mathbf{Q}$. These four Hecke groups are the only ones for which λ_q is a root of a polynomial of degree less than three.

For $q \geq 7$, $q \in \mathbf{N}$, λ_q is a root of a polynomial of degree ≥ 3. As a result of this, as we shall see in Chapter 2, we are not going to be able to determine the number λ_q as clearly as in the first four cases we already discussed. Because of this we are going to attempt to find the minimal polynomial of λ_q over $\mathbf{Q}$. This will be done in Chapter 2 where we deal with odd and even q cases seperately and give the formulae for the minimal polynomial.

One of the reasons for $H(\sqrt{2})$ and $H(\sqrt{3})$ to be two of the most important Hecke groups is that, apart from the modular group, they are the only Hecke groups whose elements are completely known. If we put $m = 2$ or 3, $H(\sqrt{m})$ consists of the set of all matrices of the following two types:

$$\begin{aligned} &\text{(i)} \begin{pmatrix} a & b\sqrt{m} \\ c\sqrt{m} & d \end{pmatrix} \qquad a, b, c, d \in \mathbf{Z},\ \mathrm{ad} - \mathrm{mbc} = 1, \\ &\text{(ii)} \begin{pmatrix} a\sqrt{m} & b \\ c & d\sqrt{m} \end{pmatrix} \qquad a, b, c, d \in \mathbf{Z},\ \mathrm{mad} - \mathrm{bc} = 1. \end{aligned} \tag{7}$$

Those of type (i) are called *even* while those of type (ii) called *odd*.

Note that if we consider the multiplication of these elements, the situation is similar to the multiplication of negative and positive numbers. Here we have

$$\begin{array}{c} \text{odd.odd=even.even=even}, \\ \text{even.odd=odd.even=odd}. \end{array} \tag{8}$$

Let now q be even. We can define an important normal subgroup of the Hecke groups $H(\lambda_q)$:

As q is even there is a homomorphism of $H(\lambda_q)$ to the cyclic group of order two, taking both elliptic generators R and S to elements of order two. Then the parabolic element $T = R.S$ goes to the identity under this homomorphism. Using the permutation method we find the signature of the kernel as $(0;\ q/2, \infty, \infty)$. That is, it is isomorphic to the free product of the infinite cyclic group $\mathbf{Z}$ and a finite cyclic group of order $q/2$.

In particular when $q = 4$ or 6, this subgroup has a rather special form. Indeed, it contains all the even elements in $H(\sqrt{m})$, $m = 2$ or 3, and therefore will be called the even subgroup denoted by $H_e(\sqrt{m})$, i.e.

$$H_e(\sqrt{m}) = \left\{ M = \begin{pmatrix} a & b\sqrt{m} \\ c\sqrt{m} & d \end{pmatrix} \ : \ M \in H(\sqrt{m}) \right\}. \tag{9}$$

In general for any even q, the even subgroup obtained above will be denoted by $H_e(\lambda_q)$. It is generated by $T = RS$ and $TU = RS^2R$, and in fact

$$H_e(\lambda_q) \cong < T > \star < TU > . \tag{10}$$

We shall see in Corollary 1 that the elements of $H(\lambda_q)$ has one of the forms $V(z) = (az + b\lambda)/(\lambda cz + d)$ or $V(z) = (\lambda\alpha z + \beta)/(\gamma z + \lambda\delta)$ where $\lambda = \lambda_q$ and $a, b, c, d, \alpha, \beta, \gamma, \delta$ are all polynomials in λ_q^2 with rational integer coefficients. In a similar way to $q = 4$ and 6 cases, we can consider the elements of the former type as even elements and the ones of the latter type as odd. Again (8) hold in this case. Therefore

$$H_e(\lambda_q) = \left\{ M = \begin{pmatrix} a & b\lambda_q \\ c\lambda_q & d \end{pmatrix} \; : \; M \in H(\lambda_q) \right\}. \tag{11}$$

The set of odd elements

$$H_o(\lambda_q) = \left\{ N = \begin{pmatrix} a\lambda_q & b \\ c & d\lambda_q \end{pmatrix} \; : \; N \in H(\lambda_q) \right\} \tag{12}$$

forms the other coset of $\mathrm{H}_e(\lambda_q)$ in $\mathrm{H}(\lambda_q)$. In fact

$$H(\lambda_q) \; = \; H_e(\lambda_q) \, + \, R.H_e(\lambda_q), \tag{13}$$

as $R \notin H_e(\lambda_q)$.

It is not possible to have the even subgroup for the odd values of q. Indeed the elliptic generator S has order q in $\mathrm{H}(\lambda_q)$ and cannot be mapped to an element of order two.

$\mathrm{H}_e(\lambda_q)$ is quite important amongst the normal subgroups of $\mathrm{H}(\lambda_q)$. In fact it contains infinitely many other normal subgroups.

We shall deal with $\mathrm{H}_e(\sqrt{m})$, $m = 2, 3$, in detail, when we discuss the normal subgroups of $\mathrm{H}(\sqrt{m})$ in Chapters 8 and 9.

Now we know all elements of Γ, $\mathrm{H}(\sqrt{2})$ and $\mathrm{H}(\sqrt{3})$. In other cases the elements of $\mathrm{H}(\lambda_q)$ are worked out by D. Rosen in [Ro,2]. Using continued λ-fractions he gave the necessary and sufficient conditions for a substitution to be an element of $\mathrm{H}(\lambda_q)$. Because of the importance of being able to determine the elements of Hecke groups, we now recall his ideas:

As shown in Chapter 1, an element of $H(\lambda_q)$ can be expressed, in terms of the generators R and T, as

$$V(z) = \frac{az+b}{cz+d} = T^{r_0}RT^{r_1}R\ldots RT^{r_n}, \tag{14}$$

where the r_i's $(0 \leq i \leq n)$ are integers such that only r_0 and r_n may be zero.

We shall write a continued fraction with arbitrary elements

$$b_0 + \frac{a_1}{b_1 + \frac{a_2}{b_2 + \frac{a_3}{b_3 + \ldots}}} \tag{15}$$

as

$$(b_0,\ a_1/b_1,\ a_2/b_2,\ \ldots). \tag{16}$$

The a_i's and b_i's $(i = 0, 1, 2, \ldots)$ will be called the $i-th$ *partial numerator* and *denominator* respectively, while a_i/b_i denotes the $i-th$ *partial quotient* or *term* of the continued fraction. The finite continued fraction consisting of the first $n+1$ terms, when written as the quotient of two polynomials in a_i, b_i, will be called the $n-th$ *convergent* of the continued fraction, and denoted by

$$P_n/Q_n = (b_0,\ a_1/b_1,\ \ldots, a_n/b_n). \tag{17}$$

Here we shall consider the continued λ–fraction

$$(r_0\lambda,\ \epsilon_1/r_1\lambda,\ \epsilon_2/r_2\lambda,\ \ldots) \tag{18}$$

where $\epsilon_i = \pm 1$, r_0 is a rational integer, r_i is a positive rational integer for $i \geq 1$. The values of $\lambda = \lambda_q$ are restricted to those for which $H(\lambda_q)$ is Fuchsian.

An equivalent form of the λ –fraction (18) is

$$(r_0\lambda,\ -1/r_1\lambda,\ -1/r_2\lambda,\ \ldots) \tag{19}$$

where the r_i's ($i \geq 0$) are now integers and only r_0 may be zero. If the λ-fraction (19) is finite, say consisting of $n+1$ terms, then r_n may also be zero.

Now we have

Theorem 1: A substitution $V(z) = (Az+B)/(Cz+D) \in \mathrm{H}(\lambda_q)$ if and only if $A/C = P_n/Q_n = (r_0\lambda_q, -1/r_1\lambda_q, \dots, -1/r_n\lambda_q)$, i.e. A/C is a finite λ_q-fraction.

Proof: [Ro,2].

Note that B/D is also a finite λ-fraction if A/C is. Moreover B/D and A/C are consecutive convergents of a finite λ-fraction consisting of $n+1$ partial quotients if $r_n \neq 0$ and n partial quotients if $r_n = 0$, i.e.

$$V = \begin{cases} \begin{pmatrix} \epsilon P_{n-1} & P_n \\ \epsilon Q_{n-1} & Q_n \end{pmatrix} & \text{if} \quad r_n \neq 0, \\ \\ \begin{pmatrix} \epsilon P_n & P_{n-1} \\ \epsilon Q_n & Q_{n-1} \end{pmatrix} & \text{if} \quad r_n = 0, \end{cases} \tag{20}$$

where $\epsilon = \pm 1$ is chosen to make the determinant equal to 1.

By Theorem 1, we can determine whether a given substitution is in $\mathrm{H}(\lambda_q)$ or not. It is also important, as in the cases $q = 4$ and 6, to know the form of the elements of $\mathrm{H}(\lambda_q)$. The following corollary will supply this to us:

Corollary 1: If $V \in \mathrm{H}(\lambda_q)$, then V has one of the forms

$$V(z) = \frac{az + b\lambda}{\lambda cz + d} \quad or \quad V(z) = \frac{\lambda\alpha z + \beta}{\gamma z + \lambda\delta} \tag{21}$$

where $a, b, c, d, \alpha, \beta, \gamma$ and δ are all polynomials in λ^2 with rational integer coefficients.

Note that the result given in Corollary 1 coincides with the one given for $q = 4$ or 6, while when $q = 3$, it is clear.

Theorem 1 gives us a characterisation of the parabolic points of the Hecke groups. These are the transforms of ∞ under the elements of $H(\lambda_q)$. As the fixed point of T, ∞ is a parabolic point. All other parabolic points are real. In fact a real point is parabolic if and only if it is congruent to ∞ under a group element. We then have

Corollary 2: The point $z = -D/C$ is a parabolic point if and only if $-D/C$ is a finite λ-fraction.

In Chapter 0, we recall some definitions and results which will often be used in the following chapters. The main ideas discussed there are Galois theory and field extensions, projective groups, basic notions concerning Fuchsian groups, the permutation method and Riemann–Hurwitz formula, the Reidemeister–Schreier method, free groups and products, all in connection with the Hecke groups, and finally, commensurability of Hecke groups.

In the first chapter, we deal with two important problems: the determination of the cuspset and the determination of the group theoretical structure of Hecke groups. These two problems are related to each other in a way that one way of solving them is to make use of fundamental regions. Therefore we begin by recalling the results concerned with the fundamental region of the modular group and then move on to the discussion of the fundamental region for Hecke groups in general. To solve both problems we introduce some polynomials denoted by α_n which give the relations between the images of the vertices of a fundamental region for $H(\lambda_q)$.

Chapter 2 is about the determination of the minimal polynomial of λ_q over $\mathbf{Q}$. As we explained above, the first four values of λ_q are obtained for $q = 3,4,5,6$ as 1, $\sqrt{2}$, $(1+\sqrt{5})/2$, $\sqrt{3}$, and are rather nice algebraic numbers. However for $q \geq 7$, it is not possible to obtain λ_q that nicely. Therefore obtaining properties of Hecke groups, involving λ_q, will only be possible by using the minimal polynomial instead of λ_q.

As it can be understood from its title, this thesis is concerned with the normal subgroups of the Hecke groups $H(\lambda_q)$. Therefore we will try to use several methods to determine these normal subgroups. One of them is to make use of regular map theory. We recall a 1:1 correspondence, given by Jones and Singerman in [Jo–Si,1], between the regular maps and normal subgroups of certain triangle groups including Hecke groups $H(\lambda_q)$. By means of this correspondence, we will try to get information about normal subgroups of $H(\lambda_q)$ from some well-known regular maps. We will see some applications of this in Chapters 4 and 5.

In Chapter 4 we discuss the normal genus 0 subgroups of $H(\lambda_q)$. We determine their total number for all q and also give a classification of them. It will be shown that most of these subgroups have torsion. Therefore beginning with the normal genus 0 subgroups having torsion, we will discuss all normal torsion subgroups of $H(\lambda_q)$. We will detemine their number in each case and give a classification of them. Torsion–free normal subgroups of $H(\lambda_q)$ will also be discussed there.

Chapter 5 is concerned with the normal genus 1 subgroups of Hecke groups $H(\lambda_q)$. We shall determine the values of q for which $H(\lambda_q)$ has normal subgroups of genus 1. We shall also determine the q such that $H(\lambda_q)$ has a torsion–free normal subgroup of genus 1. All these will be done using the regular map theory established by Jones and Singerman in [Jo–Si,1] and recalled in Chapter 3. As a nice application of this theory, we are going to calculate the number of normal genus 1 subgroups of a given index in $H(\lambda_q)$.

We have already mentioned some differences between odd and even q cases. $q =$ 4 and 6 give two of the most important Hecke groups and they are both examples of the even q situation. Therefore most properties of $H(\lambda_q)$ for even q will be discussed in Chapters 8 and 9 where we deal with the normal subgroups of $H(\sqrt{2})$ and $H(\sqrt{3})$. This leaves us the odd q case to consider, and this will be done in Chapter 6.

In Chapter 7 we discuss the principal congruence subgroups of Hecke groups. In the modular group case, they have been discussed by Newman [Ne,6] and Mc Quillan [MQ,1]. It can be said that principal congruence subgroups are the most important normal subgroups of the modular group Γ. Here we discuss them for $q = 4, 6$ and $q = p$, a prime. We use [Ma,1] to determine the quotients of $H(\lambda_q)$ by them and then we find their group theoretical structures. Also in this chapter, we prove that $H(\lambda_q)$ has infinitely many normal subgroups of finite index.

In Chapters 8 and 9, we discuss normal subgroups of $H(\sqrt{2})$ and $H(\sqrt{3})$, and make some generalisations to the even q case. The lists of normal subgroups of these two important Hecke groups with small index are given at the end of this thesis.

Another important Hecke group is $H(\lambda_5)$. As 5 is prime, this group shows a lot of similarities to the modular group. Some properties and normal subgroups of $H(\lambda_5)$ will have been discussed in the earlier chapters and they will be briefly recalled in Chapter 10.

Chapter 0

PRELIMINARIES

0.0. INTRODUCTION

In this chapter we give some definitions and results about the normal subgroups of Hecke groups $H(\lambda_q)$, which will be used often in this work. To do this we need to recall some classical notions and results such as Galois fields, field extensions, projective groups and Fuchsian groups.

0.1. GALOIS THEORY AND FIELD EXTENSIONS

Several times in this thesis we will need finite extensions of fields. Although there are other kinds of field extensions, the ones we are going to use will usually be simple extensions. Therefore we start by recalling the notion of simple extension.

Let us first recall the construction of the field **C** of complex numbers from the field **R** of real numbers. The complex number i is a zero of the second degree monic irreducible polynomial

$$f(x) = x^2 + 1 \in \mathbf{R}[x], \tag{0.1}$$

and the elements of $\mathbf{C}$ are uniquely written in the form $z = a + b\mathbf{i}$ where $a, b \in \mathbf{R}$ and $\mathbf{i}^2 = -1$. This is a simple extension of the field $\mathbf{R}$ to the field $\mathbf{C}$ by adding a single element $\mathbf{i}$ which is not in $\mathbf{R}$ but is a root of a monic irreducible polynomial in the polynomial ring $\mathbf{R}[\mathrm{x}]$.

Similarly let $\mathbf{F}$ be a field. Let f be a monic irreducible polynomial of degree n in $\mathbf{F}[\mathrm{x}]$. We can construct a *simple extension* $\mathbf{F}(\mathrm{u})$ of $\mathbf{F}$ in which u is a root of f. It is a well-known result that every element v of $\mathbf{F}(\mathrm{u})$ has a unique representation in the form

$$v = a_0 + a_1 u + \ldots + a_{n-1} u^{n-1} \tag{0.2}$$

with $a_i \in \mathbf{F}$ for $i = 0, 1, \ldots, n-1$. In this case we say that u is *algebraic of degree n over* $\mathbf{F}$.

The existence of a simple extension of a field is given by the following theorem:

Theorem 0.1: Let $\mathbf{F}$ be a field and f a monic irreducible element of $\mathbf{F}[\mathrm{x}]$ of degree n. Then there is a simple extension $\mathbf{K} = \mathbf{F}(\mathrm{u})$ of $\mathbf{F}$ such that u is algebraic over $\mathbf{F}$ with minimal polynomial f.

Proof: See [Fr,1].

One of the applications of simple extensions in our thesis will be cyclotomic extensions. If ζ is a primitive *n-th root of unity*, i.e. a root of the *cyclotomic equation of degree n*

$$\zeta^n - 1 = 0, \tag{0.3}$$

then by adding ζ to the field $\mathbf{Q}$ of rationals, we will obtain the *n-th cyclotomic extension* of $\mathbf{Q}$.

In Chapter 2 we will try to determine the degree of the minimal polynomial of λ_q. To do this we shall need some definitions and results from *Galois theory*, such as Galois group, normal extension, etc., which are recalled in the following:

Let $\mathbf{F}$ be a subfield of a field $\mathbf{K}$.

If $u, v \in \mathbf{K}$ are algebraic over $\mathbf{F}$, then u and v are called *conjugates* over $\mathbf{F}$ if they have the same minimal polynomial over $\mathbf{F}$.

The extension $\mathbf{K}$ over $\mathbf{F}$ is said to be *closed under conjugates* if whenever $\mathbf{F} \prec \mathbf{K} \prec \mathbf{L}$, $u \in \mathbf{K}$, and $v \in \mathbf{L}$ is a conjugate of u over $\mathbf{F}$, then $v \in \mathbf{K}$. $\mathbf{K}$ is closed under conjugates if and only if whenever f is an irreducible polynomial in $\mathbf{F}[\mathrm{x}]$ having any roots in $\mathbf{K}$ then it splits in $\mathbf{K}$(see [Fr,1]).

$\mathbf{K}$ is said to be a *normal extension* of $\mathbf{F}$ if $\mathbf{K}$ is closed under conjugates.

The collection of all automorphisms of $\mathbf{K}$ leaving $\mathbf{F}$ fixed forms a group denoted by $G(\mathbf{K}/\mathbf{F})$. If $\mathbf{K}$ is a finite normal extension of $\mathbf{F}$, then $G(\mathbf{K}/\mathbf{F})$ is called the *Galois group* of $\mathbf{K}$ over $\mathbf{F}$. We now have the following result which will be needed in Chapter 2:

Theorem 0.2: The Galois group of the n-th cyclotomic extension of $\mathbf{Q}$ has $\varphi(n)$ elements, where φ denotes the Euler function, and is isomorphic to the group of units *modulo* n.

Proof: See [Fr,1; pp 472].

Corollary 0.1: The Galois group of the p-th cyclotomic extension of $\mathbf{Q}$ for a prime p is of order $p-1$.

0.2. PROJECTIVE GROUPS

It is known that for every prime power $q = p^n$, there is, up to isomorphism, a unique field of q elements, denoted by $GF(q)$. This is the Galois field of q elements. All finite fields are of this form.

Let now $\mathbf{K}$ be a field of order $q = p^n$, i.e. $\mathbf{K} = \mathrm{GF(q)}$. Then the *general linear group* $GL(2, \mathbf{K})$ is defined by

$$GL(2,\mathbf{K}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \mathrm{a, b, c, d} \in \mathbf{K},\ \mathrm{ad} - \mathrm{bc} \neq 0 \right\}. \tag{0.4}$$

This group acts on the 2–dimensional vector space $\mathbf{K}^2 = \mathbf{K} \oplus \mathbf{K}$ as a group of linear fractional transformations and it permutes the set $PG(1, \mathbf{K})$ of 1–dimensional subspaces of $\mathbf{K}^2$. The center of this group, denoted by $Z(GL(2, \mathbf{K}))$ consists of all the scalar 2×2 matrices and it forms a normal subgroup of $GL(2, \mathbf{K})$. By means of this, we define the *projective general linear group* $PGL(2, \mathbf{K})$ as

$$PGL(2,\mathbf{K}) = \mathrm{GL}(2,\mathbf{K})/\mathrm{Z}(\mathrm{GL}(2,\mathbf{K})). \tag{0.5}$$

The matrices of determinant 1 in $GL(2, \mathbf{K})$ form a subgroup called the *special linear group*

$$SL(2,\mathbf{K}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,\mathbf{K}) : \mathrm{ad} - \mathrm{bc} = 1 \right\}, \tag{0.6}$$

and the *projective special linear group* is then

$$PSL(2,\mathbf{K}) = \mathrm{SL}(2,\mathbf{K})/\mathrm{Z}(\mathrm{SL}(2,\mathbf{K})). \tag{0.7}$$

Here $Z(SL(2, \mathbf{K}))$ is $\{\pm I\}$ if $p > 2$ and $\{I\}$ if $p = 2$. The order of $PSL(2, \mathbf{K})$ is $q(q-1)(q+1)/2$ if $p > 2$ and $q(q-1)(q+1)$ otherwise.

There is a natural homomorphism from $SL(2, \mathbf{K})$ onto $PSL(2, \mathbf{K})$ which takes an element $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $SL(2, \mathbf{K})$ to a unique element, i.e. the coset $\pm \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $PSL(2, \mathbf{K})$. Because of this we can represent an element of $PSL(2, \mathbf{K})$ by either of the two matrices in $SL(2, \mathbf{K})$ which induce it.

Up to now we have only considered the projective groups over finite fields. But in general the four groups defined above, i.e. $GL(2, \mathbf{K})$, $\mathrm{PGL}(2, \mathbf{K})$, $\mathrm{SL}(2, \mathbf{K})$ and $PSL(2, \mathbf{K})$, can be defined in case of $\mathbf{K}$ being an infinite field, by taking all entries of the matrices or the induced linear fractional transformations from this infinite field. The most interesting examples are $PSL(2, \mathbf{R})$, $\mathrm{PSL}(2, \mathbf{C})$ and their correspondences in the other three classes of projective groups.

It is also possible to define projective groups over rings with identity; e.g. $PSL(2, \mathbf{Z})$.

We finally give a result which determines that for what values of a prime power q, the projective special groups $PSL(2, q)$ are Hurwitz groups — groups of $84(g-1)$ automorphisms on a Riemann surface of genus g:

Theorem 0.3: The group $PSL(2, q)$ is a Hurwitz group if

(i) $q = 7$,

(ii) $q = p \equiv \pm 1 \; (mod\, 7)$,

(iii) $q = p^3, \; where\, p \equiv \pm 2, \pm 3 \; (mod\, 7)$

and for no other values of q.

Proof: See [Ma,1].

0.3. FUCHSIAN GROUPS AND THEIR SUBGROUPS, PERMUTATION METHOD

By a *Fuchsian group* Γ we understand a finitely generated discrete subgroup of $PSL(2,\mathbf{R})$— the group of conformal homeomorphisms of the upper half plane $\mathcal{U}$.

It is known that every Fuchsian group has a presentation of the following form:

$$\begin{array}{lll} \text{Generators:} & a_1, b_1, \dots, a_g, b_g & \text{(hyperbolic)}, \\ & x_1, \dots, x_r & \text{(elliptic)}, \\ & p_1, \dots, p_t & \text{(parabolic)}, \\ & h_1, \dots, h_u & \text{(hyperbolic boundary elements)}, \end{array} \tag{0.8}$$

$$\text{Relations: } x_j^{m_j} = \prod_{i=1}^{g} [a_i, b_i] \prod_{j=1}^{r} x_j \prod_{k=1}^{t} p_k \prod_{l=1}^{u} h_l = 1.$$

We then say Γ has *signature*

$$(g;\, m_1, \dots, m_r;\, t;\, u)\,; \tag{0.9}$$

where $m_1, \dots, m_r$ are integers ≥ 2 and are called the *periods* of Γ.

We must note the following facts about this presentation: every elliptic element of Γ is conjugate to a power of one of the x_j $(1 \leq j \leq r)$, every parabolic element of Γ is conjugate to a power of one of the p_k $(1 \leq k \leq t)$ and every hyperbolic boundary element of Γ is conjugate to a power of one of the h_l $(1 \leq l \leq u)$. Moreover no non–trivial power of one of the generators can be conjugate to a power of another generator. (see, for a proof of these facts [Lh,2]).

Let us now recall the *limit set* $L(\Gamma)$ for a Fuchsian group Γ. $L(\Gamma)$ is a subset of the real line satisfying one of the following conditions:

(i) $L(\Gamma)$ has at most two points,

(ii) $L(\Gamma) = \mathbf{R}$,

(iii) $L(\Gamma)$ is a perfect nowhere dense subset of $\mathbf{R}$.

Groups of type (ii) are called *groups of the first kind* and groups of type (iii) *of the second kind.* We shall mainly be interested in groups of type (ii).

For all normal subgroups of finite index of Hecke groups, $u = 0$, as they do not have hyperbolic boundary elements. Let Γ be a group with signature (0.9) such that $u = 0$. Define

$$\mu(\Gamma) = 2g - 2 + \sum_{i=1}^{r} \left(1 - \frac{1}{m_i}\right) + t. \tag{0.10}$$

If Γ is of the first kind then $\mu(\Gamma) > 0$. In this case $2\pi\mu(\Gamma)$ is the hyperbolic measure of a fundamental region for Γ. As we shall prove in Chapter 1, $\mathrm{H}(\lambda_q)$ has a signature $(0; 2, q, \infty)$ and therefore, has a fundamental region of finite hyperbolic area $2\pi(1 - 1/2 - 1/q)$. Let now Γ_1 be a subgroup of Γ with finite index. Then

$$[\Gamma : \Gamma_1] = \frac{\mu(\Gamma_1)}{\mu(\Gamma)}. \tag{0.11}$$

This formula is called the *Riemann–Hurwitz formula* and is probably the most useful tool in the study and classification of Fuchsian groups and will be used very often in this thesis (If $u = 0$, (0.11) follows from the fact that $2\pi\mu(\Gamma)$ is the hyperbolic measure of a fundamental region. If $u > 0$, ($\mu(\Gamma) = \infty$ in this case), Maclachlan proved this result in [Mc,1]).

The study of subgroups of Fuchsian groups is obviously quite related to this work, and as a result of this we shall often use the following important result, which will be called the permutation method, proved by Singerman [Si,2]:

Theorem 0.4: Let Γ_2 be a Fuchsian group with signature (0.9). Then Γ_2 contains a subgroup Γ_1 of index μ with signature

$$(g'; n_{11}, \dots, n_{1\rho_1}, \dots, n_{r1}, \dots, n_{r\rho_r}; t'; u') \tag{0.12}$$

if and only if

(a) there exists a finite permutation group G transitive on μ points, and an epimorphism $\Theta : \Gamma_2 \to G$ satisfying the following conditions:

(i) the permutation $\Theta(x_j)$ has precisely ρ_i cycles of lengths less than m_j, the lengths of these cycles being $m_j/n_{j1}, \dots, m_j/n_{j\rho_j}$;

(ii) if we denote the number of cycles in the permutation $\Theta(\gamma)$ by $\delta(\gamma)$, then

$$t' = \sum_{k=1}^{t} \delta(p_k), \quad u' = \sum_{l=1}^{u} \delta(h_l) ; \tag{0.13}$$

(b) $\mu(\Gamma_1)/\mu(\Gamma_2) = \mu$.

Proof: See [Si,2].

Recall that, in this thesis, we are concerned with the normal subgroups of the Hecke groups $H(\lambda_q)$. Furthermore Hecke groups are Fuchsian groups of the first kind. Therefore supposing $\Gamma_1 \lhd \Gamma_2$ and Γ_2 is of the first kind, we can now obtain the following corollary for normal subgroups of the first kind Fuchsian groups. As Γ_2 is of the first kind, $u = 0$. It is sometimes convenient to consider the parabolic elements as elliptic elements of infinite order. So we may write the signature (0.9) of Γ_2 in a new form

$$(g; m_1, \dots, m_r, m_{r+1}, \dots, m_{r+t}) \tag{0.14}$$

where $m_{r+1} = \dots = m_{r+t} = \infty$. Let now $[\Gamma_2 : \Gamma_1] = \mu$. Let v_i be the exponent of x_i *modulo* Γ_1, i.e. the least integer such that $x_i^{v_i} \in \Gamma_1$. Clearly $v_i < \infty$ and $v_i \mid m_i$

if $m_i < \infty$. Some of the x_i's in Γ_2 may have exponent m_i *modulo* Γ_1. Rearranging the periods so that $v_i = m_i$ only for $1 \leq i \leq p$ and x_{i+p} has exponent $n_i < m_{i+p}$ otherwise, we find that (0.14) can be written as

$$(g;\, m_1, \dots, m_p,\, n_1 k_1, \dots, n_q k_q) \tag{0.15}$$

where $p + q = r + t$ and $1 < k_i \leq \infty$. We then deduce the following result given by Singerman [Si,1]:

Corollary 0.2: Let Γ_2 be given by signature (0.15) and Γ_1 be a normal subgroup of finite index μ. Then Γ_1 has signature

$$\left(g_1;\, k_1^{(\mu/n_1)}, \dots, k_q^{(\mu/n_q)}\right) \tag{0.16}$$

where $k_i^{(\mu/n_i)}$ means that the period k_i occurs μ/n_i times. Here g_1 can be found by the Riemann–Hurwitz formula.

As Hecke groups $H(\lambda_q)$ are of the first kind and as we deal mainly with normal subgroups, when we refer to the permutation method we shall actually refer to Corollary 0.2 rather than Theorem 0.4.

We now want to define triangle groups as Hecke groups $H(\lambda_q)$ can be thought of as triangle groups with a parabolic generator.

Let $l, m, n \geq 2$ be integers. Consider the hyperbolic triangle with angles π/l, π/m, π/n.

Let σ_1, σ_2, σ_3 be the reflections on the sides of this triangle as shown in Figure 0.1. Let Γ^* be the group generated by these three reflections:

$$\Gamma^* = \left\langle \sigma_1, \sigma_2, \sigma_3 \mid \sigma_1^2 = \sigma_2^2 = \sigma_3^2 = (\sigma_2\sigma_3)^l = (\sigma_3\sigma_1)^m = (\sigma_1\sigma_2)^n = 1 \right\rangle. \tag{0.17}$$

Put $x = \sigma_2\sigma_3$ and $y = \sigma_3\sigma_1$. Then x is a rotation around the vertex A by $2\pi/l$ and y is a rotation around the vertex B by $2\pi/m$. Then xy is a rotation around C by $2\pi/n$. These are all orientation preserving isometries. Therefore we obtain a subgroup Γ of Γ^* containing only orientation preserving isometries:

$$\Gamma = \left\langle x, y \mid x^l = y^m = (xy)^n = 1 \right\rangle . \tag{0.18}$$

This subgroup has signature $(0;\ l, m, n)$ as a Fuchsian group and usually denoted by (l, m, n). It is called a *triangle group*. It has index two and is therefore a normal subgroup of Γ^*.

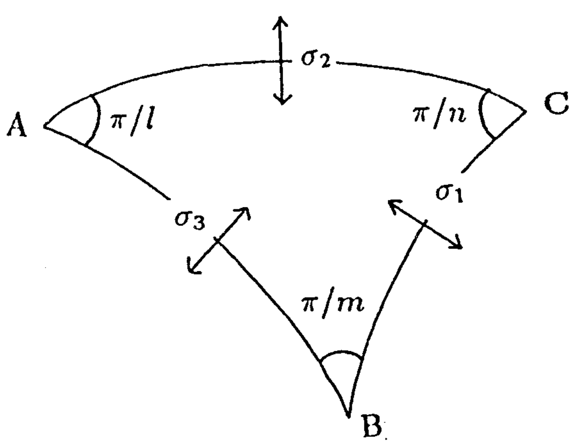


Figure 0.1.

As we shall prove in Chapter 1, the Hecke group $\mathrm{H}(\lambda_q)$ is a triangle group with signature $(0;\ 2, q, \infty)$. We also know that parabolic elements can be realized as elliptic elements of infinite order. Of course in this case $(xy)^\infty = 1$ is void, and therefore $\mathrm{H}(\lambda_q)$ is a triangle group such that

$$H(\lambda_q) \cong (2, q, \infty) \cong \left\langle x, y \mid x^2 = y^q = 1 \right\rangle \tag{0.19}$$

which is isomorphic to the free product of two finite cyclic groups of order 2 and q (an elementary proof of this result is given in section 1.3.). It is easy to see that the above triangle turns into one of the two triangles in Figure 0.2 with angles $\pi/2$, π/q, $\pi/\infty = 0$.

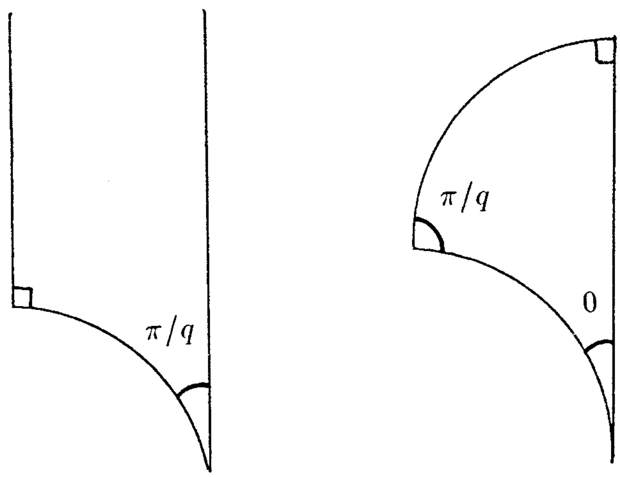


Figure 0.2.

0.4. SOME RELATIONS BETWEEN μ, n AND t

Let N be a normal subgroup of $\mathrm{H}(\lambda_q)$ with finite index μ. We define the *parabolic class number* t of N as the number of conjugacy classes of maximal parabolic cyclic subgroups and the *level* n of N as the least positive integer such that $T^n \in N$. Then it follows from Corollary 0.2 that

$$\mu = n.t. \tag{0.20}$$

The following result enables us to decide about inclusions between the normal subgroups of Hecke groups:

Lemma 0.1: Let N_1, N_2 be two normal subgroups of $\mathrm{H}(\lambda_q)$ with finite index such that $N_1 \supset N_2$. Let N_1 be of level n_1 and have t_1 parabolic classes, N_2 be of level n_2 and have t_2 parabolic classes. Then

$$n_1 | n_2 \quad and \quad t_1 | t_2. \tag{0.21}$$

Proof That $n_1|n_2$ is elementary group theory. The fact that $t_1|t_2$ follows from Corollary 0.2.

Since Hecke groups are finitely generated, a subgroup of finite index will also be finitely generated and to find these generators will be very important in our work. To be able to do this we have the following method:

0.5. THE REIDEMEISTER–SCHREIER METHOD

The Reidemeister–Schreier method is a useful technique which will be used to find the generators of subgroups of $\mathrm{H}(\lambda_q)$ with finite index.

Let G be a finitely generated group with generators $\{g_i\}$. Let H be a subgroup of G. The Reidemeister–Schreier method consists of firstly choosing a Schreier transversal for H and then taking ordered products of the elements of this transversal, generators and coset representatives, as described below:

A *Schreier transversal* Σ is defined in [Jh,1] by Johnson. It consists of a set of coset representatives satisfying the following conditions:

(i) The identity element $I \in \Sigma$,

(ii) Σ is closed under right cancellation; i.e. if $g_{i_1}.g_{i_2}.\cdots.g_{i_r} \in \Sigma$, then $g_{i_1}.g_{i_2}.\cdots.g_{i_{r-1}}$ must be in Σ.

Let Σ be a Schreier transversal for N. Then a Schreier generator of N will have the form

$$(An\ element\ of\ \Sigma)\times(A\ generator)\times(Coset\ representative\ of\ preceeding\ product)^{-1} \tag{0.22}$$

Example 0.1: We want to find out the generators of the commutator subgroup H$'(\sqrt{2})$ of H$(\sqrt{2})$, which will be discussed later in this chapter (see below for the definition). We shall see that H$'(\sqrt{2})$ is a normal subgroup of H$(\sqrt{2})$ with quotient group isomorphic to the direct product of two cyclic groups of orders two and four. Therefore it has index 8 in H$(\sqrt{2})$. There is a homomorphism

$$\Theta : H(\sqrt{2}) \longrightarrow H(\sqrt{2})/H'(\sqrt{2}) \cong C_2 \times C_4. \tag{0.23}$$

Recall that H$(\sqrt{2})$ has a presentation $< R, S : R^2 = S^4 = I >$. We choose a Schreier transversal for H$'(\sqrt{2})$ as

$$I, S, S^2, S^3, R, RS, RS^2, RS^3. \tag{0.24}$$

Now we can form all possible products formulated in (0.22):

$$\begin{array}{ll} I.R.R^{-1} = I & R.R.I^{-1} = I \\ I.S.S^{-1} = I & R.S.(RS)^{-1} = I \\ S.R.(RS)^{-1} = SRS^3R & RS.R.S^{-1} = RSRS^3 \\ S.S.(S^2)^{-1} = I & RS.S.(RS^2)^{-1} = I \\ S^2.R.(RS^2)^{-1} = S^2RS^2R & RS^2.R.(S^2)^{-1} = RS^2RS^2 \\ S^2.S.(S^3)^{-1} = I & RS^2.S.(RS^3)^{-1} = I \\ S^3.R.(RS^3)^{-1} = S^3RSR & RS^3.R.(S^3)^{-1} = RS^3RS \\ S^3.S.I^{-1} = I & RS^3.S.R^{-1} = I. \end{array} \tag{0.25}$$

Now since $(SRS^3R)^{-1} = RSRS^3$, $(S^2RS^2R)^{-1} = RS^2RS^2$ and $(S^3RSR)^{-1} = RS^3RS$, we have

$$H'(\sqrt{2}) \cong < RSRS^3,\ RS^2RS^2,\ RS^3RS >; \tag{0.26}$$

i.e. H$'(\sqrt{2})$ is the group generated by $a = RSRS^3$, $b = RS^2RS^2$ and $c = RS^3RS$. In fact it is known that

$$H'(\sqrt{2}) \cong < a, b, c : - >, \tag{0.27}$$

that is, H$'(\sqrt{2})$ is isomorphic to a free group of rank three.

0.6. COMMUTATOR SUBGROUPS, FREE GROUPS AND FREE PRODUCTS

In this section we shall recall the commutator subgroup of a group in general and discuss its basic properties. Then we shall apply these ideas to Hecke groups to obtain more information about H$'(\lambda_q)$—the commutator subgroup of H(λ_q). As H(λ_q) is isomorphic to the free product of two finite cyclic groups of orders two and q, we shall often need information about free products. Therefore we recall some results concerning them. As Hecke groups have infinitely many normal free subgroups, we also discuss the free groups briefly in this chapter.

Let us now recall the commutator subgroup of a group G. The *commutator subgroup* of G is denoted by G' or $[G, G]$ and defined by

$$< [g, h] \, : \, g, h \in G > \tag{0.28}$$

where $[g, h]{:=}ghg^{-1}h^{-1}$. We shall prefer the first notation.

G' is a normal subgroup of G (see [A1,1]). Therefore we can form the quotient group G/G'. This group is very significant in the study of the abelian quotients of a group:

Lemma 0.2: G/G' is the largest abelian quotient group of G. That is, if G/N is any other abelian quotient of G, then

$$G' \lhd N \lhd G \tag{0.29}$$

and there exists a homomorphism

$$\Theta : G/G' \longrightarrow G/N. \tag{0.30}$$

See [Al,1; pp 259] for a proof.

The second and the other commutator subgroups are defined succesively as the commutator subgroup of the previous one, e.g.

$$G'' := < [a, b] : a, b \in G' > . \tag{0.31}$$

We now have:

Lemma 0.3: Let G be a group generated by k elements $a_1, \ldots, a_k$. Let M be the normal subgroup of G generated by all the commutators $[a_i, a_j]$ of the generators. Then

$$M = G'. \tag{0.32}$$

Proof: Obviously G/M is abelian. But by Lemma 0.2, G/G' is the largest abelian quotient group of G. As $M \leq G'$, $M = G'$.

As we have noted before, $H(\lambda_q)$ has, as a free product, some free subgroups. To be able to understand the structure of these subgroups and to get more information about them we now recall some classical results:

Intuitively, a group is *free* if there is a set of generators with no relations between them. We now make this precise as follows:

Let X be a subset of a group F. Then F is a free group with basis X provided the following holds: If ϕ is any function from the set X into a group H, then there exists a unique extension of ϕ to a homomorphism ϕ^* from F to H. Here, we need the uniqueness to make X generate F.

The cardinal of X will be called the *rank* of F. If $|X| = n$, then the generated free group will be denoted by F_n. Note that all bases of a free group necessarily have the same cardinal.

It is easy to see that two free groups are isomorphic if and only if they have the same rank (see [Ly–Sc,1; pp 1]).

A free group of rank 0 is trivial, and of rank 1 is infinite cyclic.

Finitely generated Fuchsian groups of the first kind containing parabolics are free if and only if they have no elliptic element, e.g. a group of signature $(0 \, ; \infty^{(t)}) \cong F_{t-1}$.

The following is a well-known property of the subgroups of free groups:

Theorem 0.5: Every subgroup of a free group is again a free group.

It is also known that every group is a homomorphic image of a free group.

We can now determine the rank—i.e. the number of free generators—of a subgroup of a free group with a given rank. For this we need:

Theorem 0.6: Let H be a subgroup of finite index μ in a free group G of finite rank R. Then the rank r of H is also finite and given by

$$r = 1 + \mu(R - 1). \tag{0.33}$$

Proof: This easily follows from the Riemann–Hurwitz formula and from the fact that the rank of a free group of genus g having t parabolic classes is equal to $2g+t-1$.

Let now G be a free normal subgroup of $\mathrm{H}(\lambda_q)$ of finite index μ. Let G have t parabolic classes. We can use the Riemann–Hurwitz formula to find the signature of G:

Theorem 0.7: Let G be a free normal subgroup of $\mathrm{H}(\lambda_q)$ of finite index μ. Then it has the signature

$$\left(1 - \frac{t}{2} + \mu.\frac{q-2}{4q}\ ;\ \infty^{(t)}\right). \tag{0.34}$$

Proof: As G is free, it has the signature $(g\ ;\ \infty^{(t)})$. By the Riemann–Hurwitz formula

$$2g - 2 + t \ = \ \mu.\left(-2 + 1 - \frac{1}{2} + 1 - \frac{1}{q} + 1\right) \tag{0.35}$$

and therefore

$$g \ = \ 1 - \frac{t}{2} + \mu.\frac{q-2}{4q}. \tag{0.36}$$

We now briefly discuss some properties of the free products. We shall omit the definition as it is a bit detailed and also well-known.

The free product of the groups A_i, $i \in I$, is going to be denoted by

$$\prod_{i \in I} {}_{\star}\, A_i. \tag{0.37}$$

We have already noted that $\text{H}(\lambda_q)$ is isomorphic to the free product of two finite cyclic groups of order two and q. As we are studying the normal subgroups of the Hecke groups, we need a result that gives the general character of the subgroups of free products. This result is known as Kurosh subgroup theorem:

Theorem 0.8: (KUROSH SUBGROUP THEOREM) Let the group G be the free product of subgroups A_α. We write this as

$$G = \prod_{\alpha} {}_* A_\alpha. \tag{0.38}$$

If H is a subgroup of G, then we have

$$H = F \star \prod_{\beta} {}_* B_\beta, \tag{0.39}$$

where F is a free group and, for each β, B_β is conjugate to a subgroup of some A_α.

Note that $\prod_\beta {}_* B_\beta$ can be empty and that F can be trivial. However if $\prod_\beta {}_* B_\beta$ is not empty, then $[G : F]$ is infinite; for, otherwise, some power of a non–identity element of $\prod_\beta {}_* B_\beta$ would belong to F.

Proof: See [Ra,2; pp36].

Let us now discuss the commutator subgroup of $\text{H}(\lambda_q)$.

We have the relations

$$R^2 = S^q = I, \qquad RS = SR \tag{0.40}$$

in $\text{H}(\lambda_q)/\text{H}'(\lambda_q)$. So

$$H(\lambda_q)/H'(\lambda_q) \cong C_2 \times C_q \tag{0.41}$$

and hence $\cong C_{2q}$ if q is odd. Therefore

$$|\,H(\lambda_q)\,:\,H'(\lambda_q)\,|\;=\;2q. \tag{0.42}$$

If q is even, $(RS)^q = I$ while if q is odd, $(RS)^{2q} = I$. Therefore by Corollary 0.2, $\mathrm{H}'(\lambda_q)$ has parabolic class number 2 if q is even and 1 if q is odd. The genus can be computed by the Riemann–Hurwitz formula to give

Theorem 0.9:

$$H'(\lambda_q) \cong \begin{cases} \left(\frac{q}{2}-1\,;\,\infty,\infty\right) & \text{if } q \text{ is even,} \\ \left(\frac{q-1}{2}\,;\,\infty\right) & \text{if } q \text{ is odd.} \end{cases} \tag{0.43}$$

In particular, $\mathrm{H}'(\lambda_q)$ is a free group of rank $q-1$.

We also have the following immediate result:

Corollary 0.3: The genus of the commutator subgroup of a Hecke group is always positive.

The Reidemeister–Schreier method gives the generators of $\mathrm{H}'(\lambda_q)$ as

$$a_1 = RSRS^{q-1},\; a_2 = RS^2RS^{q-2},\; \ldots,\; a_{q-1} = RS^{q-1}RS. \tag{0.44}$$

By Theorem 0.6, a subgroup N of $\mathrm{H}'(\lambda_q)$ of finite index μ has finite rank; in fact, if r is the rank of N, then

$$r = 1 + \mu(q-2). \tag{0.45}$$

The following result connects the commutator subgroup and the even subgroup of $\mathrm{H}(\lambda_q)$ when q is even:

Theorem 0.10: Let q be even. Then the commutator subgroup $\mathrm{H}'(\lambda_q)$ of $\mathrm{H}(\lambda_q)$ is a normal subgroup of the even subgroup $\mathrm{H}_e(\lambda_q)$ with index q.

Proof: We have just seen that $\mathrm{H}'(\lambda_q)$ is a normal subgroup of $\mathrm{H}(\lambda_q)$ with index $2q$. The even subgroup $\mathrm{H}_e(\lambda_q)$, having index 2 , is also normal in $\mathrm{H}(\lambda_q)$. Therefore the required index is q.

Let now two elements A, B of $\mathrm{H}(\lambda_q)$ be given. Then whatever A and B are, their commutator $[A, B]$ is always even. Hence for every pair of elements A,B of $\mathrm{H}(\lambda_q)$, we have

$$[A, B] \in H_e(\lambda_q). \tag{0.46}$$

That is,

$$H'(\lambda_q) \lhd H_e(\lambda_q). \tag{0.47}$$

We now have another result that gives the relation between the second commutator subgroup of Hecke groups and the group M defined in Lemma 0.3. We actually show that these two subgroups are equivalent. We should recall, at this point, that $\mathrm{H}'(\lambda_q)$ is of rank $q-1$ and, let us say, generated by $a_1, \ldots, a_{q-1}$. Then we have

Theorem 0.11: Let M be the normal subgroup of $\mathrm{H}'(\lambda_q)$ defined in Lemma 0.3 with $k = q-1$; i.e. M is the normal subgroup containing all commutators of the $a_1, \ldots, a_{q-1}$. Then

$$M = H''(\lambda_q). \tag{0.48}$$

Proof: Follows from Lemma 0.3.

Let us now investigate the group theoretical structure of $H''(\lambda_q)$. We have seen above that $H'(\lambda_q)$ is a free normal subgroup of finite index, $2q$, and of rank $q-1$, of $H(\lambda_q)$. Therefore the second commutator subgroup $H''(\lambda_q)$, as the commutator subgroup of a free group, $H'(\lambda_q)$, is of infinite index in $H'(\lambda_q)$ and hence in $H(\lambda_q)$. Hence

Theorem 0.12: $H''(\lambda_q)$ is a free normal subgroup of infinite rank in $H(\lambda_q)$.

We also have

Theorem 0.13: $H'(\lambda_q)/H''(\lambda_q)$ is a free abelian group with free generators

$$a_1 H''(\lambda_q), \ldots, a_{q-1} H''(\lambda_q) \tag{0.49}$$

where a_i's $(1 \leq i \leq q-1)$ are the generators of $H'(\lambda_q)$ given by (0.47). Also

$$r(H'(\lambda_q)/H''(\lambda_q)) = r(H'(\lambda_q)) = q-1. \tag{0.50}$$

0.7. COMMENSURABILITY OF THE HECKE GROUPS

In this section we discuss commensurability of the Hecke groups.

Two subgroups G, H of a group Γ are said to be *directly commensurable* if $G \cap H$ is of finite index in both G and H. More generally, G, H are said to be *commensurable* in Γ if G and some conjugate of H in Γ are directly commensurable.

It is a known result that $H(\sqrt{2})$ and $H(\sqrt{3})$ are the only Hecke groups commensurable with the modular group Γ. A conjugate of $H(\sqrt{2})$ and Γ have a common subgroup, $\Gamma_0(2)$, but there is no common normal subgroup with finite index in both of them. To see this let us suppose there exists a normal subgroup N in Γ and $H(\sqrt{2})^M$ where $H(\sqrt{2})^M$ denotes the conjugation by a matrix $M \in SL(2, \mathbf{R})$. Let

$\eta(N)$ be the normalizer of N in $PSL(2,\mathbf{R})$. $\mathrm{H}(\sqrt{2})$ contains the element S^M of order 4 and also $S^M \notin \Gamma$. But $\eta(N)$ contains both Γ and S^M. As $\eta(N)$ is also a Fuchsian group, this contradicts with the maximality of Γ (see [Be,1]).

Similarly there is no common normal subgroup of finite index in both Γ and $\mathrm{H}(\sqrt{3})^M$.

Note that the proof depends on the two facts: The maximality of $\Gamma = \mathrm{H}(\lambda_3)$ and discreteness of the normalizer $\eta(N)$ of a normal subgroup N of Γ. This can be extended to any two Hecke groups as these two facts remain true for all Hecke groups:

Theorem 0.14: Let q and r be two distinct integers ≥ 3. Then the set of normal subgroups of finite index in $\mathrm{H}(\lambda_q)$ and the set of normal subgroups of finite index in $\mathrm{H}(\lambda_r)$ are disjoint.

Chapter 1

SOME BASIC RESULTS CONCERNING $H(\lambda_q)$

1.0. INTRODUCTION

As is well-known, fundamental region plays an important role in the geometrical study of a group and its subgroups. Therefore, as our thesis is concerned with the subgroups of the Hecke groups, we shall have a great deal of interest in their fundamental regions.

In this chapter we first define a fundamental region of a group. Then we recall some information about the fundamental region of the most interesting Hecke group which is the modular group. This region is well-known and there has been a lot of research related to it. E. Hecke asked the question that for what values of λ, the group $H(\lambda)$ defined in the introduction is discrete. In answering this question, he proved that $H(\lambda)$ has a fundamental region if and only if $\lambda \geq 2$ and real, or $1 \leq \lambda < 2$ and $\lambda = \lambda_q = 2cos\pi/q$. Therefore $H(\lambda)$ is discrete only for these values of λ. In particular all $H(\lambda_q)$ are discrete groups.

After obtaining fundamental regions for Hecke groups $H(\lambda_q)$, we shall deal with two important problems: Firstly we shall try to determine the parabolic point set (cuspset) of Hecke groups. Parabolic points are basically the images of infinity under the group elements. In the literature there has been several attempts to find this set, but no one has yet given a complete result. There are some results giving partial answers, and they will be recalled here. We shall particularly deal with the four important Hecke groups Γ, $H(\sqrt{2})$, $H(\lambda_5)$, $H(\sqrt{3})$ and give the result in each case.

We also calculate the vertices of the transforms of a specific fundamental region under the subgroup $< S >$ generated by the elliptic generator S of order q which will be used in the determination of the abstract group structure of Hecke groups $H(\lambda_q)$. Since infinity is one of the vertices of the original fundamental region given by Hecke, its transforms under $< S >$ form a class of parabolic points of $H(\lambda_q)$.

Our second main problem in this chapter will be the determination of the abstract group structure of $H(\lambda_q)$. Using a result of Macbeath, we shall prove that $H(\lambda_q)$ is isomorphic to the free product of two finite cyclic groups of orders two and q. This result is well-known for the modular group where $q = 3$.

We begin by the discussion of fundamental region for Hecke groups:

1.1. A FUNDAMENTAL REGION FOR $H(\lambda_q)$

Definition 1.1: An open subset F of the upper half-plane $\mathcal{U}$ is a *fundamental region (domain)* for the group G in $\mathcal{U}$ iff

(i) Each orbit $G(z), z \in \mathcal{U}$, meets $\bar{F}$, the closure of F, at least once;

(ii) Each orbit $G(z), z \in \mathcal{U}$, meets F at most once.

Obviously (i) and (ii) imply that

$$\mathcal{U} = \bigcup_{g \in G} g(\bar{F}), \tag{1.1}$$

and that

$$g(F) \cap F = \emptyset \;\; if \;\; I \neq g \in G. \tag{1.2}$$

Let us begin with the modular group Γ. A fundamental region for Γ is given by

$$F = \left\{ z \in \mathcal{U} : |\, z \,| > 1, |\, Re\; z \,| < \frac{1}{2} \right\}. \tag{1.3}$$

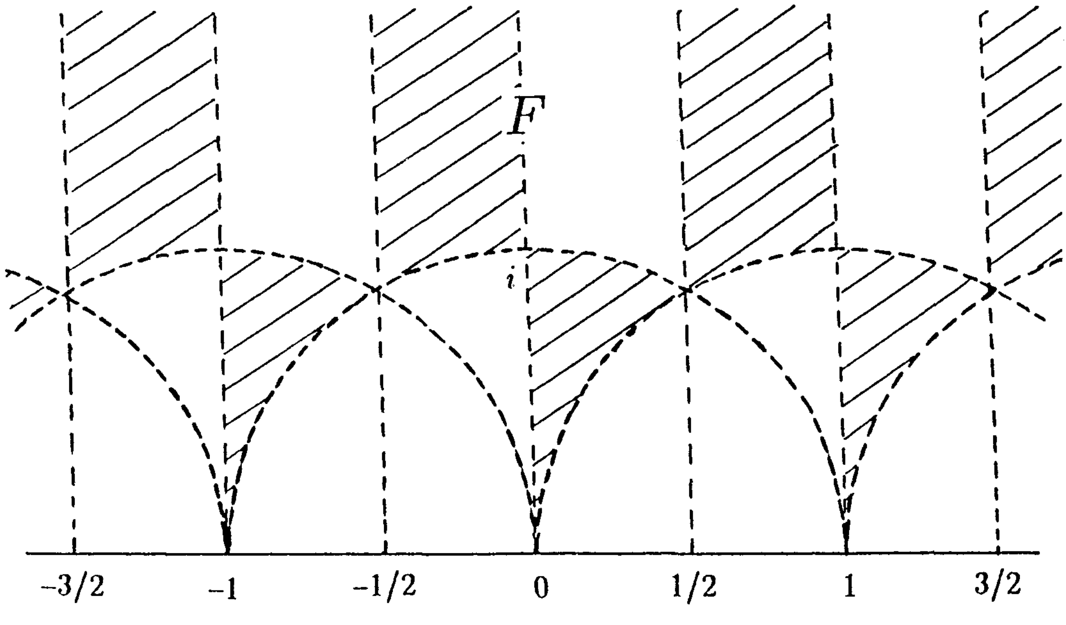


Figure 1.1. A fundamental region for the modular group

This region is determined in many books, e.g. [Ra,2], [Fo,1]. See Figure 1.1. It has three vertices in the upper half plane two of which are the fixed points of two elliptic generators and the third one is the infinity which is the unique parabolic point in this region.

Let us now discuss the situation in general for the other Hecke groups. (Of course this discussion includes Γ as well). E. Hecke, when investigating the discreteness of Hecke groups H(λ), gave the following result (see [He,1]):

Theorem 1.1: When $\lambda \geq 2$ and real, or when $\lambda = \lambda_q = 2cos\pi/q$, $q \in \mathbf{N}$, q $\geq$ 3, the set

$$F_\lambda = \{z \in \mathcal{U} : |\, Re\ z\,| < \lambda/2, |\, z\,| > 1\} \tag{1.4}$$

is a fundamental region for the group H(λ), and also F_λ fails to be a fundamental region for all other $\lambda > 0$.

R. Evans gave an elementary proof of this fact in [Ev,1].

We therefore take a fundamental region for H(λ_q) as

$$F_{\lambda_q} = \left\{z \in \mathcal{U} : |\, Re\ z\,| < \frac{\lambda_q}{2},\ |\, z\,| > 1\right\}. \tag{1.5}$$

It is well-known that fundamental region of a group is not unique. We have already seen that $F_{\lambda_q} = F_1 \cup F_2$ in Figure 1.2 is a fundamental region for H(λ_q). Actually a shaded region together with an unshaded one form a fundamental region for H(λ_q). Therefore sometimes, for convenience, we shall take it as

$$F'_{\lambda_q} = \left\{ z \in \mathcal{U} : -\frac{\lambda_q}{2} < Re\ z < 0, \left| z + \frac{1}{\lambda_q} \right| > \frac{1}{\lambda_q} \right\}. \tag{1.6}$$

which is $F_1 \cup RF_2$.

The elliptic generator S has order q so that the q transforms of $F'_{\lambda_q} = F_1 \cup RF_2$ form a pattern around the center point $-\overline{\zeta} = -e^{-i\pi/q}$ which is the fixed point of S. In another words the transforms of F_1 and RF_2 under S form a pattern alternately.

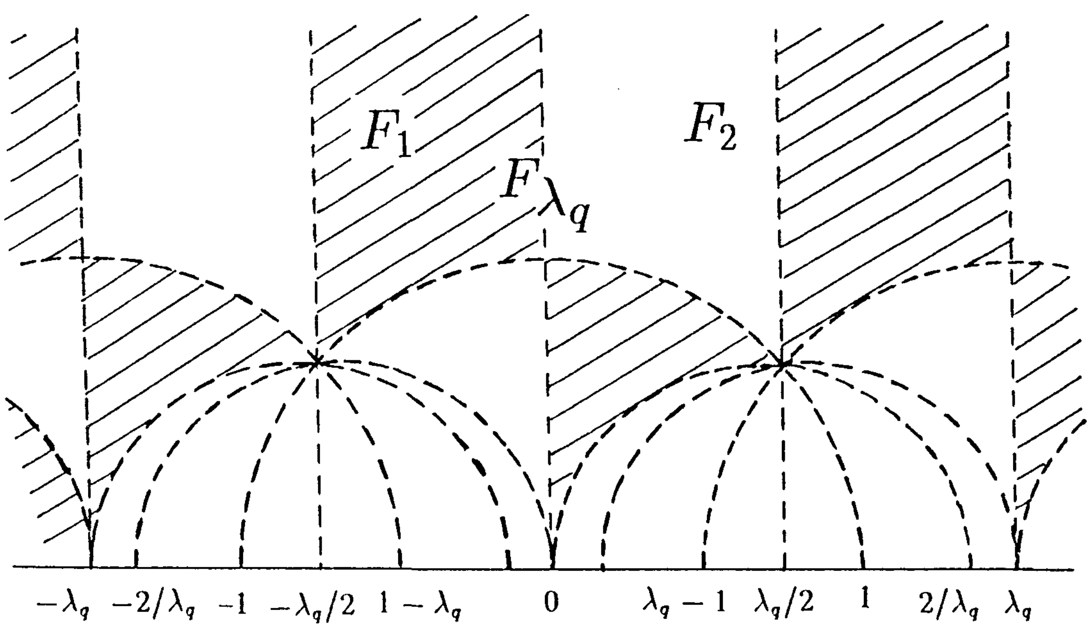


Figure 1.2. A shaded and a white region together form a fundamental region for $\mathrm{H}(\lambda_q)$

1.2. DETERMINATION OF THE IMAGES OF VERTICES OF F'_{λ_q} AND PARABOLIC POINTS OF HECKE GROUPS

In this section we first try to find formulae giving the images of the vertices of F'_{λ_q} under the subgroup $< S >$. We already know that a fundamental region for $\mathrm{H}(\lambda_q)$

has three vertices and that one of those is a parabolic point. We are specially interested in the parabolic points as the determination of them is still an open question on Hecke groups. These images will also be used in proving the group theoretical structure of Hecke groups later on in this chapter.

Let us now find the images of the vertices of F'_{λ_q} under the group $< S >$. It is sufficient to find the images of the vertices of F_2, since they coincide, in another order, with the ones of F'_{λ_q}.

The region F_2 has vertices i, $-\overline{\zeta}$ and ∞ in the compactified upper half plane $\hat{\mathcal{U}} = \mathcal{U} \cup \{\infty\}$. Being the fixed point of S, $-\overline{\zeta}$ is a vertex of every transform of F_2 under the group $< S >$. Therefore we only need to calculate the images of i and ∞. The latter ones will be real or ∞ and called *cusp* (or *parabolic*) *points* and are of great interest. They will be dealt with later on in this chapter.

After easy calculations we find the required images as follows:

$$\begin{array}{lccc}
F_1 & : & i & \infty \\
SF_1 & : & \frac{-\lambda+i}{\lambda^2+1} & 0 \\
S^2F_1 & : & \frac{-\lambda.\lambda^2+i}{\lambda^4-\lambda^2+1} & -\frac{1}{\lambda} \\
S^3F_1 & : & \frac{-\lambda(\lambda^2-1)^2+i}{\lambda^6-3\lambda^4+2\lambda^2+1} & -\frac{\lambda}{\lambda^2-1} \\
S^4F_1 & : & \frac{-\lambda(\lambda^3-2\lambda)^2+i}{\lambda^8-5\lambda^6+7\lambda^4-2\lambda^2+1} & -\frac{\lambda^2-1}{\lambda^3-2\lambda} \\
S^5F_1 & : & \frac{-\lambda(\lambda^4-3\lambda^2+1)^2+i}{\lambda^{10}-7\lambda^8+16\lambda^6-13\lambda^4+3\lambda^2+1} & -\frac{\lambda^3-2\lambda}{\lambda^4-3\lambda^2+1} \\
S^6F_1 & : & \frac{-\lambda(\lambda^5-4\lambda^3+3\lambda)^2+i}{\lambda^{12}-9\lambda^{10}+29\lambda^8-40\lambda^6+22\lambda^4-3\lambda^2+1} & -\frac{\lambda^4-3\lambda^2+1}{\lambda^5-4\lambda^3+3\lambda}
\end{array} \qquad (1.7)$$

and in general

$$S^n(i) = -\frac{|\lambda.\alpha^2_{n-1}(\lambda) - i|^2}{|\lambda.\alpha^2_{n-2}(\lambda) - i|^2}.\frac{\lambda.\alpha^2_n(\lambda) - i}{|\lambda.\alpha^2_n(\lambda) - i|^2} \tag{1.8}$$

and

$$S^n(\infty) = -\frac{\alpha_{n-1}(\lambda)}{\alpha_n(\lambda)}, \tag{1.9}$$

where, for $1 \leq n \leq q-1$, α_n's are the polynomials given by the reduction formulae

$$\begin{aligned} \alpha_{-1}(\lambda) &= \alpha_0(\lambda) = 0 \\ \alpha_1(\lambda) &= 1 \\ \alpha_n(\lambda) &= \lambda.\alpha_{n-1}(\lambda) - \alpha_{n-2}(\lambda) \quad ; \; n \geq 2. \end{aligned} \tag{1.10}$$

It is clear that

$$\begin{aligned} \alpha_2(\lambda) &= \lambda \\ \alpha_3(\lambda) &= \lambda^2 - 1 \\ \alpha_4(\lambda) &= \lambda^3 - 2\lambda \\ \alpha_5(\lambda) &= \lambda^4 - 3\lambda^2 + 1 \\ \alpha_6(\lambda) &= \lambda^5 - 4\lambda^3 + 3\lambda. \end{aligned} \tag{1.11}$$

Also $deg\ \alpha_n(\lambda) = n-1$, and α_n is not always irreducible.

We now discuss an open problem on Hecke groups which is the determination of all parabolic (cusp) points of H(λ_q), i.e. determination of the " *cuspset* " S_q of

$\mathrm{H}(\lambda_q)$ given by

$$S_q := \left\{ \frac{a}{c} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H(\lambda_q) \right\}, \tag{1.12}$$

which is the orbit of ∞ on $\mathbf{R} \cup \{\infty\}$. There are several results answering this problem for particular values of q. Before recalling them, we discuss this problem for the four important Hecke groups:

To find the parabolic points of any particular Hecke group, one needs to know the form of the elements of this Hecke group. This is because all parabolic points, being images of infinity under group elements, are quotients of the first and third coefficients of the elements of $\mathrm{H}(\lambda_q)$.

We have seen in earlier chapters that the most interesting and important Hecke group is the modular group $\Gamma = \mathrm{H}(\lambda_3)$. We determined the underlying field for this group as $\mathbf{Q}$. Therefore all coefficients of the elements of Γ are rational integers. This implies that the parabolic points of Γ are just rational numbers and S_3 is equal to $\mathbf{Q} \cup \infty$.

Next two interesting Hecke groups are obtained for $q = 4$ and 6. For these two groups the underlying fields were found as $\mathbf{Q}(\sqrt{2})$ and $\mathbf{Q}(\sqrt{3})$. Recall that the elements of $\mathrm{H}(\sqrt{m})$, $m = 2$ or 3, have been classified as odd and even ones in the Introduction. An easy calculation shows that the parabolic points of these two groups are of the form $\frac{a\sqrt{m}}{b}$ for integers a and b. This implies that the cuspset S_{2m} is a subset of $\mathbf{Q}(\sqrt{\mathrm{m}})$ consisting of $\frac{a\sqrt{m}}{b}$ with $a, b \in \mathbf{Z}$, and of ∞.

Another interesing Hecke group is $\mathrm{H}(\lambda_5)$. Because of the identity

$$\lambda_5^2 = \lambda_5 + 1, \tag{1.13}$$

the underlying field is again $\mathbf{Q}(\lambda_5)$. Rosen, in [Ro,3], showed that the parabolic points, as finite λ–fractions, are the quotients of integers in the field $\mathbf{Q}(\lambda)$. A typical one is denoted by a/b where $a = a_1 + a_2\lambda$ and $b = b_1 + b_2\lambda$. Rosen also showed that, in this case, the units λ^m are all parabolic points. Wolfart, [Wo,1], proved that the only possible values of q such that all the elements of the field $\mathbf{Q}(\lambda)$ are cusps are 3 and 5.

We can now recall some other results concerning the parabolic points of Hecke groups in general. One of the most significant results on this topic was proven by Leutbecher [Le,2]: If $q = 3, 4, 5, 6, 8, 10$ or 12 then

$$S_q = \lambda_q.\mathbf{Q}(\lambda_q^2) \cup \{\infty\}. \tag{1.14}$$

Borho and Rosenberger [Bo–Ro,1] proved that, for odd q, (1.14) is only valid when $q = 2^n + 1$. On the other hand it can only be true when the field $\mathbf{Q}(\lambda_q^2)$ has class number 1.

Let us now denote, by Λ, the ring of algebraic integers in $\mathbf{Q}(\lambda_q)$ and let

$$\Lambda_1 = \Lambda \cap \mathbf{Q}(\lambda_q^2). \tag{1.15}$$

We have seen that every $M \in \mathrm{H}(\lambda_q)$ can be written as $\begin{pmatrix} a\lambda_q & b \\ c & d\lambda_q \end{pmatrix}$ or as $\begin{pmatrix} a & b\lambda_q \\ c\lambda_q & d \end{pmatrix}$ with $a, b, c, d \in \mathbf{Z}[\lambda_q^2] \subseteq \Lambda_1$, and it is certain that

$$S_q \subseteq \lambda_q.\mathbf{Q}(\lambda_q^2)^{\mathrm{o}} \cup \{\infty\}, \tag{1.16}$$

where $\mathbf{Q}(\lambda_q^2)^o$ denotes the subset of $\mathbf{Q}(\lambda_q^2)$, whose elements are either $a\lambda_q/c$ or $a/c\lambda_q$ with $a, c \in \Lambda_1$, $(a\lambda_q, c) = 1$ and $(a, c\lambda_q) = 1$ in Λ, respectively.

By means of Borho and Rosenberger's method, Wolfart, [Wo,1], proved that (1.14) can be written in an extended form by adding the cases $q = 9, 18, 20$ and 24:

Theorem 1.2: If the cuspset S_q of the Hecke group $H(\lambda_q)$ has the form

$$S_q = \lambda_q.\mathbf{Q}(\lambda_q^2)^o \cup \{\infty\} \tag{1.17}$$

then necessarily $q = 3, 4, 5, 6, 8, 9, 10, 12, 18, 20$ or 24.

By (1.9) we have an infinite class of parabolic points in general for any Hecke group $H(\lambda_q)$. In fact applying R to this class gives another class of parabolic points given by

$$RS^n(\infty) = \frac{\alpha_n(\lambda)}{\alpha_{n-1}(\lambda)}. \tag{1.18}$$

The other parabolic points are the transforms of those already found, under the elements of $H(\lambda_q)$. Therefore the polynomials $\alpha_n(\lambda)$ play a very important role in determining the parabolic points of $H(\lambda_q)$.

1.3. $\mathbf{H}(\lambda_q) \cong C_2 \star C_q$

We have already mentioned that $\mathrm{H}(\lambda_q)$ is isomorphic to the free product of two finite cyclic groups of order 2 and order q. We now give an elementary proof of this fact using a result of Macbeath, [Ma, 2]. First we have:

Definition 1.2: Let $[G, X]$ be a topological transformation group and let $P \subseteq X$. If for $g_1, g_2 \in G$, $g_1 \neq g_2$, $g_1 P \cap g_2 P = \emptyset$, then P is called a *G-packing.*

Equivalently, if for $1 \neq g \in G$, $gP \cap P = \emptyset$ then P is a *G-packing.*

If P is a G-packing, then it contains at most one element from each orbit.

Theorem 1.3: The Hecke group $\mathrm{H}(\lambda_q)$, $q \geq 3$, $q \in \mathbb{N}$, is isomorphic to the free product of two finite cyclic groups of orders 2 and q; i.e.

$$H(\lambda_q) \cong C_2 \star C_q. \tag{1.19}$$

The proof of Theorem 1.3 depends on the following lemma:

Lemma 1.1: Let H and K be two subgroups of a transformation group $[G, X]$. If P is an H–packing, Q is a K–packing, $A =< H, K >$– the group generated by the generators of H and K– and $P \cup Q = X$, $P \cap Q \neq \emptyset$, then

$$A = H \star K. \tag{1.20}$$

Also $P \cap Q$ is an A–packing.

Proof: See [Ma,2].

We are now in a position to prove Theorem 1.3. Let $H = < R > \cong C_2$ and $K = < S > \cong C_q$. Then H and K are subgroups of $\mathrm{H}(\lambda_q)$. Let us now try to find packings P and Q for H and K, respectively, such that the conditions of Lemma 1.1 are satisfied:

Since $R(z) = -1/z = -\overline{z}/|z|^2$, it is clear that

$$Sign\ (Re\ R(z)) = -Sign\ (Re\ z)\,, \tag{1.21}$$

and that the set

$$P = \{z \in \mathcal{U} : Re\ z < 0\} \tag{1.22}$$

is an H-packing. Now consider the set

$$Q = \left\{z \in \mathcal{U} : Re\ z > -\frac{\lambda_q}{2}, \left|z + \frac{1}{\lambda_q}\right| > \frac{1}{\lambda_q}\right\}. \tag{1.23}$$

The elliptic element $S(z) = -1/(z + \lambda_q)$ can be expressed as a composition of simpler mappings as follows:

(i) $T_1(z) = \frac{z}{|z|^2} = \frac{1}{\overline{z}}$, reflection in the unit circle,

(ii) $T_2(z) = -\overline{z}$, reflection in the line $Re\ z = 0$,

(iii) $T(z) = z + \lambda_q$, translation through λ_q.

Then obviously $S(z) = T_1T_2T(z)$.

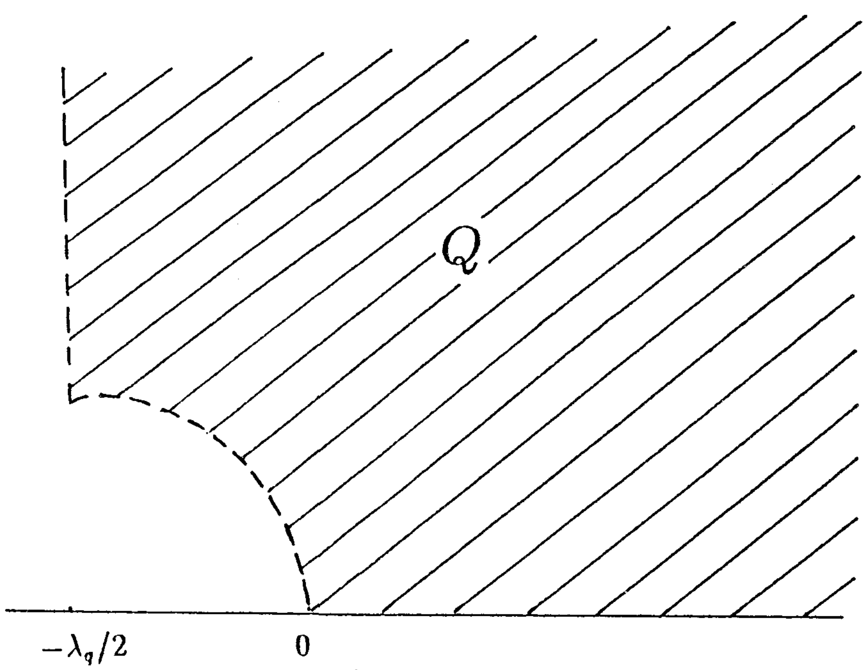


Figure 1.3. The region Q

Q has the vertices ζ, 0 and ∞. Now applying T to Q we obtain a translation of Q with vertices $\zeta + \lambda_q$, λ_q and ∞. Applying T_2 to TQ we obtain a reflection of TQ with vertices ζ, $-\lambda_q$ and ∞. Finally applying T_1 to T_2TQ we obtain a reflection of T_2TQ which is SQ with vertices ζ, $-1/\lambda_q$ and 0.

If we apply T, T_2 and T_1 respectively, this time, to SQ, the final region we obtain will be S^2Q with the vertices ζ, $\lambda_q/(1 - \lambda_q^2)$ and $-1/\lambda_q$. Repeating this process another $q - 3$ times, we obtain the regions S^3Q, S^4Q, ..., $S^{q-1}Q$. Since they do not overlap each other, Q is a K-packing.

We have already found the vertices of the transforms of Q under the group $< S >$ in (1.8) and in (1.9). Of course one of the vertices, ζ, is the fixed point under this group. Therefore the transform S^nQ, $1 \leq n \leq q-1$, will have vertices ζ, $S^n(\infty)$ and $S^{n+1}(\infty)$.

Since we now have an H-packing and a K-packing we can apply Lemma 1.1. Then the group $\mathrm{H}(\lambda_q) =< H, K >$ is isomorphic to the free product of its subgroups H and K, i.e. $\mathrm{H}(\lambda_q) \cong C_2 \star C_q$. Also

$$\begin{aligned} P \cap Q &= \left\{ z \in \mathcal{U} : -\tfrac{\lambda_q}{2} < Re\ z < 0 \,, \left| z + \tfrac{1}{\lambda_q} \right| > \tfrac{1}{\lambda_q} \right\} \\ &= F'_{\lambda_q} \end{aligned} \tag{1.24}$$

is an $\mathrm{H}(\lambda_q)$-packing.

Chapter 2

THE MINIMAL POLYNOMIAL OF λ_q

2.0. INTRODUCTION

For the first four Hecke groups Γ, $H(\sqrt{2})$, $H(\lambda_5)$ and $H(\sqrt{3})$, we can find the minimal polynomial of λ_q over $\mathbf{Q}$ as $\lambda_3 - 1$, $\lambda_4^2 - 2$, $\lambda_5^2 - \lambda_5 - 1$ and $\lambda_6^2 - 3$, respectively. However, for $q \geq 7$, the algebraic number $\lambda_q = 2cos\pi/q$ is a root of a minimal polynomial of degree ≥ 3. Therefore it is not possible to determine λ_q for $q \geq 7$ as nicely as in the first four cases. For this reason we shall be interested in the minimal polynomial of λ_q instead of λ_q itself.

In Chapter 7, we shall discuss important kind of normal subgroups, the principal congruence subgroups, of $H(\lambda_q)$. Using results given in [Ma,1], we shall find quotients of $H(\lambda_q)$ by these subgroups. There, we will need to know whether the minimal polynomial of λ_q is congruent to 0 *modulo* p, for prime p. Therefore we will need to know the constant term of it *modulo* p. Here we will determine the values of p and q satisfying this condition.

In this chapter we prove, using some results from Galois theory given in Chapter 0, that the degree of the minimal polynomial of λ_q is $\varphi(2q)/2$ where φ denotes the

Euler function. Then we find formulae for the minimal polynomial in odd and even q cases. This will be done using the Chebycheff polynomials and [Bn,1]. Our final problem in this chapter is the determination of the constant term of these minimal polynomials. This will also be done separetely for odd and even q. We shall see that both problems are easier to solve when q is odd.

In Appendix 1, we give lists of all polynomials we use here to calculate the minimal polynomial, and also list of the minimal polynomials of λ_q for $q \leq 50$.

Let us begin by recalling the Chebycheff polynomials:

For $n \in \mathbf{N}$, the n–th Chebycheff polynomial $T_n(x)$ is defined by

$$T_n(x) := cos(ncos^{-1}x), \quad x, \Theta \in \mathbf{R}, |\mathrm{x}| \leq 1, \tag{2.1}$$

or

$$T_n(cos\Theta) := cos(n\Theta), \quad \Theta \in \mathbf{R}. \tag{2.2}$$

We drop the conditions on Θ and x as they always apply.

The first few T_n's are

$$\begin{array}{lcl} T_0(x) & = & 1 \\ T_1(x) & = & x \\ T_2(x) & = & 2x^2 - 1 \\ T_3(x) & = & 4x^3 - 3x \\ T_4(x) & = & 8x^4 - 8x^2 + 1. \end{array} \tag{2.3}$$

We have the following well–known recurrence formula for T_n:

Lemma 2.1: Let $n \in \mathbf{N}$. Then

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x). \tag{2.4}$$

Here we shall also use a normalization of the Chebycheff polynomials, denoted by A_n. This normalization is given by

$$\begin{aligned} A_n(x) &= 2T_n(x/2) \\ &= 2cos(ncos^{-1}(x/2)) \\ &= 2cosn\Theta \end{aligned} \tag{2.5}$$

where $x = A_1(x) = 2cos\Theta,\ x, \Theta \in \mathbf{R},\ |x| \leq 2,\ n \in \mathbf{N}$.

For our purposes, we take $\Theta = \pi/q$, $q \in \mathbf{N}$, $q \geq 3$. Then $x = \lambda_q$ and $A_n(x)$ is a polynomial of λ_q. In fact

$$A_n(\lambda_q) = 2cos\frac{n\pi}{q} = \zeta^n + \zeta^{-n}. \tag{2.6}$$

where $\zeta = e^{i\pi/q}$.

A_n's are given explicitly by H. Weber in [We,1] as

$$\begin{aligned} A_n(x) &:= \sum_{i=0}^{[n/2]}(-1)^i\frac{n}{n-i}\binom{n-i}{i}x^{n-2i} \\ &= x^n - nx^{n-2} + \frac{n(n-3)}{2!}x^{n-4} - \frac{n(n-4)(n-5)}{3!}x^{n-6} + \ldots \end{aligned} \tag{2.7}$$

where $[\alpha]$ denotes the greatest integer less than or equal to α. Therefore

$$deg(A_n(x)) = n. \tag{2.8}$$

We have the following recurrence formulae for A_n :

Lemma 2.2: Let $n \in \mathbf{N}$. Then

$$A_2(x) = xA_1(x) - 2A_0(x), \tag{2.9}$$

$$A_{n+1}(x) = xA_n(x) - A_{n-1}(x), \quad n > 1, \tag{2.10}$$

where, for consistency, we put $A_0(x) = 1$.

Hence the first few A_n's are

$$\begin{aligned} A_1(x) &= x \\ A_2(x) &= x^2 - 2 \\ A_3(x) &= x^3 - 3x \\ A_4(x) &= x^4 - 4x^2 + 2 \\ A_5(x) &= x^5 - 5x^3 + 5x. \end{aligned} \tag{2.11}$$

Then the inverse relations, giving powers of x in terms of A_n's, are

$$\begin{aligned} 1 &= A_0(x) \\ x &= A_1(x) \\ x^2 &= A_2(x) + 2A_0(x) \\ x^3 &= A_3(x) + 3A_1(x) \\ x^4 &= A_4(x) + 4A_2(x) + 6A_0(x) \\ x^5 &= A_5(x) + 5A_3(x) + 10A_1(x) \\ x^6 &= A_6(x) + 6A_4(x) + 15A_2(x) + 20A_0(x) \end{aligned} \tag{2.12}$$

and in general

$$x^n = \sum_{k=0}^{[n/2]} \binom{n}{k} A_{n-2k}. \tag{2.13}$$

It is easy to see that

$$\begin{aligned} A_{2n} &= A_n^2 - 2 &&= A_2 o A_n, \\ A_{3n} &= A_n^3 - 3A_n &&= A_3 o A_n, \\ &\ldots\ldots\ldots\ldots \\ A_{kn} &= A_k o A_n &&, \quad k, n \geq 1, \end{aligned} \tag{2.14}$$

and in general

$$A_{m_1 \ldots m_n} = A_{m_1} o(A_{m_2} o(\ldots o(A_{m_n}))) \tag{2.15}$$

where $m_i \geq 1$, $(1 \leq i \leq n)$. Also

$$A_n o A_k = A_k o A_n \tag{2.16}$$

and

$$A_m o(A_n o A_k) = (A_m o A_n) o A_k \tag{2.17}$$

for every $m, n, k \geq 1$. Furthermore

$$A_1 o A_k = A_k o A_1 = A_k \tag{2.18}$$

for each $k \geq 1$. Hence we have

Theorem 2.1: The set of A_n's, $n \geq 1$, forms a commutative semigroup with the unit element A_1 under the composition of functions.

2.1. THE DEGREE OF THE MINIMAL POLYNOMIAL OF λ_q

NOTATION: We denote the minimal polynomial of λ_q by P_q^*.

We now want to determine the degree of P_q^*. Let

$$\zeta' = e^{2\pi i/n} = cos(2\pi/n) + isin(2\pi/n). \tag{2.19}$$

Then

$$\zeta' + \frac{1}{\zeta'} = 2cos(2\pi/n). \tag{2.20}$$

Now let $\mathbf{K}$ be the splitting field of $x^n - 1$ over $\mathbf{Q}$. Then by Theorem 0.2,

$$[\mathbf{K} : \mathbf{Q}] = \varphi(\mathrm{n}). \tag{2.21}$$

If $\sigma \in G(\mathbf{K}/\mathbf{Q})$ and $\sigma(\zeta') = \zeta'^r$, then

$$\sigma\left(\zeta' + \frac{1}{\zeta'}\right) = \zeta'^r + \frac{1}{\zeta'^r} = 2cos\frac{2\pi r}{n}. \tag{2.22}$$

But for $1 < r < n$, we have $2cos(2\pi r/n) = 2cos(2\pi/n)$ only when $r = n - 1$. Thus the only elements of $G(\mathbf{K}/\mathbf{Q})$ fixing $\zeta' + \frac{1}{\zeta'}$ are the identity automorphism and the automorphism τ with

$$\tau(\zeta') = \zeta'^{n-1} = \frac{1}{\zeta'}. \tag{2.23}$$

This shows that the subgroup of $G(\mathbf{K}/\mathbf{Q})$ leaving $\mathbf{Q}(\zeta' + \frac{1}{\zeta'})$ fixed is of order two, so by Galois theory

$$[\mathbf{Q}(\zeta' + \frac{1}{\zeta'}) \,:\, \mathbf{Q}] = \frac{\varphi(\mathrm{n})}{2}. \tag{2.24}$$

Suppose that n is even and put $q = n/2$. Then

$$\zeta + \frac{1}{\zeta} = 2cos\pi/q = \lambda_q, \tag{2.25}$$

and hence by (2.24)

$$\left[\mathbf{Q}(\zeta + \frac{1}{\zeta}) \,:\, \mathbf{Q}\right] = \frac{\varphi(2q)}{2}, \tag{2.26}$$

i.e.

$$[\mathbf{Q}(\lambda_{\mathrm{q}}) \,:\, \mathbf{Q}] = \frac{\varphi(2\mathrm{q})}{2}. \tag{2.27}$$

Hence we have the following result:

Theorem 2.2: Let φ denote the Euler function. Then

$$deg\ P_q^* = \frac{\varphi(2q)}{2}. \tag{2.28}$$

Corollary 2.1: We have

$$deg\ P_q^* = \begin{cases} \varphi(q)/2 & \text{if } q \text{ is odd,} \\ \varphi(q) & \text{if } q \text{ is even.} \end{cases} \tag{2.29}$$

Proof: Let first q be odd. Then

$$\begin{aligned} deg\ P_q^* &= \frac{\varphi(2q)}{2} \\ &= \frac{\varphi(2).\varphi(q)}{2} \\ &= \frac{\varphi(q)}{2}. \end{aligned}$$

Let secondly $q \geq 4$ be even. Then q can be written as

$$q = 2^m.k \tag{2.30}$$

where k is an odd number. Now

$$\begin{aligned} deg\ P_q^* &= \frac{\varphi(2q)}{2} \\ &= \frac{\varphi(2^{m+1}).\varphi(k)}{2} \\ &= 2^{m-1}.\varphi(k) \\ &= \varphi(2^m).\varphi(k) \\ &= \varphi(q). \end{aligned}$$

2.2. THE MINIMAL POLYNOMIAL OF λ_q

In this section we give formulae for P_q^* in odd and even q cases. We use a formula given in [Bn,1].

NOTATION: Let $\psi_{2q}(x)$ denote the minimal polynomial of $x = cos\pi/q$ over $\mathbf{Q}$.

Then $\psi_{2q}(x)$ is of degree $\varphi(2q)/2$ by Theorem 2.2.

As the minimal polynomials are monic we have the relation

$$P_q^*(x) = 2^{\varphi(2q)/2}.\psi_{2q}(x/2) \tag{2.31}$$

between the two minimal polynomials.

We now want to find the minimal polynomial $P_q^*(x)$ of λ_q in the light of this information.

First let q be odd. Then by [Bn,1]

$$T_{q+1}(x) - T_{q-1}(x) = 2^q \prod_{d|2q} \psi_d(x) \tag{2.32}$$

as $2q$ is even and

$$T_{\frac{q+1}{2}}(x) - T_{\frac{q-1}{2}}(x) = 2^{\frac{q-1}{2}} \prod_{d|q} \psi_d(x) \tag{2.33}$$

as q is odd. These can easily be proved by showing that both sides of each of them have the same leading coeefficients, same degrees and same roots. Hence

$$\frac{T_{q+1}(x) - T_{q-1}(x)}{T_{\frac{q+1}{2}}(x) - T_{\frac{q-1}{2}}(x)} = 2^{\frac{q+1}{2}} \prod_{\substack{d|2q \\ d \neq 2q \\ d\ even}} \psi_d(x).\psi_{2q}(x). \tag{2.34}$$

Therefore

$$\psi_{2q}(x) = \frac{1}{2^{\frac{q+1}{2}}}.\frac{T_{q+1}(x) - T_{q-1}(x)}{\prod_{\substack{d|2q \\ d \neq 2q \\ d\ even}} \psi_d(x).(T_{\frac{q+1}{2}}(x) - T_{\frac{q-1}{2}}(x))}. \tag{2.35}$$

Now by (2.31)

$$P_q^*(x) = 2^{\frac{\varphi(2q)}{2} - \frac{q+1}{2}}.\frac{T_{q+1}(x/2) - T_{q-1}(x/2)}{\prod_{\substack{d|2q \\ d \neq 2q \\ d\ even}} \psi_d(x/2).(T_{\frac{q+1}{2}}(x/2) - T_{\frac{q-1}{2}}(x/2))}. \tag{2.36}$$

Finally using (2.5), we obtain the minimal polynomial of λ_q, for odd q, as

$$P_q^*(x) = 2^{\frac{\varphi(q)-q-1}{2}}.\frac{A_{q+1}(x) - A_{q-1}(x)}{\prod_{\substack{d|2q \\ d \neq 2q \\ d\ even}} \psi_d(x/2).(A_{\frac{q+1}{2}}(x) - A_{\frac{q-1}{2}}(x))}. \tag{2.37}$$

With a little more effort we can reduce this equation to a simpler form. Recall that, by (2.14)

$$A_{q+1}(x) = A^2_{\frac{q+1}{2}} - 2 \tag{2.38}$$

and similarly

$$A_{q-1}(x) = A^2_{\frac{q-1}{2}} - 2. \tag{2.39}$$

Therefore

$$\begin{aligned} A_{q+1}(x) - A_{q-1}(x) &= A^2_{\frac{q+1}{2}} - 2 - A^2_{\frac{q-1}{2}} + 2 \\ &= A^2_{\frac{q+1}{2}} - A^2_{\frac{q-1}{2}}. \end{aligned} \tag{2.40}$$

Then

$$\frac{A_{q+1}(x) - A_{q-1}(x)}{A_{\frac{q+1}{2}}(x) - A_{\frac{q-1}{2}}(x)} = A_{\frac{q+1}{2}}(x) - A_{\frac{q-1}{2}}(x). \tag{2.41}$$

Hence we have

Theorem 2.3: Let q be odd. Then the minimal polynomial $P_q^*(x)$ of λ_q is given by

$$P_q^*(x) = 2^{\frac{\varphi(q)-q-1}{2}} . \frac{A_{\frac{q+1}{2}}(x) + A_{\frac{q-1}{2}}(x)}{\prod_{\substack{d|2q \\ d \neq 2q \\ d\ even}} \psi_d(x/2)}. \tag{2.42}$$

Example 2.1: **(i)** Let $q = 3$. Then by (2.42) we have

$$\begin{aligned} P_3^*(x) &= 2^{-1}.\frac{A_2(x) + A_1(x)}{\psi_2(x/2)} \\ &= x - 1. \end{aligned} \tag{2.43}$$

(ii) Let $q = 9$. Then similarly

$$\begin{aligned} P_9^*(x) &= 2^{-2}.\frac{A_5(x) + A_4(x)}{\psi_2(x/2).\psi_6(x/2)} \\ &= x^3 - 3x - 1. \end{aligned} \tag{2.44}$$

Secondly let q be even. Again by [Bn,1], we have

$$T_{q+1}(x) - T_{q-1}(x) = 2^q \prod_{d|2q} \psi_d(x) \tag{2.45}$$

as $2q$ is even and

$$T_{\frac{q}{2}+1}(x) - T_{\frac{q}{2}-1}(x) = 2^{\frac{q}{2}} \prod_{d|q} \psi_d(x) \tag{2.46}$$

as q is even. Then

$$\frac{T_{q+1}(x) - T_{q-1}(x)}{T_{\frac{q}{2}+1}(x) - T_{\frac{q}{2}-1}(x)} = 2^{\frac{q}{2}}.\frac{\prod_{d|2q} \psi_d(x)}{\prod_{d|q} \psi_d(x)}. \tag{2.47}$$

Therefore

$$\psi_{2q}(x) = \frac{1}{2^{\frac{q}{2}}}.\frac{T_{q+1}(x) - T_{q-1}(x)}{T_{\frac{q}{2}+1}(x) - T_{\frac{q}{2}-1}(x))}.\frac{\prod_{d|q} \psi_d(x)}{\prod_{\substack{d|2q \\ d \neq 2q}} \psi_d(x)}. \tag{2.48}$$

Proceeding similarly to the case of odd q, we get

Theorem 2.4: Let q be even. Then the minimal polynomial $P_q^*(x)$ of λ_q is given by

$$P_q^*(x) = 2^{\frac{\varphi(2q)-q}{2}}.\frac{A_{q+1}(x) - A_{q-1}(x)}{\prod_{\substack{d|2q \\ d \neq 2q \\ d \not| q}} \psi_d(x/2).(A_{\frac{q}{2}+1}(x) - A_{\frac{q}{2}-1}(x))}. \tag{2.49}$$

Conjecture: If $q = 2^{\alpha_0}.k$, $k \in \mathbf{N}$, odd, then

$$P_q^*(x) = 2^{\frac{\varphi(2q)-q}{2}}.\frac{A_{q+1}(x) - A_{q-1}(x)}{\prod_{d|k} \psi_{2^{\alpha_0}.d}(x/2).(A_{\frac{q}{2}+1}(x) - A_{\frac{q}{2}-1}(x))}. \tag{2.50}$$

Corollary 2.2:

$$P_{2^n}^*(x) = \frac{A_{2^n+1}(x) - A_{2^n-1}(x)}{A_{2^{n-1}+1}(x) - A_{2^{n-1}-1}(x)}. \tag{2.51}$$

Corollary 2.3:

$$P_{2p^n}^*(x) = 2^{-p^{n-1}}.\frac{A_{2p^n+1}(x) - A_{2p^n-1}(x)}{\prod_{k=0}^{n-1} \psi_{4p^k}(x/2)(A_{p^n+1}(x) - A_{p^n-1}(x))}. \tag{2.52}$$

We now find the roots of the minimal polynomial $P_q^*(x)$:

Theorem 2.5: The roots of $P_q^*(x)$ are $2cos\frac{h\pi}{q}$ with $(h,q) = 1$, h odd and $1 \leq h \leq q-1$.

Proof: Let $n = 2q$. We proved that $P_q^*(x)$ has $\varphi(n)/2$ roots. Let $h \in \mathbf{N}$ such that $(h,n) = 1$ and let σ be an automorphism of $\mathbf{Q}(\zeta)$ over $\mathbf{Q}$ such that

$$\sigma(\zeta) = \zeta^h, \tag{2.53}$$

where ζ is the primitive n–th root of unity, i.e. $\zeta = cos\frac{2\pi}{n} + i.sin\frac{2\pi}{n}$. Then

$$\begin{aligned} \sigma(2cos\tfrac{2\pi}{n}) &= \sigma(cos\tfrac{2\pi}{n} + i.sin\tfrac{2\pi}{n} + cos\tfrac{2\pi}{n} - i.sin\tfrac{2\pi}{n}) \\ &= \sigma(\zeta) + \sigma(\zeta)^{-1} \\ &= \zeta^h + \zeta^{-h} \\ &= 2cos\tfrac{2\pi h}{n} \end{aligned} \tag{2.54}$$

Therefore

$$\begin{aligned} P_q^*(2cos\tfrac{2\pi h}{n}) &= P_q^*(\sigma(2cos\tfrac{2\pi}{n})) \\ &= \sigma(P_q^*(2cos\tfrac{2\pi}{n})) \\ &= \sigma(0) \\ &= 0 \end{aligned} \tag{2.55}$$

since $2cos\frac{2\pi}{n} = \lambda_q$ is a root of $P_q^*(x) = 0$ over $\mathbf{Q}$. So $2cos\frac{2\pi h}{n}$ is a root of $P_q^*(x) = 0$ over $\mathbf{Q}$.

Now the values of $2cos\frac{2\pi h}{n}$ are distinct for $h \in \mathbf{N}$ such that $(h,n) = 1$ and $h \leq q$, since

$$0 \leq \frac{2\pi}{n} \leq \frac{2\pi h}{n} \leq \frac{2\pi q}{n} = \frac{2\pi . n/2}{n} = \pi. \tag{2.56}$$

Also

$$(h,n) = 1 \iff (h, n-h) = 1. \tag{2.57}$$

Moreover $(n,q) \neq 1$. Finally by the definition of $\varphi(n)$, there are $\varphi(n)$ values of h such that $(h,n) = 1$ and $h \leq n$. So from the above statements, there are $\varphi(n)/2$ values of $h \in \mathbf{N}$ such that $(h,n) = 1$ and $h \leq q$. That is, there are $\varphi(n)/2$ values of $2cos\frac{2\pi h}{n}$ for $h \in \mathbf{N}$ such that $(h,n) = 1$ and $h \leq q$. That is, there are $\varphi(n)/2$ values of $2cos\frac{2\pi h}{n}$ for $h \in \mathbf{N}$ such that $(h,q) = 1$, h odd and $h \leq q$. As $deg\, P_q^*(x) = \varphi(n)/2$, the proof follows.

2.3. THE CONSTANT TERM OF $P_q^*(x)$

In Chapter 7 we will need to know the constant term of the minimal polynomial. In this section we calculate this term for all values of q.

Let c denote the constant term of the minimal polynomial $P_q^*(x)$ of λ_q, i.e.

$$c = P_q^*(0). \tag{2.58}$$

We have determined the roots of $P_q^*(x)$ in Theorem 2.5. Being the constant term, c is equal to the product of all roots of $P_q^*(x)$:

$$c = \prod_{\substack{h=1 \\ (h,q)=1 \\ h\ odd}}^{q-1} 2cos\frac{h\pi}{q}. \tag{2.59}$$

Therefore we need to calculate the product on the right hand side of (2.59). To do this we need a result given in [Ke–Yu,1]:

Lemma 2.3:

$$\prod_{h=0}^{q-1} 2sin(\frac{h\pi}{q} + \Theta) = 2sinq\Theta. \tag{2.60}$$

We now want to obtain a similar formula for cosine. By replacing Θ by $\frac{\pi}{2} - \Theta$ we get

$$\prod_{h=0}^{q-1} 2cos(\frac{h\pi}{q} - \Theta) = 2sinq(\frac{\pi}{2} - \Theta) \tag{2.61}$$

Let now μ denote the Möbius function defined by

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ is not square-free} \\ 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n \text{ has } k \text{ distinct prime factors,} \end{cases} \tag{2.62}$$

for $n \in \mathbf{N}$. It is known that

$$\sum_{d|n} \mu(d) = \begin{cases} 0 & \text{if } n > 1 \\ 1 & \text{if } n = 1 \end{cases} \tag{2.63}$$

Using this last fact we obtain

$$\begin{aligned} ln \prod_{h=0}^{q-1} 2cos(\tfrac{h\pi}{q} - \Theta) &= \sum_{h=0}^{q-1} ln\ (2cos(\tfrac{h\pi}{q} - \Theta)) \sum_{d|(h,q)} \mu(d) \\ &= \sum_{d|q} \mu(d) \sum_{k=0}^{\frac{q}{d}-1} ln\ (2cos(\tfrac{kd\pi}{q} - \Theta)) \\ &= \sum_{d|q} \mu(d) \left(ln \prod_{k=0}^{\frac{q}{d}-1} 2cos(\tfrac{kd\pi}{q} - \Theta) \right) \\ &= \sum_{d|q} \mu(d).ln\ (2sin\tfrac{q}{d}(\tfrac{\pi}{2} - \Theta)) \text{ by Lemma 2.3} \\ &= ln \prod_{d|q} sind(\tfrac{\pi}{2} - \Theta)^{\mu(q/d)}. \end{aligned} \tag{2.64}$$

Therefore

$$\prod_{\substack{h=0 \\ (h,q)=1}}^{q-1} 2cos(\frac{h\pi}{q} - \Theta) = \prod_{d|q} (sind(\frac{\pi}{2} - \Theta))^{\mu(q/d)}. \tag{2.65}$$

Finally, as $(0,q) \neq 1$, we can write (2.65) as

$$\prod_{\substack{h=1 \\ (h,q)=1}}^{q-1} 2cos(\frac{h\pi}{q} - \Theta) = \prod_{d|q} (sind(\frac{\pi}{2} - \Theta))^{\mu(q/d)}. \tag{2.66}$$

Note that if q is even then

$$\prod_{\substack{h=1 \\ (h,q)=1}}^{q-1} 2cos(\frac{h\pi}{q}) = \prod_{\substack{h=1 \\ (h,q)=1 \\ h \text{ odd}}}^{q-1} 2cos(\frac{h\pi}{q}) = c \tag{2.67}$$

while if q is odd then

$$\left| \prod_{\substack{h=1 \\ (h,q)=1}}^{q-1} 2cos(\frac{h\pi}{q}) \right| = c^2, \tag{2.68}$$

as $cos(h-i)\frac{\pi}{q} = -cos\frac{i\pi}{q}$. Also note that

$$sind(\frac{\pi}{2} - \Theta) = \begin{cases} cosd\Theta & \text{if } d \equiv 1 \bmod 4 \\ sind\Theta & \text{if } d \equiv 2 \bmod 4 \\ -cosd\Theta & \text{if } d \equiv 3 \bmod 4 \\ -sind\Theta & \text{if } d \equiv 4 \bmod 4 \end{cases} \tag{2.69}$$

To compute c we will let $\Theta \to 0$ in (2.66). If d is odd, then $sind(\frac{\pi}{2} - \Theta) \to \pm 1$ as $\Theta \to 0$, by (2.69). So we are only concerned with even d. Indeed, if q is odd then the left hand side at $\Theta = 0$ is equal to ± 1. Therefore we have

Theorem 2.6: Let q be odd. Then

$$|c| = 1. \tag{2.70}$$

Proof: It follows from (2.68) and (2.69).

Let us now investigate the case of even q. As $(h,q) = 1$, h must be odd. So by a similar discussion we get

Theorem 2.7: Let q be even. Then

$$c = \lim_{\Theta \to 0} \prod_{d|q} (sind(\frac{\pi}{2} - \Theta))^{\mu(q/d)}. \tag{2.71}$$

Note that by (2.69), the right hand side of (2.71) becomes a product of $\pm(cosd\Theta)^{\pm 1}$'s and $\pm(sind\Theta)^{\pm 1}$'s. Above we saw that we can omit the former ones as they tend to ± 1 as Θ tends to 0. Now as $\sum_{d|q} \mu(d) = 0$, there are equal numbers of latter kind factors in the numerator and denominator, i.e. if there is a factor $sind\Theta$ in the numerator, then there is a factor $sind'\Theta$ in the denominator. Then using the fact that

$$\lim_{\Theta \to 0} \frac{sink\Theta}{sinl\Theta} = \frac{k}{l}, \tag{2.72}$$

we can calculate c.

In fact the calculations show that there are three possibilities:

(i) Let $q = 2^{\alpha_0}$, $\alpha_0 \geq 2$. Then the only divisors of q such that $\mu(q/d) \neq 0$ are $d = 2^{\alpha_0}$ and $2^{\alpha_0 - 1}$. Therefore

$$\begin{aligned} c &= \lim_{\Theta \to 0} \frac{sin 2^{\alpha_0}(\frac{\pi}{2} - \Theta)}{sin 2^{\alpha_0 - 1}(\frac{\pi}{2} - \Theta)} \\ &= \begin{cases} 2 & if\ \alpha_0 > 2 \\ -2 & if\ \alpha_0 = 2. \end{cases} \end{aligned} \tag{2.73}$$

(ii) Secondly let $q = 2p^{\alpha}$, $\alpha \geq 1$, p odd prime. Then the only divisors of q such that $\mu(q/d) \neq 0$ are $d = 2p^{\alpha}, 2p^{\alpha-1}, p^{\alpha}$ and $p^{\alpha-1}$. Therefore

$$
\begin{aligned}
c &= \lim_{\Theta\to 0} \frac{sin2p^{\alpha}(\frac{\pi}{2}-\Theta).sinp^{\alpha-1}(\frac{\pi}{2}-\Theta)}{sinp^{\alpha}(\frac{\pi}{2}-\Theta).sin2p^{\alpha-1}(\frac{\pi}{2}-\Theta)} \\
&= \lim_{\Theta\to 0} \epsilon.\frac{sin2p^{\alpha}\Theta.cosp^{\alpha-1}\Theta}{cosp^{\alpha}\Theta.sin2p^{\alpha-1}\Theta} \qquad (2.74) \\
&= \epsilon.p
\end{aligned}
$$

where

$$
\epsilon = \begin{cases} 1 & \text{if } p \equiv 1 \, mod 4 \\ \text{-1} & \text{if } p \equiv -1 \, mod 4. \end{cases} \qquad (2.75)
$$

(iii) Let q be different from above. Then q can be written as

$$
q = 2^{\alpha_0} p_1^{\alpha_1} \dots p_k^{\alpha_k} \qquad (2.76)
$$

where p_i are distinct odd primes and $\alpha_i \geq 1$, $0 \leq i \leq k$.

Here we consider the first two cases $k = 1$ and 2. The proof for $k \geq 3$ is similar, but rather more complicated.

Let $k = 1$, i.e. let $q = 2^{\alpha_0}.p_1^{\alpha_1}$. We have already discussed the case $\alpha_0 = 1$. Let $\alpha_0 > 1$. Then the only divisors d of q with $\mu(q/d) \neq 0$ are $d = 2^{\alpha_0}p_1^{\alpha_1}$, $2^{\alpha_0-1}p_1^{\alpha_1}$, $2^{\alpha_0}p_1^{\alpha_1-1}$ and $2^{\alpha_0-1}p_1^{\alpha_1-1}$. Therefore

$$
\begin{aligned}
c &= \lim_{\Theta\to 0} \frac{sin2^{\alpha_0}p_1^{\alpha_1}(\frac{\pi}{2}-\Theta).sin2^{\alpha_0-1}p_1^{\alpha_1-1}(\frac{\pi}{2}-\Theta)}{sin2^{\alpha_0-1}p_1^{\alpha_1}(\frac{\pi}{2}-\Theta).sin2^{\alpha_0}p_1^{\alpha_1-1}(\frac{\pi}{2}-\Theta)} \\
&= 1.
\end{aligned} \qquad (2.77)
$$

Now let $k = 2$, i.e. let $q = 2^{\alpha_0}.p_1^{\alpha_1}.p_2^{\alpha_2}$. Similarly all divisors d of q such that $\mu(q/d) \neq 0$ are $d = 2^{\alpha_0}p_1^{\alpha_1}p_2^{\alpha_2}$, $2^{\alpha_0-1}p_1^{\alpha_1}p_2^{\alpha_2}$, $2^{\alpha_0}p_1^{\alpha_1-1}p_2^{\alpha_2}$, $2^{\alpha_0}p_1^{\alpha_1}p_2^{\alpha_2-1}$, $2^{\alpha_0}p_1^{\alpha_1-1}p_2^{\alpha_2-1}$ and $2^{\alpha_0-1}p_1^{\alpha_1-1}p_2^{\alpha_2-1}$. Therefore

$$
c = 1. \qquad (2.78)
$$

In general, when $k \geq 3$, the product of all coefficients d in the factors $sind(\frac{\pi}{2}-\Theta)$ in the numerator is equal to the product of all coefficients e in the factors $sine(\frac{\pi}{2}-\Theta)$

in the denominator implying $c = 1$. But the proof, as we explained above, is omitted.

Chapter 3

NORMAL SUBGROUPS OF H(λ_q) AND REGULAR MAPS

3.0. INTRODUCTION

Normal subgroups of the modular group Γ have been studied by many people and classification theorems are given ([Gr,1], [MQ,1], [Ne,2], [Ne,4], [Ne,6]). Our aim in this chapter is to generalise these results to all Hecke groups and find some normal subgroups of them. One way of doing this is to use regular map theory.

Although the study of maps began long ago, they have been widely studied in the last hundred years by, amongst others, Tietze [Ti,1], Brahana [Bh,1], Threlfall [Th,1], Heffter [Hf,1], Coxeter and Moser [Co–Mo,1], Edmond [Ed–Ew–Ku,1], Sherk [Sh,1], [Sh,2], and Jones and Singerman [Jo–Si,2].

In this chapter we begin by recalling some definitions and results about the theory of maps, mostly from [Jo–Si,1]. We then discuss the relations between the subgroups of H(λ_q) and maps. Specially, as all regular maps with genus $g \leq 7$ are known, we can obtain a lot of information about the normal subgroups of Hecke groups with $g \leq 7$, using these regular maps.

3.1. DEFINITIONS AND APPLICATION TO HECKE GROUPS

We define a *map* $\mathcal{M}$ to be an embedding (without crossings) of a finite connected graph $\mathcal{G}$ into a compact connected surface $\mathcal{S}$ without boundary such that $\mathcal{S}$ - $\mathcal{G}$ is a union of 2-cells. We are not going to be interested here in the non-orientable case, so we will assume that $\mathcal{S}$ is orientable as well.

The *dual map* of $\mathcal{M}$ has the same underlying surface $\mathcal{S}$ while the vertices and face centers are interchanged.

If m and n are the l.c.m. of the valencies of the faces and vertices, respectively, we then say $\mathcal{M}$ has *type* $\{m, n\}$. Clearly the dual map has type $\{n, m\}$.

We define a *dart* of $\mathcal{M}$ to be a pair consisting of an edge and an incident vertex, and draw it as an arrow on the edge towards the vertex. The set of darts of $\mathcal{M}$ will be denoted by Ω.

Figure 3.1. A dart α

The study of maps is closely related to the study of subgroups of certain triangle groups. Jones and Singerman showed that there is a natural correspondence between maps and Schreier coset graphs for the subgroups of the triangle groups $(2, m, n)$. We can illustrate this correspondence in the following way:

Let H be a subgroup of $\mathrm{H}(\lambda_q)$ with finite index μ. Then there is a natural homomorphism from $\mathrm{H}(\lambda_q)$ into the symmetric group S_μ by letting $\mathrm{H}(\lambda_q)$ permute the right cosets of H by right multiplication. This takes the elliptic element R of order 2 to a product of 1–cycles and 2–cycles, such that the sum of these lengths is equal to the index μ. Geometrically each cycle corresponds to an edge of the associated map (naturally, a 1–cycle corresponds to a free edge, having only one dart, and a 2–cycle corresponds to an ordinary edge so that the two darts of this edge are represented by the two elements in this cycle).

The elliptic generator S of order q goes to a product of r cycles of lengths $q_1, \ldots q_r$ where $q_i | q$, $1 \leq i \leq r$, and again the sum of these lengths is equal to μ. Here each cycle corresponds to a vertex in the following way: If σ_i is a cycle of length q_i, then there is a vertex v_i of the associated map with valency q_i. Also each dart at this vertex is represented by an element in σ_i. S permutes the darts around each vertex following an anticlockwise orientation.

Finally the parabolic element T goes to a product of s cycles of lengths $t_1, \ldots, t_s$ with the sum equal to μ. Here each cycle corresponds to a face of the map and T permutes the darts around each face.

The permutation group S_μ mentioned above is transitive on μ points where each point corresponds to a dart. In this way we obtain a map of type {m,n} where m is the l.c.m. of the lengths of the cycles of S and n is the l.c.m. of the lengths of the cycles of T.

Similarly we can choose the cycles of S to correspond to the faces and the cycles of T to the vertices and we obtain the dual map $\{n, m\}$, defined above, which has the same number of edges but with numbers of vertices and faces interchanged.

We can illustrate this correspondence in the following example:

Example 3.1: Let $q = 6$ and let H be the subgroup given by the permutation representation

$$\begin{array}{lcl} R & \rightarrow & (1\ 2)(3\ 4)(5\ 6)(7\ 8)(9\ 10)(11)(12) \\ S & \rightarrow & (1\ 3\ 5\ 7\ 9\ 11)(2\ 4\ 8)(6\ 12)(10) \\ T & \rightarrow & (1\ 4\ 5\ 12\ 6\ 7\ 2\ 3\ 8\ 9\ 10\ 11). \end{array} \tag{3.1}$$

By the Riemann–Hurwitz formula H has the signature

$$(1;\ 2,2,2,3,6,\infty) \tag{3.2}$$

and therefore is a map on a torus. To find its type, we must calculate the l.c.m.'s of the lengths of the cycles of S and T. These are 6 and 12, respectively, and therefore it is of type {6,12}. To draw it, we must consider the cycles given for R, S and T. For example, there are five 2-cycles in the permutation representation of R, each corresponding to an ordinary edge, and there are two 1-cycles corresponding to two free edges represented by 11 and 12. In the representation of S, the cycle (2 4 8) means that there are three darts represented by 2, 4 and 8 towards a vertex of the map. Similarly there are three other vertices of the map with valencies 1, 2 and 6. Also as we have only one cycle for T, the map is one faced. See figure 3.2.

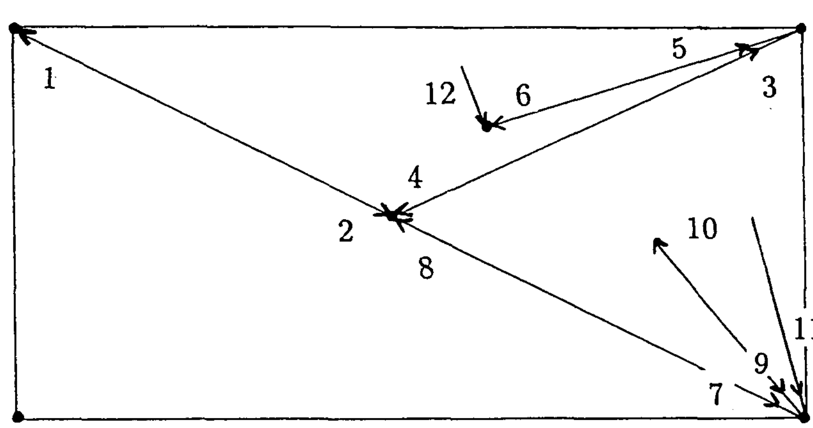


Figure 3.2. A map of type {6,12} on a torus

Conversely given a map $\mathcal{M}$ of type $\{m, n\}$ with $m|q$, we can find a permutation representation of $\mathrm{H}(\lambda_q)$ by letting R permute the two darts of an edge and S permute the darts around the vertices. Now if we take H to be the stabilizer of a dart then H is a subgroup of index μ in $\mathrm{H}(\lambda_q)$. Therefore to a given map we can associate a subgroup.

When the subgroup is normal, the situation is simpler. If we consider the permutation representation of this subgroup, then each of R, S and T has cycles of equal lengths, those being 2 (or 1 in exceptional cases–see below), m and n, respectively, where $m|q$: i.e. R goes to $\mu/2$ 2-cycles, S goes to μ/m m-cycles and T goes to μ/n n-cycles. Here the number n will correspond to the level of the normal subgroup. Clearly, $\mu/n = t$ is the number of the faces of the regular map. Jones and Singerman, in [Jo–Si,1], proved the existence of a natural 1:1 correspondence between normal subgroups and regular maps. For example, in Chapter 0, we have seen that $\mathrm{H}(\lambda_q)/\mathrm{H}'(\lambda_q) \cong C_2 \times C_q$. Clearly the relations $R^2 = S^q = I$ are satisfied and also if q is even $(RS)^q = I$ while if q is odd, $(RS)^{2q} = I$. Therefore the regular maps corresponding to the commutator subgroup $\mathrm{H}'(\lambda_q)$ are of type $\{q, q\}$ and $\{q, 2q\}$, respectively.

We define an *automorphism* of $\mathcal{M}$ to be an orientation preserving homeomorphism of $\mathcal{S}$ preserving the incidence of the darts of $\mathcal{M}$. We identify two automorphisms if they have the same effect on the darts. The automorphisms of $\mathcal{M}$ form a group $Aut\mathcal{M}$ called the *automorphism group* of $\mathcal{M}$. We shall see the importance of this group when studying properties like regularity, etc. of maps.

A map $\mathcal{M}$ is called *quasi-regular* if every vertex has the same valency, every face has the same valency, and either it has no *free edges* (an edge with only one dart) or all its edges are free. The only ones of the latter kind are called *star maps* and consist of a single vertex on the sphere surrounded by free edges towards it (Figure 3.3). Star maps lie on the sphere and correspond to the case where R maps to a product of 1–cycles.

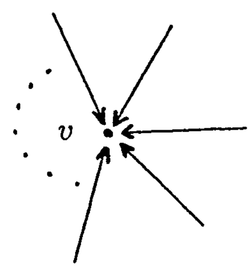


Figure 3.3. A star map

We call a map $\mathcal{M}$ *regular* if $Aut\mathcal{M}$ is transitive on Ω – the set of darts. Transitivity implies that from every vertex, the map looks the same. Obviously every regular map is also quasi-regular. The converse is not always true. However, on the sphere, every quasi-regular map is also regular (see [Jo–Si,1]). Note that even star maps are regular.

Every finite map of type $\{m, n\}$ can be finitely covered by a regular map of the same type, and hence, is the quotient of this regular map by a group of automorphisms.

Regularity is an important property of maps. Jones and Singerman showed the existence of a 1:1 correspondence between regular maps and normal subgroups of certain triangle groups including Hecke groups $\mathrm{H}(\lambda_q)$ (see [Jo–Si,1]). By means of this correspondence we can find normal subgroups of $\mathrm{H}(\lambda_q)$ and prove many important results related to them if we know the corresponding regular maps. For example, we shall classify normal subgroups of Hecke groups having genus 0 and 1 using this correspondence. Also as an important application, we shall use it to determine the number $N(\mu)$ of normal genus 1 subgroups of Hecke groups $\mathrm{H}(\lambda_q)$ having a given finite index μ in $\mathrm{H}(\lambda_q)$. This result has been proved by Kern–Isberner and Rosenberger using number theoretical methods in the special case $q = 4$ (see [Ke–Ro,1]).

We use this correspondence between regular maps and normal subgroups to obtain normal subgroups of Hecke groups from regular maps in the following way: Firstly, there is a homomorphism θ from $\mathrm{H}(\lambda_q) \cong (2, q, \infty)$ to the triangle group $(2, m, n)$ where m is a divisor of q. Let now $\mathcal{M}$ be a regular map of type $\{m, n\}$. By Jones and Singerman's result, associated to $\mathcal{M}$ there is a normal subgroup N of the triangle group $(2, m, n)$. If we consider the inverse image $\theta^{-1}(N)$ of N, it is a normal subgroup of $\mathrm{H}(\lambda_q)$. We shall say that *N is a normal subgroup of* $\mathrm{H}(\lambda_q)$ *corresponding to the regular map $\mathcal{M}$ of type $\{m, n\}$*. The number n corresponds to the level of the normal subgroup $\theta^{-1}(N)$.

Let V, E and F denote the set of vertices, edges and faces of a regular or quasi-regular map $\mathcal{M}$ with n_0, n_1 and n_2 elements respectively. Then

$$n.n_0 = 2.n_1 = m.n_2. \tag{3.3}$$

The number n_0 of vertices is the parabolic class number of $\theta^{-1}(N)$.

We have noted above that studying low genus normal subgroups by means of regular maps has many advantages. Therefore we try to obtain a classification of the regular maps of genus 0 and 1. The ones with genus 2 are listed in [Co–Mo,1], while when $g = 3$ the result is given by Sherk [Sh,1], and when $g = 4$, 5 , 6 or 7 by Garbe ([Ga,1] and [Ga,2]). It is known that the number of regular maps with genus $2 \leq g \leq 7$ is finite. An easy argument using the Riemann-Hurwitz formula implies that this is true for any $g \geq 2$.

Let us consider the spherical regular maps first. In this case an easy calculation shows that

$$(m-2)(n-2) < 4 \tag{3.4}$$

for a regular map of type $\{m,n\}$ on the sphere. Therefore all regular maps on the sphere are spherical tessellations (and star maps as a degenerate class), i.e. $\{2,n\}$, $n \in \mathrm{N}$, $\{3,3\},\{3,4\}$ and $\{3,5\}$ with their duals. We discuss them in the next chapter.

On a torus, a regular map of type $\{m,n\}$ must satisfy the equation

$$(m-2)(n-2)=4. \tag{3.5}$$

Thus only regular maps on a torus are the ones of type $\{4,4\},\{6,3\}$ or $\{3,6\}$. They are classified, in [Jo–Si,2] and [Co–Mo,1], as $\{4,4\}_{r,s}$, $\{6,3\}_{r,s}$ or $\{3,6\}_{r,s}$, respectively, with $r,s \in \mathrm{N} \cup \{0\}$ and not both of r,s zero. Also the automorphism group of $\{4,4\}_{r,s}$ is of order $4(r^2+s^2)$ and the automorphism group of $\{6,3\}_{r,s}$ or $\{3,6\}_{r,s}$ is of order $6(r^2+rs+s^2)$.

The normal subgroups of $\mathrm{H}(\lambda_q)$ having genus 1 will be studied in Chapter 5 while the ones of $\mathrm{H}(\sqrt{2})$ and $\mathrm{H}(\sqrt{3})$ are studied in Chapters 7 and 8.

Let now $\mathcal{M}$ be a given regular map of type $\{m,n\}$ and let the corresponding normal subgroup N have index μ in $\mathrm{H}(\lambda_q)$. By the permutation method and Riemann–Hurwitz formula, we see that N has the signature

$$\left(1+\frac{\mu}{2}\left(\frac{1}{2}-\frac{1}{m}-\frac{1}{n}\right);\ \frac{q}{m}^{(\mu/m)},\ \infty^{(\mu/n)}\right) \tag{3.6}$$

By (3.6), we can find whether a regular map of a given type may exist. It is then a purely group theoretical problem to show the existence of this regular map.

As we have already noted, the lists of regular maps of $g \leq 7$ are known. Therefore, for a given q, we can easily classify all regular maps with $g \leq 7$ corresponding to the normal subgroups of $\mathrm{H}(\lambda_q)$ with $g \leq 7$. As an easy example let us see how we can use the regular maps to obtain information about $g = 1$ normal subgroups of $H(\lambda_q)$. We have seen that the only regular maps of genus 1 are those of type {4,4},{3,6} and {6,3}. It is then easy to see that the first ones occur only when $4|q$, the second ones when $3|q$ and the third ones when $6|q$. Obviously when $12|q$, $H(\lambda_q)$ has normal subgroups of genus 1 corresponding to all three classes of regular maps above. It is also clear that if q is not divisible by 3 and 4, then $H(\lambda_q)$ has no normal subgroups of genus 1. For example, one of the four important Hecke groups, $H(\lambda_5)$, has no $g = 1$ normal subgroup for this reason.

To determine whether a normal subgroup is free or not is also important to us. Therefore we now consider this problem in particular for normal genus 1 subgroups of the four most important Hecke groups Γ, $H(\sqrt{2})$, $H(\lambda_5)$ and $H(\sqrt{3})$. When $q = 5$, we have noted in the above paragraph that $H(\lambda_5)$ has no normal subgroups of $g = 1$. The modular group Γ has infinitely many normal subgroups of genus 1 corresponding to the regular maps of type {3,6}, and therefore all of them are torsion-free. Similarly $H(\sqrt{2})$ has an infinite number of normal subgroups of genus 1 corresponding to the regular maps of type {4,4}, and again they are all free. The different case is $H(\sqrt{3})$. As $H(\sqrt{3})$ has signature $(0; 2,6,\infty)$ it is possible to map it to (2,3,6) and also (2,6,3). The former ones will give infinitely many normal subgroups of genus 1 with torsion (having a finite number of elements of order 2) while the latter ones give an infinite family of torsion-free genus 1 normal subgroups. This argument can easily be extended to other values of q. But significantly, the cases $q = 3$, 4 and 6 will remain as the only cases having torsion-free genus 1 normal subgroups. For a detailed discussion of normal genus 1 subgroups of Hecke groups $H(\lambda_q)$ see Chapter 5.

This idea, which we have applied to genus 1 normal subgroups only, can be extended to any g such that $g \leq 7$, but with more difficulty.

Some interesting examples of these three classes of regular maps are $\{6,3\}_{2,1}$ obtained by embedding the complete graph K_7 on a torus, and $\{4,4\}_{2,1}$ obtained by embedding K_5 on a torus (see Figure 3.4).

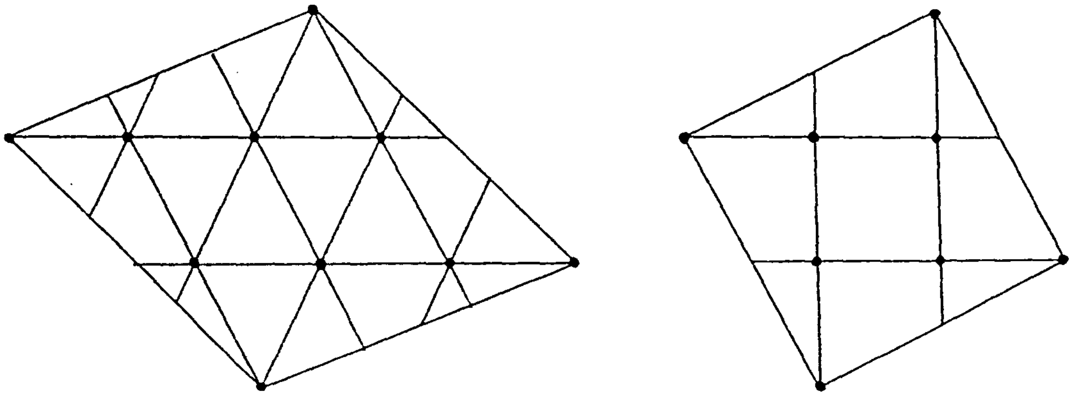


Figure 3.4. $\{6,3\}_{2,1}$ and $\{4,4\}_{2,1}$

These three types of regular maps of genus 1 will be dealt with, in detail, in Chapters 8 and 9 where we consider normal subgroups of the two important Hecke groups $H(\sqrt{2})$ and $H(\sqrt{3})$. We shall give the lists of the regular maps corresponding to low index normal subgroups of these two groups, and also pictures of some interesting ones.

Chapter 4

NORMAL SUBGROUPS OF GENUS 0, NORMAL TORSION AND TORSION–FREE SUBGROUPS OF $H(\lambda_q)$

4.0. INTRODUCTION

In this chapter we discuss normal subgroups of genus 0 of Hecke groups and also as a related topic, torsion and torsion–free subgroups of any genus $g \geq 0$.

We have already considered genus 0 normal subgroups of Hecke groups in the last chapter briefly, where we discussed the relations between normal subgroups of $H(\lambda_q)$ and regular maps. A more precise method which leads to a classification of genus 0 normal subgroups is to consider the corresponding quotient groups.

Let N be a normal subgroup of genus 0 in $H(\lambda_q)$. Then $H(\lambda_q)/N$ is a group of automorphisms of $\hat{U}/N$, where $\hat{U} = U \cup \mathbf{Q} \cup \{\infty\}$. This gives a regular map on the sphere so that $H(\lambda_q)/N$ is isomorphic to one of the finite triangle groups. These are known to be isomorphic to A_4, S_4, A_5, C_n and D_n for $n \in \mathbf{N}$. Considering each of these groups as a quotient group of $H(\lambda_q)$, whenever possible, we will find all genus

0 normal subgroups of Hecke groups. Also in this chapter, the total number $N_0(\lambda_q)$ of genus 0 normal subgroups in $H(\lambda_q)$ for all of the possible cases is calculated. It will be shown that this number is finite when q is odd, and infinite otherwise.

It can easily be seen that $N_0(\lambda_q)$ only depends on q. Indeed as it is only possible to map $H(\lambda_q)$ to the finite triangle groups, $N_0(\lambda_q)$ will depend on the divisibility of q by 2,3,4 and 5. We shall deduce that for each q, $H(\lambda_q)$ always has genus 0 normal subgroups and in fact

$$N_0(\lambda_q) \geq 2\prod_{p|q} (1 + \alpha_p) \tag{4.1}$$

where α_p is the exponent of the prime p in the prime power decomposition of q.

As most of the genus 0 normal subgroups of $H(\lambda_q)$ have torsion, we shall consider torsion subgroups of Hecke groups in this chapter. We shall classify all torsion-free normal genus 0 subgroups of $H(\lambda_q)$ of finite index and deduce that their total number does not exceed 4 in any case. Actually this number is only 1 if $q \geq 6$. We shall also find the number of normal torsion subgroups of $H(\lambda_q)$ of genus 0 as finite when q is odd, and infinite when q is even.

We then discuss the normal torsion and torsion-free subgroups of $H(\lambda_q)$ of genus $g \geq 2$. We particularly discuss the first two cases where g=2 and 3.

We shall see that the number of normal torsion-free subgroups of $H(\lambda_q)$ is always infinite. But this number is finite for any particular g.

Considering normal torsion subgroups, we find that $H(\sqrt{2})$ and $H(\lambda_p)$ for odd primes p have no normal proper torsion subgroups if $g \geq 1$, while for all other values of q, $H(\lambda_q)$ has infinitely many such subgroups.

4.1. NORMAL GENUS 0 SUBGROUPS OF $H(\lambda_q)$ WITH FINITE INDEX

We first discuss some genus 0 normal subgroups of finite index of $H(\lambda_q)$, which exist for any q, $q \geq 3$, $q \in N$:

By mapping R to identity and S to the generator α of the cyclic group of order n where $n|q$, we obtain a homomorphism of $H(\lambda_q)$ to the cyclic group of order n. For each such n we get a normal subgroup N of genus 0. By the permutation method, N has signature $(0;\, 2^{(n)},\, q/n,\, \infty)$. We denote this class of normal subgroups of $H(\lambda_q)$ by $Y_n(\lambda_q)$. They are isomorphic to the free-product of the cyclic group $C_{q/n}$ of order q/n with n cyclic groups of order two. The corresponding regular maps are star maps.

There is another homomorphism of $H(\lambda_q)$ to a cyclic group C_2 of order two with signature $(2,1,2)$ (that is, C_2 can be thought of as a finite triangle group with a presentation $< x, y | x^2 = y = (xy)^2 = I >$). But as this quotient is a member of the class $D_n \cong (2, n, 2)$ of dihedral groups of order $2n$, it will be considered in the following paragraph:

Let us now map $H(\lambda_q)$ to a dihedral group $D_n \cong (2, n, 2) \cong < x, y \,|\, x^2 = y^n = (xy)^2 = 1 >$ of order $2n$, where necessarily $n|q$, by taking R to x and S to y. This is a homomorphism and similarly we obtain a normal subgroup denoted by $S_n(\lambda_q)$ with signature $(0;\, q/n,\, q/n,\, \infty^{(n)})$. It is isomorphic to the free-product of two cyclic groups of order q/n with $n-1$ infinite cyclic groups.

Note that, if $n = 1$, we map $H(\lambda_q)$ to the cyclic group of order two and obtain the normal subgroup $S_1(\lambda_q) \cong C_q \star C_q$. If $n = q$ then $S_q(\lambda_q) \cong F_{q-1}$, a free group of rank $q-1$, is obtained.

All these subgroups occur for each value of q. There are some others, which we are now going to discuss, that occur dependently on q. Actually their occurence completely depends on the divisibility of q by 2, 3, 4 and 5, as we have noted above. Recall that if q is not divisible by these numbers, then there is no homomorphism from $\mathrm{H}(\lambda_q)$ to a finite triangle group, and therefore there is no normal subgroup of $\mathrm{H}(\lambda_q)$ having genus 0. Let us now discuss all these cases in order:

First let q be divisible by 3. Then $\mathrm{H}(\lambda_q)$ has three more normal subgroups of genus 0 in addition to those listed above:

Let $A_4 \cong (2,3,3) \cong < x, y \,|\, x^2 = y^3 = (xy)^3 = 1 >$. By mapping R to x and S to y we obtain a homomorphism of $\mathrm{H}(\lambda_q)$ onto A_4 and this gives a normal subgroup denoted by $T_1(\lambda_q)$ with signature $(0; (q/3)^{(4)}, \infty^{(4)})$.

If we map $\mathrm{H}(\lambda_q)$ to $S_4 \cong (2,3,4)$ by taking R to the generator of order 2 and S to the generator of order 3 of S_4, then we get a normal subgroup $T_2(\lambda_q)$ with signature $(0; (q/3)^{(8)}, \infty^{(6)})$.

Thirdly and finally if we map $\mathrm{H}(\lambda_q)$ to $A_5 \cong (2,3,5)$ such that R is taken to the generator of order 2 and S is taken to the generator of order 3, we obtain a normal subgroup $T_3(\lambda_q) \cong (0; (q/3)^{(20)}, \infty^{(12)})$.

Let, secondly, $4|q$. Then we have another homomorphism to S_4 taking R to the generator of order 2 and S to the generator of order 4, and we obtain a normal subgroup $T_4(\lambda_q) \cong (0; (q/4)^{(6)}, \infty^{(8)})$.

Thirdly, if $5|q$, then we can map $\mathrm{H}(\lambda_q)$ to $A_5 \cong (2,5,3)$ such that R is taken to the generator of order 2 and S to the generator of order 5. Then we obtain a normal subgroup $T_5(\lambda_q)$ with signature $(0; (q/5)^{(12)}, \infty^{(20)})$.

Furthermore when q is even, it is possible to map $\mathrm{H}(\lambda_q)$ to a dihedral group

$D_n \cong (2,2,n) \cong < x, y \,|\, x^2 = y^2 = (xy)^n = 1 >$ for each $n \in \mathbf{N}$ by mapping R to x and S to y. Here we obtain a normal subgroup with signature $(0;\, (q/2)^{(n)},\, \infty,\, \infty)$. These subgroups are important in the study of normal subgroups of Hecke groups. They are denoted by $W_n(\lambda_q)$ and isomorphic to the free–product of the infinite cyclic group $\mathbf{Z}$ with n finite cyclic groups of order two. We have the following result:

Theorem 4.1: Let $m, n \in \mathbf{N}$. Then

$$W_{mn}(\lambda_q) \lhd W_n(\lambda_q). \tag{4.2}$$

In general if q is odd, for example in the modular group case, it is not possible to obtain these subgroups and therefore there are only finitely many normal subgroups of genus 0 in $\mathrm{H}(\lambda_q)$ for odd q. Of course when q is even, $\mathrm{H}(\lambda_q)$ has infinitely many normal subgroups of genus 0, as we can map $\mathrm{H}(\lambda_q)$ to $D_n \cong (2,2,n)$ for any $n \in \mathbf{N}$.

4.2. NUMBER OF NORMAL GENUS 0 SUBGROUPS OF $\mathrm{H}(\lambda_q)$ WITH FINITE INDEX

We now calculate the number of genus 0 normal subgroups of $\mathrm{H}(\lambda_q)$ for all possible cases. Because of the $W_n(\lambda_q)$ subgroups, there will be two situations to consider mainly: Odd q and even q cases. As we have already noted, this number is finite for the former situation, and infinite otherwise. However if we exclude the subgroups of type $W_n(\lambda_q)$, then $\mathrm{H}(\lambda_q)$, now for any q, has only finitely many normal genus 0 subgroups with finite index. We will try to find this number:

Let $N_0(\lambda_q)$ denote the number of normal genus 0 subgroups of finite index in $\mathrm{H}(\lambda_q)$ except those of type $W_n(\lambda_q)$. Firstly

$$N_0(\lambda_q) < \infty. \tag{4.3}$$

We have seen that for all q we can map $\mathrm{H}(\lambda_q)$ to the cyclic group C_n such that $n|q$ by taking R to the identity and S to the generator of C_n. For each such n we obtain a normal subgroup of genus 0 and therefore the number of them will be as much as the number of divisors of q. Since the function "number of divisors" is multiplicative, we only need to determine the number of divisors of each prime power p^{α_p} in the prime power decomposition of q. But this number is $1 + \alpha_p$ as all the divisors of p^{α_p} are $1, p, p^2, \ldots, p^{\alpha_p}$. Hence if q has the prime power decomposition

$$q = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}, \tag{4.4}$$

then the number of divisors of q is

$$d(q) = \prod_{i=1}^{k} (1 + \alpha_i), \tag{4.5}$$

or in other words

$$d(q) = \prod_{p|q} (1 + \alpha_p). \tag{4.6}$$

As we can map $\mathrm{H}(\lambda_q)$ to $D_n \cong (2, n, 2)$ such that $n|q$, this will also give us $d(q)$ normal subgroups of genus 0. This shows that (4.1) is always true.

We now find the number of other normal genus 0 subgroups that occur depending on q. As we are not considering the ones of type $W_n(\lambda_q)$ we have only nine cases to investigate:

(1) If $(q, 60) = 1$, i.e. if neither 3,4 nor 5 divides q, then we do not have A_4, S_4 nor A_5 as a homomorphic image of $\mathrm{H}(\lambda_q)$ and therefore $N_0(\lambda_q)$ is just $2d(q)$.

(2) If $(q, 20) = 1$ and $3|q$, then there exist three homomorphisms to A_4, S_4 and A_5 as we have seen above and therefore the number $N_0(\lambda_q)$ is $3 + 2d(q)$.

(3) If $(q, 20) = 2$ and $3|q$, then again there exist three homomorphisms to A_4, S_4 and A_5 and therefore the number $N_0(\lambda_q)$ is $3 + 2d(q)$.

(4) If $(q, 15) = 1$ and $4|q$, then there is only one possible homomorphism which is to S_4 and $N_0(\lambda_q)$ is $1 + 2d(q)$.

(5) If $(q, 12) = 1$ and $5|q$, then again there is a unique homomorphism, this time to A_5, and $N_0(\lambda_q)$ is $1 + 2d(q)$.

(6) If $(q, 5) = 1$ and $12|q$ then there are two homomorphisms to S_4, one to A_4 and one to A_5. Therefore $N_0(\lambda_q) = 4 + 2d(q)$.

(7) If $(q, 4) = 1$ and $15|q$ then there are two homomorphisms to A_5, one to A_4 and one to S_4. Therefore $N_0(\lambda_q)$ is $4 + 2d(q)$.

(8) If $(q, 3) = 1$ and $20|q$ then $\mathrm{H}(\lambda_q)$ can be mapped to S_4 and A_5 only and $N_0(\lambda_q)$ is $2 + 2d(q)$.

(9) If $60|q$ then we have all of above homomorphisms and therefore $N_0(\lambda_q) = 5 + 2d(q)$.

Therefore we have

Theorem 4.2: Let $d(q)$ be the number of divisors of q. Then the number $N_0(\lambda_q)$ of normal genus 0 subgroups of $\mathrm{H}(\lambda_q)$ with finite index apart from the ones of type $W_n(\lambda_q)$ is

$$\begin{cases} 2d(q) & \text{if} \quad (q,60) = 1 \ or \ 2 \\ 3 + 2d(q) & \text{if} \quad (q,20) = 1 \ and \ 3|q \\ 3 + 2d(q) & \text{if} \quad (q,20) = 2 \ and \ 3|q \\ 1 + 2d(q) & \text{if} \quad (q,15) = 1 \ and \ 4|q \\ 1 + 2d(q) & \text{if} \quad (q,12) = 1 \ and \ 5|q \\ 4 + 2d(q) & \text{if} \quad (q,5) = 1 \ and \ 12|q \\ 4 + 2d(q) & \text{if} \quad (q,4) = 1 \ and \ 15|q \\ 2 + 2d(q) & \text{if} \quad (q,3) = 1 \ and \ 20|q \\ 5 + 2d(q) & \text{if} \quad 60|q. \end{cases} \tag{4.7}$$

Note that when $(q,60) = 2$ in case 1 and in cases 4, 6, 8 and 9 we also have infinitely many normal subgroups of genus 0 of type $W_n(\lambda_q)$. These cases are, of course, the ones where q is even. In all other cases $N_0(\lambda_q)$ is the number of all normal genus 0 subgroups of $H(\lambda_q)$.

4.3. NORMAL TORSION–FREE SUBGROUPS OF $H(\lambda_q)$

We have seen that most of the normal genus 0 subgroups of Hecke groups have torsion. Actually there are only a few that are torsion–free. They are found by considering the regular maps on the sphere:

Theorem 4.3: The normal genus 0 torsion–free subgroups of Hecke groups are the following:

$$\begin{cases} N & & \mathrm{H}(\lambda_q) & \text{index} \\ (0;\ \infty^{(4)}) & \lhd & (0;\ 2,3,\infty) & 12 \\ (0;\ \infty^{(6)}) & \lhd & (0;\ 2,3,\infty) & 24 \\ (0;\ \infty^{(12)}) & \lhd & (0;\ 2,3,\infty) & 60 \\ (0;\ \infty^{(8)}) & \lhd & (0;\ 2,4,\infty) & 24 \\ (0;\ \infty^{(20)}) & \lhd & (0;\ 2,5,\infty) & 60 \\ (0;\ \infty^{(q)}) & \lhd & (0;\ 2,q,\infty) & 2q. \end{cases} \tag{4.8}$$

Note that the number of parabolic classes of each normal subgroup is actually equal to the number of vertices of the corresponding regular solid. In fact each vertex can be thought of as a cusp on the sphere. For example there are four classes of parabolic points for the subgroup $(0;\ \infty^{(4)})$ and the corresponding regular solid is a blown–up tetrahedron on the sphere with four vertices being four cusp points. See Figure 4.1.

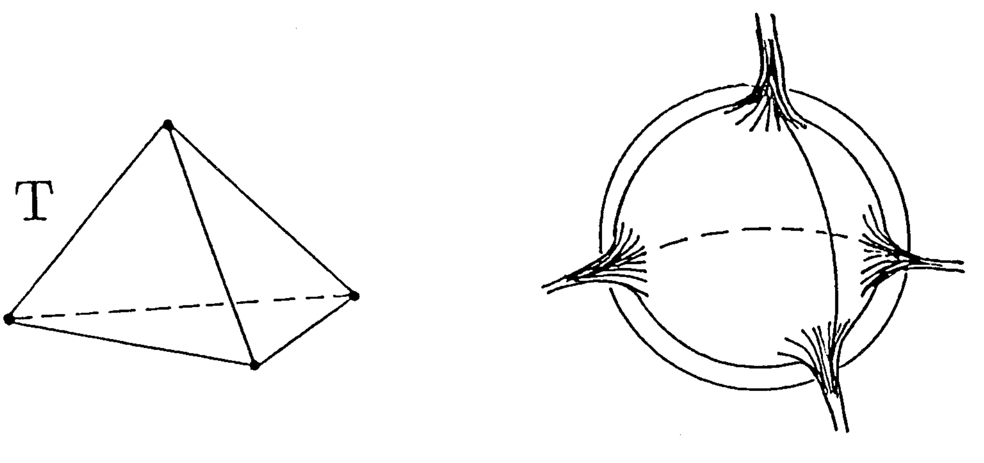


Figure 4.1. A tetrahedron corresponding to $(0;\ \infty^{(4)}) \lhd \Gamma$

Note also that the quotient group $H(\lambda_3)/N \cong A_4 \cong (2,3,3)$. Therefore corresponding regular solid, which is a tetrahedron, can be thought of as a regular map of type $\{3,3\}$ (see Chapter 3).

In the other five cases, the corresponding regular solids are octahedron, icosahedron, cube, dodecahedron and dihedron, respectively. See Figure 4.2.

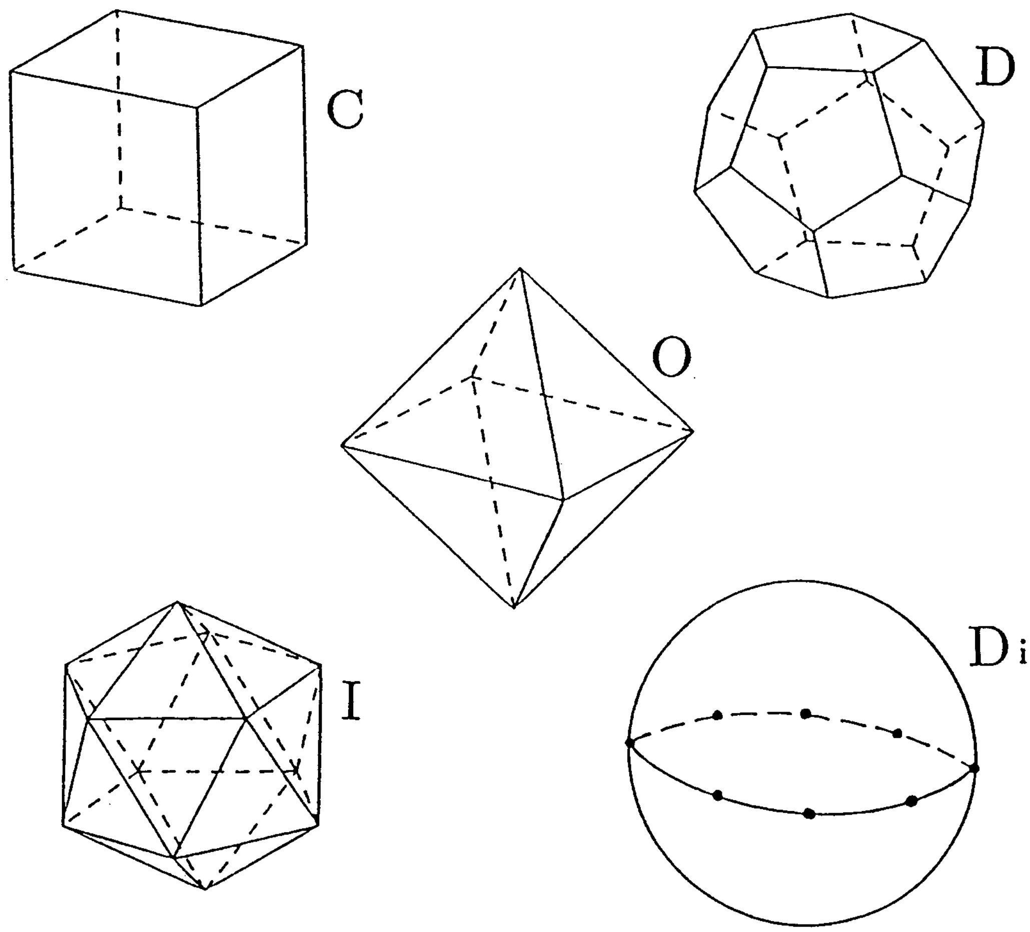


Figure 4.2. Other four platonic solids and a dihedron

Hence we have

Corollary 4.1: The number of normal genus 0 torsion–free subgroups of $\mathrm{H}(\lambda_q)$ is

$$\begin{cases} 4 & \text{if} \quad q = 3 \\ 2 & \text{if} \quad q = 4 \, or \, 5 \\ 1 & \text{if} \quad q \geq 6. \end{cases} \tag{4.9}$$

and they are $S_3(\lambda_3)$, $T_1(\lambda_3)$, $T_2(\lambda_3)$, $T_3(\lambda_3)$, $S_4(\sqrt{2})$, $T_4(\sqrt{2})$, $S_5(\lambda_5)$, $T_5(\lambda_5)$ and $S_q(\lambda_q)$.

By Theorem 4.2 and Corollary 4.1 we easily obtain the following result:

Theorem 4.4: The number of normal genus 0 subgroups of $\mathrm{H}(\lambda_q)$ having torsion is finite if q is odd, and infinite otherwise. If we omit the class $W_n(\lambda_q)$ which exists when q is even, then this number is always finite and equal to
and

$$\begin{cases} -1 + 2d(q) & \text{if} \quad (q, 60) = 1 \; or \; 2 \\ 2 + 2d(q) & \text{if} \quad (q, 20) = 1 \; and \; 3|q \\ 2 + 2d(q) & \text{if} \quad (q, 20) = 2 \; and \; 3|q \\ 2d(q) & \text{if} \quad (q, 15) = 1 \; and \; 4|q \\ 2d(q) & \text{if} \quad (q, 12) = 1 \; and \; 5|q \\ 3 + 2d(q) & \text{if} \quad (q, 5) = 1 \; and \; 12|q \\ 3 + 2d(q) & \text{if} \quad (q, 4) = 1 \; and \; 15|q \\ 1 + 2d(q) & \text{if} \quad (q, 3) = 1 \; and \; 20|q \\ 4 + 2d(q) & \text{if} \quad 60|q. \end{cases} \tag{4.10}$$

when $q \geq 6$, and

$$\begin{cases} 3 & \text{if} \quad q = 3 \\ 5 & \text{if} \quad q = 4 \\ 3 & \text{if} \quad q = 5. \end{cases} \tag{4.11}$$

and they are Γ, Γ^2, Γ^3, $H(\sqrt{2})$, $H_e(\sqrt{2})$, $Y_2(\sqrt{2})$, $S_1(\sqrt{2})$, $H^2(\sqrt{2})$, $H(\lambda_5)$, $H^2(\lambda_5)$ and $H^5(\lambda_5)$, when $q \leq 5$.

By the Riemann–Hurwitz formula, the number of normal subgroups of $H(\lambda_q)$ having genus $g > 1$ and finite index is finite. However when $g = 1$, the situation is more complicated. In Chapter 3, we have briefly discussed these subgroups. The following result is clear:

Theorem 4.5: **(i)** $H(\lambda_q)$ has no normal genus 1 subgroups if and only if $(q, 12) = 1$ or 2.

(ii) $H(\lambda_q)$ has infinitely many normal genus 1 subgroups if and only if $(q, 12) \geq 3$.

(iii) $H(\lambda_q)$ has a (and therefore infinitely many) torsion–free normal genus 1 subgroup if and only if $q = 3, 4$ or 6.

(iv) All normal genus 1 subgroups of $H(\lambda_q)$ are torsion–free if and only if $q = 3$ or 4. (In both cases, the number of these subgroups is infinite).

(v) All normal genus 1 subgroups of $H(\lambda_q)$ have torsion if and only if $q > 6$. (In this case their number is infinite again).

(vi) $H(\lambda_q)$ has both torsion and torsion–free subgroups of genus 1 if and only if $q = 6$. (Both are infinitely many).

Let us now discuss normal torsion subgroups of $H(\lambda_q)$ for several values of q:

Firstly, if $q = 4$, as we noted in the last chapter, $H(\sqrt{2})$ has infinitely many normal genus 1 subgroups which are all torsion–free. Secondly let $q = p$, a prime, it is easy to see that $H(\lambda_p)$ has no normal torsion subgroups of genus 1 as it is discussed in the last chapter. Let thirdly q be a composite number ≥ 6 and let either $3|q$ or $4|q$. Then $H(\lambda_q)$ has at least one (and therefore infinitely many) normal genus 1 subgroups with torsion. This is because we can map $H(\lambda_q)$ homomorphically to the infinite triangle groups $(2,3,6)$ or $(2,4,4)$ and this gives infinitely many normal subgroups of genus 1 with torsion. Also if $6|q$, $q \geq 12$, then $H(\lambda_q)$ can be mapped to $(2,6,3)$ homomorphically and this too gives infinitely many normal subgroups of genus 1 with torsion. Let us finally consider the remaining values of q. By means of a similar argument, we see that when q is a composite number > 4 such that $(q,12) = 1$, $H(\lambda_q)$ has no normal genus 1 subgroups with torsion (in fact no subgroups of genus 1).

We have noted above that the number of normal subgroups of $H(\lambda_q)$ having genus $g > 1$ is finite by the Riemann–Hurwitz formula. This can also be seen from the fact that the number of regular maps of genus $g > 1$ is finite. Therefore there are only finitely many normal torsion and torsion free subgroups of $H(\lambda_q)$ of genus $g > 1$.

Let us now consider the first two cases:

(1) $g = 2$: All possible regular maps on a Riemann surface of genus two are given by Coxeter and Moser in [Co–Mo,1]. They are of type $\{8,8\}$, $\{5,10\}$, $\{6,6\}$, $\{4,8\}$, $\{4,6\}$, $\{3,8\}$ and their duals. Using the 1:1 correspondence between normal subgroups and regular maps, it is not too difficult to obtain the following result:

Theorem 4.6: (i) $H(\lambda_q)$ has no normal torsion–free subgroup of genus $g = 2$ if and only if $q = 7$, 9 or $q > 10$.

(ii) $H(\lambda_q)$ has a normal torsion-free subgroup of genus two if and only if $q =$ 3,4,5,6,8 or 10.

(iii) $H(\lambda_q)$ has no normal (torsion or torsion-free) subgroup of genus two if and only if $(q, 120) \leq 2$.

(iv) Therefore, $H(\lambda_q)$ has normal genus two subgroups if and only if $(q, 120) \geq 3$.

(v) $H(\lambda_q)$ has a normal subgroup of genus two with torsion if and only if $q > 10$ and $(q, 120) \geq 3$.

Proof: To prove this theorem, we must recall the 1:1 correspondence between normal subgroups and regular maps described in Chapter 3: There is a homomorphism of $H(\lambda_q)$ to the triangle group $(2, m, n)$ where $m|q$. We saw in Chapter 3 that if $\mathcal{M}$ is a regular map of type $\{m, n\}$, then, by a result of Jones and Singerman, there is a normal subgroup N of $(2, m, n)$ and the inverse image of N is a normal subgroup of $H(\lambda_q)$ corresponding, uniquely, to $\mathcal{M}$. Using this correspondence, we can prove Theorem 4.6. We prove **(iii)**. The others can be proved in a similar way:

Let us suppose $(q, 120) = k \geq 3$. Then $k =$ 3,4,5,6,8,10,12,15,20,24,30,40,60 or 120. Let $k = 3$. Then as there exists a regular map of type $\{3, 8\}$, by the above correspondence, $H(\lambda_q)$ has a normal torsion-free subgroup of genus 2. Similarly for $k \leq 10$, there exists a regular map of type $\{k, l\}$ for some natural number l and therefore a normal torsion-free subgroup of $H(\lambda_q)$. For the other values of k $H(\lambda_q)$ has normal subgroups of genus 2 having torsion, e.g. if $k = 30$, then $H(\lambda_q)$ has at least 5 normal genus 2 subgroups having torsion corresponding to the regular maps of type $\{3, 8\}$, $\{5, 10\}$, $\{6, 4\}$, $\{6, 6\}$, $\{10, 5\}$. Therefore by contrapositive method, one side of **(iii)** is proven. Let now $H(\lambda_q)$ has a normal subgroup of genus 2. Then by Jones and Singerman's result, q must be divisible by 3,4,5,6,8 or 10. Therefore $(q,120) \geq 3$. Again by the contrapositive method, the other side of (iii) follows.

(2) $g = 3$: All regular maps of genus three are listed by Sherk in [Sh,1] . They are of type $\{12,12\}$, $\{7,14\}$, $\{8,8\}$, $\{4,12\}$, $\{6,6\}$, $\{4,8\}$, $\{3,12\}$, $\{4,6\}$, $\{3,8\}$, $\{3,7\}$ and their duals. Then we can obtain following similar result:

Theorem 4.7: **(i)** $H(\lambda_q)$ has no normal torsion-free subgroup of genus $g = 3$ if and only if $q =$ 5,9,10,11,13 or $q > 14$.

(ii) $H(\lambda_q)$ has a normal torsion-free subgroup of genus three if and only if $q =$ 3,4,6,7,8,12 or 14.

(iii) $H(\lambda_q)$ has no normal (torsion or torsion-free) subgroup of genus three if and only if $(q,168) \leq 2$.

(iv) Therefore, $H(\lambda_q)$ has normal genus three subgroups if and only if $(q,168) \geq 3$.

(v) $H(\lambda_q)$ has a normal subgroup of genus three with torsion if and only if $q > 14$ and $(q,168) \geq 3$.

Similar results can be obtained for normal subgroups of $H(\lambda_q)$ with genus $4 \leq g \leq 7$ as all regular maps of genus up to and including 7 are known.

However a problem arises when we want to calculate the number of normal subgroups of genus $g \geq 2$. It is possible that there are many homomorphisms from a triangle group $(2,m,n)$ onto a finite group G. This means that there could be more than one regular map of type $\{m,n\}$ and genus g. For example there are two regular maps $\{8,8\}_2$ and $\{4.2,4.2\}$ of type $\{8,8\}$.

Chapter 5

GENUS 1 NORMAL SUBGROUPS OF $H(\lambda_q)$

5.0. INTRODUCTION

In this chapter we discuss the normal subgroups of genus 1 of Hecke groups. They have already been discussed briefly in Chapter 3 as an application of regular map theory to Hecke groups. Here we extend this discussion and obtain all our results concerning normal subgroups of genus 1 using regular maps.

We begin by recalling some facts from Chapter 3 about regular maps on a torus. The main idea we are using is the 1:1 correspondence between regular maps and normal subgroups of the triangle groups $(2, m, n)$, proved by Jones and Singerman.

Firstly we determine the values of q such that $H(\lambda_q)$ has a normal subgroup of genus 1, and also such that $H(\lambda_q)$ has a free normal subgroup of genus 1.

Next, we consider normal subgroups of genus 1 of $H(\sqrt{2})$ and $H(\sqrt{3})$, two important Hecke groups. These subgroups will be discussed in Chapters 8 and 9 in detail. Here we determine their total number to be infinite.

Finally we give a generalisation of a result of Rosenberger and Kern–Isberner, [Ke–Ro,1]. They discussed normal subgroups of genus 1 of certain free products and showed, using number theoretical methods, that the number $N(\mu)$ of normal genus 1 subgroups of $H(\sqrt{2})$ of a given index μ is equal to a quarter of the number of representations of $\mu/4$ as the sum of two squares in $\mathbf{Z}$. Here we use some well-known number theoretical results to calculate this number explicitly. Then we calculate $N(\mu)$ for $H(\sqrt{3})$. Finally we obtain the generalisation for all values of q, that is, a formula giving the number of normal genus 1 subgroups of $H(\lambda_q)$ having a fixed index μ.

At the end of this thesis, we give, in Appendix 1, a list of values of $N(\mu)$ for small values of q and μ.

5.1. EXISTENCE OF NORMAL GENUS 1 SUBGROUPS OF $H(\lambda_q)$

Recall that, if a regular map of type $\{m, n\}$ has n_0 vertices, n_1 edges and n_2 faces, then the Euler–Poincaré characteristic χ of $\{m, n\}$ is given by

$$\chi = n_0 - n_1 + n_2 = 2 - 2g \tag{5.1}$$

and also

$$nn_0 = 2n_1 = mn_2. \tag{5.2}$$

Combining these two equalities, we obtain

$$\chi = \frac{n_1}{mn}(4 - (m-2)(n-2)). \tag{5.3}$$

We want to find out the regular maps of genus 1, that is, the regular maps on a torus. Putting $\chi = 0$ in (5.3), we obtain

$$(m-2)(n-2) = 4. \tag{5.4}$$

It is easy to see that the only solutions of (5.5) are

$$\{3,6\},\ \{4,4\} \quad \textit{and} \quad \{6,3\}. \tag{5.5}$$

This makes sense as these are the only regular Euclidean tessellations of the complex plane **C** and the universal covering of the torus is conformally equivalent to **C**.

These three types of regular maps on a torus are classified in [Jo–Si,2] and [Co–Mo,1] as

$$\{3,6\}_{r,s},\ \{4,4\}_{r,s} \quad \textit{and} \quad \{6,3\}_{r,s} \tag{5.6}$$

for non–negative integers r and s, not both zero.

In Chapter 3, we mentioned a 1:1 correspondence between the regular maps and normal subgroups of certain triangle groups, including Hecke groups, proven by Jones and Singerman. Recall that for every divisor m of q, there exists a homomorphism θ from $\mathrm{H}(\lambda_q) \cong (2,q,\infty)$ into a finite quotient of the triangle group $(2,m,n)$, $n \in \mathbf{N}$, taking the generator R of order 2 to the generator r of order 2, the second generator S of order q to the generator s of order m so that the product $T = RS$ is mapped to rs of order n in $(2,m,n)$. This homomorphism gives us a normal subgroup of $(2,m,n)$. Let N be a normal subgroup of $(2,m,n)$ of index μ obtained in this way. Then $\theta^{-1}(N)$ is a normal subgroup of $\mathrm{H}(\lambda_q)$ of index μ as well. By Jones and Singerman's result, there is a regular map of type $\{m,n\}$ corresponding to each normal subgroup of $(2,m,n)$. It is known that the number μ is also the order of the automorphism group of $\{m,n\}$. Similarly to each regular map of type $\{m,n\}$, there exists a normal subgroup of $\mathrm{H}(\lambda_q)$, $m|q$. Here the number n is also important:

Theorem 5.1: The number n is equal to the level of the normal subgroup $\theta^{-1}(N)$.

Proof: $H(\lambda_q)$ has a presentation $(2, q, \infty) \cong < R, S | R^2 = S^q = I >$. Similarly the triangle group $(2, m, n)$ has a presentation $< r, s | r^2 = s^m = (rs)^n = 1 >$. The above homomorphism θ takes the generators R, S of $H(\lambda_q)$ to the generators r, s of $(2, m, n)$. Then the parabolic element $T = RS$ is mapped to rs of order n and as $(rs)^n = 1$

$$(RS)^n \in Ker\,\theta = \theta^{-1}(1) < \theta^{-1}(N). \tag{5.7}$$

That is $\theta^{-1}(N) \lhd H(\lambda_q)$ is of level n.

As all regular maps $\{m, n\}_{r,s}$ on a torus are $\{3, 6\}_{r,s}$, $\{4, 4\}_{r,s}$ and $\{6, 3\}_{r,s}$, it follows that the existence of a normal genus 1 subgroup completely depends on the divisibility of q by 3, 4 and 6. Clearly if $4 \,|\, q$ we obtain the regular maps of type $\{4, 4\}$ corresponding to the normal subgroups of $H(\lambda_q)$ of genus 1, while the ones of type $\{6, 3\}$ (or $\{3, 6\}$) are obtained when q is divisible by six (or three). All these three types are obtained when $12 \,|\, q$. It also follows that if $(q, 12) = 1$ or 2, then $H(\lambda_q)$ does not have any normal genus 1 subgroups. Therefore we have

Theorem 5.2: $H(\lambda_q)$ has a normal subgroup of genus 1 if and only if $q \equiv 0 \ mod\, 3$ or $q \equiv 0 \ mod\, 4$.

Note that when $H(\lambda_q)$ has a normal subgroup of genus 1, it actually has infinitely many of them as each of the three classes discussed above has infinitely many regular maps. Therefore

Theorem 5.3: The total number of normal subgroups of genus 1 in $H(\lambda_q)$ is either 0 or ∞.

Let us now consider the four most important Hecke groups $\Gamma = H(\lambda_3)$, $H(\sqrt{2})$, $H(\lambda_5)$ and $H(\sqrt{3})$.

By Theorem 5.2, H(λ_5) has no normal genus 1 subgroups.

The modular group, having the signature $(0\ ;\ 2,3,\infty)$, has infinitely many normal subgroups of genus 1 corresponding to infinitely many regular maps of type $\{3,6\}$. If N is a normal subgroup of the modular group corresponding to such a regular map, then in Γ/N we have the relations

$$r^2 = s^3 = (rs)^6 = \ldots = I. \tag{5.8}$$

Therefore N must be free. The genus 1 normal subgroups of the modular group were discussed by [Ne,2].

H($\sqrt{2}$), similarly to the modular group case, has also infinitely many normal genus 1 subgroups corresponding, this time, to the regular maps of type $\{4,4\}$. Here we have the relations

$$r^2 = s^4 = (rs)^4 = \ldots = I. \tag{5.9}$$

and again the normal subgroup is free.

Finally let us consider H($\sqrt{3}$). In this case, as there exist homomorphisms onto the infinite triangle groups (2,3,6) and (2,6,3), H($\sqrt{3}$) has infinitely many normal genus 1 subgroups corresponding to the regular maps of type $\{3,6\}$ and also infinitely many normal genus 1 subgroups corresponding to the regular maps of type $\{6,3\}$. If we map H($\sqrt{3}$) to the former triangle group, then in the quotient H($\sqrt{3}$)$/N$ the relations

$$r^2 = s^3 = (rs)^6 = \ldots = I \tag{5.10}$$

are satisfied. Therefore N contains elements of order two, i.e. it is not torsion-free. If we map H($\sqrt{3}$) onto (2,6,3), then similarly to the previous cases, N must be torsion-free.

All these together imply the following result:

Theorem 5.4: **(i)** All normal subgroups of genus 1 of $H(\lambda_q)$ are free if and only if $q = 3$ or 4.

(ii) The only values of q such that $H(\lambda_q)$ has a normal free subgroup of genus 1 are 3,4 and 6.

Note that the converse of (ii) is not always true as $H(\sqrt{3})$ has normal subgroups of genus 1 with torsion.

5.2. NUMBER OF NORMAL GENUS 1 SUBGROUPS OF $H(\lambda_q)$

Normal subgroups of genus 1 of $H(\sqrt{2})$ and $H(\sqrt{3})$ will be discussed in detail in Chapters 8 and 9. As a nice application, we are now going to obtain some formulae for the number $N(\mu)$ of genus 1 normal subgroups of these two groups having a given index μ, and then generalise this to any q to find the number $N(\mu)$ of the normal genus 1 subgroups of $H(\lambda_q)$ having a given index μ.

(i) $q = 4$:

In Chapter 3, we have seen that such a regular map must be of type $\{4,4\}$. In [Jo–Si,2] and [Co–Mo,1], these are classified as $\{4,4\}_{r,s}$ for non-negative integers r and s. Also if N is a normal subgroup of $H(\sqrt{2})$ corresponding to such a regular map, then

$$|\, Aut\,\mathcal{M}\,| = |\, H(\sqrt{2}) : N\,| = 4(r^2 + s^2). \qquad (5.11)$$

As regularity of the regular map corresponds to the normality of the corresponding normal subgroup, each of these regular maps will give us a normal subgroup of

$H(\sqrt{2})$ with genus 1 and finite index $\mu = 4(r^2 + s^2)$. This implies

Theorem 5.5: $H(\sqrt{2})$ has infinitely many normal subgroups of genus 1.

We have already seen that a normal subgroup of $H(\sqrt{2})$, apart from $H(\sqrt{2})$ itself, has always even index. We have studied the normal subgroups $W_n(\sqrt{2})$ of genus 0 and found their index in $H(\sqrt{2})$ to be $2n$. If $\mu > 4$, then apart from these normal subgroups, all normal subgroups of $H(\sqrt{2})$ have index μ divisible by four, and we have often noted that this is an interesting case. Also if the genus is 1 then $\mu = 4(r^2 + s^2)$ as we have just noted.

Now given $\mu = 4(r^2 + s^2)$, $H(\sqrt{2})$ has as many normal subgroups N of genus 1 with index μ as the number of possible "non-identical" pairs (r, s) such that $r^2 + s^2 = t$ where t denotes the number of parabolic classes of N. Before proving this statement, we want to explain what we mean by non-identical pairs (or equivalently, identical pairs):

Recall that a regular map $\{4,4\}_{r,s}$ is determined by the non-negative integers r and s. Then there are three cases to consider:

(i) $r \neq 0$, $s = 0$: Then each of the pairs $(r, 0)$, $(0, r)$, $(-r, 0)$, $(0, -r)$ gives the same normal subgroup of index $4r^2$ having $t = r^2$ parabolic classes. Therefore we take these four pairs as identical. ($s \neq 0$, $r = 0$ case is similar).

(ii) r and s are different non-zero integers: Then the pairs (r, s), $(-r, s)$, $(r, -s)$ and $(-r, -s)$ give the same regular map $\{4,4\}_{r,s}$ and the pairs (s, r), $(-s, r)$, $(s, -r)$ and $(-s, -r)$ give the regular map $\{4,4\}_{s,r}$. Therefore there are two sets of identical pairs corresponding to two different normal subgroups.

(iii) $r = s \neq 0$: Then each of the four pairs (r, r), $(r, -r)$, $(-r, r)$ and $(-r, -r)$

gives the same regular map $\{4,4\}_{r,r}$, and therefore will be taken as identical pairs.

Example 5.1: **(1)** If $t = 1$, then we have four identical pairs (1,0), (-1,0), (0,1) and (0,-1) giving the regular map $\{4,4\}_{1,0}$. In this case the corresponding normal subgroup is denoted by $K = [4,4]_{1,0}$.

(2) Secondly let $t = 2$. Then the identical pairs are (1,1), (1,-1), (-1,1) and (-1,-1). They give the regular map $\{4,4\}_{1,1}$ and the corresponding normal subgroup is denoted by $H'(\sqrt{2}) = [4,4]_{1,1}$.

We can now prove our statement.

A normal subgroup of genus 1 of $H(\sqrt{2})$ has level 4: Indeed, to obtain a genus 1 normal subgroup N of $H(\sqrt{2})$, we map $H(\sqrt{2})$ into a finite quotient of (2,4,4) by a homomorphism. We also know that in a normal subgroup of (2,4,4) generated by r, s of orders 2 and 4, the parabolic element rs has exponent 4. Then the corresponding normal subgroup of $H(\sqrt{2})$ also has level 4 by Theorem 5.1. Therefore $\mu = 4t$. Then

$$4(r^2 + s^2) = 4t \tag{5.12}$$

and therefore

$$r^2 + s^2 = t. \tag{5.13}$$

Now for each pair satisfying (5.13) we have three more identical pairs. As each set of identical pairs gives us a normal subgroup N of $H(\sqrt{2})$ of genus 1, we obtain the following result:

Theorem 5.6: The number $N(\mu)$ of normal subgroups of genus 1 and index μ in $H(\sqrt{2})$ is

$$N(\mu) = N(4t) = \frac{1}{4}\#\left\{(r,s) : r,s \in \mathbf{Z},\, \mathrm{r}^2+\mathrm{s}^2=\mathrm{t}\right\}. \tag{5.14}$$

(5.14) shows that $N(\mu)$ is equal to a quarter of the number of representations of $t = \mu/4$ as the sum of two squares in $\mathbf{Z}$.

Remark 5.1: Kern–Isberner and Rosenberger proved the same result number theoretically by showing that $N(\mu)$ is a multiplicative function (see [Ke–Ro,1]).

We can now use some number theoretical results to calculate the number $N(\mu)$. We have already proved that $N(\mu)$ is equal to a quarter of the number of representations of $t = \mu/4$ as the sum of two integer squares. The following result will be useful in calculating $N(\mu)$ explicitly:

Lemma 5.1: ([Kn,1]) Let $t = 2^a \prod_b p_b{}^{l_b} . \prod_c q_c{}^{m_c}$ be the prime power decomposition of t, where the $p_b \equiv 1 \mod 4$ and the $q_c \equiv 3 \mod 4$. Then the number $r(t)$ of integer solutions of the Diophantine equation $x^2 + y^2 = t$ is given by $r(t) = 0$ if one of the m_c is odd, and by

$$r(t) = 4.\prod_b (l_b + 1) \tag{5.15}$$

if all m_c are even.

By means of Lemma 5.1, we can easily find $N(\mu)$ as

$$N(\mu) = \frac{1}{4}.r(t) \tag{5.16}$$

which is either 0 if there is, in the above prime power decomposition of t, a factor $q_c{}^{m_c}$ with $q_c \equiv 3 \mod 4$ and m_c is odd, or equal to $\prod_b (l_b + 1)$ otherwise.

Remark 5.2: The first few values of the function $N(\mu)$ are given in the following table. Note that if the index μ is not divisible by 4, then this number is 0.

t	1	2	3	4	5	6	7	8	9	10
μ	4	8	12	16	20	24	28	32	36	40
$N(\mu)$	1	1	0	1	2	0	0	1	1	2
t	11	12	13	14	15	16	17	18	19	20
μ	44	48	52	56	60	64	68	72	76	80
$N(\mu)$	0	0	2	0	0	1	2	1	0	2
t	...	25	...	65	...	325	...	625	...	1105
μ	...	100	...	260	...	1300	...	2500	...	4420
$N(\mu)$	...	3	...	4	...	6	...	5	...	8

Table 5.1: Some values of $N(\mu)$ for $q = 4$

(ii) $q = 6$:

Let us now calculate $N(\mu)$ for $H(\sqrt{3})$. The method we use is the same as the one for q =4. But this time we need to use the regular maps of type $\{6,3\}$ and $\{3,6\}$. However we must note an important difference between the two cases. In $q = 4$ case, as we can only map $H(\sqrt{2})$ to a finite quotient of the infinite triangle group (2,4,4) to get genus 1 normal subgroups, all of these subgroups were torsion-free. In $q = 6$ case, we can map to finite quotients of (2,6,3) and (2,3,6). Mapping to the former one gives torsion-free subgroups. However if we map $H(\sqrt{3})$ to the latter, then as the elliptic generator S, which is of order six in $H(\sqrt{3})$, goes to an element of order three under this homomorphism, the obtained normal subgroup will have some elements of order two implying that it has torsion. We will find the number of normal subgroups of genus 1 in both cases, i.e. for torsion and torsion-free normal subgroups. We shall see that there is a 1-1 correspondence between their numbers (as $\{6,3\}$ and $\{3,6\}$ are dual).

Let us now begin by recalling some facts about regular maps of genus 1 from Chapter 3. If a regular map corresponds to a normal subgroup of genus 1 of $H(\sqrt{3})$, then it must be of type $\{6,3\}$ or $\{3,6\}$. They are classified as $\{6,3\}_{r,s}$ and $\{3,6\}_{r,s}$ respectively for non–negative integers r and s. Also their automorphism groups have order $6(r^2+rs+s^2)$.

Now given the number $\mu = 6(r^2+rs+s^2)$, we want to find the number of normal subgroups of genus 1 in $\mathrm{H}(\sqrt{3})$ having index μ. Clearly for the other values of μ, $\mathrm{H}(\sqrt{3})$ has no normal subgroup of genus 1 with index μ as we have already seen.

Since $6 \,|\, \mu$, whenever one of $\{6,3\}_{r,s}$ and $\{3,6\}_{r,s}$ appears, the other one also appears. Therefore it is enough to find the number of normal subgroups $[6,3]_{r,s}$ for each given μ, as this is also the number of the normal subgroups $[3,6]_{r,s}$. Therefore the number of all genus 1 normal subgroups of $\mathrm{H}(\sqrt{3})$ is going to be twice that number. Now

$$\mu = 3t = 6(r^2+rs+s^2) \tag{5.17}$$

and hence

$$t = 2(r^2+rs+s^2) \tag{5.18}$$

and finally

$$r^2+rs+s^2-\frac{t}{2} = 0 \tag{5.19}$$

which is a quadratic equation of, say r, if we take s fixed (as the equation (5.18) is symmetric it does not matter which one of r and s is fixed). Solving this equation we have

$$r = -\frac{s}{2} \pm \frac{1}{2}\sqrt{2t-3s^2} \tag{5.20}$$

which are real only when $s^2 \leq 2t/3$. Therefore because of the symmetry, we have r (and s) bounded:

$$-\sqrt{\frac{2t}{3}} \leq r, s \leq \sqrt{\frac{2t}{3}}. \tag{5.21}$$

As μ is given t is also given. Therefore there are only finitely many solutions of (5.21). That is the solutions of (5.18) can be found by solving (5.21). Now similarly to the $q = 4$ case we find the number $N(\mu)$ of the normal subgroups $[6,3]_{r,s}$ of $\mathrm{H}(\sqrt{3})$ having genus 1 as

$$N_1(\mu) = \frac{1}{6}\#\left\{(r,s) \,:\, r, s \in \mathbf{Z},\, \mathrm{r}^2 + \mathrm{rs} + \mathrm{s}^2 = \frac{\mathrm{t}}{2}\right\}. \tag{5.22}$$

Therefore

Theorem 5.7: The number of all normal subgroups of genus 1 in $\mathrm{H}(\sqrt{3})$ having a given index μ is

$$N(\mu) = 2.N_1(\mu) = \frac{1}{3}\#\left\{(r,s) \,:\, r, s \in \mathbf{Z},\, \mathrm{r}^2 + \mathrm{rs} + \mathrm{s}^2 = \frac{\mathrm{t}}{2}\right\}. \tag{5.23}$$

The number $N_1(\mu)$ is the number of torsion (or torsion–free) normal subgroups of genus 1 of $\mathrm{H}(\sqrt{3})$ having index μ.

It is possible, as in $q = 4$ case, to calculate $N(\mu)$ more explicitly using the following result:

Lemma 5.2: ([Kn,1]) The number of solutions to $x^2 + xy + y^2 = k$ is $6E(k)$ where $E(k)$ is the number of divisors of k of the form $3a + 1$ subtracting the number of divisors of the form $3b + 2$.

Note that if $k = t/2 = \mu/6$, then we have

Corollary 5.1:

$$N_1(\mu) = E(k) \tag{5.24}$$

so that

$$N(\mu) = 2E(k). \tag{5.25}$$

Remark 5.3: The following table gives the first few values of the function $N(\mu)$ for $q = 6$:

t	2	4	6	8	10	12	14	16	18	20
$\mu = 3t$	6	12	18	24	30	36	42	48	54	60
$N(\mu)$	2	0	2	2	0	0	4	0	2	0
t	22	24	26	28	30	...	98	...	182	...
$\mu = 3t$	66	72	78	84	90	...	294	...	546	...
$N(\mu)$	0	2	4	0	0	...	6	...	8	...

Table 5.2: Some values of $N(\mu)$ for $q = 6$

Corollary 5.2: The number $N(\mu)$ of genus 1 normal subgroups of H($\sqrt{3}$) having a given index μ is always even.

Now we have calculated $N(\mu)$ for $q = 4$ and 6. It is then easy to generalise these to any $q \geq 3$. Recall that, by Theorem 5.2, H(λ_q) has a normal subgroup of genus 1 if and only if $q \equiv 0 \; mod 3$ or $q \equiv 0 \; mod 4$. Also recall the homomorphism of H($\sqrt{2}$) to a finite quotient of the infinite triangle group (2,4,4), giving genus 1 normal subgroups. This homomorphism, in general, exists as a homomorphism of H(λ_q) when q is divisible by four. When q is divisible by 3 or 6, we can obtain similar results. By means of all these we now obtain the following generalisation:

Theorem 5.8: The number of normal genus 1 subgroups of H(λ_q) having index μ is

$$N(\mu) = \begin{cases} 0 & \text{if } (q,12) = 1 \text{ or } 2 \\ \beta/2 & \text{if } 3 \mid q,\ q \text{ odd and } \mu = 3t_2 \\ 0 & \text{if } 3 \mid q,\ q \text{ odd and } \mu \neq 3t_2 \\ \alpha & \text{if } 4 \mid q,\ 3 \nmid q \text{ and } \mu = 4t_1 \\ 0 & \text{if } 4 \mid q,\ 3 \nmid q \text{ and } \mu \neq 4t_1 \\ \beta & \text{if } 6 \mid q,\ 4 \nmid q \text{ and } \mu = 3t_2 \\ 0 & \text{if } 6 \mid q,\ 4 \nmid q \text{ and } \mu \neq 3t_2 \\ \alpha + \beta & \text{if } 12 \mid q \text{ and } \mu = 3t_2 = 4t_1 \\ \alpha & \text{if } 12 \mid q \text{ and } \mu = 3t_2 \neq 4t_1 \\ \beta & \text{if } 12 \mid q \text{ and } \mu = 4t_1 \neq 3t_2 \\ 0 & \text{if } 12 \mid q \text{ and } 3t_2 \neq \mu \neq 4t_1 \end{cases} \qquad (5.26)$$

where t_1 and t_2 are such that $t_1 = r_1^2 + s_1^2$ and $t_2 = 2(r_2^2 + r_2 s_2 + s_2^2)$ and also

$$\alpha = \frac{1}{4} \# \left\{ (r_1, s_1) \ :\ r_1, s_1 \in \mathbf{Z},\ r_1^2 + s_1^2 = t_1 \right\} \qquad (5.27)$$

and

$$\beta = \frac{1}{3} \# \left\{ (r_2, s_2) \ :\ r_2, s_2 \in \mathbf{Z},\ r_2^2 + r_2 s_2 + s_2^2 = \frac{t_2}{2} \right\}. \qquad (5.28)$$

Example 5.2: **(i)** Let $q = 20$. As $4 \mid q$ and $3 \nmid q$, the total number of genus 1 normal subgroups in $H(\lambda_{20})$ is either α or 0. A few values of $N(\mu)$ are given in the following table:

μ	1	2	3	4	5	6	7	8	9	10
$N(\mu)$	0	0	0	1	0	0	0	1	0	0
μ	11	12	13	14	15	16	17	18	19	20
$N(\mu)$	0	0	0	0	0	1	0	0	0	2

Table 5.3

Therefore $H(\lambda_{20})$ has no genus 1 normal subgroup of index 12, for example, but it has two such subgroups, $[4,4]_{1,2}$ and $[4,4]_{2,1}$, of index 20.

(ii) Let $q = 84$. As $12 \mid q$, the total number of genus 1 normal subgroups is either 0, α, β or $\alpha + \beta$. Again the first few values of $N(\mu)$ are given in the following table:

μ	1	2	3	4	5	6	7	8	9	10
$N(\mu)$	0	0	0	1	0	2	0	1	0	0
μ	11	12	13	14	15	16	17	18	19	20
$N(\mu)$	0	0	0	0	0	1	0	2	0	2
μ	21	22	23	24	25	26	27	28	29	30
$N(\mu)$	0	0	0	2	0	0	0	0	0	0

Table 5.4

Chapter 6

NORMAL SUBGROUPS OF $H(\lambda_q)$ FOR ODD q

6.0. INTRODUCTION

In the earlier chapters, we have sometimes noted some important differences between the odd and even q cases. For example, if q is even, then $H(\lambda_q)$ has infinitely many normal subgroups of genus 0 of finite index which is not true when q is odd (including the modular group case). Similarly if q is even, then $H(\lambda_q)$ has infinitely many normal subgroups of finite index with torsion which is again not possible in the odd q case. There are many other examples like these that we have already noticed or we shall notice.

As two of the most important Hecke groups are obtained for $q = 4$ and 6, we shall deal with even q case mainly in Chapters 8 and 9 where we discuss the normal subgroups of $H(\sqrt{2})$ and $H(\sqrt{3})$ and also we shall make generalizations of these two cases to any even q.

In this chapter, we discuss some classes of normal subgroups of $H(\lambda_q)$ for odd q.

As $q = 5$ gives one of the important Hecke groups, we shall deal with it in Chapter 10 separately. But, of course, all the results in this chapter also apply to $H(\lambda_5)$ as well as to the modular group $\Gamma = H(\lambda_3)$.

We begin with the power subgroups of $H(\lambda_q)$. The *m–th power subgroup* $H^m(\lambda_q)$ *of* $H(\lambda_q)$ is the group generated by the m–th powers of the elements of $H(\lambda_q)$. The power subgroups of the modular group $\Gamma = H(\lambda_3)$ have been studied and classified in [Ne,1], [Ne,4] by Newman. In fact, it is a well–known and important result that the only normal subgroups of Γ containing torsion are Γ, Γ^2, and Γ^3 of indices 1,2,3 respectively. Here we show that this nicely generalizes to the Hecke groups $H(\lambda_p)$ with p prime. We specially discuss $H^2(\lambda_q)$ and $H^q(\lambda_q)$ as they are nicely related to $H(\lambda_q)$ and its commutator subgroup $H'(\lambda_q)$. Then we give a classification theorem for these power subgroups.

In the second part of this chapter, we discuss free normal subgroups of finite index in $H(\lambda_p)$, p prime.

If p is prime, then we shall show in Chapter 7 that we can find infinitely many homomorphisms from $H(\lambda_q)$ to PSL groups. So $H(\lambda_p)$ has infinitely many normal subgroups. If q is non–prime, then there exists a homomorphism from $H(\lambda_q)$ to $H(\lambda_p)$ where $p|q$ (p prime). Therefore $H(\lambda_q)$ has infinitely many normal subgroups for all q.

6.1. POWER SUBGROUPS OF $H(\lambda_q)$ FOR ODD q

Let $q \geq 3$ be an odd integer and let $m \in N$. The *m–th power subgroup* of $H(\lambda_q)$ is defined to be the subgroup generated by the m–th powers of all elements of $H(\lambda_q)$. As fully invariant subgroups, they are normal in $H(\lambda_q)$.

In this section we investigate these subgroups and also give some relations between them, $H(\lambda_q)$ and the commutator subgroup $H'(\lambda_q)$. We shall prove that $H(\lambda_q)$

is the product of $H^2(\lambda_q)$ and $H^q(\lambda_q)$ and that the intersection of these two subgroups is $H'(\lambda_q)$. Therefore $H^2(\lambda_q)$ and $H^q(\lambda_q)$ will be two important power subgroups.

From the definition it follows that

$$H^m(\lambda_q) > H^{mn}(\lambda_q) \tag{6.1}$$

and that

$$(H^m(\lambda_q))^n > H^{mn}(\lambda_q). \tag{6.2}$$

The last two inequalities imply that

$$H^m(\lambda_q).H^n(\lambda_q) = H^{(m,n)}(\lambda_q), \tag{6.3}$$

where $m, n \in \mathbf{N}$ and (m,n) denotes the greatest common divisor of m and n. Indeed, first note that the product is well-defined as power subgroups are normal subgroups. By (6.1) we have

$$H^{(m,n)}(\lambda_q) \geq H^m(\lambda_q) \tag{6.4}$$

and

$$H^{(m,n)}(\lambda_q) \geq H^n(\lambda_q) \tag{6.5}$$

so that

$$H^{(m,n)}(\lambda_q) \geq H^m(\lambda_q).H^n(\lambda_q). \tag{6.6}$$

Let now z be any element of $H(\lambda_q)$. Let us choose integers m_1, n_1 such that $m_1 m + n_1 n = (m,n)$. Then

$$z^{m_1 m} \in H^m(\lambda_q), \quad z^{n_1 n} \in H^n(\lambda_q) \tag{6.7}$$

and hence

$$z^{m_1 m+n_1 n} \in H^m(\lambda_q).H^n(\lambda_q). \tag{6.8}$$

That is

$$z^{(m,n)} \in H^m(\lambda_q).H^n(\lambda_q) \tag{6.9}$$

and therefore

$$H^{(m,n)}(\lambda_q) \leq H^m(\lambda_q).H^n(\lambda_q). \tag{6.10}$$

Therefore we have

$$H^{(m,n)}(\lambda_q) = H^m(\lambda_q).H^n(\lambda_q). \tag{6.11}$$

Particularly

$$H(\lambda_q) = H^2(\lambda_q).H^q(\lambda_q) \tag{6.12}$$

as q is odd.

Let us now discuss the group theoretical structures of the power subgroups. The proofs are just generalizations of the proofs in [Ne,1]. First we have

Theorem 6.1: The normal subgroup $H^2(\lambda_q)$ is the free product of two finite cyclic groups of order q. Also

$$| H(\lambda_q) : H^2(\lambda_q) | = 2, \tag{6.13}$$

$$H(\lambda_q) = H^2(\lambda_q) \cup RH^2(\lambda_q), \tag{6.14}$$

and

$$H^2(\lambda_q) = < S > \star < RSR > . \tag{6.15}$$

The elements of $H^2(\lambda_q)$ are characterised by the property that the sum of the exponents of R is even.

Proof: Set $K = \langle S, RSR \rangle$. Then clearly K is normal in $H(\lambda_q)$. Since the elements of K satisfy the requirements of the theorem, i.e. since the sum of the exponents of R is even, we find that $K \leq H^2(\lambda_q)$.

Let now z be any element of $H(\lambda_q)$. Then we can write

$$z = S^{c_1} R S^{c_2} R \ldots S^{c_n} R S^{c_{n+1}} \tag{6.16}$$

where the c_i's are integers some of which, but not all, may be zero. Thus

$$z = S^{c_1} (RSR)^{c_2} S^{c_3} \ldots (RSR)^{c_n} S^{c_{n+1}} \quad \textit{if n is even}, \tag{6.17}$$

and

$$z = S^{c_1} (RSR)^{c_2} S^{c_3} \ldots S^{c_n} (RSR)^{c_{n+1}} R \quad \textit{if n is odd}. \tag{6.18}$$

Hence either $z \in K$ or $zR \in K$. Since R is not in K, we find

$$\begin{aligned} H(\lambda_q) &= K \cup K.R \\ &= K \cup R.K. \end{aligned} \tag{6.19}$$

Now $H(\lambda_q) \geq H^2(\lambda_q) \geq K$ and $| H(\lambda_q) : K | = 2$ which altogether imply that $|H^2(\lambda_q) : K| = 1$ or 2. But as R is odd, it cannot be a square as all squares are even elements. Therefore R is not in $H^2(\lambda_q)$. Hence $H(\lambda_q) \neq H^2(\lambda_q)$ which implies (6.13), that is

$$K = H^2(\lambda_q). \tag{6.20}$$

That S and RSR generate $H^2(\lambda_q)$ can be seen by the Reidemeister–Schreier method.

Let us now consider the homomorphism

$$H(\lambda_q) \longrightarrow H(\lambda_q)/H^2(\lambda_q) \cong C_2. \tag{6.21}$$

Here R is mapped to an element of order two and S is mapped to the identity. Hence T is mapped to an element of order two. Then the permutation method and Riemann–Hurwitz formula together give the signature of $\mathrm{H}^2(\lambda_q)$ as $(0\ ;\ q, q, \infty)$, that is, $\mathrm{H}^2(\lambda_q)$ is isomorphic to the free product of two finite cyclic groups of order q.

We now have

Theorem 6.2: The normal subgroup $\mathrm{H}^q(\lambda_q)$ is isomorphic to the free product of q finite cyclic groups of order two. Also

$$|\, H(\lambda_q) : H^q(\lambda_q)\,| = q, \tag{6.22}$$

$$H(\lambda_q) = H^q(\lambda_q) \cup SH^q(\lambda_q) \cup \ldots \cup S^{q-1}H^q(\lambda_q), \tag{6.23}$$

and

$$H^q(\lambda_q) = < R > \star < SRS^{q-1} > \star < S^2RS^{q-2} > \star \ldots \star < S^{q-1}RS > . \tag{6.24}$$

The elements of $\mathrm{H}^q(\lambda_q)$ can be characterised by the requirement that the sum of the exponents of S is divisible by q.

Proof: Set $L = \langle R, SRS^{q-1}, S^2RS^{q-2}, \ldots, S^{q-1}RS\rangle$. Being closed under conjugation by the generators R and S, L is normal in $\mathrm{H}(\lambda_q)$. The elements of L satisfy the requirements of Theorem 6.2, i.e. the sum of the exponents of S for each element of L is a multiple of q. Hence $L \leq \mathrm{H}^q(\lambda_q)$.

Let now w_n be any word of the form

$$w_n = S^{c_1}RS^{c_2}R\ldots S^{c_n}R. \tag{6.25}$$

As

$$S^{c_1}R = S^{c_1}RS^{2c_1}S^{-2c_1} \tag{6.26}$$

we have

$$w_n = S^{c_1}RS^{2c_1}.w_{n-1} \tag{6.27}$$

where $w_{n-1} = S^{c_2-2c_1}R\ldots S^{c_n}R$. But

$$S^{c_1}RS^{2c_1} = R,\ SRS^{q-1},\ S^2RS^{q-2},\ \ldots,\ S^{q-1}RS. \tag{6.28}$$

This implies, by induction on n, that

$$w_n = k.S^{c_0} \tag{6.29}$$

where $k \in L$ and c_0 is any integer. Hence for any z given by (6.16) we have

$$\begin{aligned} z &= w_n.S^{c_{n+1}} \\ &= k.S^c \end{aligned} \tag{6.30}$$

where c is some integer. Since no non-trivial power of S belongs to L, this implies

$$\begin{aligned} \mathrm{H}(\lambda_q) &= \textstyle\sum_{i=0}^{q-1} L.S^i \\ &= \textstyle\sum_{i=0}^{q-1} S^i.L. \end{aligned} \tag{6.31}$$

Now we have $\mathrm{H}(\lambda_q) \geq \mathrm{H}^q(\lambda_q) \geq L$ and also $|\ \mathrm{H}(\lambda_q) : L\,| = q$. Therefore

$$|\,H(\lambda_q) : H^q(\lambda_q)\,| = d \tag{6.32}$$

where $d\,|\,q$. Here d cannot be 1 since S is not in $\mathrm{H}^q(\lambda_q)$. In $\mathrm{H}(\lambda_q)/\mathrm{H}^q(\lambda_q)$, we have the relations

$$r^2 = s^q = (rs)^q = I \tag{6.33}$$

where r and s are the images, in $\mathrm{H}(\lambda_q)/\mathrm{H}^q(\lambda_q)$, of R and S, respectively. Therefore $q\,|\,d$. As also $d\,|\,q$, we find $d = q$. Hence (6.22) is true. Therefore $L = \mathrm{H}^q(\lambda_q)$.

Now consider the homomorphism

$$H(\lambda_q) \longrightarrow H(\lambda_q)/H^q(\lambda_q) \cong C_q. \tag{6.34}$$

Here R is mapped to the identity and S is mapped to an element of order q. Hence T is mapped to an element of order q as well. Therefore

$$H^q(\lambda_q) \cong \left(0\ ;\ 2^{(q)}, \infty\right) \tag{6.35}$$

which is the required result.

Using the results above, we obtain the following theorem:

Theorem 6.3: Let p be an odd prime. The subgroups $\mathrm{H}^m(\lambda_p)$ satisfy the following:

$$H^m(\lambda_p) = \begin{cases} \mathrm{H}(\lambda_p) & \text{if } (m, 2p) = 1 \\ \mathrm{H}^2(\lambda_p) & \text{if } m \text{ is even and } (m,p) = 1 \\ \mathrm{H}^p(\lambda_p) & \text{if } m \text{ is an odd multiple of } p \end{cases} \tag{6.36}$$

Proof: When $(m, 2p) = 1$, $\mathrm{H}(\lambda_p)/\mathrm{H}^m(\lambda_p)$ is trivial and hence $\mathrm{H}^m(\lambda_p) = \mathrm{H}(\lambda_p)$.

Secondly let m be even and $(m,p) = 1$. Then in the quotient group $\mathrm{H}(\lambda_p)/\mathrm{H}^m(\lambda_p)$ we have the relations $r^2 = s = I$ and therefore this quotient is isomorphic to the cyclic group C_2. Now by the permutation method and Riemann–Hurwitz formula, $\mathrm{H}^m(\lambda_p)$ has the signature $(0\ ;\ p, p, \infty)$ implying $\mathrm{H}^m(\lambda_p) = \mathrm{H}^2(\lambda_p)$, as there exists a unique normal subgroup of $\mathrm{H}(\lambda_q)$ with index two when q is odd.

Thirdly, suppose that m is an odd multiple of p. Then similarly the quotient is isomorphic to C_p and $\mathrm{H}^m(\lambda_p)$ has the signature $(0\ ;\ 2^{(p)}, \infty)$. Again as there is a unique normal subgroup of index q in $\mathrm{H}(\lambda_q)$ when q is odd, we have $\mathrm{H}^m(\lambda_p) = \mathrm{H}^p(\lambda_p)$.

Remarks 6.1. Because of Theorem 6.3, we have left only the subgroups $\mathrm{H}^{2pm}(\lambda_p)$, $m \in \mathrm{N}$ to consider. This will be done after a discussion of the commutator subgroup $\mathrm{H}'(\lambda_q)$ of $\mathrm{H}(\lambda_q)$.

Let now $q > 3$ be a composite odd number. Then Theorem 6.3 is again satisfied, but does not cover all cases. For example the subgroups $\mathrm{H}^{2qm}(\lambda_q)$ are again left to consider as in the case of an odd prime p. Moreover, there are some other classes of these subgroups which need to be dealt with. For example, if m is odd such that $1 < (m, q) = d < q$, then in the quotient group $\mathrm{H}(\lambda_q)/\mathrm{H}^m(\lambda_q)$ we have the relations $r = s^d = 1$, that is, $\mathrm{H}(\lambda_q)/\mathrm{H}^m(\lambda_q) \cong C_d$. Then we obtain

$$H^m(\lambda_q) = (0\ ;\ 2^{(d)}, q/d, \infty). \tag{6.37}$$

Recall that in Chapter 4, we discussed a class of normal genus 0 subgroups of $\mathrm{H}(\lambda_q)$, denoted by $Y_d(\lambda_q)$ with the signature (6.37). Therefore in this case $\mathrm{H}^m(\lambda_q) = Y_d(\lambda_q)$.

Finally, if m is even such that $1 < (m, q) = d < q$, then in the quotient group $\mathrm{H}(\lambda_q)/\mathrm{H}^m(\lambda_q)$ we have the relations $r^2 = s^d = (rs)^m = 1$. Therefore the above techniques do not say much about $\mathrm{H}^m(\lambda_q)$ in this case apart from the fact that they are all normal subgroups with torsion.

We now discuss the commutator subgroup $\mathrm{H}'(\lambda_q)$ of $\mathrm{H}(\lambda_q)$:

Lemma 6.1: The commutator subgroup $\mathrm{H}'(\lambda_q)$ of $\mathrm{H}(\lambda_q)$ is isomorphic to a free group of rank $q-1$. Also

$$|\, H(\lambda_q) : H'(\lambda_q) \,| = 2q, \tag{6.38}$$

$$H(\lambda_q) = \sum_{i=0}^{2q-1} T^i.H'(\lambda_q) \tag{6.39}$$

and

$$H'(\lambda_q) = < SRS^{q-1}R > \star < S^2RS^{q-2}R > \star \ldots \star < S^{q-1}RSR > . \tag{6.40}$$

Let

$$a_1 = SRS^{q-1}R, a_2 = S^2RS^{q-2}R, \ldots, a_{q-1} = S^{q-1}RSR. \tag{6.41}$$

Note that since q is odd the quotient groups $\mathrm{H}(\lambda_q)/\mathrm{H}^2(\lambda_q)$ and $\mathrm{H}(\lambda_q)/\mathrm{H}^q(\lambda_q)$ are cyclic and therefore abelian so that

$$H^2(\lambda_q) > H'(\lambda_q), \quad H^q(\lambda_q) > H'(\lambda_q). \tag{6.42}$$

Hence

$$H^2(\lambda_q) \cap H^q(\lambda_q) > H'(\lambda_q). \tag{6.43}$$

Since $\mathrm{H}^2(\lambda_q)$ and $\mathrm{H}^q(\lambda_q)$ are normal subgroups of $\mathrm{H}(\lambda_q)$ we have, by one of the isomorphism theorems, that

$$H^2(\lambda_q)H^q(\lambda_q)/H^q(\lambda_q) \cong H^2(\lambda_q)/\left(H^2(\lambda_q) \cap H^q(\lambda_q)\right). \tag{6.44}$$

As $\mathrm{H}^2(\lambda_q)\mathrm{H}^q(\lambda_q) \cong \mathrm{H}(\lambda_q)$, we have

$$| H^2(\lambda_q) : \left(H^2(\lambda_q) \cap H^q(\lambda_q)\right) | = q. \tag{6.45}$$

Then

$$| H(\lambda_q) : \left(H^2(\lambda_q) \cap H^q(\lambda_q)\right) | = 2q. \tag{6.46}$$

Now we have

$$H(\lambda_q) > H^2(\lambda_q) \cap H^q(\lambda_q) > H'(\lambda_q) \tag{6.47}$$

and

$$|H(\lambda_q) : H'(\lambda_q)| = |H(\lambda_q) : \left(H^2(\lambda_q) \cap H^q(\lambda_q)\right)| = 2q. \tag{6.48}$$

These together imply the following result:

Theorem 6.4: The commutator subgroup $H'(\lambda_q)$ of $H(\lambda_q)$ satisfies

$$H'(\lambda_q) = H^2(\lambda_q) \cap H^q(\lambda_q). \tag{6.49}$$

By means of this result, we are going to be able to investigate the subgroups $H^{2qm}(\lambda_q)$. As $H^2(\lambda_q) > H^{2q}(\lambda_q)$ and $H^q(\lambda_q) > H^{2q}(\lambda_q)$, (6.49) implies that

$$H'(\lambda_q) > H^{2q}(\lambda_q). \tag{6.50}$$

As $H'(\lambda_q)$ is a free group, we can conclude that $H^{2q}(\lambda_q)$ is also a free group. Moreover (6.1) implies that

$$H^{2q}(\lambda_q) > H^{2qm}(\lambda_q). \tag{6.51}$$

for $m \in \mathbf{N}$. Therefore we have

Theorem 6.5: The subgroups $H^{2qm}(\lambda_q)$ are free.

6.2 FREE NORMAL SUBGROUPS OF H(λ_p) FOR PRIME p

As H(λ_q) is the free product of two finite cyclic groups of orders two and q, it has, by the Kurosh subgroup theorem, or by considering signatures, two kinds of normal subgroups: Free ones and free products of some infinite cyclic groups with some cyclic groups of order two and order d where $d \mid q$. Therefore the study of free normal subgroups and their group theoretical structures will be important to us. They have already been discussed briefly in Chapter 4 in connection with the normal genus 0 subgroups. Here we discuss them for prime p. This has been done for $p = 3$ by Newman in [Ne,1]. His results can be generalized to prime p case. When q is a composite odd number, it is possible to obtain similar results, however, it looks difficult to find all normal free subgroups in this case.

First we have

Theorem 6.6: Let p be an odd prime. If N is a non-trivial non-free normal subgroup of H(λ_p), then N is one of

$$H(\lambda_p), H^2(\lambda_p) \text{ or } H^p(\lambda_p). \tag{6.52}$$

The proof of Theorem 6.6 depends on the following two lemmas:

Lemma 6.2: Let N be a non-trivial normal subgroup of H(λ_p). Then N is free if and only if it contains no elements of finite order.

Proof: Suppose N contains no element of finite order. Now by the Kurosh subgroup theorem

$$N \cong F \star \prod{}_{\star} B_\beta \tag{6.53}$$

where F is either free or $\{I\}$ and each B_β is conjugate to either $\{R\}$ or $\{S\}$. As N has no elements of finite order the product $\prod_\star B_\beta$ is vacuous and also as N is non–trivial, N must be free.

Conversely, if N is free, then by definition, it contains no elements of finite order.

We also have

Lemma 6.3: The only normal subgroups of $\mathrm{H}(\lambda_p)$ containing elements of finite order are

$$H(\lambda_p), H^2(\lambda_p) \text{ and } H^p(\lambda_p) \tag{6.54}$$

Proof: Let N be a normal subgroup of $\mathrm{H}(\lambda_p)$ containing an element of finite order. Then N contains an element of order two or an element of order p, as p is prime. An element of order two in N is conjugate to R as p is odd and an element of order p is conjugate to a power of S. Therefore if a normal subgroup N contains an element of finite order, then it contains R or S or both. Therefore we have three cases:

(i) If N contains both R and S then $N = \mathrm{H}(\lambda_p)$.

(ii) If N contains S but not R, then $\mathrm{H}(\lambda_p)/N$ is isomorphic to C_2 as we have the relations $r^2 = s = 1$. Then by the permutation method and Riemann–Hurwitz formula we have $N = \mathrm{H}^2(\lambda_p)$.

(iii) If N contains R but not S, then $\mathrm{H}(\lambda_p)/N$ is isomorphic to C_p as, this time, we have the relations $r = s^p = 1$. Similarly $N = \mathrm{H}^p(\lambda_p)$.

The proof of Theorem 6.6 is now a direct result of Lemmas 6.2 and 6.3.

We finally have

Theorem 6.7: Let q be odd. Let N be a free normal subgroup of $\mathrm{H}(\lambda_q)$ with

$$|\,H(\lambda_q) : N\,| = \mu < \infty. \tag{6.55}$$

Then

$$2q \mid \mu. \tag{6.56}$$

Proof: The quotient group must contain elements of order 2 and q, so its order is divisible by $2q$.

Chapter 7

PRINCIPAL CONGRUENCE SUBGROUPS OF THE HECKE GROUPS H(λ_q)

7.0. INTRODUCTION

Perhaps the most interesting normal subgroups of the modular group Γ are the principal congruence subgroups. In this chapter we define these subgroups in general for any Hecke group H(λ_q). Then we find the quotients of H(λ_q) by them and finally we determine their group theoretical structure. Most of them are free groups. We shall see that these subgroups are important and interesting in the case of Hecke groups as they are in the modular group case.

In this chapter the principal congruence subgroups of H(λ_q) will be discussed for several values of q. The modular group case where $q = 3$ has been investigated for a long time, so we shall largely ignore this case. We begin with the next two interesting examples $q = 4$ and 6. There is some work done on the congruence subgroups of these two groups, see [Pa,1] and [Pa,2]. Our next case will be $q = 5$ as in this case we have the icosahedral group A_5 as a quotient group of H(λ_5) giving a torsion free principal congruence subgroup. As we shall see, this is not possible for the other values of $q > 3$. Than we shall discuss the case where q is a prime > 5. Again $q = 7$ case will be significant and different from others, and therefore will be dealt with seperately. Indeed in this special case, with only one exception, all quotient groups of $\mathrm{H}(\lambda_7)$ with the principal congruence subgroups are Hurwitz groups — i.e. the groups of $84(g-1)$ automorphisms on a Riemann surface of genus g. We shall also prove that $\mathrm{H}(\lambda_q)$ has in fact infinitely many normal subgroups.

In each case we shall find the quotient group of $\mathrm{H}(\lambda_q)$ by the principal congruence subgroup and then determine the group theoretical structure of the normal subgroup. Our main tool will be [Ma,1]. We shall recall some results from this work, which will be used in determining the required quotient groups.

Recall that Hecke groups $\mathrm{H}(\lambda_q)$ are triangle groups with a parabolic element T. We say a subgroup N of $\mathrm{H}(\lambda_q)$ is *of level* n if T^n belongs to N and n is the least positive integer with this property. It is known that $\mu = n.t$ where t denotes the parabolic class number of N and $\mu = [\mathrm{H}(\lambda_q) : N]$ (see Section 0.4).

Let us now begin with the modular group:

A complete classification of the normal congruence subgroups of the modular group Γ is given by Newman [Ne,7] and Mc Quillan [MQ,1]. The *principal congruence subgroup of level* n of Γ is defined by

$$\Gamma(n) = \left\{ T(z) = \frac{az+b}{cz+d} \in \Gamma \,:\, a \equiv d \equiv \pm 1,\, b \equiv c \equiv 0 \,(mod\, n) \right\}. \qquad (7.1)$$

A subgroup of Γ containing a principal congruence subgroup $\Gamma(n)$ is called a *congruence subgroup of level n.*

$\Gamma(n)$ is a normal subgroup of Γ. But in general, not all congruence subgroups are normal in Γ.

Another way of obtaining $\Gamma(n)$ is to consider the "*reduction homomorphism*" which reduces everything *modulo n*. Then $\Gamma(n)$ can be obtained as the kernel of this homomorphism. (This will be discussed in detail for all q in this chapter).

In [Pa,1], the principal congruence subgroup of level p of H$(\sqrt{m})$, p prime, m =2,3, is defined by

$$\Gamma_p(\sqrt{m}) = \left\{M \in H(\sqrt{m}) \ : \ M \equiv \pm I \ (mod\ p)\right\}. \tag{7.2}$$

This is equivalent to

$$\Gamma_p(\sqrt{m}) = \left\{T(z) = \frac{az + b\sqrt{m}}{c\sqrt{m}z + d} \ : \ a \equiv d \equiv \pm 1,\ b \equiv c \equiv 0\ (mod\ p),\ ad - mbc = 1\right\}. \tag{7.3}$$

See [Pa,2].

In general for any $q \in \mathbf{N}$, $q \geq 3$, we can define the *principal congruence subgroup of level p*, p prime, of H(λ_q) by

$$\begin{aligned} \Gamma_p(\lambda_q) &= \{T \in H(\lambda_q) \ : \ T \equiv \pm I \ (mod\ p)\}. \\ &= \left\{\begin{pmatrix} a & \lambda b \\ \lambda c & d \end{pmatrix} \ : \ a \equiv d \equiv \pm 1,\ b \equiv c \equiv 0\ (mod\ p),\ ad - \lambda^2 bc = 1\right\}. \end{aligned} \tag{7.4}$$

$\Gamma_p(\lambda_q)$ is always a normal subgroup of H(λ_q).

Let us once more consider the "reduction homomorphism" *modulo p*, p prime. In the modular group case we noted that the kernel of this homomorphism is $\Gamma(p)$–the principal congruence subgroup of level p of Γ. We shall see that the situation for Hecke groups H(λ_q) with $q > 3$ is more complex as there is not usually a unique way of defining the reduction homomorphism.

Let $\wp$ be an ideal of $\mathbf{Z}[\lambda_q]$. Then the natural map

$$\Theta_\wp \ : \ \mathbf{Z}[\lambda_q] \longrightarrow \mathbf{Z}[\lambda_q]/\wp \tag{7.5}$$

induces a map

$$H(\lambda_q) \longrightarrow PSL(2, \mathbf{Z}[\lambda_q]/\wp) \tag{7.6}$$

whose kernel is going to be called the principal congruence subgroup of level $\wp$.

Let now s be an integer such that $P_q^*(\lambda_q)$ has solutions in $GF(p^s)$. We know that such an s exists and satisfies $1 \le s \le d = deg\, P_q^*(\lambda_q)$. Let u be a solution of $P_q^*(\lambda_q)$ in $GF(p^s)$. Let us take $\wp$ to be the ideal generated by u in $\mathbf{Z}[\lambda_q]$. As above, we can define

$$\Theta_{p,u,q} \; : \; H(\lambda_q) \longrightarrow PSL(2, p^s) \tag{7.7}$$

as the homomorphism induced by $\lambda_q \mapsto u$. Let

$$K_{p,u}(\lambda_q) \; := \; Ker(\Theta_{p,u,q}). \tag{7.8}$$

As the kernel of a homomorphism of $H(\lambda_q)$, $K_{p,u}(\lambda_q)$ is normal in $H(\lambda_q)$.

Given p, as $K_{p,u}(\lambda_q)$ depends on p and u, we have a chance of having a different kernel for each root u. However sometimes they do coincide:

Lemma 7.1: If u, v correspond to the same irreducible factor f of $P_q^*(\lambda_q)$ over $GF(p)$, then $K_{p,u}(\lambda_q) = K_{p,v}(\lambda_q)$.

Proof: Note that $A \in K_{p,u}(\lambda_q)$ if and only if $A = \pm \begin{pmatrix} 1 + g(\lambda_q) & h(\lambda_q) \\ k(\lambda_q) & 1 + l(\lambda_q) \end{pmatrix}$ with $g(u) = h(u) = k(u) = l(u) = 0$ in $GF(p^s)$. Therefore as f is irreducible, (g, f)=1 or f. If it is 1, then there are polynomials a and b such that $ag + bf = 1$. But $f(u) = g(u) = 0$. Therefore $(g, f) = f$ and g is a multiple of f. Similarly h, k and l are all multiples of f. As v is another root of the same factor of $P_q^*(\lambda_q)$, $g(v) = h(v) = k(v) = l(v) = 0$ in $GF(p^s)$,i.e. $A \in K_{p,v}(\lambda_q)$.

Even when u, v give different factors of $P_q^*(\lambda_q)$, we may have $K_{p,u}(\lambda_q) = K_{p,v}(\lambda_q)$. As an example of this situation we have the following:

In Example 7.1, we shall find odd elements $A = \begin{pmatrix} 5\sqrt{2} & 7 \\ 7 & 5\sqrt{2} \end{pmatrix}$ and $B = \begin{pmatrix} 2\sqrt{2} & 7 \\ 21 & 37\sqrt{2} \end{pmatrix}$ in $K_{7,3}(\sqrt{2})$ - $\Gamma_7(\sqrt{2})$ and $K_{7,4}(\sqrt{2})$ - $\Gamma_7(\sqrt{2})$ respectively for the two roots of $P_4^*(\sqrt{2})$ *mod 7*. But

$$AB^{-1} = \begin{pmatrix} 5\sqrt{2} & 7 \\ 7 & 5\sqrt{2} \end{pmatrix} \cdot \begin{pmatrix} 37\sqrt{2} & -7 \\ -21 & 2\sqrt{2} \end{pmatrix} \equiv -I \ mod\, 7. \tag{7.9}$$

i.e.

$$A.\Gamma_7(\sqrt{2}) = B.\Gamma_7(\sqrt{2}), \tag{7.10}$$

so that

$$K_{7,3}(\sqrt{2}) = K_{7,4}(\sqrt{2}). \tag{7.11}$$

We now have

Theorem 7.1: $K_{p,u}(\lambda_q)$ is a normal congruence subgroup of level p of $\mathrm{H}(\lambda_q)$, i.e.

$$\Gamma_p(\lambda_q) \trianglelefteq K_{p,u}(\lambda_q). \tag{7.12}$$

Therefore

$$\Gamma_p(\lambda_q) \leq \bigcap_{all\ u} K_{p,u}(\lambda_q). \tag{7.13}$$

Proof: Before starting the proof, we want to recall a way of obtaining group homomorphisms from ring homomorphisms.

Let R and S be two rings with identity. Let

$$\psi : R \longrightarrow S \tag{7.14}$$

be a ring homomorphism. Then ψ induces a group homomorphism

$$\overline{\psi} : SL(2,R) \longrightarrow SL(2,S). \tag{7.15}$$

Similarly since $PSL(2,R)$ is obtained from $SL(2,R)$ by factoring out the center, which is $\pm I$, another group homomorphism

$$\underline{\psi} : PSL(2,R) \longrightarrow PSL(2,S) \tag{7.16}$$

is induced by the same ψ.

This general idea of obtaining group homomorphisms from ring homomorphisms can be applied to Hecke groups $\mathrm{H}(\lambda_q)$ in the following way: Consider $\mathbf{Z}[\lambda_q]$ which is just an extension of the ring of integers by the algebraic number λ_q. If we reduce all elements in this ring modulo p, for a prime p, we obtain a ring homomorphism

$$\varphi_p : \mathbf{Z}[\lambda_q] \longrightarrow \mathbf{Z_p}[\lambda_q] \tag{7.17}$$

which reduces the elements of $\mathbf{Z}[\lambda_q]$ *modulo p*. Now for each root, if there are any, $u \in GF(p)$ of $P_q^*(\lambda_q)$, there is a ring homomorphism

$$\chi_u : \mathbf{Z_p}[\lambda_q] \longrightarrow \mathbf{Z_p} = \mathrm{GF(p)} \tag{7.18}$$

taking λ_q to $u \in GF(p)$. These two ring homomorphisms induce two group homomorphisms

$$\underline{\varphi_p} : H(\lambda_q) < PSL(2,\mathbf{Z}[\lambda_q]) \longrightarrow \mathrm{H_p}(\lambda_q) < \mathrm{PSL}(2,\mathbf{Z_p}[\lambda_q]) \tag{7.19}$$

and

$$\underline{\chi_u} : H_p(\lambda_q) < PSL(2,\mathbf{Z_p}[\lambda_q]) \longrightarrow \mathrm{PSL(2,p)}, \tag{7.20}$$

where $H_p(\lambda_q)$ denotes the image of $\mathrm{H}(\lambda_q)$ *modulo p*, generated by R_p and S_p.

For each root $u \in GF(p)$ of $P_q^*(\lambda_q)$, $K_{p,u}(\lambda_q)$ is the kernel of the composite homomorphism

$$\underline{\chi_u} \, o \, \underline{\varphi_p} \ : \ H(\lambda_q) \longrightarrow PSL(2,p). \tag{7.21}$$

If a root u is not in $GF(p)$ then it is in an extension field $GF(p^s)$. Then the above idea can be applied to the homomorphism from $\mathrm{H}(\lambda_q)$ to $PSL(2,p^s)$ and the kernel of this homomorphism gives us $K_{p,u}(\lambda_q)$.

An element T of $\mathrm{H}(\lambda_q)$ has the form

$$T = \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix} \tag{7.22}$$

where each p_i is a polynomial of λ_q of degree $\leq d-1$ with d is the degree of the minimal polynomial $P_q^*(\lambda_q)$. Under $\underline{\varphi_p}$, T is mapped to $\underline{T} = \begin{pmatrix} \underline{p_1} & \underline{p_2} \\ \underline{p_3} & \underline{p_4} \end{pmatrix}$. Here $\underline{p_i}$ denotes the polynomial of λ_q with coefficients in $GF(p)$. Finally by $\underline{\chi_u}$, $\underline{T}$ is mapped to $\underline{T_u} = \begin{pmatrix} \underline{p_1(u)} & \underline{p_2(u)} \\ \underline{p_3(u)} & \underline{p_4(u)} \end{pmatrix}$ in $PSL(2,p)$, where $\underline{p_i(u)}$ denotes the value of $\underline{p_i}$ at $u \in GF(p)$.

We can now prove Theorem 7.1. Let $T \in \Gamma_p(\lambda_q)$ be in the form (7.22). Then by the definition of $\Gamma_p(\lambda_q)$, we have

$$p_1 \equiv p_4 \equiv \pm 1 \quad mod\, p \quad , \quad p_2 \equiv p_3 \equiv 0 \quad mod\, p. \tag{7.23}$$

Therefore T is an element of the kernel $K_{p,u}(\lambda_q)$ defined above. Hence

$$\Gamma_p(\lambda_q) \leq K_{p,u}(\lambda_q) \tag{7.24}$$

as required.

Furthermore, as $K_{p,u}(\lambda_q)$ and $\Gamma_p(\lambda_q)$ are normal in $\mathrm{H}(\lambda_q)$,

$$\Gamma_p(\lambda_q) \trianglelefteq K_{p,u}(\lambda_q). \tag{7.25}$$

By Theorem 7.1, $K_{p,u}(\lambda_q)$ is a congruence subgroup of $\mathrm{H}(\lambda_q)$. We shall see that the index of $\Gamma_p(\lambda_q)$ in $K_{p,u}(\lambda_q)$ is 1 or 2 except for a few cases.

In this thesis, we are not going to be concerned with $K_{p,u}(\lambda_q)$ for all roots u of $P_q^*(\lambda_q)$. We shall only consider the $K_{p,u}(\lambda_q)$ such that u is chosen from $GF(p^s)$ for the smallest possible value of s. For example, if $s = 1$, then there is a homomorphism of $\mathrm{H}(\lambda_q)$ to $PSL(2,p)$ as we shall see in the next section, and therefore the quotient of $\mathrm{H}(\lambda_q)$ by $K_{p,u}(\lambda_q)$ is going to be $PSL(2,p)$.

When the index of $\Gamma_p(\lambda_q)$ in $K_{p,u}(\lambda_q)$ is not 1, i.e. when they are different, we shall use $K_{p,u}(\lambda_q)$ to calculate $\Gamma_p(\lambda_q)$. In fact in all cases we first determine the quotient of $\mathrm{H}(\lambda_q)$ by $K_{p,u}(\lambda_q)$ and then, using this, we determine the required quotient of $\mathrm{H}(\lambda_q)$ by $\Gamma_p(\lambda_q)$. To do this we use some results of Macbeath (see [Ma,1]). As we shall use these results intensively, we now briefly recall them here:

7.1. SOME RESULTS OF MACBEATH

Let $\mathbf{k} = \mathrm{GF}(p^n)$ — a field with p^n elements, where p is prime and $n \in \mathbf{N}$, and let $\mathbf{k_1}$ be its unique quadratic extension. Let $G_0 = SL(2,\mathbf{k})$ and $G = PSL(2,\mathbf{k})$ so that $G \cong G_0/\{\pm I\}$. We shall also consider the subgroup G_1 of $SL(2,\mathbf{k_1})$ consisting of the matrices of the form

$$\begin{pmatrix} a & b \\ b^q & a^q \end{pmatrix} \tag{7.26}$$

where $a, b \in \mathbf{k_1}$ and $a^{q+1} - b^{q+1} = 1$. Macbeath, [Ma,1], classifies the G_0*-triples* (A,B,C), $C = (AB)^{-1}$, of elements of G_0 finding out what kind of subgroup they generate. The ordered triple of the traces of the elements of the G_0–triple (A,B,C)

will be a **k**–*triple* (α, β, γ). Also to each G_0–triple (A, B, C), there is an associated **N**–triple (l, m, n) where l, m, n are the orders of A, B and C in G.

Macbeath first considers the G_0–triples and then using the natural homomorphism $\phi : G_0 \longrightarrow G$, passes to the G–triples in the following way: If H is the subgroup of G generated by $\phi(A)$, $\phi(B)$ and $\phi(C)$, we shall say, by slight abuse of language, that H is the subgroup generated by the G_0–triple (A, B, C).

In the Hecke group case we have $A = r_p$, $B = s_p$ and $C = t_p$, where r_p (s_p, t_p respectively) denotes the image of R (S, T respectively) under the homomorphism $\underline{\varphi_p}$ reducing all elements of $\mathrm{H}(\lambda_q)$ *modulo p*. Hence the corresponding **k** –triple is $(0, u, 2)$ where u is a root of the minimal polynomial $P_q^*(\lambda_q)$ *modulo p* in $GF(p)$ or in a suitable extension field. Also the corresponding **N** –triple is $(2, q, n)$ where n is the level of the subgroup.

Macbeath obtained three kinds of subgroups of G: affine, exceptional and projective groups. We now consider them in relation with the Hecke groups.

Let $p > 2$. A **k** –triple (α, β, γ) is called *singular* if the quadratic form

$$Q_{\alpha,\beta,\gamma}(\xi, \eta, \zeta) = \xi^2 + \eta^2 + \zeta^2 + \alpha\eta\zeta + \beta\xi\zeta + \gamma\xi\eta \tag{7.27}$$

is singular, i.e. if

$$\begin{vmatrix} 1 & \gamma/2 & \beta/2 \\ \gamma/2 & 1 & \alpha/2 \\ \beta/2 & \alpha/2 & 1 \end{vmatrix} = 0. \tag{7.28}$$

Now consider the set of matrices of the form

$$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}. \tag{7.29}$$

They form a subgroup of G_0. By mapping it to G with the natural homomorphism ϕ we obtain a subgroup A_1 of G. Now consider the set of matrices

$$\begin{pmatrix} t & 0 \\ 0 & t^q \end{pmatrix}, \quad t \in \mathbf{k_1},\ t^{q+1} = 1 \tag{7.30}$$

in G_1, where $\mathbf{k_1}$ is the unique quadratic extension of $\mathbf{k}$. This is conjugate to a subgroup of $SL(2, \mathbf{k_1})$. It is mapped, firstly by the isomorphism from G_1 to G_0, and then by the natural homomorphism ϕ from G_0 to G, to a subgroup A_2 of G. Any subgroup of a group conjugate, in G, to either A_1 or A_2 will be called an *affine subgroup* of G.

A G_0–triple is called *singular* if the associated $\mathbf{k}$ –triple (α, β, γ) is singular. Any group associated with a singular G_0–triple is an affine group, [Ma,1].

From now on we restrict ourselves to the case $\mathbf{k}$ = GF(p), p prime.

For H(λ_q) with the generators $R(z) = -1/z$ and $T(z) = z + \lambda_q$, the above determinant is equal to $-\lambda_q^2/4$ and therefore vanishes only when $\lambda_q^2 \equiv 0 \mod p$. Then if $q = 3$, $\lambda_3^2 = 1$ cannot be congruent to 0 *modulo* p for any p; that is, there is no singular triple in the modular group case; i.e. modular group has no affine homomorphic images.

If $q = 4$ or 6, then the only singular triples are obtained when $p = 2$ or 3, respectively.

For the other values of q, we need to find primes p such that $\lambda_q^2 \equiv 0 \mod p$ to find the singular G_0–triples. To do this we shall consider the minimal polynomial $P_q^*(x)$ of λ_q over $\mathbf{Q}$, discussed in Chapter 2, and specially its constant term c. Recall that we determined c in 2.3 for all q. We found that if q is odd then $|c| = 1$. Therefore we do not have any singular triples when q is odd. When q is even, we have more possibilities. First, if $q = 2^\alpha$, $\alpha > 1$, then $|c| = 2$ and hence (r_p, s_p, t_p) is singular if and only if $p = 2$. Secondly if $q = 2r^n, n > 1$, then we showed that $|c| = r$ and hence (r_p, s_p, t_p) is singular if and only if $p = r$. Finally, let q be different from above. Then $|c| = 1$ and again no singular triples are obtained in this case.

The triples $(2,2,n)$, $n \in \mathbf{N}$, $(2,3,3)$, $(2,3,4)$, $(2,3,5)$ and $(2,5,5)$ – as $(2,3,5)$ is a homomorphic image of (2,5,5)– which are the associated $\mathbf{N}$ -triples of the finite triangle groups, are called the *exceptional triples.* The *exceptional groups* are those which are isomorphic images of the finite triangle groups.

For example when $q = 3$, we obtain exceptional triples for $p = 2, 3$ and 5. When $q = 4$ or 6 only exceptional triples are obtained for $p = 2$ and 3, respectively. In general if $q \geq 6$ is even, then except for the infinite class of exceptional dihedral triples $(2,2,n)$, we only have the exceptional triple $(2,2n,2)$ which is again dihedral. That is, only for $p = 2$, an exceptional triple can be obtained.

If $q > 5$ is prime then it is easy to see that the only exceptional triples are obtained for $p = 2$.

For composite odd values of q, the number of exceptional triples depends on the divisibility of q by 3 and 5. For example if q is divisible by 3, then there are homomorphisms to four finite triangle groups $D_3 \cong (2,3,2)$, $A_4 \cong (2,3,3)$, $S_4 \cong (2,3,4)$ and $A_5 \cong (2,3,5)$ each giving an exceptional subgroup of $\mathrm{H}(\lambda_q)$. Similarly if q is divisible by 5, there are homomorphisms of $\mathrm{H}(\lambda_q)$ to $D_5 \cong (2,5,2)$, $A_5 \cong (2,5,3)$ and again $(2,5,5)$ as it maps onto A_5, giving three exceptional subgroups. Further if $15 \mid q$, then $\mathrm{H}(\lambda_q)$ has all of the above subgroups as there are homomorphisms to the seven finite triangle groups mentioned above.

The final class of the subgroups of G is the class of the projective subgroups. We have already discussed them in Chapter 0 and seen that there are two isomorphism classes of them, $PSL(2, \mathbf{k_s})$ and $PGL(2, \mathbf{k_s})$ where $\mathbf{k_s} < \mathbf{k}$, the latter containing the former with index 2, except for $p = 2$ where the two groups are equal.

Let now $\mathbf{k_1}$ be the quadratic extension of $\mathbf{k}$. Then every element of $\mathbf{k}$ is a square in $\mathbf{k_1}$ and therefore $PGL(2,\mathbf{k})$ is contained in $PSL(2,\mathbf{k_1})$, i.e. we have the following inclusions:

$$PSL(2,\mathbf{k}) \prec \mathrm{PGL}(2,\mathbf{k}) \prec \mathrm{PSL}(2,\mathbf{k_1}). \tag{7.31}$$

If $\mathbf{k_s}$ is a subfield of $\mathbf{k}$, then clearly $PSL(2,\mathbf{k_s}) \prec \mathrm{PSL}(2,\mathbf{k})$. If also the quadratic extension $\mathbf{k_{s_1}}$ is a subfield of $\mathbf{k}$, then $PGL(2,\mathbf{k_s}) \prec \mathrm{PSL}(2,\mathbf{k})$. Briefly, the groups $PSL(2,\mathbf{k_s})$, for all subfields of $\mathbf{k}$, and whenever possible, the groups $PGL(2,\mathbf{k_s})$, together with their conjugates in $PGL(2,\mathbf{k})$ will be called projective subgroups of G.

Dickson, [Di,1], proved that every subgroup of G is either affine, exceptional or projective, and we have discussed all these above. The remaining thing to do is to determine which one of these three kinds of subgroups is generated by the G_0–triple (r_p, s_p, t_p). We shall see that in most cases it will be a projective group, and our problem is going to be to determine this subgroup. To do this we shall use the following results proven by Macbeath, [Ma,1]:

Theorem 7.2: A G_0–triple which is neither singular nor exceptional generates a projective subgroup of G.

Theorem 7.3: If a G_0–triple generates a projective subgroup of G, then it generates either a subgroup isomorphic to $PSL(2,\kappa)$ or a subgroup isomorphic to $PGL(2,\kappa_0)$ where κ is the smallest subfield of $\mathbf{k}$ containing α, β and γ, and κ_0 is the subfield, if any, of which κ is a quadratic extension.

There are some $\mathbf{k}$–triples which are neither singular nor exceptional. They are called irregular in [Ma,1], i.e. a $\mathbf{k}$–triple is called *irregular* if the subfield generated by its elements, say κ, is a quadratic extension of another subfield κ_0, and if one of the elements of the triple lies in κ_0 while the others are both square roots in κ of non–squares in κ_0, or zero. Then we have

Theorem 7.4: A G_0–triple which is neither exceptional, singular nor irregular generates in G a projective group isomorphic to $PSL(2,\kappa)$ where κ is the subfield generated by the traces of its matrices.

We have thus completed recalling some necessary results of Macbeath. We can now find the quotients of $\mathrm{H}(\lambda_q)$ by $\Gamma_p(\lambda_q)$ and $K_{p,u}(\lambda_q)$ for several values of q beginning with $q = 4$ and 6:

7.2. PRINCIPAL CONGRUENCE SUBGROUPS OF H($\sqrt{2}$) AND H($\sqrt{3}$)

In this section we discuss the principal congruence subgroups of $\mathrm{H}(\sqrt{m})$, where m stands for 2 or 3. We first find the quotients of $\mathrm{H}(\sqrt{m})$ by the principal congruence subgroups and then find the group theoretical structure of them. We find that except for a few cases, they are all free.

We first try to find the quotients of $\mathrm{H}(\sqrt{m})$ with $K_{p,u}(\sqrt{m})$. It is then easy to determine $\mathrm{H}(\sqrt{m})/\Gamma_p(\sqrt{m})$. To determine both quotients we need the results stated in 7.1.

(i) $q = 4$**:** Here we have the following result:

Theorem 7.5: The quotient groups of the Hecke group $\mathrm{H}(\sqrt{2})$ by its congruence subgroups $\mathrm{K}_{p,u}(\sqrt{2})$ and principal congruence subgroups $\Gamma_p(\sqrt{2})$ are as follows:

$$H(\sqrt{2})/K_{p,u}(\sqrt{2}) \cong \begin{cases} PSL(2,p) & \text{if} \quad p \equiv \pm 1 \ mod\, 8 \\ PGL(2,p) & \text{if} \quad p \equiv \pm 3 \ mod\, 8 \\ C_2 & \text{if} \quad p = 2, \end{cases} \tag{7.32}$$

and

$$H(\sqrt{2})/\Gamma_p(\sqrt{2}) \cong \begin{cases} C_2 \times PSL(2,p) & \text{if } \ p \equiv \pm 1 \ mod\, 8 \\ PGL(2,p) & \text{if } \ p \equiv \pm 3 \ mod\, 8 \\ D_4 & \text{if } \ p = 2. \end{cases} \tag{7.33}$$

Proof: Case 1. Let $p \neq 2$ be so that 2 is a square *modulo p*, that is, $p \equiv \pm 1$ $mod\, 8$. In that case there exists an element u in $GF(p)$ such that $u^2 = 2$. Therefore $\sqrt{2}$ can be considered as an element of $GF(p)$. Let us now recall the homomorphism of $H(\lambda_q)$ reducing all elements of it *modulo p*. The images of R, S and T under this homomorphism were denoted by r_p, s_p and t_p respectively. Then clearly r_p, s_p and t_p belong to $PSL(2,p)$. Now there is a homomorphism

$$\theta \ : \ H(\sqrt{2}) \longrightarrow PSL(2,p) \tag{7.34}$$

induced by $\begin{pmatrix} a\sqrt{2} & b \\ c & d\sqrt{2} \end{pmatrix} \mapsto \begin{pmatrix} au & b \\ c & du \end{pmatrix}$ and $\begin{pmatrix} a & b\sqrt{2} \\ c\sqrt{2} & d \end{pmatrix} \mapsto \begin{pmatrix} a & bu \\ cu & d \end{pmatrix}$ where in $SL(2,p)$ we write, with slight abuse of language, a, b, c, d for their classes in $\mathbf{Z_p}$. Then our problem is to find the subgroup of $PSL(2,p) = G$, generated by R_p, S_p and T_p.

Following Macbeath's terminology let $\mathbf{k}$ = GF(p). Then κ, the smallest subfield of $\mathbf{k}$ containing $\alpha = tr\ r_p$, $\beta = tr\ s_p$ and $\gamma = tr\ t_p$, is also $GF(p)$ as $\sqrt{2} \in GF(p)$. In this case, for all p, the $H_p(\sqrt{2})$-triple (r_p, s_p, t_p) is not singular since the discriminant of the associated quadratic form, which is $-u^2/4$, is not 0. It is also not exceptional since the associated $\mathbf{N}$-triple (giving the orders of its elements) $(2, 4, p)$ is not an exceptional triple for $p \equiv \pm 1$ *mod 8*. Then by Theorem 7.2, (r_p, s_p, t_p) generates a projective subgroup of G, and by Theorem 7.3, as κ = GF(p) is not a quadratic extension of any other field, this subgroup is the whole $PSL(2,p)$, i.e.

$$H(\sqrt{2})/K_{p,u}(\sqrt{2}) \cong PSL(2,p). \tag{7.35}$$

Let us now find the quotient of $H(\sqrt{2})$ by the principal congruence subgroup $\Gamma_p(\sqrt{2})$ in this case. Note that, by (7.3), $\Gamma_p(\sqrt{2})$ is a subgroup of the even subgroup

$H_e(\sqrt{2})$ consisting of all even elements in $H(\sqrt{2})$. Therefore there are no odd elements in $\Gamma_p(\sqrt{2})$. We have the following subgroup lattice:

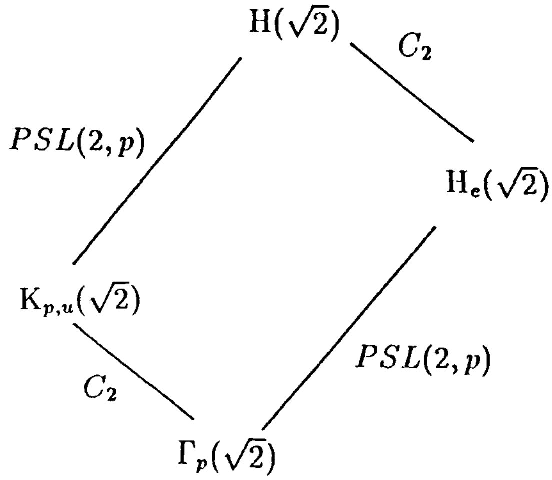


Figure 7.1. Two congruence subgroups of $H(\sqrt{2})$

We now want to find the quotient group $K_{p,u}(\sqrt{2})/\Gamma_p(\sqrt{2})$. To show that it is not the trivial group, we show that $K_{p,u}(\sqrt{2})$ contains an odd element, as $\Gamma_p(\sqrt{2})$ $< H_e(\sqrt{2})$.

Let us see what an odd element looks like. If A is such an element, then

$$A = \begin{pmatrix} x\sqrt{2} & y \\ z & t\sqrt{2} \end{pmatrix} \;;\Delta = 2xt - yz = 1,\ x, y, z, t \in \mathbf{Z}, \tag{7.36}$$

is in $K_{p,u}(\sqrt{2}) - \Gamma_p(\sqrt{2})$. Now

$$A^2 = \begin{pmatrix} x\sqrt{2} & y \\ z & t\sqrt{2} \end{pmatrix}\begin{pmatrix} x\sqrt{2} & y \\ z & t\sqrt{2} \end{pmatrix} = \begin{pmatrix} 2x^2 + yz & \sqrt{2}(xy + yt) \\ \sqrt{2}(xz + tz) & 2t^2 + yz \end{pmatrix} \tag{7.37}$$

and since $xu \equiv tu \equiv 1,\ y \equiv z \equiv 0 \ mod\ p$, we have

$$x^2u^2 = 2x^2 \equiv 1 \ mod\ p, \tag{7.38}$$

and similarly

$$t^2u^2 = 2t^2 \equiv 1 \ mod\, p. \tag{7.39}$$

Hence A is of exponent two $mod\, \Gamma_p(\sqrt{2})$. Then we can write

$$K_{p,u}(\sqrt{2}) = \Gamma_p(\sqrt{2}) \cup A.\Gamma_p(\sqrt{2}) \tag{7.40}$$

as $A \notin \Gamma_p(\sqrt{2})$.

Now we want to show that any element $\begin{pmatrix} a & b\sqrt{2} \\ c\sqrt{2} & d \end{pmatrix}$ of $\mathrm{H}_e(\sqrt{2})/\Gamma_p(\sqrt{2})$ commutes with A mod p. This is true since

$$\begin{pmatrix} x\sqrt{2} & y \\ z & t\sqrt{2} \end{pmatrix}\begin{pmatrix} a & b\sqrt{2} \\ c\sqrt{2} & d \end{pmatrix} = \begin{pmatrix} \sqrt{2}(ax+cy) & 2bx+dy \\ az+2ct & \sqrt{2}(bz+dt) \end{pmatrix} \tag{7.41}$$

and

$$\begin{pmatrix} a & b\sqrt{2} \\ c\sqrt{2} & d \end{pmatrix}\begin{pmatrix} x\sqrt{2} & y \\ z & t\sqrt{2} \end{pmatrix} = \begin{pmatrix} \sqrt{2}(ax+bz) & ay+2bt \\ 2cx+dz & \sqrt{2}(cy+dt) \end{pmatrix} \tag{7.42}$$

and since $y \equiv z \equiv 0$ and $x \equiv t \ mod\, p$. Therefore

$$\begin{aligned} H(\sqrt{2})/\Gamma_p(\sqrt{2}) &\cong K_{p,u}(\sqrt{2})/\Gamma_p(\sqrt{2}) \times H_e(\sqrt{2})/\Gamma_p(\sqrt{2}) \\ &\cong C_2 \times PSL(2,p). \end{aligned} \tag{7.43}$$

To find the odd element mentioned above we need to solve a Diophantine equation. Let us first see this with an example:

Example 7.1: (i) Let $p = 7$. Then $u = \sqrt{2} \equiv \pm 3 \ mod\ 7$. We choose $u \equiv 3 \ mod\, 7$. We are looking for an odd matrix $A = \begin{pmatrix} x\sqrt{2} & y \\ z & t\sqrt{2} \end{pmatrix}$ of $K_{7,3}(\sqrt{2})$ which is not in $\Gamma_7(\sqrt{2})$. Such an element must satisfy the following conditions:

$$\Delta = 2xt - yz = 1, \tag{7.44}$$

$$xu \equiv tu \equiv 1, \ y \equiv z \equiv 0 \ mod\, 7. \tag{7.45}$$

As $u \equiv 3 \mod 7$,

$$x \equiv t \equiv 5 \mod 7. \tag{7.46}$$

Then we have

$$2(5+7a)(5+7b) - 7c.7d = 1, \tag{7.47}$$

where a, b, c, d are non–negative integers. Hence

$$7 + 10(a+b) + 14ab = 7cd \tag{7.48}$$

which has a solution whenever $a+b$ is an integer multiple of 7. A particular solution of the Diophantine equation (7.48) is

$$a = b = 0, \quad c = d = 1 \tag{7.49}$$

and therefore

$$A = \begin{pmatrix} 5\sqrt{2} & 7 \\ 7 & 5\sqrt{2} \end{pmatrix}. \tag{7.50}$$

Notice that we have chosen $u \equiv 3 \mod 7$. If we choose the other value 4 of $u \in GF(7)$, then again we obtain an odd element

$$B = \begin{pmatrix} 2\sqrt{2} & 7 \\ 21 & 37\sqrt{2} \end{pmatrix} \tag{7.51}$$

in $K_{7,4}(\sqrt{2})$–$\Gamma_7(\sqrt{2})$. In fact, as in this special case, 3 is the negative of 4, generators of one of the two principal congruence subgroups corresponding to these two values of u are just the inverses of the generators of the other. Therefore these two subgroups are equal in $\mathrm{H}(\sqrt{2})$.

(ii) Secondly let $p = 17$. Then similarly we obtain the Diophantine equation

$$1 + 6(a+b) - 34ab = 17cd \tag{7.52}$$

and solving this one we find

$$a = 14,\ b = 0,\ c = 1,\ d = 5, \tag{7.53}$$

as a particular solution which gives the matrix

$$A = \begin{pmatrix} 241\sqrt{2} & 17 \\ 85 & 3\sqrt{2} \end{pmatrix}. \tag{7.54}$$

In general let $p \equiv \pm 1 \ mod\, 8$. Let $A = \begin{pmatrix} x\sqrt{2} & y \\ z & t\sqrt{2} \end{pmatrix}$ be as above. We have

$$\Delta = 2xt - yz = 1, \tag{7.55}$$

$$xu \equiv tu \equiv 1,\ y \equiv z \equiv 0 \ mod\, p, \tag{7.56}$$

where $u \equiv \sqrt{2} \ mod\, p$. Let $v \in GF(p)$ be such that $uv \equiv 1 \ mod\, p$. Then

$$x = v + pa,\ t = v + pb,\ y = pc,\ z = pd \tag{7.57}$$

where a, b, c, d are non–negative integers. Hence (7.55) becomes

$$\Delta = 2(v + pa)(v + pb) - p^2cd = 1 \tag{7.58}$$

and hence

$$2v^2 - 1 + 2vp(a + b) + 2p^2ab = p^2cd. \tag{7.59}$$

Therefore

$$p\,|\,(2v^2 - 1). \tag{7.60}$$

Let $2v^2 - 1 = k.p,\ k \in \mathbf{N}$. Then (7.59) becomes

$$k + 2v(a + b) + 2pab = pcd. \tag{7.61}$$

This can be solved whenever

$$p \mid (k + 2v(a + b)). \tag{7.62}$$

As k and v are known we can choose the non-negative integers a and b such that (7.62) is satisfied. Although (7.61) has infinitely many solutions, we can obtain a particular solution by choosing $b = 0$ and $c = 1$:

$$A = \begin{pmatrix} (v + pa)\sqrt{2} & p \\ pd & v\sqrt{2} \end{pmatrix} \tag{7.63}$$

where a and d are chosen uniquely. That is, it is always possible to find an odd element A of $\mathrm{K}_{p,u}(\sqrt{2})$ which does not belong to $\Gamma_p(\sqrt{2})$, when $p \equiv \pm 1 \ mod\, 8$.

Case 2. Now choose p be so that 2 is not a square *modulo* p and let $p \neq 2$, i.e. let $p \equiv \pm 3 \ mod\, 8$. In this case $\sqrt{2}$ cannot be considered as an element of $GF(p)$. Therefore we shall extend this field to its quadratic extension $GF(p^2)$. Then $u = \sqrt{2}$ can be considered to be in $GF(p^2)$ and there exists a homomorphism

$$\theta : H(\sqrt{2}) \longrightarrow PSL(2, p^2) \tag{7.64}$$

induced in a similar way to case 1.

Let $\mathbf{k} = \mathrm{GF}(\mathrm{p}^2)$. Then κ, the smallest subfield of $\mathbf{k}$ containing traces α, β, γ of R_p, S_p, T_p, is also $GF(p^2)$.

Except for $p = 3$, the G_0-triple (r_p, s_p, t_p) is not an exceptional triple. If $p = 3$ then the corresponding $\mathbf{N}$-triple is (2,4,3) and therefore the generated subgroup is isomorphic to the symmetric group S_4.

Now suppose $p > 3$. Then as in case 1, (r_p, s_p, t_p) is not a singular triple. Since κ is the quadratic extension of $\kappa_0 = \mathrm{GF(p)}$ and as $\beta = 2$ lies in κ_0 while $\alpha = 0$, and $\gamma = \sqrt{2}$ is the square root in κ of 2 which is a non-square in κ_0, by Theorem

7.3, (r_p, s_p, t_p) generates $PGL(2,p)$, i.e.

$$H(\sqrt{2})/K_{p,u}(\sqrt{2}) \cong PGL(2,p). \tag{7.65}$$

Since 2 is not a square *modulo p*, there are no odd elements in the kernel $K_{p,u}(\sqrt{2})$. Hence

$$K_{p,u}(\sqrt{2}) = \Gamma_p(\sqrt{2}) \tag{7.66}$$

and hence

$$H(\sqrt{2})/\Gamma_p(\sqrt{2}) \cong PGL(2,p). \tag{7.67}$$

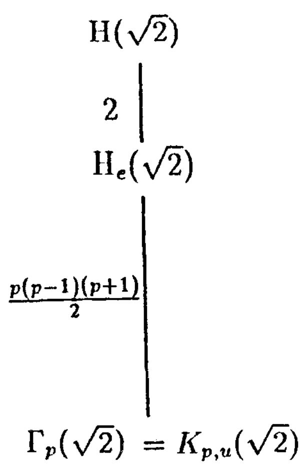


Figure 7.2.

If $p = 3$, then again the two subgroups coincide and

$$H(\sqrt{2})/\Gamma_3(\sqrt{2}) \cong H(\sqrt{2})/K_{3,u}(\sqrt{2}) \cong S_4 \cong PGL(2,3). \tag{7.68}$$

Case 3. Let finally $p = 2$. Then $\sqrt{2}^2 = 2 \equiv 0 \ mod\ 2$. It is easy to find exactly 8 elements in $H(\sqrt{2})/\Gamma_2(\sqrt{2})$ and as

$$r_2^2 = t_2^2 = s_2^4 = I, \quad s_2 = r_2 t_2, \tag{7.69}$$

(r_2, s_2, t_2) is an exceptional triple generating the dihedral group D_4 of order 8, that is

$$H(\sqrt{2})/\Gamma_2(\sqrt{2}) \cong D_4. \qquad (7.70)$$

Now $GF(2) = \{0, 1\}$ and $\sqrt{2} = 0$ in $GF(2)$. Therefore $t_2 \equiv I \ mod\ 2$. Hence $\mathrm{H}(\sqrt{2})/K_{2,0}(\sqrt{2})$, generated by r_2, s_2 and t_2 is isomorphic to the cyclic group of order 2, i.e.

$$H(\sqrt{2})/K_{2,0}(\sqrt{2}) \cong C_2. \qquad (7.71)$$

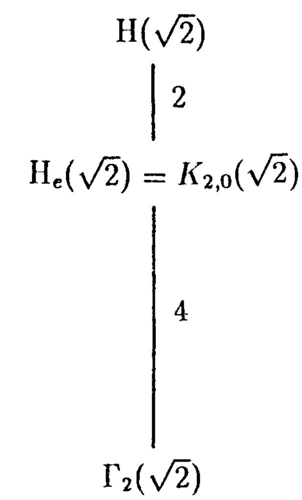


Figure 7.3. Two congruence subgroups of level two of $\mathrm{H}(\sqrt{2})$

(ii) $q = 6$: We now calculate the principal congruence subgroups of $\mathrm{H}(\sqrt{3})$. All ideas and calculations are similar to the $q = 4$ case. In fact we have the following very similar result:

Theorem 7.6: The quotient groups of the Hecke group $\mathrm{H}(\sqrt{3})$ by its congruence subgroups $\mathrm{K}_{p,u}(\sqrt{3})$ and $\Gamma_p(\sqrt{3})$ are as follows:

$$H(\sqrt{3})/K_{p,u}(\sqrt{3}) \cong \begin{cases} PSL(2,p) & \text{if } p \equiv \pm 1 \ mod\ 12 \\ PGL(2,p) & \text{if } p \not\equiv \pm 1 \ mod\ 12, \text{ and } p \neq 2 \\ C_2 & \text{if } p = 3 \\ D_3 & \text{if } p = 2, \end{cases} \qquad (7.72)$$

and

$$H(\sqrt{3})/\Gamma_p(\sqrt{3}) \cong \begin{cases} C_2 \times PSL(2,p) & \text{if } p \equiv \pm 1 \ mod\, 12 \\ PGL(2,p) & \text{if } p \not\equiv \pm 1 \ mod\, 12, \text{ and } p \neq 2 \\ (C_3 \times C_3) \wr C_2 & \text{if } p = 3 \\ D_6 & \text{if } p = 2. \end{cases} \tag{7.73}$$

Proof: Case 1. Let $p \neq 2$ be so that 3 is a square *modulo p*, that is, $p \equiv \pm 1$ $mod\, 12$. In that case there exists an element u in $GF(p)$ such that $u^2 = 3$. Therefore $\sqrt{3}$ can be considered as an element of $GF(p)$. Then we have a homomorphism

$$\Theta' : H(\sqrt{3}) \longrightarrow PSL(2,p). \tag{7.74}$$

Let **k** = GF(p). Then κ is also $GF(p)$ as $\sqrt{3}$ can be thought of as an element of $GF(p)$. (r_p, s_p, t_p) is not singular nor exceptional as $(2,6,p)$ is not an exceptional triple and as $p > 2$. Then by Theorems 7.3 and 7.4, (r_p, s_p, t_p) generates $PSL(2,p)$, i.e.

$$H(\sqrt{3})/K_{p,u}(\sqrt{3}) \cong PSL(2,p). \tag{7.75}$$

Let us now find the other quotient group $H(\sqrt{3})/\Gamma_p(\sqrt{3})$. As in the case $q = 4$, we can find an odd element

$$A = \begin{pmatrix} x\sqrt{3} & y \\ z & t\sqrt{3} \end{pmatrix} \; ; \Delta = 3xt - yz = 1, \; x, y, z, t \in \mathbf{Z}, \tag{7.76}$$

in $K_{p,u}(\sqrt{3}) - \Gamma_p(\sqrt{3})$. A is of exponent two $mod\, \Gamma_p(\sqrt{3})$, and hence

$$K_{p,u}(\sqrt{3}) = \Gamma_p(\sqrt{3}) \cup A.\Gamma_p(\sqrt{3}). \tag{7.77}$$

Also since A commutes with every $\begin{pmatrix} a & b\sqrt{3} \\ c\sqrt{3} & d \end{pmatrix}$ of $H_e(\sqrt{3})/\Gamma_p(\sqrt{3})$ mod p, we have the below commutative diagram and hence

$$\begin{aligned} H(\sqrt{3})/\Gamma_p(\sqrt{3}) &\cong K_{p,u}(\sqrt{3})/\Gamma_p(\sqrt{3}) \times H_e(\sqrt{3})/\Gamma_p(\sqrt{3}) \\ &\cong C_2 \times PSL(2,p). \end{aligned} \tag{7.78}$$

Example 7.2: **(i)** Let $p = 11$. Then $u = \sqrt{3} \equiv \pm 5 \ mod\, 11$. Let $u = 5$. After some calculations similar to the case $q = 4$, we find the required odd element as

$$A = \begin{pmatrix} 9\sqrt{3} & 11 \\ 22 & 9\sqrt{3} \end{pmatrix}. \tag{7.79}$$

(ii) Let $p = 13$. Now $u = \sqrt{3} \equiv \pm 4 \ mod\, 13$. For $u \equiv 4$, solving the corresponding Diophantine equation we find

$$A = \begin{pmatrix} 10\sqrt{3} & 13 \\ 143 & 62\sqrt{3} \end{pmatrix}. \tag{7.80}$$

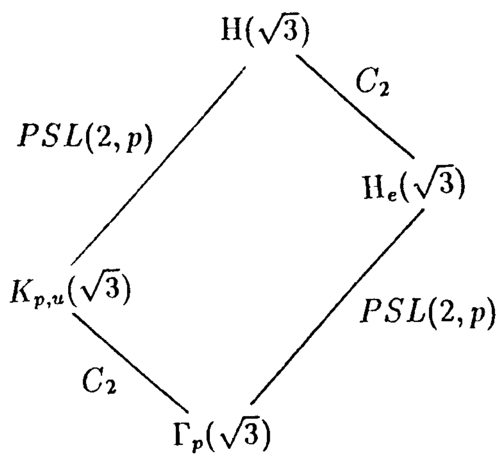


Figure 7.4. Two congruence subgroups of level p of $\mathrm{H}(\sqrt{3})$, ($p \equiv \pm 1 \ mod\, 12$)

Case 2. Let now $p \neq 3$ be such that 3 is not a square $mod\, p$, i.e. $\left(\frac{3}{p}\right) = -1$. Then $\sqrt{3}$ cannot be considered as an element of $GF(p)$. If we extend $GF(p)$ to its unique quadratic extension $GF(p^2)$, then following the similar argument of the case 2 of $q = 4$ case, we obtain

$$H(\sqrt{3})/K_{p,u}(\sqrt{3}) \cong H(\sqrt{3})/\Gamma_p(\sqrt{3}) \cong PGL(2, p). \tag{7.81}$$

When $p = 2$, (r_2, s_2, t_2) gives the exceptional **N**–triple (2,3,2) and hence generates a group isomorphic to the dihedral group D_3 of order 6.

Let us now consider $\mathrm{H}(\sqrt{3})/\Gamma_2(\sqrt{3})$. After some calculations we can see that there are the following 12 cosets in this quotient group:

$$I, s, s^2, s^3, s^4, s^5, r, rs, rs^2, rs^3, rs^4, rs^5. \tag{7.82}$$

Here r and s denote their classes in the quotient $\mathrm{H}(\sqrt{3})/\Gamma_2(\sqrt{3})$. Therefore we have the relations $r^2 = s^6 = t^2 = I$, i.e. it is isomorphic to the dihedral group D_6 of order 12. Therefore we have the following:

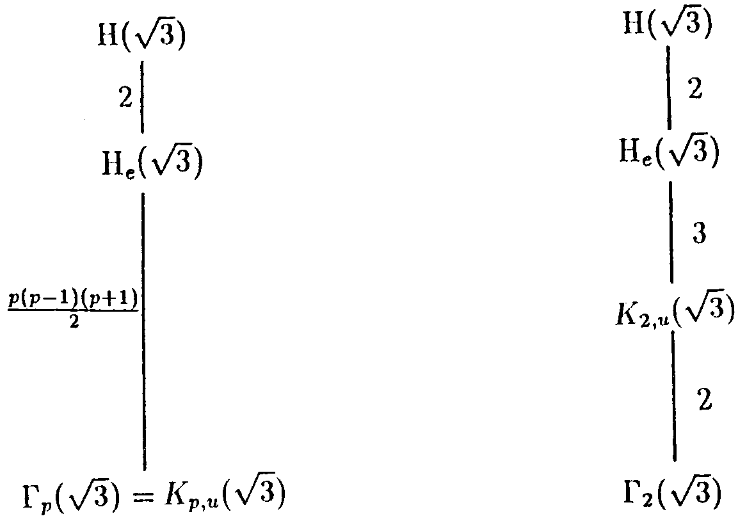


Figure 7.5. More subgroup lattices for $\mathrm{H}(\sqrt{3})$

Case 3. Let $p = 3$. As $\sqrt{3}$ can be thought of as an element 0 of $GF(3)$, $t_3 \equiv 1 \ mod\, 3$. As $r_3^2 = 1$ as well, we have

$$H(\sqrt{3})/K_{3,0}(\sqrt{3}) \cong C_2. \tag{7.83}$$

In the quotient $\mathrm{H}(\sqrt{3})/\Gamma_3(\sqrt{3})$ we have the relations

$$r_3^2 = t_3^3 = s_3^6 = I, \quad s_3 = r_3 t_3 \tag{7.84}$$

as $3 \equiv 0 \ mod\, 3$. Therefore $\mathrm{H}(\sqrt{3})/\Gamma_3(\sqrt{3})$ is a finite homomorphic image of the infinite triangle group (2,3,6). As

$$\Gamma_3(\sqrt{3}) = \left\{ M = \begin{pmatrix} a & b\sqrt{3} \\ c\sqrt{3} & d \end{pmatrix} : M \equiv \pm I \ mod\ 3 \right\}, \qquad (7.85)$$

we can find all cosets. It can be shown that the quotient group is isomorphic to the Wreath product $C_3 \wr C_2$ of order 18.

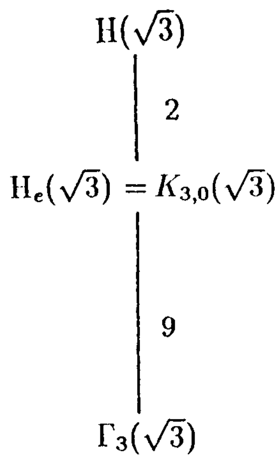


Figure 7.6. Some congruence subgroups of level 3 of $H(\sqrt{3})$

Hence we have found all quotient groups of $H(\sqrt{m})$, m= 2 or 3, with $K_{p,u}(\sqrt{m})$ and with the principal congruence subgroups $\Gamma_p(\sqrt{m})$, for all prime p. By means of them we can give the index formula for these two congruence subgroups. (This agrees with the formula given by Parson, [Pa,1]):

Corollary 7.1: The indices of the congruence subgroups $K_{p,u}(\sqrt{m})$ and $\Gamma_p(\sqrt{m})$ in $H(\sqrt{m})$ are

$$|H(\sqrt{m})/K_{p,u}(\sqrt{m})| = \begin{cases} p(p-1)(p+1)/2 & \text{if } m \text{ is a square } mod\ p \text{ and } p \neq m, \\ p(p-1)(p+1) & \text{if } m \text{ is not a square } mod\ p \text{ and } p \neq 6/m, \\ 2 & \text{if } p = m, \\ 24 & \text{if } m = 2,\ p = 3, \\ 6 & \text{if } m = 3,\ p =, 2, \end{cases} \qquad (7.86)$$

and

$$|H(\sqrt{m})/\Gamma_p(\sqrt{m})| = \begin{cases} p(p-1)(p+1) & \text{if } p \neq m,\ 6/m, \\ 2m^2 & \text{if } p = m, \\ 24 & \text{if } m = 2,\ p = 3, \\ 12 & \text{if } m = 3,\ p = 2. \end{cases} \quad (7.87)$$

We are now able to determine the group theoretical structure of the subgroups $K_{p,u}(\sqrt{m})$ and $\Gamma_p(\sqrt{m})$ of $\mathrm{H}(\sqrt{m})$, $m = 2$ or 3. First we consider the $\mathrm{H}(\sqrt{2})$ case:

We know that

$$\Gamma_p(\sqrt{2}) \trianglelefteq K_{p,u}(\sqrt{2}) \quad (7.88)$$

and also by the definition of $\Gamma_p(\sqrt{2})$

$$\Gamma_p(\sqrt{2}) \lhd H_e(\sqrt{2}). \quad (7.89)$$

We then have four cases:

(i) Let $p = 2$. In this case $\mathrm{H}(\sqrt{2})\ /\ K_{2,0}(\sqrt{2}) \cong C_2$. It is easy to see that $K_{2,0}(\sqrt{2})$ cannot have any odd elements. Indeed if there is one, say $\begin{pmatrix} a\sqrt{2} & b \\ c & d\sqrt{2} \end{pmatrix}$, then it can not be mapped to the identity *mod 2*. Since both of the normal subgroups $K_{2,0}(\sqrt{2})$ and $\mathrm{H}_e(\sqrt{2})$ have index two in $\mathrm{H}(\sqrt{2})$, they must be isomorphic by (7.71), i.e.

$$K_{2,0}(\sqrt{2}) \cong H_e(\sqrt{2}). \quad (7.90)$$

Let us now consider $\Gamma_2(\sqrt{2})$. Recall that $\mathrm{H}(\sqrt{2})/\Gamma_2(\sqrt{2}) \cong D_4 \cong <\alpha, \gamma \mid \alpha^2 = \gamma^2 = (\alpha\gamma)^4 = I>$. Recall that the kernel of the homomorphism of $\mathrm{H}(\sqrt{2})$ onto D_4 was denoted by $W_4(\sqrt{2})$. Therefore $\Gamma_2(\sqrt{2})$ is the same as $W_4(\sqrt{2})$. Here $R \mapsto \alpha$, $S \mapsto \gamma$ and therefore $RS \mapsto \alpha\gamma$, i.e.

$$\begin{aligned} R &\mapsto (1\,2)(3\,4)(5\,6)(7\,8) \\ S &\mapsto (1\,8)(2\,3)(4\,5)(6\,7) \end{aligned} \quad (7.91)$$

and therefore

$$RS \mapsto (1\,3\,5\,7)(2\,8\,6\,4). \tag{7.92}$$

Now by the permutation method and Riemann–Hurwitz formula we find the signature of $\Gamma_2(\sqrt{2})$ as $(0\ ;\ 2^{(4)}, \infty, \infty)$.

(ii) Let $p \equiv \pm 1 \ \ mod\ 8$. Then the quotient groups are $PSL(2,p)$ and $C_2 \times PSL(2,p)$ respectively as we have proved. Let now r_p and s_p be the images of R and S, respectively, in $PSL(2,p)$ or in $C_2 \times PSL(2,p)$. Then the relations $r_p^2 = s_p^4 = I$ are satisfied, that is, both $K_{p,u}(\sqrt{2})$ and $\Gamma_p(\sqrt{2})$ are free groups. The parabolic element $r_p s_p$ has order p, that is, the level of the congruence subgroup $\Gamma_p(\sqrt{2})$ or $K_{p,u}(\sqrt{2})$ is p. Then T goes to an element of order p. Let μ be the index of the congruence subgroup $K_{p,u}(\sqrt{2})$ or the principal congruence subgroup $\Gamma_p(\sqrt{2})$ in $\mathrm{H}(\sqrt{2})$. Then they have the signature $(g\ ;\ \infty^{(\mu/p)})$. By the Riemann–Hurwitz formula the genus g is given by

$$g = 1 + \frac{\mu}{8p}(p-4). \tag{7.93}$$

Let us see this with an example:

Example 7.3: Let $p = 7$. Then the two quotient groups are $PSL(2,7)$ and $C_2 \times PSL(2,7)$, respectively. Therefore the signature of $K_{7,3}(\sqrt{2}) = K_{7,4}(\sqrt{2})$ is $(10\ ;\ \infty^{(24)})$ and the signature of $\Gamma_7(\sqrt{2})$ is $(19\ ;\ \infty^{(48)})$.

As the example suggests we can easily see that if $\mathrm{K}_{p,u}(\sqrt{2})$ has genus g_k and parabolic class number t_k, and if $\Gamma_p(\sqrt{2})$ has genus g_γ and parabolic class number t_γ, then

$$g_\gamma = 2.g_k - 1 \tag{7.94}$$

and

$$t_\gamma = 2.t_k. \tag{7.95}$$

(iii) Finally let $p \equiv \pm 3 \; mod \; 8$. Then both quotient groups are isomorphic to $PGL(2,p)$. As in case (ii) we have the signature of $K_{p,u}(\sqrt{2}) = \Gamma_p(\sqrt{2})$ as

$$\left(1 + \frac{\mu}{8p}(p-4) \; ; \; \infty^{(\mu/p)}\right). \tag{7.96}$$

Example 7.4: Let $p = 5$. Then $\mathrm{H}(\sqrt{2})/K_{5,u}(\sqrt{2}) \cong \mathrm{H}(\sqrt{2})/\Gamma_5(\sqrt{2}) \cong PGL(2,5)$, and therefore

$$K_{5,u}(\sqrt{2}) = \Gamma_5(\sqrt{2}) \cong (4 \; ; \; \infty^{(24)}). \tag{7.97}$$

Let us now do the similar calculations for the principal congruence subgroups of $\mathrm{H}(\sqrt{3})$. We have the following relations:

$$\Gamma_p(\sqrt{3}) \trianglelefteq K_{p,u}(\sqrt{3}), \tag{7.98}$$

and

$$\Gamma_p(\sqrt{3}) \trianglelefteq H_e(\sqrt{3}). \tag{7.99}$$

We now consider the possibilities:

(i) Let $p = 2$. We know that $\mathrm{H}(\sqrt{3})/K_{2,u}(\sqrt{3}) \cong D_3$ and $\mathrm{H}(\sqrt{3})/\,\Gamma_2(\sqrt{3}) \cong D_6$. In the former one, the quotient group is $D_3 \cong (2,3,2)$, and hence by the permutation method it is easy to see that $K_{2,u}(\sqrt{3})$ has the signature $(0 \; ; \; 2, 2, \infty^{(3)})$ and therefore

$$K_{2,u}(\sqrt{3}) \cong C_2 \star C_2 \star F_2, \tag{7.100}$$

where F_2 denotes a free group of rank two.

Secondly let us consider $H(\sqrt{3})/\Gamma_2(\sqrt{3}) \cong D_6 \cong (2,6,2)$. In a similar way we obtain the signature of $\Gamma_2(\sqrt{3})$ as $(0\ ;\ \infty^{(6)})$ and therefore it is a free group of rank five, i.e.

$$\Gamma_2(\sqrt{3}) \cong F_5. \tag{7.101}$$

(ii) Let $p = 3$. Now we have $H(\sqrt{3})/K_{3,0}(\sqrt{3}) \cong C_2$. Since R and S both map to the generator of C_2, we find

$$K_{3,0}(\sqrt{3}) = H_e(\sqrt{3}). \tag{7.102}$$

We have also proved that $H(\sqrt{3})/\Gamma_3(\sqrt{3}) \cong C_3 \wr C_2$. This Wreath product has a presentation

$$\left\langle \alpha, \beta, \gamma\ :\ \alpha^3 = \beta^3 = \gamma^2 = \alpha\beta\alpha^{-1}\beta^{-1} = I,\ \gamma\alpha\gamma = \beta \right\rangle \tag{7.103}$$

which can be written as

$$\left\langle \alpha, \gamma\ :\ \alpha^3 = \gamma^2 = (\alpha\gamma)^2(\gamma\alpha)^{-2} = I \right\rangle \tag{7.104}$$

and therefore is a finite quotient of the infinite triangle group (2,3,6), as $(\alpha\gamma)^6 = I$. Therefore $\Gamma_3(\sqrt{3})$ has the signature $(1\ ;\ 2^{(6)}, \infty^{(3)})$ and hence

$$\Gamma_3(\sqrt{3}) \cong F_4 \star \prod_{i=1}^{6} {}_\star\, C_2. \tag{7.105}$$

(iii) Let now $p \equiv \pm 1 \ mod\ 12$. Then we have shown that $H(\sqrt{3})/K_{p,u}(\sqrt{3}) \cong PSL(2,p)$ and that $H(\sqrt{3})/\Gamma_p(\sqrt{3}) \cong C_2 \times PSL(2,p)$. Similarly we find that $K_{p,u}(\sqrt{3})$ or $\Gamma_p(\sqrt{3})$ has the signature $\left(g\ ;\ \infty^{(\mu/p)}\right)$ where

$$g = 1 + \frac{\mu}{6p}(p-3). \tag{7.106}$$

Example 7.5: Let $p = 11$. Then $K_{11,5}(\sqrt{3}) = K_{11,6}(\sqrt{3})$ has the signature $\left(81\ ;\ \infty^{(60)}\right)$ and $\Gamma_{11}(\sqrt{3})$ has $\left(161\ ;\ \infty^{(120)}\right)$.

Again (7.94) and (7.95) are valid in this case.

(iv) Finally let $p \not\equiv \pm 1$ *mod* 12 and $p \neq 2$. In that case both quotient groups are $PGL(2,p)$ and as in part (iii) of $q = 4$ case, both congruence subgroups $K_{p,u}(\sqrt{3})$ and $\Gamma_p(\sqrt{3})$ have the same signature

$$\left(1 + \frac{\mu}{6p}(p-3)\ ;\ \infty^{(\mu/p)}\right). \tag{7.107}$$

Example 7.6: Let $p = 5$. Then $K_{5,u}(\sqrt{3})$ and $\Gamma_5(\sqrt{3})$ both have the signature $\left(9\ ;\ \infty^{(24)}\right)$.

Therefore we have finished the search of the principal congruence subgroups of the two important Hecke groups $\mathrm{H}(\sqrt{2})$ and $\mathrm{H}(\sqrt{3})$. We now discuss the principal congruence subgroups of another important Hecke group $\mathrm{H}(\lambda_5)$:

7.3. PRINCIPAL CONGRUENCE SUBGROUPS OF H(λ_5)

For $q = 5$, we have $\lambda = \lambda_5 = \frac{1+\sqrt{5}}{2}$, the golden ratio, as a root of the minimal polynomial $x^2 - x - 1 = 0$. Because of $\lambda^2 = \lambda + 1$, every element of $\mathbf{Q}(\lambda)$ is linear in λ, i.e. has the form $a\lambda + b$, $a, b \in \mathbf{Q}$. Therefore all entries of the matrices of $\mathrm{H}(\lambda_5)$ will have form $a\lambda + b$, $a, b \in \mathbf{Z}$.

We know that $\mathrm{H}(\lambda_5)$ is generated by the elements corresponding, in the usual way, to the matrices

$$R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & -1 \\ 1 & \lambda_5 \end{pmatrix} \tag{7.108}$$

satisfying the relations

$$R^2 = S^5 = I. \tag{7.109}$$

Let us now reduce all elements of $\mathrm{H}(\lambda_5)$ *mod p*, for a prime p. Doing this we obtain a homomorphism of $\mathrm{H}(\lambda_5)$ to $\mathrm{H}(\lambda_5)/K_{p,u}(\lambda_5)$. Under this homomorphism R, S and T are mapped to r_p, s_p and t_p. Then $\mathrm{H}(\lambda_5)/K_{p,u}(\lambda_5)$ is a homomorphic image of

$$\left\langle r_p,\, s_p \,:\, r_p^2 = s_p^5 = t_p^p = I,\, t_p = r_p s_p \right\rangle. \tag{7.110}$$

Let us now discuss the possibilities. First we have three exceptional cases:

Case 1: $p = 2$. In this case the polynomial equation $x^2 - x - 1 = 0$ has no solutions in $GF(2) = \mathbf{Z_2} = \{0,1\}$. Therefore we extend $\mathbf{Z_2}$ by adding u where u is a root of the quadratic equation $x^2 + x + 1 = 0$. Then $\mathbf{Z_2}[\mathrm{u}] = \{0, 1, \mathrm{u}, 1 + \mathrm{u}\}$. It is then easy to see that in $\mathrm{H}(\lambda_5)/K_{2,u}(\lambda_5)$ we have the relations $r_2^2 = s_2^5 = t_2^2 = I$ which implies that this quotient is isomorphic to the dihedral group D_5.

Case 2: $p = 3$. In that case r_3, s_3 and t_3 satisfy the relations $r_3^2 = s_3^5 = t_3^3 = I$; that is, $\mathrm{H}(\lambda_5)/K_{3,u}(\lambda_5)$ is A_5, as A_5 is simple.

Case 3: $p = 5$. Now $\sqrt{5}$ can be thought of as equal to $0 \in GF(5)$. Therefore $\lambda_5 \equiv \frac{1}{2} \equiv 3 \mod 5$. As $3 \in GF(5)$, there is a homomorphism of $\mathrm{H}(\lambda_5)$ to $PSL(2,5)$. Then we have the relations $r_5^2 = s_5^5 = t_5^5 = I$ in $\mathrm{H}(\lambda_5)/K_{5,3}(\lambda_5)$. Therefore $\mathrm{H}(\lambda_5)/K_{5,3}(\lambda_5)$ is isomorphic to a finite quotient of the infinite triangle group (2,5,5). Now

$$r_5 t_5^2 \equiv \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \mod 5. \tag{7.111}$$

Let $u_5 = t_5^2$. Since $tr\,(r_5 u_5) = 1$, $r_5 u_5$ is of order three. Then $\mathrm{H}(\lambda_5)/K_{5,3}(\lambda_5)$ has a presentation $\langle r_5, u_5 \,|\, r_5^2 = u_5^5 = (r_5 u_5)^3 = I \rangle$, that is $\mathrm{H}(\lambda_5)/K_{5,3}(\lambda_5)$ is a (2,3,5)–group, i.e. it is isomorphic to the alternating group A_5.

From now on we let $p \geq 7$ be a prime. Then we have two cases according to $p \equiv \pm 1 \mod 10$ or not:

Case 4: If 5 is a square *mod* p, i.e. if $\left(\begin{array}{c}5\\p\end{array}\right) = 1$, i.e. if $p \equiv \pm 1 \mod 10$, then $\sqrt{5}$ can be considered in $GF(p)$. In fact as $P_5^*(\lambda_5)$ is quadratic, there are two values u and v of λ_5 *modulo p*. Hence the elements r_p, s_p and t_p would belong to $PSL(2,p)$. Then we have two homomorphisms

$$\theta_i : H(\lambda_5) \longrightarrow PSL(2,p), \ i = 1,2, \tag{7.112}$$

induced by $\lambda_5 \to u$ and $\lambda_5 \to v$. Since the G_0-triple (r_p, s_p, t_p) is neither exceptional nor singular, by Theorem 7.3, it generates $PSL(2,p)$. Therefore H(λ_5) has two normal congruence subgroups $K_{p,u}(\lambda_5)$ and $K_{p,v}(\lambda_5)$ for $p \equiv \pm 1 \mod 10$.

Example 7.7: Let $p = 11$. Then there are two candidates for λ_5, 4 or 8. Now consider ST^6. For $\lambda_5 \to 4$, ST^6 is of order 6 and for $\lambda_5 \to 8$, it is of order 3. Therefore there are two different kernels $K_{11,4}(\lambda_5)$ and $K_{11,8}(\lambda_5)$.

Case 5: Finally let $p \not\equiv \pm 1 \mod 10$ and $p \neq 5$. That is, p is such that 5 is not a square *mod* p. In this case $\sqrt{5}$ cannot be considered as an element of $GF(p)$. Hence we extend it to $GF(p^2)$ as two is the degree of the minimal polynomial of λ_5. Then $\sqrt{5}$ can be considered in $GF(p^2)$ and then we have a homomorphism

$$\theta' : H(\lambda_5) \longrightarrow PSL(2,p^2). \tag{7.113}$$

Since $p \geq 7$, the G_0-triple (r_p, s_p, t_p) is neither exceptional nor singular. Hence by Theorem 7.2, it generates a projective subgroup of $PSL(2,p^2)$. By Theorem 7.3, it is either $PSL(2,p^2)$ or $PGL(2,p)$. In this case we must consider the irregularity of the corresponding **k** -triple which is $(0, u, 2)$ where $\lambda_5 \equiv u$ in $GF(p^2)$. By the discussion just before Theorem 7.4, this **k**-triple is not irregular. Hence Theorem 7.4 implies that

$$H(\lambda_5)/K_{p,u}(\lambda_5) \cong PSL(2,p^2). \tag{7.114}$$

As a result of the five cases investigated above we have the following:

Theorem 7.7: The quotient groups of the Hecke group H(λ_5) by its principal congruence subgroups $K_{p,u}(\lambda_5)$ are as follows:

$$H(\lambda_5)/K_{p,u}(\lambda_5) \cong \begin{cases} PSL(2,p) & \text{if} \quad p \equiv \pm 1 \ mod\ 10, \\ PSL(2,p^2) & \text{if} \quad p \equiv \pm 3 \ mod\ 10, \text{ and } p \neq 3, \\ D_5 & \text{if} \quad p = 2, \\ A_5 & \text{if} \quad p = 3, 5. \end{cases} \tag{7.115}$$

Let us now determine the group theoretical structure of these kernels. As we have the relations

$$r_p^2 = s_p^5 = I \tag{7.116}$$

in $H(\lambda_5)/K_{p,u}(\lambda_5)$, all these subgroups are free. Also

$$t_p^p = I \tag{7.117}$$

implies that $K_{p,u}(\lambda_5)$ is of level p. Now by the permutation method and Riemann–Hurwitz formula it has the signature

$$\left(1 + \frac{\mu}{20p}(3p - 10)\ ;\ \infty^{(\mu/p)}\right) \tag{7.118}$$

depending only on the index μ of $K_{p,u}(\lambda_5)$ in H(λ_5).

Example 7.8: $K_{2,u}(\lambda_5) \cong \left(0\ ;\ \infty^{(5)}\right)$, $K_{3,u}(\lambda_5) \cong \left(0\ ;\ \infty^{(20)}\right)$ and $K_{5,3}(\lambda_5) \cong \left(4\ ;\ \infty^{(12)}\right)$.

The first of these three kernels corresponds to a dihedron. The second one geometrically corresponds to one of the five platonic solids, *icosahedron*, which can be thought of as a regular map of type $\{3,5\}$. Finally the third one corresponds to a *great dodecahedron*, a regular map of type $\{5,5\}$.

Let us remind ourselves of what we have already done in this chapter. For q = 4 and 6 we have found the kernel $K_{p,u}(\sqrt{m})$ and then by means of it we have calculated the principal congruence subgroups $\Gamma_p(\sqrt{m})$. We have seen that for a lot of values of p, these two congruence subgroups are different. We have also calculated the principal congruence subgroups of $H(\lambda_5)$. We saw that for $p \equiv \pm 1 \mod 10$ there are two $K_{p,u}(\lambda_5)$ subgroups unlike $q = 4$ and 6 cases.

7.4. PRINCIPAL CONGRUENCE SUBGROUPS OF OTHER HECKE GROUPS

We have considered the principal congruence subgroups in the cases $q = 4$, 5 and 6, and recalled some results for $q = 3$. We now discuss the case where $q \geq 7$ is a prime. We deal with the case of $q = 7$ seperately because of its close relation with the Hurwitz groups. We shall show that this is the only case, apart from the modular group, that gives the quotients $H(\lambda_q)/K_{p,u}(\lambda_q)$ as Hurwitz groups. Actually all of these quotients, except for $p = 2$, are Hurwitz groups.

Let $q = 7$. Since we do not have any exceptional or singular triples for $p > 2$, by Theorem 7.3, (r_p, s_p, t_p) generates a projective subgroup. Now the minimal polynomial $P_7^*(x)$ is of degree three, which is odd. Hence the field κ which is either $GF(p)$ or $GF(p^3)$ cannot be a quadratic extension of any other field κ_0. Therefore by Theorem 7.4 we cannot have any projective general linear groups as a quotient of $H(\lambda_7)$ by a principal congruence subgroup. That is, the only possible projective groups generated by the G_0–triple (r_p, s_p, t_p) are $PSL(2, p^n)$, $n \mid d = 3$, i.e. $PSL(2,p)$ or $PSL(2,p^3)$. Let us now deal with the possibilities:

Case 1: $p = 2$. In this case we have an exceptional **N**–triple (2,7,2) which gives

$$H(\lambda_7)/K_{2,u}(\lambda_7) \cong D_7. \tag{7.119}$$

Case 2: $p = 7$. Now the minimal polynomial $P_7^*(x)$ has a root, $u = 5$, of multiplicity three in $GF(7)$. Indeed

$$(x-5)^3 \equiv (x+2)^3 \equiv x^3 - x^2 - 2x + 1 = P_7^*(x) \mod 7. \tag{7.120}$$

Since (R_7, S_7, T_7) is neither exceptional nor singular, it generates, by Theorem 7.3, $PSL(2,7)$. Therefore the quotient group

$$H(\lambda_7)/K_{7,u}(\lambda_7) \cong PSL(2,7) \tag{7.121}$$

is a Hurwitz group.

Case 3: $p \equiv \pm 1 \; mod\, 7$. This is equivalent to say that $p \equiv \pm 1 \; mod\, 14$. Since 7 is prime and divides the order of $PSL(2,p)$, there are elements of order seven in $PSL(2,p)$. That is, there is a homomorphism of $\mathrm{H}(\lambda_7)$ to $PSL(2,p)$ for each of the three roots of $P_7^*(\lambda_7)$ whenever $p \equiv \pm 1 \; mod\, 14$. Since (r_p, s_p, t_p) is neither exceptional, singular nor irregular, by Theorem 7.3, it generates the whole group $PSL(2,p)$. Therefore, as in the case $q = 5$, $\mathrm{H}(\lambda_7)$ has three normal congruence subgroups $K_{p,u_i}(\lambda_7)$, $i = 1,2,3$ with quotient $PSL(2,p)$.

Case 4: Finally let $p \not\equiv \pm 1 \; mod\, 7$ and let $p \neq 2$. In that case, 7 does not divide the order of $PSL(2,p)$ implying that there is no homomorphism of $\mathrm{H}(\lambda_7)$ to $PSL(2,p)$. In another words, the minimal polynomial $\mathrm{P}_7^*(x)$ has no roots in $GF(p)$. Hence we need to extend it to $GF(p^3)$, as the degree of $\mathrm{P}_7^*(x)$ is three, and then we have a homomorphism

$$\theta \; : \; H(\lambda_7) \longrightarrow PSL(2,p^3) \tag{7.122}$$

induced as before. By Theorems 7.2 and 7.3, (r_p, s_p, t_p) generates $PSL(2,p^3)$ which is a Hurwitz group.

We have thus completed the discussion of the principle congruence subgroups of $\mathrm{H}(\lambda_7)$. At the end we have the following result:

Theorem 7.8: The quotient groups of the Hecke group $\mathrm{H}(\lambda_7)$ by its principal congruence subgroups $K_{p,u}(\lambda_7)$ are as follows:

$$H(\lambda_7)/K_{p,u}(\lambda_7) \cong \begin{cases} D_7 & \text{if} \quad p = 2 \\ PSL(2,7) & \text{if} \quad p = 7 \\ PSL(2,p) & \text{if} \quad p \equiv \pm 1 \;\; mod\, 7 \\ PSL(2,p^3) & \text{if} \quad p \not\equiv \pm 1 \;\; mod\, 7, \; p \neq 2, \end{cases} \tag{7.123}$$

Now we consider the prime q case where $q > 7$. Of course all ideas in this case are also true for $q = 3$, 5 and 7.

Recall that for $q = 7$ and $p \equiv \pm 1 \; mod 7$, we obtained three homomorphisms from $\mathrm{H}(\lambda_7)$ to $PSL(2,p)$ one for each root of $P_7^*(x)$ in $GF(p)$, and these homomorphisms gave three non–conjugate normal subgroups of $\mathrm{H}(\lambda_7)$. A similar thing seems to happen when $q > 7$. Everytime we reduce $P_q^*(x)$ *modulo* p, it splits either in $GF(p)$ or in a finite extension of $GF(p)$. That is, the roots of $P_q^*(x)$ *modulo* p are in $GF(p)$ or in a finite extension of $GF(p)$. If a particular root u is in $GF(p)$, then there is a homomorphism from $\mathrm{H}(\lambda_q)$ to $PSL(2,p)$, and the kernel of this homomorphism is $K_{p,u}(\lambda_q)$. Similarly, if a root u lies in $GF(p^n)$ where n is less than or equal to the degree d of the minimal polynomial $P_q^*(x)$, then there is a homomorphism from $\mathrm{H}(\lambda_q)$ to $PSL(2,p^n)$ with the kernel $K_{p,u}(\lambda_q)$. Therefore for each root u, we have a chance of obtaining another normal subgroup $K_{p,u}(\lambda_q)$.

We have already seen that the G_0–triple (r_p, s_p, t_p) generates an exceptional subgroup if $p = 2$. In this case the quotient group $\mathrm{H}(\lambda_q)/K_{2,u}(\lambda_q)$ is associated with the $\mathbf{N}$–triple $(2, q, 2)$ which is dihedral of order $2q$.

Earlier in this chapter we have shown the necessary and sufficient condition to have a singular triple as $\lambda_q^2 \equiv 0 \; mod \; p$. We have also shown that there is a unique possible singular triple when $q = 2p^n$, p odd prime, $n \geq 1$ or $q = 2^n$, $n \geq 2$, and no singular triples for the other values of q. That is, we will not have any singular triples when q is prime > 7.

Since (r_p, s_p, t_p) is neither exceptional nor singular for $p > 2$, it generates, by Theorem 7.2, a projective subgroup of G. To find which projective subgroup is generated by this triple, we must consider the field $\mathbf{k}$ and its smallest subfield κ, containing the traces α, β and γ, *modulo* p, of r_p, s_p and t_p, respectively. Here we have three possible cases:

Case 1: $p = q$. In this case $x_0 = q - 2$ is the only root of the minimal polynomial $\mathrm{P}_q^*(x)$ *mod* p. To prove this we show that -1 is the only root of $\Phi_p(x) = \frac{x^p+1}{x+1} = x^{p-1} - x^{p-2} + x^{p-3} - \ldots + x^2 - x + 1$. Consider the expansion of $(x+1)^{p-1}$. The binomial coefficients are congruent to ± 1 *mod* p:

$$\begin{pmatrix} p-1 \\ r \end{pmatrix} = \tfrac{(p-1).\dots.(p-r)}{r!} \equiv (-1)^r.\tfrac{r!}{r!} = (-1)^r \ mod\, p.$$

Therefore $\Phi_p(x)$ is congruent to $(x+1)^{p-1}$. Hence all $p-1$ roots of $\Phi_p(x)$ are congruent to -1 *modulo* p, as required. Therefore all roots are in $GF(p)$. Then there is a homomorphism of H(λ_q) to $PSL(2,p)$ for each root u. Again by a similar argument we find

$$H(\lambda_q)/K_{q,u}(\lambda_q) \cong PSL(2,q) \tag{7.124}$$

for each u.

Case 2: Let $p \equiv \pm 1 \ mod\, q$. Since q is an odd prime, this is equivalent to say that $p \equiv \pm 1 \ mod\, 2q$; i.e. $p = kq \pm 1$ with $k \in \mathbf{N}$ is even. Now

$$\frac{p(p-1)(p+1)}{2} : q = \frac{p(p-1)(p+1)}{2} : \frac{p \mp 1}{k} \in \mathbf{N} \tag{7.125}$$

and therefore q divides the order of $PSL(2,p)$; i.e. there are elements of order q in $PSL(2,p)$. Then there exists a homomorphism

$$\theta : H(\lambda_q) \longrightarrow PSL(2,p) \tag{7.126}$$

for each root u in $GF(p)$. Therefore there are $d = deg\, P_q^*(\lambda_q)$ normal congruence subgroups $K_{p,u}(\lambda_q)$ of H(λ_q). This implies

Theorem 7.9: If $p \equiv \pm 1 \ mod q$, then there exists a homomorphism Θ : $H(\lambda_q) \longrightarrow PSL(2,p)$ for each root $u \in GF(p)$. The kernel of this homomorphism is $K_{p,u}(\lambda_q)$.

Corollary 7.2: For each prime q, H(λ_q) has infinitely many normal subgroups.

Proof: This follows from Dirichlet's Theorem on primes in arithmetic progressions.

Note that as every finitely generated Fuchsian group has a surface subgroup of finite index, Corollary 7.2 also follows from Malcev's theorem on residual finiteness.

Corollary 7.3: Let $q \geq 3$, $q \in \mathbf{N}$. Then $\mathrm{H}(\lambda_q)$ has infinitely many normal subgroups.

Proof: It follows from Corollary 7.2 as there exists a homomorphism from $\mathrm{H}(\lambda_q)$ to $\mathrm{H}(\lambda_p)$ for each prime divisor p of q.

Case 3: Let $p \not\equiv \pm 1 \ \ mod\ q$ and $p \neq 2, q$. Then q does not divide the order of $PSL(2,p)$ and therefore no homomorphism from $\mathrm{H}(\lambda_q)$ to $PSL(2,p)$ exists, i.e. $\mathrm{P}_q^*(x)$ has no roots in $GF(p)$. We extend $GF(p)$ to $GF(p^n)$ where n is less than or equal to the degree d of the minimal polynomial $\mathrm{P}_q^*(x)$ which is

$$d = \frac{q-1}{2} \tag{7.127}$$

as q is an odd prime. Let u be a root of $P_q^*(x)$ in $GF(p^n)$. Then by Theorems 7.2 and 7.3, we have a homomorphism of $\mathrm{H}(\lambda_q)$ to $PSL(2,p^n)$ if n is odd, and to $PGL(2,p^{n/2})$ if n is even. The kernel of this homomorphism is $K_{p,u}(\lambda_q)$.

Chapter 8

NORMAL SUBGROUPS OF H($\sqrt{2}$)

8.0. INTRODUCTION

In the early chapters we often noted the importance of H($\sqrt{2}$). We saw that it is, after the modular group, the most worked and accessible Hecke group. Therefore the study of its normal subgroups is also important to us. In this chapter we consider the normal subgroups of H($\sqrt{2}$) and discuss the relations between them.

In the introduction we have classified the elements of H($\sqrt{2}$) into two classes as odd and even ones. We denoted by $H_e(\sqrt{2})$ the even subgroup of H($\sqrt{2}$) consisting of all even elements in H($\sqrt{2}$). Having index two, it is a normal subgroup and it contains infinitely many normal subgroups of H($\sqrt{2}$). Here we shall prove that $H_e(\sqrt{2})$ is actually isomorphic to the free product of the infinite cyclic group **Z** and a finite cyclic group of order two.

An important property of H($\sqrt{2}$) is its commensurability with the modular group. We have earlier noted that H($\sqrt{2}$) and H($\sqrt{3}$) are the only Hecke groups that are commensurable with the modular group Γ. But although a conjugate of H($\sqrt{2}$) and Γ have a common subgroup, no common normal subgroup in both of them exists, as we proved.

In this chapter we discuss the normal subgroups of $H(\sqrt{2})$. Being the free product of two finite cyclic groups of orders two and four, $H(\sqrt{2})$ has two kinds of subgroups; those which are free of rank $2g+t-1$ and those which are free products of a cyclic groups of order two, b cyclic groups of order four and c infinite cyclic groups (see the Kurosh subgroup theorem, Theorem 0.8).

We first discuss the power subgroups $H^m(\sqrt{2})$ generated by the m–th powers of all elements of $H(\sqrt{2})$. We shall deduce that, unlike odd q case (and particularly modular group case where $q=3$), it is not possible to write $H(\sqrt{2})$ as a product of two or more proper normal power subgroups. We shall investigate $H^2(\sqrt{2})$ first and deduce that for $m>2$, $H^m(\sqrt{2})$ is either free if m is divisible by four, or equal to $H(\sqrt{2})$ if m is odd, or equal to $W_m(\sqrt{2})$ if $m \equiv 2 \mod 4$.

The search of genus 0 and genus 1 normal subgroups of the Hecke groups has been done in Chapters 4 and 5. Therefore we will not go into details here and only discuss them briefly. We shall see that $H(\sqrt{2})$, unlike the modular group case, has infinitely many normal genus 0 subgroups, as we can find a homomorphism of $H(\sqrt{2})$ to the dihedral group D_n for any natural number n, each giving a normal subgroup of genus 0 of $H(\sqrt{2})$ containing a finite number of elements of order two. This will also prove that unlike odd q case (and again unlike the modular group case), $H(\sqrt{2})$ has infinitely many normal subgroups with torsion.

The study of normal subgroups of genus 1 will play an important role in the classification of normal subgroups of $H(\sqrt{2})$. They correspond to regular maps of type $\{4,4\}$. These regular maps are classified in [Jo–Si,2] and in [Co–Mo,1] as $\{4,4\}_{r,s}$ for non–negative integers r,s and therefore are infinitely many. This means that $H(\sqrt{2})$ has infinitely many normal subgroups of genus 1 like the modular group. They have also been discussed in [Ke–Ro,1] by Kern–Isberner and Rosenberger.

By the Riemann–Hurwitz formula, a normal subgroup N of finite genus $g \geq 1$ in $\mathrm{H}(\sqrt{2})$ always has finite index and therefore will be finitely generated.

$\mathrm{H}(\sqrt{2})$ has, as we shall prove, infinitely many normal free subgroups of finite index. Therefore their investigation will form an important part of this chapter. We will determine their group theoretical structure. They all have index divisible by four, while those of genus 1 particularly have level four.

In the classification of normal subgroups of genus 1, we shall often use two particular subgroups, the commutator subgroup $\mathrm{H}'(\sqrt{2})$ of $\mathrm{H}(\sqrt{2})$ and $K = H'(\sqrt{2}) \cup RS^2.H'(\sqrt{2})$. Since $\mathrm{H}'(\sqrt{2})$ has index 8 in $\mathrm{H}(\sqrt{2})$, K will have index four in $\mathrm{H}(\sqrt{2})$. They are both normal free subgroups on three and two free generators respectively, having genus 1. We shall prove that all normal subgroups of genus 1 of $\mathrm{H}(\sqrt{2})$ lie between K and its commutator subgroup K', and therefore by the Kurosh subgroup theorem, they are all free of level four, i.e. all normal subgroups of genus 1 in $\mathrm{H}(\sqrt{2})$ are free.

We have already noted that a normal subgroup N of genus 1 of $\mathrm{H}(\sqrt{2})$ corresponds to a regular map $\{4,4\}_{r,s}$ where

$$|\,Aut^{+}(\{4,4\}_{r,s})\,| = |\,H(\sqrt{2}) : N\,| = 4(r^2+s^2). \tag{8.1}$$

Using this we showed in Chapter 5 that the number of normal subgroups of genus 1 and given index $\mu = 4t$ (as the level is necessarily four) in $\mathrm{H}(\sqrt{2})$ is

$$N(\mu) = \frac{1}{4}\#\left\{(r,s) \in \mathbf{Z}^2 : \mathrm{r}^2+\mathrm{s}^2 = \mathrm{t}\right\}. \tag{8.2}$$

This number has also been found by Kern–Isberner and Rosenberger in [Ke-Ro,1] using the fact that the function $N(\mu)$ is a multiplicative function.

Jones and Singerman showed that every normal subgroup corresponds to a unique regular map (see [Jo–Si,1]). Therefore one way of studying normal subgroups of $H(\lambda_q)$ is to study corresponding regular maps.

When $g \geq 2$, $H(\sqrt{2})$ has, by the Riemann–Hurwitz formula, only finitely many normal subgroups of genus g and therefore there will only be finitely many corresponding regular maps. The final part of this chapter is about the relations between the normal subgroups of genus $g \geq 0$ and the corresponding regular maps.

Also in this chapter, we shall refer to a paper of C. Maclachlan, [Mc,2], for an infinite class of normal subgroups denoted by $\hat{K}(g)$. This class is actually obtained for any q divisible by four, but when $q > 4$, its elements contain torsion.

The principal congruence subgroups, of course, also form an important class of normal subgroups of $H(\sqrt{2})$. But because of their similarity with the ones of $H(\sqrt{3})$, and because of the length of their investigation, we have already discussed them separately in Chapter 7.

In Appendix 1, the list of all normal subgroups of index < 60 of $H(\sqrt{2})$, and the lists of all corresponding regular maps with genus $g \leq 7$ are given. The number of normal subgroups of index upto 100 in $C_2 \star C_n$ has been independently found by Conder (see [Cn,1]). The numbers found here coincide with the ones found there. Also pictures of some interesting regular maps of type $\{4, n\}$ are given at the end of this thesis.

We begin with the power subgroups $H^m(\sqrt{2})$ of $H(\sqrt{2})$:

8.1. POWER SUBGROUPS $H^m(\sqrt{2})$ OF $H(\sqrt{2})$

Let m be a positive integer. Let us define $H^m(\sqrt{2})$ to be the subgroup generated by the m–th powers of all elements of H($\sqrt{2}$). H^m($\sqrt{2}$) is called the *m–th power subgroup* of H($\sqrt{2}$). As fully invariant subgroups, they are normal in H($\sqrt{2}$).

From the definition one can easily deduce that

$$H^m(\sqrt{2}) > H^{mn}(\sqrt{2}) \tag{8.3}$$

and that

$$\left(H^m(\sqrt{2})\right)^n > H^{mn}(\sqrt{2}). \tag{8.4}$$

Using (8.3) it is easy to deduce that

$$H^m(\sqrt{2}).H^n(\sqrt{2}) = H^{(m,n)}(\sqrt{2}) \tag{8.5}$$

as in the case of odd q given before (see Chapter 6). Here (m,n) denotes the greatest common divisor of m and n. But the useful property that

$$H^2(\lambda_q).H^q(\lambda_q) = H(\lambda_q), \tag{8.6}$$

which is a direct result of (8.5) in the case of odd q (particularly modular group), does not hold here since $q = 4$. Therefore it will not be possible to express H($\sqrt{2}$) as a product of its proper power subgroups.

Let us now discuss the group theoretical structure of these subgroups. First we have

Theorem 8.1: The normal subgroup H^2($\sqrt{2}$) is isomorphic to the free product of the infinite cyclic group **Z** and two finite cyclic groups of order two. Also

$$H(\sqrt{2})/H^2(\sqrt{2}) \cong C_2 \times C_2, \tag{8.7}$$

$$H(\sqrt{2}) = H^2(\sqrt{2}) \cup RH^2(\sqrt{2}) \cup SH^2(\sqrt{2}) \cup RSH^2(\sqrt{2}), \tag{8.8}$$

and

$$H^2(\sqrt{2}) = < S^2 > \star < RS^2R > \star < RSRS^3 > . \qquad (8.9)$$

The elements of $\mathrm{H}^2(\sqrt{2})$ are characterised by the property that the sums of the exponents of R and S are both even.

Proof: Set $M = < S^2, RS^2R, RSRS^3 >$. Then M is normal in $\mathrm{H}(\sqrt{2})$ and clearly, the elements of M satisfy the requirements of the Theorem, i.e. the sums of the exponents of R and S are both even for each element.

If $r = \mathrm{H}^2(\sqrt{2})R$ and $s = \mathrm{H}^2(\sqrt{2})S$, then the quotient group $\mathrm{H}(\sqrt{2})/\mathrm{H}^2(\sqrt{2})$ is generated by r, s with $r^2 = s^2 = (rs)^2 = 1$. Now $rs = \begin{pmatrix} 1 & \sqrt{2} \\ 0 & 1 \end{pmatrix} \notin \mathrm{H}^2(\sqrt{2})$, so $r \neq s$ and so $< r, s > \cong C_2 \times C_2$. Hence (8.7) is clear. Let us now use the permutation method to find the signature of $\mathrm{H}^2(\sqrt{2})$. As each of R, S and T goes to elements of order two, they have the following permutation representations:

$$\begin{array}{ccc} R & \longmapsto & (1\ 2)(3\ 4) \\ S & \longmapsto & (1\ 3)(2\ 4) \\ T & \longmapsto & (1\ 4)(2\ 3). \end{array} \qquad (8.10)$$

Therefore the signature of $\mathrm{H}^2(\sqrt{2})$ is $(g\ ;\ 2, 2, \infty, \infty)$. Now by the Riemann–Hurwitz formula $g = 0$. Hence $\mathrm{H}^2(\sqrt{2})$ is isomorphic to the free product of $\mathbf{Z}$ and two C_2's. As the unique normal subgroup of $\mathrm{H}(\sqrt{2})$ with quotient $C_2 \times C_2$, it must be equal to this free product.

If we choose I, R, S, RS as a Schreier transversal for $\mathrm{H}^2(\sqrt{2})$ then it is easy to see that M is a set of generators for $\mathrm{H}^2(\sqrt{2})$.

We also have

Theorem 8.2: Let m be a positive odd integer. Then

$$H^m(\sqrt{2}) = H(\sqrt{2}). \tag{8.11}$$

Proof: It is clear as the quotient is trivial.

We finally have

Theorem 8.3: Let m be a positive integer such that $m \equiv 2 \mod 4$. Then $\mathrm{H}^m(\sqrt{2})$ is the free product of the infinite cyclic group $\mathbf{Z}$ and m finite cyclic groups of order two.

Proof: It is easy to show that the quotient group is isomorphic to the dihedral group D_m of order $2m$. The permutation representations of R, S and T are

$$\begin{array}{lll} R & \longmapsto & (1\ 2)(3\ 4)...(2m-1\ 2m) \\ S & \longmapsto & (2\ 3)(4\ 5)...(2m\ 1) \\ T & \longmapsto & (1\ 3\ 5\ ...\ 2m-1)(2m\ 2m-2\ ...\ 4\ 2). \end{array} \tag{8.12}$$

Then $\mathrm{H}^m(\sqrt{2})$ has the signature $(0\ ;\ 2^{(m)}, \infty, \infty)$ similarly to the previous cases, i.e. $\mathrm{H}^m(\sqrt{2})$ is the free product given in the statement of the Theorem.

Note that when $m \equiv 2 \mod 4$, $\mathrm{H}^m(\sqrt{2}) = W_m(\sqrt{2})$.

We can now conclude our research of the power subgroups of $\mathrm{H}(\sqrt{2})$ making a few remarks. Note that we have already proved

$$H^m(\sqrt{2}) = \begin{cases} \mathrm{H}(\sqrt{2}) & \text{if } m \text{ is odd,} \\ W_m(\sqrt{2}) & \text{if } m \equiv 2 \mod 4. \end{cases} \tag{8.13}$$

Because of this we have only left to consider the case where m is a multiple of four. Let now $m = 4k$, $k \in \mathrm{N}$. Then in $\mathrm{H}(\sqrt{2})/\mathrm{H}^m(\sqrt{2})$ we have the relations $r^2 = s^4 = I$ where r and s are the images of R and S, respectively, under the homomorphism of $H(\sqrt{2})$ to $H(\sqrt{2})/H^m(\sqrt{2})$. These relations imply that $H^m(\sqrt{2})$ is a free group.

We now investigate the structure of another important normal subgroup of $H(\sqrt{2})$, namely the even subgroup $H_e(\sqrt{2})$ defined in the introduction:

Theorem 8.4: The even subgroup $H_e(\sqrt{2})$ of $H(\sqrt{2})$ defined by

$$H_e(\sqrt{2}) := \left\{ M = \begin{pmatrix} a & b\sqrt{2} \\ c\sqrt{2} & d \end{pmatrix} : M \in H(\sqrt{2}) \right\} \tag{8.14}$$

is a normal subgroup of index two of $H(\sqrt{2})$. Also

$$H(\sqrt{2}) = H_e(\sqrt{2}) \cup RH_e(\sqrt{2}), \tag{8.15}$$

$$H_e(\sqrt{2}) \cong < T > \star < TU > = < RS > \star < RS^2R >, \tag{8.16}$$

and therefore $H_e(\sqrt{2})$ is isomorphic to the free product of the infinite cyclic group (generated by RS) and the finite cyclic group of order two (generated by RS^2R).

Proof: Having index two $H_e(\sqrt{2})$ is a normal subgroup of $H(\sqrt{2})$. By the permutation method the signature of $H_e(\sqrt{2})$ is $(0\ ;\ 2, \infty, \infty)$ as each of R and S go to elements of order two.

Let us now choose I, R as a Schreier transversal for the even subgroup. Then it is easy to find that $H_e(\sqrt{2})$ has the parabolic generators $T = RS$ and $U = SR$ with their product TU being the elliptic generator of order two.

Finally as $R \notin H_e(\sqrt{2})$, (8.15) follows.

The even subgroup is very important amongst the normal subgroups of $H(\sqrt{2})$. It is one of the three normal subgroups of $H(\sqrt{2})$ with cyclic quotient of order two and contains infinitely many normal subgroups of $H(\sqrt{2})$. It will often be used in the classification and determination of the group theoretical structures of certain types of normal subgroups like principal congruence subgroups, etc.

Recall that the normal subgroups of genus 0 of the Hecke groups have been discussed in Chapter 4. We now discuss these subgroups particularly for $H(\sqrt{2})$ without going into details. For some proofs see Chapter 4.

8.2. NORMAL SUBGROUPS OF GENUS 0 OF $H(\sqrt{2})$

It is well-known that if N is a normal subgroup of genus 0, then $H(\sqrt{2})/N$ is a group of automorphisms of the sphere, so that $H(\sqrt{2})/N$ is isomorphic to a finite subgroup of $SO(3)$, and therefore, is isomorphic to one of the finite triangle groups. As we can always find a homomorphism of $H(\sqrt{2})$ to the dihedral group D_n for every $n \in \mathbb{N}$, $H(\sqrt{2})$ has infinitely many normal subgroups of genus 0 unlike the odd q case and in particularly the modular group case.

If we map $H(\sqrt{2})$ to the cyclic group $C_d \cong (1, d, d)$ where $d \mid 4$, we obtain a normal subgroup $N \cong (0\ ;\ 2^{(d)}, 4/d, \infty)$. This subgroup is denoted by $Y_d(\sqrt{2})$ and is isomorphic to the free product of a cyclic group of order $4/d$ and d cyclic groups of order two. If $d \nmid 4$ then there is no homomorphism of $H(\sqrt{2})$ to a cyclic group C_d.

Secondly, if we map $H(\sqrt{2})$ to the dihedral group $D_d \cong (2, d, 2)$ where $d \mid 4$, we obtain $N \cong (0\ ;\ 4/d, 4/d, \infty^{(d)})$ which was denoted by $S_d(\sqrt{2})$. Note that $S_1(\sqrt{2})$ and $S_2(\sqrt{2})$ contain elements of finite order while $S_4(\sqrt{2})$ is free of rank three. Again if d is not a divisor of four, this process is not possible.

Thirdly, by mapping onto $S_4 \cong (2, 4, 3)$ we obtain a normal subgroup denoted by $T_4(\sqrt{2})$ with signature $(0\ ;\ \infty^{(8)})$ which is isomorphic to a free group of rank seven.

We have already found seven normal subgroups of $H(\sqrt{2})$ with genus 0. We now introduce an infinite family of normal subgroups of genus 0 by considering the homomorphism of $H(\sqrt{2})$ onto $D_n \cong (2,2,n)$ for any $n \in \mathbf{N}$. Then we obtain the normal subgroup $W_n(\sqrt{2})$ with signature $(0\ ;\ 2^{(n)},\infty,\infty)$. These subgroups have the property that each $W_n(\sqrt{2})$ contains infinitely many normal subgroups $W_m(\sqrt{2})$ of genus 0, since we have $W_{nk}(\sqrt{2}) \lhd W_n(\sqrt{2})$.

Hence we have the following result:

Theorem 8.5: All normal subgroups of $H(\sqrt{2})$ with genus 0 are $H(\sqrt{2})$, $Y_2(\sqrt{2})$, $Y_4(\sqrt{2})$, $S_1(\sqrt{2})$, $S_4(\sqrt{2})$, $T_4(\sqrt{2})$ and $W_n(\sqrt{2})$ for $n \in \mathbf{N}$.

Corollary 8.1: $H(\sqrt{2})$ has infinitely many normal subgroups of genus 0.

Remarks 8.1: **(i)** Note that in the case of modular group, and in general, of any odd q, we only have finitely many normal subgroups of genus 0. We shall see that for every even q, $H(\lambda_q)$ has infinitely many normal subgroups of genus 0.

(ii) It is clear that when $m \equiv 2 \mod 4$, the subgroups $H^m(\sqrt{2})$ and $W_m(\sqrt{2})$ coincide.

(iii) Note that the subgroups $H_e(\sqrt{2})$, $S_2(\sqrt{2})$, $H^2(\sqrt{2})$ and $H^n(\sqrt{2})$ for $n \equiv 2 \mod 4$ are automatically included in the list of Theorem 8.5, since $H_e(\sqrt{2}) = W_1(\sqrt{2})$, $S_2(\sqrt{2}) = H^2(\sqrt{2}) = W_2(\sqrt{2})$ and finally $H^n(\sqrt{2}) = W_n(\sqrt{2})$ for $n \equiv 2 \mod 4$. We can also see that the congruence subgroups $\Gamma_2(\sqrt{2})$, $K_2(\sqrt{2})$, $\Gamma_3(\sqrt{2})$ and $K_3(\sqrt{2})$ are also in this list since $K_2(\sqrt{2}) = W_1(\sqrt{2})$, $\Gamma_2(\sqrt{2}) = W_4(\sqrt{2})$ and $K_3(\sqrt{2}) = \Gamma_3(\sqrt{2}) = T_4(\sqrt{2})$.

8.3. FREE NORMAL SUBGROUPS OF $H(\sqrt{2})$

As a free product of two finite cyclic groups of orders two and four, $H(\sqrt{2})$ has, by the Kurosh subgroup theorem, some free normal subgroups. We shall prove in this section that these are actually infinitely many. We shall also give a characterisation of them. First we have

Lemma 8.1: Let N be a non-trivial subgroup of $\mathrm{H}(\sqrt{2})$. Then N is free if and only if it contains no elements of finite order.

The proof of this lemma is just a special case of the proof of Lemma 6.2.

Lemma 8.2: The only normal subgroups of $\mathrm{H}(\sqrt{2})$ containing elements of finite order are $\mathrm{H}(\sqrt{2})$, $Y_2(\sqrt{2})$, $S_1(\sqrt{2})$, $Y_4(\sqrt{2})$ and $W_n(\sqrt{2})$ for $n \in \mathbf{N}$.

Proof: Let N be a normal subgroup of $\mathrm{H}(\sqrt{2})$ containing an element of finite order. Then N contains an element of order two or an element of order four. Since every element of order two is conjugate to R or S^2, and every element of order four is conjugate to S or S^3, it follows that, as N is normal, N contains R, S and/or S^2. Then there are five possibilities:

(1) N contains R and S. Then clearly $N = \mathrm{H}(\sqrt{2})$.

(2) N contains R but not S or S^2. Then in the homomorphism from $\mathrm{H}(\sqrt{2})$ to $\mathrm{H}(\sqrt{2})/N$, R goes to the identity and S goes to a product of 4–cycles. Therefore RS goes to a product of 4–cycles as well. That means that $\mathrm{H}(\sqrt{2})/N$ is isomorphic to $C_4 \cong (1,4,4)$. Then N has the signature $(0\ ;\ 2^{(4)},\infty)$, and hence $N \cong Y_4(\sqrt{2})$.

(3) N contains R and S^2 but not S. Then R goes to identity and S goes to a product of 2–cycles. Therefore $\mathrm{H}(\sqrt{2})/N$ is isomorphic to C_2 and N has the signature $(0\ ;\ 2,2,2,\infty)$. Hence $N \cong Y_2(\sqrt{2})$.

(4) N contains S^2, but not R or S. Then both R and S go to 2–cycles. Hence the parabolic element RS could go to any product of n–cycles, which altogether imply that $H(\sqrt{2})/N$ is isomorphic to the dihedral group D_n, $n \in \mathbf{N}$. In this case we have seen that the subgroup is $W_n(\sqrt{2})$.

(5) Finally N contains S but not R. Here R goes to 2–cycles and S goes to the identity. Therefore $H(\sqrt{2})/N$ is isomorphic to C_2. Then N has the signature $(0\ ;\ 4, 4, \infty)$ which is the subgroup $S_1(\sqrt{2})$.

Remarks 8.2: (i) Note that Lemma 8.2 implies that $H(\sqrt{2})$ has infinitely many normal subgroups containing elements of finite order unlike the modular group and any odd q case.

(ii) The list of Lemma 8.2 also includes the normal subgroups $Y_1(\sqrt{2})$, $K_2(\sqrt{2})$, $H^2(\sqrt{2})$, $S_2(\sqrt{2})$ and $\Gamma_2(\sqrt{2})$, since each of them is equal to one of those listed above (see Appendix 1 for more details).

We now have the following result:

Corollary 8.2: Let N be a normal subgroup of positive genus of $H(\sqrt{2})$. Then N is torsion–free.

Corollary 8.2 does not have a converse as there are some free normal subgroups of $H(\sqrt{2})$ with genus 0, as we have seen in 8.2.

We can now characterize the freeness of a normal subgroup of $H(\sqrt{2})$ by comparing it with the following list of normal subgroups:

Theorem 8.6: Let N be a non–trivial normal subgroup of $H(\sqrt{2})$ different from $H(\sqrt{2})$, $Y_2(\sqrt{2})$, $S_1(\sqrt{2})$, $Y_4(\sqrt{2})$ and $W_n(\sqrt{2})$ for $n \in \mathbf{N}$. Then N is free.

Proof: Clear by Lemmas 8.1 and 8.2.

Now we know that what normal subgroups of $H(\sqrt{2})$ are free. It is also important to know the rank and index of these subgroups. We have seen in Chapter that if N is a free subgroup of $H(\lambda_q)$ of genus g, then the rank of N is

$$r = 2g + t - 1. \tag{8.17}$$

Note that particularly when $g = 0$, $r = t - 1$ and when $g = 1$, $r = t + 1$.

Let now N be a normal free subgroup of $H(\sqrt{2})$ of index μ. Then R goes to an element of order 2 and S goes to an element of order 4 implying the following result:

Theorem 8.7: If N is a normal free subgroup of $H(\sqrt{2})$ with finite index μ, then

$$4 \mid \mu. \tag{8.18}$$

Note that in the statement of Theorem 8.7, we need N to be free , for otherwise, we have, as a counter example, $W_n(\sqrt{2})$ with index sometimes not divisible by four.

Now by the Riemann–Hurwitz formula, the genus g of such a subgroup is given by

$$g = 1 + \mu.\frac{n-4}{8n}. \tag{8.19}$$

This implies, for a given genus $g \neq 1$, that we can only have finitely many normal free subgroups of genus g of $H(\sqrt{2})$, since the equation (8.19) has only finitely many solutions.

For $g = 1$ the situation is quite different. Here n must be four and t could be any natural number. Therefore there are infinitely many normal subgroups of genus 1 in $H(\sqrt{2})$. (We proved their existence in Chapter 5 using regular maps of type

$\{4,4\}$).

We have already found all normal subgroups of genus 0 in section 8.2. The ones of genus 1 will be studied in 8.4. But first we summarize our final remarks in the following:

Theorem 8.8: $H(\sqrt{2})$ has finitely many normal free subgroups of genus g if $g \neq 1$, and infinitely many otherwise.

8.4. NORMAL SUBGROUPS OF GENUS 1 OF $H(\sqrt{2})$

Throughout this section, unless otherwise stated, N will denote a normal subgroup of genus 1 of $H(\sqrt{2})$.

We have already seen that N is free of rank $r = t+1$, of level four, and therefore of index μ divisible by four.

We first define the commutator subgroup $H'(\sqrt{2})$ of $H(\sqrt{2})$. By adding the relation $RS = SR$ to the existing relations $R^2 = S^4 = I$ of $H(\sqrt{2})$, we obtain the quotient group $H(\sqrt{2})/H'(\sqrt{2})$. By the permutation method $H'(\sqrt{2})$ is a normal subgroup of index eight, since the quotient group is isomorphic to $C_2 \times C_4$, and of signature $(1\ ;\infty,\infty)$. Therefore $H'(\sqrt{2})$ is a free group of rank three. By the Reidemeister–Schreier method, the generators of $H'(\sqrt{2})$ can be found as

$$a = RSRS^3,\ \ b = RS^2RS^2 \ \ and\ \ c = RS^3RS. \tag{8.20}$$

As all commutators are even elements we obtain

$$H'(\sqrt{2}) \lhd H_e(\sqrt{2}). \tag{8.21}$$

Let us now concentrate on the second commutator subgroup $H''(\sqrt{2})$ of $H(\sqrt{2})$.

First we have

Theorem 8.9: $\mathrm{H}'(\sqrt{2})/\mathrm{H}''(\sqrt{2})$ is a free abelian group of rank three with the free generators

$$aH''(\sqrt{2}),\ bH''(\sqrt{2})\ \ and\ \ cH''(\sqrt{2}) \tag{8.22}$$

where a, b and c are the generators of $\mathrm{H}'(\sqrt{2})$.

Proof: We know that $\mathrm{H}'(\sqrt{2})$ is free of rank three. By Theorem 0.13, $\mathrm{H}'(\sqrt{2})/\mathrm{H}''(\sqrt{2})$ is free abelian. Obviously it has the generators given in (8.22).

Now recall that the quotient group of a free group F_n by its commutator subgroup F_n' is isomorphic to $\mathbf{Z^n}$ (see [Ra,1]). Therefore the rank of the quotient group is also three, as required.

We now have

Theorem 8.10: $\mathrm{H}''(\sqrt{2})$ is a free normal subgroup of infinite rank.

Proof: It is free by Theorem 0.5. Also by Theorem 0.6, it has infinite rank as it has infinite index.

Let $\Delta \cong (2,4,4) \cong < x, y \,|\, x^2 = y^4 = (xy)^4 = 1 >$. If we map R to x, S to y and T to xy, we obtain a homomorphism θ of $\mathrm{H}(\sqrt{2})$:

$$\theta \ : \ H(\sqrt{2}) \longrightarrow \Delta \cong (2,4,4). \tag{8.23}$$

θ has kernel $Ker\ \theta = \Delta(4)$, the normal closure of T^4. Then Δ', the commutator subgroup, is going to be the translation subgroup $\mathbf{Z} \times \mathbf{Z}$ which is abelian; actually

$$\Delta' = \langle \underline{a}, \underline{c} \ : \ \underline{a}.\underline{c} = \underline{c}.\underline{a} \rangle \tag{8.24}$$

where $\underline{a}, \underline{b}$ and $\underline{c}$ are the images of a, b and c under θ respectively. The relation in (8.24) is true since $(\underline{R}.\underline{S})^4 = I$ in Δ and therefore $\underline{aca^{-1}c^{-1}} \mapsto I$.

That $\underline{a}, \underline{b}$ and $\underline{c}$ generate Δ' can be easily seen by the Reidemeister–Schreier method.

Since Δ' is abelian, Δ'' will just be the trivial group $\{I\}$.

Let us now map $\mathrm{H}(\sqrt{2})$ onto a finite cyclic quotient of order 4 of Δ. Using the permutation method and Riemann–Hurwitz formula we obtain a normal subgroup with signature $(1\ ;\ \infty)$. We shall denote this subgroup by K. It is isomorphic to a free group of rank two.

By the Reidemeister–Schreier method the free generators are

$$\alpha = RSRS^3 \quad and \quad \beta = RS^2 \tag{8.25}$$

with matrix representations

$$\alpha = \begin{pmatrix} 3 & \sqrt{2} \\ \sqrt{2} & 1 \end{pmatrix} \quad and \quad \beta = \begin{pmatrix} \sqrt{2} & 1 \\ 1 & \sqrt{2} \end{pmatrix}. \tag{8.26}$$

Note that $\alpha = a$ and $\beta^2 = b$. Since $\beta \notin H'(\sqrt{2})$ we can express K in terms of its normal subgroup $\mathrm{H}'(\sqrt{2})$ as follows:

$$\begin{aligned} K &= \left\langle \beta,\ H'(\sqrt{2}) \right\rangle \\ &= H'(\sqrt{2}) \cup \beta.H'(\sqrt{2}). \end{aligned} \tag{8.27}$$

The commutator subgroup K' of K is a free group of infinite rank with $K/K' = \langle \alpha K',\ \beta K' \rangle$ is abelian.

The groups K and K' are very important in the classification of the normal subgroups of genus 1 of $\mathrm{H}(\sqrt{2})$. Actually all normal subgroups of genus 1 will lie between these two subgroups, as we shall prove. Therefore

Theorem 8.11: The subgroup K is maximal through all normal subgroups of genus 1 of $\mathrm{H}(\sqrt{2})$.

We now have

Lemma 8.3: We have

$$K' = \Delta(4). \tag{8.28}$$

Proof: See [Ke–Ro,1].

We have proven that K/K' is free abelian of rank two. Now if N is a normal subgroup of genus 1 of $\mathrm{H}(\sqrt{2})$, i.e. if $K' < N \leq K$, then N/K', as a subgroup of the free abelian group K/K', is also free abelian and therefore has rank

$$1 \leq r(N/K') \leq r(K/K') = 2. \tag{8.29}$$

That is, N/K' is either $\mathbf{Z}$ or $\mathbf{Z} \times \mathbf{Z}$. We shall see that it is always the latter:

Theorem 8.12: Let N be a normal subgroup of K of finite index. Then N/K' is a free abelian group of rank two.

Proof: If $N = K$, then $r(N/K') = r(K/K') = 2$.

If N is a proper normal subgroup of K, then N has rank $r = t + 1 > 2$ and finite index $\mu = 4t$ in $\mathrm{H}(\sqrt{2})$. Then $|K : N| = t < \infty$ and since $K/K' \cong F_2$, we have $r(N/K') = 2$.

We have often mentioned the existence of a 1–1 correspondence between normal subgroups of certain triangle groups (including the Hecke groups) and regular maps (see [Jo–Si,1]). Let us now consider the relationship between the normal subgroups of genus 1 of $H(\sqrt{2})$ and the corresponding regular maps. In Chapter 3, we have seen that such a regular map must be of type $\{4,4\}$. In [Jo–Si,2] and [Co–Mo,1], these are classified as $\{4,4\}_{r,s}$ for non-negative integers r and s. Also if N is a normal subgroup of $H(\sqrt{2})$ corresponding to such a regular map, then

$$|\,Aut\,\mathcal{M}\,| = |\,H(\sqrt{2}) : N\,| = 4(r^2 + s^2). \tag{8.30}$$

As regularity of the regular map corresponds to the normality of the corresponding normal subgroup, each of these regular maps will give us a normal subgroup of $H(\sqrt{2})$ with genus 1 and finite index $\mu = 4(r^2 + s^2)$. This implies

Theorem 8.13: $H(\sqrt{2})$ has infinitely many normal subgroups of genus 1.

Using (8.30), we have, in Chapter 5, determined the number $N(\mu)$ of the normal genus 1 subgroups of $H(\sqrt{2})$ having a given finite index μ. We have seen that this number is equal to a quarter of the number of representations of $\mu/4 = t$ as the sum of two integer squares. See Chapter 5 for details.

We now want to determine some relations between some of the normal subgroups of $H(\sqrt{2})$. We have already showed that $H^m(\sqrt{2}) \rhd H^{mn}(\sqrt{2})$ and $W_m(\sqrt{2}) \rhd W_{mn}(\sqrt{2})$, for $m, n \in \mathbf{N}$.

It is easy to show that

$$K' \lhd H'(\sqrt{2}). \tag{8.31}$$

Since K/K' is free abelian of rank two, as a normal subgroup, $\mathrm{H}'(\sqrt{2})/K'$ is also free abelian of rank two as $|\, K : \mathrm{H}'(\sqrt{2})\,| = 2 < \infty$. We know that $\mathrm{H}'(\sqrt{2})/\mathrm{H}''(\sqrt{2})$ is the largest abelian quotient of $\mathrm{H}'(\sqrt{2})$. Now as $\mathrm{H}'(\sqrt{2})/K'$ is also abelian, we can easily deduce that

$$K' \trianglerighteq H''(\sqrt{2}). \tag{8.32}$$

Finally as K/K' is free of rank two and $\mathrm{H}'(\sqrt{2})/\mathrm{H}''(\sqrt{2})$ is free of rank three, the quotient $K'/\mathrm{H}''(\sqrt{2})$ is just the infinite cyclic group, i.e.

$$K'/H''(\sqrt{2}) \cong \mathbf{Z}. \tag{8.33}$$

The subgroup $\mathrm{H}'(\sqrt{2})$ also contains $\mathrm{H}^4(\sqrt{2})$ generated by the fourth powers of the elements of $\mathrm{H}(\sqrt{2})$. Indeed, if A is any element of $\mathrm{H}(\sqrt{2})$, then $A.\mathrm{H}'(\sqrt{2})$ will be an element of $\mathrm{H}(\sqrt{2})/\mathrm{H}'(\sqrt{2}) \cong C_2 \times C_4$. Therefore $(A.\mathrm{H}'(\sqrt{2}))^4 = A^4.\mathrm{H}'(\sqrt{2})$ must be the identity. Therefore

$$H^4(\sqrt{2}) \triangleleft H'(\sqrt{2}). \tag{8.34}$$

As $\mathrm{H}'(\sqrt{2})$ is torsion-free we have

Theorem 8.14: $\mathrm{H}^4(\sqrt{2})$ is torsion-free.

This follows from the following result:

Lemma 8.4: Let $H < G$, G torsion-free. Then H is also torsion-free.

Now we consider the subgroup $\mathrm{H}^2(\sqrt{2})$. By its definition it is generated by the squares of the elements of $\mathrm{H}(\sqrt{2})$. Therefore all of its elements must be even. Then

$$H^2(\sqrt{2}) \triangleleft H_\epsilon(\sqrt{2}). \tag{8.35}$$

Also

$$H^4(\sqrt{2}) \lhd H^2(\sqrt{2}). \tag{8.36}$$

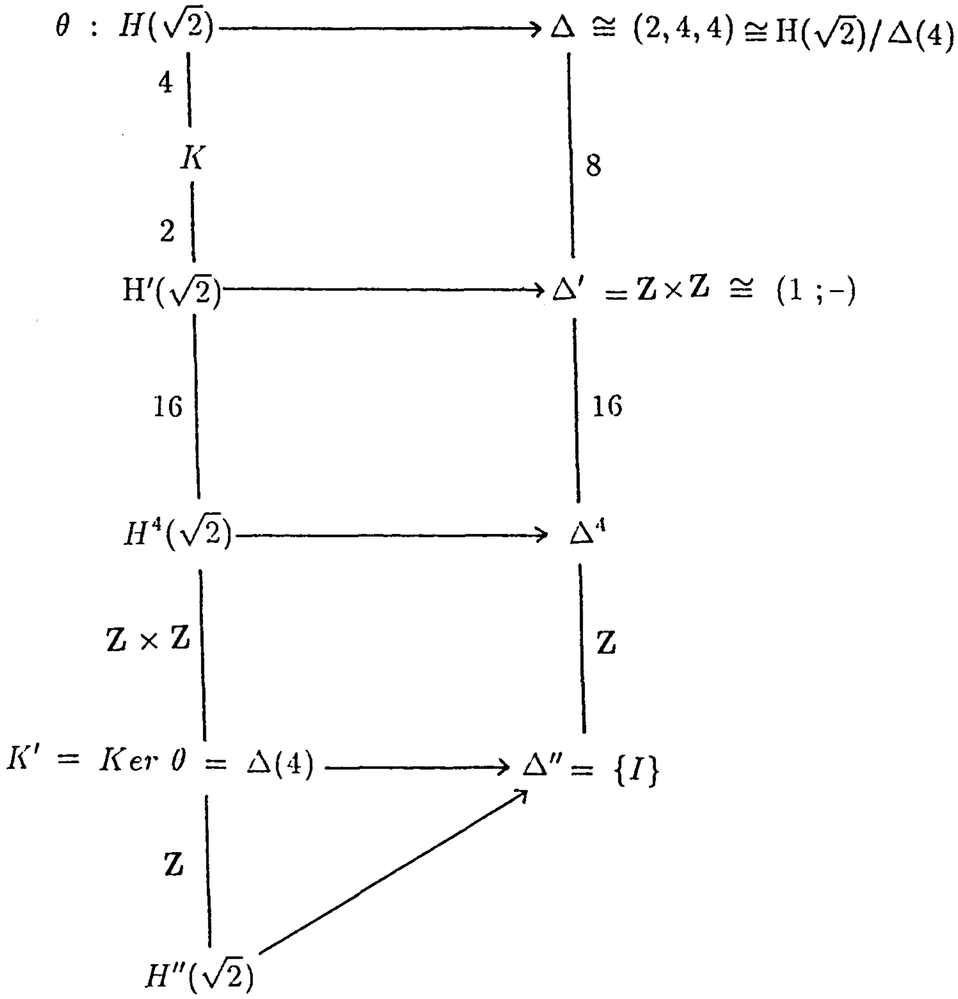


Figure 8.1

By means of all these inclusions we can now form the above subgroup lattice mainly concerning the normal subgroups of genus 1 of $H(\sqrt{2})$. Recall that the subgroups with infinite index have genus 0 or ∞.

Note that the translation subgroup $\Delta' = (1\,;-)$ is free abelian with generators

$\underline{a}, \underline{b}$ and $\underline{c}$ satisfying the relation $\underline{a}.\underline{c} = \underline{c}.\underline{a}$. Therefore the quotient Δ'/Δ^4 will have order $4.4 = 16$. Then $|\Delta : \Delta^4| = 128$ and since θ^{-1} preserves the indices we have

$$|H(\sqrt{2}) : H^4(\sqrt{2})| = 128. \tag{8.37}$$

8.5. ANOTHER CLASS OF NORMAL SUBGROUPS OF H($\sqrt{2}$) : $\hat{K}(g)$

In [Mc,2], Maclachlan introduced an infinite family of groups denoted by $\hat{K}(g)$ which also form a class of normal subgroups of H($\sqrt{2}$). In this section we shall investigate these subgroups, determine their group theoretical structure and obtain some relations between them.

Let

$$L^+(g) := \left\langle R, S : R^2 = S^4 = (RS)^{2g+2} = (S^2R)^2 = I \right\rangle. \tag{8.38}$$

It contains the central involution S^2 and

$$L^+(g)/ < S^2 > \cong D_{2(g+1)}. \tag{8.39}$$

Hence $L^+(g)$ has order $8(g+1)$. It follows that $< R > \cap < S > = \{I\}$ and hence every element of $L^+(g)$ has the form

$$S^i(RS)^j, \quad 0 \leq i \leq 3,\ 0 \leq j \leq 2g+1. \tag{8.40}$$

Since, in $L^+(g)$, we have the relations $R^2 = S^4 = I$, there is a homomorphism of H($\sqrt{2}$) onto $L^+(g)$. The kernel of this homomorphism, which is denoted by $\hat{K}(g)$, is a normal subgroup of H($\sqrt{2}$) of genus g and index $8(g+1)$, as the order of $L^+(g)$ is $8(g+1)$.

Because of the relations $R^2 = S^4 = I$ in $L^+(g)$, $\hat{K}(g)$ must be a free subgroup. Since the parabolic element T has order $2g+2$, the level of $\hat{K}(g)$ is $2g+2$. Hence the parabolic class number t of $\hat{K}(g)$ is

$$t = \frac{8(g+1)}{2(g+1)} = 4. \qquad (8.41)$$

Therefore $\hat{K}(g)$ is isomorphic to a normal subgroup with signature $(g\ ;\ \infty^{(4)})$, i.e. it is isomorphic to the free group of rank $2g+3$.

Example 8.1: **(i)** Let $g = 0$. Then we have a homomorphism

$$H(\sqrt{2}) \longrightarrow L^{+}(0) = \left\langle R, S\ :\ R^2 = S^4 = (RS)^2 = (S^2R)^2 = I \right\rangle. \qquad (8.42)$$

That is, $L^{+}(0)$ is a homomorphic image of D_4. Now $(S^2R)^2 = S^2RS^2R = S^2(S^{-1}R)SR$ $= (SR)^2$, i.e. the relation $(S^2R)^2 = I$ is deducible from the other three relations. Then $L^{+}(0) = D_4$. Hence

$$\begin{array}{lcl} R & \mapsto & (1\ 2)(3\ 4)(5\ 6)(7\ 8) \\ S & \mapsto & (1\ 7\ 6\ 4)(2\ 3\ 5\ 8) \\ T & \mapsto & (1\ 3)(2\ 7)(4\ 5)(6\ 8). \end{array} \qquad (8.43)$$

Hence we find that $\hat{K}(0)$ has the signature $(0\ ;\ \infty^{(4)})$.

(ii) Let now $g = 1$. Similarly we have a homomorphism

$$H(\sqrt{2}) \longrightarrow L^{+}(1) = \left\langle R, S\ :\ R^2 = S^4 = (RS)^4 = (S^2R)^2 = I \right\rangle. \qquad (8.44)$$

Here the relation $(S^2R)^2 = I$ cannot be reduced from the other relations. But we know that a normal subgroup of genus 1 and of index 16 is free and of level four. Hence $4t = 16$ and $t = 4$. Therefore the signature of $\hat{K}(1)$ is $(1\ ;\ \infty^{(4)})$.

8.6. CONNECTIONS BETWEEN REGULAR MAPS AND NORMAL SUBGROUPS OF H($\sqrt{2}$)

We have often noted the 1–1 correspondence between regular maps and normal subgroups of the Hecke groups. We have also discussed this correspondence for the genus 1 normal subgroups of H($\sqrt{2}$) earlier in 8.4.

In this section, we shall discuss the situation for any $g \geq 0$. At the end of the thesis we give the lists of the regular maps of type $\{4, n\}$ having genus $g \leq 7$.

Since $q = 4$, the only non–degenerate regular maps we can have are those of type $\{2, n\}$ or $\{4, n\}$. The former ones will correspond to the normal subgroups $W_n(\sqrt{2})$ with dihedral quotient $D_n \cong (2, 2, n)$, $n \in \mathbb{N}$. Therefore, having genus 0, they are regular n–gons on the sphere. For this reason, we shall not be interested in them. Hence all regular maps we shall consider here are of type $\{4, n\}$ where n corresponds to the level of the corresponding normal subgroup. Therefore each vertex will have valency four. We shall denote by $[4, n]$ the normal subgroup corresponding to $\{4, n\}$.

For $g = 0$, we have, as we have noted in the above paragraph, infinitely many regular maps of type $\{2, n\}$ with $n \in \mathbb{N}$. Apart from these, we have two more non–degenerate regular maps of genus 0. They are $\{4, 2\}$ which is a map consisting of four edges joining two antipodal points on the sphere, and $\{4, 3\}$ corresponding to a cube.

Each genus 1 normal subgroup of H($\sqrt{2}$) corresponds to a regular map $\{4, 4\}_{r,s}$, with $r^2 + s^2 = t$, as we have seen. Therefore they are infinitely many.

Let us now deal with the higher genus cases beginning with $g = 2$. Obviously as g gets bigger, the minimum index for which there exists a regular map having that index becomes higher.

Let $g = 2$. If N is a normal subgroup of H($\sqrt{2}$) with index μ, genus 2 and level

n, then by the Riemann–Hurwitz formula

$$\mu = \frac{8n}{n-4}. \tag{8.45}$$

Therefore n must be greater than four. Solving (8.46) in the integers and remembering $\mu = n.t$, we can easily find all possible maps. Some of them are known to be regular. By checking the regularity of these possible maps we obtain the list given in Appendix 1.

Let $g \geq 3$. Then similarly

$$\mu = \frac{8(g-1)n}{n-4}. \tag{8.46}$$

Again in the same way we can obtain all regular maps of type $\{4, n\}$ with genus $g \leq 7$. They are also listed in Appendix 1.

Also in Appendix 1, we give some details of all normal subgroups of $\mathrm{H}(\sqrt{2})$ with index upto 56. They give for any $\mu \leq 56$, the normal subgroup N, the quotient group $\mathrm{H}(\sqrt{2})/N$, the associated triangle group, the signature, genus and the level of N, and also the corresponding regular map with the number of its vertices, edges and faces, and finally, its automorphism group.

Chapter 9

NORMAL SUBGROUPS OF H($\sqrt{3}$)

9.0. INTRODUCTION

In this chapter we discuss normal subgroups of another interesting Hecke group H($\sqrt{3}$). Because of the similarity between the groups H($\sqrt{2}$) and H($\sqrt{3}$) we will often not go into details as the most of the results will be similar to those already proven for H($\sqrt{2}$) in Chapter 8. However there will be some results quite different from the H($\sqrt{2}$) case, and we shall mainly be interested in them.

We begin once more with the power subgroups $H^m(\sqrt{3})$ of H($\sqrt{3}$):

9.1. POWER SUBGROUPS $H^m(\sqrt{3})$ OF H($\sqrt{3}$)

The power subgroups of H($\sqrt{3}$) are defined exactly in the same way to those of H($\sqrt{2}$). As they depend on the relation between m and q, there are some important differences between the two cases $q = 4$ and $q = 6$. But first we have the following similar result:

Theorem 9.1: The normal subgroup $H^2(\sqrt{3})$ is the free product of the infinite cyclic group and two finite cyclic groups of order three. Also

$$H(\sqrt{3})/H^2(\sqrt{3}) \cong C_2 \times C_2, \tag{9.1}$$

$$H(\sqrt{3}) = H^2(\sqrt{3}) \cup RH^2(\sqrt{3}) \cup SH^2(\sqrt{3}) \cup RSH^2(\sqrt{3}), \tag{9.2}$$

and

$$H^2(\sqrt{3}) = < S^2 > \star < RS^2R > \star < RSRS^3 > . \tag{9.3}$$

The elements of $H^2(\sqrt{3})$ can be characterised by the requirement that the sums of the exponents of R and S are both even.

Proof: It is similar to the proof of Theorem 8.1.

Theorem 9.2: The normal subgroup $H^3(\sqrt{3})$ is the free product of four cyclic groups of order two. Also

$$H(\sqrt{3})/H^3(\sqrt{3}) \cong C_3, \tag{9.4}$$

$$H(\sqrt{3}) = H^3(\sqrt{3}) \cup SH^3(\sqrt{3}) \cup S^2H^3(\sqrt{3}), \tag{9.5}$$

and

$$H^3(\sqrt{3}) = < R > \star < S^3 > \star < SRS^5 > \star < S^2RS^4 > . \tag{9.6}$$

Proof: Similar to the proof of Theorem 8.1.

The following results are easy to see:

Theorem 9.3: Let $m \equiv \pm 1 \; mod\, 6$. Then $\mathrm{H}^m(\sqrt{3}) = \mathrm{H}(\sqrt{3})$.

Theorem 9.4: Let $m \equiv \pm 2 \; mod\, 6$. Then $\mathrm{H}^m(\sqrt{3}) = W_m(\sqrt{3})$.

Theorem 9.5: Let $m \equiv 3 \; mod\, 6$. Then $\mathrm{H}^m(\sqrt{3}) = \mathrm{H}^3(\sqrt{3})$.

Therefore the only case left is that when m is divisible by 6. A similar discussion will show that $\mathrm{H}^m(\sqrt{3})$ is free in this case.

We now recall an important normal subgroup of $\mathrm{H}(\sqrt{3})$:

Theorem 9.6: The even subgroup $\mathrm{H}_e(\sqrt{3})$ of $\mathrm{H}(\sqrt{3})$ defined by

$$H_e(\sqrt{3}) := \left\{ M = \begin{pmatrix} a & b\sqrt{3} \\ c\sqrt{3} & d \end{pmatrix} : M \in H(\sqrt{3}) \right\} \tag{9.7}$$

is a normal subgroup of index two of $\mathrm{H}(\sqrt{3})$. Also

$$H(\sqrt{3}) = H_e(\sqrt{3}) \cup RH_e(\sqrt{3}), \tag{9.8}$$

$$H_e(\sqrt{3}) \cong < T > \star < TU > = < RS > \star < RS^2R >, \tag{9.9}$$

and therefore $\mathrm{H}_e(\sqrt{3})$ is isomorphic to the free product of the infinite cyclic group (generated by RS) and the finite cyclic group of order three (generated by RS^2R).

9.2. NORMAL SUBGROUPS OF GENUS 0 OF $\mathrm{H}(\sqrt{3})$

In a similar way to the section 8.2, we obtain the following result:

Theorem 9.7: All normal subgroups of $\mathrm{H}(\sqrt{3})$ with genus 0 are $\mathrm{H}(\sqrt{3})$, $Y_2(\sqrt{3})$, $Y_6(\sqrt{3})$, $S_1(\sqrt{3})$, $S_3(\sqrt{3})$, $T_1(\sqrt{3})$, $\mathrm{H}^3(\sqrt{3})$, $S_6(\sqrt{3})$, $T_2(\sqrt{3})$, $T_3(\sqrt{3})$ and $W_n(\sqrt{3})$ for $n \in \mathrm{N}$.

Corollary 9.1: $H(\sqrt{3})$ has infinitely many normal subgroups of genus 0.

9.3. FREE NORMAL SUBGROUPS OF $H(\sqrt{3})$

In this section we consider free normal subgroups of $H(\sqrt{3})$. We have already seen that when the free normal subgroups of $H(\sqrt{2})$ are considered the situation was unlike modular group case where there are only finitely many normal subgroups containing elements of finite order. Here for $q = 6$, we shall find that the situation is different from these two cases as the normal subgroups of $H(\sqrt{3})$ having torsion seem to be more numerous. But $H(\sqrt{3})$ still has infinitely many normal free subgroups.

The situation is rather different than $q = 4$ case. This is because 3 is also a divisor of 6. Therefore $H(\sqrt{3}) \cong (2, 6, \infty)$ can be mapped to every finite quotient $(2, 3, k)$, $k \geq 2$, $k \in \mathbf{N}$ of the triangle group $(2, 3, \infty)$. Therefore $H(\sqrt{3})$ will have countably infinitely many normal subgroups with torsion. An infinite class of them is those with signature $(1 \; ; 2^{(2t)}, \infty^{(t)})$ which will be denoted by $V_{r,s}$ for non-negative integers r and s. They are obtained by mapping $H(\sqrt{3})$ to $\Delta = (2, 3, 6)$ such that the obtained subgroup has index $\mu = 6t$, $t = r^2 + rs + s^2$. Obviously there is no subgroup $V_{0,0}(\sqrt{3})$.

We now have

Theorem 9.8: All normal subgroups of $H(\sqrt{3})$ having torsion are $H(\sqrt{3})$, $Y_2(\sqrt{3})$, $Y_6(\sqrt{3})$, $S_1(\sqrt{3})$, $S_3(\sqrt{3})$, $T_1(\sqrt{3})$, $H^3(\sqrt{3})$, $S_6(\sqrt{3})$, $T_2(\sqrt{3})$, $T_3(\sqrt{3})$, $W_n(\sqrt{3})$ for $n \in \mathbf{N}$, $V_{r,s}(\sqrt{3})$ for non-negative integers r and s and $[3, k]$ for $k \in \mathbf{N}, \mathrm{k} \geq 8$, $\mathrm{k} \mid \mu$.

Note that unlike $q = 3$ and $q = 4$ cases, $H(\sqrt{3})$ has non-free normal subgroups with positive genus.

Theorem 9.9: Let N be a non-trivial normal subgroup of $H(\sqrt{3})$ different from those listed in Theorem 9.8. Then N is free.

To obtain a free group we must send the element S to an element of order 6. Therefore

Theorem 9.10: If N is a normal free subgroup of $H(\sqrt{3})$ with finite index μ, then

$$6 \mid \mu. \tag{9.10}$$

By the Riemann–Hurwitz formula the genus g of N is

$$g = 1 + \mu . \frac{n-3}{6n}. \tag{9.11}$$

This implies, for a given genus $g \neq 1$, that we can only have finitely many normal free subgroups of genus g in $H(\sqrt{2})$. However when $g = 1$, n must be three and t could be any natural number. We shall prove using the regular maps of type $\{6,3\}$, that $H(\sqrt{3})$ has infinitely many normal free subgroups of genus 1.

The rank of N is $2g + t - 1$, as we have found for $q = 4$. Therefore $r = t - 1$ for $g = 0$, and $r = t + 1$ for $g = 1$, etc.

We now discuss an important free subgroup of $H(\sqrt{3})$ — the commutator subgroup $H'(\sqrt{3})$. It can be obtained, as in $q = 4$ case, by adding the commutativity relation $RS = SR$ to the existing relations. In that way we obtain a homomorphism of $H(\sqrt{3})$ to $H(\sqrt{3})/H'(\sqrt{3})$. Obviously this quotient is isomorphic to $C_2 \times C_6$. Therefore $H'(\sqrt{3})$ is a normal subgroup of index 12 in $H(\sqrt{3})$ with signature $(2\ ;\ \infty, \infty)$, that is, $H'(\sqrt{3})$ is free of rank five. By the Reidemeister–Schreier method it has the free generators

$$a_1 = RSRS^5, \dots, a_5 = RS^5RS. \tag{9.12}$$

Again we have

$$H'(\sqrt{3}) \lhd H_e(\sqrt{3}). \tag{9.13}$$

Let now N be a normal subgroup of H′($\sqrt{3}$). By the Kurosh subgroup theorem, N is free of rank

$$r = 1 + 4\mu'' \tag{9.14}$$

and genus

$$g = 1 + \frac{t}{6}(n-3). \tag{9.15}$$

We also have

Theorem 9.11: H′($\sqrt{3}$)/H″($\sqrt{3}$) is free abelian of rank five with the free generators

$$a_1 H''(\sqrt{3}), \dots, a_5 H''(\sqrt{3}) \tag{9.16}$$

where $a_1, \dots, a_5$ are the generators of H′($\sqrt{3}$) given in (9.12).

Theorem 9.12: H″($\sqrt{3}$) is a free normal subgroup of infinite rank.

9.4. NORMAL SUBGROUPS OF GENUS 1 OF H($\sqrt{3}$)

In Chapter 8 we have used three subgroups in the classification of the normal subgroups of genus 1 of H($\sqrt{2}$): H′($\sqrt{2}$), K and K'. For $q = 6$, however, the commutator subgroup H′($\sqrt{3}$) does not have genus 1 (we have just seen that it has genus two) and therefore will not be of any use in the classification of the normal subgroups of genus 1 of H($\sqrt{3}$). But the subgroup K will play the same role as it did for H($\sqrt{2}$).

Let us now map H($\sqrt{3}$), by a homomorphism θ, to a finite quotient C_6 of the infinite triangle group (2,6,3) by mapping R to the generator of order two and S to the generator of order six. This gives us a normal subgroup with signature $(1\ ;\ \infty, \infty)$ denoted by K. It is isomorphic to a free group of rank three with the free generators

$$\alpha = RSRS^5,\ \beta = RS^3 \quad and \quad \gamma = RS^2RS^4. \tag{9.17}$$

They have the matrix representations

$$\alpha = \begin{pmatrix} 4 & \sqrt{3} \\ \sqrt{3} & 1 \end{pmatrix},\ \beta = \begin{pmatrix} 2 & \sqrt{3} \\ \sqrt{3} & 2 \end{pmatrix} \quad and \quad \gamma = \begin{pmatrix} 7 & 3\sqrt{3} \\ 3\sqrt{3} & 4 \end{pmatrix}. \tag{9.18}$$

Note that

$$\alpha = a_1,\ \gamma = a_2 \quad and \quad \beta^2 = a_3. \tag{9.19}$$

Since $\beta \notin$ H$'(\sqrt{3})$ we can express K in terms of H$'(\sqrt{3})$ as follows:

$$K = H'(\sqrt{3}) \cup \beta H'(\sqrt{3}). \tag{9.20}$$

The commutator subgroup K' of K is a free group of infinite rank with K/K' is isomorphic to a free abelian group of rank three. Clearly $K/K' = \langle \alpha K', \beta K', \gamma K' \rangle$ is abelian.

It is easy to show, as in the $q = 4$ case, that all normal subgroups of H($\sqrt{3}$) with genus 1 lie between K and K'. Therefore we have

Theorem 9.13: The subgroup K is maximal through all normal subgroups of genus 1 of H($\sqrt{3}$).

We have seen that K/K' is free abelian of rank three. Let now N be a normal subgroup of H($\sqrt{3}$) with genus 1, that is, let $K' < N \leq K$. Then N/K' is a normal subgroup of K/K' and therefore is also a free abelian group with rank

$$1 \leq r(N/K') \leq r(K/K') = 3. \tag{9.21}$$

Recall that, in Chapter 5, we have calculated the number $N(\mu)$ of normal genus 1 subgroups of $H(\sqrt{3})$ having a finite given index μ. We have shown that, unlike $q = 4$ case, there are ones with torsion as well as torsion–free ones. In fact we know that, as $\{6,3\}_{r,s}$ and $\{3,6\}_{r,s}$ are dual maps, there is a 1:1 correspondence between these two classes of normal genus 1 subgroups of $H(\sqrt{3})$. We have proved that $N(\mu)$ is equal to one third of the number of representations of the number $\mu/3 = t$ as a quadratic form $r^2 + rs + s^2$ in integers. Because of the duality mentioned above, $N(\mu)$ is always even.

9.5. CONNECTIONS BETWEEN REGULAR MAPS AND NORMAL SUBGROUPS OF $H(\sqrt{3})$

We have often noted the 1–1 correspondence between the regular maps and the normal subgroups of $H(\lambda_q)$. Also we have just discussed this correspondence for the genus 1 normal subgroups of $H(\sqrt{3})$. In this section we consider this correspondence for any g. At the end of the thesis we give the tables of the regular maps of type $\{6,n\}$ and $\{3,n\}$ for $g \leq 7$.

As $q = 6$, the only non–degenerate regular maps corresponding to a normal subgroup of $H(\sqrt{3})$ are those of type $\{2,n\}$, $\{3,n\}$ or $\{6,n\}$. The ones of type $\{2,n\}$ correspond to the regular n–gons on the sphere and we will not be interested in them. Recall that the number n corresponds to the level of the normal subgroup.

If $g = 0$, we have infinitely many regular maps of type $\{2,n\}$. Apart from these and a few degenerate ones (corresponding to cyclic quotients), we have $\{3,2\}$ which is a map consisting of three edges joining two antipodal vertices, $\{3,3\}$ which is a tetrahedron, $\{6,2\}$ consisting of six edges joining two antipodal vertices, $\{3,4\}$ a cube, and finally $\{3,5\}$ which is an dodecahedron. All normal genus 0 subgroups have been discussed in Chapter 4 and also in Section 9.2.

The genus 1 case is already been considered in Chapter 5 and Section 9.4.

Let now $g \geq 2$. By the Riemann–Hurwitz formula

$$\mu = \frac{6(g-1)n}{n-3}. \tag{9.22}$$

Solving (9.22) and using the relation $\mu = nt$ we can find all possible maps. Checking their regularity using group theoretical methods, we can obtain all regular maps of type $\{3,n\}$ and $\{6,n\}$ having small genus (in fact $g \leq 7$).

In Appendix 1, we give some details of all normal subgroups of $\mathrm{H}(\sqrt{3})$ with index upto 78. They give for any $\mu \leq 78$, the normal subgroup N, the quotient group $\mathrm{H}(\sqrt{3})/N$, the associated triangle group, the signature, genus and the level of N, and also the corresponding regular map with the number of its vertices, edges and faces, and finally, its automorphism group.

Chapter 10

NORMAL SUBGROUPS OF H(λ_5)

10.0. INTRODUCTION

In this chapter we discuss normal subgroups of H(λ_5). As some of them, such as genus 0 normal subgroups, power subgroups and principal congruence subgroups have already been investigated in the earlier chapters. in general, there is no need to go into details here. We shall just recall the important results and prove only the ones specific to the case $q = 5$.

The $q = 5$ case is different from $q = 4$ and 6 cases as q is an odd prime and naturally shows similarities to the modular group case where $q = 3$.

The interest in this case comes from the fact that 5 is the only value of q, apart from $q = 4$ and 6, for which Q(λ_q) is a quadratic field. Here we have the relation

$$\lambda_5^2 - \lambda_5 - 1 = 0 \tag{10.1}$$

which makes the calculations easier as every polynomial can be reduced to a linear form $a\lambda_5 + b$, $a, b \in$ Q, by means of it.

Recall that in the introduction we discussed the conditions for a linear fractional transformation to be an element of H(λ_q), using a result of Rosen [Ro,2]. There, we defined λ_q–fractions. Leutbecher [Le,1], and Rosen [Ro,1], [Ro,2] have studied some properties of the Hecke groups using these fractions. It can be shown that every finite λ_q–fraction is an element of the algebraic number field Q(λ_q). But the converse is not always true. Leutbecher [Le,1] showed that only for $q = 5$, every element of Q(λ_q) has a finite λ_q–fraction representation. Therefore a real number is an element of Q(λ_5) if and only if it has a finite λ_5–fraction representation, and every real number has a unique λ_5–fraction representation. It then follows that the parabolic points, being finite λ_5–fractions, are just the quotients of integers in the field Q(λ_5), i.e. a typical one is denoted by a/b where $a = a_1 + a_2\lambda_5$, $b = b_1 + b_2\lambda_5$ (see [Ro,3]).

Another interesting result is that the units of the field Q(λ_5) are λ_5^n which can be written in terms of two consecutive Fibonacci numbers. Let F_n be the n–th Fibonacci number. It can be shown, by induction, that, for $n > 2$

$$\lambda_5^n = F_{n-1} + F_n\lambda_5 \tag{10.2}$$

and also

$$\lambda_5^{-n} = \begin{cases} -F_{n+1} + F_n\lambda_5 & \text{if } n \text{ is odd}, \\ F_{n+1} - F_n\lambda_5 & \text{if } n \text{ is even}. \end{cases} \tag{10.3}$$

Rosen showed, in [Ro,3], that the units λ_5^n, $n \in \mathbf{Z}$ are finite λ_5–fractions and therefore parabolic points.

In this chapter we begin with the power subgroups and obtain relations between them, H(λ_5) and H$'$(λ_5). A classification theorem for these subgroups will also be given. Then we discuss normal subgroups of genus 0 of finite index. We see that there are only five of them two of which being free. In 10.3 we discuss torsion subgroups of $H(\lambda_5)$ and Theorem 10.6 shows us that there are only three of them all with genus 0. Using the Riemann–Hurwitz formula, we obtain information about the genus and the rank of a normal free subgroup N of $H(\lambda_5)$. That $H(\lambda_5)$ has no normal subgroups with genus one or three will also be proven.

In 10.4, the principal congruence subgroups are discussed. We shall see that they are all free.

Finally in 10.5, we discuss low index normal subgroups of $H(\lambda_5)$ and find values of μ such that $H(\lambda_5)$ has no normal subgroup of index μ.

We begin with the power subgroups $H^m(\lambda_5)$ of $H(\lambda_5)$:

10.1. POWER SUBGROUPS $H^m(\lambda_5)$ OF $H(\lambda_5)$

The *m–th power subgroup* $H^m(\lambda_5)$ *of* $H(\lambda_5)$ is defined, for $m \in \mathbf{N}$, as the subgroup generated by the m–th powers of all elements of $H(\lambda_5)$. We have noted in the earlier chapters that $H^m(\lambda_5)$ is a normal subgroup of $H(\lambda_5)$.

As the relations

$$H^m(\lambda_5) > H^{mn}(\lambda_5) \tag{10.4}$$

and

$$(H^m(\lambda_5))^n > H^{mn}(\lambda_5) \tag{10.5}$$

hold, we have

$$H^m(\lambda_5).H^n(\lambda_5) = H^{(m,n)}(\lambda_5) \tag{10.6}$$

where (m,n) denotes the greatest common divisor of m and n (see Chapter 6 for a detailed proof). Particularly

$$H(\lambda_5) = H^2(\lambda_5).H^5(\lambda_5). \tag{10.7}$$

We now briefly discuss the group theoretical structure of these subgroups beginning with $H^2(\lambda_5)$:

Theorem 10.1: The normal subgroup $H^2(\lambda_5)$ is isomorphic to the free product of two finite cyclic groups of order five. Also

$$H(\lambda_5)/H^2(\lambda_5) \cong C_2, \tag{10.8}$$

$$H(\lambda_5) = H^2(\lambda_5) \cup RH^2(\lambda_5), \tag{10.9}$$

and

$$H^2(\lambda_5) = < S > \star < RSR > . \tag{10.10}$$

The elements of $H^2(\lambda_5)$ are characterised by the requirement that the sum of the exponents of R is even.

Proof: A special case of Theorem 6.1.

Theorem 10.2: The normal subgroup $H^5(\lambda_5)$ is isomorphic to the free product of five finite cyclic groups of order two. Also

$$|\, H(\lambda_5) : H^5(\lambda_5) \,| = 5, \tag{10.11}$$

$$H(\lambda_5) = H^5(\lambda_5) \cup SH^5(\lambda_5) \cup \ldots \cup S^4H^5(\lambda_5), \tag{10.12}$$

and

$$H^5(\lambda_5) = < R > \star < SRS^4 > \star < S^2RS^3 > \star \ldots \star < S^4RS > . \tag{10.13}$$

The elements of $H^5(\lambda_5)$ can be characterised by the requirement that the sum of the exponents of S is divisible by five.

Proof: A special case of Theorem 6.2.

We can now obtain a classification of these subgroups:

Theorem 10.3: The subgroups $H^m(\lambda_5)$ satisfy the following:

$$H^m(\lambda_5) = \begin{cases} H(\lambda_5) & \text{if } (m, 10) = 1 \\ H^2(\lambda_5) & \text{if } m \text{ is even and } (m, 5) = 1 \\ H^5(\lambda_5) & \text{if } m \text{ is an odd multiple of five.} \end{cases} \tag{10.14}$$

Therefore we have only left the subgroups $H^{10k}(\lambda_5)$ to consider. There is nothing certain about these subgroups except they are all free. For sufficiently large k, they have infinite index as well. However some of them have finite index as we shall soon prove.

To discuss $H^{10k}(\lambda_5)$ we first need to consider the commutator subgroup $H'(\lambda_5)$:

Lemma 10.1: The commutator subgroup $H'(\lambda_5)$ of $H(\lambda_5)$ is isomorphic to a free group of rank four. Also

$$|\, H(\lambda_5) : H'(\lambda_5)\,| = 10, \tag{10.15}$$

$$H(\lambda_5) = \sum_{i=0}^{9} T^i.H'(\lambda_5) \tag{10.16}$$

and

$$H'(\lambda_5) = < SRS^4R > \star < S^2RS^3R > \star \ldots \star < S^4RSR > . \tag{10.17}$$

We let

$$a_1 = SRS^4R, a_2 = S^2RS^3R, \ldots, a_4 = S^4RSR. \tag{10.18}$$

It is easy to conclude that

$$H'(\lambda_5) = H^2(\lambda_5) \cap H^5(\lambda_5) \tag{10.19}$$

as a special case of Theorem 6.4.

Now as

$$H'(\lambda_5) > H^{10}(\lambda_5) > H^{10k}(\lambda_5), \tag{10.20}$$

we have

Theorem 10.4: The subgroups $H^{10k}(\lambda_5)$ are free.

10.2. NORMAL GENUS 0 SUBGROUPS OF H(λ_5) OF FINITE INDEX

Let now N be a normal genus 0 subgroup of H(λ_5) with finite index. We have already seen, in Chapter 4, that H(λ_5)$/N$ is isomorphic to one of the finite triangle groups. These are known to be A_4, S_4, A_5, C_n and D_n for $n \in$ N. Let us now consider all possibilities:

Firstly, if we map H(λ_5) onto a cyclic group C_n, then N has the signature $(0\ ; 2^{(n)}, 5/n, \infty)$. This class of normal subgroups was denoted by $Y_n(\lambda_5)$ in Chapter 4. Here necessarily $n\,|\,5$, i.e. $n = 1$ or 5.

If $n = 1$, then $N = \mathrm{H}(\lambda_5)$.

If $n = 5$, then $N \cong (0\ ;\ 2^{(5)}, \infty) = \mathrm{H}^5(\lambda_5)$. But $N = \mathrm{H}^5(\lambda_5)$ as this is the unique normal subgroup of index 5.

Secondly, mapping onto a dihedral group $D_n \cong (2, n, 2)$, where $n\,|\,5$ again, we obtain a normal subgroup denoted by $S_n(\lambda_5)$ with signature $(0\ ;\ 5/n, 5/n, \infty^{(n)})$.

If $n = 1$, then $N \cong (0\ ;\ 5, 5, \infty) = \mathrm{H}^2(\lambda_5)$. Again $N = \mathrm{H}^2(\lambda_5)$ as there is a unique normal subgroup of index 2.

If $n = 5$, then $N \cong (0\ ;\ \infty^{(5)}) \cong F_4$. Therefore $N = S_5(\lambda_5)$.

Thirdly and finally, we can map $\mathrm{H}(\lambda_5)$ onto $A_5 \cong (2, 5, 3)$. Then we obtain $T_5(\lambda_5)$ with signature $(0\ ;\ \infty^{(20)}) \cong F_{19}$.

Therefore we have

Theorem 10.5: $\mathrm{H}(\lambda_5)$ has only five normal genus 0 subgroups those being $\mathrm{H}(\lambda_5)$, $\mathrm{H}^2(\lambda_5)$, $\mathrm{H}^5(\lambda_5)$, $S_5(\lambda_5)$ and $T_5(\lambda_5)$.

10.3. NORMAL TORSION SUBGROUPS OF $\mathrm{H}(\lambda_5)$

As a special case of Theorem 6.6, we have

Theorem 10.6: Let N be a non-trivial normal subgroup of $\mathrm{H}(\lambda_5)$ different from

$$H(\lambda_5), H^2(\lambda_5) \text{ and } H^5(\lambda_5). \tag{10.21}$$

Then N is free.

Also

Theorem 10.7: Let N be a free normal subgroup of $\mathrm{H}(\lambda_5)$ with finite index μ. Then

$$10 \mid \mu. \tag{10.22}$$

10.4. PRINCIPAL CONGRUENCE SUBGROUPS OF $\mathrm{H}(\lambda_5)$

These subgroups have been discussed completely in Chapter 7 and therefore we only recall some of the results obtained there.

Recall that the principal congruence subgroup of level n of $\mathrm{H}(\lambda_5)$ was denoted by $\Gamma_n(\lambda_5)$. We have found the quotients of $\mathrm{H}(\lambda_5)$ with $\Gamma_n(\lambda_5)$ for all prime values of n as follows:

Theorem 10.8: The quotient groups of the Hecke group $\mathrm{H}(\lambda_5)$ by its principal congruence subgroups $\Gamma_p(\lambda_5)$ are

$$H(\lambda_5)/\Gamma_p(\lambda_5) \cong \begin{cases} PSL(2,p) & \text{if } p \equiv \pm 1 \ mod\, 10, \\ PSL(2,p^2) & \text{if } p \equiv \pm 3 \ mod\, 10, \text{ and } p \neq 3, \\ D_5 & \text{if } p = 2, \\ A_5 & \text{if } p = 3,5. \end{cases} \tag{10.23}$$

We have also seen that if μ is the index of $\Gamma_p(\lambda_5)$, then $\Gamma_p(\lambda_5)$ has the signature

$$\left(1 + \frac{\mu}{20p}(3p - 10)\ ;\ \infty^{(\mu/p)}\right) \tag{10.24}$$

and therefore is free.

10.5. LOW INDEX NORMAL SUBGROUPS OF H(λ_5)

We now investigate some low index normal subgroups of H(λ_5). Let N be a normal subgroup of index μ in H(λ_5). Let us consider some values of μ:

If $\mu = 1$, then $N = \mathrm{H}(\lambda_5)$.

If $\mu = 2$, then $\mathrm{H}(\lambda_5)/N \cong C_2 \cong (2,1,2)$. Therefore $N = \mathrm{H}^2(\lambda_5)$, as there is a unique normal subgroup of index 2.

If $\mu = 3$, then the only possibility for $\mathrm{H}(\lambda_5)/N$ is C_3. But the commutator quotient of H(λ_5) is $C_2 \times C_5$ and every abelian quotient is a subgroup of this. Therefore H(λ_5) has no normal subgroup of index 3.

$\mu = 4$ case is ruled out by the same reason.

If $\mu = 5$, then $\mathrm{H}(\lambda_5)/N$ is isomorphic to C_5 and this gives $\mathrm{H}^5(\lambda_5)$ as we have seen in Theorem 10.2.

We have seen in Theorem 10.7 that if $\mu > 5$ and $10 \not| \mu$, then H(λ_5) has no normal subgroup of index μ.

Therefore the next value of μ to consider is 10. Then $\mathrm{H}(\lambda_5)/N$ is either C_{10} or D_5. We saw in 0.6 that the former one gives the commutator subgroup $\mathrm{H}'(\lambda_5)$. We also saw, in Chapter 4, that the latter one gives $S_5(\lambda_5)$ of genus 0.

Next value of μ is 20. We can show the impossibility of this using Sylow theorems: Let

$$G = H(\lambda_5)/N. \tag{10.25}$$

Then $|G| = 20$. By Sylow theorems G has a unique Sylow 5–subgroup H. Then G/H has order 4 and there is a homomorphism from $H(\lambda_5)$ to G/H, giving a contradiction, as there is no image of $H(\lambda_5)$ of order 4. Therefore

Theorem 10.9: $H(\lambda_5)$ has no normal subgroup of index 20.

Let now $\mu = 30$. We then need the following result:

Lemma 10.2: Let G be a group of order $2r$ with r odd. Then G contains a subgroup of order r.

Proof: Let $|G| = 2r$. Consider the regular representation of G. As G contains an element of order 2, this element is a product of r 2–cycles, i.e. G contains odd permutations. Therefore the even permutations form a subgroup of index 2 and hence have order r.

We can now return to the investigation of index 30 normal subgroups of $H(\lambda_5)$. By Lemma 10.2, $G = H(\lambda_5)/N$ contains a subgroup H of order 15. All groups of order 15 are cyclic, so $H \cong C_{15}$. By Sylow theorems, G contains 1 or 6 Sylow 5–subgroups. Suppose it contains 6. Then as they are all conjugate by Sylow theorems, the normalizer of any one of them has index 6 and so each such subgroup is self normalizing. However the C_5 inside C_{15} is not, giving a contradiction. Therefore there is a unique (hence normal) Sylow 5–subgroup K. Then $|G/K| = 6$ and there is a homomorphism from $H(\lambda_5)$ to G/K which is impossible as we saw. Therefore we have

Theorem 10.10: $H(\lambda_5)$ has no normal subgroup of index 30.

A similar discussion implies that $H(\lambda_5)$ has no normal subgroups of index 70, 90 or 110.

Now let $\mu = 40$. Let $G = \mathrm{H}(\lambda_5)/N$ with $|G| = 40$. By the Sylow theorems G has a unique Sylow 5–subgroup H. Then G/H has order 8 and there is a homomorphism of $\mathrm{H}(\lambda_5)$ to G/H, which gives a contradiction. Therefore

Theorem 10.11: $\mathrm{H}(\lambda_5)$ has no normal subgroup of index 40.

To prove the existence of normal subgroups of $\mathrm{H}(\lambda_5)$ we can refer to lists of regular maps. However, if there is an elementary argument, we give it here.

Let us now consider the case $\mu = 50$. Consider the group

$$C_5 \times C_5 \cong < a, b \,|\, a^5 = b^5 = 1,\ ab = ba > . \tag{10.26}$$

This admits an automorphism of order 2 interchanging a and b. Therefore we can form the wreath product

$$\begin{aligned} C_5 \wr C_2 \quad &\cong < a, b, t \,|\, a^5 = b^5 = t^2 = 1,\ tat^{-1} = b > \\ &\cong < a, t \,|\, a^5 = t^2 = 1,\ atat = tata > . \end{aligned} \tag{10.27}$$

Clearly this is an image of $\mathrm{H}(\lambda_5)$. As $(at)^{10} = 1$, the kernel of the homomorphism of $\mathrm{H}(\lambda_5)$ to $C_5 \wr C_2$ gives a normal subgroup of level 10. A look at the regular maps with 25 edges shows that this subgroup is unique.

Let $\mu = 60$. Let G be a group of order 60. Consider the Sylow 5–subgroups of G. By the Sylow theorems, there are 1 or 6 of them. If there is only one, then it is normal and so we have a quotient of order 12 that is an image of $\mathrm{H}(\lambda_5)$ which is impossible. Therefore there are 6 Sylow 5–subgroups. (Also there cannot be a unique Sylow 3–subgroup). This gives a transitive action of G on the 6 Sylow 5–subgroups by conjugation. There is a homomorphism $\theta : G \to S_6$. Suppose $\theta(G) = H \not\leq A_6$. Then $|H : H \cap A_6| = 2$. That is $\theta^{-1}(H \cap A_6)$ has index 2 in G, i.e. G contains a normal subgroup K of order 30. Now K contains 6 Sylow 5–subgroups and at least

4 Sylow 3–subgroups. Counting the elements, we obtain a contradiction. Hence $H < A_6$.

As S is of order 5, we can assume that $S \rightarrow y = (1\ 2\ 3\ 4\ 5)(6)$. Because of the transitivity and because of the fact that the number of the cycles must be even, we can assume that $R \rightarrow x = (1\ 6)(a\ b)(c)(d)$ where $a, b, c, d \in \{2, 3, 4, 5\}$ are different. Then possibilities are as follows:

$$\text{(i)} \quad \begin{aligned} x &= (1\ 6)(2\ 3)(4)(5) \\ y &= (1\ 2\ 3\ 4\ 5)(6) \\ xy &= (1\ 6\ 2\ 4\ 5)(3) \end{aligned}$$

Therefore x and y generate a finite image of (2,5,5). To find this image, consider $xy^2 = (1\ 6\ 3\ 4)(2\ 5)$ which is of order 4. Now $< x, y > = < x, y^2 >$, as y has odd order. As $x^2 = (y^2)^5 = (xy^2)^4 = I$, G is an image of (2,5,4) of order 60. The Riemann–Hurwitz formula then gives $2g - 2 = 60.\left(1 - \frac{1}{2} - \frac{1}{5} - \frac{1}{4}\right) = 3$, a contradiction.

$$\text{(ii)} \quad \begin{aligned} x &= (1\ 6)(2\ 4)(3)(5) \\ y &= (1\ 2\ 3\ 4\ 5)(6) \\ xy &= (1\ 6\ 2\ 5)(3\ 4) \end{aligned}$$

which is ruled out by the same reason.

$$\text{(iii)} \quad \begin{aligned} x &= (1\ 6)(2\ 5)(3)(4) \\ y &= (1\ 2\ 3\ 4\ 5)(6) \\ xy &= (1\ 6\ 2)(3\ 4\ 5) \end{aligned}$$

As $x^2 = y^5 = (xy)^3 = I$, x and y generate A_5, i.e. this gives the unique homomorphism of H(λ_5) onto A_5. The kernel of this homomorphism is $\Gamma_3(\lambda_5)$.

$$\text{(iv)} \quad \begin{aligned} x &= (1\ 6)(2)(3\ 4)(5) \\ y &= (1\ 2\ 3\ 4\ 5)(6) \\ xy &= (1\ 6\ 2\ 3\ 5)(4) \end{aligned}$$

which generate an image L of (2,5,5). Now $xy^2 = (1\ 6\ 3)(2\ 4\ 5)$ so we have A_5 as in (iii).

$$(v)\quad \begin{aligned} x &= (1\ 6)(2)(3\ 5)(4) \\ y &= (1\ 2\ 3\ 4\ 5)(6) \\ xy &= (1\ 6\ 2\ 3)(4\ 5) \end{aligned}$$

which is not possible as in (i) and (ii).

$$(vi)\quad \begin{aligned} x &= (1\ 6)(2)(3)(4\ 5) \\ y &= (1\ 2\ 3\ 4\ 5)(6) \\ xy &= (1\ 6\ 2\ 3\ 4)(5). \end{aligned}$$

Now $xy^2 = (1\ 6\ 3\ 5)(2\ 4)$ which rules out this possibility.

Therefore there are only two homomorphisms of $H(\lambda_5)$ onto a finite group of order 60, given in (iii) and (iv) with kernels $\Gamma_3(\lambda_5)$ and [5,5], respectively.

Let $\mu = 80$. Then using regular maps, we can find a unique homomorphism to (2,5,5) with kernel $[5,5]_4$.

Let $\mu = 100$. There is a unique Sylow 5-subgroup of order 25, by Sylow theorems. But this is not possible as otherwise the quotient would have order 100/25=4.

Finally let $\mu = 120$. Regular map theory again implies that there are homomorphisms from $H(\lambda_5)$ to S_5 and $A_5 \times C_2$ giving two normal subgroups $[5,4]_6$ and $[5,6]_4$, respectively.

Therefore we have a list of the normal subgroups of $H(\lambda_5)$ having index ≤ 120:

μ	N
1	$H(\lambda_5)$
2	$H^2(\lambda_5)$
5	$H^5(\lambda_5)$
10	$H'(\lambda_5)$, $\Gamma_2(\lambda_5)$
50	[5,10]
60	$\Gamma_3(\lambda_5)$, $[5,5]$
80	$[5,5]_4$
120	$[5,4]_6$, $C_2(\lambda_5)$

(10.28)

If N is a free normal subgroup of $H(\lambda_5)$ having genus g and parabolic class number t, then as $H(\lambda_5)$ has level $n = \mu/t$ and by the Riemann–Hurwitz formula

$$g = 1 + \frac{\mu}{20n}(3n - 10) \tag{10.29}$$

and therefore the level n of N must be > 3. Hence

$$\mu > 3t. \tag{10.30}$$

Then the rank r of N is given by

$$r = 1 + \frac{3\mu}{10}. \tag{10.31}$$

Let us now discuss some normal subgroups of $H(\lambda_5)$ in terms of their genera.

By (10.29), if $g = 0$, then $n = 2$ or 3 giving the two normal free subgroups $S_5(\lambda_5)$ and $\Gamma_3(\lambda_5)$ of genus 0 of $H(\lambda_5)$ of indices $\mu = 10$ and 60, respectively. There are also 3 normal torsion subgroups of $H(\lambda_5)$: $H(\lambda_5)$, $H^2(\lambda_5)$ and $H^5(\lambda_5)$ of indices 1,2 and 5, respectively. These are all normal torsion subgroups of $H(\lambda_5)$.

Secondly let $g = 1$. In Chapter 5, we showed that $H(\lambda_5)$ has no normal subgroups of genus 1.

Now let $g = 2$. By the Riemann–Hurwitz formula, if μ is the index and n is the level of N of genus 2 in $H(\lambda_5)$, we have

$$\mu = \frac{20n}{3n - 10}. \tag{10.32}$$

Then possible values of n are 4,5 and 10 giving $\mu = 40$, 20 and 10, respectively. We have shown that $H(\lambda_5)$ has no normal subgroup of index 20 or 40. The final one, having level 10, gives the commutator subgroup $H'(\lambda_5)$. That is, $H(\lambda_5)$ has a unique normal subgroup of genus 2, namely its commutator subgroup.

Consider $g = 3$. Then similarly all possible values of n are 4,5,6 and 10 giving subgroups of indices 80,40,30 and 20, respectively. The last three do not exist by the calculations we have done above. The first one, if existed, would correspond to a regular map of type $\{5,4\}$. But by [Sh,1], there is no regular map of genus three of type $\{5,4\}$. Therefore

Theorem 10.12: $H(\lambda_5)$ has no normal subgroups of genus 3.

Finally let $g = 4$. Possible values of n are 4,5,6,10 and 20 with indices 120,60,45,30,24, respectively. The third and last are automatically ruled out as $10 \nmid \mu$. We showed that $H(\lambda_5)$ has no normal subgroup of index 30. So the fourth is also ruled out. $n = 4$ and 5 give the two genus 4 normal subgroups of $H(\lambda_5)$, namely [5,5] and $[5,4]_6$, as the kernels of the homomorphisms of $H(\lambda_5)$ to A_5 and S_5, respectively.

We finally discuss a class of normal subgroups of $H(\lambda_5)$ which appears in [Co–Mo,1]. Consider the homomorphism of $H(\lambda_5)$ to $A_5 \times C_k \cong \langle\langle 2,5 \,|\, 3; k \rangle\rangle$, in Coxeter and Moser's notation, for some $k \in \mathbb{N}$. Let $C_k(\lambda_5)$ denote the kernel of this homomorphism. Here $H(\lambda_5)/C_k(\lambda_5)$ is a finite quotient of the triangle group $(2,5,3k)$. We can determine the signature of $C_k(\lambda_5)$ as $(9(k-1) : \infty^{(20)})$. The first few values of k that give a normal subgroup are k = 1,2,4,5 and 10. Some of them are listed in Appendix 1.

APPENDIX 1

TABLES

THE POLYNOMIALS $T_n(x)$ FOR $0 \leq n \leq 17$

n	$T_n(x)$
0	1
1	x
2	$2x^2 - 1$
3	$4x^3 - 3x$
4	$8x^4 - 8x^2 + 1$
5	$16x^5 - 20x^3 + 5x$
6	$32x^6 - 48x^4 + 18x^2 - 1$
7	$64x^7 - 112x^5 + 56x^3 - 7x$
8	$128x^8 - 256x^6 + 160x^4 - 32x^2 + 1$
9	$256x^9 - 576x^7 + 432x^5 - 120x^3 + 9x$
10	$512x^{10} - 1280x^8 + 1120x^6 - 400x^4 + 50x^2 - 1$
11	$1024x^{11} - 2816x^9 + 2816x^7 - 1232x^5 + 220x^3 - 11x$
12	$2048x^{12} - 6144x^{10} + 6912x^8 - 3584x^6 + 840x^4 - 72x^2 + 1$
13	$4096x^{13} - 13312x^{11} + 16640x^9 - 9984x^7 + 2912x^5 - 364x^3 + 13x$
14	$8192x^{14} - 28672x^{12} + 39424x^{10} - 26880x^8 + 9408x^6 - 1568x^4 + 98x^2 - 1$
15	$16384x^{15} - 61440x^{13} + 92160x^{11} - 70400x^9 + 28800x^7 - 6048x^5 + 560x^3 - 15x$
16	$32768x^{16} - 131072x^{14} + 212992x^{12} - 180224x^{10} + 84480x^8 - 21504x^6 + 2688x^4 - 128x^2 + 1$
17	$65536x^{17} - 278528x^{15} + 487424x^{13} - 452608x^{11} + 239360x^9 - 71808x^7 + 11424x^5 - 816x^3 + 17x$

THE POLYNOMIALS $A_n(x)$ FOR $0 \leq n \leq 32$

n	$A_n(x)$
0	1
1	x
2	$x^2 - 2$
3	$x^3 - 3x$
4	$x^4 - 4x^2 + 2$
5	$x^5 - 5x^3 + 5x$
6	$x^6 - 6x^4 + 9x^2 - 2$
7	$x^7 - 7x^5 + 14x^3 - 7x$
8	$x^8 - 8x^6 + 20x^4 - 16x^2 + 2$
9	$x^9 - 9x^7 + 27x^5 - 30x^3 + 9x$
10	$x^{10} - 10x^8 + 35x^6 - 50x^4 + 25x^2 - 2$
11	$x^{11} - 11x^9 + 44x^7 - 77x^5 + 55x^3 - 11x$
12	$x^{12} - 12x^{10} + 54x^8 - 112x^6 + 105x^4 - 36x^2 + 2$
13	$x^{13} - 13x^{11} + 65x^9 - 156x^7 + 182x^5 - 91x^3 + 13x$
14	$x^{14} - 14x^{12} + 77x^{10} - 210x^8 + 294x^6 - 196x^4 + 49x^2 - 2$
15	$x^{15} - 15x^{13} + 90x^{11} - 275x^9 + 450x^7 - 378x^5 + 140x^3 - 15x$
16	$x^{16} - 16x^{14} + 104x^{12} - 352x^{10} + 660x^8 - 672x^6 + 336x^4 - 64x^2 + 2$
17	$x^{17} - 17x^{15} + 119x^{13} - 442x^{11} + 935x^9 - 1122x^7 + 714x^5 - 204x^3 + 17x$
18	$x^{18} - 18x^{16} + 135x^{14} - 546x^{12} + 1287x^{10} - 1782x^8 + 1386x^6 - 540x^4 + 81x^2 - 2$
19	$x^{19} - 19x^{17} + 152x^{15} - 665x^{13} + 1729x^{11} - 2717x^9 + 2508x^7 - 1254x^5 + 285x^3 - 19x$
20	$x^{20} - 20x^{18} + 170x^{16} - 800x^{14} + 2275x^{12} - 4004x^{10} + 4290x^8 - 2640x^6 + 825x^4 - 100x^2 + 2$
21	$x^{21} - 21x^{19} + 189x^{17} - 952x^{15} + 2940x^{13} - 5733x^{11} + 7007x^9 - 5148x^7 + 2079x^5 - 385x^3 + 21x$
22	$x^{22} - 22x^{20} + 209x^{18} - 1122x^{16} + 3740x^{14} - 8008x^{12} + 11011x^{10} - 9438x^8 + 4719x^6 - 1210x^4 + 121x^2 - 2$
23	$x^{23} - 23x^{21} + 230x^{19} - 1311x^{17} + 4692x^{15} - 10948x^{13} + 16744x^{11} - 16445x^9 + 9867x^7 - 3289x^5 + 506x^3 - 23x$
24	$x^{24} - 24x^{22} + 252x^{20} - 1520x^{18} + 5814x^{16} - 14688x^{14} + 24752x^{12} - 27456x^{10} + 19305x^8 - 8008x^6 + 1716x^4 - 144x^2 + 2$

n	$A_n(x)$
25	$x^{25} - 25x^{23} + 275x^{21} - 1750x^{19} + 7125x^{17} - 19380x^{15} + 35700x^{13} - 44200x^{11} + 35750x^{9} - 17875x^{7} + 5005x^{5} - 650x^{3} + 25x$
26	$x^{26} - 26x^{24} + 299x^{22} - 2002x^{20} + 8645x^{18} - 25194x^{16} + 50388x^{14} - 68952x^{12} + 63206x^{10} - 37180x^{8} + 13013x^{6} - 2366x^{4} + 169x^{2} - 2$
27	$x^{27} - 27x^{25} + 324x^{23} - 2277x^{21} + 10395x^{19} - 32319x^{17} + 69768x^{15} - 104652x^{13} + 107406x^{11} - 72930x^{9} + 30888x^{7} - 7371x^{5} + 819x^{3} - 27x$
28	$x^{28} - 28x^{26} + 350x^{24} - 2576x^{22} + 12397x^{20} - 40964x^{18} + 94962x^{16} - 155040x^{14} + 176358x^{12} - 136136x^{10} + 68068x^{8} - 20384x^{6} + 3185x^{4} - 196x^{2} + 2$
29	$x^{29} - 29x^{27} + 377x^{25} - 2900x^{23} + 14674x^{21} - 51359x^{19} + 127281x^{17} - 284808x^{15} + 281010x^{13} - 243542x^{11} + 140998x^{9} - 51272x^{7} + 10556x^{5} - 1015x^{3} + 29x$
30	$x^{30} - 30x^{28} + 405x^{26} - 3250x^{24} + 17250x^{22} - 63756x^{20} + 168245x^{18} - 319770x^{16} + 436050x^{14} - 419900x^{12} + 277134x^{10} - 119340x^{8} + 30940x^{6} - 4200x^{4} + 225x^{2} - 2$
31	$x^{31} - 31x^{29} + 434x^{27} - 3627x^{25} + 20150x^{23} - 78430x^{21} + 219604x^{19} - 447051x^{17} + 660858x^{15} - 700910x^{13} + 520676x^{11} - 260338x^{9} + 82212x^{7} - 14756x^{5} + 1240x^{3} - 31x$
32	$x^{32} - 32x^{30} + 464x^{28} - 4032x^{26} + 23400x^{24} - 95680x^{22} + 283360x^{20} - 615296x^{18} + 980628x^{16} - 1136960x^{14} + 940576x^{12} - 537472x^{10} + 201552x^{8} - 45696x^{6} + 5440x^{4} - 256x^{2} + 2$

THE POLYNOMIALS $\Psi_n(x)$ FOR $1 \leq n \leq 13$

1	$x - 1$
2	$x + 1$
3	$x + \frac{1}{2}$
4	x
5	$x^2 + \frac{x}{2} - \frac{1}{4}$
6	$x - \frac{1}{2}$
7	$x^3 + \frac{x^2}{2} - \frac{x}{2} - \frac{1}{8}$
8	$x^2 - \frac{1}{2}$
9	$x^3 - \frac{3x}{4} + \frac{1}{8}$
10	$x^2 - \frac{x}{2} - \frac{1}{4}$
11	$x^5 + \frac{x^4}{2} - x^3 - \frac{3x^2}{8} + \frac{3x}{16} + \frac{1}{32}$
12	$x^2 - \frac{3}{4}$
13	$x^6 + \frac{x^5}{2} - \frac{5x^4}{4} - \frac{x^3}{2} + \frac{3x^2}{8} + \frac{3x}{32} - \frac{1}{64}$

THE MINIMAL POLYNOMIAL $P_q^*(x)$ OF λ_q FOR $3 \leq q \leq 50$

q	$\varphi(q)$	d	$P_q^*(x)$
3	2	1	$x - 1$
4	2	2	$x^2 - 2$
5	4	2	$x^2 - x - 1$
6	2	2	$x^2 - 3$
7	6	3	$x^3 - x^2 - 2x + 1$
8	4	4	$x^4 - 4x^2 + 2$
9	6	3	$x^3 - 3x - 1$
10	4	4	$x^4 - 5x^2 + 5$
11	10	5	$x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1$
12	4	4	$x^4 - 4x^2 + 1$
13	12	6	$x^6 - x^5 - 5x^4 + 4x^3 + 6x^2 - 3x - 1$
14	6	6	$x^6 - 7x^4 + 14x^2 - 7$
15	8	4	$x^4 + x^3 - 4x^2 - 4x + 1$
16	8	8	$x^8 - 8x^6 + 20x^4 - 16x^2 + 2$
17	16	8	$x^8 - x^7 - 7x^6 + 6x^5 + 15x^4 - 10x^3 - 10x^2 + 4x + 1$
18	6	6	$x^6 - 6x^4 + 9x^2 - 3$
19	18	9	$x^9 - x^8 - 8x^7 + 7x^6 + 21x^5 - 15x^4 - 20x^3 + 10x^2 + 5x - 1$
20	8	8	$x^8 - 8x^6 + 19x^4 - 12x^2 + 1$
21	12	6	$x^6 + x^5 - 6x^4 - 6x^3 + 8x^2 + 8x + 1$
22	10	10	$x^{10} - 11x^8 + 44x^6 - 77x^4 + 55x^2 - 11$
23	22	11	$x^{11} - x^{10} - 10x^9 + 9x^8 + 36x^7 - 28x^6 - 56x^5 + 35x^4 + 35x^3 - 15x^2 - 6x + 1$
24	8	8	$x^8 - 8x^6 + 20x^4 - 16x^2 + 1$
25	20	10	$x^{10} - 10x^8 + 35x^6 - x^5 - 50x^4 + 5x^3 + 25x^2 - 5x - 1$
26	12	12	$x^{12} - 13x^{10} + 65x^8 - 156x^6 + 182x^4 - 91x^2 + 13$
27	18	9	$x^9 - 9x^7 + 27x^5 - 30x^3 + 9x - 1$
28	12	12	$x^{12} - 12x^{10} + 53x^8 - 104x^6 + 86x^4 - 24x^2 + 1$
29	28	14	$x^{14} - x^{13} - 13x^{12} + 12x^{11} + 66x^{10} - 55x^9 - 165x^8 + 120x^7 + 210x^6 - 126x^5 - 126x^4 + 56x^3 + 28x^2 - 7x - 1$
30	8	8	$x^8 - 7x^6 + 14x^4 - 8x^2 + 1$

q	$\varphi(q)$	d	$P_q^*(x)$
31	30	15	$x^{15}-x^{14}-14x^{13}+13x^{12}+78x^{11}-66x^{10}-220x^9+165x^8+330x^7-210x^6-252x^5+126x^4+84x^3-28x^2-8x+1$
32	16	16	$x^{16}-16x^{14}+104x^{12}-352x^{10}+660x^8-672x^6+336x^4-64x^2+2$
33	20	10	$x^{10}+x^9-10x^8-10x^7+34x^6+34x^5-43x^4-43x^3+12x^2+12x+1$
34	16	16	$x^{16}-17x^{14}+119x^{12}-442x^{10}+935x^8-1122x^6+714x^4-204x^2+17$
35	24	12	$x^{12}+x^{11}-12x^{10}-11x^9+54x^8+43x^7-113x^6-71x^5+110x^4+46x^3-40x^2-8x+1$
36	12	12	$x^{12}-12x^{10}+54x^8-112x^6+105x^4-36x^2+1$
37	36	18	$x^{18}-x^{17}-17x^{16}+16x^{15}+120x^{14}-105x^{13}-455x^{12}+364x^{11}+1001x^{10}-715x^9-1277x^8+792x^7+914x^6-462x^5-330x^4+120x^3+45x^2-9x-1$
38	18	18	$x^{18}-19x^{16}+152x^{14}-665x^{12}+1729x^{10}-2717x^8+2498x^6-1254x^4+285x^2-19$
39	24	12	$x^{12}+x^{11}-12x^{10}-12x^9+53x^8+53x^7-103x^6-103x^5+79x^4+79x^3-12x^2-12x+1$
40	16	16	$x^{16}-16x^{14}+104x^{12}-352x^{10}+659x^8-664x^6+316x^4-48x^2+1$
41	40	20	$x^{20}-x^{19}-19x^{18}+18x^{17}+153x^{16}-136x^{15}-680x^{14}+560x^{13}+1820x^{12}-1365x^{11}-3003x^{10}+2002x^9+3003x^8-1716x^7-1716x^6+792x^5+495x^4-165x^3-55x^2+10x+1$
42	12	12	$x^{12}-11x^{10}+44x^8-78x^6+60x^4-16x^2+1$
43	42	21	$x^{21}-x^{20}-20x^{19}+19x^{18}+171x^{17}-153x^{16}-816x^{15}+680x^{14}+2380x^{13}-1820x^{12}-4368x^{11}+3003x^{10}+5005x^9-3003x^8-3432x^7+1716x^6+1287x^5-495x^4-220x^3+55x^2+11x-1$
44	20	20	$x^{20}-20x^{18}+169x^{16}-784x^{14}+2172x^{12}-3664x^{10}+3683x^8-2072x^6+575x^4-60x^2+1$
45	24	12	$x^{12}-12x^{10}+x^9+54x^8-9x^7-112x^6+27x^5+105x^4-31x^3-36x^2+12x+1$.

q	$\varphi(q)$	d	$P_q^*(x)$
46	22	22	$x^{22} - 23x^{20} + 230x^{18} - 1311x^{16} + 4692x^{14} - 10938x^{12} + 16694x^{10} - 16375x^8 + 9837x^6 - 3289x^4 + 506x^2 - 23$
47	46	23	$x^{23} - x^{22} - 22x^{21} + 21x^{20} + 210x^{19} - 190x^{18} - 1140x^{17} + 969x^{16} + 3876x^{15} - 3060x^{14} - 8568x^{13} + 6188x^{12} + 12376x^{11} - 8008x^{10} - 11440x^9 + 6435x^8 + 6435x^7 - 3003x^6 - 2002x^5 + 715x^4 + 286x^3 - 66x^2 - 12x + 1$
48	16	16	$x^{16} - 16x^{14} + 104x^{12} - 352x^{10} + 660x^8 - 672x^6 + 336x^4 - 64x^2 + 1$
49	42	21	$x^{21} - 21x^{19} + 189x^{17} - 952x^{15} - x^{14} + 2940x^{13} + 14x^{12} - 5733x^{11} - 77x^{10} + 7007x^9 + 210x^8 - 5147x^7 - 294x^6 + 2072x^5 + 196x^4 - 371x^3 - 49x^2 + 14x + 1$
50	20	20	$x^{20} - 20x^{18} + 170x^{16} - 800x^{14} + 2275x^{12} - 4005x^{10} + 4300x^8 - 2675x^6 + 875x^4 - 125x^2 + 5$

NORMAL SUBGROUPS OF $H(\sqrt{2})$ WITH INDEX < 60 [1]

μ	$H(\sqrt{2})/N$	Associated triangle group	N	Signature of N	n
1	$\{1\}$	$(1,1,1)$	$H(\sqrt{2})=Y_1(\sqrt{2})$	$(0;\ 2,4,\infty)$	1
	C_2	$(2,2,1)$	$H_e(\sqrt{2}) = K_2(\sqrt{2})$	$(0;\ 2,\infty,\infty)$	1
2	C_2	$(1,2,2)$	$Y_2(\sqrt{2})$	$(0;\ 2,2,2,\infty)$	2
	C_2	$(2,1,2)$	$S_1(\sqrt{2})$	$(0;\ 4,4,\infty)$	2
	D_2	$(2,2,2)$	$H^2(\sqrt{2}) = S_2(\sqrt{2})$	$(0;\ 2,2,\infty,\infty)$	2
4	C_4	$(2,4,4)$	$K = [4,4]_{1,0}$	$(1;\ \infty)$	4
	C_4	$(1,4,4)$	$Y_4(\sqrt{2})$	$(0;\ 2,2,2,2,\infty)$	4
8	$L^+(0)$	$(2,4,2)$	$S_4(\sqrt{2}) = \hat{K}(0)$	$(0;\ \infty,\infty,\infty,\infty)$	2
	$C_2 \times C_4$	$(2,4,4)$	$H'(\sqrt{2}) = [4,4]_{1,1}$	$(1;\ \infty,\infty)$	4
16	$L^+(1)$	$(2,4,4)$	$\hat{K}(1)$	$(1;\ \infty,\infty,\infty,\infty)$	4
	$C_8 \times C_2$	$(2,4,8)$	$[4,8]_{1,1}$	$(2;\ \infty,\infty)$	8
20	$Aff(1,5)$	$(2,4,4)$	$[4,4]_{2,1}$	$(1;\ \infty^{(5)})$	4
	$Aff(1,5)$	$(2,4,4)$	$[4,4]_{1,2}$	$(1;\ \infty^{(5)})$	4
	S_4	$(2,4,3)$	$K_3(\sqrt{2}) = T_4(\sqrt{2})$	$(0;\ \infty^{(8)})$	3
24	$L^+(2)$	$(2,4,6)$	$\hat{K}(\sqrt{2})$	$(2;\ \infty,\infty,\infty,\infty)$	6
	$C_4 \times D_3$	$(2,4,12)$	$[4,12]_{1,1}$	$(3;\ \infty,\infty)$	12
	$G^{4,4,8}$	$(2,4,4)$	$[4,4]_{2,2}$	$(1;\ \infty^{(8)})$	4
32	$L^+(3)$	$(2,4,8)$	$\hat{K}(3)$	$(3;\ \infty,\infty,\infty,\infty)$	8
	$\ll 2,8\mid 2;2 \gg$	$(2,4,8)$	$[4,8]_{2,0}$	$(3;\infty,\infty,\infty,\infty)$	8
	$< 2,8\mid 2;2 >$	$(2,4,16)$	$[4,16]_{1,1}$	$(4;\ \infty,\infty)$	16
36	$(4,4\mid 2,3)$	$(2,4,4)$	$[4,4]_{3,0}$	$(1;\ \infty^{(9)})$	4
	See [Co–Mo,1]	$(2,4,4)$	$[4,4]_{3,1}$	$(1;\ \infty^{(10)})$	4
40	See [Co–Mo,1]	$(2,4,4)$	$[4,4]_{1,3}$	$(1;\ \infty^{(10)})$	4
	$L^+(4)$	$(2,4,10)$	$\hat{K}(4)$	$(4;\ \infty,\infty,\infty,\infty)$	10
	$< 2,10\mid 2;2 >$	$(2,4,20)$	$[4,20]_{1,1}$	$(5;\ \infty,\infty)$	20
	$S_4 \times C_2$	$(2,4,6)$	$[4,6]_3$	$(3;\ \infty^{(8)})$	6
48	$\ll 2,12\mid 2;2 \gg$	$(2,4,12)$	$[4,12]_{2,0}$	$(5;\ \infty,\infty,\infty,\infty)$	12
	$< 2,12\mid 2;2 >$	$(2,4,24)$	$[4,24]_{1,1}$	$(6;\ \infty,\infty)$	24
52	See [Co–Mo,1]	$(2,4,4)$	$[4,4]_{2,3}$	$(1;\ \infty^{(13)})$	4
	See [Co–Mo,1]	$(2,4,4)$	$[4,4]_{3,2}$	$(1;\ \infty^{(13)})$	4
56	$\ll 2,14\mid 2;2 \gg$	$(2,4,14)$	$[4,14]_{2,0}$	$(6;\ \infty,\infty,\infty,\infty)$	14
	$< 2,14\mid 2;2 >$	$(2,4,28)$	$[4,28]_{1,1}$	$(7;\ \infty,\infty)$	28

[1] Excluding $W_n(\sqrt{2})$ with $n \geq 3$

REGULAR MAPS CORRESPONDING TO THE NORMAL SUBGROUPS OF $H(\sqrt{2})$ WITH INDEX < 60

μ	N	g	n_0	n_1	n_2	Aut. group	Regular map
1	$H(\sqrt{2})$	0	–	–	–	$\{1\}$	degenerate
2	$H_e(\sqrt{2})$	0	1	1	2	C_2	$\{1.2, 1\}$
	$Y_2(\sqrt{2})$	0	–	–	–	C_2	degenerate
	$S_1(\sqrt{2})$	0	2	1	1	C_2	$\{1, 1.2\}$
4	$H^2(\sqrt{2})$	0	2	2	2	D_2	$\{1.2, 2\}$
	K	1	1	2	1	C_4	$\{4,4\}_{1,0}$
	$Y_4(\sqrt{2})$	0	–	–	–	C_4	degenerate
8	$\hat{K}(0)$	0	2	4	4	D_4	$\{2.2, 2\}_{2,0}$
	$H'(\sqrt{2})$	1	2	4	2	$C_2 \times C_4$	$\{2.2, 2.2\}_{1,1}$
16	$\hat{K}(1)$	1	4	8	4	$L^+(1)$	$\{2.2, 4\}_{2,0}$
	$[4,8]_{1,1}$	2	4	8	2	$C_8 \times C_2$	$\{2.2, 2.4\}_{1,1}$
20	$[4,4]_{2,1}$	1	5	10	5	$Aff(1,5)$	$\{4,4\}_{2,1}$
	$[4,4]_{1,2}$	1	5	10	5	$Aff(1,5)$	$\{4,4\}_{1,2}$
24	$\Gamma_3(\sqrt{2})$	0	6	12	8	S_4	$\{4,3\}$
	$\hat{K}(2)$	2	6	12	4	$L^+(2)$	$\{2.2, 6\}_{2,0}$
	$[4,12]_{1,1}$	3	6	12	2	$C_4 \times D_3$	$\{2.2, 2.6\}_{1,1}$
32	$[4,4]_{2,2}$	1	8	16	8	$G^{4,4,8}$	$\{4,4\}_{2,2}$
	$\hat{K}(3)$	3	8	16	4	$L^+(3)$	$\{4, 4.2\}$
	$[4,8]_{2,0}$	3	8	16	4	$\ll 2,8\|2;2 \gg$	$\{2.2, 8\}_{2,0}$
	$[4,16]_{1,1}$	4	8	16	2	$< 2,8\|2;2 >$	$\{2.2, 2.8\}_{1,1}$
36	$[4,4]_{3,0}$	1	9	18	9	$(4,4\|2,3)$	$\{4,4\}_{3,0}$
40	$[4,4]_{3,1}$	1	10	20	10	See [Co–Mo,1]	$\{4,4\}_{3,1}$
	$[4,4]_{1,3}$	1	10	20	10	See [Co–Mo,1]	$\{4,4\}_{1,3}$
	$\hat{K}(4)$	4	10	20	4	$L^+(4)$	$\{2.2, 10\}_{2,0}$
	$[4,20]_{1,1}$	5	10	20	2	$< 2,10\|2;2 >$	$\{2.2, 2.10\}_{1,1}$
48	$[4,6]_3$	3	12	24	8	$S_4 \times C_2$	$\{4,6\}_3$
	$[4,12]_{2,0}$	5	12	24	4	$\ll 2,12\|2;2 \gg$	$\{2.2, 12\}_{2,0}$
	$[4,24]_{1,1}$	6	12	24	2	$< 2,12\|2;2 >$	$\{2.2, 2.12\}_{1,1}$
52	$[4,4]_{2,3}$	1	13	26	13	See [Co–Mo,1]	$\{4,4\}_{2,3}$
	$[4,4]_{3,2}$	1	13	26	13	See [Co–Mo,1]	$\{4,4\}_{3,2}$
56	$[4,14]_{2,0}$	6	14	28	4	$\ll 2,14\|2;2 \gg$	$\{2.2, 14\}_{2,0}$
	$[4,28]_{1,1}$	7	14	28	2	$< 2,14\|2;2 >$	$\{2.2, 2.14\}_{1,1}$

NORMAL SUBGROUPS OF $H(\sqrt{3})$ WITH INDEX < 84 [2]

μ	$H(\sqrt{3})/N$	Associated triangle group	N	Signature of N	n
1	$\{1\}$	$(1,1,1)$	$H(\sqrt{3})=Y_1(\sqrt{3})$	$(0;\ 2,6,\infty)$	1
2	C_2	$(2,2,1)$	$H_e(\sqrt{3})$	$(0;\ 3,\infty,\infty)$	1
	C_2	$(1,2,2)$	$Y_2(\sqrt{3})$	$(0;\ 2,2,3,\infty)$	2
	C_2	$(2,1,2)$	$S_1(\sqrt{3})$	$(0;\ 6,6,\infty)$	2
3	C_3	$(1,3,3)$	$H^3(\sqrt{3}) = Y_3(\sqrt{3})$	$(0;\ 2,2,2,2,\infty)$	3
4	D_2	$(2,2,2)$	$H^2(\sqrt{3}) = S_2(\sqrt{3})$	$(0;\ 3,3,\infty,\infty)$	2
6	D_3	$(2,3,2)$	$S_3(\sqrt{3})$	$(0;\ 2,2,\infty,\infty,\infty)$	2
	C_6	$(2,6,3)$	$K = [6,3]_{1,0}$	$(1;\ \infty,\infty)$	3
	C_6	$(2,3,6)$	$[3,6]_{1,0}$	$(1;\ 2,2,\infty)$	6
	C_6	$(1,6,6)$	$Y_6(\sqrt{3})$	$(0;\ 2^{(6)},\infty)$	6
12	D_6	$(2,6,2)$	$S_6(\sqrt{3})$	$(0;\ \infty^{(6)})$	2
	A_4	$(2,3,3)$	$T_1(\sqrt{3})$	$(0;\ 2^{(4)},\infty^{(4)})$	3
	$C_2 \times C_6$	$(2,6,6)$	$H'(\sqrt{3}) = [6,6]_{1,0}$	$(2;\ \infty,\infty)$	6
18	$\ll 2,3\|2;3 \gg$	$(2,6,3)$	$[6,3]_{1,1}$	$(1;\ \infty^{(6)})$	3
	$\ll 2,3\|2;3 \gg$	$(2,3,6)$	$[3,6]_{1,1}$	$(1;\ 2^{(6)},\infty^{(3)})$	6
24	$G^{3,6,4}$	$(2,6,3)$	$[6,3]_{2,0}$	$(1;\ \infty^{(8)})$	3
	S_4	$(2,3,4)$	$T_2(\sqrt{3})$	$(0;\ 2^{(8)},\infty^{(6)})$	4
	$L^+(2)$	$(2,6,4)$	$\hat{K}(2)$	$(2;\ \infty^{(6)})$	4
	$G^{3,6,4}$	$(2,3,6)$	$[3,6]_{2,0}$	$(1;\ 2^{(8)},\infty^{(4)})$	6
	$A_4 \times C_2$	$(2,6,6)$	$[6,6]$	$(3;\ \infty,\infty,\infty,\infty)$	6
	$< 2,4\|2;3 >$	$(2,6,12)$	$[6,12]_{1,0}$	$(4;\ \infty,\infty)$	12
30	$< 2,5\|2;3 >$	$(2,6,15)$	$[6,15]_{1,0}$	$(5;\ \infty,\infty)$	15
36	See [Ga,1]	$(2,6,6)$	$G_{2,3}$	$(4;\ \infty^{(6)})$	6
	$\ll 2,6\|2;3 \gg$	$(2,6,6)$	$[6,6]_{1,1}$	$(4;\ \infty^{(6)})$	6
	See [Ga,1]	$(2,6,6)$	$[6,6]$	$(4;\ \infty^{(6)})$	6
42	See [Co–Mo,1]	$(2,6,3)$	$[6,3]_{2,1}$	$(1;\ \infty^{(14)})$	3
	See [Co–Mo,1]	$(2,6,3)$	$[6,3]_{1,2}$	$(1;\ \infty^{(14)})$	3
	See [Co–Mo,1]	$(2,3,6)$	$[3,6]_{2,1}$	$(1;\ 2^{(14)},\infty^{(7)})$	6
	See [Co–Mo,1]	$(2,3,6)$	$[3,6]_{1,2}$	$(1;\ 2^{(14)},\infty^{(7)})$	6
	$< 2,7\|2;3 >$	$(2,6,21)$	$[6,21]_{1,0}$	$(7;\ \infty,\infty)$	21

[2] Excluding $W_n(\sqrt{3})$ with $n \geq 3$

μ	$\mathrm{H}(\sqrt{3})/N$	Associated triangle group	N	Signature of N	n
	$S_4 \times C_2$	$(2,6,4)$	$[6,4]_3$	$(3;\ \infty^{(12)})$	4
	See [Ga,1]	$(2,6,6)$	$[6,6]_{2,0}$	$(5;\ \infty^{(8)})$	6
	$\ll 2,3\|4;2 \gg$	$(2,3,8)$	$[3,8]$	$(2;\ 2^{(16)}, \infty^{(6)})$	8
48	$< 4,3\|2;2 >$	$(2,6,8)$	$[6,8]$	$(6;\ \infty^{(6)})$	8
	$\ll 2,3\|3 \gg$	$(2,3,12)$	$[3,12]$	$(3;\ 2^{(16)}, \infty, \infty, \infty, \infty)$	12
	See [Ga,2]	$(2,6,12)$	$[6,12]$	$(7;\ \infty^{(4)})$	12
	See [Co–Mo,1]	$(2,6,24)$	$[6,24]_{1,0}$	$(8;\ \infty, \infty)$	24
	$G^{3,6,6}$	$(2,6,3)$	$[6,3]_{3,0}$	$(1;\ \infty^{(18)})$	3
	$G^{3,6,6}$	$(2,3,6)$	$[3,6]_{3,0}$	$(1;\ 2^{(18)}, \infty^{(9)})$	6
54	$\ll 2,9\|2;3 \gg$	$(2,6,9)$	$[6,9]_{1,1}$	$(7;\ \infty^{(6)})$	9
	See [Ga,2]	$(2,6,9)$	$[6,9]$	$(7;\ \infty^{(6)})$	9
	See [Ga,2]	$(2,6,9)$	$[6,9]$	$(7;\ \infty^{(6)})$	9
	A_5	$(2,3,5)$	$T_3(\sqrt{3})$	$(0;\ 2^{(20)}, \infty^{(12)})$	5
60	See [Co–Mo,1]	$(2,6,10)$	$[6,10]$	$(8;\ \infty^{(6)})$	10
	$< 2,10\|2;3 >$	$(2,6,30)$	$[6,30]_{1,0}$	$(10;\ \infty, \infty)$	30
66	See [Co–Mo,1]	$(2,6,33)$	$[6,33]_{1,0}$	$(11;\ \infty, \infty)$	33
	See [Co–Mo,1]	$(2,6,3)$	$[6,3]_{2,2}$	$1;\ \infty^{(24)})$	3
	See [Ga,1]	$(2,6,4)$	$[6,4]_4$	$(4;\ \infty^{(18)})$	4
	See [Co–Mo,1]	$(2,3,6)$	$[3,6]_{2,2}$	$(1;\ 2^{(24)}, \infty^{(12)})$	6
72	$\ll 2,6\|2;6 \gg$	$(2,6,12)$	$[6,12]_{1,1}$	$(10;\ \infty^{(6)})$	12
	See [Co–Mo,1]	$(2,6,12)$	$[6,12]$	$(10;\ \infty^{(6)})$	12
	$\ll 2,12\|2;3 \gg$	$(2,6,12)$	$[6,12]_{1,1}$	$(10;\ \infty^{(6)})$	12
	See [Co–Mo,1]	$(2,6,12)$	$[6,12]$	$(10;\ \infty^{(6)})$	12
	See [Co–Mo,1]	$(2,6,3)$	$[6,3]_{3,1}$	$(1;\ \infty^{(26)})$	3
	See [Co–Mo,1]	$(2,6,3)$	$[6,3]_{1,3}$	$(1;\ \infty^{(26)})$	3
78	See [Co–Mo,1]	$(2,3,6)$	$[3,6]_{3,1}$	$(1;\ 2^{(26)}, \infty^{(13)})$	6
	See [Co–Mo,1]	$(2,3,6)$	$[3,6]_{1,3}$	$1;\ 2^{(26)}, \infty^{(13)})$	6
	$< 2,13\|2;3 >$	$(2,6,39)$	$[6,39]_{1,0}$	$(13;\ \infty, \infty)$	39

NORMAL SUBGROUPS OF H(λ_5) WITH INDEX $\leq$ 160

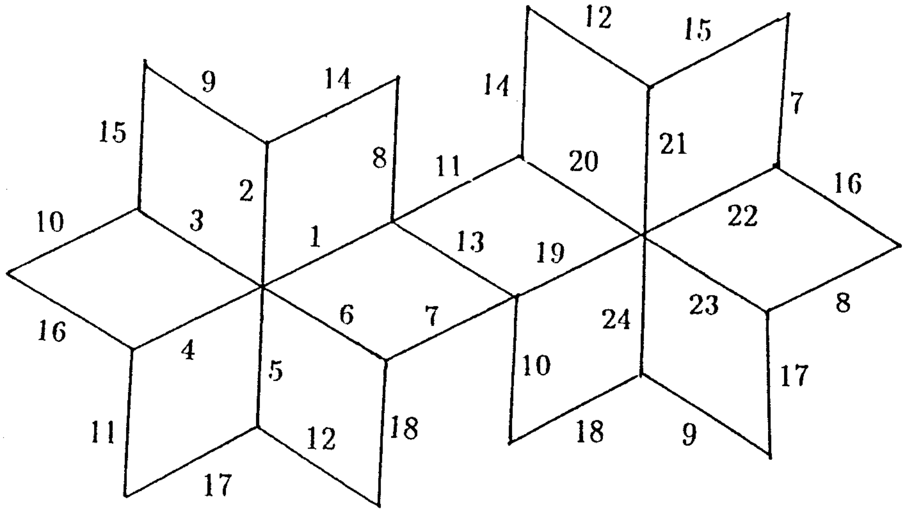
μ	$H(\lambda_5)/N$	Associated triangle group	N	Signature of N	n
1	$\{1\}$	$(1,1,1)$	$H(\lambda_5)$	$(0;\, 2,5,\infty)$	1
2	C_2	$(2,1,2)$	$H^2(\lambda_5)$	$(0;\, 5,5,\infty)$	2
5	C_5	$(1,5,5)$	$H^5(\lambda_5)$	$(0;\, 2^{(5)},\infty)$	5
10	C_{10}	$(2,5,10)$	$H'(\lambda_5)$	$(2;\, \infty)$	10
	D_5	$(2,5,2)$	$\Gamma_2(\lambda_5) = S_5(\lambda_5)$	$(0;\, \infty^{(5)})$	2
50	$C_5 \wr C_2$	$(2,5,10)$	$[5,10]$	$(6;\, \infty^{(5)})$	10
60	A_5	$(2,5,3)$	$\Gamma_3(\lambda_5) = C_1(\lambda_5)$	$(0;\, \infty^{(20)})$	3
	A_5	$(2,5,5)$	$[5,5]$	$(4;\, \infty^{(12)})$	5
80	$(4,5\|2,4)$	$(2,5,5)$	$[5,5]_4$	$(5;\, \infty^{(16)})$	5
120	S_5	$(2,5,4)$	$[5,4]_6$	$(4;\, \infty^{(30)})$	4
	$A_5 \times C_2$	$(2,5,6)$	$[5,6]_4 = C_2(\lambda_5)$	$(9;\, \infty^{(20)})$	6
160	See [Ga,1]	$(2,5,4)$	$[5,4]$	$(5;\, \infty^{(40)})$	4

REGULAR MAPS CORRESPONDING TO THE NORMAL SUBGROUPS OF $H(\lambda_5)$ WITH INDEX $\leq$ 160

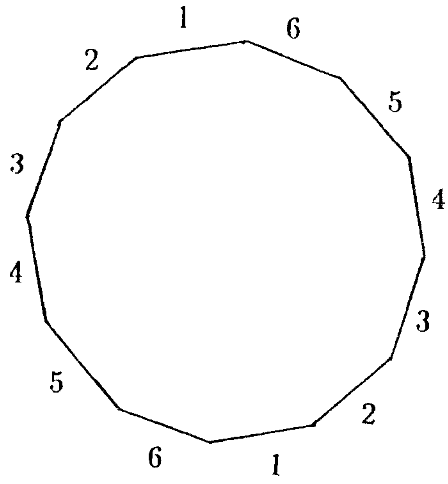
μ	N	g	n_0	n_1	n_2	Aut. group	Regular map
1	$H(\lambda_5)$	0	–	–	–	$\{1\}$	degenerate
2	$H^2(\lambda_5)$	0	2	1	1	C_2	$\{1, 1.2\}$
5	$H^5(\lambda_5)$	0	–	–	–	C_5	degenerate
10	$H'(\lambda_5)$	2	2	5	1	C_{10}	$\{5, 10\}_2$
	$\Gamma_2(\lambda_5)$	0	2	5	5	D_5	$\{5, 1.2\}$
50	$[5, 10]$	6	10	25	5	$C_5 \wr C_2$	$\{5, 5.2\}$
60	$\Gamma_3(\lambda_5)$	0	12	30	20	A_5	$\{5, 3\}$
	$[5, 5]$	4	12	30	12	A_5	$\{5, 5\|3\}$
80	$[5, 5]_4$	5	16	40	16	$(4, 5\|2, 4)$	$\{5, 5\}_4$
120	$[5, 4]_6$	4	24	60	30	S_5	$\{5, 4\}_6$
	$C_2(\lambda_5)$	9	24	60	20	$A_5 \times C_2$	$\{5, 2.3\}_4$
160	$[5, 4]$	5	32	80	40	See [Ga,1]	$\{5, 4\|4\}$

NUMBER OF NORMAL GENUS 1 SUBGROUPS OF H(λ_q) OF INDEX μ FOR μ, $q \leq 20$.

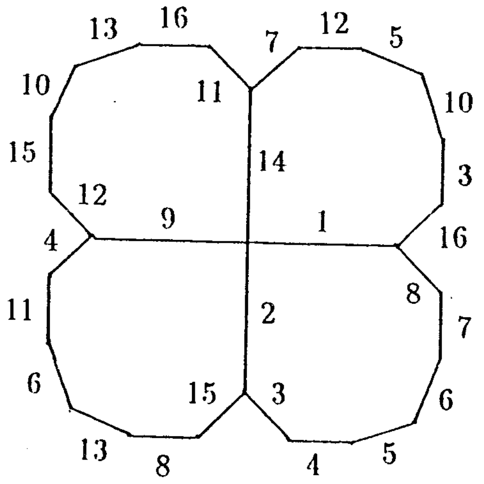
$\mu\backslash q$	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	1	0	0	2	0	0	1	0	0	2	0	0	1	0	0	2	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	1	0	0	2	0	0	1	0	0	2	0	0	1	0	0	2	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	2	0	0	0	2	0	0	0	2	0	0	0	2	0	0	0	2



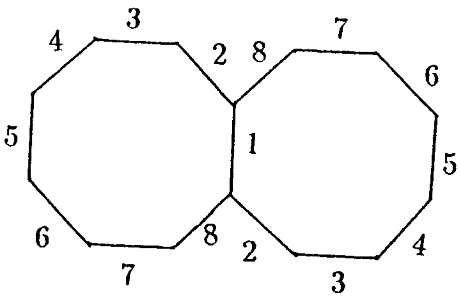
{4, 2.3}



$\{12, 12\}_{1,0}$



{4.2, 4}



$\{8, 8\}_2$

REFERENCES

[Al,1] R.B.J.T. ALLENBY, *Rings, Fields and Groups*, second ed., Edward Arnold – London–New York– Melbourne–Auckland (1991)

[Ba,1] E.P. BAUHOFF, *Zykloide Nichtkongruenzuntergruppen in den Heckeschen Gruppen* $G(\sqrt{d})$, J. reine angew. Math., 297 (1978), 172–176

[Be,1] A.F. BEARDON, *The Geometry of Discrete Groups*, Graduate Texts in Mathematics, 91, Springer – Berlin (1983)

[Bh,1] H.R. BRAHANA, *Regular Maps and Their Groups*, Amer. J. Math., 49 (1927), 268–284

[Bn,1] P. BENDING, *Some Topics in Galois Theory*, Project – Southampton (1993)

[Bo,1] W. BORHO, *Kettenbrüche im Galoisfeld*, Abh. Math. Sem. Univ. Hamburg, 39 (1973), 76–82

[Bo–Ro,1] W. BORHO & G. ROSENBERGER, *Eine Bemerkung zur Hecke-Gruppe* $G(\lambda)$, Abh. Math. Sem. Univ. Hamburg, 39 (1973), 83–87

[Br–Si,1] R.P. BRYANT & D. SINGERMAN, *Foundations of the Theory of Maps on Surfaces with Boundary*, Quart. J. Math. Oxford (2), 36 (1985), 17–41

[Cn,1] M. CONDER, *A letter to D. Singerman*, (1993)

[Co–Mo,1] H.S.M. COXETER & W.O.J. MOSER, *Generators and Relations for Discrete Groups*, Springer – Berlin (1957)

[Di,1] L.E. DICKSON, *Linear Groups with an Exposition of the Galois Field Theory*, Leipzig (1901), reprinted by Dover (1960)

[Ed–Ew–Ku,1] A.L. EDMONDS & J.H. EWING & R.S. KULKARNI, *Regular Tessellations of Surfaces and* $(p,q,2)$*–Triangle Groups*, Ann. of Maths., 116 (1982), 113–132

[Ev,1] R. EVANS, *A Fundamental Region for Hecke's Modular Group*, J. of No.

Thry., 5 (1973), 108–115

[Fo,1] L.R. FORD, *Automorphic Functions*, second ed., Chelsea–New York (1951)

[Fr,1] J.B. FRALEIGH, *A First Corse in Abstract Algebra*, sixth ed., Addison–Wesley Pub. Comp. (1974)

[Ga,1] D. GARBE, *Über die regulären Zerlegungen geschlossener orientierbarer Flächen*, J. reine. angew. Math., 237 (1969), 39–55

[Ga,2] D. GARBE, *A Remark on Nonsymmetric Compact Riemann Surfaces*, Arch. der Math., 30 (1978), 435–437

[Gi–Ma,1] J. GILMAN & B. MASKIT, *An Algorithm for two generator Fuchsian Groups*, Michigan Math. J., 38 (1991), 13–32

[Gu,1] R.C. GUNNING, *Lectures on Modular Forms*, Princeton (1962)

[Ha,1] M. HALL, *The Theory of Groups*, New York (1959)

[He,1] E. HECKE, *Über die Bestimmung Dirichletscher Reichen durch ihre Funktionalgleichungen*, Math. Ann., 112 (1936), 664–699

[Hf,1] L. HEFFTER, *Über metacyklische Gruppen und Nachbarconfigurationen*, Math. Ann., 50 (1898), 261–268

[Ho–Si,1] A.H.M. HOARE & D. SINGERMAN, *The Orientability of Subgroups of Plane Groups*, Proc. of St. Andrews Conf.–1981, L.M.S. Lecture Note Series, 71 (1982), 221–227

[Jh,1] D.L.JOHNSON, *Topics in the Theory of Group Presentations*, L.M.S. Lecture Note Series, 42 (1980), Cambridge Univ. Press

[Jo,1] G.A. JONES, *Noncongruence Subgroups of the Hecke groups $G(\sqrt{d})$*, J. reine. angew. Math., 314 (1980), 174–176

[Jo,2] G.A. JONES, *Enumerating Regular mmps and Hypermaps*, Disertaciones del Seminario de Matemáticas Fundamentales (1989)

[Jo–Si,1] G.A. JONES & D. SINGERMAN, *Theory of Maps on Orientable Surfaces*, Proc. L.M.S. (3) 37 (1978), 273–307

[**Jo–Si,2**] G.A. JONES & D. SINGERMAN, *Complex Functions*, Cambridge University Press (1987)

[**Kn,1**] H.L. KENG, *Introduction to Number Theory*, Springer–Verlag – Berlin (1982)

[**Kn–Yu,1**] H.L. KENG & W. YUAN, Applications of Number Theory to Numerical Analysis, Springer–Verlag (1981)

[**Ke–Ro,1**] G. KERN-ISBERNER & G. ROSENBERGER, *Normalteiler vom Geschlecht eins in freien Produkten endlicher zyklischer Gruppen*, Results in Mathematics, 11 (1987), 272–288

[**Le,1**] A. LEUTBECHER, *Über die Heckeschen Gruppen $G(\lambda)$*, Abh. math. Sem. Univ. Hamburg, 31 (1967), 199–205

[**Le,2**] A. LEUTBECHER, *Über die Heckeschen Gruppen $G(\lambda)$ II*, Math. Ann., 211 (1974), 63–86

[**Lh,1**] J. LEHNER, *Uniqueness of a Class of Fuchsian Groups*, Ill. J. Math., 19 (1974), 308–315

[**Lh,2**] J. LEHNER, *Discontinuous Groups and Automorphic Forms*, Math. Surveys, 8, A.M.S. Providence, R.I. (1964)

[**Lh–Ne,1**] J. LEHNER & M. NEWMAN, *Real two dimensional Representations of the Free Products of Two Finite Cyclic Groups*, (1966)

[**LV,1**] W.J. Le VEQUE, *Topics in Number Theory I*, Addison–Wesley Pub. Comp., third printing (1965)

[**LV,2**] W.J. Le VEQUE, *Topics in Number Theory II*, Addison–Wesley Pub. Comp., second printing (1961)

[**Ly–Sc,1**] R.C. LYNDON & P.E. SCHUPP, *Combinatorial Group Theory*, Springer–Verlag – Berlin–Heidelberg–New York (1977)

[**Ma,1**] A.M. MACBEATH, *Generators of the Linear Fractional Groups*, Proc. Symp. Pure Math., 12 (1969), A.M.S., 14–32

[Ma,2] A.M. MACBEATH, *Packings, Free Products and Residually Finite Groups*, Proc. Comb. Phil. Soc., 59 (1963), 555–558

[Mc,1] C. MACLACHLAN, *Maximal Normal Fuchsian Groups*, Illionis J. Math., 15 (1971), 104–113

[Mc,2] C. MACLACHLAN, *A Bound for the Number of Automorphisms of a Closed Riemann Surface*, J.L.M.S., 44 (1969), 265–272

[MQ,1] D.L. Mc QUILLAN, *Classification of Normal Subgroups of the Modular Group*, Amer. J. Math., 87 (1965), 285–296

[Ne,1] M. NEWMAN, *The Structure of Some Subgroups of the Modular Group*, Illionis J. Math., 6 (1962), 480–487

[Ne,2] M. NEWMAN, *A Complete Description of the Normal Subgroups of Genus One of the Modular Group*, Amer. J. Math., 86 (1964), 17–24

[Ne,3] M. NEWMAN, *A Note on Modular Groups*, Proc. A.M.S., 14 (1963), 124–125

[Ne,4] M. NEWMAN, *Free Subgroups and Normal Subgroups of the Modular Group*, Illionis J. Math., 8 (1964), 262–265

[Ne,5] M. NEWMAN, *Classification of Normal Subgroups of the Modular Group*, Trans. A.M.S., 126 (1967), 267–277

[Ne,6] M. NEWMAN, *Normal Congruence Subgroups of the Modular Group*, Amer. J. Math., 85 (1963), 419–427

[Pa,1] L.A. PARSON, *Generalized Kloosterman Sums and the Fourier Coefficients of Cusp Forms*, Trans. A.M.S., 217 (1976), 329–350

[Pa,2] L.A. PARSON, *Normal Congruence Subgroups of the Hecke Groups* $G(2^{(1/2)})$ *and* $G(3^{(1/2)})$, Pacific J. of Math., 70 (1977), 481–487

[Pa, 3] L.A. PARSON, *Non-congruence Subgroups for the Hecke Groups* $G(\sqrt{2})$ *and* $G(\sqrt{3})$, Illionis J. of Math., 19 (1975), 79–86

[Ra,1] R.A. RANKIN, *Lattice Subgroups of Free Congruence Groups*, Inventiones math., 2 (1967), 215–221

[Ra,2] R.A. RANKIN, *Modular Forms and Functions*, Cambridge Univ. Press (1977)

[Ro,1] D. ROSEN, *Continued Fractions in Algebraic Number Fields*, Research Problems (1977), 37–39

[Ro,2] D. ROSEN, *A Class of Continued Fractions Associated with Certain Properly Discontinuous Groups*, Duke Math. J., 21 (1954), 549–563

[Ro,3] D. ROSEN, *An Arithmetic Characterization of the Parabolic Points of* $G(2cos\pi/5)$, Proc. Glasgow Math. Assoc., 6 (1963), 88–96

[Ro,4] D. ROSEN, *The Diophantine Equation* $ax + by = c$ *in* $\mathbf{Q}(\sqrt{5})$ *and Other Number Fields*, Pacific J. of Math., 119 (1985), 465–472

[Ro,5] D. ROSEN, *The Substitutions of the Hecke Group* $\Gamma(2cos\frac{\pi}{5})$, Arch. der Math., 46 (1986), 533–538

[Sh,1] F.A. SHERK, *The Regular Maps on a Surface of Genus Three*, Canad. J. of Math., 11 (1959), 452–480

[Sh,2] F.A. SHERK, *A Family of Regular Maps of Type* $\{6, 6\}$, Canad. Math. Bull., 5 (1962), 13–20

[Si,1] D. SINGERMAN, *Finitely Maximal Fuchsian Groups*, J. of L.M.S. (2), 6 (1972), 29–38

[Si,2] D. SINGERMAN, *Subgroups of Fuchsian Groups and Finite Permutation Groups*, Bull. L.M.S., 2 (1970), 319–323

[Si,3] D. SINGERMAN, *Symmetries and Pseudo-symmetries of Hyperelliptic Surfaces*, Glasgow Math. J., 21 (1980), 39–49

[Si,4] D. SINGERMAN, $PSL(2, q)$ *as an Image of the Extended Modular Group with Applications to Group Actions on Surfaces*, Proc. Edinb. Math. Soc., 30 (1987), 143–151

[Th,1] W. THRELFALL, *Gruppenbilder*, Abh. Sächs. Akad. Wiss. Math.-Phys. Kl, 41 (1932), 1–59

[Ti,1] H. TIETZE, *Einige Bemerkungen über das Problem des Kartenfärbens auf einseitigen Flächen*, Jber. dtsch. Math.-Verein., 19 (1910), 155–159

[Wa–Ze,1] W. WATKINS & J. ZEITLIN, *The Minimal Polynomial of* $cos(2\pi/n)$, The Amer. Math. Monthly, 100 (1993), 471–474

[We,1] H. WEBER, *Traite d'algebre superieure, I*, Gauthier–Villars, Paris (1898)

[Wo,1] J. WOLFART, *Eine Bemerkung über Heckes Modulgruppen*, Arch. Math., 29 (1977), 72–77

LIST OF NOTATIONS

INDEX