T.C.

KAFKAS ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

MATEMATİK ANABİLİM DALI

MACWİLLİAMS VE CHEBYSHEV MATRİSLERİ YARDIMI İLE DEVİRLİ VE YARI GRUPLARIN ELDE EDİLMESİ

Yeşim AKÜZÜM

YÜKSEK LİSANS TEZİ

DANIŞMAN

Doç. Dr. Ömür DEVECİ

HAZİRAN-2014

KARS

T.C. Kafkas Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı Yüksek Lisans öğrencisi Yeşim AKÜZÜM' ün Doç. Dr. Ömür DEVECİ'nin danışmanlığında yüksek lisans tezi olarak hazırladığı "MacWilliams ve Chebyshev Matrisleri Yardımı ile Devirli ve Yarı Grupların Elde Edilmesi" adlı bu çalışma, yapılan tez savunması sınavı sonunda jüri tarafından Lisansüstü Eğitim Yönetmeliği uyarınca değerlendirilerek oy ..birliği.... ile kabul edilmiştir.

19./.06/2014

Adı ve Soyadı	**imza**
Başkan: Prof. Dr. Erdal KARADUMAN	....
Üye: Doç. Dr. Ömür DEVECİ	....
Üye: Yrd. Doç. Dr. Taha Yasin ÖZTÜRK	....

Bu tezin kabulü, Fen Bilimleri Enstitüsü Yönetim Kurulunun ...../...../2014 günü ve ..../........ sayılı kararı ile onaylanmıştır.

....

Doç.Dr. Muzaffer ALKAN

Enstitü Müdürü.

ÖNSÖZ

Yüksek lisans tezi olarak sunduğum bu çalışma Kafkas Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalında yapılmıştır. Tez konusunu veren, engin tecrübesiyle bana yol gösteren, çalışmalarımda etkin katkısı bulunan, vaktini ve bilgisini benden esirgemeyen Kafkas Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü Öğretim Üyesi danışman hocam Sayın Doç. Dr. Ömür DEVECİ 'ye şükranlarımı sunarım.

Çalışmalarım boyunca kendilerinden görmüş olduğum destekten dolayı aileme teşekkür ederim.

Yeşim AKÜZÜM

Kars-2014

İÇİNDEKİLER

ÖZET

Bu çalışmada “MacWilliams ve Chebyshev matrisleri yardımı ile devirli ve yarı gruplar” elde edildi ve bu cebirsel yapıların mertebeleri üzerinde duruldu.

Bu çalışmanın 2.1 bölümünde grup takdimleri hakkında temel bilgi ve teoremler sunuldu ve devirli ve yarı gruplarının tanım ve özellikleri verildi. Daha sonra 2.2 bölümünde matris cebiri hakkında genel bilgi verildi. Sonra MacWilliams ve Chebyshev matrisleri tanıtıldı ve bu matrisler için bazı önemli formüller verildi. Bölüm 3.1 de ise genelleştirilmiş Fibonacci matrisleri tanıtıldı ve bu matrislerin m modülüne göre çarpımsal katları alınarak devirli gruplar elde edildi. Daha sonra bu devirli grupların mertebeleri üzerinde duruldu. Bölüm 3.2 de Pascal ve genelleştirilmiş Pascal matrislerin çarpımsal katları alınarak devirli gruplar elde edildi ve m modülüne göre bu matrislerin çarpımsal mertebeleri ile ilgili teoremler verildi.

Son olarak 4.1 bölümünde MacWilliams ve Chebyshev matrislerinin çarpımsal katları alınarak devirli ve yarı gruplar elde edildi ve m modülüne göre bu matrislerin çarpımsal mertebeleri için teoremler verildi. Daha sonra elde edilen sonuçlar ispatlarıyla birlikte verildi.

2014, 63 Sayfa

Anahtar kelimeler: Genelleştirilmiş Fibonacci Matris, Pascal Matris, MacWilliams Matris, Chebyshev Matris, Devirli Grup, Yarı Grup, Çarpımsal Mertebeler

ABSTRACT

In this study have been obtained " the cyclic gruops and semigroups via MacWilliams and Chebyshev matrices" and orders of this algebraic structures have been emphasized.

At the 2.1 section of the study have been submitted basic information and theorems about group presentations and the definition and features of cyclic groups and semigroups have been given. At the next section 2.2 have been given general information about matrix algebra. Afterwards MacWilliams and Chebyshev matrices have been introduced and some important formulas have been given for this matrices. At the 3.1 section have been introduced generalized Fibonacci matrices and cyclic groups have been yielded by taking multiplicative orders of this matrices according to modulo m. Then orders of this cyclic groups have been emphasized**.** At the 3.2 section, cyclic groups have been obtained by taking multiplicative orders of Pascal and generalized Pascal matrices and have been given theorems associated with multiplicative orders of this matrices according to modulo m.

Ultimately, at the 4.1 section of the study, cyclic groups and semigroups have been obtained by taking multiplicative orders of MacWilliams and Chebyshev matrices and theorems have been given for multiplicative orders of this matrices according to modulo m. Later the obtained results have been submitted along with their evidences.

2014, 63 Pages

Keywords: Generalized Fibonacci Matrix , Pascal Matrix, MacWilliams Matrix, Chebyshev Matrix, Cyclic Group, Semigroup, Multiplicative Orders

SİMGELER DİZİNİ

e	Grubun birim elemanı
$\mathbb{R}$	Reel sayılar kümesi
$\mathbb{Z}$	Tamsayılar kümesi
$\mathbb{C}$	Kompleks sayılar kümesi
$\mathbb{N}$	Doğal sayılar kümesi
G	Grup
$\|G\|$	Grubun mertebesi
$G = \langle A \rangle$	A 'dan üretilen grup
G/H	G 'nin H 'a göre bölüm grubu
$H \leq G$	$H,\ G$ 'nin alt grubu
$H \Delta G$	$H,\ G$ 'nin normal alt grubu
$(H, +, \cdot)$	Halka
$A = (a_{ij})_{m \times n}$	$m \times n$ boyutlu matris
$A = (a_{ij})_{n \times n}$	$n \times n$ boyutlu kare matris
A^T	A matrisinin transpozu
I_n	$n \times n$ mertebeden birim matris
E	Elemanter matris
$detA$	A matrisinin determinantı
$\mathbb{F}_2^N$	$\mathbb{F}_2 = \{0,1\}$ çift cisim üzerinde bir N boyutlu vektör uzayı
V_n	Grup cebiri
$S_r^{(N)}$	$\mathbb{F}_2^N$ de r-inci Hamming küre
$K_r^{(N)}(x)$	N mertebeli r-inci Krawtchouck polinomu
$(M_N)_{ij}$	N mertebeli MacWilliams matrisi

$D_r^{(N)}(x)$	N mertebeli r-inci ayrık Chebyshev polinomu
$(D_N)_{ij}$	N mertebeli Chebyshev matrisi
Δ^n	$\Delta f(x) = f(x+1) - f(x)$ olarak tanımlana fark operatörünün n-inci kuvveti
$f_n^{(k)}$	$1 \leq i < k$ için $f_i^{(k)} = 0$ ve $f_k^{(k)} = 1$ sınır şartlarıyla tanımlı, $n > k$ için $f_n^{(k)} = \sum_{j=1}^{k} f_{n-j}^{(k)}$ k-basamak Fibonacci elmanı
$f(k,m)$	$f_n^{(k)}$ 'nin m 'ye göre modülü
$h_k(m)$	$f(k,m)$ 'nin en küçük periyodu
L_n	Alt Pascal üçgen matrisi
U_n	Üst Pascal üçgen matrisi
S_n	Simetrik Pascal üçgen matrisi
$P_n(x;i,j)$	1. çeşit $P_n[x]$ genelleştirilmiş Pascal matrisi
$Q_n(x;i,j)$	2. çeşit $Q_n[x]$ genelleştirilmiş Pascal matrisi
$R_n(x;i,j)$	$R_n[x]$ simetrik genelleştirilmiş Pascal matrisi

1.GİRİŞ

Matris kavramı gerek yapısal özellikleri gerekse birçok problemin çözümü noktasında modern matematiğin birçok alanında karşımıza çıkan bir kavram olup, özel tanımlı matrisler kullanılarak devirli grupların elde edilmesi ilk olarak Lü ve Wang tarafından yapılan [20] ’deki çalışmalarında karşımıza çıkmaktadır. Lü ve Wang bu çalışmada genelleştirilmiş Fibonacci matrisinin m modülüne göre çarpımsal katlarını alarak devirli gruplar elde etmiş ve bu devirli grupların mertebelerinin, m modülüne göre k- basamak Fibonacci dizilerinin periyotlarına eşit olduğunu göstermişlerdir.

Sonraki süreçte Deveci ve Karaduman [7] ’deki çalışmalarında Pascal matrisleri ve genelleştirilmiş Pascal matrislerinin m modülüne göre çarpımsal katlarını alarak devirli gruplar elde etmiş ve m modülüne göre bu matrislerin çarpımsal mertebeleri için çeşitli bağıntılar oluşturmuşlardır.

Deveci ve Aküzüm [11] ’deki çalışmalarında konsepti bir başka cebirsel yapı olan yarı gruplara genişletmişlerdir. Bu çalışmada Deveci ve Aküzüm MacWilliams ve Chebyshev matrislerinin determinantlarının durumuna göre bu matrislerin m modülüne göre çarpımsal katlarını alarak devirli ve yarı gruplar elde etmiş ve m modülüne göre bu matrislerin çarpımsal mertebeleri için çeşitli bağıntılar oluşturmuşlardır.

2.KURAMSAL TEMELLER

2.1.Grup Takdimleri

Tanım 2.1.1: K bir küme olsun. $K \times K$ dan K ya tanımlı bir

$$*: K \times K \to K\,, \qquad (x, y) \to x * y$$

fonksiyonuna K içinde bir ikili işlem denir. Bu takdirde $(K,*)$ ikili işlemine cebirsel yapı denir (Karakaş 2010).

Örnek 2.1.1: Reel elemanlı 2×2 matrislerinden oluşan $\mathbb{R}^{2\times 2}$ kümesi içinde matris toplamı ve matris çarpımı ikili işlem oluşturur (Karakaş 2010).

Tanım 2.1.2: Bir $G \neq \varnothing$ kümesinde bir $(a,b) \to ab$ ikili işlemi aşağıdaki şartları sağlıyorsa, G ye bir grup denir;

1. $\forall a,b,c \in G$ için $a(bc) \to (ab)c$ asosyatif kural verilir.

2. $\forall a \in G$ için $ae = ea = a$ olacak şekilde bir $e \in G$ vardır. e elemanına G 'nin birim elemanı denir.

3. $\forall a \in G$ için $aa^{-1} = a^{-1}a = e$ olacak şekilde bir $a^{-1} \in G$ vardır. $a^{-1} \in G$ elemanına a nın inversi (tersi) denir.

Örnek 2.1.2: $M_2(\mathbb{R})$; elemanları reel sayı olan bütün 2×2 matrislerin kümesi, yani

$$M_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} :\ a, b, c, d\ \in \mathbb{R} \right\}$$

ise o zaman bu küme matrislerin toplama işlemine göre bir gruptur (Taşcı 2010).

Tanım 2.1.3: $(G,*)$ bir grup olmak üzere $\forall\ a, b \in G$ için

$$a * b = b * a$$

oluyorsa bu gruba değişmeli (komutatif ya da abelyan) grup denir (Taşcı 2010).

Tanım 2.1.4: Bir $G \neq \varnothing$ küme ve bu küme üzerinde bir ikili işlem $*$ olsun. Buna göre aşağıdaki şart sağlanırsa $(G,*)$ cebirsel yapısına bir yarı grup denir;

1. $\forall\, a,b,c \in G$ için $a * (b * c) = (a * b) * c$ (Birleşme özelliği).

Örnek 2.1.3: $\mathbb{R}$ reel sayılar kümesi üzerinde $*$ ikili işlemi $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ olmak üzere $a, b \in \mathbb{R}^*$ için

$$a * b = max\{a, b\}$$

şeklinde tanımlanırsa, bu durumda $(\mathbb{R}^*, *)$ bir yarı gruptur (Taşcı 2010).

Teorem 2.1.1: $(G,*)$ bir grup olsun. Buna göre

(i) G 'nin birimi tektir.

(ii) G 'nin her elemanının tersi tektir.

(iii) $a \in G$ için $a * a = a$ ise $a = e$ dir.

(iv) G grubunda soldan ve sağdan kısaltma kuralları geçerlidir. Yani $a, b, c \in G$ için

$a * b = a * c$ ise $b = c$ (soldan kısaltma kuralı)

$b * a = c * a$ ise $b = c$ (sağdan kısaltma kuralı)

(v) $a, b \in G$ için $a * x = b$ ve $y * a = b$ denklemlerinin G 'deki işlemleri tektir.

(vi) $a \in G$ için $(a^{-1})^{-1} = a$'dır (Taşcı 2010).

Tanım 2.1.5: $(G,*)$ bir grup olmak üzere $a \in G$ elemanlarının kuvvetleri $n \in \mathbb{Z}^+ \cup \{0\}$ için;

$a^n = a * a * \ldots * a$ (n tane çarpan)

$a^0 = e$ (e, $(G,*)$ 'nin birim elemanı)

$$a^{-n} = (a^{-1})^n$$

şeklinde tanımlanır(Taşcı 2010).

Teorem 2.1.2: $(G,*)$ bir grup, $a \in G$ ve $m, n \in \mathbb{Z}$ olmak üzere a 'nın kuvvetleri için aşağıdaki ifadeler geçerlidir (Taşcı 2010):

(i) $a^m * a^n = a^{m+n} = a^n * a^m$

(ii) $(a^m)^n = a^{mn} = (a^n)^m$

(iii) $a^{-m} = (a^m)^{-1}$

(iv) $e^m = e$

Tanım 2.1.6: G bir grup ve $\varnothing \neq H \subseteq G$ bir alt küme olsun. H, G de tanımlanan ikili işleme göre bir grup ise H ' ya, G nin bir alt grubu denir ve $H \leq G$ ile gösterilir.

Tanım 2.1.7: $H = \{e\}$ ve $H = G$ alt kümeleri daima G grubunun alt gruplarıdır. $H = \{e\}$ alt grubuna aşikar alt grup ve G den farklı her H alt grubuna da öz alt grup denir. Eğer H, G nin bir öz alt grubu ise $H < G$ ile gösterilir.

Tanım 2.1.8: G bir grup ve $\varnothing \neq A \subseteq G$ olsun. G grubunun A 'yı içeren bütün alt gruplarının ailesinin ara kesitini $< A >$ ile gösterelim. Bu takdirde $< A >$, G 'nin bir alt grubudur. Bu alt grup A' yı içeren en küçük alt gruptur ve A tarafından üretilen alt grup olarak adlandırılır.

Tanım 2.1.9: G bir grup ve $H \leq G$ olsun. Eğer her $g \in G$ için $gHg^{-1} = H$ oluyorsa H ' ya, G' nin bir normal alt grubu denir ve $H \lhd G$ ile gösterilir.

Tanım 2.1.10: N, G' nin bir normal alt grubu olsun. G/N kümesi üzerinde $(Ng)(Nh) = N(gh)$ ile bir çarpım tanımlansın. Bu takdirde G/N bu çarpıma göre mertebesi $[G:N]$ olan bir gruptur. Bu gruba N ile G' nin bölüm (faktör) grubu denir.

Tanım 2.1.11: G bir grup ve H, G' nin bir alt grubu olsun. $H < G$ ve $H < K \leq G$ den $K = G$ elde edilirse H alt grubuna, G' nin bir maksimal alt grubu denir.

$E=\{e\}$ olmak üzere $E<H$ ve $E\leq K<H$ dan $K=E$ elde edilirse H alt grubuna, minimal alt grup denir.

Tanım 2.1.12: G bir grup olmak üzere $H=\{a^n : n \in \mathbb{Z}\}$ alt grubuna G ‘nin a elemanı tarafından üretilen devirli alt grubu denir ve $\langle a\rangle$ ile gösterilir.

Yani,

$$\langle a\rangle = \{a^n : n \in \mathbb{Z}\} = H \quad \text{dır.}$$

Buradan hareketle devirli grubu şu şekilde de tanımlanabilir:

G bir grup olmak üzere G ‘de $G=\{a^n : n \in \mathbb{Z}\}$ olacak şekilde bir a elamanı varsa o zaman G grubuna devirli grup denir. Böylece bir a elamanına G ’nin üreteci denir ve $G=\langle a\rangle$ şeklinde gösterilir (Taşcı 2010).

Örnek 2.1.4: $U(n)$; elemanları n ile aralarında asal ve n ’yi geçmeyen pozitif tamsayıların kümesi olsun. Yani

$$U(n)=\{k\in\mathbb{Z}^+ : (k,n)=1, \quad 0<k<n\}$$

olsun. Buna göre sözgelimi $n=10$ alınır ise o zaman

$$U(10)=\{1,3,7,9\}$$

olur. Buradan

$$3^1=3,\ 3^2=9,\ 3^3=7,\ 3^4=1,\ 3^5=3^4.3=3,...$$

olur. O halde

$$U(10)=\{1,3,7,9\}=\{3^0,3^1,3^3,3^2\}=\langle 3\rangle$$

yazılabilir. Yine

$$\{1,3,7,9\}=\{7^0,7^3,7^1,7^2\}=\langle 7\rangle$$

dir. Böylece hem 3 hem de 7, $U(10)$ için birer üreteçtir.

Şimdi $n=8$ olduğu varsayılır ise bu durumda

$$U(8) = \{1,3,5,7\}$$

dir. Halbuki

$$\langle 1 \rangle = \{1\},\ \ \langle 3 \rangle = \{3,1\},\ \ \langle 5 \rangle = \{5,1\},\ \ \langle 7 \rangle = \{7,1\}$$

olduğundan $U(8)$ ’deki herhangi bir α elemanı için

$$U(8) \neq \langle \alpha \rangle$$

dır (Taşçı 2010).

Tanım 2.1.12: G bir grup ve $a \in G$ olsun. a nın ürettiği $\langle a \rangle$ devirli grubunun mertebesine a elemanının mertebesi denir ve $o(a)$ ile gösterilir (Çallıalp 2001).

Teorem 2.1.3: Her devirli grup değişmelidir (Taşcı 2010).

İspat: G, $a \epsilon G$ tarafından üretilen bir devirli grup yani,

$$G = \langle a \rangle = \{a^n \, : \, n \in \mathbb{Z}\}$$

olsun. Buna göre $\forall x, y \in G$ için $xy = yx$ olduğunu gösterilir ise o zaman teorem ispatlanmış olur. $x \in G$ ise G ’nin tanımından $x = a^k$, $k \in \mathbb{Z}$ olarak alınabilir. Yine benzer düşünce ile $y \in G$ ise $y = a^s$, $s \in \mathbb{Z}$ olarak alınabilir. O halde

$$xy = a^k a^s = a^{k+s} = a^s a^k = yx$$

yazılır. Bu ise G grubunun değişmeli olduğunu gösterir.

Teorem 2.1.4: Bir devirli grubun her alt grubu da devirlidir (Taşcı 2010).

İspat: G, $a \epsilon G$ tarafından üretilen bir devirli grup yani,

$$G = \langle a \rangle = \{a^n \, : \, n \in \mathbb{Z}\}$$

şeklinde bir devirli grup ve $H \leq G$ olsun. İspat iki aşamada yapılır.

(i) Eğer $H = \{e\}$ ise yani G ’nin birim elemanından oluşan aşikar alt grubu ise o takdirde

$$\langle e \rangle = \{e^n : n \in \mathbb{Z}\} = \{e\} = H$$

olduğundan açık olarak H bir devirli gruptur.

(ii) $H \neq \{e\}$ olsun. Bu durumda $n \in \mathbb{Z}^+$ olmak üzere bir $a^n \in H$ vardır. Diğer taraftan m 'nin $a^m \in H$ olacak şekilde en küçük pozitif kuvvetli tamsayı olduğunu farzedelim. Buna göre,

$$H = \langle a^m \rangle$$

dir. Bunu iki kümenin eşitliği tanımına göre kapsama şeklinde gösterilirse o zaman istenilen gösterilmiş olur.

$$\langle a^m \rangle = \{(a^m)^q : q \in \mathbb{Z}\}$$

şeklinde a^m 'nin kuvvetlerinden oluşan bir küme olduğu biliniyor. Diğer taraftan $a^m \in H$ ve $H \leq G$ olduğundan kapalılıktan a^m 'nin bütün kuvvetleri aynı zamanda H'da olacağından buradan

$$\langle a^m \rangle \subseteq H$$

sonucu elde edilir. Şimdi de $a^n \in H$ alıp $a^n \in \langle a^m \rangle$ olduğu gösterilmeli. Bölme Algoritmasından,

$$n = mq + r, \qquad 0 \leq r < m$$

olacak şekilde bir tek q, r tamsayı çifti vardır. Buradan hareketle

$$a^n = a^{mq+r} = a^{mq}.a^r = (a^m)^q.a^r$$

olup buradan a^r çekilirse,

$$a^r = (a^m)^{-q}a^n$$

bulunur. Halbuki

$$a^n \in H, a^m \in H \text{ ve } H \leq G$$

olduğundan dolayısı ile her şeyden önce bir grup olduğundan

$$(a^m)^{-q} \in H$$

dir. Böylece

$$(a^m)^{-q} \in H \text{ ve } a^n \in H$$

olduğundan kapalılıktan

$$(a^m)^{-q} a^n \in H$$

yazılır. Buradan $a^r \in H$ sonucu elde edilir. Halbuki $0 \leq r < m$ olduğundan $a^r \in H$ olması a^m 'nin H 'daki en küçük pozitif kuvvetli elemanı olması ile çelişir. O halde bu $r = 0$ olması durumunda mümkündür. Böylece $n = mq$ ve

$$a^n = a^{mq} = (a^m)^q \in \langle a^m \rangle$$

olur. Bu da

$$H \subseteq \langle a^m \rangle$$

olmasını gerektirir. Böylece istenilen görülür teorem ispatlanmış olur.

Teorem 2.1.5: G bir grup, $a \in G$ ve a 'nın mertebesi n yani $o(a) = n$ olsun. Buna göre;

(i) Eğer a 'nın mertebesi sonsuz ise o takdirde a 'nın bütün farklı kuvvetleri grubun farklı elemanlarıdır.

(ii) Eğer a 'nın mertebesi sonlu ise yani $a^n = e$ şartını sağlayan en küçük pozitif tamsayı n ise o takdirde a 'nın ürettiği devirli grubun yani $\langle a \rangle$ 'nın mertebesi de n dir.

Diğer bir deyimle,

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$$

dir.

(iii) a 'nın mertebesi sonlu ve n olmak üzere $a^k = a^l$ olması için gerek ve yeter şart $k \equiv l (mod\, n)$ olmasıdır.

(iv) $o(a) = n$ sonlu olmak üzere $a^k = e$ olması için gerek ve yeter şart $n|k$ olmasıdır (Taşcı 2010).

İspat: (i) Eğer a 'nın mertebesi sonsuz ise o zaman e, G 'nin birim elemanı olmak üzere $a^n = e$ şartını sağlayan sıfırdan farklı bir n tamsayısı yoktur. Diğer taraftan $a^r = a^s$ olması $a^{r-s} = e$ olmasını gerektirdiğinden $r - s = 0$ olmalıdır.

(ii) a 'nın mertebesi n (sonlu) yani $o(a) = n$ olsun şimdi

$$H = \{\, a, a^2, a^3, \dots, a^{n-1}, a^n = e\}$$

olarak alınsın. Buna göre eğer $\langle a \rangle = H$ olduğu gösterilirse ispat buradan kolaylıkla görülür. Bu eşitlik iki kümenin eşitliği tanımına göre iki yanlı kapsama şeklinde göstererek ispatlanabilir.

$$H \subseteq \langle a \rangle$$

olduğu

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$$

kümesi göz önüne alınarak hemen görülür. Şimdi ters yönde kapsamayı göstermek için a^k, $\langle a \rangle$ 'nın keyfi bir elemanı yani $a^k \in \langle a \rangle$ olmak üzere $a^k \in H$ olduğunu göstermek yeterlidir. Gerçekten Bölme Algoritmasından,

$$k = nq + r, \quad 0 \leq r < n$$

olacak şekilde bir q, r tamsayı çifti vardır. Buna göre;

$$a^k = a^{nq+r} = (a^n)^q . a^r = ea^r = a^r$$

yazılır. Böylece $0 \leq r < n$ olduğundan $a^r \in H$ ve dolayısıyla $a^k \in H$ yazılır. Buradan

$$\langle a \rangle \subseteq H$$

olduğu görülür. Buna göre

$$H = \langle a \rangle = \{\, a, a^2, a^3, \dots, a^{n-1}, a^n = e\}$$

eşitliği elde edilmiş olur. Burada belirtelim ki $\{e, a, a^2, \dots, a^{n-1}\}$ kümesinin elemanları birbirinden farklıdır. Gerçekten $0 \leq j < i < n$ olmak üzere $a^i = a^j$ ise o zaman $a^{i-j} = e$ olur. Bu ise n 'nin $a^n = e$ olacak şekilde en küçük pozitif tamsayı olmasıyla çelişir. O halde H 'ın dolayısıyla a tarafından üretilen $\langle a \rangle$ kümesinin tam olarak n tane elemanı olduğundan

$$o(a) = n = o(\langle a \rangle) = o(H)$$

dir.

(iii) $\Rightarrow$ $a^k = a^l$ olsun. Buradan $a^{k-l} = e$ yazılır. Diğer taraftan Bölme Algoritmasından,

$$k - l = nq + r, \quad 0 \leq r < n$$

olacak şekilde bir tek q, r tamsayı çifti vardır. Buna göre;

$$e = a^{k-l} = a^{nq+r} = (a^n)^q . a^r = ea^r = a^r$$

yazılır. Buradan $a^r = e$ olması a 'nin mertebesinin n olması ile $0 \leq r < n$ olduğundan çelişir. O halde buradan $r = 0$ olmalıdır. Bu durumda $k - l = nq$ olur. Böylece

$$n | k - l$$

ve dolayısı ile kongrüansın tanımından $k \equiv l (mod\ n)$ bulunur.

$\Leftarrow$ $k \equiv l (mod\ n)$ ise buradan

$$n | k - l$$

ya da

$$k - l = nt, \quad t \in \mathbb{Z}$$

yazılır. Böylece

$$a^{k-l} = a^{nt} = (a^n)^t = e^t = e$$

olup buradan $a^k = a^l$ olduğu görülür.

(iv) $\Rightarrow$ $a^k = e$ olsun yine Bölme Algoritmasından,

$$k = nq + r, \quad 0 \leq r < n$$

yazılır. O halde

$$e = a^k = a^{nq+r} = a^{nq}a^r = (a^n)^q . a^r = e^q a^r = ea^r = a^r$$

ifadesinden $a^r = e$ olur bu ise $0 \leq r < n$ olması dolayısı ile $o(a) = n$ olması ile çelişir. O halde $r = 0$ yani $k = nq$ ya da $n|k$ dır.

$\Leftarrow n|k$ ise buradan $k = nt, \quad t \in \mathbb{Z}$ yazılır. O halde

$$a^k = a^{nt} = (a^n)^t = e^t = e$$

yazılır. Böylece teorem ispatlanmış olur.

Sonuç 2.1.1: $G = \langle a \rangle$ sonlu bir devir grubu ve $o(G) = k < \infty$ olsun. $H \neq \{e\}$ ve $a^n \in H$ olacak şekilde $n > 0$ pozitif tamsayılarının en küçüğü m olmak üzere $H = \langle a^m \rangle$ olduğu kabul edilsin. O halde,

$$m|k \quad \text{ve} \quad o(H) = \frac{k}{m}$$

dir (Taşcı 2010).

İspat: Bölme Algoritmasından,

$$n = mq + r, \qquad 0 \leq r < m$$

yazılabilir. Bu durumda,

$$e = a^k = a^{mq+r} = (a^m)^q . a^r$$

olup buradan a^r çekilirse,

$$a^r = a^{-mq} \in H$$

bulunur. O halde m 'nin tanımından $0 \leq r < m$ olması $a^r \in H$ olması ile çelişki teşkil eder. Bu ise $r = 0$ olmasını dolayısı ile $k = mq$ olmasını gerektirir. Buradan

$$m|k$$

yazılır. Diğer yandan

$$(a^m)^q = e$$

şartını sağlayan en küçük pozitif tamsayı q olur. Gerçekten bir an için $p < q$ olacak şekilde bir p tamsayısının olduğu kabul edilirse o takdirde

$$(a^m)^q = e \text{ ve } mp < k$$

olur. Fakat $o(G) = k$ olduğundan bu mümkün değildir. $(a^m)^q = e$ den $o(a^m) = q$ olduğundan a^m tarafından üretilen $H = \langle a^m \rangle$ alt grubunun mertebesi de q olur.

Böylece

$$o(H) = o(\langle a^m \rangle) = q = \frac{k}{m}$$

bulunur.

Uyarı 2.1.1: $G = \langle a \rangle$ sonsuz mertebeli bir devir grubu ise o takdirde a^m 'nin bütün kuvvetleri farklı olacağından $H = \langle a^m \rangle$ devir grubu da sonsuz olur (Taşçı 2010).

Teorem 2.1.6: $G = \langle a \rangle$ ve $o(G) = n$ olan bir devirli grup olsun. O takdirde G 'nin a^k tarafından üretilmesi için yani $G = \langle a^k \rangle$ olması için gerek ve yeter şart k ile n 'nin aralarında relatif asal yani $(k, n) = 1$ olmasıdır (Taşcı 2010).

İspat: ⇒ Olmayan ergi yöntemi ile ispatı yapalım. Bir an için $(k, n) = d > 1$ olduğunu varsayalım. O zaman buradan $d|k$ ve $d|n$ ya da sırası ile $k = dt$ ve $n = dr$ yazılır. Bu durumda,

$$(a^k)^r = (a^{dt})^r = (a^{dr})^t = (a^n)^t = e$$

öyle ki

$$o(a^k) \leq r < n$$

dir. Bu ise a^k 'nın G 'nin bir üreteci olmadığını gösterir. Çünkü

$$G = \langle a^k \rangle$$

olsaydı o zaman $G = \langle a \rangle$ olduğundan $o(a) = n$ dolayısı ile $o(a^k) = n$ olmalıydı. Bu bir çelişkidir. Dolayısı ile eğer $G = \langle a^k \rangle$ ise o zaman $(k, n) = 1$ olmalıdır.

⇐ $(k, n) = 1$ olsun. Buna göre $G = \langle a^k \rangle$ olduğu gösterilmeli.

$$G \subseteq \langle a^k \rangle$$

olduğu açıktır. Çünkü $a^k \in G$ ve G bir grup olduğundan kapalılıktan dolayı a^k 'nın kuvvetleri G 'ye aittir. Şimdi ters kapsama gösterilir ise,

$$(k, n) = 1 \Rightarrow ku + nv = 1$$

olacak şekilde u, v tamsayıları vardır. O halde

$$a = a^{ku+nv} = a^{ku}a^{nv}$$

yazılır. Diğer taraftan $G = \langle a^k \rangle$ ve $o(G) = n$ olduğundan $o(a) = n$ 'dir. Böylece

$$a^{nv} = (a^n)^v = e^v = e$$

olup buradan $a = a^{ku}$ eşitliği elde edilir. Buna göre $a^m \in G$ ise o takdirde

$$a^m = (a^{ku})^m = (a^k)^{um} \in \langle a^k \rangle$$

yazılır. Bu da,

$$G \subseteq \langle a^k \rangle$$

olmasını gerektirir. Böylece $G = \langle a^k \rangle$ eşitliği elde edilir. Böylece teorem ispatlanır.

Sonuç 2.1.2: Bir k tamsayısının $(\mathbb{Z}_n, +)$ grubunun bir üretici olması için gerek ve yeter şart $(k, n) = 1$ olmasıdır (Taşcı 2010).

İspat: Yukarıdaki teoremden $G = \mathbb{Z}_n$ ve $a = 1$ alınsın. Burada hemen ilgi çekelim ki yukarıdaki teoremde G çarpmaya göre bir grup idi. Fakat $\mathbb{Z}_n, +$ işlemine göre bir grup olduğu için a^k yerine ka alınmalı. Buna göre $\mathbb{Z}_n = \langle 1 \rangle$ olduğu biliniyor.

Yukarıdaki teoreme göre,

$$\mathbb{Z}_n = \langle ka \rangle = \langle k1 \rangle = \langle 1 \rangle \Leftrightarrow (k, n) = 1$$

olmasıdır şeklinde yorumlanabilir.

Tanım 2.1.14: K, G' nin alt grubu olsun (normal alt grup olması gerekmez).Eğer $K \cap Q = e$ ve $KQ = G$ olacak şekilde bir $Q \leq G$ alt grubu varsa, Q'ya, G'de , K'nın bir komplementidir denir (Dummit ve Foote 2004).

Bir H kümesi ile bu küme üzerinde toplama $(+)$ ve çarpma $(\cdot)$ ikili işlemlerinden oluşan cebirsel yapı $(H, +, \cdot)$ ile gösterilir.

Tanım 2.1.15: Bir cebirsel yapı, $(H, +, \cdot)$ verilmiş olsun. Eğer H kümesindeki her x, y, z elemanları için

$$x(y+z) = (xy) + (xz)$$

ise, $(H, +, \cdot)$'da sol dağılma özelliği vardır denir. Her $x, y, z \in H$ için

$$(x+y)z = (xz) + (yz)$$

ise, $(H, +, \cdot)$'da sağ dağılma özelliği vardır denir (Karakaş 2010).

Tanım 2.1.16: Bir cebirsel yapı, $(H, +, \cdot)$ verilmiş olsun. Aşağıdaki üç koşul sağlanırsa, $(H, +, \cdot)$ ya bir halka denir:

(i) $(H, +)$ bir değişmeli gruptur,

(ii) $(H, \cdot)$ nın birleşme özelliği vardır,

(iii) $(H, +, \cdot)$'da sol ve sağ dağılma özelliği vardır (Karakaş 2010).

Tanım 2.1.17: Birimli bir H halkasında $1_H \neq 0_H$ ise ve H nin sıfırdan farklı her elemanı tersinir ise, H'ya bir aykırı cisim denir (Karakaş 2010).

Tanım 2.1.18: Eğer H değişmeli aykırı cisim ise, H'ya bir cisim denir (Karakaş 2010).

Örnek 2.1.5: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C} +, \cdot)$ cebirsel yapıları bir cisim olmasına karşılık $(\mathbb{Z}, +, \cdot)$ tamsayılar halkası bir cisim değildir. Gerçekten sözgelimi $2 \in \mathbb{Z}$ 'nin çarpamaya göre tersi $\frac{1}{2}$ olup $\frac{1}{2} \notin \mathbb{Z}$ olduğundan $(\mathbb{Z}, +, \cdot)$ bir cisim olamaz (Taşcı 2010).

2.2. Matris Cebiri

Tanım 2.2.1: F bir cisim ve $a_{ij} \in F \quad (1 \leq i \leq m, \;\; 1 \leq j \leq n)$ olmak üzere

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

şeklindeki bir dikdörtgen tabloya matris denir. $i = 1, 2, \dots, m$ için $r_i = [a_{i1}, a_{i2}, \dots, a_{in}]$ ifadesine matrisin satırları ve $j = 1, 2, \dots, n$ için

$$c_j = \begin{bmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{bmatrix}$$

ifadesine de matrisin sütunları denir. m satırlı n sütunlu bir matrise $m \times n$ boyutlu (mertebeli) ya da kısaca bir $m \times n$ matrisi denir. i–yinci satır ve j–yinci sütunun kesişiminde bulunan cismin elemanına matrisin (i, j)–yinci elemanı denir. Matris kısaca $A = (a_{ij})_{m \times n}$ notasyonu ile gösterilir (Taşcı 2005).

Tanım 2.2.2: Verilen iki matrisin eşit olması için aşağıdaki şartlar sağlanmalıdır:

i. Verilen iki matrisin satır ve sütun sayıları aynı olmalıdır.

ii. Aynı pozisyondaki elemanlar eşit olmalıdır.

Daha açık bir ifade ile; eğer $A = (a_{ij})$ ve $B = (b_{ij})$ ise, o zaman $A = B$ olması için gerek ve yeter şart $\forall i = 1, 2, \dots, m$ ve $\forall j = 1, 2, \dots, n$ için $a_{ij} = b_{ij}$ olmasıdır (Taşcı 2005).

Tanım 2.2.3: $A = (a_{ij})_{m \times n}$ ve $B = (b_{ij})_{m \times n}$ matrislerinin $A + B$ toplamı, A ve B matrislerinin aynı adresteki elemanlarının toplamı olarak tanımlanır. Yani,

$$A + B = [a_{ij}]_{m \times n} + [b_{ij}]_{m \times n} = [a_{ij} + b_{ij}]_{m \times n}$$

olur (Başar 2012).

Tanım 2.2.5: $A = \left(a_{ij}\right)_{m\times n}$ matrisinin bir $\alpha \in \mathbb{C}$ skaleri ile αA çarpımı, A matrisinin bütün elemanlarının α skaleri ile çarpımı olarak tanımlanır. Yani,

$$\alpha A = \alpha\left[a_{ij}\right]_{m\times n} = \left[\alpha a_{ij}\right]_{m\times n}$$

olur (Başar 2012).

Teorem 2.2.1: A, B ve C aynı mertebeden matrisler ve λ_1, λ_2 birer skaler olmak üzere,

(i) $A + B = B + A$ (değişme özelliği)

(ii) $A + (B + C) = (A + B) + C$ (birleşme özelliği)

(iii) $A + 0 = A$ (etkisiz eleman)

(iv) $A - A = 0$

(v) $\lambda_1(A + B) = \lambda_1 A + \lambda_1 B$

(vi) $(\lambda_1 + \lambda_2)A = \lambda_1 A + \lambda_2 A$

(vii) $(\lambda_1\lambda_2)A = \lambda_1(\lambda_2 A)$

(viii) $1.A = A$

özellikleri vardır (Ağargün ve Özdağ 2008).

Tanım 2.2.6: Bir satır matris ile bir sütun matrisinin çarpılabilmesi için onların her birinin aynı elemana sahip olması gerekir. Eğer $u = [u_1, \dots, u_m]$ ve $v = \begin{bmatrix} v_1 \\ \vdots \\ v_m \end{bmatrix}$ ise, o zaman uv aşağıdaki gibi tanımlanan 1×1 bir matristir:

$$uv = [u_1v_1 + u_2v_2 + \cdots + u_mv_m] = \left[\sum_{j=1}^{m} u_iv_j\right]$$

(Taşcı 2005).

Tanım 2.2.7: $A = \left[a_{ij}\right]$ bir $m \times r -$ matris ve $B = \left[b_{ij}\right]$ bir $r \times n -$ matris ise bunların çarpımı $i = 1, 2, \dots, m$; $j = 1, 2, \dots, n$ için,

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ir}b_{rj} = \sum_{k=1}^{r} a_{ik}b_{kj}$$

olmak üzere $AB = \left[c_{ij}\right], m \times n -$ matristir (Ağargün ve Özdağ 2008).

Teorem 2.2.2: Eğer $A = \left(a_{ij}\right)_{m\times n}$, $B = \left(b_{ij}\right)_{n\times t}$ ve $C = \left(c_{ij}\right)_{t\times q}$ ise, o zaman matrislerin çarpma işlemine göre birleşme (assosyatif) kuralı denilen aşağıdaki kural geçerlidir (Taşcı 2005):

$$A(BC) = (AB)C \qquad (2.1).$$

İspat: İspat için matrislerin eşitliği tanımı kullanılacaktır. Buna göre eğer (2.1) eşitliğinin her iki tarafındaki matris çarpımlarından elde edilen matrislerin mertebelerinin ve karşılıklı elemanlarının eşit olduğunu göstermek ispat için yeterlidir.

Önce (2.1) eşitliğinin sol tarafını göz önüne alalım. $BC = D$ ve D' nin genel elemanı d_{ij} ile gösterilirse, o zaman

$$BC = \left(b_{ij}\right)_{n\times t}\left(c_{ij}\right)_{t\times q} = \left(d_{ij}\right)_{n\times q} = D$$

ve

$$d_{ij} = \sum_{k=1}^{t} b_{ik}c_{kj} \qquad (2.2)$$

yazılır. Şimdi ise $A(BC) = AD = E$ ve E' nin genel elemanı e_{ij} olarak alınırsa, bu takdirde

$$AD = \left(a_{ij}\right)_{m\times n}\left(d_{ij}\right)_{n\times q} = \left(e_{ij}\right)_{m\times q} = E \qquad (2.3)$$

ve

$$e_{ij} = \sum_{s=1}^{n} a_{is}d_{sj} \qquad (2.4)$$

yazılır. (2.2) ifadesinden

$$d_{sj} = \sum_{k=1}^{t} b_{sk} c_{kj} \tag{2.5}$$

eşitliğini yazmak mümkündür. (2.5) ifadesi (2.4) de yerine yazılırsa

$$\begin{aligned} e_{ij} &= \sum_{s=1}^{n} a_{is} \left(\sum_{k=1}^{t} b_{sk} c_{kj} \right) \\ &= \sum_{k=1}^{t} \sum_{s=1}^{n} a_{is} \left(b_{sk} c_{kj} \right) \\ &= \sum_{k=1}^{t} \sum_{s=1}^{n} (a_{is} b_{sk}) c_{kj} \end{aligned} \tag{2.6}$$

elde edilir. Şimdi de eşitliğin sağ tarafını göz önüne alalım. $AB = F$ ve F' nin genel elemanına f_{ij} denilirse, o zaman

$$AB = \left(a_{ij}\right)_{m\times n} \left(b_{ij}\right)_{n\times t} = \left(f_{ij}\right)_{m\times t} = F$$

ve

$$f_{ij} = \sum_{s=1}^{n} a_{is} b_{sj} \tag{2.7}$$

yazılır. Bu defa da $(AB)C = FC = G$ ve G' nin genel elemanına g_{ij} denirse, o zaman da

$$(AB)C = FC = \left(f_{ij}\right)_{m\times t} \left(c_{ij}\right)_{t\times q} = \left(g_{ij}\right)_{m\times q} = G \tag{2.8}$$

ve

$$g_{ij} = \sum_{k=1}^{t} f_{ik} c_{kj} \tag{2.9}$$

yazılır. (2.7) ifadesinden

$$f_{ik} = \sum_{s=1}^{n} a_{is} b_{sk} \qquad (2.10)$$

yazmak mümkündür. (2.10) ifadesi (2.9) da yerine yazılırsa

$$g_{ij} = \sum_{k=1}^{t} \left(\sum_{s=1}^{n} a_{is} b_{sk} \right) c_{kj}$$

$$= \sum_{k=1}^{t} \sum_{s=1}^{n} (a_{is} b_{sk}) c_{kj} \qquad (2.11)$$

elde edilir. Böylece (2.3) ve (2.8) ifadelerinden E ve G matrislerinin mertebelerinin eşit olduğu, (2.6) ve (2.11) den E ve G' nin karşılıklı elemanlarının eşit olduğu sonucu ortaya çıkar. Yani $E = G$ olur. Bu ise (2.1) eşitliğinin doğru olduğunu gösterir.

Teorem 2.2.3: (i) $A = (a_{ij})_{m \times n}$, $B = (b_{ij})_{n \times t}$ ve $C = (c_{ij})_{n \times t}$ olmak üzere, sol dağılma kuralı denilen

$$A(B + C) = AB + AC \qquad (2.12)$$

kuralı geçerlidir.

(ii) $A = (a_{ij})_{m \times n}$, $B = (b_{ij})_{t \times m}$ ve $C = (c_{ij})_{t \times m}$ olmak üzere, sağ dağılma kuralı denilen

$$(B + C)A = BA + CA \qquad (2.13)$$

kuralı geçerlidir (Taşcı 2005).

İspat: (i) Önce (2.12) 'nin sol tarafı göz önüne alalım. $B + C = D$ ve D'nin genel elemanı d_{ij} olsun. Bu durumda

$$B + C = (b_{ij})_{n \times t} + (c_{ij})_{n \times t} = (d_{ij})_{n \times t} = D$$

ve

$$d_{ij} = b_{ij} + c_{ij} \tag{2.14}$$

yazılır. Şimdi de $A(B + C) = AD = E$ ve E'nin genel elemanın e_{ij} olduğunu farzedelim. Buna göre

$$AD = (a_{ij})_{m\times n}(d_{ij})_{n\times t} = (e_{ij})_{m\times t} = E \tag{2.15}$$

ve

$$e_{ij} = \sum_{k=1}^{n} a_{ik}\, d_{kj} \tag{2.16}$$

yazılır ve (2.14) den

$$d_{kj} = b_{kj} + c_{kj} \tag{2.17}$$

yazılabileceği kolaylıkla görülür. Böylece (2.17) ifadesi (2.16) da yerine yazılırsa

$$e_{ij} = \sum_{k=1}^{n} a_{ik}\,(b_{kj} + c_{kj}) = \sum_{k=1}^{n} (a_{ik}b_{kj} + a_{ik}c_{kj})$$

$$= \sum_{k=1}^{n} a_{ik}b_{kj} + \sum_{k=1}^{n} a_{ik}c_{kj} \tag{2.18}$$

elde edilir. Şimdi de (2.12) ifadesinin sağ tarafı göz önüne alalım. Burada da $AB = Y$; Y 'nin genel elemanı y_{ij}, $AC = Z$ ve Z 'nin genel elemanın z_{ij} olduğu kabul edilsin. Buna göre

$$AB = (a_{ij})_{m\times n}(b_{ij})_{n\times t} = (y_{ij})_{m\times t} = Y \tag{2.19}$$

ve

$$y_{ij} = \sum_{k=1}^{n} a_{ik}\, b_{kj} \tag{2.20}$$

yazılır. Yine aynı şekilde

$$AC = (a_{ij})_{m\times n}(c_{ij})_{n\times t} = (z_{ij})_{m\times t} = Z \tag{2.21}$$

ve

$$z_{ij} = \sum_{k=1}^{n} a_{ik}\, c_{kj} \tag{2.22}$$

ifadeleri yazılır. Son olarak $AB + AC = T$ ve T 'nin genel elemanı t_{ij} ile gösterilirse o zaman

$$\begin{aligned} AB + AC &= Y + Z = \left(y_{ij}\right)_{m\times t} + \left(z_{ij}\right)_{m\times t} \\ &= \left(y_{ij} + z_{ij}\right)_{m\times t} = \left(t_{ij}\right)_{m\times t} = T \end{aligned} \tag{2.23}$$

$$t_{ij} = \sum_{k=1}^{n} a_{ik}\, b_{kj} + \sum_{k=1}^{n} a_{ik}\, c_{kj} \tag{2.24}$$

ifadeleri elde edilir. Bu durumda (2.15) ve (2.23) 'den E ve T matrislerinin mertebeleri eşit olduğu yine (2.18) ve (2.24) 'den E ve T matrislerinin elemanlarının eşit olduğu sonucu elde edilir. Bu da matrislerin eşitliği tanımına göre $E = T$ olmasını gerektirir. Bu eşitlik ise (2.12) ifadesinin doğru olduğunu gösterir.

(ii) için ispat benzerdir.

Tanım 2.2.8: Bir $A = \left(a_{ij}\right)_{m\times n}$ matrisinin satırlarını aynı numaralı sütunlarıyla yer değiştirmekle elde edilen matrise, A matrisinin transpozu denir ve A^T ile gösterilir. Yani, $A^T = \left[a_{ij}\right]_{m\times n}^{T} = \left[a_{ij}\right]_{n\times m}$. Mesela;

$$A = \begin{bmatrix} 1 & 2 & 5 & 4 \\ 7 & -3 & 2 & 6 \\ 0 & 1 & 3 & -1 \end{bmatrix}$$

matrisinin transpozu,

$$A^T = \begin{bmatrix} 1 & 7 & 0 \\ 2 & -3 & 1 \\ 5 & 2 & 3 \\ 4 & 6 & -1 \end{bmatrix}$$

matrisidir (Başar 2012).

Tanım 2.2.9: Her elemanı sıfır olan matrise sıfır matris denir. Sıfır matris 0 ile gösterilir (Ağargün ve Özdağ 2008).

Tanım 2.2.10: Satır sayısı sütun sayısına eşit olan bir matrise kare matris denir.

$$E = \begin{bmatrix} i-1 & 0 \\ 2 & i-5 \end{bmatrix}$$

matrisi 2 × 2 mertebeden bir kare matristir (Ağargün ve Özdağ 2008).

Tanım 2.2.11: $A = [a_{ij}]$, $n \times n$ mertebesinden bir kare matris ise $a_{11}, a_{22}, a_{33}, \dots, a_{nn}$ elemanlarına A nın asal köşegen elemanları denir. Bir kare matriste asal köşegen dışındaki elemanlar sıfırsa matrise köşegen matris denir. Köşegen matrise örnek olarak

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 5 \end{bmatrix}$$

matrisini verilebilir (Ağargün ve Özdağ 2008).

Tanım 2.2.12: Bir köşegen matriste asal köşegen elemanları birbirine eşitse yani $a_{11} = a_{22} = a_{33} = \cdots = a_{nn} = k$ ise matrise skaler matris denir.

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}$$

matrisi bir skaler matristir (Ağargün ve Özdağ 2008).

Tanım 2.2.13: Bir skaler matriste asal köşegen üzerindeki bütün elemanları 1 ise matrise birim matris denir. $n \times n$ mertebeden birim matris I_n ile gösterilir.

$$I_1 = [1], \qquad I_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad I_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

matrisleri birer birim matristir (Ağargün ve Özdağ 2008).

Tanım 2.2.14: Bir n- kare $A = [a_{ij}]$ matrisi; $j > i$ olan her $i, j \in \{1,2,\ldots,n\}$ için $a_{ij} = 0$ iken alt üçgen matris ve $j < i$ olan her $i, j \in \{1,2,\ldots,n\}$ için $a_{ij} = 0$ iken üst üçgen matris diye adlandırılır.

Buna göre; n- kare $A = [a_{ij}]$ alt ve $B = [b_{ij}]$ üst üçgen matrisler;

$$A = \begin{bmatrix} a_{11} & 0 & 0 & \cdots & 0 \\ a_{21} & a_{22} & 0 & \cdots & 0 \\ a_{31} & a_{32} & a_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn} \end{bmatrix} \quad \text{ve} \quad B = \begin{bmatrix} b_{11} & b_{12} & b_{13} & \cdots & b_{1n} \\ 0 & b_{22} & b_{23} & \cdots & b_{2n} \\ 0 & 0 & b_{33} & \cdots & b_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & b_{nn} \end{bmatrix}$$

şeklindedir (Başar 2012).

Tanım 2.2.15: Bir n- kare A matrisi; $A^T = A$ olması halinde simetrik matris ve $A^T = -A$ olması halinde de ters simetrik matris diye adlandırılır.

$$A = \begin{bmatrix} 0 & 4 & 3 \\ -4 & 0 & 2 \\ -3 & -2 & 0 \end{bmatrix} \text{ ters simetrik matris ve } B = \begin{bmatrix} 2 & 5 & -3 & 6 \\ 5 & 0 & 1 & 3 \\ -3 & 1 & 4 & 0 \\ 6 & 3 & 0 & 7 \end{bmatrix} \text{ simetrik bir matristir.}$$

Tanım 2.2.16: Kompleks cisim üzerinde bir n- kare A matrisi; $\overline{A^T} = A$ olması halinde Hermityen matris ve $\overline{A^T} = -A$ olması halinde de ters Hermityen matris diye adlandırılır.

$$A = \begin{bmatrix} 2 & 2-i & 1+2i \\ 2+i & 5 & -6i \\ 1-2i & 6i & 4 \end{bmatrix} \text{ matrisi Hermityen ve } B = \begin{bmatrix} 0 & 4i & 4 & -5-3i \\ 3i & -2i & 3+5i & 1-3i \\ -4 & -3+5i & 0 & 5-i \\ 5-3i & -1-3i & -5-i & 4i \end{bmatrix}$$

matrisi ters Hermityendir.

Tanım 2.2.17: Eğer $A = (a_{ij})_{n\times n}$ kara matrisi için $a_{i,j+1} = 1,\ a_{n1} = 1$ ve diğer bütün elemanlar sıfır oluyorsa o zaman A matrisine permütasyon matris denir (Taşcı 2005).

Tanım 2.2.18: Eğer $A\ \ n \times n$ bir kare matris ve $I\ n \times n$ birim matris olmak üzere,

$$AB = BA = I$$

olacak şekilde bir $n \times n\ \ B$ matrisi varsa, o zaman B matrisine A matrisinin tersi denir ve $B = A^{-1}$ ile gösterilir. Tersi olan matrislere de ters çevrilebilir (düzgün, tekil olmayan) matrisler denir (Taşcı 2005).

Teorem 2.2.4: Bir kare matrisin tersi varsa o zaman bu ters tekdir (Taşcı 2005).

İspat: Bir A kare matrisin B ve C gibi iki tane tersinin olduğunu varsayalım. Bu durumda ters matrisin tanımından dolayı A matrisinin tersi B ise,

$$AB = BA = I \qquad (2.25)$$

ve eğer A matrisinin tersi C ise,

$$AC = CA = I \qquad (2.26)$$

yazılır. Eğer $B = C$ olduğu gösterilirse ispat tamamlanmış olur. Bunu için (2.25) ve (2.26) ifadelerini ve matrislerin çarpma işlemine göre birleşme özelliğini göz önüne alarak

$$B = I\ \ B = (CA)B = C(AB) = C\ \ I = C$$

eşitliği elde edilir ve ispat tamamlanmış olur.

Tanım 2.2.19: Bir terse sahip olan bir A kare matrisine tekil olmayan veya ters çevrilebilir bir matris denir. Eğer A matrisi bir terse sahip değilse, o takdirde A matrisine tekil veya ters çevrilemez matris denir (Taşcı 2005).

Teorem 2.2.5: Eğer A ve B ters çevrilebilir iki $n \times n$ matris ise, o zaman AB çarpımı da ters çevrilebilirdir ve

$$(AB)^{-1} = B^{-1}A^{-1}$$

dir (Taşcı 2005).

İspat: Eğer A ve B matrisleri ters çevrilebilir matrisler ise, o takdirde ters matris tanımından

$$AA^{-1} = A^{-1}A = I \text{ ve } BB^{-1} = B^{-1}B = I$$

yazılır. Diğer taraftan matris çarpımının birleşme özelliğini kullanarak

$$(AB)(B^{-1}A^{-1}) = I \text{ ve } (B^{-1}A^{-1})(AB) = I$$

yazılır. Böylece bunları birleştirerek

$$(AB)(B^{-1}A^{-1}) = (B^{-1}A^{-1})(AB) = I$$

yazmak mümkündür. Bu son ifade ise ters matris tanımı gereğince AB matrisinin tersinin $B^{-1}A^{-1}$ olduğunu ifade eder. Böylece AB ters çevrilebilirdir ve bu invers tek olduğundan

$$(AB)^{-1} = B^{-1}A^{-1}$$

yazılır. Böylece ispat tamamlanmış olur.

Tanım 2.2.20: A sıfır olmayan bir n kare matris olmak üzere

$$AB = 0$$

olacak şekilde sıfırdan farklı bir B, n kare matris varsa, o zaman A matrisine sol sıfır bölen matrisi denir. Yine A sıfırdan farklı bir n kare matris olmak üzere

$$CA = 0$$

olacak şekilde sıfırdan farklı bir C, n kare matris varsa, o zaman da A matrisine sağ sıfır bölen matrisi denir. Eğer A matrisi hem sol sıfır bölen matrisi hem de sağ sıfır bölen matrisi ise, o takdirde A matrisine sadece sıfır bölen matris denir (Taşcı 2005).

Teorem 2.2.6: A sıfır olmayan bir kare matris olmak üzere eğer tersi mevcut ise, o takdirde A matrisi bir sıfır bölen matrisi değildir (Taşcı 2005).

İspat: Eğer $AB = 0$ ya da $CA = 0$ ve A matrisinin tersi A^{-1} ise, o takdirde

$$A^{-1}(AB) = (A^{-1}A)B = IB = B = 0$$

veya

$$(CA)A^{-1} = C(AA^{-1}) = CI = C = 0$$

yazılır. Bu ise A matrisi bir sıfır bölen matrisi olmadığını gösterir.

Tanım 2.2.21: Bir matris aşağıdaki şekilde ise satırca indirgenmiş formdadır denir:

(i) İlk k tane satır sıfırdan farklı ve $(k+1)$ inci satır ile bundan sonraki satırların tüm elemanları sıfırdır.

(ii) Her bir satırdaki sıfırdan farklı ilk eleman 1 dir ve bu 1 ler $s_1 < s_2 < \cdots < s_k$ olacak şekilde s_j ninci sütunda bulunurlar.

(iii) Bir satırdaki sıfırdan farklı ilk eleman $a_{ij} = 1$ ise j inci sütundaki a_{ij} nin altında bulunan tüm elemanlar sıfırdır.

Yukarıdaki (iii) koşulu ‘‘a_{ij} nin bulunduğu sütundaki diğer tüm elemanlar sıfırdır’’ şeklinde alınırsa, (i) - (ii) koşullarını sağlayan matrise satırca indirgenmiş eşolon formdadır denir. Satır yerine sütunlar alınarak sütunca indirgenmiş form ve sütunca indirgenmiş eşolon form elde edilir (Ağargün ve Özdağ 2008).

Tanım 2.2.22: $I,\ n \times n$ birim matris olmak üzere I dan sadece bir elemanter satır işlemi ile elde edilen bir $n \times n$ matrise bir elemanter matris denir ve E ile gösterilir(Taşçı 2005).

Teorem 2.2.7: (i) Eğer B,$m \times n$ matrisi; bir elemanter satır işleminin uygulanması ile A $m \times n$ matrisinden elde edilen bir matris ise, o takdirde B matrisi$A$ matrisi ile bu elemanter satır işlemlerine karşılık gelen $m \times m$ elemanter matrisin çarpımına eşittir. Yani eğer ε ile elemanter satır işlemi gösterilirse, o zaman

$$B = \varepsilon(A) = \varepsilon(I_m)A$$

dır.

(ii) Her elemanter matris ters çevrilebilirdir. Üstelik her elemanter matrisin tersi de yine bir elemanter matristir (Taşcı 2005).

İspat: (i) E_{ij} ile $r_i \leftrightarrow r_j$ elemanter satır işlemine karşılık gelen elemanter matris, $\alpha \neq 0$ olmak üzere $E_i(\alpha)$ ile $r_i \leftrightarrow \alpha r_i$ satır işlemine karşılık gelen elemanter matris ve $E_{ij}(\alpha)$ ile $r_i \leftrightarrow r_i + \alpha r_j$ satır işlemine karşılık gelen elemanter matris gösterilsin. Buna göre $A = (a_{ij})_{m \times n}$ matris olmak üzere,

$$E_{ij}A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{j1} & a_{j2} & \cdots & a_{jn} \\ \vdots & \vdots & \cdots & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \vdots & \vdots & \cdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

şeklinde bir matris olur. Bu da $E_{ij}A$ matrisinin i–yinci satırı ile j–yinci satırın yer değiştirilmesi ile elde edilen bir matris olduğunu gösterir. Gerçekten I, $m \times m$ birim matris olmak üzere bu birim matrisin i–yinci satırı ile j–yinci satırın yer değiştirilmesi ile elde edilen matrise $\varepsilon(I_m)$ dersek ve bu matris ile A matrisini soldan çarparsak yine $E_{ij}A$ matrisi elde edilir. Bu da E_{ij} elemanter matrisi için

$$B = E_{ij}A = \varepsilon(A) = \varepsilon(I_m)A$$

olduğunu gösterir. Benzer şekilde,

$$B = E_i(\alpha)A = \varepsilon(A) = \varepsilon(I_m)A$$

ve

$$B = E_{ij}(\alpha)A = \varepsilon(A) = \varepsilon(I_m)A$$

olduğu gösterilebilir.

(ii) Kolay bir hesap ile,

$$(E_{ij})^{-1} = E_{ij}$$

$$\left(E_i(\alpha)\right)^{-1} = E_i\left(\frac{1}{\alpha}\right)$$

$$\left(E_{ij}(\alpha)\right)^{-1} = E_{ij}(-\alpha)$$

olduğu görülebilir. Buradan gerçekten elemanter matrislerin ters çevrilebilir olduğu ve aynı zamanda elemanter matrisin tersinin de bir elemanter matris olduğu sonucu çıkar.

Tanım 2.2.23: $a_{11}, a_{12}, a_{21}, a_{22}$ reel sayılar olmak üzere 2×2 tipinde bir

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

matrisinin determinantı

$$detA = a_{11}a_{22} - a_{12}a_{21}$$

formülü ile tanımlanan bir reel sayıdır (Taşcı 2005).

Not 2.2.1: Determinant her bir 2×2 matrisine bir reel sayı karşılık getiren bir fonksiyondur. Bu fonksiyon ilk üçü bir 2×2 matrisin üzerinde satır işlemlerinin etkin olduğu, aşağıdaki dört önemli özelliğe sahiptir (Taşcı 2005):

(i) Eğer B matrisi; bir k reel sayısı ile A matrisinin bir satırının çarpılması ile A matrisinden elde edilen bir matris ise, o takdirde

$$detB = k.detA$$

dır.

(ii) Eğer B matrisi; A matrisinin satırlarının yer değiştirilmesi ile A 'dan elde edilen bir matris ise, o zaman

$$detB = -detA$$

dır.

(iii) Eğer B matrisi; A 'nın bir satırının bir skaler katının A 'nın diğer satırına ilave edilmesi ile A matrisinden elde edilen bir matris ise, o zaman

$$detB = detA$$

dır.

(iv) $det\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} = 1$ dır.

Teorem 2.2.8: Her $n \times n$ matrise bir reel sayıyı karşılık getiren ve aşağıdaki özelliklere sahip olan bir ve yalnızca bir fonksiyon, det vardır :

(i) B matrisi; verilen bir $n \times n$ A matrisinin bir satırının bir $\alpha \neq 0$ reel sayısı ile çarpılması sonucu A matrisinden elde edildiği her zaman

$$detB = \alpha detA$$

(ii) B matrisi; verilen bir $n \times n$ A matrisinin herhangi iki satırının yer değiştirilmesi ile A 'dan elde edildiği her zaman

$$detB = -detA$$

(iii) B, $n \times n$ A matrisinin bir satırının bir skaler katının diğer bir satıra ilava edilmesi ile A 'dan elde edildiği matris olduğunda

$$detB = detA$$

(iv) I, $n \times n$ birim matris olmak üzere

$$\det I = 1$$

dir (Taşcı 2005).

Teorem 2.2.9: A bir $n \times n$ kare matris olsun. Buna göre

(i) Eğer A matrisinin iki satırı eşit ise , o zaman $detA = 0$ dır,

(ii) Eğer A matrisi bir sıfır satırına sahipse, o zaman $detA = 0$ dır (Taşcı 2005).

İspat: (i) A matrisinin iki satırının eşit olduğunu farzedelim. B matrisi eşit satırların yer değiştirilmesi ile A dan elde edilen bir matris olsun. Bu durumda $detB = -detA$ yazılabilir. Halbuki yer değiştirilen satırlar eşit olduğundan $B = A$ dir. Sonuç olarak buradan $detA = detB$ olduğu görülür. Böylece

$$detA = detB = -detA$$

ifadesinden $detA = 0$ bulunur.

(ii) A matrisinin bir satırının sıfır olduğunu varsayalım. A 'nın herhangi bir başka satırını seçelim ve onu bir B matrisi elde etmek için sıfır satırına ilave edilsin. Bu durumda $detA = detB$ yazılabilir. Halbuki B matrisi iki eşit satıra sahip olduğundan $detB = 0$ yazmak mümkündür. Bundan dolayı $detA = 0$ olur.

Teorem 2.2.10: Bir köşegen matrisin determinantı matrisin köşegen elemanlarının çarpımına eşittir (Taşcı 2005).

İspat: $A = \begin{bmatrix} a_{11} & 0 & \dots & 0 \\ 0 & a_{22} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{nn} \end{bmatrix}$ olsun. $detB = \alpha detA$ özelliği kullanılarak;

$$detA = det\begin{bmatrix} a_{11} & 0 & \dots & 0 \\ 0 & a_{22} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{nn} \end{bmatrix} = \mathrm{a}_{11}\det\begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & a_{22} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{nn} \end{bmatrix}$$

$$= \mathrm{a}_{11}\mathrm{a}_{22}\det\begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{nn} \end{bmatrix} = \dots = \mathrm{a}_{11}\mathrm{a}_{22}\dots\mathrm{a}_{\mathrm{nn}}\det\begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

$$= \mathrm{a}_{11}\mathrm{a}_{22}\dots\mathrm{a}_{\mathrm{nn}}.\det \mathrm{I}$$

$$= \mathrm{a}_{11}\mathrm{a}_{22}\dots\mathrm{a}_{\mathrm{nn}}$$

elde edilir.

Teorem 2.2.11: Bir üst üçgen (ya da alt üçgen) matrisin determinantı, matrisin köşegen elemanlarının çarpımına eşittir (Taşcı 2005).

İspat: ispatımızı üst üçgen matris için yapıyoruz. Benzer düşünce ile alt üçgen matrisler için ispat yapılabilir.

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{nn} \end{bmatrix}$$

olsun. $detB = \alpha detA$ ve $detB = detA$ özelliklerini kullanarak;

$$detA = det\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{nn} \end{bmatrix} = \mathrm{a_{nn}det}\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

$$= \cdots = \mathrm{a_{22}a_{33} \dots a_{nn}det}\begin{bmatrix} a_{11} & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

$$= \mathrm{a_{11}a_{22} \dots a_{nn}det}\begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

$$= \mathrm{a_{11}a_{22} \dots a_{nn}\ det\, I}$$

$$= \mathrm{a_{11}a_{22} \dots a_{nn}}$$

yazılır.

Teorem 2.2.12: Bir A kare matrisinin determinantı ile A ’nın transpozunun determinant değeri aynıdır. Yani

$$detA = detA^T$$

dir (Taşcı 2005).

Tanım 2.2.27: $A(a_{ij})$ bir $n \times n$ kare matris olsun. A matrisinin i–yinci satır ve j–yinci sütününun silinmesiyle ede edilen matrise A matrisinin alt matrisi denir ve A_{ij} ile gösterilir (Taşcı 2005).

Teorem 2.2.13: Eğer E, bir elemanter matris ise, o zaman

(i) $detE \neq 0$,

(ii) $detE^T = detE$,

(iii) E^{-1} bir elemanter matristir (Taşcı 2005).

İspat: $\alpha \neq 0$ olmak üzere $P_i(\alpha)$ ile $r_i \leftrightarrow \alpha r_i$ elemanter satır işlemine karşılık gelen elemanter matris, P_{ij} ile $r_i \leftrightarrow r_j$ elemanter satır işlemlerine karşılık gelen elemanter matris ve $P_{ij}(\alpha)$ ile $r_i \leftrightarrow r_i + \alpha r_j$ satır işlemine karşılık gelen elemanter matris gösterilsin. Buna göre bu üç farklı tipten elemanter matrislerin determinantları alınır ise, o takdirde

$$detP_i(\alpha) = detP_i(\alpha)^T = \alpha \qquad (i = 1,2,\dots,n)$$

$$detP_{ij} = detP_{ij}{}^T = -1 \qquad (i,j = 1,2,\dots,n)$$

$$detP_{ij}(\alpha) = detP_{ij}(\alpha)^T = 1 \qquad (i,j = 1,2,\dots,n)$$

elde edilir. Bu da (i) ve (ii) yi ispatlar. (iii) ü ispatlamak için sırasıyla

$$P_i(\alpha)^{-1} = P_i(\alpha^{-1})$$

$$P_{ij}{}^{-1} = P_{ij}$$

$$P_{ij}(\alpha)^{-1} = P_{ij}(-\alpha)$$

olduğunu göz önüne almak yeterlidir.

Teorem 2.2.14: Eğer E $n \times n$ bir elemanter matris ise, o zaman her $n \times n$ A matrisi için

$$det(EA) = (detE)(detA)$$

dır (Taşcı 2005).

Teorem 2.2.15: Bir A kare matrisinin ters çevrilebilir olması için gerek ve yeter şart $detA \neq 0$ olmasıdır (Taşcı 2005).

İspat: Eğer A ters çevrilebilir bir matris ise, o zaman

$$E_1E_2 \dots E_kA = I$$

olacak şekilde $E_1, E_2, \dots, E_k$ elemanter matrisleri vardır. Böylece

$$det(E_1)det(E_2) \dots det(E_k)det(A) = \det I = 1$$

yazılır. Bundan dolayı $detA \neq 0$ sonucu elde edilir.

Tersine; eğer A ters çevrilebilir bir matris değilse, o zaman

$$E_1E_2 \dots E_kA = R$$

olacak şekilde $E_1, E_2, \dots, E_k$ elemanter matrisleri vardır. Burada R, bir sıfır satırını kapsayan $n \times n$ bir eşolon matristir.

Böylece $detR = 0$ olur ve $detE_i \neq 0$ $(i = 1,2, \dots, k)$ olduğundan $detA = 0$ olduğu görülür.

Teorem 2.2.16: A ve B, $n \times n$ iki matris olsun. O takdirde

$$det(AB) = (detA)(detB)$$

dir (Taşcı 2005).

İspat: Eğer A bir elemanter matris ise, o zaman iddianın doğru olduğu söylenebilir. A matrisi elemanter matrislerin bir çarpımı olduğundan eşitlik yine doğrudur. Gerçekten E_1 ve E_2 elemanter matrisler olmak üzere

$$A = E_1E_2$$

ise, o zaman elemanter matris için determinant özelliği iki kez art arda uygulanması ile

$$\begin{aligned} det(AB) &= det(E_1E_2B) = det(E_1)det(E_2B) \\ &= det(E_1)det(E_2)det(B) \\ &= det(E_1E_2)det(B) \\ &= det(A)det(B) \end{aligned}$$

yazılır. $k > 2$ olmak üzere

$$A = E_1 E_2 \dots E_k$$

olduğu zaman da ispat benzer olarak yapılabilir. Diğer taraftan her ters çevrilebilir matris elemanter matrislerin bir çarpımı olarak yazılabildiğinden A matrisinin ters çevrilebilir olduğu her zaman

$$det(AB) = det(A)det(B)$$

eşitliği geçerlidir. Eğer A matrisi ters çevrilebilir değilse, o takdirde $detA = 0$ ve $det(AB) = 0$ dır. Böylece bu durumda da $det(AB) = (detA)(detB)$ ifadesi geçerlidir.

$N \geq 1$ için $\mathbb{F}_2^N$, $\mathbb{F}_2 = \{0,1\}$ çift cisim üzerinde bir N boyutlu vektör uzayı ve V_n 'de, $f: \mathbb{F}_2^N \to \mathbb{C}$ şeklinde tanımlanan bütün fonksiyonların 2^N boyutlu kompleks grup cebiri olsun. V_n kümesi üzerinde tanımlanan ikili işlem $f, g \in V_n$ için

$$(f * g)(x) = \sum_{y \in F_2^N} f(y) g(x + y), \qquad x \in \mathbb{F}_2^N$$

şeklindedir.

V_n cebirinin her bir karakteri

$$\mathcal{X}y(x) = \mathcal{X}x(y) = (-1)^{x.y}, \qquad x.y \in \mathbb{F}_2^N$$

şeklinde yazılabilir. Burada $x.y = x_1 y_1, + \cdots + x_N y_N$ olup x ve y , $\{1,2, \dots, N\}$ indekslerinin alt kümesi olarak yorumlanır. Bu yorumdan

$$x.y = |x \cap y|$$

dir. Burada $|x \cap y|$ kardinaliteliği (eleman sayısını) gösterir.

Yukarıdaki yoruma göre $x \in \mathbb{F}_2^N$ 'nin Hamming ağırlığı için $|x| = wt(x)$ gösterimi kullanılır ve aynı zamanda $x + y$, x ve y alt kümelerinin simetrik farkı olur. $x \in \mathbb{F}_2^N$,

$\{1,2,\ldots,N\}$ indekslerinin bir alt kümesi olarak yorumlandığı zaman x 'in komplementi için $\bar{x}$ gösterimi kullanılır.

(Daha fazla bilgi için [15] 'e bakınız.)

Tanım 2.2.27: $T_y(x) = \begin{cases} 1, & x = y \\ 0, & x \neq y \end{cases}$ olmak üzere

$$\langle \mathcal{X}x, \mathcal{X}y \rangle = 2^N \; T_y(x)$$

şeklinde olup her $f \in V_n$ için $\mathcal{F}(f) = \hat{f} \in V_N$ Fourier dönüşüm (Hadamard dönüşümü)

$$\mathcal{F}(f)(y) = \hat{f}(y) = \sum_{x \in \mathbb{F}_2^N} f(x)\, \mathcal{X}x(y) = \langle \mathcal{X}y.f \rangle, \quad y \in \mathbb{F}_2^N \qquad (2.27)$$

şeklinde tanımlanır (Gogin ve Hirvencalo 2007).

Not 2.2.2: Hadamard dönüşümlerin en iyi bilinen iki özelliği aşağıdaki gibidir:

(i) $\hat{\hat{f}} = 2^N f, \quad \langle \hat{f}\hat{g} \rangle = 2^N \langle f, g \rangle$ (2.28)

(ii) $\mathcal{F}(f * g) = \mathcal{F}(f).\mathcal{F}(g), \qquad \mathcal{F}(f.g) = 2^{-N}\mathcal{F}(f) * \mathcal{F}(g),$ (2.29)

(Gogin ve Hirvencalo 2007).

Tanım 2.2.28: Her $r \in [O, N]$ ve $\psi_r^{(N)} (\equiv \psi_r)$,

$$\psi_r(x) = \begin{cases} 1, & x \in S_r^{(N)} \\ 0, & x \notin S_r^{(N)} \end{cases}$$

olacak şekilde,

$$S_r^{(N)} \equiv S_r = \{\, x \in \mathbb{F}_2^N \;\; | \; wt(x) = r \}$$

$\mathbb{F}_2^N$ de r-inci Hamming küre olsun.

Her $f \in V_n$ fonksiyonu için

$$A_r(f) = \langle \psi_r, f \rangle = \sum_{x \in S_r^{(N)}} f(x), \qquad 0 \leq r \leq N$$

şeklinde tanımlanır ve $\left(A_0(f), A_1(f), \ldots, A_N(f)\right)^T \in \mathbb{C}^{N+1}$, f 'nin ağırlık spektrumu olarak adlandırılır (Gogin ve Hirvencalo 2007).

Tanım 2.2.29: (2.28) formülüne göre

$$A_r(\hat{f}) = \langle \psi_r, \hat{f} \rangle = 2^{-N} \langle \hat{\psi}_r, \hat{\hat{f}} \rangle = \langle \hat{\psi}_r, f \rangle, \qquad (2.30)$$

dir. Diğer yandan, (2.27) formülüne göre

$$\hat{\psi}_r(x) = \langle \mathcal{X}x, \psi_r \rangle = \sum_{y \in S_r} \mathcal{X}y(x) = K_r^{(N)}(x)$$

dir. Burada $x = |x|$ ve $K_r^{(N)}(x)$,

$$K_r^{(N)}(x) = K_r(x) = \sum_{i=0}^{r} (-1)^i \binom{N-x}{r-i} \binom{x}{i}$$

şeklinde tanımlanan N mertebeli r-inci Krawtchouck polinomudur. Burada $K_0^0(0) = 1$ dir (Gogin ve Hirvencalo 2007).

Tanım 2.2.31: N mertebeli MacWilliams matrisi

$$(M_N)_{ij} = K_i^{(N)}(j) \qquad 0 \leq i, j \leq N$$

şeklinde tanımlanır. Burada $(M_0)_{ij} = 1$ dir (Gogin ve Hirvencalo 2007).

Not 2.2.3: Krawtchouck polinomları ve MacWilliams matrisleri için bazı önemli formüller aşağıdaki gibidir (Gogin ve Hirvencalo 2007):

1. Geren fonksiyon;

$$(1+t)^{N-z}(1-t)^z = \sum_{k=0}^{\infty} K_k^{(N)}(z) t^k$$

şeklindedir.

2. $$K_r^{(N)}(z) = \sum_{l=0}^{r} (-1)^l \binom{N-z}{r-l} \binom{z}{l}$$

$$= \sum_{l=0}^{r} (-1)^l 2^{r-l} \binom{N-r+l}{l} \binom{N-z}{r-l}$$

$$= \sum_{l=0}^{r} (-2)^l \binom{N-l}{r-l} \binom{z}{l}$$

şeklindedir. Burada $K_0^0(0) = 1$ olduğu açıktır.

$K_r^{(N)}(z)$ polinomunun baş katsayısı $\frac{(-2)^r}{r!}$ dir.

3. $C = diag\left(\binom{N}{0}, \binom{N}{1}, \dots, \binom{N}{N}\right)$ olsun. Bu durumda aşağıdaki eşitlik sağlanır:

$$\sum_{\text{İ}=0}^{N} \binom{N}{i} K_r(i)\, K_s(i) = 2^N \binom{N}{r} \delta_{r,s}$$

yani $M_N C M_M^T = 2^N C$ dir.

$$\sum_{i=0}^{N} K_r(i) K_i(s) = 2^N \delta_{r,s}$$

yani $M_N^2 = 2^N I$ dir.

4. Herhangi bir z için;

$$K_r^{(N)}(z) = (-1)^r K_r^{(N)}(N-z)$$

$z \in \{0,1,\dots,N\}$ için;

$$K_r^{(N)}(z) = (-1)^z K_{N-r}^{(N)}(z)$$

ve

$$\binom{N}{r} K_s(r) = \binom{N}{s} K_r(s)$$

yani $M_N^T = C^{-1} M_n C$ dir.

5. Krawtchouck polinomları için aşağıdaki indirgeme bağıntıları söz konusudur:

a) $$(r+1)K_{r+1}(z) = (N-2z)K_r(z) - (N-r+1)K_{r-1}(z),$$

$$K_0(z) = 1, \;\; K_1(z) = N - 2z.$$

b) $$(N-r)K_l(r+1) = (N-2l)K_l(r) - rK_l(r-1),$$

$$K_l(0) = \binom{N}{l}, \;\; K_l(1) = \binom{N}{l}\left(1 - \frac{2l}{N}\right).$$

c) $$d_N(j) = \begin{cases} 1, & j \in \{0, N\} \\ \frac{1}{2}, & j \notin \{0, N\} \end{cases}$$ ve $0 \leq i, j \leq N$ olmak üzere;

$$K_i^{(N)}(j) = d_N(j)\Big(K_i^{(N-1)}(j) + K_{i-1}^{(N-1)}(j)$$

$$+ K_i^{(N-1)}(j-1) - K_{i-1}^{(N-1)}(j-1)\Big), \quad N \geq 1$$

dir. Burada ve $K_i^{(N-1)}(N) = K_N^{(N-1)}(j) = 0$ ve $i = -1$ veya $j = -1$ için her iki durumda da $K_i(j) = 0$ dır.

Örnek 2.2.1: M_0, M_1 ve M_2 MacWilliams matrisleri olsun.

$$M_0 = (1),$$

$$M_1 = \left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right) \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$M_2 = \left(\begin{pmatrix} 1 & 1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & -1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix}\right.$$

$$\left. - \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & -1 \end{pmatrix}\right) \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 & 1 \\ 2 & 0 & -2 \\ 1 & -1 & 1 \end{pmatrix}$$

(Gogin ve Hirvencalo 2007).

Herhangi bir $y \in \mathbb{F}_2^N$ için $By : \mathbb{F}_2^N \rightarrow \mathbb{C}$ bir fonksiyonu

$$B_y(x) = \binom{|y|}{|x \cap y|} . \mathcal{X}y(x), \quad x \in \mathbb{F}_2^N$$

şeklinde tanımlanır. By fonksiyonu hakkında daha fazla bilgi için $[18]$ 'e bakınız.

Her $r \in \{0,1, \dots, N\}$ için By fonksiyonu, V_n grup cebiri için bir tabanından olup

$$\sum_{y \in S_r} B_y(x) = \sum_{i=0}^{r} (-1)^i \binom{r}{i} \binom{N-|x|}{r-i} \binom{|x|}{i}$$

eşitliği yalnızca $x = |x|$ bağlı olarak elde edilir.

Tanım 2.2.32: N mertebeli r-inci ayrık Chebyshev polinomu

$$D_r^{(N)}(x) = D_r(x) = \sum_{i=0}^{r} (-1)^i \binom{r}{i} \binom{N-x}{r-i} \binom{x}{i}$$

şeklinde tanımlanır. Burada $D_0^0(0) = 1$ dir (Gogin ve Hirvencalo 2007).

Tanım 2.2.33: $(D_N)_{ij} = D_i^{(N)}(j), \qquad 0 \leq i,j \leq N$

şeklindeki $(N+1) \times (N+1)$ boyutlu matrise N mertebeli Chebyshev matrisi denir. Burada $N = 0$ ise $(D_0)_{ij} = 1$ ve $(M_1)_{ij} = (D_1)_{ij} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ dir (Gogin ve Hirvencalo 2007).

Not 2.2.4: Chebyshev polinomları ve matrisleri için bazı önemli formüller aşağıdaki gibidir (Gogin ve Hirvencalo 2007):

1. $D_n^{(N)}(x) = (-1)^n \Delta^n \left(\binom{x}{n} \binom{x-N-1}{n} \right),$

Burada Δ^n, $\Delta f(x) = f(x+1) - f(x)$ olarak tanımlanan fark operatörünün n-inci kuvvetidir.

2.

$$D_n^{(N)}(x) = \sum_{i=0}^{n} (-1)^i \binom{n}{i}\binom{N-x}{n-i}\binom{x}{i}$$

$$= \sum_{i=0}^{n} (-1)^i \binom{n+i}{n}\binom{N-i}{n-i}\binom{x}{i}$$

$$= \sum_{i=0}^{n} \binom{n-N-1}{i}\binom{n+N+1}{n-i}\binom{x+i}{n}.$$

3. $D_N D_N^T = diag(\gamma_0, \gamma_1, \dots, \gamma_N)$ olsun. Bu durumda aşağıdaki eşitlik sağlanır:

$$\sum_{i=0}^{N} D_r\,(i) D_s(i) = \gamma_r \delta_{r,s}$$

Burada $\gamma_r = \binom{2r}{r}\binom{N+1+r}{2r+1}$ 'dır.

4. $$D_n(N-x) = (-1)^n D_n(x),$$

$$D_n^{(N)}(0) = \binom{N}{n}, \quad D_N^{(N)}(m) = (-1)^m \binom{N}{m}.$$

N çift sayısı için,

$$D_n^{(N)}\left(\frac{N}{2}\right) = \begin{cases} O, & n \; tek \; ise \\ (-1)^m \binom{\frac{N}{2}}{m}\binom{\frac{N}{2}+m}{m}, & n = 2m \; ise \end{cases}$$

$D_n^{(N)}$ polinomunun baş katsayısı $\frac{(-1)^n}{n!}\binom{2n}{n}$ dir.

$$D_0(x) = 1, \; D_1(x) = -2x + N, \; D_2(x) = 3x^2 - 3Nx + \binom{N}{2}.$$

5. Chebyshev polinomları için aşağıdaki indirgeme bağıntıları söz konusudur:

a) $$n^2 D_n = (2n-1)D_1 D_{n-1} - (N+n)(N-n+2)D_{n-2},$$

b) $$\Delta\big((x+1)(x-N)\Delta D_n(x)\big) = n(n+1)D_n(x+1),$$

$$D_n(0) = \binom{N}{n}, \quad D_n(1) = \binom{N-1}{n} - n\binom{N-1}{n-1}.$$

c) $$nD_n^{(N)}(x) = nD_n^{(N-1)}(x-1) + (N-x)D_{n-1}^{(N-1)}(x)$$

$$-(N+n-x)D_{n-1}^{(N-1)}(x-1), \qquad N \geq 1.$$

Örnek 2.2.2: D_0, D_1 ve D_2 Chebyshev matrisleri olsun.

$$D_0 = (1),$$

$$D_1 = \left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right)$$

$$-\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\left(\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\right)\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$+\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

$$D_2 = \left(\begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & -1 \end{pmatrix}\right)$$

$$-\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{2} \end{pmatrix}\left(\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & -1 \end{pmatrix} - \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & -1 & 0 \end{pmatrix}\right)\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$+\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 0 & -2 \\ 1 & -2 & 1 \end{pmatrix}$$

(Gogin ve Hirvencalo 2007).

3. MATERYAL VE YÖNTEM

3.1 Genelleştirilmiş Fibonacci Matrisi Yardımı ile Devirli Grupların Elde Edilmesi

Tanım 3.1.1: $\boldsymbol{f_n^{(k)}}$**,** $1 \leq i < k$ için $f_i^{(k)} = 0$ ve $f_k^{(k)} = 1$ sınır şartlarıyla tanımlı, $n > k$ için,

$$f_n^{(k)} = \sum_{j=1}^{k} f_{n-j}^{(k)} \tag{3.1}$$

k-basamak Fibonacci dizisinin n. elemanıdır. $f_i^{(k,m)} \equiv f_i^{(k)}(mod\ m)$ olmak üzere bu dizi m modülüne göre indirgenirse, tekrar eden,

$$f(k,m) = \left(f_1^{(k,m)}, f_2^{(k,m)}, \dots, f_n^{(k,m)} \dots\right)$$

dizisi elde edilir.

O zaman $\left(f_1^{(k,m)}, f_2^{(k,m)}, \dots, f_k^{(k,m)}\right) = (0,0,\dots,1)$ olup bu dizi için (3.1) deki tekrar eden dizi bağıntıları aynıdır (Lü ve Wang 2007).

Tanım 3.1.2: Eğer dizi belli bir noktadan sonra sabit bir dizinin tekrarı şeklinde meydana geliyorsa bu diziye periyodik dizi denir. Tekrar eden alt dizideki eleman sayısına ise dizinin periyodu denir. Örneğin; $a, b, c, d, e, f, g, d, e, f, g, \cdots$dizisi periyodik olup periyodu 4' dir.

Tanım 3.1.3: Eğer bir dizideki ilk l eleman tekrar eden bir alt dizi şeklinde ise bu diziye l periyotlu basit periyodik dizi denir. Örneğin;$a,b,c,d,e,a,b,c,d,e,\cdots$ dizisi basit periyodik olup periyodu 5' dir.

Teorem 3.1.1: $f\left(k,m\right)$ basit periyodik bir dizidir (Lü ve Wang 2007).

İspat: $S_k = \{(a_1, a_2, \dots, a_k) \mid 0 \leq a_i \leq m-1\}$

olsun.$|S_k| = m^k$ olup sonludur, yani her $u \geq 0$ için

$$f_{u+1}^{(k,m)} = f_{v+1}^{(k,m)}, \dots, f_{u+k}^{(k,m)} = f_{v+k}^{(k,m)}$$

olacak şekilde $v \geq u$ sayısı vardır. Tanımdan,

$$f_{n+k}^{(k)} = \sum_{j=0}^{k-1} f_{n+j}^{(k)}$$

olur. Yani,

$$f_n^{(k)} = f_{n+k}^{k} - \sum_{j=0}^{k-1} f_{n+j}^{(k)}$$

dir. Buradan kolaylıkla,

$$f_u^{(k,m)} = f_v^{(k,m)}, f_{u-1}^{(k,m)} = f_{v-1}^{(k,m)}, f_{u-2}^{(k,m)} = f_{v-2}^{(k,m)}, \dots, f_2^{(k,m)} = f_{v-u+2}^{(k,m)}$$

ve $\mathrm{f}_1^{(\mathrm{k,m})} = f_{v-u+1}^{(k,m)}$ olduğu görülebilir. Böylece $f(k,m)$ basit periyodik bir dizidir. Böylece ispat tamamlanır.

$h_k(m)$ ile $f(k,m)$ nin en küçük periodu gösterilir, $f(k,m)$ nin periodu veya m modülüne göre k-basamak Fibonacci dizisinin Wall sayısı diye adlandırılır.

Örnek 3.1.1: $s(4,3) = (0,0,0,1,1,2,1,2,0,2,2,0,1,2,2,2,1,1,0,1,0,2,0,0,2,1,0,0,0,1, \dots)$ dizisi ele alınırsa, bu dizi $k = 4$ basamak için her 26 terimde bir başlangıç elemanlarıyla tekrar edip $h_4(3) = 26$ olur (Lü ve Wang 2007).

p_i ler asal sayılar ve e_i ler pozitif tamsayılar olmak üzere, $m = \prod_{i=1}^{t} p_i^{e_i} (t \geq 1)$ ise $h_k(m)$, $h_k(p_i^{e_i})$ lerin en küçük ortak katıdır.

$$G = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 1 & 1 & \dots & 1 \end{bmatrix}$$

şeklinde ifade edilen $k \times k$ tipli karesel bir matris olsun.

a_{ij} 'ler tamsayılar olmak üzere verilen bir $A = [a_{ij}]$ matrisi için, A matrisinin her elemanının $mod\, m$ ye göre indirgenmesi $A\, mod(m)$ şeklinde ifade edilir. Yani, $A\, mod(m) = a_{ij}(mod\, m)$ 'dir. $\langle G \rangle_m = \{G^i(modm) | \, i \geq 0\}$ olsun.

$$G^i(0,0,\dots,1)^T(mod\, m) = \left(f_{i+1}^{(k,m)}, f_{i+2}^{(k,m)}, \dots, f_{i+k}^{(k,m)}\right)$$

dir. Bu durumda $h_k(m)$, aşağıdaki eşitliği sağlayan en küçük h pozitif tamsayısı olarak elde edilir;

$$G^h(0,0,\dots,1)^T(mod\, m) = (0,0,\dots,1).$$

Şimdi, $a_1 = (a_{11}, a_{12}, \dots, a_{1k}) = (0,1,0,\dots,0)$ şeklinde k boyutlu bir vektör olsun. Burada, $a_n = (a_{n1}, a_{n2}, \dots, a_{nk})$ $(n > 0)$ şeklinde tanımlanıp,

$$a_{n1} = a_{(n-1)k} \text{ ve } a_{ni} = a_{(n-1)k} + a_{(n-1)(i-1)} \quad (i > 1) \qquad (3.2)$$

dir.

$$G_n' = \begin{bmatrix} a_n \\ a_{n+1} \\ \vdots \\ a_{n+k-1} \end{bmatrix} = \begin{bmatrix} a_{n1} & a_{n2} & \cdots & a_{nk} \\ a_{(n+1)1} & a_{(n+1)2} & \cdots & a_{(n+1)k} \\ \vdots & \vdots & \cdots & \vdots \\ a_{(n+k-1)1} & a_{(n+k-1)2} & \cdots & a_{(n+k-1)k} \end{bmatrix}$$

olsun.

Lemma 3.1.1: $G_n = G_n'$ dir (Lü ve Wang 2007).

$g_k(p^\alpha)$, $\langle G \rangle_{p^\alpha}$ grubunun mertebesi olsun. Aşağıdaki teorem $h_k(p^\alpha)$ ve $g_k(p^\alpha)$ arasındaki ilişkiyi verir (Lü ve Wang 2007).

Teorem 3.1.2: $h_k(p^\alpha) = g_k(p^\alpha)$ dir (Lü ve Wang 2007).

İspat: $h_k(p^\alpha) | g_k(p^\alpha)$ olduğu açıktır. O zaman sadece $g_k(p^\alpha) | h_k(p^\alpha)$ olduğunu ispatlamak yeterlidir. $h_k(p^\alpha) = n$ olsun. O zaman n aşağıdaki eşitliği sağlayan en küçük tamsayıdır;

$$G^n(0,0,\dots,1)^T(mod\, p) = (0,0,\dots,1).$$

O halde Lemma 3.1.1 ’den, $0 \leq j \leq k-1$ için

$$a_{(n+j)k} \equiv 0(mod\, p^{\alpha}) \text{ ve } a_{(n+k-1)k} \equiv 1(mod\, p^{\alpha})$$

olur. Buradan ve (3.2) ’den, bütün $j = 0,1,\dots,k-1$ için

$$a_{(n+j-1)i} = a_{(n+j)(i+1)} - a_{(n+j-1)k} \equiv a_{(n+j)(i+1)}\ (mod\, p^{\alpha})$$

olur. Böylece

$$a_{n1} \equiv a_{(n+1)2} \equiv \cdots \equiv a_{(n+k-1)k} \equiv 1\ (mod\, p^{\alpha})$$

elde edilir. $j+1 < i < k$ olduğunda,

$$a_{(n+j)i} \equiv a_{(n+j+1)(i+1)} \equiv \cdots \equiv a_{(n+k-i+j)k} \equiv 0\ (mod\, p^{\alpha})$$

ve $j \geq i$ olduğunda, (3.2) ’den $a_{(n+j-i+1)1} = a_{(n+j-i)k}$ olur. Bundan dolayı

$$a_{(n+j)i} \equiv a_{(n+j-1)(i-1)} \equiv \cdots \equiv a_{(n+j-i+1)1} = a_{(n+j-i)k} \equiv 0\ (mod\, p^{\alpha})$$

dir. Bu takdirde $G^n \equiv I\ (mod\, p^{\alpha})$ elde edilir ve böylece ispat tamamlanır.

Teorem 3.1.3: t, $g_k(p) = g_k(p^t)$ olacak şekilde en büyük pozitif tamsayı olsun. Bu takdirde her $\alpha \geq t$ için, $g_k(p^{\alpha}) = p^{\alpha-t} g_k(p)$ olur. Özellikle eğer $g_k(p) \neq g_k(p^2)$ ise her $\alpha > 1$ için, $g_k(p^{\alpha}) = p^{\alpha-1} g_k(p)$ dir (Lü ve Wang 2007).

İspat: Tanımdan her pozitif r tamsayısı için $G^{g_k(p^{r+1})} \equiv I(mod\, p^{r+1})$ olduğu görülür. Bundan dolayı $G^{g_k(p^{r+1})} \equiv I(mod\, p^{r})$ dır, burada $g_k(p^{r+1}) | g_k(p^r)$ dır. Öte yandan $G^{g_k(p^r)} \equiv I + \left(b_{ij}^{(r)} p^r\right)$ yazılarak $g_k(p^{r+1})$, $g_k(p^r)p$ ile bölünebilirliğini sağlayan;

$$G^{g_k(p^r)p} = \left(I + \left(b_{ij}^{(r)} p^r\right)\right)^p = \sum_{i=0}^{p} \binom{p}{i} \left(b_{ij}^{(r)} p^r\right)^i \equiv I\ (mod\, p^{r+1})$$

elde edilir. Böylece bu da ya $g_k(p^{r+1}) = g_k(p^r)$ ya da $g_k(p^{r+1}) = g_k(p^r)p$ olduğunu gösterir ki buradaki ikinci durum, ancak ve ancak p tarafından bölünemeyen bir $b_{ij}^{(r)}$ nin varlığı ile mümkündür. $g_k(p^t) \neq g_k(p^{t+1})$ olduğunda p tarafından bölünemeyen bir $b_{ij}^{(t+1)}$ vardır. Böylece $g_k(p^{t+1}) \neq g_k(p^{t+2})$ 'dır ve ispat tamamlanır.

3.2 Pascal ve Genelleştirilmiş Pascal Matrisleri Yardımı ile Devirli Grupların Elde Edilmesi

Pascal matrisi, elemanları binom katsayıları içeren sonsuz bir matristir.

Pascal üçgeni için L_n alt üçgen, U_n üst üçgen ve S_n simetrik olmak üzere üç farklı matris tanımlanabilir.

L_n alt üçgen matrisi,

$$(L)_{ij} = \binom{i}{j}$$

olarak tanımlanır ve $j > i$ ise $\binom{i}{j} = 0$ dır.

U_n üst üçgen matrisi,

$$(U)_{ij} = \binom{j}{i}$$

olarak tanımlanır ve $i > j$ ise $\binom{j}{i} = 0$ dır.

S_n simetrik matrisi,

$$(S)_{ij} = \binom{i+j}{i}$$

olarak tanımlanır ve burada $i, j = 0, \dots, n-1$ dir.

Bu matrislerin determinantları,

$$(\det\ S_n) = (\det\ L_n) = (\det\ U_n) = 1$$

ve $S_n = L_n U_n$ dir.

(Daha fazla bilgi için $[13, 24, 25]$ 'e bakınız.)

Call ve Velleman (1993) çalışmalarında, x sıfırdan farklı herhangi bir reel sayı olmak üzere 1. çeşit $P_n[x]$ genelleştirilmiş Pascal matrisini;

$$P_n(x;i,j) = x^{i-j}\binom{i}{j}$$

olarak tanımlamışlardır ve burada $j > i$ ise $\binom{i}{j} = 0$ dır.

2. çeşit $Q_n[x]$ genelleştirilmiş Pascal matrisi;

$$Q_n(x;i,j) = x^{i+j}\binom{i}{j}$$

olarak tanımlanır ve $j > i$ ise $\binom{i}{j} = 0$ dır.

$R_n[x]$ simetrik genelleştirilmiş Pascal matrisi;

$$R_n(x;i,j) = x^{i+j}\binom{i+j}{j}$$

olarak tanımlanır ve burada $i,j = 0,\dots,n$ dir.

2. çeşit $Q_n[x]$ genelleştirilmiş Pascal matrisi ve $R_n[x]$ simetrik genelleştirilmiş Pascal matrisi hakkında daha fazla bilgi için $[30]$ 'a bakınız.

Teorem 3.2.1: n $(n \geq 2)$ bir pozitif tamsayı, G, U_n veya L_n matrisleri ve m de bir pozitif tamsayı olsun. O zaman $G \bmod m$ 'nin çarpımsal mertebesi m dir (Deveci ve Karaduman 2012).

İspat: U_n üst üçgen matrisi için $U_n = I_n + T_n$ olsun. Burada I_n , n boyutlu birim matristir. O zaman T_n 'nin (i,j) elemanları,

$$T_{i,j} = 0\,, \qquad i \geq j$$

$$T_{i,j} = \binom{j}{i}, \qquad i < j$$

olur. Binom teoreminden;

$$(U_n)^m = (I_n)^m + m(T_n) + \binom{m}{2}(T_n)^2 + \cdots + (T_n)^m$$

olduğu kolaylıkla görülür. Öte yandan (i,j) elemanları için aşağıdaki durumlar söz konusudur;

Eğer $m < n$ ise o zaman $i \geq j$ ve $j = i + 1$ için $T_{i,j} = 0$ ve $i + 2 \leq j$ için $T_{i,j} = \alpha . m$ dır. Burada $\alpha \in N$ dır.

Eğer $m \geq n$ ise o zaman $T_{i,j} = 0$ dır.

Dolayısıyla,

$$m(T_n) + \binom{m}{2}(T_n)^2 + \cdots + (T_n)^m \equiv 0_n \ (mod\ m)$$

elde edilir. Burada 0_n, n boyutlu sıfır matristir.

Böylece, U_n yerine U yazarak

$$U^m = \begin{cases} 0, & i > j \quad ise \\ 1, & i = j \quad ise \end{cases}$$

ve

$$U^m \equiv 0 \qquad i < j \ ise$$

eşitlikleri elde edilir. O zaman $|\langle U_n \rangle_m| = m$ olur. L_n alt üçgen matris için ispat benzerdir.

Teorem 3.2.2: n $(n \geq 2)$ ve m birer pozitif tamsayı olsun. O zaman $S_n \ mod\ m$ 'nin çarpımsal mertebeleri için aşağıdaki ifadeler geçerlidir (Deveci ve Karaduman 2012):

(i) Eğer α bir pozitif tamsayı ve q bir asal sayı olmak üzere $n = q^\alpha$ ise o zaman $u = 1{,}2$ için $\left|\langle S_n \rangle_{q^u}\right| = 3$ olur.

(ii) (a) Eğer her $v_1, v_2 \in [u_1, u_2]$ için $\left|\langle S_n \rangle_{p^{v_1}}\right| = \left|\langle S_n \rangle_{p^{v_2}}\right|$ ise,

$$\left|\langle S_n \rangle_{p^{u_2+n}}\right| = p^n \left|\langle S_n \rangle_{p^{u_2}}\right|$$

olur (burada $[u_1, u_2] = \{x \in Z\colon\ u_1 \leq x \leq u_2\}$ dir).

(b) Eğer her $v_1, v_2 \in [u_1, u_2]$ için $\left|\langle S_n \rangle_{p^{v_1}}\right| \neq \left|\langle S_n \rangle_{p^{v_2}}\right|$ ise o zaman her $u \in [u_1, u_2]$ için $\left|\langle S_n \rangle_{p^{u+n}}\right| = p^n \left|\langle S_n \rangle_{p^u}\right|$ olur.

(iii) p_k 'lar farklı asal sayılar olmak üzere eğer $m = \prod_{k=1}^{t} {p_k}^{e_k}$ $(t \geq 1)$ ise

$$|\langle S_n \rangle_m| = okek\left[\left|\langle S_n \rangle_{p_1{}^{e_1}}\right|, \left|\langle S_n \rangle_{p_2{}^{e_2}}\right|, \dots, \left|\langle S_n \rangle_{p_t{}^{e_t}}\right|\right]$$

olur.

İspat: S_n, S ile ifade edilmiş olsun.

(i) α bir pozitif tamsayı ve q bir asal sayı olmak üzere $n = q^\alpha$ ise o zaman

$$S^3 = \begin{cases} q^2\epsilon_1 \binom{i+j}{i} & i < j, \\ q^2\epsilon_2 \binom{i+j}{i} + 1 & i = j, \\ q^2\epsilon_3 \binom{i+j}{i} & i > j, \end{cases}$$

ifadeleri yazılır. Burada $i = j = 0$ için $q^2 \nmid \chi\epsilon_2\binom{i+j}{i}$ dır ve $\epsilon_1, \epsilon_{2,} \epsilon_3$ pozitif tamsayılardır. O zaman

$$q^2\epsilon_1 \binom{i+j}{i} \equiv 0 \; (mod\; q^u) \qquad i < j \;\; ve\, u = 1{,}2$$

$$q^2\epsilon_2 \binom{i+j}{i} + 1 \equiv 1 \; (mod\; q^u) \qquad i = j \;\; ve\, u = 1{,}2$$

$$q^2\epsilon_3 \binom{i+j}{i} \equiv 0 \; (mod\; q^u) \qquad i > j \;\; ve\, u = 1{,}2$$

eşitlikleri elde edilir. Böylece $u = 1{,}2$ için $\left|\langle S_n \rangle_{q^u}\right| = 3$ sonucuna ulaşılır.

(ii)

(a) Her $v_1, v_2 \in [u_1, u_2]$ için $\left|\langle S_n \rangle_{p^{v_1}}\right| = \left|\langle S_n \rangle_{p^{v_2}}\right|$ olsun. O zaman

$$S^a = \begin{cases} p^{u_2}\varepsilon_1^* \binom{i+j}{i} & i < j, \\ p^{u_2}\varepsilon_2^* \binom{i+j}{i} + p^{u_2} & i = j, \\ p^{u_2}\varepsilon_3^* \binom{i+j}{i} & i > j, \end{cases}$$

ifadeleri yazılır. Burada $i = j = 0$ için $p^{u_2} \nmid \varepsilon_2^*\binom{i+j}{i}$ dır ve $\varepsilon_1^*,\ \varepsilon_2^*,\ \varepsilon_3^*$ pozitif tamsayılardır. Matrislerdeki genel çarpım ile,

$$S^{p^n a} = \begin{cases} p^{n+u_2}\mathring{\varepsilon}_1\binom{i+j}{i} & i<j, \\ p^{n+u_2}\mathring{\varepsilon}_2\binom{i+j}{i} + \quad p^{n+u_2} & i=j, \\ p^{n+u_2}\mathring{\varepsilon}_3\binom{i+j}{i} & i>j\ , \end{cases}$$

olduğu kolaylıkla görülür. Burada $i=j=0$ için $p^{n+u_2} \nmid \mathring{\varepsilon}_2\binom{i+j}{i}$ dır ve $\mathring{\varepsilon}_1,\ \mathring{\varepsilon}_2,\ \mathring{\varepsilon}_3$ pozitif tamsayılardır. Bu durumda

$$p^{n+u_2}\mathring{\varepsilon}_1\binom{i+j}{i} \equiv 0\ (mod\ p^{n+u_2}) \qquad i<j,$$

$$p^{n+u_2}\mathring{\varepsilon}_2\binom{i+j}{i} + p^{n+u_2} \equiv 1\ (mod\ p^{n+u_2}) \qquad i=j,$$

$$p^{n+u_2}\mathring{\varepsilon}_3\binom{i+j}{i} \equiv 0\ (mod\ p^{n+u_2}) \qquad i>j,$$

eşitlikleri elde edilir. Böylece $|\langle S_n\rangle_{p^{u_2+n}}| = p^n|\langle S_n\rangle_{p^{u_2}}| = p^n.a$ sonucuna ulaşılır.

(b) İspat (a) 'nın ispatına benzerdir.

(iii) p_k 'lar farklı asal sayılar olmak üzere $m=\prod_{k=1}^{t} p_k{}^{e_k}$ $(t\geq 1)$ ve $okek\ [|\langle S_n\rangle_{p_1{}^{e_1}}|, |\langle S_n\rangle_{p_2{}^{e_2}}|, \dots, |\langle S_n\rangle_{p_t{}^{e_t}}|] = \lambda$ olsun. O zaman

$$S^{\lambda} = \begin{cases} \lambda\varepsilon_1'\binom{i+j}{i} & i<j, \\ \lambda m\varepsilon_2'\binom{i+j}{i} + m & i=j, \\ \lambda\varepsilon_3'\binom{i+j}{i} & i>j, \end{cases}$$

ifadeleri yazılır. Burada $i=j=0$ için $m\ \chi\lambda\varepsilon_2'\binom{i+j}{i}$ ve $\varepsilon_1',\ \varepsilon_2',\ \varepsilon_3'$ pozitif tamsayılardır. $m|\lambda\varepsilon_1'\binom{i+j}{i}$, $\lambda m\varepsilon_2'\binom{i+j}{i}$, $\lambda\varepsilon_3'\binom{i+j}{i}$ olduğunda,

$$\lambda\varepsilon_1'\binom{i+j}{i} \equiv 0\ (mod\ m) \qquad i<j,$$

$$\lambda m\varepsilon_2'\binom{i+j}{i} \equiv 1\ (mod\ m) \qquad i=j,$$

$$\lambda\varepsilon_3'\binom{i+j}{i} \equiv 0 \ (mod\ m) \qquad\qquad i > j,$$

eşitlikleri elde edilir. Böylece $|\langle S_n \rangle_m| = okek\left[\left|\langle S_n \rangle_{p_1^{e_1}}\right|, \left|\langle S_n \rangle_{p_2^{e_2}}\right|, \dots, \left|\langle S_n \rangle_{p_t^{e_t}}\right|\right]$ sonucuna ulaşılır.

Varsayım 3.2.1: Eğer $p \geq n$ ise o zaman $\left|\langle S_n \rangle_p\right| \big| (p^n - p^\sigma)$ olacak şekilde $0 \leq \sigma \leq n-1$ aralığında bir σ tamsayısı mevcuttur (Deveci ve Karaduman 2012).

Teorem 3.2.3: n $(n \geq 2)$ ve m birer pozitif tamsayı ve q_k ’lar da farklı asal sayılar olmak üzere $x = \prod_{k=1}^{l} q_k{}^{e_k}$ $(l \geq 1)$ olsun. O zaman $x \geq 2$ için $P_n[x]\ mod\ m$ ’nin çarpımsal mertebeleri için aşağıdaki durumlar söz konusudur (Deveci ve Karaduman 2012):

(i) $u \in [1, l]$ için $\left|\langle P_n[x] \rangle_{q_u{}^{e_u}}\right| = 1$ olur.

(ii) Eğer w, $w > e_1, \dots, e_l$ olacak şekilde bir pozitif tamsayı ise o zaman $u \in [1, l]$ için $\left|\langle P_n[x] \rangle_{q_u{}^{w}}\right| = q_u{}^{w-e_u}$ olur.

(iii) Eğer θ bir pozitif tamsayı ve $p \neq q_1, \dots, q_l$ ise o zaman $\left|\langle P_n[x] \rangle_{p^\theta}\right| = p^\theta$ olur.

(iv) Eğer p_k ’lar farklı asal sayılar olmak üzere $m = \prod_{k=1}^{t} p_k{}^{e_k}$ $(t \geq 1)$ ise o zaman $|\langle P_n[x] \rangle_m| = okek\left[\left|\langle P_n[x] \rangle_{p_1^{e_1}}\right|, \left|\langle P_n[x] \rangle_{p_2^{e_2}}\right|, \dots, \left|\langle P_n[x] \rangle_{p_t^{e_t}}\right|\right]$ olur.

İspat: (i) $u \in [1, l]$ için $q_u{}^{e_u} | x$ olduğunda

$$P_n(x; i, j) = 0 \qquad\qquad i < j,$$

$$P_n(x; i, j) = 1 \qquad\qquad i = j,$$

$$P_n(x; i, j) = x^{\,i-j}\binom{i}{j} \equiv 0 \ (mod\ q_u{}^{e_u}) \qquad\qquad i > j,$$

eşitlikleri elde edilir. Böylece $u \in [1, l]$ için $\left|\langle P_n[x] \rangle_{q_u{}^{e_u}}\right| = 1$ sonucuna ulaşılır.

(ii) $w > e_1, \dots, e_l$ ve $u \in [1, l]$ olacak şekilde u ve w pozitif tamsayılar ise o zaman,

$$P_n(x; i, j)^{q_u{}^{w-e_u}} = 0 \qquad\qquad i < j,$$

$$P_n(x;i,j)^{q_u^{w-e_u}} = 0 \qquad\qquad i = j,$$

$$P_n(x;i,j)^{q_u^{w-e_u}} = q_u^{w-e_u}\eta_1\, x^{\,i-j}\binom{i}{j} \equiv 0 \ (mod\ q_u^{w}) \qquad\qquad i > j,$$

eşitlikleri elde edilir. Burada η_1 bir pozitif tamsayıdır. Böylece $\left|\langle P_n[x]\ \rangle_{q_u^w}\right| = q_u^{w-e_u}$ sonucuna ulaşılır.

(iii) θ bir pozitif tamsayı ve $p \neq q_1, \dots, q_l$ ise o zaman

$$P_n(x;i,j)^{p^\theta} = 0 \qquad\qquad i < j,$$

$$P_n(x;i,j)^{p^\theta} = 1 \qquad\qquad i = j,$$

$$P_n(x;i,j)^{p^\theta} = p^\theta\eta_2 x^{\,i-j}\binom{i}{j} \equiv 0\ \left(mod\ p^\theta\right) \qquad\qquad i > j,$$

eşitlikleri elde edilir. Burada η_2 bir pozitif tamsayıdır. Böylece $\left|\langle P_n[x]\ \rangle_{p^\theta}\right| = p^\theta$ sonucuna ulaşılır.

(iv) İspat Teorem 3.2.2 (iii) ispatı ile benzerdir.

Teorem 3.2.4: $n\ \ (n \geq 2)$ bir pozitif tamsayı, G , $Q_n[x]$ veya $R_n[x]$ matrisleri ve m de bir pozitif tamsayı olsun. O zaman $x \geq 2$ için $G\ mod\ m$ 'nin çarpımsal mertebesi için aşağıdaki durumlar söz konusudur (Deveci ve Karaduman 2012):

(i) $(p, x) = 1$ olsun.

(a) Eğer her $v_1, v_2 \in [u_1, u_2]$ için $\left|\langle\ G\rangle_{p^{v_1}}\right| = \left|\langle\ G\rangle_{p^{v_2}}\right|$ ise o zaman $\left|\langle\ G\rangle_{p^{u_2+n}}\right| = p^n\left|\langle\ G\rangle_{p^{u_2}}\right|$ olur.

(b) Eğer her $v_1, v_2 \in [u_1, u_2]$ için $\left|\langle\ G\rangle_{p^{v_1}}\right| \neq \left|\langle\ G\rangle_{p^{v_2}}\right|$ ise o zaman her $u \in [u_1, u_2]$ için $\left|\langle\ G\rangle_{p^{u+n}}\right| = p^n\left|\langle\ G_n\rangle_{p^u}\right|$ olur.

(ii) Eğer $(m, x) = 1$ ve p_k 'lar farklı asal sayılar olmak üzere $m = \prod_{k=1}^{t} p_k{}^{e_k}\ \ (t \geq 1)$ ise o zaman $|\langle\ G\rangle_m| = okek\left[\left|\langle\ G\rangle_{p_1{}^{e_1}}\right|,\ \left|\langle\ G\rangle_{p_2{}^{e_2}}\right|, \dots,\ \left|\langle G\rangle_{p_t{}^{e_t}}\right|\right]$ olur.

Varsayım 3.2.2: Eğer $(p,x)=1$ ve $\left|\langle Q_n[x]\rangle_p\right| < p$ ise o zaman $\left|\langle Q_n[x]\rangle_p\right| \Big| \, p-1$ ’dir (Deveci ve Karaduman 2012).

Varsayım 3.2.3: Eğer $(p,x)=1$ ve $\left|\langle Q_{n_1}[x]\rangle_p\right|$, $\left|\langle Q_{n_2}[x]\rangle_p\right| < p$ ise o zaman $\left|\langle Q_{n_1}[x]\rangle_p\right| = \left|\langle Q_{n_2}[x]\rangle_p\right|$ ’dir (Deveci ve Karaduman 2012).

Varsayım 3.2.4: Eğer $(p,x)=1$ ve $p \geq n+1$ ise o zaman $\left|\langle R_n[x]\rangle_p\right| \Big| \, (p^{n+2}-p^{\sigma})$ olacak şekilde $0 \leq \sigma \leq n+1$ aralığında bir σ tamsayısı mevcuttur (Deveci ve Karaduman 2012).

4.ARAŞTIRMA BULGULARI

4.1 MacWilliams ve Chebyshev Matrisleri Yardımı ile Devirli ve Yarı Grupların Elde Edilmesi

m_{ij} 'ler tamsayılar olmak üzere verilen bir $M = \left[m_{ij}\right]$ matrisi için, M 'nin her elemanının $mod\, m$ ye göre indirgenmesi $M\,(mod\, m)$ şeklinde ifade edilir. Yani, $M\,(mod\, m) = \left(m_{ij}(mod\, m)\right)$ 'dir. $\langle M\rangle_m = \left\{M^i(mod\, m) \middle|\, i \geq 0\right\}$ olsun.

Eğer $obeb\,(m, \det M) = 1$ ise o zaman $\langle M\rangle_m$ bir devirli grup; $obeb\,(m, \det M) \neq 1$ ise $\langle M\rangle_m$ bir yarı gruptur. $|\langle M\rangle_m|$ ile $\langle M\rangle_m$ 'nin mertebesi gösterilmiştir.

Matrislerdeki genel çarpım ile;

$$\left((M_N)_{ij}\right)^{2k} = \left[m_{ij}\right]_{(N+1)\times(N+1)} = \begin{bmatrix} 2^{kN} & 0 & \dots & 0 & 0 \\ 0 & 2^{kN} & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 2^{kN} \end{bmatrix}, \quad (k \geq 0) \qquad (4.1.1)$$

yani $\left((M_N)_{ij}\right)^{2k}$ matrisinin köşegen elemanları $2^{kN}, \dots, 2^{kN}$ olan $(N+1)\times(N+1)$ boyutlu bir köşegen matris olduğu kolaylıkla görülür.

Ayrıca $N \geq 1$ için,

$$det\left((M_N)_{ij}\right) = \begin{cases} -2^{\frac{N^2+N}{2}}, & N \equiv 1,2\, mod\ 4, \\ 2^{\frac{N^2+N}{2}}, & N \equiv 0,3\, mod\ 4. \end{cases} \qquad (4.1.2)$$

şeklindedir.

m bir tek tamsayı ise $\langle M_N\rangle_m$ bir devirli grup, m bir çift tamsayı ise $\langle M_N\rangle_m$ bir yarı grup olduğu (4.1.2) deki ifadeden kolaylıkla görülür.

Teorem 4.1.1: Eğer m bir tek tamsayı ise $\langle M_N\rangle_m$ devirli grubun mertebesi $2k$ dır. Burada k, $2^{kN} \equiv 1(mod\, m)$ olacak şekilde en küçük pozitif tamsayıdır (Deveci ve Aküzüm 2014).

İspat: (4.1.1) 'den $\left((M_N)_{ij}\right)^{2k}(mod\, m) = I_{(N+1)}$ yazılır. $I_{(N+1)}$, $(N+1)\times(N+1)$ boyutlu bir birim matristir. k, $2^{kN} \equiv 1(mod\, m)$ olacak şekilde en küçük pozitif tamsayı olarak seçilir ise $|\langle M_N\rangle_m| = 2k$ elde edilir.

Örnek 4.1.1: $M_2 = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 0 & -2 \\ 1 & -1 & 1 \end{bmatrix}$ matrisini için $m = 5$ olarak seçelim.$detM_2 = -8$ dir. $obeb(5,-8) = 1$ olduğundan $\langle M_2\rangle_5$ bir devirli grup olup Teorem 4.1.1 'den mertebesi $2k$ dır ve $2^{2k} \equiv 1(mod\ 5)$ denkliğini sağlayan en küçük k tamsayısı 2 olur. Buradan $|\langle M_2\rangle_5| = 4$ elde edilir.

Teorem 4.1.2: m bir çift tamsayı olsun. O zaman $\langle M_N\rangle_m$ yarı grubun mertebesi için iki durum söz konusudur (Deveci ve Aküzüm 2014):

(i) Eğer $m = 2^u$ $(u \in N)$ ise, $\langle M_N\rangle_{2^u}$ yarı grubun mertebesi $2k$ dır. Burada k, $2^{kN} \equiv 0(mod\, m)$ olacak şekilde en küçük pozitif tamsayıdır.

(ii) Eğer t bir tek tamsayı olmak üzere $m = 2^u t$ $(u \in N)$ ise o zaman,

$|\langle M_N\rangle_{2^u t}| = |\langle M_N\rangle_{2^u}| + |\langle M_N\rangle_t| - 1$ dir.

İspat: **(i)** (4.1.1) 'den $\left((M_N)_{ij}\right)^{2k}(mod\, m) = 0_{(N+1)}$ yazılır. Burada $0_{(N+1)}$, $(N+1)\times(N+1)$ boyutlu bir sıfır matristir. k, $2^{kN} \equiv 0(mod\, m)$ olacak şekilde en küçük pozitif tamsayı olarak seçilir ise $|\langle M_N\rangle_m| = 2k$ elde edilir.

(ii) $|\langle M_N\rangle_t| = 2\alpha$ ve $|\langle M_N\rangle_{2^u}| = 2\beta$ olsun. O zaman $k_1, k_2 \in \mathbb{N}$ ve $obeb(t, k_2) = 1$ olmak üzere $2^{\alpha N} = k_1 t + 1$ ve $2^{\beta N} = k_2 2^u$ olur. Dolayısıyla $2^{(\alpha+\beta)N} \equiv 2^u k_2(mod\, m)$ yani $\left((M_N)_{ij}\right)^{2\alpha+2\beta}(mod\, m) \equiv \left((M_N)_{ij}\right)^{2\beta}$ olur. Böylece $|\langle M_N\rangle_{2^u t}| = |\langle M_N\rangle_{2^u}| + |\langle M_N\rangle_t| - 1$ elde edilir.

Örnek 4.1.2: $M_3 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 3 & 1 & -1 & -3 \\ 3 & -1 & -1 & 3 \\ 1 & -1 & 1 & -1 \end{bmatrix}$ matrisi için $m = 8$ olsun.$detM_3 = 64$ dır.

$obeb(8,64) \neq 1$ olduğu için $\langle M_3\rangle_8$ grubu bir yarı grup belirtir ve $8 = 2^3$ şeklinde olduğundan Teorem 4.1.2 (i) 'den mertebesi $2k$ dır.

$2^{3k} \equiv 0(mod\, 8)$ denkliğini sağlayan en küçük k pozitif tamsayı 1 dir. Buradan $|\langle M_3\rangle_{2^3}| = 2$ olur.

Örnek 4.1.3: $M_4 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 4 & 2 & 0 & -2 & -4 \\ 6 & 0 & -2 & 0 & 6 \\ 4 & -2 & 0 & 2 & -4 \\ 1 & -1 & 1 & -1 & 1 \end{bmatrix}$ matrisi için $m = 192$ olsun. $detM_4 = 1024$ dir. $obeb(192{,}1024) \neq 1$ olduğu için $\langle M_4\rangle_{192}$ grubu bir yarı grup belirtir ve $192 = 2^6 \cdot 3$ olduğundan Teorem 4.1.2 (ii) 'den $|\langle M_4\rangle_{2^6 3}| = |\langle M_4\rangle_{2^6}| + |\langle M_4\rangle_3| - 1$ dir.

Burada $\langle M_4\rangle_{2^6}$ grubunun mertebesi Teorem 4.1.2 (i) 'den $2k$ dır ve $2^{4k} \equiv 0(mod\, 2^6)$ denkliğini sağlayan en küçük k pozitif tamsayı 2 dir. Böylece $|\langle M_4\rangle_{2^6}| = 4$ olur.

Diğer yandan $\langle M_4\rangle_3$ grubunun mertebesi Teorem 4.1.1 'den $2k$ dır ve $2^{4k} \equiv 1(mod\, 3)$ denkliğini sağlayan en küçük k pozitif tamsayı 1 dir. Böylece $|\langle M_4\rangle_3| = 2$ olur. Dolayısıyla;

$$|\langle M_4\rangle_{2^6 3}| = |\langle M_4\rangle_{2^6}| + |\langle M_4\rangle_3| - 1 = 4 + 2 - 1 = 5$$

olur.

Uyarı 4.1.1: $p,\ det\big((D_N)_{ij}\big)$ 'nin en büyük bir asal çarpanı ise $p!|det\big((D_N)_{ij}\big)$ dir (Deveci ve Aküzüm 2014).

Teorem 4.1.3: $obeb\Big(p, det\big((D_N)_{ij}\big)\Big) = 1$ ve t, $|\langle D_N\rangle_P| = |\langle D_N\rangle_{P^t}|$ olacak şekilde en büyük pozitif bir tamsayı olsun. Bu takdirde her $\alpha \geq t$ için $|\langle D_N\rangle_{P^\alpha}| = p^{\alpha - t}|\langle D_N\rangle_P|$ dır. Özellikle $|\langle D_N\rangle_P| \neq |\langle D_N\rangle_{P^2}|$ ise, her $\alpha > 1$ için $|\langle D_N\rangle_{P^\alpha}| = p^{\alpha-1}|\langle D_N\rangle_P|$ olur (Deveci ve Aküzüm 2014).

İspat: İlk önce her $u \geq 1$ için $\langle D_N\rangle_{P^u}$ 'nın bir devirli grup olduğunu belirtelim. θ pozitif bir tamsayı olsun ve $|\langle D_N\rangle_m|$, $h_N(m)$ ile gösterilsin.

${(D_N)_{ij}}^{h_N(p^{\theta+1})} \equiv I_{N+1}\left(mod\ p^{\theta+1}\right)$ yani ${(D_N)_{ij}}^{h_N(p^{\theta+1})} \equiv I_{N+1}\left(mod\ p^{\theta}\right)$ olduğunda dolayı $h_N\left(p^{\theta}\right)$ 'nin , $h_N\left(p^{\theta+1}\right)$ 'yi böldüğü elde edilir. Öte yandan ${(D_N)_{ij}}^{h_N(p^{\theta})} = I_{N+1} + \left({a_{ij}}^{(\theta)} p^{\theta}\right)$ yazılarak,

$${(D_N)_{ij}}^{h_N(p^{\theta})p} = \left(I_{N+1} + \left({a_{ij}}^{(\theta)} p^{\theta}\right)\right)^p = \sum_{i=0}^{p} \binom{p}{i} \left({a_{ij}}^{(\theta)} p^{\theta}\right)^i \equiv I_{N+1}\left(mod\ p^{\theta+1}\right)$$

elde edilir ki, bu da $h_N\left(p^{\theta+1}\right) | h_N\left(p^{\theta}\right)p$ olduğunu gösterir. Böylece ya $h_N\left(p^{\theta+1}\right) = h_N\left(p^{\theta}\right)$ ya da $h_N\left(p^{\theta+1}\right) = h_N\left(p^{\theta}\right)p$ olduğunu gösterir ki buradaki ikinci durum ancak ve ancak $p | {a_{ij}}^{(\theta)}$ olacak şekilde bir ${a_{ij}}^{(\theta)}$ 'nin var olması ile mümkündür. $h_N(p^t) \neq h_N(p^{t+1})$ olduğundan $p | {a_{ij}}^{(\theta)}$ olacak şekilde bir ${a_{ij}}^{(\theta)}$ vardır. Böylece $h_N(p^{t+1}) \neq h_N(p^{t+2})$ olur. t üzerinde tümevarım yöntemiyle ispat tamamlanır.

Teorem 4.1.4: $obeb\left(m, det\left((D_N)_{ij}\right)\right) = 1$ ve p_i 'ler farklı asal sayılar olmak üzere $m = \prod_{i=1}^{t} {p_i}^{e_i}$ $(t \geq 1)$ olsun. O zaman,

$$|\langle D_N \rangle_m| = okek\left[\left|\langle D_N \rangle_{{p_1}^{e_1}}\right|, \left|\langle D_N \rangle_{{p_2}^{e_2}}\right|, \dots, \left|\langle D_N \rangle_{{p_t}^{e_t}}\right|\right]$$

dir (Deveci ve Aküzüm 2014).

İspat: $1 \leq k \leq t$ için $\left|\langle D_N \rangle_{{p_k}^{e_k}}\right| = \lambda_k$ ve $|\langle D_N \rangle_m| = \lambda$ olsun. O zaman,

$${(D_N)_{ij}}^{\lambda_k} = \begin{cases} {p_k}^{e_k} \varepsilon_{ij} K_i^N(j) & i > j, \\ {p_k}^{e_k} \varepsilon_{ij} K_i^N(j) + 1 & i = j, \\ {p_k}^{e_k} \varepsilon_{ij} K_i^N(j) & i < j, \end{cases}$$

ve

$${(D_N)_{ij}}^{\lambda} = \begin{cases} m {\varepsilon_{ij}}' K_i^N(j) & i > j, \\ m {\varepsilon_{ij}}' K_i^N(j) + 1 & i = j, \\ m {\varepsilon_{ij}}' K_i^N(j) & i < j, \end{cases}$$

eşitlikleri elde edilir. Burada $0 \leq i, j \leq N$ için ε_{ij} ve ${\varepsilon_{ij}}'$ tamsayılardır. Bu nedenle k 'nın tüm değerleri için ${(D_N)_{ij}}^{\lambda_k}$, $c.{(D_N)_{ij}}^{\lambda}$ $(c \in \mathbb{N})$ şeklindedir ve böyle herhangi bir λ sayısı verildiğinde $\lambda = okek\ [\lambda_1, \lambda_2, \dots, \lambda_t]$ dir.

Sonuç 4.1.1: $\langle D_2 \rangle_{2^k}$ ve $\langle D_2 \rangle_{3^k}$ yarı grupların mertebeleri sırasıyla $2k+1$ ve $2^k(k-1)+2k+1$ dir (Deveci ve Aküzüm 2014).

İspat: İlk önce $det\big((D_2)_{ij}\big) = -12$ olduğundan her $k \geq 1$ için $\langle D_2 \rangle_{2^k}$ ve $\langle D_2 \rangle_{3^k}$'nın yarı grup olduğunu belirtelim. Matrislerdeki genel çarpım ile;

$$(D_2)_{ij}{}^{2k} = \begin{bmatrix} 2^{2k} & 2^{k-1}(2^k - 3^k) & 0 \\ 0 & 6^k & 0 \\ 2^k(2^k - 3^k) & 2^{k-1}(2^k - 3^k) & 6^k \end{bmatrix}$$

ve

$$(D_2)_{ij}{}^{2k+1} = \begin{bmatrix} 2^k(2^{k+1} - 3^k) & 2^{2k} & 6^k \\ 2.6^k & 0 & -2.6^k \\ 2^k(2^{k+1} - 3^k) & 2^k(2^k - 3^{k+1}) & 6^k \end{bmatrix} \quad (k \geq 1)$$

kolaylıkla ispatlanır.

$(D_2)_{ij}{}^{2k+1} \equiv 0_3 (mod\ 2^k)$ ve $(D_2)_{ij}{}^{2^k(k-1)+2k+1} \equiv (D_2)_{ij}{}^{2k} (mod\ 3^k)$ olduğundan $\left|\langle D_2 \rangle_{2^k}\right| = 2k+1$ ve $\left|\langle D_2 \rangle_{3^k}\right| = 2^k(k-1)+2k+1$ elde edilir.

TARTIŞMA VE SONUÇ

Bu tez çalışmasında, $N \geq 1$ için $(M_N)_{ij}$ MacWilliams ve $(D_N)_{ij}$ Chebyshev matrislerinin m modülüne göre çarpımsal mertebeleri ele alınmıştır ve bu matrisler m modülüne göre indirgenerek üretilen devirli ve yarı grupların mertebeleri incelenmiştir.

KAYNAKLAR

[1] Ağargün, A.G. and Özdağ, H., "Lineer Cebir ve Çözümlü Problemleri", Birsen Yayınevi, İstanbul, 2008.

[2] Başar, F., "Lineer Cebir" , Sürat Üniversite Yayınları, İstanbul 2012.

[3] Bateman H. and Erdelyi A., 1953 "Higher transcendental function", *McGraw-Hill*, Vol.2.

[4] Call, G.S. and Velleman, D.J., 1993. "Pascal's matrices" Amer.Math.Monthly 100, 372-376.

[5] Çallıalp, F., "Soyut Cebir" İstanbul 2001.

[6] Deveci, Ö., 2011. "The polytopic-k-step Fibonacci sequences in finite groups" *Discrete Dyn. Nat. Soc.*, Volume 2011, Article ID 431840, 12 pages, http://dx.doi.org/10.1155/2011/431840

[7] Deveci, Ö. and Karaduman, E., 20012. "The cyclic groups via the Pascal matrices and the generalized Pascal matrices", Linear Algebra and its Applications, 437, 2538-2545.

[8] Deveci, Ö. and Karaduman, E., 2012. " The generalized order-*k* Lucas sequences in Finite groups", *J. Appl. Math.*, Volume 2012, Article ID 464580, 15 pages, http://dx.doi.org/10.1155/2012/464580

[9] Deveci, Ö. and Karaduman, E. (to appear). "The Pell sequences in finite groups", *Util. Math.*

[10] Deveci, Ö. (to appear). "The Pell-Padovan sequences and the Jacobsthal-Padovan sequences in finite groups", *Util. Math.*

[11] Deveci, Ö. and Aküzüm, Y., 2014. " The cyclic groups and semigroups via MacWilliams and Chebyshev matrices". 6(2), 55-59.

[12] Dummit, D.S. and Foote, R.M., 2004. "Abstract Algebra", 3^{nd} editon (John Wiley & Sons,Inc.).

[13] Edelman, A. and Strang, G., 2003, "Pascal matrices", MIT, Cambridge, MA.

[14] Gluesing-Luerssen, H. and Schneider, G., 2008. “On the MacWilliams identity for convolutional codes”, *IEEE Transations on Information Theory,* 54 (4).

[15] Gogin, N. and Hirvencalo, M., 2012. “Recurrent construction of MacWilliams and Chebyshev matrices”, *Fundamenta Informaticae*, 116(1-4), 93-110.

[16] Gogin, N. and Hirvencalo, M., 2007. “On the generating function of discrete Cheyshev polynomial”, TUCS technical Reports, 819, Turku Centre for Computer Science.

[17] Gogin, N.D. and Myllari, A.A., 2007. “The Fibonacci-Padovan sequence and MacWilliams transform matrices”, *Programing and Computer Software, Published in Programmirovanie,* 33(2), 74-79.

[18] Hirvencalo, M., 2003. “*Studies on Boolean functions related to quantum computing*”, Ph.D. Thesis, Univesity of Turku.

[19] Karakaş, H.İ., “Cebir Dersleri”, Tüba Yayınları, Ankara, 2010 (ikinci baskı).

[20] Lü, K. and Wang, J., 2007. “ k-step Fibonacci sequence modulo m”, Util. Math., 71, 169-178.

[21] MacWilliams, F.J. and Sloane, N.J.A., 1977. “*The theory of error-correcting codes*”, North-Holland.

[22] Özkan, E., Aydin, H.and Dikici, R., 2003. “3-step Fibonacci series modulo m”, *Applied Mathematics and Computation*, 143, 165-172.

[23] Pan, J.H. and Wang, R., 2012. “Uniform asymptotic expansions for the discrete Chebyshev polynomials” *Studies in Applied Mathematics*, 128(4) 337-384.

[24] Pascal matrix, October 2010, Available from: <http://en.wikipedia.org/wiki/Pascal_matrix>.

[25] Tang, Z., Duraiswami, R. and Gumerov, N., 2004. “Fast algorithms to computematrix- computematrix- vector products for Pascal matrices”, Technical Reports from UMIACS.

[26] Taşcı, D., “Lineer Cebir”, Gazi Kitapevi, Ankara, 2005 (üçüncü baskı).

[**27**] Taşcı, D., "Soyut Cebir", Alp Yayınevi, Ankara 20010 (ikinci baskı).

[**28**] Szegö, G., 1975. "Orthogonal polynomials. *Providence", Rhode Island, American Mathematical Society, Colloquium Publications*, Vol. 23.

[**29**] Wall, D.D., 1960. "Fibonacci series modulo *m"* , *Amer. Math. Monthly*, 67, 525-532.

[**30**] Zhizheng, Z., 1997. " The linear algebra of the generalized Pascal matrix", Linear Algebra Appl. 250 ,51–60.

ÖZGEÇMİŞ

1989 yılında Kars ilinde doğdu. İlköğrenimimi Atatürk İlköğretim okulunda, liseyi Hüsnü Özyeğin Anadolu Lisesinde tamamladı. 2008 yılında Kafkas Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümüne başladı ve 2012 yılında mezun oldu. Aynı yıl Kafkas Üniversitesi Fen Enstitüsü Matematik Anabilim dalında yüksek lisans öğrenimine başladı. Halen öğrenimine devam etmektedir.