Bulletin of the Institute of Mathematics
Academia Sinica (New Series)
Vol. **1** (2006), No. 4, pp. 549-556

A CLASS OF CONGRUENCE SUBGROUPS OF HECKE GROUP $H(\lambda_5)$

BY

MUSA DEMİRCİ AND İSMAİL NACİ CANGÜL

Abstract

In [2], it is shown that, for some Hecke groups, unlike the modular group, two definitions of the principal congruence subgroups may not coincide and congruence and principal congruence subgroups of two important Hecke groups $H(\sqrt{m})$, for $m = 2$ or 3, are classified and the quotients of $H(\sqrt{m})$ with these normal subgroups are given. Here we obtain a classification of the congruence subgroups obtained as the kernel of reduction homomorphism for another important Hecke group $H(\lambda_5)$ and also obtain the quotient groups. Finally the indices and abstract group structure of all these subgroups are determined.

1. Introduction

Hecke groups $H(\lambda_q)$ are discrete subgroups of isometries of the upper half plane $\mathbb{U}$ generated by two elements

$$R(z) = -\frac{1}{z} \text{ and } S(z) = -\frac{1}{z+\lambda_q}$$

of order 2 and q, respectively, where $\lambda_q = 2\cos\frac{\pi}{q}$, $q \in \mathbb{N}$, $q \geqslant 3$. For $q = 3$, we obtain the most popular discrete group named modular group. For $q = 4$

Received November 10, 2005.

AMS Subject Classification: 20H05, 11F06, 11F41, 11F46.

Key words and phrases: Congruence subgroups, Hecke groups, level, principal congruence subgroups.

This work was supported by the research fund of Uludag University project no: F-2004/40 and F-2003/63.

or 6, we obtain two Hecke groups $H(\sqrt{2})$ and $H(\sqrt{3})$. These two groups appear in the study of Dirichlet series, modular forms, Kloosterman sums etc., and their normal subgroups of small index are given in [2].

$H(\lambda_5)$ is the fourth important Hecke group. Its elements are classified in a different way than the above Hecke groups by means of the continued fractions. Its subgroups are also studied and classified in [2] and [6]. Because λ_5 is also known as the golden ratio, this group appear in the related fields where this number plays an important role.

In this work, we classify the congruence and principal congruence subgroups of $H(\lambda_5)$. The principal congruence subgroups of level p of $H(\lambda_5)$ are defined in [2], as

$$\begin{aligned}\Gamma_p(\lambda_5) &= \{T \in H(\lambda_5) : \; T \equiv \pm I \pmod p\} \\ &= \left\{ \begin{pmatrix} a & b\lambda_5 \\ c\lambda_5 & d \end{pmatrix} : a \equiv d \equiv \pm 1, \; b \equiv c \equiv 0 \pmod p), \; ad - 5bc = 1 \right\}\end{aligned}$$

for prime p. (There are many algebraic problems in defining these subgroups for any non-prime level $n \in \mathbb{N}$.) $\Gamma_p(\lambda_5)$ is always normal in $H(\lambda_5)$.

Congruence subgroups are possibly the most interesting ones amongst the infinitely many normal subgroups of $H(\lambda_5)$.

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 $\mathbb{Q}(\lambda)$ is linear in λ, i.e. has the form $a\lambda + b$, $a, b \in \mathbb{Q}$. Therefore all entries of the matrices of $H(\lambda_5)$ will have a form $a\lambda + b$, $a, b \in \mathbb{Z}$.

We know that $H(\lambda_5)$ is generated by the elements corresponding, in usual way, to the matrices

$$R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & -1 \\ 1 & \lambda_5 \end{pmatrix},$$

satisfying the relations

$$R^2 = S^5 = I.$$

Let us now reduce all elements of $H(\lambda_5) \bmod p$, for a prime p. In this way we obtain a homomorphism of $H(\lambda_5)$ to $H(\lambda_5)/K_{p,u}(\lambda_5)$, where $K_{p,u}(\lambda_5)$ denotes the kernel of this homomorphism $\bmod p$, and u is a root of the minimal polynomial of $\lambda_5 \bmod p$. Under this homomorphism R, S and T are mapped to r_p, s_p and t_p. Then $H(\lambda_5)/K_{p,u}(\lambda_5)$ is a homomorphic image of

$$\left\langle r_p, s_p : r_p^2 = s_p^5 = t_p^p = I,\ t_p = r_p s_p \right\rangle .$$

Let us 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 solution in $GF(2) = \mathbb{Z}_2 = \{0, 1\}$. Therefore we extend $\mathbb{Z}_2$ by adding a root u of the quadratic equation $x^2+x+1 = 0$. Then $\mathbb{Z}_2[u] = \{0, 1, u, 1+u\}$. It is easy to see that in $H(\lambda_5)/K_{2,u}(\lambda_5)$ 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, t_3 satisfy the relations

$$r_3^2 = s_3^5 = t_3^2 = I,$$

that is $H(\lambda_5)/K_{3,u}(\lambda_5)$ is isomorphic to A_5.

Case 3. $p = 5$. Now $\sqrt{5}$ can be thought of as equal to $0 \in GF(5)$. Therefore $\lambda_5 \equiv \frac{1}{2} \equiv 3 \pmod 5$. As $3 \in GF(5)$, there is a homomorphism of $H(\lambda_5)$ to $PSL(2, 5)$. Then we have the relations

$$r_5^2 = s_5^5 = t_5^5 = I$$

in $H(\lambda_5)/K_{5,3}(\lambda_5)$. Therefore $H(\lambda_5)/K_{5,3}(\lambda_5)$ is isomorphic to a finite quotient of the infinite triangle group $(2, 5, 5)$. Now

$$r_5 t_5^2 \equiv \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \pmod 5.$$

Let $u_5 = t_5^2$. Since $tr(r_5 u_5) = 1$, $r_5 u_5$ is of order 3. Then $H(\lambda_5)/K_{5,3}(\lambda_5)$ has a presentation

$$\left\langle r_5, u_5 : r_5^2 = u_5^5 = (r_5 u_5)^3 = I \right\rangle ,$$

that is $H(\lambda_5)/K_{5,3}(\lambda_5)$ is a $(2,3,5)$-group, i.e. it is isomorphic to the alternating group A_5.

2. General Case And Macbeath's Results

From now on we let $p \geqslant 7$ be a prime. Then we have two cases according to $p \equiv \pm 1 \pmod{10}$ or not. To obtain the quotients of $H(\lambda_5)$ with the congruence subgroups $K_{p,u}(\lambda_5)$, we first recall some results of Macbeath [4].

Let $k = GF(p^n)$- a field with p^n elements and k_1 be its unique quadratic extension. Let $G_0 = SL(2,k)$ and $G = PSL(2,k)$ so that $G \approxeq G_0/\{\pm I\}$. We shall also consider the subgroup G_1 of $SL(2,k_1)$ consisting of the matrices of the form $\begin{pmatrix} a & b \\ b^q & a^q \end{pmatrix}$ where $a, b \in k_1$ and $a^{q+1} - b^{q+1} = 1$. Macbeath 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 $\phi : G_0 \to G$ passes to the G-triples in the following way:

If H is a subgroup 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 $H(\sqrt{m})$ case, we have $A = r_p$, $B = s_p$ and $C = t_p$, where r_p, s_p and t_p denote the images of R, S and T, respectively, under the homomorphism φ_p^* reducing all elements of $H(\sqrt{m})$ modulo p. Hence the corresponding k-triple is $(0,u,2)$, where u is a root of the minimal polynomial $P(\sqrt{m})$ in $GF(p)$ or in a suitable extension field. Also the corresponding N-triple is $(2,q,n)$, where n is the level (i.e. the least positive integer so that T^n belongs to the subgroup) of normal subgroup.

Macbeath obtained three kinds of subgroups of G: affine, exceptional and projective groups. We now consider them in connection with $H(\sqrt{m})$.

Let $p > 2$. A k-triple (α,β,γ) is called *singular* if the quadratic form

$$\mathbb{Q}_{\alpha,\beta,\gamma}(\xi,\eta,\zeta) = \xi^2 + \eta^2 + \zeta^2 + \alpha\eta\zeta + \beta\xi\zeta + \gamma\xi\eta$$

is singular, i.e. if

$$\begin{vmatrix} 1 & \gamma/2 & \beta/2 \\ \gamma/2 & 1 & \alpha/2 \\ \beta/2 & \alpha/2 & 1 \end{vmatrix} = 0.$$

Now consider the set of matrices of the form $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$. They form a subgroup 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 $\begin{pmatrix} t & 0 \\ 0 & t^q \end{pmatrix}$, $t \in k_1$, $t^{q+1} = 1$ in G_1, where k_1 is a unique quadratic extension of k. This is conjugate to a subgroup $SL(2, k_1)$. 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 $k-$triple (α, β, γ) is singular. Any group associated with a singular G_0-triple is an *affine group.*

We now restrict ourselves to the case $k = GF(p)$, p prime.

For $H(\sqrt{m})$, the above determinant is equal to $-\frac{m}{4}$ and therefore vanishes only when $m \equiv 0 \pmod{p}$. Therefore, it only vanishes when $p = m$.

The triples $(2, 2, n)$, $n \in \mathbb{N}$, $(2, 3, 3)$, $(2, 3, 4)$, $(2, 3, 5)$ and $(2, 5, 5)$ as $(2, 3, 5)$ is a homomorphic image of $(2, 5, 5)$, which are the associated 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. Therefore for $H(\sqrt{m})$, the only exceptional triples are obtained for $p = 2$ and 3.

The final class of the subgroups of G is the class of the projective subgroups. It is known that there are two kinds of them: $PSL(2, k_s)$ and $PGL(2, k_s)$, where $k_s < k$, the latter containing the former with index two, except for $p = 2$ where two groups are equal. The groups $PSL(2, k_s)$ for all subfields of k, and whenever possible, the groups $PGL(2, k_s)$, together with their conjugates in $PGL(2, k)$ will be called *projective subgroups* of G.

Dickson, [4], proved that every subgroup of G is either affine, exceptional or projective. Therefore 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 is a projective group, and our problem will be to determine this subgroup. In doing this, we shall make use of the following results of Macbeath.

Theorem 2.1. *A G_0-triple which is neither singular nor exceptional generates a projective subgroup of G.*

Theorem 2.2. *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 k containing α, β and γ, and κ_0 is a subfield, if any, of which, κ is a quadratic extension.*

There are some k-triples which are neither exceptional nor singular. These are called *irregular* by Macbeath, i.e. a 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 2.3. *A G_0-triple which is neither singular, exceptional 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 now consider the last two cases in the light of Macbeath$'$s results:

Case 4. If 5 is a square mod p, i.e. $\left(\dfrac{5}{p}\right)=1$, i.e. if $p\equiv\pm1 \pmod{10}$, then $\sqrt{5}$ can be considered in $GF(p)$. In fact as the minimal polynomial of λ_5 is quadratic, there are two values u and v of $\lambda_5 \mod p$. Hence the elements r_p, s_p and t_p would belong to $PSL(2,p)$. Then we have two homomorphisms:

$$\theta_i : H(\lambda_5)\to PSL(2,p),\ i=1,2$$

induced by $\lambda_5\to u$ and $\lambda_5\to v$. Since (r_p,s_p,t_p) is neither exceptional nor singular, by Theorem 2.2., it generates $PSL(2,p)$. Therefore $H(\lambda_5)$ has two normal congruence subgroups $K_{p,u}(\lambda_5)$ and $K_{p,v}(\lambda_5)$ for $p\equiv\pm1 \pmod{10}$.

Example 2.1. Let $p=11$. Then there are two candidates for λ_5, 4 and 8 as $\lambda_5=\frac{1+\sqrt{5}}{2}\equiv\frac{1+\sqrt{49}}{2}=4$ and $\lambda_5=\frac{1+\sqrt{5}}{2}\equiv\frac{1+\sqrt{225}}{2}=8$ in mod 11. 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 $p \equiv \pm 3 \pmod{10}$ and $p \neq 3$. That is, p is such that 5 is not a square mod p. In this case $\sqrt{5}$ can not be considered as an element of $GF(p)$. Hence we extend it to $GF(p^2)$ as the degree of the minimal polynomial is 2. Then $\sqrt{5}$ can be considered in $GF(p^2)$ and then we have a homomorphism

$$\theta' : H(\lambda_5) \to PSL(2, p^2).$$

since $p \geqslant 7$, the G_0-triple (r_p, s_p, t_p) is neither exceptional nor singular. Hence by Theorem 2.1., it generates a projective subgroup of $PSL(2, p^2)$. By Theorem 2.2., 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 $GF(p^2)$. Therefore Theorem 2.3. implies that

$$H(\lambda_5)/K_{p,u}(\lambda_5) \approxeq PSL(2, p^2).$$

As a result of the five cases investigated above, we have the following:

Theorem 2.4. *The quotient groups of the Hecke group $H(\lambda_5)$ by its principal congruence subgroups $K_{p,u}(\lambda_5)$ are as follows:*

$$H(\lambda_5)/K_{p,u}(\lambda_5) \approxeq \begin{cases} PSL(2,p) & \text{if } \ p \equiv \pm 1 \pmod{10}, \\ PSL(2,p^2) & \text{if } \ p \equiv \pm 3 \pmod{10} \text{ and } p \neq 3, \\ D_5 & \text{if } \ p = 2, \\ A_5 & \text{if } \ p = 3, 5. \end{cases}$$

3. Abstract Group Structure of Congruence Subgroups $K_{p,u}(\lambda_5)$

Now we want to determine the group theoretical structure of these kernels. As we have the relations

$$r_p^2 = s_p^5 = I$$

in $H(\lambda_5)/K_{p,u}(\lambda_5)$, all these groups are free. Also $t_p^p = I$ implies that $K_{p,u}(\lambda_5)$ is of level p. Now by the permutation method [6] and Riemann-Hurwitz formula, we obtain the following result.

Theorem 3.1. *A congruence subgroup $K_{p,u}(\lambda_5)$ of $H(\lambda_5)$ is a free group with signature*

$$(1 + \frac{\mu}{20}(3p - 10);\ \infty^{(\mu/p)})$$

depending only on the index μ of $K_{p,u}(\lambda_5)$ in $H(\lambda_5)$.

Example 3.1. $K_{2,u}(\lambda_5) \approxeq (0;\ \infty^{(5)})$, $K_{3,u}(\lambda_5) \approxeq (0;\ \infty^{(20)})$, $K_{5,3}(\lambda_5) \approxeq (4;\ \infty^{(12)})$. The first of these three kernels corresponds to a dihedron. The second one corresponds to one of the five platonic solids called *icosahedron*, which can be thought as a regular map of the type $\{3, 5\}$. Finally the third one corresponds to a great dodecahedron, a regular map of the type $\{5, 5\}$.

References

1. İ. N. Cangül and O. Bizim, Congruence subgroups of some Hecke groups, *Bull. Inst. Math. Acad. Sinica*, **30**(2002), no. 2, 115-131.

2. İ. N. Cangül and D. Singerman, Normal subgroups of Hecke groups and regular maps, *Math. Proc. Cambridge Philos. Soc.*, **123**(1998), 59-74.

3. L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Leipzig ,1901, reprinted by Dover, 1960.

4. A. M. Macbeath, Generators of the linear fractional groups, *Proc. Sympos. Pure Math.*, **12** (1969), A.M.S. 14-32.

5. L. A. Parson, Normal congruence subgroups of the Hecke groups $G(2^{(1/2)})$ and $G(3^{(1/2)})$, *Pacific. J. Math.*, **70**(1977), 481-487.

6. D. Singerman, Subgroups of Fuchsian groups and finite permutation groups, *Bull. London Math. Soc.*, **2**(1970), 313-323.

Department of Mathematics, Faculty of Arts and Science, University of Uludag, Görükle 16059, Bursa, Turkey.

E-mail: mdemirci@uludag.edu.tr

E-mail: cangul@uludag.edu.tr