

**T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ**

BULANIK ALT GRUPLARIN ve KODLARIN SAYISI İLE BAZI UYGULAMALAR

ESENGÜL SALTÜRK

**DOKTORA TEZİ
MATEMATİK ANABİLİM DALI
MATEMATİK PROGRAMI**

**DANIŞMAN
PROF. DR. İRFAN ŞİAP**

İSTANBUL, 2013

T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BULANIK ALTGRUPLARIN ve KODLARIN SAYISI ile BAZI UYGULAMALAR

Esengül SALTÜRK tarafından hazırlanan tez çalışması 26.12.2012 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda **DOKTORA TEZİ** olarak kabul edilmiştir.

Tez Danışmanı

Prof. Dr. İrfan ŞİAP

Yıldız Teknik Üniversitesi

Jüri Üyeleri

Prof. Dr. İrfan ŞİAP

Yıldız Teknik Üniversitesi

Prof. Dr. Ahmet Göksel AĞARGÜN

Yıldız Teknik Üniversitesi

Doç. Dr. Ünsal TEKİR

Marmara Üniversitesi

Doç. Dr. Bahattin YILDIZ

Fatih Üniversitesi

Doç. Dr. Gürsel YEŞİLOT

Yıldız Teknik Üniversitesi

Bu alıřma, 2007-2012 yılları arasında 2211 kodlu TÜBİTAK Yurt İi Doktora Bursu ve 2011-2012 yılları arasında Yıldız Teknik Üniversitesi Bilimsel Arařtırma Projeleri Koordinatörlüğü' nün 2011-03-DOP01 numaralı projeleri ile desteklenmiştir.

ÖNSÖZ

Bu çalışmanın ortaya çıkmasında ilmi ve manevi desteğini her daim hissettiren, bana yepyeni ufuklar açan, bilgilerini paylaşırken fazlasıyla cömert davranan, çalışmalarıyla örnek aldığım değerli hocam Prof. Dr. Sayın İrfan ŞİAP'a en içten saygı ve teşekkürler...

Her türlü durum ve problem karşısında yalnız olmadığımı hissettiren, üzerimde çok emeği olan hocam Prof. Dr. Sayın Ahmet Göksel AĞARGÜN'e canı gönülden teşekkürler...

Bu çalışmanın gerçek bir tez olarak ortaya çıkmasında başından sonuna kadar maddi manevi yanımda olan, her şeyden daha çok önemsedığım, annem ve babama; ayrıca kardeşlerim Arş. Gör. Serkan SALTÜRK, Arş. Gör. Tuba SALTÜRK ve Yunus SALTÜRK'e sonsuz teşekkürler...

Bu süreçte maddi destek kaynağım olan TÜBİTAK'a ciddi manada teşekkürler...

Aralık, 2012

Esengül SALTÜRK

İÇİNDEKİLER

Sayfa

SİMGE LİSTESİ.....	viii
KISALTMA LİSTESİ.....	x
ŞEKİL LİSTESİ.....	xi
ÇİZELGE LİSTESİ	xii
ÖZET	xiii
ABSTRACT.....	xv
BÖLÜM 1	
GİRİŞ.....	1
1.1 Literatür Özeti	1
1.2 Tezin Amacı	2
1.3 Orijinal Katkı.....	2
BÖLÜM 2	
GRUP-HALKA-ÇİSİM	3
2.1 Gruplar ile İlgili Temel Kavramlar	3
2.2 Direkt Toplamlar [15].....	4
2.3 Halkalar ile İlgili Temel Kavramlar [15,16]	4
BÖLÜM 3	
BULANIK (FUZZY) GRUP TEORİ.....	7
3.1 Giriş	7
3.2 Bulanık Teori ile İlgili Yakın Zamanlarda Yapılan Araştırmalar [21]	8
3.3 Bulanık (Fuzzy) Teori ile İlgili Temel Cebirsel Kavramlar	9
3.4 Bulanık Kümeler ile İlgili Alternatif Tanımlar	10
3.4.1 Bulanık Alt Kümeler	10

3.4.2	Bulanık Alt Gruplar.....	13
3.4.3	Bulanık Alt Halkalar.....	15
BÖLÜM 4		
SONLU ABEL GRUPLARI, MAKSİMAL ZİNCİRLER, BULANIK ALT GRUPLAR.....		17
4.1	Giriş	17
4.2	Abel p – Gruplarının Alt Grupları, Maksimal Zincirleri ve Bulanık Alt Grupları	21
BÖLÜM 5		
BAZI GRUPLARIN BULANIK ALT GRUPLARININ SAYISI		23
5.1	Giriş	23
5.2	Ön Bilgiler.....	24
5.3	$\mathbb{Z}_p \times \mathbb{Z}_p \times \dots \times \mathbb{Z}_p = \mathbb{Z}_p^n$ Grubunun Bulanık Alt Gruplarının Sayısı	26
5.3.1	$\mathbb{Z}_p^n$ Grubunun Alt Gruplarının Maksimal Zincirlerinin Sayısı.....	26
5.3.2	$\mathbb{Z}_p^n$ Grubunun Bulanık Alt Gruplarının Sayısı	29
5.4	$\mathbb{Z}_{2^k} \times \mathbb{Z}_{2^k}$ ($2 \leq k \leq 3$) Grubunun Bulanık Alt Gruplarının Sayısı	47
5.4.1	$\mathbb{Z}_4 \times \mathbb{Z}_4$ grubunun bulanık alt grupları	47
5.4.2	$\mathbb{Z}_8 \times \mathbb{Z}_8$ grubunun bulanık alt grupları	50
BÖLÜM 6		
CEBİRSEL KODLAMA TEORİSİNİN TEMELLERİ		53
6.1	Giriş	53
6.2	Temel Kavramlar	55
BÖLÜM 7		
BAZI HALKALAR ÜZERİNDE LİNEER KODLARI SAYMA PROBLEMİ		61
7.1	Giriş	61
7.2	F_q Cismi Üzerinde Lineer Kodların Sayısı	61
7.3	$\mathbb{Z}_{p^m}$ Halkası Üzerinde Lineer Kodların Sayısı.....	62
7.3.1	Örnekler	72
7.4	Sayma Probleminde Literatür ile Tezdeki Yaklaşımın Karşılaştırılması.....	74
7.4.1	Sonlu Zincir Halkaları Üzerinde Lineer Kodlar	74
7.4.2	Karşılaştırma	78
7.5	Toplamsal (Additive) Kodlar.....	79
7.6	Galois Halkaları Üzerinde Lineer ve Toplamsal Kodlar	81
7.7	$\mathbb{Z}_{p^m}[\xi]$ Halkası Üzerinde Toplamsal Kodların Sayıları	84
7.8	$\mathbb{Z}_{p^m}[\xi]$ Halkası Üzerinde Lineer Kodların Sayıları.....	86
7.5.1	Örnekler	87

7.9	$F_q + uF_q$ Halkası Üzerinde Kodların Sayısı	90
7.10	Sonlu Zincir Halkaları Üzerinde Kodlar	91
7.11	Esas İdeal Halkaları Üzerinde Kodlar.....	98
BÖLÜM 8		
BAZI UYGULAMALAR.....		99
8.1	Genelleştirilmiş Gauss (Gaussian) Sayıları	99
8.2	Yeni Tanımlanan Diziler	100
8.3	Dizayn Teori ile İlgili Bazı Kavramlar	103
8.3.1	t – Dizaynlar	103
8.4	Tez Çalışması Sırasında Elde Edilen Dizaynlar	104
8.4.1	p mertebeli (1 boyutlu) alt grupların dizaynı.....	104
8.4.1.1	Örnekler	105
8.4.2	p^s ($s \in \mathbb{Z}^+$) mertebeli alt grupların dizaynı.....	107
8.4.2.1	Sonuçlar.....	107
BÖLÜM 9		
SONUÇ VE ÖNERİLER		109
KAYNAKLAR.....		110
ÖZGEÇMİŞ		113

SİMGE LİSTESİ

$\emptyset$	Boş küme
$\langle a \rangle$	a elemanı ile üretilen küme
$A \cong B$	A ile B izomorftur.
$A \setminus B$	A kümesinin B kümesinden farklı elemanlarının kümesi
A / B	Bölüm grubu
A^n	A kümesinin B kümesinden farklı elemanlarının kümesi
$A < B$	A grubu B 'nin alt grubudur.
$C_p(n, k)$	Gauss binom katsayısı
G^*	G kümesinin sıfırdan farklı elemanlarının kümesi
$ G $	G kümesinin eleman sayısı
$G \oplus H$	G ile H kümelerinin direkt toplamı
$f: G \rightarrow H$	G kümesinden H kümesine fonksiyon
F_q	q elemanlı sonlu cisim
$F(p, n)$	$\mathbb{Z}_p^n$ grubunun bulanık alt gruplarının sayısı
$\phi(n)$	n 'in Euler fi fonksiyonu
G/H	Bölüm grubu
$H \times K$	H ile K 'nin iç direkt çarpımı
$\text{Im}(\mu)$	μ bulanık alt kümesinin görüntü kümesi
$I(G)$	G 'nin tüm bulanık alt gruplarının kümesi
μ_a	μ 'nün a – kesimi (a – seviye alt kümesi)
μ_A	A kümesinin üyelik fonksiyonu
$\mu \sim \nu$	μ bulanık alt kümesi ν bulanık alt kümesine denktir.
μ^*	μ 'nün desteği
μ'	μ 'nün eşleniği
$N_{k_1, k_2, \dots, k_m}^R$	R halkası üzerinde $(k_1, k_2, \dots, k_m)$ – tipinde kodların sayısı
$[n, k]_q$	F_q üzerinde uzunluğu n , boyutu k olan bir lineer kod
$[n, k, d]_q$	F_q üzerinde uzunluğu n , boyutu k , uzaklığı d olan bir lineer kod

$\begin{bmatrix} n \\ k \end{bmatrix}_q$	Gauss binom katsayısı
$\binom{n}{k}$	Binom katsayısı
$\bigcup_{i \in I} \mu_i$	μ_i bulanık alt kümelerinin birleşimi
$\bigcap_{i \in I} \mu_i$	μ_i bulanık alt kümelerinin kesişimi
$o(v)$	v elemanının toplamsal mertebesi
$[0,1]^X$	X 'in tüm bulanık alt kümelerinin kümesi
$R[x]$	Katsayıları R 'den alınan polinomlar halkası
$(v_1, v_2, \dots, v_n)$	n uzunluğunda söz
$\mathbb{Z}$	Tam sayılar kümesi
$\mathbb{Z}^+$	Pozitif tam sayılar kümesi
$\mathbb{Z}_n$	Modülo n 'e göre tam sayılar halkası

KISALTMA LİSTESİ

IFSA International Fuzzy System Association

ŞEKİL LİSTESİ

	Sayfa
Şekil 5. 1 Bir G grubunun Hasse şeması	29
Şekil 5. 2 $\mathbb{Z}_{p^2}$ grubunun bulanık alt gruplarının ağaç diyagramı.....	40
Şekil 5. 3 $\mathbb{Z}_2 \times \mathbb{Z}_2$ grubunun Hasse şeması	41
Şekil 5. 4 $\mathbb{Z}_3 \times \mathbb{Z}_3$ grubunun Hasse şeması	43
Şekil 5. 5 $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ grubunun Hasse şeması.....	44
Şekil 5. 6 $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ grubunun alternatif Hasse şeması.....	45
Şekil 5. 7 $\mathbb{Z}_4 \times \mathbb{Z}_4$ grubunun Hasse şeması	49
Şekil 5. 8 $\mathbb{Z}_4 \times \mathbb{Z}_4$ grubunun alternatif Hasse şeması	49
Şekil 5. 9 $\mathbb{Z}_8 \times \mathbb{Z}_8$ grubunun Hasse şeması.....	51
Şekil 6. 1 Kodlama şeması	55
Şekil 7. 1 Young Diyagramı I	75
Şekil 7. 2 Young Diyagramı II	75
Şekil 7. 3 C kodun Young diyagramı	77

ÇİZELGE LİSTESİ

Sayfa

Çizelge 7. 1 Bazı n 'ler için $\mathbb{Z}_4$ üzerinde lineer kodların sayısı	71
Çizelge 7. 2 Bazı n 'ler için $\mathbb{Z}_4$ üzerinde lineer kodların sayısı (devam).....	72
Çizelge 7. 3 Teorem 7.28'den ve Teorem 7.6'dan elde edilen sonuçların karşılaştırılması	78
Çizelge 7. 4 Teorem 7.28'den ve Teorem 7.6'dan elde edilen sonuçların karşılaştırılması (devam).....	79
Çizelge 8. 1 $k_1 = 0$ için elde edilen bazı diziler.....	101
Çizelge 8. 2 Bazı genel k_1, k_2 değerleri için elde edilen diziler.....	101
Çizelge 8. 3 $n=2, n=3$ ve $n=4$ için $R = \mathbb{Z}_4[\xi]$ üzerinde lineer kod sayıları.....	103

BULANIK ALT GRUPLARIN ve KODLARIN SAYISI ile BAZI UYGULAMALAR

Esengül SALTÜRK

Matematik Anabilim Dalı

Doktora Tezi

Tez Danışmanı: Prof. Dr. İrfan ŞİAP

Klasik mantıkta bir önerme ya doğrudur ya da yanlıştır, üçüncü bir durum söz konusu olamaz. Ancak bazen, hatta genelde dünyadaki olayları açıklamak için kesin tanımlamalar yetersiz kalır. Bu olayları açıklamak için belli terim ve ölçülere ihtiyaç duyulur. İşte bu yeni mantık “Bulanık Mantık (Fuzzy Logic)” olarak adlandırılır.

Bulanık Mantık ilk olarak, M.Ö. 500 yılında Buda tarafından ve ondan 200 yıl kadar sonra da Yunan filozof Aritoteles tarafından ortaya atılmıştır. Bu alanda matematiğe uygulanması bakımından yapılan en önemli çalışma 1965 yılında University of California, Berkeley’den Lotfi A. Zadeh’in klasik mantık yaklaşımının kesin çizgilerini yok eden “Fuzzy Sets (Bulanık Kümeler)” (Zadeh [19]) adlı çalışmasıdır. Bu eser, var olan çizgilerin dışına çıkmış ve bu alandaki diğer araştırmacılara öncü olmuştur. Bulanıklık ile ilgili cebirsel alt yapı ise A. Rosenfeld (Rosenfeld [1]) ve P. S. Das (Das [2]) tarafından inşa edilmiştir.

“Fuzzy” kelime anlamı olarak bulanıklığı ifade eder. Bulanık kümelerin elemanlarından bahsederken “kümeye aittir ya da değildir” gibi kesin ifadeler kullanılmaz. Bunun yerine “belli derecelerle kümenin elemanıdır” şeklinde ifadeler kullanılır. Güzellik, gençlik, yaşlılık, uzun boyluluk, çalışkanlık, zeka kavramları bulanıklık ifade eden ve kişiden kişiye göre değişen ifadeler olduğundan bulanık küme mantığı konusu içerisinde yer alan başlıklardan bazılarıdır.

Öte yandan bu çalışmada yer verilen, cebirin en önemli uygulama alanlarından biri olan Cebirsel Kodlama Teorisi, son zamanlarda birçok matematikçi tarafından çalışılmaktadır. Teori ilk olarak 1948’de Claude Shannon’ın “A Mathematical Theory of Communication” (Shannon [7]) adlı meşhur makalesi ile başladı. İlk zamanlarda tüm çalışmalar cisimler üzerinde iken, 1994’den itibaren, P. V. Kumar ve arkadaşlarının çalışması (Hammons [8]) ile birlikte halkalar üzerinde kodlar çalışılmaya başlandı. Son yıllarda ise bazı özel halkalar üzerinde kodlar ve özellikleri oldukça popüler olmuştur. Bu çalışmaların yanı sıra, lineer kodları kombinatorik açıdan incelemek, yani lineer kodların alt lineer kodlarının sayılarını bulmak oldukça önemli bir problemdir. Bu problem, cisimler üzerinde lineer kodlar için tamamıyla çözülmüştür ve kodların sayısı Gauss binom katsayıları ile gösterilmektedir. Öte yandan, halkalar üzerinde kodların sayıları ile ilgili de çok çeşitli çalışmalar ([9], [10], [11], [42]) yapılmıştır. Bu nedenle, 7. Bölüm’de, bazı halkalar üzerinde kodlar incelenerek bunların sayılarını çok basit bir şekilde bulmaya yarayan formüller elde edilmiştir.

Bu çalışmada; 2. ve 5. Bölümlerde genel cebirsel bilgiler, 3. ve 4. Bölümlerde Bulanık Teori ile ilgili kavramlar ve bazı Abel gruplarının bulanık alt gruplarının sayısı, 6., 7. ve 8. Bölümlerde ise Cebirsel Kodlama Teorisi ile ilgili kavramlar, bazı lineer kodların sayısı ve bazı uygulamaları verilmektedir.

Anahtar Kelimeler: Bulanık alt gruplar, Denklik sınıfları, Maksimal zincirler, Cebirsel Kodlama Teorisi, Gauss binom katsayıları, Dizaynlar, Sayı dizileri.

THE NUMBER OF FUZZY SUBGROUPS AND CODES WITH SOME APPLICATIONS

Esengül SALTÜRK

Department of Mathematics

PhD Thesis

Advisor: Prof. Dr. İrfan ŞİAP

Any statement in classical logic is true or not, there is no third case. However sometimes even general definite descriptions are not enough to explain things. In order to define these things we need some grades. The new logic with grades of elements is called “Fuzzy Logic”.

Fuzzy Logic was first born in 500 B.C. with Buddha and also with Aristoteles after 200 years. However the most important scientific study that lightens the studies about fuzzy logic for the last half century is Professor Zadeh’s -from the University of California, Berkeley- original paper: “Fuzzy Sets” (Zadeh [19]). This work is the pioneer of the fuzzy studies. Algebraic constructions related with fuzzy is due to A. Rosenfeld (Rosenfeld [1]) and P. S. Das (Das [2]).

The word “fuzzy” means blurriness. When talking about the elements of any fuzzy set, we do not use definite expressions such as “an element or not” but “an element with any degree”. Beauty, youth, senility, lankiness, diligence, intelligence are some examples of fuzzy expressions since they vary from person to person.

On the other hand, Algebraic Coding Theory, one of the most important field of application of algebra, has being studied recently by mathematicians. This theory was first begun with the marvellous paper of Claude Shannon: “A mathematical theory of

communication” (Shannon [7]). While in the earlier stages everything was over finite fields, in 1994, by the work (Hammons [8]) of P.V. Kumar and his collaborates, codes over finite rings have been studied. In recent years, codes over some special rings and their properties are popular. Besides, examining linear codes in terms of combinatorial structure, namely finding the number of the subcodes of a linear code, is a really important problem. This problem is completely solved for the codes over finite fields and presented by Gaussian binomial coefficients. On the other hand, a wide range of studies about the number of the codes over rings ([9], [10], [11], [42]) has been done. Hence, in Section 7, linear codes over some finite rings were examined and formulas which makes easier to find their number were obtained.

In this work; we give some fundamentals of abstract algebra in Sections 2 and 5, concepts of fuzzy algebra and number of fuzzy subgroups of some Abelian groups in Sections 3 and 4, notions about Algebraic Coding Theory, number of linear codes and some applications in Sections 6, 7 and 8.

Key words: Fuzzy subgroups, Equivalence classes, Maximal chains, Algebraic Coding Theory, Gaussian binomial coefficients, Designs, Number sequences.

1.1 Literatür Özeti

Bulanık Mantığın temelleri ilk olarak M.Ö. 500 yılında Buda tarafından, 200 yıl sonra da ünlü filozof Aristoteles tarafından atılmıştır. Bulanık alt grup kavramı ilk olarak 1971 yılında A. Rosenfeld (Rosenfeld [1]) tarafından çalışıldı. Daha sonra P. S. Das (Das [2]), bulanık alt grupların seviye alt gruplarını inceledi. Son zamanlarda ise Murali ([3], [4], [5]), verilen bir grubun bulanık alt gruplarının kümesi üzerinde denklik tanımladı ve bazı p -grupların bulanık alt gruplarının sayısını hesapladı. 2008 yılında Marius Turneaceanu $\mathbb{Z}_p^n$ grubunun bulanık alt gruplarının sayısı için yinelemeli (rekursif) bir formül (Tarnauceanu [6]) verdi.

Cebirsel Kodlama Teorisi ile ilgili ilk çalışmalar ise 1948 yılında Claude Shannon'ın "A Mathematical Theory of Communication" (Shannon [7]) adlı meşhur makalesi ile başladı. 1994 yılında, P. V. Kumar ve arkadaşlarının "The $\mathbb{Z}_4$ -linearity of Kerdock, Preparata, Goethals and Related Codes" (Hammons [8]) adlı çalışması halkalar üzerinde kod çalışmaları için ciddi bir ışık olmuştur.

Cisimler üzerinde lineer kodların sayısı Gauss binom katsayıları ile belirlidir. S. Delsarte [9], P. E. Džubjuk [10] ve Yeh [11], 1948 yılında birbirlerinden bağımsız olarak, verilen λ tipinde bir grubun, μ tipinde alt gruplarının sayısını veren formülü yinelemeli (rekursif) olarak inşa ettiler. 2004 yılında Calugareanu verilen bir Abel grubunun tüm alt gruplarının sayısını yinelemeli (rekursif) olarak elde etti (Calugareanu [12]). Thomas

Honold da bu konudaki alıřmaları toparlamıř ve modller zerine uygulamıřtır (Honold [13], [14]).

1.2 Tezin Amacı

Bu alıřmanın temeli Bulanık Alt Gruplar Teorisi ve Kodlama Teorisi'ne dayanmaktadır. Bazı halkaların bulanık alt grup sayılarını ve bilinen bazı zel halkalar zerinde lineer kodların sayılarını hesaplamak; lineer kodlarla dizilerin iliřkisini, grupların alt grup řemalarıyla dizaynların iliřkisini incelenmek amalanmaktadır.

1.3 Orijinal Katkı

Daha nceki alıřmalarda ([6], [12], [13]) verilen metotların aksine daha basit ve anlařılır yntemlerle bulanık alt grupların ve lineer kodların sayıları hesaplanmış ve literatrdeki alıřmalarla karřılařtırılmıştır. Bu tezde verilen formllerle daha kısa srede sonuca ulařmak mmkndr. Ayrıca bu formllerden yola ıkılarak, Genelleřtirilmiş Gauss Sayıları dediėimiz yeni sayılar ve bu sayılardan elde ettiėimiz yeni diziler tanımlanmıştır. Bunlara ek olarak, tezde konu olan grupların Hasse řemalarından yararlanılarak yeni dizaynlar elde edilmiştir.

BÖLÜM 2

GRUP-HALKA-CİSİM

2.1 Gruplar ile İlgili Temel Kavramlar

Tanım 2.1 [15] G boştan farklı bir küme ve “ $\bullet$ ” işlemi de G üzerinde tanımlı bir ikili işlem olsun. Yani, $(G, \bullet)$ cebirsel yapısı düşünülmektedir. Eğer G kümesi aşağıdaki özellikleri sağlıyorsa G ’ye “ $\bullet$ ” işlemi üzerinde bir **gruptur** denir:

- i. (Birleşme) Her $a, b, c \in G$ için $(a \bullet b) \bullet c = a \bullet (b \bullet c)$,
- ii. (Birim eleman) Her $a \in G$ için $a\tau = \tau a = a$ olacak şekilde $\exists \tau \in G$ vardır,
- iii. (Ters eleman) Her $a \in G$ için $ab = ba = \tau$ olacak şekilde $\exists b \in G$ vardır.

Bu özelliklere ek olarak, Her $a, b \in G$ için $a \bullet b = b \bullet a$ özelliği de sağlanıyorsa G ye **değişmeli grup (Abel grubu)** denir.

Tez çalışması boyunca incelenen yapılar sonlu gruplar üzerinde olduğundan, sonlu gruplar konusu, bilhassa sonlu Abel grupları konusu Bölüm 4’de detaylı bir şekilde incelenecektir. Bu kısımda kısaca sonlu gruplar kavramı takdim edilmektedir.

Burada, anlaşılması kolay olan bazı kavramlar okuyucuya bırakılmıştır ve literatürde kolaylıkla bulunabilir ([15], [16], [17], [18]).

Sonlu sayıda (k) eleman içeren bir gruba **sonlu grup** denir ve grubun eleman sayısı olan k sayısına da **grubun mertebesi** denir ve $k = |G|$ ile gösterilir.

“Bir grubun bir elemanının mertebesi” kavramı ilk olarak 1815 yılında A. L. Cauchy tarafından tanımlanmıştır. Günümüzde bu kavramın farklı tanımları verilmektedir.

Bir $g \in G$ için, $g^n = e$ olacak şekildeki en küçük n tam sayısına g **elemanının mertebesi** denir.

Bir G grubunun mertebesi k , bir H alt grubunun mertebesi de l olsun. Bu durumda, H 'nin mertebesi G 'nin mertebesini böler, yani; $l \mid k$ 'dır. $k/l = m$ oranına ise H alt grubunun G 'deki **indeksi** denir.

2.2 Direkt Toplamlar [15]

Direkt toplamlar, Abel gruplarının sınıflandırılması açısından oldukça önemlidir. Eğer bir grup, alt grupların bir direkt toplamı olarak yazılabiliyorsa, çoğu durumda, verilen grubun yapısını incelemek yerine, daha basit olan, alt gruplarının yapısını incelemek de yeterli olacaktır. Ayrıca bilinen grupların direkt toplamı ile yeni gruplar inşa edilebilir.

$(G, \bullet)$ ve $(H, \circ)$ grupları verildiğinde, bu iki grubun direkt toplamı $G \oplus H$ ile gösterilir ve bu yapı “*” işlemi altında bir gruptur:

$$(g_1, h_1), (g_2, h_2) \in G \oplus H \text{ olmak üzere, } (g_1, h_1) * (g_2, h_2) = (g_1 \bullet g_2, h_1 \circ h_2).$$

Bu tanım, Abel gruplarının direkt toplamı olarak genelleştirilebilir.

2.3 Halkalar ile İlgili Temel Kavramlar [15,16]

Halka Teorisi, halkaların iki özel çalışma konusu olan “reel veya kompleks sayılar üzerinde n değişkenli polinom halkaları” ve “bir cebirsel sayılar cisminin tam sayıları” konularından ortaya çıkmıştır. Halka kavramı ilk olarak David Hilbert (1862-1943) tarafından tanımlanmıştır. Değişmeli halkalar teorisi ise ilk olarak 1921 yılında Emmy Noether tarafından, “Ideal Theory in Rings” isimli makalesi ile verilmiştir. Bu makalede esas olarak bir halkanın ideallerinin artan zincir yapısından bahsedilmektedir.

Bu kısımda, halkalar ile ilgili bazı temel tanımlar sunulmaktadır.

Tanım 2.2 [15,16] R boştan farklı bir küme ve “ $\bullet, \circ$ ” işlemleri de R üzerinde tanımlı birer ikili işlem olsun. Yani, $(R, \bullet, \circ)$ yapısı düşünülmektedir. Eğer R kümesi aşağıdaki özellikleri sağlıyorsa R 'ye $\bullet, \circ$ işlemleri üzerinde bir **halka** denir:

- i. R kümesi, $\bullet$ işlemine göre değişmeli bir gruptur,

ii. (Birleşme) Her $a, b, c \in R$ için $(a \circ b) \circ c = a \circ (b \circ c)$,

iii. (Dağılma) Her $a, b, c \in R$ için,

$$a \bullet (b \circ c) = (a \bullet b) \circ (a \bullet c), (a \circ b) \bullet c = (a \bullet c) \circ (b \bullet c).$$

$\bullet$ ve $\circ$ işlemleri sırasıyla R halkasının birinci ve ikinci işlemleri olarak adlandırılır.

Her $a \in R$ için, $1_R \neq 0_R$ olmak üzere, $1_R a = a 1_R = a$ olacak şekilde $1_R \in R$ elemanı var ise bu elemana R halkasının **birim elemanı** ve R ye de **birimli halka** denir.

İkinci işleme göre değişmeli olan halkaya **değişmeli halka** denir.

Tanım 2.3 [15,16] R bir halka ve $\emptyset \neq I \subset R$ olsun.

i. Her $a, b \in I$ için $a - b \in I$,

ii. Her $a \in I, r \in R$ için $ar \in I$

özellikleri sağlanıyorsa I ya R halkasının bir **ideali** denir. $\{0_R\}$ ve R 'ye R halkasının aşikar idealleri denir.

$a \in R$ olmak üzere, a elemanının ürettiği ideal $\langle a \rangle$ şeklinde gösterilir ve elemanları $\langle a \rangle = \{a.r : r \in R\}$ şeklindedir.

Tanım 2.4 [15,16] R ve S iki halka olmak üzere $f: R \rightarrow S$ dönüşümü aşağıdaki özellikleri sağlıyorsa, f 'ye **halka homomorfizması** denir.

i. $f(a+b) = f(a) + f(b), \forall a, b \in R$,

ii. $f(ab) = f(a)f(b), \forall a, b \in R$,

iii. $f(1) = 1$.

Tanım 2.5 [15,16]

i. R bir halka olsun. $0 \neq a \in R$ için, $ab = 0$ olduğunda $b \neq 0$ oluyorsa, b elemanına R 'nin bir sağ sıfır böleni denir. Burada $a \in R$ elemanı da R 'nin bir sol sıfır bölenidir. Eğer bir $a \in R$ elemanı, R 'nin hem sağ hem de sol sıfır böleni ise a 'ya R 'nin bir **sıfır böleni** denir.

- ii. Birimli, deęişmeli ve sıfır bölensiz bir halkaya **tamlık bölgesi** denir.
- iii. Birimli bir halkada her eleman birimsel ise, yani; her $a \in R$ için, $ab = ba = 1_R$ olacak şekilde tek türlü belirli $b \in R$ elemanı mevcut ise bu halkaya **bölenler halkası** denir.
- iv. Deęişmeli bölenler halkasına **cisim** denir.

Tanım 2.6 [15,16] R bir halka ve olsun. $(A, +)$ bir Abel grubu olsun. $R \times A \rightarrow A, (r, a) \mapsto r * a$ şeklinde tanımlı bir ikili işlem göz önüne alınsın. Her $a, b \in A, r, s \in R$ için,

- i. $r * (a + b) = r * a + r * b,$
- ii. $(r + s) * a = r * a + s * a,$
- iii. $(rs) * a = r * (s * a).$

özellikleri sağlanıyorsa A 'ya bir **R -modül** denir. Eğer, her $a \in A$ için, R 'nin, $1 * a = a$ olacak şekilde bir birim elemanı varsa A 'ya bir **birimsel R -modül** denir.

BULANIK (FUZZY) GRUP TEORİ

3.1 Giriş

Bulanık mantık ve bulanık matematik çalışmaları ilk olarak 1965 yılında California Berkeley Üniversitesi'nden Lotfi A. Zadeh (Zadeh [19]) tarafından başlatıldı. O zamandan beri bulanık matematik birçok yazar tarafından çalışıldı ve mühendislik, coğrafya, psikoloji gibi çeşitli alanlara uygulandı. Son zamanlarda ise çoğunlukla bilgi bilimleri ve biyoloji alanlarına uygulanmaktadır.

Bulanık küme kavramı [20]: Yeryüzünde, nesneler ya bir şeye sahiptir ya da değildir. Ya da bir nesne, bir kümenin elemanıdır veya değildir. İşte bu kavram bildiğimiz anlamdaki kümeleri ifade eder. Oysa bazen kesin olmayan çizgilere de ihtiyaç duyarız. Klasik mantığın tanımlayamadığı belirsiz kavramların matematiksel olarak ifade edilebilmesi bulanık teoriyi akla getirir. Belirsizlik problemleri; matematikçiler, mantıkçılar, filozoflar ve son zamanlarda ise bilgisayar ve yapay zeka ile ilgilenen bilim adamları tarafından çalışılan önemli konulardan biri haline gelmiştir. Bu teori, klasik teorinin kesin çizgilerine tam bir meydan okuma şeklindedir. Çünkü net olmayan ara değerlerden bahseder.

Bu olgu bir örnek ile şu şekilde açıklanabilir: 'Saat 15.00'da A305 no'lu sınıftaki öğrenciler' kümesi bilinen klasik anlamda bir kümedir. Yani tüm öğrencilerin kümesi evrensel küme olarak alınırsa, herhangi bir öğrenci saat 15.00'da, ya A305 sınıfındadır ya da değildir. Burada bir kesinlik vardır. Fakat 'Saat 15.00'da, A305 sınıfındaki uzun boylu öğrenciler' kümesini düşünecek olursak, buradaki 'uzun boyluluk' kavramı kafa

karıştırıcıdır. Hangi ölçü ‘uzun boyluluk’ ölçüsü içine girer? Bunu tespit etmek gerekir. Oysa, bu kavram kişiden kişiye göre değişen nesnel bir yaklaşımdır. Yani, kimine göre 1.85 bir uzun boy ölçüsü iken, kimi de 1.75’in uzun boy ölçüsü olduğunu düşünür. İşte bu şekilde net çizgilerle belirli olmayan kümeleri yorumlamak için bulanık teori kullanılır. Yukarıdaki örneği bir bulanık küme yardımıyla belirleyebiliriz. Her boy ölçüsüne $[0,1]$ aralığında üyelik dereceleri verilerek, ‘Saat 15.00’da, A305 sınıfındaki uzun boylu öğrenciler’ kümesi oluşturulabilir. Bu da üyelik fonksiyonu dediğimiz bir karakteristik fonksiyon yardımıyla olur. Eğer bir elemanın üyelik derecesi ‘0’ ise o eleman hiçbir şekilde o kümeye ait değildir, üyelik derecesi ‘1’ ise o eleman tamamıyla o kümeye aittir. Bunlar dışındaki değerler ara değerler olup, o elemanın hangi üyelikle (ne derece) belirtilen kümeye ait olduğunu gösterir. A , ‘Saat 15.00’da, A305 sınıfındaki öğrenciler’ in kümesi olsun. ‘Saat 15.00’da, A305 sınıfındaki uzun boylu öğrenciler’ kümesi aşağıdaki gibi oluşturulabilir.

$A = \{\text{Elif, Esen, Ahmet, Ali}\}$ olmak üzere, bu küme, öğrencilerin uzun boylu olma üyelik dereceleri ile birlikte aşağıdaki gibi yazılır:

$A = \{(\text{Elif}, 0.0), (\text{Esen}, 0.5), (\text{Ahmet}, 0.8), (\text{Ali}, 1.0)\}$ kümesi bir bulanık kümedir.

$\mu_{\text{uzunboy}} : X \rightarrow [0,1]$ (X : evrensel küme) olmak üzere;

$$\mu_{\text{uzunboy}}(x) = \begin{cases} 0.0, & x \leq 1.65 \\ 0.5, & 1.65 \leq x \leq 1.75 \\ 0.8, & 1.75 \leq x \leq 1.85 \\ 1.0, & x \geq 1.85 \end{cases}$$

şeklindedir.

3.2 Bulanık Teori ile İlgili Yakın Zamanlarda Yapılan Araştırmalar [21]

Yapay zeka tekniklerine ilişkin ilk görüşler günümüzden yıllarca önce, 1965 yılında ortaya atılmış [19], 1969 yılında bulanık küme teorisinin tıp alanında kullanılabilirliğinin açıklanması ile pek çok çalışmalar yapılmaya başlanmış [22], 1975 yılında kardiyovasküler sistemlerin klinik uygulamalarda kullanılması önerilmiş [23], 1980’de kardiyak fonksiyonların değerlendirilmesinde bulanık küme teorisinin kullanılması ile

ilgili çalışmalar yapılmıştır. 1989'da EKG verilerinin sınıflandırılması ve tanısı konusunda ilk çalışmalar yapılmış ve bu çalışmalarda elde edilen bilgiler, bulanık küme formuna getirilerek istatistiksel yaklaşımlarla sınıflandırılmıştır.

1990'lı yılların ortalarında kalp hastalıklarında bulanık küme ve hibrit sistemlerle tanısı ile ilgili çalışmalar yapılmış, 1994 yılında koroner arter hastalığı yapay sinirsel sistemle %89 doğruluk oranında sınıflandırılmış ve sonraki yıllarda da yapay zeka teknikleri ile çeşitli kalp hastalıklarında tanı koymada büyük başarı kaydedilmiştir. 1996 yılında kalbin tomografik görüntüleri bulanık mantık ile %94 doğruluk oranında sınıflandırılmış, 1998 yılında koroner arter hastalıklarının bulanık mantıkla sınıflandırılması konusunda genetik bulanık kural tabanı kullanılarak %96 oranında başarı elde edilmiştir [24], [25].

Bulanık kuram ile ilgili çalışmalar, Japonya'da 1980'lerin başında ortaya çıkmıştır. Tokyo'da Bulanık Mantık çalışmaları yapan bir grubun önderliğinde IFSA (International Fuzzy System Association) kuruluşu kuruldu ve Japonya'da Bulanık Teori çalışma merkezi haline geldi. Bu kuruluş kendinden sonraki kuruluşlara öncülük etmesi bakımından önemli bir yer taşır. İlk uygulama, metro trenlerinde otomatik sürücü bulanık kontrol sistemini kullanmak oldu [26]. Daha sonra bulanık mantık ve bulanık küme kavramı, bulaşık makineleri, çamaşır makineleri, elektrik süpürgelerinde uygulamaya konuldu. Yine bir Japon profesör (Muchiyo Sugeno) uzaktan kumandayla pilotsuz bir helikopterin bulanık mantık ile nasıl kontrol edildiğinin modelini çıkardı ve bu pilotsuz helikopter Hiroşima depreminde kullanıldı. Bir mil mesafeye kadar uzaktan kontrol ile o bölgeye gitti, oranın resimlerini çekti ve geri geldi. Bunlar dışında bulanık kontrolün kullanıldığı bazı alanlar; su arıtma tesislerinde kbr kontrolü, asansör kontrol sistemleri, trafik kontrol sistemleri, buldozer kontrolü, havalandırma sistemleri, video kamera, buzdolabı vb.'dir.

3.3 Bulanık (Fuzzy) Teori ile İlgili Temel Cebirsel Kavramlar

Tanım 3.1 [19] $\emptyset \neq X$ herhangi bir küme ve $A \subseteq X$ olmak üzere $\mu_A : X \rightarrow [0,1]$ fonksiyonunun karakterize ettiği

$$A = \{(x, \mu_A(x)) : x \in X\}$$

kümesine X 'de bir **bulanık (fuzzy)** küme denir. μ_A fonksiyonuna A bulanık kümesinin **üyelik fonksiyonu**, her $x \in X$ için $\mu_A(x) \in [0,1]$ değerine de x elemanının A kümesindeki **üyelik değeri** denir.

$\mu_A : X \rightarrow [0,1]$ şeklindeki tüm fonksiyonların kümesi $[0,1]^X$ ile gösterilir. $[0,1]^X$ ailesinin her bir elemanına X 'de bir bulanık küme denir.

Tanım 3.2 [19] $X = \{x_1, x_2, x_3, \dots\}$ olmak üzere, $X = \{(x_1, 1), (x_2, 1), (x_3, 1), \dots\}$ kümesi bir bulanık kümedir.

Tanım 3.3 [19] $\emptyset = \{(x_1, 0), (x_2, 0), (x_3, 0), \dots\}$ kümesi bir bulanık kümedir.

Tanım 3.4 [19] A ve B , X kümesinde iki bulanık küme olmak üzere, her $x \in X$ için, $\mu_A(x) = \mu_B(x)$ ise A ve B bulanık kümeleri eşittir.

Tanım 3.5 [19] A ve B , X kümesinde iki bulanık küme olmak üzere, $A \cap B$ kümesi, $\mu_{A \cap B}(x) = \min \{\mu_A(x), \mu_B(x)\}$

şeklinde tanımlanır.

Tanım 3.6 [19] A ve B , X kümesinde iki bulanık küme olmak üzere, $A \cup B$ kümesi, $\mu_{A \cup B}(x) = \max \{\mu_A(x), \mu_B(x)\}$

şeklinde tanımlanır.

Tanım 3.7 [19] A ve B , X kümesinde iki bulanık küme olmak üzere,

$A \subseteq B$ olması için gerek ve yeter koşul $\mu_A \leq \mu_B$ olmasıdır.

3.4 Bulanık Kümeler ile İlgili Alternatif Tanımlar

Bu kısımda, Kısım 3.3'de verilen tanımlara alternatif olan tanımlar verilmektedir.

3.4.1 Bulanık Alt Kümeler

Tanım 3.8 [27] $\emptyset \neq X$ herhangi bir küme olmak üzere $\mu : X \rightarrow [0,1]$ şeklinde tanımlanan fonksiyona X 'in bir **bulanık alt kümesi** denir.

X 'in bütün bulanık alt kümelerinin oluşturduğu kümeye X 'in **bulanık kuvvet kümesi** denir ve $[0,1]^X$ şeklinde gösterilir.

Tanım 3.9 [27] $\mu \in [0,1]^X$ olmak üzere,

$$\mu(X) = \text{Im}(\mu) = \{\mu(x) : x \in X\}$$

kümesine μ 'nün **görüntü kümesi** denir.

Tanım 3.10 [27] $\mu \in [0,1]^X$ olmak üzere,

$$\mu^* = \{x \in X : \mu(x) > 0\}$$

kümesine μ 'nün **desteği** (support) denir.

Eğer $1 \in \mu(X)$ ise, μ 'ye X 'in **normal bulanık alt kümesi** denir. μ^* sonlu ise μ sonlu bulanık küme, μ^* sonsuz ise μ sonsuz bulanık kümedir.

Tanım 3.11 [27] $Z \subseteq X$ ve $a \in [0,1]$ olmak üzere $a_Z \in [0,1]^X$ bulanık kümesi aşağıdaki şekilde tanımlanır:

$$a_Z(x) = \begin{cases} a, & x \in Z \\ 0, & x \in X \setminus Z \end{cases}.$$

Eğer $Z = \{z\}$ şeklinde ise, $a_{\{z\}}$ fonksiyonuna **bulanık-nokta (fuzzy-singleton)** denir.

$$a = 1 \text{ için } 1_Z = \begin{cases} 1, & x \in Z \\ 0, & x \in X \setminus Z \end{cases}$$

fonksiyonuna Z 'nin **karakteristik fonksiyonu** denir.

Tanım 3.12 [27] $\mu, \nu \in [0,1]^X$ olmak üzere her $x \in X$ için $\mu(x) \leq \nu(x)$ ise ν bulanık kümesi μ bulanık kümesini kapsar denir ve $\mu \subseteq \nu$ şeklinde gösterilir.

Tanım 3.13 [27] $\mu, \nu \in [0,1]^X$ olmak üzere $\mu \cup \nu$ ve $\mu \cap \nu \in [0,1]^X$ kümeleri aşağıdaki şekilde tanımlanır. Her $x \in X$ için,

$$(\mu \cup \nu)(x) = \max\{\mu(x), \nu(x)\} = \mu(x) \vee \nu(x),$$

$$(\mu \cap \nu)(x) = \min\{\mu(x), \nu(x)\} = \mu(x) \wedge \nu(x),$$

dir.

Yukarıdaki kesişim ve birleşim işlemleri ikiden çok bulanık küme için genelleştirilebilir:

$\{\mu_i : i \in I\}$, X in bulanık alt kümelerinin bir ailesi olsun. Her $x \in X$ için,

$$\left(\bigcup_{i \in I} \mu_i \right)(x) = \bigvee_{i \in I} \mu_i(x),$$

$$\left(\bigcap_{i \in I} \mu_i \right)(x) = \bigwedge_{i \in I} \mu_i(x),$$

olur.

Tanım 3.14 [27] $\mu \in [0,1]^X$ ve $a \in [0,1]$ olmak üzere,

$$\mu_a = \{x \in X : \mu(x) \geq a\}$$

kümesine μ nün **seviye alt kümesi** (level-set) ya da μ nün a – **kesimi** (a – cut) denir.

Teorem 3.15 [27] $\mu, \nu \in [0,1]^X$ olmak üzere, aşağıdaki ifadeler sağlanır:

1. $\mu \subseteq \nu, \quad a \in [0,1] \Rightarrow \mu_a \subseteq \nu_a,$
2. $a \leq b, \quad a, b \in [0,1] \Rightarrow \mu_b \subseteq \mu_a,$
3. $\mu = \nu \Leftrightarrow \mu_a = \nu_a, \quad \forall a \in [0,1].$

İspat [27]:

1. $\mu \subseteq \nu$ olsun. Buradan $\forall x \in X$ için, $\mu(x) \leq \nu(x)$ olur. $a \in [0,1]$, $y \in \mu_a$ için $\mu(y) \geq a$ 'dır. Böylece $\nu(y) \geq \mu(y) \geq a$ olur ve bu ifadeden de $y \in \nu_a$ elde edilir. Yani, $\mu_a \subseteq \nu_a$ 'dır.
2. $a, b \in [0,1]$ için $x \in \mu_b$ alalım. Buradan $\mu(x) \geq b$ olur. Ayrıca $a \leq b$ olduğundan; $a \leq b \leq \mu(x)$ olur ki bu da $x \in \mu_a$ demektir. Yani, $\mu_b \subseteq \mu_a$ elde edilir.

3. $a \in [0,1]$ için $x \in \mu_a$ alalım, buradan $\mu(x) \geq a$ elde edilir. $\mu = \nu$ olduğundan, her $x \in X$ için $\mu(x) = \nu(x) \geq a$ yani $x \in \nu_a$ elde edilir. Böylece $\mu_a \subseteq \nu_a$ olur. Benzer şekilde, $\nu_a \subseteq \mu_a$ olduğu gösterilebilir. Bu iki durumdan $\mu_a = \nu_a$ elde edilir. $\square$

Tersine $a \in [0,1]$ için $\mu_a = \nu_a$ olsun. Her $x \in X$ için $\mu(x) = \nu(x) \geq a$ ve $\mu = \nu$ elde edilir.

Tanım 3.16 [27] X ve Y herhangi iki küme, $\mu \in [0,1]^X$, $\nu \in [0,1]^Y$ ve f de $f: X \rightarrow Y$ şeklinde bir fonksiyon olsun. $f(\mu) \in [0,1]^Y$ ve $f^{-1}(\nu) \in [0,1]^X$ bulanık kümeleri aşağıdaki şekilde tanımlanır:

Her $y \in Y$ için,

$$f(\mu)(y) = \begin{cases} \max \{ \mu(x) : x \in X, f(x) = y \}, & f^{-1}(y) \neq \emptyset \\ 0, & f^{-1}(y) = \emptyset, \end{cases}$$

her $x \in X$ için,

$$f^{-1}(\nu)(x) = \nu f(x)$$

şeklindedir. Bu fonksiyonlara sırasıyla f 'in μ altındaki görüntüsü ve f 'in ν altındaki ters görüntüsü denir.

3.4.2 Bulanık Alt Gruplar

Tanım 3.17 [27] G bir grup ve $\mu: G \rightarrow [0,1]$ dönüşümü aşağıdaki iki koşulu sağlıyor ise, μ 'ye G 'nin bir **bulanık alt grubu** denir:

1. Her $x, y \in G$ için, $\mu(xy) \geq \min\{\mu(x), \mu(y)\}$,
2. Her $x \in G$ için, $\mu(x^{-1}) \geq \mu(x)$.

G 'nin tüm bulanık alt gruplarının kümesi, $[0,1] = I$ olmak üzere, $I(G)$ ile gösterilir.

Teorem 3.18 [27] $\mu \in I(G)$ olsun. Her $x \in G$ için,

1. $\mu(e) \geq \mu(x)$,

$$2. \quad \mu(x) = \mu(x^{-1})$$

şeklindedir.

Teorem 3.19 [27] G bir grup ve $\mu \in [0,1]^G$ olsun. μ 'nün G grubunun bulanık alt grubu olması için gerek ve yeter koşul, her $a \in [0,1]$ olmak üzere, μ_a 'nın G 'nin alt grubu olmasıdır.

Bulanık Alt Gruplar ile İlgili Örnekler

1. $\mathbb{Z}_2 = \{0,1\}$ kümesi toplamsal bir gruptur. $\mu: \mathbb{Z}_2 \rightarrow [0,1]$ bulanık alt kümesi, $\mu(0) = 1$ ve $\mu(1) = t \in [0,1]$ koşulları altında, $\mathbb{Z}_2$ 'nin bir bulanık alt grubudur.

2. $\mathbb{Z}_4 = \{0,1,2,3\}$ kümesi toplamsal bir gruptur. $\mu: \mathbb{Z}_4 \rightarrow [0,1]$ bulanık alt kümesi, $\mu(1) = \mu(3) = \frac{1}{3}$; $\mu(2) = \frac{1}{2}$; $\mu(0) = 1$ koşulları altında, $\mathbb{Z}_4$ 'ün bir bulanık alt grubudur.

3. $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$ kümesi toplamsal bir gruptur. $\mu: \mathbb{Z}_2 \times \mathbb{Z}_2 \rightarrow [0,1]$ bulanık alt kümesi, $\mu((0,1)) = \mu((1,0)) = \frac{1}{3}$; $\mu((1,1)) = \frac{1}{2}$; $\mu((0,0)) = 1$ koşulları altında, $\mathbb{Z}_2 \times \mathbb{Z}_2$ 'nin bir bulanık alt grubudur.

4. p asal ve $\mathbb{Z}_p = \{0,1,2,\dots,p-1\}$ olmak üzere, $\mu: \mathbb{Z}_p \rightarrow [0,1]$ bulanık alt kümesi, her $x \in \mathbb{Z}_p$ için, $\mu(0) = 1$ ve $\mu(x) = t \in [0,1]$ koşulları altında, $\mathbb{Z}_p$ 'nin bir bulanık alt grubudur.

5. $G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \right\}$ kümesi bilinen standart çarpma işlemine göre bir gruptur. $\mu: G \rightarrow [0,1]$ kümesi,

$\mu\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = 1$, $\mu\left(\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}\right) = \mu\left(\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}\right) = \frac{1}{3}$ koşulları altında, G 'nin bir bulanık alt grubudur.

Yukarıdaki 5 örnekte de bulanık alt grup olma koşullarının sağlandığı açıktır:

Her $x, y \in G$ için, $\mu(xy) \geq \min\{\mu(x), \mu(y)\}$, her $x \in G$ için, $\mu(x^{-1}) \geq \mu(x)$.

3.4.3 Bulanık Alt Halkalar

Tanım 3.20 [27] R değişmeli bir halka ve $\mu, \nu \in [0,1]^R$ olsun. “*” işlemi, R halkası üzerinde aşağıdaki şekilde tanımlanır:

$$(\mu * \nu)(x) = \max\{\min\{\mu(y), \nu(z)\} : y, z \in R, y * z = x\}.$$

Ayrıca,

$$(-\mu)(x) = \mu(-x)$$

şeklinde tanımlanan μ bulanık kümesine ise μ ’nün negatifi denir.

Tanım 3.21 [27] R değişmeli bir halka ve $\mu \in [0,1]^R$ olsun. Aşağıdaki iki koşulu sağlayan μ bulanık alt kümesine R ’nin bir **bulanık alt halkası** denir:

1. Her $x, y \in R$ için, $\mu(x - y) \geq \min\{\mu(x), \mu(y)\}$,
2. Her $x, y \in R$ için, $\mu(xy) \geq \min\{\mu(x), \mu(y)\}$.

Tanım 3.22 [27] R değişmeli bir halka ve $\mu \in [0,1]^R$ olsun. Aşağıdaki iki koşulu sağlayan μ bulanık alt kümesine R ’nin bir **bulanık ideali** denir:

1. Her $x, y \in R$ için, $\mu(x - y) \geq \min\{\mu(x), \mu(y)\}$,
2. Her $x, y \in R$ için, $\mu(xy) \geq \max\{\mu(x), \mu(y)\}$.

Teorem 3.23 [27] μ , R halkasının bir bulanık alt halkası olsun. μ ’nün bulanık ideal olması için gerek ve yeter koşul, her $a \in \mu(R) \cup \{b \in [0,1] : b \leq \mu(0)\}$ olmak üzere, μ_a ’nın R halkasının bir ideali olmasıdır.

Örnek 3.24 $\mathbb{Z}_4 = \{0,1,2,3\}$ kümesi toplama ve çarpma işlemleri altında bir halkadır.

$\mu: \mathbb{Z}_4 \rightarrow [0,1]$ bulanık alt kümesi, $\mu(1) = \mu(3) = \frac{1}{3}$; $\mu(2) = \frac{1}{2}$; $\mu(0) = 1$ koşulları

altında, $\mathbb{Z}_4$ ’ün bir bulanık alt halkasıdır, aynı zamanda $\mathbb{Z}_4$ ’ün bir bulanık idealidir.

Tanım 3.25 [27] F bir cisim olsun. μ , F toplamsal grubunun ve F çarpımsal grubunun bulanık alt grubu ve $\mu(1) = 1$ ise μ 'ye F 'nin **bulanık alt cismi** denir.

Örnek 3.26 $\mathbb{Z}_2 = \{0,1\}$ kümesi bir cisimdir. $\mu: \mathbb{Z}_2 \rightarrow [0,1]$ bulanık alt kümesi $\mu(0) = \mu(1) = 1$ koşulu altında, $\mathbb{Z}_2$ 'nin bir bulanık alt cismidir.

SONLU ABEL GRUPLARI, MAKSİMAL ZİNCİRLER, BULANIK ALT GRUPLAR
4.1 Giriş

Bu bölümde, ilk olarak Grup Teori'nin önemli konularından biri olan sonlu Abel gruplarına ilişkin temel tanım ve teoremler verilmektedir. Daha sonra bulanık alt grupları kolaylıkla belirlemeye yarayan maksimal zincirler konusu ele alınacak ve bu zincirler vasıtasıyla bulanık alt gruplar belirlenecektir.

Tanım 4.1 [28,29,30] $0 \leq i < m$ için $G_i < G_{i+1}$ ve $G_{i+1} \setminus G_i$ grubu bir Abel grubu iken, G 'nin alt grupları $\{0\} = G_0 \subset G_1 \subset G_2 \subset \dots \subset G_m = G$ şartını sağlıyor ise G 'ye **çözülebilir** (solvable) **grup** denir.

Abel grupları çözülebilir gruplardır. Mertebesi asal bir sayının kuvveti şeklinde olan her grup çözülebilir bir gruptur.

Tanım 4.2 [28,29,30] Bütün elemanlarının mertebesi bir p asal sayısının bir kuvveti şeklinde olan bir gruba **p -grup** denir.

Teorem 4.3 [28,29,30] Her sonlu Abel grubu, mertebesi bir p asal sayısının bir kuvveti şeklinde olan devirli grupların direkt çarpımı olarak yazılabilir. Yani, her sonlu G Abel grubu $\mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \dots \times \mathbb{Z}_{p_k^{n_k}}$ formundaki bir gruba izomorftur; burada, $n_i (i=1,2,\dots,k) \in \mathbb{Z}^+$, p_i sayıları farklı olması gerekmeyen asal sayılardır ve $p_i^{n_i}$ sayıları da G tarafından tek türlü belirlidir.

Tanım 4.4 [28,29,30] $(G, +)$ bir grup ve G grubunun aşağıdaki şekilde verilen G_i alt grupları ele alınsın:

$$G_0 \subset G_1 \subset G_2 \subset \dots \subset G_n, \quad G_0 = \{0\}, \quad G_n = G.$$

Yukarıdaki zincire $i = 0, \dots, n$ olmak üzere G_i alt gruplarının bir **maksimal zinciri** denir.

Bir maksimal zincir tek türlü belirlidir.

Tanım 4.5 [28,29,30] $i = 0, \dots, n$ ve $\lambda_i \in [0,1]$ olsun. Burada, her bir G_i 'ye bir λ_i ($i = 0, \dots, n$) karşılık gelmek üzere,

$$1 = \lambda_0 \geq \lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n \geq 0$$

zincirine bir **anahtar zincir (keychain)** denir. Her bir λ_i 'ye de **üyelik değeri (pin)** denir.

Bir anahtar zincir muhakkak λ_0 sayısını içerir. 1 sayısı birinci pozisyonda; λ_i sayısı da $(i+1)$. pozisyonda yer alır ($i = 1, 2, \dots, n$). Dolayısıyla bir n -zincirin $(n+1)$ adet yeri vardır. Bu durumda, bir n -zincirin uzunluğunun $n+1$ olduğu söylenir.

Bir maksimal zincirle anahtar zincir aşağıdaki şekilde birleştirilebilir:

$$G_0 = \mu_{\lambda_0}, \quad G_1 = \mu_{\lambda_1}, \quad G_2 = \mu_{\lambda_2}, \dots, \quad G_n = \mu_{\lambda_n} \text{ olmak üzere,}$$

$$\{0\}^1 \subset G_1^{\lambda_1} \subset G_2^{\lambda_2} \subset \dots \subset G_n^{\lambda_n}$$

şeklinde bir zincir elde edilir.

Örnek 4.6 [28,29,30] $\lambda_0 = 1 > \frac{1}{2} > \frac{1}{4} > \frac{1}{8}$ anahtar zinciri $\{0\} \subset \langle 4 \rangle \subset \langle 2 \rangle \subset \langle 1 \rangle = \mathbb{Z}_8$

maksimal zinciri ile birleştirilirse,

$$\{0\}^1 \subset \langle 4 \rangle^{\frac{1}{2}} \subset \langle 2 \rangle^{\frac{1}{4}} \subset \langle 1 \rangle^{\frac{1}{8}} = \mathbb{Z}_8^{\frac{1}{8}}$$

zinciri elde edilir.

$$\mu: \mathbb{Z}_8 \rightarrow [0,1]; \quad \mu(0) = 1, \quad \mu(1) = \mu(3) = \mu(5) = \mu(7) = \frac{1}{3}, \quad \mu(2) = \mu(6) = \frac{1}{2} \text{ olmak}$$

üzere, μ bulanık alt grubunu düşünelim. Bu durumda μ 'nün seviye alt kümeleri aşağıdaki gibidir:

$$\mu_1 = \{0\} = \langle 0 \rangle, \quad \mu_{\frac{1}{2}} = \{0, 4\} = \langle 4 \rangle, \quad \mu_{\frac{1}{4}} = \{0, 2, 4, 6\} = \langle 2 \rangle, \quad \mu_{\frac{1}{8}} = \{0, 1, 2, 3, 4, 5, 6\} = \mathbb{Z}_8.$$

Tanım 4.7 [28,29,30] $G_0^{\lambda_0} \subset G_1^{\lambda_1} \subset \dots \subset G_n^{\lambda_n}$, $(\lambda_0=1)$ şeklindeki bir zincir ile birleştirilmiş bir bulanık alt küme aşağıdaki şekilde gösterilir:

$$\mu(x) = \begin{cases} 1, & x = 0 \\ \lambda_1, & x \in G_1 \setminus \{0\} \\ \lambda_2, & x \in G_2 \setminus G_1 \\ \vdots & \vdots \\ \lambda_n, & x \in G_n \setminus G_{n-1}. \end{cases} \quad (4.1)$$

Önerme 4.8 [28,29,30] (4.1)'de verilen bulanık alt küme bir bulanık alt gruptur.

İspat: $a, b \in G$ için $a \in G_i \setminus G_{i-1}$ ve $b \in G_j \setminus G_{j-1}$ olacak şekilde i, j ($1 \leq i \leq j \leq n$) indisleri vardır. $a, b \in G_j$ alınırsa $a+b \in G_j$ olur ve buradan da $\mu(a+b) \geq \lambda_j$ elde edilir. Fakat $\lambda_j \geq \lambda_i \wedge \lambda_j$ olduğundan, $\mu(a+b) \geq \mu(a) \wedge \mu(b)$ olur. Öte yandan $a \in G$ için, $a \in G_i \setminus G_{i-1}$ olacak şekilde i indisi vardır. $-a \in G_i$ olduğundan, bir i için $\mu(a) = \lambda_i \geq \mu(-a)$ dir. Ayrıca, her $a \in G$ için $\mu(0) \geq \mu(a)$ dir. Böylece μ bir bulanık alt gruptur. $\square$

Önerme 4.8'in tersi de doğrudur. Bir G grubunun bir μ bulanık alt grubu verildiğinde, μ , (4.1)'deki gibi yazılarak, ilgili anahtar zincir ile buna karşılık gelen maksimal zincir yazılabilir.

Örnek 4.9 [28,29,30] $\mathbb{Z}_8 = \{0,1,2,3,4,5,6,7\}$ kümesi toplamsal bir gruptur.

$\mu: \mathbb{Z}_8 \rightarrow [0,1]$ bulanık alt kümesi Tanım 3.17'den,

$$\mu(0)=1, \quad \mu(1)=\frac{1}{2}, \quad \mu(2)=\mu(6)=\frac{1}{4}, \quad \mu(3)=\mu(5)=\mu(7)=\frac{1}{8}$$

koşulları altında, $\mathbb{Z}_8$ in bir bulanık alt grubudur.

Öte yandan, Tanım 4.7'den,

$$\{0\}^1 \subset \langle 4 \rangle^{\frac{1}{2}} \subset \langle 2 \rangle^{\frac{1}{4}} \subset \langle 1 \rangle^{\frac{1}{8}} = \mathbb{Z}_8^{\frac{1}{8}} \text{ zinciri ile birleştirilmiş bulanık alt küme;}$$

$$\mu(x) = \begin{cases} 1, & x = 0 \\ \frac{1}{2}, & x \in \langle 4 \rangle \setminus \{0\} \\ \frac{1}{4}, & x \in \langle 2 \rangle \setminus \langle 4 \rangle \\ \frac{1}{8}, & x \in \mathbb{Z}_8 \setminus \langle 2 \rangle. \end{cases} \quad (4.2)$$

şeklinde gösterilir ve Önerme 4.8'den, bu bulanık alt küme bir bulanık alt gruptur.

Önerme 4.10 [28,29,30] μ , G 'nin bir bulanık alt grubu olsun ve G 'nin alt gruplarının bir maksimal zinciri aşağıdaki gibi verilsin:

$$G_0^{\lambda_0} \subset G_1^{\lambda_1} \subset \dots \subset G_n^{\lambda_n}.$$

Bu durumda, yukarıdaki maksimal zincir ile birleştirilmiş μ bulanık alt grubu aşağıdaki şekilde verilir:

$$\mu(x) = \begin{cases} 1, & x = 0 \\ \lambda_1, & x \in G_1 \setminus \{0\} \\ \lambda_2, & x \in G_2 \setminus G_1 \\ \vdots & \vdots \\ \lambda_n, & x \in G_n \setminus G_{n-1}. \end{cases} \quad (4.3)$$

Örnek 4.11 [28,29,30] $\{0\}^1 \subset \langle 4 \rangle^{\frac{1}{2}} \subset \langle 2 \rangle^{\frac{1}{4}} \subset \langle 1 \rangle^{\frac{1}{8}} = \mathbb{Z}_8^{\frac{1}{8}}$ maksimal zinciri aşağıdaki şekilde yazılır:

$$\mu(x) = \begin{cases} 1, & x = 0 \\ \frac{1}{2}, & x \in \langle 4 \rangle \setminus \{0\} \\ \frac{1}{4}, & x \in \langle 2 \rangle \setminus \langle 4 \rangle \\ \frac{1}{8}, & x \in \mathbb{Z}_8 \setminus \langle 2 \rangle. \end{cases} \quad (4.4)$$

μ , $\mathbb{Z}_8$ 'in bir bulanık alt grubudur.

Bulanık alt grupların sayılarını hesaplamak için ilk olarak maksimal zincir sayılarını hesaplamak gerekir.

4.2 Abel p – Gruplarının Alt Grupları, Maksimal Zincirleri ve Bulanık Alt Grupları

Tanım 4.12 [4,28] λ_i , $(i = 0, \dots, n)$, sayılarının $1 = \lambda_0 > \lambda_1 > \dots > \lambda_n > 0$ şeklindeki sıralanışına bir n -**zincir** denir. $1 = \lambda_0 \geq \lambda_1 \geq \dots \geq \lambda_n \geq 0$ şeklindeki bir n – zincire **anahtar zincir** (keychain) denir. Bir anahtar zincir basitçe $1\lambda_1\lambda_2\dots\lambda_n$ şeklinde yazılır. Art arda birbirine eşit olan λ ’ların birbirine bağlı olduğu söylenir (en baştaki 1 ihmal edilir). Birbirine bağlı üyelik değerlerine **bileşen** denir. k farklı bileşen içeren bir zincire bir **k ’lı anahtar zincir** (k – pad) denir. Bileşen şeklindeki λ ’ların sayısının kümesine **k ’lı anahtar zincirin içeriği** (indeksi) denir. İndekste tekli bileşenler kolaylık sağlama açısından yazılmaz.

Örnek 4.13 [4,28] $1 > \lambda_1 = \lambda_2 > \lambda_3 = \lambda_4 = \lambda_5 > \lambda_6 > 0$ şeklinde verilen bir 7 – zincir, bir 4 parçalı anahtar zincirdir (4 – pad keychain). İndeksi ise $(2, 3, 1, 1) = (2, 3)$ şeklindedir.

$$\lambda_1 = \lambda_2 = \lambda, \quad \lambda_3 = \lambda_4 = \lambda_5 = \beta, \quad \lambda_6 = \gamma$$

olmak üzere,

$$G_0^{\lambda_0} \subset G_1^{\lambda_1} \subset G_2^{\lambda_2} \subset G_3^{\lambda_3} \subset G_4^{\lambda_4} \subset G_5^{\lambda_5} \subset G_6^{\lambda_6} \subset G_7^{\lambda_7}$$

zincirinin bir 4 parçalı anahtar zincir olduğu görülür. Bu zincirden aşağıdaki bulanık alt grup elde edilir:

$$\mu(x) = \begin{cases} 1, & x = 0 \\ \lambda, & x \in G_2 \setminus \{0\} \\ \beta, & x \in G_5 \setminus G_2 \\ \gamma, & x \in G_6 \setminus G_5 \\ 0, & x \in G_n \setminus G_{n-1}. \end{cases} \quad (4.5)$$

Örnek 4.14 [4,28] $1 = \lambda_1 = \lambda_2 = \lambda_3 > \lambda_4 > \lambda_5 = \lambda_6 = \lambda_7$, 7 – zinciri bir 3 parçalı anahtar zincirdir (3 – pad keychain), indeksi $(3, 1, 3) = (3, 3)$ şeklindedir.

$$\lambda_1 = \lambda_2 = \lambda_3 = 1, \quad \lambda_4 = \lambda, \quad \lambda_5 = \lambda_6 = \lambda_7 = \beta \text{ olmak üzere,}$$

$$G_0^{\lambda_0} \subset G_1^{\lambda_1} \subset G_2^{\lambda_2} \subset G_3^{\lambda_3} \subset G_4^{\lambda_4} \subset G_5^{\lambda_5} \subset G_6^{\lambda_6} \subset G_7^{\lambda_7}$$

7 – zinciri bir 3 parçalı anahtar anahtar zincirdir (3 – pad keychain).

zincirinden aşağıdaki bulanık alt grup elde edilir:

$$\mu(x) = \begin{cases} 1, & x \in G_3 \setminus \{0\} \\ \lambda, & x \in G_4 \setminus G_3 \\ \beta, & x \in G_7 \setminus G_4. \end{cases} \quad (4.6)$$

Not 4.15 $n \geq 2$ için 3 adet 1 – pad anahtar zincir vardır ($\lambda_1 = \lambda_2 = \dots = \lambda_{n-1}$):

$$1 \underbrace{11\dots1}_{n-1}, \quad 1 \underbrace{\lambda\lambda\dots\lambda}_{n-1}, \quad 1 \underbrace{00\dots0}_{n-1}.$$

BAZI GRUPLARIN BULANIK ALT GRUPLARININ SAYISI

5.1 Giriş

Sonlu bir grubun bulanık alt gruplarını sayma problemi son zamanlarda üzerinde çalışılan konulardan biridir. Bu konu ile ilgili günümüze en yakın çalışmalar aşağıdaki gibi verilebilir:

- i. “On an equivalence of fuzzy subgroups I” [3] makalesinde uygun bir denklik bağıntısı altında sonlu Abel gruplarının ve p -grupların bulanık alt grup sayıları incelenmiştir.
- ii. “On an equivalence of fuzzy subgroups II” [4] çalışmasında, “On an equivalence of fuzzy subgroups I” makalesinin devamı olarak $\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \dots \times \mathbb{Z}_{p_n}$ grubuna izomorf olan grupların bulanık alt gruplarının sayısı indeks ve parçalar (pad) kullanılarak hesaplanmıştır.
- iii. “Counting the number of fuzzy subgroups of an Abelian group of order $p^n q^m$ ” [5] çalışmasında $\mathbb{Z}_{p^n} \times \mathbb{Z}_{q^m}$ Abel grubunun maksimal zincirleri ve bulanık alt gruplarının sayısı incelenmiştir.
- iv. 2005 (Ngcibi) yılında Rhodes Üniversitesi’nde yapılan “Studies of finite equivalent fuzzy subgroups of finite Abelian p -groups of rank two and their subgroup lattices” adlı doktora tezinde [28] Bulanık Teori’den geniş kapsamlı bir şekilde bahsedilmiştir. [28]’de, bazı Abel gruplarının $(\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^m}, (1 \leq m \leq 5))$ maksimal zincir sayıları ve bulanık alt gruplarının sayıları incelenmiştir.

5.2 Ön Bilgiler

Tezin ilerleyen bölüm ve kısımlarında, “ G ” ile değişmeli bir grup gösterilecektir.

Bu kısımda, Teorem 3.19’a vurgu yapmak için örnekle başlanmaktadır.

Örnek 5.1 [3,10] $\mu : \mathbb{Z}_8 \rightarrow [0,1]$ bulanık alt kümesi verilsin.

$$\mu(x) = \begin{cases} 1, & x = 0 \\ \frac{1}{2}, & x \in \langle 4 \rangle \setminus \{0\} \\ \frac{1}{4}, & x \in \langle 2 \rangle \setminus \langle 4 \rangle \\ \frac{1}{8}, & x \in \mathbb{Z}_8 \setminus \langle 2 \rangle \end{cases}$$

kümesi bir bulanık alt gruptur. Burada, $\mathbb{Z}_8$ grubunun bir maksimal zinciri, $\langle 0 \rangle \subset \langle 4 \rangle \subset \langle 2 \rangle \subset \langle 1 \rangle = \mathbb{Z}_8$ şeklindedir ve Teorem 3.19’dan,

$$\begin{aligned} \mu_{\frac{1}{8}} &= \mathbb{Z}_8, \\ \mu_{\frac{1}{4}} &= \langle 2 \rangle = \{0, 2, 4, 6\}, \\ \mu_{\frac{1}{2}} &= \langle 4 \rangle = \{0, 4\}, \\ \mu_1 &= \langle 0 \rangle = \{0\} \end{aligned}$$

kümelerinden her biri $\mathbb{Z}_8$ in alt grubudur. Burada, $\text{Im}(\mu) = 1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8} \in [0,1]$ dir.

Tanım 5.2 [3,10] (Bulanık alt gruplarda denklik) μ ve ν , G ’nin bulanık alt grupları olsun.

$$\begin{aligned} \mu \sim \nu &\Leftrightarrow (i) \forall x, y \in G; \mu(x) \geq \mu(y) \Leftrightarrow \nu(x) \geq \nu(y) \\ &\quad (ii) \forall x \in G; \mu(x) = 0 \Leftrightarrow \nu(x) = 0 \end{aligned}$$

şeklinde tanımlanan “ $\sim$ ” bağıntısı bir denklik bağıntısıdır.

Önerme 5.3 [3,10] μ ve ν iki bulanık alt grup olsun. Sırasıyla, μ ve ν ’ye karşılık gelen maksimal zincirler aşağıdaki şekilde verilsin:

$$X_0^1 \subset X_1^{\lambda_1} \subset X_2^{\lambda_2} \subset X_m^{\lambda_m} \text{ ve } Y_0^1 \subset Y_1^{\beta_1} \subset Y_2^{\beta_2} \subset Y_n^{\beta_n}.$$

Bu durumda $\mu \sim \nu$ olması için gerek ve yeter koşul aşağıdakilerin sağlanmasıdır:

- i. $n = m$,
- ii. $X_i = Y_i, i = 0, 1, \dots, n, \lambda_i$ ve β_j sayıları ayrık,
- iii. $\lambda_i > \lambda_j \Leftrightarrow \beta_i > \beta_j, 1 \leq i, j \leq n$.

Örnek 5.4 [3,10] $G = \mathbb{Z}_2^3 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ olmak üzere, μ ve ν , G 'nin bulanık alt grupları olsun:

$$\mu(x) = \begin{cases} 1, & x = \{0, 0, 0\} \\ \frac{1}{2}, & x \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \{0\} \setminus \{0, 0, 0\} \\ \frac{1}{3}, & \text{diğer durumlar} , \end{cases} \quad \nu(x) = \begin{cases} 1, & x = \{0, 0, 0\} \\ \frac{1}{3}, & x \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \{0\} \setminus \{0, 0, 0\} \\ \frac{1}{5}, & \text{diğer durumlar} . \end{cases}$$

Yukarıdaki bulanık alt gruplar denktir. Yani, $\mu \sim \nu$ 'dir.

Örnek 5.5 [3,10] $G = S_3 = \{(1), (123), (132), (12), (13), (23)\}$ permütasyon grubu, μ ve ν de S_3 grubunun bulanık alt grupları olsun:

$$\mu(x) = \begin{cases} 1, & x = e = (1) \\ \frac{1}{3}, & x = (12) \\ \frac{1}{5}, & \text{diğer durumlar} , \end{cases} \quad \nu(x) = \begin{cases} 1, & x = e = (1) \\ \frac{1}{3}, & x = (13) \\ \frac{1}{5}, & \text{diğer durumlar} . \end{cases}$$

Burada, $\text{Im}(\mu) = \text{Im}(\nu)$ ve $\mu^* = \nu^*$ 'dir. Ancak, $\mu((12)) > \mu((13))$ iken $\nu((12)) < \nu((13))$ olduğundan, μ ile ν denk değildir.

Önerme 5.6 [3,10] $n+1$ uzunluğunda bir maksimal zincirden elde edilen bulanık alt grupların $2^{n+1} - 1$ adet denklik sınıfı vardır.

Örnek 5.7 [3,10] $\mathbb{Z}_4$ grubunun $1 \geq \lambda \geq \beta$ anahtar zinciriyle birleştirilmiş zinciri aşağıdaki şekilde verilir:

$$\langle 0 \rangle^1 \subset \langle 2 \rangle^\lambda \subset \mathbb{Z}_4^\beta. \quad (5.1)$$

(5.1) ile verilen maksimal zincir $n+1=3$ uzunluğunda bir maksimal zincirdir ve bu maksimal zincirden Tanım 4.12'ye göre $1\lambda\beta$ şeklinde bulanık alt gruplar elde edilir:

$1 \geq \lambda \geq \beta = 111, 11\lambda, 110, 1\lambda\lambda, 1\lambda\beta, 1\lambda 0, 100$. Sayısı: $2^{n+1} - 1 = 2^3 - 1 = 7$ 'dir.

5.3 $\mathbb{Z}_p \times \mathbb{Z}_p \times \dots \times \mathbb{Z}_p = \mathbb{Z}_p^n$ Grubunun Bulanık Alt Gruplarının Sayısı

5.3.1 $\mathbb{Z}_p^n$ Grubunun Alt Gruplarının Maksimal Zincirlerinin Sayısı

Verilen sonlu bir grubun bulanık alt gruplarının sayısını hesaplamak için ilk olarak bu grubun maksimal zincirlerini gösteren alt grup şemasını (latisi) belirlemek gerekir. Bu şemaya "**Hasse şeması**" da denir. Hasse şemasından yararlanılarak, maksimal zincirlerin yapısı incelenebilir ve maksimal zincir sayıları belirlenir. Daha sonra ise bu zincirlerdeki bulanık alt grupların sayısı hesaplanabilir. Bu hesaplamalar için öncelikle bilinen Gauss binom katsayıları ile ilgili teorem; daha sonra ise verilen grubun bulanık alt gruplarının sayısının hesabı için ilgili önerme ve teoremler verilecektir.

Tanım 5.8 Alt grup latisi, bir grubun alt grupları arasındaki ilişkiyi açıklayan diyagramatik bir yaklaşımdır. Bir grubun tüm alt grupları bir latis diyagramında kapsanır. Bir seviyedeki H alt grubu daha yüksek seviyedeki K alt grubu ile ilişkilidir. Alt grup latisini çizmek için birçok yol vardır. Burada mühim olan tüm durumlarda alt gruplar arası ilişkinin aynı olmasıdır.

Verilen bir Abel grubunun alt grup latisini belirlemek zor bir problemdir. Bu problem grubu çarpanlarına parçalamakla daha basit hale gelir.

G , n . mertebeden bir grup olsun. G 'nin mertebesinin asal çarpanlara ayrılışı, $|G| = n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ şeklindedir. $G = G_{p_1} \times G_{p_2} \times \dots \times G_{p_k}$ olsun. Bu durumda G 'nin alt grup latisi ile her bir G_i 'nin ($i = p_1, p_2, \dots, p_k$) alt grup latisi arasında bire bir denklik vardır.

Tanım 5.9 [33] $b \neq 1$ ve n birer gerçel (reel) sayı ve k negatif olmayan bir tam sayı

olmak üzere, $\left[\begin{matrix} n \\ k \end{matrix} \right]_b$ Gauss binom katsayıları aşağıdaki şekilde tanımlanır:

$$\begin{bmatrix} n \\ k \end{bmatrix}_b = \frac{(b^n - 1)(b^{n-1} - 1) \dots (b^{n-k+1} - 1)}{(b^k - 1)(b^{k-1} - 1) \dots (b - 1)}.$$

Önerme 5.10 [33] Gauss binom katsayılarının bazı özellikleri aşağıdaki şekildedir:

$$1. \quad \lim_{b \rightarrow 1} \begin{bmatrix} n \\ k \end{bmatrix}_b = \binom{n}{k}.$$

$$2. \quad \begin{bmatrix} n \\ k \end{bmatrix}_b = \begin{bmatrix} n \\ n-k \end{bmatrix}_b.$$

$$3. \quad \begin{bmatrix} n \\ n \end{bmatrix}_b = \begin{bmatrix} n \\ 0 \end{bmatrix}_b = 1.$$

$$4. \quad \begin{bmatrix} n \\ k \end{bmatrix}_b = \begin{bmatrix} n-1 \\ k \end{bmatrix}_b + b^{n-k} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_b.$$

$$5. \quad \begin{bmatrix} n \\ k \end{bmatrix}_b = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_b + b^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_b.$$

$$6. \quad [0]_b = 1 \text{ ve } [n]_b = (b^n - 1)(b^{n-1} - 1) \dots (b - 1), \quad n = 1, 2, \dots \text{ olarak tanımlanırsa,}$$

$$\begin{bmatrix} n \\ k \end{bmatrix}_b = \frac{[n]_b}{[k]_b [n-k]_b} \text{ elde edilir.}$$

Teorem 5.11 [31] F_q üzerinde, n boyutlu bir vektör uzayının k boyutlu alt uzaylarının

sayısı $\begin{bmatrix} n \\ k \end{bmatrix}_q$ Gauss binom katsayısıdır.

Önerme 5.12 $\mathbb{Z}_p^n$ grubunun alt gruplarının maksimal zincirlerinin sayısı

$$\prod_{i=1}^{n-1} \begin{bmatrix} i+1 \\ i \end{bmatrix}_p \text{ sayıdır.}$$

İspat: G grubunun vektör uzayı olarak boyutu k olsun. Bu durumda, G grubunun alt gruplarının Hasse şeması açık olarak Şekil 5.1'deki gibi belirlenir. Burada, G 'nin bir boyut altında bulunan $G_1, G_2, \dots, G_{C_p(k,k-1)}$ alt grupları $k-1$ boyutludur ve $k-1$ boyutlu grupların altında $k-2$ boyutlu alt gruplar bulunmakta, şemanın en alt kısmında ise en

az elemanlı alt grup olan, aşikar alt grup, $G_0 = \{0\}$ grubu yer almaktadır. Burada, en soldan başlanmak üzere, maksimal zincirlerin yapıları ve sayıları belirlenecektir.

G sonlu bir Abel p -grubu olsun. Vektör uzayı olarak (k boyutlu), $k-1$ boyutlu alt uzaylarının sayısı $\begin{bmatrix} k \\ k-1 \end{bmatrix}_p$ Gauss binom katsayısıdır. $k-1$ boyutlu alt uzayların $k-2$

boyutlu alt uzaylarının sayısı ise $\begin{bmatrix} k-1 \\ k-2 \end{bmatrix}_p$ Gauss binom katsayısıdır. Benzer şekilde

devam edilirse, 2 boyutlu alt uzayların 1 boyutlu alt uzaylarının sayısı elde edilir:

$\begin{bmatrix} 2 \\ 1 \end{bmatrix}_p$. Bu durum, G 'nin Hasse şemasında, Şekil 5.1'deki gibi gösterilebilir. Bu şemada,

maksimal zincirlerin daha net görülmesi açısından kesişimler gösterilmemiştir. Ayrıca, en soldaki grupların alt grupları açıkça gösterilmiş, aynı hizadakilerin (aynı yatay sıradaki gruplar) alt grup sayıları aynı olacağından, yalnızca bir grubun alt grupları gösterilmiş, diğerlerini göstermeye gerek görülmemiştir. Bu açıklamalardan sonra, Şekil 5.1'den, tüm maksimal zincirlerin sayısı,

$$\begin{bmatrix} k \\ k-1 \end{bmatrix}_p \begin{bmatrix} k-1 \\ k-2 \end{bmatrix}_p \cdots \begin{bmatrix} 3 \\ 2 \end{bmatrix}_p \begin{bmatrix} 2 \\ 1 \end{bmatrix}_p = \prod_{i=1}^{k-1} \begin{bmatrix} i+1 \\ i \end{bmatrix}_p$$

olarak belirlenir.

Burada $k = n$ için, maksimal zincirlerin sayısı $\prod_{i=1}^{n-1} \begin{bmatrix} i+1 \\ i \end{bmatrix}_p$ dir.

Kolaylık olması bakımından, 1 boyutlu alt gruplar $\begin{bmatrix} 2 \\ 1 \end{bmatrix}_p$ gruplara ayrılmıştır. Dolayısıyla

alt grup şemasının en altındaki $\begin{bmatrix} 2 \\ 1 \end{bmatrix}_p$ adet maksimal zincir, tek zincir olarak

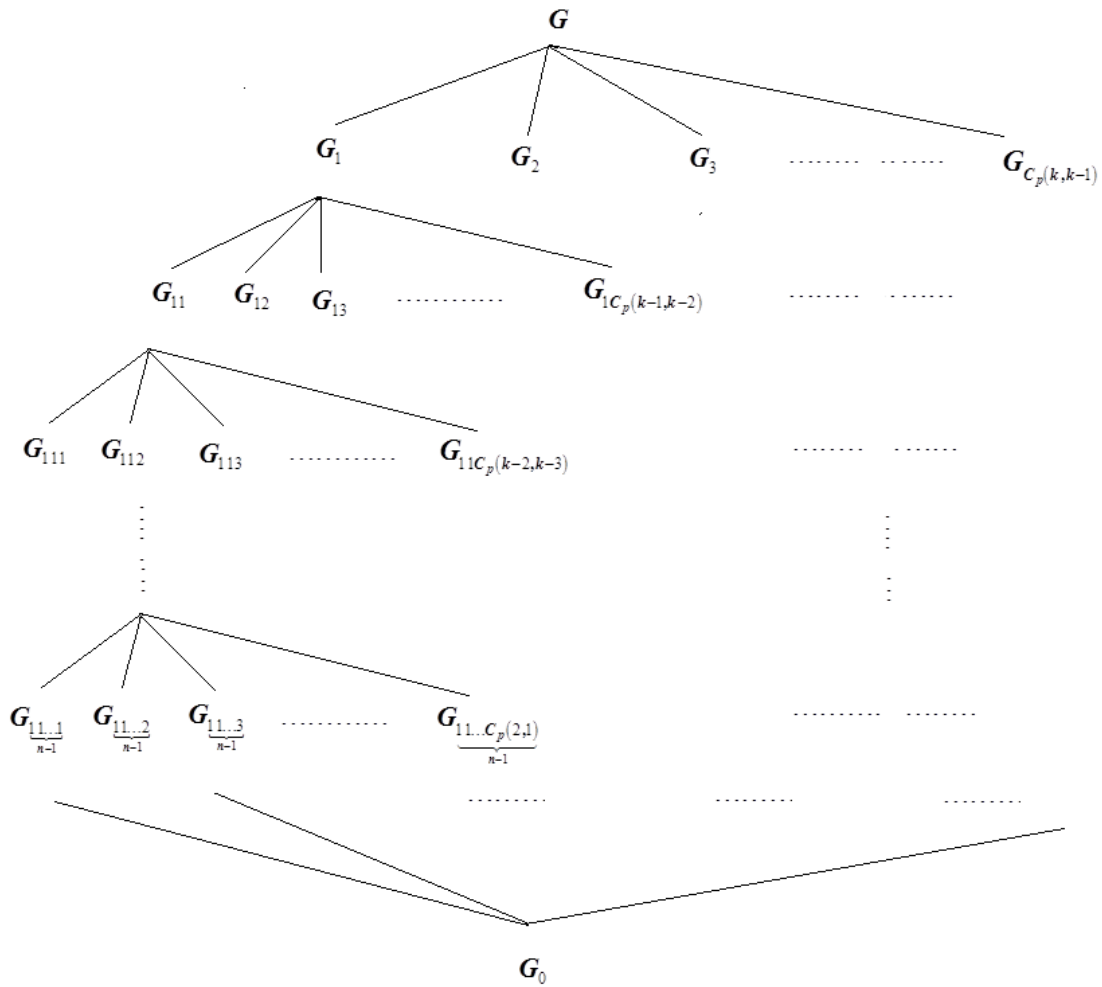
düşünülecektir. Dolayısıyla maksimal zincirlerin sayısına en alttakiler dahil edilmemiştir,

yani maksimal zincirlerin sayısı $\prod_{i=2}^{n-1} \begin{bmatrix} i+1 \\ i \end{bmatrix}_p$ olarak alınmıştır.

Önerme 5.6'dan, $n+1$ uzunluğunda bir maksimal zincirin bulanık alt gruplarının $2^{n+1} - 1$ adet denklik sınıfı olduğu biliniyor. Fakat bir grubun alt grup şemasından alınan

iki maksimal zincirden elde edilen bulanık alt grupların sayısı, $2^{n+1} - 1$ sayısının iki katı değildir. Çünkü iki zincirden elde edilen bulanık alt gruplardan, tanımlanan denkleğe göre, denk olan bulanık alt gruplar vardır. Örneğin [3] çalışmasında tanımlanan ve bu tezde kullanılan denkleğe göre, herhangi iki zincir karşılaştırıldığında en azından 3 adet denk bulanık alt grup vardır. Bunlar: $11\dots 1$, $00\dots 0$, $1\lambda\lambda\dots\lambda$ bulanık alt gruplarıdır.

Şekil 5.1’de, $C_p(n, k) = \begin{bmatrix} n \\ k \end{bmatrix}_p$ şeklindedir.



Şekil 5. 1 Bir G grubunun Hasse şeması

5.3.2 $\mathbb{Z}_p^n$ Grubunun Bulanık Alt Gruplarının Sayısı

Teorem 5.12 $\mathbb{Z}_p^n$ grubunun ayık bulanık alt gruplarının sayısı,

$$F(p, n) = A_1 2^n (p+1) + A_2 (2^n + 2^{n-1} p) + (2^n - 1)$$

sayısıdır. Burada,

$$A_1 = \frac{\begin{bmatrix} n \\ 1 \end{bmatrix}_p - 1}{p}, \quad A_2 = \left(\prod_{i=2}^{n-1} \begin{bmatrix} i+1 \\ i \end{bmatrix}_p - A_1 \right)$$

şeklindedir.

Teorem 5.12'yi ispat etmeden önce, gerekli bazı önermeler verilecektir.

Önerme 5.13 G_α ve G_β , G grubunun t boyutlu iki alt grubu olsun. G_α ve G_β gruplarının, $t-1$ boyutlu en fazla bir tek ortak alt grubu vardır, diğerleri birbirinden farklıdır.

İspat: G_α ve G_β gruplarının birer bazları sırasıyla ${}^T G_\alpha$ and ${}^T G_\beta$ olsun. ${}^T G_\alpha^* = {}^T G_\alpha \setminus \{0\}$ ve ${}^T G_\beta^* = {}^T G_\beta \setminus \{0\}$ olmak üzere, eğer ${}^T G_\alpha^* \cap {}^T G_\beta^* = \emptyset$ ise G_α ve G_β gruplarının mertebesi $t-1$ olan alt grupları karşılaştırıldığında, hiç biri aynı değildir. Bu nedenle, G_α ve G_β nin alt gruplarının kesişimi boştur yani hiçbir alt grupları ortak değildir. Öte yandan en fazla $t-1$ adet baz elemanı ortak olabileceğinden, örneğin, $g_{\alpha_i} = g_{\beta_i}$ ($i=1,2,\dots,t-1$) olsun. (Çünkü, t adet baz elemanı ile G_α ve G_β grupları elde edilir.) Daha sonra, G_α 'nın, boyutu $t-1$ olan G_{α_1}' ve G_{α_2}' alt gruplarını ve G_β 'nin boyutu $t-1$ olan G_{β_1}' ve G_{β_2}' alt grupları düşünülmektedir. ${}^T G_{\alpha_i}'$ ve ${}^T G_{\beta_i}'$ ($i=1,2$) gruplarının elemanları, ${}^T G_\alpha$ ve ${}^T G_\beta$ grupları ile inşa edilecektir:

$${}^T G_\alpha = \begin{bmatrix} g_{\alpha_1} \\ g_{\alpha_2} \\ \vdots \\ g_{\alpha_{t-1}} \\ g_{\alpha_t} \end{bmatrix}, \quad {}^T G_\beta = \begin{bmatrix} g_{\beta_1} \\ g_{\beta_2} \\ \vdots \\ g_{\beta_{t-1}} \\ g_{\beta_t} \end{bmatrix}$$

olmak üzere,

$${}^T G_{\alpha_1}' = \begin{bmatrix} g_{\alpha_{11}} \\ g_{\alpha_{12}} \\ \vdots \\ g_{\alpha_{1(t-2)}} \\ g_{\alpha_{1(t-1)}} \end{bmatrix}, \quad {}^T G_{\alpha_2}' = \begin{bmatrix} g_{\alpha_{21}} \\ g_{\alpha_{22}} \\ \vdots \\ g_{\alpha_{2(t-2)}} \\ g_{\alpha_{2(t-1)}} \end{bmatrix}, \quad {}^T G_{\beta_1}' = \begin{bmatrix} g_{\beta_{11}} \\ g_{\beta_{12}} \\ \vdots \\ g_{\beta_{1(t-2)}} \\ g_{\beta_{1(t-1)}} \end{bmatrix}, \quad {}^T G_{\beta_2}' = \begin{bmatrix} g_{\beta_{21}} \\ g_{\beta_{22}} \\ \vdots \\ g_{\beta_{2(t-2)}} \\ g_{\beta_{2(t-1)}} \end{bmatrix}$$

şeklindedir.

Şimdi ${}^T G_{\alpha_1}' = {}^T G_{\beta_1}'$ olduğu düşünülüp G_α ve G_β gruplarının $t-1$ mertebeli başka ortak alt grubu olmadığı gösterilecektir. Öte yandan, ${}^T G_{\alpha_2}'$ and ${}^T G_{\beta_2}'$ ($i=1,2$) gruplarının en fazla $t-1$ elemanı aynı olabilir. Yani, $g_{\alpha_{2i}} = g_{\beta_{2i}}$ ($i=1,2,\dots,t-1$)'dir. (Ayrıca, ${}^T G_{\alpha_i}'$ ve ${}^T G_{\beta_i}'$ alt gruplarının elemanlarının sırasıyla ${}^T G_\alpha$ ve ${}^T G_\beta$ grupları ile üretildiği biliniyor.) Eğer $g_{\alpha_{ij}} = g_{\beta_{ij}}$ ($i=1,2, j=1,2,\dots,t$) ise, bu durumda $G_\alpha = G_\beta$ olur ki bu doğru değildir. Buradan, G_α ve G_β gruplarının boyutu $t-1$ olan bir tek ortak alt grupları olduğu sonucu elde edilir. $\square$

Önerme 5.14 $\mathbb{Z}_p^n$ grubunun $t-1$ boyutlu bir alt grubu verildiğinde, bu alt grup $\mathbb{Z}_p^n$ in t boyutlu $N(t-1, p)$ adet grubunun alt grubudur. Burada,

$$N(t-1, p) = \frac{\begin{bmatrix} t+1 \\ t \end{bmatrix}_p \times \begin{bmatrix} t \\ t-1 \end{bmatrix}_p}{\begin{bmatrix} n \\ t-1 \end{bmatrix}_p}$$

şeklindedir.

İspat: $\mathbb{Z}_p^n$ grubunun Hasse şemasını düşünüldüğünde, $t+1$ boyutlu her bir alt grubun

altında t boyutlu $\begin{bmatrix} t+1 \\ t \end{bmatrix}_p$ adet ve t boyutlu her bir alt grubun altında $t-1$ boyutlu

$\begin{bmatrix} t \\ t-1 \end{bmatrix}_p$ adet alt grup vardır. ($t+1$ boyutlu grubun $\begin{bmatrix} t+1 \\ t \end{bmatrix}_p$ adet t boyutlu alt grubu ve

t boyutlu grubun $\begin{bmatrix} t \\ t-1 \end{bmatrix}_p$ adet $t-1$ boyutlu alt grubu vardır.) Ayrıca, $\mathbb{Z}_p^n$ grubunun $t-1$ boyutlu alt gruplarının sayısı $\begin{bmatrix} n \\ t-1 \end{bmatrix}_p$ ’dir. $\begin{bmatrix} t+1 \\ t \end{bmatrix}_p$ ile $\begin{bmatrix} t \\ t-1 \end{bmatrix}_p$ sayıları çarpılarak, $t+1$ boyutlu alt gruplar ile t boyutlu alt gruplar arasındaki maksimal zincir sayısı bulunur. Bu çarpımı $\begin{bmatrix} n \\ t-1 \end{bmatrix}_p$ sayısı ile bölerek istenen elde edilir. $\square$

Önerme 5.15 $\mathbb{Z}_p^n$ grubunun alt gruplarının bir maksimal zinciri kendinden önceki maksimal zincirlerle karşılaştırıldığında, alt grupların zincirlerdeki dizilimi düşünüldüğünde, aynı yerde farklılık gösteriyorsa, bu ilk zinciri kendinden önceki zincirlerden yalnız biriyle karşılaştırmak yeterlidir. Bu maksimal zincirden 2^n bulanık alt grup elde edilir.

İspat: $G = \mathbb{Z}_p^n$ grubunun iki maksimal zinciri ele alınsın:

$$G_0 = G_{\alpha_0} \subset G_{\alpha_1} \subset G_{\alpha_2} \subset G_{\alpha_3} \subset \dots \subset G_{\alpha_{n-2}} \subset G_{\alpha_{n-1}} \subset G_{\alpha_n} = G \quad (5.1)$$

$$G_0 = G_{\alpha_0} \subset G_{\alpha_1} \subset G_{\beta_2} \subset G_{\alpha_3} \subset \dots \subset G_{\alpha_{n-2}} \subset G_{\alpha_{n-1}} \subset G_{\alpha_n} = G \quad (5.2)$$

(5.1) ve (5.2) maksimal zincirleri karşılaştırıldığında, zincir sıralamasında soldan üçüncü alt grupların farklı olduğu görülür: G_{α_2} ve G_{β_2} . Dolayısıyla bu iki zincirdeki bulanık alt grupların bazıları denk olacaktır. (5.1) ve (5.2) maksimal zincirlerine karşılık gelen bulanık alt gruplar aşağıdaki şekildedir:

$$\mu(x) = \begin{cases} 1, & x \in G_{\alpha_0} \\ \lambda_1, & x \in G_{\alpha_1} \setminus G_{\alpha_0} \\ \lambda_2, & x \in G_{\alpha_2} \setminus G_{\alpha_1} \\ \lambda_3, & x \in G_{\alpha_3} \setminus G_{\alpha_2} \\ \vdots & \vdots \\ \lambda_n, & x \in G_{\alpha_n} \setminus G_{\alpha_{n-1}} \end{cases} \quad \nu(x) = \begin{cases} 1, & x \in G_{\alpha_0} \\ \lambda'_1, & x \in G_{\alpha_1} \setminus G_{\alpha_0} \\ \lambda'_2, & x \in G_{\beta_2} \setminus G_{\alpha_1} \\ \lambda'_3, & x \in G_{\alpha_3} \setminus G_{\beta_2} \\ \vdots & \vdots \\ \lambda'_n, & x \in G_{\alpha_n} \setminus G_{\alpha_{n-1}} \end{cases}$$

Denklik için μ ve ν bulanık alt gruplarının yukarıdaki yazılışında sağ kısımların aynı olması gerekir. G_{α_2} , G_{β_2} alt gruplarından dolayı sağ kısımlar farklıdır. Bu nedenle eğer

$\lambda_2 = \lambda_3$ ve $\lambda'_2 = \lambda'_3$ alınırsa, (5.1) ve (5.2) maksimal zincirlerini mukayese ile elde edilen denk bulanık alt gruplar elde edilir. Bu durumda,

$$\mu(x) = \begin{cases} 1, & x \in G_{\alpha_0} \\ \lambda_1, & x \in G_{\alpha_1} \setminus G_{\alpha_0} \\ \lambda_2, & x \in G_{\alpha_2} \setminus G_{\alpha_1} \\ \lambda_3 = \lambda_2, & x \in G_{\alpha_3} \setminus G_{\alpha_2} \\ \vdots & \vdots \\ \lambda_n, & x \in G_{\alpha_n} \setminus G_{\alpha_{n-1}} \end{cases} \quad \text{ve} \quad \nu(x) = \begin{cases} 1, & x \in G_{\alpha_0} \\ \lambda'_1, & x \in G_{\alpha_1} \setminus G_{\alpha_0} \\ \lambda'_2, & x \in G_{\beta_2} \setminus G_{\alpha_1} \\ \lambda'_3 = \lambda'_2, & x \in G_{\alpha_3} \setminus G_{\beta_2} \\ \vdots & \vdots \\ \lambda'_n, & x \in G_{\alpha_n} \setminus G_{\alpha_{n-1}} \end{cases}$$

denktir. Çünkü son durumda aşağıdaki gibi görünürler:

$$\mu(x) = \begin{cases} 1, & x \in G_{\alpha_0} \\ \lambda_1, & x \in G_{\alpha_1} \setminus G_{\alpha_0} \\ \lambda_2 = \lambda_2, & x \in G_{\alpha_3} \setminus G_{\alpha_1} \\ \vdots & \vdots \\ \lambda_n, & x \in G_{\alpha_n} \setminus G_{\alpha_{n-1}} \end{cases} \quad \text{ve} \quad \nu(x) = \begin{cases} 1, & x \in G_{\alpha_0} \\ \lambda'_1, & x \in G_{\alpha_1} \setminus G_{\alpha_0} \\ \lambda'_2 = \lambda'_3, & x \in G_{\alpha_2} \setminus G_{\alpha_1} \\ \vdots & \vdots \\ \lambda'_n, & x \in G_{\alpha_n} \setminus G_{\alpha_{n-1}} \end{cases} \quad (5.3)$$

(5.3)'deki gösterimler bir n – zincire ait olduğundan ve (5.1) ile (5.2)'de incelenen zincirler $(n+1)$ – zincir olduğundan, (5.3)'deki gösterimler gerçekte doğru değildir. Bu gösterimler sadece maksimal zincirlerdeki bulanık alt grupları saymak için kullanılacaktır. (5.3)'den, $2^n - 1$ bulanık alt grup elde edilir. Yani, (5.1) ve (5.2) zincirlerinden $2^n - 1$ denk bulanık alt grup elde edilir.

Bir maksimal zincir düşünüldüğünde, diğer zincirlerle denklik düşünülmemektedir, Önerme 5.6'dan, $2^{n+1} - 1$ bulanık alt grup elde edilir. Verilen bir grubun ayırık bulanık alt gruplarını bulmak için, bu sayıdan denk bulanık alt grupların sayısının çıkarılması gerekir. Bu nedenle, bu zincirlerden elde edilen ayırık bulanık alt grupların sayısı $(2^{n+1} - 1) - (2^n - 1) = 2^n$ 'dir. Öte yandan, herhangi bir maksimal zincir kendinden önceki maksimal zincirlerle karşılaştırıldığında, eğer bu maksimal zincir kendinden önceki maksimal zincirlerden her biri ile aynı yerde bir tek farklı alt gruba sahip ise, bu ilk verilen maksimal zinciri kendinden öncekilerden yalnızca biriyle karşılaştırmak yeterlidir. Çünkü biriyle karşılaştırıldığında elde edilen denk bulanık alt gruplar ile diğer

her biri ile karşılaştırıldığında elde edilen denk alt gruplar birbirine denktir. Sayısı da $2^n - 1$ dir. $\square$

Önerme 5.16 (Herhangi bir maksimal zincirin diğer iki maksimal zincir ile karşılaştırılması) Herhangi bir maksimal zincir, alt grup diziliminde, diğer iki maksimal zincirle farklı yerlerde bir farklı alt gruba sahipse, bu durumda o maksimal zincirden $2^{n-1} - 1$ bulanık alt grup elde edilir.

İspat: $\mathbb{Z}_p^n$ grubunun herhangi üç maksimal zinciri aşağıdaki gibi verilsin:

1. $G_0 = G_{\alpha_0} \subset G_{\alpha_1} \subset G_{\alpha_2} \subset G_{\alpha_3} \subset \dots \subset G_{\alpha_{n-2}} \subset G_{\alpha_{n-1}} \subset G_{\alpha_n} = G,$
2. $G_0 = G_{\alpha_0} \subset G_{\alpha_1} \subset G_{\beta_2} \subset G_{\alpha_3} \subset \dots \subset G_{\alpha_{n-2}} \subset G_{\alpha_{n-1}} \subset G_{\alpha_n} = G,$
3. $G_0 = G_{\alpha_0} \subset G_{\alpha_1} \subset G_{\alpha_2} \subset G_{\beta_3} \subset \dots \subset G_{\alpha_{n-2}} \subset G_{\alpha_{n-1}} \subset G_{\alpha_n} = G.$

Bu maksimal zincirlerin dizilimi, Hasse şemasında, soldan sağa doğru ilk üç maksimal zincir olsun. 1. zincirdeki bulanık alt grupların sayısı aşağıdaki şekilde bulunur.

1. maksimal zincir 2. maksimal zincir ile karşılaştırıldığında, $2^n - 1$ denk bulanık alt grup elde edilir (Önerme 5.15). 1. zincir bu kez 3. zincir ile karşılaştırıldığında, benzer şekilde $2^n - 1$ adet denk bulanık alt grup elde edilir. Bu denk bulanık alt grupların tamamı $(2^n - 1) + (2^n - 1)$ eder. Ancak 1. zincir ayrı iki zincir ile karşılaştırıldığında elde edilen denk bulanık alt gruplar arasında da denk bulanık alt gruplar olabileceğinden, bu toplam tüm denklemin sayısından daha büyük bir sayı verir. Dolayısıyla $(2^n - 1) + (2^n - 1)$ sayısından denklemin sayısının çıkarılması gerekir. Başa dönülürse, 1. maksimal zincir 2. maksimal zincir ile karşılaştırıldığında $1\lambda_1\lambda_2\lambda_2\lambda_3\lambda_4\dots\lambda_n$ tipindeki bulanık alt gruplar; 3. ile karşılaştırıldığında ise $1\lambda_1\lambda_2\lambda_3\lambda_3\lambda_4\dots\lambda_n$ tipindeki bulanık alt gruplar denktir (burada “...” farklı üyelik (pin) değerlerini göstermektedir). Bu son iki durumda da $(1\lambda_1\lambda_2\lambda_2\lambda_3\lambda_4\dots\lambda_n$ ve $1\lambda_1\lambda_2\lambda_3\lambda_3\lambda_4\dots\lambda_n)$ $1\lambda_1\lambda_2\lambda_2\lambda_2\lambda_3\dots\lambda_n$ bulanık alt grupları sayılmış oldu (3., 4. ve 5. pin değerleri aynı). Yani, $1\lambda_1\lambda_2\lambda_2\lambda_2\lambda_3\dots\lambda_n$ şeklindeki bulanık alt gruplar iki kere sayılmış olur. $1\lambda_1\lambda_2\lambda_2\lambda_3\lambda_4\dots\lambda_n$ ve $1\lambda_1\lambda_2\lambda_3\lambda_3\lambda_4\dots\lambda_n$ tipindeki

bulanık alt grupların kesişimi $1\lambda_1\lambda_2\lambda_2\lambda_2\lambda_3\ldots\lambda_n$ tipindeki bulanık alt gruptur. Dolayısıyla kesişimi incelemek gerekir. Önerme 5.15'den, $1\lambda_1\lambda_2\lambda_2\lambda_2\lambda_3\ldots\lambda_n$ bulanık alt grubunda, 3., 4. ve 5. pin değerleri aynı olduğundan, sayma kolaylığı sağlaması bakımından, bu bulanık alt grup bir $(n-1)$ -zincir olarak düşünülebilir. Bu $(n-1)$ -zincirden $2^{n-1}-1$ adet bulanık alt grup elde edilir. Bu sayı, en son hesaplanan, $(2^n-1)+(2^n-1)$ sayısından çıkarılacaktır:

$$(2^n-1)+(2^n-1)-(2^{n-1}-1)=3.2^{n-1}-1.$$

Bir $(n+1)$ -zincirden denklik düşünülmezsizin toplamda $2^{n+1}-1$ bulanık alt grup elde edildiği Önerme 5.6'dan biliniyor. O halde ayırık bulanık alt grupların sayısı aşağıdaki gibi verilir:

$$(2^{n+1}-1)-(3.2^{n-1}-1)=2^{n-1}. \square$$

Teorem 5.12'nin ispatı: $\mathbb{Z}_p^n$ grubunun bulanık alt gruplarını saymak için ilk olarak maksimal zincirlerinin sayısının bulunması gerekir. Alt grup şeması düşünüldüğünde, 2 boyutlu alt grupları 1 boyutlu alt gruplara bağlayan zincirler düşünülerek sayma yapılacaktır. Bu nedenle, maksimal zincirler $\begin{bmatrix} 2 \\ 1 \end{bmatrix}_p$ 'li gruplara ayrılmaktadır. Yani her

$\begin{bmatrix} 2 \\ 1 \end{bmatrix}_p$ maksimal zincir tek maksimal zincirmiş gibi düşünülür. Bu nedenle, grubun

maksimal zincirlerinin sayısı aşağıdaki gibidir:

$$\prod_{i=2}^{n-1} \begin{bmatrix} i+1 \\ i \end{bmatrix}_p.$$

Önerme 5.13'den, t boyutlu iki grubun, $t-1$ boyutlu alt gruplarından en fazla bir adedinin aynı olabileceği ve Önerme 5.14 den, $t-1$ boyutlu bir alt grubun, t boyutlu $N(t-1, p)$ adet grubun alt grubu olduğu biliniyor. Şekil 1'den yararlanarak, maksimal

zincir sıralamasında en soldan başlanarak maksimal zincirlerin sayısı hesaplanacaktır.

ilk $\begin{bmatrix} 2 \\ 1 \end{bmatrix}_p$ adet maksimal zincir aşağıdaki şekilde yazılır:

$$G_0 \subset G_1 \subset G_{\alpha_2} \subset G_{\alpha_3} \subset \dots \subset G_{\alpha_{n-2}} \subset G_{\alpha_{n-1}} \subset G_{\alpha_n},$$

$$G_0 \subset G_2 \subset G_{\alpha_2} \subset G_{\alpha_3} \subset \dots \subset G_{\alpha_{n-2}} \subset G_{\alpha_{n-1}} \subset G_{\alpha_n},$$

$$G_0 \subset G_3 \subset G_{\alpha_2} \subset G_{\alpha_3} \subset \dots \subset G_{\alpha_{n-2}} \subset G_{\alpha_{n-1}} \subset G_{\alpha_n},$$

.....

$$G_0 \subset G_{\begin{bmatrix} 2 \\ 1 \end{bmatrix}_p} \subset G_{\alpha_2} \subset G_{\alpha_3} \subset \dots \subset G_{\alpha_{n-2}} \subset G_{\alpha_{n-1}} \subset G_{\alpha_n}.$$

Yukarıdaki maksimal zincirlerin diziliminde yalnızca birer alt grupları (soldan ikinci alt grup) farklılık gösterir. Dolayısıyla ilk maksimal zincir dışındaki zincirlerden 2^n adet ayrık bulanık alt grup elde edilir. İlk maksimal zincirden elde edilen ayrık bulanık alt gruplar, Önerme 5.6'dan, $2^{n+1} - 1$ 'dir. O halde ilk $\begin{bmatrix} 2 \\ 1 \end{bmatrix}_p$ adet maksimal zincirden toplam

$$(2^{n+1} - 1) + \underbrace{2^n + 2^n + \dots + 2^n}_{\begin{bmatrix} 2 \\ 1 \end{bmatrix}_p - 1} \text{ ayrık bulanık alt grup elde edilir.}$$

ikinci $\begin{bmatrix} 2 \\ 1 \end{bmatrix}_p$ adet maksimal zincir aşağıdaki şekildedir:

$$G_0 \subset G_1 \subset G_{\beta_2} \subset G_{\beta_3} \subset \dots \subset G_{\alpha_{n-1}} \subset G_{\alpha_n},$$

$$G_0 \subset G_{\begin{bmatrix} 2 \\ 1 \end{bmatrix}_p + 1} \subset G_{\beta_2} \subset G_{\beta_3} \subset \dots \subset G_{\alpha_{n-1}} \subset G_{\alpha_n},$$

$$G_0 \subset G_{\begin{bmatrix} 2 \\ 1 \end{bmatrix}_p + 2} \subset G_{\beta_2} \subset G_{\beta_3} \subset \dots \subset G_{\alpha_{n-1}} \subset G_{\alpha_n},$$

.....

$$G_0 \subset G_{\begin{bmatrix} 2 \\ 1 \end{bmatrix}_p + \begin{bmatrix} 2 \\ 1 \end{bmatrix}_p - 1} \subset G_{\beta_2} \subset G_{\beta_3} \subset \dots \subset G_{\alpha_{n-1}} \subset G_{\alpha_n}.$$

Burada, sayma kolaylığı sağlaması bakımından maksimal zincirler uygun bir şekilde dizayn edilmiştir. Şekil 1'den ilk $\begin{bmatrix} 2 \\ 1 \end{bmatrix}_p$ adet maksimal zincir açık olarak görülmektedir.

İkinci $\begin{bmatrix} 2 \\ 1 \end{bmatrix}_p$ maksimal zincirin ilk zinciri yazılırken zincir sıralamasında G_1 grubu yazılmıştır. Bu yazılım keyfi değildir. G_1 alt grubu 1 boyutlu olduğundan, Önerme 5.13'den, 2 boyutlu $N(0, p)$ adet grubun altında olacaktır. 1 boyutlu alt gruplar, sayma kolaylığı bakımından, indis sıralamasına göre değerlendirilecektir. Daha açık olarak, ilk $\begin{bmatrix} 2 \\ 1 \end{bmatrix}_p$ adet maksimal zincirin birinci zincirinde 1 boyutlu alt grup olarak G_1

alındı. Öte yandan dikkat edilirse, ikinci $\begin{bmatrix} 2 \\ 1 \end{bmatrix}_p$ zincirin ilk zincirinde de 1 boyutlu alt grup olarak G_1 alındı. G_1 , 1 boyutlu alt grup olarak $N(0, p)$ kere yazılacağından, bu sayı tamamlanana kadar ilk zincirlerde G_1 bulunacaktır. Daha sonra indis artışına göre $G_2, G_3, \dots$ şeklinde devam edilecektir.

Öte yandan, ikinci $\begin{bmatrix} 2 \\ 1 \end{bmatrix}_p$ adet maksimal zincir, kendinden önceki zincirlerle karşılaştırıldığında, zincir diziliminde yalnızca bir farklı alt grup olduğundan, ilk $\begin{bmatrix} 2 \\ 1 \end{bmatrix}_p$ adet maksimal zincirdeki işlemlere benzer olarak bu zincirlerden, $\underbrace{2^n + 2^n + \dots + 2^n}_{\begin{bmatrix} 2 \\ 1 \end{bmatrix}_p}$ adet

ayrık bulanık alt grup elde edilir. O halde ilk $A_1 = \frac{\begin{bmatrix} n \\ 1 \end{bmatrix}_p - 1}{p}$ maksimal zincirden

$2^n \left(\begin{bmatrix} n \\ 1 \end{bmatrix}_p \right) = 2^n (p+1)$ ayrık bulanık alt grup elde edilir. Geriye kalan

$A_2 = \left(\prod_{i=2}^{n-1} \begin{bmatrix} i+1 \\ i \end{bmatrix}_p - A_1 \right)$ maksimal zincirden $2^n + 2^{n-1} p$ adet ayrık bulanık alt grup elde

edilir. O halde toplamda, ilk zincirden elde edilen bulanık alt gruplar da dahil olmak üzere, toplam

$$F(p, n) = A_1 2^n (p+1) + A_2 (2^n + 2^{n-1} p) + (2^n - 1)$$

bulanık alt grup elde edilir. $\square$

Örnek 5.17 (Teorem) [10] $\mathbb{Z}_p \times \mathbb{Z}_p \supset \langle a \rangle \supset \langle 0 \rangle$ zincirinde $\langle a \rangle$, p . mertebeden bir alt gruptur. $\mathbb{Z}_p \times \mathbb{Z}_p$ grubunun alt grupları sıralandığında $(p+1)$ adet maksimal zincir oluşur.

İspat: $G = \mathbb{Z}_p \times \mathbb{Z}_p$ Abel grubunun mertebesi p asal olmak üzere p^2 olduğundan G 'nin aşıklarlar dışındaki tüm alt grupları p . mertebededir. Bu nedenle $1 \leq i, j < p$ için $a, (i, j)$ formunda olmak üzere G 'nin alt gruplarının maksimal zincirleri $\langle 0 \rangle \subset \langle a \rangle \subset G$ şeklindedir. a elemanlarının ürettiği ayrık alt gruplar $\langle 1, p \rangle, \langle p, 1 \rangle, \langle 1, 1 \rangle, \langle 1, 2 \rangle, \langle 1, 3 \rangle, \dots, \langle 1, p-2 \rangle$ 'dir. Yani, i ile $p-1$ arasındaki her i için $\langle i, p-i \rangle$ şeklindedir. $i \neq j$ ve $i+j \neq p$ olmak üzere, (i, j) elemanının ürettiği alt grup $(1, 2), (1, 3), \dots, (1, p-2)$ elemanlarından biridir. $i = j$ durumunda üretilen grup $(1, 1)$; $i+j = p$ durumunda üretilen grup ise $(i, p-i)$ dir. Diğer iki durum da $(1, p)$ ve $(p, 1)$ durumlarıdır. Dolayısıyla $(p+1)$ maksimal zincir vardır.

Önerme 5.18 [10] p bir asal sayı olmak üzere, $G = \mathbb{Z}_p \times \mathbb{Z}_p$ grubunun bulanık alt gruplarının sayısı ise $4p+7$ 'dir.

İspat: G 'nin her maksimal zincirinde 3 alt grup vardır ($\mathbb{Z}_{p^2}$ de olduğu gibi). Tüm maksimal zincirlerde oluşan 7 adet bulanık alt gruptan 3 adedi birbirine denktir. Ayrık olanlar; $11\lambda, 110, 1\lambda\beta, 1\lambda 0$ şeklindedir. $p+1$ maksimal zincir olduğundan $4(p+1)$ ayrık bulanık alt grup vardır. İlk zincirdeki 3 adet bulanık alt grupla birlikte G 'nin $4(p+1)+3 = 4p+7$ adet bulanık alt grubu vardır. $\square$

Örnek 5.19 İlk olarak, $\mathbb{Z}_p$ grubu düşünülmektedir. $\mathbb{Z}_p$ grubunun maksimal zincirleri düşünüldüğünde,

$$\langle 0 \rangle \subset \mathbb{Z}_p$$

şeklinde 2 alt gruptan (aşıkâr alt gruplar) oluşan **tek bir** zincir oluşur. Yukarıdaki zincir anahtar zincirle birlikte, $\langle 0 \rangle^1 \subset \mathbb{Z}_p^\lambda$ şeklinde gösterilir. Bu zincirden $2^2 - 1 = 3$ adet denk olmayan bulanık alt grup elde edilir: 11, 1λ, 10. Bu bulanık alt gruplar aşağıdaki gibidir:

$$11 \rightarrow \mu(x) = \begin{cases} 1, & x \in \mathbb{Z}_p \end{cases} \equiv \mathbb{Z}_p,$$

$$10 \rightarrow \nu(x) = \begin{cases} 1, & x = \{0\} \\ 0, & x \in \mathbb{Z}_p \setminus \{0\} \end{cases} \equiv \{0\},$$

$$1\lambda \rightarrow \eta(x) = \begin{cases} 1, & x = \{0\} \\ \lambda, & x \in \mathbb{Z}_p \setminus \{0\} \end{cases}.$$

Diğer bulanık alt grupların tümü, bu 3 adetten birine denktir.

Örnek 5.20 $\mathbb{Z}_{p^2}$ grubunda, $\langle a \rangle$, p . mertebeden bir alt grup olmak üzere,

$$\langle 0 \rangle \subset \langle a \rangle \subset \mathbb{Z}_{p^2}$$

şeklinde **tek bir** zincir oluşur. Anahtar zincirle birlikte, $\langle 0 \rangle^1 \subset \langle a \rangle^\lambda \subset \mathbb{Z}_{p^2}^\beta$ şeklinde gösterilir. Bu zincirden $2^3 - 1 = 7$ adet denk olmayan bulanık alt grup elde edilir:

$$111, 11\lambda, 110, 1\lambda\lambda, 100, 1\lambda 0, 1\lambda\beta.$$

Bu bulanık alt gruplar aşağıdaki gibidir:

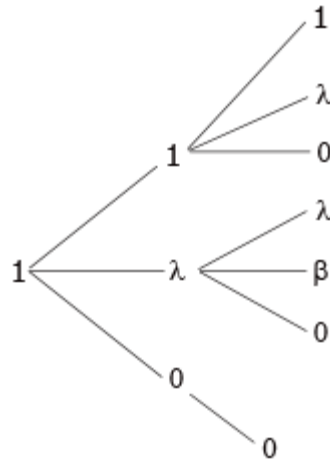
$$111 \rightarrow \mu(x) = \begin{cases} 1, & x \in \mathbb{Z}_{p^2} \end{cases} \equiv \mathbb{Z}_{p^2}, \quad 100 \rightarrow \nu(x) = \begin{cases} 1, & x = \{0\} \\ 0, & x \in \mathbb{Z}_{p^2} \setminus \{0\} \end{cases} \equiv \langle 0 \rangle,$$

$$11\lambda \rightarrow \eta(x) = \begin{cases} 1, & x = \langle a \rangle \\ \lambda, & x \in \mathbb{Z}_{p^2} \setminus \langle a \rangle, \end{cases} \quad 1\lambda\beta \rightarrow \alpha(x) = \begin{cases} 1, & x = \{0\} \\ \lambda, & x \in \langle a \rangle \setminus \{0\} \\ \beta, & x \in \mathbb{Z}_{p^2} \setminus \langle a \rangle, \end{cases}$$

$$1\lambda 0 \rightarrow \lambda(x) = \begin{cases} 1, & x = \{0\} \\ \lambda, & x \in (a) \setminus \{0\} \\ 0, & x \in \mathbb{Z}_{p^2} \setminus (a), \end{cases} \quad 110 \rightarrow \varphi(x) = \begin{cases} 1, & x = (a) \\ 0, & x \in \mathbb{Z}_{p^2} \setminus (a), \end{cases}$$

$$1\lambda\lambda \rightarrow \beta(x) = \begin{cases} 1, & x = \{0\} \\ \lambda, & x \in \mathbb{Z}_{p^2} \setminus \{0\}. \end{cases}$$

$\mathbb{Z}_{p^2}$ grubunun bulanık alt grupları ayrıca ağaç diyagramı ile,



Şekil 5. 2 $\mathbb{Z}_{p^2}$ grubunun bulanık alt gruplarının ağaç diyagramı

şeklinde gösterilir.

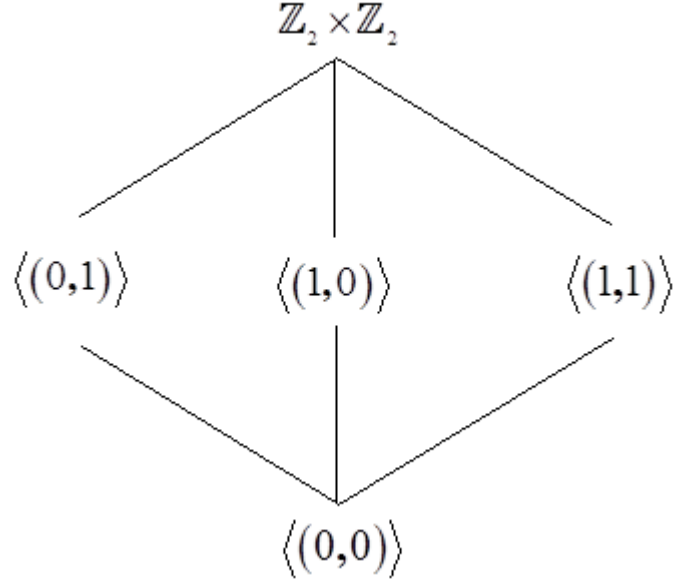
Örnek 5.21 [3] $\mathbb{Z}_{p^k}$ grubunun maksimal zinciri aşağıdaki şekildedir:

$$\langle 0 \rangle^1 \subset \langle a_p \rangle^{\lambda_1} \subset \dots \subset \langle a_{p^{k-1}} \rangle^{\lambda_{k-1}} \subset \mathbb{Z}_{p^k}^{\lambda_k}, \quad i=1,2,\dots,k-1, \quad k \in \mathbb{N} \quad (5.4)$$

Burada $\langle a_{p^i} \rangle$; $i=1,2,\dots,k-1, \quad k \in \mathbb{N}$ olmak üzere p^i . mertebeden alt gruptur. (5.4)

maksimal zincirinden toplam $2^{k+1} - 1$ bulanık alt grup elde edilir.

Örnek 5.22 $\mathbb{Z}_2 \times \mathbb{Z}_2$ grubunun maksimal zincirleri ve bulanık alt grupları



Şekil 5. 3 $\mathbb{Z}_2 \times \mathbb{Z}_2$ grubunun Hasse şeması

Teorem 5.17'den $2+1=3$ adet maksimal zincir oluşur. Bu maksimal zincirler, soldan sağa doğru;

1. $\langle(0,0)\rangle \subset \langle(0,1)\rangle \subset \mathbb{Z}_2 \times \mathbb{Z}_2,$
2. $\langle(0,0)\rangle \subset \langle(1,0)\rangle \subset \mathbb{Z}_2 \times \mathbb{Z}_2,$
3. $\langle(0,0)\rangle \subset \langle(1,1)\rangle \subset \mathbb{Z}_2 \times \mathbb{Z}_2$

şeklindedir.

Görüldüğü gibi 3 maksimal zincir de 3 alt gruptan oluşur. Birinci maksimal zincirden Önerme 5.16'ya göre 7 adet bulanık alt grup elde edilir: $111, 1\lambda\lambda, 100, 11\lambda, 110, 1\lambda0, 1\lambda\beta$.

İkinci ve üçüncü maksimal zincirlerdeki bulanık alt gruplardan üçü $(111, 1\lambda\lambda, 100)$ birinci zincirdekilere denktir:

$$111 \rightarrow \mu_1(x) = \{1, x \in \mathbb{Z}_2 \times \mathbb{Z}_2 = \mathbb{Z}_2 \times \mathbb{Z}_2, \quad (1. \text{ zincir için})$$

$$111 \rightarrow \nu_1(x) = \{1, x \in \mathbb{Z}_2 \times \mathbb{Z}_2 = \mathbb{Z}_2 \times \mathbb{Z}_2, \quad (2. \text{ zincir için})$$

$$111 \rightarrow \eta(x) = \{1, x \in \mathbb{Z}_2 \times \mathbb{Z}_2 = \mathbb{Z}_2 \times \mathbb{Z}_2, \quad (3. \text{ zincir için})$$

$$\mu_1 \sim \nu_1 \sim \eta_1 .$$

$$1\lambda\lambda \rightarrow \mu_2(x) = \begin{cases} 1, & x = \{0\} \\ \lambda, & x \in \mathbb{Z}_2 \times \mathbb{Z}_2 \setminus \{0\}, \end{cases} \quad (1. \text{ zincir için})$$

$$1\lambda\lambda \rightarrow \nu_2(x) = \begin{cases} 1, & x = \{0\} \\ \lambda, & x \in \mathbb{Z}_2 \times \mathbb{Z}_2 \setminus \{0\}, \end{cases} \quad (2. \text{ zincir için})$$

$$1\lambda\lambda \rightarrow \eta_2(x) = \begin{cases} 1, & x = \{0\} \\ \lambda, & x \in \mathbb{Z}_2 \times \mathbb{Z}_2 \setminus \{0\}, \end{cases} \quad (3. \text{ zincir için})$$

$$\mu_2 \sim \nu_2 \sim \eta_2 .$$

$$100 \rightarrow \mu_3(x) = \begin{cases} 1, & x = \{0\} \\ 0, & x \in \mathbb{Z}_2 \times \mathbb{Z}_2 \setminus \{0\} \end{cases} = \langle (0,0) \rangle, \quad (1. \text{ zincir için})$$

$$100 \rightarrow \nu_3(x) = \begin{cases} 1, & x = \{0\} \\ 0, & x \in \mathbb{Z}_2 \times \mathbb{Z}_2 \setminus \{0\} \end{cases} = \langle (0,0) \rangle, \quad (2. \text{ zincir için})$$

$$100 \rightarrow \eta_3(x) = \begin{cases} 1, & x = \{0\} \\ 0, & x \in \mathbb{Z}_2 \times \mathbb{Z}_2 \setminus \{0\} \end{cases} = \langle (0,0) \rangle, \quad (3. \text{ zincir için})$$

$$\mu_3 \sim \nu_3 \sim \eta_3 .$$

O halde ikinci ve üçüncü zincirlerde birinciye denk olan 3 er adet bulanık alt grup elde edilir. Diğerleri denk değildir. Örneğin;

$$\mu_4 = \begin{cases} 1, & x = \{(0,0)\} \\ 1, & x \in \langle (0,1) \rangle \setminus \{(0,0)\} \\ \lambda, & \mathbb{Z}_2 \times \mathbb{Z}_2 \setminus \langle (0,1) \rangle \end{cases} = \begin{cases} 1, & x \in \langle (0,1) \rangle \\ \lambda, & \mathbb{Z}_2 \times \mathbb{Z}_2 \setminus \langle (0,1) \rangle, \end{cases} \quad (1. \text{ zincir için})$$

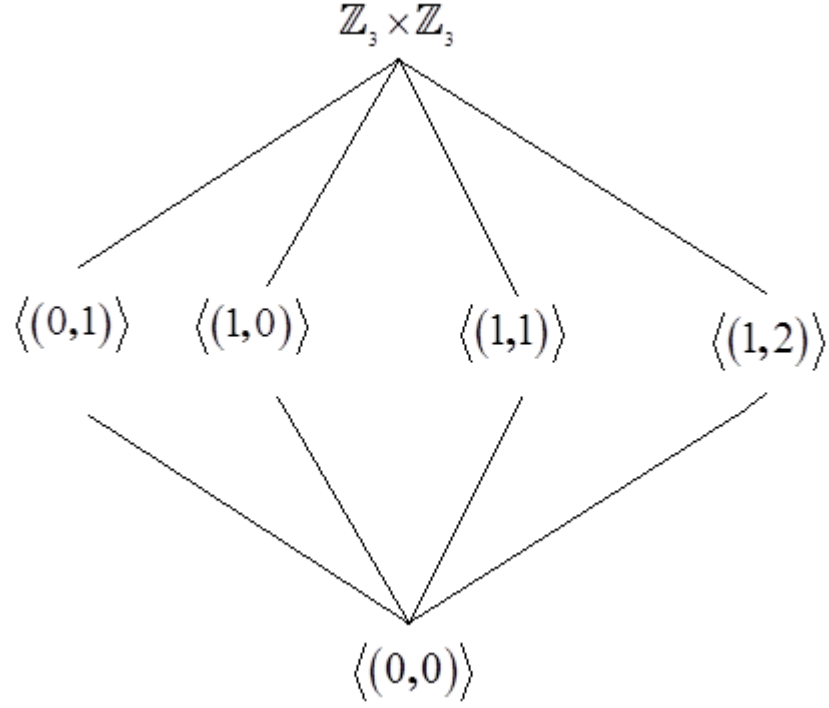
$$\nu_4 = \begin{cases} 1, & x = \{(0,0)\} \\ 1, & x \in \langle (1,0) \rangle \setminus \{(0,0)\} \\ \lambda, & \mathbb{Z}_2 \times \mathbb{Z}_2 \setminus \langle (1,0) \rangle \end{cases} = \begin{cases} 1, & x \in \langle (1,0) \rangle \\ \lambda, & \mathbb{Z}_2 \times \mathbb{Z}_2 \setminus \langle (1,0) \rangle, \end{cases} \quad (2. \text{ zincir için})$$

Bulanık alt grupları için $\mu^* = \nu^*$ şeklindedir. Ancak;

$$\mu_4((0,1))=1 > \lambda = \mu_4((1,0)) \text{ iken } \nu_4((0,1))=\lambda < 1 = \nu_4((1,0)).$$

Sonuçta $7-3=4$ 'er adet denk olmayan bulanık alt grup elde edilir. Toplam:
 $7+4 \times 2=15$ adet bulanık alt grup elde edilir.

Örnek 5.23 $\mathbb{Z}_3 \times \mathbb{Z}_3$ grubunun maksimal zincirleri ve bulanık alt grupları



Şekil 5. 4 $\mathbb{Z}_3 \times \mathbb{Z}_3$ grubunun Hasse şeması

Yukarıdaki şekle göre, Teorem 5.17'den, $3+1=4$ maksimal zincir oluşur. Buradaki maksimal zincirler ele alındığında, Önerme 5.18'den, $7+4 \times 3=19$ adet bulanık alt grup oluşur.

Örnek 5.24 $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ grubunun maksimal zincirlerini ve bulanık alt grupları aşağıdaki şekilde incelenir:

$G_{15} = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ grubunun alt grupları aşağıda verilmiştir:

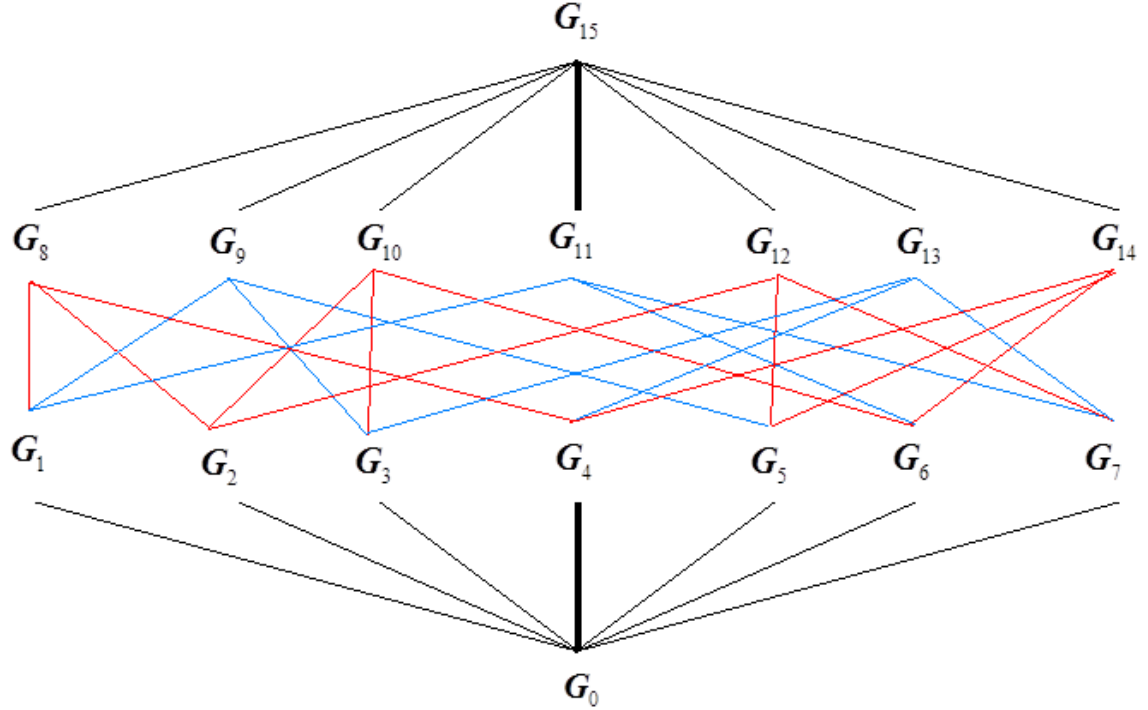
$$G_0 = \{(0,0,0)\}, \quad G_1 = \langle(1,0,0)\rangle, \quad G_2 = \langle(0,1,0)\rangle, \quad G_3 = \langle(0,0,1)\rangle,$$

$$G_4 = \langle(1,1,0)\rangle, \quad G_5 = \langle(1,0,1)\rangle, \quad G_6 = \langle(0,1,1)\rangle, \quad G_7 = \langle(1,1,1)\rangle,$$

$$G_8 = \langle(1,0,0),(0,1,0)\rangle, \quad G_9 = \langle(1,0,0),(0,0,1)\rangle, \quad G_{10} = \langle(0,1,0),(0,0,1)\rangle,$$

$$G_{11} = \langle (1,0,0), (0,1,1) \rangle, \quad G_{12} = \langle (0,1,0), (1,0,1) \rangle, \quad G_{13} = \langle (0,0,0), (1,1,0) \rangle,$$

$$G_{14} = \langle (1,1,0), (1,0,1) \rangle, \quad G_{15} = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$



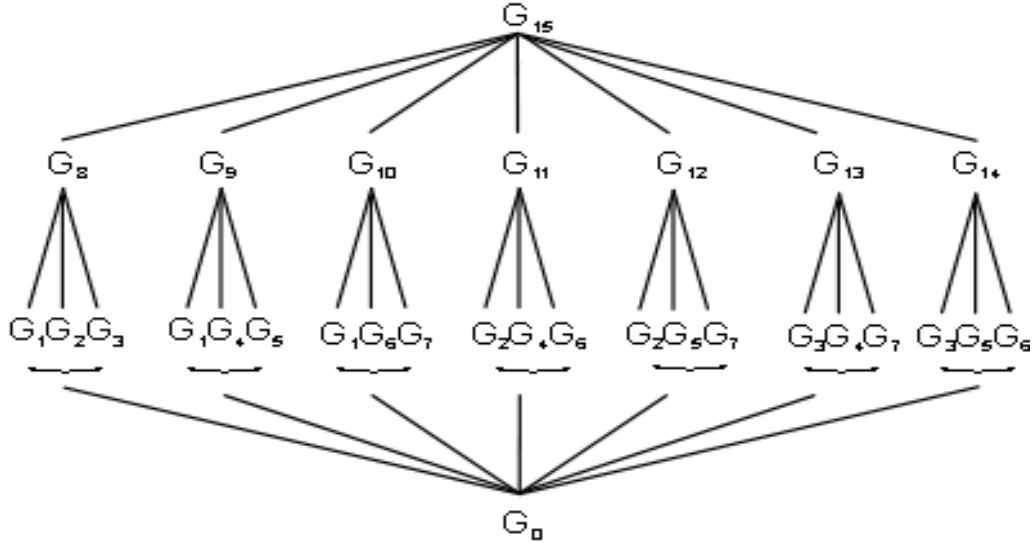
Şekil 5. 5 $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ grubunun Hasse şeması

G_{15} grubunun bulanık alt gruplarının sayısını bulmak için ilk olarak maksimal zincirlerin yapı ve sayılarını incelemek gerekir. Bunun için de maksimal zincirlerin daha açık görüldüğü, Şekil 5.4'e alternatif olan şekil 5.5 incelenecektir.

$$p^1 = 2^1. \text{ mertebeden alt grupların sayısı: } \binom{3}{1}_2 = \frac{2^3 - 1}{2^1 - 1} = 7,$$

$$p^2 = 2^2. \text{ mertebeden alt grupların sayısı: } \binom{3}{2}_2 = \frac{(2^3 - 1)(2^2 - 1)}{(2^1 - 1)(2^2 - 1)} = 7.$$

Dördüncü mertebeden her alt grubun altında 3 adet ikinci mertebeden alt grup vardır. Toplam 7 adet dördüncü mertebeden alt grup olduğundan $3 \times 7 = 21$ adet maksimal zincir vardır.



Şekil 5. 6 $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ grubunun alternatif Hasse şeması

Bulanık alt grupları saymak ise daha zor bir problemdir. Soldan itibaren ilk üç zincir aşağıdaki şekildedir:

1. $G_0 \subset G_1 \subset G_8 \subset G_{15}$,
2. $G_0 \subset G_2 \subset G_8 \subset G_{15}$,
3. $G_0 \subset G_3 \subset G_8 \subset G_{15}$.

Yukarıda görüldüğü gibi dörtlü zincirler oluşur, yani bulanık alt gruplar $1\lambda\beta\gamma$ şeklindedir. Her üç zincirde de G_8 grubu ortak olduğundan denklik durumları söz konusu olacaktır. İlk zincirden, $2^4 - 1 = 15$ adet bulanık alt grup elde edilir:

1111, 1110, 1100, 1000, $1\lambda\lambda\lambda$, $1\lambda\lambda 0$, $1\lambda 00$, $1\lambda\beta\gamma$, $1\lambda\beta\beta$, $1\lambda\lambda\beta$, $1\lambda\beta 0$, 111 λ , 11 $\lambda\lambda$, 11 $\lambda\beta$, 11 $\lambda 0$.

Şekil 5.5'deki maksimal zincirler incelendiğinde, her birinde üçer adet bulanık alt gruplar denktir: 1111, $1\lambda\lambda\lambda$, 1000. Eğer maksimal zincirlerde hiç ortak grup olmasaydı (aşıklarlar dışında), ilk üç zincirdeki bulanık alt grup sayısı için $15 + 12 \times 2 = 39$ bulanık alt grup olurdu. Ancak yukarıdaki durumda ikinci ve üçüncü zincirlerdeki $1\lambda\beta\gamma$ şeklindeki bulanık alt gruplardan $1 \geq \lambda = \beta \geq \gamma$ olanlar birinci zincirdekilere denk olanlardır. Sayısı 7'dir. Bu bulanık alt gruplar aşağıda verilmektedir:

1000, $1\lambda\lambda\lambda$, 1111 ve 1110, 111 λ , $1\lambda\lambda 0$, $1\lambda\lambda\beta$.

(İlk 3 bulanık alt grup (1000, $1\lambda\lambda\lambda$, 1111), daha önce de bahsedildiği gibi her durumda birbirine denktir.)

O halde, ilk üç zincirden: $15 + 8 + 8 = 31$ bulanık alt grup elde edilir.

İkinci üç zincir aşağıdaki şekildedir:

4. $G_0 \subset G_1 \subset G_9 \subset G_{15},$

5. $G_0 \subset G_3 \subset G_9 \subset G_{15},$

6. $G_0 \subset G_5 \subset G_9 \subset G_{15}.$

Kendi aralarında incelendiğinde, ilk üç maksimal zincire benzer durum oluşur. Ancak ilk maksimal zincirleri de hesaba katmak gerekir. 4. maksimal zincir ile 1. maksimal zincirin ortak noktası G_1 grubudur. O halde; 4. maksimal zincirden elde edilen $1 \geq \lambda \geq \beta = \gamma$ şeklindeki alt gruplar 1. maksimal zincirden elde edilen bulanık alt gruplara denktir. Bunlar:

1000, 1111, $1\lambda\lambda\lambda$ ve 1100, $1\lambda 00$, $1\lambda\beta\beta$, $11\lambda\lambda$

şeklindedir.

O halde 4. maksimal zincirdeki ayırık bulanık alt gruplar (denk olanlar hariç) aşağıdakilerdir:

1110, $1\lambda\lambda 0$, $1\lambda\beta\gamma$, $1\lambda\lambda\beta$, $1\lambda\beta 0$, 111λ , $11\lambda\beta$, $11\lambda 0$.

5. ve 6. maksimal zincirlerin ilk üç maksimal zincirle ortak noktası yoktur; ancak 4. maksimal zincir ile G_9 grubu ortaktır. O halde, 4. maksimal zincir ile $1 \geq \lambda = \beta \geq \gamma$ şeklindeki bulanık alt gruplar denktir. Yani, 5. ve 6. maksimal zincirlerdeki toplam 15 adet bulanık alt gruptan denk olmayan bulanık alt gruplar:

1110, $1\lambda\lambda 0$, $1\lambda\beta\gamma$, $1\lambda\lambda\beta$, $1\lambda\beta 0$, 111λ , $11\lambda\beta$, $11\lambda 0$

şeklindedir.

İkinci üç zincirden; $8 + 8 + 8 = 24$ ayırık bulanık alt grup elde edilir. Diğerleri de benzer şekilde incelenirse toplam $15 + 8 \times 12 + 4 \times 8 = 143$ adet bulanık alt grup elde edilir. Bu problem maksimal zincirleri çok fazla olan gruplar için oldukça zordur. Z_p^n grubu için küçük örnekler bazı çalışmalarda incelenmiştir. Ancak yapılan çalışmalarda, bu tezde kullanılan denklikten farklı bir denklik kullanılmış ve orada kullanılan formül yinelemeli (rekursif) bir formüldür.

5.4 $\mathbb{Z}_{2^k} \times \mathbb{Z}_{2^k}$ ($2 \leq k \leq 3$) Grubunun Bulanık Alt Gruplarının Sayısı

$\mathbb{Z}_{2^k} \times \mathbb{Z}_{2^k}$ ($2 \leq k \leq 3$) gruplarının bulanık alt gruplarını incelemek $\mathbb{Z}_p^n$ (p asal) gruplarının bulanık alt gruplarını incelemekten daha zor bir iştir. Çünkü $\mathbb{Z}_{2^k} \times \mathbb{Z}_{2^k}$ ($2 \leq k \leq 3$) gruplarının alt gruplarının maksimal zincirleri $\mathbb{Z}_p^n$ gruplarındaki gibi düzgün ve basit değildir.

$k = 2$ için $\mathbb{Z}_4 \times \mathbb{Z}_4$ grubunun bulanık alt gruplarının sayısı aşağıdaki şekilde bulunur:

5.4.1 $\mathbb{Z}_4 \times \mathbb{Z}_4$ grubunun bulanık alt grupları

İlk olarak $\mathbb{Z}_4 \times \mathbb{Z}_4$ grubunun alt grupları ve Hasse şeması aşağıdaki şekildedir:

$$G_{14} = \mathbb{Z}_4 \times \mathbb{Z}_4,$$

$$G_1 = \langle (1,0), (0,2) \rangle, \quad G_2 = \langle (0,1), (2,0) \rangle, \quad G_3 = \langle (1,1), (0,2) \rangle,$$

$$G_4 = \langle (1,0) \rangle, \quad G_5 = \langle (1,2) \rangle, \quad G_6 = \langle (0,1) \rangle, \quad G_7 = \langle (2,0), (0,2) \rangle, \quad G_8 = \langle (2,1) \rangle, \quad G_9 = \langle (1,3) \rangle, \quad G_{10} = \langle (1,1) \rangle,$$

$$G_{11} = \langle (2,0) \rangle, \quad G_{12} = \langle (0,2) \rangle, \quad G_{13} = \langle (2,2) \rangle,$$

$$\text{ve } G_0 = \langle (0,0) \rangle.$$

Maksimal zincirleri daha açık görmek için alternatif alt grup şeması, Şekil 5.8 ile verilmektedir.

Şekil 5.8’de alt grupların dizilimi değişse de bulanık alt grupların sayısı değişmeyecektir. Ancak, dizilim değiştiğinde, yani indisler değiştiğinde örüntüyü yakalamak zordur.

$\mathbb{Z}_4 \times \mathbb{Z}_4$ grubunun Şekil 5.8’de alternatif Hasse şeması düşünüldüğünde, Şekil 5.8’den de görüldüğü gibi toplam 58 maksimal zinciri vardır. Teorem 5.12 nin ve Örnek 5.24’ün ispatına benzer şekilde bulanık alt grupların sayısı hesaplanır. $\mathbb{Z}_p^n$ grubunun alt grupları Hasse şemasında düzenli dağılım gösterirken, $\mathbb{Z}_4 \times \mathbb{Z}_4$ grubundaki dizilim biraz daha farklıdır. Burada da zincirleri tek tek incelemek gerekir. İlk 5 maksimal zincir aşağıdaki şekildedir:

1. $G_0 \subset G_{11} \subset G_4 \subset G_1 \subset G_{14},$
2. $G_0 \subset G_{11} \subset G_5 \subset G_1 \subset G_{14},$
3. $G_0 \subset G_{11} \subset G_7 \subset G_1 \subset G_{14},$
4. $G_0 \subset G_{12} \subset G_7 \subset G_1 \subset G_{14},$
5. $G_0 \subset G_{13} \subset G_7 \subset G_1 \subset G_{14}.$

Yukarıdaki maksimal zincirlerden de görüldüğü gibi beşli maksimal zincirler oluşur. En genel anlamda bulanık alt gruplar $1\lambda\beta\gamma\theta$ şeklindedir. 1. maksimal zincirden $2^5 - 1 = 31$ bulanık alt grup elde edilir.

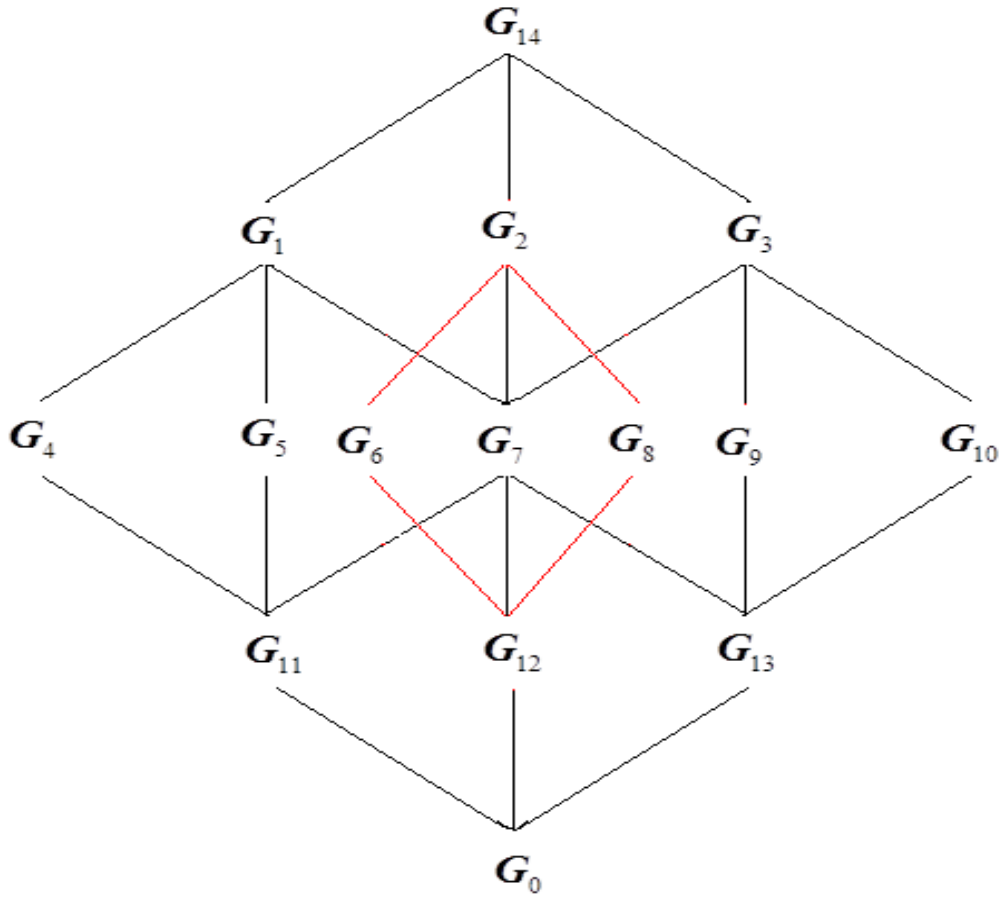
2. maksimal zincir ile 1. maksimal zincirde G_4 ve G_5 grupları farklılık gösterir. O halde, Örnek 5.24'e benzer şekilde, bulanık alt gruplardan $1 \geq \lambda \geq \beta = \gamma \geq \theta$ şeklinde olanlar denktir. Yani, $1\lambda\beta\beta\gamma$ şeklindeki bulanık alt gruplar 1. maksimal zincirdeki bulanık alt gruplar ile denk olanlardır. Bunların sayısı $2^4 - 1 = 15$ 'dir. O halde, 2. maksimal zincirden $31 - 15 = 16$ adet bulanık alt grup elde edilir.

Geriye kalan 3 maksimal zincirden de, benzer şekilde 16'şar adet bulanık alt grup elde edilir. O halde, ilk 5 maksimal zincirden, $31 + 16 + 16 + 16 + 16$ adet bulanık alt grup elde edilir.

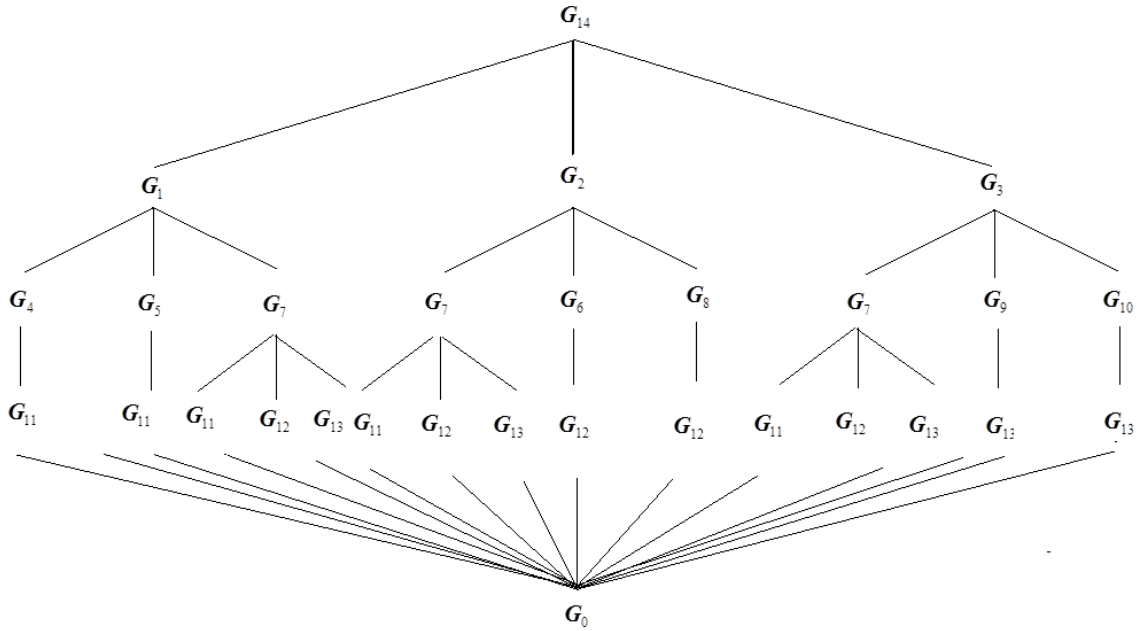
İkinci 5 maksimal zincir aşağıdaki şekildedir:

6. $G_0 \subset G_{11} \subset G_7 \subset G_2 \subset G_{14},$
7. $G_0 \subset G_{12} \subset G_7 \subset G_2 \subset G_{14},$
8. $G_0 \subset G_{13} \subset G_7 \subset G_2 \subset G_{14},$
9. $G_0 \subset G_{12} \subset G_6 \subset G_2 \subset G_{14},$
10. $G_0 \subset G_{12} \subset G_8 \subset G_2 \subset G_{14}.$

6. maksimal zincirden; 2., 3., 4. ve 5. maksimal zincirlere benzer şekilde 16 bulanık alt grup elde edilir.



Şekil 5. 7 $\mathbb{Z}_4 \times \mathbb{Z}_4$ grubunun Hasse şeması



Şekil 5. 8 $\mathbb{Z}_4 \times \mathbb{Z}_4$ grubunun alternatif Hasse şeması

7. maksimal zincir, 6. maksimal zincir ile karşılaştırıldığında, G_{11} ve G_{12} gruplarının farklılık gösterdiği görülebilir. O halde, 7. maksimal zincirde, bulanık alt gruplardan $1 \geq \lambda = \beta \geq \gamma \geq \theta$ şeklinde olanlar denktir. Yani, $1\lambda\lambda\beta\gamma$ şeklindeki bulanık alt gruplar 6. maksimal zincirdeki bulanık alt gruplar ile denk olanlardır. Bunların sayısı $2^4 - 1 = 15$ 'dir. Öte yandan, 7. maksimal zincir, 4. maksimal zincir ile karşılaştırıldığında, $1 \geq \lambda \geq \beta \geq \gamma = \theta$ şeklindeki bulanık alt grupların denk olduğu görülür. Denk olanlar, $1\lambda\beta\gamma\gamma$ şeklinde olanlardır. Bu durumda da 15 denk bulanık alt grup elde edilir. Ancak ilk durumda elde edilen 15 adet bulanık alt grup ile son elde edilen bulanık alt gruplardan 4 adedi birbirine denktir. O halde tüm denklemlerin sayısı: $15 + 15 - 7 = 23$ 'dür. Dolayısıyla 7. maksimal zincirden, $31 - 23 = 8$ bulanık alt grup elde edilir. Diğer maksimal zincirler de bezer şekilde incelenirse, ikinci beş maksimal zincirden, $16 + 8 + 8 + 16 + 16$ adet bulanık alt grup elde edilir.

Son beş maksimal zincirden benzer şekilde, $16 + 8 + 8 + 16 + 16$ adet bulanık alt grup elde edilir.

Sonuç olarak, $\mathbb{Z}_4 \times \mathbb{Z}_4$ grubunun bulanık alt gruplarının sayısı,

$$31 + 16 + 16 + 16 + 16 + 16 + 8 + 8 + 16 + 16 + 16 + 8 + 8 + 16 + 16 = 223$$

adet bulanık alt grup elde edilir. $\square$

5.4.2 $\mathbb{Z}_8 \times \mathbb{Z}_8$ grubunun bulanık alt grupları

$\mathbb{Z}_8 \times \mathbb{Z}_8$ grubunun alt grupları ve Hasse şeması Şekil 5.9 ile verilmektedir.

$$G_{36} = \mathbb{Z}_8 \times \mathbb{Z}_8$$

$$G_1 = \langle (1,0), (0,2) \rangle, \quad G_2 = \langle (0,1), (2,0) \rangle, \quad G_3 = \langle (1,1), (0,2) \rangle, \quad G_4 = \langle (1,2), (0,4) \rangle, \quad G_5 = \langle (1,0), (0,4) \rangle,$$

$$G_6 = \langle (2,0), (0,2) \rangle, \quad G_7 = \langle (0,1), (4,0) \rangle, \quad G_8 = \langle (2,1), (4,0) \rangle, \quad G_9 = \langle (1,1), (0,4) \rangle, \quad G_{10} = \langle (1,3), (0,4) \rangle,$$

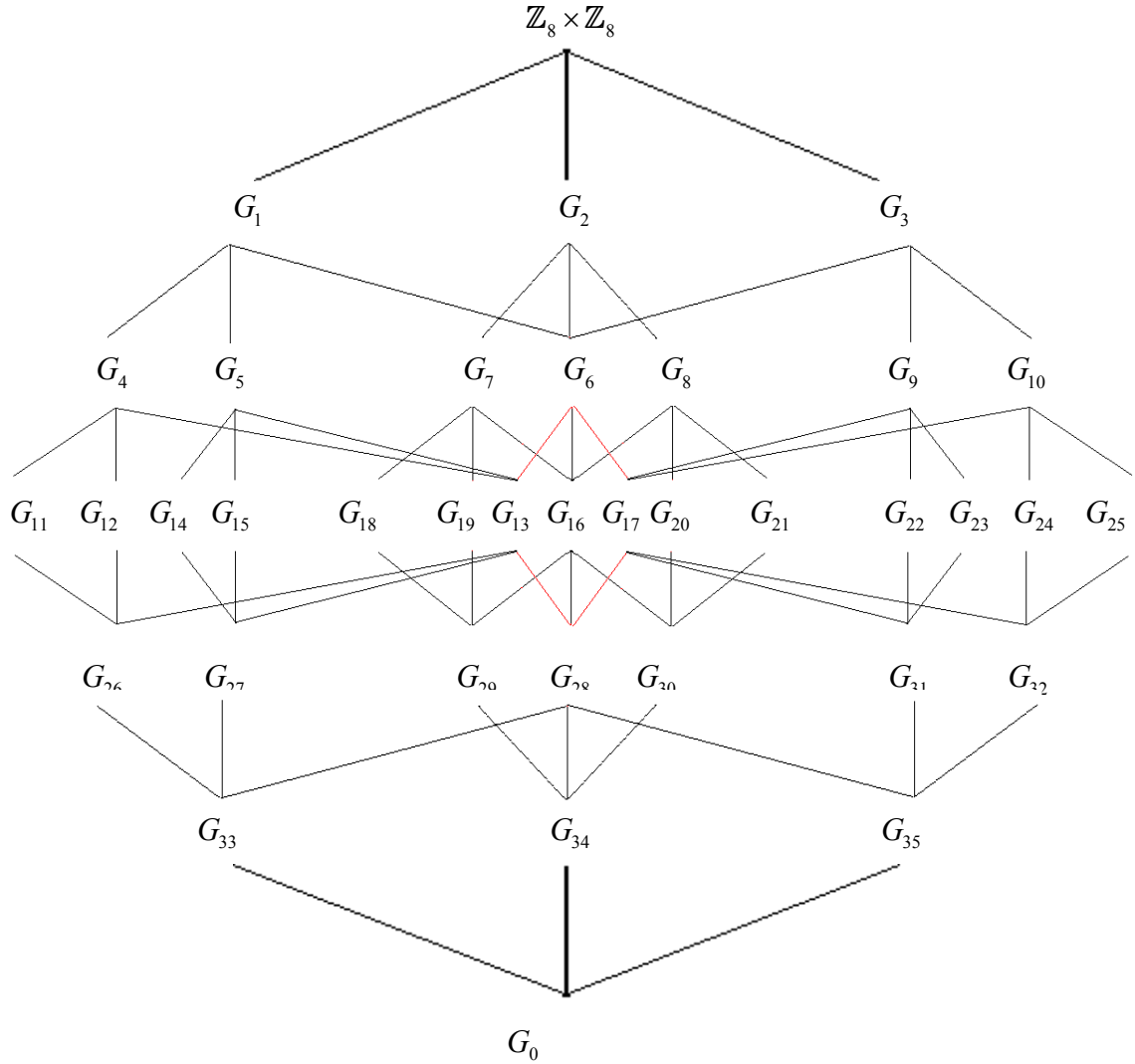
$$G_{11} = \langle (1,2) \rangle, \quad G_{12} = \langle (1,6) \rangle, \quad G_{13} = \langle (2,0), (0,4) \rangle, \quad G_{14} = \langle (1,0) \rangle, \quad G_{15} = \langle (1,4) \rangle, \quad G_{16} = \langle (4,0), (0,2) \rangle,$$

$$G_{17} = \langle (2,2), (0,4) \rangle, \quad G_{18} = \langle (0,1) \rangle, \quad G_{19} = \langle (4,1) \rangle, \quad G_{20} = \langle (2,3) \rangle, \quad G_{21} = \langle (2,1) \rangle, \quad G_{22} = \langle (1,1) \rangle,$$

$$G_{23} = \langle (1,5) \rangle, \quad G_{24} = \langle (1,3) \rangle, \quad G_{25} = \langle (1,7) \rangle, \quad G_{26} = \langle (2,4) \rangle, \quad G_{27} = \langle (2,0) \rangle, \quad G_{28} = \langle (4,0), (0,4) \rangle,$$

$$G_{29} = \langle (0, 2) \rangle, \quad G_{30} = \langle (4, 2) \rangle, \quad G_{31} = \langle (2, 2) \rangle, \quad G_{32} = \langle (2, 6) \rangle, \quad G_{33} = \langle (4, 0) \rangle, \quad G_{34} = \langle (0, 4) \rangle,$$

$$G_{35} = \langle (4, 4) \rangle, \quad G_0 = \langle (0, 0) \rangle.$$



Şekil 5. 9 $\mathbb{Z}_8 \times \mathbb{Z}_8$ grubunun Hasse şeması

$\mathbb{Z}_8 \times \mathbb{Z}_8$ grubunun Şekil 5.9'da verilen alternatif Hasse şeması incelendiğinde 15 maksimal zincir elde edilir. Teorem 5.12'nin ve Örnek 5.24'ün ispatına benzer şekilde bulanık alt grupların sayısı hesaplanır. İşlemler uzun olduğundan, burada, tüm maksimal zincirler incelenmeyecektir. İlk dokuz zincir aşağıdaki şekildedir:

1. $G_0 \subset G_{33} \subset G_{26} \subset G_{11} \subset G_4 \subset G_1 \subset G_{36},$
2. $G_0 \subset G_{33} \subset G_{26} \subset G_{12} \subset G_4 \subset G_1 \subset G_{36},$

3. $G_0 \subset G_{33} \subset G_{26} \subset G_{13} \subset G_4 \subset G_1 \subset G_{36},$
4. $G_0 \subset G_{33} \subset G_{27} \subset G_{13} \subset G_4 \subset G_1 \subset G_{36},$
5. $G_0 \subset G_{33} \subset G_{28} \subset G_{13} \subset G_4 \subset G_1 \subset G_{36},$
6. $G_0 \subset G_{34} \subset G_{27} \subset G_{13} \subset G_4 \subset G_1 \subset G_{36},$
7. $G_0 \subset G_{35} \subset G_{28} \subset G_{13} \subset G_4 \subset G_1 \subset G_{36},$
8. $G_0 \subset G_{33} \subset G_{26} \subset G_{13} \subset G_5 \subset G_1 \subset G_{36},$
9. $G_0 \subset G_{33} \subset G_{27} \subset G_{13} \subset G_5 \subset G_1 \subset G_{36}.$

Yukarıdaki maksimal zincirlerden de görüldüğü gibi yedili zincirler oluşur. En genel anlamda bulanık alt gruplar $1\lambda\beta\gamma\theta\eta\nu$ şeklindedir. 1. maksimal zincirden $2^7 - 1 = 127$ bulanık alt grup elde edilir. 2. maksimal zincir ile 1. maksimal zincirde G_{11} ve G_{12} grupları farklılık gösterir. O halde daha önceki kısımlardakine benzer şekilde, $1\lambda\beta\gamma\theta\eta\nu$ şeklindeki bulanık alt gruplardan $1 \geq \lambda \geq \beta \geq \gamma = \theta \geq \eta \geq \nu$ şeklinde olanlar denktir. Yani, $1\lambda\beta\gamma\gamma\eta\nu$ şeklindeki bulanık alt gruplar 1. maksimal zincirdeki bulanık alt gruplar ile denk olanlardır. Bunların sayısı $2^6 - 1 = 63$ 'dür. O halde, 2. maksimal zincirden $127 - 63 = 64$ adet bulanık alt grup elde edilir. Diğer zincirler de benzer şekilde incelenirse, 3., 4., 5., 6., 7. Ve 8. zincirlerden de 64 bulanık alt grup elde edilir. 9. maksimal zincir incelendiğinde, 4. ve 8. maksimal zincirlerle karşılaştırmak yeterli olacaktır. 4. maksimal zincirle $1\lambda\beta\gamma\theta\theta\nu$ şeklindeki ve 8. maksimal zincirle de $1\lambda\lambda\gamma\theta\eta\nu$ şeklindeki bulanık alt gruplar denktir. İlk durumdan, $127 - 63 = 64$ bulanık alt grup elde edilir. İkinci durumdan sonra, $64 - 32 = 32$ denk olmayan bulanık alt grup elde edilir. O halde ilk dokuz zincirden,

$$127 + 64 + 64 + 64 + 64 + 64 + 64 + 64 + 32$$

bulanık alt grup elde edilir. Diğer maksimal zincirler de $\mathbb{Z}_4 \times \mathbb{Z}_4$ grubunun maksimal zincirlerine benzer şekilde incelendiğinde,

$$127.1 + 64.23 + 32.34 = 2687 \text{ adet bulanık alt grup elde edilir. } \square$$

CEBİRSEL KODLAMA TEORİSİNİN TEMELLERİ

6.1 Giriş

Cebirsel Kodlama Teorisi, bilgi ya da mesajların iletimi veya depolanması esnasında meydana gelen hataların tespiti ve düzeltilmesi için cebirsel yapılardan faydalanarak uygun kodların üretilmesi ve incelenmesi ile ilgilenen ve matematiğin içinde yer bulan bir bilim dalıdır. Kodlama Teorisi modern iletişim sistemlerinin temelini teşkil eder ve son 70 yıldır cebirin uygulamasının en önemli olduğu alanlardan biri haline gelmiştir. Farklı bir çalışma alanı ve kodlama teorisi ile olasılığın birleşimi olan Bilgi Bilimleri'ne açılan bir kapıdır. Cebirsel kodlar; tarayıcılar, optik gereçler ve telekom donanımı gibi tüm donanım uygulamalarında kullanılır. Örneğin, uzun mesafe iletişimi yalnızca cebirsel kodlarla yapılabilmektedir. Bunlar dışında, kodlama teorisi, matematik ve mühendislik bilimlerinde kompakt disk kaydı, bilgi depolama, hücreli telefon iletimi gibi hemen hemen her alana uygulanabilir hale gelmiştir.

Kodlama teorisinde, hata kontrol eden kodlar, parazitli bir kanala bilgi gönderilmeden önce bilgiyi kodlamak için kullanılır. Böylece, bilgi kanaldan geçerken bozulsa bile, orijinal bilgi düzeltilebilir. Hata düzelten kodlar teorisinin (MacWilliams, Sloane, 1977) teorik alt yapısı matematik alanı olarak çalışılmaktadır. Kompakt diskler (CD) hata düzelten kodlar ailesinden olan Reed-Solomon kodları kullanırlar. Böylece bir CD çalar, CD üzerinde bilgi bozulmuş olsa bile, bilgiyi CD'den okuyabilir. Başka bir örnek olarak da, günümüzdeki cep telefonları düşünüldüğünde, aynı hat üzerinde aynı anda ve aynı bantı kullanan çok sayıda kullanıcı olmasına rağmen, bu kullanıcıların birbirinden bağımsız bir şekilde ve sesleri karışmadan konuşmaları verilebilir.

Kodlama Teorisi ilk olarak 1948 yılında Claude Shannon' ın, "A Mathematical Theory of Communication" [7] adlı makalesi ile başladı. Shannon, Amerika'da Bell laboratuvarlarında çalışarak, gönderilen ekstra bitlerin sayısının olabildiğince küçük olduğu mesajları kodlamanın mümkün olduğunu gösterdi. Ancak bu yaklaşım, optimal kodlar için bir çözüm yolu vermedi. İki yıl sonra Richard Hamming, Bell laboratuvarlarında, bilgi iletimi bakımından tekrar kodlarından daha etkili olan hata düzelten kodlar üzerinde çalıştı ve 4 bilgi bitini 3 kontrol bitinin takip ettiği bir kod üretti. Bu kod, hata tespit etmekle kalmayıp, ayrıca 1-hata düzeltebiliyordu. Shannon ve Hamming Amerika'da bilgi iletimi üzerine çalışırken, John Leech de Cambridge'de küre paketleme problemi ile ilgilendi ve bu çalışma 24-boyutlu Leech Latisi (Leech Kafesi) (Leech, 1964) ile sonuçlandı. Bu ise sonlu simetri gruplarını sınıflandırma için önemli bir adımdı.

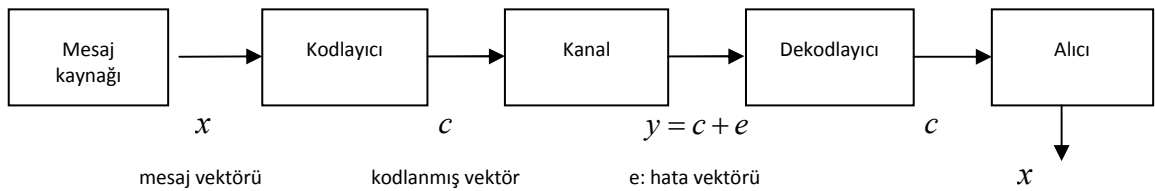
Bilgi iletimi için hata düzelten kodların değeri oldukça büyüktür. 1969 ve 1973 yılları arasında, NASA Mariner uzay roketi gönderilirken, 6 bilgi biti ve 26 kontrol biti olmak üzere toplam 32 bitlik kodsözden oluşan güçlü bir Reed-Muller kodu kullanıldı ve bu kod 7-hata düzeltiyordu. Bilginin saniyede 16.000 'bit' den fazlası dünyaya geri gönderildi.

Cebirsel Kodlama daha çok iletişim sistemlerinde yaygındır. İletişim sırasında, kullanıcının çevreye yaydığı sinyal, kozmik arka plan radyasyonu gibi sebeplerden kaynaklanan "gürültü (noise)" sebebiyle geliştirilmeye çalışılmıştır. Gürültü her daim iletişimin içinde olmuştur ve bilgiyi bozma yetisine sahiptir.

Bilgisayar bilimcileri, gürültüden kaynaklı hataların üstesinden gelmek için birçok yol geliştirdiler. Bunlardan en basiti parite-kontrol (parity check) metodudur. Bu metotta, bilgi bloğunun sonuna 0 ya da 1 eklenerek 1'lerin çift sayıda olması sağlanır. Kanaldan geçiş sırasında eğer bir bileşende hata meydana geldiyse alınan bilgide tek sayıda 1 vardır. Bu da alınan bilginin hatalı olduğunu gösterir ve böyle bir durumda yeniden iletim (gönderme) istenebilir. Fakat çoğu durumda parite kontrol biti ekleme işlemi kullanışlı olmayabilir. Örneğin, uydu iletişimi sırasında, yeniden gönderme işlemi oldukça pahalı ve zaman alıcı bir iştir. Genellikle bilgiyi kodlamak için en uygun yol, alıcının hatayı tespit edebileceği ve düzeltebileceği şekilde bir kodlama yapmaktır.

Sezgisel bir yaklaşım da tekrar ile yapılan kodlamadır. Bu kodlama şeklinde her bir bit n kez gönderilir. Örneğin, 00000 olarak gönderilen mesaj 00101 şeklinde alınmış olsun. Alınan bilgide 1'lerden çok 0'ların olduğu görüleceğinden, 00101 şeklinde alıcıya ulaşan mesaj 00000 şeklinde dekodlanacaktır. Böylece iki hata düzeltilmiş olur. Burada kullanılan koda “tekrar kodu” denir.

Kodlama teorisinin iki ana dalı kaynak kodlaması ve kanal kodlamasıdır. Kaynak kodlamasının temel teoremi 1948’de Claude Shannon tarafından verildi. Teorem, belli parametreleriyle verilen bir kodun mümkün olan en iyi hata düzeltmesinin nasıl olabileceğini ifade eder. Daha çok bilgisayar bilimleri ve mühendislik alanlarında kullanılır. Kanal kodlamasında ise daha çok hatalarla ilgilenilir. Kanal kodlamasında, hataları bulmanın tek yolu, ilgili mesaj üzerine bazı kısıtlamaların koyulmuş olmasıdır. Alıcı, alacağı mesajı tahmin etme gereksinimi duyar. Eğer mesaj uzayı tamamen mantıklı kodsözlerden oluşuyorsa, bu durumda herhangi bir hata bir kodsözü diğerine çevirecektir ve alıcı, aldığı kodsöz kodun içinden bir kodsöz olduğu için, onun gönderilen kodsöz olmadığını fark edemeyecektir. Burada şunu unutmamak gerekir ki, ilgili dekodlama metodu olmadan kodlamayı anlamak oldukça zordur. Temel durum, mesaja ekstra bileşen (bit) eklemektir. Aşağıdaki şekil temel bir kodlama şemasını göstermektedir.



Şekil 6. 1 Kodlama şeması

6.2 Temel Kavramlar

Tanım 6.1 [32] $A = \{a_1, a_2, \dots, a_q\}$, q elemandan oluşan bir küme olsun. A kümesine **kod alfabesi**, elemanlarına ise **kod sembolleri** denir. A üzerinde n uzunluğunda bir **söz** denilen; $\forall v_i \in A$ ($i = 1, \dots, n$) için, $v = v_1 v_2 \dots v_n$ şeklinde bir kümedir. ‘ v ’ sözü vektör notasyonu ile; $v = (v_1, v_2, \dots, v_n)$ şeklinde gösterilir. A kümesi üzerinde, n uzunluğundaki bütün sözlerin kümesi A^n ile gösterilir.

- i. A üzerinde n uzunluğunda bir kod aynı uzunluktaki (n) sözlerin bir $C \neq \emptyset$ kümesidir.
- ii. C 'nin elemanlarına **kodsözler** denir.
- iii. C 'deki kodsözlerin sayısına C 'nin **eleman sayısı** denir. M ile gösterilir.
- iv. Uzunluğu n , eleman sayısı M olan bir koda (n, M) kod denir. Burada n ve M **kodun parametreleri** olarak adlandırılır.

Özel olarak, $q = 2$ için $C \subseteq A^n$ koda **ikili kod**; $q = 3$ için $C \subseteq A^n$ koda **üçlü kod** denir.

Tanım 6.2 [32] x ve y , A üzerinde n uzunluğunda iki söz olsun. x ile y arasındaki **Hamming uzaklığı**, $d(x, y)$, x ve y nin koordinatlarının farklı oldukları yer sayısıdır.

Yani; $x = x_1x_2...x_n$, $y = y_1y_2...y_n$ olmak üzere;

$$d(x, y) = d(x_1, y_1) + d(x_2, y_2) + \dots + d(x_n, y_n)$$

şeklindedir. Burada,

$$d(x_i, y_i) = \begin{cases} 1, & x_i \neq y_i \\ 0, & x_i = y_i \end{cases}$$

şeklindedir.

Örnek 6.3 $x = 100011$, $y = 101101 \Rightarrow d(x, y) = 3$ 'tür.

Önerme 6.4 [32] $d : A^n \times A^n \rightarrow \mathbb{Z}$ uzaklık fonksiyonu bir metriktir:

- i. $0 \leq d(x, y) \leq n$,
- ii. $d(x, y) = 0 \Leftrightarrow x = y$,
- iii. $d(x, y) = d(y, x)$,
- iv. $d(x, z) \leq d(x, y) + d(y, z)$.

Tanım 6.5 [32] C , en az iki kodsözden oluşan bir kod olmak üzere, C 'nin **minimum uzaklığı**;

$$d(C) = \min \{d(x, y) : x, y \in C, x \neq y\}$$

şeklinde tanımlanır.

Tanım 6.6 [32] Uzunluğu n , eleman sayısı M ve (minimum) uzaklığı d olan bir koda (n, M, d) kod; n , M ve d elemanlarına da **kodun parametreleri** denir.

Örnek 6.7 $C = \{0000, 0101, 1111\}$ olmak üzere;

$$d(0000, 0101) = 2, \quad d(0000, 1111) = 4, \quad d(0101, 1111) = 2.$$

Buradan, C bir $(4, 3, 2)$ koddur.

Tanım 6.8 [32] $u \in \mathbb{Z}^+$ olsun. Eğer C deki bir kodsöz en az bir, en fazla u hataya maruz kaldığında sonuçtaki söz kodsöz değilse, C koda, u – **hata tespit eden kod** denir. Eğer bir C kod u – hata tespit edebilir fakat $(u+1)$ – hata tespit edemez ise, C 'ye **tam u – hata tespit eden kod** denir.

Örnek 6.9 $q = 2$ için $C = \{00000, 00111, 11111\}$ kodu 1 – hata tespit edebilir. Çünkü, C koddaki herhangi bir kodsözün koordinatlarından biri değiştiğinde (1 kere yer değiştirdiğimizde) sonuç bir kodsöz değildir. Fakat herhangi bir kodsözün iki hanesi değiştiğinde sonuç bir kodsöz olduğundan, C , 2 – hata tespit edemez.

Teorem 6.10 [32] Bir C kodun u – hata tespit edebilmesi için gerek ve yeter koşul $d(C) \geq u+1$ olmasıdır. Yani d minimum uzaklığına sahip bir kod tam $(d-1)$ – hata tespit edebilir.

Tanım 6.11 [32] $v \in \mathbb{Z}^+$ olsun. Eğer C , v ya da daha az hata düzeltebilir ise, C 'ye v – **hata düzelten kod** denir. Eğer bir C kodu v adet hata düzeltebilir fakat $(v+1)$ – hata düzeltemez ise, C **tam v – hata düzelten kod** denir.

Teorem 6.12 [32] Bir C kodun v -hata düzeltebilmesi için gerek ve yeter koşul, $d(C) \geq 2v+1$ olmasıdır. Yani d uzaklığında bir kod tam $\left\lfloor \frac{d-1}{2} \right\rfloor$ -hata düzeltebilir.

Burada $\lfloor x \rfloor$, x 'e eşit ya da x 'den küçük en büyük tam sayıdır.

Tanım 6.13 [32] K bir cisim ve $(V, +)$ bir Abel grubu olsun. Bir $K \times V \rightarrow V$ fonksiyonu için $(k, v) \mapsto kv$ olarak tanımlansın. $\forall k_1, k_2 \in K$ ve $\forall v_1, v_2 \in V$ için,

i. $k_1(v_1 + v_2) = k_1v_1 + k_1v_2,$

ii. $(k_1 + k_2)v_1 = k_1v_1 + k_2v_1,$

iii. $(k_1k_2)v_1 = k_1(k_2v_1),$

iv. $1v_1 = v_11.$

özellikleri sağlanıyorsa, V 'ye K cismi üzerinde bir **vektör uzayı** denir.

Not 6.14 Kodlama Teorisi'nde hata kontrol eden kodların cebirsel yapılarını incelemek için alfabe sonlu bir cisim olarak seçilir. q elemanlı sonlu bir cisim, F_q ya da $GF(q)$ ile gösterilir. Kod sembolleri F_q 'dan alınan n uzunluğundaki bütün vektörlerin kümesi F_q^n ile gösterilir:

$$F_q^n = \{(v_1, v_2, \dots, v_n) : v_i \in F_q\}.$$

Açıktır ki; F_q^n kümesi bir vektör uzayıdır.

Tanım 6.15 [32] F_q üzerinde n uzunluğunda bir C **lineer kod**, F_q^n vektör uzayının bir alt vektör uzayıdır.

Tanım 6.16 [32] C , F_q^n vektör uzayında bir lineer kod olsun.

i. C 'nin *duali*: $C^\perp = \{x \in F_q^n : \langle x, c \rangle = 0, \forall c \in C\}$ şeklindedir. Burada,

$$\langle x, y \rangle = \sum_{i=1}^n x_i y_i$$

şeklindedir (Öklid İç Çarpımı).

ii. C lineer kodun boyutu, C 'nin, F_q^n üzerinde vektör uzayı olarak boyutudur ve $\dim(C)$ ile gösterilir.

Tanım 6.17 [32] F_q üzerinde, uzunluğu n , boyutu $\dim(C)=k$ olan bir kod $[n, k]_q$ – kod; uzunluk ve boyuta ek olarak minimum uzaklığı d olan bir lineer kod da $[n, k, d]_q$ – kod şeklinde gösterilir.

Tanım 6.18 [32] Bir $C [n, k]_q$ – kodu, F_q^n uzayının bir alt uzayıdır. Dolayısıyla bir bazı vardır. C nin bir bazı $\{c_1, c_2, \dots, c_k\}$ olsun. Bazdaki vektörleri satır kabul eden G matrisine, C kodun **üreteç matrisi** denir ve aşağıdaki şekilde verilir:

$$G = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{bmatrix}_{k \times n}.$$

G 'nin satırları bazdan seçildiğinden, bu satırlar lineer bağımsızdır. Bu nedenle, C 'deki her kodsöz G 'nin satırlarının bir F_q lineer kombinasyonu olarak yazılabilir. O halde her bir lineer kod üreteç matrisi ile belirlidir; yani üreteç matrisi bir kodu tam anlamıyla temsil eder. Bir kodun birden fazla üreteç matrisi olabilir. Bir üreteç matrisi, kendisinden çeşitli sütun dönüşümleri ile elde edilen yeni üreteç matrislerine denktir. Böylece denk kodlar elde edilebilir.

C bir $[n, k]_q$ – kod ise, G üreteç matrisi $k \times n$ tipindedir.

Tanım 6.19 [32] G matrisi bir $C [n, k]_q$ – kodun üreteç matrisi olsun. $G = [I_k \mid A]_{k \times n}$ ise, G matrisinin standart formda olduğu söylenir.

Örnek 6.20 $C = \{000000, 100100, 010010, 110110, 001001, 101101, 011011, 111111\}$

lineer kodu verilsin. C bir $[6, 3]_2$ – koddur ve C 'nin bir üreteç matrisi ise aşağıdaki gibidir:

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

Örnek 6.21 F_5 cismi üzerinde bir lineer kodun üreteç matrisi olarak

$$G = \begin{bmatrix} 2 & 2 & 2 & 2 & 1 \\ 2 & 2 & 1 & 2 & 1 \\ 2 & 2 & 1 & 1 & 1 \end{bmatrix}$$

verilsin. G , standart formda aşağıdaki şekilde yazılır:

$$\begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 \end{matrix} \\ \begin{bmatrix} 2 & 2 & 2 & 2 & 1 \\ 2 & 2 & 1 & 2 & 1 \\ 2 & 2 & 1 & 1 & 1 \end{bmatrix}_{H_1(3)} \approx \begin{bmatrix} 1 & 1 & 1 & 1 & 3 \\ 2 & 2 & 1 & 2 & 1 \\ 2 & 2 & 1 & 1 & 1 \end{bmatrix}_{H_{21}(-2), H_{31}(-2)} \approx \begin{bmatrix} 1 & 1 & 1 & 1 & 3 \\ 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 4 & 0 \end{bmatrix}_{H_2(4), H_3(4)} \approx \\ \begin{matrix} 1 & 3 & 4 & 2 & 5 \end{matrix} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 3 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}_{K_{34}, K_{23}} \approx \begin{bmatrix} 1 & 1 & 1 & 1 & 3 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix}_{H_{13}(4), H_{32}(4)} \approx \begin{bmatrix} 1 & 0 & 0 & 1 & 3 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} = G'. \end{array}$$

Burada elde edilen G' üreteç matrisi, G 'nin ürettiği koda denk bir kod üretir. Çünkü G üzerinde sütun dönüşümleri yapılmıştır. Yapılan sütun dönüşümleri G' matrisinde geri alınırsa, G matrisine dönülür. O halde bir üreteç matrisini standart formda yazmak her zaman mümkündür ancak; bulduğumuz üreteç matrisi verilen koda ya da ona denk olan başka bir koda aittir. Kodlama Teorisi'nde denk kodlar birbiri ile aynı düşünülür. Çünkü kodlama bakımından çoğu özellikleri aynıdır: Eleman sayıları, uzunlukları, minimum uzaklıkları (dolayısıyla hata düzeltme kapasiteleri), vs.

BAZI HALKALAR ÜZERİNDE LİNEER KODLARI SAYMA PROBLEMİ

7.1 Giriş

Hata düzelten kodlar teorisi ilk zamanlarda cisimler üzerine inşa edilmişti. Halkalar üzerinde kod çalışmaları ile ilgili ilk önemli çalışma, 1994 yılında P. Vijay Kumar ve arkadaşlarının “The $\mathbb{Z}_4$ -Linearity of Kerdock, Preparata, Goethals and Related Codes” [8] adlı çalışmalarıdır. Bu çalışmada, lineer olmayan kodların $\mathbb{Z}_4$ -lineerliğinden bahsedilmiştir. İlerleyen yıllarda ise farklı özel halkalar üzerinde kod yapıları incelenmiştir. Bu bölümde ilk olarak, literatürde mevcut olan, cisimler üzerinde kodların sayısını veren formül verilecek, daha sonra ise bundan yola çıkılarak elde edilen, $\mathbb{Z}_{p^m}$ halkası ve Galois halkaları üzerinde kodların sayılarını veren formüller ve ilgili örnekler verilecektir. Son kısımda ise, bu çalışmaların bir genelleştirilmesi olan sonlu zincir halkaları üzerinde kodların sayısı verilecektir.

7.2 F_q Cismi Üzerinde Lineer Kodların Sayısı

F_q cismi üzerinde lineer kodların sayısı, Gauss binom katsayıları olarak adlandırılan sayılar ile belirlidir. Bu katsayılar ile ilgili tanım ve özellikler Bölüm 5’de verilmiştir.

Teorem 7.1 [31] q asal bir sayı olmak üzere, F_q üzerinde n uzunluğunda, boyutu k olan ayrık (permütasyon denk olanlar da dahil) kodların sayısı $\begin{bmatrix} n \\ k \end{bmatrix}_q$ sayısıdır.

$R = \mathbb{Z}_{p^m}$ halkası modülo p^m ’de (p asal, $m \in \mathbb{Z}^+$) tam sayıların sonlu bir halkası olsun.

Tanım 7.2 [31] R^n ’in bir C alt modülüne bir R – lineer kod denir.

Teorem 7.3 [33] R üzerinde bir C lineer kod aşağıdaki formdaki üreteç matrisine sahip bir koda permütasyon denktir:

$$\begin{pmatrix} I_{k_1} & A_{11} & A_{12} & \dots & A_{1s} \\ 0 & pI_{k_2} & pA_{22} & \dots & pA_{2s} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & p^{m-1}I_{k_m} & p^{m-1}A_{ms} \end{pmatrix} \quad (7.1)$$

(7.1)'deki matriste $A_{ij} \in R$ ve $I_{k_1}, I_{k_2}, \dots, I_{k_m}$ matrisleri, tipleri sırasıyla $k_1, k_2, \dots, k_m$ olan birim matrislerdir. C kodun eleman sayısı $p^{\sum_{i=1}^m k_i(m-i+1)}$ 'dir.

(7.1)'de verilen matris ile üretilen kodun $(k_1, k_2, \dots, k_m)$ – tipinde olduğu söylenir.

7.3 $\mathbb{Z}_{p^m}$ Halkası Üzerinde Lineer Kodların Sayısı

Tanım 7.4 $q = p^m$ ve $v \in \mathbb{Z}_q^n$ olsun. v 'nin $\mathbb{Z}_q^n$ toplamsal grubundaki mertebesi $o(v)$ ile gösterilir.

Buradan itibaren aksi belirtilmedikçe $q = p^m$ olarak alınacaktır.

Tanım 7.5 $\mathbb{Z}_q$ üzerinde uzunluğu n ve tipi $(k_1, k_2, \dots, k_m)$ olan koda $[n, (k_1, k_2, \dots, k_m)]$ – kod denir. Burada $k_1 + k_2 + \dots + k_m \leq n$ dir.

Teorem 7.6 $\mathbb{Z}_q$ üzerinde ayrık (permütasyon denk olanlar ile birlikte)

$[n, (k_1, k_2, \dots, k_m)]$ lineer kodların sayısı

$$\left[\begin{matrix} n \\ k_1, k_2, \dots, k_m \end{matrix} \right]_q = N_{k_1, k_2, \dots, k_m}^q(n) = \frac{A}{B} \quad (7.2)$$

sayısıdır. Burada,

$$A = \prod_{t=1}^m \prod_{i=0}^{k_t-1} \left(\left(p^{m-(t-1)} \right)^n - \left(p^{m-1-(t-1)} \right)^n \cdot p^{\sum_{j=0}^{t-1} k_j} \cdot p^i \right),$$

$$B = \prod_{s=1}^m \prod_{r=0}^{k_s-1} \left(\prod_{z=1}^s \left(p^{m-(s-1)} \right)^{k_z} \prod_{j=s+1}^m \left(p^{m-(j-1)} \right)^{k_j} - \left(\prod_{z=1}^s \left(p^{m-s} \right)^{k_z} \right) \left(p^{m-(s-1)} \right)^{k_{s+1}} \cdot \prod_{t=s+2}^m \left(p^{m-(t-1)} \right)^{k_t} \cdot p^r \right)$$

şeklindedir.

İspat: $\mathbb{Z}_q$ üzerinde n uzunluğunda, ayrık, tipi $k_1, k_2, \dots, k_m$ olan lineer kodları incelemek için, bu kodların üreteç matrislerini inşa etmek ve üreteç matrislerinin sayılarını bulmak gerekir. Böyle bir kodun üreteç matrisini inşa etmek için mertebesi p^{m-i+1} olan k_i ($i \in \{1, 2, \dots, m\}$) adet sıralı lineer bağımsız eleman seçilecektir:

$$S = \left(v_1^{(p^m)}, v_2^{(p^m)}, \dots, v_{k_1}^{(p^m)}; v_1^{(p^{m-1})}, \dots, v_{k_2}^{(p^{m-1})}; v_1^{(p^{m-2})}, \dots, v_{k_3}^{(p^{m-2})}; \dots, v_1^{(p^2)}, v_2^{(p^2)}, \dots, v_{k_{m-1}}^{(p^2)}; v_1^{(p)}, v_2^{(p)}, \dots, v_{k_m}^{(p)} \right)$$

Burada $v_i^{(j)}$, mertebesi j olan i ninci elemanı göstermektedir, $p \leq j \leq p^m$, $1 \leq i \leq k_z$ ($1 \leq z \leq m$).

İlk olarak, $\mathbb{Z}_q^n$ grubundan mertebesi p^{m-i+1} olan k_i ($i \in \{1, 2, \dots, m\}$) adet sıralı lineer bağımsız eleman seçilecektir. Bu seçimlerin sayısı A olsun. Öte yandan, $\mathbb{Z}_q$ üzerinde, uzunluğu n , tipi $(k_1, k_2, \dots, k_m)$ olan lineer kodların sayısı N olsun. İkinci durum olarak, bu kodların içinden, mertebesi p^{m-i+1} olan k_i ($i \in \{1, 2, \dots, m\}$) adet sıralı lineer bağımsız eleman (kodsöz) seçilecektir. Bu seçimlerin sayısı da B olsun. Bu kod ile aynı tip ve uzunlukta N kod mevcut olduğundan, ikinci durumdaki tüm seçimlerin sayısı $N.B$ olacaktır. Dolayısıyla $\mathbb{Z}_q^n$ grubu taranmış olacaktır. Bu durumda, $\mathbb{Z}_q^n$ grubundan yapılacak seçimler: $N.B$ şeklindedir. Öte yandan ilk durumda tüm kümeden ($\mathbb{Z}_q^n$) yapılan seçimlerin sayısı A idi. O halde son durumda,

$$A = N.B$$

eşitliği elde edilir ki buradan da istenen sayı, N , hesaplanır. Aşağıda, A ve B sayılarının bulunuşu detaylı bir şekilde açıklanmaktadır.

$\mathbb{Z}_q^n$ grubunda toplam $q^n = (p^m)^n$ eleman vardır. Bu elemanlardan, ilk olarak $v_1^{(p^m)}$ elemanı seçilmektedir. $v_1^{(p^m)}$ elemanı mertebesi p^m olan bir elemandır. O halde bu

elemanın n bileşeninden en az biri $\mathbb{Z}_q$ halkasının bir birimsel elemanıdır. Çünkü mertebesi p^m olan elemanlar $\mathbb{Z}_q$ halkasının birimsel elemanlarıdır. Bu elemanı seçmek için tüm elemanlardan mertebesi p^m olmayanları çıkarmak gerekir. $\mathbb{Z}_q$ halkasındaki birimsel elemanların sayısı Euler fi fonksiyonu yardımıyla hesaplanır: $\phi(p^m) = p^{m-1}(p-1)$. Bu durumda mertebesi p^m olmayan elemanlar $p^m - \phi(p^m) = p^{m-1}$ dir. $\mathbb{Z}_q^n$ halkasındaki elemanlar için (n bileşen için) düşünülürse, mertebesi p^m olmayan elemanların sayısı $(p^{m-1})^n$ dir. O halde, $v_1^{(p^m)}$ eleman $(p^m)^n - (p^{m-1})^n$

farklı şekilde seçilir.

Sıralı seçim yapıldığı için, ikinci olarak, $\langle v_1^{(p^m)}, v_2^{(p^m)} \rangle = C_2$ ve $|C_2| = (p^m)^2$ olacak şekilde $v_2^{(p^m)}$ elemanı seçilmektedir. Bu eleman da mertebesi p^m olan bir elemandır. İlk elemanın seçimine benzer şekilde, mertebesi p^m olmayan elemanlar alınmayacaktır. Fakat bu, yeterli değildir. Taban oluşturulduğundan, ilk seçilen $v_1^{(p^m)}$ elemanı ile lineer bağımlı olan elemanların da dikkate alınması (yani çıkarılması) gerekir. $v_2^{(p^m)}$ elemanı olarak seçilemeyecek elemanların kümesi:

$$K_2 = \left\{ \alpha_1 v_1^{(p^m)} + w \mid w \in \mathbb{Z}_{p^m}^n, o(w) \neq p^m, \alpha_1 \in \mathbb{Z}_p \right\}$$

kümesidir.

($\mathbb{Z}_4^3$ kümesi göz önüne alındığında, $v_1 = (1, 0, 0) \in \mathbb{Z}_4^3$ vektörü için,

$$K_2 = \{(0, 0, 0), (0, 0, 2), (0, 2, 0), (2, 0, 0), (0, 2, 2), (2, 0, 2), (2, 2, 0), (2, 2, 2), (1, 0, 2), (1, 2, 0), (3, 0, 0), (1, 2, 2), (3, 0, 2), (3, 2, 0), (3, 2, 2), (3, 2, 2)\}$$

şeklindedir.)

$|K_2| = (p^{m-1})^n p$ olduğundan, $v_2^{(p^m)}$ elemanı için

$$(p^m)^n - (p^{m-1})^n \cdot p$$

farklı seçim yolu vardır. Benzer şekilde, $\left\langle C_2 \cup \left\{ v_3^{(p^m)} \right\} \right\rangle = C_3$ ve $|C_3| = (p^m)^3$ olacak

şekilde $v_3^{(p^m)}$ elemanının seçimi yapılacaktır. Tüm durumlardan aşağıdaki kümenin eleman sayısının çıkarılması gerekir:

$$K_3 = \left\{ \alpha_1 v_1^{(p^m)} + \alpha_2 v_2^{(p^m)} + w \mid w \in \mathbb{Z}_{p^m}^n, o(w) \neq p^m, \alpha_1, \alpha_2 \in \mathbb{Z}_p \right\}.$$

$|K_3| = (p^{m-1})^n p^2$ olduğundan, $v_3^{(p^m)}$ elemanı için

$$(p^m)^n - (p^{m-1})^n \cdot p^2$$

farklı seçim yolu vardır.

Benzer şekilde devam edilirse, p^m mertebeli k_1 . eleman, $v_{k_1}^{(p^m)}$, $\left\langle C_{k_1-1} \cup \left\{ v_{k_1}^{(p^m)} \right\} \right\rangle = C_{k_1}$

ve $|C_{k_1}| = (p^m)^{k_m}$ olacak şekilde seçilir. Bu seçim yapılırken seçilemeyecek elemanların kümesi:

$$K_{k_1} = \left\{ \alpha_1 v_1^{(p^m)} + \alpha_2 v_2^{(p^m)} + \dots + \alpha_{k_1-1} v_{k_1-1}^{(p^m)} + w \mid w \in \mathbb{Z}_{p^m}^n, o(w) \neq p^m, \alpha_i \in \mathbb{Z}_p, i = 1, 2, \dots, k_1 - 1 \right\}$$

kümesidir. $|K_{k_1}| = (p^{m-1})^n p^{k_1-1}$ olduğundan, k_1 . eleman,

$$(p^m)^n - (p^{m-1})^n \cdot p^{k_1-1}$$

farklı şekilde seçilir.

O halde, $\mathbb{Z}_q$ halkasından mertebesi p^m olan k_1 adet eleman seçimi için aşağıdaki kadar farklı yol vardır:

$$\begin{aligned} & \left((p^m)^n - (p^{m-1})^n \right) \left((p^m)^n - (p^{m-1})^n \cdot p \right) \left((p^m)^n - (p^{m-1})^n \cdot p^2 \right) \dots \left((p^m)^n - (p^{m-1})^n \cdot p^{k_1-1} \right) \\ &= \prod_{j=0}^{k_1-1} \left\{ (p^m)^n - (p^{m-1})^n \cdot p^j \right\}. \end{aligned}$$

Şimdi $\mathbb{Z}_q^n$ halkasından mertebesi p^{m-1} olan k_2 adet sıralı eleman seçimi yapılacaktır.

Bu durumda p^{m-1} mertebeli elemanların kümesi düşünülüp, bunların sayısından, p^{m-1} mertebeli olmayanların sayısı çıkarılacaktır. Burada düşünülmesi gereken bir diğer durum da, daha önceden seçilen p^m mertebeli k_2 adet elemandır. Çünkü bu elemanlarla lineer bağımlı olan elemanlar seçilemez. Yani, $v_1^{(p^{m-1})}$ elemanı,

$\left\langle C_{k_1} \cup \left\{ v_1^{(p^{m-1})} \right\} \right\rangle = C_{k_1+1}$ ve $|C_{k_1+1}| = (p^m)^{k_1} (p^{m-1})^1$ olacak şekilde seçilir. O halde bu seçim

yapılırken seçilemeyecek elemanların kümesi aşağıdaki K_{k_1+1} kümesidir:

$$K_{k_1+1} = \left\{ \alpha_1 v_1^{(p^m)} + \alpha_2 v_2^{(p^m)} + \dots + \alpha_{k_1} v_{k_1}^{(p^m)} + w \mid w \in \mathbb{Z}_{p^m}^n, o(w) \leq p^{m-1}, \alpha_i \in \mathbb{Z}_p, i=1,2,\dots,k_1 \right\}.$$

$|K_{k_1+1}| = (p^{m-2})^n \cdot p^{k_1}$ olduğundan ve $\mathbb{Z}_q$ halkasında mertebesi $\leq p^{m-1}$ olan $(p^{m-1})^n$ adet

eleman bulunduğundan, $v_1^{(p^{m-1})}$ elemanı için yapılabilecek seçimlerin sayısı:

$$(p^{m-1})^n - (p^{m-2})^n \cdot p^{k_1}$$

sayısıdır.

Mertebesi p^{m-1} olan ikinci eleman, $v_2^{(p^{m-1})}$, $\left\langle C_{k_1+1} \cup \left\{ v_2^{(p^{m-1})} \right\} \right\rangle = C_{k_1+2}$ ve

$|C_{k_1+2}| = (p^m)^{k_1} (p^{m-1})^2$ olacak şekilde seçilir. Yine diğer elemanların seçimine benzer

şekilde, bu elemanı seçmek için, mertebesi p^{m-1} ve daha küçük olan elemanların sayısından, önceki seçilen elemanlar ile lineer bağımlı olan elemanların sayısının

çıkarılması gerekir. O halde, benzer şekilde, gerekli işlemler yapıldıktan sonra, $v_2^{(p^{m-1})}$

elemanını seçmek için,

$$(p^{m-1})^n - (p^{m-2})^n \cdot p^{k_1} \cdot p$$

kadar farklı yol vardır. Aynı şekilde devam edilirse, p^{m-1} mertebeli k_2 . eleman,

$$\left\langle C_{k_1+1} \cup \left\{ v_2^{(p^{m-1})} \right\} \right\rangle = C_{k_1+2} \quad \text{ve} \quad |C_{k_1+2}| = (p^m)^{k_1} (p^{m-1})^2 \quad \text{olacak} \quad \text{şekilde}$$

$$(p^{m-1})^n - (p^{m-2})^n \cdot p^{k_1} \cdot p^{k_2-1} \text{ kadar farklı yolla seçilir.}$$

O halde, $\mathbb{Z}_q$ halkasından mertebesi p^{m-1} olan k_2 adet eleman seçimi için aşağıdaki kadar farklı yol vardır:

$$\begin{aligned} & \left((p^{m-1})^n - (p^{m-2})^n \cdot p^{k_1} \right) \left((p^{m-1})^n - (p^{m-2})^n \cdot p^{k_1+1} \right) \left((p^{m-1})^n - (p^{m-2})^n \cdot p^{k_1+2} \right) \\ & \dots \left((p^{m-1})^n - (p^{m-2})^n \cdot p^{k_1+k_2-1} \right) = \prod_{j=0}^{k_2-1} \left((p^{m-1})^n - (p^{m-2})^n \cdot p^{k_1+j} \right). \end{aligned}$$

Mertebesi $p^{m-2}, p^{m-3}, \dots, p^2$ olan elemanların seçimi de benzer şekilde yapılır. Son olarak da mertebesi p olan elemanlar seçilir. Mertebesi p olan ilk eleman, $v_1^{(p)}$

$$\text{elemanı, } \left\langle C_{k_1+k_2+\dots+k_{m-1}+1} \cup \left\{ v_2^{(p^m)} \right\} \right\rangle = C_{k_1+k_2+\dots+k_{m-1}+1} \quad \text{ve}$$

$$|C_{k_1+k_2+\dots+k_{m-1}+1}| = (p^m)^{k_1} (p^{m-1})^{k_2} (p^{m-2})^{k_3} \dots (p^2)^{k_{m-1}} \cdot p \text{ olacak şekilde seçilir. Bu seçim için}$$

$$(p)^n - (p^0)^n p^{k_1+k_2+\dots+k_{m-1}} \cdot p^0$$

kadar yol vardır. $v_2^{(p)}$ elemanı için de benzer şekilde düşünülürse, seçim için yolların sayısı

$$(p)^n - (p^0)^n p^{k_1+k_2+\dots+k_{m-1}} \cdot p^{k_{m-1}} \cdot p^1$$

sayısıdır. Benzer şekilde, k_m . eleman, $v_{k_m}^{(p)}$,

$$(p)^n - (p^0)^n p^{k_1+k_2+\dots+k_{m-1}} \cdot p^{k_{m-1}} \cdot p^{k_m-1}$$

farklı şekilde seçilir.

Benzer şekilde devam edilirse, mertebesi p olan k_m adet eleman aşağıdaki kadar farklı yolla seçilir:

$$\left((p)^n - (p^0)^n p^{k_1+k_2+\dots+k_{m-1}} \cdot p^0 \right) \left((p)^n - (p^0)^n p^{k_1+k_2+\dots+k_{m-1}} \cdot p^{k_{m-1}} \cdot p^1 \right) \dots \left((p)^n - (p^0)^n p^{k_1+k_2+\dots+k_{m-1}} \cdot p^{k_{m-1}} \cdot p^{k_{m-1}-1} \right).$$

Sonuç olarak, $\mathbb{Z}_q^n$ halkasından mertebesi p^{m-i+1} olan k_i , $i \in \{1, 2, \dots, m\}$ adet elemanın seçimi için tüm yolların sayısı:

$$\prod_{t=1}^n \prod_{i=0}^{k_t-1} \left((p^{m-(t-1)})^n - (p^{m-1-(t-1)})^n \cdot p^{\sum_{j=0}^{t-1} k_j} \cdot p^j \right) \quad (7.3)$$

sayısıdır.

Öte yandan, $\mathbb{Z}_q$ üzerinde, uzunluğu n , tipi $(k_1, k_2, \dots, k_m)$ olan kodların sayısı N olsun:

$C_1, C_2, \dots, C_N$. Bu kodlardan biri göz önüne alınmaktadır: $C_\alpha, \alpha \in \{1, 2, \dots, N\}$. C_α koddan, mertebesi p^{m-i+1} olan k_i , $i \in \{1, 2, \dots, m\}$ adet kodsöz (eleman) seçilmektedir.

C_α 'da toplam $(p^m)^{k_1} (p^{m-1})^{k_2} \dots (p^2)^{k_{m-1}} (p)^{k_m}$ kodsöz vardır. C_α 'da mertebesi j olan i ninci kodsöz $u_i^{(j)}$ olsun. İlk olarak, $u_1^{(p^m)}$ kodsözünün seçimi yapılacaktır. Mertebesi p^m olan bir elemanla üretilen bir kodun, mertebesi p^m olmayan $\frac{p^m}{p}$ adet kodsözü vardır.

O halde $u_1^{(p^m)}$ elemanını seçmek için tüm durumlardan mertebesi p^m olmayanları ($< p^m$) çıkarmak gerekir. O halde yapılabilecek seçimlerin sayısı aşağıdaki gibidir:

$$E_1^{(1)} = (p^m)^{k_1} (p^{m-1})^{k_2} \dots (p^2)^{k_{m-1}} (p)^{k_m} - (p^{m-1})^{k_1} (p^{m-1})^{k_2} \dots (p^2)^{k_{m-1}} (p)^{k_m}.$$

C_α koddan $u_2^{(p^m)}$ kodsözü $\hat{C}_2 = \langle u_1^{(p^m)}, u_2^{(p^m)} \rangle$ ve $|\hat{C}_2| = (p^m)^2$ olacak şekilde seçilir. $v_2^{(p^m)}$

kodsözünün seçiminde yapıldığı gibi, C_α 'nın eleman sayısından aşağıdaki kümenin eleman sayısını çıkarmak gerekir:

$$K_2 = \left\{ \alpha_1 u_1^{(p^m)} + w : w \in C, o(w) < p^{m-1}, \alpha_1 \in \mathbb{Z}_p \right\}.$$

Dolayısıyla, C_α koddan $u_2^{(p^m)}$ kodsözü,

$$E_1^{(2)} = (p^m)^{k_1} (p^{m-1})^{k_2} \dots (p^2)^{k_{m-1}} (p)^{k_m} - (p^{m-1})^{k_1} (p^{m-1})^{k_2} \dots (p^2)^{k_{m-1}} (p)^{k_m} \cdot p^1$$

farklı şekilde seçilir.

Benzer şekilde devam edilirse, k_1 . kodsöz, $u_{k_1}^{(p^m)}$, $\hat{C}_{k_1} = \langle \hat{C}_{k_1-1}, u_{k_1}^{(p^m)} \rangle$ ve $|\hat{C}_{k_1}| = (p^m)^{k_1}$

olacak şekilde seçilir. O halde, $u_{k_1}^{(p^m)}$ elemanı,

$$E_1^{(k_1)} = (p^m)^{k_1} (p^{m-1})^{k_2} \dots (p^2)^{k_{m-1}} (p)^{k_m} - (p^{m-1})^{k_1} (p^{m-1})^{k_2} \dots (p^2)^{k_{m-1}} (p)^{k_m} \cdot p^{k_1-1}$$

farklı şekilde seçilir.

Tüm $E_1^{(i)}$, $(i=1,2,\dots,k_1)$ sayılarının çarpımı, C_α koddan mertebesi p^m olan k_1 adet kodsözün seçiminin sayısını verir:

$$I^{(1)} = E_1^{(1)} \cdot E_1^{(2)} \dots E_1^{(k_1)}.$$

Mertebesi p^{m-1} olan k_2 adet lineer bağımsız eleman seçimi için aşağıdaki yollar izlenir.

$u_1^{(p^{m-1})}$ kodsözü, $\hat{C}_{k_1+1} = \langle \hat{C}_{k_1}, u_1^{(p^{m-1})} \rangle$ ve $|\hat{C}_{k_1+1}| = (p^m)^{k_1} (p^{m-1})$ olacak şekilde belirlenir.

C_α kodda, mertebesi $\leq p^{m-1}$ olan elemanların sayısı

$(p^{m-1})^{k_1} (p^{m-1})^{k_2} (p^{m-2})^{k_3} \dots (p^2)^{k_{m-1}} (p)^{k_m}$ 'dir. Mertebesi p^{m-1} olan bir eleman, eleman

sayısı p^{m-1} olan bir kod üretir ve bu kodun, mertebesi p^{m-1} den farklı olan elemanların

sayısı $\frac{p^{m-1}}{p} = p^{m-2}$ 'dir. Bu durumda, $u_1^{(p^{m-1})}$ elemanının seçimi için tüm durumların sayısı

aşağıdaki $E_2^{(1)}$ sayısıdır:

$$E_2^{(1)} = (p^{m-1})^{k_1} (p^{m-1})^{k_2} \dots (p^2)^{k_{m-1}} (p)^{k_m} - (p^{m-1})^{k_1} (p^{m-2})^{k_2} (p^{m-2})^{k_3} \dots (p^2)^{k_{m-1}} (p)^{k_m}.$$

Benzer şekilde mertebesi p^{m-1} olan tüm elemanlar seçilir ve sonuncusu, $u_{k_2}^{(p^{m-1})}$, için seçim yolları aşağıdaki gibidir:

$$E_2^{(k_2)} = (p^{m-1})^{k_1} (p^{m-1})^{k_2} (p^{m-2})^{k_3} \dots (p^2)^{k_{m-1}} (p)^{k_m} - (p^{m-1})^{k_1} (p^{m-2})^{k_2} (p^{m-2})^{k_3} \dots (p^2)^{k_{m-1}} (p)^{k_m} \cdot p^{k_2-1}.$$

Tüm $E_2^{(i)}$, $(i=1,2,\dots,k_2)$ sayılarının çarpımı, C_α koddan mertebesi p^{m-1} olan k_2 adet kodsözün seçiminin sayısını verir:

$$I^{(2)} = E_2^{(1)} . E_2^{(2)} \dots E_2^{(k_2)} .$$

Benzer şekilde tüm $E_i^{(j)}$, $(1 \leq i \leq k_i (i \in \{1,2,\dots,m\}), p \leq j \leq p^m)$, sayıları hesaplanır ve buradan da $I^{(t)}$, $t=1,2,\dots,k_m$, sayıları hesaplanır. Dolayısıyla C_α koddan mertebesi p^{m-i+1} olan k_i , $i \in \{1,2,\dots,m\}$ adet kodsöz seçimi için tüm yolların sayısı:

$$I^{(1)} . I^{(2)} \dots I^{(k_m)}$$

sayısıdır.

$\mathbb{Z}_q$ üzerinde, uzunluğu n , tipi $(k_1, k_2, \dots, k_m)$ olan kodların sayısı N olarak alınmıştır. O halde, C_α koddan yapılan seçimlerin sayısından N adet mevcuttur. Bu durumda,

$$I^{(1)} . I^{(2)} \dots I^{(k_m)} . N \quad (7.4)$$

sayısı, $\mathbb{Z}_q^n$ halkasından mertebesi p^{m-i+1} olan k_i , $i \in \{1,2,\dots,m\}$ adet elemanın seçiminin sayısını verir. O halde (7.3) de hesaplanan sayı ile (7.4)'deki sayılar birbirine eşittir:

$$I^{(1)} . I^{(2)} \dots I^{(k_m)} . N = \prod_{t=1}^n \prod_{i=0}^{k_i-1} \left(\left(p^{m-(t-1)} \right)^n - \left(p^{m-1-(t-1)} \right)^n . p^{\sum_{j=0}^{t-1} k_j} . p^j \right).$$

Buradan, N hesaplanır:

$$N = \frac{\prod_{t=1}^n \prod_{i=0}^{k_i-1} \left(\left(p^{m-(t-1)} \right)^n - \left(p^{m-1-(t-1)} \right)^n . p^{\sum_{j=0}^{t-1} k_j} . p^j \right)}{I^{(1)} . I^{(2)} \dots I^{(k_m)}} \quad (7.5)$$

(7.5)'de payda kısmı toparlanırsa,

$$I^{(1)} . I^{(2)} \dots I^{(k_m)} =$$

$$\prod_{s=1}^m \prod_{r=0}^{k_s-1} \left(\prod_{z=1}^s (2^{m-(s-1)})^{k_z} \prod_{j=s+1}^m (2^{m-(j-1)})^{k_j} - \left(\prod_{z=1}^s (2^{m-s})^{k_z} \right) (2^{m-(s+1)})^{k_{s+1}} \cdot \prod_{t=s+2}^m (2^{m-(t-1)})^{k_t} \cdot 2^r \right) \quad (7.6)$$

elde edilir.

Sonuç 7.7 Özel olarak, $k_1 = 0$, $m = 1$ için cisimler üzerinde kodların sayısını veren formül (Gauss binom katsayıları) elde edilir.

Sonuç 7.8 $\mathbb{Z}_4$ üzerinde ayrık $[n, (k_1, k_2)]$ – kodların sayısı

$$\left[\begin{matrix} n \\ k_1, k_2 \end{matrix} \right]_4 = N_{k_1, k_2}^4(n) = \frac{\prod_{i=0}^{k_1-1} (4^n - 2^{n+i}) \prod_{j=0}^{k_2-1} (2^n - 2^{k_1+i})}{\prod_{t=0}^{k_1-1} (4^{k_1} \cdot 2^{k_2} - 2^{k_1+k_2+t}) \prod_{l=0}^{k_2-1} (2^{k_1} \cdot 2^{k_2} - 2^{k_1+l})}$$

sayısıdır.

Çizelge 7. 1 Bazı n ’ler için $\mathbb{Z}_4$ üzerinde lineer kodların sayısı

$\begin{matrix} n \\ \text{Tip} \end{matrix}$	n=3	n=4	n=5	n=6	$\begin{matrix} n \\ \text{Tip} \end{matrix}$	n=3	n=4	n=5	n=6
(0,1)	7	15	31	63	(2,2)	--	35	4340	36456
(0,2)	7	35	155	651	(2,3)	--	--	155	39060
(0,3)	1	15	155	1395	(2,4)	--	--	--	651
(0,4)	--	1	31	651	(3,0)	1	120	9920	714240
(0,5)	--	--	1	63	(3,1)	--	15	3720	624960
(0,6)	--	--	--	1	(3,2)	--	--	155	78120
(1,0)	28	120	496	2016	(3,3)	--	--	--	1395
(1,1)	42	420	3720	31248	(4,0)	--	1	496	166656
(1,2)	7	210	4340	78120	(4,1)	--	--	31	31248
(1,3)	--	15	930	39060	(4,2)	--	--	--	651
(1,4)	--	--	31	3906	(5,0)	--	--	1	2016

Çizelge 7. 2 Bazı n 'ler için $\mathbb{Z}_4$ üzerinde lineer kodların sayısı (devam)

(1,5)	--	--	--	63	(5,1)	--	--	--	63
(2,0)	28	560	9920	166656	(6,0)	--	--	--	1
(2,1)	7	420	17360	624960					

7.3.1 Örnekler

Not 7.9 $\mathbb{Z}_4^n$ 'deki toplamsal mertebesi 4 olan bir vektör **serbest** (*free*), 2 olan bir vektör **serbest olmayan** (*non-free*) vektör olarak adlandırılır.

Örnek 7.10 $n = 3$ olmak üzere, $\mathbb{Z}_4$ üzerinde $(k_1, k_2) = (2, 1)$ tipindeki (ayrık) kodların sayısı 7'dir.

$$N = \frac{(4^3 - 2^3)(4^3 - 2^4)(2^3 - 2^2)}{(4^2 \cdot 2^1 - 2^2 \cdot 2^1)(4^2 \cdot 2^1 - 2^4)(2^2 \cdot 2^1 - 2^2)} = 7$$

ayrık $[3, (2, 1)]$ kod elde edilir. Bu kodlar aşağıda üreteç matrisleri ile verilen kodlardır:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Örnek 7.11 $\mathbb{Z}_8$ üzerinde $n = 2$ uzunluğunda, tipi $(1, 1, 0)$ olan kodların sayısı 3'dür.

Teorem 7.3'den, $\mathbb{Z}_8$ üzerinde bir kod, aşağıda verilen üreteç matrisi ile üretilen bir koda denktir:

$$\begin{bmatrix} I_{k_1} & A & B & D \\ 0 & 2I_{k_2} & 2C & 2E \\ 0 & 0 & 4I_{k_3} & 4F \end{bmatrix} \quad (7.9)$$

(7.9)'da verilen matriste $I_{k_1}, I_{k_2}, I_{k_3}$ matrisleri sırasıyla k_1, k_2, k_3 tipinde birim matrisler; $A, C, F \in \mathbb{Z}_2$; $B, E \in \mathbb{Z}_4$, $D \in \mathbb{Z}_8$ 'dir. $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ halkasının elemanlarından,

1,3,5,7 elemanları birimsel elemanlardır, yani mertebeleri 8'dir. Halkanın sıfır bölenleri ise: 2, 4, 6'dır. 2 ve 6 elemanlarının mertebesi 4'tür ve 4 elemanının mertebesi ise 2'dir.

$$N = \frac{(8^2 - 4^2)(4^2 - 2^2 \cdot 2)}{(8^1 \cdot 4^1 - 4^1 \cdot 4^1)(4^1 \cdot 4^1 - 4^1 \cdot 2)} = 3.$$

Bu kodlar aşağıda üreteç matrisleri ile verilen kodlardır:

$$\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}.$$

Örnek 7.12 $p^m = 2^3$ için $\mathbb{Z}_8$ üzerinde, $n = 2$ uzunluğunda $(k_1, k_2, k_3) = (2, 0, 0)$ tipindeki (ayrık) lineer kodların sayısı 1'dir.

$$N = \frac{(8^2 - 4^2)(8^2 - 4^2 \cdot 2)}{(8^2 - 4^2)(8^2 - 4^2 \cdot 2)} = 1.$$

Bu kod $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ matrisinin ürettiği koddur.

Örnek 7.13 $\mathbb{Z}_8$ üzerinde $n = 3$ uzunluğunda, tipi $(1, 1, 1)$ olan kodların sayısı 42'dir.

Teorem 6.3'den,

$$N = \frac{(8^3 - 2^6)(4^3 - 2^4)(2^3 - 2^2)}{(8^1 \cdot 4^1 \cdot 2^1 - 4^1 \cdot 4^1 \cdot 2^1)(4^1 \cdot 4^1 \cdot 2^1 - 4^1 \cdot 2^1 \cdot 2^1)(2^1 \cdot 2^1 \cdot 2^1 - 2^1 \cdot 2^1)} = 42$$

elde edilir. Burada olduğu gibi kodları açık yazmak her zaman kolay olmayabilir. Bu kodların 37'si aşağıda üreteç matrisleri ile verilen kodlardır:

$$\begin{bmatrix} 1 & x_1 & y_1 \\ 0 & 2 & z_1 \\ 0 & 0 & 4 \end{bmatrix}, \begin{bmatrix} 1 & x_2 & y_2 \\ 0 & 4 & 0 \\ 0 & 0 & 2 \end{bmatrix}, \begin{bmatrix} 4 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 4 & 0 & 0 \\ 0 & 1 & z_4 \\ 0 & 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 0 & y_5 \\ 0 & 1 & z_5 \\ 0 & 0 & 4 \end{bmatrix}, \begin{bmatrix} 2 & x_6 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

$$x_1, y_2, z_4 \in \mathbb{Z}_2, x_2, y_1, z_5 \in \mathbb{Z}_4, x_6, y_5, z_1 \in 2\mathbb{Z}_2$$

x_i, y_j, z_k bileşenlerinin durumuna göre toplam 37 durum elde edilir. Geriye kalan 5 durum da aşağıdaki gibidir:

$$\begin{bmatrix} 2 & 1 & 0 \\ 0 & 0 & 2 \\ 4 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 2 & 1 \\ 2 & 0 & 0 \\ 0 & 4 & 0 \end{bmatrix} \begin{bmatrix} 2 & 0 & 1 \\ 0 & 2 & 0 \\ 4 & 0 & 0 \end{bmatrix} \begin{bmatrix} 2 & 1 & 1 \\ 0 & 0 & 2 \\ 4 & 0 & 0 \end{bmatrix} \begin{bmatrix} 2 & 1 & 1 \\ 0 & 2 & 0 \\ 4 & 0 & 0 \end{bmatrix}.$$

7.4 Sayma Probleminde Literatür ile Tezdeki Yaklaşımın Karşılaştırılması

İlk olarak bazı temel tanım ve teoremler takdim edilmektedir.

7.4.1 Sonlu Zincir Halkaları Üzerinde Lineer Kodlar

Bu kısımdaki tanım ve teoremler çalışmalarından alınmıştır.

Tanım 7.14 [13,14] Tek maksimal ideali olan bir halkaya **yerel (lokal) halka** denir.

Tanım 7.15 [13,14] Her ideali esas ideal olan halkaya **esas ideal halkası** denir.

Tanım 7.16 [13,14] Bir esas ideal halkasının sol (sağ) idealleri bir zincir oluşturuyorsa bu halkaya **sol (sağ) zincir halkası** denir. Bir sol (sağ) zincir halkasına **zincir halkası** denir.

Tanım 7.17 [13,14] Bir A kümesi ve I indeks kümesi verildiğinde $\forall i \in I$ için $\emptyset \neq A_i \subseteq A$ olsun. Eğer aşağıdaki iki özellik sağlanıyorsa $\{A_i\}_{i \in I}$ kümesine, A kümesinin **ayrışım kümesi** denir:

- i. $A = \bigcup_{i \in I} A_i,$
- ii. $A_i \cap A_j = \emptyset, \quad i, j \in I, \quad i \neq j.$

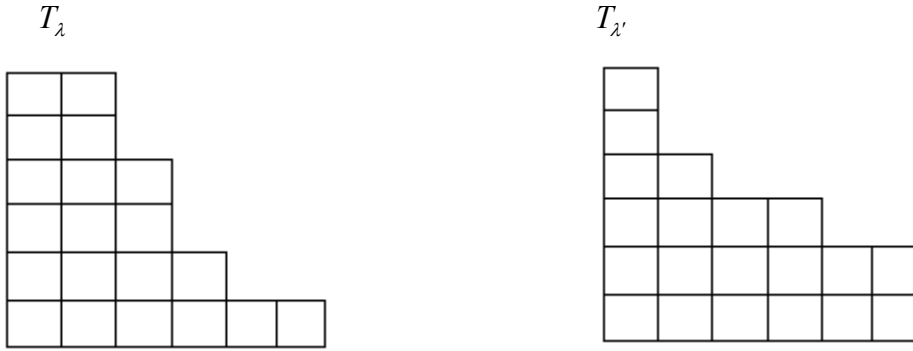
Burada her bir A_i (n elemanlı) kümesine **ayrışımın bloğu** denir.

Bir A kümesinin ayrışımı $A = A_1 \cup A_2 \cup \dots \cup A_n$ olsun. Bu durumda, n_i , A_i kümesinin eleman sayısını göstermek üzere, $n = n_1 + n_2 + \dots + n_k$ ($n_i \neq 0$) denklemi n tamsayısının k parçaya ayrışımını ifade eder.

Tanım 7.18 [13,14] (*Tamsayıların ayrışımı*) Tamsayı ayrışimleri her sayıdaki blokların eleman sayılarını hesaplamak için kullanılır. Bu hesabı kolay bir şekilde yapmak için ‘Genç (Young) Diyagram’ denilen bir gösterim kullanılır. Bu yolla bir ayrışımı başka bir

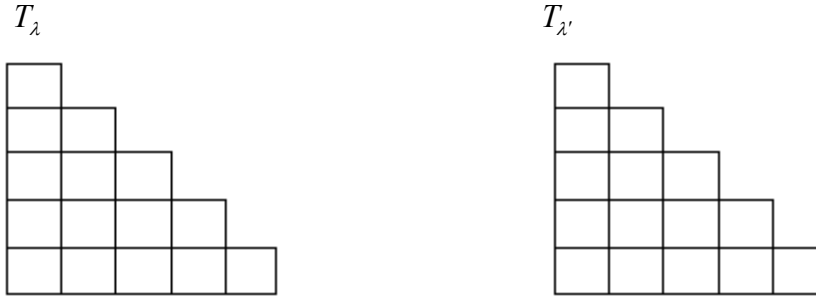
ayrışma dönüştürmek de oldukça kolaydır. Diyagramdaki satır ve sütun yer değiştirdiğinde eşlenik ayrışım elde edilir. $y=x$ alındığında birbirine dönüşen ayrışımara eşlenik ayrışımalar denir. Eğer $y=x$ durumunda diyagramda hiç bir değişiklik olmuyorsa, o ayrışma kendine eştir denir.

Örnek 7.19 [13,14] λ bir ayrışım olmak üzere, $\lambda = (6,6,4,2,1,1)$ ve eşleniği $\lambda' = (6,4,3,3,2,2)$ dir.



Şekil 7. 1 Young Diyagramı I

$\lambda = (5,4,3,2,1)$ ayrışımı kendine eştir. Yani $\lambda = \lambda'$:



Şekil 7. 2 Young Diyagramı II

Özellikler [13,14]

λ bir ayrışım ;

- $|\lambda| = \lambda_1 + \lambda_2 + \dots + \lambda_k$ sayısına λ 'nın ağırlığı denir.
- $|\lambda| = n$ ise, λ 'ya n 'in sıralı olmayan ayrışımı denir
- Her bir $\lambda_i > 0$ sayısına λ 'nın bölümü denir.

- Ayrışımındaki 0 sayıları yazılmaz.
- λ ayrışımını şu şekilde yazabiliriz: $\lambda = 1^{r_1}.2^{r_2}.3^{r_3} \dots$ Buradaki her bir r_i , üssü olduğu tabanın ayrışımında kaç kere tekrarlandığıdır.

Örnek 7.20 [13,14] $\lambda = (3, 3, 3, 2, 1, 1) = 1^2.2^1.3^3$.

- λ' eşlenik ayrışımının bölümleri şu şekilde bulunur: $\lambda'_i = \left| \{j : \lambda_j \geq i\} \right|$.

Örnek 7.21 [13,14] $\lambda = (7, 6, 6, 4, 2, 2, 1, 1, 1) \Rightarrow \lambda = 1^4.2^2.4^1.6^2.7^1 \Rightarrow |\lambda| = 31 \Rightarrow |\lambda'| = 31$.

$$\lambda'_1 = \left| \{j : \lambda_j \geq 1\} \right| = 10, \lambda'_2 = \left| \{j : \lambda_j \geq 2\} \right| = 6, \lambda'_3 = \left| \{j : \lambda_j \geq 3\} \right| = 4,$$

$$\lambda'_4 = 4, \lambda'_5 = 3, \lambda'_6 = 3, \lambda'_7 = 1 \Rightarrow \lambda' = (10, 6, 4, 4, 3, 3, 1) \text{ şeklindedir.}$$

Not 7.22 Eğer sonlu bir Abel p -grubu G , $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_k$ ve λ , n 'in ayrışımı olmak üzere, devirli grupların $\mathbb{Z}_{p^{\lambda_1}} \times \mathbb{Z}_{p^{\lambda_2}} \times \dots \times \mathbb{Z}_{p^{\lambda_k}}$ direkt çarpımına izomorf ise, bu grup $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k)$ tipindedir.

Tanım 7.23 R bir değişmeli halka ve I , R halkasının bir ideali olsun. I idealinin radikali aşağıdaki gibi tanımlanır:

$$\sqrt{I} = \{r \in R : r^n \in I, \exists n \in \mathbb{Z}^+\}.$$

Teorem 7.24 Radikali N olan sonlu bir R halkası için aşağıdakiler denktir:

- R bir sol zincir halkasıdır.
- R halkasının esas sol idealleri bir zincir oluşturur.
- R yerel halkadır ve herhangi $\theta \in N/N^2$ için, $N = R\theta$ esas sol idealdir.
- R bir sol zincir halkasıdır.

Eğer R yukarıdaki durumları sağlıyorsa R 'nin her N ($N \subset R$) ideali, i pozitif tam sayı olmak üzere, $N^i = R\theta^i = \theta^i R$ şeklinde yazılabilir.

Teorem 7.25 [13,14] (*Modül Sınıflandırma Teoremi*) R bir halka, M bir sonlu R -modül ve $|\lambda| = \lambda_1 + \lambda_2 + \dots + \lambda_n = \log_q |M|$ olsun. Herhangi bir sonlu M modülü için,

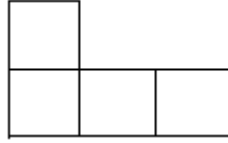
$M \cong R/N^{\lambda_1} \oplus R/N^{\lambda_2} \oplus \dots \oplus R/N^{\lambda_r}$ olacak şekilde tek türlü belirli bir $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_r)$ ayrışımı vardır. Burada, r , λ 'nın bölümlerinin sayısıdır.

Tanım 7.26 [13,14] $M \cong R/N^{\lambda_1} \oplus R/N^{\lambda_2} \oplus \dots \oplus R/N^{\lambda_r}$ olacak şekilde $|\lambda| = \log_q |M|$ ayrışımına M modülünün tipi denir. $\lambda'_i = \text{boy}_{R/N}(\theta^{i-1}M / \theta^i M)$ bölümlerinden oluşan λ' eşlenik ayrışımına da M 'nin eşlenik tipi denir. $r = \lambda'_1$ sayısına M 'nin rankı denir. Burada $\text{boy}_{R/N}(\theta^{i-1}M / \theta^i M)$ ifadesi, $\theta^{i-1}M / \theta^i M$ vektör uzayının R/N üzerindeki boyutunu göstermektedir.

Örnek 7.27 $\mathbb{Z}_4$ üzerinde, üreteç matrisi aşağıda verilen C kodunu düşünelim.

$$G = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 2 & 0 \\ 0 & 2 & 2 \end{bmatrix}.$$

C 'nin modül olarak tipi $\lambda = (2,1,1)$ dir. C 'nin Young diyagramı:



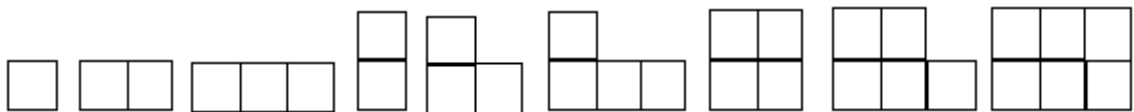
Şekil 7. 3 C kodun Young diyagramı

şeklinde olup, rankı 3'dür ve $|C| = 2^{2+1+1} = 16$ 'dır.

Teorem 7.28 [12,14] M , λ tipinde bir R modül olsun. $\mu \leq \lambda$ eşitsizliğini sağlayan her μ ayrışımı için, M modülünün μ tipinde aşağıdaki kadar alt modülü vardır:

$$\alpha_\lambda(\mu; q) = \prod_{i=1}^m q^{\mu'_{i+1}(\lambda'_i - \mu'_i)} \binom{\lambda'_i - \mu'_{i+1}}{\mu'_i - \mu'_{i+1}}.$$

Örnek 7.29 [13] $\mathbb{Z}_4^n$ modülünde $n=3$ için tüm alt modüllerin *şekil*, *tip* ve *alt grup* sayıları aşağıdaki gibidir:



(1)	(1,1)	(1,1,1)	(2)	(2,1)	(2,1,1)	(2,2)	(2,2,1)	(2,2,2)
7	7	1	28	42	7	28	7	1

7.4.2 Karşılaştırma

Son olarak, elde edilen formül ile Teorem 7.6'da verilen formül bir örnek ile karşılaştırılmaktadır. Alt grubun tipi μ , μ nün eşleniği μ' ve μ'_i ($i \in N$) sayıları da μ' 'nün bölümleri olmak üzere, ($n=6$) için aşağıdaki tablo elde edilir: (Buradaki verilerin hesabı için C++ programı kullanılmıştır.)

Çizelge 7. 3 Teorem 7.28'den ve Teorem 7.6'dan elde edilen sonuçların karşılaştırılması

k_1	k_2	μ	(μ'_1, μ'_2)	Literatür	$N_{k_1, k_2}(n)$
0	6	(111111)	(6,0)	1	1
0	5	(11111)	(5,0)	63	63
0	4	(1111)	(4,0)	651	651
0	3	(111)	(3,0)	1395	1395
0	2	(11)	(2,0)	651	651
0	1	(1)	(1,0)	63	63
0	0	()	(0,0)	1	1
1	5	(211111)	(6,1)	63	63
1	4	(21111)	(5,1)	3906	3906
1	3	(2111)	(4,1)	39060	39060
1	2	(211)	(3,1)	78120	78120
1	1	(21)	(2,1)	31248	31248
1	0	(2)	(1,1)	2016	2016
2	4	(221111)	(6,2)	651	651
2	3	(22111)	(5,2)	39060	39060

Çizelge 7. 4 Teorem 7.28'den ve Teorem 7.6'dan elde edilen sonuçların karşılaştırılması
(devam)

k_1	k_2	μ	(μ'_1, μ'_2)	Literatür	$N_{k_1, k_2}(n)$
2	2	(2211)	(4,2)	364560	364560
2	1	(221)	(3,2)	624960	624960
2	0	(22)	(2,2)	166656	166656
3	3	(222111)	(6,3)	1395	1395
3	2	(22211)	(5,3)	78120	78120
3	1	(2221)	(4,3)	624960	62960
3	0	(222)	(3,3)	714240	714240
4	2	(222211)	(6,4)	651	651
4	1	(22221)	(5,4)	31248	31248
4	0	(2222)	(4,4)	166656	166656
5	1	(222221)	(6,5)	63	63
5	0	(22222)	(5,5)	2016	2016
6	0	(222222)	(6,6)	1	1

7.5 Toplamsal (Additive) Kodlar

Bu kısımda F_4 cismi üzerinde toplamsal kodların tanımı verilmektedir [33].

$f(x) = 1 + x + x^2$ olmak üzere, $F_4 = \mathbb{Z}_2[x] / \langle f(x) \rangle$ bölüm halkası 4 elemanlı bir cisimdir:

$$\begin{aligned}
 F_4 = \mathbb{Z}_2[x] / \langle f(x) \rangle &= \{h(x) + \langle f(x) \rangle : h(x) \in \mathbb{Z}_2[x]\} \\
 &= \{a + bx + \langle f(x) \rangle : a, b \in \mathbb{Z}_2\} \\
 &= \{\langle f(x) \rangle, 1 + \langle f(x) \rangle, x + \langle f(x) \rangle, 1 + x + \langle f(x) \rangle\}.
 \end{aligned}$$

Burada $w = x + \langle f(x) \rangle$ ve $\bar{w} = 1 + w$ olarak alınırsa,

$F_4 = \{0, 1, w, \bar{w}\}$, 4 elemanlı cismi elde edilir.

Tanım 7.30 [34] Vektör toplamı altında kapalı olan, F_4^n 'in n uzunluğunda bir alt kümesine F_4 üzerinde bir **toplamsal kod** denir. Dolayısıyla bir C toplamsal kod, F_4^n 'in toplamsal bir alt grubudur. $c \in C$ için $c + c = 0$ olduğundan, C bir ikili vektör uzayıdır ve $\exists k \in \mathbb{Z}^+$ için 2^k elemanı vardır. n uzunluğunda bir C toplamsal kod bir $(n, 2^k)$ koddur.

F_4 üzerinde bir toplamsal kod ile bir lineer kod farklıdır. Toplamsal kod skaler çarpma (nokta çarpımı) altında kapalı olmayabilir, dolayısıyla F_4 üzerinde lineer olmayabilir. Bir $(n, 2^k)$ toplamsal C kodun k kodsözden oluşan bir bazı vardır. C 'nin üreteç matrisi $k \times n$ tipinde bir matristir.

Örnek 7.31 [34] F_4 üzerinde lineer olan $[6, 3, 4]$ kodun (hexacode) üreteç matrisi aşağıdaki gibidir:

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & w & w \\ 0 & 1 & 0 & w & 1 & w \\ 0 & 0 & 1 & w & w & 1 \end{bmatrix}.$$

Öte yandan, yukarıdaki kod $(6, 2^6, 4)$ toplamsal kod olarak düşünülürse, üreteç matrisi:

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & w & w \\ w & 0 & 0 & w & \bar{w} & w \\ 0 & 1 & 0 & w & 1 & w \\ 0 & w & 0 & \bar{w} & w & \bar{w} \\ 0 & 0 & 1 & w & w & 1 \\ 0 & 0 & w & \bar{w} & \bar{w} & w \end{bmatrix}$$

şeklindedir.

7.6 Galois Halkaları Üzerinde Lineer ve Toplamsal Kodlar

Tanım 7.32 [35] Sıfır bölenleri ile sıfırının birlikte oluşturduğu küme, p bir asal sayı olmak üzere, $\langle p \rangle$ esas idealini veren ve birimi 1 olan sonlu halkaya **Galois halkası** denir.

$$p1 = \underbrace{1+1+\dots+1}_p$$

Örnek 7.33 [35] p bir asal sayı ve k pozitif tam sayı olsun. Bu durumda, $\mathbb{Z}_{p^k}$ halkası birimlidir ve birim elemanı 1'dir. Sıfır bölenlerinin kümesi (0 ile birlikte), $\{0, p, p^2, p^3, \dots, p^{k-1}\} = \langle p \rangle$ idealidir. Dolayısıyla, $\mathbb{Z}_{p^k}$ bir Galois halkasıdır.

Not 7.34 [35] F_p sonlu bir cisim olmak üzere, aşağıdaki dönüşüm bir halka homomorfizmasıdır:

$$\begin{aligned} \tau : \mathbb{Z}_{p^k} &\rightarrow F_p \\ c_0 + c_1p + \dots + c_{k-1}p^{k-1} &\mapsto c_0. \end{aligned}$$

τ dönüşümünü, $\mathbb{Z}_{p^k}[x]$ polinomlar halkasından $F_p[x]$ polinomlar halkasına genişletebiliriz:

$$\begin{aligned} - : \mathbb{Z}_{p^k}[x] &\rightarrow F_p[x] \\ a_0 + a_1x + \dots + a_nx^n &\mapsto \bar{a}_0 + \bar{a}_1x + \dots + \bar{a}_nx^n \end{aligned}$$

Burada, $a_0, a_1, a_2, \dots, a_n \in \mathbb{Z}_{p^k}$ olmak üzere, verilen bir $g(x) \in \mathbb{Z}_{p^k}[x]$ polinomu için, $g(x) \in \mathbb{Z}_{p^k}[x] \Rightarrow \bar{g}(x) \in F_p[x]$ dir.

Tanım 7.35 [35] $f(x)$ polinomu $\mathbb{Z}_{p^k}[x]$ polinomlar halkasında derecesi $m \geq 1$ olan monik bir polinom olsun. Eğer $\bar{f}(x)$ polinomu $F_p[x]$ 'de indirgenemez ise $f(x)$, $\mathbb{Z}_{p^k}[x]$ polinomlar halkasında **monik temel indirgenemez** bir polinomdur.

Örnek 7.36 [35] $h(x)$ polinomu $\mathbb{Z}_{p^k}[x]$ polinomlar halkasında derecesi m olan monik temel indirgenemez bir polinom olsun. Bu durumda, $\langle h(x) \rangle$, $h(x)$ polinomu

tarafından üretilen ideali göstermek üzere, $\mathbb{Z}_{p^k}[x]/\langle h(x) \rangle$ bölüm halkasının yapısı aşağıdaki şekildedir:

$\mathbb{Z}_{p^k}[x]/\langle h(x) \rangle$ halkasının birim elemanı $1 + \langle h(x) \rangle$ 'dir.

$\langle p[1 + \langle h(x) \rangle] \rangle = \langle p + \langle h(x) \rangle \rangle$ esas ideali $\mathbb{Z}_{p^k}[x]/\langle h(x) \rangle$ halkasının, tüm sıfır bölenlerini ve sıfırını ($0 + \langle h(x) \rangle = \langle h(x) \rangle$) içerir. Bunun için, $\langle p + \langle h(x) \rangle \rangle$ ideale ait olmayan bir elemanın halkanın birimsel elemanı olduğunu göstermek yeterlidir.

$a(x) + \langle h(x) \rangle \in \mathbb{Z}_{p^k}[x]/\langle h(x) \rangle$ ve $a(x) + \langle h(x) \rangle \notin \langle p + \langle h(x) \rangle \rangle$ olsun. O halde, $\langle a(x) + \langle h(x) \rangle, p + \langle h(x) \rangle \rangle$ ideali tüm halkayı üretecektir. Yani;

$$1 + \langle h(x) \rangle = [m(x) + \langle h(x) \rangle][a(x) + \langle h(x) \rangle] + [n(x) + \langle h(x) \rangle][p + \langle h(x) \rangle] \quad (7.12)$$

olacak şekilde $m(x) + \langle h(x) \rangle, n(x) + \langle h(x) \rangle \in \mathbb{Z}_{p^k}[x]/\langle h(x) \rangle$ elemanları vardır.

(7.12)'den,

$$1 + \langle h(x) \rangle = m(x)a(x) + pn(x) + \langle h(x) \rangle \quad (7.13)$$

elde edilir.

(7.13)'de eşitliğin her iki tarafının p ninci kuvvetini alalım. $1 + \langle h(x) \rangle \in \mathbb{Z}_{p^k}[x]/\langle h(x) \rangle$ elemanı halkanın birim elemanı olduğundan,

$$\begin{aligned} 1 + \langle h(x) \rangle &= [1 + \langle h(x) \rangle]^p = [m(x)a(x) + pn(x) + \langle h(x) \rangle]^p \\ 1 + \langle h(x) \rangle &= [m(x)a(x)]^p + \binom{p}{1}[m(x)a(x)]^{p-1}pn(x) + \binom{p}{2}[m(x)a(x)]^{p-2}[pn(x)]^2 + \\ &\dots + \binom{p}{p-1}[m(x)a(x)][pn(x)]^{p-1} + [pn(x)]^p + \langle h(x) \rangle. \end{aligned}$$

elde edilir. Yukarıdaki eşitliğin sağ tarafındaki toplamda, $[m(x)a(x)]^p$ ifadesi ile $\langle h(x) \rangle$ arasındaki toplamlar p^2 parantezine alınır, $n_1(x) \in \mathbb{Z}_{p^k}[x]$ olmak üzere,

$$1 + \langle h(x) \rangle = [m(x)a(x)]^p + p^2 n_1(x) + \langle h(x) \rangle$$

elde edilir.

(7.13) eşitliğinin her iki tarafının bu sefer p^2 ninci kuvveti alınırsa aşağıdaki elde edilir:

$$\begin{aligned} 1 + \langle h(x) \rangle &= [1 + \langle h(x) \rangle]^{p^2} = [m(x)a(x) + pn(x) + \langle h(x) \rangle]^{p^2}, \\ 1 + \langle h(x) \rangle &= [m(x)a(x)]^{p^2} + \binom{p^2}{1} [m(x)a(x)]^{p^2-1} pn(x) + \binom{p^2}{2} [m(x)a(x)]^{p^2-2} [pn(x)]^2 + \\ &\cdots + \binom{p^2}{p^2-1} [m(x)a(x)] [pn(x)]^{p^2-1} + [pn(x)]^{p^2} + \langle h(x) \rangle. \end{aligned} \quad (7.14)$$

(7.14) eşitliğinin sağ tarafındaki toplamda, bir önceki aşamadakine benzer şekilde, $[m(x)a(x)]^p$ ifadesi ile $\langle h(x) \rangle$ arasındaki toplamalar p^3 parantezine alınırsa, $n_2(x) \in \mathbb{Z}_{p^k}[x]$ olmak üzere,

$$1 + \langle h(x) \rangle = [m(x)a(x)]^{p^2} + p^3 n_2(x) + \langle h(x) \rangle$$

elde edilir.

Yukarıda yapılanlara benzer şekilde devam edilirse ve son olarak (7.12)'deki eşitliğin her iki tarafının p^{k-1} ninci kuvveti alındığında,

$$1 + \langle h(x) \rangle = [m(x)a(x)]^{p^{k-1}} + p^k n_{k-1}(x) + \langle h(x) \rangle = [m(x)a(x)]^{p^{k-1}} + \langle h(x) \rangle,$$

buradan da,

$$[m(x)a(x)]^{p^{k-1}} + \langle h(x) \rangle = [a(x) + \langle h(x) \rangle] [m(x)^{p^{k-1}} a(x)^{p^{k-1}-1} + \langle h(x) \rangle]$$

elde edilir ki, bu da $a(x) + \langle h(x) \rangle$ elemanının $\mathbb{Z}_{p^k}[x]/\langle h(x) \rangle$ halkasının bir birimsel elemanı olduğunu gösterir. Sonuç olarak, $\langle p + \langle h(x) \rangle \rangle$ esas ideali, $\mathbb{Z}_{p^k}[x]/\langle h(x) \rangle$ halkasının tüm sıfır bölenlerini ve sıfırını kapsar. Dolayısıyla, $\mathbb{Z}_{p^k}[x]/\langle h(x) \rangle$ bir Galois halkasıdır.

Not 7.37 [35] $\mathbb{Z}_{p^k}[x]/\langle h(x) \rangle$ halkasının, $a \in \mathbb{Z}_{p^k}$ olmak üzere, elemanları $a + \langle h(x) \rangle$ şeklinde olan bir R' alt halkası vardır. Ayrıca, $\mathbb{Z}_{p^k} \rightarrow R'$ tasviri, $a \mapsto a + \langle h(x) \rangle$ ile bir halka izomorfizmasıdır. Dolayısıyla, bir $a \in \mathbb{Z}_{p^k}$ elemanı $a + \langle h(x) \rangle \in \mathbb{Z}_{p^k}[x]/\langle h(x) \rangle$ şeklinde gösterilebilir. Kolaylık olması bakımından, $\xi = x + \langle h(x) \rangle$ alınırsa, $h(\xi) = 0$ olur. Bir $a_0 + a_1x + \dots + a_{m-1}x^{m-1} + \langle h(x) \rangle \in \mathbb{Z}_{p^k}[x]/\langle h(x) \rangle$ elemanı için,

$a_0 + a_1x + \dots + a_{m-1}x^{m-1} + \langle h(x) \rangle = a_0 + a_1\xi + \dots + a_{m-1}\xi^{m-1}$ elde edilir. $a_i \in \mathbb{Z}_{p^k}$ ($i = 0, 1, \dots, m-1$) olmak üzere, $\mathbb{Z}_{p^k}[x]/\langle h(x) \rangle$ halkasının tüm elemanları $a_0 + a_1\xi + \dots + a_{m-1}\xi^{m-1}$ şeklinde yazılabilir. Bu yazılım aşağıdaki notasyon ile gösterilir:

$$\mathbb{Z}_{p^k}[\xi] = \{a_0 + a_1\xi + \dots + a_{m-1}\xi^{m-1} : a_i \in \mathbb{Z}_{p^k} (i = 0, 1, \dots, m-1)\}.$$

O halde; $\mathbb{Z}_{p^k}[x]/\langle h(x) \rangle = \mathbb{Z}_{p^k}[\xi]$ 'dir ve $\mathbb{Z}_{p^k}[\xi]$ halkası bir Galois halkasıdır.

7.7 $\mathbb{Z}_{p^m}[\xi]$ Halkası Üzerinde Toplamsal Kodların Sayıları

Bu kısımda, $\mathbb{Z}_{p^m}[\xi]$ halkası üzerinde toplamsal kodlar incelenmektedir. Bunun için kolaylık olması bakımından, ilk olarak $p^m = 4$ olmak üzere $\mathbb{Z}_4[\xi]$ halkasının özellikleri aşağıdaki şekilde verilmektedir:

$h(x) = 1 + x + x^2$ olmak üzere,

$$\begin{aligned} \mathbb{Z}_4[x]/\langle h(x) \rangle &= \{a + bx + \langle h(x) \rangle : a, b \in \mathbb{Z}_4\} \Rightarrow \mathbb{Z}_4[\xi] = \{a + b\xi : a, b \in \mathbb{Z}_4, 1 + \xi + \xi^2 = 0\} \\ &= \{0, 1, 2, 3, \xi, 1 + \xi, 2 + \xi, 3 + \xi, 2\xi, 1 + 2\xi, 2 + 2\xi, 3 + 2\xi, 3\xi, 1 + 3\xi, 2 + 3\xi, 3 + 3\xi\} \end{aligned}$$

$\mathbb{Z}_4[\xi]$ halkasındaki elemanların toplamsal mertebeleri aşağıdaki şekildedir:

$$\begin{aligned}
\langle 1 \rangle &= \langle 3 \rangle = \mathbb{Z}_4, \\
\langle 2 \rangle &= \{0, 2\}, \\
\langle 2\xi \rangle &= \{0, 2\xi\}, \\
\langle 2+2\xi \rangle &= \{0, 2+2\xi\}, \\
\langle \xi \rangle &= \langle 3\xi \rangle = \{0, \xi, 2\xi, 3\xi\}, \\
\langle 1+\xi \rangle &= \langle 3+3\xi \rangle = \{0, 1+\xi, 2+2\xi, 3+3\xi\}, \\
\langle 2+3\xi \rangle &= \langle 2+\xi \rangle = \{0, 2+\xi, 2\xi, 2+3\xi\}, \\
\langle 3+\xi \rangle &= \langle 1+3\xi \rangle = \{0, 3+\xi, 2+2\xi, 1+3\xi\}, \\
\langle 1+2\xi \rangle &= \langle 3+2\xi \rangle = \{0, 1+2\xi, 2, 3+2\xi\}.
\end{aligned}$$

$\mathbb{Z}_4[\xi]$ üzerinde bir toplamsal kodun üreteç matrisi:

$$G = \begin{bmatrix} I_{k_1} & A & B \\ 0 & 2I_{k_2} & 2C \end{bmatrix}$$

şeklinde. Burada, I_{k_1}, I_{k_2} sırasıyla k_1, k_2 tipinde birim matrislerdir. A matrisinin girdileri $\mathbb{Z}_2[\xi] = \{0, 1, \xi, 1+\xi\}$ halkasının elemanlarından; B matrisinin girdileri ise $\mathbb{Z}_4[\xi]$ halkasını elemanlarından oluşmaktadır. G üreteç matrisine sahip bir kodun (k_1, k_2) tipinde olduğu söylenir.

Teorem 7.38 $\mathbb{Z}_{p^m}[\xi]$ üzerinde n uzunluğunda, $(k_1, k_2, \dots, k_m)$ tipinde ayrık (permütasyon denk olan kodlar da dahil) toplamsal kodların sayısı

$$\left[\begin{matrix} n \\ k_1, k_2, \dots, k_m \end{matrix} \right]_{\mathbb{Z}_{p^m}[\xi]}^+ = \frac{N_1}{N_2}$$

sayısıdır. Burada,

$$\begin{aligned}
N_1 &= \prod_{t=1}^m \prod_{i=0}^{k_t-1} \left(\left(p^{m-(t-1)} \right)^{2n} - \left(p^{m-1-(t-1)} \right)^{2n} \cdot p^{\sum_{j=0}^{t-1} k_j} \cdot p^i \right), \\
N_2 &= \prod_{s=1}^m \prod_{r=0}^{k_s-1} \left(\prod_{z=1}^s \left(p^{m-(s-1)} \right)^{k_z} \prod_{j=s+1}^m \left(p^{m-(j-1)} \right)^{k_j} - \left(\prod_{z=1}^s \left(p^{m-s} \right)^{k_z} \right) \left(p^{m-(s+1)} \right)^{k_{s+1}} \cdot \prod_{t=s+2}^m \left(p^{m-(t-1)} \right)^{k_t} \cdot p^r \right)
\end{aligned}$$

şeklinde.

İspat: Teorem 7.6'nın ispatına benzer şekilde yapılır. Burada, $\mathbb{Z}_{p^m}[\xi]$ halkasının elemanlarının mertebelerine dikkat etmek gerekir. $\square$

Sonuç 7.39 $\mathbb{Z}_4[\xi]$ üzerinde n uzunluğunda, (k_1, k_2) tipinde ayırık (permütasyon denk olanlar da dahil) toplamsal kodların sayısı

$$\left[\begin{matrix} n \\ k_1, k_2 \end{matrix} \right]_{\mathbb{Z}_4[\xi]}^+ = \frac{\prod_{i=0}^{k_1-1} (16^n - 4^n \cdot 2^i) \prod_{j=0}^{k_2-1} (4^n - 2^{k_1+j})}{\prod_{i=0}^{k_1-1} (4^{k_1} \cdot 2^{k_2} - 2^{k_1+k_2+i}) \prod_{j=0}^{k_2-1} (2^{k_1+k_2} - 2^{k_1+j})}$$

sayısıdır.

Örnek 7.40 $m=2$ için $\mathbb{Z}_4[\xi]$ üzerinde, $n=3$ uzunluğunda $(k_1, k_2) = (2, 1)$ tipindeki (ayırık) toplamsal kodların sayısı:

$$N = \frac{(16^3 - 4^3)(16^3 - 4^3 \cdot 2)(4^3 - 4)}{(4^2 \cdot 2 - 2^2 \cdot 2)(4^2 \cdot 2 - 2^2 \cdot 2^2)(2^2 \cdot 2 - 2^2)} = 624960$$

sayısıdır.

Örnek 7.41 $m=2$ için $\mathbb{Z}_4[\xi]$ üzerinde, $n=2$ uzunluğunda $(k_1, k_2) = (1, 1)$ tipindeki (ayırık) kodların sayısı:

$$N = \frac{(64^2 - 16^2)(16^2 - 4^2 \cdot 2)}{(8 \cdot 4 - 4 \cdot 4)(4 \cdot 4 - 4 \cdot 2)} = 6720$$

sayısıdır.

7.8 $\mathbb{Z}_{p^m}[\xi]$ Halkası Üzerinde Lineer Kodların Sayıları

Teorem 7.42 $\mathbb{Z}_{p^m}[\xi]$ üzerinde n uzunluğunda, $(k_1, k_2, \dots, k_m)$ tipinde ayırık (permütasyon denk olanlar dahil) lineer kodların sayısı

$$\left[\begin{matrix} n \\ k_1, k_2, \dots, k_m \end{matrix} \right]_{\mathbb{Z}_{p^m}[\xi]} = \frac{N_1}{N_2}$$

sayısıdır. Burada,

$$N_1 = \prod_{t=1}^m \prod_{i=0}^{k_t-1} \left(\left(p^{m-(t-1)} \right)^{2n} - \left(p^{m-1-(t-1)} \right)^{2n} \cdot p^{2 \sum_{j=0}^{t-1} k_j} \cdot p^{2i} \right),$$

$$N_2 = \prod_{s=1}^m \prod_{r=0}^{k_s-1} \left(\prod_{z=1}^s \left(p^{m-(s-1)} \right)^{2k_z} \prod_{j=s+1}^m \left(p^{m-(j-1)} \right)^{2k_j} - \left(\prod_{z=1}^s \left(p^{m-s} \right)^{2k_z} \right) \left(p^{m-(s+1)} \right)^{2k_{s+1}} \cdot \prod_{t=s+2}^m \left(p^{m-(t-1)} \right)^{2k_t} \cdot p^{2r} \right)$$

şeklindedir.

İspat: Teorem 7.6'nın ispatına benzer şekilde yapılır. $\square$

7.5.1 Örnekler

Örnek 7.43 $m=2$ için $\mathbb{Z}_4[\xi]$ üzerinde, $n=2$ uzunluğunda $(k_1, k_2) = (1, 0)$ tipindeki (ayrık) lineer kodların sayısı 20'dir.

$$16^2 - 4^2 = (16 - 4) \cdot N \Rightarrow N = \frac{16^2 - 4^2}{16 - 4} = 20.$$

Gerçekten de, bu kodlar aşağıda verilen üreteç matrisleri ile üretilen kodlardır:

$$[1 \ x], [0 \ 1], [2 \ 1], [2 \ \xi], [2 \ 1+\xi], \ x \in \mathbb{Z}_4[\xi].$$

Örnek 7.44 $m=2$ için $\mathbb{Z}_4[\xi]$ üzerinde, $n=2$ uzunluğunda $(k_1, k_2) = (1, 1)$ tipindeki (ayrık) lineer kodların sayısı:

$$N = \frac{(16^2 - 4^2)(4^2 - 4)}{(16 \cdot 4 - 16)(16 - 4)} = 5$$

sayısıdır. Gerçekten de, bu kodlar aşağıda verilen üreteç matrisleri ile üretilen kodlardır:

$$\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & \xi \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 1+\xi \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}.$$

Örnek 7.45 $m=2$ için $\mathbb{Z}_4[\xi]$ üzerinde, $n=3$ uzunluğunda $(k_1, k_2)=(2,1)$ tipindeki (ayrık) lineer kodların sayısı:

$$N = \frac{(16^3 - 4^3)(16^3 - 4^4)(4^3 - 4^2)}{(16^2 \cdot 4^1 - 4^2 \cdot 4^1)(16^2 \cdot 4^1 - 4^2 \cdot 4^2)(4^2 \cdot 4 - 4^2)} = 21$$

sayısıdır. Bu kodlar aşağıda verilen üreteç matrisleri ile üretilen kodlardır:

$$\begin{bmatrix} 1 & 0 & x_1 \\ 0 & 1 & y_1 \\ 0 & 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & x_2 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

$x_1, x_2, y_1 \in \mathbb{Z}_2[\xi]$ durumları düşünülürse 21 durum elde edilir.

Not 7.46 Örnek 7.45 ile Örnek 7.40 ile karşılaştırıldığında, aynı halka üzerinde aynı parametrelere sahip olan toplamsal kodların sayılarının lineer kodların sayılarından fazla olduğu görülür.

Örnek 7.47 $m=2$ için $\mathbb{Z}_4[\xi]$ üzerinde, $n=3$ uzunluğunda $(k_1, k_2)=(1,2)$ tipindeki (ayrık) lineer kodların sayısı:

$$N = \frac{(16^3 - 4^3)(4^3 - 4)(4^3 - 4^2)}{(16 \cdot 4^2 - 4 \cdot 4^2)(4 \cdot 4^2 - 4)(4 \cdot 4^2 - 4^2)} = 21$$

sayısıdır. Gerçekten de, bu kodlar aşağıda verilen üreteç matrisleri ile üretilen kodlardır:

$$\begin{bmatrix} 1 & x_1 & y_1 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & x_2 \\ 0 & 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

$x_1, x_2, y_1 \in \mathbb{Z}_2[\xi]$ durumları düşünülürse 21 durum elde edilir.

Örnek 7.48 $m=2$ için $\mathbb{Z}_4[\xi]$ üzerinde, $n=3$ uzunluğunda $(k_1, k_2)=(1,1)$ tipindeki (ayrık) lineer kodların sayısı:

$$N = \frac{(16^3 - 4^3)(4^3 - 4)(4^3 - 4^2)}{(16 \cdot 4^2 - 4 \cdot 4^2)(4 \cdot 4^2 - 4)(4 \cdot 4^2 - 4^2)} = 21$$

sayısıdır. Bu kodlar aşağıda verilen üreteç matrisleri ile üretilen kodlardır:

$$\begin{bmatrix} 1 & x_1 & y_1 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & x_2 \\ 0 & 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

$x_1, x_2, y_1 \in \mathbb{Z}_2[\xi]$ durumları düşünülürse 21 durum elde edilir.

Örnek 7.49 $m=3$ için $\mathbb{Z}_8[\xi]$ üzerinde, $n=3$ uzunluğunda $(k_1, k_2, k_3) = (1, 1, 1)$ tipindeki (ayrık) lineer kodların sayısı:

$$N = \frac{(64^3 - 16^3)(16^3 - 4^3 \cdot 4)(4^3 - 4^2)}{(64 \cdot 16 \cdot 4 - 16 \cdot 16 \cdot 4)(16 \cdot 16 \cdot 4 - 16 \cdot 4 \cdot 4)(4 \cdot 4 \cdot 4 - 4 \cdot 4)} = 420$$

sayısıdır. Bu kodları açıkça yazmak diğerleri kadar kolay değildir.

Örnek 7.50 $m=3$ için $\mathbb{Z}_8[\xi]$ üzerinde, $n=3$ uzunluğunda $(k_1, k_2, k_3) = (0, 1, 2)$ tipindeki (ayrık) lineer kodların sayısı:

Formülden,

$$N = \frac{(16^3 - 4^3)(4^3 - 4)(4^3 - 4^2)}{(16 \cdot 4^2 - 4 \cdot 4^2)(4 \cdot 4^2 - 4)(4 \cdot 4^2 - 4^2)} = 21$$

sayısıdır. Bu kodlar aşağıda verilen üreteç matrisleri ile üretilen kodlardır:

$$\begin{bmatrix} 2 & x_1 & y_1 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{bmatrix}, \begin{bmatrix} 4 & 0 & 0 \\ 0 & 2 & x_2 \\ 0 & 0 & 4 \end{bmatrix}, \begin{bmatrix} 4 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}.$$

$x_1, x_2, y_1 \in 2\mathbb{Z}_2[\xi]$ durumları düşünülürse 21 durum elde edilir.

Örnek 7.51 $m=3$ için $\mathbb{Z}_8[\xi]$ üzerinde, $n=4$ uzunluğunda $(k_1, k_2, k_3) = (0, 2, 0)$ tipindeki (ayrık) lineer kodların sayısı:

$$N = \frac{(16^4 - 4^4)(16^4 - 4^4 \cdot 4)}{(16^2 - 4^2)(16^2 - 4^2 \cdot 4)} = 91392$$

sayısıdır.

Örnek 7.52 $m=2$ için $\mathbb{Z}_9[\xi]$ üzerinde, $n=3$ uzunluğunda $(k_1, k_2) = (1, 2)$ tipindeki (ayrık) lineer kodların sayısı:

$$N = \frac{(81^3 - 9^3)(9^3 - 9)(9^3 - 9^2)}{(81 \cdot 9^2 - 9 \cdot 9^2)(9 \cdot 9^2 - 9)(9 \cdot 9^2 - 9^2)} = 91$$

sayısıdır. Bu kodlar aşağıda verilen üreteç matrisleri ile üretilen kodlardır:

$$\begin{bmatrix} 1 & x_1 & y_1 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{bmatrix} \begin{bmatrix} 3 & 0 & 0 \\ 0 & 1 & x_2 \\ 0 & 0 & 3 \end{bmatrix} \begin{bmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

$x_1, x_2, y_1 \in \mathbb{Z}_3[\xi]$ durumları düşünülürse 91 durum elde edilir.

Örnek 7.53 $m=2$ için $\mathbb{Z}_9[\xi]$ üzerinde, $n=3$ uzunluğunda $(k_1, k_2) = (2, 1)$ tipindeki (ayrık) lineer kodların sayısı:

$$N = \frac{(81^3 - 9^3)(81^3 - 9^4)(9^3 - 9^2)}{(81^2 \cdot 9^1 - 9^2 \cdot 9^1)(81^2 \cdot 9^1 - 9^2 \cdot 9^2)(9^2 \cdot 9 - 9^2)} = 91$$

elde edilir. Bu kodlar aşağıda verilen üreteç matrisleri ile üretilen kodlardır:

$$\begin{bmatrix} 1 & 0 & x_1 \\ 0 & 1 & y_1 \\ 0 & 0 & 3 \end{bmatrix} \begin{bmatrix} 1 & x_2 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

$x_1, x_2, y_1 \in \mathbb{Z}_2[\xi]$ durumları düşünülürse 91 durum elde edilir.

7.9 $F_q + uF_q$ Halkası Üzerinde Kodların Sayısı

$q = p^m$ olmak üzere, $R_q = F_q + uF_q$ halkasının eleman sayısı q^2 dir. Ayrıca, $u^2 = 0$ olmak üzere $R_q = F_q[u]/\langle u^2 \rangle$ dir. R_q halkasının elemanlarından u elemanının

toplamsal bir katı olmayanlar birimsel elemanlardır, geriye kalan elemanlar ise birimsel değildir. Bu durumda R_q halkasının $(q-1)q$ adet birimsel elemanı ve $q-1$ adet de birimsel olmayan elemanı vardır. Birimsel elemanların mertebesi q^2 ve sıfır dışındaki elemanlarının mertebesi ise q dur.

Teorem 7.54 [36] R_q üzerinde bir C lineer kod aşağıdaki formda verilen üreteç matrisine sahip koda denktir:

$$G = \begin{bmatrix} I_{k_1} & A_{11} & A_{12} \\ 0 & uI_{k_2} & uA_{22} \end{bmatrix}.$$

A_{ij} matrislerinin girdileri R_q halkasının elemanlarıdır. C kodun eleman sayısı $q^{2k_1+k_2}$ dir. G matrisi ile üretilen kodun tipi (k_1, k_2) dir.

Teorem 7.55 R_q üzerinde n uzunluğunda, tipinde ayırık lineer kodların sayısı

$$N_{k_1, k_2}^{R_q} = \frac{\prod_{t=1}^2 \prod_{i=0}^{k_t-1} \left((q^{3-t})^n - (q^{2-t})^n q^{\sum_{j=0}^{t-1} k_j} q^i \right)}{\prod_{s=1}^2 \prod_{r=0}^{k_s-1} \left(\prod_{p=1}^s (q^{3-s})^{k_p} \prod_{j=s+1}^2 (q^{3-j})^{k_j} - \left(\prod_{p=1}^s (q^{2-s})^{k_p} \right) (q^{1-s})^{k_{s+1}} \prod_{t=s+2}^2 (q^{3-t})^{k_t} q^r \right)}$$

sayısıdır.

İspat Teorem 7.6'nın ispatındaki sayma metodu kullanılarak istenen sonuç elde edilir.

7.10 Sonlu Zincir Halkaları Üzerinde Kodlar

Bu kısımda, herhangi bir sonlu zincir halkası üzerinde kodların sayıları verilmektedir.

Önerme 7.56 [37,38,39,40] Her sonlu değişmeli halka yerel halkaların Çin Kalan çarpımına izomorftur. Her sonlu değişmeli esas ideal halkası sonlu zincir halkalarının Çin Kalan çarpımına izomorftur.

Önerme 7.57 [37,38,39,40] R , maksimal ideali γ olan bir sonlu zincir halkası ve γ da nilpotentlik derecesi e olan bir eleman olsun. R halkası üzerinde bir kodun üreteç matrisi aşağıdaki matrise permütasyon denktir:

$$\begin{bmatrix} I_{k_0} & A_{01} & A_{02} & \cdots & \cdots & A_{0e} \\ 0 & \gamma I_{k_1} & \gamma A_{12} & \cdots & \cdots & \gamma A_{1e} \\ 0 & 0 & \gamma^2 I_{k_2} & \cdots & \cdots & \gamma^2 A_{2e} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & \gamma^{e-1} I_{k_{e-1}} & \gamma^{e-1} A_{e-1,e} \end{bmatrix} \quad (7.15)$$

Burada, A_{ij} matrisinin girdileri R halkasının elemanlarıdır.

Tanım 7.58 [37,38,39,40] (7.15) ile verilen matris ile üretilen bir kod $(k_0, k_1, \dots, k_{e-1})$

tipindedir ve eleman sayısı $|R / \langle \gamma \rangle|^{\sum_{i=0}^{e-1} (e-i)k_i} = q^{\sum_{i=0}^{e-1} (e-i)k_i}$ sayıdır.

Tanım 7.59 [37,38,39,40] R , maksimal ideali m olan bir yerel halka ve $w_1, \dots, w_s$ vektörleri R^n halkasının elemanları olsun. $w_1, \dots, w_s$ vektörlerinin modüler bağımsız olması için gerek ve yeter koşul $\sum \alpha_j w_j = 0$ eşitliğinde her j için $\alpha_j \in m$ olmasıdır.

Tanım 7.60 [37,38,39,40] R sonlu bir halka ve her bir R_i yerel halka olmak üzere, $R = CRT(R_1, R_2, \dots, R_s)$ olsun. Eğer $\Phi_i(v_1), \dots, \Phi_i(v_k)$, bir i için modüler bağımsız ise $v_1, \dots, v_k \in R^n$ vektörleri de modüler bağımsızdır. Burada CRT , Çin Kalan Teoremi'ndeki çarpımı ifade etmektedir.

Tanım 7.61 [37,38,39,40] R bir halka ve $v_1, \dots, v_k \in R^n$ olsun. Eğer $\sum \alpha_j v_j = 0$ eşitliği için $\alpha_j v_j = 0$ sağlanırsa $v_1, \dots, v_k$ vektörleri modüler bağımsızdır.

Tanım 7.62 [37,38,39,40] R bir yerel halka olsun. Eğer $\sum \alpha_i v_i = 0$ eşitliği için $\alpha_i = 0$ sağlanırsa, $v_1, \dots, v_t$ vektörleri lineer bağımsızdır.

Tanım 7.63 Bir R halkası üzerinde bir kod s adet lineer bağımsız vektör ile üretiliyorsa bu koda **serbest (free) kod** denir.

Önerme 7.64 $v_1, \dots, v_t$ vektörleri, bir yerel Frobenius halkası olan R üzerinde n uzunluğunda vektörler olsun. Eğer $v_{t+1} \notin \langle v_1, v_2, \dots, v_t, mR^n \rangle$ ise $v_1, v_2, \dots, v_t, v_{t+1}$ vektörleri lineer bağımsızdır.

İspat: $v_1, v_2, \dots, v_t, v_{t+1}$ vektörleri lineer bağımlı olsun. Bu durumda, en az bir $\alpha_i \neq 0$ için

$\sum_{i=1}^{t+1} \alpha_i v_i = 0$ olur. Eğer $\alpha_{t+1} \notin m$ ise bu durumda, $\sum_{i=1}^t \alpha_i v_i = -\alpha_{t+1} v_{t+1}$ olur. α_{t+1} vektörü

m idealinin elemanı olmadığından, terslenebilir. Bu durumda, $v_{t+1} \in \langle v_1, v_2, \dots, v_t \rangle$ olur ki bu bir çelişkidir. Dolayısıyla, $\alpha_{t+1} \in m$ olmalıdır. m , uzunluğu 1 olan bir kod olduğundan ve halka Frobenius olduğundan, $m^\perp$, uzunluğu 1 olan aşikar olmayan bir koddur. Bu nedenle, $\gamma \neq 0$ olmak üzere, $\gamma \in m^\perp$ 'dir. Bu durumda,

$$\gamma \alpha_1 v_1 + \gamma \alpha_2 v_2 + \dots + \gamma \alpha_t v_t + \gamma \alpha_{t+1} v_{t+1} = 0,$$

$$\gamma \alpha_1 v_1 + \gamma \alpha_2 v_2 + \dots + \gamma \alpha_t v_t = 0$$

eşitlikleri sağlanır. Ayrıca, $v_1, v_2, \dots, v_t$ lineer bağımsız olduğundan, her i için $\gamma \alpha_i = 0$ olur. Buradan da,

$$\gamma (\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_t v_t) = 0,$$

dolayısıyla da $\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_t v_t \in mR^n$ elde edilir ki bu bir çelişkidir. Sonuç olarak, $v_1, v_2, \dots, v_t, v_{t+1}$ vektörleri lineer bağımsızdır.

Önerme 7.65 $v_1, \dots, v_t$ vektörleri, bir yerel Frobenius halkası olan R üzerinde vektörler olsun. Bu durumda $\langle v_1, v_2, \dots, v_t, mR^n \rangle$ kümesinin eleman sayısı $q^t m^n$ sayıdır.

İspat: $w_1, w_2 \in mR^n$ olmak üzere,

$$\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_t v_t + w_1 = \beta_1 v_1 + \beta_2 v_2 + \dots + \beta_t v_t + w_2 \quad (7.16)$$

olduğunu farzedelim. (7.16) ile verilen ifadededen,

$$(\alpha_1 - \beta_1) v_1 + (\alpha_2 - \beta_2) v_2 + \dots + (\alpha_t - \beta_t) v_t = w_2 - w_1 \quad (7.17)$$

elde edilir.

m ideali, $|m| < |R|$ olmak üzere, 1 uzunluğunda bir lineer koddur. Bu nedenle $m^\perp$, R halkasında 1 uzunluğunda aşikar olmayan bir lineer koddur. $\gamma \neq 0$ olmak üzere $\gamma \in m^\perp$ olsun. (7.17) ile verilen ifadenin her iki tarafı γ ile çarpılırsa,

$$\gamma(\alpha_1 - \beta_1)v_1 + \gamma(\alpha_2 - \beta_2)v_2 + \cdots + \gamma(\alpha_t - \beta_t)v_t = 0$$

elde edilir. $v_1, \dots, v_t$ vektörleri lineer bağımsızdır. Bu nedenle her i için $\gamma(\alpha_i - \beta_i) = 0$ olur. $(\alpha_i - \beta_i) \in m$ ifadesinden $\alpha_i \in \beta_i + m$ elde edilir. Buradan q^t eleman elde edilir. Öte yandan, $|mR^n| = m^n$ olduğundan istenen sonuç elde edilir.

Önerme 7.66 R , maksimal ideali m olan bir yerel halka olsun, $|R| = r$ ve $|m| = m$. Bu durumda R^n halkasından seçilebilecek lineer bağımsız vektörlerin sayısı

$$(m^n)^s (q^n - 1)(q^n - q) \dots (q^n - q^{s-1})$$

sayısıdır.

İspat: Bir lineer bağımsız vektör vektör seçmek için $R^n - mR^n$ kümesi göz önüne alınmalıdır. mR^n kümesindeki sıfırdan farklı vektörler modüler bağımsız olmalarına rağmen lineer bağımsız değildirler. Bu nedenle ilk vektör için $r^n - m^n$ farklı şekilde seçim yapılabilir. t adet vektör seçilmiş olsun: $v_1, \dots, v_t$. Önerme 7.65'den, $\langle v_1, v_2, \dots, v_t, mR^n \rangle$ kümesinin eleman sayısının $q^t m^n$ olduğu biliniyor. Dolayısıyla $t+1$ inci vektörün seçimi için yolların sayısı $r^n - q^t m^n$ dir. Buradan, istenen elemanların seçimi için yolların sayısı

$$\begin{aligned} & (r^n - m^n)(r^n - qm^n)(r^n - q^2 m^n) \dots (r^n - q^{s-1} m^n) \\ &= (q^n m^n - m^n)(q^n m^n - qm^n)(q^n m^n - q^2 m^n) \dots (q^n m^n - q^{s-1} m^n) \\ &= (m^n)^s (q^n - 1)(q^n - q) \dots (q^n - q^{s-1}) \end{aligned}$$

sayısıdır.

Önerme 7.67 R , maksimal ideali m olan bir yerel halka olsun, $|R| = r$ ve $|m| = m$. Bu durumda s adet lineer bağımsız vektör ile üretilen bir kodu üreten s vektörü n seçimi için yolların sayısı

$$m^{s^2} (q^s - 1)(q^s - q) \dots (q^s - q^{s-1})$$

sayısıdır.

İspat: Önerme 7.66'nın ispatındaki saymaya benzer şekilde yapılır. Sonuçta,

$$\begin{aligned} & (r^s - m^s)(r^s - qm^s)(r^s - q^2m^s) \dots (r^s - q^{s-1}m^s) \\ &= (q^s m^s - m^s)(q^s m^2 - qm^s) \dots (q^s m^s - q^{s-1}m^s) \\ &= (m^s)^s (q^s - 1)(q^s - q) \dots (q^s - q^{s-1}) \end{aligned}$$

sayısıdır.

Theorem 7.68 R , maksimal ideali m olan bir yerel halka olsun, $|R| = r$ ve $|m| = m$. Bu durumda, R^n kümesinde, s lineer bağımsız vektör ile üretilen ayırık kodların sayısı

$$\frac{(m^n)^s (q^n - 1)(q^n - q) \dots (q^n - q^{s-1})}{(m^s)^s (q^s - 1)(q^s - q) \dots (q^s - q^{s-1})}$$

sayısıdır.

İspat: Önerme 7.66 ve Önerme 7.67'den sonuca ulaşılır.

Maksimal ideali m olan bir yerel R halkası üzerinde serbest kodların sayısı $\left\{ \begin{matrix} n \\ s \end{matrix} \right\}_{q,m}$ ile gösterilecektir.

Theorem 7.69 $v_1, v_2, \dots, v_s$ vektörleri, bir R yerel Frobenius halkası üzerinde lineer bağımsız vektörler olsun. Bu vektörler ile üretilen kod, $(I_s \ A)$ üreteç matrisine sahip olan koda permütasyon denktir.

İspat: v_1 vektörünün en az bir bileşeni birimseldir. Bu vektörün bir bileşeni 1 ve diğer vektörlerin aynı bileşeni 0 olsun. Bu vektörler lineer bağımsız olduğundan, bu vektörlerin lineer kombinasyonları da lineer bağımsız vektörler verir. Satır indirgeme yoluyla istenen sonuca ulaşılır. Bu durum esas ideal halkaları için de böyledir.

Theorem 7.70 C , s lineer bağımsız vektörden oluşan, R^n kümesinde serbest (free) kod olsun. Bu durumda $C^\perp$, $n - s$ lineer bağımsız vektörden oluşan bir serbest koddur.

İspat: Teorem 7.70'den üreteç matrisi $(I_s \ A)$ formuna dönüştürülebilir. $(B \ I_{n-s})$ matrisinin B_{ij} elemanı göz önüne alınsın. Buradan i ninci satır ile v_j vektörü diktir.

$(B \ I_{n-s})$ matrisi, eleman sayısı $|R|^{n-s}$ olan bir kod üretir. Halka Frobenius olduğundan, $|C||C^\perp| = |R|^n$ eşitliği sağlanır ve $(B \ I_{n-s})$ matrisi dik kodu üretir.

Teorem 7.71 $|R| = r$, $|m| = m$ ve $|R/m| = q$ olmak üzere, aşağıdaki eşitlik sağlanır:

$$\left\{ \begin{matrix} n+1 \\ s \end{matrix} \right\}_{q,m} = q^s m^s \left\{ \begin{matrix} n \\ s \end{matrix} \right\}_{q,m} + m^{n-s+1} \left\{ \begin{matrix} n \\ s-1 \end{matrix} \right\}_{q,m}.$$

İspat: Eşitliğin sağ tarafından başlanır:

$$\begin{aligned} & q^s m^s \left\{ \begin{matrix} n \\ s \end{matrix} \right\}_{q,m} + m^{n-s+1} \left\{ \begin{matrix} n \\ s-1 \end{matrix} \right\}_{q,m} \\ &= q^s m^s \frac{(m^{ns-s^2})(q^n-1)(q^n-q)\dots(q^n-q^{s-1})}{(q^s-1)(q^s-q)\dots(q^s-q^{s-1})} + m^{n-s+1} \frac{(m^{n(s-1)-(s-1)^2})(q^n-1)(q^n-q)\dots(q^n-q^{s-2})}{(q^{s-1}-1)(q^{s-1}-q)\dots(q^{s-1}-q^{s-2})} \\ &= m^{(n+1)s-s^2} \frac{(q^n-1)(q^n-q)\dots(q^n-q^{s-2})}{(q^{s-1}-1)(q^{s-1}-q)\dots(q^{s-1}-q^{s-2})} \left[\frac{q^s(q^n-q^{s-1})}{(q^s-1)q^{s-1}} + 1 \right] \\ &= m^{(n+1)s-s^2} \frac{(q^n-1)(q^n-q)\dots(q^n-q^{s-2})}{(q^{s-1}-1)(q^{s-1}-q)\dots(q^{s-1}-q^{s-2})} \left[\frac{q(q^n-q^{s-1})+q^s-1}{(q^s-1)} \right] \\ &= m^{(n+1)s-s^2} \frac{(q^n-1)(q^n-q)\dots(q^n-q^{s-2})}{(q^{s-1}-1)(q^{s-1}-q)\dots(q^{s-1}-q^{s-2})} \left[\frac{q^{n+1}-1}{q^s-1} \right] \\ &= \left\{ \begin{matrix} n+1 \\ s \end{matrix} \right\}_{q,m}. \end{aligned}$$

Teorem 7.72 $|R| = r$, $|m| = m$ ve $|R/m| = q$ olmak üzere, aşağıdaki eşitlik sağlanır:

$$\left\{ \begin{matrix} n+1 \\ s \end{matrix} \right\}_{q,m} = m^s \left\{ \begin{matrix} n \\ s \end{matrix} \right\}_{q,m} + (qm)^{n-s+1} \left\{ \begin{matrix} n \\ s-1 \end{matrix} \right\}_{q,m}.$$

İspat: Eşitliğin sağ tarafından başlanır:

$$\begin{aligned}
& m^s \left\{ \begin{matrix} n \\ s \end{matrix} \right\}_{q,m} + (qm)^{n-s+1} \left\{ \begin{matrix} n \\ s-1 \end{matrix} \right\}_{q,m} \\
&= m^{(n+1)s-s^2} \frac{(q^n-1)(q^n-q)\dots(q^n-q^{s-2})}{(q^{s-1}-1)(q^{s-1}-q)\dots(q^{s-1}-q^{s-2})} \left[\frac{(q^n-q^{s-1})}{q^{s-1}(q^s-1)} + q^{n-s+1} \right] \\
&= m^{(n+1)s-s^2} \frac{(q^n-1)(q^n-q)\dots(q^n-q^{s-2})}{(q^{s-1}-1)(q^{s-1}-q)\dots(q^{s-1}-q^{s-2})} \left[\frac{q^{n-s+1}-1+q^{n-s+1}(q^s-1)}{(q^s-1)} \right] \\
&= m^{(n+1)s-s^2} \frac{(q^n-1)(q^n-q)\dots(q^n-q^{s-2})}{(q^{s-1}-1)(q^{s-1}-q)\dots(q^{s-1}-q^{s-2})} \left[\frac{q^{n+1}-1}{q^s-1} \right] \\
&= \left\{ \begin{matrix} n+1 \\ s \end{matrix} \right\}_{q,m}.
\end{aligned}$$

Önerme 7.73 R , maksimal ideali γ olan bir sonlu zincir halkası ve γ da nilpotentlik derecesi $e+1$ olan bir eleman olsun. Bu durumda, $(k_1, k_2, \dots, k_e)$ tipinde bir kod üretmek için seçilecek vektörlerin sayısı

$$(q)_{\sum_{j=0}^{e-1} nk_j(e-j)} \prod_{a=0}^e \prod_{i=0}^{k_a-1} \left(q^n - q^{\sum_{b=0}^{a-1} k_b} q^j \right)$$

sayısıdır.

İspat: Teorem 7.6, Önerme 7.66 ve Önerme 7.67'nin ispatlarından yararlanılarak istenen elde edilir.

Önerme 7.74 R , maksimal ideali γ olan bir sonlu zincir halkası ve $|R/\langle \gamma \rangle| = q$ olsun. Bu durumda, $(k_1, k_2, \dots, k_e)$ tipinde bir lineer bağımsız kod üretmek için seçilecek vektörlerin sayısı

$$(q)_{\sum_{j=0}^{e-1} (e-j)k_j^2 + \sum_{a=0}^{e-1} \left\{ (e-a)k_{a+1} \sum_{i=0}^a k_i \right\} + \sum_{r=0}^{e-1} \left(\sum_{l=r+1}^e (e-l)k_r k_l \right)} \prod_{a=0}^e (q^{k_i} - 1)(q^{k_i} - q) \dots (q^{k_i} - q^{k_i-1})$$

sayısıdır.

İspat: Teorem 7.6, Önerme 7.67 ve Önerme 7.68'nin ispatlarından yararlanılarak istenen elde edilir.

Teorem 7.75 R , maksimal ideali γ olan bir sonlu zincir halkası ve γ da nilpotentlik derecesi $e+1$ olan bir eleman olsun. Bu durumda, $(k_1, k_2, \dots, k_e)$ tipinde ayrık kodların sayısı

$$\frac{(q)^{\sum_{j=0}^{e-1} nk_j(e-j)} \prod_{a=0}^e \prod_{i=0}^{k_a-1} \left(q^n - q^{\sum_{b=0}^{a-1} k_b} q^j \right)}{(q)^{\sum_{j=0}^{e-1} (e-j)k_j^2 + \sum_{a=0}^{e-1} \left\{ (e-a)k_{a+1} \sum_{i=0}^a k_i \right\} + \sum_{r=0}^{e-1} \left(\sum_{l=r+1}^e (e-l)k_r k_l \right)} \prod_{a=0}^e (q^{k_i} - 1)(q^{k_i} - q) \dots (q^{k_i} - q^{k_i-1})}$$

sayısıdır.

İspat Önerme 7.73 pay kısmını, Önerme 7.74 ise payda kısmını verir.

7.11 Esas İdeal Halkaları Üzerinde Kodlar

Teorem 7.76 $R = CRT(R_1, R_2, \dots, R_h)$ ve her bir R_i , maksimal ideali γ_i (nilpotentlik derecesi e_i) olan halka olmak üzere R bir esas ideal halkası olsun. Bu durumda, R üzerindeki kodların sayısı, her bir $\psi_i(C)$ nin tipi $(k_{i,1}, k_{i,2}, \dots, k_{i,e_i})$ olmak üzere,

$$\prod_{i=1}^h \left[\begin{matrix} n \\ k_{i,1}, k_{i,2}, \dots, k_{i,e_i} \end{matrix} \right]_{q_i, e_{i+1}}$$

sayısıdır.

İspat: Teorem 7.75'deki sayıların çarpımı sonucu verir.

BAZI UYGULAMALAR

8.1 Genelleştirilmiş Gauss (Gaussian) Sayıları

Bu bölümde, Kısım 5.3’de tanım ve özellikleri verilen Gauss binom katsayılarına benzer olarak inşa edilen Genelleştirilmiş Gauss sayıları ve özellikleri verilmektedir.

Tanım 8.1 $R = \mathbb{Z}_{p^m}$ olsun. Teorem 7.6’da, (7.2) ile verilen

$$\left[\begin{matrix} n \\ k_1, k_2, \dots, k_m \end{matrix} \right]_R = N_{k_1, k_2, \dots, k_m}^R(n)$$

sayısına **Genelleştirilmiş Gauss sayısı** denir.

Teorem 8.2 $R = \mathbb{Z}_{p^m}$, $k \leq n$, $k_i \leq n$, $n \in \mathbb{Z}^+$ için Genelleştirilmiş Gauss sayılarının özellikleri aşağıdaki şekilde verilir:

1. $\sum_{i=1}^m k_i = n$ ise, $\left[\begin{matrix} n \\ k_1, k_2, \dots, k_m \end{matrix} \right]_R = \left[\begin{matrix} n \\ k_m, k_{m-1}, \dots, k_1 \end{matrix} \right]_R$,
2. $\left[\begin{matrix} n \\ k_1, k_2, \dots, k_m \end{matrix} \right]_R = \left[\begin{matrix} n \\ n - \sum_{i=1}^m k_i, k_m, k_{m-1}, \dots, k_2 \end{matrix} \right]_R$,
3. $\left[\begin{matrix} n+1 \\ n-(k-1), k, 0, \dots, 0 \end{matrix} \right]_R = \left[\begin{matrix} n \\ n-(k-1), k-1, 0, 0, \dots, 0 \end{matrix} \right]_R + p^k \left[\begin{matrix} n \\ n-k, k, 0, 0, \dots, 0 \end{matrix} \right]_R$,
4. $(p-1) \left[\begin{matrix} n \\ 0, 0, 0, \dots, k, 1 \end{matrix} \right]_R = (p^n - 1) \left[\begin{matrix} n-1 \\ 0, 0, 0, \dots, k, 0 \end{matrix} \right]_R$,

$$5. \quad \begin{bmatrix} n \\ n, 0, 0, \dots, 0 \end{bmatrix}_R = \begin{bmatrix} n \\ 0, n, 0, \dots, 0 \end{bmatrix}_R = \dots = \begin{bmatrix} n \\ 0, 0, 0, \dots, n \end{bmatrix}_R = 1.$$

6. Aşağıdakiler sağlanır:

$$6.1 \quad \begin{bmatrix} n \\ k, 0, 0, \dots, 0 \end{bmatrix}_R = \begin{bmatrix} n \\ n-k, 0, 0, \dots, 0 \end{bmatrix}_R,$$

$$6.2 \quad \begin{bmatrix} n \\ 0, k, 0, \dots, 0 \end{bmatrix}_R = \begin{bmatrix} n \\ 0, n-k, 0, \dots, 0 \end{bmatrix}_R,$$

.....

$$6.m \quad \begin{bmatrix} n \\ 0, 0, 0, \dots, k \end{bmatrix}_R = \begin{bmatrix} n \\ 0, 0, 0, \dots, n-k \end{bmatrix}_R.$$

$$7. \quad m = 2, 3, \dots \text{ için, } \begin{bmatrix} n \\ 0, k_1, k_2, \dots, k_{m-1} \end{bmatrix}_{\mathbb{Z}_{p^m}} = \begin{bmatrix} n \\ k_1, k_2, \dots, k_{m-1} \end{bmatrix}_{\mathbb{Z}_{p^{m-1}}}.$$

$$8. \quad \begin{bmatrix} n \\ k, 0, 0, \dots, 0 \end{bmatrix}_R = (p^k)^{n-k} \begin{bmatrix} n \\ 0, k, 0, \dots, 0 \end{bmatrix}_R = \left((p^k)^{n-k} \right)^2 \begin{bmatrix} n \\ 0, 0, k, \dots, 0 \end{bmatrix}_R = \\ \left((p^k)^{n-k} \right)^3 \begin{bmatrix} n \\ 0, 0, 0, k, 0, \dots, 0 \end{bmatrix}_R = \dots = \left((p^k)^{n-k} \right)^{m-1} \begin{bmatrix} n \\ 0, 0, 0, \dots, 0, k \end{bmatrix}_R.$$

İspat: Tanım 8.1'den, yukarıdaki ifadelerin sağlandığı kolaylıkla görülebilir. $\square$

8.2 Yeni Tanımlanan Diziler

$q = 4$ için $N_{k_1, k_2}^{\mathbb{Z}_q}(n)$ Genelleştirilmiş Gauss sayılarından n, k_1, k_2 sayılarının farklı değerlerine göre, bazıları bilinen bazıları da literatürde mevcut olmayan diziler elde edilir. Bu dizilerden bazılarına burada yer verilmektedir. Elde edilen dizilerin genel terimleri $a_n^{k_1, k_2} = N_{k_1, k_2}^{\mathbb{Z}_4}(n)$ ile gösterilmektedir.

Çizelge 8. 1 $k_1 = 0$ için elde edilen bazı diziler

$n \backslash \text{Tip}$	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(0,6)
n=1	1	--	--	--	--	--
n=2	3	1	--	--	--	--
n=3	7	7	1	--	--	--
n=4	15	35	15	1	--	--
n=5	31	155	155	31	1	--
n=6	63	651	1395	651	63	1
n=7	127	2667	11811	11811	2667	127
n=8	255	10795	97155	200787	97155	10795
n=9	511	43435	788035	3309747	3309747	788035
Dizi	$a_n^{0,1}$	$a_n^{0,2}$	$a_n^{0,3}$	$a_n^{0,4}$	$a_n^{0,5}$	$a_n^{0,6}$

Çizelge 8. 2 Bazı genel k_1, k_2 değerleri için elde edilen diziler

$n \backslash \text{Tip}$	(1,0)	(1,1)	(1,2)	(2,1)	(2,2)
n=1	1	--	--	--	--
n=2	6	1	--	--	--
n=3	28	42	7	7	--
n=4	120	420	210	420	35
n=5	496	3720	4340	17360	4340
n=6	2016	31248	78120	624960	36456
n=7	8128	256032	1322832	21165312	26456640
Dizi	$a_n^{1,0}$	$a_n^{1,1}$	$a_n^{1,2}$	$a_n^{2,1}$	$a_n^{2,2}$

Çizelge 8.1’de, verilen tüm diziler literatürde mevcuttur. Detaylı araştırma için [41] incelenebilir.

Örneğin, Çizelge 8.1’de, ilk sütundaki dizi, $a_n^{0,1}$, Mersenne Asallarını verir: 1,3,7,15,31,63,127,255,...

İkinci sütundaki dizi, $a_n^{0,2} = 1, 7, 35, 155, 651, 2667, 10795, \dots$ dizisidir. Bu dizi, $\begin{bmatrix} n \\ 2 \end{bmatrix}_2$ Gauss

binom katsayıları ile belirlidir. Yani, $\begin{bmatrix} n \\ 0, 2 \end{bmatrix}_4 = \begin{bmatrix} n \\ 2 \end{bmatrix}_2$ dir.

$a_n^{0,3}$ dizisi de benzer şekilde, $\begin{bmatrix} n \\ 3 \end{bmatrix}_2$ Gauss binom katsayıları ile belirlidir: $\begin{bmatrix} n \\ 0, 3 \end{bmatrix}_4 = \begin{bmatrix} n \\ 3 \end{bmatrix}_2$.

Benzer şekilde devam edilirse, $\begin{bmatrix} n \\ 0, k \end{bmatrix}_4 = \begin{bmatrix} n \\ k \end{bmatrix}_2$ olduğu görülür.

Çizelge 8.2’de, (1,0) değeri için elde edilen n değerleri de bilinen bir dizinin terimleridir.

$a_n^{1,0} = 1, 6, 28, 120, 496, 2016, 8128, 32640, \dots$ Bu dizi **A006516** [41] dizisidir ve $2^{n-1}(2^n - 1)$ formülüyle belirlidir.

$a_n^{1,1}$ dizisinin ilk 4 terimi **A160873** [41] ile tanımlıdır. Dizin geri kalan terimleri de Genelleştirilmiş Gauss sayıları ile tanımlanmıştır: 3, 42, 420, 3720, 31248, 256032, ...

Çizelge 8.2’de, $a_n^{1,2}, a_n^{2,1}$ ve $a_n^{2,2}$ dizileri, Genelleştirilmiş Gauss sayıları ile tanımlanan yeni dizilerdir.

Çizelge 8.3’de $n = 2, n = 3$ ve $n = 4$ için $R = \mathbb{Z}_4[\xi]$ üzerinde lineer kodların sayıları verilmektedir. R üzerinde lineer kodlar düşünüldüğünde, değişen n sayıları için ($n = 2, 3, 4, \dots$), $k_1 = 0, k_2 = 1$ alındığında, 5, 21, 85, 341, 1365, ... dizisi elde edilir. Bu dizi, $\frac{4n-1}{3}$ formülü ile belirli olup, **A002450** [41] ile tanımlıdır. Öte yandan, $k_1 = 1, k_2 = 0$ alındığında, **A166984** [41] ile tanımlı olan 20, 336, 5440, ... dizisi elde edilir. Özet olarak;

belirli bir (k_1, k_2) çifti için farklı n sayıları alınarak, bir kısmı literatürde tanımlanmış, bir kısmı ise tanımlanmamış yeni diziler elde edilebilir.

Çizelge 8. 3 $n=2$, $n=3$ ve $n=4$ için $R = \mathbb{Z}_4[\xi]$ üzerinde lineer kod sayıları

n	(k_1, k_2)	Sayı (Kod)	n	(k_1, k_2)	Sayı (Kod)
n=2	(0,1)	5	n=4	(0,1)	85
	(0,2)	1		(0,2)	357
	(1,0)	20		(0,3)	85
	(1,1)	5		(0,4)	31
	(2,0)	1		(1,0)	5440
n=3	(0,1)	21		(1,1)	28560
	(0,2)	21		(1,2)	7140
	(0,3)	1		(1,3)	85
	(1,0)	336		(2,0)	91392
	(1,1)	420		(2,1)	85680
	(1,2)	21		(2,2)	357
	(2,0)	336		(3,0)	5440
	(2,1)	21		(3,1)	85
	(3,0)	1		(4,0)	1

8.3 Dizayn Teori ile İlgili Bazı Kavramlar

8.3.1 t – Dizaynlar

Tanım 8.3 [31] X , v elemanlı bir küme olsun. Bir t -dizayn, X kümesinin herhangi t alt kümesi λ blokta bulunmak üzere, X 'in k 'lı alt kümelerinin bir topluluğudur. Bu yapıya bir $t-(v, k, \lambda)$ **dizayn** denir.

Bu durum daha somut bir şekilde aşağıdaki gibi ifade edilir:

v kişi arasından k 'lı gruplar ele alınsın ve herhangi (en fazla) t kişi λ komitede bulunabilsin. Bu durum, $t-(v, k, \lambda)$ dizayna bir örnektir.

8.4 Tez Çalışması Sırasında Elde Edilen Dizaynlar

Bölüm 5'de, verilen bir Abel grubunun bulanık alt gruplarının sayısı hesaplanırken maksimal zincirlerden faydalanılmaktadır. Bölüm 5'deki maksimal zincirler, sayma kolaylığı bakımından, belli gruplar şeklinde düşünülmektedir. Verilen bir Abel grubunun Hasse şemasının en altındaki alt grupları düşünülecek olursa, bu alt gruplar bir dizayn oluşturur. Burada, Hasse şemasının en altındaki alt gruplar, G_0 grubunun kapsayan en az eleman sayısına sahip (1 boyutlu) alt gruplardır.

8.4.1 p mertebeli (1 boyutlu) alt grupların dizaynı

Teorem 8.4 $\mathbb{Z}_p^r$ (p asal, $r \in \mathbb{Z}^+$) Abel gruplarının maksimal zincirlerinin dizilimi incelendiğinde aşağıdaki dizaynlar elde edilir:

$$2 - \left(\begin{bmatrix} r \\ 1 \end{bmatrix}_p, \begin{bmatrix} 2 \\ 1 \end{bmatrix}_p, 1 \right).$$

İspat: Bölüm 5'den, $\mathbb{Z}_p^r$ grubunun maksimal zincirlerinin dizilimi bilinmektedir. Burada dizaynı oluşturan gruplar 1 boyutlu gruplardır. k boyutlu bir grubun 1 boyutlu alt

grupları $\begin{bmatrix} 2 \\ 1 \end{bmatrix}_p$ adetlik gruplar şeklinde ele alınsın. k boyutlu bir grubun 1 boyutlu alt

gruplarının sayısının $\begin{bmatrix} k \\ 1 \end{bmatrix}_p$ olduğunu, Bölüm 5'de verilen Gauss binom katsayılarından

bilinmektedir. Herhangi birbirinden farklı iki $\begin{bmatrix} 2 \\ 1 \end{bmatrix}_p$ adet alt gruptan (eleman) oluşan

bloğun en fazla bir ortak elemanı olacağını göstermek yeterlidir. (Burada elemanlar, 1 boyutlu alt gruplardır.) Bu iki bloğun iki ortak elemanı olsun. Bu durumda her iki

bloktaki bu ortak iki eleman aynı 2 boyutlu grubu üretir. Yani bu iki bloğun aynı iki blok olduğu anlamına gelir ki bu bir çelişkidir. $\square$

8.4.1.1 Örnekler

$$\diamond \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ grubunun maksimal zincirlerinin alternatif şemadaki dizilimi düşünülürse, bu dizilim bir $2-(7,3,1)$ dizayndır. Bu dizayn şöyle gösterilir:

$$G_1G_2G_3 \quad G_1G_4G_5 \quad G_1G_6G_7 \quad G_2G_5G_6 \quad G_2G_4G_7 \quad G_3G_5G_7 \quad G_3G_4G_6.$$

Grupların yalnızca indisleri göz önüne alınırsa,

$$123 \quad 145 \quad 167 \quad 256 \quad 247 \quad 357 \quad 346$$

diziliminde, toplamda $v=7$ sayı vardır. Önemli olan zincirlerin en altındaki (2 boyutlu alt gruplar) alt grupların sayısının ve her bir alt grubun kaç blokta olduğunun bilinmesidir. Bu sayılar, Gauss binom katsayıları olarak Bölüm 5'den biliniyor. O halde,

$$v \text{ sayısı bu grup için } v = \begin{bmatrix} 3 \\ 1 \end{bmatrix}_2 = 7 \text{ dir.}$$

Bu sayılar $k=3$ 'erli bloklar halinde dizilmişlerdir ve herhangi $t=2$ alt grup en fazla $\lambda=1$ blokta bulunabilir.

$$\diamond \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ grubunun maksimal zincir diziliminde, Hasse şemasının en altında bulunan grupların dizilimi düşünülürse $2-(15,3,1)$ dizayn elde edilir. Dizayn oluşturulacak gruplar aşağıdaki gibi yazılabilir:

$$G_1G_2G_5 \quad G_1G_3G_6 \quad G_1G_4G_7 \quad G_1G_8G_{11} \quad G_1G_9G_{12} \quad G_1G_{10}G_{14} \quad G_1G_{13}G_{15} \quad G_2G_3G_8 \quad G_2G_4G_9 \\ G_2G_6G_{11} \quad G_2G_7G_{12} \quad G_2G_{10}G_{13} \quad G_2G_{14}G_{15} \quad G_4G_5G_{12} \quad G_4G_6G_{12} \quad \dots$$

Devamını yazmaya gerek görülmemiştir. Bu grupların indisleri düşünülmektedir. Bu durumda, dizilimde toplam $v = \begin{bmatrix} 4 \\ 1 \end{bmatrix}_2 = 15$ sayı vardır. Her bir blokta $k = 3$ sayı ve herhangi $t = 2$ alt grup en fazla $\lambda = 1$ blokta bulunabilir.

$$\diamond \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ grubunun maksimal zincir diziliminde en altta bulunan grupların dizilimi düşünülürse $2 - (31, 3, 1) = 2 - \left(\begin{bmatrix} 5 \\ 1 \end{bmatrix}_2, \begin{bmatrix} 2 \\ 1 \end{bmatrix}_2, 1 \right)$ dizayn elde edilir.

$$\diamond \quad \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$$

Benzer şekilde düşünülürse $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ grubunun maksimal zincir diziliminde en altta bulunan grupların diziliminden $2 - (13, 4, 1) = 2 - \left(\begin{bmatrix} 3 \\ 1 \end{bmatrix}_3, \begin{bmatrix} 2 \\ 1 \end{bmatrix}_3, 1 \right)$ dizayn elde edilir. Daha az sayıda grup olduğundan dizilimi yazmak çok zor değildir:

$$\begin{array}{cccccc} G_1 G_2 G_3 G_4 & G_1 G_5 G_6 G_7 & G_1 G_8 G_9 G_{10} & G_1 G_{11} G_{12} G_{13} & G_2 G_5 G_8 G_{12} & G_2 G_6 G_9 G_{13} & G_2 G_7 G_{10} G_{11} \\ G_3 G_5 G_9 G_{11} & G_3 G_7 G_8 G_{13} & G_3 G_6 G_{10} G_{12} & G_4 G_6 G_8 G_{11} & G_4 G_7 G_9 G_{12} & G_4 G_5 G_{10} G_{13} \end{array}$$

Benzer şekilde, bu grupların indisleri düşünülmektedir. Bu durumda, dizilimde toplam $v = \begin{bmatrix} 3 \\ 1 \end{bmatrix}_3 = 13$ sayı vardır. Her bir blokta $k = \begin{bmatrix} 2 \\ 1 \end{bmatrix}_3 = 4$ sayı ve herhangi $t = 2$ alt grup en fazla $\lambda = 1$ blokta bulunabilir.

$$\diamond \quad \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$$

Yukarıdaki diğer gruplara benzer şekilde, $v = \begin{bmatrix} 4 \\ 1 \end{bmatrix}_3 = 40$, $k = \begin{bmatrix} 2 \\ 1 \end{bmatrix}_3 = 4$, $t = 2$ ve $\lambda = 1$ olduğundan, bu dizilim bir $2 - (40, 4, 1)$ dizayndır.

8.4.2 $p^s (s \in \mathbb{Z}^+)$ mertebeli alt grupların dizaynı

$\mathbb{Z}_2^r$ gruplarındaki dizayn incelenirken 2 mertebeli alt grupların dizaynından, $\mathbb{Z}_3^r$ gruplarındaki dizayn incelenirken 3 mertebeli alt grupların dizaynından, yani $\mathbb{Z}_p^r$ gruplarındaki dizayn incelenirken p mertebeli (1 boyutlu) alt grupların dizaynından bahsedildi. Bunların dışında, $\mathbb{Z}_p^r$ gruplarını incelerken $p^2, p^3, \dots$, mertebeli alt gruplar da bir dizayn oluşturur. Bunları aşağıdaki kısımda incelenmektedir:

Teorem 8.5 $\mathbb{Z}_p^r$ gruplarının $p^s (s \in \mathbb{Z}^+)$ mertebeli alt grupların dizilimi bir

$$2 - \left(\begin{bmatrix} r \\ s \end{bmatrix}, \begin{bmatrix} s+1 \\ s \end{bmatrix}, 1 \right) \text{ dizayndır.}$$

İspat: Teorem 8.4'ün ispatına benzer şekilde yapılır.

8.4.2.1 Sonuçlar

❖ p^2 mertebeli alt grupların dizaynı

Bölüm 4'de $\mathbb{Z}_p^r$ gruplarının her mertebeden alt gruplarının sayısının Gaus Sayıları ile hesaplanabileceğini görmüştük. Örneğin, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 = \mathbb{Z}_2^4$ grubunun 2^2

mertebeli alt gruplarının sayısı $\begin{bmatrix} 4 \\ 2 \end{bmatrix}_2 = 35$ dir. O halde $v=35$ dir. Alt grup şeması

(alternatif Hasse şeması) düşünülürse, 35 alt grup, $k=7 = \begin{bmatrix} 3 \\ 2 \end{bmatrix}_2$ şerli bloklar halinde

düşünülürse (bulanık alt grupların sayısı, bu dizayn ile hesaplanmıştı), herhangi $t=2$ alt grup (birlikte) en fazla $\lambda=1$ blokta bulunabilir. O halde, $\mathbb{Z}_p^r$ grubunun alternatif Hasse şeması incelendiğinde 2^2 mertebeli alt grupların dizilimi $2-(35,7,1)$ dizayn oluşturur.

$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 = \mathbb{Z}_3^4$ grubunun 3^2 mertebeli alt gruplarının dizilimi bir $2-(130,13,1)$ dizayndır.

Genelleştirilirse, $\mathbb{Z}_p^r$ gruplarının p^2 mertebeli alt gruplarının dizilimi bir

$$2 - \left(\begin{bmatrix} r \\ 2 \end{bmatrix}_p, \begin{bmatrix} 3 \\ 2 \end{bmatrix}_p, 1 \right) \text{ dizayndır.}$$

❖ p^3 mertebeli alt grupların dizaynı

Diğer durumlara benzer şekilde düşünülürse, $\mathbb{Z}_p^r$ grubunun p^3 mertebeli alt

gruplarının oluşturduğu dizilim bir $2 - \left(\begin{bmatrix} r \\ 3 \end{bmatrix}_p, \begin{bmatrix} 4 \\ 3 \end{bmatrix}_p, 1 \right)$ dizayndır. Örneğin; $\mathbb{Z}_2^5$ grubunun

2^3 mertebeli alt gruplarının sayısının $\begin{bmatrix} 5 \\ 3 \end{bmatrix}_2 = 155$ olduğunu Bölüm 2 den biliyoruz.

Bölüm 4 den, 155 grup $\begin{bmatrix} 4 \\ 3 \end{bmatrix}_2 = 15$ li bloklar halinde dizilirler (bu sayı 4 boyutlu alt

grubun 3 boyutlu alt gruplarının sayısıdır). O halde, $v=155, k=15$ dir. Öte yandan her bir $k=15$ li blokta $t=2$ alt grup (birlikte) en fazla $\lambda=1$ blokta bulunabilir. O halde bu dizilim bir $2 - (155, 15, 1)$ dizayndır.

Sonuç 8.6 $\mathbb{Z}_p^3$ grubunun p mertebeli alt gruplarının dizaynı, p mertebeli projektif düzlem teşkil eder.

SONUÇ VE ÖNERİLER

Bu tezde, ilk olarak, bazı grupların bulanık alt grupları incelenmiş ve sayıları direkt bir formül yardımıyla hesaplanmıştır. Daha sonra, bazı halkalar üzerinde lineer ve toplamsal kodların sayısı hesaplanmış ve bunlarla ilgili bazı uygulamalara yer verilmiştir.

KAYNAKLAR

- [1] Rosenfeld, A., (1971), Fuzzy Groups, J. Math. Anal. and Appl., 35: 512-517.
- [2] Das, P.S., (1981), Fuzzy groups and level subgroups, J. Math. Anal. Appl. 84: 264-269.
- [3] Murali, V. ve Makamba, B., (2001), "On an Equivalence of Fuzzy Subgroups I", Fuzzy Sets and Systems, 123: 259-264.
- [4] Murali, V. ve Makamba, B., (2003), "On an Equivalence of Fuzzy Subgroups II", Fuzzy Sets And Systems, 136: 93-104.
- [5] Murali, V. ve Makamba, B., (2004), "Counting the Number of Fuzzy Subgroups of an Abelian Group of Order $p^n q^m$ ", Fuzzy Sets And Systems, 144: 459-470.
- [6] Tarnauceanu, M. ve Bentea, L., (2008), "On the number of fuzzy subgroups of finite abelian groups", Fuzzy Sets and Systems, 159: 1084–1096.
- [7] Shannon, C.E., (1948), "A Mathematical Theory of Communication" Bell System Technical Journal, 27: 379-423.
- [8] Hammons A.R, Kumar P. V., Calderbank A.R., Sloane N.J. ve Sole P., (1994), "The Z4-Linearity of Kerdock, Preparata Goethals and Related Codes", IEEE Trans. Inform. Theory, 40: 301-319.
- [9] Delsarte, S., (1948), "Fonctions de Möbius Sur les Groups Abeliens Finis", Annals of Math. 49, No. 3: 600-609.
- [10] Djubjuk, P.E., (1948), "On the number of subgroups of a finite abelian group", Izv. Akad. Nauk SSSR Ser. Mat. 12: 351-378.
- [11] Yeh, Y. (1948), "On Prime Power Abelian Groups". Bull. AMS, 54: 323-327.
- [12] Calugareanu, G., (2004), "The Total Number of Subgroups of a Finite Abelian Group", Scientiae Mathematicae Japonicae, 1(60): 157-167.
- [13] T. Honold and Landjev I., (2000), "Linear codes over finite chain rings", The Electronic Journal of Combinatorics 7, R11.
- [14] Honold T. ve Landjev I., (2009), "Linear Codes over Finite Chain Rings and Projective Hjelmslev Geometries", Codes Over Rings, Proceedings of the Cimpa Summer Shool, 18-29 August 2008, Ankara, Turkey.
- [15] Hungerford T. W., (1974), Algebra, University of Washington, Addison-Wesley

Publishing Company.

- [16] Spindler K., (1994), Abstract Algebra with Applications (Volume II), Marcel Dekker, Inc.
- [17] Fuchs, L., (1967), Abelian Groups, Addison-Wesley Publishing Company.
- [18] Hall, P., (1933), "A Contribution to the Theory of Groups of Prime Power Order", Proc., London Math. Soc. 2(36): 29-95.
- [19] Zadeh, L. A., (1965), "Fuzzy Sets", Information and Control, 8: 338-353.
- [20] Şekercioğlu A., (1994), "Bulanık Kümeler", 3: 14-17.
- [21] Serhatlıoğlu S. ve Hardalaç F., (2009), "Yapay Zeka Teknikleri ve Radyolojiye Uygulanması", Fırat Tıp Dergisi, 1(14): 1-6.
- [22] Zadeh, L. A., (1969), "Biological Application of the Theory of Fuzzy Sets and Systems on Biocybernetics of the Central Nervous System", Proc. Int. Sym., 199-212.
- [23] Kalmanson D. ve Stegall H.F., (1975), "Cardiovascular Investigations and Fuzzy Set Theory", American Journal of Cardiology, 35: 80-84.
- [24] Guo Z., Durand L.G., Allard L., Cloutier G., Lee H.C., ve Langlois Y.E. (1993), "Cardiac Doppler Blood Flow Signal Analysis", Part II: The Time Frequency Distribution by Using Autoregressive Modeling. Med Biol Eng Comput, 31: 242-248.
- [25] Nauck D. ve Kruse R. (1999), "Obtaining Interpretable Fuzzy Classification Rules from Medical Data", Artificial Intelligence in Medicine, 16: 149-169.
- [26] Takagi T. ve Sugeno M., (1985), "Fuzzy Identification of Systems and Its Applications to Modeling and Control," IEEE Trans. Sys., Man., Cybern., vol. smc-15, 1: 116-132.
- [27] Malik, D. S. ve J. N. Mordeson, (1998), "Fuzzy Commutative Algebra", World Scientific Publishing, Co. Pte. Ltd.
- [28] Ngcibi S. Leonard, (2005), Studies of Equivalent Fuzzy Subgroups of Finite Abelian Groups of Rank Two and Their Subgroup Lattices, Doktora tezi, Institute of Sciences, Rhodes University.
- [29] Fraleigh, J. B., (1982), A First Course in Abstract Algebra, Addison-Wesley, London.
- [30] Gallian, J. A., (1994), Contemporary Abstract Algebra 3rd ed., Heath and Company, Lexington.
- [31] MacWilliams, F.J. ve Sloane, N.J.A., (1977), The Theory of Error-Correcting Codes, North-Holland Pub. Co.
- [32] Ling, S. ve Xing, C., (2004), Coding Theory: A First Course, Cambridge University press.
- [33] Huffman, W.C., (1998), "Decompositions and extremal Type II Codes over $\mathbb{Z}_4$ ", IEEE Trans. Inform. Theory, 44: 800-809.

- [34] Huffman, W.C. ve Pless V., (2003), Fundamentals of Error-Correcting Codes, Cambridge University Press.
- [35] Wan Z.X., (1997), Quaternary Codes, Series on Applied Math., Vol. 8, World Scientific pub., Singapore.
- [36] Özen M., Şiap İ., (2006), "Linear Codes Over $F_q[u]/\langle u^s \rangle$ With Respect to the Rosenbloom-Tsfasman Metric", Designs, Codes and Cryptography., 38: 17-29.
- [37] Dougherty, S.T., Han, S., (2010), "Higher weights and generalized MDS codes", J. Korean Math. Soc., 6(47): 1167-1182.
- [38] Dougherty, S.T., Han, S., Liu H., (2011), "Higher weights for codes over rings", Appl. Algebra Engrg. Comm. Comput., 2(22): 113-135.
- [39] Dougherty, S.T., Kim, J. L., Kulosman, H., (2008), "MDS codes over finite principal ideal rings", Designs, Codes, Cryptogr., vol. 50, no. 1, pp. 77-92.
- [40] Dougherty, S.T., Liu, H., (2009), "Independence of vectors in codes over rings", Designs, Codes, Cryptogr., vol. 51, no. 1, pp. 55-68.
- [41] Sloane N.J.A., (2013), On-Line Encyclopaedia of Integer Sequences, Published electronically at <https://oeis.org/>.
- [42] Bhowmik, G., (1996), "Evaluation of the divisor function of matrices", Acta Arithmetica 74: 155-159.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : Esengül SALTÜRK
Doğum Tarihi ve Yeri : 11.10.1983- Bursa
Yabancı Dili : İngilizce
E-posta : esalturk@yildiz.edu.tr

ÖĞRENİM DURUMU

Derece	Alan	Okul/Üniversite	Mezuniyet Yılı
Y. Lisans	Matematik	Yıldız Teknik Üniversitesi	2007
Lisans	Matematik	Yıldız Teknik Üniversitesi	2006
Lise	Yab. Dil A. L.	Nuri Erbak Lisesi	2001

İŞ TECRÜBESİ

Yıl	Firma/Kurum	Görevi
2006-	Yıldız Teknik Üniversitesi	Araştırma Görevlisi

YAYINLARI

Makale

1. Saltürk E., Şiap İ., (2012). "Generalized Gaussian Numbers Related to Linear Codes over Galois Rings", *European Journal of Pure and Applied Mathematics*, 2(5): 250-259.
2. Saltürk E., Şiap İ., (2012). "On Generalized Gaussian Numbers", *Albanian J. Math.*, 2(6): 87-102.
3. Çelik S., Saltürk E., (2008). "A Differential Calculus on $\hbar$ -Superspace", *Noncommutative Structures in Mathematics and Physics, Proceedings*, 1: 63-70.

Bildiri

1. Saltürk E., Şiap İ., (February 4-8, 2013). "On Designs of Subgroups of Finite Abelian p-Groups", "2nd Biennial International Group Theory Conference", Doğuş University, İstanbul.
2. Saltürk E., Şiap İ., (September 20-23, 2012). "Generalized Gaussian Numbers and Some New Sequences", "9th Conference of the Society of Physicists of Macedonia", Makedonya, Ohrid.
3. Saltürk E., Şiap İ., (April 14, 2012). "The Number of codes over $F_q + uF_q$ and some new sequences", "10th UAE MathDay Conference", American University of Sharjah, Dubai.
4. Saltürk E., Şiap İ., (October 26-29, 2011). "Generalised Gaussian Numbers", "Integers Conference 2011", University of West Georgia in Carrollton, Georgia, USA.
5. Saltürk E., Şiap İ., (June 27-July 01, 2011). "The Total Number of Fuzzy Subgroups Of $\mathbb{Z}_p^n$ ", International conference "2nd Istanbul Design Theory, Graph Theory and Combinatorics Conference", Koc University, İstanbul.
6. Saltürk E., Şiap İ., (June 29-30-July 1-2, 2011). "On The Number of Codes over $\mathbb{Z}_{p^m}$ ", International conference on Applied Analysis and Algebra", Yıldız Technical University, İstanbul.
7. Saltürk E., Şiap İ., (May 31-June 11, 2010). "The Number of Quaternary Fuzzy Codes", "NATO Advanced Study Institute on Information Security and Related Combinatorics", Opatija, Croatia.
8. Çelik S., Saltürk E., (July 22-26, 2008). "A Differential Calculus on $\hbar$ -Superspace", "Noncommutative Structures in Mathematics and Pyhsics", Vrije University of Brussels.

Proje

1. YTÜ DOP projesi Yönetici: Prof. Dr. İrfan ŞİAP, (2011-2012). “Bulanık Alt Grupların ve Kodların Sayısı ile Bazı Uygulamalar”, Proje No: 2011-DOP-01-03.