T.C.
NİĞDE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

# $\Gamma^0(N)$ KONGRÜANS ALT GRUBUNUN ALT YÖRÜNGESEL GRAFLARI

DUYGU BIYIKLI

Ağustos 2012

D. BIYIKLI, 2012
YÜKSEK LİSANS TEZİ
NİĞDE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

T.C.
NİĞDE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

# $\Gamma^0(N)$ KONGRÜANS ALT GRUBUNUN ALT YÖRÜNGESEL GRAFLARI

DUYGU BIYIKLI

Yüksek Lisans Tezi

Danışman

Yrd. Doç. Dr. Serkan KADER

Ağustos 2012

**Duygu BIYIKLI** tarafından **Yrd. Doç.Dr Serkan Kader** danışmanlığında hazırlanan "**$\Gamma^{0}(N)$ Kongrüans Alt Grubunun Alt Yörüngesel Grafları**" adlı bu çalışma jürimiz tarafından Niğde Üniversitesi Fen Bilimleri Enstitüsü **Matematik** Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir.

Başkan : **Doç.Dr. Atakan Tuğkan YAKUT** **Niğde Üniversitesi**

Üye : **Yrd. Doç. Dr. Bahadır Özgür GÜLER** **Karadeniz Teknik Üniversitesi**

Üye : **Yrd. Doç. Dr. Serkan KADER** **Niğde Üniversitesi**

**ONAY:**

Bu tez, Fen Bilimleri Enstitüsü Yönetim Kurulunca belirlenmiş olan yukarıdaki jüri üyeleri tarafından …./…./20.... tarihinde uygun görülmüş ve Enstitü Yönetim Kurulu'nun …./…./20.... tarih ve ............................ sayılı kararıyla kabul edilmiştir.

**....../...../20...**

**Doç. Dr. Osman SİVRİKAYA**

**MÜDÜR**

# ÖZET

## $\Gamma^0(N)$ KONGRÜANS ALT GRUBUNUN ALT YÖRÜNGESEL GRAFLARI

BIYIKLI, Duygu
Niğde Üniversitesi
Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

Danışman: Yrd. Doç. Dr. Serkan KADER

Ağustos 2012, 49 sayfa

Bu çalışmada $\Gamma^0(N)$ kongrüans alt grubunun yapısı incelendi. Birinci bölümde, konuyla ilgili kısa bir tarihçe verildi. İkinci bölümde Öklid olmayan kristalize grupların yapısı irdelendi. $\mathrm{PSL}(2,\mathbb{R})$, $\Gamma$- Modüler grubu, kongrüans alt gruplarının bazı özellikleri ve temel bölgeler, graf teori, imprimitif hareket ile ilgili ihtiyaç duyduğumuz temel tanımlar verildi.. Üçüncü bölümde $\Gamma^0(N)$ nin transitif olarak ettiği bir yörünge bulundu. $\Gamma^0(N)$ nin alt yörüngesel graflarında kenar şartları belirlendi ve bundan faydalanılarak alt yörüngesel grafın kendisiyle eşleşmiş kenar ve üçgen ihtiva etmesi için gerek ve yeter şartlar elde edildi.

Anahtar sözcükler: Modüler grup, Kongrüans alt grupları,Grup hareketi, Alt yörüngesel graflar,.

## SUMMARY

SUBORBITAL GRAPHS OF THE CONGRUENCE SUBGROUP $\Gamma^0(N)$

BIYIKLI, Duygu
Nigde University
Graduate School of Natural and Applied Sciences
Department of Mathematics

Supervisor: Assistant Professor Dr. Serkan KADER

August 2012, 49 pages

In this study, the structure of the congruence subgroup $\Gamma^0(N)$ is examined.In the first chapter, a brief history is given on the subject. In the second chapter, the structure of Non-Euclidean Crystalllographic Groups is discussed and some properties of $\mathrm{PSL}(2,\mathbb{R})$, $\Gamma$ -Modular group, congruence subgroups and also the preliminary definitions we require for fundamental domains, graph theory and imprimitive action are given. In the third chapter, an orbit which $\Gamma^0(N)$ acts on transitively is found. Then we obtained edge conditions in suborbital graphs of $\Gamma^0(N)$ and by using them necessary and sufficient conditions for which the suborbital graph contain self-paired edge and the triangle are obtained.

Keywords: Modular Group, Congruence subgroups, Group action, Suborbital graphs..

# TEŞEKKÜR

Bu tezin hazırlanmasında yardımlarını esirgemeyen danışman hocam Yrd.Doç.Dr. Serkan KADER' e, Niğde Üniversitesi Matematik bölümü öğretim üyelerine ve hayatım boyunca her türlü desteği ve sabrı gösteren kıymetli aileme teşekkür ederim.

**İÇİNDEKİLER**

# ŞEKİLLER DİZİNİ

## SİMGELER VE KISALTMALAR

| | |
|---|---|
| $\mathbb{C}$ | : Kompleks sayılar kümesi |
| $\mathbb{C}_\infty$ | : Genişletilmiş kompleks sayılar kümesi ( Riemann Küresi) |
| $\varphi(a)$ | : Euler fonksiyonu |
| $\Gamma$ | : Modüler grup |
| $\Gamma_0(m)$ | : $\Gamma$ nın $m \mid c$ olan bir alt grubu |
| $\mathcal{N}or(m)$ | : $\Gamma_0(m)$ nin PSL(2,$\mathbb{R}$) deki normalliyeni |
| $\mathrm{PSL}(2,\mathbb{R})$ | : Gerçel katsayılı, lineer, kesir dönüşümlerinin grubu |
| $\hat{\mathbb{R}}$ | : Genişletilmiş reel sayılar kümesi |
| $\hat{\mathbb{Q}}$ | : Genişletilmiş rasyonel sayılar kümesi |
| $\mathcal{U}$ | : $\mathbb{C}$ de üst yarı düzlem |
| $A \le B$ | : $A$ grubu $B$ grubunun alt grubudur |
| $\lvert A : B \rvert$ | : $B$ alt grubunun $A$ daki indeksi |
| $a \mid b$ | : $a$ sayısı $b$ sayısını böler |
| $a \nmid b$ | : $a$ sayısı $b$ sayısını bölmez |
| $a \parallel b$ | : $a$ sayısı $b$ sayısının bir tam bölenidir |
| $a \equiv b (\mathrm{mod} n)$ | : $n$ sayısı $(a-b)$ sayısını böler |
| $(a,b)$ | : $a$ ile $b$ sayısının en büyük ortak böleni |
| $\overset{\circ}{F}$ | : $F$ kümesinin içi |
| $Gx$ | : $x$ noktasının $G$ -yörüngesi |
| $G_x$ | : $x$ noktasının $G$ deki sabitleyeni |
| $\mu(E)$ | : $E$ kümesinin hiperbolik alanı |
| $\ell(C)$ | : Parçalı, sürekli, diferansiyellenebilir bir $C$ eğrisinin hiperbolik uzunluğu |

# BÖLÜM I

# GİRİŞ

19. yüzyılın sonlarına doğru ayrık gruplar teorisine temel teşkil edebilecek bazı önemli sonuçlar ilk defa Henry Poincare tarafından göz önüne getirilmiş ve eliptik fonksiyonlar teorisinin genelleştirilmesi için kullanılmıştır. Lineer kesirli dönüşümler grubu özellikle 19. yüzyılda Öklid olmayan geometriler ve İnvaryant teorinin keşfiyle birlikte büyük önem kazanmış, topolojik grup yapısına uygun olması nedeniyle gerek analiz, gerekse cebirsel yöntemlerle derinlemesine incelenmiştir. Eliptik eğrilerin aritmetiği, integral kuadratik formlar ve eliptik modüler fonksiyonlar teorilerindeki önemi nedeniyle en çok $\mathrm{PSL}(2,\mathbb{R})$ nin ayrık bir alt grubu olan $\Gamma$ modüler grubunun kongrüans alt grupları olan $\Gamma(N)$, $\Gamma_0(N)$ , $\Gamma^0(N)$, $\Gamma_1(N)$ grupları üzerinde çalışılmıştır.

$\Gamma_0(N)$'nin $\mathrm{PSL}(2,\mathbb{R})$'deki normalliyeni üzerinde ilk çalışma Felix Christian Klein ve Robert Fricke tarafından yapılmış, 1951'de Bruno Schoeneberg ve 1964'te J. Lehner ile Morris Newman tarafından $\Gamma_0(N)$ 'nin Weierstrass noktalarını bulma probleminin normalliyene bağlı olduğu ifade edilmiştir. Daha sonra 1970'te Arthur Oliver L. Atkin ile J. Lehner'in çalışmalarını yazdığı "Hecke Operators on $\Gamma_0(N)$" adlı makalede normalliyenin önemi vurgulanmış ancak normalliyenin elemanlarının net bir şekilde karakterize edilmesi John Horton Conway ve Simon Phillips Norton tarafından verilmiştir.

1973' te Bernd Fischer ve Bob Griess'in çalışmalarında bağımsız olarak, mertebesi

$$2^{46}\cdot 3^{20}\cdot 5^{9}\cdot 7^{6}\cdot 11^{2}\cdot 13^{3}\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71$$

olan yeni bir basit $M$ grubu için deliller üretmesi ve Robert L. Griess'in varlığını ispatlamasının ardından bu yeni basit grubun özellikle $\Gamma_0(N)$'nin $\mathrm{PSL}(2,\mathbb{R})$ 'deki normalliyeni ile ilgili olması normalliyeni tekrar ön plana getirmiştir.1979'da John Horton Conway ve Simon Phillips Norton bu basit grubu Monster olarak adlandırarak "Monstrous Moonshine" (Dev Ayışığı) adlı çalışmalarında normalliyenin elemanlarına son şeklini vermişlerdir. Sonraki dönemlerde Andrew P. Ogg $|M|$ yi bölen p asal sayıları için $\mathrm{PSL}(2,\mathbb{R})$'deki normalliyeninin belirlediği fonksiyon cisminin sıfır cinsine sahip olduğunu gösterdi. A. Pizer, bu asalların 2-ağırlıklı modüler formlarla quaternion cebir teta-serisini ilişkilendiren Hecke konjektürünü sağlayan yegâne asallar olduğunu gösterdi.

Heinz Helling 1970 yılında "On the commensurability class of the rational modular groups" adlı çalışmasında $N$ karesiz ( $N$ nin karesiz olması için gerek ve yeter şart $p$ asal ve $p|\ N$ olmak üzere $(N,\dfrac{N}{p})=1$ olmasıdır.) olduğunda normalliyen gruplarının maksimal ayrık grup olduğunu ve $\Gamma$ modüler grubu ile orantılı olan her ayrık $\Delta$ grubunun bu gruplardan birine eşlenik olduğunu gösterdi. Ayrıca $\Delta$ ile belirlenen fonksiyon cisminin cinsi sıfır ise normalliyen ile belirli fonksiyon cisminin cinsi de sıfırdır ve eşlenik yapan her eleman $p,q$ ve $r$ ortak çarpanı olamayan tam sayılar olmak üzere

$$z \to \frac{pz+q}{r}$$

biçimindedir.

Normalliyen, $\mathrm{PSL}(2,\mathbb{R})$ grubunun ayrık bir alt grubu ve sonlu üretilmiş olduğundan, topolojik ve geometrik özelliklerini veren bir simgeye sahiptir. Bu simge problemi bir bakıma bir ayrık grubun kimliğidir. Simgedeki parametreler; grubun cinsi, üretici eliptik elemanların mertebeleri ve parabolik sınıf sayısıdır. Simge problemi ayrık gruplar üzerine çalışan bilim adamlarının bu yolda daha fazla çaba sarf etmelerini gerektirmektedir. NEC gruplarının (Non-Euclidean Crystallographic Groups) yüzey sembolleri düzenli bir şekilde H.C. Wilkie tarafından incelenmiştir. Daha sonra A.M. Macbeath, NEC gruplarının simgelerine geniş bir açıklama getirmiştir. 1974'te David Singerman "On the structure of non-euclidean crystallographic groups" adlı makalesinde $\mathrm{PSL}(2,\mathbb{R})$'nin herhangi bir ayrık $\Gamma$ alt grubu verildiğinde simgesi verilen sonlu indeksli bir alt gruba sahip olur problemini çözmüştür. $N$ sayısının karesiz olması durumunda simge problemini Colin Maclachlan 1981 yılındaki "Groups of units of zero ternary quadratic forms" adlı çalışmasında çözmüştür. Fakat $N$ sayısının keyfi olması durumunda yukarıdaki problem oldukça zor bir hal almakta olup hâlâ açıktır. Şayet her $N$ sayısı için simge bulunabilirse bunun $M$ basit grubu ile nasıl bir bağlantısı olduğu da ayrı bir durumdur. Ancak 1992 yılında “The signature of the normalizer of $\Gamma_0(N)$ ” adlı çalışmada M. Akbaş ve D. Singerman normalliyenin parabolik sınıf sayısını verdiler ve 3, 4 ve 6 mertebeli eliptik üretici elemanları da tam olarak belirlediler. Dolayısı ile geriye 2 mertebeli üretici elemanların sayısını ve $g$ cinsini bulma problemi kalmıştır.

Bu çalışmada $\Gamma^0(N)$ kongrüans alt grubunun alt yörüngesel grafları araştırılmıştır. Bölüm II de temel kavramlar verilmiştir. Bölüm III te ise $\Gamma^0(N)$ nin $\hat{\mathbb{Q}}$ üzerindeki hareketi incelenmiş, alt yörüngesel graflarındaki kenar şartları verilmiştir. Ayrıca graflardaki ikili devre ve üçgen olma bulunmuştur.

# BÖLÜM II

# TEMEL KAVRAMLAR

## 2.1 Topolojik Gruplar

**Tanım 2.1.** $(G,\cdot)$ bir grup ve aynı zamanda bir topolojik uzay olsun. Bu takdirde

**i)** $M : G\times G \longrightarrow G$, $(g,h) \longrightarrow g\cdot h$

**ii)** $m : G \longrightarrow G$, $g \longrightarrow g^{-1}$

dönüşümleri sürekli ise $G$ ye bir *topolojik grup* denir.

**Tanım 2.2.** $G$ bir topolojik grup ve $X$ bir topolojik uzay olsun. Bu takdirde

$$\wedge : G\times X \longrightarrow X, \quad (g,x) \longrightarrow \wedge(g,x) =: g\wedge x$$

sürekli bir dönüşüm ve

**(i)** $g\wedge(h\wedge x) = gh\wedge x$ , $g,h\in G,\ x\in X$

**(ii)** $e\wedge x = x$ , $e\in G,\ x\in X$

şartları sağlanıyorsa $[G,X,\wedge]$ üçlüsüne veya $[G,X]$ ikilisine bir *topolojik dönüşüm grubu* adı verilir. Bu durumda $G$ ye $X$ *üzerinde hareket eder* veya $G$ ye $X$ üzerinde bir *hareket grubu* denir.

**Önerme 2.3.** $[G,X]$ bir topolojik dönüşüm grubu ve $x,y\in X$ olsun. Bu takdirde

$$x \approx y :\Leftrightarrow \exists g\in G :\ gx = y$$

şeklinde tanımlanan $\approx$ bağıntısı $X$ üzerinde bir denklik bağıntısıdır.

**Tanım 2.4.** "$\approx$" bağıntısının denklik sınıflarına *hareketin yörüngeleri* denir. Ayrıca $x\in X$ noktasını içeren yörüngeye *x-in yörüngesi* denir ve bu $Gx := \{gx \mid g\in G\}$ kümesidir.

**Tanım 2.5.** *G*, *X* üzerinde hareket etsin ve $x, y \in X$ keyfi olsun. $gx = y$ olacak biçimde bir $g \in G$ elemanı varsa *G* ye *X* üzerinde *transitif olarak hareket ediyor* denir.

Bu tanıma göre hareket transitif ise $\forall x \in X$ için $Gx = X$ elde edilir. Yani bir tek yörünge vardır. Yörünge grubun transitif olarak hareket ettiği kümedir.

**Önerme 2.6.** $[G, X]$ bir topolojik dönüşüm grubu olsun. $\begin{array}{l} p : X \longrightarrow X/G \\ \quad x \longrightarrow Gx \end{array}$ dönüşümünü göz önüne alalım. Bu durumda

$$"U \subset X/G \text{ açıktır} :\Leftrightarrow p^{-1}(U) \subset X \text{ açıktır}"$$

tanımı ile verilen açık kümelerin topolojisi ile $X/G$ ye bir *yörünge uzayı* diyeceğiz. *p* dönüşümü açıkça süreklidir ve *projeksiyon* olarak adlandırılır.

**Tanım 2.7.** *G* bir grup ve $H<G$ olsun. *H* alt grubuna göre sağ ve sol denklik sınıflarının sayısı aynıdır. Bu sayıya *H* alt grubunun *G* içerisindeki indeksi denir ve $|G:H|$ ile gösterilir.

**Tanım 2.8.** *G*, *X* üzerinde hareket etsin ve $x \in X$ olsun. $G_x := \{g \in G \mid gx = x\}$ kümesine x noktasının *sabitleyeni* denir.

**Tanım 2.9.** *G* bir grup olsun. $C := \{g \in G \mid \forall x \in G \text{ için } gx = xg\}$ kümesine *G* nin *merkezi* denir.

**Tanım 2.10.** *G* bir grup olsun. $G = \langle a \rangle$ olacak şekilde bir $a \in G$ varsa *G* ye *bir devirli grup* denir.

**Tanım 2.11.** *G* bir grup ve $H < G$ olsun. $\mathcal{N}_G(H) := \{g \in G \mid gHg^{-1} = H\}$ kümesine *H* nın *G* deki *normalliyeni* denir. Normalliyen, *H* yı normal alt grup olarak içeren en büyük kümedir.

**Tanım 2.12.** Bir *T* dönüşümünün *periyodu* ( veya *mertebesi*) $T^m = I$ eşitliğini sağlayan en küçük pozitif tamsayıdır. Böyle bir *m* yoksa *T* ye *sonsuz periyotludur* denir.

**Tanım 2.13.** $N \in \mathbb{Z}$ için $1 \le a \le N$ ve $(a, N) = 1$ olan $a$ tamsayılarının sayısı $\varphi(N)$ ile gösterilir. Bu fonksiyona *Euler fonksiyonu* denir.

$m = p_1^{r_1} p_2^{r_2} \ldots p_s^{r_s}$ ise bu takdirde

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_s}\right)$$

dir.

## 2.2 Öklid Olmayan Kristalize Gruplar

**1)** $\mathcal{G}$ ile $\mathbb{C}_\infty := \mathbb{C} \cup \{\infty\}$ genişletilmiş kompleks düzlemin

(A) $\left\{ z \to \dfrac{az+b}{cz+d} \mid a,b,c,d \in \mathbb{R} \text{ ve } ad - bc = 1 \right\}$

(B) $\left\{ z \to \dfrac{a\bar{z}+b}{c\bar{z}+d} \mid a,b,c,d \in \mathbb{R} \text{ ve } ad - bc = -1 \right\}$

biçimindeki dönüşümlerin grubunu gösterelim. $\mathcal{G}$ nin her bir elemanı $\mathcal{U} := \{ z \in \mathbb{C} \mid \operatorname{Im} z > 0 \}$ üst yarı düzlemin kendi üzerine bir konform veya ters konform homeomorfizmasıdır.

(A) biçimindeki dönüşümlerin grubunu $\mathrm{PSL}(2,\mathbb{R})$ ile göstereceğiz. Bu grup $\mathcal{G}$ de 2 indeksli bir alt gruptur. $\mathcal{U}$ nun her konform homeomorfizmi $\mathrm{PSL}(2,\mathbb{R})$ dedir [12].

$\mathcal{G}$ üzerinde bir topolojik yapı aşağıdaki biçimde oluşturulabilir:

$\tau = \{(a,b,c,d) : ad - bc = \pm 1\} \subset \mathbb{R}^4$ alt kümesini alalım. Bu alt küme üzerinde $\mathbb{R}^4$ deki adi topolojinin kondurduğu alt uzay topolojisini göz önüne alalım. Bu $\tau$ alt uzayında $(a,b,c,d)$ ile $(-a,-b,-c,-d)$ noktalarını özdeşleştirirsek $\mathcal{G}$, özdeşlik topolojisi ile bir topolojik grup yapısına sahip olur. $\mathcal{G}$ topolojik grubu $\mathrm{PSL}(2,\mathbb{R})$ ve $\mathcal{G} \setminus \mathrm{PSL}(2,\mathbb{R})$ olmak üzere iki bileşene sahiptir.

$\mathcal{G}$ nin ayrık alt gruplarına *Öklid olmayan kristalize gruplar*, kısaca *NEC grupları* adı verilir.

Katsayıları reel ve determinantı 1 olan 2×2 tipindeki matrislerin grubunu

$$\mathrm{SL}(2,\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{R},\ ad - bc = 1 \right\}$$

ile gösterelim. $\mathrm{SL}(2,\mathbb{R})$ nin kendi merkezi $\{\pm \mathrm{I}\}$ ile bölümünden

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

grubu elde edilir. Burada

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ ve } \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$$

elemanları özdeş olarak aynı kabul edilir ve aynı elemanla temsil edilir.

$\mathrm{PSL}(2,\mathbb{R})$ grubu $\mathcal{U} = \{ \mathrm{z} \in \mathbb{C} : \mathrm{Im}(\mathrm{z}) > 0 \}$ üst-yarı düzlemi üzerinde

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \to \frac{az+b}{cz+d}$$

ile hareket eder.

$\mathcal{U}$ üst yarı düzlemi, Öklid olmayan (hiperbolik) düzlemin bir modeline aşağıdaki biçimde dönüştürülebilir:

Bir yay elemanının *ds* hiperbolik uzunluğu

$$ds^2 = \frac{dx^2 + dy^2}{y^2}$$

ile tanımlanır. Böylece parçalı, sürekli, diferansiyellenebilir bir *C* eğrisinin hiperbolik uzunluğu

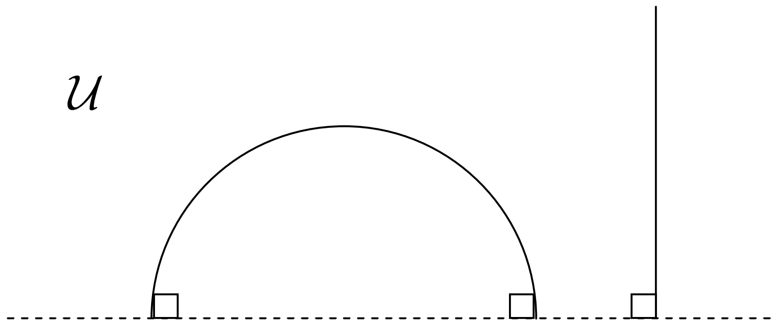
$$\ell(C) := \int_C ds = \int_C \frac{\sqrt{dx^2 + dy^2}}{y}$$

ve ölçülebilir bir $E$ kümesinin hiperbolik alanı

$$\mu(E) := \iint_E \frac{dxdy}{y^2}$$

olarak tanımlanır. Yukarıdaki metriğin geodezikleri, reel eksene dik yarı çemberler ve yarı doğrulardır. Bunlar *hiperbolik doğrular* olarak adlandırılır.

$\mathcal{U}$ üst yarı düzlemde iki nokta arasındaki hiperbolik uzaklık, bu iki noktayı birleştiren bir tek hiperbolik doğru parçasının uzunluğudur. Bu metrikle tanımlanan topoloji, bilinen Öklid topolojisine eş değerdir. Yani bir topolojideki açık küme, diğer topolojide de açıktır. Hiperbolik uzaklık ve alan $\mathrm{PSL}(2,\mathbb{R})$ nin dönüşümleri altında invaryant kalır [12].




Şekil 2.1 Hiperbolik doğrular

**2)** Şimdi $\mathcal{G}$ nin elemanlarını yön durumlarına ve sabit nokta kümelerine göre sınıflandıralım:

**(*i*)** $T \in \mathrm{PSL}(2,\mathbb{R})\backslash\{I\}$ dönüşümünün sabit noktalarını bulalım. Bunun için, $\dfrac{az+b}{cz+d}=z$ yazılırsa,

$$cz^2+(d-a)z-b=0 \tag{2.1}$$

denklemi elde edilir. Bu denklemin kökleri *T* nin sabit noktalarıdır. *T* nin en fazla iki sabit noktası vardır. (2.1) denkleminin kökleri ise,

$$z_{1,2}=\frac{-(d-a)\mp\sqrt{(a+d)^2-4}}{2c}$$

olarak bulunur. Burada üç durum söz konusudur;

$1^\circ$) $|a+d|>2$ ise, iki farklı sabit nokta vardır ve bunlar $\mathbb{R}\cup\{\infty\}$ üzerindedirler. Bu durumda *T* ye bir *hiperbolik dönüşüm* adı verilir.

$2^\circ$) $|a+d|=2$ ise, birbirine eşit iki sabit nokta vardır ve bunlar $\mathbb{R}\cup\{\infty\}$ üzerindedirler. Bu durumda *T* ye bir *parabolik dönüşüm* adı verilir.

$3^{\circ})$ $|a+d|<2$ ise, birbirinin eşleniği olan iki kompleks sabit nokta vardır. Bu sabit noktalardan biri açıkça $\mathcal{U}$ kümesindedir. Bu durumda $T$ -ye bir *eliptik dönüşüm* adı verilir.

**(*ii*)** Şimdi de $T \in \mathcal{G} \setminus \mathrm{PSL}(2,\mathbb{R})$ olsun. Bu durumda $z = \dfrac{a\overline{z}+b}{c\overline{z}+d}$ yazılırsa

$$cz\overline{z} + dz - a\overline{z} - b = 0 \tag{2.2}$$

denklemi elde edilir. (2.2) denkleminde $z = x+iy$ ve $\overline{z} = x-iy$ ifadeleri yerlerine yazılırsa,

$$c(x+iy)(x-iy) + d(x+iy) - a(x-iy) - b = 0 \Rightarrow$$

$$c(x^2+y^2) + dx - ax + i(dy+ay) - b = 0 \Rightarrow$$

$$\left.\begin{array}{r} c(x^2+y^2)+(d-a)x-b=0 \\ (d+a)y=0 \end{array}\right\}$$

biçiminde iki durum elde edilir. Bu iki durumu inceleyelim:

$1^{\circ})$ $a+d \neq 0$ ise $y=0$ dır. Bu durumda $cx^2+(d-a)x-b=0$ denklemi elde edilir. Bu denklemin diskriminantı

$$\Delta = (d-a)^2 + 4bc = d^2 - 2ad + a^2 + 4bc$$

dir. Buradan $ad-bc=-1$ eşitliği kullanılırsa $\Delta = (a+d)^2 + 4 > 0$ elde edilir. Dolayısıyla $T$ nin iki farklı sabit noktası vardır ve bunlar $\mathbb{R} \cup \{\infty\}$ üzerindedirler. Bu durumda $T$ ye bir *kayan-yansıma* denir.

$2^{\circ})$ $a+d=0$ ise $(a+d).y=0$ eşitliği özdeş olarak gerçekleşeceğinden $c(x^2+y^2)+(d-a)x-b=0$ eşitliği gereği $T$ nin sabit noktaları kümesi bir çemberdir. $a+d=0$ ve $ad-bc=-1$ eşitlikleri yardımıyla bu çemberin merkezinin $\left(\dfrac{a}{c},0\right)$ ve yarıçapının $\dfrac{1}{|c|}$ olduğu görülür. Bu durumda $T$ dönüşümüne bir *yansıma* adı verilir.

Buna göre $\mathcal{G}$ nin, hiperbolik, parabolik, eliptik, kayan-yansıma ve yansıma diye adlandırılan beş tip elemanı vardır.

Buna göre $\mathcal{G}$ nin, hiperbolik, parabolik, eliptik, kayan-yansıma ve yansıma diye adlandırılan beş tip elemanı vardır.

**Tanım 2.14.** $T_1$ ve $T_2$ , $\mathcal{G}$ grubunun herhangi iki elemanı olsun. $T_1 = TT_2T^{-1}$ olacak şekilde bir $T \in \mathcal{G}$ elemanı varsa $T_1$ ve $T_2$ birbirinin *eşleniğidir* denir.

**Önerme 2.15.** $T_1$ ve $T_2$ birbirinin eşleniği iseler aynı tiptendirler.

$\mathcal{G}$ nin elemanlarını *iz* (trace) lerine, $a+d$, ve ayrıca determinantlarına göre sınıflandırabiliriz.

$\mathcal{G}$ nin eşlenik elemanlarının aynı tip olduğu gerçeği kullanıldığında, dönüşümlerin her biri bir doğal gösterime sahiptir. Doğal gösterimler aşağıdaki şekilde sınıflandırılır:

| Eleman Türü | Doğal Gösterim |
|---|---|
| Hiperbolik | $z \to \lambda z \quad (\lambda > 1)$ |
| Eliptik | $z \to w, \quad \dfrac{w-i}{w+i} = e^{i\theta}\dfrac{z-i}{z+i}, \quad \theta \neq 2\mathrm{n}\pi$ |
| Parabolik | $z \to z \pm 1$ |
| Kayan-yansıma | $z \to \lambda \overline{z} \quad (\lambda < -1)$ |
| Yansıma | $z \to -\overline{z}$ |

**Tanım 2.16.** $\Lambda$, $\mathrm{PSL}(2,\mathbb{R})$ nin bir alt grubu olmak üzere I-birim matrisinin $\mathrm{U} \cap \Lambda = \{\mathrm{I}\}$ şartını sağlayan bir U-komşuluğu varsa $\Lambda$ ya $\mathrm{PSL}(2,\mathbb{R})$ nin bir *ayrık alt grubu* veya *Fuchsian grup* adı verilir.

Her sonlu üretilmiş Fuchsian grubu da aşağıdaki gibi bir gösterime sahiptir:

Üreticiler : $a_1, b_1, \ldots, a_g, b_g$ (hiperbolik)

$x_1, \ldots x_r$ (eliptik)

$p_1, \ldots, p_s$ (parabolik)

Bağıntılar : $x_1^{m_1} = \ldots = x_r^{m_r} = \prod_{i=1}^{g} \mathrm{a}_i b_i a_i^{-1} b_i^{-1} \prod_{j=1}^{r} x_j \prod_{k=1}^{s} p_k = 1$

$$\text{Simge} : (\ g\ ;\ m_1, \ldots, m_r\ ;\ s\ ).$$

Burada $g$-grubun cinsini, $m_i$- üretici eliptik elemanların mertebelerini ve $s$-parabolik sınıf sayısını temsil etmektedir. Simge, üzerinde çalışılan grubun invaryantlarını ortaya koyması bakımından son derece önemlidir [5].

**Tanım 2.17.** $\Lambda$ bir Fuchsian grubu olsun. Bu takdirde

**(i)** $\bigcup_{T\in\Lambda} T(F) = \mathcal{U}$

**(ii)** $\forall T \in \Lambda \setminus \{I\}$ için $\overset{\circ}{F} \cap T(\overset{\circ}{F}) = \varnothing$.

şartlarını sağlayan $F$ kapalı kümesine $\Lambda$ için bir *temel bölge* adı verilir

**Tanım 2.18.** $\Lambda$ bir Fuchsian grup ve $p \in \mathcal{U}$, $\forall \gamma \in \Lambda \setminus \{I\}$ için $\gamma(p) \neq p$ koşulunu sağlayan bir nokta olsun. $d$ hiperbolik metrik olmak üzere

$$F = \{ z \in \mathcal{U} \mid \forall g \in \Lambda \text{ için } d(z,p) \le d(g(z),p) \}$$

kümesine, $\Lambda$ için *Dirichlet Bölgesi* denir.

**Tanım 2.19.** $\Lambda \le \mathrm{PSL}(2,\mathbb{R})$, $T \in \Lambda$ ve $T(z) = \dfrac{az+b}{cz+d}$ , $c \neq 0$ olsun. $I(T) : |cz+d|^2 = 1$ çemberi, $T$ nin *izometrik çemberi* olarak adlandırılır. $|T'(z)| = 1 \Leftrightarrow z \in I(T)$ olduğundan izometrik çember, diferansiyel Öklid uzunluğunu değiştirmeden $T$ ile dönüştürülen noktaların geometrik yeridir. $F_\infty$; $\Lambda$ da sonsuzun $\Lambda_\infty$ sabitleyeni için bir temel bölge ve $K$; $\Lambda$ nın tüm izometrik çemberlerinin dışında kalan bölge ise $F = F_\infty \cap K$ , $\Lambda$ için bir temel bölgedir.

**Tanım 2.20.** $X$ bir bağlantılı, Hausdorff topolojik uzayı olsun. Bir $A \subset X$ ve $B \subset \mathbb{C}$ açık alt kümeler olmak üzere $\varphi : A \to B$ homoemorfizmasına $X$ üzerinde bir *kompleks kart* ve $(A,\varphi)$ çiftine $X$ in bir *koordinat komşuluğu* denir.

**Tanım 2.21.** Eğer $\varphi_1 \circ \varphi_2^{-1} : \varphi_2(A_1 \cap A_2) \to \varphi_1(A_1 \cap A_2)$ fonksiyonu holomorf ise $(A_1,\varphi_1)$ ve $(A_2,\varphi_2)$ *koordinat komşulukları uyumludur* denir.

**Tanım 2.22.** Koordinat komşuluklarının bir $(A_i,\varphi_i)_{i\in I}$ ailesini alalım.

(1) $X = \cup\left(A_i\right)$

(2) $\forall(i,j)\in I\times I$ için $(A_i,\varphi_i)$ ile $(A_i,\varphi_j)$ uyumludur,

koşullarının sağlanması halinde $(A_i,\varphi_i)_{i\in I}$ ailesine bir *örtüm* adı verilir. İki örtümün birleşimlerinin de bir örtüm meydana getirmesi halinde bu *örtümler eşdeğerdir* denir.

Bu örtümlerin kümesi üzerinde bir denklik bağıntısı tanımlanır ve denklik sınıfına da bir *kompleks yapı* adı verilir.

**Tanım 2.23 (**Riemann Yüzeyi**).** Bir bağlantılı Hausdorff topolojik uzayına bir kompleks yapıyla birlikte bir *Riemann yüzeyi* adı verilir.

Her noktasının bir komşuluğu $\mathbb{R}^2$ nin bir açık alt kümesine homeomorf olan bir bağlantılı Hausdorff uzayına bir *yüzey* adı verilir. Eliptik eleman içermeyen keyfi bir $\Lambda$-Fuchsian grubu da PSL( $2,\mathbb{R}$ ) nin bir alt grubu olarak $\mathcal{U}$ üzerinde hareket eder ve bölüm topolojisi ile meydana gelen bölüm uzayı bir yüzeydir.

Diğer taraftan $\mathcal{U}$ daki kompleks yapı $\mathcal{U}/\Lambda$-yüzeyine transfer edildiğinde bir Riemann yüzeyi elde edilir. Eğer $\Lambda$ eliptik eleman içeriyorsa sonuç yine bir Riemann yüzeyidir, ancak bu durumda $\mathcal{U}\to\mathcal{U}/\Lambda$ izdüşümü dallanmıştır. Ancak oluşan yüzey kompakt değildir, bunu sağlamak için $\mathcal{U}$ yerine $\mathcal{U}\cup\{\infty\}$ alınır [12].

**Teorem 2.24.** Her basit bağlantılı Riemann yüzeyi aşağıdakilerden birine konform eşdeğerdir [12]:

**(i)** $\mathbb{C}_\infty$-Riemann Küresi

**(ii)** $\mathbb{C}$-Kompleks Düzlem

**(iii)** $\mathcal{U}$-Üst Yarı Düzlem.

Bu Riemann yüzeylerinin otomorfizm grupları aşağıdaki gibidir;

**Teorem 2.25** [12].

**(i)** $Aut(\mathbb{C}_\infty) = \mathrm{PSL}(2,\mathbb{R})$

**(ii)** $Aut(\mathbb{C}) = \{z \to az+b : a,b \in \mathbb{C}, a \neq 0\}$

**(iii)** $\mathrm{Aut}(\mathcal{U}) = \mathrm{PSL}(2,\mathbb{R})$ .

**Teorem 2.26.** $\mathcal{U}/\Lambda$ kompakt ise $\Lambda$ parabolik eleman içermez [12].

## 2.3 PSL$(2, \mathbb{R})$ deki Parabolik ve Eliptik Altgruplar

**Teorem 2.27.** PSL(2,$\mathbb{R}$) nin bir parabolik (eliptik, hiperbolik) elemanının PSL(2,$\mathbb{R}$) deki merkezleyeni, aynı sabit nokta kümeli tüm parabolik ( eliptik, hiperbolik ) elemanlardan meydana gelir [6].

**Teorem 2.28.** Her Abel, Fuchsian grup devirlidir [12].

**Tanım 2.29.** $\Lambda$ bir Fuchsian grup olsun. $\Lambda$ nın birim elemandan ve parabolik (eliptik) elemanlardan oluşan devirli bir maksimal alt grubuna $\Lambda$ nın bir *parabolik* (*eliptik*) *alt grubu* denir.

**Tanım 2.30.** Bir $\Lambda$ Fuchsian grubunun parabolik (eliptik) alt gruplarının eşlenik sınıflarının sayısına $\Lambda$ Fuchsian grubunun *parabolik* (*eliptik*) *sınıf sayısı* denir.

**Tanım 2.31.** $\Lambda$ bir Fuchsian grup olsun. Bir $r \in \hat{\mathbb{Q}} := \mathbb{Q} \cup \{\infty\}$ noktası keyfi verildiğinde $\gamma(r) = r$ olacak şekilde bir $\gamma \in \Lambda$ parabolik elemanı bulunabiliyorsa, bu noktaya $\Lambda$ Fuchsian grubunun bir *parabolik noktası* veya *cusp*'ı denir. $\gamma$ nın parabolik noktalarının kümesine $\gamma$ nın *cusp kümesi* denir.

Benzer şekilde $z \in \mathcal{U}$ noktası keyfi verildiğinde $\sigma(z) = z$ olacak şekilde bir $\sigma \in \Lambda$ eliptik elemanı bulunabiliyorsa bu noktaya , $\Lambda$ nın bir *eliptik noktası* adı verilir.

## 2.4 Modüler Grup

$\mathrm{PSL}(2,\mathbb{R})$ nin üzerinde en çok çalışılan alt grubu olan Modüler grup,

$$\Gamma = \mathrm{PSL}(2,\mathbb{Z}) = \mathrm{SL}(2,\mathbb{Z}) \big/ \{\pm I\} = \{z \to Tz : T \in \mathrm{SL}(2,\mathbb{Z})\}$$

ile tanımlanır.

Bu grup aşağıdaki gibi 2x2 lik tamsayılar matrisiyle de temsil edilebilir:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad , \quad \det A = 1 .$$

$A$ ve $-A$ aynı dönüşümü temsil ettiğinden söz konusu matrisi negatifi ile eş tutacağız. Böylece matris ve dönüşüm arasında bir ayrım yapılmayacaktır. Ayrıca

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{ve} \quad \begin{pmatrix} ka & kb \\ kc & kd \end{pmatrix}, \quad k \neq 0$$

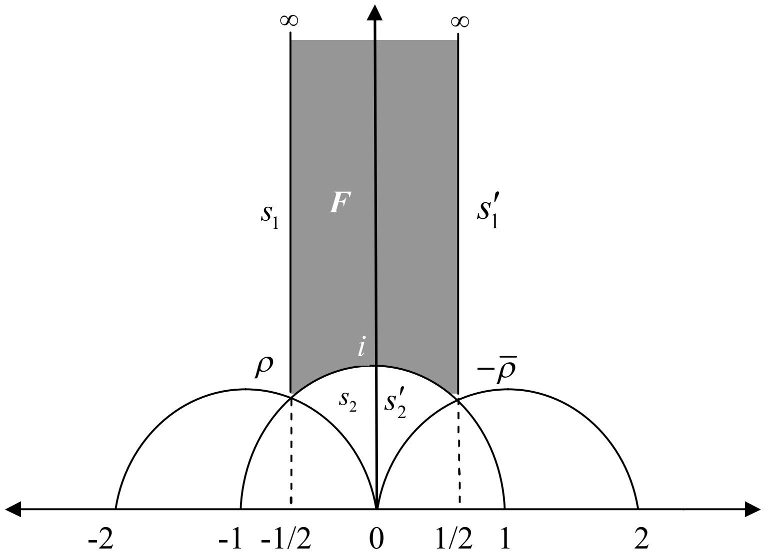
matrisleri yine aynı dönüşümü temsil ettiğinden, matris hesaplamalarında uygun olduğu yerde bu matrisleri eşit gibi yazabiliriz ( burada determinantın 1 olma şartı aranmayabilir).

**Teorem 2.32.** $\Gamma$ modüler grubu $T=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ve $U=\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ matrisleriyle üretilir.

**İspat .** Önce $\Gamma$ için Ford bölgesini bulalım. $\Gamma$ da $\infty$ un sabitleyeni $\Gamma_\infty$ ile gösterilsin. $F_\infty = \left\{ z \in \mathcal{U} : |\operatorname{Re} z| \leq \frac{1}{2} \right\}$ olsun. Bu $F_\infty$ şeridi , $\Gamma_\infty$ sabitleyeni için bir temel bölgedir. En geniş izometrik çemberler 1 yarıçaplıdır ve bu çemberlerin merkezleri reel eksen üzerindeki tam sayılardır. Sadece merkezleri 0,-1,1 olan üç çember $F_\infty$ ile kesişir. Burada $\rho = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ ve $-\bar{\rho} = \frac{1}{2} + i\frac{\sqrt{3}}{2}$ olmak üzere 0-merkezli çember $\rho, -\bar{\rho}$ da; 1-merkezli çember $-\bar{\rho}$ da; -1 merkezli çember $\rho$ da $F_\infty$ ile kesişir. Diğer çemberlerin yarıçapı $\frac{1}{2}$ den küçük veya eşittir. Bu nedenle şekilde görüldüğü gibi $F$ bölgesi üzerinde bu çemberler önem taşımaz. Buna göre;

$$F = \left\{ (x,y) \in \mathbb{R}^2 : x^2 + y^2 \geq 1 , \ |x| \leq \frac{1}{2} , \ y > 0 \right\}$$

kümesi $\Gamma$ modüler grubu için bir temel bölgedir.




Şekil 2.2 $\Gamma$ nın $F$ temel bölgesi

$T(z) = z+1$ için $T(z) = s_1'$ ve $U(z) = -\frac{1}{z}$ için $U(s_2) = s_2'$ olduğundan $(s_1, s_1')$ ve $(s_2, s_2')$ kongrü kenar çiftleridir. Bu nedenle $T$ ve $U$ dönüşümleri $\Gamma$ modüler grubunu üretir. Burada $T$ bir parabolik eleman ve $U$, 2. mertebeden bir eliptik elemandır. Buna göre; $TU = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ 3. mertebeden bir eliptik, $V := TU$ olmak üzere $\Gamma, U(z) = -\frac{1}{z}$ ve $V(z) = \frac{z-1}{z}$ elemanlarıyla da üretilir. Dolayısıyla da $U^2 = V^3 = I$ dır. Buradan $\Gamma$ nın üreticileri $U, T, V$ olduğundan $\Gamma$ nın simgesi $(0; 2, 3, \infty)$ olur.■

Şimdi de $\Gamma$ nın cusp kümesi $\hat{\mathbb{Q}} := \mathbb{Q} \cup \{\infty\}$ üzerindeki hareketini inceleyelim. $\hat{\mathbb{Q}}$ nın elemanları $(x, y) = 1$ olmak üzere $\frac{x}{y}$ olarak yazılabilir. Burada $\infty = \frac{1}{0} = -\frac{1}{0}$ dır. $\frac{x}{y} = \frac{-x}{-y}$ olduğundan bu gösterim tek türlü değildir. $T \in \Gamma$ ise

$$T\left(\frac{x}{y}\right)=\frac{ax+by}{cx+dy} \quad \text{ve} \quad T\left(\frac{-x}{-y}\right)=\frac{-ax-by}{-cx-dy}=\frac{ax+by}{cx+dy}=T\left(\frac{x}{y}\right)$$

olduğundan $\Gamma$ nın $\hat{\mathbb{Q}}$ üzerindeki hareketi iyi tanımlıdır.

Eğer $(x,\ y)=1$ ve $ad-bc=1$ ise $\dfrac{ax+by}{cx+dy}$ indirgenmiş formdadır.

Aksini varsayalım; $\dfrac{ax+by}{cx+dy}$ indirgenmiş formda olmasın. Buna göre $n\,|\,ax+by$ ve $n\,|\,cx+dy$ olacak şekilde bir $n\in\mathbb{Z}$ elemanı vardır. Bu durumda $k,\ell\in\mathbb{Z}$ için

$$ax+by=kn \tag{2.3}$$

ve

$$cx+dy=\ell n \tag{2.4}$$

dir.

(2.3) eşitliğinin her iki tarafı $d$ ile (2.4) de $-b$ ile çarpıldığında

$$(ad-bc)x=(kd-b\ell)n \tag{2.5}$$

ve benzer şekilde (2.3) eşitliği $-c$ ve (2.4) eşitliği $a$ ile çarpıldığında

$$(ad-bc)y=(a\ell-ck)n \tag{2.6}$$

elde edilir. (2.5) ve (2.6) den $n\,|\,x,y$ çelişkisi elde edilir.

**Teorem 2.33.** $\Gamma$ **,** $\hat{\mathbb{Q}}$ üzerinde transitif olarak hareket eder.

**İspat.** $\dfrac{a}{b},\dfrac{c}{d}\in\hat{\mathbb{Q}}$ ; $\dfrac{a}{b}\neq\dfrac{c}{d}$ ve $(a,b)=(c,d)=1$ olsun. Bu durumda $a\beta - b\alpha=1$ ve $c\delta - d\gamma=1$ olacak şekilde $\alpha,\beta,\delta,\gamma\in\mathbb{Z}$ tam sayıları vardır. Burada

$$\xi(z)=\frac{az+\alpha}{bz+\beta} \quad \text{ve} \quad \eta(z)=\frac{cz+\gamma}{dz+\delta}$$

şeklinde tanımlanırsa $\xi(\infty)=\dfrac{a}{b}$ ve $\eta(\infty)=\dfrac{c}{d}$ olacak şekilde bir $\varphi:=\eta\xi^{-1}\in\Gamma$ dönüşümü vardır. Dolayısıyla $\Gamma$, $\hat{\mathbb{Q}}$ üzerinde transitif olarak hareket eder.

**Teorem 2.34.** $\Gamma$ nın $\infty$ noktasının sabitleyeni $\Gamma_\infty$ sonsuz devirli bir gruptur.

**İspat.** $T\in\Gamma$ ve $T(\infty)=\infty$ olsun. $T(z)=\dfrac{az+b}{cz+d}$ ise $T(\infty)=\infty$ olduğundan $c=0$ ve $ad=1$ dir. Buradan $T(z)=\dfrac{a}{d}z+\dfrac{b}{d}=a^2z+m=z+m$ $(m=b$ veya $m=-b)$ bulunur. Dolayısıyla $U(z)=z+1$ olmak üzere $\Gamma_\infty=\left\langle\begin{pmatrix}1&1\\0&1\end{pmatrix}\right\rangle$ dur.

## 2.5 Modüler Grubun Kongrüans Alt Grupları

Kongrüans alt grupları eliptik eğrilerin aritmetiği, integral kuadratik formlar, eliptik modüler formlar gibi konulardaki önemleri itibariyle modüler grubun üstünde en çok durulan alt gruplarıdır. İlk hesaplamalar F.Klein, R. Fricke, A. Hurwitz tarafından yapılmış, sonraki dönemde A. Ogg, B. Schoeneberg, J. P. Serre bu konudaki çalışmaları ileri seviyelere taşımışlardır.

**Tanım 2.35.** $N$ pozitif tamsayı olmak üzere $\Gamma$ nın *temel kongrüans alt grubu*

$$\Gamma(N):=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\Gamma \mid a\equiv d\equiv 1 \bmod N\ ,b\equiv c\equiv 0 \bmod N\right\}$$

ile tanımlanır. $\Gamma$ nın $\Gamma(N)$-temel kongrüans alt gruplarını içeren herhangi bir alt kümesine *kongrüans alt grubu* denir. Üzerinde en çok çalışılan bazı kongrüans alt grupları;

$$\Gamma_1(N):=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\Gamma \mid a\equiv d\equiv 1 \bmod N,\ c\equiv 0 \bmod N\right\}$$

$$\Gamma_0(N):=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\Gamma \mid c\equiv 0 \bmod N\right\}$$

$$\Gamma^0(N):=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\Gamma \mid b\equiv 0 \bmod N\right\}$$

gruplarıdır. Bunlar arasındaki ilişki keyfi $N\in\mathbb{Z}$ için

$$\Gamma(N)\leq\Gamma_1(N)\leq\Gamma_0(N)\leq\Gamma$$

biçimindedir.

Ayrıca $\Gamma(N)$, $\Gamma$ nın normal bir alt grubudur, dolayısıyla $\Gamma(N), \Gamma_0(N)$ ve $\Gamma_1(N)$ nin de normal alt grubudur. Diğer taraftan $\Gamma_1(N) \lhd \Gamma_0(N)$ dir. Buna göre indeksler $N > 2$ için

$$\mu_0(N) := |\Gamma : \Gamma_0(N)| = N\prod_{p|N}\left(1+\frac{1}{p}\right), \quad |\Gamma : \Gamma_1(N)| = \frac{N^2}{2}\prod_{p|N}\left(1-\frac{1}{p^2}\right),$$

$$\frac{\mu(N)}{2} := |\Gamma : \Gamma(N)| = \frac{N^3}{2}\prod_{p|N}\left(1-\frac{1}{p^2}\right)$$

dir.

$N = 2$ durumunda $|\Gamma : \Gamma_0(2)| = 3$, $|\Gamma : \Gamma_1(2)| = 3$, $|\Gamma : \Gamma(2)| = 6$ biçimindedir. $N > 2$ için yukarıda verilen indekslerden

$$|\Gamma_0(N) : \Gamma_1(N)| = \frac{|\Gamma : \Gamma_1(N)|}{|\Gamma : \Gamma_0(N)|} = \frac{N}{2}\prod_{p|N}\left(1-\frac{1}{p}\right) = \frac{\varphi(N)}{2} \quad ;$$

$$|\Gamma_1(N) : \Gamma(N)| = \frac{|\Gamma : \Gamma(N)|}{|\Gamma : \Gamma_1(N)|} = N$$

elde edilir.

$\Gamma_0(N)$, $\Gamma_1(N)$ ve $\Gamma(N)$'nin cusp kümesi de $\hat{\mathbb{Q}}$ dır. Çünkü bunlar $\Gamma$ nın sonlu indeksli alt gruplarıdır ve bir $\Lambda$-Fuchsian grubunun sonlu indeksli herhangi bir alt grubu da $\Lambda$ ile aynı cusp kümesine sahiptir [25].

**Teorem 2.36.** $\Gamma_0(N)$ nin $\hat{\mathbb{Q}}$ üzerindeki hareketi transitif değildir.

**İspat.** Aksini varsayalım ve $0, \infty \in \hat{\mathbb{Q}}$ seçelim. Bu durumda

$$\begin{pmatrix} a & b \\ cN & d \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

olacak şekilde bir $\begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma_0(N)$ elemanı vardır.

Bu eşitlikten $b = 1$ ve $d = 0$ elde edilir. Determinant göz önüne alındığında bunun $c = -1$ ve $N = 1$ olmasıyla, diğer bir ifadeyle ancak $\begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma$ olması durumunda mümkün olduğu görülür.

## 2.6 Temel Bölgenin Cinsi

Bir kompakt, yönlendirilebilir $X$- Riemann yüzeyini göz önüne alalım. $X$ de reellerin kapalı birim aralığının bir homeomorf resmine $X$ üzerinde bir *basit yay* (*simple arc*) adı verilir. Bir yayın bitim noktası ile bir sonrakinin başlangıç noktasının birleşimiyle oluşan yayların sonlu bir dizisine $X$ üzerinde bir *eğri* (*curve*) denir.

Bir eğrinin başlangıç noktası ile bitim noktası çakışıyorsa bu eğriye bir *kapalı eğri* adı verilir. Öklid düzlemindeki bir kapalı dairenin $X$ deki bir homeomorf resmine $X$ üzerinde bir *poligon* adı verilir.

Şimdi $\Im$, $X$ üzerinde sonlu sayıdaki noktada kesişen sonlu sayıda eğrinin meydana getirdiği bir sistem olsun. Ayrıca $\Im$ nın bütünleyenlerinin bağlantılı bileşenlerinin kapanışları poligonlar olsun ve kesişimleri de ya tek bir nokta ya tek bir kenar ya da boş küme olsun. Eğrilerin böyle bir sistemine $X$ in bir *poligonal ayrışması* denir.

Bir poligonal ayrışmada meydana gelen köşe, kenar ve yüz'ün anlamı açıktır. Bunların sayısını sırasıyla $v$,$e$ ve $f$ ile göstereceğiz.

**Teorem 2.37 (**Euler**).** $X$ in her poligonal ayrışmasında $v-e+f$ sayısı invaryant kalır [25].■

**Tanım 2.38.** $g := 1 - \dfrac{v-e+f}{2}$, kesişimleri boş olan ve $X$ i ayrıştırmayan kapalı eğrilerin maksimal sayısıdır. Bu önemli topolojik invaryanta $X$ in *cinsi* (*genus*) denir.

**Teorem 2.39.** $\Gamma_0(N)$ kongrüans alt grubunun temel bölgesinin cinsi

$$g = 1 + \frac{\mu_0(N)}{12} - \frac{\varepsilon_\rho}{3} - \frac{\varepsilon_i}{4} - \frac{\sigma_\infty}{2}$$

dir. Burada

$$\varepsilon_\rho = \begin{cases} 0 & , 9 \mid N \\ \prod_{p \mid N}\left(1+\left(\frac{-3}{p}\right)\right) & , 9 \nmid N \end{cases} \quad , \quad \varepsilon_i = \begin{cases} 0 & , 4 \mid N \\ \prod_{p \mid N}\left(1+\left(\frac{-1}{p}\right)\right) & , 4 \nmid N \end{cases}$$

dir ve $\sigma_\infty = \sum_{t \mid N} \varphi\left(\left(t, N/t\right)\right)$ biçimindedir . $\varphi$-Euler fonksiyonu olmak üzere,

$$\left(\frac{-1}{\mathrm{p}}\right) := \begin{cases} 0 & , \quad \mathrm{p}=2 \\ 1 & , \quad \mathrm{p} \equiv 1 \bmod 4 \\ -1 & , \quad \mathrm{p} \equiv 3 \bmod 4 \end{cases} \quad , \quad \left(\frac{-3}{\mathrm{p}}\right) := \begin{cases} 0 & , \quad \mathrm{p}=3 \\ 1 & , \quad \mathrm{p} \equiv 1 \bmod 3 \\ -1 & , \quad \mathrm{p} \equiv 2 \bmod 3 \end{cases}$$

dir[25].■

$N \leq 25$ için elde edilen sonuçları verelim;

$g$=0 $N$=1, …, 10, 12, 13, 16, 18, 25 için;

$g$=1 $N$=11, 14, 15, 17, 19, 20, 21, 24 için;

$g$=2 $N$=22, 23 için;

## 2.7 Bazı Kongrüans Alt Gruplarının Normalliyenleri

**Teorem 2.40.** $\Gamma(N)$'nin $\mathrm{PSL}(2,\mathbb{R})$ deki normalliyeni $\Gamma$ dır.

**İspat.** $\aleph$, $\Gamma(N)$'nin $\mathrm{PSL}(2,\mathbb{R})$ deki normalliyeni olsun.

$$\Gamma(N) \lhd \Gamma < \mathrm{PSL}(2,\mathbb{R})$$

olduğundan, $\Gamma \leq \aleph$. Ancak $\aleph$, $\mathrm{PSL}(2,\mathbb{R})$ de döngüsel-olmayan bir Fuchsian grubunun normalliyenidir, dolayısıyla o da Fuchsian'dır. Fuchsian gruplarının sonlu indekse sahip tüm alt gruplarının bir sınıflandırmasını bulabiliriz, buradan $\Gamma$ nın herhangi bir Fuchsian grubunun sonlu indeksli bir alt grubuna karşılık gelmediği görülür. Diğer taraftan $\Gamma$ yı sonsuz-indeksli bir alt grup olarak içeren hiçbir $G$-Fuchsian grubu yoktur, aksi halde $G$ nin herhangi bir temel bölgesinin alanı 0 olurdu. Sonuç olarak $\Gamma \leq \aleph$ olamaz, $\Gamma = \aleph$ elde edilir.

**Teorem 2.41.** $\Gamma_1(N)$ nin $\mathrm{PSL}(2,\mathbb{Z})$ deki normalliyeni $\begin{cases}\Gamma_0(N), & N \neq 4 \\ \Gamma_0(N), & N = 4\end{cases}$ dir.

**İspat.** $\Gamma_1(N)$ nin $\mathrm{PSL}(2,\mathbb{Z})$ deki normalliyeni $\aleph$ olsun. $\Gamma_1(N) \lhd \Gamma_0(N)$ olduğundan $\Gamma_0(N) \subset \aleph$. Tersini gösterelim.

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \aleph \quad ve \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_1(N)$$

alalım. Buradan,

$$A \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} A^{-1} \in \Gamma_1(N)$$

ve daha açık yazıldığında,

$$\begin{pmatrix} ad - ac - bc & * \\ cd - c^2 - cd & -bc + ac + ad \end{pmatrix} \in \Gamma_1(N)$$

böylece,

$$\begin{pmatrix} 1 - ac & * \\ -c^2 & 1 + ac \end{pmatrix} \in \Gamma_1(N)$$

buna göre,

$$-c^2 \equiv 0 (\mathrm{mod}\, N) \text{ ve } 1 - ac \equiv 1 + ac \equiv 1 (\mathrm{mod}\, N)$$

ya da

$$-c^2 \equiv 0 (\mathrm{mod}\, N) \text{ ve } 1 - ac \equiv 1 + ac \equiv -1 (\mathrm{mod}\, N)$$

Birinci durumda $-c^2 \equiv 0 (\mathrm{mod}\, N)$ ve $ac \equiv 0 (\mathrm{mod}\, N)$ kongrüanslarından $N \mid c^2$ ve $N \mid ac$. Eğer $(a,N)=1$ olduğunu gösterirsek, $N \mid ac$ olduğundan $N \mid c$, dolayısıyla aradığımız neticeyi $A \in \Gamma_0(N)$ 'yi elde etmiş oluruz. Şüphesiz $(a,N) \neq 1$ ise $\exists\, p \in \mathbb{P}$ öyle ki $p \mid a$ ve $p \mid N$. $N \mid c^2$ olduğundan $p \mid c^2$ ve $p$-asal olduğundan $p \mid c$ olur. Ancak $p \mid a$ ve $p \mid c$ olması çelişkidir, çünkü $(a, c)=1$ dir.

İkinci durumda $1 - ac \equiv -1 (\mathrm{mod}\, N)$ ve $1 + ac \equiv -1 (\mathrm{mod}\, N)$ denklemlerinden $2 \equiv -2 (\mathrm{mod}\, N)$ elde edilir. Böylece $N \mid 4$ yani $N$=1, 2, veya 4 olur. Bu durumlarda $\Gamma_1(N) = \Gamma_0(N)$, dolayısıyla normalliyenlerin sırasıyla $\Gamma_0(1)$, $\Gamma_0(2)$ ve $\Gamma_0(4)$ e karşılık geldiği görülür.

**Teorem 2.42.** $\Gamma_0(N)$'nin PSL (2,$\mathbb{R}$) deki *normalliyeni*

$$\mathcal{N}or(N) := \left\{ \begin{pmatrix} ae & b/h \\ cN/h & de \end{pmatrix} : ade^2 - bcN/h^2 = e > 0 \right\}$$

dir. Buradaki bütün harfler tamsayı, $e \| N/h^2$ ve $h$, $h^2 | N$ şartını sağlayan 24'ün en büyük bölenidir. ($r\|s$ yani "$r$, $s$'nin bir tam bölenidir $:\Leftrightarrow \left(r, s/r\right) = 1$ dir) [1].

**Teorem 2.43.** $N \in \mathbb{Z}$ keyfi ve $N = 2^{\alpha_1} 3^{\alpha_2} p_3^{\alpha_3} \ldots p_n^{\alpha_n}$ asal çarpanlarına parçalanışı olsun. $\mathcal{N}or(N)$ nin $\hat{\mathbb{Q}}$ üzerinde transitif olarak hareket etmesi için gerek ve yeter şart

$$\alpha_1 \le 7,\ a_2 \le 3, ve\ \alpha_i \le 1 \ :\ i = 3,\ \ldots,\ n$$

olmasıdır [4].■

**Teorem 2.44.** $\rho$, $N/h^2$ nin farklı asal çarpanlarının sayısı olsun ve

$$\varepsilon_1 = \begin{cases} 1 \ ; & 2^2, 2^4, 2^6 \| N \\ 0 \ ; & \text{aksi takdirde} \end{cases}, \quad \varepsilon_2 = \begin{cases} 1 \ ; & 9 \| N \\ 0 \ ; & \text{aksi takdirde} \end{cases}$$

olmak üzere $\tau = \left(\frac{3}{2}\right)^{\varepsilon_1} . \left(\frac{4}{3}\right)^{\varepsilon_2}$ olsun. Bu takdirde $\Gamma_0(N)$' nin $\mathcal{N}or(N)$ deki indeksi

$|\mathcal{N}or(N) : \Gamma_0(N)| = 2^\rho h^2 \tau$ dur [22].■

**Lemma 2.45.** Bir $\frac{k}{s} \in \mathbb{Q}$ $(s \neq 0)$, $(k, s) = 1$ rasyonel sayısı verildiğinde $A\left(\frac{k}{s}\right) = \left(\frac{k_1}{s_1}\right)$, $s_1 | N$ koşulunu sağlayan bir $A \in \Gamma_0(N)$ vardır [1].

**Lemma 2.46.** $d_1 | N$ ve $(a_1, d_1) = (a_2, d_1) = 1$ olmak üzere $A\begin{pmatrix} a_1 \\ d_1 \end{pmatrix} = \begin{pmatrix} a_2 \\ d_1 \end{pmatrix}$ olsun. Bu takdirde $t = \left( d_1, \frac{N}{d_1} \right)$ olmak üzere $a_1 \equiv a_2 \bmod t$ dir [1].

**Lemma 2.47.** $d \mid N$ ve $(a_1,d)=(a_2,d)=1$ olsun. Bu durumda $t=\left(d,\dfrac{N}{d}\right)$ olmak üzere

$$\begin{pmatrix} a_1 \\ d \end{pmatrix} \text{ ve } \begin{pmatrix} a_2 \\ d \end{pmatrix} \ \Gamma_0(N) \text{ altında eşleniktir} \Leftrightarrow a_1 \equiv a_2 \mod t$$

dir [1].

**Teorem 2.48.** $d \mid N$ olsun. $\dfrac{a}{d}$ nin $\Gamma_0(N)$ ile hareketiyle oluşan yörünge

$$\begin{pmatrix} a \\ d \end{pmatrix} = \left\{ \frac{x}{y} \in \hat{\mathbb{Q}} : (N,y)=d,\ a \equiv x\frac{y}{d} \mod\left(d,\frac{N}{d}\right) \right\}$$

kümesidir. Üstelik $\begin{pmatrix} a \\ d \end{pmatrix}$, $d \mid N$ yörüngelerinin sayısı $Y=\sum_{d \mid N} \varphi\left(\left(d, {}^{N}\!/_{d}\right)\right)$, $\varphi$-Euler fonkiyonudur [4].

## 2.8 İmprimitif Hareket

**Tanım 2.49. (i)** $X \neq \varnothing$ bir küme olsun. $\xi : X \to X$ bire-bir, örten ise $\xi$'ye $X$' in bir *permütasyonu* denir. $X$ in tüm *permütasyonlarının kümesi* $S^X$ ile gösterilir.

**(ii)** $\xi_1, \xi_2 \in S^X$ ise $\xi_1 \circ \xi_2 \in S^X$ olduğu açıktır. $S^X$ grubuna $X$ üzerinde *simetrik grup* denir. $S^X$ in alt gruplarına da $X$ üzerinde *permütasyon grupları* denir.

**Tanım 2.50.** $G$, $X$ üzerinde bir permütasyon grubu olsun. Bu takdirde $G$, $X$ üzerinde hareket eder. Gerçekten $g \in G$ ise g:$G \to G$ bire-bir ve örten bir dönüşümdür. Bu durumda $gx := g(x)$ olarak alınırsa $(g_1 g_2)x = g_1(g_2 x)$ ve $1x = x$ olduğu açıktır. Bu harekete $G$ nin $X$ üzerindeki *doğal hareketi* denir ve "$(G,X)$ *permütasyon grubu*" ifadesi kullanılır.

**Tanım 2.51.** $(G,X)$ bir transitif permütasyon grubu ve "$\approx$", $X$ üzerinde bir denklik bağıntısı olsun. $x,y \in X$ için $x \approx y$ olduğunda $\forall g \in G$ için $g(x) \approx g(y)$ ise "$\approx$" bağıntısına bir *G-invaryant denklik bağıntısı* denir.

**Tanım 2.52.** Bir $G$-invaryant denklik bağıntısının denklik sınıflarına *denklik bağıntısının blokları* denir.

Bu tanıma göre;

i) *Özdeşlik bağıntısı*: $x \approx y \Leftrightarrow x = y$

ii) *Evrensel bağıntı*: $\forall x,y \in X$ için $x \approx y$

bağıntılarının $G$-invaryant denklik bağıntıları olduğu açıktır. Bu bağıntılara *aşikâr* (*trivial*) *bağıntılar* adı verilir.

**Tanım 2.53.** $X$ üzerinde yukarıdaki aşikâr bağıntıların dışında bir $G$-invaryant denklik bağıntısı yoksa $(G,X)$'e *primitif* (*ilkel*), aksi halde *imprimitif* (*ilkel olmayan*) denir [6].

**Lemma 2.54.** $(G,X)$ bir transitif permütasyon grubu, $H \le G$ ve bir $\alpha \in X$ için $G_\alpha \le H$ olsun. Bu takdirde $g \in G$, $h \in H$ için

$$g(\alpha) \approx gh(\alpha))$$

bir $G$-invaryant denklik bağıntısıdır. Ayrıca

$$" \approx " \text{özdeşlik bağıntısıdır} \Leftrightarrow H = G_\alpha \text{ , } " \approx " \text{ evrensel bağıntıdır} \Leftrightarrow H=G$$

dir [6].

**Lemma 2.55.** $(G,X)$ bir transitif permütasyon grubu olsun. $(G,X)$ hareketi primitiftir $\Leftrightarrow$ $\forall x \in X$ için $G_x$, $X$ in maksimal bir alt grubudur [6].

**Teorem 2.56.** $(G,X)$ bir transitif permütasyon grubu olsun. $G_\alpha \lneq H \lneq G$ ise

$$g(\alpha) \approx h(\alpha) \Leftrightarrow g^{-1}h \in H$$

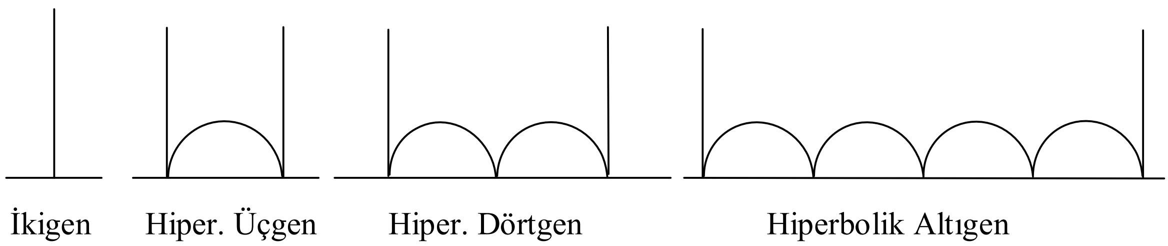
iyi tanımlı bir $G$-invaryant denklik bağıntısıdır. Denklik sınıflarının sayısı da $|G:H|$ indeksidir [6].

## 2.9 Graf Teori

**Tanım 2.57.** $X \neq \varnothing$ bir küme, $\Delta \subset X \times X$ bir bağıntı olsun. $G=(X,\Delta)$ ikilisine bir *graf* (graph) denir. $X$ in elemanlarına *grafın köşeleri* ve $\Delta$'nın elemanlarına *grafın kenarları* adı verilir.
$(a,b)\in\Delta$ ise bu durum $a\rightarrow b$ ile gösterilir. Eğer $(a,b)\in\Delta$ veya $(b,a)\in\Delta$ ise $a$ ile $b$ *bir kenar ile bağlanmıştır* denir. Bu durumda $a$ ve $b$ ye *komşu köşeler* denir.

**Tanım 2.58.** $G=(X,\Delta)$ bir graf ve $A\subset X$ olsun. $G' = (A, \Delta \cap A \times A)$ grafına *köşe kümesi A olan G nin bir alt grafı* adı verilir.

**Tanım 2.59.** $a = a_0, a_1, \ldots, a_n = b$ bir $G$-grafının köşelerinin bir dizisi olsun. Eğer $1 \leq i \leq n$ için $a_{i-1}$ ve $a_i$ bir kenar ile bağlanmışlarsa $a$'dan $b$'ye *n-uzunluğunda bir yol vardır* denir.
Eğer $a=b$ ve $a_0, a_1, \ldots, a_{n-1}$ köşelerinin tümü farklı ise bu yola *n-kenarlı bir devre* denir. Ayrıca $a_i, a_{i+1}$ ikilileri için $a_i \rightarrow a_{i+1}$ ise bu devreye *yönlenmiş bir devre* (*circuit*) denir.
Üç kenarlı bir devreye bir *üçgen*, dörtkenarlı bir devreye bir *dörtgen* ve altı kenarlı bir devreye bir *altıgen* denir.




Şekil 2.3 Devreler

**Tanım 2.60.** $G=(X,\Delta)$ bir graf olsun. $X$ üzerinde bir $\approx$-bağıntısını şöyle tanımlayalım:

"$a\approx b$ :$\Leftrightarrow$ $a=b$ veya $a$'dan $b$'ye bir yol vardır ".

Açık olarak, $\approx$ bir denklik bağıntısıdır.

**Tanım 2.61. (i)** $X$ in kendisi bu $\approx$-bağıntısı altında denklik sınıfı ise $G$-grafına *bağlantılıdır* denir.

**(ii)** Eğer $X_1$, $\approx$-bağıntısı altında bir denklik sınıfı ise $(X_1, \Delta \cap X_1 \times X_1)$ bağlantılı bir graftır ve bu grafa $G$-grafının *bağlantılı bileşeni* denir.

İki grafın köşeleri arasında 1-1 ve örten bir dönüşüm mevcut ve bu dönüşüm komşu köşeleri, komşu köşelere gönderiyorsa bu iki grafa *izomorf graflar* denir [29].

# BÖLÜM III

## $\Gamma^0(N)$ KONGRÜANS ALT GRUBUNUN ALT YÖRÜNGESEL GRAFLARI

$N$ pozitif tamsayı olmak üzere $\Gamma$ -modüler grubun bir alt grubu olan

$$\Gamma^0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : b \equiv 0 \bmod N \right\}$$

kongrüans grubunu göz önüne alalım ve $\Gamma(N)$ye 0-ın sabitleyinini eklemekle oluşan grubu $\Gamma^*(N)$ ile gösterelim. Yani

$$\Gamma^*(N) := \left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \Gamma(N) \right\rangle$$

olsun. Buna göre

$$\Gamma^*(N) = \left\{ \begin{pmatrix} 1+aN & bN \\ c & 1+dN \end{pmatrix} : a,b,c,d \in \mathbb{Z} \right\}$$

tir.

### 3.1 $\Gamma^0(N)$ nin $\hat{\mathbb{Q}}$ Üzerindeki Hareketi

$(x, y) = 1$ olan $\forall x, y \in \mathbb{Z}$ sayıları için $\hat{\mathbb{Q}}$- nın her bir elemanı $\dfrac{x}{y}$ indirgenmiş formu ile verilir. $\dfrac{x}{y} = \dfrac{-x}{-y}$ olduğundan bu gösterim tek türlü değildir. Burada $0 = \dfrac{0}{1} = \dfrac{0}{-1}$ dır. $\Gamma$ -nın $\hat{\mathbb{Q}}$ üzerindeki hareketi, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ olmak üzere,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : \begin{pmatrix} x \\ y \end{pmatrix} \to \frac{ax+by}{cx+dy}$$

şeklindedir

**Teorem 3.1.** $\Gamma^0(N)$ nin $\hat{\mathbb{Q}}$ üzerindeki hareketi transitif değildir.

**İspat.** $\begin{pmatrix} a & bN \\ c & d \end{pmatrix} \in \Gamma^0(N)$ olsun. Bu takdirde

$$\begin{pmatrix} a & bN \\ c & d \end{pmatrix}\begin{pmatrix} N \\ 1 \end{pmatrix} = \frac{aN+bN}{cN+d}$$

indirgenmiş formdadır ve böylece $N$, $\Gamma^0(N)$ altında $N+1$ ' e resmedilemez. ■

Bu durumda $\Gamma^0(N)$ -nin transitif olduğu $\hat{\mathbb{Q}}$-nın bir maksimal alt kümesini bulmalıyız. Bunun için ilk önce aşağıdaki teoremi verelim.

**Lemma 3.2.** $a,b \in \mathbb{Z}$ ve $(a,b)=1$ olsun. Bu takdirde $c \in \mathbb{Z}$ ve $c \neq 0$ ise $(a+bx,\ c) = 1$ olacak şekilde bir $x \in \mathbb{Z}$ tamsayısı vardır.

**İspat.** Eğer $c$ sayısının her asal böleni $a$ sayısını bölüyorsa $(x,c)=1$ şartını sağlayan $x \in \mathbb{Z}$ tamsayısı $(a+bx,\ c) = 1$ koşulunu sağlar.

Şimdi $p \mid c$ ve $p \nmid a$ olan bir $p$ asal sayısı mevcut olsun. Bu durumda

$$x := \prod_{\substack{p\mid c \\ p\nmid a}} p$$

olarak alınırsa $(a+bx,\ c) = 1$ olduğu kolayca gösterilir. ■

**Teorem 3.3.** $(k,s)=1$ olmak üzere $\frac{k}{s}$ keyfi rasyonel sayısı verilsin. Bu $A\left(\frac{k}{s}\right) = A\left(\frac{k_1}{s_1}\right)$ ve $k_1 = (k,N)$ olacak şekilde bir $A \in \Gamma^0(N)$ vardır.

**İspat.** $k_1 = (N,k)$ olsun. Bu durumda $(k,\ Ns) = k_1$ ve dolayısıyla $\left(\frac{Ns}{k_1}, \frac{k}{k_1}\right) = 1$ dir. Buna göre

$$\frac{k}{k_1}a_0 + \frac{Ns}{k_1}b_0 = 1$$

olacak biçimde $a_0, b_0 \in \mathbb{Z}$ tam sayıları vardır. Bu durumda açıkça $\left(\dfrac{Ns}{k_1}, a_0\right)$ = 1'dir. Lemma 3.2'e göre

$$\left(a_0 - \frac{Ns}{k_1}m, N\right) = 1$$

olacak biçimde $m \in \mathbb{Z}$ tamsayısı vardır.

$$a = a_0 - \frac{Ns}{k_1}m \text{ ve } b = b_0 + \frac{k}{k_1}m$$

olarak alınırsa $\dfrac{k}{k_1}a + \dfrac{Ns}{k_1}b = 1$ elde edilir. Çünkü

$$\frac{Ns}{k_1}\left(b_0 + \frac{k}{k_1}m\right) + \frac{k}{k_1}\left(a_0 - \frac{Ns}{k_1}m\right) = \frac{Ns}{k_1}b_0 + \frac{k}{k_1}a_0 = \frac{1}{k_1}\left(Nsb_0 + ka_0\right) = 1$$

dir. Böylece $(a, N) = 1$ ve $(b, a) = 1$ olduğundan $(bN, a) = 1$ olur. Dolayısıyla $ad - bcN =$ 1 olacak biçimde $c, d \in \mathbb{Z}$ tamsayıları vardır. Böylece

$$A = \begin{pmatrix} a & bN \\ c & d \end{pmatrix} \in \Gamma^0(N) \text{ ve } A\left(\frac{k}{s}\right) = A\left(\frac{k_1}{s_1}\right)$$

bulunur. ■

**Teorem 3.4.** $a_1 \mid N$ ve $(a_1, d_1) = (a_1, d_2) = 1$ olsun. Bu durumda $\dfrac{a_1}{d_1}$ ve $\dfrac{a_1}{d_2}$, $\Gamma^0(N)$ altında eşleniktir $\Leftrightarrow t = \left(a_1, \dfrac{N}{a_1}\right)$ için $d_1 \equiv d_2 \pmod{t}$ dir.

**İspat.** $\dfrac{a_1}{d_1}$ ve $\dfrac{a_1}{d_2}$ $\Gamma^0$ $(N)$ altında eşlenik olsunlar. Buna göre

$$A(z) = \frac{az + bN}{cz + d} \text{ ve } ad - bcN = 1$$

olmak üzere $A\left(\dfrac{a_1}{d_1}\right) = \dfrac{a_1}{d_2}$ olacak şekilde $A \in \Gamma^0(N)$ vardır. Buradan

$$\begin{pmatrix} a & bN \\ c & d \end{pmatrix}\begin{pmatrix} \frac{a_1}{d_1} \end{pmatrix} = \frac{aa_1 + bNd_1}{ca_1 + dd_1} = \frac{a_1}{d_2}$$

bulunur. Böylece

$$aa_1 + bNd_1 = \varepsilon\, a_1 \text{ ve } ca_1 + dd_1 = \varepsilon \,.\, d_2$$

olacak biçimde $\varepsilon \in \{1,-1\}$ vardır. $aa_1 + bNd_1 = \varepsilon\, a_1$ olduğundan

$$\frac{aa_1}{a_1} + \frac{bNd_1}{a_1} = \frac{\varepsilon a_1}{a_1}$$

olup $a \equiv \varepsilon\, (\mathrm{mod}\, t)$ ve $ad - bcN = 1$ den $ad \equiv 1 \left(\mathrm{mod}\, t\right)$ bulunur. Buradan $d\varepsilon \equiv 1 \left(\mathrm{mod}\ t\right)$ olur. $\varepsilon \in \{1,-1\}$ olduğundan $d \equiv \varepsilon \left(\mathrm{mod}\ t\right)$

$$ca_1 + dd_1 = \varepsilon d_2 \text{ ve } t = \left(a_1, \frac{N}{a_1}\right)$$

olduğundan

$$dd_1 \equiv \varepsilon d_2\ (\mathrm{mod}\, t)$$

bulunur. Buradan ve $d \equiv \varepsilon \left(\mathrm{mod}\ t\right)$ den

$$d_1 \equiv d_2 \left(mod\ t\right)$$

olduğu görülür.

$\Leftarrow$ $m = \dfrac{N}{a_1}$ olsun. $t = (m, a_1)$ ve $(d_1\ d_2, a_1) = 1$ olduğu dikkate alınırsa $(m\, d_1\ d_2, a_1) = t$ olduğu görülür. Diğer yandan $d_1 \equiv d_2 \left(mod\ t\right)$ olduğundan $t \,|\left(d_2 - d_1\right)$ dir ve dolayısıyla

$$m\, d_1\ d_2 x + a_1 y = d_2 - d_1$$

denklemi bir çözüme sahiptir. $k, s \in \mathbb{Z}$ bir çözüm olsun. Buna göre

$$md_1 d_2 k + d_1 + a_1 s = d_2$$

dir. Böylece

$$d_1\left(md_2 k + 1\right) + a_1 s = d_2$$

elde edilir.

$$b = ma_1 k \text{ ve } a = 1 - md_1 k$$

alınırsa

$$bd_1 + aa_1 = a_1 \quad \text{ve} \quad N \mid b$$

sağlanır. Ayrıca

$$d = 1 + md_2k \quad \text{ve} \quad c = s$$

alınırsa

$$dd_1 + ca_1 = d_2$$

olur. Böylece $A(z) = \dfrac{az+b}{cz+d}$ olmak üzere

$$\det A = ad - bc = d\left(1 - md_1k\right) - c\left(ma_1k\right) = d - mk\left(dd_1 + ca_1\right) = d - md_2k = 1$$

dir. $N \mid b$ olduğundan $A \in \Gamma^0\left(N\right)$ ve $A\left(\dfrac{a_1}{d_1}\right) = \dfrac{a_1}{d_2}$ elde edilir.■

Yukarıdaki iki teoremden $\Gamma^0\left(N\right)$ nin yörüngelerinin kümesi aşağıdaki gibi verilir.

**Teorem 3.5.** $a|N$ olsun. Bu takdirde $\dfrac{a}{b} - nin$ $\mathbf{\Gamma}^0(N)$ ile hareketiyle oluşan yörünge

$$\begin{pmatrix} a \\ b \end{pmatrix} = \left\{ \frac{x}{y} \in \hat{\mathbb{Q}} : (N, x) = a,\ b \equiv y\frac{x}{a} \bmod\left(a,\ \frac{N}{a}\right) \right\}$$

kümesidir. Üstelik $\Gamma^0(N)$ altında bu yörüngelerin sayısı $\varphi\left(a, \dfrac{N}{a}\right)$ dır. Burada $\varphi$-Euler fonksiyonudur.■

**Not:** Çalışmanın bundan sonraki kısımlarında hesaplamalarda kolaylık olsun diye $N = p$ asal alınacaktır.

**Sonuç 3.6.** $\Gamma^0(p) -$ nin yörüngeleri $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ *ve* $\begin{pmatrix} p \\ 1 \end{pmatrix}$ dir.

**İspat:** $a|p$ ise $a$=1 ve a=$p$ dir. $a$ =1 ise $\begin{pmatrix} 1 \\ b \end{pmatrix}$ olur. Buradan

$$b \equiv y\ \frac{x}{1} \bmod\ (1, p/1) \Rightarrow b \equiv 1 \bmod(1)$$

olup $\begin{pmatrix}1\\1\end{pmatrix}$ yörüngesi elde edilir. $a$=p ise durum benzerdir.■

**Lemma 3.7.** $\Gamma^0(p)-$de $0-$ın sabitleyeni sonsuz devirli bir gruptur.

**İspat:** $T=\begin{pmatrix}a & bp\\c & d\end{pmatrix}\in\Gamma^0(p)$ $ve$ $T\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}$ olsun. Bu takdirde

$$\begin{pmatrix}a & bp\\c & d\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}bp\\d\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}$$

den $bp$=0 ve $d$=1 olur. $p$ asal olduğundan $b$=0 ve det T=$ad-bc=1$ olduğundan $a=1$ olur. Buradan $T=\begin{pmatrix}1 & 0\\1 & 1\end{pmatrix}$ elde edilir. Buna göre $\Gamma^0(p)_0=\left\langle\begin{pmatrix}1 & 0\\1 & 1\end{pmatrix}\right\rangle dir.$ ■

Teorem 2.56 da $G_\alpha=\Gamma^0(p)_0$, $H=\Gamma^*(p)$, $G=\Gamma^0(p)$ ve $X=\hat{\mathbb{Q}}$ alınırsa açıkça

$$\Gamma^0(p)_0<\Gamma^*(p)<\Gamma^0(p)$$

olur. Buna göre 0-ın sabitleyeni $\Gamma^0(p)_0$, $\Gamma^0(p)$ de maksimal bir alt grup değildir. O halde Lemma 2.55' e göre aşağıdaki sonucu verebiliriz.

**Sonuç 3.8.** $\left(\Gamma^0(p),\hat{\mathbb{Q}}\right)$ bir imprimitif permütasyon grubudur. ■

$\Gamma^0(p)$, $\begin{pmatrix}p\\1\end{pmatrix}$ yörüngesi üzerinde transitif ve imprimitif olarak hareket eder. Böylece

"$\approx$",$\begin{pmatrix}p\\1\end{pmatrix}$ yörüngesi üzerinde $\Gamma^*(p)$ ile indirgenmiş $\Gamma^0(p)$-invaryant denklik bağıntısı

Teorem 2.56 ya göre $g_1,g_2\in\Gamma^0(p)$ olmak üzere

$$g_1(0)\approx g_2(0)\Leftrightarrow g_1^{-1}g_2\in\Gamma^*(p)$$

şeklindedir.

$$v=\frac{b_1p}{d_1},\ w=\frac{b_2p}{d_2}\in\begin{pmatrix}p\\1\end{pmatrix}$$

ise bu durumda

$$g_1 = \begin{pmatrix} a_1 & b_1 p \\ c_1 & d_1 \end{pmatrix},\ g_2 = \begin{pmatrix} a_2 & b_2 p \\ c_2 & d_2 \end{pmatrix} \in \mathbf{\Gamma}^0(p)$$

elemanları için $g_1(0) = v \;\; ve \;\; g_2(0) = w$ dır. Buna göre

$$g_1^{-1} g_2 = \begin{pmatrix} d_1 & -b_1 p \\ -c_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 p \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_2 d_1 - b_1 c_2 p & d_1 b_2 p - b_1 p d_2 \\ -c_1 a_2 + a_1 c_2 & -c_1 b_2 p + a_1 d_2 \end{pmatrix} \in \Gamma^*(p)$$

olacağından

$$a_2 d_1 \equiv 1 \bmod p \;\; ve \;\; a_1 d_2 \equiv 1 \bmod p$$

olur. Buradan

$$d_1 a_1 d_2 \equiv d_1 \bmod p$$

ve determinanttan

$$a_1 d_1 - b_1 c_1 p = 1 \text{ yani } a_1 d_1 \equiv 1 \bmod p$$

olduğundan

$d_2 \equiv d_1 \bmod p$ elde edilir.

Böylece invaryant denklik bağıntısı

$$v \approx w \Leftrightarrow d_1 \equiv d_2 \bmod p \tag{3.1}$$

olarak bulunur.

İmpirimitif hareket sonucunda $"\approx"$ altında denklik sınıflarının sayısı

$$\eta(p) = \left| \Gamma^0(p) : \Gamma^*(p) \right|$$

dir. $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^p \in \Gamma(p)$ dir. Örneğin

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \in \Gamma(2)$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \in \Gamma(3)$$

tür. Buna göre

$$\left| \Gamma^*(p) : \Gamma(p) \right| = p$$

dir. [25] ten

$$\left|\Gamma:\Gamma(N)\right| = N^3\prod_{p/N}\left(1-\frac{1}{p^2}\right)$$

ve

$$\left|\Gamma:\Gamma^0(N)\right| = N\prod_{p/N}\left(1+\frac{1}{p}\right)$$

olduğunu biliyoruz. $N=p$ için hesaplama yapılırsa

$$\left|\Gamma:\Gamma(p)\right| = \left|\Gamma:\Gamma^0(p)\right|.\left|\Gamma^0(p):\Gamma^*(p)\right|.\left|\Gamma^*(p):\Gamma(p)\right|$$

den

$$\left|\Gamma^0(p):\Gamma^*(p)\right| = p-1$$

bulunur. Buna göre

$$\begin{pmatrix} p \\ 1 \end{pmatrix} = \begin{bmatrix} p \\ 1 \end{bmatrix} \cup \begin{bmatrix} p \\ 2 \end{bmatrix} \cup \ldots \cup \begin{bmatrix} p \\ P-1 \end{bmatrix}$$

dir. (3.1) bağıntısından [0]- bloğu

$$\begin{bmatrix} p \\ 1 \end{bmatrix} = \left\{ \frac{xp}{1+yp} : x, y \in Z \right\} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = [0]$$

şeklindedir.

## 3.2 Alt Yörüngesel Graflar

**Tanım 3.9.** $(G,X)$ bir transitif permütasyon grubu olsun. $G$ nin $X\times X$ üzerindeki hareketini $g\in G$ olmak üzere

$$g:(\alpha,\beta)\rightarrow(\ g(\alpha),\ g(\beta)\ )\ ,\ (\alpha,\beta)\in X\times X$$

ile tanımlayalım. Bu hareketin yörüngelerine $G$ nin *alt yörüngeleri* denir. $(\alpha,\beta)$ yı içeren alt yörüngeyi $\boldsymbol{O}(\alpha,\beta)$ ile gösterelim.

$\boldsymbol{O}(\alpha,\beta)$ dan bir $G(\alpha,\beta)$ *alt yörüngesel grafını* aşağıdaki gibi elde edelim:
$G(\alpha,\beta)$ nın köşeleri $X$ in elemanlarıdır. Yukarıda da verildiği gibi, $x$, $y\in X$ noktaları için $(x,\ y)\in\boldsymbol{O}(\alpha,\beta)$ ise $x$ den $y$ ye yönlenmiş bir kenar vardır ve bu durum $x\rightarrow y$ olarak gösterilir. Kısaca $\gamma\rightarrow\delta$ nın $G(\alpha,\beta)$ da bir kenar olması için gerek ve yeter şart bir

$T \in G$ vardır öyle ki $T(\alpha)=\gamma$ ve $T(\beta)=\delta$ dır. Bu kenarı $\mathcal{U}$-üst yarı düzleminde bir hiperbolik geodezik olarak çizebiliriz.

Açık olarak $\boldsymbol{O}(\beta,\alpha)$ da alt yörüngedir. $\boldsymbol{O}(\alpha,\beta) = \boldsymbol{O}(\beta,\alpha)$ veya $\boldsymbol{O}(\alpha,\beta) \neq \boldsymbol{O}(\beta,\alpha)$ dır.

**(i)** $\boldsymbol{O}(\alpha,\beta) = \boldsymbol{O}(\beta,\alpha)$ ise $G(\alpha,\beta) = G(\beta,\alpha)$ dır ve bu graf karşılıklı yönlendirilmiş kenarlardan oluşur. Yani, $G(\alpha,\beta)$ grafında $x \to y$ ise yine $G(\alpha,\beta)$ grafında $y \to x$ dir. Bu durumda $G(\alpha,\beta)$ grafına *kendisiyle eşleşmiş graf* denir.

**(ii)** $\boldsymbol{O}(\alpha,\beta) \neq \boldsymbol{O}(\beta,\alpha)$ ise $G(\beta,\alpha)$ , $G(\alpha,\beta)$ nın oklarının ters yönlendirilmişlerinden ibarettir. Yani, $G(\alpha,\beta)$ grafında $x \to y$ ise $G(\beta,\alpha)$ grafında $y \to x$ dir. Bu durumda ise $G(\alpha,\beta)$ ve $G(\beta,\alpha)$ graflarına *birbirleriyle eşleşmiş graflar* denir.

$\boldsymbol{O}(\alpha,\alpha)=\{(x,x):\, x \in X\}$, $X \times X$ in köşegenidir. $\boldsymbol{O}(\alpha,\alpha)$ ya uygun $G(\alpha,\alpha)$ alt yörüngesel grafına *aşikâr alt yörüngesel graf* denir. Bu graf her bir köşesi $\alpha \in X$ olan bir sıçramadan ibarettir.

$G$, $X$ üzerinde transitif olarak hareket ettiğinden blokları transitif olarak permüte eder, dolayısıyla alt grafların hepsi izomorftur.

Yukarıda özetlenen fikirler ilk defa Sims tarafından ortaya konmuş, daha sonra Biggs ve White sonlu gruplar için uygulamaları üzerinde durmuşlar, ardında da Tsuzuku bu düşünceleri bir kitapta toparlanmıştır.

**Tanım 3.10.** Bir yönlendirilmiş devre, $m \geq 3$ ve $v_1, v_2, ..., v_m$ farklı köşeleri için

$$v_1 \to v_2 \to ... \to v_m \to v_1$$

şeklindedir.

$m=3$ ise $v_1 \to v_2 \to v_3 \to v_1$ -e bir *üçgen* denir.

$m=2$ ise $v_1 \to v_2 \to v_1$ -e *kendisi ile eşleşmiş kenar* denir.

Hiçbir devre içermeyen grafa ise bir *orman* adı verilir.

**Önerme 3.11.** $G'$, $(G,X)$ transitif permütasyon grubu için bir alt yörüngesel graf olsun. Bu takdirde

**(i)** $G$, $G'$-nin otomorfizmalarının bir grubu olarak hareket eder.

**(ii)** $G$, $G'$-nin köşeleri üzerinde transitif olarak hareket eder.

**(iii)** Eğer $G'$ kendisiyle eşleşmiş ise bu takdirde $G$, $G'$-nin ardışık köşelerinin sıralı çiftleri üzerinde transitif olarak hareket eder.

**(iv)** Eğer $G'$ kendisiyle eşleşmiş değil ise bu takdirde $G$, $G'$-nin kenarları üzerinde transitif olarak hareket eder.

Bu bölümde $\Gamma^0(p)$ nin alt yörüngesel graflarını belirleyeceğiz. $\Gamma^0(p)$, $\begin{pmatrix} p \\ 1 \end{pmatrix}$ yörüngesi üzerinde transitif olduğundan her bir alt yörünge $v \in \begin{pmatrix} p \\ 1 \end{pmatrix}$ için $(0,v)$ ikilisini ihtiva eder öyle ki $(u,p) = 1$ olmak üzere $v = \frac{p}{u}$ dur. Bu altyörüngeyi $O_{p,u}$ ile ve buna karşılık gelen $G(0,v)$ alt yörüngesel grafını da $G_{p,u}$ ile göstereceğiz. $\Gamma^0(p)$ yörüngeler üzerinde transitif olarak hareket ettiğinden blokları transitif olarak permüte eder. Dolayısıyla alt grafların hepsi izomorftur. Böylece hesapları sadece [0]- bloğu için yapmak yeterlidir.

**Teorem 3.12.** $\frac{r}{s}, \frac{x}{y} \in \begin{pmatrix} p \\ 1 \end{pmatrix}$ olsun. Bu taktirde $\frac{r}{s} \to \frac{x}{y}$ 'nin $G_{p,u}$' da bir kenar olması için gerek ve yeter şart

**(i)** $x \equiv ur \pmod p : r \equiv 0 \pmod p,\ y \equiv us \pmod p,\ ry - sx = -p$ veya

**(ii)** $x \equiv -ur \pmod p : r \equiv 0 \pmod p,\ y \equiv -us \pmod p,\ ry - sx = p$

olmasıdır.

**İspat.** $\frac{r}{s} \to \frac{x}{y}$, $G_{p,u}$' da bir kenar olsun. Bu taktirde

$$T(0) = \frac{r}{s} \quad \text{ve} \quad T\left(\frac{p}{u}\right) = \frac{x}{y}$$

olacak şekilde bir $T \in \Gamma^0(p)$ vardır

$$T\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}a & pb\\c & d\end{pmatrix}.\begin{pmatrix}0\\1\end{pmatrix} = \frac{pb}{d} = \frac{r}{s}$$

Buradan $pb = \mathrm{r}$ ve $s = d$ şeklindedir. $r \equiv 0 \bmod p$ dir. Ayrıca

$$T\begin{pmatrix}p\\u\end{pmatrix} = \begin{pmatrix}a & pb\\c & d\end{pmatrix}.\begin{pmatrix}p\\u\end{pmatrix} = \left(\frac{ap+pbu}{cp+du}\right) = \frac{x}{y}$$

olduğundan

$$x = \pm(ap+pbu) \text{ ve } y = \pm(cp+du)$$

elde edilir. Sonuç olarak $i\,, j = 0{,}1$ olmak üzere

$$\begin{pmatrix}a & pb\\c & d\end{pmatrix}.\begin{pmatrix}0 & p\\1 & u\end{pmatrix} = \begin{pmatrix}pb & ap+pbu\\d & cp+du\end{pmatrix} = \begin{pmatrix}(-1)^j.r & (-1)^i x\\(-1)^j.s & (-1)^i.y\end{pmatrix} \tag{3.2}$$

elde edilir.

Eğer $i = j = 0$ ise bu takdirde $x \equiv ur \bmod p$, $y \equiv us \bmod p$ ve (3.2) den determinant alınırsa $ry - sx = -p$ elde edilir.

Benzer şekilde, $i = 1$ ve $j = 0$ ise bu takdirde $x \equiv -ur \bmod p$, $y \equiv -us \bmod p$ ve (3.2) den determinant alınırsa $ry - sx = p$ elde edilir.

Şimdi tersine (i) şartı sağlansın. Yani

$$x \equiv ur\ (\bmod\ p) : r \equiv 0(\bmod\ p),\ y \equiv us(\ \bmod\ p),\ ry - sx = -p$$

olsun. Bu takdirde

$$x = ur + kp \text{ ve } y = us + \ell p$$

olacak şekilde $k, \ell \in \mathbb{Z}$ tamsayıları vardır. Bu değerler $ry - sx = -p$ eşitliğinde yazılırsa

$$ry - sx = r(us + \ell p) - s(ur + kp) = -p$$

olup buradan

$$p(r\ell - ks) = -p,$$

yani $ks-r\ell=1$ bulunur. Buradan ve $r\equiv 0\left(\text{mod } p\right)$ olduğundan $\begin{pmatrix} k & r \\ \ell & s \end{pmatrix}\in\Gamma^0(p)$ olur

ve bu dönüşüm; 0'ı $\left(\frac{r}{s}\right)$'ye $\frac{p}{u}$' yu $\frac{x}{y}$'ye resmeder.

Benzer şekilde eğer (ii) geçerli ise

$$x=-ur+mp \text{ ve } y=-us+np$$

olacak şekilde $m,n\in\mathbb{Z}$ tamsayıları vardır. Bu değerler $ry-sx=p$ eşitliğinde yazılırsa

$$ry-sx=r\left(-us+np\right)-s\left(-ur+mp\right)=p$$

olup buradan

$$p\left(rn-ms\right)=p,$$

yani $-ms+rn=1$ bulunur. Buradan ve $r\equiv 0\left(\text{mod } p\right)$ olduğundan $\begin{pmatrix} m & -r \\ n & -s \end{pmatrix}\in\Gamma^0(p)$

olur ve bu dönüşüm de 0'ı $\left(\frac{r}{s}\right)$'ye $\frac{p}{u}$' yu $\frac{x}{y}$'ye resmeder.■

**Teorem 3.13.** $uv\equiv -1 \text{ mod } p$ ise bu takdirde $G_{p,u}$ ile $G_{p,v}$ eşleşmiş alt yörüngesel graflardır.

**İspat. 1. Durum** $x\equiv ur\left(\text{mod } p\right): r\equiv 0\left(\text{mod } p\right)$, $y\equiv us\left(\text{ mod } p\right)$, $ry-sx=-p$ ise, buradan

$$\left.\begin{array}{l} vx\equiv vur\left(\text{mod } p\right) \Rightarrow r\equiv -vx\left(\text{mod } p\right): x\equiv 0\left(\text{mod } p\right) \\ uy\equiv uvs\left(\text{mod } p\right) \Rightarrow s\equiv -uy\left(\text{mod } p\right) \end{array}\right\} \text{ve } sx\text{-}ry=1$$

olduğundan $\frac{x}{y}\rightarrow\frac{r}{s}\in G_{p,v}$ olur. Buradan $G_{p,u}$ ile $G_{p,v}$ eşleşmiştir.

**2. Durum** $x\equiv -ur\left(\text{mod } p\right): r\equiv 0\left(\text{mod } p\right)$, $y\equiv -us\left(\text{ mod } p\right)$, $ry-sx=p$ ise, buradan

$$\left.\begin{array}{l} vx\equiv -vur\left(\text{mod } p\right) \Rightarrow r\equiv vx\left(\text{mod } p\right): x\equiv 0\left(\text{mod } p\right) \\ uy\equiv -uvs\left(\text{mod } p\right) \Rightarrow s\equiv uy\left(\text{mod } p\right) \end{array}\right\} \text{ve } sx\text{-}ry=-1$$

olduğundan $\frac{x}{y}\rightarrow\frac{r}{s}\in G_{p,v}$ olur. Buradan $G_{p,u}$ ile $G_{p,v}$ eşleşmiştir.■

**Teorem 3.14.** $G_{p,u}$ nin kendisiyle eşleşmiş olması için gerek ve yeter şart $u^2 \equiv -1 \bmod p$ olmasıdır.

**İspat** $'' \Rightarrow ''$ **:** Kabul edelim ki $G_{p,u}$ kendisiyle eşleşmiş olsun. Böylece $\left(0,\frac{p}{u}\right) \xrightarrow{T} \left(\frac{p}{u},0\right)$ olacak şekilde bir $T \in \Gamma^0(N)$ vardır. Buradan

$$T = \begin{pmatrix} u & -p \\ k & -u \end{pmatrix} \in \Gamma^0(N)$$

dir. $\det T = 1$ olduğundan $-u^2 + bp = 1$ yani

$$u^2 \equiv -1 \bmod p$$

bulunur.

$'' \Leftarrow ''$**:** $u^2 \equiv -1 \bmod p$ ise buradan $u^2 + bp = -1$ olacak şekilde bir $b \in \mathbb{Z}$ vardır. Böylece $\begin{pmatrix} u & -p \\ b & -u \end{pmatrix} \in \Gamma^0(N)$ dır ve bu dönüşüm ile $0 \to \frac{p}{u}$ ve $\frac{p}{u} \to 0$ olur. $G_{p,u}$ kendisiyle eşleşmiştir.■

## 3.3 $F_{p,u}$ Alt Grafı

Bu bölümde $F\left(0,\frac{p}{u}\right)$ ile köşeleri [0]- bloğunun elemanları olan $G\left(0,\frac{p}{u}\right)$ alt yörüngesel grafının alt grafını göstereceğiz. Kısaca $F\left(0,\frac{p}{u}\right)$ yerine $F_{p,u}$ yazacağız.

Buna göre Teorem 3.12 den aşağıdaki teorem elde edilir

**Teorem 3.15.** $\frac{r}{s}, \frac{x}{y} \in [0]$ olsun. Bu takdirde $\frac{r}{s} \to \frac{x}{y}$ nin $F_{p,u}$ de bir kenar olması için gerek ve yeter şart

**(i)** $y \equiv us \pmod{p}$ , $ry - sx = -p$ veya

**(ii)** $y \equiv -us \pmod{p}$ , $ry - sx = p$

olmasıdır.■

**Teorem 3.16.** $\Gamma^*(p)$, $F_{p,u}$ 'nun köşelerini ve kenarlarını transitif olarak permüte eder.

**İspat.** $v,w\in[0]$ olmak üzere $v$ ve $w$ $F_{p,u}$ 'da iki köşe olsun. $\Gamma^0(p)$, $\begin{pmatrix} p \\ 1 \end{pmatrix}$ üzerinde transitif olduğundan $g(u)=v$ olacak şekilde bir $g\in\Gamma^0(p)$ vardır. $u\approx 0$ ve $\approx -\Gamma^0(p)$ invaryant denklik bağıntısı olduğundan

$$g(u)\approx g(0) \text{ yani } v\approx g(0)$$

dır. Böylece $g(0)\in[0]$ olduğundan $g\in\Gamma^*(p)$ dır ve $[0]$ bloğunu korur. Buradan $\Gamma^*(p)$, $F_{p,u}$ nin köşelerini transitif olarak permüte eder.

Şimdi $v,w\in[0]$ olmak üzere $v\rightarrow w$ *ve* $x\rightarrow y$, $F_{p,u}$ da iki kenar olsun. Bu takdirde $(v,w)\in O_{p,u}$ ve $(x,y)\in O_{p,u}$ dur. Böylece $S,T\in\Gamma^0(p)$ için

$$S(0)=v,\ S\left(\frac{p}{u}\right)=w \text{ ve } T(0)=x,\ T\left(\frac{p}{u}\right)=y$$

dir. $S(0),T(0)\in[0]$ olduğundan $S,T\in\Gamma^*(p)$ dır. Ayrıca

$$TS^{-1}(v)=x \text{ ve } TS^{-1}(w)=y$$

dir, yani $TS^{-1}\in\Gamma^*(p)$ dir. Böylece $\Gamma^*(p)$, $F_{p,u}$ nin kenarlarını transitif olarak permüte eder.■

**Lemma 3.17.** $\frac{r}{s},\frac{x}{y}\in\mathbb{Q}$ için $s\geq 1,\ y\geq 1$ olmak üzere $\frac{r}{s}-\frac{x}{y}=-1$ olsun. Bu takdirde $\frac{r}{s}$ ve $\frac{x}{y}$ arasında tam sayı bulunmaz.

**İspat.** Kabul edelim ki $\frac{r}{s}<k<\frac{x}{y}$ şartını sağlayan bir $k\in\mathbb{Z}$ vardır. Buradan

$$r<ks \text{ ve } ky<x$$

dir. Buna göre

$$1=sx-ry>sx-sky=s(x-ky)\geq s$$

çelişkisi elde edilir.O halde böyle bir tamsayı bulunamaz.■

**Teorem 3.18.** $F_{p,u}$ nun kenarları $\mathcal{U}=\{z\in\mathbb{C}:\operatorname{Im}(z)>0\}$ üst-yarı düzlemi üzerinde kesişmez.

**İspat.** Genelliği kaybetmeden

$$0\to\frac{p}{u}\ ,\qquad \frac{x_1p}{1+y_1p}\to\frac{x_2p}{1+y_2p}\ \text{ ve }\ \frac{x_1p}{1+y_1p}<\frac{p}{u}<\frac{x_2p}{1+y_2p}$$

alalım. Burada $x_1,x_2,y_1,y_2,p,u\in\mathbb{Z}^+$ dır. Buradan

$$\frac{1+y_1p}{x_1}>u>\frac{1+y_2p}{x_2}$$

dir. Diğer taraftan kenar şartlarından

$$x_1-x_2-p.\left(x_1y_2-x_2y_1\right)=-1$$

olur. Lemma 3.17 den sonuç elde edilir.■

**Teorem 3.19.** $F_{p,u}$ nin kendisiyle eşleşmiş bir kenar ihtiva etmesi için gerek ve yeter şart $u^2\equiv-1\bmod p$ olmasıdır.

**İspat.** Transitiflikten kendiyle eşleşmiş kenarı $\frac{0}{1}\to\frac{p}{u}\to\frac{0}{1}$ alabiliriz. Teorem 3.15.(ii) den $u^2\equiv-1\bmod p$ bulunur. Gerek şartın isparı Teorem 3.12 ye benzer şekilde yapılır.■

Burada ihtiyaç duyduğumuz bazı tanım ve teoremleri verelim.

**Tanım 3.20 (** Legendre Sembolü **).** $p$ tek asal sayı olsun. $\left(\frac{\bullet}{p}\right)$ değerlerine *Legendre sembolü* denir ve

$$\left(\frac{a}{p}\right):=\begin{cases}1\ , & p\nmid a \text{ ve } x^2\equiv a \bmod p \text{ çözümü var}\\ 0\ , & p\mid a\\ -1, & p\nmid a \text{ ve } x^2\equiv a \bmod p \text{ çözümü yok}\end{cases}$$

şeklinde tanımlanır [24].

**Teorem 3.21 (** Euler Kriteri **).** Eğer $p$ tek asal sayı ve $(a,p)=1$ ise bu takdirde

$$\left(\frac{a}{p}\right)=1 \text{ dir } \Leftrightarrow (a)^{\frac{p-1}{2}}\equiv1 \bmod p$$

dir veya, denk olarak,

$$\left(\frac{a}{p}\right) \equiv (a)^{\frac{p-1}{2}} \bmod p$$

dir [24].■

Aşağıdaki teorem Legendre sembollerinin hesaplanmasında bize kolaylık sağlayacaktır.

**Teorem 3.22.** **(i)** $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

**(ii)** $a \equiv b \bmod p$ ise, bu takdirde $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

**(iii)** $\left(\frac{a^2}{p}\right) = 1$ ve böylece $\left(\frac{1}{p}\right) = 1$

**(iv)** $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

dir [24].■

**Teorem 3.23.** $p$ ve $q$ farklı tek asal sayılar ise, bu takdirde

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

dir [24].■

**Teorem 3.24 (**Wilson Teoremi**).** $P$ nin asal olması için gerek ve yeter şart $(p-1)! \equiv -1(\bmod p)$ olmasıdır [20]..■

**Teorem 3.25.** $F_{p,u}$ kendisiyle eşleşmiş bir kenar içermesi için gerek ve yeter şart $p \equiv 1\ (mod\ 4)$ veya $p = 2$ olmasıdır.■

**İspat.** Teorem 3.19 dan biliyoruz ki $F_{p,u}$ nun kendisiyle eşleşmiş bir kenar ihtiva etmesi için gerek ve yeter şart $u^2 \equiv -1(mod\ p)$ olmasıdır.

Eğer $p = 2$ ise $u = 1$ çözümüne sahiptir.

$p$ bir tek asal sayı olsun. Wilson Teoremi

$$\left(1\cdot 2\cdot 3\cdot\ldots\cdot\frac{p-1}{2}\right)\left(\frac{p+1}{2}\cdots(p-k)\cdots(p-2)(p-1)\right) \equiv -1(\bmod p)$$

şeklinde yazılırsa buradan

$$\prod_{k=1}^{\frac{p-1}{2}} k\left(p-k\right) \equiv -1\left(\bmod p\right)$$

olur. $k\left(p-k\right) \equiv -k^2\left(\bmod p\right)$ olduğundan

$$-1 \equiv \prod_{k=1}^{\frac{p-1}{2}} k\left(p-k\right) \equiv \prod_{k=1}^{\frac{p-1}{2}} -k^2 \equiv \left(-1\right)^{\frac{p-1}{2}} \left(\prod_{k=1}^{\frac{p-1}{2}} k\right)^2 \left(\bmod p\right)$$

elde edilir. $p \equiv 1\left(mod\, 4\right)$ ise olduğundan $\left(-1\right)^{\frac{p-1}{2}} = 1$ olduğundan

$$u = \left(\frac{p-1}{2}\right)!$$

$u^2 \equiv -1\left(mod\ p\right)$ nin bir çözümüdür. Dolayısıyla $F_{p,u}$ bir iki gen içerir.

Tersine $F_{p,u}$ kendisiyle eşleşmiş bir kenar içersin. Bu durumda $u^2 \equiv -1\left(mod\ p\right)$ nin bir çözümü vardır. O halde Tanım 3.20 den $\left(\frac{-1}{p}\right) = 1$ dir. Teorem 3.22 ye göre $\left(-1\right)^{\frac{p-1}{2}} = 1$ olmalıdır ki bu ancak $\frac{p-1}{2}$ çiftken mümkündür. Yani $k \in \mathbb{Z}$ tamsayı için $\frac{p-1}{2} = 2k$ olmak üzere $p = 4k+1$ olmalıdır. Bu da $p \equiv 1\left(mod\, 4\right)$ olması anlamına gelir.

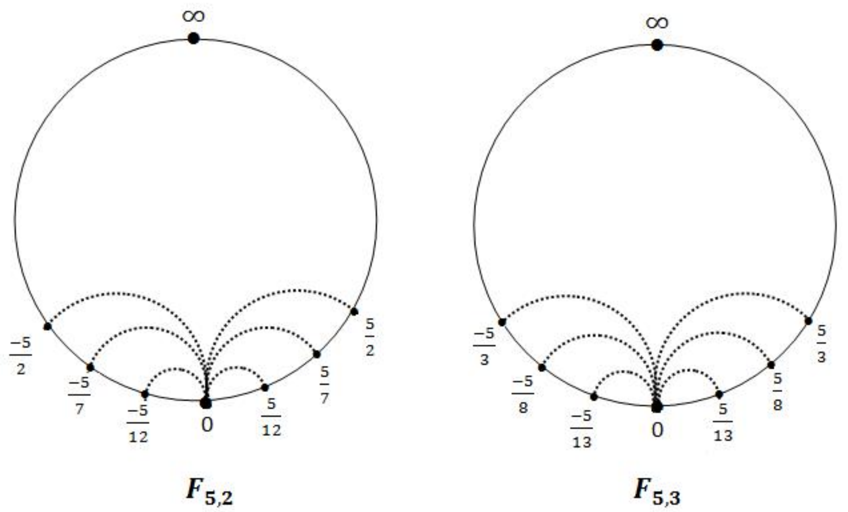
$u^2 \equiv -1\left(mod\ p\right)$ nin bir çözümü mevcut olduğunda $p \equiv 3\left(mod\, 4\right)$ olamaz. Çünkü bu durumda $\left(-1\right)^{\frac{p-1}{2}} = 1$ dir ve $p = 3+4\ell$ olacak şekilde bir $\ell \in \mathbb{Z}$ tamsayısı vardır. Ancak buradan

$$1 = \left(-1\right)^{\frac{p-1}{2}} = \left(-1\right)^{\frac{3+4\ell-1}{2}} = \left(-1\right)^{\frac{2+4\ell}{2}} = \left(-1\right)^{1+2\ell} = -1$$

çelişkisi elde edilir.

Sonuç olarak $F_{p,u}$ kendisiyle eşleşmiş bir kenar ihtiva ediyorsa $p \equiv 1\left(mod\, 4\right)$ veya $p = 2$ dir.■

**Örnek:** $p = 5$ olsun. $\left|U_5\right| = \varphi(5) = 4$ olduğundan $u = 1,2,3,4$ olur. $F_{p,u}$ sadece $u = 2,3$ için kendisiyle eşleşmiş bir kenar içerir. $p < 100$ olmak üzere $p = 5,13,17,29,37,41,53,61,73,79,97$ için elde edilen alt graflar kendisiyle eşleşmiş bir kenar içerir.




Şekil 3.1 $F_{5,2}$ ve $F_{5,3}$ graflarında kendisiyle eşleşmiş kenarlar

**Teorem 3.26.** $F_{p,u}$ nun yönlendirilmiş üçgen ihtiva etmesi için gerek ve yeter şart $u^2 \pm u + 1 \equiv 0 \pmod p$ olmasıdır.

**İspat.** $\frac{a}{b} \to \frac{c}{d} \to \frac{k}{\ell} \to \frac{a}{b}$ $F_{p,u}$ da yönlendirilmiş üçgen olsun. $\Gamma^*(p)$ $\Gamma^*(p)$, $F_{p,u}$ nun kenarlarını transitif olarak permüte ettiğinden $0 \to \frac{p}{u} \to \frac{x}{y} \to 0$ olarak alabilirz.

$\frac{x}{y} \to \frac{0}{1}$ için kenar şartlarından

$$1 \equiv uy \pmod p \text{ ve } x = p$$

olur. $\frac{p}{u} \to \frac{x}{y}$ olduğundan $\frac{p}{u} \to \frac{p}{y}$ dir. Buradan

$$y \equiv u^2 \pmod p \text{ ve } y = u - 1,$$

yani

$$u^2 - u + 1 \equiv 0 \pmod p$$

bulunur. Ayrıca $\frac{p}{u} \to \frac{p}{y}$ de

$$y \equiv -u^2 \pmod p \text{ ve } y = u + 1$$

olduğunda

$$u^2 + u + 1 \equiv 0 \pmod p$$

elde edilir.

Şimdi tersine $u^2 \pm u + 1 \equiv 0 \pmod p$ olsun. Buradan $\pm u + 1 \equiv -u^2 \pmod p$ olur.

$u + 1 \equiv -u^2 \pmod p$ ise bu takdirde $\frac{p}{u} > \frac{p}{u+1}$ olmak üzere $\frac{p}{u} \to \frac{p}{u+1}$ elde edilir.

$-u + 1 \equiv -u^2 \pmod p$ ise $u - 1 \equiv u^2 \pmod p$ olup buradan $\frac{p}{u} < \frac{p}{u-1}$ olmak üzere $\frac{p}{u} \to \frac{p}{u-1}$ bulunur.

Sonuç olarak $u^2 \pm u + 1 \equiv 0 \pmod p$ ise $\frac{0}{1} \to \frac{p}{u} \to \frac{p}{u \pm 1} \to \frac{0}{1}$ üçgeni elde edilir.■

# BÖLÜM IV

# SONUÇ VE ÖNERİLER

Cebirin temel konularından olan “Bir grubun bir küme üzerindeki etkisi(hareketi)” konusu bu çalışmada $\Gamma^0(N)$ kongrüans alt grubu ve $\hat{\mathbb{Q}}$ genişletilmiş rasyonel sayılar kümesi için uygulanmıştır.

$2x2$’lik Matris cebirinin geometrik yorumu, “düzlem üzerinde hareket” olarak özetlenebilir. Modüler grubun alt-üçgensel ve üst-üçgensel matrislerinin grupları sırasıyla $\Gamma_0(N)$ ve $\Gamma^0(N)$ kongrüans altgruplarıdır. Dolayısıyla karakterize ettikleri düzlem üzerindeki hareketin özelliklerinin bilinmesi oldukça önemlidir.

Bu çalışmada cusp noktalarının kümesi $\hat{\mathbb{Q}}$ üzerinde $\Gamma^0(N)$ kongrüans altgrunun hareketi incelenmiştir.

$\Gamma^0(N)$’nin $\hat{\mathbb{Q}}$ üzerindeki transitif hareketinin yörüngeleri elde edilmiştir. $\Gamma^0(N)$’nin $\hat{\mathbb{Q}}$ üzerindeki imprimitif hareketinin blokları elde edilmiştir.

Graf teori ile hareketin yapısını karakterize etmek için önce kenar şartları, daha sonra devre şartları bulunmuş, böylece $\Gamma^0(N)$ için altyörüngesel graflar elde edilmiştir.

Açıkça görüldüğü üzere, imprimitif hareketin tabiatını *H*-grubunun seçimi belirlemektedir. Dolayısıyla bu çalışmada seçilen $\Gamma^*(N)$ grubu yerine farklı seçimler yapılarak hareketin yapısı incelenebilir.

H-grubunun seçimindeki farklılıkların graflardaki devrelerin türünü değiştirmemekle beraber, gerek ve yeter şartlar olarak farklı kongrüans denklemleri ortaya çıkarabilir. Bu denklemler ve çözümleri incelenebilir.

Bu çalışmada elde edilen sonuçların geometrik görselleri için yüzey-döşemeleri (tessellations) üzerinde çalışılabilir.

$\Gamma_0(N)$ ve $\Gamma^0(N)$ kongrüans alt grupları birbirleriyle simetriktir. $\Gamma_0(N)$ kongrüans alt grubunun hareketinin, sürekli kesirlerle ilişkisi çeşitli çalışmalarda ortaya konmuştur. Dolayısıyla simetrik yapı göz önüne alınarak, benzer bir çalışma $\Gamma^0(N)$ için de yapılabilir.

## KAYNAKLAR


1. Akbaş, M., The Normalizer of Modular Subgroups, Ph.D. Thesis, University of Southampton,1989.

2. Akbaş, M., On Suborbital Graphs for The Modular Group, Bull. London Math. Soc., 33, 647-652, 2001.

3. Akbaş, M. and Başkan, T., Suborbital Graphs for The Normalizer of $\Gamma_0(N)$, Tr. J. Of Math., Tübitak, 20, 379-387, 1996.

4. Akbaş, M. and Singerman, D., The Signature of The Normalizer of $\Gamma_0(N)$, London Math. Soc. Lecture Notes, CUP, Cambridge, 165, 77–86, 1992.

5. Beardon, A. F., The Geometry of Discrete Groups, Springer Verlag, New York, 1983.

6. Biggs, N. L. and White, A. T., Permutation groups and combinatorial structures, London Math. Soc. Lecture Notes 33, Cambridge University Pres, Cambridge,1979.

7. Conway, J. H. and Norton, S. P., Montrous Moonshine, Bull.London Math. Soc., 11, 308-339, 1979.

8. Griess, R. L., The Friendly Giant, Invent. Math. 69, 1–102, 1982.

9. Güler, B.Ö., $\Gamma_0(N)$ Kongrüans Alt Grubunun $\mathrm{PSL}_2(\mathbb{R})$ deki Normalliyeninin Alt yörüngesel Grafları, Doktora Tezi, K.T.Ü. Fen Bilimleri Enstitüsü, Trabzon, 2006.

10. Guler, B.O., Besenk, M., Deger, A.H. and Kader, S., Elliptic Elements and Circuıts in Suborbital Graphs, Hacettepe Journal Of Mathematics And Statistics,Vol. 40, No. 2, 203-210, 2011.

11. Helling, H., On the commensurability class of rational modular group, London Math. Soc., 2, 67-72, 1970.

12. Jones, G. A. and Singerman, D., Complex Functions : An Algebraic and Geometric Viewpoint, Cambridge University Press, Cambridge, 1987.

13. Jones , G. A., Singerman, D. and Wicks, K., The Modular Group and Generalized Farey Graphs, London Math. Soc. Lecture Notes, CUP, Cambridge, 160, 316–318,1991.

14. Kader, S., Guler, B.O. and Deger, A.H., Suborbital Graphs for a Special Subgroup of The Normalizer of $\Gamma_0(m)$, Iranian Journal of Science & Technology, Transaction A, Vol. 34, No. A4, 305-312, 2010.

15. Keskin, R., Suborbital Graphs for The Normalizer of $\Gamma_0(m)$, Europan Juornal of Combinatorics, Vol. 27, No. 2, 193-206, 2006.

16. Keskin, R. and Demirturk, B., On Suborbital Graphs for The Normalizer of $\Gamma_0(N)$, Electronic Juornal of Combinatorics, Vol. 16, No. 1, R116., 2009.

17. Lehner, J. and Newman, M., Weierstrass points of $\Gamma_0(N)$, Annals of Mathematics Vol. 79, No.2, March, 360–368, 1964.

18. Maclachlan, C., Groups of Units of Zero Ternary Quadratic Forms, Proceedings of the Royal Society of Edinburg, 88, 141-157, 1981.

19. Newman, M., The Normalizer of Certain Modular Subgroups, Can. J. Math, 8, 29-31, 1956.

20. Niven, I., Zuckerman, H. S. and Montgomery, H. L., An Introduction to the Theory of Numbers, 5 th ed., John Wiley & Sons, Inc.New York, 1991.

21. Ogg, A. P., Automorphismes des Courbes Modulaires, Seminaire Delange-Pisot, Poitou, 7, 1974.

22. Ogg, A. P., Modular functions, Proceedings of Symposia in Pure Mathematics, Vol. 37, 1980.

23. Pizer, A., A Note on a Conjecture of Hecke, Pasific J. Math. Vol. 79, 2, 541–548, 1978.

24. Rose, H. E., A Course in Number Theory, Oxford University Press, Oxford, 1988.

25. Schoeneberg, B., Elliptic Modular Functions, Springer Verlag, Berlin, 1974.

26. Shimura, G., Inroduction to The Arithmetic Theory of Automorphic Functions. Princeton Univ. Press, 1971.

27. Sims, C. C., Graphs and Finite Permutation Groups, Math. Z., 95, 76-86, 1967.

28. Singerman, D., Subgroups of Fuchsian Groups and Finite Permutation Groups, Bull. London Math. Soc. 2, 319–323, 1970.

29. Tsuzuku, T., Finite Groups and Finite Geometries, Cambridge University Pres, Cambridge,1982.