T.C.

TRAKYA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

$\mathbb{Z}_4 + u\mathbb{Z}_4$ HALKASI ÜZERİNDE TANIMLI LİNEER KODLAR HAKKINDA

BUSE YAVUZ

YÜKSEK LİSANS TEZİ

MATEMATİK ANABİLİM DALI

TEZ DANIŞMANI: PROF. DR. YASEMİN ÇENGELLENMİŞ

EDİRNE-2020

Buse YAVUZ 'un hazırladığı "$\mathbb{Z}_4 + u\mathbb{Z}_4$ **Halkası Üzerinde Tanımlı Lineer Kodlar Hakkında**'' başlıklı bu tez, tarafımızca okunmuş, kapsam ve niteliği açısından **Matematik** Anabilim Dalında bir **Yüksek Lisans Tezi** olarak kabul edilmiştir.

Jüri Üyeleri (Ünvan, Ad, Soyad):	İmza
Prof. Dr. Yasemin ÇENGELLENMİŞ	……
Prof. Dr. Figen ÖKE	……
Dr. Öğr. Üyesi Abdullah DERTLİ	……

Tez Savunma Tarihi: 11 / 09 / 2020

Bu tezin Yüksek Lisans Tezi olarak gerekli şartları sağladığını onaylarım.

İmza

Prof. Dr. Yasemin ÇENGELLENMİŞ

Tez Danışmanı ……

Trakya Üniversitesi Fen Bilimleri Enstitüsü onayı

……

Prof. Dr. Murat YURTCAN

Fen Bilimleri Enstitüsü Müdürü

T.Ü. FEN BİLİMLERİ ENSTİTÜSÜ

MATEMATİK YÜKSEK LİSANS PROGRAMI

DOĞRULUK BEYANI

Trakya Üniversitesi Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında, tüm verilerin bilimsel ve akademik kurallar çerçevesinde elde edildiğini, kullanılan verilerde tahrifat yapılmadığını, tezin akademik ve etik kurallara uygun olarak yazıldığını, kullanılan tüm literatür bilgilerinin bilimsel normlara uygun bir şekilde kaynak gösterilerek ilgili tezde yer aldığını ve bu tezin tamamı ya da herhangi bir bölümünün daha önceden Trakya Üniversitesi ya da farklı bir üniversitede tez çalışması olarak sunulmadığını beyan ederim.

11 / 09 / 2020

Buse YAVUZ

İmza

Yüksek Lisans Tezi

$\mathbb{Z}_4 + u\mathbb{Z}_4$ HALKASI ÜZERİNDE TANIMLI LİNEER KODLAR HAKKINDA

T.Ü. Fen Bilimleri Enstitüsü

Matematik Anabilim Dalı

ÖZET

Bu tez çalışmasında, öncelikle tez organizasyonu ile birlikte cebir ve kodlama ile ilgili gerekli temel kavramlara yer verilmiştir. Ardından tezin 3. bölümünde $r = a + ub \in \mathbb{Z}_4 + u\mathbb{Z}_4$ olmak üzere $\mathbb{Z}_4[u]/\langle u^2 - r\rangle \cong R_r = \mathbb{Z}_4 + u\mathbb{Z}_4, u^2 = r$ tipindeki 16 halkanın cebirsel özellikleri araştırılmıştır. Bu halkaların birimselleri bulunmuş, idealleri ve özellikleri belirlenmiştir. Ayrıca bu halkaların birbirleri ile olan izomorfluk durumları incelenmiştir.

Tezin 4. bölümünde, R_u sonlu halkası üzerinde tanımlı lineer kodların özellikleri incelenmiştir. Ayrıca yine aynı halka üzerinde tanımlı uzunluğu tek olan $(1 + 2u)$-sabit devirli kodlar ile devirli kodlar arasındaki ilişki ifade edilerek, bunların Gray görüntüleri verilmiştir. Buna ek olarak, R_0, R_1 ve R_3 halkaları üzerinde $(1 + 2u)$ birimseli seçilerek elde edilmiş benzer sonuçlar verilmiştir. Bu bölümde farklı halkalar üzerinde tanımlı bazı özel kodlar yardımıyla sonlu cisimler üzerinde tanımlı iyi kodlar edilmenin sağlandığı makaleler incelenmiştir.

Tezin 5. bölümünde, R_1 ve R_u halkaları üzerinde tanımlı devirli kodların DNA özelliklerine sahip olması için gerekli ve yeterli koşulların verildiği makaleler incelenmiştir.

6. bölümde, R_1 halkası üzerinde yeni bir Gray dönüşümü tanımlanarak ve u birimseli seçilerek u-sabit devirli kodlar ve devirli kodların Gray görüntüleri elde edilmiştir.

Son bölümde, sonuç ve tartışmalara yer verilmiştir.

Yıl : 2020

Sayfa Sayısı : 139

Anahtar Kelimeler : Lineer Kodlar, Devirli Kodlar, Sabit Devirli Kodlar, Gray Dönüşüm, Devirli DNA kodlar ve DNA Dönüşüm

Master of Science Thesis

ON THE LINEAR CODES OVER RING $\mathbb{Z}_4 + u\mathbb{Z}_4$

Trakya University Institute of Natural Sciences

Department of Mathematics

ABSTRACT

In this thesis, firstly, the thesis organization is given, later basic concepts related to algebra and coding are given. In that 3th section of the thesis, algebraic properties of 16 rings in type $\mathbb{Z}_4[u]/\langle u^2 - r\rangle \cong R_r = \mathbb{Z}_4 + u\mathbb{Z}_4$, where $u^2 = r, r = a + ub \in \mathbb{Z}_4 + u\mathbb{Z}_4$ are investigated. The units and ideals of the rings are found the structures of the ideals are determined. In addition, these rings are examined into isomorphic states with each other.

In the 4th section of the thesis, the properties of the linear codes defined on the finite ring R_u are examined. In addition, the relationship between $(1 + 2u)$-constacyclic codes and cyclic codes over the ring R_u is expressed and their Gray images are given. In addition, similar results are given by selecting $(1 + 2u)$-units on the rings R_0, R_1 and R_3. The articles that are obtained optimal codes over the ring $\mathbb{Z}_4$ are examined.

In the 5th section of the thesis, necessary and sufficient conditions are given for the cyclic codes defined on the R_1 and R_u rings to have DNA properties.

In the 6th section, by defining a new Gray map on the ring R_1 and selecting the unit u, the Gray images of u-constacyclic codes and cyclic codes are obtained.

In the last section, results and discussions are given.

Year : 2020

Number of Pages : 139

Keywords : Linear Codes, Cyclic Codes, Constacyclic Codes, Gray map, Cyclic DNA Codes and DNA Map

ÖNSÖZ

Yüksek Lisans Tez danışmanlığımı üstlenerek akademik hayata adım atmamı sağlayan, öğrencisi olmakla kendimi şanslı hissettiğim danışmanım, aynı zamanda çok sevgili hocam Prof. Dr. Yasemin ÇENGELLENMİŞ'e üzerimdeki tüm emekleri için çok teşekkür ederim.

Dolaylı olarak başarımda katkısı olan beni yetiştiren Trakya Üniversitesi Matematik Bölümü programı hocalarına çok teşekkür ederim.

Eğitim hayatım boyunca maddi ve manevi desteğini esirgemeden yanımda olan annem Sümran YAVUZ, babam Emir YAVUZ ve ablam Damla YAVUZ'a sonsuz teşekkür ederim.

Çalışmamın sonunda tezimi tekrar tekrar okuyarak eleştirileriyle yol gösteren Dr. Abdullah DERTLİ'ye teşekkür ederim.

Ayrıca, tez çalışmam boyunca beni motive etmiş ve manevi olarak destek sağlamış olan Abdullah GERBAĞA'ya çok teşekkür ederim.

Bu çalışma, çok sevdiğim aileme ithaf olunur…

Buse YAVUZ

İÇİNDEKİLER

ÖZET ……... iv

ABSTRACT…… v

ÖNSÖZ…… vi

İÇİNDEKİLER…… vii

SEMBOLLER ve KISALTMALAR DİZİNİ ……. xi

ŞEKİLLER DİZİNİ……xiii

ÇİZELGELER DİZİNİ……..xv

BÖLÜM 1 GİRİŞ…… 1

1.1. Tez Organizasyonu…… 3

BÖLÜM 2 TEMEL KAVRAMLAR…… 4

2.1. Cebir ile İlgili Temel Kavramlar……... 4

2.2. Kodlama ile İlgili Temel Kavramlar……. 15

BÖLÜM 3 $\mathbb{Z}_4[u]/\langle u^2 - r\rangle \cong R_r = \mathbb{Z}_4 + u\mathbb{Z}_4, u^2 = r$ HALKALARININ ÖZELLİKLERİ VE SINIFLANDIRILMASI ..…….. 24

3.1. $\mathbb{Z}_4[u]/\langle u^2\rangle$ Halkası……24

3.2. $\mathbb{Z}_4[u]/\langle u^2 - 1\rangle$ Halkası……30

3.3. $\mathbb{Z}_4[u]/\langle u^2 - 2\rangle$ Halkası……31

3.4. $\mathbb{Z}_4[u]/\langle u^2 - 3\rangle$ Halkası……32

3.5. $\mathbb{Z}_4[u]/\langle u^2-u\rangle$ Halkası…… 34

3.6. $\mathbb{Z}_4[u]/\langle u^2-2u\rangle$ Halkası…….. 36

3.7. $\mathbb{Z}_4[u]/\langle u^2-3u\rangle$ Halkası…….. 37

3.8. $\mathbb{Z}_4[u]/\langle u^2-u-1\rangle$ Halkası…….. 39

3.9. $\mathbb{Z}_4[u]/\langle u^2-u-2\rangle$ Halkası…….. 40

3.10. $\mathbb{Z}_4[u]/\langle u^2-u-3\rangle$ Halkası…….. 41

3.11. $\mathbb{Z}_4[u]/\langle u^2-2u-1\rangle$ Halkası……... 43

3.12. $\mathbb{Z}_4[u]/\langle u^2-2u-2\rangle$ Halkası……... 44

3.13. $\mathbb{Z}_4[u]/\langle u^2-2u-3\rangle$ Halkası……... 45

3.14. $\mathbb{Z}_4[u]/\langle u^2-3u-1\rangle$ Halkası……... 47

3.15. $\mathbb{Z}_4[u]/\langle u^2-3u-2\rangle$ Halkası……... 48

3.16. $\mathbb{Z}_4[u]/\langle u^2-3u-3\rangle$ Halkası……... 50

3.17. $r=a+ub\in\mathbb{Z}_4+u\mathbb{Z}_4$ Olmak Üzere R_r Halkalarının Sınıflandırılması……...…… 51

BÖLÜM 4 R_u, R_1, R_0 VE R_3 HALKALARI ÜZERİNDE TANIMLI $(1+2u)$-SABİT DEVİRLİ VE DEVİRLİ KODLARIN GRAY GÖRÜNTÜLERİ……..……..59

4.1. R_u Halkası Üzerinde Tanımlı Lineer Kodlar……... 59

4.2. R_u Halkası Üzerinde Uzunluğu Tek Olan $(1+2u)$-Sabit Devirli Kodlar ile Devirli Kodlar Arasındaki İlişki……. 66

4.3. R_u Halkası Üzerinde Tanımlı Gray Dönüşüm, $(1+2u)$-Sabit Devirli Kodlar ve Tek Uzunluklu Devirli Kodların Gray Görüntüleri…... 67

4.4. R_1 Halkası Üzerinde Uzunluğu Tek Olan $(1+2u)$-Sabit Devirli Kodlar ile Devirli Kodlar Arasındaki İlişki……. 69

4.5. R_1 Halkası Üzerinde Tanımlı Gray Dönüşüm, $(1+2u)$-Sabit Devirli Kodlar ve Tek Uzunluklu Devirli Kodların Gray Görüntüleri…… 70

4.6. R_0 Halkası Üzerinde Uzunluğu Tek Olan $(1+2u)$-Sabit Devirli Kodlar ile Devirli Kodlar Arasındaki İlişki……. 71

4.7. R_0 Halkası Üzerinde Tanımlı Gray Dönüşüm, $(1+2u)$-Sabit Devirli Kodlar ve Tek Uzunluklu Devirli Kodların Gray Görüntüleri…… 72

4.8. R_3 Halkası Üzerinde Uzunluğu Tek Olan $(1+2u)$-Sabit Devirli Kodlar ile Devirli Kodlar Arasındaki İlişki……. 74

4.9. R_3 Halkası Üzerinde Tanımlı Gray Dönüşüm, $(1+2u)$-Sabit Devirli Kodlar ve Tek Uzunluklu Devirli Kodların Gray Görüntüleri….. 75

BÖLÜM 5 R_1 VE R_u HALKALARI ÜZERİNDE TANIMLI DEVİRLİ DNA KODLAR……...78

5.1. R_1 Halkası Üzerinde Tanımlı Devirli DNA Kodlar……. 80

5.1.1. R_1 Halkası Üzerinde Tanımlı Devirli Kodlar……... 80

5.1.2. R_1 Halkası Üzerinde Tanımlı Devirli DNA Kodlar……. 81

5.1.3. R_1 Halkası Üzerinde Tanımlı Ters Sıralı Kodlar……. 83

5.1.4. R_1 Halkası Üzerinde Tanımlı Ters Sıralı Tamamlayan Kodlar……...92

5.2. R_u Halkası Üzerinde Tanımlı Devirli DNA Kodlar …….. …….. 103

5.2.1. $\mathbb{Z}_4$ Halkası Üzerinde Tanımlı Devirli Kodlar……..…….. 103

5.2.2. R_u Halkası Üzerinde Tanımlı Devirli DNA Kodlar.…….. 104

5.2.3. R_u Halkası Üzerinde Tanımlı Ters Sıralı Kodlar … …….. 106

5.2.4. R_u Halkası Üzerinde Tanımlı Ters Sıralı Tamamlayan Kodlar …… 108

BÖLÜM 6 R_1 HALKASI ÜZERİNDE TANIMLI u-SABİT DEVİRLİ KODLAR İLE DEVİRLİ KODLARIN GRAY GÖRÜNTÜLERİ……111

6.1. R_1 Halkası Üzerinde Uzunluğu Tek Olan u-Sabit Devirli Kodlar ile Devirli Kodlar Arasındaki İlişki……..…….... 111

6.2. R_1 Halkası Üzerinde Tanımlı Gray Dönüşüm, u-Sabit Devirli Kodlar ve Tek Uzunluklu Devirli Kodların Gray Görüntüleri…… 115

BÖLÜM 7 SONUÇLAR VE TARTIŞMA……. 120

7.1. Sonuçlar……120

7.2. Gelecek Çalışma……...121

KAYNAKLAR…….. 122

ÖZGEÇMİŞ……... 124

SEMBOLLER VE KISALTMALAR DİZİNİ

$\mathbb{F}_q$	q elemanlı sonlu cisim
$\mathbb{F}_q^n$	n boyutlu $\mathbb{F}_q$-vektör uzayı
(n, M, d)	uzunluğu n, eleman sayısı M ve minimum uzaklığı d olan kodun temsili
$[n, k, d]$	uzunluğu n, boyutu k ve minimum uzaklığı d olan lineer kodun temsili
$d(x, y)$	x ile y arasındaki uzaklık
d_H, d_L	Sırasıyla Hamming ve Lee uzaklık fonksiyonları
w_H, w_L	Sırasıyla Hamming ve Lee ağırlık fonksiyonları
$\mathbb{F}_q[x]$	Katsayıları $\mathbb{F}_q$'da olan x değişkenli polinom halkası
$g^*(x)$	$g(x)$ polinomunun reciprocal polinomu
$\|C\|$	C kodunun eleman sayısı
$C^\perp$	C kodunun duali
ϕ	Gray dönüşüm
φ	Devirli öteleme
σ	Sabit devirli öteleme
R_r	$r = a + ub \in \mathbb{Z}_4 + u\mathbb{Z}_4$ olan sonlu halka sınıfı

$c^R(x)$ $c = (c_0, c_1, \dots, c_{n-1})$ kod sözcüğüne karşılık gelen $c(x)$'in ters sıralı polinomu

$c^{RC}(x)$ $c = (c_0, c_1, \dots, c_{n-1})$ kod sözcüğüne karşılık gelen $c(x)$'in ters sıralı tamamlayan polinomu

ŞEKİLLER DİZİNİ

Şekil 1.1 Temel İletişim Sistemi……. 1

Şekil 3.1 R_0 Halkasının İdeallerinin Oluşturduğu Kafes…… 29

Şekil 3.2 R_1 Halkasının İdeallerinin Oluşturduğu Kafes…….31

Şekil 3.3 R_2 Halkasının İdeallerinin Oluşturduğu Kafes…… 32

Şekil 3.4 R_3 Halkasının İdeallerinin Oluşturduğu Kafes…… 34

Şekil 3.5 R_u Halkasının İdeallerinin Oluşturduğu Kafes…… 35

Şekil 3.6 R_{2u} Halkasının İdeallerinin Oluşturduğu Kafes…….. 37

Şekil 3.7 R_{3u} Halkasının İdeallerinin Oluşturduğu Kafes…….. 38

Şekil 3.8 R_{1+u} Halkasının İdeallerinin Oluşturduğu Kafes…… 40

Şekil 3.9 R_{2+u} Halkasının İdeallerinin Oluşturduğu Kafes…… 41

Şekil 3.10 R_{3+u} Halkasının İdeallerinin Oluşturduğu Kafes……..……. 42

Şekil 3.11 R_{1+2u} Halkasının İdeallerinin Oluşturduğu Kafes……...44

Şekil 3.12 R_{2+2u} Halkasının İdeallerinin Oluşturduğu Kafes……...45

Şekil 3.13 R_{3+2u} Halkasının İdeallerinin Oluşturduğu Kafes……...47

Şekil 3.14 R_{1+3u} Halkasının İdeallerinin Oluşturduğu Kafes……...48

Şekil 3.15 R_{2+3u} Halkasının İdeallerinin Oluşturduğu Kafes……...49

Şekil 3.16 R_{3+3u} Halkasının İdeallerinin Oluşturduğu Kafes……...51

Şekil 6.1 R_1 Halkası Üzerindeki Devirli ve Sabit Devirli Kodların Gray Görüntülerinin Diyagramı……..119

ÇİZELGELER DİZİNİ

Çizelge 3.1 R_0 Halkasının Elemanlarının Toplama İşlem Tablosu……27

Çizelge 3.2 R_0 Halkasının Elemanlarının Çarpma İşlem Tablosu……. 28

Çizelge 3.3 $r = a + ub \in \mathbb{Z}_4 + u\mathbb{Z}_4$ Olmak Üzere R_r Halkalarının Sınıflandırılması……...58

Çizelge 5.1 R_1 Halkasının Elemanlarına Karşılık Gelen DNA Çiftleri …….82

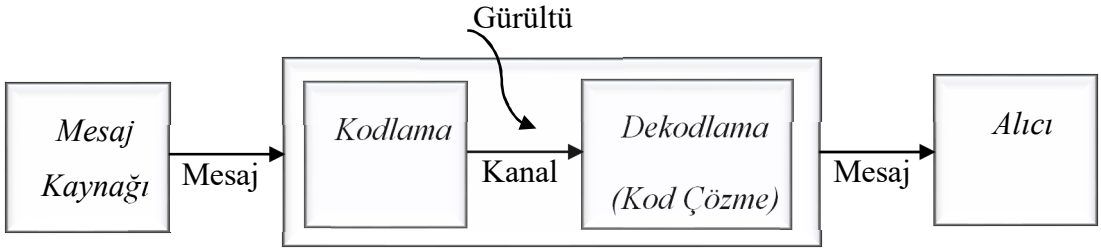
Çizelge 5.2 $r = a + ub \in R_1$ Elemanlarına Karşılık Gelen $\overline{r}$ Tamamlayanları Tablosu …… 94

Çizelge 5.3 R_u Halkasının Elemanlarınına Karşılık Gelen DNA Çiftleri 105

BÖLÜM 1

GİRİŞ

Kodlama teorisinin başlangıcı Claude Shannon'un 1948 yılında yayımlamış olduğu 'A Mathematical Theory of Communication' adlı makalesi kabul edilir. Bu makalede bir iletişim kanalında (radyo, telefon, uydu...) eğer özel bir kodlama ve kod çözme teknikleri kullanılırsa, belirlenen bir sayının altındaki değerler için güvenilir iletişimin sağlanacağı ifade edilmiştir. Başlangıç kabul edilen bu makaleden sonra kodlama teorisinde, kanal boyunca kodlanmış verinin iletimi ve bozulan mesajı düzeltme gibi konular ile ilgilenilmiş ve doğru iletim oranı yüksek, zaman ve enerji tasarrufu sağlayan kodlama yöntemleri geliştirmek amaç edinilmiştir.



Şekil 1.1 Temel İletişim Sistemi

Şekil 1.1'de temel bir iletişim sisteminde iletilecek olan mesajın, kaynağından alıcıya ulaşıncaya kadar izlediği süreç ifade edilmektedir. Böyle bir temel iletişim sisteminde iletilecek mesaj, mesaj kaynağından kanala aktarılır, kanalda iletilecek mesaja oluşabilecek hatalardan (ekipman eksikliği, insan hatası, hava koşulları, vb..) korumak üzere çeşitli matematiksel kodlama yöntemleri uygulanır, kodlanan mesaj, bir takım hatalar sebebiyle bozulmuş olarak dekodlama (kod çözme) birimine geldiğinde, mesajın

kodlama algoritması ile uyumlu olarak tasarlanmış bir dekodlama yöntemi ile dekodlanıp alıcıya doğru olarak iletimini sağlamak amaçlanır.

Kodlama teorisinde, yapılan ilk çalışmalar $\mathbb{F}_2$ sonlu cismi üzerindedir. İlk olarak 1972 yılında Blake tarafından çalışmalar sonlu halkalar üzerine taşınmıştır. 1994 yılında Hammons ve diğerleri, $\mathbb{Z}_4$ sonlu halkası üzerinde tanımlı bir Gray dönüşümü yardımıyla lineer olmayan ancak iyi parametrelere sahip kod ailelerinin, $\mathbb{Z}_4$ üzerinde lineer kodların Gray görüntüsü olduğunu bulması, kodlama teorisinde çığır açan bir çalışma olmuştur. Bu buluşun ardından lineer olmayan kodlarla çalışma daha kolay bir hale gelmiştir ve böylece kodlama teorisi sonlu halkalar üzerinde taşınmıştır.

Halkalar ya da cisimler üzerinde lineer ve lineer olmayan kodlar tanımlanabilir. Ancak lineer kodların cebirsel yapısı (alt vektör uzayı ya da alt modüle karşılık gelmesi) nedeniyle çalışmaya daha elverişlidir.

Devirli kodlar ilk kez 1957 yılında Prange tarafından lineer kodların önemli bir sınıfı olarak tanımlanmıştır. Prange sonlu bir cisim üzerinde uzunluğu n olan devirli bir kodu, katsayıları sonlu cisimde x değişkenine bağlı polinom halkasını $\langle x^n - 1 \rangle$ idealine bölerek, bu bölüm halkasının ideallerine karşılık getirmiştir. Böylece devirli kodun ideallerinin zengin cebirsel yapısı ile çalışma imkanı sağlamıştır. Daha geniş bir sınıf olan ve devirli kodları da kapsayan sabit devirli (constacylic) kodların tanımlanmasının ardından, devirli kodlar ile sabit devirli kodların Gray dönüşümü yardımıyla aralarındaki ilişkiyi inceleyen bir çok makale bulunmaktadır (Ashraf & Mohammad, 2015; Yu vd., 2016; Aydin vd., 2017; Shi vd., 2017; Dinh vd., 2018; Bag vd., 2018).

Kodlama teorisinin daha da gelişmesi ile birlikte, DNA dizilerindeki matematiksel özellikler, birçok araştırmacıya biyoloji ve cebirsel kodlama teorisini kullanarak disiplinler arası keşif için ilham kaynağı olmuştur. İlk DNA hesaplama fikri 1987 yılında Tom Head tarafından ortaya atılmıştır. Fakat ilk deneysel çalışma L. Adleman tarafından yapılmıştır. Son zamanlarda, Silikon bazlı hesaplama sistemlerinden daha fazla depolama kapasitesine sahip DNA tabanlı veri depolama sistemleri birçok araştırmacının dikkatini çekmiştir. DNA molekülünün bu elverişli yapısı sonlu cisimler ve sonlu halkalar üzerinde kodlama teorisine büyük katkıda bulunmuştur. Devirli DNA kodlarındaki

çalışmalar, farklı eleman sayılarına sahip cisim ve halkalar üzerinde günümüze kadar devam etmektedir.

1.1. Tez Organizasyonu

Tezin geri kalan kısmı şu şekilde düzenlenmektedir:

Bölüm 2'de, tezde kullanılacak olan bir takım temel önerme, teorem ve sonuçları kapsayan iki alt bölüm yer almaktadır.

Bölüm 3'de, $r = a + ub \in \mathbb{Z}_4 + u\mathbb{Z}_4$ olmak üzere $\mathbb{Z}_4[u]/\langle u^2 - r\rangle \cong R_r = \mathbb{Z}_4 + u\mathbb{Z}_4$, $u^2 = r$ şeklindeki 16 sonlu halkanın idealleri, birimsel elemanları ve özellikleri verilmiştir. Ayrıca bu halkaların birbirleri ile aralarındaki izomorfluk durumları araştırılarak sınıflandırılmıştır.

Bölüm 4'de R_u sonlu halkası üzerinde tanımlı lineer kodlar ve bu halka üzerinde tanımlı $(1 + 2u)$-sabit devirli ve devirli kodların Gray görüntülerinin verildiği makaleler incelenmiştir. Ayrıca R_0, R_1 ve R_3 halkaları üzerinde $(1 + 2u)$ birimsel elemanı kullanılarak sabit devirli kodlar ve devirli kodların Gray görüntülerinin elde edildiği makalelerdeki bazı teorem ve sonuçlara yer verilmiştir.

Bölüm 5'de, R_1 ve R_u halkaları üzerinde tanımlı devirli kodların yapısı, bu kodların DNA özelliklerine sahip olması için gerekli ve yeterli koşulları içeren sonuçların verildiği makaleler incelenmiştir.

Bölüm 6'da, R_1 halkası üzerinde tanımlı yeni bir Gray dönüşümü tanımlanarak, u-sabit devirli ve devirli kodların Gray görüntüleri elde edilmiştir.

Bölüm 7'de, tezin kapsamında elde edilen sonuçlara yer verilmiştir.

BÖLÜM 2

TEMEL KAVRAMLAR

2.1. Cebir ile İlgili Temel Kavramlar

Kodlama teorisi, matematiğin bir alt dalı olan cebir ile yakından ilişkilidir. Kodlama teorisinde; sayılar teorisi, lineer cebir ve soyut cebir gibi cebir konularını içeren tanım, teorem ve sonuçlar sıkça kullanılmaktadır. Bu sebeple tezin bütünlüğünü korumak amacıyla, bu bölümde tezin kapsamı içinde bulunan konularla ilgili bazı temel tanım, önerme, teorem ve sonuçlara yer verilmektedir.

2.1.1. Tanım:

G boş olmayan herhangi bir küme olsun. $G \times G$ kümesinden G kümesine tanımlı bir

$$*: G \times G \to G$$
$$(a, b) \mapsto a * b$$

fonksiyonuna G üzerinde tanımlı bir ‘‘*ikili işlem*’’ denir. Bir küme üzerinde bir ya da daha fazla ikili işlem tanımlı ise bu kümeye ‘‘*cebirsel yapı*’’ denir (Karakaş, 2012).

2.1.2. Tanım:

G boş olmayan herhangi bir küme ve $*$, G kümesi üzerinde bir ikili işlem olsun.

i) $*$ işleminin birleşme özelliği vardır. Yani $\forall\, a, b, c \in G$ için $a * (b * c) = (a * b) * c$ dir.

ii) $*$ işleminin etkisiz eleman özelliği vardır. Yani $\exists\, e \in G \ni \forall\, a \in G$ için $a * e = e * a = a$ dir.

iii) $*$ işleminin ters eleman özelliği vardır. Yani $\forall\, a \in G$ için $a * a^{-1} = a^{-1} * a = e$ olacak şekilde en az bir $a^{-1} \in G$ vardır.

Koşullarını sağlayan $(G,*)$ cebirsel yapısına ‘‘*grup*’’ denir.

Ek olarak,

iv) $*$ işleminin değişme özelliği vardır. Yani $\forall\, a, b \in G$ için $a * b = b * a$ dır.

Koşulunu sağlayan $(G,*)$ grubuna, ‘‘*değişmeli grup*’’ (veya *Abel grubu*) denir (Karakaş, 2012).

2.1.3. Tanım:

R boş olmayan herhangi bir küme ve $''+''$ ile $''.''$, R kümesi üzerinde tanımlı iki ikili işlem olsun.

i) $(R,+)$ değişmeli bir gruptur,

ii) $\forall\, a,b,c \in R$ için $(a.b).c = a.(b.c)$ dir.

iii) $\forall\, a,b,c \in R$ için $(a+b).c = a.c + b.c$ ve $a.(b+c) = a.b + a.c$ dir.

koşullarını sağlayan $(R,+,.)$ cebirsel yapısına ‘‘*halka*’’ denir.

Ek olarak,

iv) $\forall\, a,b \in R$ için $a.b = b.a$ olur.

koşulunu sağlayan $(R,+,.)$ halkasına ‘‘*değişmeli halka*’’ denir (Hungerford, 1973).

2.1.4. Tanım:

Eğer $(R,+,.)$ halkasında, $\forall\, a \in R$ için $1_R.a = a.1_R = a$ koşulunu sağlayan bir 1_R elemanı varsa, R'ye ''*birimli halka*'' ve 1_R elemanına ''*birim eleman*'' denir (Hungerford, 1973).

2.1.5. Tanım:

R halkasında $0 \neq a \in R$ elemanı için, $a.b = 0_R$ (veya b.$a = 0_R$) olacak biçimde $\exists\, 0_R \neq b \in R$ varsa a'ya bir ''*sol (sağ) bölen''* denir. R halkasının hem sol hemde sağ sıfır bölen elemanına ''*sıfır bölen*'' denir (Hungerford, 1973).

2.1.6. Tanım:

R , $1_R \neq 0$ birim elemanlı değişmeli bir halka olsun. R'nin sıfır böleni yoksa R halkasına ''*tamlık bölgesi*'' denir (Hungerford, 1973).

2.1.7. Tanım:

R , $1_R \neq 0$ birim elemanlı bir halka olsun. R halkasının 0'dan farklı her elemanı birimsel (tersinir) ise R'ye ''*bölüm halkası (division ring)*'' denir (Hungerford, 1973).

2.1.8. Tanım:

R, bir tamlık bölgesi olsun. $m.1_R = 0_R$ olacak şekilde bir m pozitif tam sayısı varsa bu m'lerin en küçüğüne ''*karakteristik*'' denir. Bu özelliği sağlayan hiçbir m sayısı yoksa R'nin karakteristiği sıfırdır (Çallıalp, 2013).

2.1.9. Tanım:

R bir halka ve $\emptyset \neq S \subseteq R$ olsun. Eğer $\forall\, a, b \in S$ için $a - b \in S$ ve $a.b \in S$ ise S halkasına R'nin bir ''*alt halkası*'' denir (Çallıalp, 2013).

2.1.10. Tanım:

R ve S iki halka olsun. $\forall\, a, b \in R$ için,

i) $f(a+b) = f(a) + f(b)$

ii) $f(a.b) = f(a).f(b)$

koşullarını sağlayan bir $f: R \to S$ fonksiyonuna ‘‘*halka homomorfizması*’’ denir (Hungerford, 1973).

2.1.11. Tanım:

$f: R \to S$ bir halka homomorfizması olsun. Eğer f;

i) Birebir ise ‘‘*monomorfizma*’’,

ii) Örten ise ‘‘*epimorfizma*’’,

iii) Hem birebir hemde örten ise ‘‘*izormorfizma*’’olarak adlandırılır. (Bu durumda, R ve S halkaları *izormorftur* denir. $R \cong S$ ile gösterilir.)

Ek olarak,

R bir halka olmak üzere, eğer $f: R \to R$ bir izomorfizma ise f’ye R’nin ‘‘*otomorfizması*’’ denir (Hungerford, 1973).

2.1.12. Tanım:

0_R, R halkasının etkisiz elemanı olmak üzere, $f: R \to S$ bir halka homomorfizması olsun.

$$Çek\ f = \{a \in R \mid f(a) = 0_R\}$$

biçiminde tanımlanan kümeye f’nin ‘‘*çekirdeği*’’ denir (Çallıalp, 2013).

2.1.13. Teorem:

R bir halka ve $\emptyset \neq I \subseteq R$ olsun. I kümesinin bir ‘‘*sol (sağ) ideal*’’ olması için gerekli ve yeterli koşul $\forall\ a, b \in I$ ve $\forall\ g \in R$ için,

i) $a - b \in I$ ve

ii) $g.a \in I\ (a.g \in I)$

olmasıdır. Eğer I hem sol hemde sağ ideal ise I kümesine ‘‘*ideal*’’ denir (Hungerford, 1973).

2.1.14. Tanım:

R bir halka ve X, R’nin bir alt kümesi olsun. $\{A_i \mid i \in I\}$ ailesi R’nin X kümesini içeren tüm ideallerinin ailesi olsun. Bu durumda, $\cap_{i\in I} A_i$ ailesine ‘‘ X kümesi ile üretilen ideal’’ denir. Bu ideal (X) ile gösterilir.

X kümesinin elamanlarına (X) idealinin ‘‘*üreteçleri*’’ denir. Eğer X sonlu bir küme ise (X) idealine ‘‘*sonlu üretilmiştir*’’ denir. Eğer $X = \{x\}$ tek elemanlı bir küme ise (x) tek elemanı ile üretilen ideale ‘‘*esas ideal*’’ denir (Hungerford, 1973).

2.1.15. Tanım:

Her ideali esas ideal olan halkaya ‘‘*esas ideal halkası*’’, her ideali esas ideal olan tamlık bölgesine ‘‘*esas ideal bölgesi*’’ denir (Hungerford, 1973).

2.1.16. Önerme:

R bir halka ve I, R’nin bir ideali olsun. $\forall\, a, b \in R$ için R halkasının bir I idealine göre her $a, b \in R$ için

$a \equiv b\ (mod\ I) \Leftrightarrow a - b \in I$

şeklinde tanımlanan $\equiv$ bağıntısı bir denklik bağıntısıdır (Çallıalp, 2013).

2.1.17. Önerme:

R/I, R halkasının bir I idealine göre tanımlanan denklik sınıfları kümesi olsun. Herhangi $a + I, b + I \in R/I$ için

$(a + I) \oplus (b + I) = (a + b) + I$ ve $(a + I) \odot (b + I) = (a.b) + I$

biçiminde tanımlanan $\oplus$ ve $\odot$ işlemlerine göre R/I bir bölüm halkasıdır (Çallıalp, 2013).

2.1.18. Teorem:

$f: R \to S$ bir halka homomorfizması ise $\text{Çek}\ f$ kümesi R'nin bir idealidir. Tersine, I, R'nin bir ideali ise $\varphi: R \to R/I$, $\varphi(a) = a + I = \overline{a}$ dönüşümü I çekirdek kümesi ile bir epimorfizmadır. Bu dönüşüme ''*doğal epimorfizma (ya da projeksiyon dönüşümü)*'' denir (Hungerford, 1973).

2.1.19. Teorem:

R birimli ve değişmeli bir halka ve P, R halkasının R'den farklı bir ideali olsun. Eğer $\forall\ a, b \in R$ için,

$a.b \in P \Rightarrow a \in P$ veya $b \in P$

sağlanıyorsa P'ye ''*asal ideal*'' denir. Tersine, P asal ideal ve R değişmeli bir halka ise P ideali yukarıdaki koşulu sağlar (Hungerford, 1973).

2.1.20. Teorem:

R, birimseli $1_R \neq 0$ olan değişmeli bir halka ve P, R halkasının bir ideali olsun. P'nin asal ideal olması için gerekli ve yeterli koşul R/P'nin tamlık bölgesi olmasıdır (Hungerford, 1973).

2.1.21. Tanım:

M, R halkasının bir ideali olsun. Eğer $M \neq R$ ve her $M \subset N \subset R$ koşulunu sağlayan N ideali için $N = M$ ya da $N = R$ oluyorsa M'ye R halkasının bir ''*maksimal ideali*'' denir (Hungerford, 1973).

2.1.22. Teorem:

R, birimseli $1_R \neq 0$ olan değişmeli bir halka ve M,R'nin bir ideali olsun.

i) M maksimal ideal ve R değişmeli ise R/M bölüm halkası bir cisimdir.

ii) R/M bölüm halkası cisim ise M maksimal idealdir (Hungerford, 1973).

2.1.23. Teorem:

Her esas ideal bölgesi tek türlü asal çarpanlarına ayrılabilen bölgedir (Hungerford, 1973).

2.1.24. Tanım:

R birimli ve değişmeli bir halka olsun. Eğer R halkası tek bir maksimal ideale sahip ise R halkasına ‘‘*lokal (yerel) halka*’’ denir. Eğer R halkasının sonlu sayıda birden fazla ideali varsa R halkasına ‘‘*semilokal (yarı yerel) halka*’’ denir (Jitman vd., 2012).

2.1.25. Tanım:

R birimli, değişmeli, lokal ve sonlu bir halka ve aynı zamanda p asal olmak üzere maksimal ideali (p) olan bir halka olsun. Bu durumda R halkasına ‘‘*Galois halkası*’’ denir (Holdman, 2016).

2.1.26. Örnek:

$(\mathbb{Z}_4, +, .)$ halkası bir Galois halkasıdır.

2.1.27. Tanım:

R birimli ve değişmeli bir halka olsun. R halkasının tüm ideallerinin ailesi kapsama bağıntısına göre sıralı ise R halkasına ‘‘*sonlu zincir halkası*’’ denir (Jitman vd., 2012).

2.1.28. Önerme:

R bir sonlu zincir halkası olsun. Bu durumda, R halkasının tüm idealleri esas idealdir ve R’nin tek bir maksimal ideali vardır. τ, R halkasının maksimal idealinin bir üreteci olsun. R halkasının tüm idealleri,

$$R = \langle 1 \rangle \supsetneq \langle \tau \rangle \supsetneq \langle \tau^2 \rangle \supsetneq \cdots \supsetneq \langle \tau^{s-1} \rangle \supsetneq \langle \tau^s \rangle = \langle 0 \rangle$$

olacak şekilde zincir formundadır. Burada s’ye R halkasının ‘‘*nilpotentlik derecesi*’’ denir (Jitman vd., 2012).

2.1.29. Teorem:

R bir halka ve $R[x], R$ halkasının elemanlarından oluşan ve belirli bir yerden sonraki terimleri 0 olan $(a_0, a_1, \dots, a_i, 0,0,0, \dots ,0)$ biçiminde ifade edilen dizilerin kümesi olsun.

i) $R[x]$, toplama ve çarpma işlemleri ile bir halkadır.

ii)

a) R halkası değişmeli ise $R[x]$ halkası da değişmelidir.

b) R halkası birimli ise $R[x]$ halkası da birimlidir.

c) R halkası sıfır bölensiz ise $R[x]$ halkası da sıfır bölensizdir.

d) R halkası tamlık bölgesi ise $R[x]$ halkası da tamlık bölgesidir.

iii) $\psi: R \to R[x]$ dönüşümü bir halka monomorfizmasıdır.
$a \mapsto \psi(a) = (a, 0,0, \dots ,0)$

Bu koşulları sağlayan $R[x]$ halkasına ‘‘*polinom halkası*’’ denir. Bu halkanın elamanlarına ‘‘*polinom*’’ denir (Hungerford, 1973).

2.1.30. Teorem:

R birimli bir halka ve $R[x]$’deki bir $(0, 1_G, 0,0, \dots ,0)$ elemanı x ile gösterilsin. Bu durumda,

i) $x^n = (0,0, \dots ,0, 1_R, 0, \dots)$ dir. Ayrıca buradaki 1_R elemanı dizinin $(n+1)$-inci bileşenidir.

ii) $g \in R$ ise $\forall\, n \geq 0$ için, $gx^n = x^n g = (0,0, \dots ,0, g, 0, \dots)$ dır. Ayrıca buradaki g elemanı dizinin $(n+1)$-inci bileşenidir.

iii) Sıfırdan farklı her $f \in R[x]$ için, $f(x) = r_0 + r_1 x + \cdots + r_{n-1} x^{n-1} + r_n x^n$ eşitliği teklikle belirli olacak şekilde bir n pozitif tam sayısı ve $r_0, r_1, \dots, r_{n-1}, r_n \in R$ elemanları vardır (Hungerford, 1973).

2.1.31. Tanım:

$f(x) = \sum_{i=0}^{n} r_i x^i$ polinom fonksiyonu için, r_o elemanına ‘‘*sabit terim*’’, r_i elemanlarına ‘‘*f’in katsayıları*’’ ve r_n elemanına ‘‘*f’in baş katsayısı*’’, baş katsayısı 1_R olan polinoma ‘‘*monik polinom*’’, $x = (0, 1_R, 0, 0, \dots, 0)$ elemanına ‘‘*bilinmeyen*’’ denir (Hungerford, 1973).

2.1.32. Tanım:

$(R, +, .)$ bir halka ve $(A, +)$ toplamsal değişmeli bir grup olsun. $\forall\, g \in R, a \in A$ için

$\cdot : R \times A \to A$ biçiminde bir fonksiyon tanımlansın. $\forall\, k, l \in R$ ve $\forall\, a, b \in A$ için,
$(g, a) \mapsto g.a$

i) $k.(a + b) = k.a + k.b$

ii) $(k + l).a = k.a + l.a$

iii) $k(l.a) = (kl).a$

koşulları sağlanıyorsa, A’ya bir ‘‘*(sol) R-modül*’’ denir.

Buna ek olarak,

iv) $1_R \in R$ ve $\forall\, k$ için, $1_R.k = k$ koşulu sağlanıyor ise A’ya ‘‘*birimli R-modül*’’ denir. Eğer R bir cisim ise R-modüle ‘‘*vektör uzayı*’’ denir (Hungerford, 1973).

2.1.33. Not:

$\cdot : A \times G \to A$ biçiminde tanımlanan bir fonksiyon olmak üzere,
$(a, g) \mapsto a.g$

sağ R-modül tanımı benzer şekilde ifade edilir.

2.1.34. Tanım:

R, bir halka ve A ile B, R halkası üzerinde iki modül olsun. Bu durumda, $\forall\, a, b \in A$ ve $\forall\, g \in R$ için,

i) $f(a+b) = f(a) + f(b)$

ii) $f(g.a) = g.f(a)$

koşullarını sağlayan $f: A \to B$ fonksiyonuna ‘‘*R-modül homomorfizması*’’ denir (Hungerford, 1973).

2.1.35. Tanım:

$\emptyset \neq A \subseteq B$ olmak üzere, R bir halka ve B kümesi R-modül olsun. Eğer A kümesi, B’nin toplamsal bir alt grubu ve $\forall\, g \in R, a \in A$ için, $ga \in A$ oluyorsa, A’ya B’nin bir ‘‘*alt modülü*’’ denir. Bir kesir halkası üzerinde tanımlı bir vektör uzayın alt modülüne ‘‘*alt uzay*’’ denir (Hungerford, 1973).

2.1.36. Tanım:

N bir R-modül ve bir $n \in \mathbb{N}$ için A kümesi N’nin bir alt kümesi olsun.

i) A kümesi N’yi üretir Yani $\forall\, x \in N$ için, $g_1, g_2, \dots, g_n \in R$ olmak üzere $x = g_1x_1 + g_2x_2 + \cdots + g_nx_n$ olacak şekildeki $x_1, x_2, \dots, x_n \in A$ vardır.

ii) A kümesi doğrusal bağımsızdır. Yani, her $g_1, g_2, \dots, g_n \in R$ ve $x_1, x_2, \dots, x_n \in A$ için $g_1x_1 + g_2x_2 + \cdots + g_nx_n = 0$ ise $g_1 = g_2 = \cdots = g_n = 0$ dır.

koşulları sağlanıyorsa A kümesine, N R-modülü için bir ‘‘*baz*’’ denir. Bazın elaman sayısına ise ‘‘*rank*’’ adı verilir. Bir baza sahip modüle ‘‘*serbest modül*’’ denir (Taşçı, 2007).

2.1.37. Tanım:

V, F cismi üzerinde tanımlı bir vektör uzayı ve $S \in V$ bir vektör olsun.

$S = c_1a_1 + c_2a_2 + \cdots + c_na_n = \sum_{i=1}^{n} c_ia_i$

koşulunu sağlayan $c_1, c_2, \dots c_n \in F$ skalerleri varsa S vektörüne $a_1, a_2, \dots, a_n \in V$ vektörlerinin ‘‘*doğrusal birleşimi*’’ denir (Hoffman ve Kunze, 1971).

2.1.38. Tanım:

V, F cismi üzerinde tanımlı bir vektör uzayı ve $A \subseteq V$ olsun. A kümesi F cismi üzerinde vektör toplamı ve skalerle çarpma işlemlerine göre bir vektör uzayı oluyorsa, A kümesine ‘‘*V'nin bir alt uzayı*’’ denir (Hoffman ve Kunze, 1971).

2.1.39. Teorem:

V, F cismi üzerinde tanımlı bir vektör uzayı ve $A \subseteq V$ olsun. A kümesinin V'nin bir alt uzayı olması için gerekli ve yeterli koşul $\forall\, a, b \in A$ ve $\forall\, c \in F$ için $ca + b \in A$ olmasıdır (Hoffman ve Kunze, 1971).

2.1.40. Tanım:

V bir vektör uzayı ve $A \subseteq V$ olsun. V vektör uzayının A'yı kapsayan bütün alt uzaylarının arakesiti B'ye ‘‘*A tarafından gerilen alt uzay*’’ denir (Hoffman ve Kunze, 1971).

2.1.41. Teorem:

Herhangi bir vektör uzayının boş kümeden farklı A kümesi ile gerilen alt uzayı, A'daki vektörlerin bütün doğrusal kombinasyonlarının kümesidir (Hoffman ve Kunze, 1971).

2.1.42. Tanım:

V, F cismi üzerinde tanımlı bir vektör uzayı ve $A \subseteq V$ olsun. Eğer,

$$c_1 a_1 + c_2 a_2 + \cdots + c_n a_n = 0$$

koşulunu sağlayan $a_1, a_2, \ldots, a_n \in A$ vektörleri ve tümü 0 olmayan $c_1, c_2, \ldots c_n \in F$ skalerleri varsa, A kümesine ‘‘*doğrusal bağımlıdır*’’ aksi takdirde ‘‘*doğrusal bağımsızdır*’’ denir (Hoffman ve Kunze, 1971).

2.1.43. Tanım:

V bir vektör uzayı olmak üzere, V'yi geren ve V'nin doğrusal bağımsız vektörlerinden oluşan kümeye ''*V'nin bir tabanı*'' denir. Eğer V'nin tabanı sonlu ise, V'ye ''*sonlu boyutlu vektör uzayı*'' denir (Hoffman ve Kunze, 1971).

2.1.44. Tanım:

$A \neq \emptyset$ ve $f: A \to A$ fonksiyonu verilsin. Eğer f birebir ve örten ise, f'e A kümesi üzerinde bir ''*permütasyon*'' denir. Özel olarak, $A_n = \{1,2, \dots, n\}$ kümesi üzerinde tanımlı tüm permütasyonların grubu S_n ile gösterilir. S_n kümesine ''*n-inci simetrik grup*'' denir. S_n kümesindeki herhangi bir δ permütasyonu, $\delta = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \delta(1) & \delta(2) & \delta(3) & \dots & \delta(n) \end{pmatrix}$ biçiminde gösterilir (Karakaş, 2012).

2.2. Kodlama Teorisi ile İlgili Temel Kavramlar

Kodlama teorisinin konuları, bilgi iletimi ya da depolanması sürecinde iletişim kanalında mesajın kodlanmasından başlayarak alıcıya ulaşana kadar olan tüm aşamaları kapsamaktadır. Eğer hata varsa tespit edilmesi ve düzeltilmesi de bu sürece dahildir. Bu bölümde, tezin bütünlüğünü korumak amacıyla, tezin kapsamı içinde bulunan kodlama teorisinin kapsadığı genel tanım ve teoremlere yer verilmektedir.

2.2.1. Tanım:

$A = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ sonlu kümesine ''*alfabe*'' ve bileşenleri A kümesinin elemanlarından oluşan sonlu dizilişlerin kümesine ''*q-ary kod (q-lu kod)*'' denir (Roman, 1992).

2.2.2. Tanım:

Her $i \in \{1,2, \dots, n\}$ için $\alpha_i \in A$ olmak üzere $\alpha = \alpha_1 \alpha_2 \dots \alpha_n$ elemanına A üzerinde tanımlı n uzunluğunda bir ''*q-lu sözcük*'' denir.

$$\alpha_1 \alpha_2 \dots \alpha_n \leftrightarrow (\alpha_1, \alpha_2, \dots, \alpha_n)$$

ile gösterilir (Roman, 1992).

2.2.3. Tanım:

$\emptyset \neq C \subseteq A^n$ olmak üzere C kümesine A üzerinde tanımlı n uzunluğunda ‘‘*q-lu blok*’’ kod ve kodun bir elemanına da ‘‘*kod sözcüğü*’’ denir.

C kodunun eleman sayısı $|C| = M$ ile gösterilirse C koduna n uzunluğunda M elemanlı bir kod denir ve (n, M) ile gösterilir (Roman, 1992).

2.2.4. Tanım:

p asal $n \in \mathbb{Z}_+$ olmak üzere $q = p^n$ elemanlı sonlu cisme ‘‘*Galois cismi*’’ denir. $\mathbb{F}_q$ ya da $G\mathbb{F}(q)$ ile gösterilir (Holdman, 2016).

2.2.5. Tanım:

$V(q, n) = \mathbb{F}_q^n = \{x = (x_1, x_2, \dots, x_n) \mid x_i \in \mathbb{F}_q, i = 1,2, \dots, n\}$ kümesi $\mathbb{F}_q$ sonlu cismi üzerinde bir vektör uzayı olmak üzere, $\mathbb{F}_q^n$, $\mathbb{F}_q$ vektör uzayının bir C alt uzayına ‘‘*lineer kod*’’ denir.

C, $\mathbb{F}_q^n$ vektör uzayının k boyutlu bir alt uzayı ise C ye $\mathbb{F}_q$ üzerinde tanımlı bir ‘‘*lineer [n, k]-kod*’’ ya da kısaca ‘‘*[n, k]-kod*’’ denir (Huffman vd., 2003).

2.2.6. Tanım:

$C, \mathbb{F}_q$ üzerinde tanımlı bir $[n, k]$-kod olsun. Bir C lineer kodunun taban elemanlarının bileşenlerinin oluşturduğu $k \times n$ mertebeli matrise C kodunun ‘‘*üreteç matrisi*’’ denir ve G ile gösterilir. G üreteç matrisi, $I_k, k \times k$ mertebeli birim matris, A, $k \times (n - k)$ mertebeli bileşenleri $\mathbb{F}_q$’dan seçilen bir matris olmak üzere $[\, I_k \mid A \,]$ şeklinde düzenlenirse $[\, I_k \mid A \,]$ matrisine G’nin ‘‘*standart formu*’’ adı verilir (Huffman vd., 2003).

2.2.7. Tanım:

$C = \{(\, v_1, v_2, \dots, v_n\,) \in \mathbb{F}_q^n \mid [\, v_1 v_2 \dots v_n\,] H^T = 0\,\}$ ile tanımlı $(n-k) \times n$'lık H matrisine, $C, [n,k]$ lineer kodunun ''*kontrol matrisi (parity-check matrisi)*'' denir (Huffman vd., 2003).

2.2.8. Teorem:

$C, \mathbb{F}_q$ üzerinde tanımlı bir $[n,k]$-kod olsun. Eğer C kodunun standart formdaki üreteç matrisi $G = [\, I_k \mid A\,]$ ise $H = [-A^T \mid I_k]$, C kodunun kontrol matrisidir (Huffman vd., 2003).

2.2.9. Tanım:

Her $x = (x_1, x_2, \dots, x_n), y = (y_1, y_2, \dots, y_n) \in \mathbb{F}_q^n$ için

$$d: \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{N} \cup \{0\}$$
$$(x, y) \mapsto d(x, y) = |\{i \mid x_i \neq y_i, i = 1, \dots, n\}|$$

biçiminde tanımlanan d dönüşümüne ''*Hamming uzaklığı*'' denir (Ling ve Xing, 2004).

2.2.10. Tanım:

Bir C kodunun birbirinden farklı kod sözcüklerinin Hamming uzaklığının en küçüğüne C kodunun ''*minimum uzaklığı''* denir ve

$d = d(C) = min\{\, d(x,y) \mid x \neq y,\ x, y \in C\,\}$ biçiminde gösterilir (Ling ve Xing, 2004).

2.2.11. Tanım:

Uzunluğu n, eleman sayısı M ve minimum uzaklığı d olan bir C koduna ''$(\, n, M, d)$-*kod*'' denir (Ling ve Xing, 2004).

2.2.12. Teorem:

Minimum uzaklığı d olan bir lineer kod, $d-1$ tane hatayı tespit eder ve $\left\lfloor \frac{d-1}{2} \right\rfloor$ tane hatayı düzeltir (Ling ve Xing, 2004).

2.2.13. Tanım:

$x, \mathbb{F}_q^n$ bir vektör uzayın herhangi bir elemanı olsun. Bu durumda, x elemanının sıfırdan farklı bileşenlerinin sayısına ‘‘*x elemanının Hamming ağırlığı*’’ denir. $w(x)$ ya da $w_H(x)$ ile gösterilir.

Bir C kodunun sıfırdan farklı tüm kod sözcüklerinin ağırlıklarının en küçüğüne C kodunun ‘‘*minimum ağırlığı*’’ denir. $w(C)$ ya da $w_H(C)$ ile gösterilir (Ling ve Xing, 2004).

2.2.14. Lemma:

$\forall\, x, y \in \mathbb{F}_q^n$ için, $d_H(x,y) = w_H(x-y)$ eşitliği sağlanır (Ling ve Xing, 2004).

2.2.15. Teorem:

C bir lineer kod olsun. Bu durumda, $d_H(C) = w_H(C)$ eşitliği sağlanır (Ling ve Xing, 2004).

2.2.16. Tanım:

$C, \mathbb{F}_q^n$ vektör uzayının bir alt kümesi ve φ, $c = (c_0, c_1, \dots, c_{n-1}) \in \mathbb{F}_q^n$ için $\varphi(c) = (c_{n-1}, c_0, \dots, c_{n-2}) \in \mathbb{F}_q^n$ biçiminde tanımlı bir devirli öteleme olmak üzere $\varphi(C) = C$ oluyorsa C kümesine ‘‘*devirli (cyclic) küme*’’ denir. C lineer bir kod ve devirli bir küme ise C koduna ‘‘*devirli kod*’’ denir (Hill, 1986).

2.2.17. Tanım:

C lineer bir kod olsun. n pozitif tam sayı ve $1 \leq i \leq n$ olacak biçimdeki i sayısı n’nin bir böleni olmak üzere $c = (c_0, c_1, \dots, c_{n-1}) \in C$ iken

$(c_{n-i}, c_{n-i+1}, \dots, c_{n-1}, c_0, c_1, \dots, c_{n-i-1}) \in C$ oluyorsa, C lineer koduna ‘‘*i-indeksli quasicyclic kod*’’ denir.

1-indeksli quasicyclic koda ‘‘*devirli kod*’’ denir (Ling ve Xing, 2004).

2.2.18. Tanım:

$C, \mathbb{F}_q$ üzerinde tanımlı lineer bir kod ve $\lambda \in {\mathbb{F}_q}^*$ olsun. Bu durumda, her $c = (c_0, c_1, \dots, c_{n-1}) \in C$ iken $\sigma(C) = (\lambda c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in C$ sağlanıyorsa, C lineer koduna ‘‘*λ- sabit devirli kod (λ-constacyclic kod)*’’ denir. σ’ya ‘‘*sabit devirli öteleme*’’ denir. Ek olarak, $\lambda = -1$ olması durumunda, C lineer koduna ‘‘*negacyclic kod*’’ denir.

$\lambda = 1$ olması durumunda sabit devirli kod ile devirli kod tanımları çakışır. Bu tanımdaki $c = (c_0, c_1, \dots, c_{n-1}) \in \mathbb{F}_q^n$ için $\sigma(C) = (\lambda c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in \mathbb{F}_q^n$ biçiminde tanımlı σ’ya ‘‘*sabit devirli öteleme (constacyclic shift)*’’ denir (Ling ve Xing, 2004).

2.2.19. Tanım:

C, R sonlu halkası üzerinde tanımlı uzunluğu n olan bir kod ve λ, R halkasında tersi olan bir eleman olsun.

$$\sigma: R^n \to R^n$$
$$c = (c_0, c_1, \dots, c_{n-1}) \mapsto \sigma(c) = (\lambda c_{n-1}, c_0, c_1, \dots, c_{n-2})$$

biçiminde tanımlanan dönüşüm için $\sigma(C) = C$ sağlanıyorsa C koduna ‘‘*λ- sabit devirli kod (λ-constacyclic kod)*’’ denir.

Buna ek olarak, eğer $\lambda = 1$ ise bu koda ‘‘*devirli (cyclic) kod*’’ ve $\lambda = -1$ ise bu koda ‘‘*negacyclic kod*’’ denir (Dinh, 2010).

2.2.20. Önerme:

λ, R halkasında birimsel eleman olsun. $\pi: R^n \to R[x]/\langle x^n - \lambda \rangle$ şeklinde tanımlanan dönüşüm R-modül homomorfizmasıdır. C, R halkası üzerinde tanımlı λ-sabit devirli kod olması için gerekli ve yeterli koşul $\pi(C) \subseteq R[x]/\langle x^n - \lambda \rangle$ ideal

olmasıdır. $\lambda = 1$ alınırsa, devirli kodun polinom temsili tanımı elde edilir (Ling ve Xing, 2004).

2.2.21. Teorem:

$1 \neq n \in \mathbb{N}$ olsun. Bu durumda, $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ halkası bir esas ideal halkasıdır (MacWilliams vd., 1983).

2.2.22. Teorem:

$$\pi : \mathbb{F}_q^n \to \mathbb{F}_q[x]/\langle x^n - 1\rangle$$

$$a = (a_0, a_1, \dots, a_{n-1}) \mapsto \pi(a) = a_0 + a_1 x + \dots + a_{n-1}x^{n-1} + \langle x^n - 1\rangle = \overline{a(x)}$$

biçiminde tanımlanan fonksiyon bir vektör uzayı izomorfizması olmak üzere $C, \mathbb{F}_q^n$ üzerinde tanımlı uzunluğu n olan lineer bir kodun devirli olması için gerekli ve yeterli koşul $I = \pi(C)$'nin $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ halkasının bir ideali olmasıdır (Ling ve Xing, 2004).

2.2.23. Teorem:

I, $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ halkasının bir ideali olsun. Eğer $\overline{a(x)}, I$ idealinin sıfırdan farklı en küçük dereceli bir monik polinomu ise,

i) $\overline{a(x)}$ polinomu I idealinin bir üretecidir ve bu monik polinom tektir.

ii) $a(x)$ üreteç polinomu $x^n - 1$'i böler.

koşulları sağlanır (Ling ve Xing, 2004).

2.2.24. Teorem:

$C, \mathbb{F}_q$ üzerinde tanımlı uzunluğu n olan devirli bir kod olsun. C koduna karşılık gelen $\overline{a(x)}$ polinomu, $\pi(C)$ idealinin sıfırdan farklı en küçük dereceli bir monik polinomu ise $a(x)$ polinomuna C'nin ''*üreteç polinomu*'' denir.

$$\pi(C) = \langle \overline{a(x)} \rangle = \{\overline{r(x)}\ \overline{a(x)} \mid \overline{r(x)} \in \mathbb{F}_q[x]/\langle x^n - 1\rangle\}$$

biçiminde ifade edilir (Ling ve Xing, 2004).

2.2.25. Teorem:

$\mathbb{F}_q[x]$ halkasında tanımlı $x^n - 1$ polinomunun her monik böleni $\mathbb{F}_q$ üzerinde tanımlı n uzunluğunda devirli bir kod üretir (Ling ve Xing, 2004).

2.2.26. Teorem:

$a(x) = a_0 + a_1x + \cdots + a_rx^r$ polinomu devirli bir kodun üreteci ise $a_0 \neq 0$ dır (Hill, 1986).

2.2.27. Teorem:

$\text{der}\big(a(x)\big) = r$ olmak üzere, $a(x) = a_0 + a_1x + \cdots + a_rx^r$ polinomu uzunluğu n olan C devirli kodunun üreteç polinomu olsun. Bu durumda, C kodunun boyutu $boy\ (C) = n - r = k$ ve C'nin üreteç matrisi,

$$G = \begin{bmatrix} a_0 & a_1 & \cdots & a_r & 0 & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_r & 0 & \cdots & 0 \\ \vdots & \ddots & & \ddots & & \ddots & & \vdots \\ 0 & 0 & & \cdots & a_0 & a_1 & \cdots & a_r \end{bmatrix}$$

biçimindedir (Hill, 1986).

2.2.28. Tanım:

Bir kodun kod sözcüklerinin bileşenlerine bir permütasyon uygulandığında diğer kodun kod sözcükleri elde ediliyorsa bu iki koda ‘‘*permütasyon denk kod*’’ denir (Huffman vd., 2003).

2.2.29. Tanım:

S sonlu bir halka olsun. $\forall\ g = (g_0, g_1, \dots, g_{n-1}) \in S^n$ için $(g_{n-1}, g_{n-2}, \dots, g_1, g_0) \in S^n$ vektörüne g'nin ‘‘*ters sıralısı (reversible)*’’ denir ve g^R ile gösterilir. C kodu S halkası üzerinde tanımlı lineer bir kod olmak üzere, eğer $\forall g \in C$ için $g^R \in C$ oluyorsa, C koduna ‘‘*ters sıralı kod*’’ denir.

g kod sözcüğüne karşılık gelen polinom $g(x) = g_0 + g_1x + \cdots + g_{n-1}x^{n-1}$ ile temsil edilsin. Bu durumda $g(x)$'in ters sıralı polinomu $g(x)^R = g_{n-1} + g_{n-2}x + \cdots + g_0x^{n-1}$ biçiminde gösterilir (Dinh vd., 2018).

2.2.30. Tanım:

S sonlu bir halka olsun. $\forall\, g = (g_0, g_1, \ldots, g_{n-1}) \in S^n$ için $(\overline{g_0}, \overline{g_1}, \ldots, \overline{g_{n-1}}) \in S^n$ vektörüne g'nin ''*tamamlayanı (complement)*'' denir ve g^C ile gösterilir. Burada $\bar{a}$, $a \in S$'nin tamamlayanını belirtmektedir. C kodu S üzerinde tanımlı lineer bir kod olmak üzere, eğer $g \in C$ için $g^C \in C$ oluyorsa, C koduna ''*tamamlayan kod*'' denir.

g kod sözcüğüne karşılık gelen polinom $g(x) = g_0 + g_1x + \cdots + g_{n-1}x^{n-1}$ ile temsil edilsin. Bu durumda $g(x)$'in tamamlayan polinomu $g(x)^C = \overline{g_0} + \overline{g_1}x + \cdots + \overline{g_{n-1}}x^{n-1}$ biçiminde gösterilir (Dinh vd., 2018).

2.2.31. Tanım:

S sonlu bir halka olsun. $\forall\, g = (g_0, g_1, \ldots, g_{n-1}) \in S^n$ için $(\overline{g_{n-1}}, \overline{g_{n-2}}, \ldots, \overline{g_1}, \overline{g_0}) \in S^n$ vektörüne g'nin ''*ters sıralı tamamlayanı (reversible complement)*'' denir ve g^{RC} ile gösterilir. C kodu S üzerinde tanımlı lineer bir kod olmak üzere, eğer $g \in C$ için $g^{RC} \in C$ oluyorsa, C koduna '' *ters sıralı tamamlayan kod*'' denir.

g kod sözcüğüne karşılık gelen polinom $g(x) = g_0 + g_1x + \cdots + g_{n-1}x^{n-1}$ ile temsil edilsin. Bu durumda $g(x)$'in ters sıralı tamamlayan polinomu $g(x)^{RC} = \overline{g_{n-1}} + \overline{g_{n-2}}x + \cdots + \overline{g_0}x^{n-1}$ biçiminde gösterilir (Dinh vd., 2018).

2.2.32. Tanım:

$a_t \neq 0$ olmak üzere, $f(x) = a_0 + a_1x + \cdots + a_tx^t$ olsun. $f^*(x) = x^t f(\frac{1}{x})$ biçiminde tanımlanan $f^*(x)$ polinomuna $f(x)$'in ''*reciprocal polinomu*'' denir (Dinh vd., 2018).

2.2.33. Tanım:

S sonlu bir halka olsun. $f^*(x)$, $f(x) = a_0 + a_1x + \cdots + a_tx^t \in S[x]$ polinomunun reciprocal polinomu olmak üzere, bir m birimsel elemanı için $f^*(x) = mf(x)$ oluyorsa, $f(x)$ polinomuna ‘‘*self-reciprocal polinom*’’ denir (Dinh vd., 2018).

2.2.34. Tanım:

C, S halkası üzerinde tanımlı uzunluğu n olan devirli bir kod olsun. Bu durumda, $\forall\, a = (a_0, a_1, \dots, a_{n-1}) \in C$ için $a^{RC} = (\overline{a_{n-1}}, \overline{a_{n-2}}, \dots, \overline{a_0}) \in C$ ise C koduna ‘‘*devirli DNA kodu*’’ denir (Dinh vd., 2018).

BÖLÜM 3

$\mathbb{Z}_4[u]\,/\langle u^2 - r\rangle \cong R_r = \mathbb{Z}_4 + u\mathbb{Z}_4, u^2 = r$ HALKALARININ ÖZELLİKLERİ VE SINIFLANDIRILMASI

Bu bölümde, $r = a + ub \in \mathbb{Z}_4 + u\mathbb{Z}_4$ olmak üzere $\mathbb{Z}_4[u]\,/\langle u^2 - r\rangle \cong R_r = \mathbb{Z}_4 + u\mathbb{Z}_4, u^2 = r$ olacak şekildeki tüm halkaların idealleri, birimsel elemanları ve özellikleri verilmektedir. Ayrıca bu bölümde tanıtılan halkaların birbirleri ile aralarındaki izomorfluk durumları araştırılarak sınıflandırılmaktadır.

3.1. $\mathbb{Z}_4[u]/\langle u^2\rangle$ Halkası

$\mathbb{Z}_4[u]/\langle u^2\rangle = \{a + ub + \langle u^2\rangle \mid a, b \in \mathbb{Z}_4\}$ halkası için,

$u^2 = 0$ şartı göz önüne alındığında,

$$a + ub + \langle 0\rangle = \{a + ub + 0k \mid a, b \in \mathbb{Z}_4, k \in \mathbb{Z}_4 + u\mathbb{Z}_4\}$$

$$= \{a + ub\}$$

olduğundan, $\mathbb{Z}_4[u]/\langle u^2\rangle = \{\{a + ub\} \mid a, b \in \mathbb{Z}_4\}$ bulunur. Bu durumda,

$R_0 = \mathbb{Z}_4 + u\mathbb{Z}_4 = \{a + ub \mid a, b \in \mathbb{Z}_4\,, u^2 = 0\,\}$ kümesinin $\mathbb{Z}_4[u]/\langle u^2\rangle$ halkasına izomorf olduğu *3.1.1. teorem*' deki gibi gösterilerek bir halka olduğu görülür.

3.1.1. Teorem:

$a, b \in \mathbb{Z}_4, u^2 = 0$ olmak üzere,

$f: R_0 \to \mathbb{Z}_4[u]/\langle u^2 \rangle$

$a + ub \mapsto f(a + ub) = \{a + ub\}$

biçiminde tanımlanan f bir izomorfizmadır.

Kanıt:

Herhangi iki $x_1 = a_1 + ub_1$, $x_2 = a_2 + ub_2 \in R_0$ için,

$$f(x_1) = f(x_2) \Leftrightarrow \{a_1 + ub_1\} = \{a_2 + ub_2\}$$

$$\Leftrightarrow \{(a_1 - a_2) + u(b_1 - b_2)\} = 0$$

$$\Leftrightarrow a_1 - a_2 = b_1 - b_2 = 0$$

$$\Leftrightarrow a_1 = a_2 , b_1 = b_2$$

$$\Leftrightarrow x_1 = x_2$$

olduğundan f iyi tanımlı ve birebir bir dönüşümdür.

f dönüşümü birebir ve $|R_0 = \mathbb{Z}_4 + u\mathbb{Z}_4| = |\mathbb{Z}_4[u] / \langle u^2 \rangle| = 2^4 = 16$ olduğundan, f dönüşümü örtendir.

Herhangi iki $x_1 = a_1 + ub_1$, $x_2 = a_2 + ub_2 \in R_0$ için,

i) $f(x_1 + x_2) = f((a_1 + ub_1) + (a_2 + ub_2))$

$$= f((a_1 + a_2) + u(b_1 + b_2))$$

$$= \{(a_1 + a_2) + u(b_1 + b_2)\}$$

$$= \{a_1 + ub_1\} + \{a_2 + ub_2\}$$

$$= f(a_1 + ub_1) + f(a_2 + ub_2)$$

$$= f(x_1) + f(x_2)$$

ii) $f(x_1.x_2) = f((a_1 + ub_1).(a_2 + ub_2))$

$$= f(a_1.a_2 + u(a_1.b_2 + a_2.b_1))$$

$$= \{a_1.a_2 + u(a_1.b_2 + a_2.b_1)\} \quad (1)$$

$f(x_1).f(x_2) = f(a_1 + ub_1).f(a_2 + ub_2)$

$$= \{a_1 + ub_1\}.\{a_2 + ub_2\}$$

$$= \{a_1.a_2 + u(a_1.b_2 + a_2.b_1)\} \quad (2)$$

bulunur. (1) ve (2) den,

$f(x_1.x_2) = f(x_1).f(x_2)$

elde edilir. Bu durumda (i) ve (ii) sağlandığından f dönüşümü bir halka homomorfizmasıdır.

Dolayısıyla f birebir, örten ve bir homomorfizma olduğundan f bir izomorfizmadır.

3.1.2. Sonuç:

$u^2 = 0$ olmak üzere,

$R_0 = \mathbb{Z}_4 + u\mathbb{Z}_4 \cong \mathbb{Z}_4[u] / \langle u^2 \rangle$

biçiminde gösterilir.

3.1.3. Sonuç:

$u^2 = 0$ olmak üzere,

$R_0 = \{0,1,2,3,u,2u,3u,1+u,2+u,3+u,1+2u,2+2u,3+2u,1+3u,2+3u,3+3u\}$ kümesi karakteristiği 4 olan 16 elemanlı değişmeli bir halkadır.

Aşağıda R_0 halkasının elemanları için toplama ve çarpma işlem tabloları sırasıyla *Çizelge 3.1* ve *Çizelge 3.2*' de verilmiştir.

Çizelge 3.1 R_0 Halkasının Elemanlarının Toplama İşlem Tablosu

$+$	0	1	2	3	u	$2u$	$3u$	$1+u$	$2+u$	$3+u$	$1+2u$	$2+2u$	$3+2u$	$1+3u$	$2+3u$	$3+3u$
0	0	1	2	3	u	$2u$	$3u$	$1+u$	$2+u$	$3+u$	$1+2u$	$2+2u$	$3+2u$	$1+3u$	$2+3u$	$3+3u$
1	1	2	3	0	$1+u$	$1+2u$	$1+3u$	$2+u$	$3+3u$	u	$2+2u$	$3+2u$	$2u$	$2+3u$	$3+3u$	$3u$
2	2	3	0	1	$2+u$	$2+2u$	$2+3u$	$3+u$	u	$1+u$	$3+2u$	$2u$	$1+2u$	$3+3u$	$3u$	$1+3u$
3	3	0	1	2	$3+u$	$3+2u$	$3+3u$	u	$1+u$	$2+u$	$2u$	$1+2u$	$2+2u$	$3u$	$1+3u$	$2+3u$
u	u	$1+u$	$2+u$	$3+u$	$2u$	$3u$	0	$1+2u$	$2+2u$	$3+2u$	$1+3u$	$2+3u$	$3+3u$	1	2	3
$2u$	$2u$	$1+2u$	$2+2u$	$3+2u$	$3u$	0	u	$1+3u$	$2+3u$	$3+3u$	1	2	3	$1+u$	$2+u$	$3+u$
$3u$	$3u$	$1+3u$	$2+3u$	$3+3u$	0	u	$2u$	1	2	3	$1+u$	$2+u$	$3+u$	$1+2u$	$2+2u$	$3+2u$
$1+u$	$1+u$	$2+u$	$3+u$	u	$1+2u$	$1+3u$	1	$2+2u$	$3+2u$	$2u$	$2+3u$	$3+3u$	$3u$	2	3	0
$2+u$	$2+u$	$3+u$	u	$1+u$	$2+2u$	$2+3u$	2	$3+2u$	$2u$	$1+2u$	$3+3u$	$3u$	$1+3u$	3	0	1
$3+u$	$3+u$	u	$1+u$	$2+u$	$3+2u$	$3+3u$	3	$2u$	$1+2u$	$2+2u$	$3u$	$1+3u$	$2+3u$	0	1	2
$1+2u$	$1+2u$	$2+2u$	$3+2u$	$2u$	$1+3u$	1	$1+u$	$2+3u$	$3+3u$	$3u$	2	3	0	$2+u$	$3+u$	u
$2+2u$	$2+2u$	$3+2u$	$2u$	$1+2u$	$2+3u$	2	$2+u$	$3+3u$	$3u$	$1+3u$	3	0	1	$3+u$	u	$1+u$
$3+2u$	$3+2u$	$2u$	$1+2u$	$2+2u$	$3+3u$	3	$3+u$	$3u$	$1+3u$	$2+3u$	0	1	2	u	$1+u$	$2+u$
$1+3u$	$1+3u$	$2+3u$	$3+3u$	$3u$	1	$1+u$	$1+2u$	2	3	0	$2+u$	$3+u$	u	$2+2u$	$3+2u$	$2u$
$2+3u$	$2+3u$	$3+3u$	$3u$	$1+3u$	2	$2+u$	$2+2u$	3	0	1	$3+u$	u	$1+u$	$3+2u$	$2u$	$1+2u$
$3+3u$	$3+3u$	$3u$	$1+3u$	$2+3u$	3	$3+u$	$3+3u$	0	1	2	u	$1+u$	$2+u$	$2u$	$1+2u$	$2+2u$

Çizelge 3.2 R_0 Halkasının Elemanlarının Çarpım İşlem Tablosu

.	0	1	2	3	u	$2u$	$3u$	$1+u$	$2+u$	$3+u$	$1+2u$	$2+2u$	$3+2u$	$1+3u$	$2+3u$	$3+3u$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	u	$2u$	$3u$	$1+u$	$2+u$	$3+u$	$1+2u$	$2+2u$	$3+2u$	$1+3u$	$2+u$	$3+3u$
2	0	2	0	2	$2u$	0	$2u$	$2+2u$	$2u$	$2+2u$	2	0	2	$2+2u$	$2u$	$2+2u$
3	0	3	2	1	$3u$	$2u$	u	$3+3u$	$2+3u$	$1+3u$	$3+2u$	$2+2u$	$1+2u$	$3+u$	$2+u$	$1+u$
u	0	u	$2u$	$3u$	0	0	0	u	$2u$	$3u$	u	$2u$	$3u$	u	$2u$	$3u$
$2u$	0	$2u$	0	$2u$	0	0	0	$2u$	0	$2u$	$2u$	0	$2u$	$2u$	0	$2u$
$3u$	0	$3u$	$2u$	u	0	0	0	$3u$	$2u$	u	$3u$	$2u$	u	$3u$	$2u$	u
$1+u$	0	$1+u$	$2+2u$	$3+3u$	u	$2u$	$3u$	$1+2u$	$2+3u$	3	$1+3u$	2	$3+u$	1	$2+u$	$3+2u$
$2+u$	0	$2+u$	$2u$	$2+3u$	$2u$	0	$2u$	$2+3u$	0	$2+u$	$2+u$	$2u$	$2+3u$	$2+3u$	0	$2+u$
$3+u$	0	$3+u$	$2+2u$	$1+3u$	$3u$	$2u$	u	3	$2+u$	$1+2u$	$3+3u$	2	$1+u$	$3+2u$	$2+3u$	1
$1+2u$	0	$1+2u$	2	$3+2u$	u	$2u$	$3u$	$1+3u$	$2+u$	$3+3u$	1	$2+2u$	3	$1+u$	$2+3u$	$3+u$
$2+2u$	0	$2+2u$	0	$2+2u$	$2u$	0	$2u$	2	$2u$	2	$2+2u$	0	$2+2u$	2	$2u$	2
$3+2u$	0	$3+2u$	2	$1+2u$	$3u$	$2u$	u	$3+u$	$2+3u$	$1+u$	3	$2+2u$	1	$3+3u$	$2+u$	$1+3u$
$1+3u$	0	$1+3u$	$2+2u$	$3+u$	u	$2u$	$3u$	1	$2+3u$	$3+2u$	$1+u$	2	$3+3u$	$1+2u$	$2+u$	3
$2+3u$	0	$2+3u$	$2u$	$2+u$	$2u$	0	$2u$	$2+u$	0	$2+3u$	$2+3u$	$2u$	$2+u$	$2+u$	0	$2+3u$
$3+3u$	0	$3+3u$	$2+2u$	$1+u$	$3u$	$2u$	u	$3+2u$	$2+u$	1	$3+u$	2	$1+3u$	3	$2+3u$	$1+2u$

3.1.4. Sonuç:

i) R_0 halkasının idealleri ;

$\langle 0\rangle = \{0\}$,

$\langle 1\rangle = \langle 3\rangle = \langle 1+u\rangle = \langle 3+u\rangle = \langle 1+2u\rangle = \langle 3+2u\rangle = \langle 1+3u\rangle = \langle 3+3u\rangle = R_0$,

$\langle 2\rangle = \langle 2+2u\rangle = \{0, 2, 2u, 2+2u\}$,

$\langle u\rangle = \langle 3u\rangle = \{0, u, 2u, 3u\}$,

$\langle 2u\rangle = \{0, 2u\}$,

$\langle 2+u\rangle = \langle 2+3u\rangle = \{0, 2u, 2+u, 2+3u\}$,

$\langle 2, u\rangle = \langle 2,2+u\rangle = \langle u, 2+u\rangle = \{0, 2, u, 2u, 3u, 2+u, 2+2u, 2+3u\}$

biçimindedir.

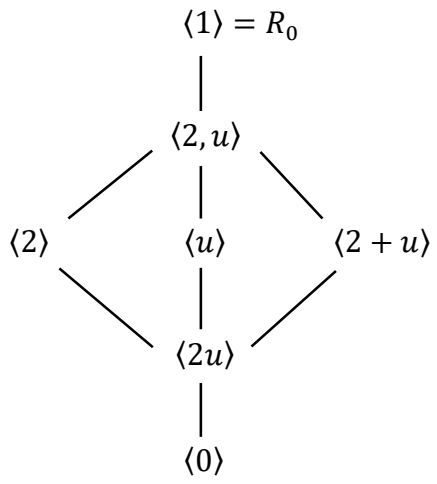
ii) R_0 halkasının birimsel elemanlar kümesi ;

$U(R_0)$=$\{1, 3, 1+u, 3+u, 1+2u, 3+2u, 1+3u, 3+3u\}$ dir.

iii) R_0 halkasının tek maksimal ideali $\langle 2, u\rangle$ olduğundan R_0 halkası lokal bir halkadır.

iv) R_0 halkasının tüm idealleri esas ideal olmadığından, esas ideal halkası değildir.

v) R_0 halkası sonlu bir zincir halkası değildir. R_0 halkasının ideallerinin oluşturduğu kafes *Şekil 3.1*'de verilmiştir.



Şekil 3.1 R_0 Halkasının İdeallerinin Oluşturduğu Kafes

3.2. $\mathbb{Z}_4[u]/\langle u^2-1\rangle$ Halkası

$\mathbb{Z}_4[u]/\langle u^2-1\rangle$ halkasında $u=1$ koşulu göz önüne alındığında *Bölüm 3.1.'*dekine benzer şekilde $R_1=\mathbb{Z}_4+u\mathbb{Z}_4$ kümesinin de toplama ve çarpma işlemlerine göre karakteristiği 4 olan 16 elemanlı değişmeli bir halka olduğu görülür. Ayrıca $u^2=1$ olmak üzere $\mathbb{Z}_4+u\mathbb{Z}_4$ ile $\mathbb{Z}_4[u]/\langle u^2-1\rangle$ halkası arasında bir f izomorfizması tanımlanır. R_1 halkasının elemanlarının toplama ve çarpma işlemlerine göre tablosu *Bölüm3.1.'*dekine benzer şekilde oluşturulur.

3.2.1. Sonuç:

i) R_1halkasının idealleri ;

$\langle 0\rangle=\{0\}$,

$\langle 1\rangle=\langle 3\rangle=\langle u\rangle=\langle 3u\rangle=\langle 2+u\rangle=\langle 1+2u\rangle=\langle 3+2u\rangle=\langle 2+3u\rangle=R_1$,

$\langle 2\rangle=\langle 2u\rangle=\{0,2,2u,2+2u\}$,

$\langle 1+u\rangle=\langle 3+3u\rangle=\{0,1+u,2+2u,3+3u\}$,

$\langle 3+u\rangle=\langle 1+3u\rangle=\{0,3+u,2+2u,1+3u\}$,

$\langle 2+2u\rangle=\{0,2+2u\}$,

$\langle 2{,}1+u\rangle=\langle 2{,}3+u\rangle=\langle 1+u,3+u\rangle$

$=\{0,2,2u,1+u,3+u,2+2u,1+3u,3+3u\}$

biçimindedir.

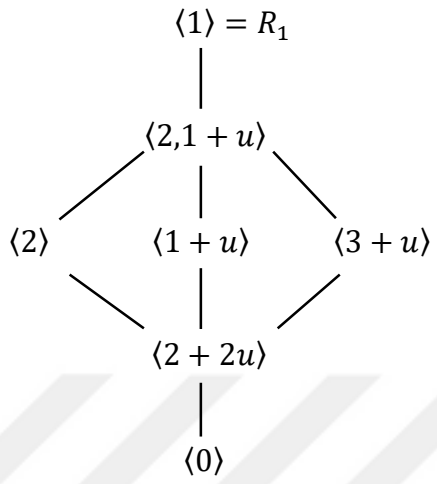
ii) R_1 halkasının birimsel elemanlar kümesi ;

$U(R_1)=\{1,3,u,3u,2+u,1+2u,3+2u,2+3u\}$ dir.

iii) R_1 halkasının tek maksimal ideali $\langle 2{,}1+u\rangle$ olduğundan R_1 halkası lokal bir halkadır.

iv) R_1 halkası esas ideal halkası değildir.

v) R_1 halkası sonlu bir zincir halkası değildir. R_1 halkasının ideallerinin oluşturduğu kafes *Şekil 3.2*'de verilmiştir.



Şekil 3.2 R_1 Halkasının İdeallerinin Oluşturduğu Kafes

3.3. $\mathbb{Z}_4[u]/\langle u^2-2\rangle$ Halkası

$\mathbb{Z}_4[u]/\langle u^2-2\rangle$ halkasında $u^2=2$ koşulu göz önüne alındığında *Bölüm 3.1.*'dekine benzer şekilde $R_2=\mathbb{Z}_4+u\mathbb{Z}_4$ kümesinin de, toplama ve çarpma işlemlerine göre karakteristiği 4 olan 16 elemanlı değişmeli bir halka olduğu görülür. Ayrıca $u^2=2$ olmak üzere $\mathbb{Z}_4+u\mathbb{Z}_4$ ile $\mathbb{Z}_4[u]/\langle u^2-2\rangle$ halkası arasında bir f izomorfizması tanımlanır. R_2 halkasının elemanlarının toplama ve çarpma tablosu *Bölüm3.1.*'dekine benzer şekilde oluşturulur.

3.3.1. Sonuç:

i) R_2 halkasının idealleri ;

$\langle 0\rangle=\{0\}$,

$\langle 1\rangle=\langle 3\rangle=\langle 1+u\rangle=\langle 3+u\rangle=\langle 1+2u\rangle=\langle 3+2u\rangle=\langle 1+3u\rangle=\langle 3+3u\rangle=R_2$,

$\langle 2\rangle=\langle 2+2u\rangle=\{0,2,2u,2+2u\}$,

$\langle u\rangle=\langle 3u\rangle=\langle 2+u\rangle=\langle 2+3u\rangle=\{0,2,u,2u,3u,2+u,2+2u,2+3u\}$,

$\langle 2u \rangle = \{0, 2u\}$

biçimindedir.

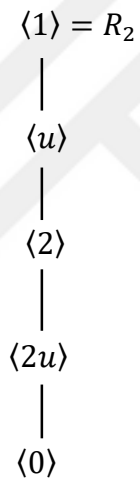
ii) R_2 halkasının birimsel elemanlar kümesi ;

$U(R_2) = \{1, 3, 1+u, 3+u, 1+2u, 3+2u, 1+3u, 3+3u\}$ dir.

iii) R_2 halkasının tek maksimal ideali $\langle u \rangle$ olduğundan R_2 halkası lokal bir halkadır.

iv) R_2 halkası bir esas ideal halkasıdır.

v) R_2 halkası sonlu bir zincir halkasıdır. R_2 halkasının ideallerinin oluşturduğu kafes *Şekil 3.3*'de verilmiştir.



Şekil 3.3 R_2 Halkasının İdeallerinin Oluşturduğu Kafes

3.4. $\mathbb{Z}_4[u]/\langle u^2 - 3 \rangle$ Halkası

$\mathbb{Z}_4[u]/\langle u^2 - 3 \rangle$ halkasında $u^2 = 3$ koşulu göz önüne alındığında *Bölüm 3.1.*'dekine benzer şekilde $R_3 = \mathbb{Z}_4 + u\mathbb{Z}_4$ kümesinin de, toplama ve çarpma işlemlerine göre karakteristiği 4 olan 16 elemanlı değişmeli bir halka olduğu görülür. Ayrıca $u^2 = 3$ olmak üzere $\mathbb{Z}_4 + u\mathbb{Z}_4$ ile $\mathbb{Z}_4[u]/\langle u^2 - 3 \rangle$ halkası arasında bir f izomorfizması tanımlanır. R_3 halkasının elemanlarının toplama ve çarpma tablosu *Bölüm3.1.*'dekine benzer şekilde oluşturulur.

3.4.1. Sonuç:

i) R_3 halkasının idealleri ;

$\langle 0\rangle = \{0\}$,

$\langle 1\rangle = \langle 3\rangle = \langle u\rangle = \langle 3u\rangle = \langle 2+u\rangle = \langle 1+2u\rangle = \langle 3+2u\rangle = \langle 2+3u\rangle = R_3$,

$\langle 2\rangle = \langle 2u\rangle = \{0, 2, 2u, 2+2u\}$,

$\langle 1+u\rangle = \langle 3+u\rangle = \langle 1+3u\rangle = \langle 3+3u\rangle$

$= \{0, 2, 2u, 1+u, 3+u, 2+2u, 1+3u, 3+3u\}$,

$\langle 2+2u\rangle = \{0, 2+2u\}$

biçimindedir.

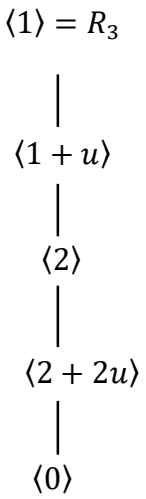
ii) R_3 halkasının birimsel elemanlar kümesi ;

$U(R_3) = \{1, 3, u, 3u, 2+u, 1+2u, 3+2u, 2+3u\}$ dir.

iii) R_3 halkasının tek maksimal ideali $\langle 1+u\rangle$ olduğundan R_3 halkası lokal bir halkadır.

iv) R_3 halkası bir esas ideal halkasıdır.

v) R_3 halkası sonlu bir zincir halkasıdır. R_3 halkasının ideallerinin oluşturduğu kafes *Şekil 3.4*'de verilmiştir.



Şekil 3.4 R_3 Halkasının İdeallerinin Oluşturduğu Kafes

3.5. $\mathbb{Z}_4[u]/\langle u^2 - u\rangle$ Halkası

$\mathbb{Z}_4[u]/\langle u^2 - u\rangle$ halkasında $u^2 = u$ koşulu göz önüne alındığında *Bölüm 3.1.'*dekine benzer şekilde $R_u = \mathbb{Z}_4 + u\mathbb{Z}_4$ kümesinin de, toplama ve çarpma işlemlerine göre karakteristiği 4 olan 16 elemanlı değişmeli bir halka olduğu görülür. Ayrıca $u^2 = u$ olmak üzere $\mathbb{Z}_4 + u\mathbb{Z}_4$ ile $\mathbb{Z}_4[u]/\langle u^2 - u\rangle$ halkası arasında bir f izomorfizması tanımlanır. R_u halkasının elemanlarının toplama ve çarpma tablosu *Bölüm3.1.'*dekine benzer şekilde oluşturulur.

3.5.1. Sonuç:

i) R_u halkasının idealleri ;

$\langle 0\rangle = \{0\}$,

$\langle 1\rangle = \langle 3\rangle = \langle 1 + 2u\rangle = \langle 3 + 2u\rangle = R_u$,

$\langle 2\rangle = \{0, 2, 2u, 2 + 2u\}$,

$\langle u\rangle = \langle 3u\rangle = \{0, u, 2u, 3u\}$,

$\langle 2u\rangle = \{0, 2u\}$,

$\langle 1+u\rangle = \langle 3+3u\rangle = \{0, 2, 2u, 1+u, 3+u, 2+2u, 1+3u, 3+3u\}$,

$\langle 2+u\rangle = \langle 2+3u\rangle = \{0, 2, u, 2u, 3u, 2+u, 2+2u, 1+3u, 2+3u\}$,

$\langle 3+u\rangle = \langle 1+3u\rangle = \{0, 3+u, 2+2u, 1+3u\}$,

$\langle 2+2u\rangle = \{0, 2+2u\}$

biçimindedir.

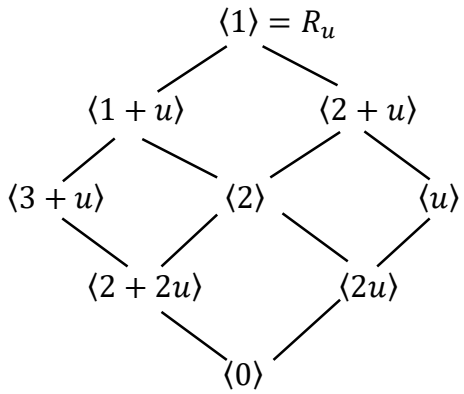
ii) Herhangi $r = a + ub \in R_u$ elemanının birimsel olması için gerekli ve yeterli koşul $a \not\equiv 0(mod2)$ ve $a + b \not\equiv 0(mod2)$ olmasıdır. Dolayısıyla R_u halkasının birimsel elemanlar kümesi ;

$U(R_u) = \{1, 3, 1+2u, 3+2u\}$ dir.

iii) R_u halkasının maksimal idealleri $\langle 1+u\rangle$ ve $\langle 2+u\rangle$ olduğundan R_u halkası semi-lokal bir halkadır.

iv) R_u halkası bir esas ideal halkasıdır.

v) R_u halkası sonlu bir zincir halkası değildir. R_u halkasının ideallerinin oluşturduğu kafes *Şekil 3.5*'de verilmiştir.



Şekil 3.5 R_u Halkasının İdeallerinin Oluşturduğu Kafes

3.6. $\mathbb{Z}_4[u]/\langle u^2-2u\rangle$ Halkası

$\mathbb{Z}_4[u]/\langle u^2-2u\rangle$ halkasında $u^2=2u$ koşulu göz önüne alındığında *Bölüm 3.1.'*dekine benzer şekilde $R_{2u}=\mathbb{Z}_4+u\mathbb{Z}_4$ kümesinin de, toplama ve çarpma işlemlerine göre karakteristiği 4 olan 16 elemanlı değişmeli bir halka olduğu görülür. Ayrıca $u^2=2u$ olmak üzere $\mathbb{Z}_4+u\mathbb{Z}_4$ ile $\mathbb{Z}_4[u]/\langle u^2-2u\rangle$ halkası arasında bir f izomorfizması tanımlanır. R_{2u} halkasının elemanlarının toplama ve çarpma tablosu *Bölüm3.1.'*dekine benzer şekilde oluşturulur.

3.6.1. Sonuç:

i) R_{2u} halkasının idealleri ;

$\langle 0\rangle=\{0\}$,

$\langle 1\rangle=\langle 3\rangle=\langle 1+u\rangle=\langle 3+u\rangle=\langle 1+2u\rangle=\langle 3+2u\rangle=\langle 1+3u\rangle=\langle 3+3u\rangle=R_{2u}$,

$\langle 2\rangle=\langle 2+2u\rangle=\{0,2,2u,2+2u\}$,

$\langle u\rangle=\langle 3u\rangle=\{0,u,2u,3u\}$,

$\langle 2u\rangle=\{0,2u\}$,

$\langle 2+u\rangle=\langle 2+3u\rangle=\{0,2u,2+u,2+3u\}$,

$\langle 2,u\rangle=\langle 2,2+u\rangle=\langle u,2+u\rangle=\{0,2,u,2u,3u,2+u,2+2u,2+3u\}$

biçimindedir.

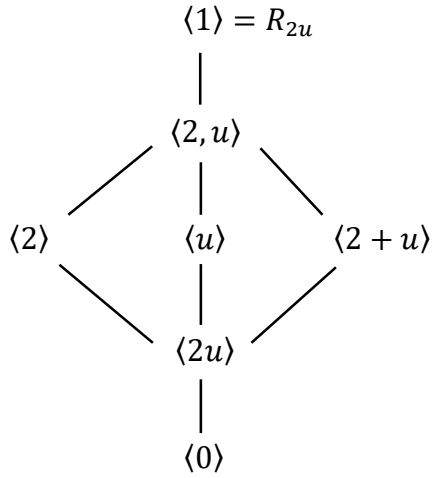
ii) R_{2u} halkasının birimsel elemanlar kümesi ;

$U(R_{2u})=\{1,3,1+u,3+u,1+2u,3+2u,1+3u,3+3u\}$ dir.

iii) R_{2u} halkasının tek maksimal ideali $\langle 2,u\rangle$ olduğundan R_{2u} halkası lokal bir halkadır.

iv) R_{2u} halkasının tüm idealleri esas ideal olmadığından, esas ideal halkası değildir.

v) R_{2u} halkası sonlu bir zincir halkası değildir. R_{2u} halkasının ideallerinin oluşturduğu kafes *Şekil 3.6*'da verilmiştir.



Şekil 3.6 R_{2u} Halkasının İdeallerinin Oluşturduğu Kafes

3.7. $\mathbb{Z}_4[u]/\langle u^2 - 3u\rangle$ Halkası

$\mathbb{Z}_4[u]/\langle u^2 - 3u\rangle$ halkasında $u^2 = 3u$ koşulu göz önüne alındığında *Bölüm 3.1.*'dekine benzer şekilde $R_{3u} = \mathbb{Z}_4 + u\mathbb{Z}_4$ kümesinin de, toplama ve çarpma işlemlerine göre karakteristiği 4 olan 16 elemanlı değişmeli bir halka olduğu görülür. Ayrıca $u^2 = 3u$ olmak üzere $\mathbb{Z}_4 + u\mathbb{Z}_4$ ile $\mathbb{Z}_4[u]/\langle u^2 - 3u\rangle$ halkası arasında bir f izomorfizması tanımlanır. R_{3u} halkasının elemanlarının toplama ve çarpma tablosu *Bölüm3.1.*'dekine benzer şekilde oluşturulur.

3.7.1. Sonuç:

i) R_{3u} halkasının idealleri ;

$\langle 0\rangle = \{0\}$,

$\langle 1\rangle = \langle 3\rangle = \langle 1 + 2u\rangle = \langle 3 + 2u\rangle = R_{3u}$,

$\langle 2\rangle = \{0, 2, 2u, 2 + 2u\}$,

$\langle u\rangle = \langle 3u\rangle = \{0, u, 2u, 3u\}$,

$\langle 2u\rangle = \{0, 2u\}$,

$\langle 1+u\rangle = \langle 3+3u\rangle = \{0, 1+u, 2+2u, 3+3u\}$,

$\langle 2+u\rangle = \langle 2+3u\rangle = \{0, 2, u, 2u, 3u, 2+u, 2+2u, 2+3u\}$,

$\langle 3+u\rangle = \langle 1+3u\rangle = \{0, 2, 2u, 1+u, 3+u, 2+2u, 1+3u, 3+3u\}$,

$\langle 2+2u\rangle = \{0, 2+2u\}$

biçimindedir.

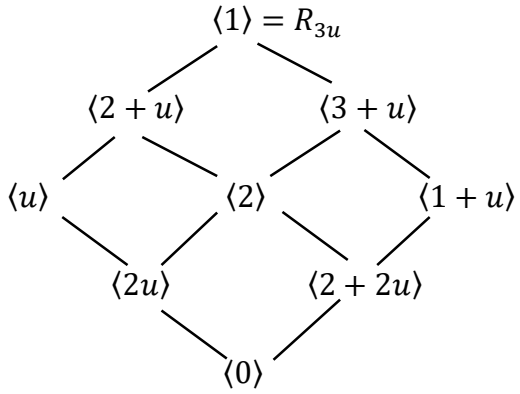
ii) R_{3u} halkasının birimsel elemanlar kümesi ;

$U(R_{3u}) = \{1, 3, 1+2u, 3+2u\}$ dir.

iii) R_{3u} halkasının maksimal idealleri $\langle 2+u\rangle$ ve $\langle 3+u\rangle$ olduğundan R_{3u} halkası semi-lokal bir halkadır.

iv) R_{3u} halkası bir esas ideal halkasıdır.

v) R_{3u} halkası sonlu bir zincir halkası değildir. R_{3u} halkasının ideallerinin oluşturduğu kafes *Şekil 3.7*'de verilmiştir.



Şekil 3.7 R_{3u} Halkasının İdeallerinin Oluşturduğu Kafes

3.8. $\mathbb{Z}_4[u]/\langle u^2-u-1\rangle$ Halkası

$\mathbb{Z}_4[u]/\langle u^2-u-1\rangle$ halkasında $u^2=1+u$ koşulu göz önüne alındığında *Bölüm 3.1.'*dekine benzer şekilde $R_{1+u}=\mathbb{Z}_4+u\mathbb{Z}_4$ kümesinin de, toplama ve çarpma işlemlerine göre karakteristiği 4 olan 16 elemanlı değişmeli bir halka olduğu görülür. Ayrıca $u^2=1+u$ olmak üzere $\mathbb{Z}_4+u\mathbb{Z}_4$ ile $\mathbb{Z}_4[u]/\langle u^2-u-1\rangle$ halkası arasında bir f izomorfizması tanımlanır. R_{1+u} halkasının elemanlarının toplama ve çarpma tablosu *Bölüm3.1.'*dekine benzer şekilde oluşturulur.

3.8.1. Sonuç:

i) R_{1+u} halkasının idealleri ;

$\langle 0\rangle=\{0\}$,

$\langle 1\rangle=\langle 3\rangle=\langle u\rangle=\langle 3u\rangle=\langle 1+u\rangle=\langle 2+u\rangle=\langle 3+u\rangle=\langle 1+2u\rangle=\langle 3+2u\rangle$

$=\langle 1+3u\rangle=\langle 2+3u\rangle=\langle 3+3u\rangle=R_{1+u}$

$\langle 2\rangle=\langle 2u\rangle=\langle 2+2u\rangle=\{0,2,2u,2+2u\}$

biçimindedir.

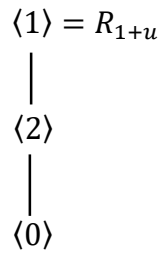
ii) R_{1+u} halkasının birimsel elemanlar kümesi ;

$U(R_{1+u})=\{1,3,u,3u,1+u,2+u,3+u,1+2u,3+2u,1+3u,2+3u,3+3u\}$ dir.

iii) R_{1+u} halkasının tek maksimal ideali $\langle 2\rangle$ olduğundan R_{1+u} halkası lokal bir halkadır.

iv) R_{1+u} halkası bir esas ideal halkasıdır.

v) R_{1+u} halkası sonlu bir zincir halkasıdır. R_{1+u} halkasının ideallerinin oluşturduğu kafes *Şekil 3.8*'de verilmiştir.



Şekil 3.8 R_{1+u} Halkasının İdeallerinin Oluşturduğu Kafes

3.9. $\mathbb{Z}_4[u]/\langle u^2 - u - 2\rangle$ Halkası

$\mathbb{Z}_4[u]/\langle u^2 - u - 2\rangle$ halkasında $u^2 = 2 + u$ koşulu göz önüne alındığında *Bölüm 3.1.'*dekine benzer şekilde $R_{2+u} = \mathbb{Z}_4 + u\mathbb{Z}_4$ kümesinin de, toplama ve çarpma işlemlerine göre karakteristiği 4 olan 16 elemanlı değişmeli bir halka olduğu görülür. Ayrıca $u^2 = 2 + u$ olmak üzere $\mathbb{Z}_4 + u\mathbb{Z}_4$ ile $\mathbb{Z}_4[u]/\langle u^2 - u - 2\rangle$ halkası arasında bir f izomorfizması tanımlanır. R_{2+u} halkasının elemanlarının toplama ve çarpma tablosu *Bölüm3.1.'*dekine benzer şekilde oluşturulur.

3.9.1. Sonuç:

i) R_{2+u} halkasının idealleri ;

$\langle 0\rangle = \{0\}$,

$\langle 1\rangle = \langle 3\rangle = \langle 1 + 2u\rangle = \langle 3 + 2u\rangle = R_{2+u}$,

$\langle 2\rangle = \{0, 2, 2u, 2 + 2u\}$,

$\langle u\rangle = \langle 3u\rangle = \{0, 2, u, 2u, 3u, 2 + u, 2 + 2u, 2 + 3u\}$,

$\langle 2u\rangle = \{0, 2u\}$,

$\langle 1 + u\rangle = \langle 3 + 3u\rangle = \{0, 1 + u, 2 + 2u, 3 + 3u\}$,

$\langle 2 + u\rangle = \langle 2 + 3u\rangle = \{0, 2u, 2 + u, 2 + 3u\}$,

$\langle 3 + u\rangle = \langle 1 + 3u\rangle = \{0, 2, 2u, 1 + u, 3 + u, 2 + 2u, 1 + 3u, 3 + 3u\}$,

$\langle 2+2u\rangle = \{0, 2+2u\}$

biçimindedir.

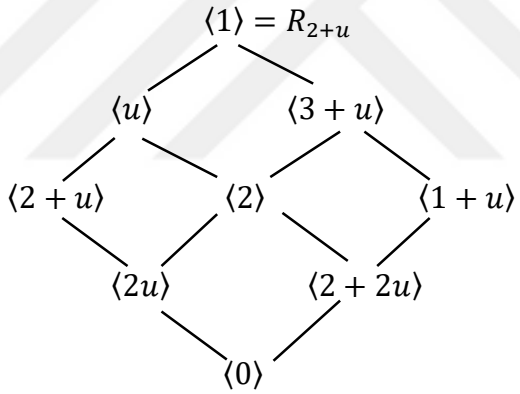
ii) R_{2+u} halkasının birimsel elemanlar kümesi ;

$U(R_{2+u}) = \{1, 3, 1+2u, 3+2u\}$ dir.

iii) R_{2+u} halkasının maksimal idealleri $\langle u\rangle$ ve $\langle 3+u\rangle$ olduğundan R_{2+u} halkası semi-lokal bir halkadır.

iv) R_{2+u} halkası bir esas ideal halkasıdır.

v) R_{2+u} halkası sonlu bir zincir halkası değildir. R_{2+u} halkasının ideallerinin oluşturduğu kafes *Şekil 3.9*'da verilmiştir.



Şekil 3.9 R_{2+u} Halkasının İdeallerinin Oluşturduğu Kafes

3.10. $\mathbb{Z}_4[u]/\langle u^2-u-3\rangle$ Halkası

$\mathbb{Z}_4[u]/\langle u^2-u-3\rangle$ halkasında $u^2 = 3+u$ koşulu göz önüne alındığında *Bölüm 3.1.*'dekine benzer şekilde $R_{3+u} = \mathbb{Z}_4 + u\mathbb{Z}_4$ kümesinin de, toplama ve çarpma işlemlerine göre karakteristiği 4 olan 16 elemanlı değişmeli bir halka olduğu görülür. Ayrıca $u^2 = 3+u$ olmak üzere $\mathbb{Z}_4 + u\mathbb{Z}_4$ ile $\mathbb{Z}_4[u]/\langle u^2-u-3\rangle$ halkası arasında bir f izomorfizması

tanımlanır. R_{3+u} halkasının elemanlarının toplama ve çarpma tablosu *Bölüm3.1.*'dekine benzer şekilde oluşturulur.

3.10.1. Sonuç:

i) R_{3+u} halkasının idealleri ;

$\langle 0\rangle = \{0\}$ **,**

$\langle 1\rangle = \langle 3\rangle = \langle u\rangle = \langle 3u\rangle = \langle 1+u\rangle = \langle 2+u\rangle = \langle 3+u\rangle = \langle 1+2u\rangle = \langle 3+2u\rangle$

$= \langle 1+3u\rangle = \langle 2+3u\rangle = \langle 3+3u\rangle = R_{3+u}$

$\langle 2\rangle = \langle 2u\rangle = \langle 2+2u\rangle = \{0, 2, 2u, 2+2u\}$

biçimindedir.

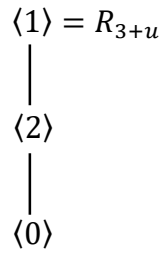
ii) R_{3+u} halkasının birimsel elemanlar kümesi ;

$U(R_{3+u}) = \{1, 3, u, 3u, 1+u, 2+u, 3+u, 1+2u, 3+2u, 1+3u, 2+3u, 3+3u\}$ dir.

iii) R_{3+u} halkasının tek maksimal ideali $\langle 2\rangle$ olduğundan R_{3+u} halkası lokal bir halkadır.

iv) R_{3+u} halkası bir esas ideal halkasıdır.

v) R_{3+u} halkası sonlu bir zincir halkasıdır. R_{3+u} halkasının ideallerinin oluşturduğu kafes *Şekil 3.10*'da verilmiştir.



Şekil 3.10 R_{3+u} Halkasının İdeallerinin Oluşturduğu Kafes

3.11. $\mathbb{Z}_4[u]/\langle u^2-2u-1\rangle$ Halkası

$\mathbb{Z}_4[u]/\langle u^2-2u-1\rangle$ halkasında $u^2=1+2u$ koşulu göz önüne alındığında *Bölüm 3.1.*'dekine benzer şekilde $R_{1+2u}=\mathbb{Z}_4+u\mathbb{Z}_4$ kümesinin de, toplama ve çarpma işlemlerine göre karakteristiği 4 olan 16 elemanlı değişmeli bir halka olduğu görülür. Ayrıca $u^2=1+2u$ olmak üzere $\mathbb{Z}_4+u\mathbb{Z}_4$ ile $\mathbb{Z}_4[u]/\langle u^2-2u-1\rangle$ halkası arasında bir f izomorfizması tanımlanır. R_{1+2u} halkasının elemanlarının toplama ve çarpma tablosu *Bölüm3.1.*'dekine benzer şekilde oluşturulur.

3.11.1. Sonuç:

i) R_{1+2u} halkasının idealleri ;

$\langle 0\rangle=\{0\}$,

$\langle 1\rangle=\langle 3\rangle=\langle u\rangle=\langle 3u\rangle=\langle 2+u\rangle=\langle 1+2u\rangle=\langle 3+2u\rangle=\langle 2+3u\rangle=R_{1+2u}$,

$\langle 2\rangle=\langle 2u\rangle=\{0,2,2u,2+2u\}$,

$\langle 1+u\rangle=\langle 3+u\rangle=\langle 1+3u\rangle=\langle 3+3u\rangle$

$=\{0,2,2u,1+u,3+u,2+2u,1+3u,3+3u\}$,

$\langle 2+2u\rangle=\{0,2+2u\}$

biçimindedir.

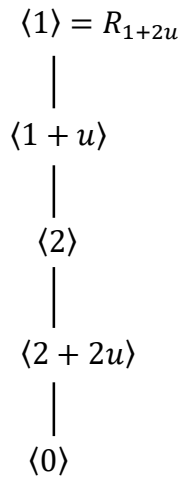
ii) R_{1+2u} halkasının birimsel elemanlar kümesi ;

$U(R_{1+2u})=\{1,3,u,3u,2+u,1+2u,3+2u,2+3u\}$ dir.

iii) R_{1+2u} halkasının tek maksimal ideali $\langle 1+u\rangle$ olduğundan R_{1+2u} halkası lokal bir halkadır.

iv) R_{1+2u} halkası bir esas ideal halkasıdır.

v) R_{1+2u} halkası sonlu bir zincir halkasıdır. R_{1+2u} halkasının ideallerinin oluşturduğu kafes *Şekil 3.11*'de verilmiştir



Şekil 3.11 R_{1+2u} Halkasının İdeallerinin Oluşturduğu Kafes

3.12. $\mathbb{Z}_4[u]/\langle u^2 - 2u - 2\rangle$ Halkası

$\mathbb{Z}_4[u]/\langle u^2 - 2u - 2\rangle$ halkasında $u^2 = 2 + 2u$ koşulu göz önüne alındığında *Bölüm 3.1.*'dekine benzer şekilde $R_{2+2u} = \mathbb{Z}_4 + u\mathbb{Z}_4$ kümesinin de, toplama ve çarpma işlemlerine göre karakteristiği 4 olan 16 elemanlı değişmeli bir halka olduğu görülür. Ayrıca $u^2 = 2 + 2u$ olmak üzere $\mathbb{Z}_4 + u\mathbb{Z}_4$ ile $\mathbb{Z}_4[u]/\langle u^2 - 2u - 2\rangle$ halkası arasında bir f izomorfizması tanımlanır. R_{2+2u} halkasının elemanlarının toplama ve çarpma tablosu *Bölüm3.1.*'dekine benzer şekilde oluşturulur.

3.12.1. Sonuç:

i) R_{2+2u} halkasının idealleri ;

$\langle 0\rangle = \{0\}$,

$\langle 1\rangle = \langle 3\rangle = \langle 1 + u\rangle = \langle 3 + u\rangle = \langle 1 + 2u\rangle = \langle 3 + 2u\rangle = \langle 1 + 3u\rangle = \langle 3 + 3u\rangle$

$= R_{2+2u}$,

$\langle 2\rangle = \langle 2 + 2u\rangle = \{0, 2, 2u, 2 + 2u\}$,

$\langle u\rangle = \langle 3u\rangle = \langle 2 + u\rangle = \langle 2 + 3u\rangle = \{0, 2, u, 2u, 3u, 2 + u, 2 + 2u, 2 + 3u\}$,

$\langle 2u\rangle = \{0, 2u\}$

biçimindedir.

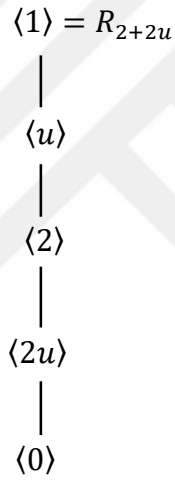
ii) R_{2+2u} halkasının birimsel elemanlar kümesi ;

$U(R_{2+2u}) = \{1, 3, 1+u, 3+u, 1+2u, 3+2u, 1+3u, 3+3u\}$ dir.

iii) R_{2+2u} halkasının tek maksimal ideali $\langle u \rangle$ olduğundan R_{2+2u} halkası lokal bir halkadır.

iv) R_{2+2u} halkası bir esas ideal halkasıdır.

v) R_{2+2u} halkası sonlu bir zincir halkasıdır. R_{2+2u} halkasının ideallerinin oluşturduğu kafes *Şekil 3.12*'de verilmiştir.



Şekil 3.12 R_{2+2u} Halkasının İdeallerinin Oluşturduğu Kafes

3.13. $\mathbb{Z}_4[u]/\langle u^2 - 2u - 3 \rangle$ Halkası

$\mathbb{Z}_4[u]/\langle u^2 - 2u - 3 \rangle$ halkasında $u^2 = 3 + 2u$ koşulu göz önüne alındığında *Bölüm 3.1.*'dekine benzer şekilde $R_{3+2u} = \mathbb{Z}_4 + u\mathbb{Z}_4$ kümesinin de, toplama ve çarpma işlemlerine göre karakteristiği 4 olan 16 elemanlı değişmeli bir halka olduğu görülür. Ayrıca $u^2 = 3 + 2u$ olmak üzere $\mathbb{Z}_4 + u\mathbb{Z}_4$ ile $\mathbb{Z}_4[u]/\langle u^2 - 2u - 3 \rangle$ halkası arasında bir f izomorfizması tanımlanır. R_{3+2u} halkasının elemanlarının toplama ve çarpma tablosu *Bölüm3.1.*'dekine benzer şekilde oluşturulur.

3.13.1. Sonuç:

i) R_{3+2u} halkasının idealleri ;

$\langle 0\rangle = \{0\}$,

$\langle 1\rangle = \langle 3\rangle = \langle u\rangle = \langle 3u\rangle = \langle 2+u\rangle = \langle 1+2u\rangle = \langle 3+2u\rangle = \langle 2+3u\rangle = R_{3+2u}$,

$\langle 2\rangle = \langle 2u\rangle = \{0, 2, 2u, 2+2u\}$,

$\langle 1+u\rangle = \langle 3+3u\rangle = \{0, 1+u, 2+2u, 3+3u\}$,

$\langle 3+u\rangle = \langle 1+3u\rangle = \{0, 3+u, 2+2u, 1+3u\}$,

$\langle 2+2u\rangle = \{0, 2+2u\}$,

$\langle 2{,}1+u\rangle = \langle 2{,}3+u\rangle = \langle 1+u, 3+u\rangle$

$= \{0, 2, 2u, 1+u, 3+u, 2+2u, 1+3u, 3+3u\}$

biçimindedir.

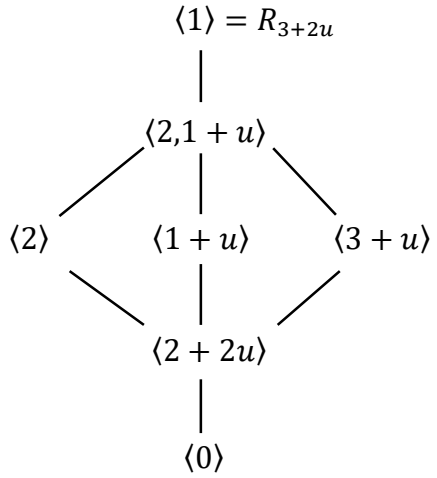
ii) R_{3+2u} halkasının birimsel elemanlar kümesi ;

$U(R_{3+2u}) = \{1, 3, u, 3u, 2+u, 1+2u, 3+2u, 2+3u\}$ dir.

iii) R_{3+2u} halkasının tek maksimal ideali $\langle 2{,}1+u\rangle$ olduğundan R_{3+2u} halkası lokal bir halkadır.

iv) R_{3+2u} halkası esas ideal halkası değildir.

v) R_{3+2u} halkası sonlu bir zincir halkası değildir. R_{3+2u} halkasının ideallerinin oluşturduğu kafes *Şekil 3.13*'de verilmiştir.



Şekil 3.13 R_{3+2u} Halkasının İdeallerinin Oluşturduğu Kafes

3.14. $\mathbb{Z}_4[u]/\langle u^2 - 3u - 1\rangle$ Halkası

$\mathbb{Z}_4[u]/\langle u^2 - 3u - 1\rangle$ halkasında $u^2 = 1 + 3u$ koşulu göz önüne alındığında *Bölüm 3.1.'*dekine benzer şekilde $R_{1+3u} = \mathbb{Z}_4 + u\mathbb{Z}_4$ kümesinin de, toplama ve çarpma işlemlerine göre karakteristiği 4 olan 16 elemanlı değişmeli bir halka olduğu görülür. Ayrıca $u^2 = 1 + 3u$ olmak üzere $\mathbb{Z}_4 + u\mathbb{Z}_4$ ile $\mathbb{Z}_4[u]/\langle u^2 - 3u - 1\rangle$ halkası arasında bir f izomorfizması tanımlanır. R_{1+3u} halkasının elemanlarının toplama ve çarpma tablosu *Bölüm3.1.'*dekine benzer şekilde oluşturulur.

3.14.1. Sonuç:

i) R_{1+3u} halkasının idealleri ;

$\langle 0\rangle = \{0\}$ **,**

$\langle 1\rangle = \langle 3\rangle = \langle u\rangle = \langle 3u\rangle = \langle 1 + u\rangle = \langle 2 + u\rangle = \langle 3 + u\rangle = \langle 1 + 2u\rangle = \langle 3 + 2u\rangle$

$= \langle 1 + 3u\rangle = \langle 2 + 3u\rangle = \langle 3 + 3u\rangle = R_{1+3u}$

$\langle 2\rangle = \langle 2u\rangle = \langle 2 + 2u\rangle = \{0, 2, 2u, 2 + 2u\}$

biçimindedir.

ii) R_{1+3u} halkasının birimsel elemanlar kümesi ;

$U(R_{1+3u}) = \{1, 3, u, 3u, 1+u, 2+u, 3+u, 1+2u, 3+2u, 1+3u, 2+3u, 3+3u\}$ dir.

iii) R_{1+3u} halkasının tek maksimal ideali $\langle 2 \rangle$ olduğundan R_{1+3u} halkası lokal bir halkadır.

iv) R_{1+3u} halkası bir esas ideal halkasıdır.

v) R_{1+3u} halkası sonlu bir zincir halkasıdır. R_{1+3u} halkasının ideallerinin oluşturduğu kafes *Şekil 3.14*'de verilmiştir.



Şekil 3.14 R_{1+3u} Halkasının İdeallerinin Oluşturduğu Kafes

3.15. $\mathbb{Z}_4[u]/\langle u^2 - 3u - 2 \rangle$ Halkası

$\mathbb{Z}_4[u]/\langle u^2 - 3u - 2 \rangle$ halkasında $u^2 = 2 + 3u$ koşulu göz önüne alındığında *Bölüm 3.1.'*dekine benzer şekilde $R_{2+3u} = \mathbb{Z}_4 + u\mathbb{Z}_4$ kümesinin de, toplama ve çarpma işlemlerine göre karakteristiği 4 olan 16 elemanlı değişmeli bir halka olduğu görülür. Ayrıca $u^2 = 2 + 3u$ olmak üzere $\mathbb{Z}_4 + u\mathbb{Z}_4$ ile $\mathbb{Z}_4[u]/\langle u^2 - 3u - 2 \rangle$ halkası arasında bir f izomorfizması tanımlanır. R_{2+3u} halkasının elemanlarının toplama ve çarpma tablosu *Bölüm3.1.'*dekine benzer şekilde oluşturulur.

3.15.1. Sonuç:

i) R_{2+3u} halkasının idealleri ;

$\langle 0 \rangle = \{0\}$,

$\langle 1\rangle = \langle 3\rangle = \langle 1+2u\rangle = \langle 3+2u\rangle = R_{2+3u}$,

$\langle 2\rangle = \{0, 2, 2u, 2+2u\}$,

$\langle u\rangle = \langle 3u\rangle = \{0, 2, u, 2u, 3u, 2+u, 2+2u, 2+3u\}$,

$\langle 2u\rangle = \{0, 2u\}$,

$\langle 1+u\rangle = \langle 3+3u\rangle = \{0, 2, 2u, 1+u, 3+u, 2+2u, 1+3u, 3+3u\}$,

$\langle 2+u\rangle = \langle 2+3u\rangle = \{0, 2u, 2+u, 2+3u\}$,

$\langle 3+u\rangle = \langle 1+3u\rangle = \{0, 3+u, 2+2u, 1+3u\}$,

$\langle 2+2u\rangle = \{0, 2+2u\}$

biçimindedir.

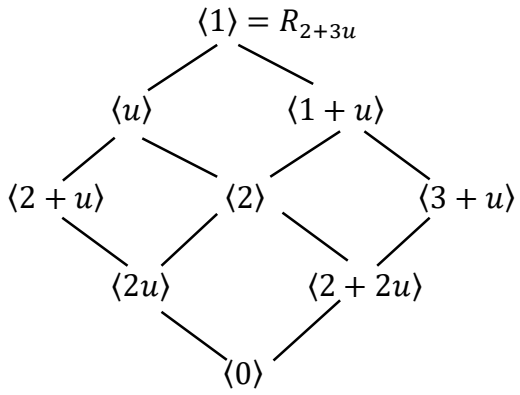
ii) R_{2+3u} halkasının birimsel elemanlar kümesi ;

$U(R_{2+3u}) = \{1, 3, 1+2u, 3+2u\}$ dir.

iii) R_{2+3u} halkasının maksimal idealleri $\langle u\rangle$ ve $\langle 1+u\rangle$ olduğundan R_{2+3u} halkası semi-lokal bir halkadır.

iv) R_{2+3u} halkası bir esas ideal halkasıdır.

v) R_{2+3u} halkası sonlu bir zincir halkası değildir. R_{2+3u} halkasının ideallerinin oluşturduğu kafes *Şekil 3.15*'de verilmiştir.



Şekil 3.15 R_{2+3u} Halkasının İdeallerinin Oluşturduğu Kafes

3.16. $\mathbb{Z}_4[u]/\langle u^2 - 3u - 3\rangle$ Halkası

$\mathbb{Z}_4[u]/\langle u^2 - 3u - 3\rangle$ halkasında $u^2 = 3 + 3u$ koşulu göz önüne alındığında *Bölüm 3.1.*'dekine benzer şekilde $R_{3+3u} = \mathbb{Z}_4 + u\mathbb{Z}_4$ kümesinin de, toplama ve çarpma işlemlerine göre karakteristiği 4 olan 16 elemanlı değişmeli bir halka olduğu görülür. Ayrıca $u^2 = 3 + 3u$ olmak üzere $\mathbb{Z}_4 + u\mathbb{Z}_4$ ile $\mathbb{Z}_4[u]/\langle u^2 - 3u - 3\rangle$ halkası arasında bir f izomorfizması tanımlanır. R_{3+3u} halkasının elemanlarının toplama ve çarpma tablosu *Bölüm3.1.*'dekine benzer şekilde oluşturulur.

3.16.1. Sonuç:

i) R_{3+3u} halkasının idealleri ;

$\langle 0\rangle = \{0\}$,

$\langle 1\rangle = \langle 3\rangle = \langle u\rangle = \langle 3u\rangle = \langle 1+u\rangle = \langle 2+u\rangle = \langle 3+u\rangle = \langle 1+2u\rangle = \langle 3+2u\rangle$

$= \langle 1+3u\rangle = \langle 2+3u\rangle = \langle 3+3u\rangle = R_{3+3u}$

$\langle 2\rangle = \langle 2u\rangle = \langle 2+2u\rangle = \{0, 2, 2u, 2+2u\}$

biçimindedir.

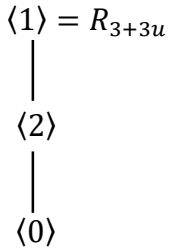
ii) R_{3+3u} halkasının birimsel elemanlar kümesi ;

$U(R_{3+3u}) = \{1, 3, u, 3u, 1+u, 2+u, 3+u, 1+2u, 3+2u, 1+3u, 2+3u, 3+3u\}$ dir.

iii) R_{3+3u} halkasının tek maksimal ideali $\langle 2\rangle$ olduğundan R_{3+3u} halkası lokal bir halkadır.

iv) R_{3+3u} halkası bir esas ideal halkasıdır.

v) R_{3+3u} halkası sonlu bir zincir halkasıdır. R_{3+3u} halkasının ideallerinin oluşturduğu kafes *Şekil 3.16*'da verilmiştir.



Şekil 3.16 R_{3+3u} Halkasının İdeallerinin Oluşturduğu Kafes

3.17. $r = a + ub \in \mathbb{Z}_4 + u\mathbb{Z}_4$ Olmak Üzere R_r Halkalarının Sınıflandırılması

Bu alt bölümde, 3.bölüm boyunca cebirsel özellikleri incelenen tüm halkaların birbirlerine izomorflukları araştırılmış ve son kısımda bunlarla ilgili bir çizelge verilmiştir.

3.17.1. Önerme:

$\psi_1 \colon R_0 \to R_{3+2u}$

$a + ub \mapsto \psi_1(a + ub) = a + (3 + u)\, b$

biçiminde tanımlanan ψ_1 bir izomorfizmadır.

Kanıt:

Herhangi iki $x_1 = a_1 + ub_1$, $x_2 = a_2 + ub_2 \in R_0$ için,

$\psi_1(x_1) = \psi_1(x_2) \Leftrightarrow a_1 + (3 + u)b_1 = a_2 + (3 + u)\, b_2$

$\Leftrightarrow (a_1 - a_2) + (3 + u)(b_1 - b_2) = 0$

$\Leftrightarrow a_1 - a_2 = b_1 - b_2 = 0$

$\Leftrightarrow a_1 = a_2 \, , b_1 = b_2$

$\Leftrightarrow x_1 = x_2$

çift taraflı gerektirmeler sağladığından ψ_1 iyi tanımlı ve birebir bir dönüşümdür.

ψ_1 dönüşümü birebir ve $|R_0| = |R_{3+2u}| = 2^4 = 16$ olduğundan ψ_1 dönüşümü örtendir.

Herhangi iki $x_1 = a_1 + ub_1$, $x_2 = a_2 + ub_2 \in R_0$ için,

i) $\psi_1(x_1 + x_2) = \psi_1((a_1 + ub_1) + (a_2 + ub_2))$

$= \psi_1((a_1 + a_2) + u(b_1 + b_2))$

$= a_1 + a_2 + (3 + u)(b_1 + b_2)$

$= a_1 + a_2 + 3b_1 + 3b_2 + ub_1 + ub_2$

$= a_1 + (3 + u)b_1 + a_2 + (3 + u)b_2$

$= \psi_1(a_1 + ub_1) + \psi_1(a_2 + ub_2)$

$= \psi_1(x_1) + \psi_1(x_2)$

ii) $\psi_1(x_1.x_2) = \psi_1((a_1 + ub_1).(a_2 + ub_2))$

$= \psi_1((a_1.a_2) + u(a_1.b_2 + a_2.b_1) + u^2(b_1.b_2))$

$= \psi_1((a_1.a_2) + u(a_1.b_2 + a_2.b_1))$ $(u^2 = 0$ idi.$)$

$= (a_1.a_2) + (3 + u)(a_1.b_2 + a_2.b_1)$

$= (a_1.a_2) + 3(a_1.b_2 + a_2.b_1) + u(a_1.b_2 + a_2.b_1)$ (1)

$\psi_1(x_1).\psi_1(x_2) = \psi_1(a_1 + ub_1).\psi_1(a_2 + ub_2)$

$= (a_1 + 3b_1 + ub_1).(a_2 + 3b_2 + ub_2)$

$= a_1.a_2 + 3a_1.b_2 + ua_1.b_2 + 3a_2.b_1 + b_1.b_2 + 3ub_1.b_2 + ua_2.b_1 + 3ub_1.b_2 + u^2b_1.b_2$

$= a_1.a_2 + 3a_1.b_2 + ua_1.b_2 + 3a_2.b_1 + b_1.b_2 + 3ub_1.b_2 + ua_2.b_1 + 3ub_1.b_2 + 3b_1.b_2 + 2ub_1.b_2$ $(u^2 = 3 + 2u$ idi.$)$

$$= (a_1.a_2) + 3(a_1.b_2 + a_2.b_1) + u(a_1.b_2 + a_2.b_1) \qquad (2)$$

bulunur. Bu durumda (1) ve (2) den,

$\psi_1(x_1.x_2) = \psi_1(x_1).\psi_1(x_2)$

elde edilir. Bu durumda (i) ve (ii) sağlandığından ψ_1 dönüşümü bir halka homomorfizmasıdır.

Dolayısıyla ψ_1 birebir, örten ve bir homomorfizma olduğundan ψ_1 bir izomorfizmadır.

3.17.2. Sonuç:

$R_0 \cong R_{3+2u}$

biçiminde gösterilir.

3.17.3. Önerme:

$\psi_2 \colon R_1 \to R_{2u}$

$a + ub \mapsto \psi_2(a + ub) = a + (1 + u)\, b$

biçiminde tanımlanan ψ_2 bir izomorfizmadır.

Kanıt:

3.17.1.Önerme'nin kanıtına benzer şekilde elde elde edilir.

3.17.4. Sonuç:

$R_1 \cong R_{2u}$

biçiminde gösterilir.

3.17.5. Önerme:

$\psi_3 \colon R_2 \to R_{1+2u}$

$a + ub \mapsto \psi_3(a + ub) = a + (1 + u)\, b$

biçiminde tanımlanan ψ_3 bir izomorfizmadır.

Kanıt:

3.17.1.Önerme'nin kanıtına benzer şekilde elde elde edilir.

3.17.6. Sonuç:

$R_2 \cong R_{1+2u}$

biçiminde gösterilir.

3.17.7. Önerme:

$\psi_4 \colon R_3 \to R_{2+2u}$

$a + ub \mapsto \psi_4(a + ub) = a + (1 + u)\, b$

biçiminde tanımlanan ψ_4 bir izomorfizmadır.

Kanıt:

3.17.1.Önerme'nin kanıtına benzer şekilde elde elde edilir.

3.17.8. Sonuç:

$R_3 \cong R_{2+2u}$

biçiminde gösterilir.

3.17.9. Önerme:

$\psi_5 \colon R_u \to R_{2+u}$

$a + ub \mapsto \psi_5(a + ub) = a + (2 + u)\, b$

biçiminde tanımlanan ψ_5 bir izomorfizmadır.

Kanıt:

3.17.1.Önerme'nin kanıtına benzer şekilde elde elde edilir.

3.17.10. Sonuç:

$R_u \cong R_{2+u}$

biçiminde gösterilir.

3.17.11. Önerme:

$\psi_6 \colon R_{2+u} \to R_{2+3u}$

$a + ub \mapsto \psi_6(a + ub) = a + (1 + u)\, b$

biçiminde tanımlanan ψ_6 bir izomorfizmadır.

Kanıt:

3.17.1.Önerme'nin kanıtına benzer şekilde elde elde edilir.

3.17.12. Sonuç:

$R_{2+u} \cong R_{2+3u}$

biçiminde gösterilir.

3.17.13. Önerme:

$\psi_7 \colon R_{2+3u} \to R_{3u}$

$a + ub \mapsto \psi_7(a + ub) = a + (2 + u)\, b$

biçiminde tanımlanan ψ_7 bir izomorfizmadır.

Kanıt:

3.17.1.Önerme'nin kanıtına benzer şekilde elde elde edilir.

3.17.14. Sonuç:

$R_{2+3u} \cong R_{3u}$

biçiminde gösterilir.

3.17.9.Önerme, *3.17.11.Önerme* ve *3.17.13.Önerme*'nin bir sonucu olarak aşağıdaki sonuç verilir.

3.17.15. Sonuç:

$R_u \cong R_{2+u} \cong R_{2+3u} \cong R_{3u}$

biçiminde gösterilir.

Kanıt:

*3.17.10.Sonuç'*dan $R_u \cong R_{2+u}$, *3.17.12.Sonuç*'dan $R_{2+u} \cong R_{2+3u}$ ve *3.17.14.Sonuç'*dan $R_{2+3u} \cong R_{3u}$ biçiminde gösterildiğini biliyoruz. Bu sebeple;

$R_u \cong R_{2+u} \cong R_{2+3u} \cong R_{3u}$

elde edilir.

3.17.16. Önerme:

$\psi_8 \colon R_{1+u} \to R_{3+u}$

$a + ub \mapsto \psi_8(a + ub) = a + (2 + u)\, b$

biçiminde tanımlanan ψ_8 bir izomorfizmadır.

Kanıt:

*3.17.1.Önerme'*nin kanıtına benzer şekilde elde elde edilir.

3.17.17. Sonuç:

$R_{1+u} \cong R_{3+u}$

biçiminde gösterilir.

3.17.18. Önerme:

ψ_9: $R_{3+u} \to R_{3+3u}$

$a + ub \mapsto \psi_9(a + ub) = a + (1 + u)\, b$

biçiminde tanımlanan ψ_9 bir izomorfizmadır.

Kanıt:

*3.17.1.Önerme'*nin kanıtına benzer şekilde elde elde edilir.

3.17.19. Sonuç:

$R_{3+u} \cong R_{3+3u}$

biçiminde gösterilir.

3.17.20. Önerme:

ψ_{10}: $R_{3+3u} \to R_{1+3u}$

$a + ub \mapsto \psi_{10}(a + ub) = a + (2 + u)\, b$

biçiminde tanımlanan ψ_{10} bir izomorfizmadır.

Kanıt:

*3.17.1.Önerme'*nin kanıtına benzer şekilde elde elde edilir.

3.17.21. Sonuç:

$R_{3+3u} \cong R_{1+3u}$

biçiminde gösterilir.

3.17.16.Önerme, *3.17.18.Önerme* ve *3.17.20.Önerme*'nin bir sonucu olarak aşağıdaki sonuç verilir.

3.17.22. Sonuç:

$R_{1+u} \cong R_{3+u} \cong R_{3+3u} \cong R_{1+3u}$

biçiminde gösterilir.

Kanıt:

*3.17.17.Sonuç'*dan $R_{1+u} \cong R_{3+u}$, *3.17.19.Sonuç'*dan $R_{3+u} \cong R_{3+3u}$ ve *3.17.21.Sonuç'*dan $R_{3+3u} \cong R_{1+3u}$ biçiminde gösterildiğini biliyoruz. Bu sebeple;

$R_{1+u} \cong R_{3+u} \cong R_{3+3u} \cong R_{1+3u}$

elde edilir.

Çizelge 3.3 $r = a + ub \in \mathbb{Z}_4 + u\mathbb{Z}_4$ Olmak Üzere R_r Halkalarının Sınıflandırılması

$R_0 \cong R_{3+2u}$
$R_1 \cong R_{2u}$
$R_2 \cong R_{1+2u}$
$R_3 \cong R_{2+2u}$
$R_u \cong R_{2+u} \cong R_{2+3u} \cong R_{3u}$
$R_{1+u} \cong R_{3+u} \cong R_{3+3u} \cong R_{1+3u}$

BÖLÜM 4

R_u, R_1, R_0 VE R_3 HALKALARI ÜZERİNDE TANIMLI $(1+2u)$ -SABİT DEVİRLİ VE DEVİRLİ KODLARIN GRAY GÖRÜNTÜLERİ

Tezin bu bölümünde, $r = u, 1, 0, 3$ olmak üzere R_r halkası üzerinde tanımlı devirli ve $(1+2u)$-sabit devirli kodların Gray görüntülerinin belirlendiği makaleler incelenmiştir.

4.1. R_u Halkası Üzerinde Tanımlı Lineer Kodlar

4.1.1. Tanım:

$a, b \in \mathbb{Z}_4, u^2 = u$ olmak üzere,

$\phi_u : R_u \rightarrow \mathbb{Z}_4^2$
$a + ub \mapsto (a, a + b)$

biçiminde tanımlanan dönüşüme "*Gray dönüşümü*" denir (Gao ve Gao, 2014).

4.1.2. Teorem:

$a, b \in \mathbb{Z}_4, u^2 = u$ olmak üzere,

$$\phi_u : R_u \rightarrow \mathbb{Z}_4^2$$
$$a + ub \mapsto (a, a + b)$$

biçiminde tanımlanan ϕ_u Gray dönüşümü bir $\mathbb{Z}_4$-modül izomorfizmasıdır (Bandi ve Bhaintwal, 2014).

4.1.3. Not:

$0 \leq i \leq n-1$ ve $c_i = a_i + ub_i$ olmak üzere herhangi bir $(c_0, c_1, \dots, c_{n-1}) \in R_u^n$

için ϕ_u Gray dönüşümü,

$$\phi_u : R_u^n \rightarrow \mathbb{Z}_4^{2n}$$

$$(c_0, c_1, \dots, c_{n-1}) \mapsto \phi_u(c_0, c_1, \dots, c_{n-1})$$
$$= (a_0, a_1, \dots, a_{n-1}, a_0 + b_0, a_1 + b_1, \dots, a_{n-1} + b_{n-1})$$

biçiminde R_u^n kümesine genişletilebilir.

4.1.4. Tanım:

$(\mathbb{Z}_4, +, .)$ halkası verilsin. Herhangi bir $e \in \mathbb{Z}_4$ için,

$$w_L(e) = \min\{e, 4 - e\}$$

biçiminde tanımlanan değere e elemanının "Lee ağırlığı" denir (Dinh vd., 2018).

Bu durumda $\mathbb{Z}_4$ halkasının elemanlarının Lee ağırlıkları sırasıyla,

$w_L(0) = 0, w_L(1) = w_L(3) = 1$ ve $w_L(2) = 2$ dir.

4.1.5. Tanım:

$a, b \in \mathbb{Z}_4$ ve $u^2 = u$ olmak üzere,

$r = a + ub$, R_u halkasının herhangi bir elemanı olsun. Bu durumda,

$$w_G : R_u \rightarrow IN$$

$$r = a + ub \mapsto w_G(r) = \begin{cases} 0\,; & a = b = 0 \\ 1\,; & a = 1, b = 3 \; ya \; da \; a = 3, b = 1 \\ 1\,; & a = 0, b = 1 \; ya \; da \; a = 0, b = 3 \\ 2\,; & a = b = 2 \;\; ya \;\; da \; a = 0, b = 2 \\ 2\,; & a = 1, b = 0 \; ya \; da \; a = 1, b = 3 \\ 2\,; & a = 3, b = 0 \; ya \; da \; a = 3, b = 2 \\ 3\,; & a = b = 1 \; ya \; da \; a = b = 3 \\ 3\,; & a = 2, b = 1 \; ya \; da \; a = 2, b = 3 \\ 4\,; & a = 2, b = 0 \end{cases}$$

biçiminde tanımlanan değere r elemanının "Gray ağırlığı" denir. Kısaca bir $r \in R_u$ elemanının Gray ağırlığı $w_G(r) = w_L(a) + w_L(a + b)$ şeklindedir (Gao ve Gao, 2014).

4.1.6. Not:

Herhangi bir $c = (c_0, c_1, \dots, c_{n-1}) \in R_u^n$ elemanının Gray ağırlığı, bileşenlerinin Gray ağırlıklarının toplamı şeklindedir. Kısaca,

$w_G(c) = \sum_{i=0}^{n-1} w_G(c_i)$ dir.

4.1.7. Tanım:

$c_1 \neq c_2$ olmak üzere, herhangi iki $c_1, c_2 \in R_u^n$ elemanları için,

$$d_G(c_1, c_2) = w_G(c_1 - c_2)$$

biçiminde tanımlanan değere c_1 ve c_2 elemanlarının "Gray uzaklığı" denir (Gao ve Gao, 2014).

4.1.8. Not:

C, R_u halkası üzerinde tanımlı (n, M, d_G) parametrelerine sahip bir lineer kod olsun. C kodunun minimum Gray uzaklığı $d_G(C) = d_G$, birbirinden farklı tüm kod sözcüklerinin Gray uzaklıklarının en küçüğüdür. C lineer kod olduğu için $d_G = w_G$ dir. Benzer şekilde C kodunun minimum Gray ağırlığı $w_G = w_G(C)$, sıfırdan farklı tüm kod sözcüklerinin Gray ağırlıklarının en küçüğüdür (Gao ve Gao, 2014).

4.1.9. Teorem:

d_G minimum Gray uzaklığı, d_L minimum Lee uzaklığı olmak üzere, (R_u^n, d_G) kümesinden $(\mathbb{Z}_4^{2n}, d_L)$ kümesine tanımlı ϕ_u Gray dönüşümü hem lineer hem de uzaklık koruyan bir dönüşümdür (Gao ve Gao, 2014).

Kanıt:

Her $x, y \in R_u, k \in \mathbb{Z}_4$ için $x = a_1 + ub_1, y = a_2 + ub_2$ olmak üzere,

i) $\phi_u(x+y) = \phi_u\big((a_1 + ub_1) + (a_2 + ub_2)\big)$

$= \phi_u((a_1 + a_2) + u(b_1 + b_2))$

$= (a_1 + a_2, a_1 + a_2 + b_1 + b_2)$

$= (a_1, a_1 + b_1) + (a_2, a_2 + b_2)$

$= \phi_u(x) + \phi_u(y)$

ii) $\phi_u(k.x) = \phi_u(k.(a_1 + ub_1))$

$= \phi_u(k.a_1 + k.ub_1)$

$= (k.a_1, k.a_1 + k.b_1)$

$= k.(a_1, a_1 + b_1)$

$= k.\phi_u(x)$

elde edilir. Bu durumda ϕ_u lineer bir dönüşümdür. O halde ϕ_u dönüşümünün R_u^n kümesine genişletilmiş hali de lineerdir.

Herhangi iki $c_1, c_2 \in R_u^n$ için,

$d_G(c_1, c_2) = w_G(c_1 - c_2)$

$= w_L(\phi_u(c_1 - c_2))$

$= w_L\big(\phi_u(c_1) - \phi_u(c_2)\big)$

$= d_L(\phi_u(c_1), \phi_u(c_2))$

elde edilir. Bu durumda ϕ_u uzaklık koruyan bir dönüşümdür.

4.1.10. Teorem:

C, R_u halkası üzerinde tanımlı (n, M, d_G) parametreli lineer bir kod ise $d_G = d_L$ olmak üzere, $\phi_u(C)$ kodu $\mathbb{Z}_4$ üzerinde tanımlı $(2n, M, d_L)$ parametreli lineer bir koddur (Gao ve Gao, 2014).

4.1.11. Teorem:

C, R_u halkası üzerinde tanımlı uzunluğu n olan lineer bir kod olsun. C lineer kodunun duali $C^{\perp}$ olmak üzere, $\phi_u(C^{\perp}) = \phi_u(C)^{\perp}$ dir. Ayrıca C self-dual kod ise $\phi_u(C)$'de self-dual koddur (Gao ve Gao,2014).

Kanıt:

$\Rightarrow$:

Herhangi bir $\phi_u(x) \in \phi_u(C^{\perp})$ olsun.

$\phi_u(x) \in \phi_u(C^{\perp}) \Rightarrow x \in C^{\perp}$

$$\Rightarrow \forall\, y \in C \; için \; x.y = 0$$

$$\Rightarrow \; \phi_u(x.y) = \phi_u(x).\phi_u(y) = 0$$

$$\Rightarrow \phi_u(x) \in \phi_u(C)^{\perp}$$

elde edilir. O halde $\phi_u(C^{\perp}) \subseteq \phi_u(C)^{\perp}$ dir. (i)

$\Leftarrow$:

Herhangi bir $\phi_u(z) \in \phi_u(C)^{\perp}$ olsun.

$\phi_u(z) \in \phi_u(C)^{\perp} \Rightarrow \forall\, \phi_u(t) \in \phi_u(C) \; için \; \phi_u(z).\phi_u(t) = 0$

$$\Rightarrow \forall\, t \in C \; için \; \phi_u(z.t) = 0$$

$$\Rightarrow \forall\, t \in C \; için \; z.t = 0$$

$$\Rightarrow z \in C^{\perp}$$

$$\Rightarrow \phi_u(z) \in \phi_u(C^{\perp})$$

elde edilir. O halde $\phi_u(C)^{\perp} \subseteq \phi_u(C^{\perp})$ dir. (ii)

Bu durumda (i) ve (ii) den $\phi_u(C^{\perp}) = \phi_u(C)^{\perp}$ dir.

Ayrıca C self-dual ise $C = C^{\perp}$ dir. Her iki yana ϕ_u uygulanırsa $\phi_u(C) = \phi_u(C^{\perp})$ elde edilir. $\phi_u(C^{\perp}) = \phi_u(C)^{\perp}$ eşitliği kullanılırsa $\phi_u(C)^{\perp} = \phi_u(C)$ elde edilir. Bu durumda $\phi_u(C)$'de self-dualdir.

4.1.12. Önerme:

R_u halkası üzerinde tanımlı uzunluğu n olan C kodu lineer bir kod olsun. Bu durumda,

$C_1 = \{ a \in \mathbb{Z}_4^n \mid \exists\, b \in \mathbb{Z}_4^n \, için \, a + ub \in C \}$

$C_2 = \{ a + b \in \mathbb{Z}_4^n \mid \exists\, a \in \mathbb{Z}_4^n \, için \, a + ub \in C \}$

biçiminde tanımlanan C_1 ve C_2 kodları $\mathbb{Z}_4$ üzerinde tanımlı uzunluğu n olan iki lineer koddur.

Kanıt:

C, R_u halkası üzerinde n uzunluğunda bir lineer kod ise C, R_u^n'in bir alt modülüdür. Herhangi iki $a_1, a_2 \in C_1$ için $a_1 + ub_1 \in C$ ve $a_2 + ub_2 \in C$ olacak biçimde en az bir tane $b_1, b_2 \in \mathbb{Z}_4^n$ elemanları vardır. $(C, +)$ abel grup olduğu için $(a_1 + ub_1) + (a_2 + ub_2) \in C$ dir. Bu durumda, $(a_1 + a_2) + u(b_1 + b_2) \in C$ olacak şekilde $\exists\, b_1 + b_2 \in \mathbb{Z}_4^n$ olduğu için $a_1 + a_2 \in C_1$ dir.

Her $k \in \mathbb{Z}_4$ ve her $a \in C_1$ olsun. Bu durumda $a + ub \in C$ olacak şekilde en az bir tane $b \in \mathbb{Z}_4^n$ vardır. C, R_u-alt modül olduğu için $k.(a + ub) \in C$ dir. Bu durumda $k.a + (k.b)u \in C$ olacak şekilde $\exists\, k.b \in \mathbb{Z}_4^n$ olduğu için $k.a \in C_1$ dir. O halde C_1, $\mathbb{Z}_4$ üzerinde uzunluğu n olan lineer bir koddur.

C_2'nin $\mathbb{Z}_4$ üzerinde tanımlı uzunluğu n olan lineer bir kod olduğu benzer şekilde gösterilir.

4.1.13. Not: Bu bölüm boyunca C, C_1 ve C_2 lineer kodları denildiğinde *4.1.12.Önerme*'de tanımlanan kodlar düşünülecektir.

4.1.14. Gösterim:

A ve B kümesinin elemanları sırasıyla, sıralı n'liler ve sıralı m'liler olmak üzere,

$A \otimes B = \{ (a_1, a_2, \dots a_n, b_1, b_2, \dots, b_m) \mid (a_1, a_2, \dots a_n) \in A,\ (b_1, b_2, \dots, b_m) \in B \}$ dir.

4.1.15. Teorem:

C, R_u halkası üzerinde tanımlı uzunluğu n olan lineer bir kod olsun. Bu durumda,

$\phi_u(C) = C_1 \otimes C_2$ ve $|C| = |C_1|.|C_2|$ dir (Bandi ve Bhaintwal, 2014).

Kanıt:

ϕ_u birebir ve örten olduğu için herhangi bir $c' = (a_1, \dots, a_n, a_1 + b_1, \dots, a_n + b_n) \in \phi_u(c)$ için $\phi_u(c) = c'$ olacak şekilde $c_i = a_i + ub_i$ olmak üzere $c = (c_1, c_2, \dots, c_n) \in C$ vardır. Bu nedenle, $\phi_u(C) \subseteq C_1 \otimes C_2$ dir.

Diğer yandan, $a = (a_1, a_2, \dots, a_n) \in C_1,\ b = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n) \in C_2$ olmak üzere herhangi bir $(a, b) \in C_1 \otimes C_2$ elemanı için $x = a + us$ veya $b + (1 + 3u)t$, $s, t \in \mathbb{Z}_4^n$ olmak üzere $x = (x_1, x_2, \dots, x_n), y = (y_1, y_2, \dots, y_n) \in C$ elemanları vardır. C lineer olduğu için $x(1 + 3u) + yu = a + (3a + b)u \in C$ dir. Dolayısıyla, $\phi_u(a + (3a + b)u) = (a, b) \in \phi_u(C)$ dir. Bu durumda, $C_1 \otimes C_2 \subseteq \phi_u(C)$ dir.

$|\phi_u(C)| = |C_1 \otimes C_2| = |C_1|.|C_2|$ olduğu kolaylıkla görülür. ϕ_u birebir bir dönüşüm olduğu için $|C| = |\phi_u(C)| = |C_1|.|C_2|$ dir.

4.1.16. Sonuç:

R_u halkası üzerinde tanımlı uzunluğu n olan bir C lineer kodu, $C = (1 + 3u)C_1 + uC_2$ şeklinde yazılabilir.

Kanıt:

Her $i = 1,2, \dots, n$ için $c_i = a_i + ub_i$ olmak üzere, $c = (c_1, c_2, \dots, c_n) \in C$ olsun. Bu durumda $a = (a_1, a_2, \dots, a_n), b = (b_1, b_2, \dots, b_n)$ olmak üzere, $\phi_u(C) = (a, a + b)$ dir. $\phi_u(C) = C_1 \otimes C_2$ olduğundan, $a \in C_1$ ve $a + b \in C_2$ dir. Bu durumda, $(1 + 3u)a + u(a + b) = a + ub = c \in (1 + 3u)C_1 \oplus uC_2$ dir. O halde, $C \subseteq (1 + 3u)C_1 \oplus uC_2$ dir.

Diğer taraftan, $a \in C_1$ ve $b \in C_2$ olmak üzere, $x = (1 + 3u)a + ub \in (1 - u)C_1 \oplus uC_2$ olsun. Bu durumda, $\phi_u(x) = (a, b) \in C_1 \otimes C_2 = \phi_u(C)$ olur. ϕ_u birebir ve örten olduğundan $x \in C$ dir. Bu durumda, $(1 + 3u)C_1 \oplus uC_2 \subseteq C$ dir.

Dolayısıyla, $C = (1 + 3u)C_1 + uC_2$ dir.

4.2. R_u Halkası Üzerinde Uzunluğu Tek Olan $(1 + 2u)$-Sabit Devirli Kodlar İle Devirli Kodlar Arasındaki İlişki

Bu bölümde, $u^2 = u$ olmak üzere R_u halkası üzerindeki $(1 + 2u)$-sabit devirli kodlarla devirli kodlar arasındaki ilişkiler verilmiştir. Öncelikle R_u halkasının karakteristiği 4 olduğundan;

$$(1 + 2u)^n = \begin{cases} 1; & n \text{ çift ise} \\ 1 + 2u; & n \text{ tek ise} \end{cases}$$

şeklindedir. Bu sonuç doğrultusunda aşağıdaki önerme sağlanır.

4.2.1.Önerme:

$$\mu_u : R_u[x]/\langle x^n - 1\rangle \to R_u[x]/\langle x^n - (1 + 2u)\rangle$$

$$\overline{c(x)} \mapsto \mu_u\left(\overline{c(x)}\right) = \overline{c((1 + 2u)x)}$$

dönüşümü tanımlansın. n tek olması durumunda, μ_u bir halka izomorfizmasıdır (Dinh vd., 2018).

4.2.2.Sonuç:

n pozitif tek tam sayı olsun. I kümesinin $R_u[x]/\langle x^n - 1\rangle$ halkasının bir ideali olması için gerekli ve yeterli koşul $\mu_u(I)$ kümesinin $R_u[x]/\langle x^n - (1+2u)\rangle$ halkasının bir ideali olmasıdır (Dinh vd., 2018).

4.2.3.Sonuç:

n pozitif tek bir tam sayı ve C, R_u^n kümesinin bir alt kümesi olsun. $\overline{\mu_u}$ permütasyonu R_u^n kümesi üzerinde,

$$\overline{\mu_u}(c_0, c_1, \dots, c_{n-1}) = (c_0, (1+2u)c_1, (1+2u)^2 c_2, \dots, (1+2u)^{n-1} c_{n-1})$$

biçiminde tanımlansın. Bu durumda, C'nin devirli bir kod olması için gerekli ve yeterli koşul $\overline{\mu_u}(C)$'nin $(1+2u)$-sabit devirli bir kod olmasıdır (Dinh vd., 2018).

4.3. R_u Halkası Üzerinde Tanımlı Gray Dönüşüm, $(1+2u)$-Sabit Devirli Kodlar ve Tek Uzunluklu Devirli Kodların Gray Görüntüleri

4.3.1.Tanım:

$a, b \in \mathbb{Z}_4$, $u^2 = u$, olmak üzere R_u halkası üzerinde,

$\phi_u: R_u \to \mathbb{Z}_4^2$

$a + ub \mapsto (a, 2b + a)$

biçiminde tanımlanan dönüşüme ''*Gray dönüşümü*'' denir (Dinh vd., 2018).

4.3.2. Not:

$0 \le i \le n-1$ ve $c_i = a_i + ub_i$ olmak üzere herhangi bir $(c_0, c_1, \dots, c_{n-1}) \in R_u^n$

için ϕ_u Gray dönüşümü,

$$\phi_u : R_u^n \to \mathbb{Z}_4^{2n}$$

$$(c_0, c_1, \dots, c_{n-1}) \mapsto \phi_u(c_0, c_1, \dots, c_{n-1})$$

$$= (a_0, 2b_0 + a_0, a_1, 2b_1 + a_1, \dots, a_{n-1}, 2b_{n-1} + a_{n-1})$$

biçiminde R_u^n kümesine genişletilebilir.

4.3.3. Önerme:

φ ve σ sırasıyla, R_u^n üzerinde devirli ve $(1 + 2u)$-sabit devirli öteleme olsun. Bu durumda, $\phi_u \circ \sigma = \varphi^2 \circ \phi_u$ sağlanır (Dinh vd., 2018).

4.3.4. Teorem:

R_u halkası üzerinde tanımlı uzunluğu n olan $(1 + 2u)$-sabit devirli bir kodun Gray görüntüsü $\mathbb{Z}_4$ üzerinde tanımlı uzunluğu $2n$ ve indeksi 2 olan bir quasicyclic koddur (Dinh vd., 2018).

4.3.5. Önerme:

φ, R_u^n üzerinde tanımlı devirli öteleme olsun. Bu durumda, $\phi_u \circ \varphi = \varphi^2 \circ \phi_u$ sağlanır (Dinh vd., 2018).

4.3.6. Teorem:

C, R_u halkası üzerinde tanımlı uzunluğu n olan devirli bir kod ise bu kodun Gray görüntüsü, $\mathbb{Z}_4$ üzerinde tanımlı, uzunluğu $2n$ ve indeksi 2 olan bir quasicyclic koddur (Dinh vd., 2018).

4.4. R_1 Halkası Üzerinde Uzunluğu Tek Olan $(1+2u)$-Sabit Devirli Kodlar ile Devirli Kodlar Arasındaki İlişki

Bu bölümde, $u^2 = 1$ olmak üzere R_1 halkası üzerinde tanımlı $(1+2u)$-sabit devirli kodlarla devirli kodlar arasındaki ilişki verilmiştir. Öncelikle R_1 halkasının karakteristiği 4 olduğundan;

$$(1+2u)^n = \begin{cases} 1; & n \text{ çift ise} \\ 1+2u; & n \text{ tek ise} \end{cases}$$

şeklindedir. Bu sonuç doğrultusunda aşağıdaki önerme sağlanır.

4.4.1. Önerme:

$$\mu_1 : R_1[x]/\langle x^n - 1\rangle \to R_1[x]/\langle x^n - (1+2u)\rangle$$

$$\overline{c(x)} \mapsto \mu_1(\overline{c(x)}) = \overline{c((1+2u)x)}$$

dönüşümü tanımlansın. n tek olması durumunda, μ_1 bir halka izomorfizmasıdır (Shi vd., 2017).

4.4.2. Sonuç:

n pozitif tek tam sayı olsun. I kümesinin $R_1[x]/\langle x^n - 1\rangle$ halkasının bir ideali olması için gerekli ve yeterli koşul $\mu_1(I)$ kümesinin $R_1[x]/\langle x^n - (1+2u)\rangle$ halkasının bir ideali olmasıdır (Shi vd., 2017).

4.4.3. Sonuç:

n pozitif tek bir tam sayı ve C, R_1^n kümesinin bir alt kümesi olsun. $\overline{\mu_1}$ permütasyonu R_1^n kümesi üzerinde,

$$\overline{\mu_1}(c_0, c_1, \dots, c_{n-1}) = (c_0, (1+2u)c_1, (1+2u)^2 c_2, \dots, (1+2u)^{n-1} c_{n-1})$$

biçiminde tanımlansın. Bu durumda, C'nin devirli bir kod olması için gerekli ve yeterli koşul $\overline{\mu_1}(C)$'nin $(1+2u)$-sabit devirli bir kod olmasıdır (Shi vd., 2017).

4.5. R_1 Halkası Üzerinde Tanımlı Gray Dönüşüm, $(1+2u)$-Sabit Devirli Kodlar ve Devirli Kodların Gray Görüntüleri

4.5.1. Tanım:

$u^2 = 1$, olmak üzere R_1 halkası üzerinde,

$$\phi_1 : R_1 \to \mathbb{Z}_4^2$$

$$a + ub \mapsto (b, 2a + b)$$

biçiminde tanımlanan dönüşüme ‘‘*Gray dönüşümü*’’ denir. Bu dönüşüm lineerdir fakat birebir ve örten değildir (Shi vd., 2017).

4.5.2. Not:

$0 \le i \le n-1$ ve $c_i = a_i + ub_i$ olmak üzere herhangi bir $(c_0, c_1, \dots, c_{n-1}) \in R_1^n$ için ϕ_1 Gray dönüşümü,

$$\phi_1 : R_1^n \to \mathbb{Z}_4^{2n}$$

$$(c_0, c_1, \dots, c_{n-1}) \mapsto \phi_1(c_0, c_1, \dots, c_{n-1})$$

$$= (b_0, b_1, \dots, b_{n-1}, 2a_0 + b_0, 2a_1 + b_1, \dots, 2a_{n-1} + b_{n-1})$$

biçiminde R_1^n kümesine genişletilebilir.

4.5.3. Önerme:

φ ve σ sırasıyla, R_1^n üzerinde devirli ve $(1+2u)$-sabit devirli öteleme olsun. Bu durumda, $\phi_1 \circ \sigma = \varphi \circ \phi_1$ sağlanır (Shi vd., 2017).

4.5.4. Teorem:

R_1 halkası üzerinde, uzunluğu n olan $(1+2u)$-sabit devirli kodun Gray görüntüsü $\mathbb{Z}_4$ üzerinde tanımlı, uzunluğu $2n$ olan bir devirli koddur (Shi vd., 2017).

4.5.5. Not:

Bazı durumlarda, $\phi_1^*(c) = (b_0, 2a_0 + b_0, b_1, 2a_1 + b_1, \dots, b_{n-1}, 2a_{n-1} + b_{n-1})$ ile tanımlanan ϕ_1'nin permütasyon versiyonunu kullanmak daha uygundur. ϕ_1 ve ϕ_1^* kullanılarak elde edilen kodlar bir permütasyon yardımıyla biri diğerinden elde edilir. Kısaca kodlar birbirine denktir (Shi vd., 2017).

4.5.6. Önerme:

φ, R_1^n üzerinde devirli öteleme olsun. Bu durumda, $\phi_1^* \circ \varphi = \varphi^2 \circ \phi_1^*$ sağlanır (Shi vd., 2017).

4.5.7. Teorem:

C, R_1 halkası üzerinde tanımlı uzunluğu n olan devirli bir kod ise $\phi_1^*(C)$, $\mathbb{Z}_4$ üzerinde tanımlı, uzunluğu $2n$ ve indeksi 2 olan bir quasicyclic koda denktir (Shi vd., 2017).

4.6. R_0 Halkası Üzerinde Uzunluğu Tek Olan $(1 + 2u)$-Sabit Devirli Kodlar ile Devirli Kodlar Arasındaki İlişki

Bu bölümde, $u^2 = 0$ olmak üzere R_0 halkası üzerinde tanımlı $(1 + 2u)$-sabit devirli kodlarla devirli kodlar arasındaki ilişki verilmiştir. Öncelikle R_0 halkasının karakteristiği 4 olduğundan;

$$(1 + 2u)^n = \begin{cases} 1; & n \text{ çift ise} \\ 1 + 2u; & n \text{ tek ise} \end{cases}$$

şeklindedir. Bu sonuç doğrultusunda aşağıdaki önerme sağlanır.

4.6.1. Önerme:

$$\mu_0 : R_0[x]/\langle x^n - 1\rangle \to R_0[x]/\langle x^n - (1 + 2u)\rangle$$

$$\overline{c(x)} \mapsto \mu_0\big(\overline{c(x)}\big) = \overline{c((1 + 2u)x)}$$

dönüşümü tanımlansın. n tek olması durumunda, μ_0 bir halka izomorfizmasıdır (Ashraf ve Mohammad, 2015).

4.6.2. Sonuç:

n pozitif tek tam sayı olsun. I kümesinin $R_0[x]/\langle x^n - 1\rangle$ halkasının bir ideali olması için gerekli ve yeterli koşul $\mu_0(I)$ kümesinin $R_0[x]/\langle x^n - (1+2u)\rangle$ halkasının bir ideali olmasıdır (Ashraf ve Mohammad, 2015).

4.6.3. Sonuç:

n pozitif tek bir tam sayı ve C, R_0^n kümesinin bir alt kümesi olsun. $\overline{\mu_0}$ permütasyonu R_0^n kümesi üzerinde,

$$\overline{\mu_0}(c_0, c_1, \dots, c_{n-1}) = (c_0, (1+2u)c_1, (1+2u)^2 c_2, \dots, (1+2u)^{n-1} c_{n-1})$$

biçiminde tanımlansın. Bu durumda, C'nin devirli bir kod olması için gerekli ve yeterli koşul $\overline{\mu_0}(C)$'nin $(1+2u)$-sabit devirli bir kod olmasıdır (Ashraf ve Mohammad, 2015).

4.7. R_0 Halkası Üzerinde Tanımlı Gray Dönüşüm, $(1+2u)$-Sabit Devirli Kodlar ve Tek Uzunluklu Devirli Kodların Gray Görüntüleri

4.7.1. Tanım:

$u^2 = 0$, olmak üzere R_0 halkası üzerinde,

$$\phi_0 : R_0 \to \mathbb{Z}_4^2$$
$$a + ub \mapsto (b, 2a + b)$$

şeklinde tanımlanan dönüşüme ‘‘*Gray dönüşümü*’’ denir (Ashraf ve Mohammad, 2015).

4.7.2. Tanım:

R_0 halkasının bir $r = a + ub$ elemanının Lee ağırlığı, $w_L(b, 2a + b)$ $\mathbb{Z}_4^2$ üzerinde tanımlı Lee ağırlığı olmak üzere, $w_L(a + ub) = w_L(b) + w_L(2a + b)$ şeklinde tanımlanır.

$c = (c_0, c_1, \dots, c_{n-1}) \in R_0^n$ kod sözcüğünün Lee ağırlığı bileşenlerinin Lee ağırlıklarının toplamı şeklindedir. d_L, Lee uzaklığı $\overline{c_1}, \overline{c_2} \in R_0^n$ için $d_L(\overline{c_1}, \overline{c_2}) = w_L(\overline{c_1} - \overline{c_2})$ şeklinde tanımlanır. C kodunun minimum Lee uzaklığı C'deki birbirinden farklı kod sözcükleri arasındaki Lee uzaklıklarının en küçüğüdür. C kodunun minimum Lee ağırlığı C kodunun içindeki sıfırdan farklı tüm kod sözcüklerinin Lee ağırlıklarının en küçüğüdür.

4.7.3. Not:

$0 \leq i \leq n - 1$ ve $c_i = a_i + ub_i$ olmak üzere herhangi bir $(c_0, c_1, \dots, c_{n-1}) \in R_0^n$

için ϕ_0 Gray dönüşümü,

$$\phi_0 : R_0^n \to \mathbb{Z}_4^{2n}$$

$$(c_0, c_1, \dots, c_{n-1}) \mapsto \phi_0(c_0, c_1, \dots, c_{n-1})$$

$$= (b_0, b_1, \dots, b_{n-1}, 2a_0 + b_0, 2a_1 + b_1, \dots, 2a_{n-1} + b_{n-1})$$

biçiminde R_0^n kümesine genişletilebilir.

4.7.4. Önerme:

d_L, R_0^n üzerinde tanımlı minimum Lee uzaklığı, d_L, $\mathbb{Z}_4^{2n}$ üzerinde tanımlı minimum Lee uzaklığı olmak üzere, (R_0^n, d_L) kümesinden $(\mathbb{Z}_4^{2n}, d_L)$ kümesine tanımlı ϕ_0 Gray dönüşümü hem lineer hem de uzaklık koruyan bir dönüşümdür.

4.7.5. Teorem:

C, R_0 halkası üzerinde tanımlı bir (n, M, d_L) parametreli bir lineer kod ise $\phi_0(C)$ kodu $\mathbb{Z}_4$ üzerinde tanımlı bir $(2n, M, d_L)$ parametreli bir lineer koddur.

4.7.6. Önerme:

φ ve σ sırasıyla, R_0^n üzerinde devirli ve $(1+2u)$-sabit devirli öteleme olsun. Bu durumda, $\phi_0 \circ \sigma = \varphi \circ \phi_0$ sağlanır (Ashraf ve Mohammad, 2015).

4.7.7. Teorem:

R_0 halkası üzerinde tanımlı uzunluğu n olan $(1+2u)$-sabit devirli kodun Gray görüntüsü $\mathbb{Z}_4$ üzerinde tanımlı, uzunluğu $2n$ olan bir devirli koddur (Ashraf ve Mohammad, 2015).

4.7.8. Not:

Bazı durumlarda, $\phi_0^*(c) = (b_0, 2a_0 + b_0, b_1, 2a_1 + b_1, \ldots, b_{n-1}, 2a_{n-1} + b_{n-1})$ ile tanımlanan ϕ_0'nin permütasyon versiyonunu kullanmak daha uygundur. ϕ_0 ve ϕ_0^* kullanılarak elde edilen kodlar birbirine denktir.

4.7.9. Önerme:

φ, R_0^n üzerinde devirli öteleme olsun. Bu durumda, $\phi_0^* \circ \varphi = \varphi^2 \circ \phi_0^*$ sağlanır.

4.7.10. Teorem:

n pozitif tek tam sayı olmak üzere, R_0 halkası üzerinde tanımlı devirli bir kodun Gray görüntüsü, $\mathbb{Z}_4$ üzerinde tanımlı, uzunluğu $2n$ olan devirli bir koda denktir.

4.8. R_3 Halkası Üzerinde Tanımlı Uzunluğu Tek Olan $(1+2u)$-Sabit Devirli Kodlar ile Devirli Kodlar Arasındaki İlişki

Bu bölümde, $u^2 = 3$ olmak üzere R_3 halkası üzerindeki $(1+2u)$-sabit devirli kodlarla devirli kodlar arasındaki ilişkiler verilmiştir. Öncelikle R_3 halkasının karakteristiği 4 olduğundan;

$$(1+2u)^n = \begin{cases} 1; & n \text{ çift ise} \\ 1+2u; & n \text{ tek ise} \end{cases}$$

biçiminde tanımlanır. Bu sonuç doğrultusunda aşağıdaki önerme sağlanır.

4.8.1. Önerme:

$$\mu_3 : R_3[x]/\langle x^n - 1\rangle \to R_3[x]/\langle x^n - (1+2u)\rangle$$
$$\overline{c(x)} \mapsto \mu_3\left(\overline{c(x)}\right) = \overline{c((1+2u)x)}$$

dönüşümü tanımlansın. n tek olması durumunda, μ_3 bir halka izomorfizmasıdır (Bag vd., 2018).

4.8.2. Sonuç:

n pozitif tek tam sayı olsun. I kümesinin $R_3[x]/\langle x^n - 1\rangle$ halkasının bir ideali olması için gerekli ve yeterli koşul $\mu_3(I)$ kümesinin $R_3[x]/\langle x^n - (1+2u)\rangle$ halkasının bir ideali olmasıdır (Bag vd., 2018).

4.8.3. Sonuç:

n pozitif tek bir tam sayı ve C, R_3^n kümesinin bir alt kümesi olsun. $\overline{\mu_3}$ permütasyonu R_3^n kümesi üzerinde,

$$\overline{\mu_3}(c_0, c_1, \dots, c_{n-1}) = (c_0, (1+2u)c_1, (1+2u)^2 c_2, \dots, (1+2u)^{n-1} c_{n-1})$$

biçiminde tanımlansın. Bu durumda, C'nin devirli bir kod olması için gerekli ve yeterli koşul $\overline{\mu_3}(C)$'nin $(1+2u)$-sabit devirli bir kod olmasıdır (Bag vd., 2018).

4.9. R_3 Halkası Üzerinde Tanımlı Gray Dönüşüm, $(1+2u)$-Sabit Devirli Kodlar ve Tek Uzunluklu Devirli Kodların Gray Görüntüleri

4.9.1. Tanım:

$a, b \in \mathbb{Z}_4, u^2 = 3$, olmak üzere R_3 üzerinde,

$$\phi_3 : R_3 \to \mathbb{Z}_4^2$$
$$a + ub \mapsto (a, a+2b) \quad \text{ve}$$

ϕ_3': $R_3 \to \mathbb{Z}_4^2$

$a + ub \mapsto (a + 2b, 3a)$

şeklinde tanımlanan iki dönüşüme ‘‘*Gray dönüşümleri*’’ denir (Bag vd., 2018).

4.9.2. Not:

$0 \leq i \leq n-1$ ve $c_i = a_i + ub_i$ olmak üzere herhangi bir $(c_0, c_1, \dots, c_{n-1}) \in R_3^n$ için ϕ_3 ve ϕ_3' Gray dönüşümleri,

$$\phi_3 : R_3^n \to \mathbb{Z}_4^{2n}$$

$$(c_0, c_1, \dots, c_{n-1}) \mapsto \phi_3(c_0, c_1, \dots, c_{n-1})$$

$$= (a_0, a_1, \dots, a_{n-1}, a_0 + 2b_0, a_1 + 2b_1, \dots, a_{n-1} + 2b_{n-1}) \quad \text{ve}$$

$$\phi_3': R_3 \to \mathbb{Z}_4^2$$

$$(c_0, c_1, \dots, c_{n-1}) \mapsto \phi_3'(c_0, c_1, \dots, c_{n-1})$$

$$= (a_0 + 2b_0, a_1 + 2b_1, \dots, a_{n-1} + 2b_{n-1}, 3a_0, 3a_1, \dots, 3a_{n-1})$$

biçiminde R_3^n kümesine genişletilebilir.

4.9.3.Önerme:

φ ve σ sırasıyla, R_3^n üzerinde devirli ve $(1 + 2u)$-sabit devirli öteleme olsun. Bu durumda, $\phi_3 \circ \sigma = \varphi \circ \phi_3$ sağlanır (Bag vd., 2018).

4.9.4. Teorem:

R_3 halkası üzerinde, uzunluğu n olan $(1 + 2u)$-sabit devirli kodun Gray görüntüsü $\mathbb{Z}_4$üzerinde tanımlı, uzunluğu $2n$ olan bir devirli koddur (Bag vd., 2018).

4.9.5. Not:

Bazı durumlarda, $\phi_3'^*(c) = (a_0 + 2b_0, 3a_0, a_1 + 2b_1, 3a_1, \ldots, a_{n-1} + 2b_{n-1}, 3a_{n-1})$ ile tanımlanan ϕ_3''ın permütasyon versiyonunu kullanmak daha uygundur. ϕ_3' ve $\phi_3'^*$ kullanılarak elde edilen kodlar birbirine denktir.

4.9.6. Önerme:

φ, R_3^n üzerinde devirli öteleme olsun. Bu durumda, $\phi_3'^* \circ \varphi = \varphi^2 \circ \phi_3'^*$ sağlanır (Bag vd., 2018).

4.9.7. Teorem:

n tek tam sayı olmak üzere, R_3 halkası üzerinde tanımlı uzunluğu n olan devirli bir kodun Gray görüntüsü, $\mathbb{Z}_4$ üzerinde tanımlı, uzunluğu $2n$ ve indeksi 2 olan bir quasicyclic koda denktir (Bag vd., 2018).

BÖLÜM 5

R_1 VE R_u HALKALARI ÜZERİNDE TANIMLI DEVİRLİ DNA KODLAR

Deoksiribonükleik asit (DNA), yaşamın yapısı ve biyolojik gelişimi için genetik bilgiler içerir. Biyolojik hücrenin nasıl çalıştığı, yeniden ürettiği ve kendini onardığı konusunda bilgi sahibidir. DNA iplikçikleri dört ana nükleotid olan A (Adenin), T (Timin), G (Guanin) ve C (Sitozin)'den oluşur. İki DNA zinciri, Watson-Crick Tamamlayanı (WCC) adı verilen bir kural ile birbirlerine eşlenir. WCC kuralına göre, her bir A ile her bir T ve her bir G ile her bir C birbirine eşlenir. Kısaca $\bar{A} = T, \bar{T} = A, \bar{G} = C$ ve $\bar{C} = G$ dir.

DNA dizilerindeki matematiksel özellikler, birçok araştırmacıya biyoloji ve cebirsel kodlama teorisini kullanarak disiplinler arası keşif için ilham kaynağı olmuştur. DNA iplikçiklerini kullanarak hesaplama yapabilmek için, birtakım özelliklere sahip bir DNA dizi kümesi gerekmektedir.

İlk DNA hesaplama fikri 1987 yılında Tom Head tarafından ortaya atılmıştır. Fakat ilk deneysel çalışma L. Adleman tarafından yapılmıştır. Adleman 1994 yılında, test tüpünde zor bir Hamilton yolu hesaplama probleminin bir örneğini çözmek için DNA moleküllerinin kullanımını içeren bir deney başlatmıştır. Çalışması DNA iplikçiklerinin WCC özelliklerine dayanmaktadır. Bazı çalışmalarda, hibritleşme yoluyla birbirleri ile istenmeyen bağlar oluşturma olasılığı düşük olan bir dizi DNA kod sözcüğü oluşturmak için farklı teknikler geliştirilmiştir.

Herhangi bir uygulamada DNA kodlarını kullanabilmek için dört farklı kısıtlama mevcuttur. Bunlar, Hamming kısıtlaması, ters sıralı kısıtlaması, ters sıralı tamamlayan

kısıtlaması ve sabit GC içeriği kısıtlamasıdır. İlk üç kısıtlama, farklı iplikçikler arasında istenmeyen hibritleşmeyi önlemek içindir. Sabit GC içeriği kısıtlaması, tüm kod sözcükleri arasında benzer termodinamik özelliklere sahip olmasını sağlar.

DNA iplikçiklerinin tasarımının genetik ve biyo-mühendislik alanlarında birçok uygulaması vardır. Örneğin, biyomoleküler hesaplamanın uygulanması, mutasyonel analiz için DNA iplikçiklerinin tasarımıdır. DNA iplikçikleri, her bir iplikçiğin WCC dizisi ile benzersiz bir şekilde eşleşeceği şekilde tasarlanmıştır. DNA iplikçikleri, belirlenmiş minimum Hamming uzaklığına sahip büyük miktarda DNA kod sözcüğü oluşturmaya odaklanır.

Son zamanlarda, silikon bazlı hesaplama sistemlerinden daha fazla depolama kapasitesine sahip DNA tabanlı veri depolama sistemleri birçok araştırmacının dikkatini çekmiştir. DNA molekülünün bu elverişli yapısı sonlu cisimler ve sonlu halkalar üzerinde tanımlı kodlar ile ilişkilendirilmiştir. DNA devirli kodlarının yapımı, (Abualrub vd., 2006), (Bayram vd., 2015), (Bennenni vd., 2015), (Gaborit & King, 2005), (Ling & Wang, 2015), (Siap vd., 2009), (Pattanayak & Singh, 2015) ve (Yildiz & Siap, 2012)'de birçok yazar tarafından tartışılmıştır. (Gaboit & King, 2005)'de DNA kodlarının lineer yapılarını araştırdılar. (Abualrub vd., 2006)'da, 4 elemanlı sonlu cisim olan $GF(4)$ üzerindeki DNA kodlarını çalıştılar. Daha sonra, (Siap vd., 2009)'da $\mathbb{F}_2[v]/\langle v^2-1\rangle$, (Liang & Wang, 2015)'de $\mathbb{F}_2+v\mathbb{F}_2$ halkaları ve (Yildiz & Siap, 2012)'de $\mathbb{F}_2[v]/\langle v^4-1\rangle$ halkası üzerinde DNA kodlar ile çalışmıştır. Ardından, bu çalışmalar (Bayram vd., 2015)'de $v^2=v$ olan 16 elemanlı $\mathbb{F}_4+v\mathbb{F}_4$ sonlu halkaları üzerine taşınmıştır. Farklı eleman sayılarına sahip sonlu halkalar üzerindeki çalışmalar günümüze kadar devam etmiştir. (Zhu & Chen, 2015)'de $\mathbb{F}_2[u,v]/\langle u^2, v^2-v, uv-vu\rangle$ halkası, (Bennenni vd., 2015)'de $\mathbb{F}_2[v]/\langle v^6\rangle$ halkası , (Yildiz & Aydin, 2014) ve (Yildiz & Karadeniz, 2014)'da $v^2=0$ olan $\mathbb{Z}_4+v\mathbb{Z}_4$ halkası ve (Özen vd., 2016)'de $v^2=1$ olan $\mathbb{Z}_4+v\mathbb{Z}_4$ halkası üzerindeki DNA kodlarını ele almışlardır.

Tezin bu bölümünde, *3.Bölüm*'de tanıtılan 16 elemanlı R_1 ve R_u sonlu halkaları üzerindeki çalışmalar iki alt başlıkta verilmektedir. Her iki alt başlıkta da, ilgili halkalar üzerindeki devirli kod yapıları, bu yapılar üzerindeki devirli DNA kodlarının inşası, ters sıralı kısıtlaması, ters sıralı tamamlayan kısıtlaması ve devirli DNA kodların DNA

görüntüleri ile ilgili teorem ve sonuçlar ve farklı uzunluktaki devirli DNA kodlarına bazı örnekler verilmektedir.

5.1. R_1 Halkası Üzerinde Tanımlı Devirli DNA Kodlar

$u^2 = 1$ olmak üzere R_1 Halkasının cebirsel özellikleri *3.2.Bölüm*'de verilmiş idi. Bu bölümde, H.Q.Dinh ve arkadaşları tarafından belirlenen $u^2 = 1$ olmak üzere R_1 Halkası üzerinde tanımlı uzunluğu n olan devirli kodların ters sıralı ve ters sıralı tamamlayan olması için gerekli ve yeterli koşullar verilmiştir.

Ayrıca bu bölümde, $u^2 = 1$, olmak üzere R_1 halkası üzerinde Gray dönüşümü,

$$\phi: R_1 \to \mathbb{Z}_4^2$$
$$a + ub \mapsto (a, b)$$

biçiminde tanımlanır.

5.1.1. R_1 Halkası Üzerinde Tanımlı Devirli Kodlar

5.1.1.1. Not:

C, R_1 halkası üzerinde tanımlı uzunluğu n olan devirli bir kod olmak üzere,

$\pi: R_1^n \to R_1[x]/\langle x^n - 1\rangle$ bir R-modül izomorfizması olduğundan, $\pi(C), R_1[x]/\langle x^n - 1\rangle$ halkasının bir idealidir.

5.1.1.2.Teorem:

n tek tam sayı olmak üzere, C, R_1 halkası üzerinde tanımlı uzunluğu n olan devirli bir kod olsun. Bu durumda,

i) $a_1(x)$ ve $a_3(x)$, $\mathbb{Z}_4$ üzerinde tanımlı devirli kodların üreteç polinomları ve $a_3(x) \mid a_1(x) \mid (x^n - 1)$ olmak üzere $\pi(C) = \langle a_1(x) + (1+u)a_2(x), (1+u)a_3(x) \rangle$ şeklindedir.

ii) Eğer $a_1(x) = a_3(x)$ ise, bu durumda $\pi(C) = \langle a_1(x) + (1+u)a_2(x) \rangle$ dir (Dinh vd., 2018).

5.1.2. R_1 Halkası Üzerinde Tanımlı Devirli DNA Kodlar

DNA alfabesi $S_{D_4} = \{A, T, G, C\}$ ile gösterilsin. $x_i \in \{A, T, G, C\}$ olmak üzere, $(x_0, x_1, \dots, x_{n-1})$ kod sözcükleri kümesi uzunluğu n olan bir DNA kodu olarak tanımlanır. $\mathbb{Z}_4$'ün elemanları $0 \to A$, $1 \to T$, $2 \to G$ ve $3 \to C$ olacak şekilde S_{D_4} kümesinin elemanlarına birebir eşlenir. Bu dönüşüm, *5.2. Bölüm*'de tanımlanan Gray dönüşümü ve $\theta: R_1 \to {S_{D_4}}^2 = S_{D_{16}}$ dönüşümü yardımı ile R_1 halkasının elemanlarına karşılık gelen DNA çiftleri tablosu *Çizelge 5.1*'de verilmiştir. DNA çiftleri kümesi ${S_{D_4}}^2 = S_{D_{16}} = \{AA, TA, GA, CA, AT, AG, AC, TT, GT, CT, TG, GG, CG, TC, GC, CC\}$ olmak üzere; S_{D_4} kümesindeki elemanların Watson-Crick tamamlayanları; $\overline{A} = T, \overline{T} = A, \overline{G} = C, \overline{C} = G$ idi. Benzer şekilde $S_{D_{16}}$ kümesindeki elemanların Watson-Crick tamamlayanları; $\overline{AA} = TT, \overline{TA} = AT, \overline{GA} = CT, \dots, \overline{TC} = AG, \overline{GC} = CG, \overline{CC} = GG\}$ şeklindedir.

Çizelge 5.1 R_1 Halkasının Elemanlarına Karşılık Gelen DNA Çiftleri

R_1 Halkasının Elemanları $r = a + ub$	**Gray Görüntüleri** $\phi(r) = (a, b)$	**DNA Çiftleri** $\theta(r)$
0	(0,0)	AA
1	(1,0)	TA
2	(2,0)	GA
3	(3,0)	CA
u	(0,1)	AT
$2u$	(0,2)	AG
$3u$	(0,3)	AC
$1 + u$	(1,1)	TT
$2 + u$	(2,1)	GT
$3 + u$	(3,1)	CT
$1 + 2u$	(1,2)	TG
$2 + 2u$	(2,2)	GG
$3 + 2u$	(3,2)	CG
$1 + 3u$	(1,3)	TC
$2 + 3u$	(2,3)	GC
$3 + 3u$	(3,3)	CC

5.1.3. R_1 Halkası Üzerinde Tanımlı Ters Sıralı Kodlar

Bu bölümde, n uzunluğu pozitif tek tam sayı alınacaktır. Ayrıca R_1 halkası üzerinde tanımlı, uzunluğu olan devirli bir kodun ters sıralı olması için gerekli ve yeterli koşullar verilmiştir.

5.1.3.1. Lemma:

$\text{der}\, a(x) \geq \text{der}\, b(x)$ olmak üzere, $a(x), b(x) \in R_1[x]$ olsun. Bu durumda;

i) $[a(x).b(x)]^* = a^*(x).b^*(x)$

ii) $[a(x) + b(x)]^* = a^*(x) + x^{\text{der}\, a(x) - \text{der}\, b(x)}.b^*(x)$ dir (Dinh vd., 2018).

5.1.3.2. Lemma:

$\pi(C) = \langle \overline{c(x)} \rangle$, $\mathbb{Z}_4[x]/\langle x^n - 1 \rangle$ halkasının bir ideali olsun. Bu durumda, C'nin ters sıralı olması için gerekli ve yeterli koşul $c(x)$ polinomunun self-reciprocal olmasıdır (Dinh vd., 2018).

Kanıt:

$i = 0,1, \dots, n-1$ ve $c_i \in \mathbb{Z}_4$ olmak üzere $c(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1} \in \pi(C)$ olsun. C ters sıralı olsun. Bu durumda $(c_{n-1}, c_{n-2}, \dots, c_1, c_0) \in C$ olur. Ayrıca $c(x)^* = c_{n-1} + c_{n-2}x + \cdots + c_1x^{n-2} + c_0x^{n-1} \in \pi(C)$ dir. Bu sebeple C ters sıralı ise $c(x)$ polinomu self-reciprocaldir. Benzer şekilde, $c(x)$ polinomu self-reciprocal ise bu durumda C'nin ters sıralı olduğu görülür.

5.1.3.3. Teorem:

n pozitif tek tam sayı olmak üzere $\pi(C) = \langle a_1(x) + (1+u)a_2(x) \rangle$, $R_1[x]/\langle x^n - 1 \rangle$ halkasının bir ideali olsun. Bu durumda C'nin ters sıralı olması için gerekli ve yeterli koşul;

i) $a_1(x)$'in self-reciprocal polinom,

ii) Eğer $i = \text{der}\, a_1(x) - \text{der}\, a_2(x) \geq 0$ ise $a_1(x) \mid (x^i a_2{}^*(x) - a_2(x))$ ya da

$i = \operatorname{der} a_2(x) - \operatorname{der} a_1(x) > 0$ ise $a_1(x) \mid (a_2^*(x) - x^i a_2(x))$ olmasıdır (Dinh vd., 2018).

Kanıt:

i) C, R_1 halkası üzerinde tanımlı ters sıralı bir kod olsun. Böylece, $\pi(C) = \langle a_1(x) + (1+u)a_2(x) \rangle$, $\pi(C)$ kodunun $mod(1+u)$ ye göre eşiti $\langle a_1(x) \rangle$ dir. $a_1(x).h(x) \in \pi(C) mod(1+u)$ olsun. $\big(a_1(x) + (1+u)a_2(x)\big).h(x) \in \pi(C)$ ve C ters sıralı olduğundan,

$$[\big(a_1(x) + (1+u)a_2(x)\big).h(x)]^* \in \pi(C) \Rightarrow \Big({a_1}^*(x) + (1+u)x^i {a_2}^*(x)\Big).h^*(x) \in \pi(C)$$

$$\Rightarrow {a_1}^*(x).h^*(x) = (a_1(x).h(x))^* \in \pi(C)\ mod(1+u)$$

biçiminde yazılır. Bu durumda, $\pi(C)\ mod(1+u) = \langle a_1(x) \rangle$'in ters sıralı olmasını gerektirir. Böylece, *5.1.3.2. Lemma*'dan $a_1(x)$ self-reciprocal olur.

ii) Sırasıyla, $i = \operatorname{der} a_1(x) - \operatorname{der} a_2(x) \geq 0$ ve $i = \operatorname{der} a_2(x) - \operatorname{der} a_1(x) > 0$ olması durumlarını inceleyelim.

<u>Durum 1:</u> $i = \operatorname{der} a_1(x) - \operatorname{der} a_2(x) \geq 0$ olsun.

$a_1(x)$ self-reciprocal olduğundan,

$$\big(a_1(x) + (1+u)a_2(x)\big)^* = {a_1}^*(x) + (1+u)x^i {a_2}^*(x) = a_1(x) + (1+u)x^i {a_2}^*(x) \quad (1)$$

olur. C ters sıralı olduğundan, $b(x) \in R_1[x]$ olmak üzere;

$$\big(a_1(x) + (1+u)a_2(x)\big)^* = [a_1(x) + (1+u)a_2(x)].b(x) \quad (2)$$

dir. (1) ve (2)' den aşağıdaki denklem elde edilir.

$$a_1(x) + (1+u)x^i {a_2}^*(x) = [a_1(x) + (1+u)a_2(x)].b(x) \quad (3)$$

(3) Eşitliğinin her iki tarafını $2(1+u)$ ile çarparsak $2(1+u)a_1(x)\big(1 - b(x)\big) = 0$ elde edilir.

$b(x) \in R_1[x]$ olduğundan, $b_1(x), b_2(x) \in \mathbb{Z}_4[x]$ olmak üzere, $b(x) = b_1(x) + (1+u)b_2(x)$ biçiminde yazılır. Bu durumda,

$2(1+u)a_1(x)\big(1 - b_1(x) - (1+u)b_2(x)\big) = 0$

$\Rightarrow 2(1+u)a_1(x)\big(1 - b_1(x)\big) = 0$

$\Rightarrow 2a_1(x)\big(1 - b_1(x)\big) = 0, a_1(x), b_1(x) \in \mathbb{Z}_4[x]$

$\Rightarrow 1 - b_1(x) \in Ann\big(2a_1(x)\big)$

$\Rightarrow 1 - b_1(x) = (2 + (x^n - 1)/a_1(x)).h(x), h(x) \in \mathbb{Z}_4[x]$

$\Rightarrow b_1(x) = 1 - (2 + (x^n - 1)/a_1(x)).h(x)$

olur. Böylece, $b(x) = 1 - (2 + (x^n - 1)/a_1(x)).h(x) + (1+u)b_2(x)$ elde edilir. Şimdi (3) Eşitliğinde $b(x)$'i yerine yazalım.

$a_1(x) + (1+u)x^i a_2{}^*(x) = a_1(x)[1 - (2 + (x^n - 1)/a_1(x)).h(x) + (1+u)b_2(x)] + (1+u)a_2(x)[1 - (2 + (x^n - 1)/a_1(x)).h(x) + (1+u)b_2(x)]$ (4)

elde edilir. (4) eşitliğinin her iki tarafını $2a_1(x)$ ile çarparsak;

$2a_1{}^2(x) + 2a_1(x)(1+u)x^i a_2{}^*(x) = 2a_1{}^2(x)[1 - (2 + (x^n - 1)/a_1(x)).h(x) + (1+u)b_2(x)] + (1+u)a_2(x)2a_1(x)[1 - (2 + (x^n - 1)/a_1(x)).h(x) + (1+u)b_2(x)]$

$\Rightarrow 2a_1{}^2(x) + 2a_1(x)(1+u)x^i a_2{}^*(x) = 2a_1{}^2(x) + 2(1+u)a_1{}^2(x)b_2(x) + 2a_1(x)(1+u)a_2(x)$

$\Rightarrow 2a_1(x)(1+u)x^i a_2{}^*(x) = 2(1+u)a_1{}^2(x)b_2(x) + 2(1+u)a_1(x)a_2(x)$

$\Rightarrow 2(1+u)a_1(x)(x^i a_2{}^*(x) - a_2(x)) = 2(1+u)a_1{}^2(x)b_2(x)$

elde edilir. Bu sebeple, $a_1(x) \mid (x^i a_2{}^*(x) - a_2(x))$ elde edilir.

Durum 2: $i = \deg a_2(x) - \deg a_1(x) > 0$ olsun.

Bu durumda, $\pi(C) = \langle (1+u)a_2(x) + a_1(x) \rangle$ olarak yazabiliriz. $a_1(x)$ self-reciprocal olduğundan,

$$((1+u)a_2(x) + a_1(x))^* = (1+u){a_2}^*(x) + x^i {a_1}^*(x) = (1+u){a_2}^*(x) + x^i a_1(x) \quad (5)$$

olur. C ters sıralı kod olduğundan, $b(x) \in R_1[x]$ olmak üzere;

$$((1+u)a_2(x) + a_1(x))^* = \big((1+u)a_2(x) + a_1(x)\big).b(x) \quad (6)$$

olur. (5) ve (6)' dan aşağıdaki denklem elde edilir.

$$(1+u){a_2}^*(x) + x^i a_1(x) = \big((1+u)a_2(x) + a_1(x)\big).b(x) \quad (7)$$

(7) Eşitliğinin her iki tarafını $2(1+u)$ ile çarparsak $2(1+u)a_1(x)(x^i - b(x)) = 0$ elde edilir.

$b(x) \in R_1[x]$ olduğundan, $b_1(x), b_2(x) \in \mathbb{Z}_4[x]$ olmak üzere, $b(x) = b_1(x) + (1+u)b_2(x)$ biçiminde yazılır. Bu durumda,

$$2(1+u)a_1(x)\big(x^i - b_1(x) - (1+u)b_2(x)\big) = 0$$

$$\Rightarrow 2(1+u)a_1(x)(x^i - b_1(x)) = 0$$

$$\Rightarrow 2a_1(x)(x^i - b_1(x)) = 0, a_1(x), b_1(x) \in \mathbb{Z}_4[x]$$

$$\Rightarrow x^i - b_1(x) \in Ann(2a_1(x))$$

$$\Rightarrow x^i - b_1(x) = (2 + (x^n - 1)/a_1(x)).h(x), h(x) \in \mathbb{Z}_4[x]$$

$$\Rightarrow b_1(x) = x^i - (2 + (x^n - 1)/a_1(x)).h(x)$$

olur. Böylece, $b(x) = x^i - (2 + (x^n - 1)/a_1(x)).h(x) + (1+u)b_2(x)$ elde edilir. Şimdi (7) Eşitliğinde $b(x)$'i yerine yazalım.

$$(1+u){a_2}^*(x) + x^i a_1(x) = (1+u)a_2(x)\big[x^i - (2 + (x^n - 1)/a_1(x)).h(x) + (1+u)b_2(x)\big] + a_1(x)[x^i - (2 + (x^n - 1)/a_1(x)).h(x) + (1+u)b_2(x)] \quad (8)$$

elde edilir. (8) eşitliğinin her iki tarafını $2a_1(x)$ ile çarparsak;

$2a_1(x)(1+u){a_2}^*(x) + 2x^i {a_1}^2(x) = 2a_1(x)(1+u)a_2(x)\big[x^i - (2 + (x^n-1)/a_1(x)).h(x) + (1+u)b_2(x)\big] + 2{a_1}^2(x)[x^i - (2 + (x^n-1)/a_1(x)).h(x) + (1+u)b_2(x)]$

$\Rightarrow 2a_1(x)(1+u){a_2}^*(x) + 2x^i {a_1}^2(x) = 2a_1(x)(1+u)a_2(x)x^i + 2x^i {a_1}^2(x) + 2{a_1}^2(x)(1+u)b_2(x)$

$\Rightarrow 2a_1(x)(1+u){a_2}^*(x) = 2a_1(x)(1+u)a_2(x)x^i + 2{a_1}^2(x)(1+u)b_2(x)$

$\Rightarrow 2(1+u)a_1(x)\left({a_2}^*(x) - x^i a_2(x)\right) = 2(1+u){a_1}^2(x)b_2(x)$

elde edilir. Bu sebeple, $a_1(x) \mid ({a_2}^*(x) - x^i a_2(x))$ olur.

Bu durumda, i) ve ii) sağlanır.

Diğer taraftan, i) ve ii) sağlansın. Bu durumda,

$\big(a_1(x) + (1+u)a_2(x)\big)^* = {a_1}^*(x) + (1+u)x^i {a_2}^*(x)$

$= a_1(x) + (1+u)a_2(x) - (1+u)a_2(x) + (1+u)x^i {a_2}^*(x)$

$= \big(a_1(x) + (1+u)a_2(x)\big) + (1+u)(x^i {a_2}^*(x) - a_2(x)) \in \pi(C)$

olur. $a_1(x) \mid (x^i {a_2}^*(x) - a_2(x))$ olduğundan, $h(x) \in \mathbb{Z}_4[x]$ için $\left(x^i {a_2}^*(x) - a_2(x)\right) = a_1(x).h(x)$ elde edilir. Böylece,

$(1+u)\left(x^i {a_2}^*(x) - a_2(x)\right) = (1+u)a_1(x).h(x) \in \pi(C)$ ve

$(a_1(x) + (1+u)a_2(x))^* = \big(a_1(x) + (1+u)a_2(x)\big) + (1+u)a_1(x).h(x) \in \pi(C)$

dir. Bunun bir sonucu olarak, C ters sıralıdır.

5.1.3.4. Teorem:

n pozitif tek tam sayı olsun. $a_3(x) \mid a_1(x) \mid (x^n - 1)$ ve $a_2(x) \in R_1[x]$ olmak üzere $\pi(C) = \langle a_1(x) + (1+u)a_2(x), (1+u)a_3(x) \rangle$, $R_1[x]/\langle x^n - 1 \rangle$ halkasının bir ideali olsun. Bu durumda C'nin ters sıralı olması için gerekli ve yeterli koşul;

i) $a_1(x)$ ve $a_3(x)$'ün self-reciprocal,

ii) Eğer $i = \operatorname{der} a_1(x) - \operatorname{der} a_2(x) \geq 0$ ise $a_3(x) \mid (x^i a_2{}^*(x) - a_2(x))$ ya da

$i = \operatorname{der} a_2(x) - \operatorname{der} a_1(x) > 0$ ise $a_3(x) \mid (a_2{}^*(x) - x^i a_2(x))$ olmasıdır (Dinh vd., 2018).

Kanıt:

i) $\pi(C) = \langle a_1(x) + (1+u)a_2(x), (1+u)a_3(x) \rangle$, ters sıralı bir kod olsun. Bu durumda, $\langle a_1(x) \rangle$ ve $\langle a_3(x) \rangle$, $\mathbb{Z}_4$ halkası üzerinde tanımlı ters sıralı kodlardır. Böylece, *5.1.3.2. Lemma*'dan $a_1(x)$ ve $a_3(x)$ self-reciprocal polinomlardır.

ii) Sırasıyla, $i = \operatorname{der} a_1(x) - \operatorname{der} a_2(x) \geq 0$ ve $i = \operatorname{der} a_2(x) - \operatorname{der} a_1(x) > 0$ olması durumlarını inceleyelim.

<u>Durum 1:</u> $i = \operatorname{der} a_1(x) - \operatorname{der} a_2(x) \geq 0$ olsun.

$a_1(x)$ self reciprocal olduğundan,

$$\big(a_1(x) + (1+u)a_2(x)\big)^* = a_1{}^*(x) + (1+u)x^i a_2{}^*(x) = a_1(x) + (1+u)x^i a_2{}^*(x) \quad (1)$$

olur. C ters sıralı olduğundan, $b(x)$ ve $c(x) \in R_1[x]$ olmak üzere,

$$\big(a_1(x) + (1+u)a_2(x)\big)^* = \big(a_1(x) + (1+u)a_2(x)\big)b(x) + \big((1+u)a_3(x)\big)c(x) \quad (2)$$

dir. (1) ve (2)' den aşağıdaki denklem elde edilir.

$$a_1(x) + (1+u)x^i a_2{}^*(x) = \big(a_1(x) + (1+u)a_2(x)\big)b(x) + \big((1+u)a_3(x)\big)c(x) \quad (3)$$

(3) Eşitliğinin her iki tarafını $2(1+u)$ ile çarparsak $2(1+u)a_1(x)\big(1-b(x)\big)=0$ elde edilir.

$b(x) \in R_1[x]$ üzerinde bir polinom olduğundan, $b_1(x), b_2(x) \in \mathbb{Z}_4[x]$ olmak üzere, $b(x)=b_1(x)+(1+u)b_2(x)$ biçiminde yazılır. Bu durumda,

$2(1+u)a_1(x)\big(1-b_1(x)-(1+u)b_2(x)\big)=0$

$\Rightarrow 2(1+u)a_1(x)\big(1-b_1(x)\big)=0$

$\Rightarrow 2a_1(x)\big(1-b_1(x)\big)=0, a_1(x), b_1(x) \in \mathbb{Z}_4[x]$

$\Rightarrow 1-b_1(x) \in Ann\big(2a_1(x)\big)$

$\Rightarrow 1-b_1(x)=(2+(x^n-1)/a_1(x)).h(x), h(x) \in \mathbb{Z}_4[x]$

$\Rightarrow b_1(x)=1-(2+(x^n-1)/a_1(x)).h(x)$

olur. Böylece, $b(x)=1-(2+(x^n-1)/a_1(x)).h(x)+(1+u)b_2(x)$ elde edilir. Şimdi (3) Eşitliğinde $b(x)$'i yerine yazalım.

$$a_1(x)+(1+u)x^i{a_2}^*(x)=a_1(x)[1-(2+(x^n-1)/a_1(x)).h(x)+(1+u)b_2(x)]+(1+u)a_2(x)[1-(2+(x^n-1)/a_1(x)).h(x)+(1+u)b_2(x)]+(1+u)a_3(x)c(x) \quad (4)$$

elde edilir. (4) eşitliğinin her iki tarafını $2a_1(x)$ ile çarparsak;

$2{a_1}^2(x)+2a_1(x)(1+u)x^i{a_2}^*(x)=2{a_1}^2(x)[1-(2+(x^n-1)/a_1(x)).h(x)+(1+u)b_2(x)]+(1+u)a_2(x)2a_1(x)[1-(2+(x^n-1)/a_1(x)).h(x)+(1+u)b_2(x)]+2a_1(x)(1+u)a_3(x)c(x)$

$\Rightarrow 2{a_1}^2(x)+2a_1(x)(1+u)x^i{a_2}^*(x)=2{a_1}^2(x)+2(1+u){a_1}^2(x)b_2(x)+2a_1(x)(1+u)a_2(x)+2a_1(x)(1+u)a_3(x)(c_1(x)+(1+u)c_2(x))$

$\Rightarrow 2a_1(x)(1+u)x^i{a_2}^*(x)=2(1+u){a_1}^2(x)b_2(x)+2(1+u)a_1(x)a_2(x)+2a_1(x)(1+u)a_3(x)c_1(x)$

$\Rightarrow 2(1+u)a_1(x)\left(x^i a_2{}^*(x) - a_2(x)\right) = 2(1+u)a_1{}^2(x)b_2(x) + 2a_1(x)(1+u)a_3(x)c_1(x)$

$\Rightarrow (x^i a_2{}^*(x) - a_2(x)) = a_1(x)b_2(x) + a_3(x)c_1(x)$

elde edilir. $a_3(x) \mid a_1(x)$ olduğundan, $\exists\, h_1(x) \in \mathbb{Z}_4[x]$ için, $a_1(x) = a_3(x)h_1(x)$ biçiminde yazılır. Böylece,

$\left(x^i a_2{}^*(x) - a_2(x)\right) = a_3(x)(h_1(x)b_2(x) + c_1(x))$

olur. Bu sebeple, $a_3(x) \mid (x^i a_2{}^*(x) - a_2(x))$ dir.

Durum 2: $i = \operatorname{der} a_2(x) - \operatorname{der} a_1(x) > 0$ olsun.

Bu durumda, $\pi(C) = \langle (1+u)a_2(x) + a_1(x) \rangle$ olarak yazabiliriz. $a_1(x)$ self-reciprocal olduğundan,

$((1+u)a_2(x) + a_1(x))^* = (1+u)a_2{}^*(x) + x^i a_1{}^*(x) = (1+u)a_2{}^*(x) + x^i a_1(x)$ (5)

dir. C ters sıralı olduğundan, $b(x)$ ve $c(x) \in R_1[x]$ olmak üzere;

$((1+u)a_2(x) + a_1(x))^* = \left((1+u)a_2(x) + a_1(x)\right).b(x) + (1+u)a_3(x)c(x)$ (6)

dir. (5) ve (6)' dan aşağıdaki denklem elde edilir.

$(1+u)a_2{}^*(x) + x^i a_1(x) = \left((1+u)a_2(x) + a_1(x)\right).b(x) + (1+u)a_3(x)c(x)$ (7)

(7) Eşitliğinin her iki tarafını $2(1+u)$ ile çarparsak $2(1+u)a_1(x)(x^i - b(x)) = 0$ elde edilir.

$b(x) \in R_1[x]$ üzerinde bir polinom olduğundan, $b_1(x), b_2(x) \in \mathbb{Z}_4[x]$ olmak üzere, $b(x) = b_1(x) + (1+u)b_2(x)$ biçiminde yazılır. Bu durumda,

$2(1+u)a_1(x)\left(x^i - b_1(x) - (1+u)b_2(x)\right) = 0$

$\Rightarrow 2(1+u)a_1(x)(x^i - b_1(x)) = 0$

$\Rightarrow 2a_1(x)(x^i - b_1(x)) = 0, a_1(x), b_1(x) \in \mathbb{Z}_4[x]$

$\Rightarrow x^i - b_1(x) \in Ann(2a_1(x))$

$\Rightarrow x^i - b_1(x) = (2 + (x^n - 1)/a_1(x)).h(x), h(x) \in \mathbb{Z}_4[x]$

$\Rightarrow b_1(x) = x^i - (2 + (x^n - 1)/a_1(x)).h(x)$

olur. Böylece, $b(x) = x^i - (2 + (x^n - 1)/a_1(x)).h(x) + (1 + u)b_2(x)$ elde edilir. Şimdi (7) Eşitliğinde $b(x)$'i yerine yazalım.

$(1 + u)a_2{}^*(x) + x^i a_1(x) = (1 + u)a_2(x)\left[x^i - (2 + (x^n - 1)/a_1(x)).h(x) + (1 + u)b_2(x)\right] + a_1(x)\left[x^i - (2 + (x^n - 1)/a_1(x)).h(x) + (1 + u)b_2(x)\right] + (1 + u)a_3(x)c(x)$ (8)

elde edilir. (8) eşitliğinin her iki tarafını $2a_1(x)$ ile çarparsak;

$2a_1(x)(1 + u)a_2{}^*(x) + 2x^i a_1{}^2(x) = 2a_1(x)(1 + u)a_2(x)\left[x^i - (2 + (x^n - 1)/a_1(x)).h(x) + (1 + u)b_2(x)\right] + 2a_1{}^2(x)\left[x^i - (2 + (x^n - 1)/a_1(x)).h(x) + (1 + u)b_2(x)\right] + 2a_1(x)(1 + u)a_3(x)c(x)$

$\Rightarrow 2a_1(x)(1 + u)a_2{}^*(x) + 2x^i a_1{}^2(x) = 2a_1(x)(1 + u)a_2(x)x^i + 2x^i a_1{}^2(x) + 2a_1{}^2(x)(1 + u)b_2(x) + 2a_1(x)(1 + u)a_3(x)(c_1(x) + (1 + u)c_2(x))$

$\Rightarrow 2a_1(x)(1 + u)a_2{}^*(x) = 2a_1(x)(1 + u)a_2(x)x^i + 2a_1{}^2(x)(1 + u)b_2(x) + 2a_1(x)(1 + u)a_3(x)c_1(x)$

$\Rightarrow 2(1 + u)a_1(x)\left(a_2{}^*(x) - x^i a_2(x)\right) = 2(1 + u)a_1{}^2(x)b_2(x) + 2a_1(x)(1 + u)a_3(x)c_1(x)$

$\Rightarrow \left(a_2{}^*(x) - x^i a_2(x)\right) = a_1(x)b_2(x) + a_3(x)c_1(x)$

elde edilir. $a_3(x) \mid a_1(x)$ olduğundan, $h_2(x) \in \mathbb{Z}_4[x]$ olmak üzere, $a_1(x) = a_3(x)h_2(x)$ biçiminde yazılır. Böylece,

$\left(a_2{}^*(x) - x^i a_2(x)\right) = a_3(x)(h_2(x)b_2(x) + c_1(x))$

olur. Bu sebeple, $a_3(x) \mid (a_2{}^*(x) - x^i a_2(x))$ olur.

Bu durumda, i) ve ii) sağlanır.

Diğer taraftan, i) ve ii) sağlansın. Bu durumda, $i = derg_1(x) - derg_2(x)$ olmak üzere,

$\left(a_1(x) + (1+u)a_2(x)\right)^* = a_1{}^*(x) + (1+u)x^i a_2{}^*(x)$

$= a_1(x) + (1+u)a_2(x) - (1+u)a_2(x) + (1+u)x^i a_2{}^*(x)$

$= \left(a_1(x) + (1+u)a_2(x)\right) + (1+u)(x^i a_2{}^*(x) - a_2(x)) \in \pi(C)$

dir. $a_3(x) \mid (x^i a_2{}^*(x) - a_2(x))$ olduğundan, $h(x) \in \mathbb{Z}_4[x]$ için $\left(x^i a_2{}^*(x) - a_2(x)\right) = a_3(x).h(x)$ olur. Böylece,

$(1+u)\left(x^i a_2{}^*(x) - a_2(x)\right) = (1+u)a_3(x).h(x) \in \pi(C)$ ve

$(a_1(x) + (1+u)a_2(x))^* = \left(a_1(x) + (1+u)a_2(x)\right) + (1+u)a_3(x).h(x) \in \pi(C)$

bulunur. O halde, C ters sıralıdır.

5.1.4. R_1 Halkası Üzerinde Tanımlı Ters Sıralı Tamamlayan Kodlar

Bu bölümde, R_1 halkası üzerinde tanımlı tek uzunluğa sahip devirli bir kodun ters sıralı tamamlayan olması için gerekli ve yeterli koşullar verilmiştir.

5.1.4.1. Lemma:

Herhangi $a \in R_1$ için,

i) $a + \overline{a} = 1 + u$

ii) $\overline{(1+u)a} = 3(1+u)a + (1+u)$

eşitlikleri sağlanır. Burada herhangi bir $a \in R_1$ için $\bar{a}, a$ elemanının tamamlayanını belirtmektedir (Dinh vd., 2018).

Kanıt:

i) Aşikardır.

ii) (i)'den $(1+u)a + \overline{(1+u)a} = 1+u$ olduğu açıktır.

$$(1+u)a + \overline{(1+u)a} = 1+u \Rightarrow \overline{(1+u)a} = 1+u-(1+u)a$$

$$\Rightarrow \overline{(1+u)a} = 1+u+3(1+u)a \qquad \big(-1 \equiv 3mod(4)\big)$$

Bu durumda $\overline{(1+u)a} = 3(1+u)a + (1+u)$ sağlanır.

5.1.4.2. Lemma:

Herhangi iki $a, b \in R_1$ için,

i) $\overline{a+b} = \overline{a} + \overline{b} + 3(1+u)$

ii) $\overline{a+(1+u)b} = \overline{a} + 3(1+u)b$

eşitlikleri sağlanır (Dinh vd., 2018).

Kanıt:

i) $\overline{a+b} + a + b = 1+u \Rightarrow \overline{a+b} = 1+u-(a+b)$

$$\Rightarrow \overline{a+b} = 1+u+3(a+b) \qquad (1)$$

$$\overline{a} + a + \overline{b} + b = 2(1+u) \Rightarrow \overline{a} + \overline{b} = 2(1+u) - (a+b)$$

$$\Rightarrow \overline{a} + \overline{b} = 2(1+u) + 3(a+b) \qquad (2)$$

Bu durumda, (1) ve (2)'den,

$$\overline{a+b} - (1+u) = \overline{a} + \overline{b} - 2(1+u) \Rightarrow \overline{a+b} = \overline{a} + \overline{b} + 3(1+u)$$

elde edilir.

ii) $\overline{a+(1+u)b} = \overline{a} + \overline{(1+u)b} + 3(1+u)$

$= \overline{a} + 3(1+u)b + (1+u) + 3(1+u)$

$= \overline{a} + 3(1+u)b$

5.1.4.3. Lemma:

Herhangi $a \in R_1$ için, $\overline{a} + 3(1+u) = 3a$ olur (Dinh vd., 2018).

Kanıt:

$a + \overline{a} = 1 + u \Rightarrow \overline{a} = 1 + u - a$

$\Rightarrow \overline{a} - (1+u) = -a$

$\Rightarrow \overline{a} + 3(1+u) = 3a$

Çizelge 5.2 $r = a + ub \in R_1$ Elemanlarına Karşılık Gelen $\overline{r}$ Tamamlayanları Tablosu

$\boldsymbol{r = a + ub \in R_1}$ **Elemanları**	$\boldsymbol{\overline{r}}$ **Tamamlayanları**
0	$1+u$
1	u
2	$3+u$
3	$2+u$
u	1
$2u$	$1+3u$
$3u$	$1+2u$
$1+u$	0
$2+u$	3
$3+u$	2
$1+2u$	$3u$
$2+2u$	$3+3u$
$3+2u$	$2+3u$
$1+3u$	$2u$
$2+3u$	$3+2u$
$3+3u$	$2+2u$

5.1.4.1. Lemma, 5.1.4.2. Lemma ve *5.1.4.3. Lemma*'nın, doğrulandığı *Çizelge 5.2*'den kolayca görülür.

5.1.4.4. Teorem:

n pozitif tek tam sayı olmak üzere, $\pi(C) = \langle a_1(x) + (1+u)a_2(x) \rangle$, $R_1[x]/\langle x^n - 1\rangle$ halkasının bir ideali olsun. Bu durumda C'nin ters sıralı tamamlayan olması için gerekli ve yeterli koşul;

i) $a_1(x)$'in self-reciprocal ve $3(1+u)((1-x^n)/(1-x)) \in \pi(C)$,

ii) Eğer $i = \text{der}\, a_1(x) - \text{der}\, a_2(x) \geq 0$ ise $a_1(x) \mid (x^i a_2{}^*(x) - a_2(x))$ ya da

$i = \text{der}\, a_2(x) - \text{der}\, a_1(x) > 0$ ise $a_1(x) \mid (a_2{}^*(x) - x^i a_2(x))$ olmasıdır (Dinh vd., 2018).

Kanıt:

i) n pozitif tek tam sayı olmak üzere, $\pi(C) = \langle a_1(x) + (1+u)a_2(x) \rangle$, $R_1[x]/\langle x^n - 1\rangle$ halkasının bir ideali olsun. C'de tüm bileşenleri 0 olan **0** kod sözcüğü bulunur. C ters sıralı tamamlayan kod olduğu için $\overline{\mathbf{0}} \in C$ olmalıdır. *5.1.4.1. Lemma*'dan,

$3\overline{(0,0,0,\ldots,0)} = 3(1+u,1+u,\ldots,1+u) \in C \leftrightarrow 3(1+u)((1-x^n)/(1-x)) \in \pi(C)$ dir.

ii)

$a_1(x) = k_0 + k_1 x + \cdots + k_{s-1}x^{s-1} + k_s x^s$ ve

$a_2(x) = l_0 + l_1 x + \cdots + l_{r-1}x^{r-1} + l_r x^r$ olsun.

Durum 1: $i = \text{der}\, a_1(x) - \text{der}\, a_2(x) \geq 0$ yani $s \geq r$ olsun.

$a_1(x) + (1+u)a_2(x) = (k_0 + k_1 x + \cdots + k_{s-1}x^{s-1} + k_s x^s) + (1+u)(l_0 + l_1 x + \cdots + l_{r-1}x^{r-1} + l_r x^r)$

$= (k_0 + (1+u)l_0) + (k_1 + (1+u)l_1)x + \cdots + (k_{r-1} + (1+u)l_{r-1})x^{r-1} + (k_r + (1+u)l_r)x^r + (k_{r+1} + (1+u)l_{r+1})x^{r+1} + \cdots + k_{s-1}x^{s-1} + k_s x^s$

biçiminde yazılır. Bu sebeple,

$(a_1(x) + (1+u)a_2(x))^{RC} = (1+u)(1 + x + \cdots + x^{n-s-2}) + \overline{k_s}x^{n-s-1} + \overline{k_{s-1}}x^{n-s} + \cdots + \overline{k_{r+1}}x^{n-r-2} + \overline{(k_r + (1+u)l_r)}x^{n-r-1} + \overline{(k_{r-1} + (1+u)l_{r-1})}x^{n-r} + \cdots + \overline{(k_1 + (1+u)l_1)}x^{n-2} + \overline{(k_0 + (1+u)l_0)}x^{n-1}$

$= (1+u)(1 + x + \cdots + x^{n-s-2}) + \overline{k_s}x^{n-s-1} + \overline{k_{s-1}}x^{n-s} + \cdots + \overline{k_{r+1}}x^{n-r-2} + \overline{k_r}x^{n-r-1} + 3(1+u)l_r x^{n-r-1} + \overline{k_{r-1}}x^{n-r} + 3(1+u)l_{r-1}x^{n-r} + \cdots + \overline{k_1}x^{n-2} + 3(1+u)\overline{l_1}x^{n-2} + \overline{k_0}x^{n-1} + 3(1+u)\overline{l_0}x^{n-1}$

$= (1+u)(1 + x + \cdots + x^{n-s-2}) + \overline{k_s}x^{n-s-1} + \overline{k_{s-1}}x^{n-s} + \cdots + \overline{k_{r+1}}x^{n-r-2} + \overline{k_r}x^{n-r-1} + \cdots + \overline{k_1}x^{n-2} + \overline{k_0}x^{n-1} + 3(1+u)\overline{l_r}x^{n-r-1} + 3(1+u)\overline{l_{r-1}}x^{n-r} + \cdots + 3(1+u)\overline{l_1}x^{n-2} + 3(1+u)\overline{l_0}x^{n-1} \in \pi(C)$

olur. C lineer olduğundan,

$$(a_1(x) + (1+u)a_2(x))^{RC} + 3(1+u)((1-x^n)/(1-x)) \in \pi(C) \qquad (1)$$

olur. Bu durumda (1)'den,

$\left(a_1(x) + (1+u)a_2(x))^{RC} + 3(1+u)((1-x^n)/(1-x)\right) = (1+u)(1 + x + \cdots + x^{n-s-2}) + \overline{k_s}x^{n-s-1} + \overline{k_{s-1}}x^{n-s} + \cdots + \overline{k_{r+1}}x^{n-r-2} + \overline{k_r}x^{n-r-1} + \cdots + \overline{k_1}x^{n-2} + \overline{k_0}x^{n-1} + 3(1+u)l_r x^{n-r-1} + 3(1+u)l_{r-1}x^{n-r} + \cdots + 3(1+u)l_1 x^{n-2} + 3(1+u)l_0 x^{n-1} + 3(1+u)(1 + x + \cdots + x^{n-1})$

$= \left(\overline{k_s} + 3(1+u)\right)x^{n-s-1} + \left(\overline{k_{s-1}} + 3(1+u)\right)x^{n-s} + \cdots + \left(\overline{k_1}x^{n-2} + 3(1+u)\right)x^{n-2} + \left(\overline{k_0}x^{n-2} + 3(1+u)\right)x^{n-1} + 3(1+u)l_r x^{n-r-1} + 3(1+u)l_{r-1}x^{n-r} + \cdots + 3(1+u)l_1 x^{n-2} + 3(1+u)l_0 x^{n-1}$

$= 3x^{n-s-1}(k_s + k_{s-1}x + \cdots + k_1 x^{s-1} + k_0 x^s) + 3(1+u)x^{n-r-1}(l_r + l_{r-1}x + \cdots + l_1 x^{r-1} + l_0 x^r)$

$= 3x^{n-s-1}{a_1}^*(x) + 3(1+u)x^{n-r-1}{a_2}^*(x)$

$= 3x^{n-s-1}({a_1}^*(x) + (1+u)x^{s-r}{a_2}^*(x))$

elde edilir. $({a_1}^*(x) + (1+u)x^{s-r}{a_2}^*(x)) \in \pi(C)$ olduğundan,

$\left({a_1}^*(x) + (1+u)x^{s-r}{a_2}^*(x)\right) = \left(a_1(x) + (1+u)a_2(x)\right)b(x)$ dir.

$b(x) = 1 - (2 + (x^n - 1)/(x-1))h(x) + (1+u)b_2(x)$

olduğu açıktır. *5.1.3.3. Teorem*'den $a_1(x) = {a_1}^*(x)$ dir. Yani $a_1(x)$ self-reciprocaldir. Ayrıca $i = s - r$ olmak üzere, $a_1(x) \mid (x^i{a_2}^*(x) - a_2(x))$ dir.

Durum 2: $i = \operatorname{der} a_2(x) - \operatorname{der} a_1(x) > 0$ yani $r > s$ olsun.

$(1+u)a_2(x) + a_1(x) = (1+u)(l_0 + l_1x + \cdots + l_{r-1}x^{r-1} + l_rx^r) + (k_0 + k_1x + \cdots + k_{s-1}x^{s-1} + k_sx^s)$

$= \left((1+u)l_0 + k_0\right) + \left((1+u)l_1 + k_1\right)x + \cdots + \left((1+u)l_{s-1} + k_{s-1}\right)x^{s-1} + \left((1+u)l_s + k_s\right)x^s + (1+u)l_{s+1}x^{s+1} + \cdots + (1+u)l_{r-1}x^{r-1} + (1+u)l_rx^r$

biçiminde yazılır. Bu sebeple,

$((1+u)a_2(x) + a_1(x))^{RC} = (1+u)(1 + x + \cdots + x^{n-r-2}) + \overline{(1+u)l_r}x^{n-r-1} + \overline{(1+u)l_{r-1}}x^{n-r} + \cdots + \overline{(1+u)l_{s+1}}x^{n-s-2} + \overline{\left((1+u)l_s + k_s\right)}x^{n-s-1} + \overline{\left((1+u)l_{s-1} + k_{s-1}\right)}x^{n-s} + \cdots + \overline{\left((1+u)l_1 + k_1\right)}x^{n-2} + \overline{((1+u)l_0 + k_0)}x^{n-1}$

$= (1+u)(1 + x + \cdots + x^{n-r-2}) + 3(1+u)l_rx^{n-r-1} + (1+u)x^{n-r-1} + 3(1+u)l_{r-1}x^{n-r} + (1+u)x^{n-r} + \cdots + 3(1+u)l_{s+1}x^{n-s-2} + (1+u)x^{n-s-2} + \overline{k_s}x^{n-s-1} + 3(1+u)l_sx^{n-s-1} + \overline{k_{s-1}}x^{n-s} + 3(1+u)l_{s-1}x^{n-s} + \cdots + \overline{k_1}x^{n-2} + 3(1+u)l_1x^{n-2} + \overline{k_0}x^{n-1} + 3(1+u)l_0x^{n-1}$

$= (1+u)\left(1 + x + \cdots + x^{n-r-2}\right) + (1+u)x^{n-r-1} + (1+u)x^{n-r} + \cdots + (1+u)x^{n-s-2} + 3(1+u)l_rx^{n-r-1} + 3(1+u)l_{r-1}x^{n-r} + \cdots + 3(1+u)l_{s+1}x^{n-s-2} + 3(1+u)l_sx^{n-s-1} +$

$3(1+u)l_{s-1}x^{n-s}+\cdots+3(1+u)l_1x^{n-2}+3(1+u)l_0x^{n-1}+\overline{k_{s-1}}x^{n-s}+\cdots+\overline{k_1}x^{n-2}+\overline{k_0}x^{n-1}$

$=(1+u)(1+x+\cdots+x^{n-r-2})+(1+u)x^{n-r-1}+(1+u)x^{n-r}+\cdots+(1+u)x^{n-s-2}+3(1+u)l_rx^{n-r-1}+3(1+u)l_{r-1}x^{n-r}+\cdots+3(1+u)l_1x^{n-2}+3(1+u)l_0x^{n-1}+\overline{k_s}x^{n-s-1}+\overline{k_{s-1}}x^{n-s}+\cdots+\overline{k_1}x^{n-2}+\overline{k_0}x^{n-1}\in\pi(C)$

olur. C lineer olduğundan,

$$((1+u)a_2(x)+a_1(x))^{RC}+3(1+u)((1-x^n)/(1-x))\in\pi(C) \qquad (2)$$

olur. Bu durumda (2)'den,

$\big((1+u)a_2(x)+a_1(x)\big)^{RC}+3(1+u)((1-x^n)/(1-x)\big)=3(1+u)l_rx^{n-r-1}+3(1+u)l_{r-1}x^{n-r}+\cdots+3(1+u)l_1x^{n-2}+3(1+u)x^{n-1}+(\overline{k_s}+3(1+u))x^{n-s-1}+(\overline{k_{s-1}}+3(1+u))x^{n-s}+\cdots+(\overline{k_1}+3(1+u))x^{n-2}+(\overline{k_0}+3(1+u))x^{n-1}$

$=3(1+u)x^{n-r-1}(l_r+l_{r-1}x+\cdots+l_1x^{r-1}+l_0x^r)+3x^{n-s-1}(k_s+k_{s-1}x+\cdots+k_1x^{s-1}+k_0x^s)$

$=3(1+u)x^{n-r-1}a_2{}^*(x)+3x^{n-s-1}a_1{}^*(x)$

$=3x^{n-r-1}((1+u)a_2{}^*(x)+x^{r-s}a_1{}^*(x))$

elde edilir. $(1+u)a_2{}^*(x)+x^{r-s}a_1{}^*(x)\in\pi(C)$ olduğundan,

$(1+u)a_2{}^*(x)+x^{r-s}a_1{}^*(x)=\big((1+u)a_2(x)+a_1(x)\big)b(x)$ dir.

$b(x)=x^i-(2+(x^n-1)/a_1(x)).h(x)+(1+u)b_2(x)$

olduğu açıktır. *5.1.3.3. Teorem*'den $a_1(x)=a_1{}^*(x)$ dir. Yani $a_1(x)$ self-reciprocaldir. Ayrıca $i=r-s$ olmak üzere, $a_1(x)\mid(a_2{}^*(x)-x^ia_2(x))$ olur.

Bu durumda, i) ve ii) sağlanır.

Diğer taraftan, i) ve ii) sağlansın. Herhangi bir $c(x)\in\pi(C)$ olsun. Bu durumda,

$c(x) = \big(a_1(x) + (1+u)a_2(x)\big)m(x)$ biçiminde yazılabilir.

$a_1(x)$ self-reciprocal ve $i = \operatorname{der} a_1(x) - \operatorname{der} a_2(x)$ olmak üzere $a_1(x) \mid (x^i {a_2}^*(x) - a_2(x))$ ya da $i = \operatorname{der} a_2(x) - \operatorname{der} a_1(x)$ olmak üzere $a_1(x) \mid ({a_2}^*(x) - x^i a_2(x))$ olduğundan, $\operatorname{der} a_1(x) > \operatorname{der} a_2(x)$ ise $b(x) = 1 - (2 + (x^n - 1)/(x-1))h(x) + (1+u)b_2(x)$ ya da $\operatorname{der} a_2(x) \geq \operatorname{der} a_1(x)$ ise $b(x) = x^i - (2 + (x^n - 1)/a_1(x)).h(x) + (1+u)b_2(x)$ olmak üzere,

$c^*(x) = (\big(a_1(x) + (1+u)a_2(x)\big)m(x))^*$

$= ({a_1}^*(x) + (1+u)x^i {a_2}^*(x))m^*(x)$

$= (a_1(x) + (1+u)x^i {a_2}^*(x))m^*(x)$

$= (a_1(x) + (1+u)x^i {a_2}^*(x))b(x)m^*(x)$

olur. Bu sebeple, $c^*(x) \in \pi(C)$ olur. $3(1+u)((1-x^n)/(1-x)) \in \pi(C)$ olduğundan,

$3(1+u)((1-x^n)/(1-x)) = 3(1+u) + 3(1+u)x + \cdots + 3(1+u)x^{n-1} \in \pi(C)$

olur. $c(x) = c_0 + c_1 x + \cdots + c_s x^s \in \pi(C)$ olsun. Bu durumda, C uzunluğu n olan devirli bir kod olduğu için,

$x^{n-s-1}c(x) = c_0 x^{n-s-1} + c_1 x^{n-s} + \cdots + c_s x^{n-1} \in \pi(C)$ dir.

$3(1+u) + 3(1+u)x + \cdots + 3(1+u)x^{n-s-2} + \big(c_0 + 3(1+u)\big)x^{n-s-1} + \big(c_1 + 3(1+u)\big)x^{n-s} + \cdots + \big(c_s + 3(1+u)\big)x^{n-1} = 3(1+u) + 3(1+u)x + \cdots + 3(1+u)x^{n-s-2} + 3\overline{c_0}x^{n-s-1} + 3\overline{c_1}x^{n-s} + \cdots + 3\overline{c_s}x^{n-1} = 3((1+u) + (1+u)x + \cdots + (1+u)x^{n-s-2} + \overline{c_0}x^{n-s-1} + \overline{c_1}x^{n-s} + \overline{c_s}x^{n-1}) \in \pi(C)$

olduğundan, $(c^*(x))^{RC} \in \pi(C)$ olur. Bu sebeple, $((c^*(x))^{RC})^* = c(x)^{RC} \in \pi(C)$ olur. Yani C ters sıralı tamamlayandır.

5.1.4.5. Teorem:

n pozitif tek tam sayı, $a_3(x) \mid a_1(x) \mid (x^n-1)$ olmak üzere $\pi(C) = \langle a_1(x) + (1+u)a_2(x), (1+u)a_3(x) \rangle$, $R_1[x]/\langle x^n-1\rangle$ halkasının bir ideali olsun. Bu durumda C'nin ters sıralı tamamlayan olması için gerekli ve yeterli koşul;

i) $a_1(x)$ ve $a_3(x)$'ün self-reciprocal ve $3(1+u)((1-x^n)/(1-x)) \in \pi(C)$,

ii) Eğer $i = \operatorname{der} a_1(x) - \operatorname{der} a_2(x) \geq 0$ ise $a_3(x) \mid (x^i a_2{}^*(x) - a_2(x))$ ya da

$i = \operatorname{der} a_2(x) - \operatorname{der} a_1(x) > 0$ ise $a_3(x) \mid (a_2{}^*(x) - x^i a_2(x))$ olmasıdır (Dinh vd., 2018).

Kanıt:

i) n pozitif tek tam sayı, $a_3(x) \mid a_1(x) \mid (x^n-1)$ olmak üzere $\pi(C) = \langle a_1(x) + (1+u)a_2(x), (1+u)a_3(x) \rangle$, $R_1[x]/\langle x^n-1\rangle$ halkasının bir ideali olsun. C'de tüm bileşenleri 0 olan **0** kod sözcüğü bulunur, C ters sıralı tamamlayan kod olduğundan $\overline{\mathbf{0}} = \overline{(0,0,\dots,0)} \in C$ dir. *5.1.4.1. Lemma*'dan,

$3\overline{(0,0,0,\dots,0)} = 3(1+u,1+u,\dots,1+u) \in C \leftrightarrow 3(1+u)((1-x^n)/(1-x)) \in \pi(C)$ dir.

ii) n pozitif tek tam sayı, $a_3(x) \mid a_1(x) \mid (x^n-1)$ olmak üzere $\pi(C) = \langle a_1(x) + (1+u)a_2(x), (1+u)a_3(x) \rangle$, $R_1[x]/\langle x^n-1\rangle$ halkasının bir ideali olsun.

$a_1(x) = k_0 + k_1x + \cdots + k_{s-1}x^{s-1} + k_sx^s$ ve

$a_2(x) = l_0 + l_1x + \cdots + l_{r-1}x^{r-1} + l_rx^r$ olsun.

Durum 1: $i = \operatorname{der} a_1(x) - \operatorname{der} a_2(x) \geq 0$ yani $s \geq r$ olsun.

5.2.4.4. Teorem' e benzer şekilde, $(a_1{}^*(x) + (1+u)x^{s-r}a_2{}^*(x)) \in \pi(C)$ bulunur.

$\left(a_1{}^*(x) + (1+u)x^{s-r}a_2{}^*(x)\right) = \left(a_1(x) + (1+u)a_2(x)\right)b(x) + (1+u)a_3(x)c(x)$ ve $b(x) = 1 - (2 + (x^n-1)/(x-1))h(x) + (1+u)b_2(x)$ olduğu kolayca görülür.

5.1.3.4. Teorem'den $a_1(x) = {a_1}^*(x)$ dir. Yani $a_1(x)$ self-reciprocaldir. Ayrıca $i = s - r$ olmak üzere, $a_3(x) \mid (x^i {a_2}^*(x) - a_2(x))$ olur.

Durum 2: $i = \text{der}\, a_2(x) - \text{der}\, a_1(x) > 0$ yani $r > s$ olsun.

5.2.4.4. Teorem' e benzer şekilde, $(1+u){a_2}^*(x) + x^{r-s}{a_1}^*(x) \in \pi(C)$ bulunur. Böylece

$(1+u){a_2}^*(x) + x^{r-s}{a_1}^*(x) = \big((1+u)a_2(x) + a_1(x)\big)b(x) + (1+u)a_3(x)c(x)$ elde edilir. $b(x) = x^i - (2 + (x^n - 1)/a_1(x)).h(x) + (1+u)b_2(x)$ olduğu kolayca görülür.
5.1.3.4. Teorem'den $a_1(x) = {a_1}^*(x)$ dir. Yani $a_1(x)$ self-reciprocaldir. Ayrıca $i = r - s$ olmak üzere, $a_3(x) \mid ({a_2}^*(x) - x^i a_2(x))$ olur.

Bu durumda, i) ve ii) sağlanır.

Diğer taraftan, i) ve ii) sağlansın. Herhangi bir $c(x) \in \pi(C)$ olsun. Bu durumda,

$c(x) = \big(a_1(x) + (1+u)a_2(x)\big)p(x) + (1+u)a_3(x)q(x)$ biçiminde yazılabilir.

$a_1(x)$ ve $a_3(x)$ self-reciprocal olduğundan ve $i = \text{der}\, a_1(x) - \text{der}\, a_2(x) \geq 0$ için $a_3(x) \mid (x^i {a_2}^*(x) - a_2(x))$ ya da $i = \text{der}\, a_2(x) - \text{der}\, a_1(x) > 0$ için $a_3(x) \mid ({a_2}^*(x) - x^i a_2(x))$ olduğundan, $j = \text{der}\,\big(a_1(x)p(x)\big) - \text{der}\,(a_3(x)q(x))$ olmak üzere,

$$c^*(x) = \big(\big(a_1(x) + (1+u)a_2(x)\big)p(x)\big)^* + ((1+u)a_3(x)q(x))^*$$

$$= ({a_1}^*(x) + (1+u)x^i {a_2}^*(x))p^*(x) + (1+u)x^j {a_3}^*(x)q^*(x)$$

$$= \big(a_1(x) + (1+u)a_2(x)\big)p^*(x) + (1+u)m^*(x)\left(x^i {a_2}^*(x) - a_2(x)\right) + (1+u)x^j a_3(x)q^*(x)$$

$$= \big(a_1(x) + (1+u)a_2(x)\big)p^*(x) + (1+u)a_3(x)m(x)$$

dir. Bu sebeple, $c^*(x) \in \pi(C)$ olur. $3(1+u)((1-x^n)/(1-x)) \in \pi(C)$ olduğundan,

$$3(1+u)((1-x^n)/(1-x)) = 3(1+u) + 3(1+u)x + \cdots + 3(1+u)x^{n-1} \in \pi(C)$$

olur. $c(x) = c_0 + c_1x + \cdots + c_sx^s$ olsun. Bu durumda, C uzunluğu n olan devirli bir kod olduğu için,

$x^{n-s-1}c(x) = c_0x^{n-s-1} + c_1x^{n-s} + \cdots + c_sx^{n-1} \in C$ dir.

$3(1+u) + 3(1+u)x + \cdots + 3(1+u)x^{n-s-2} + \big(c_0 + 3(1+u)\big)x^{n-s-1} + \big(c_1 + 3(1+u)\big)x^{n-s} + \cdots + \big(c_s + 3(1+u)\big)x^{n-1} = 3(1+u) + 3(1+u)x + \cdots + 3(1+u)x^{n-s-2} + 3\overline{c_0}x^{n-s-1} + 3\overline{c_1}x^{n-s} + \cdots + 3\overline{c_s}x^{n-1} = 3((1+u) + (1+u)x + \cdots + (1+u)x^{n-s-2} + \overline{c_0}x^{n-s-1} + \overline{c_1}x^{n-s} + \overline{c_s}x^{n-1}) \in \pi(C)$

olduğundan, $(c^*(x))^{RC} \in \pi(C)$ olur. Bu sebeple, $((c^*(x))^{RC})^* = c(x)^{RC} \in C$ olur. Yani C ters sıralı tamamlayandır.

5.1.4.6. Örnek:

$x^3 - 1 = (x-1)(x^2+x+1) = m_1(x).m_2(x) \in \mathbb{Z}_4[x]$ olsun.

i) $a_1(x) = a_2(x) = m_2(x) = (x^2+x+1)$ olmak üzere, $\pi(C) = \langle a_1(x) + (1+u)a_2(x) \rangle$ olsun. Bu durumda, $a_1(x)$'in self-reciprocal ve $i = \text{der}\, a_1(x) - \text{der}\, a_2(x) \geq 0$ olmak üzere, $a_1(x) \mid (x^i a_2{}^*(x) - a_2(x))$ olduğu açıktır. Böylece, C ters sıralı tamamlayan özelliğine sahip uzunluğu 3, minimum Hamming uzaklığı 3 olan bir devirli DNA koddur. C'nin θ dönüşümü altındaki DNA görüntüsü, uzunluğu 6, eleman sayısı 16 ve minimum Hamming uzaklığı 3 olan bir DNA kodudur.

ii) $a_1(x) = a_2(x) = m_1(x).m_2(x)$ ve $a_3(x) = m_2(x)$ olmak üzere, $\pi(C) = \langle a_1(x) + (1+u)a_2(x), (1+u)a_3(x) \rangle$ olsun. Bu durumda, $a_1(x)$ ve $a_3(x)$'in self-reciprocal polinomlar olduğu ve $a_3(x) \mid ((1+u)x^i a_2{}^*(x) + (1+u)a_2(x))$ olduğu açıktır. Böylece, C ters sıralı tamamlayan özelliğine sahip uzunluğu 3, minimum Hamming uzaklığı 3 olan bir devirli DNA koddur. C'nin θ dönüşümü altındaki DNA görüntüsü, uzunluğu 6, eleman sayısı 64 ve minimum Hamming uzaklığı 2 olan bir DNA kodudur.

5.2. R_u Halkası Üzerinde Tanımlı Devirli DNA Kodlar

$u^2 = u$ olmak üzere R_u halkasının özellikleri *3.5.Bölüm*'de verilmişti. Bu bölümde, N. Kumar ve A. K. Singh tarafından belirlenen $u^2 = u$ olmak üzere, R_u halkası üzerinde tanımlı uzunluğu n olan devirli kodların ters sıralı ve ters sıralı tamamlayan olması için gerekli ve yeterli koşullar verilmiştir.

Bu bölümde, $u^2 = u$ olmak üzere R_u üzerinde Gray dönüşümü,

$\phi: R_u \to \mathbb{Z}_4^2$

$a + ub \mapsto (a, a + b)$

şeklindedir.

5.2.1. $\mathbb{Z}_4$ Halkası Üzerinde Tanımlı Devirli Kodlar

5.2.1.1.Teorem:

$C, \mathbb{Z}_4$ halkası üzerinde tanımlı uzunluğu n olan devirli bir kod olsun. ($\pi(C) \subseteq \mathbb{Z}_4[x]/\langle x^n - 1\rangle$ halkasının bir ideali olsun.) Bu durumda,

i) Eğer n pozitif tek tam sayı ise, $a_1(x) \mid a_2(x) \mid (x^n - 1)(mod\ 4)$ özelliklerini sağlayan $a_1(x),\ a_2(x) \in \mathbb{Z}_4[x]$ polinomları olmak üzere, $\pi(C) = \langle a_2(x), 2a_1(x)\rangle = \langle a_2(x) + 2a_1(x)\rangle$ dir. Kısaca $\mathbb{Z}_4[x]/\langle x^n - 1\rangle$ esas ideal halkasıdır.

ii) Eğer n çift tam sayı ise,

a) $a_2(x),\ a_3(x) \in \mathbb{Z}_4[x],\ a_2(x) \mid (x^n - 1)(mod\ 2)$ ve $a_2(x) + 2a_3(x) \mid (x^n - 1)(mod\ 4)$ özelliklerini sağlayan iki polinom olmak üzere, $\pi(C) = \langle a_2(x), 2a_3(x)\rangle$ dir.

b) $a_1(x),\ a_2(x)$ ve $a_3(x) \in \mathbb{Z}_4[x],\ a_1(x) \mid a_2(x) \mid (x^n - 1)(mod\ 2)$ ile $a_1(x) \mid a_3(x) \mid (x^n - 1)/a_2(x)\ (mod 2)$ ve $\deg a_2(x) > \deg a_1(x) > \deg a_3(x)$ özelliklerini sağlayan polinomlar olmak üzere, $\pi(C) = \langle a_2(x), 2a_3(x), 2a_1(x)\rangle$ dir (Kumar ve Singh, 2018).

5.2.2. R_u Halkası Üzerinde Tanımlı Devirli DNA Kodlar

DNA alfabesi $S_{D_4} = \{A, T, G, C\}$ ile gösterilsin. $x_i \in \{A, T, G, C\}$ olmak üzere, $(x_0, x_1, \dots, x_{n-1})$ kod sözcükleri kümesi uzunluğu n olan bir DNA kodu olarak tanımlanır. *5.3. Çizelge*'de $\mathbb{Z}_4$'ün elemanları $0 \to G$, $1 \to A$, $2 \to C$ ve $3 \to T$ olacak şekildeki bir dönüşüm yardımı ile S_{D_4} kümesinin elemanlarına birebir eşlenir. Bu dönüşüm, *5.2. Bölüm*'de tanımlanan Gray dönüşümü yardımıyla $\theta: R_u \to {S_{D_4}}^2$ dönüşümü tanımlanır. Bu sayede R_u halkasının elemanlarına karşılık gelen DNA çiftleri tablosu *Çizelge 5.3*'de verilmiştir. S_{D_4} kümesindeki elemanların Watson-Crick tamamlayanları sağlaması; $\overline{A} = T, \overline{T} = A, \overline{G} = C, \overline{C} = G$ biçimindedir. Benzer şekilde $S_{D_{16}}$ kümesindeki elemanların Watson-Crick tamamlayanları; $\overline{AA} = TT, \overline{TA} = AT, \overline{GA} = CT, \dots, \overline{TC} = AG, \overline{GC} = CG, \overline{CC} = GG\}$ şeklindedir.

5.2.2.1. Not:

C, R_u halkası üzerinde tanımlı uzunluğu n olan devirli bir kod olsun. Bu durumda, *4.2.20. Sonuç*'dakine benzer şekilde C_1 ve $C_2, \mathbb{Z}_4$ üzerinde tanımlı uzunluğu n olan lineer kodlar olmak üzere C, $C = uC_1 + (1 + 3u)C_2$ biçiminde teklikle ifade edilir.

5.2.2.2. Teorem:

i) C, R_u halkası üzerinde tanımlı uzunluğu n olan $C = uC_1 + (1 + 3u)C_2$ olacak şekilde bir lineer kod olsun. Bu durumda, C'nin devirli olması için gerekli ve yeterli koşul C_1 ve C_2 kodlarının $\mathbb{Z}_4$ halkası üzerinde tanımlı devirli kod olmasıdır.

ii) C, R_u halkası üzerinde tanımlı uzunluğu n olan devirli bir kod olsun. Bu durumda $f_1(x)$ ve $f_2(x)$ sırasıyla, $\mathbb{Z}_4$ halkası üzerinde tanımlı C_1 ve C_2 kodlarının üreteç polinomları olmak üzere, $\pi(C) = \langle uf_1(x) + (1 + 3u)f_2(x) \rangle$ dir (Kumar ve Singh, 2018).

Çizelge 5.3 R_u Halkasının Elemanlarına Karşılık Gelen DNA Çiftleri

R_V Halkasının Elemanları $r = a + ub$	**Gray Görüntüleri** $\phi(r) = (a, a + b)$	**DNA Çiftleri** $\theta(r)$
0	(0,0)	GG
1	(1,1)	AA
2	(2,2)	CC
3	(3,3)	TT
u	(0,1)	GA
$2u$	(0,2)	GC
$3u$	(0,3)	GT
$1 + u$	(1,2)	AC
$2 + u$	(2,3)	CT
$3 + u$	(3,0)	TG
$1 + 2u$	(1,3)	AT
$2 + 2u$	(2,0)	CG
$3 + 2u$	(3,1)	TA
$1 + 3u$	(1,0)	AG
$2 + 3u$	(2,1)	CA
$3 + 3u$	(3,2)	TC

5.2.3. R_u Halkası Üzerinde Tanımlı Ters Sıralı Kodlar

Bu bölümde, R_u halkası üzerinde tanımlı, uzunluğu n olan devirli bir kodun ters sıralı olması için gerekli ve yeterli koşullar $\mathbb{Z}_4$ halkası üzerinde tanımlı ters sıralı kodlar yardımıyla verilmiştir.

5.2.3.1. Lemma:

der $a(x) \geq$ der $b(x)$ olmak üzere, $a(x), b(x) \in \mathbb{Z}_4[x]$ olsun. Bu durumda;

i) $[a(x).b(x)]^* = a^*(x).b^*(x)$

ii) $[a(x) + b(x)]^* = a^*(x) + x^{\text{der}\, a(x) - \text{der}\, b(x)}.b^*(x)$ dir (Kumar ve Singh, 2018).

5.2.3.2. Lemma:

$\pi(C) = \langle c(x) \rangle$, $\mathbb{Z}_4[x]/\langle x^n - 1 \rangle$ halkasının bir ideali olsun. Bu durumda, C'nin ters sıralı olması için gerekli ve yeterli koşul $c(x)$ polinomunun self-reciprocal olmasıdır (Kumar ve Singh, 2018).

Kanıt:

5.1.3.2. Teorem'in kanıtına benzer şekilde kanıtlanır.

5.2.3.3. Teorem:

n pozitif tek tam sayı olmak üzere, $\pi(C) = \langle a_2(x), 2a_1(x) \rangle = \langle a_2(x) + 2a_1(x) \rangle$, $\mathbb{Z}_4[x]/\langle x^n - 1 \rangle$ halkasının bir ideali olsun. Bu durumda, C'nin ters sıralı olması için gerekli ve yeterli koşul $a_1(x)$ ve $a_2(x)$ polinomlarının self-reciprocal olmasıdır (Kumar ve Singh, 2018).

Kanıt:

5.1.3.3. Teorem'in (i) şıkkının kanıtına benzer şekilde kanıtlanır.

5.2.3.4. Teorem:

n çift tam sayı olmak üzere, $\pi(C)$, $\mathbb{Z}_4[x]/\langle x^n - 1\rangle$ halkasının bir ideali olsun. Bu durumda,

i) $\propto = 1$ ya da 2 olmak üzere, $\pi(C) = \langle \propto c(x)\rangle$'in ters sıralı olması için gerekli ve yeterli koşul $c(x)$ 'in self-reciprocal olmasıdır.

ii) $a_1(x)$, $a_2(x)$ ve $a_3(x) \in \mathbb{Z}_4[x]$, $a_1(x) \mid a_2(x) \mid (x^n - 1)(mod\ 2)$ ile $a_1(x) \mid a_3(x) \mid (x^n - 1)/a_2(x)$ ve $\operatorname{der} a_2(x) > \operatorname{der} a_1(x) > \operatorname{der} a_3(x)$ özelliklerini sağlayan polinomlar olmak üzere, $\pi(C) = \langle a_2(x), 2a_3(x), 2a_1(x)\rangle$'in ters sıralı olması için gerekli ve yeterli koşul

a) $a_1(x)$ ve $a_2(x)$'in self-reciprocal olması,

b) $i = \operatorname{der} a_2(x) - \operatorname{der} a_3(x)$ olmak üzere, $a_1(x) \mid (x^i {a_3}^*(x) + a_3(x))$ olmasıdır (Kumar ve Singh, 2018).

Kanıt:

5.1.3.3. Teorem'in kanıtına benzer şekilde kanıtlanır.

5.2.3.5. Teorem:

$C = uC_1 + (1 + 3u)C_2$ olacak şekilde R_u halkası üzerinde tanımlı uzunluğu n olan devirli bir kod olsun. Bu durumda, C'nin ters sıralı kod olması için gerekli ve yeterli koşul C_1 ve C_2'nin $\mathbb{Z}_4$ üzerinde tanımlı ters sıralı kod olmasıdır (Kumar ve Singh, 2018).

Kanıt:

C_1 ve C_2 ters sıralı kodlar olsun. C kodundaki herhangi bir k elemanı, $k_1 \in C_1$ ve $k_2 \in C_2$ olmak üzere, $k = uk_1 + (1 + 3u)k_2$ biçiminde yazılır. ${k_1}^R \in C_1$ ve ${k_2}^R \in C_2$ olduğu açıktır. Bu durumda, $k^R = u{k_1}^R + (1 + 3u){k_2}^R \in C$ olur. Böylece C ters sıralıdır.

Diğer taraftan, C ters sıralı olsun. $k_1 \in C_1$ ve $k_2 \in C_2$ olmak üzere, $k = uk_1 + (1 + 3u)k_2$ biçiminde yazılsın. Bu durumda, $l_1 \in C_1$ ve $l_2 \in C_2$ olmak üzere, $k^R = u{k_1}^R + (1 + 3u){k_2}^R \in C$ ve $k^R = u{k_1}^R + (1 + 3u){k_2}^R = ul_1 + (1 + 3u)l_2$ olur. Böylece,

$u\left({k_1}^R - l_1\right) + (1+3u)\left({k_2}^R - l_2\right) = 0$ dır. Bu durumda, ${k_1}^R = l_1 \in C_1$ ve ${k_2}^R = l_2 \in C_2$ olur, ki bu C_1 ve C_2'nin ters sıralı olmasını gerektirir.

5.2.4. R_u Halkası Üzerinde Tanımlı Ters Sıralı Tamamlayan Kodlar

Bu bölümde, R_u halkası üzerinde tanımlı bir kodun ters sıralı tamamlayan bir kod olması için gerekli ve yeterli koşullar verilmiştir.

5.2.4.1. Lemma:

Herhangi iki $a, b \in \mathbb{Z}_4$ için,

i) $a + \overline{a} = 0$ ya da 2,

ii) $\overline{a+b} = \overline{a} + \overline{b} + 2$,

iii) $\overline{a} + 2 = a$,

iv) $\overline{2a} + 2 = 2a$

eşitlikleri sağlanır (Kumar ve Singh, 2018).

Kanıt:

5.1.4.1. Lemma, *5.1.4.2. Lemma* ve *5.1.4.3. Lemma*'nın kanıtına benzer şekilde kanıtlanır.

5.2.4.2. Teorem:

n pozitif tek tam sayı olmak üzere, $\pi(C) = \langle a_2(x), 2a_1(x)\rangle$, $\mathbb{Z}_4[x]/\langle x^n - 1\rangle$ halkasının bir ideali olsun. Bu durumda C'nin ters sıralı tamamlayan olması için gerekli ve yeterli koşul, $a_1(x)$ ve $a_2(x)$'ün self-reciprocal ve $2((1-x^n)/(1-x)) \in \pi(C)$ olmasıdır (Kumar ve Singh, 2018).

Kanıt:

5.1.4.5. Teorem'in (i) şıkkının kanıtına benzer şekilde kanıtlanır.

5.2.4.3. Teorem:

n çift olmak üzere $\pi(C)$, $\mathbb{Z}_4[x]/\langle x^n-1\rangle$ halkasının bir ideali olsun. Bu durumda,

i) $\propto = 1$ ya da 2 olmak üzere, $\pi(C) = \langle \propto c(x)\rangle$'in ters sıralı tamamlayan olması için gerekli ve yeterli koşul $c(x)$ 'in self-reciprocal ve $2((1-x^n)/(1-x)) \in \pi(C)$ olmasıdır.

ii) $a_1(x)$, $a_2(x)$ ve $a_3(x) \in \mathbb{Z}_4[x]$, $a_1(x) \mid a_2(x) \mid (x^n-1)(mod\ 2)$ ile $a_1(x) \mid a_3(x) \mid (x^n-1)/a_2(x)$ ve $\operatorname{der} a_2(x) > \operatorname{der} a_1(x) > \operatorname{der} a_3(x)$ özelliklerini sağlayan polinomlar olmak üzere, $\pi(C) = \langle a_2(x), 2a_3(x), 2a_1(x)\rangle$'in ters sıralı tamamlayan olması için gerekli ve yeterli koşul,

a) $a_1(x)$ ve $a_2(x)$'in self-reciprocal olması ve $2((1-x^n)/(1-x)) \in \pi(C)$ olmasıdır.

b) $i = \operatorname{der} a_2(x) - \operatorname{der} a_3(x)$ olmak üzere, $a_1(x) \mid (x^i {a_3}^*(x) + a_3(x))$ olmasıdır (Kumar ve Singh, 2018).

Kanıt:

5.1.4.5. Teorem'in kanıtına benzer şekilde kanıtlanır.

5.2.4.4. Teorem:

$C = uC_1 + (1+3u)C_2$ olacak şekilde R_u halkası üzerinde tanımlı uzunluğu n olan devirli bir kod olsun. Bu durumda, C'nin ters sıralı tamamlayan bir kod olması için gerekli ve yeterli koşul C'nin ters sıralı bir kod olması ve $(\overline{0}, \overline{0}, \overline{0}, \dots, \overline{0}) \in C$ olmasıdır (Kumar ve Singh, 2018).

Kanıt:

C ters sıralı tamamlayan bir kod olsun. Bu durumda, $c = (c_1, c_2, \dots, c_{n-1}) \in C$ için $c^{RC} = (\overline{c_{n-1}}, \overline{c_{n-2}}, \dots, \overline{c_1}, \overline{c_0}) \in C$ dir.

C lineer olduğuna göre $\mathbf{0} = (0, 0, \dots, 0) \in C$'dir. Bu durumda C ters sıralı tamamlayan bir kod olduğu için $(\overline{0}, \overline{0}, \overline{0}, \dots, \overline{0}) \in C$ dir. Ayrıca, $c^R = (c_{n-1}, c_{n-2}, \dots, c_1, c_0) = (\overline{c_{n-1}}, \overline{c_{n-2}}, \dots, \overline{c_1}, \overline{c_0}) + (\overline{0}, \overline{0}, \overline{0}, \dots, \overline{0}) \in C$ dir. Bu C'nin ters sıralı bir kod olmasını gerektirir.

Diğer taraftan, C ters sıralı ve $(\overline{0}, \overline{0}, \overline{0}, \dots, \overline{0}) \in C$ olsun. Bu durumda, $c = (c_1, c_2, \dots, c_{n-1}) \in C$ için $c^R = (c_{n-1}, c_{n-2}, \dots, c_1, c_0) \in C$ dir. $c^{RC} = (\overline{c_{n-1}}, \overline{c_{n-2}}, \dots, \overline{c_1}, \overline{c_0}) = (c_{n-1}, c_{n-2}, \dots, c_1, c_0) + (\overline{0}, \overline{0}, \overline{0}, \dots, \overline{0}) \in C$ olduğu için C ters sıralı tamamlayan bir koddur.

BÖLÜM 6

R_1 HALKASI ÜZERİNDE TANIMLI u-SABİT DEVİRLİ KODLAR İLE DEVİRLİ KODLARIN GRAY GÖRÜNTÜLERİ

Bu bölümde, R_1 halkası üzerinde, u birimsel elemanı seçilerek, bu halka üzerinde uzunluğu tek olan u-sabit devirli ve devirli kodların Gray görüntüleri elde edilmiştir. Elde edilen teorem ve sonuçlar *Şekil 6.1'*deki dönüşümlerin komütatifliğini sağlayacak şekilde verilmiştir.

6.1. R_1 Halkası Üzerinde Tanımlı Uzunluğu Tek Olan u-Sabit Devirli Kodlar ile Devirli Kodlar Arasındaki İlişki

Bu bölümde, $u^2 = 1$ olmak üzere R_1 halkası üzerinde tanımlı u-sabit devirli kodlarla devirli kodlar arasındaki ilişki verilmiştir.

$$(u)^n = \begin{cases} 1; & n \text{ çift ise} \\ u; & n \text{ tek ise} \end{cases}$$

şeklindedir. Bu sonuç doğrultusunda aşağıdaki önerme sağlanır.

6.1.1. Önerme:

$$\mu: R_1[x]/\langle x^n - 1\rangle \to R_1[x]/\langle x^n - u\rangle$$

$$\overline{c(x)} \mapsto \mu(\overline{c(x)}) = \overline{c(ux)}$$

dönüşümü tanımlansın. n tek olması durumunda, μ bir halka izomorfizmasıdır.

Kanıt:

i) $\forall \overline{c(x)}, \overline{d(x)} \in R_1[x]/\langle x^n - 1\rangle$ için $c(x) \equiv d(x)(mod\ x^n - 1)$ olsun.

$c(x) \equiv d(x)(mod\ x^n - 1) \Rightarrow \overline{c(x)} = (x^n - 1).\overline{k(x)} + \overline{d(x)}$ olacak şekilde $\exists\ \overline{k(x)}$ vardır.

$x \mapsto ux$ yazılırsa;

$$\overline{c(ux)} = ((ux)^n - 1).\overline{k(ux)} + \overline{d(ux)}$$

$$= (u^n x^n - u^2).\overline{k(ux)} + \overline{d(ux)}$$

$$= u(x^n - u).\overline{k(ux)} + \overline{d(ux)}$$

elde edilir. Buradan,

$$\overline{c(ux)} = u(x^n - u).\overline{k(ux)} + \overline{d(ux)}$$

olduğu görülür. O halde, $\mu(c(x)) \equiv \mu(d(x))(mod\ x^n - u)$ dir.

Bu durumda, μ iyi tanımlıdır.

ii) $\forall \overline{c(x)}, \overline{d(x)} \in R_1[x]/\langle x^n - 1\rangle$ için $\mu(c(x)) \equiv \mu(d(x))(mod\ x^n - u)$ olsun.

$$\mu\overline{(c(x))} = \mu\big(\overline{d(x)}\big) \Rightarrow c(ux) \equiv d(ux)(mod\ x^n - u)$$

$$\Rightarrow \overline{c(ux)} = \overline{k(ux)}.(x^n - u) + \overline{d(ux)}$$

olur. $x \mapsto ux$ yazılırsa;

$$\overline{c(x)} = \overline{k(x)}.((ux)^n - u) + \overline{d(x)}$$

$$= \overline{k(x)}.(u^n x^n - u) + \overline{d(x)}$$

$$= \overline{k(x)}.(ux^n - u) + \overline{d(x)} \quad (n \text{ tek olduğundan})$$

$$= u.\overline{k(x)}.(x^n - 1) + \overline{d(x)}$$

elde edilir. Bu durumda, $c(x) \equiv d(x)(mod\ x^n - 1)$ olur.

Bu durumda, μ birebirdir.

iii) $R_1[x]/\langle x^n - 1\rangle$ ve $R_1[x]/\langle x^n - u\rangle$ halkaları sonlu ve μ birebir olduğundan μ örtendir.

iv)

a) $\forall\ \overline{c(x)}, \overline{d(x)} \in R_1[x]/\langle x^n - 1\rangle$ olsun.

$$\mu(\overline{c(x)} + \overline{d(x)}) = \mu\big(\overline{(c+d)(x)}\big)$$

$$= \overline{(c+d)(ux)}$$

$$= \overline{c(ux)} + \overline{d(ux)}$$

$$= \mu\big(\overline{c(x)}\big) + \mu(\overline{d(x)})$$

elde edilir.

b) $\forall\ \overline{c(x)}, \overline{d(x)} \in R_1[x]/\langle x^n - 1\rangle$ olsun.

$$\mu(\overline{c(x)}.\overline{d(x)}) = \mu\big(\overline{(c.d)(x)}\big)$$

$$= \overline{(c.d)(ux)}$$

$$= \overline{c(ux)}.\overline{d(ux)}$$

$$= \mu\big(\overline{c(x)}\big).\mu(\overline{d(x)})$$

elde edilir. Bu durumda (a) ve (b) sağlandığından μ bir halka homomorfizmasıdır.

Bu durumda μ bir halka izomorfizmasıdır.

6.1.2. Sonuç:

n pozitif tek tam sayı olsun. I kümesinin $R_1[x]/\langle x^n - 1\rangle$ halkasının bir ideali olması için gerekli ve yeterli koşul $\mu(I)$ kümesinin $R_1[x]/\langle x^n - u\rangle$ halkasının bir ideali olmasıdır.

Kanıt:

⇒:

I kümesi $R_1[x]/\langle x^n - 1\rangle$ halkasının bir ideali olsun. Bu durumda,

$\forall\, c(x), d(x) \in I$ için $c(x) - d(x) \in I$ ve

$\forall\, c(x) \in I, \forall\, k(x) \in R_1[x]/\langle x^n - 1\rangle$ için $c(x).k(x) \in I, (k(x).c(x) \in I)$

özellikleri sağlanır.

i) $\forall\, \mu\big(c(x)\big) = c(ux),\ \mu\big(d(x)\big) = d(ux) \in \mu(I)$ $(\forall\, c(x), d(x) \in I)$ için μ homomorfizma olduğundan $\mu\big(c(x)\big) - \mu\big(d(x)\big) = \mu\big(c(x) - d(x)\big) \in \mu(I)$ dir.

ii) $\forall\, \mu\big(c(x)\big) = c(ux) \in \mu(I)$ ve $\forall\, k(x) \in R_1[x]/\langle x^n - u\rangle$ için μ homomorfizma olduğundan $\mu\big(c(x)\big).k(x) = \mu\big(c(x).k(x)\big) \in \mu(I)$ ve $k(x).\mu\big(c(x)\big) = \mu\big(k(x).c(x)\big) \in \mu(I)$ dir.

Bu durumda, (i) ve (ii) den $\mu(I)$ kümesi $R_1[x]/\langle x^n - u\rangle$ halkasının bir idealidir.

⇐:

$\mu(I)$ kümesi $R_1[x]/\langle x^n - u\rangle$ halkasının bir ideali olsun. Bu durumda,

$\forall\, \mu(c(x)), \mu(d(x)) \in \mu(I)$ için $\mu(c(x)) - \mu(d(x)) \in \mu(I)$ ve

$\forall\, \mu\big(c(x)\big) \in \mu(I), \forall\, k(x) \in R_1[x]/\langle x^n - u\rangle$ için

$\mu\big(c(x)\big).k(x) \in \mu(I), (k(x).\mu(c(x)) \in \mu(I))$ özellikleri sağlanır.

μ homomorfizma olduğundan $\mu\big(c(x)-d(x)\big)=\mu\big(c(x)\big)-\mu\big(d(x)\big)\in\mu(I)$ olduğu ve $\mu\big(c(x).k(x)\big)=\mu\big(c(x)\big).k(x)\in\mu(I)$ olduğu bilinmektedir. Bu durumda $\forall\, c(x),d(x)\in I$ için $c(x)-d(x)\in I$ ve $k(x).c(x)\in I$ olur. Ayrıca, $\mu\big(k(x).c(x)\big)=k(x).\mu\big(c(x)\big)\in\mu(I)$ ise $c(x).k(x)\in I$ olur.

Bu durumda I kümesi $R_1[x]/\langle x^n-1\rangle$ halkasının bir idealidir.

6.1.3. Sonuç:

n pozitif tek bir tam sayı ve C, R_1^n kümesinin bir alt kümesi olsun. $\bar{\mu}$ permütasyonu R_1^n kümesi üzerinde,

$$\bar{\mu}(c_0,c_1,\dots,c_{n-1})=(c_0,uc_1,u^2c_2,\dots,u^{n-1}c_{n-1})$$

biçiminde tanımlansın. Bu durumda, C'nin devirli bir kod olması için gerekli ve yeterli koşul $\bar{\mu}(C)$'nin u-sabit devirli bir kod olmasıdır.

Kanıt:

C, n (tek) uzunluğunda devirli bir kod olsun. C kodunun polinom gösterimi, gösterim kolaylığı sağlamak amacıyla yine $\pi(C)$ yerine C olarak gösterilsin. Bu durumda, C kümesi $R_1[x]/\langle x^n-1\rangle$ halkasının bir idealidir. *Sonuç 4.3.2*'den $\mu(C)$ kümesi $R_1[x]/\langle x^n-u\rangle$ halkasının bir idealidir. Bu durumda, $\bar{\mu}(C)$ kümesi R_1 üzerinde tanımlı bir u-sabit devirli koddur.

6.2. R_1 Halkası Üzerinde Tanımlı Gray Dönüşüm, u-Sabit Devirli Kodlar ve Tek Uzunluklu Devirli Kodların Gray Görüntüleri

6.2.1. Tanım:

$a,b\in\mathbb{Z}_4, u^2=1$, olmak üzere R_1 halkası üzerinde,

$$\phi_1: R_1\to\mathbb{Z}_4^2$$

$$a+ub\mapsto(a,b)$$

şeklinde tanımlanan dönüşüme ‘‘*Gray dönüşümü*’’ denir.

6.2.2. Tanım:

$a, b \in \mathbb{Z}_4, u^2 = 1$, olmak üzere $r = a + ub$, R_1 halkasından alınan bir eleman olsun. Bu durumda,

$w_G(r) = w_L(a) + w_L(b)$

biçiminde tanımlanan değere r’nin ‘‘*Gray ağırlığı*’’ denir.

6.2.3. Not:

$0 \leq i \leq n-1$ ve $c_i = a_i + ub_i$ olmak üzere herhangi bir $(c_0, c_1, \dots, c_{n-1}) \in R_1^n$

için ϕ_1 Gray dönüşümü,

$$\phi_1 : R_1^n \to \mathbb{Z}_4^{2n}$$

$$(c_0, c_1, \dots, c_{n-1}) \mapsto \phi_1(c_0, c_1, \dots, c_{n-1}) = (a_0, a_1, \dots, a_{n-1}, b_0, b_1, \dots, b_{n-1})$$

biçiminde R_1^n kümesine genişletilebilir.

6.2.4. Önerme:

d_G minimum Gray uzaklığı, d_L minimum Lee uzaklığı olmak üzere, (R_1^n, d_G) kümesinden $(\mathbb{Z}_4^{2n}, d_L)$ kümesine tanımlı ϕ_1 Gray dönüşümü hem lineer hem de uzaklık koruyan bir dönüşümdür.

Kanıt:

*4.1.9.Teorem’*in kanıtına benzer şekilde kanıtlanır.

6.2.5. Teorem:

C, R_1 halkası üzerinde tanımlı bir (n, M, d_G) lineer kod ise $d_G = d_L$ olmak üzere,

$\phi_1(C)$ kodu $\mathbb{Z}_4$ üzerinde tanımlı bir $(2n, M, d_L)$ lineer koddur.

6.2.6. Önerme:

σ, R_1^n üzerinde tanımlı u-sabit devirli öteleme ve φ, $\mathbb{Z}_4^{2n}$ üzerinde tanımlı devirli öteleme olsun. $\phi_1 \circ \sigma = \varphi \circ \phi_1$ sağlanır.

Kanıt:

$i = 0, 1, \dots, n-1$ için $c_i = a_i + ub_i$ olmak üzere $c = (c_0, c_1, \dots, c_{n-1}) \in R_1^n$ olsun. Bu durumda,

$$\sigma(c) = (uc_{n-1}, c_0, c_1, \dots, c_{n-2})$$

$$= (b_{n-1} + ua_{n-1}, a_0 + ub_0, a_1 + ub_1, \dots, a_{n-2} + ub_{n-2})$$

dir. ϕ_1 Gray dönüşümü tanımından,

$$\phi_1(\sigma(c)) = (b_{n-1}, a_0, a_1, \dots, a_{n-2}, a_{n-1}, b_0, b_1, \dots, b_{n-2})$$

elde edilir. Diğer Taraftan,

$$\phi_1(c) = (a_0, a_1, \dots, a_{n-1}, b_0, b_1, \dots, b_{n-1})$$

eşitliğine φ dönüşümü uygulanırsa,

$$\varphi(\phi_1(c)) = (b_{n-1}, a_0, a_1, \dots, a_{n-2}, a_{n-1}, b_0, b_1, \dots, b_{n-2})$$

eşitliği elde edilir.

Bu durumda $\phi_1 \circ \sigma = \varphi \circ \phi_1$ sağlanır.

6.2.7. Teorem:

R_1 halkası üzerinde, uzunluğu n olan u-sabit devirli kodun Gray görüntüsü $\mathbb{Z}_4$ üzerinde tanımlı, uzunluğu $2n$ olan devirli bir koddur.

Kanıt:

C, R_1 halkası üzerinde uzunluğu n olan u-sabit devirli kod olsun. Bu durumda $\sigma(C) = C$ dir. Bu eşitliğin her iki yanına ϕ_1 Gray dönüşümü uygulanırsa,

$\phi_1(\sigma(C)) = \phi_1(C)$ elde edilir. Son eşitlik ve *4.4.5.Önerme* kullanılırsa $\phi_1(C) = \varphi(\phi_1(C))$ elde edilir. Bu durumda, $\phi_1(C)$ halkası üzerinde tanımlı uzunluğu $2n$ olan devirli bir koddur.

6.2.8. Önerme:

n pozitif tek tam sayı olsun. $\bar{\mu}$, *6.1.3. Sonuç*'da olduğu gibi tanımlansın. Bu durumda, $\delta = (1, n+1)(3, n+3) \dots (n-2, 2n-2)$ Nechaev permütasyonu olmak üzere $\phi_1\bar{\mu} = \delta\phi_1$ dir.

Kanıt:

$i = 0, 1, \dots, n-1$ için $c_i = a_i + ub_i$ olmak üzere $c = (c_0, c_1, \dots, c_{n-1}) \in R_1^n$ olsun. Bu durumda,

$\bar{\mu}(c_0, c_1, \dots, c_{n-1}) = (c_0, uc_1, u^2c_2, \dots, u^{n-1}c_{n-1})$

dir. ϕ_1 Gray dönüşümü tanımından,

$\phi_1(\bar{\mu}(c)) = (a_0, b_1, a_2, b_3, \dots, a_{n-1}, b_0, a_1, \dots, b_{n-1})$

elde edilir. Diğer taraftan,

$\phi_1(c) = (a_0, a_1, \dots, a_{n-1}, b_0, b_1, \dots, b_{n-1})$ olduğu için $\pi(\phi_1(c)) = \phi_1(\bar{\mu}(c))$ olduğu görülür. Dolayısıyla, $\phi_1\bar{\mu} = \delta\phi_1$ dir.

6.2.9. Sonuç:

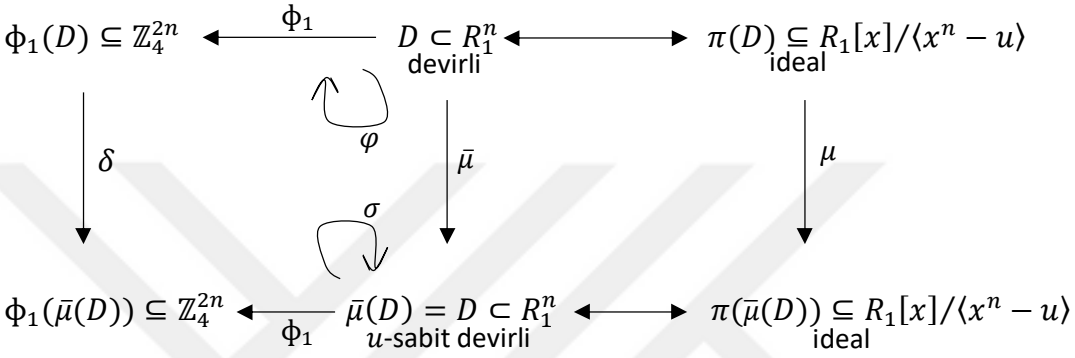
δ Nechaev permütasyonu olsun. n tek olmak üzere Γ, R_1 halkası üzerinde tanımlı devirli bir kodun Gray görüntüsü ise $\delta(\Gamma)$ devirli bir koddur.

Kanıt:

D, R_1 halkası üzerinde tanımlı bir devirli kod ise $\Gamma = \phi_1(D)$ dir. *6.2.8.Önerme*'den $\phi_1(\bar{\mu}(D)) = \delta(\phi_1(D)) = \delta(\Gamma)$ elde edilir. *6.1.3. Sonuç*'dan $\bar{\mu}(D)$'nin C, u-sabit devirli bir kod olduğunu biliyoruz. Bu durumda, $\phi_1(\bar{\mu}(D)) = (\phi_1(C))$ elde edilir. *6.2.7. Teorem*'den $\phi_1(C)$, $\mathbb{Z}_4$ üzerinde tanımlı, uzunluğu $2n$ olan devirli bir koddur.

6.2.10. Sonuç:

R_1 halkası üzerinde tanımlı uzunluğu n olan bir devirli kodun Gray görüntüsü $\mathbb{Z}_4$ üzerinde tanımlı, uzunluğu $2n$ olan devirli bir koda denktir.



Şekil 6.1 R_1 Halkası Üzerindeki Devirli ve Sabit Devirli Kodların Gray Görüntülerinin Diyagramı

BÖLÜM 7

SONUÇLAR VE TARTIŞMALAR

7.1. Sonuçlar

Bu çalışmada, $r = a + ub \in \mathbb{Z}_4 + u\mathbb{Z}_4$ olmak üzere $R_r \cong \mathbb{Z}_4[u]/\langle u^2 - r \rangle$ şeklindeki 16 sonlu halkanın cebirsel yapıları belirlenmiştir. Ayrıca tüm bu halkaların birbirleri ile olan izomorfluk durumları, yeni dönüşümler tanımlanarak belirlenip Çizelge 3.3'de sınıflandırılmıştır.

Bu tez çalışmasının dördüncü bölümünde $\mathbb{Z}_4$ halkası üzerinde tanımlı (optimal) iyi kodlar elde etmekte kullanılan bir yöntemin anlatıldığı makalelerdeki sonuçlar verilmiştir.

Tezin beşinci bölümünde R_1 ve R_u halkaları üzerinde tanımlı kodların ters sıralı ve ters sıralı tamamlayan olabilmesi için gerekli ve yeterli koşulların verildiği makaleler incelenmiştir. Bu şekilde devirli DNA kodlarının DNA görüntüleri ile arzu edilen nitelikte DNA dizileri elde etmek mümkündür.

Bu tez çalışmasının orijinal kısmı olarak altıncı bölümde R_1 halkası üzerinde yeni bir Gray dönüşümü tanımlanıp yeni bir birimsel eleman yardımı ile belirli uzunluğa sahip sabit devirli ve devirli kodların aralarındaki ilişkiler belirlenerek bu kodların Gray görüntüleri elde edilmiştir.

7.2. Gelecek Çalışma

Bu tez çalışmasında cebirsel yapıları belirlenen 16 halka üzerinde aşikar olmayan otomorfizmalar tanımlanarak, bu çalışma skew devirli (cyclic) kodlar üzerine taşınabilir.

Koşullar değiştirilerek veya yeni halkalar seçilerek buradaki çalışmaya benzer şekilde sabit devirli ve devirli kodlar arasındaki ilişkiler, yeni Gray dönüşümleri belirlenerek bulunabilir.

Bu çalışmada iki halka üzerinde verilen devirli DNA kodları tezin kapsamı içinde kalan diğer halkalar veya yeni halkalar üzerinde tanımlanarak, devirli DNA kodların ters sıralı (reversible) ve ters sıralı tamamlayan (reversible complament) olması için gerekli ve yeterli koşullar belirlenebilir.

KAYNAKLAR

Ashraf, M. & Mohammad, G. (2015). $(1+2u)$-constacyclic codes over $\mathbb{Z}_4+u\mathbb{Z}_4$, https://arxiv.org/pdf/1504.03445.

Aydin, N., Cengellenmis, Y. & Dertli, A. (2018). On Some Constacyclic Codes over $\mathbb{Z}_4[u]/\langle u^2-1\rangle$, Their $\mathbb{Z}_4$ Images, and New Codes. *Des. Codes Cryptogr*, *86*, 1249-1255.

Bag, T., Islam, H., Prakash, O. & Upadhyay, A.K. (2018). A Study Of Constacyclic Codes over the rings $\mathbb{Z}_4[u]/\langle u^2-3\rangle$. *Discrete Mathematics,Algorithsm and Application*, DOI: 10.1142/S1793830918500568.

Bandi, R.K., & Bhaintwal, M. (2014). Codes over $\mathbb{Z}_4+v\mathbb{Z}_4$. *International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, *978*, 422-427.

Çallıalp, F. (2013). *Örneklerle Soyut Cebir*. İstanbul: Birsen yayınevi.

Dinh, H.Q., Singh, A.K., Kumar, N. & Sriboonchitta S. (2018). On Constacyclic Codes Over $\mathbb{Z}_4[v]/\langle v^2-v\rangle$ and Their Gray Images. *IEEE*, *22*(9),1758-1761.

Dinh, H.Q., Singh, A.K., Kumar, Pattanayak S. & Sriboonchitta S. (2018). Construction of Cyclic DNA codes over the ring $\mathbb{Z}_4[u]/\langle u^2-1\rangle$ based on the deletion distance. *Theoretical Computer Science*, https://doi.org/10.1016/j.tcs.2018.06.002.

Gao, J. & Gao, Y. (2014). Some Results on Linear Codes over $\mathbb{Z}_4+v\mathbb{Z}_4$, https://arxiv.org/pdf/1402.6771.

Gao, J., Fu, F.W., Gao, Y. (2017). Some classes of linear codes over $\mathbb{Z}_4+v\mathbb{Z}_4$ and their applications to constuct good and new $\mathbb{Z}_4$-linear codes. *Journal of Applicable Algebra in Engineering, Communication and Computing (AAECC)*, *28*, 131-153.

Hill, R. (1986). *First Course in Coding Theory*. Oxford: Claredon Press

Hoffman, K. & Kunze, R. (1971). *Linear Algebra Second Edition*. New Jersey:Pretice-Hall, Inc., Englewood Cliffs.

Holdman, G.R. (2016). *Error-Correcting Codes Over Galois Rings*. (Yayımlanmış Yükseklisans Tezi) Whitman College, Washington.

Huffman, W.C., Cary, W. & Pless, V. (2003). *Fundamentals of Error-Correcting Codes*. Cambridge: Cambridge University Press.

Hungerford, T. (1973). *Algebra*. New York: Springer-Verlag.

Jitman, S., Udomkavanich, P. & Ling, S. (2012). Skew Constacyclic Codes over Finite Chain Rings. *Advances Mathematics Communications*, *6*, 29-63.

Karakaş, H. İ. (2012). *Cebir Dersleri*. Ankara: Tüba yayınları.

Kumar, N. & Singh. A.K. (2018). DNA computing over the ring $\mathbb{Z}_4[v]/\langle v^2 - v\rangle$. *International Journal of Biomathematics*, DOI:10.1142/s1793524518500900.

Ling, S. & Xing, C. (2004). *Coding Theory A First Course*. Cambridge: Cambridge UniversityPress.

Shannon, C.E. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal*, cilt *28*,656-715.

Shi, M., Qian, L., Sok, L.,Aydin, N. & Sole, P. (2017). On Constacyclic codes over $\mathbb{Z}_4[u]/\langle u^2 - 1\rangle$ and their Gray images. *Finite Fields and Their Applications*, http://dx.doi.org/10.1016/j.ffa.2016.11.016.

Taşçı, D. (2007). *Soyut Cebir*. Ankara: Alp Yayınevi.

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı Soyadı : Buse YAVUZ

Eğitim Bilgileri

Lise	: Recep Güngör Anadolu Lisesi, Beylikdüzü, İST	2014
Lisans	: Matematik Bölümü, Trakya Üniversitesi, Fen Fakültesi, Edirne	2018
Y. Lisans	: Matematik, Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Edirne	2020

Yabancı Diller

İngilizce