

**T.C.
AĞRI İBRAHİM ÇEÇEN ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI**

Zehra ÇELİK KARADENİZ

**SİMPLEKTİK TİP GRUPLARIN MAKSİMAL ALT GRUPLARININ
ÇÖZÜLEBİLİR KALANLARI, İNVOŁÜSYONLARI VE BUNLARA BAĞLI
İNDİRGEME ALGORİTMA ANALİZLERİ
DOKTORA TEZİ**

Danışman: Doç. Dr. Abdullah ÇAĞMAN

Jüri: Prof. Dr. Rıdvan ŞAHİN

Jüri: Doç. Dr. Sait TAŞ

Jüri: Doç. Dr. Evrim TOKLU

Jüri: Kadirhan POLAT

AĞRI-2025

	LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ TEZ KABUL VE ONAY TUTANAĞI	Doküman No	FR-211
		İlk Yayın Tarihi	26.02.2024
		Revizyon Tarihi	
		Revizyon No	00
		Sayfa No	1/1

Simplektik Tip Grupların Maksimal Alt Gruplarının Çözülebilir Kalanları, İnvolüsyonları ve Bunlara Bağlı İndirgeme Algoritma Analizleri

Doç. Dr. Abdullah ÇAĞMAN danışmanlığında, Zehra ÇELİK KARADENİZ tarafından hazırlanan bu çalışma, 11/12/2025 tarihinde aşağıda isimleri belirtilen jüri tarafından değerlendirilmiş olup Matematik Anabilim Dalı Cebir ve Sayılar Teorisi Bilim Dalı doktora tezi olarak oybirliği / oy çokluğu (.../...) ile kabul edilmiştir.

Başkan : Prof. Dr. Rıdvan ŞAHİN	İmza :
Üye : Doç. Dr. Sait TAŞ	İmza :
Üye : Doç. Dr. Evrim TOKLU	İmza :
Üye : Doç. Dr. Kadirhan POLAT	İmza :
Üye : Doç. Dr. Abdullah ÇAĞMAN	İmza :

Yukarıdaki sonuç;

Enstitü Yönetim Kurulu .../.../... tarih ve / numaralı kararı ile onaylanmıştır.

.....
Enstitü Müdürü

Bu çalışma Tübitak 3501-Kariyer Geliştirme Programı projeleri kapsamında desteklenmiştir.
Proje No: 121F477

Not: Bu tezde kullanılan özgün ve başka kaynaklardan yapılan bildiriş, çizelge, şekil ve fotoğrafların kaynak olarak kullanımı, 5846 sayılı Fikir ve Sanat Eserleri Kanunundaki hükümlere tabidir.

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN

	LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ TEZ BENZERLİK RAPORU	Doküman No	FR-213
		İlk Yayın Tarihi	26.02.2024
		Revizyon Tarihi	
		Revizyon No	00
		Sayfa No	1 / 2

Benzerlik Oranlarına Dair Beyannamedir		
Öğrenci Adı Soyadı	ZEHRA ÇELİK KARADENİZ	
Numarası	216052018	
Ana Bilim Dalı	MATEMATİK	
Bilin Dalı	CEBİR VE SAYILAR TEORİSİ	
Programı	DOKTORA	
Danışman Unvanı Adı Soyadı	DOÇ. DR. ABDULLAH ÇAĞMAN	
Tez Başlığı	Simplektik Tip Grupların Maksimal Alt Gruplarının Çözülebilir Kalanları, İnvolüsyonları ve Bunlara Bağlı İndirgeme Algoritma Analizleri	
Bölümler	Turnitin Sonucu	En Yüksek Değer
Giriş	% 2	% 25
Kuramsal Temeller/Kavramsal Çerçeve	% 27	% 30
Materyal ve Yöntem	% 27	% 30
Araştırma Bulguları	% 18	% 20
Sonuç/Tartışma/Öneri	% 0	% 20
TEZ (GENEL)	% 23	% 25

18/11/2025

Yukarıda bilgileri yazılı tez çalışmasının benzerlik oranları Turnitin raporundan alındığı haliyle yazılmış olup tüm bilgilerin doğru olduğunu, aksi halde doğacak hukuki sorumlulukları kabul ve beyan ederiz.

İmza

Zehra ÇELİK KARADENİZ

İmza

Doç. Dr. Abdullah Çağman

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
------------	--------------	-----------

ÖZET
DOKTORA TEZİ
SİMPLEKTİK TİP GRUPLARIN MAKSİMAL ALT GRUPLARININ
ÇÖZÜLEBİLİR KALANLARI, İNVLÜSYONLARI VE BUNLARA BAĞLI
İNDİRGEME ALGORİTMA ANALİZLERİ

Tez Danışmanı: Doç. Dr. Abdullah ÇAĞMAN

2025, 63 Sayfa

Jüri: Prof. Dr. Rıdvan ŞAHİN

Doç. Dr. Sait TAŞ

Doç. Dr. Evrim TOKLU

Doç. Dr. Kadirhan POLAT

Hesaplamalı Cebir özellikle Hesaplamalı Grup Teorisi (HGT) kapsamında, klasik grupların yapısını incelemeye yönelik algoritmaların geliştirilmesiyle ilgilenir. Bu alanda önemli araştırma konularından biri Ascbacher sınıflandırmasında yer alan klasik grupların maksimal alt gruplarına yönelik indirgeme (homomorfizma kurma) algoritmalarını tasarlamak ve bu algoritmaların analizlerini gerçekleştirmektir.

Bu çalışma, Ascbacher sınıflandırmasındaki C_6 sınıfına giren gruplar için daha önce $d = r, d = r^2, d = r^3$ koşulları üzerinde yapılan BlindDescent algoritması analizlerinin devamı niteliğindedir. Çalışmada, herhangi bir ek koşul olmaksızın $d = r^4, d = r^5, d = r^6$ durumları ele alınmıştır. Analizler sırasıyla $Sp(8, r), Sp(10, r), Sp(12, r)$ grupları üzerinde gerçekleştirilmiştir.

Analiz sürecinde maksimal alt grupların çözülebilir kalanları ve bu kalanların mükemmel alt grupları ve bu gruplarda yer alan involüsyonlar ayrıntılı biçimde incelenmiştir. Elde edilen sonuçlar, BlindDescent algoritmasının yüksek boyutlu klasik gruplarda herhangi bir ek yapısal koşul olmaksızın güvenilir biçimde uygulanabileceğini göstermektedir.

2025, 63 sayfa

Anahtar Sözcükler: Ascbacher Sınıflandırması, Çözülebilir Kalan, Hesaplamalı Grup Teori, İndirgeme Algoritması, İnvolüsyon, Simplektik Grup

Bu tez TÜBİTAK tarafından 121F477 numaralı proje ile desteklenmiştir.

ABSTRACT
Ph. D. DISSERTATION
SOLVABLE RESIDUES, INVOLUTIONS AND RELATED REDUCTION
ALGORITHM ANALYSES OF MAXIMAL SUBGROUPS OF SYMPLECTIC TYPE
GROUPS

Advisor: Assoc. Prof. Abdullah AĞMAN

2025, Page: 63

Jury: Prof. Dr. Rıdvan ŞAHİN

Assoc. Prof. Dr. Sait TAŞ

Assoc. Prof. Dr. Evrim TOKLU

Assoc. Prof. Dr. Kadirhan POLAT

Computational Algebra, particularly within the field of Computational Group Theory (CGT), Focuses on developing algorithmic methods to analyze the structure of classical groups. One of the major research topics in this area is the design of reduction (homomorphism) algorithms for the maximal subgroups of classical groups classified under the Aschbacher framework and the detailed analyses of these algorithms.

This study extends previous analyses of the BlindDescent algorithm conducted for the case $d = r, d = r^2, d = r^3$ within the Aschbacher class C_6 . Here, the cases $d = r^4, d = r^5, d = r^6$ are examined without any additional assumptions. The analyses are carried out on the symplectic groups $Sp(8, r), Sp(10, r), Sp(12, r)$.

During the analysis, the solvable residuals of the maximal subgroups, the perfect subgroups of these residuals and the involutions contained within these groups have been thoroughly investigated. The obtained results demonstrate that the BlindDescent algorithm can be effectively applied to higher dimensional classical groups even in the absence of additional structural constraints.

2025, 63 pages,

Keywords: Aschbacher Classification, BlindDescent Algorithm, Computational Group Theory, Solvable Residuals, Symplectic Group

This thesis has been supported by Tübitak under the project number 121F477.

TEŞEKKÜR

Doktora eğitimim boyunca, benden bilgi ve deneyimlerini esirgemeyen, çalışmalarımın tamamlanabilmesi için her türlü şartı sağlayan ve bana her zaman her türlü şartı sağlayan ve bana her zaman her türlü desteği sunan çok değerli danışman hocam Sayın Doç. Dr. Abdullah ÇAĞMAN' a teşekkürlerimi sunarım.

Çalışmalarım esnasında değerli yardımları ile bana yardımcı olan çok kıymetli hocalarım Sayın Prof. Dr. Ahmet Ocak AKDEMİR ve Doç. Dr. Kadirhan POLAT' a teşekkürlerimi bir borç bilirim.

Eğitimim hayatım boyunca her türlü destekleriyle beni hiç yalnız bırakmayan başta ailem olmak üzere çok kıymetli eşim Ahmet KARADENİZ ve dünyadaki en değerli varlığım kızım; Melis KARADENİZ' e teşekkür ederim.

Bu tez Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) tarafından 121F477 numaralı proje ile desteklenmiştir. Katkılarından dolayı TÜBİTAK a teşekkür ederim.

TÜBİTAK 2211-A Ulusal Doktora Burs Programı kapsamında sağladığı burs için Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK)' na içtenlikle teşekkür ederim.

11/12/2025

Zehra ÇELİK KARADENİZ

İÇİNDEKİLER

ÖZET	ii
TEŞEKKÜR.....	vi
SİMGELER VE KISALTMALAR DİZİNİ	viii
ŞEKİL VE ÇİZELGELER DİZİNİ	ix
1.GİRİŞ.....	1
2. KURAMSAL TEMELLER	4
2.1.Temel Kavramlar	4
2.2. Klasik Gruplar	7
2.2.1. Lineer Gruplar	7
2.2.2. Ortogonal Gruplar	8
2.2.3. Siplektik Gruplar	9
2.2.4. Üniter Gruplar	10
3. MATERYAL ve YÖNTEM	11
3.1. Klasik Grupların Aschbacher Sınıflandırması	11
3.2. C_6 Tipli Gruplar.....	12
3.3. $Sp(6, p)$, $Sp(8, p)$, $Sp(10, p)$ ve $Sp(12, p)$ nin Maksimal Alt Grupları	16
3.4. Algoritmik Kavramlar.....	20
3.5. Monte Carlo Algoritmaları ve Alt Sınıfları.....	20
3.6. BlindDescent Algoritması.....	22
4. ARAŞTIRMA BULGULARI	26
4.1. Çözülebilir Alt Gruplar	26
4.2. Mükemmel Alt Gruplar.....	31
4.3. Analizler.....	40
4.3.1. Doğrudan Hesaplamalar	40
4.3.2. İnvolüsyon Hesaplamaları	47
5. SONUÇ, TARTIŞMA ve ÖNERİLER	55
KAYNAKLAR	56
EKLER	62
ÖZGEÇMİŞ	63

SİMGELER VE KISALTMALAR DİZİNİ

A_n	n . mertebeden alterne grup
D_n	n . mertebeden dihedral grup
E_{p^n}	p^n mertebeden elementer abelyen grup
E_q^{x+y}	E_q^x mertebesinden elementer abelyen normal alt grup içeren ve bu alt grupla bölüm grubu E_q^y mertebeli elementer abelyen grup ile q^{x+y} mertebeden elementer abelyen grup
G'	G nin türev grubu
G^n	G grubunun n . türev grubu
GAP	Grup, Programlama, Algoritma
$GL(n, q)$	Genel lineer grup
$GU(n, q)$	Genel üniter grup
$GO(n, q)$	Genel ortogonal grup
n	n mertebeli devirli grup
$Prob(A)$	A olayının olma olasılığı
$Prob(A \setminus B)$	A ile B olaylarının.koşullu olasılığı
Q_n	n mertebeli kuaterniyon grup
δ_{ij}	Kronoker deltası
$SL(n, r)$	Özel lineer grup
$Sp(n, r)$	Simplektik grup
S_n	n mertebeli simetrik grup
$\{1\}$	Aşık birim grup
$X \rtimes Y$	X ile Y nin yarı direkt çarpımı
$X \circ Y$	X ile Y nin direkt çarpımı

ŞEKİL VE ÇİZELGELER DİZİNİ

Tablo 1: Simplektik-tip grupların yapısı	14
Tablo 2: Normalleştiricinin Yapısı	15
Tablo 3: $Sp(6, p)$ maksimal alt grupları ($d = Z(Sp(6, p)) = (p-1, 2), \phi = e, p = q^e$).....	16
Tablo 4: $Sp(8, p)$ maksimal alt grupları ($d = Z(Sp(8, p)) = (p-1, 2), \phi = e, p = q^e$).....	17
Tablo 5: $Sp(10, p)$ maksimal alt grupları ($d = Z(Sp(10, p)) = (p-1, 2), \phi = e, p = q^e$). ..	18
Tablo 6: $Sp(12, p)$ maksimal alt grupları ($d = Z(Sp(12, p)) = (p-1, 2), \phi = e, p = q^e$) ..	19
Şekil 1: $Sp(6, 3)$ için çözülebilir alt grup örneği	28
Şekil 2: $Sp(8, 3)$ için çözülebilir alt grup örneği	29
Şekil 3: $Sp(10, 3)$ için çözülebilir alt grup örneği	30
Tablo 7: $Sp(8, p)$ nin maksimal alt gruplarına ait çözülebilir kalanlar	34
Tablo 8: $Sp(10, p)$ nun maksimal alt gruplarına ait çözülebilir kalanlar.....	36
Tablo 9: $Sp(12, p)$ nin maksimal alt gruplarına ait çözülebilir kalanlar.....	38
Şekil 4: $Sp(6, 3)$ için örnek hesaplama.....	42
Şekil 5: $Sp(8, 2)$ için örnek hesaplama.....	43
Şekil 6: $Sp(10, 3)$ için örnek hesaplama.....	44
Şekil 7: $Sp(12, 2)$ için örnek hesaplama.....	46
Tablo10: $Sp(2n, r)$ grubundaki involüsyonlar ve merkezdeki durumları.....	47

1. GİRİŞ

Klasik gruplar, sonlu grup teorisinin en önemli yapı taşlarından birini oluşturarak hem yapısal teori hem de uygulamalar bağlamında merkezi bir rol oynamaktadır. Bu grupların kökeni, Felix Klein'ın 1872'deki Erlanger Programı'na kadar uzanır; Klein, geometriyi bir dönüşüm grubunun değişmezleri üzerinden tanımlayarak, lineer grupların temel önemini vurgulamıştır (Klein 1872). Ardından, Wilhelm Killing ve Elie Cartan'ın Lie grupları üzerine yaptığı sınıflandırma, sonlu cisimler üzerinde benzer yapıların araştırılmasına zemin hazırlamıştır (Hawkins 2000).

Sonlu cisimler üzerindeki klasik grupların sistematik inşası, Leonard E. Dickson'ın 1901 tarihli çalışmasıyla gerçekleştirilmiştir (Dickson 1901). Dickson, genel lineer grup (GL_n), özel lineer grup (SL_n), simplektik grup (Sp_n), ortogonal grup (O_n) ve üniter grup (U_n) gibi yapıları sonlu cisimler üzerinde tanımlayarak, bunların bir bilineer veya kuadratik formu koruyan matris grupları olduğunu göstermiştir.

20. yüzyıl boyunca klasik gruplar, hem cebirsel hem de geometrik açıdan derinlemesine incelenmiş; özellikle sonlu basit grupların sınıflandırması projesinde temel bir rol üstlenmişlerdir. Michael Aschbacher'ın 1984 yılında yayımladığı sınıflandırma teoremi, sonlu klasik grupların maksimal alt gruplarını C_1 'den C_9 'a kadar dokuz kategoride yapılandırmış ve bu alana sistematik bir çerçeve kazandırmıştır (Aschbacher 1984). Bu sınıflandırma özellikle C_6 sınıfı gibi yapısal olarak karmaşık ailelerin algoritmik analizi için bir çerçeve sunmuştur.

Klasik grupların yapısal analizlerinde öne çıkan bir diğer kavram da çözülebilir kalandır. Bir grubun en büyük normal çözülebilir alt grubu olarak tanımlanan bu yapı, Jordan-Hölder kuramı çerçevesinde anlam kazanmıştır. Klasik gruplar için çözülebilir kalanın genellikle merkezle sınırlı olması, onların neredeyse basit karakterini ortaya koymaktadır (Huppert 1967).

Bu teorik zemin üzerine, Hesaplamalı Cebir alanında gelişen Matris Grup Tanıma Projesi (MGTP) gibi uluslararası araştırma girişimleri, sonlu cisimler üzerinde tanımlı matris grupları için etkili algoritmalar geliştirmeyi hedeflemektedir. Bu proje kapsamında, matris

gruplarının yapısını analiz etmek üzere indirgeme algoritmaları ve bölüm ağaçları gibi yöntemler geliştirilmiştir. Özellikle, C_6 sınıfındaki gruplar için tasarlanmış olan ve BlindDescent olarak adlandırılan indirgeme algoritması (Leedman-Green 2006), ekstra-özel normal alt grupların tespiti ve bunlar üzerinden homomorfizmaların inşası yoluyla grupların özelliklerinin hesaplamalı olarak kontrol altına alınmasını sağlamaktadır.

Öte yandan, mertebesi 2 olan elemanlar olarak tanımlanan involüsyonlar da klasik grupların incelenmesinde kritik bir öneme sahiptir. Richard Brauer ve K. A. Fowler' ın 1950' lerdeki öncü makaleleri (Brauer and Fowler 1955) ve ardından Daniel Gorenstein ile bu alanda çalışan diğer araştırmacıların involüsyon merkezleyicileri üzerine geliştirdiği yöntemler, sonlu basit grupların sınıflandırmasının temel taşlarından birini oluşturmuştur (Gorenstein 1982).

Bu tez çalışmasında, sonlu cisimler üzerinde tanımlanmış klasik grupların çözülebilir kalanlarının yapısı ile involüsyonların merkezleyicileri arasındaki ilişkiler incelenecek ve bu bağlamda C_6 sınıfı gruplarına odaklanılarak, BlindDescent algoritmasının performans analizi gerçekleştirilecektir. Çalışmamızda, girdi grubunun çözülebilir normal alt gruplarını içeren mükemmel alt grupları için kapsamlı analizler sunulacak ve algoritmanın bu grupları tespit etmedeki etkinliği değerlendirilecektir.

Tezin yapısal organizasyonu beş ana kısımdan oluşmakta olup, her bir kısım araştırmanın farklı bir aşamasına odaklanmaktadır.

Birinci bölümde yer alan girişte grupların tarihsel gelişimi ve araştırmanın amacına yer verilmiştir.

İkinci bölüm olan kuramsal temellerde ise tezin ilerleyen bölümlerinde kullanılacak olan temel tanım ve teoremlere yer verilmiştir.

Üçüncü bölümde; Aschbacher sınıflandırması, C_6 sınıfının özellikleri ve BlindDescent algoritmasının teorik çerçevesi açıklanmıştır.

Dördüncü bölümde; grupların çözülebilir, mükemmel alt grupları ve involüsyonlar üzerine elde edilen bulgular sunulmuştur.

Beşinci ve son bölüm olan sonuç kısmında ise; çalışmanın ana hatlarıyla sonuçları ve genel değerlendirmesi paylaşılmıştır.



2. KURAMSAL TEMELLER

2.1. Temel Kavramlar

Tanım 2.1.1: G bir grup ve onun boştan farklı alt kümesi S olsun. $*$: $G \times S \rightarrow S$ fonksiyonu, $(g, s) \mapsto (g, s) = g * s$ şeklinde tanımlanır ve

- i. her $s \in S$ için $s * e = s$,
- ii. her $s \in S$ ve $g, a \in G$ için $(ga) * s = g * (a * s)$,

koşullarını sağlarsa $*$ fonksiyonuna. G nin S üzerine bir etkisi denir (Asar vd 2009).

Tanım 2.1.2: Her $s \in S$ ve $g \in G$ için $g * s = s$ şeklinde tanımlanan $*$ fonksiyonu, G nin S üzerine bir etkisidir. Bu etki aşikâr etki olarak adlandırılır (Asar vd 2009).

Tanım 2.1.3: G bir grup ve G nin bir alt grubu S olsun. Her $s \in S$ ve $g \in G$ için $s * g = sgs^{-1}$ şeklinde tanımlanan $*$ fonksiyonu S nin G üzerine etkisidir. Gerçekten her $s, t \in S$ ve $g \in G$ için;

$$(st) * g = (st)g(st)^{-1} = s(tgt^{-1})s^{-1} = s * (tgt^{-1}) = s * (t * g) \text{ ve}$$

$$e * g = ege = g$$

olur. Buna S nin G üzerine eşlenikleme etkisi denir (Asar vd 2009).

Tanım 2.1.4: G bir grup ve p bir asal sayı olsun. Eğer her $x \in G$ için. $x^{p^k} = e$ olacak şekilde bir $k \geq 0$ tamsayısı varsa G ye bir p -grubu denir (Asar vd 2009).

Tanım 2.1.5: G bir grup. $S \leq G$ olsun. $N_G(S) = \{x \in G : xSx^{-1} = S\}$ kümesine S nin G deki normalleyeni denir.(Bilgiç 2013).

Tanım 2.1.6: G grubunun aşikâr alt gruplarından başka normal alt grupları yoksa o zaman bu G grubuna basit grup denir (Taşçı 2008).

Teorem 2.1.1: $n \geq 5$ için A_n basit bir gruptur (Asar vd 2009).

Tanım 2.1.7: G bir grup ve $0 \leq i < n$ için H_i ler de G grubunun alt grupları olsun.

$\{e\} = H_0 \leq H_1 \leq \dots \leq H_n = G$ serisine G grubunun alt normal serisi denir (Asar vd 2009).

Tanım 2.1.8: G bir grup ve $H = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_n = G$, G nin bir altnormal serisi olsun. Eğer her $0 \leq i < n$ için H_{i+1}/H_i bölüm grubu abelyen ise G ye bir çözülebilir grup denir. Ayrıca $H_n = \{e\}$ koşulunu sağlayan en küçük n sayısına G grubunun türev uzunluğu denir (Asar vd 2009).

Teorem 2.1.2: G çözülebilir ise G grubunun alt grupları ve bölüm grupları da çözülebilirdir.(Rotman 1995).

Sonuç 2.1.1: $n \geq 5$ ise G_n çözülebilir değildir.

Teorem 2.1.3: G bir grup ve $N \triangleleft G$ olmak üzere, eğer N grubunun çözülebilir olması ve G/N bölüm grubunun çözülebilir olması durumunda G grubu da çözülebilirdir (Asar vd 2009).

Tanım 2.1.9: G bir grup ve $H, S \leq G$ olsun.

$$[H, S] = \langle [h, s] \mid h \in H, s \in S \rangle$$

grubuna H ile S nin alt gruplarının komütatör alt grubu denir.

Tanım 2.1.10: G bir grup ve komütatör alt grubu G' olmak üzere, eğer $G' = G$ oluyorsa G grubu mükemmel grup olarak adlandırılır.

Teorem 2.1.4: Bir G grubu mükemmel grup ise G nin her bölüm grubu da mükemmeldir.(Dummit and Foote 2004).

Tanım 2.1.11: Bir G grubu; eğer $G \cong (\mathbb{Z}_p)^n$ (p asal) biçiminde izomorf bir yapıya sahipse G grubuna elementer abelyen p - grup denir. (Rotman 1995).

Tanım 2.1.12: Bir grubun tüm maksimal alt gruplarının kesişimi o grubun Frattini alt grubu oluşturur.

Tanım 2.1.13: Bir G grubundaki her elemanın mertebesi göz önüne alındığında bu mertebelerin en küçük ortak katı grubun eksponenti olarak tanımlanır (Çallıalp 2009).

Tanım 2.1.14: G bir grup H da bu grubun alt grubu olsun. Eğer G nin tüm otomorfizmleri φ için, $\varphi(H) \leq H$ ise H karakteristik alt gruptur.

Tanım 2.1.15: $\mathbb{F}$ bir cisim olmak üzere $GL(n, \mathbb{F}) = \{X \in M: \det(X) \neq 0\}$ grubuna genel lineer grup denir (Bray et al. 2013).

Tanım 2.1.16: $SL(n, q) = \{X \in M: \det(X) = 1\}$ grubu özel lineer grup olarak adlandırılır (Bray *et al.* 2013).

Tanım 2.1.17: G bir grup ve G/N bölüm grubu çözülebilir olacak şekilde N normal alt gruplarının arakesitine G grubunun çözülebilir kalanı denir (Rose 1978).

Teorem 2.1.5: G bir grup ve N de G grubunun çözülebilir kalanı ise bu durumda N , G grubunun türev serisindeki son gruptur (Kantor 2003).



2.2. Klasik Gruplar

Tanım 2.2.1: p bir asal sayı ve $\mathbb{F}$ karakteristiği p olan sonlu bir cisim olsun. $\mathbb{F}$ cismi üzerinde bir sol lineer veya kuadratik form q tarafından belirlenen ve aşağıda ele alınan dört durumun her biri için $S \leq I \leq \Delta \leq \Gamma$ şeklinde bir grup zinciri mevcuttur. Eğer bir Y grubuna karşılık gelen $\bar{Y}$, $PY = Y/Z(Y)$ şeklinde gösterilen projektif grup yukarıdaki zincirin projektif karşılığı olarak $\bar{S} \leq \bar{I} \leq \bar{\Delta} \leq \bar{\Gamma}$ şeklinde olur.

Söz konusu dört klasik grup ailesine ilişkin temel özellikler aşağıdaki tabloda verilmiştir:

L durumu ; q sıfır form
S durumu; $q = f$, dejenere olmayan simplektik form
O durumu; $q = \vartheta$, dejenere olmayan kuadratik form
U durumu; $q = f$, dejenere olmayan üniter form

2.2.1. Lineer Gruplar

Burada **L** durumu geçerli olacaktır. Böylece q sıfır formdur ve

$$\Gamma = \Gamma L(V, \mathbb{F}) \cong \Gamma L_n(q)$$

$$I = \Delta = GL(V, \mathbb{F}) \cong GL_n(q)$$

$$\Omega = S = SL(V, \mathbb{F}) \cong SL_n(q)$$

dır.

Önerme 2.2.1.1 : $|I| = q^{n(n-1)/2} \prod_{i=1}^n (q^i - 1)$ dir (Kleidman and Lebeck 1990).

Tanım 2.2.1.1: $\mathbb{F}$ bir cisim ve V , $\mathbb{F}$ cismi üzerinde tanımlanan n boyutlu vektör uzayı olsun. V nin tüm tersinir lineer dönüşümlerinin kümesi bileşke işlemi altında bir grup oluşturur. Bu gruba V nin genel doğrusal lineer grubu denir ve $GL(V)$ olarak gösterilir. $V = \mathbb{F}^n$ alınırsa bu grup, $\mathbb{F}$ cismi üzerindeki $n \times n$ boyutlu tersinir matrislerin grubuna izomorf olur. Yani;

$$GL(n, \mathbb{F}) = \{X \in M_{n \times n}(\mathbb{F}) | \det(X) \neq 0\}$$

dır.

Tanım 2.2.1.2: Determinantı bir olan tüm $n \times n$ matrislerin oluşturduğu $GL(n, \mathbb{F})$ grubunun alt gruplarına özel lineer grup denir ve $SL(n, \mathbb{F})$ şeklinde gösterilir. Yani;

$$SL(n, \mathbb{F}) = \{X \in GL(n, \mathbb{F}) | \det(X) = 1\}$$

dir. $SL(n, \mathbb{F})$ alt grubu aynı zamanda $GL(n, \mathbb{F})$ nin bir normal alt grubudur.

Teorem 2.2.1.1: $\mathbb{F}_q$ sonlu bir cisim olsun. Bu durumda, $GL(n, \mathbb{F})$ grubunun mertebesi;

$$|GL(n, q)| = (q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{n-1}).$$

şeklindedir (Grove 2002).

Tanım 2.2.1.3: Özel lineer grubun skaler matrislerinden oluşan merkezine bölümüne projektif özel lineer grup denir ve $PSL(n, \mathbb{F})$ şeklinde gösterilir. Yani;

$$PSL(n, \mathbb{F}) = SL(n, \mathbb{F})/Z(SL(n, \mathbb{F})).$$

dir. Sonlu cisimler üzerinde $n \geq 2$ ve $(n, q) \neq (2, 2), (2, 3)$ koşulu altında $PSL(n, q)$ grubu basit bir gruptur (Wilson 2009).

2.2.2. Ortogonal Gruplar

Bu kısımda **O** durumu geçerli olacaktır. Ortogonal gruplar dejenere olmayan simetrik bir çift doğrusal formu veya ona denk olarak bir kuadratik formu koruyan dönüşümlerden oluşur.

Tanım 2.2.2.1: V , $\mathbb{F}$ cismi üzerinde sonlu boyutlu bir vektör uzayı ve $Q: V \rightarrow \mathbb{F}$ dejenere olmayan bir kuadratik form olsun. Bu durumda Q formunu koruyan tüm lineer dönüşümlerin kümesi ortogonal grup olarak adlandırılır. Yani;

$$O(V, Q) = \{g \in GL(V) | Q(g(v)) = Q(v) \forall v \in V\}$$

dır. Eğer $V = \mathbb{F}^n$ ve form $Q(v) = v^T J v$ olarak verilirse (J cisim üzerinde simetrik, tersinir bir matristir), o zaman matris,

$$O(n, \mathbb{F}, J) = \{X \in GL(n, \mathbb{F}) | X^T J X = J\}$$

şeklını alır.

Tanım 2.2.2.2: Ortogonal gruptaki determinanı bir olan elemanların alt grubuna özel ortogonal grup denir. Yani;

$$SO(n, \mathbb{F}, Q) = O(n, \mathbb{F}, Q) \cap SL(n, \mathbb{F})$$

dir.

$\mathbb{F}_q$ sonlu cismi üzerinde kuadratik formun artin invaryantına bağılı olarak farklı izomorfizm sınıfları vardır. Boyutu $n = 2m$ yani çift boyutlu olanlar için;

- i. Hiperbolik veya split tip $O^+(2m, q)$,
- ii. Eliptik veya non-split tip $O^-(2m, q)$

şeklinde gösterilir.

Tek boyutlu olanlar için yani; $n = 2m+1$ boyutlu olanlar genellikle $O(2m+1, q)$ şeklinde tek tipi vardır (Wilson 2009).

2.2.3. Simplektik Gruplar

Bu kısımda **S** durumu geçerli olacaktır. Simplektik gruplar, dejenere olmayan alterne bir çift doğrusal formu koruyan dönüşümlerden oluşur.

Tanım 2.2.3.1: $V, \mathbb{F}$ cismi üzerinde $2m$ boyutlu bir vektör uzayı ve $\mathcal{F}: V \times V \rightarrow \mathbb{F}$ dejenere olmayan alterne bir çift doğrusal form olsun. Yani, tüm $v, w \in V$ için $\mathcal{F}(v, w) = -\mathcal{F}(w, v)$ ve $\mathcal{F}(v, v) = 0$ olması durumudur. $\mathcal{F}$ yi koruyan tüm lineer dönüşümlerin grubuna simplektik grup denir.

$$Sp(V, \mathcal{F}) = \{g \in GL(V) | \mathcal{F}(g(v), g(w)) = \mathcal{F}(v, w) \forall v, w \in V\}$$

şeklindedir.

$V = \mathbb{F}^{2m}$ ve $\mathcal{F}(a, b) = a^T J b$, seçilirse standart simplektik matris;

$$J = \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix}$$

olarak alınır ve bu durumda simplektik grup matrislerle;

$$Sp(2m, \mathbb{F}) = \{A \in GL(2m, \mathbb{F}) | A^T J A = J\}$$

şeklinde ifade edilir (Carter 1989).

Teorem 2.2.3.1: Simplektik grubun tüm elemanlarının determinanı 1'dir. Yani;

$$Sp(2m, \mathbb{F}) \subseteq SL(2m, \mathbb{F})$$

dir (Wilson 2009).

Tanım 2.2.3.2: Simplektik grubun merkezine bölümüne projektif simplektik grup denir. Yani;

$$PSp(2m, \mathbb{F}) = Sp(2m, \mathbb{F}) / Z(Sp(2m, \mathbb{F}))$$

dir. Sonlu cisimler üzerinde $m \geq 1$ ve $(m, q) \neq (1, 2), (1, 3)$ için $PSp(2m, q)$ grubu basittir (Wilson 2009).

2.2.4. Üniter Gruplar

Bu kısımda U durumu geçerli olacaktır. Burada $\kappa = f$ dejenere olmayan üniter form olacaktır.

Tanım 2.2.4.1: $V, \mathbb{F}$ cismi üzerinde sonlu boyutlu bir vektör uzayı ve ϕ, V üzerinde dejenere olmayan bir hermityen form olsun. ϕ yi koruyan tüm lineer dönüşümlerin grubuna üniter grup denir. Yani;

$$U(V, \phi) = \{g \in GL(V) | \phi(g(u), g(v)) = \phi(u, v) \forall u, v \in V\}$$

Şeklindedir(Carter 1989).

Tanım 2.2.4.2: Üniter gruptaki determinanı bir olan elemanların alt gruplarına özel üniter grup denir. Yani;

$$SU(n, \mathbb{F}) = U(n, \mathbb{F}) \cap SL(n, \mathbb{F}) \text{ dir (Wilson 2009).}$$

3. MATERYAL ve YÖNTEM

3.1. Klasik Grupların Aschbacher Sınıflandırması

Geometrik yaklaşım, bir lineer grubun ilgili vektör uzayı üzerindeki etkisinde doğal ve kalıtsal geometrik özelliklerin sağlanıp sağlanmadığını araştırır. Bu yaklaşımı destekleyen en önemli faktörlerden biri Aschbacher (1984)'de verilen klasik grupların maksimal alt gruplarının bir sınıflandırmasıdır.

$Z, G \leq GL(d, q)$ nun skaler matrislerinin alt grubu olmak üzere, eğer $T \leq G/Z \leq Aut(T)$ olacak şekilde abelyen olmayan basit bir T grubu varsa G ye hemen hemen basit modülo skaler denir. Bu bilgiler ışığında Aschbacher sınıflandırması şu şekilde verilebilir:

Teorem 3.1.1: $V, GL(d, q)$ grubunun etki ettiği bir vektör uzayı; $G, GL(d, q)$ nun bir maksimal alt grubu ve Z, G nin skaler matrislerden oluşan bir alt grubu ($Z = Z(GL(d, q)) \cap G$) olsun. Bu durumda aşağıdaki durumlardan en az biri geçerlidir:

C_1 . G grubunun etkisi indirgenebilirdir.

C_2 . G grubunun etkisi ilkel değildir.

C_3 . G grubu $n > 1$ olmak üzere $\mathbb{F}_{q^n}$ cisim genişlemesi üzerinde tanımlanmış boyutu d/n olan bir vektör uzayının yarı-doğrusal otomorfizmlerinin grubu olarak V üzerinde etkir.

C_4 . G grubu $m_1, m_2 > 1$ boyutlarındaki X, Y uzaylarının $X \otimes Y$ tensör çarpımı şeklinde V nin bir ayrışımını korur.

C_5 . G grubu $\mathbb{F}_{q'}, \mathbb{F}_q$ nun has bir alt cismi olmak üzere bir $g \in GL(d, q)$ olmak üzere, $G^g \leq GL(d, q')$ Z şeklindedir.

C_6 . G grubu bazı r asal sayıları için $d = r^n$ için mertebesi 2^{2n+2} olan simplektik grubu veya mertebesi r^{2n+1} olan ekstra-özel grubunu normalleştirir.

C_7 . G grubunun yapısı tensör-induced yapıdadır.

C_8 . G grubu bir klasik grubu içerir ve aynı zamanda onun normalleştiricisidir.

C_9 . G/Z bölüm grubu merkezi olmayan bir minimal normal alt gruba sahip basit bir yapıdadır (Aschbacher 1984).

3.2. C_6 Tipli Gruplar

Aschbacher sınıflandırmasında yer alan C_6 sınıfında bir G grubu r^m boyutlu indirgenemez bir temsilde normal alt grubu olarak ekstra-özel veya simplektik tip r -grubu içeren bir normalleyici olarak ifade edilebilir. Şimdi C_6 sınıfına giren gruplar için önemli olan bazı tanım ve teoremler vereceğiz.

Tanım 3.2.1: G, p -grup olsun ve

- I. G grubu elementer abelyan p -grup
- II. G' elementer abelyan ve $\psi(G) = Z(G) = G'$

şartlarından biri sağlanır ise G grubuna özel p -grubu denir (Suzuki 1986).

Tanım 3.2.2: Eğer değişmeli olmayan G özel p - grubunun merkezi devirliyse bu G grubu ekstra-özel p -grup olarak adlandırılır (Suzuki 1986).

Teorem 3.2.1: E değişmeli grubu $\forall a \in E$ için $a^p = 1$ (p asal sayı) eşitliği sağlanıyorsa E grubu $\mathbb{F}_p$ cismi üzerinde bir vektör uzayı olur (Suzuki 1982).

Teorem 3.2.2: G, p -grup olsun. G grubunun her maksimal N alt grubu normaldir ve G/N grubu p mertebeli bir devirli grup olur (Suzuki 1982).

Teorem 3.2.3: G bir p -grup ve G grubunun Frattini alt grubu $\varphi(G)$ olsun. O zaman $G/\varphi(G)$ grubunun her elemanı $a^p = 1$ koşulunu sağlayan bir değişmeli grup olur (Suzuki 1982).

Teorem 3.2.4: G bir p -grup ve G grubunun Frattini alt grubu $\varphi(G)$ olsun. Teorem 3.2.3. den $H = G/\varphi(G)$ nin her elemanı $a^p = 1$ koşulunu sağlayan bir değişmeli grup olur. Böylece Teorem 3.2.1. den $H, \mathbb{F}_p$ cismi üzerinde bir vektör uzayı olur. $|G/\varphi(G)| = p^t$ olarak alırsa, G nin elemanları $x_1, x_2, \dots, x_n$ ve $i = 1, 2, \dots, n$ ve $h_i = \varphi(G)x_i \in H$ için;

- i. H nin $\mathbb{F}_p$ üzerindeki boyutu t olur.
- ii. $G = \langle x_1, x_2, \dots, x_n \rangle$ olması için gerek ve yeter koşul H nin $h_1, h_2, \dots, h_n$ elemanlarıyla gerilen uzayla çakışmasıdır. Özel olarak $G = \langle x_1, x_2, \dots, x_n \rangle$ ise $n \geq t$ olur. G grubu t eleman tarafından gerilir ve $\{x_1, x_2, \dots, x_t\}$ alt kümesinin G grubunu germesi için gerek ve yeter koşul $\{h_1, h_2, \dots, h_t\}$ nin $\mathbb{F}_p$ cismi üzerinde tanımlı olan H vektör uzayının bir tabanı olmasıdır (Suzuki 1982).

Teorem 3.2.5: G , mertebesi $g = p^m$ olan bir p -grup olsun. G grubunun deęişmeli olmadığı ve M 'nin bir maksimal alt grubunun devirli olduğunu kabul edelim. Bu durumda, $m \geq 3$ tür ve eęer p tek olursa;

$$M(p^m) = \langle a, b | a^{p^{m-1}} = b^p = 1, b^{-1}ab = a^{1+p^{m-2}} \rangle$$

temsiliyle $M(p^m)$ grubu, $p = 2$ için $M(2^m)$ ($m \geq 4$), dihedral grup D_g , genelleştirilmiş kuaterniyon grup Q_g veya kuasi-dihedral grup QD_g a izomorf olur (Suzuki 1986).

Teorem 3.2.6: p^3 mertebeden deęişmeli olmayan bir G, p -grubu aşığıdaki gruplardan birine izomorftur:

- i. Eęer $p = 2$ ise $G \cong D_8$ ya da $G \cong Q_8$.
- ii. Eęer $p > 2$ ise ya $G \cong M(p^3)$ ya da $G \cong E(p^3) = \langle a, b | a^p = b^p = [a, b]^p = 1, [a, b] \in Z(E(p^3)) \rangle$. (Suzuki 1986).

Tanım 3.2.3. n ($n \geq 3$) kenarlı bir çokgenin tüm dönme ve yansımalarının oluşturduğu gruba dihedral grup denir ve

$$D_n = \langle a, b | b^2 = e, a^n = e, bab = a^{-1} \rangle = \{e, a, a^2, \dots, a^{n-1}, b, ab, \dots, a^{n-1}b\}$$

şeklinde ifade edilir (Hungerford 2003).

Tanım 3.2.4. $4n$ elemandan oluşan abelyen olmayan gruba genelleştirilmiş kuaterniyon grup denir ve

$$Q_n = \langle r, s | r^{2n} = 1, s^2 = r^n, s^{-1}rs = r^{-1} \rangle$$

şeklinde ifade edilir (Hungerford 2003).

Tanım 3.2.5. $n \geq 4$ için mertebesi 2^n olan abelyen olmayan gruba kuasi-dihedral grup denir ve

$$QD_n = \langle r, s | r^{2^{n-1}} = 1, s^2 = 1, s^{-1}rs = r^{2^{n-2}-1} \rangle$$

şeklinde ifade edilir.

Simplektik-tip grupların yapısı ekstra-özel gruplarla olan yakın ilişkisi üzerinden kurulabilir. Bu bağlamda simplektik-tip grupların yapısı temel olarak şu şekildedir:

Tanım 3.2.6: G bir p -grup olsun. G grubunun simplektik-tip grup olması için G nin her abelyen karakteristik alt grubu devirli olmalıdır.

Teorem 3.2.7: R bir simplektik-tip p -grup olsun. Bu taktirde R ;

- i. $E = \{1\}$ ya da E ekstra-özel grup,
- ii. S devirli ya da $p = 2$ ve $S, n \geq 4$ için hepsi 2^n mertebeden olmak üzere, D_n, Q_n veya QD_n gruplarından birine izomorftur,

olacak şekilde E ve S gruplarının merkeziz çarpımıdır. (Gorenstein 1980).

Bu çalışmada R simplektik-tip p -grubunun eksponenti üzerine bir kısıtlama getiriyoruz: p nin tek olması halinde eksponenti p, p nin çift olması halinde eksponenti 4 olacak şekilde Teorem 3.2.7 sayesinde bu tür simplektik-tip p -gruplarını aşağıdaki gibi sınıflandırabiliriz. Burada R_0 Teorem 3.2.6 da tanımlanan $E(p^3)$ grubudur.

Tablo 1: Simplektik-tip grupların yapısı

Grubun yapısı	Mertebe	Merkez	Notasyon
$R_0^{\circ n}$	p^{1+2n}	p	p^{1+2n}
$D_8^{\circ n}$	2^{1+2n}	2	2_+^{1+2n}
$(D_8^{\circ(n-1)}) \circ Q_8$	2^{1+2n}	2	2_-^{1+2n}
$Z_4 \circ D_8^{\circ n}$	2^{2+2n}	4	2^{2+2n}

R yukarıda tanımlanan simplektik-tip p -grup olsun. $\mathbb{F}_q$ cismi q mertebeli olmak üzere $p|q - 1$ koşulunu ve 2^{2+2n} durumunu için $4|q - 1$ olduğunu varsayalım. Bu durumda, $d = p^n$ için R den $GL(d, q)$ ya tanımlı ve çekirdeği trivial olan bir temsil bulunur (Kleidman and

Liebeck 1990). Sonuç olarak R ye izomorf $GL(d, q)$ alt grubu mevcuttur ve böylece R grubunu bir matris grubu olarak düşünülebilir. Bu izomorf grup da yine R ile gösterilecek.

Aschbacher' in sınıflandırmasındaki C_6 grupları $d = p^n$ olmak üzere bir R simplektik-tip grubunu normal alt grup olarak barındıran ve R nin $GL(d, q)$ daki normalleştiricisinin alt gruplarından oluşur. Başka bir deyişle her C_6 grubu G için $R \trianglelefteq G \leq N_{GL(d, q)}(R)$ koşulunu sağlayan bir R simplektik-tip grubu mevcuttur. Bu normalleştiricinin yapısı ise aşağıda verilmiştir.

Tablo 2: Normalleştiricinin Yapısı

$N_{GL(d, q)}(R)$ nin yapısı	Mertebe
$Z(GL(d, q)) \circ p^{1+2n}.Sp(2n, p)$	p tek
$Z(GL(d, q)) \circ 2^{2+2n}.Sp(2n, 2)$	$p = 2$ ve $4 q - 1$
$Z(GL(d, q)) \circ 2_+^{1+2n}.O^+(2n, 2)$	$p = 2$
$Z(GL(d, q)) \circ 2_-^{1+2n}.O^-(2n, 2)$	$p = 2$

$p|q - 1$ koşulu göz önüne alındığında çalışmamız kapsamında bu gruplardan yalnızca ilk iki grup tipi ele alınacaktır. C_6 sınıfındaki grupların yapılarının detaylı bir incelemesi Kleidman and Liebeck (1990)'de mevcuttur.

3.3. $Sp(6, p)$, $Sp(8, p)$, $Sp(10, p)$ ve $Sp(12, p)$ nin Maksimal Alt Grupları

Bu bölümde Bray *et al.* (2013)'ten alınan $Sp(6, p)$, $Sp(8, p)$, $Sp(10, p)$ ve $Sp(12, p)$ gruplarının maksimal alt grupları aşağıda verilmiştir.

Tablo 3: $Sp(6, p)$ maksimal alt grupları ($d = Z(Sp(6, p)) = (p - 1, 2), |\phi| = e, p = q^e$)

Sınıf	Maksimal Alt Grup	Şart	$p = 2$	$p = 3$	$p \geq 5$
C_1	$E_p^{1+4}: ((p-1) \times Sp(4, p))$	p tek		✓	✓
	$E_p^5: ((p-1) \times Sp(4, p))$	p çift	✓		
	$E_p^{3+4}: (GL(2, p) \times Sp(2, p))$	-	✓	✓	✓
	$E_p^6: GL(3, p)$	-	✓	✓	✓
	$Sp(2, p) \times Sp(4, p)$	-	✓	✓	✓
C_2	$Sp(2, p)^3: S_3$	$p \geq 3$		✓	✓
	$GL(3, p).2$	p tek		✓	✓
C_3	$Sp(2, p^3): 3$	-	✓	✓	✓
	$GU(3, p).2$	p tek		✓	✓
C_4	$Sp(2, p) \circ GO(3, p)$	$p \geq 5$ tek			✓
C_8	$SO^+(6, p)$	p çift	✓		
	$SO^-(6, p)$	p çift	✓		
C_9	$2'A_5$	$p = q \equiv \pm 3, \pm 13 \pmod{40}$		✓	✓
	$N1$	$p = q \equiv \pm 11, \pm 19 \pmod{40}$			✓
	$2'S_5^-$	$p = q \equiv \pm 1 \pmod{8}$			✓
	$2'L_2(7).2^+$	$p = q \equiv \pm 1 \pmod{16}$			✓
	$2'L_2(7)$	$p = q \equiv \pm 7 \pmod{16}, p \neq 7$			✓
	$2'L_2(13)$	$p = q \equiv \pm 1, \pm 3, \pm 4 \pmod{13}$		✓	✓
	$U_3(3): 2$	$p = 2$	✓		
	$2 \times U_3(3)$	$p = q \equiv \pm 7, \pm 17 \pmod{60}$			✓
	$N1$	$p = q \equiv \pm 19, \pm 29 \pmod{60}$			✓
	$(2 \times U_3(3)).2$	$p = q \equiv \pm 1 \pmod{12}$			✓
	$2'J_2$	$p = q \equiv \pm 1 \pmod{5}$			✓
	$2'J_2$	$p = 5$			✓
	$2'L_2(p)$	$q \geq 7$			✓

Tablo 4: $Sp(8, p)$ maksimal alt grupları ($d = Z(Sp(8, p)) = (p - 1, 2), |\phi| = e, p = q^e$)

Sınıf	Maksimal Alt Grup	Şart	$p = 2$	$p = 3$	$p \geq 5$
C_1	$E_p^{1+6}: ((p-1) \times Sp(6, p))$	p tek		✓	✓
	$E_p^7: ((p-1) \times Sp(6, p))$	p çift	✓		
	$E_p^{3+8}: (GL(2, p) \times Sp(4, p))$	-	✓	✓	✓
	$E_p^{6+6}: (GL(3, p) \times Sp(2, p))$	-	✓	✓	✓
	$E_p^{10}: GL(4, p)$	-	✓	✓	✓
	$Sp(6, p) \times Sp(2, p)$	-	✓	✓	✓
C_2	$Sp(2, p)^4: S_4$	$p \geq 3$		✓	✓
	$Sp(4, p)^2: S_2$		✓	✓	✓
	$GL(4, p).2$	p tek		✓	✓
C_3	$Sp(4, p^2): 2$	-	✓	✓	✓
	$GU(4, p).2$	p tek		✓	✓
C_4	$(Sp(2, p) \circ GO^-(4, p)).2$	p tek		✓	✓
C_6	$2_-^{1+6} \cdot SO_6^-(2)$	$p = q \equiv \pm 1 \pmod{8}$			✓
	$2_-^{1+6} \cdot GO_6^-(2)$	$p = q \equiv \pm 3 \pmod{8}$		✓	✓
C_7	$(Sp(2, p) \circ Sp(2, p))$	$p \geq 5$ tek			✓
C_8	$SO^+(8, p)$	p çift	✓		
	$SO^-(8, p)$	p çift	✓		
C_9	$2 \cdot L_2(7)$	$p = q \equiv \pm 5 \pmod{12}, p \neq 7$			✓
	$2 \cdot L_2(7).2$	$p = q \equiv \pm 1 \pmod{12}$			✓
	$2 \cdot A_6$	$p = q \equiv \pm 9 \pmod{20}$			✓
	$2 \cdot A_6.2_2$	$p = q \equiv \pm 1 \pmod{20}$			✓
	$L_2(17)$	$p = 2$	✓		
	$2 \cdot L_2(17)$	$p = q \equiv \pm 1, \pm 2, \pm 4, \pm 8 \pmod{17}, p \neq$			✓
	S_{10}	$p = 2$	✓		
	$2 \cdot L_2(p)$	$q \geq 11$			✓
	$2 \cdot L_2(p^3).3$	p tek		✓	✓

Tablo 5: $Sp(10, p)$ maksimal alt grupları ($d = Z(Sp(10, p)) = (p - 1, 2), |\phi| = e, p = q^e$)

Sınıf	Maksimal Alt Grup	Şart	$p = 2$	$p = 3$	$p \geq 5$
C_1	$E_p^{1+8} : ((p - 1))$	p tek		✓	✓
	$E_p^9 : ((p - 1) \times Sp(8, p))$	p çift	✓		
	$E_p^{3+12} : (GL(2, p))$	-	✓	✓	✓
	$E_p^{6+12} : (GL(3, p))$	-	✓	✓	✓
	$E_p^{10+8} : (GL(4, p))$	-	✓	✓	✓
	$E_p^{15} : GL(5, p)$	-	✓	✓	✓
	$Sp(8, p) \times Sp(2, p)$	-	✓	✓	✓
	$Sp(6, p) \times Sp(4, p)$	-	✓	✓	✓
C_2	$Sp(2, p)^5 : S_5$	$p \geq 3$		✓	✓
	$GL(5, p).2$	p tek		✓	✓
C_3	$Sp(2, p^5) : 5$	-	✓	✓	✓
	$GU(5, p).2$	p tek		✓	✓
C_4	$Sp(2, p) \circ GO(5, p)$	p tek		✓	✓
C_8	$SO^+(10, p)$	p çift	✓		
	$SO^-(10, p)$	p çift	✓		
C_9	$2'A_6$	$p = q \equiv \pm 7 \pmod{16}$			✓
	$2'A_6.2_2$	$p = q \equiv \pm 1 \pmod{16}$			✓
	$2'L_2(11)$	$p = q \equiv \pm 3 \pmod{8}, p \neq 11$		✓	✓
	$2'L_2(11).2$	$p = q \equiv \pm 1 \pmod{8}$			✓
	$2'L_2(11)$	$p = q \equiv \pm 11 \pmod{24}, p \neq$			✓
	$2'L_2(11)$	$p = q \equiv \pm 11 \pmod{24}, p \neq$			✓
	$2'L_2(11).2$	$p = q \equiv \pm 1 \pmod{24}$			✓
	$2'L_2(11).2$	$p = q \equiv \pm 1 \pmod{24}$			✓
	$2 \times U_5(2)$	$p = q \equiv \pm 3 \pmod{8}$		✓	✓
	$(2 \times U_5(2)).2$	$p = q \equiv \pm 1 \pmod{8}$			✓
	$2'L_2(p)$	$q \geq 11$			✓

Tablo 6: $Sp(12, p)$ maksimal alt grupları ($d = Z(Sp(12, p)) = (p - 1, 2), |\phi| = e, p = q^e$)

Sinif	Maksimal Alt Grup	Şart	$p = 2$	$p = 3$	$p \geq 5$
C_1	$E_p^{1+10}: ((p - 1)$	p tek		✓	✓
	$E_p^{11}: ((p - 1) \times Sp(10, p))$	p çift	✓		
	$E_p^{3+16}: (GL(2, p)$	-	✓	✓	✓
	$E_p^{6+18}: (GL(3, p)$	-	✓	✓	✓
	$E_p^{10+16}: (GL(4, p)$	-	✓	✓	✓
	$E_p^{15+10}: (GL(5, p)$	-	✓	✓	✓
	$E_p^{21}: GL(6, p)$	-	✓	✓	✓
	$Sp(10, p) \times Sp(2, p)$	-	✓	✓	✓
	$Sp(8, p) \times Sp(4, p)$	-	✓	✓	✓
C_2	$Sp(2, p)^6: S_6$	$p \geq 3$		✓	✓
	$Sp(4, p)^3: S_3$		✓	✓	✓
	$Sp(6, p)^2: S_2$		✓	✓	✓
	$GL(6, p).2$	p tek		✓	✓
C_3	$Sp(6, p^2): 2$	-	✓	✓	✓
	$Sp(4, p^3): 3$	-	✓	✓	✓
	$GU(6, p).2$	p tek		✓	✓
C_4	$(Sp(2, p) \circ GO^+(6, p)).2$	p tek		✓	✓
	$(Sp(2, p) \circ GO^-(6, p)).2$	p tek		✓	✓
	$Sp(4, p) \circ GO(3, p)$	$p \geq 5$ tek		✓	✓
C_8	$SO^+(12, p)$	p çift	✓		
	$SO^-(12, p)$	p çift	✓		
C_9	$2'L_2(11)$	$p = q \equiv \pm 9 \pmod{20}, p \neq$			✓
	$2'L_2(11)$	$p = q \equiv \pm 9 \pmod{20}, p \neq$			✓
	$2'L_2(11).2$	$p = q \equiv \pm 1 \pmod{20}$			✓
	$2'L_2(11).2$	$p = q \equiv \pm 1 \pmod{20}$			✓
	$2'L_2(13)$	$p = q \equiv \pm 13 \pmod{28}, p \neq$			✓
	$2'L_2(13)$	$p = q \equiv \pm 13 \pmod{28}, p \neq$			✓
	$2'L_2(13)$	$p = q \equiv \pm 13 \pmod{28}, p \neq$			✓
	$2'L_2(13).2$	$p = q \equiv \pm 1 \pmod{28}$			✓
	$2'L_2(13).2$	$p = q \equiv \pm 1 \pmod{28}$			✓
	$2'L_2(13).2$	$p = q \equiv \pm 1 \pmod{28}$			✓
	$2'L_2(13).2$	$p = q \equiv \pm 1 \pmod{28}$			✓
	$2'L_2(25)$	$p = q \equiv \pm 2 \pmod{5}, p \neq$			✓
	$L_2(25).2_2$	$p = 2$	✓		
	$2'S_4(5)$	$p = q \equiv \pm 1 \pmod{5}$			✓

$2 \cdot G_2(4)$	$p = q \equiv \pm 3 \pmod{8}, q \neq 3$			✓
$2 \cdot G_2(4) \cdot 2$	$p = q \equiv \pm 1 \pmod{8}$			✓
S_{14}	$p = 2$	✓		
$2 \cdot \text{Suz}$	$p = 3$		✓	
$2 \cdot L_2(p)$	$q \geq 13$			✓
$2 \cdot S_4(p)$	$q = 5$			✓

3.4. Algoritmik Kavramlar

Bu başlık altında sık sık kullanacak olduğumuz BlindDescent algoritmasını anlamak için gerekli olan bazı algoritmik bilgiler verilecektir.

Hesaplamalı Grup Teori (HGT) de geliştirilen algoritmaların büyük bir kısmı rastgele yapıya sahiptir. Bu durumun temel nedeni ise bu tür algoritmaların çoğu zaman deterministik (belirleyici olan) algoritmalara göre çok daha hızlı ve verimli sonuçlar üretmesidir.

Bu bağlamda bir hesaplama görevi genel olarak girdi a ve buna karşılık elde edilen çıktı b arasında tanımlanan bir bağıntı $R(a, b)$ biçiminde ifade edilir. Eğer a 'ya karşılık gelen b çıktısı doğru sonucu veriyorsa, $R(a, b)$ bağıntısının tutarlı olduğu söylenir.

Grup teorisine uygulandığında bu algoritmalarda girdi genellikle bir grubun üreteç kümesi olur. Çıktı ise, bu grubun belirli bir alt grubunu üreten elemanlar kümesinden oluşabileceği gibi, grubun mertebesi gibi sayısal bir değer veya bir karar verme probleminin sonucu da olabilir.

Genel olarak algoritmalar iki ana sınıfa ayrılır. Bunlar deterministik (belirleyici) ve nondeterministik (belirleyici olmayan) algoritmalarıdır. Nondeterministik (belirleyici olmayan) algoritmalarda aynı girdi tekrar kullanılsa dahi, farklı çalıştırmalarda farklı sonuçlar üretebilir. Buna karşın doğru biçimde tasarlanmış bir deterministik (belirleyici) algoritma her girdi a için $R(a, b)$ bağıntısını sağlayan tek ve tutarlı bir çıktı üretir.

3.5. Monte Carlo Algoritmaları ve Alt Sınıfları

Bir önceki bölümde rastgele algoritmaların genel yapısı ve Hesaplamalı Grup Teori (HGT) sindeki kullanımı ele alınmıştır. Bu bölümde ise, rastgele algoritmaların özel bir sınıfı olan Monte Carlo algoritmaları ve bu algoritmalara ait alt sınıflar incelenecektir.

Tanım 3.5.1: $\varepsilon < 1/2$ olacak şekilde bir hata payı tanımlansın. Eğer her a girdisi için

$$Prob(R(af(a, r)) \text{ tutarlı}) \geq 1 - \varepsilon$$

koşulu sağlanıyorsa, bu tür rastgele algoritmalara Monte Carlo algoritması denir. Burada ε değeri algoritma tasarlandıktan sonra olasılık temelli hata sınırı olarak belirlenir ve algoritmanın güvenilirlik düzeyini ifade eder.

Rastgele algoritmaların güvenilirliği aynı girdiler üzerinde algoritmanın birden fazla kez çalıştırılması veya farklı girdilerle uygulanarak deneme sayısının artırılması yoluyla değerlendirilebilir. Bu yöntemle algoritmanın ürettiği sonuçların doğruluk olasılığı gözlemlenir ve böylece algoritmanın güvenilirliği konusundaki olası eksiklikler azaltılabilir.

Monte Carlo algoritmaları, rastgeleliğe dayalı bu tür yaklaşımların en yaygın örneklerinden biridir. Bu algoritmaların özel bir türü olan tek taraflı Monte Carlo (1MC) algoritmaları, özellikle karar verme problemlerinde kullanılır. 1MC algoritmalarında olası çıktılarından yalnızca biri için doğruluk garantisi sağlanır. Eğer doğru cevap ‘evet’ ise algoritma bazen yanlış bir sonuç üretebilir; ancak doğru cevap ‘hayır’ olduğunda algoritma mutlaka ‘hayır’ sonucunu üretmelidir. Yani; ‘evet’ çıktısı her koşulda güvenilir kabul edilirken, ‘hayır’ çıktısı her koşulda doğru olmayabilir.

Bu yapıya karşılık olarak tanımlanan co-1MC algoritmaları, 1MC algoritmalarındaki ‘evet’ ve ‘hayır’ çıktılarının rollerinin yer değiştirmesiyle elde edilir. Böylece bu algoritmalarda ‘hayır’ çıktısı garanti altına alınırken, ‘evet’ çıktısının doğruluğu olasılıksal olur.

Monte Carlo algoritmalarının önemli bir alt sınıfı Las Vegas algoritmalarıdır. Bu algoritmalar ilk kez Babai (1979) tarafından tanımlanmıştır. Las Vegas algoritmalarında rastgelelik kullanılmasına rağmen her zaman doğru sonuç üretilir ancak bu doğruluk çalışma süresinin rastgele olması ile mümkündür. Başka bir ifade ile Las Vegas algoritmaları hatasızdır fakat çalışma süreleri farklılık gösterebilir.

Tanım 3.5.2: Verilen bir girdiye karşılık hiçbir koşulda yanlış sonuç üretmeyen bir Monte Carlo algoritmasına Las Vegas algoritması denir.

Las Vegas algoritmaları doğru sonucu $1 - \varepsilon$ dan büyük bir olasılıkla elde ederler, doğru sonuca ulaşamadıkları durumlarda ise yanlış bir çıktı vermek yerine ‘hata’ uyarısı verirler. Burada ε , 1 den küçük sabit bir hata olasılığıdır. Ayrıca, algoritmanın doğru sonucu bulma olasılığı algoritmanın n kez tekrarlanması durumunda en az $1 - \varepsilon^n$ seviyesine çıkarılabilir.

3.6. BlindDescent Algoritması

Hesaplamalı Grup Teori (HGT)de birçok algoritmanın temel amacı, bir grubun içyapısını analiz etmek veya belirli alt grupları tespit etmektir. Özellikle klasik gruplarda, normal alt grupların bulunması ve uygun homomorfizmlerin kurulması oldukça karmaşık problemlerdir. Bu tür problemlere yönelik geliştirilen rastgele tabanlı yöntemlerden biri de BlindDescent algoritmasıdır.

BlindDescent, verilen bir grubun içinde belirli yapısal özelliklere sahip bir normal alt grup bulmak ve bu bilgiyi kullanarak gruptan başka bir gruba açık olmayan bir homomorfizm inşa etmek amacıyla tasarlanmıştır. Bu algoritma, Las Vegas tipli olasılıksal bir yöntem olup, doğruluğu garanti edilen sonuçlar üretir.

2006 yılında Brooksbank *et al.* C_6 grupları için bir indirgeme algoritması kurulmuşlardır ve bu algoritmayı aşağıdaki teorem ile gösterebiliriz:

Teorem 3.6.1: $n \geq 2$ ve $d = p^n$ (n asal) olmak üzere $R \leq GL(d, q)$ ekstra-özel p -grup olsun. $R \triangleleft G \leq N := N_{GL(d, q)}(R)$ ve eğer $n > 2$ ise $G/RZ(G) \cong N/RZ(N)$ olacak şekilde $G = \langle A \rangle$ grubu verildiğinde bazı $t \in \{1, 2, \dots, n\}$ için $K = GL(2t, p)$ ya da $K = S_{p^t}$ olacak şekilde $\psi: G \rightarrow K$ aşikar olmayan homomorfizmini kuran bir Las Vegas algoritması vardır. (Brooksbank *et al.* 2006).

Bu algoritma temel olarak iki parçadan oluşur. İlk önce bir normal alt grup bulan ve BlindDescent algoritması denen algoritma kurulur ardından grubun üreteçlerinin homomorfizm görüntüsü hesaplanır.

BlindDescent algoritmasından önce bu algoritma içinde kullanılacak olan *NORMALCLOSURE* ve *TESTABELIAN* algoritmaları için ön bilgiler verilecektir.

NORMALCLOSURE algoritmasında verilen bir alt grubun normal kapanışını belirlemek için kullanılır (Cooperman and Finkelstein 1993). Bu algoritmada rastgele alt çarpımlar kullanarak yapılan hesaplamalar vardır. Yani, bir grubun elemanlarının oluşturduğu $T = \{t_1, t_2, \dots, t_n\}$ kümesi için rastgele alt çarpımlar $t_1^{\varepsilon_1} t_2^{\varepsilon_2} \dots t_n^{\varepsilon_n}$ şeklindedir. Burada ε_i düzgün dağılımlı, bağımsız ve $\{0, 1\}$ -değerli rastgele değişkenlerdir.

NORMALCLOSURE(a, δ)

```

     $L := (a);$ 
    repeat  $\lceil 16n \log r \log(1/\delta) \rceil$  times
     $y :=$  random subproduct of  $L$ ;
     $x :=$  random subproduct of generators of  $G$ ;
    Add  $y^x$  to  $L$ ;
    done;
    return  $L$ ;

```

TESTABELIAN algoritması ise, algorithmada verilen bir elemanın oluşturduğu bölüm grubunun abelyen olup olmadığı test edilir. Yani $a \in G$ için $\langle a^G \rangle / \langle a^G \rangle \cap Z(G)$ bölüm grubunun abelyenliği test edilir. Bu algoritma bir co-1MC algoritmasıdır; yani “abelyen değil” cevabı her zaman doğru, “abelyen” cevabı ise olasılıksal olabilir.

TESTABELIAN(a, δ)

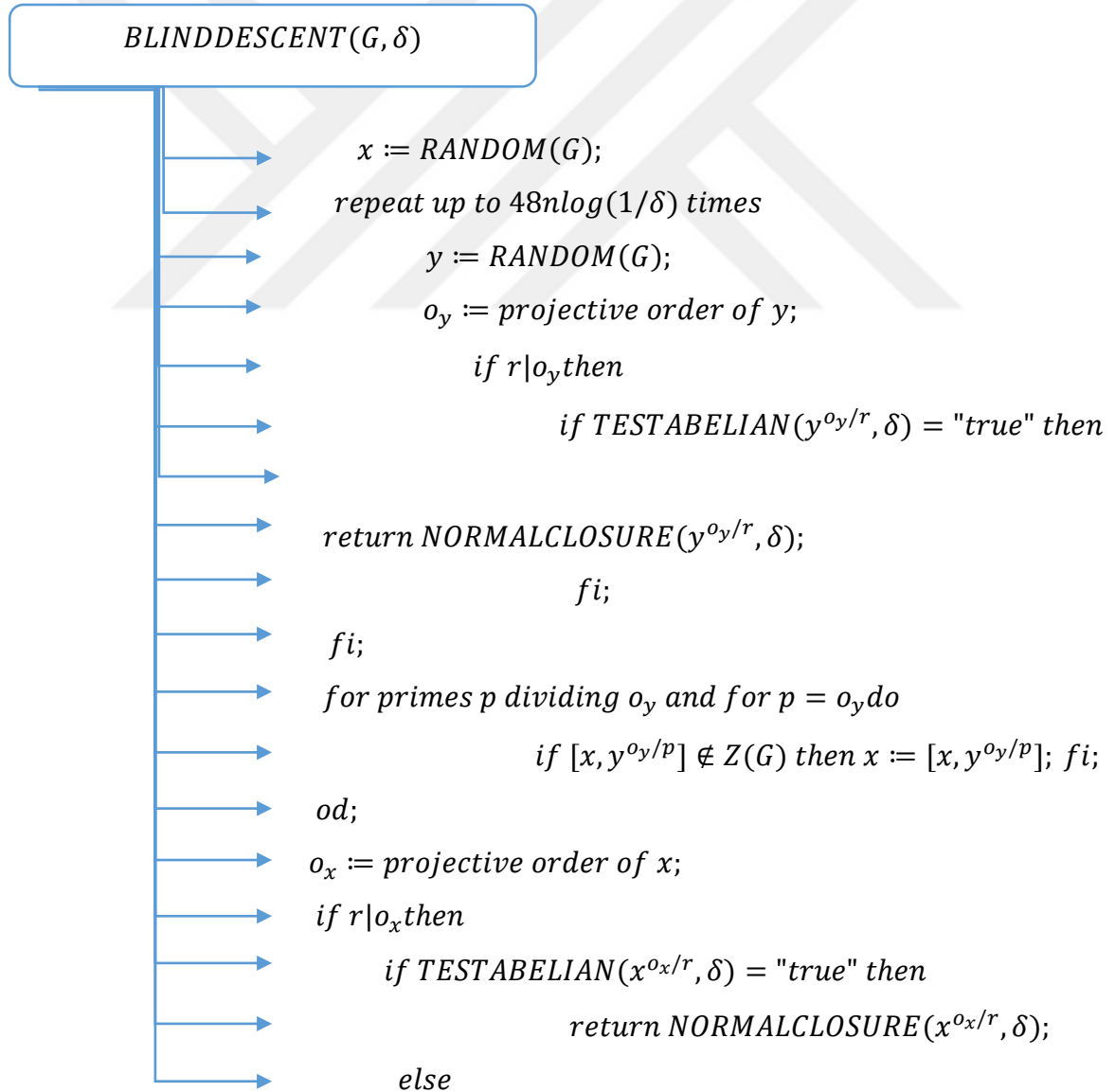
```

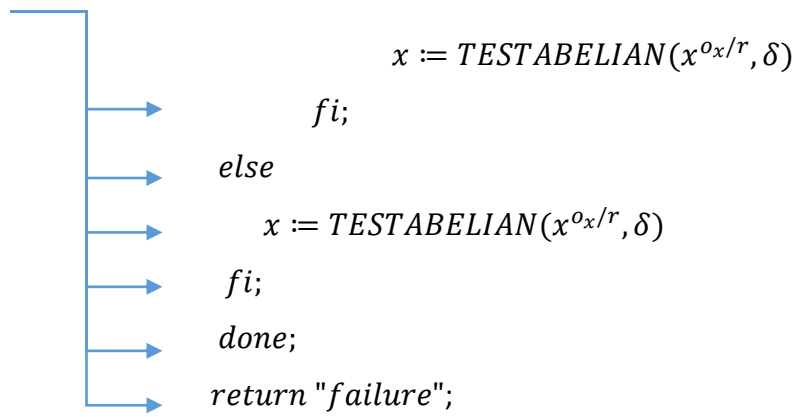
     $L := \text{NORMALCLOSURE}(a, \delta/2);$ 
    repeat  $\lceil (4/3) \log(2/\delta) \rceil$  times
     $y :=$  random subproduct of  $L$ ;
     $x :=$  random subproduct of  $L$ ;
    if  $[x, y]$  is nonscalar then
        return  $[x, y]$ ;
    fi;
    done;
    return "true"

```

Bu algoritmaları temel alan BlindDescent, 1999 yılında Babai ve Beals tarafından geliştirilmiştir. Bu algoritma, bir grubun herhangi bir normal alt grubuna ait bir elemanı bulan Monte Carlo tipi bir algoritmadır. Algoritmanın amacı rastgele seçilen grup elemanları üzerinden komütatörler oluşturarak normal alt grup bulmaktır. Örneğin; $c_2 = [t_1, t_2]$ ve $3 \leq i \leq n$ olmak üzere $c_i = [c_{i-1}, t_i]$ komütatörleri kullanılarak $(t_1, t_2, \dots, t_n)$ şeklinde rastgele bir eleman dizisi oluşturulur. Eğer bu dizideki bir g_i elemanı normal alt grubun bir elemanı ise son komütatör c_n de aynı normal alt grubun elemanı olacaktır. Aşağıda verilen BlindDescent algoritması, $\langle a^G \rangle / (\langle a^G \rangle \cap Z(G))$ elementer abelyen olacak şekilde skaler olmayan bir a elemanını bulmayı amaçlamaktadır.

Bu algoritma şu şekildedir:





4. ARAŞTIRMA BULGULARI

BlindDescent algoritmasının teorik analizi, girdi olarak girilen C_6 grubunun çözülebilirlik ve mükemmellik özellikleri temel alınarak gerçekleştirilecektir. BlindDescent algoritmasının çözülebilir gruplar üzerindeki başarısını kanıtlamak amacıyla aşağıdaki temel bilgiler verilmiştir.

4.1. Çözülebilir Alt Gruplar

Sonlu bir G grubunun türev serisinin eğer grup çözülebilir ise aşikâr alt grupla, çözülebilir değilse çözülebilir kalan olarak adlandırılan mükemmel bir grupla sona erdiği bilinmektedir. Bu durumdan dolayı grupları çözülebilirlik ve mükemmellik açısından inceleyeceğiz.

G , m . dereceden çözülebilir bir lineer grup olsun. G nin türev uzunluğu η ile gösterilsin. Bu durumda η için bir üst sınır olacak şekilde $\eta(m): \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ fonksiyonu vardır.

m . dereceden çözülebilir lineer grupların türev uzunluğu için bir üst sınır arayışı ilk olarak Zassenhaus (1937) tarafından inşa edilmiş ve bu sınır, Huppert (1957) ve Dixon (1968) tarafından daha da genişletilmiştir. Newman (1972) ise aşağıdaki sonuçlara ulaşmıştır:

σ fonksiyonu pozitif rasyonel sayılar üzerinde tanımlansın ve $k(m) = \lfloor \log_9 m \rfloor$ olmak üzere $\sigma(m)$ nın değeri aşağıdaki gibi olsun:

m nin Aralığı	$\sigma(m)$ Değeri
$9^{k(m)} \leq m \leq 16 \cdot 9^{k(m)-1}$	$5k(m)$
$16 \cdot 9^{k(m)-1} \leq m \leq 3 \cdot 9^{k(m)}$	$5k(m) + 1$
$3 \cdot 9^{k(m)} \leq m \leq 4 \cdot 9^{k(m)}$	$5k(m) + 2$
$4 \cdot 9^{k(m)} \leq m \leq 64 \cdot 9^{k(m)-1}$	$5k(m) + 3$
$64 \cdot 9^{k(m)-1} \leq m \leq 9^{k(m)+1}$	$5k(m) + 4$

Bu durumda $\eta(m)$ değeri;

m nin Değeri	$\eta(m)$ Değeri
$m = 1$ için	1
$m = 2$ için	4
$m \in \{6, 7, 17, 59, 60, 61, 62, 63, 64, 65\}$ için	$9 + \sigma((m - 2)/8)$
Diğer durumlarda	$10 + \sigma((m - 2)/8)$

şeklindedir.

Bu $\eta(m)$ fonksiyonuna göre bazı üst sınırlar aşağıdaki gibi gösterebilir:

Grup	Maksimum Türev Uzunluğu
$Sp(6, r)$	7
$Sp(8, r)$	8
$Sp(10, r)$	10
$Sp(12, r)$	10

BlindDescent algoritmasının girdisi olan C_6 grubunun çözülebilir normal alt grubundan rastgele eleman gelmesi durumuyla ilgili aşağıdaki teorem ifade edilebilir:

Teorem 4.1.1: $d = r^n$ olarak alınsın ve BlindDescent(G, δ) algoritmasının ana döngüsünün herhangi bir adımında G nin çözülebilir normal alt grubu N içinde skaler olmayan bir $x \in N$ elemanının üretildiğini düşünelim. Bu varsayım altında BlindDescent(G, δ) algoritması en

C_6 grubunun çözülebilir radikali için aranan skaler olmayan x elemanını ve elemanter abelyen r -grubun üreteçlerini BlindDescent algoritmasının başarılı bir şekilde oluşturduğu görülmektedir.

Şekil 2: $Sp(8,3)$ için çözülebilir alt grup örneği

Şekil 3 te $Sp(10,3)$ ün C_2 sınıfındaki $GL(5,3):C_2$ maksimal alt grubunun çözülebilir kalanı $PSL(5,3)$ ün mükemmel alt grubu A_5 den faydalanarak oluşturulan C_6 grubunun çözülebilir radikali için aranan skaler olmayan x elemanını ve elemanter abelyen r -grubun üreteçlerini BlindDescent algoritmasının başarılı bir şekilde oluşturduğu görülmektedir.



gap>

Şekil 3: $Sp(10,3)$ için çözülebilir alt grup örneği

4.2. Mükemmel Alt Gruplar

R , r^{1+2n} mertebeli bir ekstra-özel grup ve G , R nin skaler olmayan elemanlarını içeren şekilde $N = N_{GL(d,q)}(R)$ nin bir alt grubu olsun. Burada, N nin yapısı $(Z(GL(d,q)) \circ R)Sp(2n,r)$ şeklinde olduğundan $N/R \cong Sp(2n,r)$ olur. 2. İzomorfizm Teoremi'ni uygulayarak $G/(R \cap G) \cong GR/R \leq N/R$ elde edilir yani, $\bar{G} = G/(R \cap G) \leq Sp(2n,r)$ grubudur.

Eğer bu G grubu mükemmel bir grup ise bölüm grupları da mükemmel olacağı için $\bar{G}$ mükemmeldir. Bu nedenle, G grubunun mükemmel olduğu durumlar incelenirken, $Sp(2n,r)$ grubunun mükemmel alt gruplarından yararlanılacaktır. Bilindiği üzere her alt grup en az bir maksimal alt grup tarafından ve tüm mükemmel alt gruplar da çözülebilir kalanlar tarafından kapsanır. Dolayısıyla, bu maksimal alt grupların çözülebilir kalanlarını ve çözülebilir kalanların da mükemmel alt gruplarını belirlediğimizde $Sp(2n,r)$ grubunun bütün mükemmel alt gruplarını elde etmiş oluruz. Aşağıda yer alan teorem, lemma, önermeler ve ayrıca GAP (Grup, Algoritma, Programlama) yardımıyla (12th Gen Intel(R) Core(TM) i7-12700H 2.70 GHz işlemci ve 32gb RAM özelliklerine sahip bilgisayar ile birlikte) $n \in \{4,5,6\}$ için $Sp(2n,r)$ nin çözülebilir kalanları tablolar halinde verilmiştir:

İlk olarak Goncalves and Guaschi (2009) da yer alan aşağıdaki tanım ve teoremler kullanılacaktır:

Tanım 4.2.1: G ve H birer grup olsun ve G nin H üzerinde etkisi olduğunu kabul edelim. Bu etkiye bağlı olarak komütatör alt grup, g^h ifadesi g nin h üzerindeki etkisi olmak üzere,

$$\Gamma_G(H) = \langle g^h k h^{-1} k^{-1} \mid g \in G \text{ ve } h, k \in H \rangle$$

olarak tanımlanır.

Tanım 4.2.2: G bir grup olsun. G nin alt merkezil serisi $\{\Gamma_i(G)\}_{i \in \mathbb{N}}$ tümevarımsal olarak şu şekilde tanımlanır:

$\Gamma_1(G) = G$ ve her $i \in \mathbb{N}$ için $\Gamma_{i+1}(G) = [G, \Gamma_i(G)]$. Benzer şekilde, G nin türev serisi $\{G^{(i)}\}_{i \in \mathbb{N} \cup \{0\}}$ de $G^{(0)} = G$ ve her $i \in \mathbb{N}$ için $G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$ şeklinde tanımlanır.

Burada, $\Gamma_2(G) = G^{(1)} = G'$ olduğuna dikkat ediniz.

Herhangi bir grup-teorik $\mathcal{P}$ özelliği için, eğer herhangi bir aşikâr olmayan $x \in G$ elemanı için $\mathcal{P}$ özelliğine sahip bir H grubu ve $\varphi(x) \neq 1$ olacak şekilde $\varphi: G \rightarrow H$ örten homomorfizması varsa G ye kalanlı $\mathcal{P}$ özelliğine sahiptir denir. Bir G grubunun kalanlı nilpotent (sırasıyla kalanlı çözülebilir) olması için gerek ve yeter şart $\bigcap_{i \geq 1} \Gamma_i(G) = \{1\}$ (sırasıyla $\bigcap_{i \geq 0} G^{(i)} = \{1\}$) olduğu bilinmektedir.

Önerme 4.2.1: G ve H birer grup ve $\varphi: G \rightarrow \text{Aut}(H)$ dönüşümü G nin H üzerinde bir etkisi olsun. $\hat{H}$, $g \in G$ ve $h \in H$ olmak üzere $\varphi(g)(h)h^{-1}$ formundaki elemanlar tarafından üretilen H nin bir alt grubu ve L de $\Gamma_2(H)$ ve $\hat{H}$ tarafından üretilen H nin bir diğer alt grubu olsun. Bu durumda, φ , $\Gamma_2(G)$ nin L üzerinde yine φ ile gösterilen etkisini indükler ve $L \rtimes_{\varphi} \Gamma_2(G) = \Gamma_2(H \rtimes_{\varphi} G)$ dir. Özel olarak, $\Gamma_2(H \rtimes_{\varphi} G)$ grubu $\Gamma_2(H)$, $\Gamma_2(G)$ ve $\hat{H}$ tarafından üretilen alt gruptur.

Önerme 4.2.1 in ispatına geçmeden aşağıdaki hatırlatmayı vermek yerinde olacaktır.

Hatırlatma 4.2.1: L grubu aslında $\Gamma_G(H)$ komütatör alt grubudur. Gerçekten, $\Gamma_G(H)$, $\varphi(g)(h)kh^{-1}k^{-1}$ formundaki elemanlar tarafından üretilen H nin bir alt grubudur. $g = e$ (sırasıyla $k = e$) alınır, $\Gamma_G(H) \supseteq \Gamma_2(H)$ (sırasıyla $\Gamma_G(H) \supseteq \hat{H}$) ve böylece $L \subseteq \Gamma_G(H)$ olur. Tersine, $\varphi(g)(h)kh^{-1}k^{-1} = \varphi(g)(h)h^{-1}hkh^{-1}k^{-1} \in L$ olup $\Gamma_G(H) \subseteq L$ dir. Dolayısıyla, $L = \Gamma_G(H)$ bulunur. Ayrıca, eğer $h' \in H$ ise $\varphi(g)(h'') = h'$ olacak şekilde bir $h' \in H$ mevcut olup

$$h'(\varphi(g)(h)h^{-1})h'^{-1} = \varphi(g)(h''h)(h''h)^{-1}(\varphi(g)(h'')h''^{-1})^{-1}$$

dir. Dolayısıyla, $\hat{H}$ ve L , H in normal alt gruplarıdır. Özel olarak, $\Gamma_G(H)$ da H da normaldir.

Önerme 4.2.1 İspat: Bundan sonra H nin her bir H_1 alt grubu (sırasıyla G nin her bir G_1 alt grubu) $H \rtimes_{\varphi} G$ nin $\{(h, 1) | h \in H_1\}$ (sırasıyla $\{(1, g) | g \in G_1\}$) formundaki karşılık gelen alt grubu olarak tanımlanacaktır. $H \rtimes_{\varphi} G$ deki grup işlemi $(h, g), (h', g') \in H \rtimes_{\varphi} G$ olmak üzere,

$$(h, g) \cdot (h', g') = (h\varphi(g)(h'), gg')$$

şeklinde tanımlanır.

L alt grubunun H da normal olduğu Hatırlatma 4.2.1 de verilmişti. Şimdi φ nin G nin L üzerinde bir etkiyi (yine φ ile gösterilecektir) indüklediğini gösterelim. $g \in G$ olsun. Her $h_1, h_2 \in H$ için

$$\varphi(g)([h_1, h_2]) = [\varphi(g)(h_1), \varphi(g)(h_2)] \in \Gamma_2(H)$$

ve her $h \in H$ ve $g' \in G$ için;

$$\varphi(g)(\varphi(g')(h)h^{-1}) = \varphi(gg')(h)h^{-1}(\varphi(g)(h)h^{-1})^{-1} \in \hat{H}$$

olup $\varphi(g)(L) \subseteq L$ dir. $\varphi(g)$ nin $1 - 1$ olduğu açıktır. $\varphi(g)$ nin örtenliği (L ye kısıtlanışının) aşağıdakilerden çıkarılabilir:

(1) Eğer $i = 1, 2$ ve $h'_i \in H$ ise $\varphi(g)(h_i) = h'_i$ olacak şekilde $h_i \in H$ vardır ve böylece $\varphi(g)[h_1, h_2] = [h'_1, h'_2]$ dir.

(2) Eğer $g' \in G$ ve $h, h' \in H$ ise

$$\varphi(g)(\varphi(g^{-1}g')(h)h^{-1}h(\varphi(g^{-1})(h^{-1})h)h^{-1}) = \varphi(g')(h)h^{-1}$$

dir. Dolayısıyla, $\varphi, \Gamma_2(G)$ nin L üzerinde (yine φ ile gösterilen) bir etkisini indükler ve $L \rtimes_{\varphi} \Gamma_2(G), H \rtimes_{\varphi} G$ nin bir alt grubudur.

$\Gamma_2(H)$ 'nın (sırasıyla $\Gamma_2(G)$ nin) her elemanının $\Gamma_2(H \rtimes_{\varphi} G)$ nin bir elemanı olarak yazılabileceği açıktır. Dahası, eğer $g \in G$ ve $h \in H$ ise

$$[(1, g), (h, 1)] = (\varphi(g)(h), 1)(h^{-1}, 1) = (\varphi(g)(h)h^{-1}, 1)$$

dir. Böylece, $\hat{H}$ nın her elemanı $\Gamma_2(H \rtimes_{\varphi} G)$ nin bir elemanı olarak yazılabilir. Dolayısıyla, $L \rtimes_{\varphi} \Gamma_2(G) \subseteq \Gamma_2(H \rtimes_{\varphi} G)$ bulunur.

Ters kapsama için, $(h_1, g_1), (h_2, g_2) \in H \rtimes_{\varphi} G$ elemanlarının komütatörünün

$$[(h_1, g_1), (h_2, g_2)] = (h_1(\varphi(g_1)(h_2)\varphi(g_1g_2g_1^{-1})(h_1^{-1})\varphi([g_1, g_2])(h_2^{-1}), [g_1, g_2]))$$

şeklinde yazılabildiğine dikkat ediniz. İkinci çarpan $\Gamma_2(G)$ ye aittir. İlk çarpan ise

$$[h_1, h_2]h_2h_1h_2^{-1}(\varphi(g_1)(h_2)h_2^{-1})h_2h_1^{-1}h_2^{-1}h_2h_1(\varphi(g_1g_2g_1^{-1})(h_1^{-1})h_1)h_1^{-1}h_2^{-1}h_2(\varphi([g_1, g_2])(h_2^{-1})h_2)h_2$$

şeklinde olup L nin elemanlarının çarpımı şeklindedir. Böylece, $\Gamma_2(H \rtimes_{\varphi} G) \subseteq L \rtimes_{\varphi} \Gamma_2(G)$ bulunur. Bu ise ispatı tamamlar.

Teorem 4.2.1: G bir grup ve $H \leq G$ olsun. Bu takdirde, $G' \leq H$ olması için gerek ve yeter şart $H \trianglelefteq G$ ve G/H nin abelyen olmasıdır (Isaacs 2008).

Teorem 4.2.2: G bir grup $D_1, D_2, \dots, D_n$ de G nin alt grupları olsun. Eğer $G = D_1 \times D_2 \times \dots \times D_n$ ise G nin çözülebilir kalanı D_i ($1 \leq i \leq n$) alt gruplarının çözülebilir kalanlarının direkt çarpımıdır (Doerk and Hawkes 1978).

Önerme 4.2.2: $r \geq 4$ olması durumunda $Sp(2n, r)$ grubu mükemmel bir gruptur (Grove 2002).

Önerme 4.2.3: $r = 3$ ve $n \geq 2$ olması durumunda $Sp(2n, r)$ grubu mükemmel bir gruptur yani; türev grubu kendisine eşit olur (Grove 2002).

Lemma 4.2.1: $p \geq 3$ için $Sp(4, p^2)$: 2'nin çözülebilir kalanı $Sp(4, p^2)$ dir.

İspat: $Sp(4, p^2)$, G nin bir N normal alt grubuna izomorftur. Ayrıca $G/N \cong 2$ değişmeli olup $G' \leq Sp(4, p^2)$ dir. $p \geq 3$ için $Sp(4, p^2)$, Önerme 4. 2.1. göz önüne alındığında mükemmel grup olur ve G grubunun çözülebilir kalanı tarafından kapsanır. Çözülebilir kalan türev serisindeki son grup olup G' tarafından kapsanır. Dolayısıyla, $Sp(4, p^2)$ de G' tarafından kapsanır. Yani, $G' \subseteq Sp(4, p^2)$ olup $G' = Sp(4, p^2)$ dir.

Eğer $G = G_1 : G_2$ yarı direk çarpım ise Önerme 4.2.1. kullanılarak elde edilen $G' = (G'_1[G_1, G_2]) : G_2'$ eşitliği yardımıyla G nin türev serisi oluşturulup çözülebilir kalanı bulunur. Aşağıda $Sp(2n, p)$ ($p \in \{4, 5, 6\}$)' nin maksimal alt gruplarının çözülebilir kalanları verilmiştir Burada yarı direkt çarpım şeklinde olan grupların $(G'_1[G_1, G_2])$ kısmı için G gösterimi kullanılmıştır. Ayrıca grupların genel gösterimlerinde Conway et al. (2003) baz alınmıştır.

Tablo 7: $Sp(8, p)$ nin maksimal alt gruplarına ait çözülebilir kalanlar

Sınıf	Maksimal Alt Grup	Çözülebilir Kalanlar		
		$p = 2$	$p = 3$	$p \geq 5$
C_1	$E_p^{1+6} : ((p-1) \times Sp(6, p))$	-	$G_{37} : (C_2.PSp(6, 3))$	$G_{p^7} : (C_2.PSp(6, p))$

C_1	$E_p^7: ((p-1) \times Sp(6, p))$	$G_2^7: Sp(6, 2)$	-	-
C_1	$E_p^{3+8}: (GL(2, p) \times Sp(4, p))$	$G_2^6: (G_2^5: A_6)$	$G_{3^6}: (G_{3^5}: (C_2 \cdot GO(5, 3)))$	$G_{3^6}: (G_{3^5}: (SL(2, p) \cdot GO(5, 3)))$
C_1	$E_p^{6+6}: (GL(3, p) \times Sp(2, p))$	$G_{2^9}: (G_{2^3}: L_3)$	$G_{2^9}: (G_{2^3}: L_3(3))$	$G_{2^9}: (G_{2^3}: L_3(p))$
C_1	$E_p^{10}: GL(4, p)$	$G_2^{10}: A_8$	$G_3^{10}: SL(4, 3)$	$G_p^{10}: SL(4, p)$
C_1	$Sp(6, p) \times Sp(2, p)$	$GO(7, 2)$	$C_2 \cdot PSp(6, 3)$	$(C_2 \cdot PSp(6, p)) \times SL(2, p)$
C_2	$Sp(2, p)^4: S_4$	-	()	$SL(2, p)^4$
C_2	$Sp(4, p)^2: S_2$	A_6^2	$(C_2 \cdot GO(5, 3))^2$	$C_2 \cdot GO(5, p)^2$
C_2	$GL(4, p) \cdot 2$	-	$SL(4, 3)$	$SL(4, p)$
C_3	$Sp(4, p^2): 2$	$GO(5, 2^2)$	$C_2 \cdot GO(5, 3^2)$	$C_2 \cdot GO(5, p^2)$
C_3	$GU(4, p) \cdot 2$	-	$C_4 \cdot PSU(4, 3)$	$C_2 \cdot PSU(4, 5)$ 5 için $C_4 \cdot PSU(4, p)$ $p \geq 7$ için
C_4	$(Sp(2, p) \circ GO^-(4, p)) \cdot 2$	-	A_6	$PSL(2, p^2) \times SL(2, p)$
C_6	$2_-^{1+6} \cdot SO_6^-(2)$	-	-	$C_2 \cdot (C_2^6 \cdot GO(5, 3))$ 7 için
C_6	$2_-^{1+6} \cdot \Omega_6^-(2)$	-	$E_2^7 \cdot GO(5, 3)$	$C_2 \cdot (C_2^6 \cdot GO(5, 3))$ 5 için
C_7	$(Sp(2, p) \circ Sp(2, p) \circ Sp(2, p)) \cdot 2^2 \cdot S_3$	-	-	$(SL(2, 5): A_5): A_5$ 5 için $(SL(2, 7): PSL(3, 2)): PSL(3, 2)$ $(SL(2, p): PSL(2, p)): PSL(2, p)$ $p \geq 11$ için
C_8	$SO^+(8, p)$	$\Omega^+(8, 2)$	-	-
C_8	$SO^-(8, p)$	$\Omega^-(8, 2)$	-	-
C_9	$2 \cdot L_2(7)$	-	-	$2 \cdot L_2(7) \cong SL(2, 7)$
C_9	$2 \cdot L_2(7) \cdot 2$	-	-	$SL(2, 7)$ 11 için

C_9	$2'A_6$	-	-	$2'A_6 \cong SL(2,9)$ 11 için
C_9	$2'A_6.2_2$	-	-	19 için th
C_9	$L_2(17)$	$L_2(17)$	-	-
C_9	$2'L_2(17)$	-	-	$SL(2,17)$ 13 için
C_9	S_{10}	A_{10}	-	-
C_9	$2'L_2(p)$	-	-	$SL(2,p)$ 11 için
C_9	$2'L_2(p^3).3$	-	$SL(2,3^3)$	$SL(2,p^3)$

Tablo 8: $Sp(10, p)$ nun maksimal alt gruplarına ait çözülebilir kalanlar

Sınıf	Maksimal Alt Grup	Çözülebilir Kalanlar		
		$p = 2$	$p = 3$	$p \geq 5$
C_1	$E_p^{1+8}: ((p-1) \times Sp(8, p))$	-	$G_{3^9}: (C_2.PSp(8,3))$	$G_{p^9}: (C_2.PSp(8, p))$
C_1	$E_p^9: ((p-1) \times Sp(8, p))$	$C_2^9: GO(8,2)$	-	-
C_1	$E_p^{3+12}: (GL(2, p) \times Sp(6, p))$	$G_{2^8}: (G_{2^7}: GO(7,2))$	$G_3^{15}: (SL(2,3) \times Sp(6,3))$	$G_p^{15}: (SL(2, p) \times Sp(6, p))$
C_1	$E_p^{6+12}: (GL(3, p) \times Sp(4, p))$	$G_2^{18}: (SL(3,2) \times A_6)$	$G_3^{18}: (SL(3,3) \times Sp(4,3))$	$G_p^{18}: (SL(3, p) \times Sp(4, p))$
C_1	$E_p^{10+8}: (GL(4, p) \times Sp(2, p))$	$G_{2^{14}}: (G_{2^4}: A_8)$	$G_3^{18}: SL(4,3)$	$G_p^{18}: (SL(4, p) \times Sp(2, p))$
C_1	$E_p^{15}: GL(5, p)$	$G_2^{15}: GL(5,2)$	$G_3^{15}: PSL(5,3)$	$G_p^{15}: PSL(5, p)$
C_1	$Sp(8, p) \times Sp(2, p)$	$GO(9,2)$	$Sp(8,3)$	$Sp(8, p) \times SL(2, p)$
C_1	$Sp(6, p) \times Sp(4, p)$	$GO(7,2) \times A_6$	$Sp(6,3) \times Sp(4,3)$	$Sp(6, p) \times Sp(4, p)$

C_2	$Sp(2, p)^5 : S_5$	-	$SL(2, 3)^5 \cdot C_2$	$G : A_5$
C_2	$GL(5, p) \cdot 2$	-	$PSL(5, 3)$	$PSL(5, p)$
C_3	$Sp(2, p^5) : 5$	$PSL(2, 2^5)$	$SL(2, 3^5)$	$SL(2, p^5)$
C_3	$GU(5, p) \cdot 2$	-	$PSU(5, 3)$	$PSU(5, p)$
C_4	$Sp(2, p) \circ GO(5, p)$	-	$GO(5, 3)$	$GO(5, p) \times SL(2, p)$
C_8	$SO^+(10, p)$	$\Omega^+(10, 2)$	-	-
C_8	$SO^-(10, p)$	$\Omega^-(10, 2)$	-	-
C_9	$2 \cdot A_6$	-	-	$SL(2, 9)$
C_9	$2 \cdot A_6 \cdot 2_2$	-	-	$SL(2, 9)$ 17 için
C_9	$2 \cdot L_2(11)$	-	$SL(2, 11)$	$SL(2, 11)$
C_9	$2 \cdot L_2(11) \cdot 2$	-	-	$SL(2, 11)$ 7 için
C_9	$2 \cdot L_2(11)$	-	-	$SL(2, 11)$ 11 için
C_9	$2 \cdot L_2(11)$	-	-	$SL(2, 11)$ 13 için
C_9	$2 \cdot L_2(11) \cdot 2$	-	-	$SL(2, 11)$ 23 için
C_9	$2 \cdot L_2(11) \cdot 2$	-	-	$SL(2, 11)$ 23 için
C_9	$2 \times U_5(2)$	-	$PSU(5, 2)$	$PSU(5, 2)$
C_9	$(2 \times U_5(2)) \cdot 2$	-	-	$PSU(5, 2)$ 7 için
C_9	$2 \cdot L_2(p)$	-	-	$SL(2, p)$ 11 için

Tablo 9: $Sp(12, p)$ nin maksimal alt gruplarına ait çözülebilir kalanlar

Sınıf	Maksimal Alt Grup	Çözülebilir Kalanlar		
		$p = 2$	$p = 3$	$p \geq 5$
C_1	$E_p^{1+10}: ((p-1) \times Sp(10, p))$	-	$G_{3^{11}}: (C_2 \cdot PSp(10, 3))$	$G_{p^{11}}: (C_2 \cdot PSp(10, p))$
C_1	$E_p^{11}: ((p-1) \times Sp(10, p))$	$G_2^{11}: Sp(10, 2)$	-	-
C_1	$E_p^{3+16}: (GL(2, p) \times Sp(8, p))$	$G_{2^{19}}: Sp(8, 2)$	$G_3^{19}: Sp(8, 3)$	$G_p^{19}: (SL(2, p) \times Sp(8, p))$
C_1	$E_p^{6+18}: (GL(3, p) \times Sp(6, p))$	$G_2^{24}: (SL(3, 2) \times Sp(6, 2))$	$G_3^{24}: (SL(3, 3) \times Sp(6, 3))$	$G_p^{24}: (SL(3, p) \times Sp(6, p))$
C_1	$E_p^{10+16}: (GL(4, p) \times Sp(4, p))$	$G_2^{26}: (SL(4, 2) \times A_6)$	$G_3^{26}: (SL(4, 3) \times Sp(4, 3))$	$G_p^{26}: (SL(4, p) \times Sp(4, p))$
C_1	$E_p^{15+10}: (GL(5, p) \times Sp(2, p))$	$G_2^{25}: GL(5, 2)$	$G_3^{35}: PSL(5, 3)$	$G_p^{25}: PSL(5, p)$
C_1	$E_p^{21}: GL(6, p)$	$G_2^{21}: GL(6, 2)$	$G_3^{21}: SL(6, 3)$	$G_p^{21}: PGL(6, p)$
C_1	$Sp(10, p) \times Sp(2, p)$	$GO(11, 2)$	$Sp(10, 3)$	$Sp(10, p) \times Sp(2, p)$
C_1	$Sp(8, p) \times Sp(4, p)$	$GO(9, 2) \times A_6$	$Sp(8, 3) \times Sp(4, 3)$	$Sp(8, p) \times Sp(4, p)$
C_2	$Sp(2, p)^6: S_6$	-	$G: A_6$	$G: A_6$
C_2	$Sp(4, p)^3: S_3$	A_6^3	$Sp(4, 3)^3$	$Sp(4, p)^3$
C_2	$Sp(6, p)^2: S_2$	$GO(7, 2)^2$	$Sp(6, 3)^2$	$Sp(6, p)^2$
C_2	$GL(6, p).2$	-	$PSL(6, 3).2$	$PSL(6, p).2$
C_3	$Sp(6, p^2): 2$	$Sp(6, 2^2)$	$Sp(6, 3^2)$	$Sp(6, p^2)$
C_3	$Sp(4, p^3): 3$	$Sp(4, 2^3)$	$Sp(4, 3^3)$	$Sp(4, p^3)$
C_3	$GU(6, p).2$	-	$PSU(6, 3).2$	$PSU(6, p).2$

C_4	$(Sp(2, p) \circ GO^+(6, p)).2$	-		
C_4	$(Sp(2, p) \circ GO^-(6, p)).2$	-		
C_4	$Sp(4, p) \circ GO(3, p)$	-	-	
C_8	$SO^+(12, p)$	$\Omega^+(12, 2)$	-	-
C_8	$SO^-(12, p)$	$\Omega^-(12, 2)$	-	-
C_9	$2 \cdot L(2, 11)$	-	-	$SL(2, 11)$
C_9	$2 \cdot L(2, 11).2$	-	-	$SL(2, 11)$
C_9	$2 \cdot L(2, 13)$	-	-	$SL(2, 13)$
C_9	$2 \cdot L(2, 13).2$	-	-	$SL(2, 13)$
C_9	$2 \cdot L(2, 25)$	-	-	$SL(2, 25)$
C_9	$L(2, 25).2_2$	$PSL(2, 25)$	-	-
C_9	$2 \cdot S(4, 5)$	-	-	$2 \cdot S(4, 5)$
C_9	$2 \cdot G(2, 4)$	-	-	$2 \cdot G(2, 4)$
C_9	$2 \cdot G(2, 4).2$	-	-	$2 \cdot G(2, 4)$
C_9	S_{14}	A_{14}	-	-
C_9	$2 \cdot Suz$	-	$2 \cdot Suz$	-
C_9	$2 \cdot L(2, p)$	-	-	$SL(2, p)$

Yukarıda yer alan çözülebilir kalanların mükemmel alt grupları, 12th Gen Intel® Core™ i7-12700H 2.70 GHz işlemci ve 32 gb ram özellikli bilgisayar ile Intel® Core™ i7-10870 2.20

GHz İşlemci 64 gb ram özelliklerine sahip bilgisayar ve Tübitak ULAKBİM bünyesinde faaliyet gösteren TRUBA sisteminde yer alan Orkinos sunucusu yardımıyla hesaplanmıştır.

4.3. Analizler

4.3.1. Doğrudan Hesaplamalar

Çözülebilir gruplar için analizler $Sp(2n, p)$ nin türev uzunluğu yardımı ile Teorem 4.1.1 de verilmiştir.

Mükemmel gruplar için analizler ise şu şekilde yapılmıştır:

Analizlerimiz BlindDescent algoritmasının 11. satırında üretilen doğru x elemanını baz almaktadır. Bunun için ilgili gruplarda böyle bir elemanın bulunma ihtimaline dayanarak aşağıdaki bilgiler ışığında analizler yapılmıştır.

G abelyen olmayan sonlu bir grup olsun. Herhangi bir A kümesi için A daki eleman sayısını $|A|$ ile gösterelim.

$$\text{Comm}(G) = \{(x, y) \in G \times G: xy = yx\}$$

olmak üzere

$$\text{Pr}(G) = \frac{|\text{Comm}(G)|}{|G|^2}$$

olarak tanımlansın.

Burada $\text{Pr}(G)$ sayısı, grup elemanlarının bütün sıralı ikililerinin kümesinin örnek uzay ve $\text{Comm}(G)$ tarafından sayılan kümenin de rastgele seçilen bir çiftin değişmeli olma olayı olarak alındığı G grubundaki iki elemanın değişmeli olma olasılığıdır.

Ayrıca, k sayısı G deki eşlenik sınıflarının sayısı olmak üzere Erdős and Turan (1968) tarafından

$$|\text{Comm}(G)| = k \cdot |G|$$

olduğu ispatlanmıştır.

Dolayısıyla, bizim çalışmamızda birim eleman hariç tutulduğundan aşağıdaki yardımcı teorem yardımıyla değişmeli olan elemanların oranları daha etkili bir şekilde bulunabilmektedir.

Yardımcı Teorem 4.3.1. G bir grup ve k da G deki eşlenik sınıflarının sayısı olsun. Bu durumda,

$$\text{Pr}^*(G) = \frac{(k \cdot |G| - (2 \cdot |G| - 1))}{|G|^2}$$

dir. Burada, $\text{Pr}^*(G)$ ile G den birim eleman hariç diğer elemanların değişmeli olma olasılıkları gösterilmiştir.

Yardımcı Teorem 4.3.2. H bir sonlu grup ve A ise H nın elementer abelyen normal r (r asal) alt grubu olsun. Bu kabul ile aşağıdaki koşullar sağlanır:

- i. $r > 2$ olsun ve $c \in H$ in da A üzerinde -Id indükleyen sabit bir eleman olduğu kabul edilsin. b ise cA yan kümesinin herhangi bir elemanı olsun. Bu durumda, düzgün dağılımlı rastgele $h \in H$ elemanı ve herhangi bir k tamsayısı için

$$\text{Prob}(h^k = b | h^k \in cA) = 1/|A|$$

dır.

- ii. $b \in H$ elemanı A üzerinde aşık olmaya sahip sabit bir eleman olsun. Bu durumda, A nın H daki sabit bir C yan kümesi ve düzgün dağılımlı rastgele $h \in C$ için

$$\text{Prob}([b, h] \neq 1 | [b, h] \in A) \geq 1 - 1/r$$

dir (Brooksbank *et al.* 2006).

Analizlere başlamadan önce daha önceden GAP formatında oluşturulmuş olan GAP klasörü (Github) içinde verilen ilgili gruplara ve Yardımcı Teorem 4.3.1 in kodu olan stepNumber fonksiyonuna ulaşabilmek için aşağıdaki başlangıç yapılır:

```
gap> gapPath:="C:/Users/kullanıcı/GAP";;
gap> Read("C:/Users/kullanıcı/GAP/All.txt");;
```

Yukarıda verilen Yardımcı Teorem 4.3.1 ve Brooksbank et al. (2006) da yer alan Yardımcı Teorem 4.3.2 den faydalanarak aşağıdaki analizler örnek olarak yapılmıştır.

Aşağıda $Sp(6,3)$ ün maksimal alt gruplarından $GU(3,3).2$ nin çözülebilir kalanı olan $SU(3,3)$ için değişmeli olan elemanların oranı elde edilmiştir:



GAP 4.12.1 of 2022-10-20

<https://www.gap-system.org>

Architecture: x86_64-pc-cygwin-default64-kv8

Configuration: gmp 6.2.1, GASMAN, readline

Loading the library and packages ...

Packages: Aclib 1.3.2, Alnuth 3.2.1, AtlasRep 2.1.6, AutoDoc 2022.10.20, AutPGrp 1.11, Browse 1.8.18, CaratInterface 2.3.4, CRISP 1.4.5, Cryst 4.1.25, CrystCat 1.1.10, CTblLib 1.3.4, curlInterface 2.3.1, FactInt 1.6.3, FGA 1.4.0, Forms 1.2.9, GAPDoc 1.6.6, genss 1.6.8, IO 4.8.0, IRREDSOL 1.4.3, LAGUNA 3.9.5, orb 4.9.0, Polenta 1.3.10, Polycyclic 2.16, PrimGrp 3.4.2, RadiRoot 2.9, recog 1.4.2, ResClasses 4.7.3, SmallGrp 1.5, Sophus 1.27, SpinSym 1.5.2, TomLib 1.2.9, TransGrp 3.6.3, utils 0.77

Try '??help' for help. See also '?copyright', '?cite' and '?authors'

gap> gapPath:="C:/Users/Ahmet/GAP";

"C:/Users/Ahmet/GAP"

gap> Read("C:/Users/Ahmet/GAP/All.txt");

gap>

gap> G:=sympGrps[6,3].maxSubGrpsByClass[3][2].self;

<matrix group with 3 generators>

gap> ord:=sympGrps[6,3].maxSubGrpsByClass[3][2].order;

48384

gap> Order(GU(3,3))*2;

48384

gap> sol:=sympGrps[6,3].maxSubGrpsByClass[3][2].solRsd.self;

<matrix group with 5 generators>

gap> ordsol:=sympGrps[6,3].maxSubGrpsByClass[3][2].solRsd.order;

6048

gap> Order(SU(3,3));

6048

gap> StepNumber(sol);

504.

gap>

Şekil 4: $Sp(6,3)$ için örnek hesaplama

Bu mükemmel alt grup için analizi içeren teorem aşağıdaki gibidir:

Teorem 4.3.3. Eğer $\bar{G} = G/(R \cap G) \cong SU(3,3)$ ise BlindDescent $750\log(1/\delta)$ tane y elemanın işlenmesini takiben, $1 - \delta$ dan yüksek olasılıkla geçerli bir x elemanı üretilir.

İspat: $r = 3$ olup Yardımcı Teorem 4.3.1 yardımıyla $Prob([x, y] \in R \cap G) \geq 1/500$ olup Yardımcı Teorem 4.3.2 den $Prob([x, y] \notin Z(R \cap G) | [x, y] \in R \cap G) \geq 2/3$ olduğundan,

$$Prob([x, y] \notin Z(R \cap G) \wedge [x, y] \in R \cap G) \geq 1/750$$

bulunur.

Benzer şekilde $Sp(6,3)$ ün maksimal alt gruplarından $2 \cdot L(2,13)$ ün çözülebilir kalanı olan $Sp(2,13)$ için aşağıdaki ifade elde edilir:

Teorem 4.3.4. Eğer $\bar{G} = G/(R \cap G) \cong Sp(2,13)$ ise BlindDescent $225 \log(1/\delta)$ tane y elemanın işlenmesini takiben, $1 - \delta$ dan yüksek olasılıkla geçerli bir x elemanı üretilir.

İspat: $r = 3$ olup Yardımcı Teorem 4.3.1 yardımıyla $Prob([x, y] \in R \cap G) \geq 1/150$ olup Yardımcı Teorem 4.3.2'den $Prob([x, y] \notin Z(R \cap G) | [x, y] \in R \cap G) \geq 2/3$ olduğundan,

$$Prob([x, y] \notin Z(R \cap G) \wedge [x, y] \in R \cap G) \geq 1/225$$

bulunur.

Aşağıda $Sp(8,2)$ nin maksimal alt gruplarından $SO^+(8,2)$ nin çözülebilir kalanı olan $\Omega^+(8,2)$ nin mükemmel alt gruplarından $PSU(4,2)$ için değişmeli olan elemanların oranı

```

GAP
GAP 4.12.1 of 2022-10-20
https://www.gap-system.org
Architecture: x86_64-pc-cygwin-default64-kv8
Configuration: gmp 6.2.1, GASMAN, readline
Loading the library and packages ...
Packages: Aclib 1.3.2, Alnuth 3.2.1, AtlasRep 2.1.6, AutoDoc 2022.10.20, AutPGrp 1.11, Browse 1.8.18,
CaratInterface 2.3.4, CRISP 1.4.5, Cryst 4.1.25, CrystCat 1.1.10, CTblLib 1.3.4, curlInterface 2.3.1,
FactInt 1.6.3, FGA 1.4.0, Forms 1.2.9, GAPDoc 1.6.6, genss 1.6.8, IO 4.8.0, IRREDSOL 1.4.3, LAGUNA 3.9.5,
orb 4.9.0, Polenta 1.3.10, Polycyclic 2.16, PrimGrp 3.4.2, RadiRoot 2.9, recog 1.4.2, ResClasses 4.7.3,
SmallGrp 1.5, Sophus 1.27, SpinSym 1.5.2, TomLib 1.2.9, TransGrp 3.6.3, utils 0.77
Try '?help' for help. See also '?copyright', '?cite' and '?authors'
gap> gapPath:="C:/Users/Ahmet/GAP";
"C:/Users/Ahmet/GAP"
gap> Read("C:/Users/Ahmet/GAP/All.txt");
gap> G:=sympGrps[8,2].maxSubGrpsByClass[8][1].solRsd.perSubGrps[79].self;
<matrix group with 2 generators>
gap> sympGrps[8,2].maxSubGrpsByClass[8][1].solRsd.perSubGrps[79].order;
25920
gap> IsomorphismGroups(G,PSU(4,2));
CompositionMapping( [ (2,124)(3,156)(4,225)(5,158)(6,231)(8,126)(9,236)(10,145)(11,113)(13,119)(15,238)(16,151)(17,
244)(18,137)(19,105)(21,111)(23,246)(24,143)(26,100)(27,132)(28,249)(29,134)(30,255)(32,102)(34,92)(35,188)(36,
193)(37,190)(38,199)(40,94)(41,204)(42,177)(43,81)(45,87)(47,206)(48,183)(49,212)(50,169)(51,73)(53,79)(55,
214)(56,175)(58,68)(59,164)(60,217)(61,166)(62,223)(64,70)(65,218)(66,163)(71,224)(72,165)(75,170)(76,211)(77,
176)(78,213)(83,178)(84,203)(85,184)(86,205)(89,194)(90,187)(95,200)(96,189)(97,250)(98,131)(103,256)(104,
133)(107,138)(108,243)(109,144)(110,245)(115,146)(116,235)(117,152)(118,237)(121,226)(122,155)(127,232)(128,
157)(129,251)(135,253)(140,242)(142,248)(148,234)(150,240)(153,227)(159,229)(161,219)(167,221)(172,210)(174,
216)(180,202)(182,208)(185,195)(191,197), (2,16,161,184,125)(3,200,22,13,105)(4,201,182,188,21)(5,208,179,189,
20)(6,193,19,12,112)(7,9,168,177,124)(10,169,17,205,123)(11,97,166,120,111)(14,104,163,113,106)(15,176,24,204,
126)(18,196,219,191,213)(23,197,222,186,212)(25,108,203,115,175)(26,101,107,198,211)(27,173,224,127,199)(28,164,
128,202,187)(29,165,121,207,190)(30,172,217,122,194)(31,100,110,195,214)(32,109,206,118,170)(33,151,230,69,
253)(34,154,70,244,129)(35,82,241,73,149)(36,95,81,256,233)(37,90,88,249,240)(38,87,248,80,148)(39,159,67,245,
136)(40,146,227,68,252)(41,50,86,64,251)(42,63,246,137,135)(43,247,65,52,147)(44,250,225,133,239)(45,255,232,132,
234)(46,242,72,53,150)(47,58,243,144,130)(48,55,83,57,254)(49,91,160,78,85)(51,158,139,66,61)(54,155,142,71,
60)(56,94,153,75,84)( [ ... ] ) -> [ (1,52)(2,49)(4,42)(5,39)(6,69)(7,83)(9,34)(10,77)(11,54)(12,31)(15,28)(16,
64)(17,72)(18,25)(20,78)(21,59)(22,80)(23,60)(26,63)(27,70)(32,75)(33,57)(36,66)(37,85)(40,47)(41,45)(44,46)(50,
51)(56,74)(61,81)(62,71)(67,84), (1,68,80,43,52)(2,35,27,23,31)(3,8,11,63,77)(4,53,69,10,54)(5,82,38,83,13)(6,81,
30,60,42)(7,39,9,26,49)(12,61,71,48,34)(14,17,25,20,72)(15,75,58,33,64)(16,46,51,66,28)(18,44,36,78,19)(21,32,56,
57,59)(22,70,76,55,62)(24,45,84,79,73)(29,74,65,47,85)(37,41,50,67,40) ], <action isomorphism> )
gap> StepNumber(G);
1440.
gap> IsomorphismGroups(Omega(1,8,2),sympGrps[8,2].maxSubGrpsByClass[8][1].solRsd.self);
CompositionMapping( [ (2,125)(3,166)(4,218)(5,223)(6,163)(7,124)(9,176)(10,212)(12,119)(13,114)(15,213)(16,169)(17,
184)(18,204)(20,111)(21,106)(23,205)(24,177)(26,101)(27,190)(28,194)(29,199)(30,187)(31,100)(33,251)(34,135)(35,
96)(38,89)(39,130)(40,254)(41,86)(43,241)(44,141)(45,140)(46,248)(48,83)(49,78)(51,233)(52,149)(53,148)(54,
240)(56,75)(57,227)(58,159)(59,72)(62,65)(63,154)(64,230)(67,153)(68,229)(69,228)(70,160)(73,147)(74,239)(79,
234)(80,150)(81,139)(82,247)(87,242)(88,142)(91,129)(92,253)(93,252)(94,136)(97,200)(98,188)(103,189)(104,
193)(107,206)(108,178)(109,183)(110,203)(115,214)(116,170)(117,175)(118,211)(121,224)(122,164)(127,165)(128,
217)(131,256)(134,249)(137,246)(144,243)(145,238)(152,235)(155,232)(158,225)(162,221)(167,220)(172,215)(173,
210)(180,207)(181,202)(186,197)(191,196), (2,22,184,78,112,160,149,169,212,239,129,11,42,205,113)(3,244,238,103,
81)(4,231,91,44,64,158,104,70,182,191,131,250,197,171,33)(5,168,73,222,97)(6,179,256,145,16,156,52,225,15,143,133,
174,98,18,17)(7,85,166,188,49)(8,66,19,247,96,154,193,14,105,223,135,95,141,120,65)(9,219,34,23,82,24,69,161,10,
208,151,92,63,137,209)(12,61,124,62,111,139,36,230,189,114,21,163,251,35,241)(13,126,106,204,50,20,228,233,213,
176,147,253,119,86,177)(25,224,148,234,194)(26,203,37,165,175,136,76,60,59,48,153,214,187,38,178)(27,45,127,144,
146)(28,58,202,195,255,134,185,215,93,128,155,39,88,68,226)(29,121,220,53,162)(30,110,109,122,207,132,237,116,232,
80,157,115,243,249,210)(31,140,55,83,242)(32,159,130)(40,67,245,173,117,167,94,107,46,108,57,221,118,180,
235)( [ ... ] ) -> [ <an immutable 8x8 matrix over GF2>, <an immutable 8x8 matrix over GF2> ],
<action isomorphism> )
gap>

```

Şekil 5: $Sp(8,2)$ için örnek hesaplama

Teorem 4.3.5. Eğer $\bar{G} = G/(R \cap G) \cong PSU(4,2)$ ise BlindDescent $2800\log(1/\delta)$ tane y elemanın işlenmesini takiben, $1 - \delta$ dan yüksek olasılıkla geçerli bir x elemanı üretilir.

İspat: $r = 2$ olup Yardımcı Teorem 4.3.1 yardımıyla $Prob([x, y] \in R \cap G) \geq 1/1400$ olup Yardımcı Teorem 4.3.2’den $Prob([x, y] \notin Z(R \cap G) | [x, y] \in R \cap G) \geq 1/2$ olduğundan,

$$Prob([x, y] \notin Z(R \cap G) \wedge [x, y] \in R \cap G) \geq 1/2800$$

bulunur.

$Sp(10,3)$ ün maksimal mükemmel alt grubu olan $2'L(2,11)$ için değişmeli olan elemanların oranı şu şekildedir:



```

GAP 4.12.1 of 2022-10-20
https://www.gap-system.org
Architecture: x86_64-pc-cygwin-default64-kv8
Configuration: gmp 6.2.1, GASMAN, readline
Loading the library and packages ...
Packages: AClib 1.3.2, Alnuth 3.2.1, AtlasRep 2.1.6, AutoDoc 2022.10.20, AutPGrp 1.11, Browse 1.8.18,
CaratInterface 2.3.4, CRISP 1.4.5, Cryst 4.1.25, CrystCat 1.1.10, CTblLib 1.3.4, curlInterface 2.3.1,
FactInt 1.6.3, FGA 1.4.0, Forms 1.2.9, GAPDoc 1.6.6, genss 1.6.8, IO 4.8.0, IRREDSOL 1.4.3, LAGUNA 3.9.5,
orb 4.9.0, Polenta 1.3.10, Polycyclic 2.16, PrimGrp 3.4.2, RadiRoot 2.9, recog 1.4.2, ResClasses 4.7.3,
SmallGrp 1.5, Sophus 1.27, SpinSym 1.5.2, TomLib 1.2.9, TransGrp 3.6.3, utils 0.77
Try '??help' for help. See also '?copyright', '?cite' and '?authors'
gap> gapPath:="C:/Users/Ahmet/GAP";
"C:/Users/Ahmet/GAP"
gap> Read("C:/Users/Ahmet/GAP/All.txt");
gap> G:=sympGrps[10,3].maxSubGrpsByClass[9][1].self;
<matrix group with 3 generators>
gap> sympGrps[10,3].maxSubGrpsByClass[9][1].order;
1320
gap> StructureDescription(sympGrps[10,3].maxSubGrpsByClass[9][1].self);
"SL(2,11)"
gap> per:=sympGrps[10,3].maxSubGrpsByClass[9][1].solRsd.perSubGrps[4].self;
<matrix group with 3 generators>
gap> IsomorphismGroups(SL(2,11),per);
CompositionMapping( [ (2,67,7,12)(3,78,8,23)(4,89,9,34)(5,100,10,45)(6,111,11,56)(13,68,73,18)(14,79,74,29)(15,90,75,
40)(16,101,76,51)(17,112,77,62)(19,24,69,84)(20,35,70,95)(21,46,71,106)(22,57,72,117)(25,80,85,30)(26,91,86,
41)(27,102,87,52)(28,113,88,63)(31,36,81,96)(32,47,82,107)(33,58,83,118)(37,92,97,42)(38,103,98,53)(39,114,99,
64)(43,48,93,108)(44,59,94,119)(49,104,109,54)(50,115,110,65)(55,60,105,120)(61,116,121,66),
(2,67,18)(3,78,30)(4,89,42)(5,100,54)(6,111,66)(7,12,68)(8,23,80)(9,34,92)(10,45,104)(11,56,116)(13,79,19)(14,46,
27)(15,112,44)(16,24,47)(17,57,61)(20,101,98)(21,90,108)(22,35,114)(25,91,31)(26,58,39)(28,36,59)(29,69,73)(32,
113,110)(33,102,120)(37,103,43)(38,70,51)(40,48,71)(41,81,85)(49,115,55)(50,82,63)(52,60,83)(53,93,97)(62,94,
75)(64,72,95)(65,105,109)(74,106,87)(76,84,107)(77,117,121)(86,118,99)(88,96,119) ] ->
[ < immutable compressed matrix 10x10 over GF(3) >, < immutable compressed matrix 10x10 over GF(3) > ],
<action isomorphism> )
gap> StepNumber(per);
102.
gap>

```

Şekil 6: $Sp(10,3)$ için örnek hesaplama

Teorem 4.3.6: Eğer $\bar{G} = G/(R \cap G) \cong 2 \cdot L(2,11)$ ise BlindDescent $150 \log(1/\delta)$ tane y elemanın işlenmesini takiben, $1 - \delta$ dan yüksek olasılıkla geçerli bir x elemanı üretilir.

İspat: $r = 3$ olup Yardımcı Teorem 4.3.1 yardımıyla $Prob([x, y] \in R \cap G) \geq 1/100$ olup Yardımcı Teorem 4.3.2 den $Prob([x, y] \notin Z(R \cap G) | [x, y] \in R \cap G) \geq 2/3$ olduğundan,

$$Prob([x, y] \notin Z(R \cap G) \wedge [x, y] \in R \cap G) \geq 1/150$$

bulunur.

Benzer şekilde $Sp(10,3)$ ün maksimal alt grubu $2 \times U(5,2)$ nin mükemmel alt grubu $PSU(5,2)$ için aşağıdaki teorem elde edilir.

Teorem 4.3.7: Eğer $\bar{G} = G/(R \cap G) \cong PSU(5,2)$ ise BlindDescent $456180 \log(1/\delta)$ tane y elemanın işlenmesini takiben, $1 - \delta$ dan yüksek olasılıkla geçerli bir x elemanı üretilir.

İspat: $r = 3$ olup Yardımcı Teorem 4.3.1 yardımıyla $Prob([x, y] \in R \cap G) \geq 1/304120$ olup Yardımcı Teorem 4.3.2'den $Prob([x, y] \notin Z(R \cap G) | [x, y] \in R \cap G) \geq 2/3$ olduğundan,

$$Prob([x, y] \notin Z(R \cap G) \wedge [x, y] \in R \cap G) \geq 1/456180$$

bulunur.

$Sp(12,2)$ nin maksimal alt grubu $L(2,25) \cdot 2_2$ in çözülebilir kalanı $PSL(2,25)$ için değişmeli olan elemanların oranı aşağıda verilmiştir:



```

GAP 4.12.1 of 2022-10-20
https://www.gap-system.org
Architecture: x86_64-pc-cygwin-default64-kv8
Configuration: gmp 6.2.1, GASMAN, readline
Loading the library and packages ...
Packages: Aclib 1.3.2, Alnuth 3.2.1, AtlasRep 2.1.6, AutoDoc 2022.10.20, AutPGrp 1.11, Browse 1.8.18,
CaratInterface 2.3.4, CRISP 1.4.5, Cryst 4.1.25, CrystCat 1.1.10, CTblLib 1.3.4, curlInterface 2.3.1,
FactInt 1.6.3, FGA 1.4.0, Forms 1.2.9, GAPDoc 1.6.6, genss 1.6.8, IO 4.8.0, IRREDSOL 1.4.3, LAGUNA 3.9.5,
orb 4.9.0, Polenta 1.3.10, Polycyclic 2.16, PrimGrp 3.4.2, RadiRoot 2.9, recog 1.4.2, ResClasses 4.7.3,
SmallGrp 1.5, Sophus 1.27, Spinsym 1.5.2, TomLib 1.2.9, TransGrp 3.6.3, utils 0.77
Try '??help' for help. See also '?copyright', '?cite' and '?authors'
gap> gapPath:="C:/Users/Ahmet/GAP";
"C:/Users/Ahmet/GAP"
gap> Read("C:/Users/Ahmet/GAP/All.txt");
gap> G:=sympGrps[12,2].maxSubGrpsByClass[9][1].self;
<matrix group with 3 generators>
gap> sol:=sympGrps[12,2].maxSubGrpsByClass[9][1].solRsd.self;
<matrix group with 4 generators>
gap> IsomorphismGroups(sol,PSL(2,25));
CompositionMapping( [ (1,266)(2,324)(3,179)(4,28)(5,279)(6,60)(7,262)(8,175)(9,156)(10,316)(11,92)(12,308)(13,166)(14,
249)(15,232)(16,182)(17,191)(18,226)(19,171)(20,127)(21,304)(22,48)(23,306)(24,124)(25,180)(26,119)(27,235)(29,
74)(30,40)(31,303)(32,260)(33,234)(34,186)(35,138)(36,130)(37,76)(41,227)(42,132)(43,237)(44,99)(45,273)(46,
245)(47,300)(49,256)(50,313)(51,122)(52,320)(53,278)(54,108)(55,151)(56,301)(57,157)(58,71)(61,125)(62,295)(63,
69)(64,252)(65,189)(66,152)(67,135)(68,78)(72,239)(73,297)(75,82)(77,238)(79,250)(80,284)(81,95)(84,145)(85,
241)(86,193)(87,109)(88,153)(89,136)(90,168)(91,158)(93,106)(94,192)(96,251)(97,274)(98,101)(100,148)(102,
198)(103,222)(104,325)(105,242)(107,149)(110,215)(111,288)(112,281)(113,317)(114,146)(115,176)(116,293)(117,
292)(118,123)(121,319)(128,142)(129,150)(131,267)( [ ... ] ), (1,183,114,90,256,295,133,271,132,108,266,177,303)(2,
128,98,210,190,219,63,67,294,105,320,149,268)(3,234,221,318,158,289,81,225,161,168,109,230,178)(4,296,173,250,113,
233,222,137,147,68,20,175,193)(5,241,197,18,23,35,44,199,285,195,87,314,245)(6,223,237,13,248,187,207,310,215,129,
162,93,243)(7,84,172,71,50,186,61,138,29,143,214,235,135)(8,300,91,19,51,33,43,277,9,257,185,321,272)(10,66,85,31,
60,165,40,78,151,73,122,319,58)(11,25,159,287,308,293,278,298,140,291,218,118,155)(12,299,75,317,163,325,322,164,
307,107,167,125,246)(14,59,316,229,42,236,69,242,202,146,276,141,224)(15,176,145,283,41,94,70,305,323,65,117,281,
104)(16,304,196,205,38,217,131,204,275,37,286,249,27)(17,208,53,284,103,72,213,30,282,209,265,247,279)(21,261,239,
106,227,232,290,253,156,228,260,49,270)( [ ... ] ) ->
[ (1,13)(2,16)(3,15)(5,23)(6,11)(7,18)(8,9)(10,24)(12,26)(14,22)(19,25)(20,21), (1,4,18,20,15,7,5,21,6,24,22,13,25)(2,
26,17,8,3,9,10,14,23,16,11,12,19) ], <action isomorphism> )
gap> StepNumber(sol);
600.
gap>

```

Şekil 7: $Sp(12,2)$ için örnek hesaplama

Teorem 4.3.8: Eğer $\bar{G} = G/(R \cap G) \cong PSL(2,25)$ ise BlindDescent $1200\log(1/\delta)$ tane y elemanın işlenmesini takiben, $1 - \delta$ dan yüksek olasılıkla geçerli bir x elemanı üretilir.

İspat: $r = 2$ olup Yardımcı Teorem 4.3.1 yardımıyla $Prob([x, y] \in R \cap G) \geq 1/600$ olup Yardımcı Teorem 4.3.2'den $Prob([x, y] \notin Z(R \cap G) | [x, y] \in R \cap G) \geq 1/2$ olduğundan,

$$Prob([x, y] \notin Z(R \cap G) \wedge [x, y] \in R \cap G) \geq 1/1200$$

bulunur.

4.3.2. İnvölüsyon Hesaplamaları

Bir grup için involüsyon mertebesi 2 olan ve kendisiyle çarpıldığında birimi veren birimden farklı olan elemandır. Yani bir G grubu için $g \in G$ verildiğinde $g^2 = e$ ve $g \neq e$ olması durumudur.

İnvölüsyonlarla ilgili bazı teoremler aşağıda verilmiştir.

Teorem 4.3.2.1: G grubunun bir g elemanının involüsyon olması için gerek ve yeter koşul $g = g^{-1}$ koşulunun sağlanmasıdır.

Teorem 4.3.2.2: G grubunun bir a elemanı involüsyon ise her $g \in G$ için gag^{-1} de bir involüsyon olur.

Teorem 4.3.2.3: Sonlu bir G grubunun mertebesi tek ise G grubunun hiç involüsyonu yoktur.

Şimdi $Sp(2n, q)$ simplektik grubunun bazı maksimal alt gruplarının, merkez elemanlarının ve involüsyonlarının olduğu tabloyu verelim.

Tablo10: $Sp(2n, r)$ grubundaki involüsyonlar ve merkezdeki durumları

$Sp(2n, r)$	Maksimal Alt Grubu	Merkezdeki Eleman
$Sp(2, 2)$	$E_2: 1$	—
	$2:A_5$	I_2
$Sp(2, 3)$	$E_3: 2$	$2I_2$
	Q_8	$2I_2$
$Sp(2, 5)$	$2:A_4$	$4I_2$
	$E_5: 4$	$4I_2$

	$Q_{2(5+1)}$	$4I_2$
$Sp(2, 7)$	"C2.S4=SL(2,3).C2"	$6I_2$
	"C2.S4=SL(2,3).C2"	$6I_2$
	$E_7: 6$	$6I_2$
$Sp(2, 11)$	"C3 : Q8"	$10I_2$
	"C3 : Q8"	$10I_2$
	$E_{11}: 10$	$10I_2$
	$Q_{2(11+1)}$	$10I_2$
$Sp(2, 13)$	$E_{13}: 12$	$12I_2$
	$Q_{2(13+1)}$	$12I_2$
	$Q_{2(13-1)}$	$12I_2$
	$2A_4$	$12I_2$
$Sp(2, 17)$	$E_{17}: 16$	$16I_2$
	"C2.S4=SL(2,3).C2"	$16I_2$
	"C2.S4=SL(2,3).C2"	$16I_2$
	$Q_{2(17+1)}$	$16I_2$
	$Q_{2(17-1)}$	$16I_2$
	$E_{19}: 18$	$18I_2$
	$SL(2,5)$	$18I_2$

$Sp(2, 19)$	$SL(2, 5)$	$18I_2$
	$Q_{2(19+1)}$	$18I_2$
	$Q_{2(19-1)}$	$18I_2$
$Sp(4, 2)$	A_6	—
	S_5	—
	S_5	—
	"(S3 x S3) : C2"	—
	"C2 x S4"	$\left\{ \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \right\}$
	"C2 x S4"	$\left\{ \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \right\}$
$Sp(4, 3)$	"C2 . ((C2 x C2 x C2 x C2) : A5)"	$2I_4$
	"SL(2,9) : C2"	$2I_4$
	"(((C3 x C3 x C3) : Q8) : C3) : C2"	$2I_4$
	"C2 x (((C3 x C3) : C3) : Q8) : C3)"	$2I_4$
	"(((Q8 x Q8) : C3) : C2) : C3"	$2I_4$
	"(C5 x C5 x C5) : GL(2,5)"	$4I_4$
	"((C5 x C5) : C5) : (C4 x SL(2,5))"	$4I_4$

$Sp(4, 5)$	"SL(2,5) : C2"	$4I_4$
	"(SL(2,5) x SL(2,5)) : C2"	$4I_4$
	"C2 . ((C2 x C2 x C2 x C2) : A5)"	$4I_4$
	"C3 : ((C2 . S5 = SL(2,5) . C2) : C2)"	$4I_4$
	"((C2 . S5 = SL(2,5) . C2) : C2) : C2"	$4I_4$
	"((C2 . S5 = SL(2,5) . C2) : C2) : C2"	$4I_4$
$Sp(6, 2)$	$E_2^5 : (1 \times Sp_4(2))$	—
	$E_2^{3+4} : (GL_2(2) \times Sp_2(2))$	—
	$E_2^6 : GL_3(2)$	$\left\{ \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \right\}$
	$Sp_2(2) \times Sp_4(2)$	—
	$Sp_2(2^3) : 3$	—
	$SO_6^+(2)$	$\left\{ \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \right\}$
	$SO_6^-(2)$	—
	$U_3(3) : 2$	—

Yukarıdaki bilgilerin sonucunda aşağıdaki önerme elde edilir:

Önerme 4.4.1: r asal olmak üzere $GL(n, r)$ genel lineer grubunda;

$$A = \begin{bmatrix} r-1 & 0 & \cdots & 0 \\ 0 & r-1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & r-1 \end{bmatrix} \text{ matrisi bir involüsyondur ve aynı zamanda merkezin}$$

elemanıdır.

$$\begin{aligned} \text{İspat: } & \begin{bmatrix} r-1 & 0 & \cdots & 0 \\ 0 & r-1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & r-1 \end{bmatrix} \cdot \begin{bmatrix} r-1 & 0 & \cdots & 0 \\ 0 & r-1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & r-1 \end{bmatrix} \\ &= \begin{bmatrix} (r-1)^2 & 0 & \cdots & 0 \\ 0 & (r-1)^2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & (r-1)^2 \end{bmatrix} \end{aligned}$$

olup burada $(r-1)^2 = 1$ olduğundan A matrisi bir involüsyondur. Ayrıca,

$A = (a_{ij}) \in GL(n, r)$ olmak üzere;

$$\begin{aligned} & \begin{bmatrix} r-1 & 0 & \cdots & 0 \\ 0 & r-1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & r-1 \end{bmatrix} \cdot \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{21} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n1} & \cdots & a_{nn} \end{bmatrix} = \\ & \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{21} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n1} & \cdots & a_{nn} \end{bmatrix} \cdot \begin{bmatrix} r-1 & 0 & \cdots & 0 \\ 0 & r-1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & r-1 \end{bmatrix} \end{aligned}$$

dir. Gerçekten;

$$\begin{aligned} & \begin{bmatrix} r-1 & 0 & \cdots & 0 \\ 0 & r-1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & r-1 \end{bmatrix} \cdot \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{21} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n1} & \cdots & a_{nn} \end{bmatrix} = \\ & \begin{bmatrix} (r-1)a_{11} & (r-1)a_{12} & \cdots & (r-1)a_{1n} \\ (r-1)a_{21} & (r-1)a_{22} & \cdots & (r-1)a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ (r-1)a_{n1} & 0 & \cdots & (r-1)a_{nn} \end{bmatrix} \end{aligned}$$

ve

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n1} & \cdots & a_{nn} \end{bmatrix} \cdot \begin{bmatrix} r-1 & 0 & \cdots & 0 \\ 0 & r-1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & r-1 \end{bmatrix} =$$

$$\begin{bmatrix} a_{11}(r-1) & a_{12}(r-1) & \cdots & a_{1n}(r-1) \\ a_{21}(r-1) & a_{22}(r-1) & \cdots & a_{2n}(r-1) \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}(r-1) & 0 & \cdots & a_{nn}(r-1) \end{bmatrix}$$

dir.

Önerme 4.4.2: G bir grup olsun. Eğer bu grubun merkezinde bir involüsyon bulunuyorsa G nin elemanlarının en az yarısının mertebesi çifttir.

İspat: $a \in Z(G)$ ve $a^2 = e$ ve $a \neq e$ olsun. Her $x \in G$ için $ax = xa$ dır.

G nin, z merkezde olan bir involüsyon olmak üzere $H = \{e, z\}$ alt grubunu alalım. H ın G deki sol kosetleri

$$gH = \{g, gz\}$$

şeklindedir. Kosetler ayrık olduğundan ve birleşimleri G yi kapsadığından toplam koset sayısı

$$[G:H] = \frac{|G|}{2}$$

olur.

Şimdi, her gH kosetindeki iki elemandan en az birinin mertebesinin çift olması durumuna bakalım:

Durum I: g nin mertebesi çift ise durum açıktır.

Durum II: g nin mertebesi tek ise, $|g| = 2k + 1$ olması durumunda;

$$(gz)^{2k+1} = g^{2k+1}z^{2k+1} = e.z = z \neq e,$$

$$(gz)^{2(2k+1)} = g^{2(2k+1)}z^{2(2k+1)} = e.e = e$$

olduğundan $|gz|$ çift olur.

Her kosette en az bir çift mertebeli eleman bulunduğundan çift mertebeli eleman sayısı en az $|G|/2$ olur.

Bu bilgelere dayanarak aşağıdaki örnek verilebilir;

Örnek 4.4.1: $Sp(2,5)=\left\{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 4 & 4 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 4 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 3 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 4 \\ 3 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 3 \\ 1 & 4 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 2 & 3 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 0 & 3 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 4 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 4 \\ 3 & 4 \end{bmatrix}, \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 4 & 0 \\ 0 & 4 \end{bmatrix}, \begin{bmatrix} 4 & 1 \\ 2 & 2 \end{bmatrix}, \begin{bmatrix} 4 & 2 \\ 4 & 1 \end{bmatrix}, \begin{bmatrix} 4 & 4 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 4 & 3 \\ 3 & 0 \end{bmatrix}, \begin{bmatrix} 3 & 0 \\ 3 & 2 \end{bmatrix}, \begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 3 & 2 \\ 4 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 4 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 3 & 3 \\ 1 & 3 \end{bmatrix}\right\}$ grubunu göz önüne alalım. $Z=\left\{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 4 & 0 \\ 0 & 4 \end{bmatrix}\right\}$ grubun merkezidir. Buradaki elemanların mertebeleri ise GAP programında `listord:=List(maksrep[1],x->Order(x));` komutu kullanarak ;
[1, 3, 4, 3, 6, 6, 2, 3, 3, 6, 3, 6, 4, 4, 6, 4, 3, 6, 3, 6, 4, 4, 6, 3]

şeklinde bulunur. Ayrıca $Sp(2,5)$ grubunun $\begin{bmatrix} 4 & 0 \\ 0 & 4 \end{bmatrix}$ elemanının mertebesi 2 ve bir involüsyondur. Aynı zamanda bu eleman merkezdendir. Dolayısıyla, buradan $Sp(2,5)$ grubunun elemanlarının en az yarısının çift mertebeli olduğu anlaşılır.

Bütün bu özelliklerin ışığında aşağıdaki teorem ile dördüncü mertebeden bir grup için 2006 yılında Brooksbank ve arkadaşlarının yapmış olduğu analizlerin geçerli olduğu gösterilecektir.

Teorem 4.4.4: $H = G/Z(R \cap G)$ ve $A = (R \cap G)/Z(R \cap G)$ olsun. $\bar{G} = G/(R \cap G) \cong Sp(2, r)^4$ ise BlindDescent $122 \log(1/\delta)$ tane y elemanı işlendikten sonra $1 - \delta$ dan büyük bir olasılıkla doğru sonuç üretir.

İspat: $Sp(2, r)^4$ grubunun merkezinin mertebesi 16 dır ve tüm involüsyonlar bu merkezin içindedir. Bu gruptaki elemanların en az yarısının mertebesi çifttir. Hatta mertebesi 16 ya bölündüğünde 2,4,6,8,10,12,14 çift kalan veren elemanlarının oranı en az $1/3$ tür. Bundan dolayı $1/81$ den büyük bir ihtimalle bu elemanlarla belirlenen $\bar{G} = Sp(2, r)^4$ bölüm grubundaki $\bar{y} = (\bar{y}_1, \bar{y}_2, \bar{y}_3, \bar{y}_4)$ görüntüsünde $\bar{y}_1, \bar{y}_2, \bar{y}_3$ ve $\bar{y}_4$ çift mertebeli olup aynı

zamanda $\bar{y}$ 16 ile bölünmez. Görüntüsü $\bar{y}$ olan $y \in G$ için $y^{o_y/2}$ A kümesi üzerinde $-Id$ olarak etki eder. O halde,

$$\begin{aligned}
x(R \cap G)y^{o_y/2}(R \cap G) &= y^{o_y/2}(R \cap G)x(R \cap G) \\
\Rightarrow x^{-1}(R \cap G)(y^{o_y/2})^{-1}(R \cap G)x(R \cap G)y^{o_y/2}(R \cap G) &= (R \cap G) \\
\Rightarrow x^{-1}(y^{o_y/2})^{-1}xy^{o_y/2}(R \cap G) &= (R \cap G) \\
\Rightarrow [x, y^{o_y/2}] &\in (R \cap G)
\end{aligned}$$

olup $Prob([x, y^{o_y/2}] \in (R \cap G) = 1$ bulunur. Ayrıca $r \geq 3$ olup Yardımcı Teorem 4.3.2 (ii) den

$$Prob([x, y^{o_y/2}] \notin Z(R \cap G) | [x, y^{o_y/2}] \in (R \cap G) \geq 2/3$$

elde edilir. O halde,

$$\begin{aligned}
Prob([x, y^{o_y/2}] \notin Z(R \cap G) \wedge [x, y^{o_y/2}] \in (R \cap G) &\geq 1 \cdot \frac{2}{3} \cdot \frac{1}{81} \\
Prob([x, y^{\frac{o_y}{2}}] \notin Z(R \cap G) \wedge [x, y^{\frac{o_y}{2}}] \in (R \cap G) &\geq \frac{2}{243} \approx \frac{1}{122}
\end{aligned}$$

bulunur. Dolayısıyla BlindDescent algoritmasının 11. Satırını $p = 2$ olarak alırsak $1 - \delta$ dan büyük bir ihtimalle uygun bir x elemanın üretildiği görülür.

Bu analizlerin sonucunda eğer girdi grubu olan G çözülebilir grup ya da mükemmel bir grup olmasın durumunda algoritma doğru sonucu verecektir. Eğer girdi grubu olan G yerine G grubunun çözülebilir kalanını alırsak bu grup mükemmel grup olacağından yukarıdaki analiz çözülebilir kalanlar için de geçerli olacaktır.

Analizlerin geri kalan kısımlarına ilişkin hesaplamalar dosya halinde;
<https://github.com/zehracikcp/analysis-site> adresinde bulunabilir.

5. SONUÇ, TARTIŞMA ve ÖNERİLER

Bu tez çalışmasında, BlindDescent algoritmasının çözülebilir gruplar üzerindeki etkinliği detaylı bir şekilde incelenmiştir. İlk aşamada, algoritmanın 8,10,12 boyutlu çözülebilir gruplar üzerindeki çalışmaları gerçekleştirilmiş ve performansı değerlendirilmiştir.

İkinci aşamada ise literatürde tanımlı r asal olmak üzere $Sp(8, r)$, $Sp(10, r)$ ve $Sp(12, r)$ gruplarının maksimal alt grupları üzerinden çözülebilir kalanları ve bu kalanların mükemmel alt grupları aşamalı olarak elde edilmiştir. Bu alt grupların bir kısmı doğrudan hesaplama yöntemleriyle, bir kısmı ise involüsyonların kullanımıyla analiz edilmiş ve sonuçlar tablolar halinde verilmiştir. Analizlerin ayrıntısına ve hesaplama süreçlerine ilişkin bağlantılar okuyucunun erişimine sunulmuştur. Parçalar halinde yürütülen hesaplamalar sırasında özellikle 12 boyutlu gruplar için mevcut donanımın RAM kapasitesi yetersizliği nedeniyle bazı teknik güçlüklerle karşılaşmıştır.

Elde edilen bulgular, çözülebilir kalan analizlerinin özellikle yüksek boyutlarda önemli hesaplama kaynakları gerektirdiğini göstermektedir. Bu durum, gelecekte yapılacak çalışmalar için yüksek performanslı hesaplama merkezlerinde paralel programlama tekniklerinin uygulanmasının gerekli olduğunu ortaya koymaktadır. Ayrıca, elde edilen mükemmel alt gruplar ve yapılan analizler ilgili grup teorisi literatürüne somut katkılar sağlamaktadır.

Sonuç olarak, bu tez çalışması hem algoritmanın farklı boyutlardaki performansını hem de spesifik grup yapıları üzerinden elde edilen çözülebilir ve mükemmel alt grup analizlerini kapsamlı bir şekilde ortaya koymuştur. Elde edilen veriler ve metodolojik yaklaşım, ileri çalışmalar için bir referans niteliği taşımaktadır.

KAYNAKLAR

- Asar, A.O., Arıkan, A., 2009. Cebir. Eflatun Yayınevi, 371s, Ankara.
- Aschbacher, M., 1984. On the maximal subgroups of finite classical groups. Invent.Math., 76(3), 469-514.
- Aschbacher, M., 2000. Finite group theory. Cambridge University Press, New York: NY.
- Babai, L. and Beals, R., 1999. A polynomial time theory of black box groups, I. Groups St. Andrews 1997 in Bath, I, London Math. Soc. Lecture Note Ser., 260,30-64.
- Babai, L., 1979. Monte Carlo algorithms for graph isomorphism testing. Technical Report DMS 79,10.
- Beals, R. and Babai, L., 1993. Las vegas algorithms for matrix groups. Proc. 34th IEEE FOCS, 427-436.
- Beals, R., 1997. Towards polynomial time algorithms for matrix groups. In Groups and Computation II, 1995 DIMACS Workshop (L. Finkelstein and W.M. Kantor rdt.) DIMACS Ser. In Discrete Math. And Teor. Comp Sci., 28.
- Bilgiç, H., 2013. Soyut Cebir Ders Notları. Kahraman Maraş Sütçü İmam Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü, Maraş.
- Bray, J., Holt, D. and Rooney-Dougal, C., 2013. The maximal subgroups of the low dimensional finite classical groups. Cambridge University Press, 438.
- Brooksbank, P. and Niemeyer, A.C. and Seress, A., 2006. A reduction algorithm for matrix groups with an extraspecial normal subgroup. Finite Geometries, Groups and Computation, deGruyter, 1-16.

- Butler, G. and Cannon J., 1991. Computing Sylow subgroups of permutation groups using homomorphic images of centralizers. *J. Symbolic Computation*, 12, 443-457.
- Bosma, W., Cannon, J. and Playoust, C., 1997. The Magma algebra system I: The user language. *J. Symbolic Comput.*, 24, 235-265.
- Cannon, J. J., and Holt, D. F., 2003. Computing maximal subgroups of finite groups. *Journal of Symbolic Computation*, 37, 589-609.
- Cannon, J., and Souvignier, B., 1997. On the computation of conjugacy classes in permutation groups. *Proc. Of International Symposium on Symbolic and Algebraic Computation ISSAC'97*, ACM Press, New York, 392-399.
- Carter, R. W., 1989. *Simple Groups of Lie Type*. John Wiley & Sons, London. New York. Sydney. Toronto, 352p.
- Conway, J. H. and Curtis, R.T. and Norton, S.P. and Parker, R.A. and R. A. Wilson, 1985. *An ATLAS of Finite Groups*. Clarendon Press, Oxford; reprinted with corcorrections in 2003, 252p.
- Cooperman, G. and Finkelstein, L., 1993. Combinatorial tools for computational group theory. *Groups and Computation*, DIMACS Ser. Discrete Math. Theoret. Comput. Sci. Amer. Math Soc., 11, 53-86.
- Çağman, A., 2014. *C_6 Grupları İçin İndirgeme Algoritma Analizleri*. Doktora Tezi, Atatürk Üniversitesi Fen Bilimleri Enstitüsü. Erzurum.
- Çallıalp, F., 2009. *Örneklerle Soyut Cebir*, Birsen Yayınevi, 300s, İstanbul.
- Çelik, Z., 2025. analysis-site. GitHub, <https://github.com/zehraclkcp/analysis-site> (Erişim: 18.11.2025).
- Dickson, L. E., 1901. *Linear Groups: With an Exposition of the Galois Field Theory*. Teubner.

- Dixon, J. D., 1968. The solvable length of a solvable linear group. *Mathematische Zeitschrift*, 107, 151–158. doi:10.1007/BF01111027.
- Doerk, K. and Hawkes, T., 1978. On the residual of a direct product. *Arch. Math. (Basel)*, 30, 458-468.
- Doerk, K. and Hawkes, T., 1992. *Finite Soluble Groups*. De Gruyter Expositions in Mathematics 4, 891p.
- Dummit, D. S. and Froote, R. M., 2004. *Abstract Algebra*. John Wiley & Sons, Inc., 945p.
- Erdős, P., and Turan, P., 1968. On some problems of a statistical group-theory. IV. *Acta Mathematica Hungarica*, 19(3-4), 413-435.
- Furst, M., Hopcroft, J., and Luks, E. M., 1980. Polynomial-time algorithms for permutation groups. *Proc. 21 st IEEE Symposium on Foundations of Computer Science*, IEEE Press, Washington, 36-41.
- Goncalves, D. L., & Guaschi, J., 2009. The lower central and derived series of the braid groups of the finitely-punctured sphere. *Journal of Knot Theory and Its Ramifications*, 18(05), 651-704.
- Gorenstein, D., 1980. *Finite Groups*. Chelsea Publishing Company, 519p, New York, N.Y.
- Grillet, P.A., 2007. *Abstract Algebra*. Mathematics Subject Classification (2000): 20-01 16-01, 669p, New York, USA.
- Grove, L.C., 2002. *Classical Groups and Geometric Algebra*. American Mathematical Society, 169p, Providence, Rhode Island, USA.
- Hawkins, T., 2020. *Emergence of the Theory of Lie Groups*. Springer.
- Holt, D. F., and Plesken, W., 1989. *Perfect Groups*. Clarendon Press, Oxford, 376p, New York, USA.

- Humphrey, J.F., 1996. A Course in Group Theory. Oxford University Press, 285p, New York, USA.
- Hungerford, T. W., 2003. Algebra (graduate texts in mathematics). (12). New York: Springer-Verlag, 24, 31, 35, 50-51.
- Huppert, B., 1957. Lineare auflösbare Gruppen. Mathematische Zeitschrift, 67, 479–518. doi:10.1007/BF01258878.
- Huppert, B., 1967. Endliche Gruppen I. Springer.
- Isaacs, I. M., 2008. Finite Group Theory. American Mathematical Society, 352p, Providence, Rhode Island, USA.
- Kantor, W.M., and Seress, A., 2003. Computing with matrix groups. In Groups, Combinatorics and Geometry (Durham 2001), World Sci. Publishing, River Edge, NJ, 123-137.
- Kleidman P. and Liebeck, M., 1990. The subgroup structure of the finite classical groups. Cambridge University Press, New York: NY.
- Klein, F., 1872. Vergleichende Betrachtungen über neuere geometrische Forschungen. Verlag von Andreas Deichert.
- Knuth, D.E., 1991. Efficient representation of perm groups. Combinatorica 11 (1), 33-43.
- Leedham-Green, C.R., 2001. The computational matrix group project. Groups and Computation III (Columbus, OH, 1999), Ohio State Univ. Math. Res. Inst. Publ., 8, 229-247.
- Leedham-Green, C.R., & O'Brien, E.A., 2006. Recognising matrix groups over finite fields. Preprint.

- Neubüser, J., 1995. An invitation to computational group theory. In Groups'93 Galways/St. Andrews, London mathematical soc. Lecture note ser., 212, 457-475.
- Newman, M. F., 1972. The soluble length of soluble linear groups. Math. Z., 126, 59-70.
- Neimeyer, A.C., 2005. Constructive recognition of normalizers of small extra-special matrix groups. Inten. J. Algebra and Computation, 15(2), 367-394.
- Rose, J. S., 1978. A Course on Group Theory. Cambridge University Press, 310p, London-New York-Melbourne.
- Rotman, J.J., 1995. An Introduction to the Theory of Groups. Springer Verlag, 513p, New York, USA.
- Seress, A., 1997. An introduction to computational group theory. Notices Amer. Math. Soc., 44,671-679.
- Sims, C.C., 1970. Computational methods in the study of permutation groups. Computational Problems in Abstract Algebra, Pergamon Press, Oxford, 169–183.
- Sims, C. C., 1971. Computational methods in the study of permutation groups. Computational Problems in Abstract Algebra, Pergamon Press, Oxford, 169-183.
- Suzuki, M., 1982. Group Theory I. Springer Verlag, 434p, Berlin-Heidelberg-New York.
- Suzuki, M., 1986. Group Theory II. Sringer Verlag, 621p, New York USA.
- Taşçı, D., 2008. Soyut Cebir. Alp Yayınevi, 671s, Ankara.
- The GAP Group, 2014. GAP-Groups, Algorithms, and Programming, Version 4.12.2, <http://www.gap-system.org>.
- Weyl, H., 1939. The Classical Groups: their invariants and representations. Princeton Univ. Press, 336p, Princeton New Jersey.

Wilson, R. A., 2009. The Finite Simple Groups (graduate texts in mathematics). New York: Springer-Verlag London Limited, 310p.

Zassenhaus, H., 1938. Beweis eines Satzes über diskrete Gruppen. Abh. Math. Sem. Univ. Hamburg, 12, 289-312.



EKLER

Ek 1. Türev uzunluğu Mathematica Kodu

```

k[m] := Floor[Log[9, m]];
σ[m] := Piecewise[{{5k[m], 9k[m] ≤ n ≤ 169k[m]-1}, {5k[m] + 1, 169k[m]-1 ≤ m
≤ 39k[m]}, {5k[m] + 2, 39k[m] ≤ m ≤ 49k[m]}, {5k[m] + 3, 49k[m] ≤ m
≤ 649k[m]-1}, {5k[m] + 4, 649k[m]-1 ≤ m ≤ 9k[m]+1}}];
η[m_] := Piecewise[{{1, m == 1}, {4, m =
= 2}, {9 + σ[ $\frac{m-2}{8}$ ], MemberQ[{6, 7, 17, 59, 60, 61, 62, 63, 64, 65}, m]}}, 10
+ σ[ $\frac{m-2}{8}$ ]];
{#, η[#]}&/@Range[30]

```

ÖZGEÇMİŞ

Kişisel Bilgiler	
Adı Soyadı	Zehra ÇELİK KARADENİZ
Doğum Yeri ve Tarihi	
Eğitim Durumu	
Lisans Öğrenimi	Erzincan Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü
Yüksek Lisans Öğrenimi	Erzincan Binali Yıldırım Üniversitesi Lisansüstü Enstitüsü Matematik Anabilim Dalı Cebir ve Sayılar Teorisi Bilim Dalı
Bildiği Yabancı Diller	İngilizce
İş Deneyimi	
Çalıştığı Kurumlar	Ağrı İbrahim Çeçen Üniversitesi
Projeler	TÜBİTAK 3501-Kariyer Geliştirme Projesi Proje No: 121F477