139250

KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MATEMATİK ANABİLİM DALI

H^5 HECKE GRUBUNUN KONGRÜANS ALT GRUPLARI VE $H_0^5((2)^\alpha I')$' NİN H^5' DEKİ NORMALLİYENİ

Süleyman UZUN

Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsünce
"Doktor"
Ünvanı Verilmesi İçin Kabul Edilen Tezdir.

138250

Tezin Enstitüye Verildiği Tarih : 14.01.2003
Tezin Savunma Tarihi : 25.03.2003

Tez Danışmanı : Prof. Dr. Mehmet AKBAŞ
Jüri Üyesi : Prof. Dr. Yusuf AVCI
Jüri Üyesi : Prof. Dr. Abdullah ÇAVUŞ

Enstitü Müdürü : Prof Dr. Yusuf AYVAZ

Trabzon 2003

T.C. YÜKSEKÖĞRETİM KURULU
DOKÜMANTASYON MERKEZİ

ÖNSÖZ

Bu çalışmada, H^5 Hecke grubunun kongrüans alt grupları ve $H_0^5((2)^\alpha I')$ nin H^5 deki normalliyeni incelendi.

Öncelikle, tez konusunun seçiminde, çalışmanın planlanmasında ve değerlendirilmesinde bana yardımlarını esirgemeyen sayın hocam, Prof. Dr. Mehmet AKBAŞ'a teşekkür eder, saygılarımı sunarım.

Ayrıca şu ana kadar bana emeği geçmiş, başta ailem ve hocalarım olmak üzere bütün arkadaşlarıma yürekten sevgiler sunuyor ve teşekkür ediyorum.

Süleyman UZUN

Ocak 2003, Trabzon

İÇİNDEKİLER

ÖZET

Bu çalışmada, [3] deki " $I=(2)^{\alpha} I'$, $\mathbb{Z}[\lambda_5]$'in bir ideali ve $(2, I')=1$ olsun. Bu takdirde $H_0^5(I)$ kongrüans alt grubunun H^5 Hecke grubundaki normalliyeni, $\alpha'=\alpha - \min\left(2, \left[\!\left[\frac{\alpha}{2}\right]\!\right]\right)$ olmak üzere, $H_0^5((2)^{\alpha'} I')$ dır." konjektür'ün, I' nın bir asal ideal olması durumunda ispatı yapıldı.

Birinci bölümde, çalışmalarımızla ilgili bir takım tanım ve teoremler verildi.

İkinci bölümde, $G=GL(2, \mathbb{Z}[\lambda_5])$ üzerinde bir $\sim$ eşdeğerlik bağıntısı tanımlandı. $\sim$ bağıntısı için $G/\sim$ denklik sınıfları kümesi belirlendi. Bunun yardımıyla da H^5 Hecke grubu ve $H_0^5(2)$ kongrüans alt grubu için $H^5/\sim$ ve $H_0^5(2)/\sim$ denklik sınıfları kümesi belirlendi.

Sonuç olarak I', $\mathbb{Z}[\lambda_5]$' in bir asal ideali ve $(2, I')=1$ (veya $I' \neq (2)$) için, $H_0^5((2)^{\alpha} I')$ kongrüans alt grubunun H^5 Hecke grubundaki normalliyeni, $\alpha'=\alpha - \min\left(2, \left[\!\left[\frac{\alpha}{2}\right]\!\right]\right)$ olmak üzere, $H_0^5((2)^{\alpha'} I')$ olarak elde edildi.

Anahtar Kelimeler : Hecke Grup, İdeal, Kongrüans Alt Grup, Denklik Bağıntısı, Denklik Sınıfları.

SUMMARY

The Congruence Subgroups of Hecke Group H^5 and The Normalizer of $H_0^5((2)^\alpha I')$ in H^5

Almost all of the thesis is devoted to a partly proof of a conjeture in [3] that when $I=(2)^\alpha I'$, where $(2, I')=1$, is an ideal of $\mathbb{Z}[\lambda_5]$ then the Normalizer of $H_0^5((2)^\alpha I')$ in H^5 is $H_0^5((2)^{\alpha'} I')$, where $\alpha'=\alpha-\min\left(2,\left[\!\left[\frac{\alpha}{2}\right]\!\right]\right)$.

Here, a proof is given by taking I' as a prime ideal.

In chapter 1, the preliminary definitions and results we require for the subsequent work are given.

In chapter 2, an equivalence relation $\sim$ on $G:=GL(2, \mathbb{Z}[\lambda_5])$ is defined. Then we get the set $G/\sim$ of equivalence classes. And using this set, the sets of equivalence classes $H^5/\sim$ and $H_0^5(2)/\sim$ for the Hecke group H^5 and the congruence subgroups $H_0^5(2)$ are determined.

Consequently, the normalizer of the congruence subgroups $H_0^5((2)^\alpha I')$ in the Hecke group H^5 is obtained as the $H_0^5((2)^{\alpha'} I')$, where $\alpha'=\alpha-\min\left(2,\left[\!\left[\frac{\alpha}{2}\right]\!\right]\right)$, and I' is a prime ideal in $\mathbb{Z}[\lambda_5]$ and $(2, I')=1$ (or $I'\neq(2)$).

Key Words : Hecke Group, Ideal, Congruence Subgroup, Equivalence Relation, Equivalence Classes.

SEMBOLLER DİZİNİ

$A \backslash B$	B nin A daki tümleyeni
$a \in A$	a, A nın bir elemanıdır
$a \notin A$	a, A nın elemanı değildir
$a \mid b$	a, b yi böler
$a \equiv b \bmod m$	m sayısı a-b sayısını böler
(a)	a elemanı ile üretilen esas ideal
$<a>$	a elemanı ile üretilen devirli (alt) grup
(a, b)	a ve b nin en büyük ortak böleni
$B \subset A$	B, A nın bir alt kümesidir
$H < G$	H, G nin bir alt grubudur
$H \lhd G$	H, G nin bir normal alt grubudur
$[G : H]$	H alt grubunun G deki indeksi
$\mathbb{C}$	Kompleks sayılar kümesi
$\mathbb{C}_\infty$	Genişletilmiş kompleks sayılar kümesi
$\mathbb{N}$	$= \{ 0, 1, 2, ..., n, ... \}$ " Doğal sayılar kümesi,,
$\mathbb{N}^*$	$= \{ 1, 2, ..., n, ... \}$ " Sayma sayıları- Pozitif tam sayılar kümesi,,
$N(I)$	I idealinin normu
$\mathbb{Q}$	Rasyönel sayılar kümesi
$\mathbb{Q}(u)$	u ve $\mathbb{Q}$ ile üretilen alt cisim
$\mathbb{R}$	Reel sayılar kümesi
$\mathfrak{R}$	Birim elemanlı bir halka
$\mathfrak{R}[x]$	$\mathfrak{R}$ üzerindeki polinomlar halkası
$\mathcal{U}$	$= \{ z \in \mathbb{C} : Im(z) > 0 \}$
$\mathbb{Z}$	$= \{..., -3, -2, -1, 0, 1, 2, 3, ... \}$ " Tam sayılar kümesi,,
$\mathbb{Z}_+$	$= \mathbb{N}^*$
$\mathbb{Z}_m$	m –moduna göre kalanların kümesi
$\mathbb{Z}[\lambda]$	$\mathbb{Z}$ nin $\mathbb{Q}(\lambda)$ cisimindeki tam kapanışı
$<X>$	X kümesi ile üretilen (alt) grup
(X)	kümesi ile üretile bir ideal

λ	$= 2\cos(\frac{\pi}{5}) = \frac{1+\sqrt{5}}{2}$
$:=$	Tanım gereğince eşittir
$\Rightarrow$	ise
$\Leftrightarrow$	ancak ve ancak (gerek ve yeter şart)
$\forall$	her
$\exists$	en az bir tane var
$\varnothing$	Boş küme

1. GENEL BİLGİLER

1.1. Giriş

Bu kısımda yapılan çalışmalara temel oluşturacak tanımlar ve teoremler verilmiştir.

Tanım 1: G bir grup ve H, G nin bir alt grubu olsun.

$$N_G(H):=\{g\in G \mid gH=Hg\} \qquad (1)$$

kümesine H nın G deki normalleyeni denir[4].

Tanım 2: $X\neq\emptyset$ bir küme ve G bir grup olsun. Bir $f : GxX\to X$ dönüşümü

i) $\forall x\in X$ ve $\forall g_1, g_2\in G$ için $f(g_1g_2,x)=f(g_1,f(g_2,x))$,

ii) $1\in G$ birim eleman ise $\forall x\in X$ için $f(1,x)= x$,

şartlarını sağlıyorsa G ye X üzerinde bir hareket grubu denir. Kolaylık olsun diye f(g,x) yerine kısaca gx yazılacaktır. Buna göre

i') $(g_1g_2)x = g_1(g_2x)$,

ii') $1x = x$

olur[4].

Önerme 1: G, X üzerinde bir hareket grubu olsun. Bu takdirde X üzerinde

$$x\approx y \Leftrightarrow \exists g\in G \text{ öyleki } gx = y \quad (x,y\in X)$$

ile tanımlanan $\approx$ bağıntısı bir eşdeğerlik bağıntısıdır[4].

Tanım 3: Önerme 1.de verilen $\approx$ bağıntısının eşdeğerlik sınıflarına hareketin yörüngeleri denir. Bu durumda bir $x\in X$ noktasının yörüngesi $Gx = \{gx : g\in G\}$ kümesidir[4].

Tanım 4: G, X üzerinde bir hareket grubu olsun. $x,y\in X$ keyfi olmak üzere $gx=y$ olacak biçimde bir $g\in G$ elemanı varsa G ye X üzerinde geçişli hareket grubu denir[4].

Tanım 5: G, X üzerinde bir hareket grubu olsun. $x\in X$ olmak üzere $G_x:=\{g\in G:gx=x\}$ kümesine x in G deki sabitleyeni denir[4].

Sonuç 1: G_x sabitleyeni G nin bir alt grubudur[4].

Sonuç 2: $x,y\in X$ ve $g\in G$ olmak üzere $y=gx$ olsun. Bu taktirde G_x ve G_y eşleniktir.

İspat : $G_{gx} = gG_xg^{-1}$ olduğu açıktır.

1.2. Topolojik Gruplar ve Fuchsian Grupları

Tanım 6:

i) G hem bir grup ve hem de bir topolojik uzay olsun.

$\alpha : G \to G,\ \alpha(x) = x^{-1}$

ve

$\beta : G \times G \to G,\ \beta(x,y) = xy$

dönüşümleri sürekli ise G ye bir topolojik grup denir.

ii) $H \leq G$ olmak üzere H üzerindeki alt uzay topolojisi ayrık ise H ya G nin ayrık bir alt grubu adı verilir[4].

Önerme 2: G bir topolojik grup ve $a \in G$ olsun. Bu takdirde

$f : G \to G,\ f(x) = xax^{-1}$

bir topolojik dönüşümdür. Yani f bir homoemorfizimdir[4].

Önerme 3:

$$M = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{C} \right\}$$

kümesi bir $\mathbb{C}$-vektör uzayıdır. Ayrıca $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M$ için **iz**(A) = a+d olarak tanımlandığında her $A, B \in M$ ve $\lambda \in \mathbb{C}$ için

i) **iz**(AB) = **iz**(BA)

ii) **iz**(λA) = λ **iz**(A)

iii) **iz**(A^t) = **iz**(A)

iv) **iz**(BAB^{-1}) = **iz**($AB^{-1}B$) = **iz**(A)

dir[1].

Önerme 4: $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, B = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in M$ olsun. $B^+ = (\overline{B})^t = \begin{bmatrix} \overline{\alpha} & \overline{\gamma} \\ \overline{\beta} & \overline{\delta} \end{bmatrix}$ olmak üzere

$$\langle A, B \rangle := \mathbf{iz}(AB^+) = a\overline{\alpha} + b\overline{\beta} + c\overline{\gamma} + d\overline{\delta}$$

olarak tanımlansın. Bu takdirde her $A, A_1, A_2, B \in M$ ve $\lambda_1, \lambda_2 \in \mathbb{C}$ için

i) $\langle A, A \rangle \geq 0$ ve $\langle A, A \rangle = 0 \Leftrightarrow A = 0$

ii) $\langle \lambda_1 A_1 + \lambda_2 A_2, B \rangle = \lambda_1 \langle A_1, B \rangle + \lambda_2 \langle A_2, B \rangle$

iii) $\langle \overline{A,B} \rangle = \langle B,A \rangle$

özellikleri sağlanır. Üstelik $(M,\langle .,. \rangle)$ bir iç çarpım uzayıdır ve

$$\|A\| := (\langle A,A \rangle)^{1/2}$$

olarak tanımlanırsa M bir normlu vektör uzayı olur. Ayrıca

iv) $\|AB\| \le \|A\|\|B\|$

v) $2|\det(A)| \le \|A\|^2$ dir [1].

$(M, \|\cdot\|)$ bir normlu vektör uzayı olduğundan ve herhangi iki $A, B \in M$ matrisleri arasındaki uzaklık,

$$d(A,B) = \|A-B\|$$

ile tanımlanırsa (M,d) bir metrik uzay olur. Bu uzayda

$$\begin{bmatrix} a_n & b_n \\ c_n & d_n \end{bmatrix} \mapsto \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

olması için gerek ve yeter şart $a_n \mapsto a$, $b_n \mapsto b$, $c_n \mapsto c$ ve $d_n \mapsto d$ olmasıdır[1]. Diğer yandan d-metriğinin M üzerinde indirgediği τ_d topolojisi ile (M, τ_d) bir topolojik uzaydır.

$$GL(2,\mathbb{C}) := \{ A \in M : \det(A) \neq 0 \} \qquad (2)$$

olsun. $GL(2,\mathbb{C})$ matris çarpımına göre bir gruptur. Alt uzay topolojisi ile $GL(2,\mathbb{C})$ bir topolojik uzay olur. $\alpha : GL(2,\mathbb{C}) \to GL(2,\mathbb{C})$, $\alpha(A) = A^{-1}$ fonksiyonu süreklidir. Ayrıca her $n \in \mathbb{N}$ için $A_n, B_n, A, B \in GL(2,\mathbb{C})$ için $A_n \mapsto A$ ve $B_n \mapsto B$ ise $A_nB_n \mapsto AB$ olur. Bu durumda $GL(2,\mathbb{C})$ bir topolojik gruptur.

$$SL(2,\mathbb{C}) := \{ A \in GL(2,\mathbb{C}) : \det(A) = 1 \} \qquad (3)$$

ile verilen küme $GL(2,\mathbb{C})$ nin bir alt grubudur. $G \le SL(2,\mathbb{C})$ olsun. G nin ayrık olabilmesi için gerek ve yeter şart her $k>0$ için $\{ A \in G : \|A\| \le k \}$ kümesinin sonlu olmasıdır[1]. Dolayısıyla $SL(2,\mathbb{C})$ nin her ayrık alt grubu sayılabilirdir. Örneğin

$$SL(2,\mathbb{Z}) := \{ A \in SL(2,\mathbb{C}) : A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ ve } a,b,c,d \in \mathbb{Z} \} \qquad (4)$$

ile tanımlanan alt grup, $SL(2,\mathbb{C})$ nin ayrık bir alt grubudur[1].

Şimdi de

$$PSL(2,\mathbb{C}) := \{ T : T: \mathbb{C}_\infty \to \mathbb{C}_\infty, T(z) = \frac{az+b}{cz+d}, ad-bc=1, a,b,c,d \in \mathbb{C} \} \qquad (5)$$

kümesini gözönüne alalım.(5) de verilen PSL(2,$\mathbb{C}$) kümesi dönüşümlerin bileşke işlemine göre bir gruptur.Diğer yandan $A=\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \overline{A}(z)=\frac{az+b}{cz+d}$ olmak üzere;

$$\theta : SL(2, \mathbb{C}) \rightarrow PSL(2, \mathbb{C}), \quad \theta(A) = \overline{A}(z) = \frac{az+b}{cz+d}$$

olarak tanımlayalım. Bu takdirde $\theta(A) = \theta(B) \Leftrightarrow A = \pm B$ dir. θ nın örten bir homomorfi olduğu açıktır. θ nın PSL(2, $\mathbb{C}$) üzerinde oluşturduğu bölüm topolojisini τ_θ ile gösterelim. τ_θ, PSL(2, $\mathbb{C}$) üzerinde θ yi sürekli yapan en ince topolojidir. Diğer yandan d(z, w), $\mathbb{C}_\infty$ de z ile w arasındaki kirişsel uzaklığı göstermek üzere f, g$\in$ PSL(2, $\mathbb{C}$) ise

$$\sigma(f, g) = \sup\{ d(f(z), g(z)) : z \in \mathbb{C}_\infty \}$$

olarak tanımlayalım. σ, PSL(2, $\mathbb{C}$) üzerinde bir metriktir[1]. σ-metriğinin oluşturduğu topolojiyi τ_σ ile gösterelim.

Teorem 1: PSL(2, $\mathbb{C}$), τ_σ topolojisi ile bir topolojik gruptur[1].

Teorem 2: $\theta : SL(2, \mathbb{C}) \rightarrow (PSL(2, \mathbb{C}), \tau_\sigma)$ açık ve sürekli bir dönüşümdür. Dolayısıyla τ_σ ve τ_θ topolojileri aynıdır[1].

Her X$\in$ SL(2, $\mathbb{C}$) için Önerme 4, v) şartından dolayı $\|X\| \geq \sqrt{2}$ dir. Dolayısıyla $\|X-(-X)\| = 2\|X\| \geq 2\sqrt{2}$ sağlanır. Bu durumda aşağıdaki sonucu verebiliriz.

Sonuç 3: θ fonksiyonunun yarıçapı $\sqrt{2}$ olan bir küreye kısıtlanışı bir topolojik dönüşümdür[1].

Sonuç 3 den G, PSL(2, $\mathbb{C}$) nın ayrık bir alt grubu ise $\theta^{-1}(G)$, SL(2, $\mathbb{C}$) nin ayrık bir alt grubudur. Tersine olarak Γ, SL(2, $\mathbb{C}$) nin ayrık bir alt grubu ise $\theta(\Gamma)$, PSL(2, $\mathbb{C}$) nin ayrık bir alt grubudur. Dolayısıyla PSL(2, $\mathbb{C}$) nin ayrık alt grupları sayılabilirdir.

Şimdi de

$$PSL(2, \mathbb{R}) := \{ T \in PSL(2, \mathbb{C}) : T(z) = \frac{az+b}{cz+d}; a,b,c,d \in \mathbb{R} \} \qquad (6)$$

kümesini gözönüne alalım. PSL(2, $\mathbb{R}$), PSL(2, $\mathbb{C}$) nin bir alt grubudur.

Tanım 7: PSL(2, $\mathbb{R}$) nin ayrık her alt grubuna bir Fuchsian grup denir. Buna göre Fuchsian grubun herhangi bir alt grubu da bir Fuchsian gruptur. Özel olarak

$$\Gamma := PSL(2, \mathbb{Z}) = \{ T \in PSL(2, \mathbb{R}) : T(z) = \frac{az+b}{cz+d}; a,b,c,d \in \mathbb{Z} \} \qquad (7)$$

alt grubu bir Fuchsian gruptur. Gerçekten Γ, PSL(2, $\mathbb{R}$) nin bir alt grubudur ve

$\theta(SL(2, \mathbb{Z})) = \Gamma$ olduğundan Γ ayrıktır. Dolayısıyla Γ bir Fuchsian gruptur ve $\Gamma := PSL(2, \mathbb{Z})$ Fuchsian grubu Modüler grup olarak adlandırılır[4].

Önerme 5: $PSL(2, \mathbb{R})$ nın elemanları $\mathcal{U} = \{ z \in \mathbb{C} : Im(z) > 0 \}$ üst yarı düzlemini kendi üzerine resmeder[4].

Tanım 8: $T \in PSL(2, \mathbb{R})$, $T \neq I$ ve $T(z) = \frac{az+b}{cz+d}$ olsun.

i) $|a+d| < 2$ ise T ye eliptik

ii) $|a+d| = 2$ ise T ye parabolik

iii) $|a+d| > 2$ ise T ye hiperbolik dönüşüm denir.

$T \in PSL(2, \mathbb{C})\backslash\{I\}$ ise T nin en fazla iki sabit noktası vardır. Yukarıdaki sınıflandırmaya ek olarak $PSL(2, \mathbb{R})\backslash\{I\}$ nın elemanları sabit nokta kümelerine göre de sınıflandırılır[4].

Teorem 3: $T \in PSL(2, \mathbb{R})\backslash\{I\}$ olsun. Bu taktirde,

i) T eliptik dönüşümdür $:\Leftrightarrow \exists\, z_0 \in \mathcal{U}$ ö.k. z_0 ve $\overline{z}_0$ T nin sabit noktalarıdır.

ii) T parabolik dönüşümdür $:\Leftrightarrow$ T, $\mathbb{R} \cup \{\infty\}$ da bir tek sabit noktaya sahiptir.

iii) T hiperbolik dönüşümdür $:\Leftrightarrow$ T, $\mathbb{R} \cup \{\infty\}$ da iki farklı sabit noktaya sahiptir[4].

Teorem 4: $S,T \in PSL(2, \mathbb{R})\backslash\{I\}$ olsun. ST=TS olması için gerek ve yeter şart S ve T nin sabit nokta kümelerinin aynı olmasıdır[4].

Teorem 5: Λ bir Fuchsian grup ve Λ nın birim elemanından farklı bütün elemanları aynı sabit nokta kümesine sahip ise Λ devirlidir[4].

Teorem 6: Her Abel Fuchsian grup devirlidir[4].

Teorem 7: Λ devirli olmayan bir Fuchsian grup olsun. Λ nın $PSL(2, \mathbb{R})$ deki normalleyeni bir Fuchsian gruptur[4].

1.3 Modüler Grubun Kongrüans Alt Grupları

Tanım 9: $N \in \mathbb{Z}_+$ olmak üzere Γ nın

$$\Gamma(N) = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma : a \equiv d \equiv 1 \bmod N \text{ ve } b \equiv c \equiv 0 \bmod N \}$$

alt grubuna bir esas kongrüans alt grup denir[4]. Bu alt grup

$$\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \bmod N\} \qquad (8)$$

olarakta verilebilir. $\Gamma(N)$ esas kongrüans alt grubunu içeren Γ nın herhangi bir G alt grubuna bir kongrüans alt grup denir ve $\Gamma(N) \leq G$ şartını gerçekleyen en küçük N sayısına G nin seviyesi denir[4].

İki özel kongrüans alt grup olarak,

$$\Gamma_1(N) := \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma : a \equiv d \equiv 1 \bmod N,\ c \equiv 0 \bmod N\} \qquad (9)$$

ve

$$\Gamma_0(N) := \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma : c \equiv 0 \bmod N\} \qquad (10)$$

verilir. (8), (9) ve (10) dan $\Gamma(N) \leq \Gamma_1(N) \leq \Gamma_0(N) \leq \Gamma$ olduğu açıktır. Diğer yandan $\Gamma(N) \trianglelefteq \Gamma$ olduğundan $\Gamma(N) \trianglelefteq \Gamma_0(N)$ ve $\Gamma(N) \trianglelefteq \Gamma_1(N)$ dir. Ayrıca $\Gamma_1(N) \trianglelefteq \Gamma_0(N)$ dir.

Önerme 6: $A=\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $B=\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} \in \Gamma$ matrisleri verilsin. Bu takdirde,

i) A ve B matrisleri $\Gamma_0(N)$ nin ayni yansınıfına sahiptir: $\Leftrightarrow ac' - ca' \equiv 0 \bmod N$,

ii) A ve B matrisleri $\Gamma_1(N)$ nin ayni yansınıfına sahiptir: $\Leftrightarrow a \equiv a' \bmod N$, $c \equiv c' \bmod N$ veya $a \equiv -a' \bmod N$, $c \equiv -c' \bmod N$,

iii) A ve B matrisleri $\Gamma(N)$ nin ayni yansınıfına sahiptir: $\Leftrightarrow a \equiv a' \bmod N$, $b \equiv b' \bmod N$, $c \equiv c' \bmod N$, $d \equiv d' \bmod N$ veya $a \equiv -a' \bmod N$, $b \equiv -b' \bmod N$, $c \equiv -c' \bmod N$, $d \equiv d' \bmod N$ dir[3].

Önerme 7: $N \in \mathbb{Z}^+$ ve $N > 2$ olsun. p ler N nin farklı asal bölenleri olmak üzere,

i) $[\Gamma : \Gamma_0(N)] = N \prod_{P|N} (1 + \frac{1}{P})$

ii) $[\Gamma : \Gamma_1(N)] = \frac{N^2}{2} \prod_{P|N} (1 - \frac{1}{P^2})$

iii) $[\Gamma : \Gamma(N)] = \frac{N^3}{2} \prod_{P|N} (1 - \frac{1}{P^2})$

dir[9]. $N = 2$ için

$[\Gamma : \Gamma_0(2)] = 3 \quad [\Gamma : \Gamma_1(2)] = 3 \quad [\Gamma : \Gamma(2)] = 6$

dır[3].

Önerme 8: $N_{PSL(2,\ \mathbb{R})}(\Gamma(N)) = \Gamma$ dır[3].

Önerme 9:

i) Γ da ∞ un sabitleyeni, $S_\infty := \{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} : n \in \mathbb{Z} \}$,

ii) $S_\infty \Gamma(N) = \Gamma_1(N)$ dir[3].

Önerme 10:

$$N_\Gamma(\Gamma_1(N)) = \begin{cases} \Gamma_0(N), & N \neq 4 \\ \Gamma_0(2), & N = 4 \end{cases}$$

dir[3].

Teorem 8: G sonlu üretilmiş bir grup olmak üzere H<G ve [G:H]<∞ olsun. Bu takdirde H alt grubuda sonlu üretilmiştir[7].

Sonuç 4: $\Gamma_0(N)$, $\Gamma_1(N)$ ve $\Gamma(N)$ alt grupları sonlu üretilmiş gruplardır.

Tanım 10: G bir grup, G_i <G, $i \in I$ ve $G = < G_i : i \in I >$ öyleki $i \neq j$ ise $G_i \cap G_j \neq \{I\}$, (I, G nin birim elemanı) olsun. G ye G_i lerin serbest çarpımıdır denir: $\Leftrightarrow$ Her $g \in G$ için $g = g_1 g_2 ... g_n$ olacak biçimde bir tek $g_1 g_2 ... g_n$ çarpımı vardır. Bu çarpımdaki ardışık iki eleman ayni G_i de olamaz.

Teorem 9: Γ modüler grubu sonlu üretilmiştir ve $T(z) = \frac{-1}{z}$, $U(z) = \frac{-1}{z+1}$ olmak üzere $\Gamma = < T, U >$ dır. Burada $T^2 = U^3 = I$ dır[9].

Sonuç 5: Γ modüler grubu mertebesi 2 olan bir grup ile mertebesi 3 olan bir grubun serbest çarpımına izomorftur. Yani $\Gamma = < T, U > \cong \mathbb{Z}_2 * \mathbb{Z}_3$ dır[3].

1. 4 $\mathbb{C}_\infty$ da Çemberler

$\mathbb{C}_\infty$ da bir çember ile $\mathbb{C}$ de bir çemberi veya D, $\mathbb{C}$ de bir doğru olmak üzere $D \cup \{\infty\}$ kümesini anlayacağız $PSL(2,\mathbb{C})$ nin elemanları ile $\mathbb{C}_\infty$ daki çemberler arasındaki ilişki aşağıdaki teorem ile verilir.

Teorem 10: Eğer C, $\mathbb{C}_\infty$ da bir çember ve $T \in PSL(2,\mathbb{C})$ ise T(C) de $\mathbb{C}_\infty$ da bir çemberdir[4].

Teorem 11: $T \in PSL(2,\mathbb{C})$ ise $T : \mathbb{C}_\infty \to \mathbb{C}_\infty$ bir konform topolojik dönüşümdür[4].

$PSL(2,\mathbb{R})$ nin elemanları üst yarı düzlemi yine üst yarı düzleme resmettiğinden $\mathbb{C}_\infty$ daki bir çemberin üst yarı düzlemde kalan parçası yine üst yarı düzleme resmedilir. Ayrıca, $PSL(2, \mathbb{R})$ nin elemanları konform dönüşümler olduğundan ve $\mathbb{R} \cup \{\infty\}$ çemberini sabit bıraktıklarından üst yarı düzlemde x-eksenine dik bir yarım çember parçası $PSL(2, \mathbb{R})$ nin elemanları altında yine üst yarı düzlemde x-eksenine dik bir yarım çember parçasına dönüşür[4].

1.5. $\Lambda < PSL(2, \mathbb{R})$ Fuchsian Grubunun En Genel Gösterimi

$\Lambda < PSL(2, \mathbb{R})$ ve Λ Fuchsian olsun. Teorem 1.2.6 dan dolayı Λ nın Abel olması için gerek ve yeter şartın Λ nın devirli olması gerektiğini biliyoruz. Bu durumda Λ nın birim elemandan farklı bütün elemanları ayni sabit nokta kümesine sahiptir. Dolayısıyla Λ nın birim elemandan farklı bütün elemanları ya eliptik, ya parabolik, ya da hiperbolik olmak zorundadır[4].

Tanım 11: Λ bir Fuchsian grup olsun. Λ nın birim elemandan ve parabolik elemanlardan oluşan devirli bir maksimal alt grubuna Λ nın bir parabolik alt grubu denir[4].

Tanım 12: Λ bir Fuchsian grup olsun. Λ nın parabolik alt gruplarının eşlenik sınıflarının sayısına Λ Fuchsian grubunun parabolik sınıf sayısı denir[4].

Bu kısımda $\Gamma = PSL(2, \mathbb{Z})$ modüler grup ve $\Lambda \leq \Gamma$ olarak alınacaktır.

Lemma 1: Γ, $\hat{\mathbb{Q}} = \mathbb{Q} \cup \{\infty\}$ üzerinde geçişli (transitif) olarak hareket eder[4].

Sonuç 6: Λ nın parabolik alt grupları Λ_r $(r \in \hat{\mathbb{Q}})$ sabitleyenleri ve Λ nın parabolik sınıf sayısı Λ nın $\hat{\mathbb{Q}}$ üzerindeki yörüngelerinin sayısına eşittir[4].

Sonuç 7: s, Λ nın parabolik sınıf sayısı ve $[\Gamma : \Lambda] = N$ olsun. Bu takdirde s sonludur ve $1 \leq s \leq N$ dir[4].

Λ, $PSL(2, \mathbb{R})$ nin sonlu tane elemanı tarafından üretilmiş ayrık bir alt grubu olsun. Bu grubun en genel gösterimi aşağıdaki gibi verilir

Üreticiler :

$a_1, b_1, ..., a_g, b_g$ (Hiperbolik)

$X_1, X_2, ..., X_r$ (Eliptik)

$P_1, P_2, \ldots, P_s$ (Parabolik)

Bağıntılar :

$$X_1^{m_1} = X_2^{m_2} = \ldots = X_r^{m_r} = \prod_{i=1}^{g}[a_i, b_i]\prod_{j=1}^{r}X_j\prod_{k=1}^{s}P_k = I .$$

Bu durumda Λ nın simgesi, $(g ; m_1, m_2, \ldots, m_r; s)$ olarak verilir.

Yukarıda verilen grup gösteriminden aşağıdakiler kolayca elde edilebilir.

Λ nın her eliptik elemanı ; X_j $(1 \le j \le r)$ elemanlarından birinin bir kuvvetine, her parabolik eleman ; P_k $(1 \le k \le s)$ elemanlarından birinin bir kuvvetine eşleniktir. Ayrıca, üreteçlerinin birinin aşikar olmayan bir kuvveti, diğer bir üretiçinin bir kuvvetine eşlenik olamaz[11].

1.6. İdeallerin Cebirsel özellikleri ve Cebirsel Tamlık

Aksi belirtilmediği sürece $\Re$ birim elemanlı bir halkadır.

Tanım 13: $\Re$ bir halka ve $\varnothing \neq A \subset \Re$ olsun. A ya $\Re$ halkasının bir idealidir denir : $\Leftrightarrow$ Her $a, b \in A$ ve $r \in \Re$ için

i) $a - b \in A$,

ii) $ra, ar \in A$ dır[2].

Tanım 14: A, $\Re$ nın bir ideali olsun. A ideali için bir $a_0 \in A$ elemanı

$$A := a_0\Re = \{ a_0 r : r \in \Re \}$$

olacak şekilde mevcut ise A idealine $\Re$ nın bir esas ideali denir ve $A := (a_0)$ ile gösterilir. Bütün idealleri esas ideal olan bir halkaya da esas ideal halkası (EİH) denir[2].

Tanım 15: A ve B, $\Re$ nın herhangi iki ideali olsun. Bu takdirde A ve B idealinin toplamı,

$$A + B := \{ a + b : a \in A , b \in B \}$$

ile verilir. Bu tanımdan aşağıdakiler açıktır.

i) $A + B = B + A$ (değişmeli)

ii) $A + (B + C) = (A + B) + C$ (birleşmeli)

iii) $A, B \subseteq A + B$

Notasyon olarak $A + B = (A, B)$ veya $A = (a_0)$, $B = (b_0)$ ise $A + B = (a_0 , b_0)$ olarak verilir. Bu durumda,

$$A = (a_1, a_2, \dots , a_n) = a_1 \mathfrak{R} + a_2 \mathfrak{R} + \dots + a_n \mathfrak{R} = \{ \sum_{i=1}^{n} a_i r_i : r_i \in \mathfrak{R} \}$$

olarak verilir[2].

Tanım 16: A ve B, $\mathfrak{R}$ nın herhangi iki ideali olsun. A ve B nin çarpımı,

$$AB := (ab : a \in A, b \in B) = \{ \sum_{i=1}^{m} a_i b_i : a_i \in A, b_i \in B, m \in \mathbb{N}^* \} \qquad (11)$$

dır. $\mathfrak{R}$ nın sonlu sayıda $A_1, A_2, \dots , A_n$ idealleri için çarpım;

$$A_1 A_2 \dots A_n := \{ \sum_{i=1}^{m} a_1^{(i)} a_2^{(i)} \dots a_n^{(i)} : a_j^{(i)} \in A_j \ \ 1 \le j \le n, \ 1 \le i \le m, \ m \in \mathbb{N}^* \} \qquad (12)$$

ile verilir. Buna göre, eğer $A = (a_1, a_2, \dots , a_s)$ ve $B = (b_1, b_2, \dots , b_t)$ ise

$$AB := (a_1b_1, a_1b_2, \dots , a_1b_t, \ a_2b_1, a_2b_2, \dots , a_2b_t, \dots , a_sb_1, a_sb_2, \dots , a_sb_t)$$

olur.

Eğer A ve B esas idealler ise bu takdirde $A = (a_0)$ ve $B = (b_0)$ olacak şekilde $a_0 \in A$ ve $b_0 \in B$ elemanları mevcuttur. Bu durumda A ve B nin çarpımı,

$$AB := (a_0)(b_0) = (a_0 b_0) \qquad (13)$$

olur. Yani esas ideallerin çarpımı yine bir esas ideal olur[2].

Tanım 17: A, C, $\mathfrak{R}$ nın iki ideali olsun.

$$A \mid C \ : \Leftrightarrow \ C = AB$$

olacak şekilde $\mathfrak{R}$ nın bir B ideali mevcuttur. Tanım 16 ve 17 den $C \subseteq A \cap B$ dır. Dolayısıyla bir ideal her böleni tarafından içerilir[2].

Tanım 18: P, $\mathfrak{R}$ nin bir ideali olsun. P ye bir asal ideal denir : $\Leftrightarrow P \mid AB$ şartını gerçekleyen $\mathfrak{R}$ nın her A, B idealleri için ya $P \mid A$ yada $P \mid B$ dir[2]

Tanım 19: A, B $\mathfrak{R}$ nın iki ideali osun. A ve B ye aralarında asal denir : $\Leftrightarrow$ $C \mid A$ ve $C \mid B$ olan her C ideali için $C = (1)$ dir. Burada 1, $\mathfrak{R}$ nın birim elemanıdır[2].

Teorem 12: Ave B aralarında asal iki ideal olsun. Bu takdirde,

$$A + B = (A, B) = (1) \ (= \mathfrak{R})$$

dir[2].

Sonuç 8: A ve B aralarında asal iki ideal ise $a + b = 1$ olacak şekilde $a \in A$ ve $b \in B$ elemanları mevcuttur[2].

Tanım 20: $\mathfrak{R}$ halkasına tamlık bölgesi denir : $\Leftrightarrow$ $\mathfrak{R}$ birim elemanlı, sıfır bölensiz, değişmeli bir halkadır[10].

$0 \notin S \subset \Re$ alt kümesine bir çarpımlı küme denir : $\Leftrightarrow$ Her a, b$\in$ S için ab$\in$ S dir[10].

Önerme 11: S, $\Re$ nın bir çarpımlı alt kümesi olsun. S nin her elemanının çarpmaya göre bir tersi'nin olduğu ve $\Re$ yi içeren (izomorfi hariç) bir $\Re_S$ halkası vardır[10].

Önerme 11 de verilen $\Re_S$ halkası, $\Re_S := \{ \frac{r}{s} : r \in \Re, s \in S \}$ dir. Burada $\Re$ bir tamlık bölgesi ve $S = \Re \setminus \{0\}$ alınırsa $\Re_S$ bir cisim olur. Diğer yandan $\Re_S$, $\Re$ yi içeren en dar cisimdir. Bu cisime $\Re$ nın kesir (bölüm) cisimi denir[10].

Aşağıdaki tanımda, $\Re'$ komutatif bir halka ve $\Re$ de $\Re'$ nin $1_{\Re} = 1_{\Re'}$ şartını sağlayan bir alt halkası alarak alınmıştır.

Tanım 21: b$\in$ $\Re'$ elemanına $\Re$-üzerinde tamdır denir: $\Leftrightarrow$ f(b)=0 olacak şekilde bir monik $f(x)=a_0+a_1x+...+a_{n-1}x^{n-1}+x^n \in \Re[x]$ polimomu mevcuttur. Bu durumda f(x)'e de tam bağımlı denklem denir[10].

Tanım 22: $\Re$ bir tamlık bölgesi ve K, $\Re$ nin kesir cismi olmak üzere ,

$$D := \{ x \in K : x, \Re\text{-üzerinde tamdır} \}$$

ile tanımlanan D kümesi K nın bir alt halkası ve $\Re \subset D$ dir. Bu D alt halkasına $\Re$ nın tam kapanışı denir. $\Re = D$ olması durumunda $\Re$ tamlık bölgesine tamamıyla kapalıdır denir[10]

Önerme 12: $\Re \subseteq \Re' \subseteq \Re''$ halkaları verilsin. $\Re'$, $\Re$-üzerinde ve $\Re''$ de $\Re'$ – üzerinde tam ise $\Re''$ de $\Re$ - üzerinde tamdır[10] .

Tanım 23: E,F iki cisim olsun. E ye F nin bir cisim genişlemesi denir :$\Leftrightarrow$F$\subset$E dir.

E, F nin bir cisim genişlemesi olmak üzere E F-uzay olarak gözönüne alındığından $|E : F|$ boyutuna , E nin F-üzerindeki genişleme dercesi denir.

f(x)$\in$ F[x] polinomu, F[x] halkasında $d^0g(x) \geq 1$ ve $d^0h(x) \geq 1$ olmak üzere

$$f(x) = g(x)h(x)$$

olacak biçimde yazılabiliyorsa f(x) polinomuna F[x] halkasında indirgenebilir denir. Aksi takdirde f(x) polinomuna indirgenemez denir[14].

Aşağıdaki önermede $\Re$, kesir cismi K olan bir bölge olarak alınacaktır.

Önerme 13: E,K nın bir cisim genişlemesi ve b$\in$E olmak üzere f(x)$\in$K[x], f(b)=0 olan indirgenemez bir polinom olsun.Eğer b, $\Re$-üzerinde tam ise f(x) in katsayıları $\Re$-üzerinde tamdır. Eğer $\Re$ tamamıyla kapalı ise bu takdirde b $\Re$-üzerinde tamdır : $\Leftrightarrow$ f(x) $\in$ $\Re$[x] dır[10].

Önerme 14: $d \in \mathbb{Z}_+$, her $p \in IP$ için $p^2 \neq d$ olan bir sayı olsun. Bu takdirde $\mathbb{Z}$ nın $\mathbb{Q}(\sqrt{d})$ deki tam kapanışı D ise,

$$D = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2} & , d \equiv 1 \bmod 4 \\ \mathbb{Z}\left[\sqrt{d}\right] = \mathbb{Z} + \mathbb{Z}\sqrt{d} & , d \equiv 2,3 \bmod 4 \end{cases}$$

dır[10].

Tanım 24: K, $\mathbb{Q}$ nun bir cebirsel genişlemesi, D, $\mathbb{Z}$ nin K daki tam kapanışı ve A da D nin bir ideali olsun. Bu takdirde D/A bölüm (faktör) halkasının eleman sayısına A idealinin normu denir ve N(A) ile gösterilir. Tanımdan $N(A) = |D/A|$ dir. Bu tanım sıfırdan farklı idealler için geçerlidir[10].

Önerme 15: A ve B, D nin iki ideali olsun. Bu takdirde

$N(AB) = N(A)N(B)$

dir[10].

Sonuç 9: A, D nin bir ideali ve A nın asal ayrışımı, P_i ler D nin asal idealleri ve $a_i \in \mathbb{Z}_+$ olmak üzere $A = P_1^{a_1}P_2^{a_2}...P_t^{a_t}$ ise

$N(A) = N(P_1)^{a_1}N(P_2)^{a_2}...N(P_t)^{a_t}$

dir[10].

Önerme 16: $\lambda_q = 2\cos\frac{\pi}{q}$, $q>2$ olmak üzere $\mathbb{Q}(\lambda_q)$ nın tamlarının halkası $\mathbb{Z}[\lambda_q]$ dir[12].

Φ- Euler fonksiyonu (yani, $\Phi : \mathbb{Z}_+ \to \mathbb{Z}$, $\Phi(n) = n\prod_{i=1}^{k}(1-\frac{1}{p_i})$, $n = \prod_{i=1}^{k} p_i^{a_i}$, $p_i \in IP$ ve $a_i \in \mathbb{Z}_+$) olmak üzere, eğer $d = \frac{\Phi(2q)}{2}$, λ_q nin minimal polinomunun derecesi ise bu takdirde $\mathbb{Q}(\lambda_q)$ nin bütün tamları, $n_{d-1}, n_{d-2}, \ldots, n_1, n_0$ rasyönel tamlar olmak üzere,

$$n_{d-1}\lambda_q^{d-1} + n_{d-2}\lambda_q^{d-2} + \ldots + n_1\lambda_q + n_0$$

biçimindeki sayılardır. Diğer bir ifade ile

$$\{ 1, \lambda_q, \ldots, \lambda_q^{d-1} \} \qquad (14)$$

kümesi $\mathbb{Q}(\lambda_q)$ nin tamlarının halkası için bir tam tabandır. Diğer yandan birimin 2q inci kökü $\xi_{2q} = e^{\frac{2\pi i}{2q}} = e^{\frac{\pi i}{q}}$ ve

$$\xi_{2q} + \xi_{2q}^{-1} = e^{\frac{\pi i}{q}} + e^{-\frac{\pi i}{q}} = (\cos\frac{\pi}{q} + i\sin\frac{\pi}{q}) + (\cos\frac{\pi}{q} - i\sin\frac{\pi}{q}) = 2\cos\frac{\pi}{q} = \lambda_q$$

olmak üzere $\mathbb{Q}(\xi_{2q})$ nin reel maksimal alt cisimi $\mathbb{Q}(\xi_{2q}+\xi_{2q}^{-1}) = \mathbb{Q}(\lambda_q) = \mathbb{Q}(\xi_{2q}) \cap \mathbb{R}$ dir[12].

Önerme 17: $q < 68$ için $\mathbb{Z}[\lambda_q]$ bir esas ideal halkasıdır[12].

$\mathbb{Z}[\lambda_q]$ halkasının ideallerini sınıflandırmak için, $\mathbb{Z}[\lambda_q]$ bir AEP (Asal Elemanlara Parçalanabilen) halkası olduğundan, asal ideallerini sınıflandırmak yeterli olacaktır. Eğer P, $\mathbb{Z}[\lambda_q]$ nin bir asal ideali ise $P \mid \langle n \rangle$ olacak şekilde bir n –rasyönel tam sayısı mevcuttur. Örneğin n = N(P) alınırsa $P \mid \langle N(P) \rangle$ dir. n'nin $\mathbb{Z}$ deki tektürlü ayrışımı ve keza ideallerin $\mathbb{Z}[\lambda_q]$ deki tektürlü ayrışımlarından, $P \mid \langle p \rangle$ olacak biçimde bir tek asal rasrasyönel tam p sayısı vardır ve $p \in P$ dir[12].

Önerme 18: $d = \frac{\Phi(2q)}{2} = [\mathbb{Q}(\lambda_q) : \mathbb{Q}]$ ve $\mathbb{Z}(\lambda_q)$ nın birimlerinin grubu U^q ise $U^q \cong \mathbb{Z}_2 x \mathbb{Z}^{d-1}$ dir[3].

$q = 4, 5, 6$ durumlarında $\mathbb{Q}$ nun $\mathbb{Q}(\lambda_q)$ genişlemesinin derecesi $d = \frac{\Phi(2q)}{2} = 2$ dir. Diğer yandan $\mathbb{Q}(\lambda_4) = \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\lambda_5) = \mathbb{Q}(\sqrt{5})$ ve $\mathbb{Q}(\lambda_6) = \mathbb{Q}(\sqrt{3})$ dir.

1.7. Hecke Grupları

$$T : z \to -\frac{1}{z} \text{ ve } U : z \to z + \lambda, \quad (\lambda \in \mathbb{R})$$

elemanları ile üretilen $PSL(2, \mathbb{R})$ nin alt gruplarının ayrık olması durumu özel bir önem taşır. Bu durumda karşımıza, "λ nın hangi değerleri için bu gruplar ayrık olur ?" sorusu çıkmaktadır. λ nın

$$\lambda = \lambda_q = 2\cos\frac{\pi}{q}, \quad q \geq 2$$

değerleri için yukarıda verilen grupların ayrık olduğu Hecke tarafından gösterildi(-1936).

Tanım 25: Yukarıda tanımlanan ve ayrık oldukları Hecke tarafından verilmiş .gruplara özel olarak Hecke grupları denir ve $\lambda = \lambda_q = 2\cos\frac{\pi}{q}$ değerine karşılık gelen Hecke grubunu H^q ile göstereceğiz. T ve U dönüşümlerinin $PSL(2, \mathbb{R})$ deki matris gösterimini kullanırsak,

$$H^q = <T, U> = <\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & \lambda_q \\ 0 & 1 \end{bmatrix}>$$

olur. q=3 olması durununda, $U = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ olur. Bu durumda H^3 - Hecke grubu, Γ-Modüler grubu olarak karşımıza çıkar.Herhangi bir H^q-Hecke grubu için,

$$S := TU = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & \lambda_q \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & \lambda_q \end{bmatrix}$$

tanımlansın. T ve S sırası ile 2 ve q mertebeli eliptik elemanlardır. U-paraboliktir. Bu durumda,

$$H^q = <T, U> = <T, S>$$

olur. H^q-Hecke grupları T ve S ile üretilen devirli grupların serbest çarpımıdır. Dolayısıyla

$$H^q = <T, S> \cong \mathbb{Z}_2 * \mathbb{Z}_q$$

olur. H^q nin temsilcileri hem

$$H^q = <T, S : T^2 = S^q = I> \qquad (15)$$

hem de

$$H^q = <T, S, U : T^2 = S^q = TSU = I>$$

dir. Böylece H^q- Hecke grubu $H^q \cong (2, q, \infty)$ üçgen grubuna izomorf olur. $\mathcal{U}/H^q$-bölümü delinmiş bir küre olduğundan H^q nun genus'ü 0 dir. Bu takdirde H^q nun simgesi $(0 ; 2, q, \infty)$ olur[3].

1.8. Kelimeler

Tanım 26: G bir grup ve $\varnothing \neq X \subset G$ olsun. G nin X-alt kümesine G nin üreteçlerinin serbest kümesi denir : $\Leftrightarrow$ $\forall g \in G$ elemanı, $k \in \mathbb{N}$, $x_i \in X$, $n_i \in \mathbb{Z}$, $1 \leq i \leq k$ olmak üzere

$$g := x_1^{n_1} \ldots x_k^{n_k} \quad , \quad x_i \neq x_{i+1} \, , \, 1 \leq i \leq k\text{-}1 \qquad (16)$$

çarpımı olarak tektürlü verilir[15].

Tanım 27: Elemanları arasında (16) den başka bağıntısı olmayan üreteçlerin kümesine serbest denir. Eğer bir G grubu üreteçlerin serbest kümesine sahip ise G grubuna serbest grup denir[15].

Tanım 28: $\varnothing \neq X$ kümesi verilsin. Aşağıdaki gibi, serbest kümesi X olacak biçimde bir grup inşa edilir:

$$x_1^{m_1} \ldots x_s^{m_s} \, , \quad x_i \in X \text{ ve } m_i \in \mathbb{Z} \, , \, 1 \leq i \leq s \qquad (17)$$

sonlu çarpımına bir kelime (word) denir. Eğer $x_i \neq x_{i+1}$ ve $m_i \in \mathbb{Z} \setminus \{0\}$, $1 \leq i \leq s$ ise bu durumda (17) kelimesine düzenli (reduced) denir. Her kelime, bitişik elemanların eşit olması durumunda kuvvetlerin toplanmasıyla bir düzenli kelime haline getirilebilir. Burada sıfırıncı kuvvetler yok kabul edilir. Eğer gerekirse bu yöntem birkaç kere uygulanabilir[15]. Örneğin, X = { x, y, z } serbest kümesinde

$$w = x^{-3}x^2y^5y^{-5}x^7z^2z^{-2}x^{-1}xzy^2x^{-1}$$

kelimesinin düzenlisi,

$$\overline{w} = x^{-1}y^0x^7z^0x^0zy^2x^{-1} = x^{-1}x^7zy^2x^{-1} = x^6zy^2x^{-1}$$

olur[15].

Teorem 14: Her kelime yalnız bir tane düzenli kelime verir[15].

x_1^0 kelimesinin düzenlisi boş kelime olarak alınır. Bir düzenli $w = x_1^{n_1} \ldots x_k^{n_k}$ kelimesinin tersi $w^{-1} = x_k^{-n_k} \ldots x_1^{-n_1}$ ile verilir ve w^{-1} de düzenlidir. Diğer yandan w_1 ve w_2 düzenli iki kelime ise w_1w_2 çarpımının düzenli olması gerekmez. Çünkü w_1'in son sembolü ile w_2 nin ilk sembolü ayni olabilir. Yani $w_1w_2 = \overline{w_1w_2}$ olması gerekmez. Eğer çarpım olarak $\overline{w_1w_2}$ alınırsa bütün düzenli kelimelerin kümesi bir grup oluşturur. Bu gruba X ile üretilen serbest grup denir[15].

Teorem 15: Γ - modüler grubu, 2- mertebeli $T = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ ve sonsuz mertebeli

$U = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ elemanlarından oluşan $X = \{ T, U \}$ serbest kümesi tarafından üretilen bir serbest gruptur ve her $A \in \Gamma$ için $\exists\, m \in \{ 0,1, 2 \}$; $q_0, q_1, \ldots, q_{n+1} \in \mathbb{Z}$ ve $q_0, q_1, \ldots, q_n \neq 0$ öyleki $A = T^m U^{q_0} T U^{q_1} \ldots T U^{q_n} T U^{q_{n+1}}$ dır[9].

Sonuç 10: H^5-grubu, 2- mertebeli $T = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ ve sonsuz mertebeli $U = \begin{bmatrix} 1 & \lambda_5 \\ 0 & 1 \end{bmatrix}$ elemanlarından oluşan $X = \{ T, U \}$ serbest kümesi tarafından üretilen bir gruptur ve her $A \in H^5$ için $\exists\, q_0, q_1, \ldots, q_{n+1} \in \mathbb{Z}$ ve $q_1, q_2, \ldots, q_n \neq 0$ öyleki

$$A = U^{q_0} T U^{q_1} \ldots T U^{q_n} T U^{q_{n+1}} \qquad (18)$$

dır[8].

2. YAPILAN ÇALIŞMALAR VE BULGULAR

2. 1. H^q nın Kongrüans Altgrupları

Modüler grubun esas kongrüans alt gruplarının tanımlarına benzer şekilde, $\mathbb{Z}[\lambda_q]$ nin herhangi bir I ideali için $G := PSL(2, \mathbb{Z}[\lambda_q])$ nin esas kongrüans alt gruplarını tanımlayabiliriz.

Tanım 29:

$$G(I) = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G : a-1, b, c, d-1 \in I\}$$

alt grubuna G nin I ya karşılık gelen esas kongrüans alt grubu adı verilir. Benzer şekilde I idealine karşılık gelen özel kongrüans alt grupları,

$$G_1(I) := \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G : a-1, c, d-1 \in G\}$$

ve

$$G_0(I) := \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G : c \in G\}$$

olarak tanımlanır[3].

Yukarıda verilen kongrüans alt grup tanımlarından

$G(I) \leq G_1(I) \leq G_0(I) \leq G$

olduğu açıktır. Diğer yandan $G(I) \trianglelefteq G$ ve $G_1(I) \trianglelefteq G_0(I)$ olduğu gösterilebilir. Dolayısıyla Modüler grup için Önerme 7 de verilen formüllere benzer şekilde,G grubu içinde verilebilir:

Teorem 16: P' ler I nın farklı asal bölenleri olmak üzere,

$$\text{i)}\ [G : G(I)] = N(I)^3 \prod_{P|I} (1 - \frac{1}{N(P)^2})$$

$$\text{ii)}\ [G : G_1(I)] = N(I)^2 \prod_{P|I} (1 - \frac{1}{N(P)^2})$$

iii) $[G : G_0(I)] = N(I)\prod_{P|I}(1+\frac{1}{N(P)})$

dir[3].

Tanım 30: H, G nin herhangi bir alt grubu ve I, $\mathbb{Z}[\lambda_q]$ nin bir ideali olsun. Bu durumda,

$H(I) := G(I)\cap H$

$H_1(I) := G_1(I)\cap H$

$H_0(I) := G_0(I)\cap H$

alt gruplarına, H nın özel kongrüans alt grupları denir[3]. Bu tanımda $H = H^q$ alınırsa, H^q nin özel kongrüans alt grupları

$H^q(I) := G(I)\cap H^q$

$H_1^q(I) := G_1(I)\cap H^q$

$H_0^q(I) := G_0(I)\cap H^q$

olur. Dolayısıyla $H^q(I) \le H_1^q(I) \le H_0^q(I) \le H^q$, $H^q(I) \trianglelefteq H^q$ ve $H_1^q(I) \trianglelefteq H_0^q(I)$ dir.

Teorem 16 da verilen formüller bir çok durumda H^q-Hecke grubu ve onun özel kongrüans alt grupları için de verilebilir.

Uyarı 1: $q = 4, 5, 6$ için $\mathbb{Z}[\lambda_q]$ bir esas ideal halkası olduğundan her I ideali için $I = <u> = u\mathbb{Z}[\lambda_q]$ olacak biçimde bir $u \in \mathbb{Z}[\lambda_q]$ elemanı vardır. Bu takdirde $H^q(I)$ yerine $H^q(u)$ alacağız.

Önerme 19: $0 \neq I$, $\mathbb{Z}[\lambda_q]$ nin bir ideali ve I idealinin asal ayrışımı $I = \prod_{i=1}^{k} P_i^{e_i}$, ($e_i \in \mathbb{Z}_+$, $1 \le i \le k$), olmak üzere $(6q, I) = 1$ ve $q = 3$ için $(5, I) = 1$ olsun. Eğer $I^* = I\cap\mathbb{Q}(\lambda_q^2)$ ve $N(I^*)$, I^* ın $\mathbb{Q}(\lambda_q^2)$ deki normu ise bu takdirde,

$$[H^q : H^q(I)] = 2^s N(I^*)^3 \prod_{P^*|I^*}(1-\frac{1}{N(P^*)^2}) \text{ , } (P^*, I^* \text{ ın asal böleni}) \qquad (19)$$

olur. Burada

$$s=\begin{cases} 0, & \exists 1\le i\ne j\le k \text{ öyleki } P_i^*=P_j^* \text{ veya } \exists 1\le i\le k \text{ öyleki } H^q/H^q(P_i)\cong PGL(2,\mathbb{Z}[\lambda_q^2]) \\ -1, & \text{diğer durumlarda} \end{cases}$$

dir[3].

Örneğin $q=5$ için $\mathbb{Q}(\lambda_5^2)=\mathbb{Q}(1+\lambda_5)=\mathbb{Q}(\lambda_5)$ ve $I^*=I$ dır. Dolayısıyla her $1\le i\le k$ için $P_i=P_i^*$ olur. Bu durumda I nın asal ayrışımında $P_i=P_j$ olacak biçimde hiçbir $1\le i\ne j\le k$ yoktur. O halde $(30, I)=1$ durumunda (1) de verilen formülde $s=-1$ olur. $(30, I)=1$ şartını sağlayan her I idealine karşılık gelen H^5 in özel kogrüans alt grupları arasıdaki indeksleride verilir[3].

$q=4, 6$ için $[H^q:H^q(I)]$ indeksi hesaplandı[16].

Lemma 2: $0\ne I$, $\mathbb{Z}[\lambda_5]$ nin bir ideali ve I idealinin asal ayrışımı $I=\prod_{i=1}^{k}P_i^{e_i}$,

$(e_i\in\mathbb{Z}_+, 1\le i\le k)$ olsun. Bu takdirde

$$[H^5:H_0^5(I)]=N(I)\prod_{i=1}^{k}(1+\frac{1}{N(P_i)})$$

dır[15].

2.2 H^q' nin Özel Kongrüans Alt Gruplarının Yansımfları

Bu kısımda, 1.3 de verilen sonuçların genelleştirilmesi yapılmıştır. $A, B\in H^q$ ve $A=\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $B=\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$ olsun.

Önerme 20: I, $\mathbb{Z}[\lambda_q]$ nin bir ideali olsun. Bu takdirde,

i.) A, B matrisleri $H_0^q(I)$ nın ayni yansımfındadır $:\Leftrightarrow ac'-ca'\equiv 0 \bmod$,

ii.) "," " " $H_1^q(I)$ nın " " $:\Leftrightarrow a\equiv a' \bmod I, c\equiv c' \bmod I$, $a\equiv -a' \bmod I, c\equiv -c' \bmod I$,

iii.) "," " " $H^q(I)$ nın " " $:\Leftrightarrow a\equiv a' \bmod I, b\equiv b' \bmod I$, $c\equiv c' \bmod I, d\equiv d' \bmod I$ veya $a\equiv -a' \bmod I, b\equiv -b' \bmod I, c\equiv -c' \bmod I, d\equiv -d' \bmod I$ dır[3].

Önerme 21: $\mathbb{Z}[\lambda_q]$ nin yalnız sonlu sayıda I ideali için $H^q(I)$ esas kongrüans alt grubu eliptik elemanlar içerir[3].

İspat : $H^q \cong (2, q, \infty)$ üçgen grubunun aşikar olmayan maksimal, sonlu, devirli alt gruplarının iki eşlenik sınıfı vardır[4]. Bu sınıfların birini 2-mertebeli gruplar oluşturur ve $T = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ ile üretilen grup, bu sınıfın bir temsilcisidir. Diğer sınıfı ise q-mertebeli gruplar oluşturur ve $S = \begin{bmatrix} 0 & -1 \\ 1 & \lambda_q \end{bmatrix}$ ile üretilen grup, bu sınıfın bir temsilcisidir. Yani, H^q nın maksimal, sonlu, devirli herhangi bir alt grubu T ve S nin bir eşleniği ile üretilir. Maksimal olmayan sonlu, devirli herhangi bir alt grup, maksimal olan bir grupta içerilir. Bu durumda maksimal olmayan bir alt grup, T veya S' nun bir eşleniğinin bir kuvveti ile veya buna denk olarak T veya S' nun bir kuvvetinin bir eşleniği ile üretilir. Diğer yandan $< a >$ n-mertebeli, sonlu, devirli bir grup olsun. $< a >$- grubunun aşikar olmayan farklı alt grupları, $d|n$ ve $d \neq n$ olmak üzere, a^d - elemanları ile üretilir[14].

Böylece H^q nın aşikar olmayan bütün sonlu, devirli alt grupları, $g \in H^q$ olmak üzere, gTg^{-1} veya gS^dg^{-1} (burada $d|q$ ve $d \neq q$) biçiminde elemanlar tarafından üretilir. Eğer bu sonlu, devirli alt gruplar H^q nin bir N-normal alt grubunda içeriliyorsa bu takdirde,

$$gTg^{-1} \in N \Leftrightarrow T \in gNg^{-1} \Leftrightarrow T \in N \qquad (20)$$

veya

$$gS^dg^{-1} \in N \Leftrightarrow S^d \in gNg^{-1} \Leftrightarrow S^d \in N$$

elde edilir. Buradan $q = 4, 5, 6$ olmak üzere, esas kongrüans alt grubu olarak $N := H^q(I)$ alınırsa (20) den $T = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \in H^q(I)$ olur. Böylece $1 \in I$ elde ederiz. Yani $I = \mathbb{Z}[\lambda_q]$ aşikar durumu olur. Diğer yandan $S^d = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in H^q(I)$ ise bu durumda $c \neq 0$ dır. Aksi takdirde S^d elemanı, $\begin{bmatrix} 1 & n\lambda_q \\ 0 & 1 \end{bmatrix}$ $(n \in \mathbb{Z})$ formuna sahip olur ve bu durumda da parabolik olur[5]. Dolayısıyla $c \in I$ dan

$$\text{Norm}(I) < \text{Norm}(c)$$

olur. Diğer yandan q nin d-bölenleri sonlu sayıda olduğundan Norm(c) nın mümkün değerleri de sonlu sayıdadır. Bu durumda Norm(c) üstten sınırlı olur. Dolayısıyla bu bize Norm(I) nın da üstten sınırlı olduğunu verir. Yani, I için yalnız sonlu sayıda mümkün değer vardır.

Önerme 22: q = 4, 5, 6 için H^q nın eliptik eleman içeren aşikar olmayan esas kongrüans alt grupları;

$$H^q(I)=\begin{cases} H^4(\sqrt{2}) & , \ q=4 \ \ (I=(\sqrt{2})) \\ \text{Mevcut değil} & , \ q=5 \\ H^6(1+\sqrt{3}) & , \ q=6 \ \ (I=(1+\sqrt{3})) \end{cases}$$

dir[3]

İspat : Önerme 21 nın ispatın da yapıldığı gipi, q = 4, 5, 6 olmak üzere,

$S^d \in H^q(I), \quad d|q \ \text{ve} \ d\neq q$

olacak biçimde $\mathbb{Z}[\lambda_q]$' nın I ideallerini belirleyeceğiz.

i) $q=4$ olsun. $d|q$ ve $d\neq 4$ ise $d=1$ veya $d=2$ olur. Bu durumda,

$$d=1 \Rightarrow S=\begin{bmatrix} 0 & -1 \\ 1 & \sqrt{2} \end{bmatrix} \in H^4(I) \Rightarrow 1\in I \Rightarrow I=\mathbb{Z}[\lambda_4] \Rightarrow H^4(I)=H^4(\mathbb{Z}[\lambda_4])=H^4$$

elde deriz. Yani, aşikar durum olur.

$$d=2 \Rightarrow S^2=\begin{bmatrix} 0 & -1 \\ 1 & \sqrt{2} \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & \sqrt{2} \end{bmatrix}=\begin{bmatrix} -1 & -\sqrt{2} \\ \sqrt{2} & 1 \end{bmatrix} \in H^4(I)$$

dır. $H^4(I)$' nın tanımından, -1-1 = -2, $\sqrt{2}$, $1-1=0\in I$ olacağından $I=<\sqrt{2}>$ veya $I=\mathbb{Z}[\lambda_4]$ olur. Yani, $q=4$ için $H^4(I)=H^4(\sqrt{2})$ dır. $I=\mathbb{Z}[\lambda_4]$ durumu aşikardır.

ii) $q=5$ olsun. $d|5$ ve $d\neq 5$ için, 5 asal olduğundan $d=1$ olur ki bu durumda

$S=\begin{bmatrix} 0 & -1 \\ 1 & \lambda_5 \end{bmatrix} \in H^5(I)$ olacağından $1\in I$ dır. Yani, $I=\mathbb{Z}[\lambda_5]$ olur. Buradan $H^5(I)=H^5$

aşikar durumunu elde ederiz. Dolayısıyla bu durumda, aşikar olmayan eliptik eleman içeren esas kongrüans alt grup yoktur.

iii) $q=6$ olsun. $d|6$ ve $d\neq 6$ için $d=1, 2, 3$ olur.

$d=1$, aşikar durum.

$d=2$ için,

$$S^2=\begin{bmatrix}0 & -1\\ 1 & \sqrt{3}\end{bmatrix}\begin{bmatrix}0 & -1\\ 1 & \sqrt{3}\end{bmatrix}=\begin{bmatrix}-1 & -\sqrt{3}\\ \sqrt{3} & 2\end{bmatrix}\in H^6(I)$$

olur. $H^6(I)$ nın tanımından, $-1-1=-2$, $\sqrt{3}$, $2-1=1\in I$ olmalıdır. $1\in I$ olduğundan $I=\mathbb{Z}[\lambda_6]$ aşikar durumu elde ederiz.

$d=3$ için,

$$S^3=\begin{bmatrix}-1 & -\sqrt{3}\\ \sqrt{3} & 2\end{bmatrix}\begin{bmatrix}0 & -1\\ 1 & \sqrt{3}\end{bmatrix}=\begin{bmatrix}-\sqrt{3} & -2\\ 2 & \sqrt{3}\end{bmatrix}\in H^6(I)$$

olur. $H^6(I)$ nın tanımından, $-\sqrt{3}-1$, 2, $\sqrt{3}-1\in I$ dır. $1+\sqrt{3}$, $-1+\sqrt{3}\in I$ ise $(1+\sqrt{3})(-1+\sqrt{3})=2\in I$ ve $-1+\sqrt{3}=-2+1+\sqrt{3}\in I$ olduğundan $I=<1+\sqrt{3}>$ alırsak ispat biter. Yani, $H^6(I)=H^6(1+\sqrt{3})$ olur.

Önerme 23:

i) $N_{PSL(2,\mathbb{R})}(H^q(I))=H^q$,

ii) ∞ un H^q deki sabitleyeni

$$S_\infty=\{\begin{bmatrix}1 & n\lambda_q\\ 0 & 1\end{bmatrix} : n\in\mathbb{Z}\}$$

dır[3].

Önerme 24: $S_\infty H^q(I)\le H_I^q(I)$ dır[3].

İspat : $S_\infty\le H_I^q(I)$ ve $H^q(I)\le H_I^q(I)$ olduğundan

$S_\infty H^q(I)\le H_I^q(I)$

olur.

Önerme 25: $q=4,6$ için $S_\infty H^q(I)=H_I^q(I)$ dır[3].

Lemma 3: I, $\mathbb{Z}[\lambda_5]$ nin bir asal ideali olsun. Bu takdirde

$N_{PSL(2,\mathbb{Z}[\lambda_5])}(H_0^5(I))=H_0^5(I)$

dır[6].

2. 3. $q=3,4,6$ için $H_0^q(I)$' nın H^q deki Normalliyeni

Teorem 17: $q=3$, $(N_0,6)=1$ olmak üzere $N=2^\alpha 3^\beta N_0\ge 1$ olsun. Bu takdirde,

$$N_\Gamma(\Gamma_0(N))=\Gamma_0(N/2^u3^v),\ u=\min\left(3,\left[\!\left[\frac{\alpha}{2}\right]\!\right]\right),\quad v=\min\left(1,\left[\!\left[\frac{\beta}{2}\right]\!\right]\right)$$

dır[3]. ($q=3$ için $\Gamma=H^3$ dır.)

Teorem 18: $q=4$, $(I', 3\sqrt{2})=1$ olmak üzere $I=(\sqrt{2})^\alpha(3)^\beta I'$, $\mathbb{Z}[\sqrt{2}]$ nin bir ideali olsun. Bu takdirde,

i) $N_{H^4}(H_0^4(I))=H_0^4(I)$, $\alpha=0$

ii) $N_{H^4}(H_0^4(I))=H_0^4((\sqrt{2})^{\alpha'}(3)^{\beta'}I')$, $\alpha\geq 1$;

$$\alpha'=\alpha-\min\left(6,\left[\!\left[\frac{\alpha+1}{2}\right]\!\right]\right),\ \beta'=\beta-\min\left(1,\left[\!\left[\frac{\beta}{2}\right]\!\right]\right)$$

dır[3].

Teorem 19: $q=6$, $(I', (1+\sqrt{3})\sqrt{3})=1$ olmak üzere $I=(1+\sqrt{3})^\alpha(\sqrt{3})^\beta I'$, $\mathbb{Z}[\sqrt{3}]$ in bir ideali olsun. Bu takdirde,

i) $N_{H^6}(H_0^6(I))=H_0^6((1+\sqrt{3})^{\alpha'}I')$, $\beta=0$, $\alpha'=\alpha-\min\left(2,\left[\!\left[\frac{\alpha}{2}\right]\!\right]\right)$

ii) $N_{H^6}(H_0^6(I))=H_0^6((1+\sqrt{3})^{\alpha'}(\sqrt{3})^{\beta'}I')$,

$$\beta\geq 1,\ \alpha'=\alpha-\min\left(6,\left[\!\left[\frac{\alpha}{2}\right]\!\right]\right),\ \beta'=\beta-\min\left(2,\left[\!\left[\frac{\beta+1}{2}\right]\!\right]\right)$$

dır[3].

2. 4. $q=5$ için $H_0^q(I)$'nın H^q deki Normalliyeni

Uyarı 2: Bundan sonra aksi belirtilmediği sürece $\lambda=\lambda_5$ alınacaktır. Bu durumda $\mathbb{Z}[\lambda]=\mathbb{Z}[\lambda_5]$ olur.

Tanım 31: $G=GL(2, \mathbb{Z}[\lambda])$ olmak üzere

$$A=\begin{bmatrix} a_1+b_1\lambda & a_2+b_2\lambda \\ a_3+b_3\lambda & a_4+b_4\lambda \end{bmatrix},\quad A^*=\begin{bmatrix} a_1^*+b_1^*\lambda & a_2^*+b_2^*\lambda \\ a_3^*+b_3^*\lambda & a_4^*+b_4^*\lambda \end{bmatrix}\in G$$

olsun. Bu takdirde

$$A\equiv A^* \bmod 2 \Leftrightarrow a_i+b_i\lambda\equiv a_i^*+b_i^*\lambda \bmod 2,\ 1\leq i\leq 4$$

olarak tanımlanır.

Önerme 24: $G = GL(2, \mathbb{Z}[\lambda])$ olsun. Bu takdirde G –üzerinde bir $\sim$ -eşdeğerlik bağıntısı, $G/\sim = \left\{ \overline{\begin{bmatrix} a & b \\ c & d \end{bmatrix}} : a,b,c,d \in \mathbb{Z}_2[\lambda] \right\}$ olacak şekilde mevcuttur.

İspat : Önce

$$\mathbb{Z}_2[\lambda] = \{ a_n\lambda^n + a_{n-1}\lambda^{n-1} + ... + a_1\lambda + a_0 : a_0, a_1, ..., a_n \in \mathbb{Z}_2, n \in \mathbb{N} \} \qquad (21)$$

halkasının elemanlarını belirleyelim. Bunun için $n \in \mathbb{N}$ olmak üzere,

$$\lambda^n \equiv \begin{cases} 1 \bmod 2 & , n \equiv 0 \bmod 3 \\ \lambda \bmod 2 & , n \equiv 1 \bmod 3 \\ 1+\lambda \bmod 2 & , n \equiv 2 \bmod 3 \end{cases} \qquad (22)$$

olduğunu göstermek yeterlidir. n- üzerinden tümevarım yöntemi uygulayalım:

$\underline{n = 0,1 \text{ için,}}$ (22) doğrudur.

$\underline{n = 2 \text{ için,}}$ $\lambda^n = \lambda^2 = 1+\lambda \equiv 1+ \lambda \bmod 2$ ve $n = 2 \equiv 2 \bmod 3$ olduğundan (22) doğrudur.

$\underline{n = 3 \text{ için,}}$ $\lambda^n = \lambda^3 = 1+2\lambda \equiv 1 \bmod 2$ ve $n = 3 \equiv 0 \bmod 3$ olduğundan (22) doğrudur.

$\underline{n = 4 \text{ için,}}$ $\lambda^n = \lambda^4 = \lambda\lambda^3 \equiv \lambda.1 \equiv \lambda \bmod 2$ ve $n = 4 \equiv 1 \bmod 3$ olduğundan (22) doğrudur.

$\underline{\text{İddia,}}$ $n \geq 4$ için doğru olsun; $n + 1$ için doğru olduğunu gösterelim:

$$\lambda^{n+1} = \lambda.\lambda^n \equiv \begin{cases} \lambda \bmod 2 & , n \equiv 0 \bmod 3 \Rightarrow n+1 \equiv 1 \bmod 3 \\ 1+\lambda \bmod 2 & , n \equiv 1 \bmod 3 \Rightarrow n+1 \equiv 2 \bmod 3 \\ 1 \bmod 2 & , n \equiv 2 \bmod 3 \Rightarrow n+1 \equiv 0 \bmod 3 \end{cases}$$

olduğundan (22) ifadesi her $n \in \mathbb{N}$ için doğru olur. (21) de verilen $\mathbb{Z}_2[\lambda]$ halkası (22) ile

$$\mathbb{Z}_2[\lambda] = \{ 0, 1, \lambda, 1+\lambda \} \qquad (23)$$

olur. Bu takdirde (23) yardımı ile

$$G^* := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{Z}_2[\lambda] \right\} \qquad (24)$$

kümesini tanımlayalım. Diğer yandan her $a+b\lambda \in \mathbb{Z}[\lambda]$ için,

$$a+b\lambda = \begin{cases} 0+2(a'+b'\lambda) & , a,b \in 2\mathbb{Z} \\ 1+2(a'+b'\lambda) & , a \notin 2\mathbb{Z} \text{ ve } b \in 2\mathbb{Z} \\ \lambda+2(a'+b'\lambda) & , a \in 2\mathbb{Z} \text{ ve } b \notin 2\mathbb{Z} \\ 1+\lambda+2(a'+b'), & a \notin 2\mathbb{Z} \text{ ve } b \notin 2\mathbb{Z} \end{cases} \qquad (25)$$

olduğundan

$$a+b\lambda \equiv a^*+b^*\lambda \bmod 2 \qquad (26)$$

olacak şekilde $a^*+b^*\lambda \in \mathbb{Z}_2[\lambda]$ mevcuttur. Dolayısıyla her $A \in G$ için Tanım 31, (24) ve (26) ifadelerinden

$$A \equiv A^* \bmod 2 \qquad (27)$$

olan $A^* \in G^*$ vardır.

Şimdi de G üzerinde $\sim$ eşdeğerlik bağıntısını tanımlayalım: $A, B \in G$ olsun. (27) den $A \equiv A^* \bmod 2$ ve $B \equiv B^* \bmod 2$ olacak şekilde $A^*, B^* \in G^*$ matrisleri mevcuttur. Bu takdirde $\sim$ bağıntısı,

$$A \sim B :\Leftrightarrow A^* = B^* \qquad (28)$$

ile tanımlansın. $\sim$ bağıntısı G üzerinde bir eşdeğerlik bağıntısıdır:

1) (27) ve (28) den her $A \in G$ için $A \sim A$ dir. (yansıma)

2) $A, B \in G$ için $A \sim B$ olsun. (27) ve (28) den,

$$A \sim B \Leftrightarrow A^* = B^* \Leftrightarrow B^* = A^* \Leftrightarrow B \sim A$$

olur. (simetri).

3) $A, B, C \in G$ için $A \sim B$ ve $B \sim C$ olsun. (27) ve (28) den,

$$\left.\begin{array}{l} A \sim B \Leftrightarrow A^* = B^* \\ B \sim C \Leftrightarrow B^* = C^* \end{array}\right\rangle \Rightarrow A^* = C^* \Leftrightarrow A \sim C$$

olur. (geçişme).

1), 2) ve 3) den $\sim$ bir eşdeğerlik bağıntısıdır.

Şimdi de herhangi bir $A \in G$ matrisinin $\sim$ bağıntısına göre $\overline{A}$ denklik sınıfını belirleyelim. $A \in G$ olduğundan (27) den $A \equiv A^* \bmod 2$ olacak şekilde bir $A^* \in G^*$ matrisi vardır. Diğer yandan,

$$B \in \overline{A} \Leftrightarrow B \sim A \Leftrightarrow B \sim A \sim A^* \Leftrightarrow B \sim A^* \Leftrightarrow B \in \overline{A^*}$$

olduğundan

$$\overline{A} = \overline{A^*} \qquad (29)$$

olur. Bu takdirde denklik sınıflarından oluşan $G/\sim$ -kümesi,

$$G/\sim = \{ \overline{A^*} : A^* \in G^* \}$$

olur.

Teorem 19: (28) de tanımlanan $\sim$ bağıntısına göre $H^5/\sim = \Im$ olacak şekilde bir $\Im \subset G/\sim$ alt kümesi vardır ve

$$\Im = \left\{ \overline{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}, \overline{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}, \overline{\begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}}, \overline{\begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix}}, \overline{\begin{bmatrix} \lambda & 1 \\ 1 & 0 \end{bmatrix}}, \overline{\begin{bmatrix} 0 & 1 \\ 1 & \lambda \end{bmatrix}}, \overline{\begin{bmatrix} 1 & \lambda \\ \lambda & \lambda \end{bmatrix}}, \overline{\begin{bmatrix} \lambda & \lambda \\ \lambda & 1 \end{bmatrix}}, \overline{\begin{bmatrix} \lambda & 1 \\ \lambda & \lambda \end{bmatrix}}, \overline{\begin{bmatrix} \lambda & \lambda \\ 1 & \lambda \end{bmatrix}} \right\}$$

dır.

İspat : $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, T = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, T' = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, U = \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}$ olsun. (26) dan

$-1 \equiv 1 \bmod 2$ ve $-\lambda \equiv \lambda \bmod 2$ olduğundan Tanım 32 ve Önerme 23 den

$$U^{-1} \equiv U \bmod 2, T \equiv T' \bmod 2 \Rightarrow U^{-1} \in \overline{U} \text{ ve } T \in \overline{T'} \qquad (30)$$

ve $q \in \mathbb{N}$ için,

$$U^q = \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}^q = \begin{bmatrix} 1 & q\lambda \\ 0 & 1 \end{bmatrix} \equiv \begin{cases} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \bmod 2, & q = 0 \bmod 2 \\ \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix} \bmod 2, & q = 1 \bmod 2 \end{cases}$$

$$\Rightarrow q = 0 \bmod 2 \text{ için } U^q \in \bar{I} \text{ ve } q = 0 \bmod 2 \text{ için } U^q \in \overline{U} \qquad (31)$$

dır. Diğer yandan,

$$U^{-q}=\left[\begin{bmatrix}1 & \lambda\\ 0 & 1\end{bmatrix}^{q}\right]^{-1}=\begin{bmatrix}1 & q\lambda\\ 0 & 1\end{bmatrix}^{-1}=\begin{bmatrix}1 & -q\lambda\\ 0 & 1\end{bmatrix}\equiv\begin{cases}\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\bmod 2\ ,\ q=0\bmod 2\\ \begin{bmatrix}1 & \lambda\\ 0 & 1\end{bmatrix}\bmod 2\ ,\ q=1\bmod 2\end{cases}$$

$$\Rightarrow q=0 \bmod 2 \text{ için} U^{-q}\in \bar{I} \quad \text{ve} \quad q=0 \bmod 2 \text{ için } U^{-q}\in \overline{U} \qquad (32)$$

olur.

$A\in H^5$ keyfi olsun. Sonuç 10 , (18) den $\exists n\in \mathbb{N}^*=\mathbb{N}\setminus\{0\}$ öyleki $q_1, q_2, ...,q_n\in \mathbb{Z}\setminus\{0\}$ ve $q_0, q_{n+1}\in \mathbb{Z}$ olmak üzere A-matrisi,

$$A = U^{q_0}TU^{q_1}TU^{q_2}T...TU^{q_n}TU^{q_{n+1}} \qquad (33)$$

düzenli kelimesi ile verilir.

Bunun ispatını, önce $q_0 = q_{n+1} = 0$ olması durumunda yapalım. Bu halde (33) de verilen düzenli kelime

$$A = TU^{q_1}TU^{q_2}T...TU^{q_n}T \qquad (34)$$

olur.

i) $q_1, q_2, ...,q_n \equiv 1 \bmod 2$ olsun. Bu durumda iddia, (34) de verilen her A matrisi için,

$$A = TU^{q_1}TU^{q_2}T...TU^{q_n}T \Rightarrow \begin{cases} A\in \overline{\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}}, n\equiv 0\bmod 5\\ A\in \overline{\begin{bmatrix}1 & 0\\ \lambda & 1\end{bmatrix}}, n\equiv 1\bmod 5\\ A\in \overline{\begin{bmatrix}\lambda & 1\\ \lambda & \lambda\end{bmatrix}}, n\equiv 2\bmod 5\\ A\in \overline{\begin{bmatrix}\lambda & \lambda\\ 1 & \lambda\end{bmatrix}}, n\equiv 3\bmod 5\\ A\in \overline{\begin{bmatrix}1 & \lambda\\ 0 & 1\end{bmatrix}}, n\equiv 4\bmod 5\end{cases} \qquad (35)$$

olur. İspatı tümevarım yöntemini kullanarak yapacağız.

<u>n = 1 için,</u> (30), (31), (32) ve (34) den,

$$A = TU^{q_1}T \equiv T'UT' \equiv \begin{bmatrix}1 & 0\\ \lambda & 1\end{bmatrix}\bmod 2 \Rightarrow A\in \overline{\begin{bmatrix}1 & 0\\ \lambda & 1\end{bmatrix}} \qquad (36)$$

olur ve $n\equiv 1 \bmod 5$ dir.

n = 2 için, (30), (31), (32), (34) ve (36) den,

$$A = TU^{q_1}TU^{q_2}T \equiv T'UT'UT' \equiv \begin{bmatrix} \lambda & 1 \\ \lambda & \lambda \end{bmatrix} \bmod 2 \Rightarrow A \in \overline{\begin{bmatrix} \lambda & 1 \\ \lambda & \lambda \end{bmatrix}} \qquad (37)$$

olur ve $n \equiv 2 \bmod 5$ dir.

n = 3 için, (30), (31), (32), (34) ve (37) den,

$$A = TU^{q_1}TU^{q_2}TU^{q_3}T \equiv T'UT'UT'UT' \equiv \begin{bmatrix} \lambda & \lambda \\ 1 & \lambda \end{bmatrix} \bmod 2 \Rightarrow A \in \overline{\begin{bmatrix} \lambda & \lambda \\ 1 & \lambda \end{bmatrix}} \qquad (38)$$

olur ve $n \equiv 3 \bmod 5$ dir.

n = 4 için, (30), (31), (32), (34) ve (38) den,

$$A = TU^{q_1}TU^{q_2}TU^{q_3}TU^{q_4}T \equiv T'UT'UT'UT'UT' \equiv \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix} \bmod 2$$

$$\Rightarrow A \in \overline{\begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}} \qquad (39)$$

olur ve $n \equiv 4 \bmod 5$ dir.

n = 5 için, (30), (31), (32), (34) ve (39) dan,

$$A = TU^{q_1}TU^{q_2}TU^{q_3}TU^{q_4}TU^{q_5}T \equiv T'UT'UT'UT'UT'UT' \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \bmod 2$$

$$\Rightarrow A \in \overline{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}} \qquad (40)$$

olur ve $n \equiv 0 \bmod 5$ dir.

n = 6 için, (30), (31), (32), (34) ve (40) dan,

$$A = TU^{q_1}TU^{q_2}TU^{q_3}TU^{q_4}TU^{q_5}TU^{q_6}T \equiv T'UT'UT'UT'UT'UT'UT' \equiv \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix} \bmod 2$$

$$\Rightarrow A \in \overline{\begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}} \qquad (41)$$

olur ve $n \equiv 1 \bmod 5$ dir.

İddia, $n \geq 6$ için doğru olsun, $n + 1$ için doğru olduğunu gösterelim.

$n + 1$ için,

$$A = TU^{q_1}TU^{q_2}T...TU^{q_n}TU^{q_{n+1}}T$$

ile verilen düzenli kelimede,

$$A_n := TU^{q_1}TU^{q_2}T...TU^{q_n}T$$

alırsak, iddia n için doğru olduğundan,

$$A_n \equiv \begin{cases} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \bmod 2\ ,\ n \equiv 0 \bmod 5 \\ \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix} \bmod 2\ ,\ n \equiv 1 \bmod 5 \\ \begin{bmatrix} \lambda & 1 \\ \lambda & \lambda \end{bmatrix} \bmod 2\ ,\ n \equiv 2 \bmod 5 \\ \begin{bmatrix} \lambda & \lambda \\ 1 & \lambda \end{bmatrix} \bmod 2\ ,\ n \equiv 3 \bmod 5 \\ \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix} \bmod 2\ ,\ n \equiv 4 \bmod 5 \end{cases}$$

elde edilir. Bu durumda,

$$A = A_n U^{q_{n+1}} T \equiv \begin{cases} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix} \bmod 2,\ n \equiv 0 \bmod 5 \Rightarrow n+1 \equiv 1 \bmod 5 \\ \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix}\begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \equiv \begin{bmatrix} \lambda & 1 \\ \lambda & \lambda \end{bmatrix} \bmod 2,\ n \equiv 1 \bmod 5 \Rightarrow n+1 \equiv 2 \bmod 5 \\ \begin{bmatrix} \lambda & 1 \\ \lambda & \lambda \end{bmatrix}\begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \equiv \begin{bmatrix} \lambda & \lambda \\ 1 & \lambda \end{bmatrix} \bmod 2,\ n \equiv 2 \bmod 5 \Rightarrow n+1 \equiv 3 \bmod 5 \\ \begin{bmatrix} \lambda & \lambda \\ 1 & \lambda \end{bmatrix}\begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \equiv \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix} \bmod 2,\ n \equiv 3 \bmod 5 \Rightarrow n+1 \equiv 4 \bmod 5 \\ \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \bmod 2,\ n \equiv 4 \bmod 5 \Rightarrow n+1 \equiv 0 \bmod 5 \end{cases}$$

olur. Buradan,

$$\begin{cases} A \in \overline{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}, & n+1 \equiv 0 \bmod 5 \\ A \in \overline{\begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix}}, & n+1 \equiv 1 \bmod 5 \\ A \in \overline{\begin{bmatrix} \lambda & 1 \\ \lambda & \lambda \end{bmatrix}}, & n+1 \equiv 2 \bmod 5 \\ A \in \overline{\begin{bmatrix} \lambda & \lambda \\ 1 & \lambda \end{bmatrix}}, & n+1 \equiv 3 \bmod 5 \\ A \in \overline{\begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}}, & n+1 \equiv 4 \bmod 5 \end{cases} \qquad (42)$$

elde edilir. Dolayısıyla (36), (37), (38), (39), (40), (41) ve (42) den, (34) ifadesi her $n \in \mathbb{N}^*$ için doğru olur.

Bu takdirde $\mathfrak{I}_1$ kümesi

$$\mathfrak{I}_1 = \left\{ \overline{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}, \overline{\begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix}}, \overline{\begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}}, \overline{\begin{bmatrix} \lambda & 1 \\ \lambda & \lambda \end{bmatrix}}, \overline{\begin{bmatrix} \lambda & \lambda \\ 1 & \lambda \end{bmatrix}} \right\} \qquad (43)$$

olarak tanımlanırsa; i) ve (34) şartını sağlayan her $A \in H^5$ matrisi için, (35) den, $\overline{A} \in \mathfrak{I}_1$ elde ederiz.

Diğer yandan, (43) den,

$$\mathfrak{I}_1^* := \left\{ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix}, \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} \lambda & 1 \\ \lambda & \lambda \end{bmatrix}, \begin{bmatrix} \lambda & \lambda \\ 1 & \lambda \end{bmatrix} \right\} \qquad (44)$$

kümesini ve (44) den de $\mathfrak{I}_2^*$ kümesini,

$$\mathfrak{I}_2^* := \mathfrak{I}_1^* T' = T' \mathfrak{I}_1^* = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} \lambda & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & \lambda \end{bmatrix}, \begin{bmatrix} 1 & \lambda \\ \lambda & \lambda \end{bmatrix}, \begin{bmatrix} \lambda & \lambda \\ \lambda & 1 \end{bmatrix} \right\} \qquad (45)$$

olarak tanımlayalım. (44) ve (45) den

$$\mathfrak{I}_1^* = T' \mathfrak{I}_2^* = \mathfrak{I}_2^* T' \qquad (46)$$

olduğu açıktır.

Şimdi de keyfi $A^*, B^* \in \mathfrak{I}_1^*$ matrisleri için $A^* B^*$ çarpımlarının oluşturduğu kümenin belirlenmesi gerekir.

$A^* = T'$ veya $B^* = T'$ olması durumunda, (45) den,

$$A^*B^* \in \mathfrak{I}_2^* \qquad (47)$$

dır.

Şimdi de $A^* \neq T'$ ve $B^* \neq T'$ olmak üzere A^*B^* çarpımını belirleyelim. Burada $A^*\mathfrak{I}_1^*$ çarpımını, Tanım 31 den,

$$A^*\mathfrak{I}_1^* := \{ C^* : \exists B^* \in \mathfrak{I}_1^* ;\ A^*B^* \equiv C^* \bmod 2 \} \qquad (48)$$

tanımlayalım. Bu takdirde,

$A^* = \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix}$ için, (48) den,

$$A^*\mathfrak{I}_1^* = \left\{ \begin{bmatrix} 0 & 1 \\ 1 & \lambda \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & \lambda \\ \lambda & \lambda \end{bmatrix}, \begin{bmatrix} \lambda & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} \lambda & \lambda \\ \lambda & 1 \end{bmatrix} \right\} \qquad (49)$$

elde edilir.

$A^* = \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}$ için, (48) den,

$$A^*\mathfrak{I}_1^* = \left\{ \begin{bmatrix} \lambda & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} \lambda & \lambda \\ \lambda & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & \lambda \\ \lambda & \lambda \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & \lambda \end{bmatrix} \right\} \qquad (50)$$

olur.

$A^* = \begin{bmatrix} \lambda & 1 \\ \lambda & \lambda \end{bmatrix}$ için, (48) den,

$$A^*\mathfrak{I}_1^* = \left\{ \begin{bmatrix} 1 & \lambda \\ \lambda & \lambda \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & \lambda \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} \lambda & \lambda \\ \lambda & 1 \end{bmatrix}, \begin{bmatrix} \lambda & 1 \\ 1 & 0 \end{bmatrix} \right\} \qquad (51)$$

olur.

$A^* = \begin{bmatrix} \lambda & \lambda \\ 1 & \lambda \end{bmatrix}$ için, (48) den,

$$A^*\mathfrak{I}_1^* = \left\{ \begin{bmatrix} \lambda & \lambda \\ \lambda & 1 \end{bmatrix}, \begin{bmatrix} 1 & \lambda \\ \lambda & \lambda \end{bmatrix}, \begin{bmatrix} \lambda & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & \lambda \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\} \qquad (52)$$

dır. Sonuç olarak (47), (48), (49), (50), (51) ve (52) den,

$$A^*B^* \in \mathfrak{I}_2^* \qquad (53)$$

elde ederiz.

Eğer $A^* \in \mathfrak{I}_1^*$ alınıp, $A^*\mathfrak{I}_2^*$ çarpımı için, (48) kullanılıp, (49), (50), (51) ve (52) de yapılan işlemler tekrarlanırsa, ve (46) den,

$$A^* \mathfrak{I}_2^* = \mathfrak{I}_1^* \qquad (54)$$

elde ederiz.

Eğer $A^* \in \mathfrak{I}_2^*$ alınıp, $A^* \mathfrak{I}_2^*$ çarpımı için, (48) kullanılıp, (49), (50), (51) ve (52) de yapılan işlemler tekrarlanırsa,

$$A^* \mathfrak{I}_2^* = \mathfrak{I}_2^* \qquad (55)$$

elde ederiz.

Bu durumda $\mathfrak{I}^*$ kümesini,

$$\mathfrak{I}^* := \mathfrak{I}_1^* \cup \mathfrak{I}_2^* \qquad (56)$$

olarak tanımlarsak; her $A^* \in \mathfrak{I}^*$ için (48), (53), (54) ve (55) den

$$A^* \mathfrak{I}^* = \mathfrak{I}^* \qquad (57)$$

elde edilir. Dolayısıyla, herhangi $A, B \in H^5$ matrisleri için $A \equiv A^* \bmod 2$ ve $B \equiv B^* \bmod 2$ olacak biçimde $A^*, B^* \in \mathfrak{I}^*$ matrisleri var ise, (48) ve (57) dan, bir $C^* \in \mathfrak{I}^*$ matrisi de

$$AB \equiv A^* B^* \equiv C^* \bmod 2 \qquad (58)$$

olacak biçimde vardır. $\mathfrak{I}$ kümesini, (56) den,

$$\mathfrak{I} := \{ \overline{A^*} : A^* \in \mathfrak{I}^* \} \qquad (59)$$

olarak tanımlayalım.Bu takdirde (59) de verilen $\mathfrak{I}$ kümesi üzerinde bir " . „ çarpım işlemini; $\overline{A^*}, \overline{B^*} \in \mathfrak{I}$ olmak üzere,

$$\overline{A^*} . \overline{B^*} = \overline{A^* B^*} \qquad (60)$$

olarak tanımlarsak, (57) ve (60) dan $(\mathfrak{I}, .)$, birim elemanı $\bar{I} = \overline{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}$ olan, bir gruptur.

ii) $q_1, q_2, \ldots, q_n \equiv 0 \bmod 2$ olsun.İddia, her $n \in \mathbb{N}^*$ için

$$A = TU^{q_1} TU^{q_2} T \ldots TU^{q_n} T \equiv \begin{cases} T' \bmod 2 , & n \equiv 0 \bmod 2 \\ I \bmod 2 , & n \equiv 1 \bmod 2 \end{cases}$$

veya

$$A = TU^{q_1} TU^{q_2} T \ldots TU^{q_n} T \Rightarrow \begin{cases} A \in \overline{T'} , & n \equiv 0 \bmod 2 \\ A \in \bar{I} , & n \equiv 1 \bmod 2 \end{cases} \qquad (61)$$

olduğunu ispatlamak yeterlidir. İspatı n – üzerinden tümevarımla yapacağız:

$n=1$ için, (31), (32) ve (34) den,

$$A = TU^{q_1}T \equiv T'IT' \equiv T'T' \equiv I \bmod 2 \Rightarrow A \in \bar{I} \qquad (62)$$

olur ve $n \equiv 1 \bmod 2$ dir.

$n=2$ için, (31), (32), (34) ve (62) den,

$$A = TU^{q_1}TU^{q_2}T \equiv T'IT'IT' \equiv T'T'T' \equiv T' \bmod 2 \Rightarrow A \in \overline{T'} \qquad (63)$$

olur ve $n \equiv 1 \bmod 2$ dir.

İddia, $n \geq 2$ için doğru olsun, $n+1$ için doğru olduğunu gösterelim: $n+1$ için,

$$A = TU^{q_1}TU^{q_2}T...TU^{q_n}TU^{q_{n+1}}T$$

ile verilen düzenli kelimede, A_n – matrisi olarak,

$$A_n := TU^{q_1}TU^{q_2}T...TU^{q_n}T$$

alırsak, iddia n için doğru olduğundan,

$$A = TU^{q_1}TU^{q_2}T...TU^{q_n}T \equiv T'IT'IT'...T'IT' \equiv \begin{cases} T' \bmod 2, & n \equiv 0 \bmod 2 \\ I \bmod 2, & n \equiv 1 \bmod 2 \end{cases}$$

dır. Bu durumda,

$$A = A_n U^{q_{n+1}} T \equiv \begin{cases} T'IT' \equiv I \bmod 2, & n \equiv 0 \bmod 2 \Rightarrow n+1 \equiv 1 \bmod 2 \\ IIT' \equiv T' \bmod 2, & n \equiv 1 \bmod 2 \Rightarrow n+1 \equiv 0 \bmod 2 \end{cases}$$

$$\Rightarrow A \equiv \begin{cases} T' \bmod 2, & n+1 \equiv 0 \bmod 2 \\ I \bmod 2, & n+1 \equiv 1 \bmod 2 \end{cases}$$

$$\Rightarrow \begin{cases} A \in \overline{T'}, & n+1 \equiv 0 \bmod 2 \\ A \in \bar{I}, & n+1 \equiv 1 \bmod 2 \end{cases} \qquad (64)$$

elde ederiz. Yani her $n \in \mathbb{N}^*$ için (61) ifadesi doğru olur.

Bu durumda, i), ii) ve (34) şartlarını sağlayan her $A \in H^5$ için, (29), (59) ve (61) den,

$$\bar{A} = \overline{A^*} \in \mathfrak{I} \qquad (65)$$

dır. Diğer yandan, q_0 , $q_{n+1} \in \mathbb{Z}$ keyfi olmak üzere

$$B = U^{q_0} \text{ ve } C = U^{q_{n+1}} \qquad (66)$$

olsun. (29), (31) ve (32) den

$$\bar{B}, \bar{C} \in \mathfrak{I} \qquad (67)$$

olduğu açıktır. Bu takdirde i), ii) ve (34) şartlarını sağlayan herhangi bir $A \in H^5$ matrisi ve (66) da verilen B ve C matrisleri için $K := BAC$ çarpımını gözönüne alalım. (60) dan,

$$\overline{BAC} = \overline{BAC} = \overline{K} \qquad (68)$$

olur. $(\Im, .)$ grup olduğundan, (65), (67) ve (68) den

$$\overline{K} \in \Im \qquad (69)$$

elde ederiz.

iii) A-matrisinin (30) da verilen düzenli kelimesinde, $q_1, q_2, ..., q_n \in \mathbb{Z} \setminus \{0\}$ sayıları için $1 \le i \ne j \le n$ olmak üzere $q_i \equiv 0 \bmod 2$ ve $q_j \equiv 1 \bmod 2$ olacak şekilde $q_i, q_j \in \mathbb{Z} \setminus \{0\}$ olsun.Bu takdirde, $m \in \mathbb{N}^*$ olmak üzere $1 \le k_1 \le k_2 \le ... \le k_{m-1} \le k_m \le n$ parçalanışı için

$$\begin{aligned}
A_1 &= TU^{q_1}TU^{q_2}T...TU^{q_{k_1-1}} \\
A_2 &= TU^{q_{k_1}}TU^{q_{k_1+1}}T...TU^{q_{k_2-1}} \\
&\vdots \\
A_{m-1} &= TU^{q_{k_{m-2}}}TU^{q_{k_{m-2}+1}}T...TU^{q_{k_{m-1}-1}} \\
A_m &= TU^{q_{k_{m-1}}}TU^{q_{k_{m-1}+1}}T...TU^{q_{k_m-1}} \\
A_n &= TU^{q_{k_m}}TU^{q_{k_m+1}}T...TU^{q_n}T
\end{aligned} \qquad (70)$$

olmak üzere

$$A = A_1A_2.....A_{m-1}A_mA_n \qquad (71)$$

dır. Diğer yandan, q_i – değerleri için,

$$q_i \equiv \begin{cases} 0 \bmod 2\,, & 1 \le i \le k_1 - 1 \\ 1 \bmod 2\,, & k_1 \le i \le k_2 - 1 \\ 0 \bmod 2\,, & k_2 \le i \le k_3 - 1 \\ 1 \bmod 2\,, & k_3 \le i \le k_4 - 1 \\ \vdots & \\ .. \bmod 2\,, & k_{m-1} \le i \le k_m - 1 \\ .. \bmod 2\,, & k_m \le i \le n \end{cases} \qquad (72)$$

olsun. Bu takdirde (29), (31), (32), (34), (35), (60), (61), (69), (70) ve (72) den her $i \in \{ 1, 2, 3, ..., m, n \}$ için

$$\overline{A_i} \in \Im \qquad (73)$$

dır. (60) ve (71) den

$$\overline{A_1A_2}...\overline{A_mA_n} = \overline{A_1A_2...A_mA_n} = \overline{A} \qquad (74)$$

olur. $(\Im, .)$ grup olduğundan, (73) ve (74) den,

$$\overline{A} \in \Im \qquad (75)$$

elde ederiz.

Sonuç olarak, i), ii), (69) ve iii) den, her $A \in H^5$ için $\overline{A} \in \Im$ olur.

Sonuç 11: $\mathbb{Z}[\lambda]$ halkasının $I = (2) = 2\mathbb{Z}[\lambda]$ ideali verilsin. Bu takdirde

$$H_0^5(2)/\sim = \left\{\overline{\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}}, \overline{\begin{bmatrix}1 & \lambda\\ 0 & 1\end{bmatrix}}\right\}$$

dir.

İspat : $A = \begin{bmatrix}a & b\\ c & d\end{bmatrix} \in H_0^5(2)$ herhangi bir matris olsun. $H_0^5(2)$ nın tanımından

$c \equiv 0 \bmod 2$ dir.Teorem 19 dan A -matrisi için iki durum vardır: ya $A \in \overline{\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}}$ ya da $A \in \overline{\begin{bmatrix}1 & \lambda\\ 0 & 1\end{bmatrix}}$ dir.Dolayısıyla

$$H_0^5(2)/\sim = \left\{\overline{\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}}, \overline{\begin{bmatrix}1 & \lambda\\ 0 & 1\end{bmatrix}}\right\}$$

olur.

Sonuç 12: $I = (2) = 2\mathbb{Z}[\lambda]$ ideali için

i) $S_\infty H^5(2) = H_1^5(2)$

ii) $H_0^5(2) = H_1^5(2)$

dir.

İspat : i) Önerme 24 den $S_\infty H^5(2) \le H_1^5(2)$ dir. Bu takdirde $S_\infty H^5(2) \ge H_1^5(2)$ olduğunu gösterirsek ispat biter. Bunun için $a_2, c_2, d_2 \in I = <2>$ olmak üzere (Uyarı .1 den $H_1^5(2) = H_1^5(I)$ dir.)

$$\begin{bmatrix}1+a_2 & b\\ c_2 & 1+d_2\end{bmatrix} \in H_1^5(2) \qquad (76)$$

keyfi olsun.

$$\begin{bmatrix} 1 & n\lambda \\ 0 & 1 \end{bmatrix} A = \begin{bmatrix} 1+a_2 & b \\ c_2 & 1+d_2 \end{bmatrix} \qquad (77)$$

olacak şekilde bir $n \in \mathbb{Z}$ ve $A \in H^5(2)$ bulunabilirse ispat biter. (76) dan

$$A = \begin{bmatrix} 1 & n\lambda \\ 0 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 1+a_2 & b \\ c_2 & 1+d_2 \end{bmatrix} = \begin{bmatrix} 1+a_2-nc_2\lambda & b-n(1+d_2)\lambda \\ c_2 & 1+d_2 \end{bmatrix}$$

olur. $a_2 - nc_2\lambda \in I$ ve $d_2 \in I$ olduğundan $A \in H_1^5(2)$ olur. (76) ve Sonuç 10 dan

$b \equiv \lambda \bmod 2$ veya $b \equiv 0 \bmod 2$ dir.

a) $b \equiv \lambda \bmod 2$ olsun. Bu takdirde

$$b - n(1+d_2)\lambda \equiv \lambda - n\lambda \equiv (1-n)\lambda \bmod 2$$

olur. Buradan,

$$(1-n)\lambda \equiv \begin{cases} 0 \bmod 2 \ , & n \notin 2\mathbb{Z} \\ \lambda \bmod 2 \ , & n \in 2\mathbb{Z} \end{cases}$$

elde ederiz. Dolayısıyla $b \equiv \lambda \bmod 2$ olması durumunda n tek sayı olmalıdır. Bu durumda $A \in H^5(2)$ olur.

b) $b \equiv 0 \bmod 2$ olsun. Bu takdirde

$$b-n(1+d_2)\lambda \equiv -n\lambda \equiv \begin{cases} 0 \bmod 2 \ , & n \in 2\mathbb{Z} \\ \lambda \bmod 2 \ , & n \notin 2\mathbb{Z} \end{cases}$$

elde ederiz. Dolayısıyla n –çift sayı alınırsa $A \in H^5(2)$ olur. a) ve b) den

$$H_1^5(I) \leq S_\infty H^5(I)$$

elde ederiz.

ii) $H_0^5(2)$ ve $H_1^5(2)$ nin tanımından

$$H_1^5(2) \leq H_0^5(2) \qquad (78)$$

olduğu açıktır. Diğer yandan her $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in H_0^5(2)$ matrisi için Sonuç 10 dan

$a \equiv 1 \bmod 2$ ve $d \equiv 1 \bmod 2$ dir. Bu durumda, $a-1 \equiv 0 \bmod 2$ ve $d-1 \equiv 0 \bmod 2$ olur.

$H_1^5(2)$ nin tanımından $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in H_1^5(2)$ ve sonuç olarak

$$H_0^5(2) \leq H_1^5(2) \qquad (79)$$

elde ederiz. (78) ve (79) dan

$$H_0^5(2) = H_1^5(2)$$

olur.

Teorem 20: I', $\mathbb{Z}[\lambda]$ nın bir asal ideali olmak üzere $(2, I') = 1$ ve $I = (2)^{\alpha} I'$ olsun. Bu takdirde,

$$N_{H^5}(H_0^5(I)) = H_0^5((2)^{\alpha'} I') , \qquad \alpha' = \alpha - \min\{2, [\![\frac{\alpha}{2}]\!]\}$$

dir.

İspat :

$$X = \begin{bmatrix} x & z \\ y & t \end{bmatrix} \in N_{H^5}(H_0^5(I)) \tag{80}$$

keyfi bir matris olsun. Bu takdirde her

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in H_0^5(I) \tag{81}$$

için, Tanım 1 den,

$$A = \begin{bmatrix} x & z \\ y & t \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x & z \\ y & t \end{bmatrix}^{-1} \in H_0^5(I) \tag{82}$$

dir. (82) de matris çarpımı yapılırsa,

$$A = \begin{bmatrix} axt - bxy + czt - dzy & * \\ ayt - by^2 + ct^2 - dty & * \end{bmatrix} \in H_0^5(I) \tag{83}$$

olur. $H_0^5(I)$ nın tanımı, (81) ve (83) den

$$c \equiv 0 \bmod I$$

$$ayt - by^2 + ct^2 - dty \equiv 0 \bmod I$$

olduğundan

$$ayt - by^2 - dty \equiv 0 \bmod I \tag{84}$$

dır. Diğer yandan

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}$$

olarak alırsak (84) den

$$\lambda y^2 \equiv 0 \bmod I \tag{85}$$

olur ve $(-1 + \lambda)\lambda = 1$ olduğundan, (85) den,

$$y^2 \equiv 0 \bmod I \tag{86}$$

elde ederiz. (84) ve (86) dan

$$(a-d)ty \equiv 0 \bmod I \qquad (87)$$

olur. Bu takdirde her $x \in \mathbb{Z}[\lambda]$ için, (87) den,

$$(a-d)xty \equiv 0 \bmod I \qquad (88)$$

dır. Ayrıca, (80) den $\det(X) = xt - yz = 1$ olduğundan

$$xt = 1+yz \qquad (89)$$

dır. (88) de xt yerine (89) dan $1 + yt$ yazılırsa, (86) dan,

$$(a-d)y \equiv 0 \bmod I \qquad (90)$$

elde ederiz. Diğer yandan (81) den $ad - bc = 1$ ve $c \equiv 0 \bmod I$ olduğundan

$$ad \equiv 1 \bmod I \qquad (91)$$

olur. Eğer (90) denklemi a ile çarpılırsa, (91) den,

$$(a^2-1)y \equiv 0 \bmod I \qquad (92)$$

ve (90) denklemi d ile çarpılırsa, (91) den,

$$(d^2-1)y \equiv 0 \bmod I \qquad (93)$$

elde ederiz. Ayrıca, Tanım 14 den

$$I = (2)^{\alpha} I' \subseteq (2)^{\alpha} \cap I' \subset (2) \cap I' \qquad (94)$$

ve Önerme 17 den $\Re = \mathbb{Z}[\lambda]$ bir EİH olduğundan $\exists\ x_0 + y_0\lambda \in \mathbb{Z}[\lambda]$ öyleki

$$I' = (x_0 + y_0\lambda) \qquad (95)$$

dir. Tanım 14 den $(2)^{\alpha} = (2^{\alpha})$ olduğundan, (95) den

$$I = (2)^{\alpha} I' = (2^{\alpha}(x_0 + y_0\lambda)) = 2^{\alpha}(x_0 + y_0\lambda)\mathbb{Z}[\lambda] \qquad (96)$$

olur. (86), (94), (95) ve (96) dan

$$y^2 \equiv 0 \bmod 2^{\alpha} \qquad (97)$$

$$y^2 \equiv 0 \bmod (x_0 + y_0\lambda) \qquad (98)$$

olur. (97) den,

$$y^2 \equiv 0 \bmod 2 \qquad (99)$$

dır. (2) ve $I' = (x_0 + y_0\lambda)$ asal idealler olduğundan, (98) ve (99) dan,

$$y \equiv 0 \bmod (x_0 + y_0\lambda) \qquad (100)$$

$$y \equiv 0 \bmod 2 \qquad (101)$$

olur. (97) ve (101) den

$$y^2 \in 2^{\alpha}\mathbb{Z}[\lambda] \quad \text{ve} \quad y \in 2\mathbb{Z}[\lambda] \qquad (102)$$

dır. Diğer yandan, $n \in \mathbb{Z}_+$ keyfi olmak üzere $\mathbb{Z}[\lambda]$ halkasının $2^n\,\mathbb{Z}[\lambda]$ ve $2^{n+1}\mathbb{Z}[\lambda]$ ideallerini gözönüne alalım. $x_1 + y_1\lambda \in \mathbb{Z}[\lambda]$ keyfi olsun;

1) Eğer $(x_1 + y_1\lambda, 2) = 1$ ve $y := 2^n(x_1 + y_1\lambda)$ alınırsa, $y \in 2^n\,\mathbb{Z}[\lambda]$ ve $y \notin 2^{n+1}\,\mathbb{Z}[\lambda]$ dir.

2) Eğer $(x_1 + y_1\lambda, 2) \neq 1$ ise, 2, $\mathbb{Z}[\lambda]$ da asal olduğundan $(x_1 + y_1\lambda, 2) = 2$ dir. Bu takdirde $x_1 + y_1\lambda \in 2\mathbb{Z}[\lambda]$ olur. Yani $x_1 + y_1\lambda = 2(x_2 + y_2\lambda)$ olacak biçimde bir $x_2 + y_2\lambda \in \mathbb{Z}[\lambda]$ sayısı vardır. Bu durumda,

$$y := 2^n(x_1 + y_1\lambda) = 2^{n+1}(x_2 + y_2\lambda) \in 2^{n+1}\mathbb{Z}[\lambda]$$

elde ederiz.

Dolayısıyla, 1) ve 2) den

$$2^{n+1}\mathbb{Z}[\lambda] \underset{\neq}{\subset} 2^n\,\mathbb{Z}[\lambda] \tag{103}$$

olur. $n \in \mathbb{Z}_+$ keyfi olduğundan, (103) den,

$$\ldots 2^{n+1}\mathbb{Z}[\lambda] \underset{\neq}{\subset} 2^n\,\mathbb{Z}[\lambda] \underset{\neq}{\subset} \ldots \underset{\neq}{\subset} 2^2\mathbb{Z}[\lambda] \underset{\neq}{\subset} 2\mathbb{Z}[\lambda] \underset{\neq}{\subset} \mathbb{Z}[\lambda] \tag{104}$$

zincirini elde ederiz. (102) ve (104) den y için bir $\alpha' \in \mathbb{N}$ sayısı

$$y \in 2^{\alpha'}\,\mathbb{Z}[\lambda] \text{ ve } y \notin 2^{\alpha'+1}\,\mathbb{Z}[\lambda] \tag{105}$$

olacak şekilde mevcuttur. (105) den

$$y = 2^{\alpha'}(u + v\lambda) \tag{106}$$

olacak biçimde bir $u + v\lambda \in \mathbb{Z}[\lambda]$ vardır. (102) ve (106) dan

$$y^2 = 2^{2\alpha'}(u + v\lambda)^2 \in 2^{\alpha}\,\mathbb{Z}[\lambda] \tag{107}$$

olur. Burada $\alpha < \alpha'$ olması durumunda (100) den (86), (92) ve (93) şartları sağlanır.

Şimdi de $\alpha' \leq \alpha$ durumunu irdeleyelim. Bu durumda

$$0 \leq \alpha - \alpha' \tag{108}$$

olur. Ayrıca (107) den

$$\alpha \leq 2\alpha' \Rightarrow \frac{\alpha}{2} \leq \alpha' \leq \alpha \tag{109}$$

elde ederiz. Diğer yandan (81), (94) ve Sonuç 11 den,

$$\text{ya } \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \bmod 2 \text{ ya da } \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix} \bmod 2$$

dir. Burada her iki durum için de, Tanım 32. den,

$$a \equiv 1 \bmod 2 \tag{110}$$

olur. (110) dan,

$$a+1 \equiv 0 \bmod 2 \text{ ve } a-1 \equiv 0 \bmod 2 \tag{111}$$

dır. (111) den,

$$a^2-1=(a+1)(a-1) \equiv 0 \bmod 2^2 \tag{112}$$

elde ederiz. (112) den

$$a^2-1 \in 2^2\mathbb{Z}[\lambda] \tag{113}$$

olur. (105) ve (113) den

$$(a^2-1)y \in 2^{\alpha'+2}\,\mathbb{Z}[\lambda] \tag{114}$$

dır. (92), (108) ve (114) den

$$\alpha \le \alpha' +2 \Rightarrow 0 \le \alpha - \alpha' \le 2 \tag{115}$$

elde ederiz. Bu durumda, α-değerleri için (109) ve (115) şartlarını sağlayan en küçük $\alpha' \in \mathbb{N}$ sayılarını belirlemek yeterlidir.

$\underline{\alpha=0 \text{ için}}$, (109) ve (115) den $\alpha' = 0$ (116)

$\underline{\alpha=1 \text{ için}}$, (109) dan $\frac{1}{2} \le \alpha' \Rightarrow \alpha' \in \mathbb{Z}^+$

(115) den $0 \le 1 - \alpha' \le 2 \Rightarrow \alpha' = 1$ (117)

olur.

$\underline{\alpha=2 \text{ için}}$, (109) dan $\frac{\alpha}{2}=1 \le \alpha' \Rightarrow \alpha' \in \mathbb{Z}^+$ (118)

(115) den $0 \le 2 - \alpha' \le 2 \Rightarrow \alpha' = 1, 2$ (119)

dir. (118) ve (119) dan

$$\alpha' = 1 \tag{120}$$

olur.

$\underline{\alpha=3 \text{ için}}$, (109) dan $\frac{\alpha}{2}=\frac{3}{2} \le \alpha' \Rightarrow \alpha' \in \mathbb{Z}^+ \setminus \{1\}$ (121)

(115) den $0 \le 3 - \alpha' \le 2 \Rightarrow \alpha' = 1, 2, 3$ (122)

dır. (121) ve (122) den

$$\alpha' = 2 \tag{123}$$

olur. Bu takdirde, $\alpha \in \{0, 1, 2, 3\}$ için (116), (117), (120) ve (123) den

$$\alpha' = \begin{cases} 0 = 0 - [\![0]\!] \ , \ \alpha = 0 \\ 1 = 1 - \left[\!\left[\frac{1}{2}\right]\!\right] \ , \ \alpha = 1 \\ 1 = 2 - \left[\!\left[\frac{2}{2}\right]\!\right] \ , \ \alpha = 2 \\ 2 = 3 - \left[\!\left[\frac{3}{2}\right]\!\right] \ , \ \alpha = 3 \end{cases} \tag{124}$$

olur. (107), (114) ve (124) den

$$X = \begin{bmatrix} x & z \\ y & t \end{bmatrix} \in H_0^5((2)^{\alpha'} I')$$

dır ve X matrisi keyfi olduğundan

$$N_{H^5}(H_0^5((2)^{\alpha} I') \leq H_0^5((2)^{\alpha'} I') \tag{125}$$

elde ederiz.

$$\underline{\alpha \geq 4 \text{ için}}, \quad \alpha = \beta + 4 \tag{126}$$

olacak şekilde bir $\beta \in \mathbb{N}$ sayısı mevcuttur. Bu takdirde (109) dan,

$$\alpha' \geq \frac{\alpha}{2} = \frac{\beta+4}{2} = \frac{\beta}{2} + 2 \geq 2 \Rightarrow \alpha' \geq 2 \tag{127}$$

olur. (115) ve (126) dan

$$0 \leq \beta + 4 \leq \alpha' + 2 \Rightarrow \beta + 2 \leq \alpha' \tag{128}$$

elde ederiz. (128) den her $\beta \in \mathbb{N}$ için $\alpha' = \beta + 2$, $\beta + 3$, $\beta + 4$ olabilir. Ancak (127) ve (128) de verilen şartları gerçekleyen en küçük $\alpha' \in \mathbb{Z}^+$ sayısını alacağımızdan $\alpha' = \beta + 2$ olur.Bu durunda, (126) dan $\alpha \geq 4$ için

$$\alpha' = \beta + 2 = \beta + 4 - 2 = \alpha - 2 \Rightarrow \alpha' = \alpha - 2 \tag{129}$$

olur. (107), (114) ve (129) dan

$$X = \begin{bmatrix} x & z \\ y & t \end{bmatrix} \in H_0^5((2)^{\alpha-2} I')$$

olur ve X – matrisi keyfi olduğundan

$$N_{H^5}(H_0^5((2)^{\alpha} I') \leq H_0^5((2)^{\alpha-2} I') \tag{130}$$

elde ederiz. Dolayısıyla (124) ve (129) dan α değerlerine karşılık gelen α' için

$$\alpha' = \alpha - \min\{ 2, [\![\frac{\alpha}{2}]\!] \} \tag{131}$$

ve (131) de verilen α' değerleri için de (125) ve (130) dan,

$$N_{H^5}(H_0^5((2)^{\alpha} I')) \leq H_0^5((2)^{\alpha-2} I') \tag{132}$$

elde ederiz.

Şimdi de $\alpha' = \alpha - \min\{ 2, [\![\frac{\alpha}{2}]\!] \}$ için

$$H_0^5((2)^{\alpha'} I') \leq N_{H^5}(H_0^5(2)^{\alpha} I')$$

olduğunu gösterelim: Bunun için

$$X = \begin{bmatrix} x & z \\ y & t \end{bmatrix} \in H_0^5((2)^{\alpha'} I') \tag{133}$$

keyfi olsun. Bu durumda

$$y \equiv 0 \bmod ((2)^{\alpha'} I') \quad (\text{veya } y \in (2)^{\alpha'} I') \tag{134}$$

dır. (96) ve (134) den

$$y = 2^{\alpha'} (x_0 + y_0 \lambda)(u + v\lambda) \tag{135}$$

olacak şekilde bir $u + v\lambda \in \mathbb{Z}[\lambda]$ sayısı vardır. (135) de y' nın karesi alınırsa,

$$y^2 = 2^{2\alpha'} (x_0 + y_0 \lambda)^2 (u + v\lambda)^2 \tag{136}$$

olur. $\alpha \leq 2\alpha'$ olduğundan, (96) ve (136) dan,

$$y^2 = 2^{\alpha} (x_0 + y_0 \lambda)[2^{2\alpha'-\alpha} (x_0 + y_0 \lambda)(u + v\lambda)^2]$$

$$\Rightarrow y^2 \in 2^{\alpha} (x_0 + y_0 \lambda) \mathbb{Z}[\lambda]$$

$$\Rightarrow y^2 \equiv 0 \bmod ((2)^{\alpha} I') \tag{137}$$

elde ederiz.

Diğer yandan, (81) de verilen her $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ matrisi için (112) den

$$a^2 - 1 = 2^2 (x + y\lambda) \tag{138}$$

olacak şekilde bir $x + y\lambda \in \mathbb{Z}[\lambda]$ sayısı mevcuttur. (135) ve (138) de verilenler taraf tarafa çarpılırsa, $\mathbb{Z}[\lambda]$ değişmeli halka olduğundan,

$$(a^2 - 1)y = 2^{\alpha'+2} (x_0 + y_0\lambda)(u + v\lambda)(x + y\lambda) \tag{139}$$

olur. (115) ve (139) den

$$(a^2 - 1)y = 2^{\alpha} (x_0 + y_0\lambda)[2^{\alpha'+2-\alpha} (u + v\lambda)(x + y\lambda)]$$

$$\Rightarrow (a^2 - 1)y \equiv 0 \bmod ((2)^{\alpha} I') \tag{140}$$

elde ederiz. (137) ve (140) den

$$X = \begin{bmatrix} x & z \\ y & t \end{bmatrix} \in N_{H^5}(H_0^5((2)^{\alpha} I'))$$

olur. Burada $X = \begin{bmatrix} x & z \\ y & t \end{bmatrix}$ matrisi keyfi olduğundan

$$H_0^5((2)^{\alpha'} I') \leq N_{H^5}(H_0^5(2)^{\alpha} I') \tag{141}$$

elde ederiz. (132) ve (141) den

$$N_{H^5}(H_0^5(I)) = H_0^5((2)^{\alpha'} I') , \qquad \alpha' = \alpha - \min\{ 2, [\![\frac{\alpha}{2}]\!] \}$$

olur.

Sonuç 13: I, $\mathbb{Z}[\lambda]$ nın bir asal ideali ise

$$N_{H^5}(H_0^5(I)) = H_0^5((I)) \tag{142}$$

dır.

İspat: i) Eğer $(2, I) = 1$ ise Teorem 20 de $\alpha = 0$ ($(2)^0 = \mathbb{Z}[\lambda]$) alırsak (142) ifadesi gerçeklenir.

ii) Eğer $(2, I) \neq 1$ ise bu takdirde, $\mathbb{Z}[\lambda]$' nın birimlerinin kümesi $(\mathbb{Z}[\lambda])^*$ olmak üzere

$$(2, I) = d \tag{143}$$

olacak şekilde bir $d \in \mathbb{Z}[\lambda] \setminus (\mathbb{Z}[\lambda])^*$ sayısı vardır. (143) den $d \in 2\mathbb{Z}[\lambda]$ ve 2, $\mathbb{Z}[\lambda]$ de asal olduğundan $d = 2$ olur. Bu durumda (143) den

$$2(x + y\lambda) + (u + v\lambda) = 2 \tag{144}$$

olacak şekilde $x + y\lambda \in \mathbb{Z}[\lambda]$, $u + v\lambda \in I$ sayıları vardır. (144) den

$$u + v\lambda = 2(1 - (x + y\lambda)) \Rightarrow u + v\lambda \in (2)$$

$$\Rightarrow I = (u + v\lambda)I \subset (2) \tag{145}$$

olur. $\mathbb{Z}[\lambda]$, değişmeli bir AEP halkasi olduğundan I ideali maksimaldır. Dolayısıyla (145) den $I = (2)$ elde ederiz. (100) den (142) ifadesi gerçeklenir.

Uyarı 3: Sonuç 13, Lemma 3 için de bir sonuçtur.

3. İRDELEME

Teorem 19. da Tanım 31.yardımı ile $G = GL(2, \mathbb{Z}[\lambda])$ üzerinde (28) de tanımlanan $\sim$-bağıntısına göre $H^5/\sim$ denklik sınıfları kümesi belirlendi.

Sonuç 11. de $H^5/\sim$ kümesi yardımıyla da $H^5(2)/\sim$ kümesi belirlendi.

$H^5(2)/\sim$ kümesinin belirlenmiş olması Teorem 20. nin ispatını yapmakta büyük kolaylık sağlamiştır.

4. SONUÇLAR

Yapılan çalışmalarda ele alınan konular ve elde edilen sonuçlar aşağıdaki gibidir.

1. [3], sayfa 63 te verilen Önerme 3.3.2 hatalı bulunup, aşağıdaki gibi düzeltilip ispat yapıldı.

$q = 4, 5, 6$ için H^q' nın eliptik eleman içeren aşikar olmayan esas kongrüans alt grupları;

$$H^q(I)=\begin{cases} H^4(\sqrt{2}) & , q=4 \ \ (I=(\sqrt{2})) \\ \text{Mevcut değil} & , q=5 \\ H^6(1+\sqrt{3}) & , q=6 \ \ (I=(1+\sqrt{3})) \end{cases}$$

dir.

2. $G = GL(2, \mathbb{Z}[\lambda])$ olmak üzere, G – üzerinde bir $\sim$ - eşdeğerlik bağıntısı verilerek

$$G/\sim = \left\{ \overline{\begin{bmatrix} a & b \\ c & d \end{bmatrix}} : a,b,c,d \in \mathbb{Z}_2[\lambda] \right\}$$

olduğu gösterildi.

3.

$$\mathfrak{I}=\left\{ \overline{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}, \overline{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}, \overline{\begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}}, \overline{\begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix}}, \overline{\begin{bmatrix} \lambda & 1 \\ 1 & 0 \end{bmatrix}}, \overline{\begin{bmatrix} 0 & 1 \\ 1 & \lambda \end{bmatrix}}, \overline{\begin{bmatrix} 1 & \lambda \\ \lambda & \lambda \end{bmatrix}}, \overline{\begin{bmatrix} \lambda & \lambda \\ \lambda & 1 \end{bmatrix}}, \overline{\begin{bmatrix} \lambda & 1 \\ \lambda & \lambda \end{bmatrix}}, \overline{\begin{bmatrix} \lambda & \lambda \\ 1 & \lambda \end{bmatrix}} \right\}$$

olmak üzere $H^5/\sim = \mathfrak{I}$ olduğu gösterildi.

4. $\mathbb{Z}[\lambda]$ halkasının $I=(2)$ ideali için

$$H_0^5(2)/\sim = \left\{ \overline{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}, \overline{\begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}} \right\}$$

olduğu gösterildi.

5. $\mathbb{Z}[\lambda]$ halkasının $I=(2)$ ideali için $S_\infty H^5(2) = H_1^5(2)$ ve $H_0^5(2) = H_1^5(2)$ olduğu gösterildi.

6. [3], sayfa 125 te, Prof. Dr. David SİNGERMAN ve doktora öğrencisi, Dr. Ioannis Panagioti IVRİSSİMTZİS'in ortaya koyduğu konjektür:

Konjektür: $(2, I') = 1$ olmak üzere $\mathbb{Z}[\lambda]$ nın bir ideali $I = (2)^{\alpha} I'$ olsun. Bu takdirde

$$N_{H^5}(H_0^5(I)) = H_0^5((2)^{\alpha'} I'), \quad \alpha' = \alpha - \min(2, \left[\!\left[\frac{\alpha}{2}\right]\!\right])$$

dır.

Bu Konjektür'ün, I' nın asal ve $(2, I') = 1$ (veya $I' \neq (2)$) olması durununda ispatı yapıldı.

5. ÖNERİLER

1. (28) de verilen $\sim$- bağıntısı ve (60) da tanımlanan " . „ çarpım işlemine göre $GL(2, \mathbb{Z}[\lambda])/\sim$ kümesi tarafından içerilen en geniş grubun ve $(SL(2, \mathbb{Z}[\lambda])/\sim, .)$ grubunun mertebeleri araştırılabilir.

2. Teorem 20. de verilen $I = (2)^{\alpha} I'$ idealinde I' nin asal olmaması durumunda iddia doğru olabilir mi? Eğer iddia doğru değilse, olmadığını gösteren somut bir örnek varmıdır ?

3. $I = (2)^{\alpha} I'$ ve $(2, I') = 1$ olmak üzere $H_0^5(I)$ nın $PSL(2, \mathbb{R})$ deki normalliyeni araştırılabilir.

6. KAYNAKLAR

1. Beardon, A. F., The Geometry of Discrete Groups, Springer Verlag, New York, Heidelberg, Berlin, 1983.
2. Cohn, H., A Second Course in Number Theory, Wiley, New York, 1962.
3. Ivrissimtzis,I.P., Congruence Subgroups of Hecke and Reguler Dessings, Ph.D. Thesis, University of Southampton, 1998.
4. Jones, G. A.ve Singerman, D., Complex Functions: an algebraic and geometric viewpoint, Gambridge University Press, Cambridge, 1987.
5. Lang, M. – L., Lim, C. – H. ve Tan, S. – P., Independet Generators for Congruence Subgroups of Hecke Groups, Math. Z. 220, (1995), 569- 594.
6. Lang, M. – L.ve Tan, S. – P., Normalizers of The Congruence Subgroups of The Hecke Group G_5, A. Math. Soc., Vol. 127, 11(1999), 3131- 3140.
7. Rabinson, D. J., A Course in The Theory of Groups, Springer Verlag, New York, Heidelberg, Berlin, 1982.
8. Rosen, D., The Substitutions of The Hecke Group $\Gamma(2\cos\frac{\pi}{5})$, Arch. Math., Vol. 46, (1986), 533-538.
9. Schoeneberg, B., Elliptic Modular Functions, Springer Verlag, Berlin, Heildelberg, New York, 1974.
10. Lang, S., Algebraic Number Theory, Springer Verlag, 1994.
11. Washington, L. C., İntroduction to Cyclotomic Fields, Springer Verlag, New York, Berlin, Heidelberg, 1997.
12. Hungerfort, T. W., Algebra, Springer Verlag, New York, Heidelberg, Berlin, 1980.
13. Armstrong, M. A., Groups and Symmetry, Springer Verlag, New York, Berlin, Heildelberg, London, Paris, Tokyo, 1988.
14. Chan, S.-P., Lang, M.-L., Lim, C.-H. ve Tan, S.-P., The İnvariants of The Congruence Subgroups $G_0(I)$ of The Hecke Group G_5, Illinois J.of Math. 38 (1994), 636-652.
15. Person, L. A., Generalised Kloosterman Sums and The Fourier Coefficients of Cusp Forms, Trans.of The American Math. Soc., 217 (1976), 329-350.

ÖZGEÇMİŞ

1967 yılında Trabzon'un Akçaabat ilçesi Akçaköy Köyünde doğdu. İlkokulu Fındıklı II. İlkokulunda, Ortaokulu Akçaköy- Ortaokulunda, Liseyi de Akçaköy Lisesinde tamamladı. 1984 yılında K.T.Ü Fen Edebiyat Fakültesi Matematik Bölümünde lisans öğrenimine başladı. 1989 yılında bu bölümden mezun oldu. 07.11.1989 tarihinde K.T.Ü Fen Edebiyat Fakültesi Matematik Bölümünde Matematiğin Temelleri ve Lojik Matematik Anabilim Dalına Araştırma Görevlisi olarak atandı.1990 yılında K.T.Ü Fen Bilimleri Enstitüsü Yüksek Lisans (Matematik) programına başladı ve 1993 yılında bu programdan mezun oldu. Askerlik görevini, Nisan 1994 – Kasım 1994, 237. Kısa Dönem olarak yaptı. 1995 yılında K.T.Ü Fen Bilimleri Enstitüsü Doktora (Matematik) programına başladı. Halen K.T.Ü Fen Edebiyat Fakültesi Matematik Bölümünde Araştırma Görevlisi olarak görev yapmaktadır.