T.C.
İSTANBUL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

BAZI SONLU HALKALAR ÜZERİNDE DUALİNİ İÇEREN DEVİRLİ KODLAR

Ali SUBATAN

Matematik Anabilim Dalı

Matematik Programı

DANIŞMAN
Doç. Dr. Fatma ÇALIŞKAN

Temmuz, 2025

İSTANBUL

Bu çalışma 31.07.2025 tarihinde aşağıdaki jüri tarafından Matematik Anabilim Dalı Matematik Programında Yüksek Lisans Tezi olarak kabul edilmiştir.

Tez Jürisi

Doç. Dr. Fatma ÇALIŞKAN (Danışman)
Üniversite
Fakülte

Doç. Dr. Temha ERKOÇ
İstanbul Üniversitesi
Fen Fakültesi

Doç. Dr. İsmail AYDOĞDU
Yıldız Teknik Üniversitesi
Fen-Edebiyat Fakültesi

- **İntihal Programı Beyanı**

20.04.2016 tarihli resmi gazetede yayımlanan Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 9/2 ve 22/2 maddeleri gereğince; Bu Lisansüstü teze, İstanbul Üniversitesi'nin abonesi olduğu intihal yazılım programı kullanılarak Fen Bilimleri Enstitüsü'nün belirlemiş olduğu ölçütlere uygun rapor alınmıştır.

ÖNSÖZ

Yüksek lisans eğitimim boyunca beni her koşulda destekleyen, motive eden, yanımda olan, büyük bir sabır ve özveriyle tüm sorularımı yanıtlayan, akademik yaşamımdaki en büyük şansım, kıymetli danışmanım Doç. Dr. Fatma ÇALIŞKAN'a, yaşamım boyunca desteğini benden esirgemeyen başta annem olmak üzere aileme ve arkadaşlarıma teşekkür ederim.

Ayrıca yüksek lisansım boyunca Bilim İnsanı Destek Programları Başkanlığı 2210-A kapsamında sağladığı maddi desteklerden ötürü TÜBİTAK'a teşekkür ederim.

Temmuz, 2025 Ali SUBATAN

İÇİNDEKİLER

Sayfa No

SİMGE VE KISALTMA LİSTESİ

Simgeler	Açıklama
$\mathfrak{C}^{\perp}$	: $\mathfrak{C}$ kodunun duali
$\mathbb{F}_q$	: Eleman sayısı q olan sonlu cisim
$d(x,y)$	: x ve y vektörleri arasındaki Hamming uzaklık
$\mid \mathfrak{C} \mid$	: $\mathfrak{C}$ kodunun eleman sayısı
$w(x)$	: x vektörünün Hamming ağırlığı
$f^*(x)$	: $f(x)$ polinomunun resiprokal polinomu
$\widehat{f}(x)$	: $\frac{x^n-1}{f(x)}$
$Boy(W)$	: W vektör uzayının boyutu
$< S >$	: S kümesindeki vektörlerin tüm lineer kombinezonlarının kümesi

ÖZET

YÜKSEK LİSANS TEZİ

BAZI SONLU HALKALAR ÜZERİNDE DUALİNİ İÇEREN DEVİRLİ KODLAR

Ali SUBATAN

İstanbul Üniversitesi

Fen Bilimleri Enstitüsü

Matematik Anabilim Dalı

Danışman: Doç. Dr. Fatma ÇALIŞKAN

Cebirsel kodlama teorisinde dualini içeren kodlar önemli bir araçtır. Örneğin, kuantum hata düzelten kodların inşasında kullanılan Calderbank-Shor-Steane metodu, dualini içeren lineer kodları kullanır. Bu tezde bazı sonlu halkalar üzerindeki devirli kodların dualini içermesi için sağlaması gereken koşullar araştırılmıştır.

Literatürdeki çalışmaların bir derlemesi niteliğinde olan ve beş bölüme ayrılan bu tez çalışmasının Giriş bölümünde cebirsel kodlama teorisi tanıtılmış, literatürün kısa bir özeti verilmiş ve bu tezin araştırma alanından bahsedilmiştir. Genel Kısımlar bölümünde bu araştırmada kullanımına ihtiyaç duyulan cebirsel yapılar ve özellikleri ile cebirsel kodlama teorisine ilişkin bazı kavramlar ve teoremler verilmiştir. Malzeme ve Yöntem bölümünde bu tez kapsamında kullanılan halkalar tanıtılmış, Bulgular bölümünde ise göz önüne alınan halkalar üzerindeki devirli kodların dualini içerme koşulları verilmiştir. Tezin son bölümü olan Tartışma ve Sonuç bölümünde ise genel bir değerlendirme yapılmıştır.

Temmuz 2025, 73 sayfa.

Anahtar kelimeler: Halka, lineer kod, dual kod, devirli kod.

SUMMARY

M.Sc. THESIS

DUAL CONTAINING CYCLIC CODES OVER SOME FINITE RINGS

Ali SUBATAN

İstanbul University

Institute of Graduate Studies in Sciences

Department of Mathematics

Supervisor: Assoc. Prof. Dr. Fatma ÇALIŞKAN

In algebraic coding theory, self-orthogonal codes constitute an important tool. For instance, the Calderbank-Shor-Steane (CSS) method used in the construction of quantum error-correcting codes relies on linear codes that contain their duals. This thesis investigates the conditions under which cyclic codes over certain finite rings contain their duals.

This thesis is a compilation of studies in the literature and organized into five chapters. In the Introduction, algebraic coding theory is introduced, a brief overview of the literature is presented, and the scope of the research is outlined. The Preliminaries chapter provides the necessary algebraic structures and their properties, as well as key definitions and theorems from algebraic coding theory. In the Materials and Methods chapter, the rings employed in this study are introduced. The Results chapter presents the conditions under which cyclic codes over the specified rings contain their duals. The final chapter, Discussion and Conclusion, offers a general assessment of the findings and their implications.

July 2025, 73 pages.

Keywords: Ring, linear code, dual code, cyclic code.

1. GİRİŞ

Cebirsel kodlama teorisi, bir iletişim veya bir bilginin depolanma sırasında verilerin bozulmasını önlemek ya da bozulmuş verileri düzeltmek amacıyla kullanılan hata düzeltme kodlarının yapısını ve özelliklerini cebirsel yöntemlerle inceleyen bir matematiksel disiplindir. Bu alan, özellikle soyut cebir (örneğin grup teorisi, halka ve cisim kuramı) ile yakın ilişkilidir ve kodların inşasında bu yapılar temel olarak göz önüne alınır.

Cebirsel kodlama teorisinin temel amacı, güvenilir veri iletimini mümkün kılacak şekilde veriyi temsil eden kodların oluşturulması ve bu kodların hata tespiti ile hata düzeltme kapasitelerinin matematiksel olarak analiz edilmesidir. Bu çerçevede, kodların minimum Hamming uzaklıkları, kod oranları ve hata düzeltme sınırları gibi parametreler incelenir.

Modern iletişim sistemleri, veri depolama aygıtları ve dijital haberleşme protokolleri gibi birçok uygulama alanında cebirsel kodlar (örneğin, lineer blok kodlar, devirli kodlar, Reed-Solomon kodlar, BCH kodlar) yaygın olarak kullanılmaktadır. Bu nedenle, cebirsel kodlama teorisi hem teorik matematik hem de mühendislik açısından stratejik öneme sahiptir.

Bir $\mathfrak{C} \subseteq \mathbb{F}_q^n$ lineer kodunun duali $\mathfrak{C}^\perp = \{v \in \mathbb{F}_q^n \mid v \cdot c = 0, \forall c \in \mathfrak{C}\}$ şeklinde tanımlanır. Yani dual kod, orijinal kodun tüm elemanlarıyla iç çarpımı sıfır olan vektörlerden oluşur. Dual kodların kodlama teorisinde birçok yönden önemi vardır. Örneğin dual kodun boyutu ile kodun boyutu veya dual kodun minimum uzaklığı ile kodun parametreleri ilgilidir. Dual kodlar sendrom kod çözümleme yönteminin temelini oluşturur. Çünkü alıcı tarafındaki hata düzeltme işlemlerinde, alınan kod kelimesi ile dual kodun oluşturduğu parite kontrol matrisi (parity-check matrix) yardımıyla sendrom hesaplanır ve hata tesbiti ve hatanın yerinin belirlenmesi için kullanılır. Bazı özel kodlar, dual kodlarıyla birlikte tanımlanır. Bu kapsamda iyi bilinen bir örnek dualine eşit olan yani kendine dual (self dual) kodlardır, bu kodlar kriptografi ve kuantum hata düzeltme sistemlerinde kullanılır. Diğer bir örnek duali ile kesişimi yalnızca sıfır vektörü içeren komplementary dual (LCD-linear complementary dual) kodlardır, bu kodlar yan kanal saldırılarına karşı dirençli sistemlerde kullanılır. Üstelik dual kodlar kodun ağırlık dağılımı ile ilgili önemli sonuçlar verir. Örneğin MacWilliams

eşitliği, bu eşitlik dual kodun ağırlık dağılımı ile kodun ağırlık dağılımı arasındaki ilişkiyi tanımlar. Diğer yandan kuantum hata düzeltme kodlarının yapısı klasik kodların dualleri ile ilişkisine dayanır. Örneğin Calderbank-Shor-Steane kuantum kod oluşturma metodu dualini içeren klasik lineer kod çiftleri ile kuantum kodları inşa etme sürecini ihtiva eder. Dolayısıyla dualini içeren kodlar yalnızca teorik açıdan değil aynı zamanda farklı alanlarada uygulamaların temelini oluşturan yapılardır.

Cebirsel kodlama teorisinde, kodlar genellikle bir cebirsel yapı (örneğin cisim veya halka) üzerinde tanımlanır. Cisimler ve halkalar farklı cebirsel özelliklere sahip olduğundan, bu yapıların üzerinde tanımlanan kodların özellikleri de önemli ölçüde değişiklik gösterir. Cisim üzerindeki kodlar lineer cebir araçları ile kolayca incelenirken halka üzerindeki kodlar için modül teorisi gerekir. Cisim üzerinde uzaklık kavramı standarttır ancak halkalarda alternatif uzaklık ve ağırlık tanımları vardır. Halka üzerindeki kodlar genellikle daha fazla çeşitlilik ve esneklik sunar.

Bu tez çalışması literatürdeki farklı cebirsel yapılar üzerinde dualini içeren kodların bir derlemesidir. Bu çalışma için literatürden beş farklı cebirsel yapı göz önüne alınmış ve bu cebirsel yapılar üzerinde dualini içeren kodların sağladığı koşullar araştırılmıştır. Bu tez çalışmasının Genel Kısımlar bölümünde grup, halka, cisim, polinom halkası, vektör uzayı ve modül gibi bazı cebirsel yapılar tanıtılmış, ardından kodlama teorisiyle ilgili bazı temel tanımlar ve önemli teoremler verilmiştir. Cisim üzerindeki lineer kodlar ile halka üzerindeki lineer kodlar ayrı alt başlıklar altında incelenmiştir. Malzeme ve Yöntem kısmında öncelikle döngüsel kosetler tanıtılmış daha sonra sırasıyla $\mathbb{F}_2+v\mathbb{F}_2$ $(v^2=v)$ halkasının, $\mathbb{F}_p+u\mathbb{F}_p$ $(u^2=1)$ halkasının, $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$ $(u^2=0)$ halkasının ve son olarak $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}+\cdots+u^k\mathbb{F}_{2^m}$ $(u^{k+1}=0)$ halkasının cebirsel yapıları incelenmiştir. Bulgular kısmında ilk olarak döngüsel kosetler yardımıyla $\mathbb{F}_2$ üzerinde daha sonra $\mathbb{F}_2+v\mathbb{F}_2$ halkası üzerinde, $\mathbb{F}_p+u\mathbb{F}_p$ halkası üzerinde, $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}$ halkası üzerinde ve son olarak $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}+\cdots+u^k\mathbb{F}_{2^m}$ halkası üzerindeki devirli kodların dualini içermesi için sağlaması gereken koşullar verilmiştir. Tartışma ve Sonuç bölümünde, araştırmanın bulgularının değerlendirilmesi, çalışmanın sınırlılıkları, katkıları ve gelecekte yapılabilecek araştırmalar gibi unsurlar ele alınmıştır.

2. GENEL KISIMLAR

2.1. CEBİRSEL YAPILAR VE ÖZELLİKLERİ

Cebirsel kodlama teorisinde cebirsel yapılar, özellikle sonlu cisimler (Galois cisimleri), halkalar ve vektör uzayları, kodların tanımlanması, analizi ve çözülmesi açısından temel bir rol oynamaktadır. Bu yapılar sayesinde hata düzeltme ve tespit etme yeteneklerine sahip kodlar sistematik ve yapısal bir biçimde geliştirilebilir. Bu cebirsel yapıların kullanımı, yalnızca kodların etkinliğini artırmakla kalmaz, aynı zamanda kodlama ve çözme algoritmalarının hesaplama açısından verimli bir şekilde tasarlanmasına da olanak tanır. Dolayısıyla, cebirsel yapılar cebirsel kodlama teorisinin kuramsal temelini oluşturmakla birlikte, bilgi iletiminin güvenilirliğini artırmak adına pratik uygulamalarda da vazgeçilmez bir yere sahiptir.

Bu bölümde bu tez çalışmasında kullanılan cebirsel yapılardan ve bu cebirsel yapıların özelliklerinden bahsedilmiş, bazı temel tanımlar ve teoremler verilmiştir. Bu kısım için Wan [1], Hungerford [2], Hill [3], Ling ve Xing [4] ve Ding *ve diğ.*[5] kaynaklardan faydalanılarak hazırlanmıştır.

Tanım 2.1.1. Boş olmayan bir T kümesi için $T \times T$'den T'ye tanımlanan her fonksiyon, T kümesi üzerinde bir ikili işlem olarak adlandırılır. İkili işlem genellikle $*$ sembolüyle gösterilir. $k,l \in T$ için işlem sonucu $k*l$ olarak yazılır ve bu ifade, (k,l) ikilisinin fonksiyon altındaki görüntüsünü temsil eder; yani $*(k,l) = k*l$.

Tanım 2.1.2. Üzerinde en azından bir tane ikili işlem tanımlanmış olan bir T kümesi cebirsel yapı olarak adlandırılır ve genellikle $(T,*)$ ile gösterilir.

Tanım 2.1.3. Boş olmayan bir T kümesi üzerinde tanımlanmış "$*$" ikili işlemi

- Her $k,l,m \in T$ için $(k*l)*m = k*(l*m)$ (birleşme özelliği),
- Her $k \in T$ için $k*e = e*k = k$ olacak şekilde en az bir $e \in T$ vardır (birim eleman özelliği),

- Her $k \in T$ için $k * k^{-1} = k^{-1} * k = e$ olacak şekilde tek türlü belirli bir $k^{-1} \in T$ vardır (ters eleman özelliği)

koşullarını sağlanıyorsa $(T, *)$ cebirsel yapısına bir grup denir.

Tanım 2.1.4. $(T, *)$ cebirsel yapısı bir grup olsun. Her $k, l \in T$ için $k * l = l * k$ oluyorsa $(G, *)$ cebirsel yapısına bir komütatif (değişmeli) grup denir.

Tanım 2.1.5. T kümesi sonlu sayıda eleman içeriyorsa $(T, *)$ grubuna sonlu grup denir. T'nin eleman sayısına grubun mertebesi denir ve $\mid T \mid$ ile gösterilir.

Tanım 2.1.6. T bir grup olsun. Eğer $A \subseteq T$ ve A kümesi, T'de tanımlanan işleme göre bir grup oluşturuyorsa, A'ya T'nin bir alt grubu denir.

Tanım 2.1.7. Boş olmayan bir H kümesi üzerinde tanımlı ikili işlemler $*$ ve $\sim$ ile gösterilsin. O halde her $k, l, m/inH$ in

- $(H, *)$ cebirsel yapısı bir komütatif grup,
- $(k \sim l) \sim m = k \sim (l \sim m)$ ($\sim$ işleminin birleşme özelliği),
- $k * (l \sim m) = (k * l) \sim (k * m)$ ve $(l \sim m) * k = (l * k) \sim (m * k)$ ($*$ işleminin $\sim$ işlemi üzerine dağılma özelliği)

koşulları sağlanıyorsa $(H, *, \sim)$ cebirsel yapısına halka denir. Kolaylık olması için $(H, *, \sim)$ halkası kısaca H ile gösterilir.

Tanım 2.1.8. Bir $(H, *, \sim)$ halkasının $*$ işlemine göre birim elemanına H halkasının sıfırı denir ve genellikle O_H ile gösterilir. H halkasının $\sim$ ikili işlemine göre birim elemanı varsa bu elemana H halkasının çarpımsal birimi veya halkanın birimi denir ve genellikle 1_H ile gösterilir. Çarpımsal birimi olan halkalara birimli halka denir. Ayrıca, H halkasının $\sim$ işlemi her $k, l \in H$ için $k \sim l = l \sim k$ koşulunu sağlıyorsa bu halka komütatif halka olarak adlandırılır.

Tanım 2.1.9. Birimli bir H halkasının birimi $1_H \neq 0_H$ olsun. Bir $u \in H$ için $uv = vu = 1_H$ olacak şekilde bir $v \in H$ varsa u'ya halkanın aritmetik birimi denir.

Teorem 2.1.10. *Bir H halkasının $k, l, m \in H$ elemanları için aşağıdaki ifadeler doğrudur:*

i) $k+m=l+m$ *ise* $k=l$,

ii) $0_H\,k=k\,0_H=0_H$,

iii) $-(-k)=k$,

(iv) $-(k+l)=(-k)+(-l)$,

v) $(-k)l=k(-l)=-kl$,

vi) $(-k)(-l)=kl$,

vii) H'nin birim elemanı varsa tek türlü belirlidir,

viii) H birimli halka ise $-k=(-1_H)\,k$.

Tanım 2.1.11. Bir H halkasında, sıfırdan farklı k ve l elemanları için $kl=0_H$ eşitliği sağlanıyorsa, k ve l elemanlarına H'nin sıfır bölenleri denir. Eğer bir halkada en az bir sıfır bölen bulunuyorsa bu halkaya sıfır bölenli halka, sıfır böleni yoksa sıfır bölensiz halka denir.

Tanım 2.1.12. Eğer bir halka, birim elemana sahip (birimli), komütatif ve sıfır bölen içermiyorsa, bu halka tamlık bölgesi olarak adlandırılır.

Tanım 2.1.13. Bir H halkasının $h\in H$ elemanı için $h^2=h$ ise h'ye H halkasının idempotent elemanı denir.

Tanım 2.1.14. Bir H halkasının iki idempotenti k,l olsun. $kl=lk=0_H$ ise k ve l'ye ortogonal idempotent elemanlar denir.

Tanım 2.1.15. Bir H halkasının boştan farklı bir S alt kümesi, H içindeki aynı toplama ve çarpma işlemleriyle bir halka yapısı oluşturuyorsa, S'ye H halkasının bir alt halkası denir.

Önerme 2.1.16. *Bir H halkasının boştan farklı bir S alt kümesinin bir alt halka olması için gerek ve yeter koşul (g.y.k.) her* $k,l\in S$ *elemanı için* $k-l\in S$ *ve* $k\cdot l\in S$ *olmasıdır.*

Tanım 2.1.17. H bir halka ve $\emptyset\neq I\subseteq H$ olsun. I kümesi

- $k,l\in I$ için $k-l\in I$,
- $h\in H$ ve $k\in I$ için $hk\in I$,

koşullarını sağlıyorsa I, H halkasının bir sağ ideali olarak adlandırılır. Benzer şekilde, $k \in I$ ve $h \in H$ için $kh \in I$ sağlanıyorsa I, H halkasının bir sol idealidir. Eğer I, hem sağ ideal olma hem de sol ideal olma koşullarını sağlıyorsa, I'ya kısaca ideal denir.

Her halkada aşağıdaki iki özel ideal bulunur:

- H'nin kendisi: H,
- Sıfır ideali: $\{0_H\}$.

Bu iki ideale aşikar (trivial) idealler denir. H'nin kendisi dışında kalan ideallere ise öz (non-trivial) idealler adı verilir.

Tanım 2.1.18. Bir H halkasının iki ideali I, J olsun. O halde

- $I+J = \{i+j \mid \ i \in I, j \in J\}$ idealine I ve J idealinin toplamı denir.
- $I \cdot J = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n \mid \ a_i \in I, b_i \in J, n \in \mathbb{Z}, i = 1,2,\ldots,n\}$ idealine I ve J idealinin çarpımı denir.

Tanım 2.1.19. Bir H halkasının iki ideali I ile J olsun. $I+J=H$ ise I ve J ideallerine komaksimal (comaximal) ideal denir.

Bir H halkasının bir ideali I olsun. H'nin k ve l elemanları arasında

$$k \equiv l \pmod{I} \quad \Leftrightarrow \quad k-l \in I$$

şeklinde tanımlanan bağıntı H üzerinde bir denklik bağıntısıdır. Bu denklik bağıntısı H'yi denklik sınıflarına ayırır. H'nin bu bağıntıya göre denklik sınıflarının kümesi H/I şeklinde gösterilir. $k \in H$ elemanı için $k+I \in H/I$ dır. $l \in H$ için $l \in k+I$ olması için g.y.k. $l \equiv k \pmod{I}$ olmasıdır. $I = 0$ için $H/I = H$'dir. $H/I = \{k+I \mid k \in H\}$ kalan sınıfları kümesi üzerinde toplama ve çarpma işlemleri, sırasıyla,

$$(k+I)+(l+I) = (k+l)+I \quad \text{ve} \quad (k+I)\cdot(l+I) = (kl)+I \tag{2.1}$$

şeklinde tanımlanır.

Teorem 2.1.20. *$(k+I)$ ve $(l+I)$ kalan sınıfları için (2.1)'de tanımlanan toplama ve çarpma işlemleri $(k+I)$ ve $(l+I)$ kalan sınıfınlarındaki k ve l elemanlarının özel seçiminden bağımsızdır. Üstelik H/I, (2.1)'de tanımlanan işlemlere göre bir halkadır. H/I halkası H'nin I'ya göre bölüm halkası olarak adlandırılır.*

Tanım 2.1.21. Bir H komütatif halkasının bir alt kümesi $A = \{a_1, a_2, \ldots, a_n\}$ olsun.

$$\langle A \rangle = \{a_1 r_1 + a_2 r_2 + \cdots + a_n r_n \mid r_1, r_2, \ldots, r_n \in H\}$$

idealine H'nin A kümesi ile üretilen ideali denir. $A = \{a\}$ ise $\langle A \rangle$'a esas ideal denir ve kısaca $\langle a \rangle$ ile gösterilir.

Tanım 2.1.22. Bir H halkasının bir öz ideali M olsun. $M \subseteq J \subseteq H$ koşulunu sağlayan her J ideali için $J = M$ veya $J = H$ ise yani H, M'yi içeren başka bir ideale sahip değilse M'ye bir maksimal ideal denir.

Tanım 2.1.23. Bir H halkasının sıfır elemanı 0_H olsun. Her $k \in H$ için $mk = 0_H$ olacak şekilde bir m pozitif tam sayısı varsa bu eşitliği sağlayan en küçük pozitif tam sayıya H'nin karakteristiği denir. Eğer bu şekilde bir tam sayı yoksa H'nin karakteristiği sıfırdır, denir.

Teorem 2.1.24. *H birimli bir halka ve birimi 1_H olsun. Her m pozitif tam sayısı için $m1_H \neq 0_H$ ise H'nin karakteristiği sıfırdır. Eğer $m1_H = 0_H$ olacak şekilde m tam sayıları varsa bu tam sayıların en küçüğü H'nin karakteristiğidir.*

Tanım 2.1.25. Boştan farklı bir K kümesi üzerinde tanımlı, sırasıyla, toplama ve çarpma olarak adlandırılan iki işlem $+$ ve $\cdot$ ile gösterilsin. Eğer

- $(K, +)$ bir abelyen grup,
- 0, $(K, +)$ grubunun sıfırı olmak üzere $K^* = K \setminus \{0\}$ kümesi için $(K^*, \cdot)$ bir abelyen grup,
- Her $k, l, m \in K$ için $k(l+m) = kl + km$

koşulları sağlanıyorsa K'ye bir cisim denir.

Teorem 2.1.26. *Bir tamlık bölgesinin sıfırdan farklı her elemanının çarpmaya göre tersi varsa bu tamlık bölgesi bir cisimdir.*

Tanım 2.1.27. *K* bir cisim olsun. *K*'deki elemanların sayısı sonsuz ise *K*'ye sonsuz cisim denir. Eğer *K*'deki elemanların sayısı sonlu ise *K*'ye sonlu cisim veya Galois cismi denir.

Teorem 2.1.28. *K bir cisim olsun. O halde her* $k,l,m \in K$ *için*

(i) $km = lm$ *ve* $m \neq 0$ *ise* $k = l$,

(ii) $kl = 0$ *ise* $k = 0$ *ya da* $l = 0$

sağlanır.

Teorem 2.1.29. *K bir cisim olsun. O halde sıfırdan farklı her* $k,l \in K$ *elemanları için*

(i) $(k^{-1})^{-1} = k$,

(ii) $(kl)^{-1} = k^{-1}l^{-1}$,

(iii) $(-k)^{-1} = -k^{-1}$

sağlanır.

Bir *K* cisminin bir *k* elemanı ve bir *n* pozitif tam sayısı için *n* tane *k*'nin toplamı *nk* ile gösterilir, yani

$$nk = \underbrace{k+k+\cdots+k}_{n \text{ tane}}$$

şeklindedir. Özel olarak $0k = 0$ olarak tanımlanır. Eğer *n* bir pozitif tam sayı ise $-n$ bir negatif tam sayıdır ve $(-n)k = -(nk)$ olarak tanımlanır.

Teorem 2.1.30. *K bir cisim ve* m,n *tam sayılar olsun. Her* $k,l \in K$ *için*

(i) $(m+n)k = mk+nk \quad ve \quad (mn)k = m(nk)$

(ii) $n(k+l) = nk+nl$

(iii) $(mk)(nl) = (mn)(kl)$

sağlanır.

K cisminin bir k elemanı ve bir n pozitif tam sayısı için k'nın n kez çarpımı k^n ile gösterilir, yani

$$k^n = \underbrace{k\,k\,\ldots\,k}_{n \text{ tane}}$$

şeklindedir. Özel olarak $k \neq 0$ için $k^0 = e$ olarak tanımlanır. Ayrıca bir n pozitif tam sayı için $-n$ negatif tam sayıdır ve $k^{-n} = (k^{-1})^n$ olarak tanımlanır.

Teorem 2.1.31. *K bir cisim ve m,n tam sayılar olsun. Her $a,b \in K$ için*

(i) $a^{m+n} = a^m a^n$ *ve* $a^{mn} = (a^m)^n$ *dır, burada* $a = 0$ *ise* $m > 0$ *ve* $n > 0$ *olmalıdır.*

(ii) $(ab)^m = a^m b^m$ *dır, burada* $a = 0$ *veya* $b = 0$ *ise* $m > 0$ *olmalıdır.*

Teorem 2.1.32. ***(Binom Teoremi)*** *Bir K cisminin her a,b elemanı için*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$$

sağlanır, burada n bir pozitif tam sayıdır ve $\binom{n}{i} = \frac{n!}{i!(n-i)!}$ *eşitliği n elemandan i tanesinin seçiminin sayısıdır.*

Önerme 2.1.33. *Bir cismin karakteristiği,* 1 *elemanının kendisiyle kaç kez toplandığında* 0 *elde edildiğini belirler. Eğer bu hiçbir zaman* 0 *vermezse, karakteristik* 0 *kabul edilir. Aksi hâlde, en küçük pozitif tam sayı olan p için* $p \cdot 1 = 0$ *olur ve bu durumda karakteristik p asal olmak zorundadır.*

Lemma 2.1.34. *K, karakteristiği bir p asal sayısı olan bir cisim oldun. $a,b \in K$ elemanları için*

(i) $(a+b)^p = a^p + b^p$

(ii) $(a-b)^p = a^p - b^p$

(iii) $a_1, a_2, \ldots, a_m \in K$ *için* $(a_1 + a_2 + \cdots + a_m)^p = a_1^p + a_2^p + \cdots + a_m^p$

sağlanır.

Tanım 2.1.35. H bir halka ve x bir bilinmeyen olsun. r_m sıfırdan farklı olmak üzere $r_0, r_1, \ldots, r_m \in H$ için

$$r(x) = r_0 + r_1 x + \cdots r_m x^m = \sum_{i=0}^{m} r_i x^i$$

şeklinde tanımlanan toplama derecesi m olan H üzerinde bir polinom denir ve $r(x)$ polinomunun derecesi $\deg r(x) = m$ şeklinde gösterilir. $r_0, r_1, \ldots, r_m$ elemanlarına $r(x)$ polinomunun katsayıları ve r_m katsayısına baş katsayı denir. Eğer $r_m = 1$ ise bu polinom monik polinom olarak adlandırılır. Özel olarak $r(x) = 0$ polinomunun derecesi $-\infty$ olarak tanımlanır. $H[x]$ ile katsayıları H'de olan polinomların kümesi gösterilir.

$H[x]$'de iki polinom

$$r(x) = \sum_{i=0}^{n} = a_i x^i \,, \quad s(x) = \sum_{i=0}^{m} = b_i x^i$$

ve $M = max\{n, m\}$ olsun. $H[x]$ üzerinde toplama ve çarpma işlemi, sırasıyla,

$$r(x) + s(x) = \sum_{i=0}^{M} (a_i + b_i) x^i \quad \text{ve} \quad r(x)s(x) = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) x^i \tag{2.2}$$

şeklinde tanımlanır. $H[x]$ kümesi (2.2)'de tanımlı işlemlere göre bir halkadır. $H[x]$'e H üzerindeki tek değişkenli (x'e bağlı) polinom halkası denir. $H[x]$'in sıfırı H'nin sıfırı olan 0_H dir. Eğer H komütatif bir halka ise $H[x]$ de komütatiftir. Eğer H birimli bir halka ise $H[x]$ de birimlidir ve birimi H'nin birimi olan 1_H'dir.

Teorem 2.1.36. *Bir H halkası için $r(x), s(x) \in H[x]$ olsun. O halde*

$$\deg(r(x)s(x)) \leq \deg r(x) + \deg s(x) \quad \textit{ve} \quad \deg(r(x) + s(x)) \leq \max\{\deg r(x), \deg s(x)\}$$

sağlanır. Eğer H bir tamlık bölgesi ise sıfırdan farklı $r(x), s(x) \in H[x]$ polinomları için $\deg(r(x)s(x)) = \deg r(x) + \deg s(x)$ *dır.*

Teorem 2.1.37. *H komütatif birimli bir halka ve $l(x)$'in baş katsayısı H'de bir aritmetik birim olmak üzere $k(x), l(x) \in H[x]$ için*

$$k(x) = q(x)l(x) + r(x), \quad \deg r(x) < \deg l(x) \;\; \textit{veya} \;\; r(x) = 0$$

olacak şekilde tek türlü belirli $q(x)$ bölüm polinomu ve $r(x)$ kalan polinomu vardır.

Sonuç 2.1.38. K bir cisim olsun. $s(x) \neq 0$ olmak üzere her $r(x), s(x) \in K[x]$ polinomuna Teorem 2.1.37'deki bölme algoritması uygulanabilir.

Önerme 2.1.39. *(i) D bir tamlık bölgesi ise $D[x]$ bir tamlık bölgesidir.*

(ii) K bir cisim ise $K[x]$ bir tamlık bölgesidir.

H komütatif birimli bir halka olmak üzere

$$r(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

polinomu $H[x]$'te bir polinom ve $\alpha \in H$ olsun. $r(x)$ polinomunda x yerine α yazılarak elde edilen sonuç H'nin elemanıdır, bu elemana $r(x)$ polinomunun $x = \alpha$'daki değeri denir ve $r(\alpha)$ ile gösterilir. $r(\alpha) = 0$ ise α'ya $r(x)$ polinomunun kökü denir.

Aşağıdaki teorem bölme algoritmasından elde edilir.

Teorem 2.1.40. *$r(x)$, $H[x]$'te bir polinom ve $\alpha \in H$ olsun. $r(x)$ polinomunun $x - \alpha$ ile bölümünden kalan $r(\alpha)$'dır.*

Sonuç 2.1.41. $r(x)$, $H[x]$'te bir polinom ve $\alpha \in H$ olsun. α'nın $r(x)$'in bir kökü olması için g.y.k. $x - \alpha \mid r(x)$ olmasıdır.

Teorem 2.1.42. *$r(x), k(x), l(x) \in H[x]$ ve $r(x) \neq 0$ olsun. $r(x) \mid k(x)l(x)$ ve $ebob(r(x), k(x)) = 1$ ise o halde $r(x) \mid l(x)$'tir.*

Lemma 2.1.43. *$k(x), l(x) \in H[x]$ olsun. $ebob(k(x), l(x)) = 1$ ise $k(x)m(x) + l(x)n(x) = 1$ olacak şekilde $m(x), n(x) \in H[x]$ vardır.*

Tanım 2.1.44. H bir halka olsun. $r(x) \in H[x]$ için $r(x) = k(x)l(x)$ olacak şekilde $\deg k(x)$, $\deg l(x) < \deg r(x)$ koşulunu sağlayan $k(x), l(x) \in H[x]$ polinomları bulunabiliyorsa $r(x)$ polinomuna indirgenebilir denir. Bir polinom indirgenebilir değilse indirgenemez olarak adlandırılır.

$H[x]$ polinomlar kümesinde derecesi $r(x)$'in derecesinden küçük olan polinomların kümesi $H[x]/\langle r(x)\rangle$ ile gösterilecektir, yani $\deg r(x) = n$ olmak üzere

$$H[x]/\langle r(x)\rangle = \left\{ \sum_{i=0}^{n-1} a_i x^i \mid i = 0, 1, \ldots, n-1 \text{ için } a_i \in H \right\}$$

şeklinde tanımlıdır. Polinomlar üzerinde tanımlı $(\text{mod } r(x))$'e göre toplama ve çarpma işlemleri ile bu küme bir halkadır.

Teorem 2.1.45. *$H[x]/\langle r(x)\rangle$ halkasının bir cisim olması için g.y.k. $r(x)$'in $H[x]$'te indirgenemez olmasıdır.*

Tanım 2.1.46. Bir $r(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_0$ polinomu için

$$r^*(x) = x^k r(x^{-1})$$

yani $r^*(x) = a_0 x^k + a_1 x^{k-1} + \cdots + a_k$ şeklinde tanımlanan fonksiyona $r(x)$ polinomunun **resiprokal polinomu** denir. Eğer

$$r(x) = \varepsilon r^*(x)$$

olacak şekilde bir ε aritmetik birimi varsa $r(x)$'e **kendine resiprokal polinom** denir. Özel olarak

$$(r^*(x))^* = r(x) \quad \text{ve} \quad (r(x)s(x))^* = r^*(x)s^*(x)$$

dır. $r(x)$, $x^n - 1$'in indirgenemez ve kendine resiprokal olmayan bir böleni ise $r^*(x)$ de $x^n - 1$'in indirgenemez ve kendine resiprokal olmayan bir bölenidir. Bu şekildeki $r(x)$ ve $r^*(x)$ polinomları, indirgenemez resiprokal polinom çifti olarak adlandırılır.

Tanım 2.1.47. H ve S iki halka olsun. $\varphi : H \to S$ dönüşümü her $k, l \in H$ için

- $\varphi(k+l) = \varphi(k) + \varphi(l)$
- $\varphi(kl) = \varphi(k)\varphi(l)$

koşullarını sağlıyorsa φ'ye bir halka homomorfizması denir.

Tanım 2.1.48. $\varphi : H \to S$ bir halka homomorfizması olsun. $\{k \in H \mid \varphi(k) = 0_H\}$ kümesine homomorfizmanın çekirdeği (kernel) denir. φ homomorfizmasının çekirdeği $ker\ \varphi$ ile gösterilir.

Tanım 2.1.49. Hem birebir hem örten olan bir homomorfizmaya izomorfizma denir.

Önerme 2.1.50. *H bir komütatif ve birimli halka olsun.*

i) $I+J=H$ *ise* $IJ=I\cap J$*'dir.*

ii) $I_1,I_2,\ldots,I_n$ *ikişerli olarak komaksimal ise* $I_1I_2\cdots I_n=\bigcap_{i=1}^{n}I_i$*'dir.*

İspat. i) $r\in IJ$ olsun. O halde $i\in I$ ve $j\in J$ için $r=ij$'dir. I ve J ideal olduğundan $r\in I$ ve $r\in J$'dır. O halde $r\in I\cap J$'dir. Böylece $IJ\subseteq I\cap J$'dir. I ve J idealleri için $I+J=H$ olduğundan $(I+J)(I\cap J)=(I\cap J)$ olur. Diğer yandan

$$(I+J)(I\cap J)=I(I\cap J)+J(I\cap J)=II\cap IJ+JI\cap JJ\subseteq IJ$$

sağlandığından $I\cap J\subseteq IJ$ elde edilir. Dolayısıyla $I+J=H$ ise $IJ=I\cap J$'dir.

ii) İspat n üzerinden tümevarımla yapılır. $n=2$ iken doğru olduğu (i) kısmında yapıldı. $n>2$ için $I_1I_2\cdots I_{n-1}=\bigcap_{i=1}^{n-1}I_i$ olduğu kabul edilsin. $J:=\prod_{i=1}^{n-1}I_i=\bigcap_{i=1}^{n-1}I_i$ olsun. $1\leq i\leq n-1$ için $I_i+I_n=H$ olduğundan $x_i+y_i=1$ olacak şekilde $x_i\in I_i$ ve $y_i\in I_n$ vardır. $x_i\in I_i$ elemanlarının çarpımı ile $\prod_{i=1}^{n-1}x_i=\prod_{i=1}^{n-1}(1-y_i)\equiv 1 \pmod{I_n}$'dir, yani $x=x_1\ldots x_{n-1}$ olmak üzere $x+y=1$ olacak şekilde $x\in J$ ve $y\in I_n$ elemanları vardır. Böylece $J+I_n=H$ elde edilir. O halde $\prod_{i=1}^{n}I_i=JI_n=J\cap I_n=\bigcap_{i=1}^{n}I_i$'dir.

□

Çinlilerin Kalan Teoremi ile Peirce ayrışımı, özellikle sonlu halka yapıların anlaşılmasında ve çözümlemesinde oldukça etkili yöntemler sunar. Çinlilerin Kalan Teoremi, bir yapının daha küçük ve birbirinden bağımsız alt yapılara ayrılmasını sağlar ve böylece başlangıçta karmaşık olan ilişkileri sadeleştirir. Peirce ayrışımı ise, halkadaki birim elemanın belirli yapı taşlarıyla parçalanması yoluyla, halkayı bu yapı taşlarına karşılık gelen daha küçük bileşenlerin direkt toplamı şeklinde ifade etme imkanı tanır. Bu iki yaklaşım yalnızca soyut yapının analizini kolaylaştırmakla kalmaz, aynı zamanda kodlama teorisi gibi uygulamalı alanlarda da önemli hesaplama avantajları sunar. Özellikle kodlama teorisinde, bu yöntemlerin kullanılması sayesinde, bir kod yapısının her bileşeninin ayrı ayrı ele alınarak analiz edilebilme imkanı doğar. Böylece, başlangıçta karmaşık görünen bir kod, daha basit alt kodlara indirgenmiş olur ve bu alt kodların özellikleri incelenerek ana yapıya dair bilgi elde

edilir. Bu yaklaşım, yalnızca teorik çözümlerde değil, aynı zamanda algoritma geliştirme süreçlerinde de önemli bir rol oynar.

Teorem 2.1.51 (Çinlilerin Kalan Teoremi (İki İdeal İçin))**.** *H komütatif bir halka ve I, J bu halkada $I+J=H$ olacak şekilde iki ideal ise $H/(I\cap J)\cong H/I\oplus H/J$'dir.*

İspat. H komütatif halkasının $I+J=H$ koşulunu sağlayan I ve J idealleri ile tanımlanan

$$\begin{aligned}\phi : H &\to H/I\oplus H/J\\ r &\mapsto (r+I, r+J)\end{aligned}$$

dönüşüm bir izomorfizmadır. Çünkü

i) ϕ iyi tanımlıdır: $r,s\in H$ için $r=s$ olsun. Bu durumda $\phi(r)=(r+I,r+J)$ ve $\phi(s)=(s+I,s+J)$ olur. $r=s$ olduğundan $r+I=s+I$ ve $r+J=s+J$ dır. Buradan $(r+I,r+J)=(s+I,s+J)$. Böylece $\phi(r)=\phi(s)$'dir.

ii) ϕ işlemleri korur:

$$\phi(a+b)=(a+b+I,a+b+J)=(a+I,a+J)+(b+I,b+J)=\phi(a)+\phi(b)$$

ve

$$\begin{aligned}\phi(ab) &= (ab+I,ab+J)=((a+I)(b+I),(a+J)(b+J))\\ &= (a+I,a+J)(b+I,b+J)=\phi(a)\phi(b).\end{aligned}$$

iii) ϕ örtendir: $a,b\in H$ için $(\overline{a},\overline{b})\in H/I\oplus H/J$ olsun. O halde

$$(\overline{a},\overline{b})=(a+I,b+J)\in H/I\oplus H/J$$

dir. $H=I+J$ olduğundan $a=x+y$ ve $b=s+t$ olacak şekilde x, $s\in I$ ve y, $t\in J$ elemanları vardır. $s\in I$ ve $y\in J$ olduğundan

$$\phi(y+s)=(y+s+I,y+s+J)=(y+I,s+J)$$

elde edilir. Diğer taraftan $x \in I$ ve $t \in J$ olduğundan

$$(\overline{a},\overline{b}) = (a+I, b+J) = (x+y+I, s+t+J) = (y+I, s+J)$$

olur. Dolayısıyla $\phi(y+s) = (\overline{a},\overline{b})$'dir. O halde ϕ örtendir. Birinci İzomorfizma Teoremi'nden $H/\ker\phi \cong \phi(H)$'dir. $\phi(H) = H/I \oplus H/J$ olduğundan $H/\ker\phi \cong H/I \oplus H/J$ elde edilir.

iv) $\ker\phi = I \cap J$'dir: $r \in I \cap J$ olsun. O halde $r \in I$ ve $r \in J$'dir. Buradan

$$\phi(r) = (r+I, r+J) = (I, J)$$

olur. Dolayısıyla $r \in \ker\phi$'dır, böylece $I \cap J \subseteq \ker\phi$'dir. Diğer taraf için $b \in \ker\phi$ olsun. O halde $(b+I, b+J) = \phi(b) = (I,J)$'dir. Böylece $b \in I$ ve $b \in J$ olur. Buradan $b \in I \cap J$'dır, böylece $\ker\phi \subseteq I \cap J$'dır.

Böylece $H/(I \cap J) \cong H/I \oplus H/J$ elde edilir. □

Teorem 2.1.52 (Çinlilerin Kalan Teoremi (n İdeal İçin))**.** *H bir halka ve $I_1, I_2, ..., I_n$, H halkasının ikişerli aralarında asal idealler, yani her $i \neq j$ için $I_i + I_j = H$ ve $I = \bigcap_{i=1}^{n} I_i$ ise $H/I \cong H/I_1 \oplus H/I_2 \oplus \cdots \oplus H/I_n$'dır.*

İspat. H'nin ideal sayısı üzerinden tümevarım ile ispat yapılır. $n = 1$ için $H/I \cong H/I$'dır. n tane ideal için verilen ifadenin doğru olduğu, yani H'nin $I_1, I_2, ..., I_n$ idealleri çiftler halinde aralarında asal (yani her $i \neq j$ için $I_i + I_j = H$) ve $I = \bigcap_{i=1}^{n} I_i$ ise $H/I \cong H/I_1 \oplus H/I_2 \oplus \cdots \oplus H/I_n$ olduğu kabul edilsin. $J = I_{n+1}$ olarak alınırsa Teorem 2.1.51'den

$$H/(I \cap J) \cong H/I \oplus H/J \cong H/I_1 \oplus H/I_2 \oplus \cdots \oplus H/I_n \oplus H/J$$

olur. Böylece $I = \bigcap_{i=1}^{n+1} I_i$ olmak üzere

$$H/I \cong H/I_1 \oplus H/I_2 \oplus \cdots \oplus H/I_n \oplus H/I_{n+1}$$

elde edilir. □

Teorem 2.1.53 (Peirce Ayrışımı)**.** *Bir H komütatif halkasının sıfırdan farklı ortogonal*

idempotentleri $e_1, e_2, \ldots e_n$ *olsun. Eğer* $\sum_{i=1}^{n} e_i = 1$ *ise*

$$H = e_1H \oplus e_2H \oplus \cdots \oplus e_nH$$

dir.

İspat. H komütatif halkasının sıfırdan farklı ortogonal idempotentleri $e_1, e_2, \ldots e_n$ olsun. $e_1, e_2, \ldots e_n$ sıfırdan farklı ortogonal idempotentler olduğundan

$$i \neq j \Rightarrow e_ie_j = 0 \quad \text{ve} \quad i = j \Rightarrow e_je_j = e_j^2 = e_j$$

dır. Her $r \in H$ elemanı için

$$r = 1r = \left(\sum_{i=1}^{n} e_i\right) r = \sum_{i=1}^{n} e_ir$$

ve $e_ir \in e_iH$ olduğundan

$$r = \sum_{i=1}^{n} e_ir \in \sum_{i=1}^{n} e_iH$$

elde edilir. Dolayısıyla $H = e_1H + e_2H + \cdots + e_nH$'dir. Direkt toplam olduğunu göstermek için $e_kH \cap \left(\sum_{i\neq k}^{n} e_iH\right) = \{0\}$ olduğu gösterilmelidir: $y \in e_kH \cap \left(\sum_{i\neq k}^{n} e_iH\right)$ olsun. Bu durumda

$$y = e_kr_k$$

olacak şekilde bir $r_k \in H$ vardır. Aynı zamanda

$$y = \sum_{i\neq k} e_ir_i$$

olacak şekilde $i \neq k$ için $r_i \in H$ vardır. Buradan $y = e_kr_k$ olduğundan,

$$e_ky = e_k(e_kr_k) = e_k^2r_k = e_kr_k = y$$

olur. Diğer yandan, $y = \sum_{i \neq k} e_i r_i$ olduğundan,

$$e_k y = e_k \left(\sum_{i \neq k} e_i r_i \right) = \sum_{i \neq k} e_k (e_i r_i)$$

olur. Böylece $i \neq k$ için $e_k e_i = 0$ olduğundan

$$e_k y = \sum_{i \neq k} (e_k e_i) r_i = \sum_{i \neq k} 0 \, r_i = 0$$

elde edilir. Bu durumda $y = e_k y = 0$ bulunur. O halde

$$e_k H \cap \left(\sum_{i \neq k} e_i H \right) = \{0\}$$

olup toplamın direkt olduğu elde edilir. □

Tanım 2.1.54. n ile q aralarında asal olmak üzere q'nun modülo n'ye göre i'yi içeren döngüsel (cyclotomic) koseti

$$C_i = \{(iq^j (mod n)) \in \mathbb{Z}_n ; j = 0, 1, ...\}$$

dir. Diğer bir ifade ile $(n, q) = 1$ olmak üzere $0 \leq i \leq n$ olacak şekilde bir i tam sayı ve $q^k i \equiv i \pmod{n}$ olacak şekilde bir k pozitif tam sayısı için

$$C_i = \{i, qi, q^2 i, \ldots, q^{k-1} i\} \pmod{n}$$

kümesine modülo n'de i'nin q-döngüsel koseti denir.

Tanım 2.1.55. C_i bir döngüsel koset olmak üzere $n - i \in C_i$ ise C_i'ye simetriktir denir. Aksi takdirde asimetriktir denir. $n - i \equiv -i \pmod{n}$ olduğundan $C_{-i} = C_{n-i}$'dir ve asimetrik kosetler C_i ve C_{-i} şeklinde çiftler halinde bulunur.

Örnek 2.1.56. Modülo 15'te 2'nin döngüsel kosetleri

$$C_0 = \{0.2^j \ (mod 15);\ j = 0,1,...\} = \{0\}$$
$$C_1 = \{1.2^j \ (mod 15);\ j = 0,1,...\} = \{1,2,4,8\}$$
$$C_3 = \{3.2^j \ (mod 15);\ j = 0,1,...\} = \{3,6,9,12\}$$
$$C_5 = \{5.2^j \ (mod 15);\ j = 0,1,...\} = \{5,10\}$$
$$C_7 = \{7.2^j \ (mod 15);\ j = 0,1,...\} = \{7,11,13,14\}$$

şeklindedir. Burada $C_1 = C_2 = C_4 = C_8$'dir. Ayrıca $C_3 = C_6 = C_9 = C_{12}, C_5 = C_{10}$ ve $C_7 = C_{11} = C_{13} = C_{14}$'tür. Üstelik $\{0,1,3,5,7\}$ kümesi modülo 15'te 2'nin döngüsel kosetlerinin bir tam temsilci kümesidir.

Örnek 2.1.57. Modülo 21'de 2'nin döngüsel kosetleri

$$C_0 = \{0.2^j \ (mod 21);\ j = 0,1,...\} = \{0\}$$
$$C_1 = \{1.2^j \ (mod 21);\ j = 0,1,...\} = \{1,2,4,8,11,16\}$$
$$C_3 = \{3.2^j \ (mod 21);\ j = 0,1,...\} = \{3,6,12\}$$
$$C_5 = \{5.2^j \ (mod 21);\ j = 0,1,...\} = \{5,10,13,17,19,20\}$$
$$C_7 = \{7.2^j \ (mod 21);\ j = 0,1,...\} = \{7,14\}$$
$$C_9 = \{9.2^j \ (mod 21);\ j = 0,1,...\} = \{9,15,18\}$$

şeklindedir. Dolayısıyla $\{0,1,3,5,7,9\}$ kümesi modülo 21'de 2'nin döngüsel kosetlerinin bir tam temsilci kümesidir.

2.2. VEKTÖR UZAYI VE MODÜL

Vektör uzayları, cebirin temel yapı taşlarından biri olup, herhangi bir cisim üzerinde tanımlanırlar. Bir vektör uzayı, bir cisim üzerinde tanımlanan toplama ve skalerle çarpma işlemleri altında belirli aksiyomları sağlayan bir yapıdır. Cismin sıfırdan farklı tüm elemanlarının çarpmaya göre tersinin olması vektör uzaylarına birçok güçlü cebirsel özellik kazandırır. Bu sayede, cebirsel işlemler yapmak büyük ölçüde kolaylaşır ve yapı daha iyi anlaşılabilir bir hale gelir. Diğer taraftan modül kavramı ise vektör uzaylarının daha genel bir biçimidir ve vektör uzaylarının bazı temel özelliklerini taşımakla birlikte, daha geniş ve esnek bir yapıda tanımlanır. Bir cisim üzerinde değil bir halka üzerinde tanımlanan modüller vektör uzaylarının halkalar düzeyine genelleştirilmiş halidir. Her vektör uzayı aynı zamanda

bir modül olarak da kabul edilebilirken her modül bir vektör uzayı değildir. Bu ilişki, vektör uzaylarının modüllerin özel bir durumu olduğunu da açıkça ortaya koymaktadır. Bir halka, genel itibariyle cisimden daha zayıf bir cebirsel yapı olduğundan, modüller de vektör uzaylarına kıyasla daha genel, fakat bazı yönlerden daha karmaşık yapılardır. Cisimlerin sahip olduğu düzen, vektör uzaylarını daha sade, öngörülebilir cebirsel yapılar haline getirip cebirsel işlem yapma kolaylığı sağlarken halkalar üzerinde tanımlanan modüller halkaların cebirsel yapısı nedeniyle daha genel ve teorik açıdan daha güçlü bir çerçeve sunar. Örneğin sıfır bölenlere sahip halkalar ya da birim elemana sahip olmayan halkalar ele alındığında, modül teorisi vektör uzayı kavramından büyük ölçüde farklılık gösterir. Bu yapısal farklılıklar sebebiyle modül çalışmaları vektör uzayları alanından daha fazla zorluklarla dolu olsa da daha zengin bir yapıya sahiptir ve daha fazla uygulama alanı sunar.

Tanım 2.2.1. W boş olmayan bir küme ve K bir cisim olsun. Her $k,l,m \in W$ ve her $\lambda,\mu \in K$ için

- $k+l \in W$,
- $(k+l)+m = k+(l+m)$,
- $0_W + k = k + 0_W = k$ olacak şekilde bir $0_W \in W$ vardır,
- $k+(-k) = (-k)+k = 0_W$ olacak şekilde her $k \in W$ için tek türlü belirli bir $-k \in W$ vardır,
- $k+l = l+k$,
- $\lambda l \in W$,
- $\lambda(k+l) = \lambda k + \lambda l$ ve $(\lambda+\mu)k = \lambda k + \mu k$,
- $(\lambda\mu)k = \lambda(\mu k)$,
- 1_K, K'nin çarpmaya göre birim elemanı olmak üzere $1_K k = k$

koşulları sağlanıyorsa W'ya K cismi üzerinde bir vektör uzayıdır denir.

Tanım 2.2.2. K cismi üzerinde bir W vektör uzayı için $\emptyset \neq U \subseteq W$ olsun. Eğer U, W'daki işlemlere göre bir vektör uzayı ise U'ya W'nin bir alt uzayı denir.

Teorem 2.2.3. *K cismi üzerinde bir W vektör uzayı için $\emptyset \neq U \subseteq W$ olsun. $k,l \in U$ ve $\lambda \in K$ olmak üzere U'nun W'nin bir alt uzayı olması için g.y.k.*

$$i)\ k+l \in U \quad ve \quad ii)\ \lambda k \in U$$

olmasıdır.

Örnek 2.2.4. $\mathbb{F}_q$ eleman sayısı q olan bir sonlu cisim olmak üzere $\mathbb{F}_q$ üzerinde sıralı n'lilerin kümesi $\mathbb{F}_q^n$ ile gösterilir ve

$$\begin{aligned}\mathbb{F}_q^n &= \underbrace{\mathbb{F}_q \times \mathbb{F}_q \times \cdots \times \mathbb{F}_q}_{n \text{ tane}} \\ &= \{(v_1, v_2, \cdots, v_n) \mid i = 1,2,\cdots,n \text{ için } v_i \in \mathbb{F}_q\}\end{aligned}$$

şeklinde ifade edilir. $v = (v_1, v_2, \ldots, v_n)$, $u = (u_1, u_2, \ldots, u_n) \in \mathbb{F}_q^n$ ve $\lambda \in \mathbb{F}_q$ olmak üzere

- $v + u = (v_1 + u_1, v_2 + u_2, \ldots, v_n + u_n)$
- $\lambda v = (\lambda v_1, \lambda v_2, \ldots, \lambda v_n)$

biçiminde tanımlanan, sırasıyla toplama ve skalerle çarpma işlemlerine göre $\mathbb{F}_q^n$, $\mathbb{F}_q$ cismi üzerinde bir vektör uzayıdır. $\mathbb{F}_q$'nun bir elemanına skaler, $\mathbb{F}_q^n$'nin bir elemanına uzunluğu n olan vektör denir.

Tanım 2.2.5. $a_1, a_2, \ldots, a_r \in K$ skalerleri ve $w_1, w_2, \ldots w_r \in W$ vektörleri için $a_1w_1 + a_2w_2 + \cdots + a_rw_r$ toplamına $w_1, w_2, \ldots w_r$ vektörlerinin lineer kombinezonu denir.

Tanım 2.2.6. W, K cismi üzerinde bir vektör uzayı olsun. $a_1, a_2, \ldots, a_r \in K$ skalerleri ve $w_1, w_2, \ldots w_r \in W$ vektörleri için

$$a_1w_1 + a_2w_2 + \cdots + a_rw_r = 0$$

denklemini sağlayan en az bir tane sıfırdan farklı $a_i \in K$ $(1 \leq i \leq r)$ skaleri varsa $\{w_1, w_2, \ldots w_r\}$ kümesine lineer bağımlıdır, denir. $\{w_1, w_2, \ldots w_r\}$ kümesi lineer bağımlı değilse yani $a_1w_1 + a_2w_2 + \cdots + a_rw_r = 0$ denkleminin tek çözümü $a_1 = a_2 = \cdots = a_r = 0$ ise $\{w_1, w_2, \ldots w_r\}$ kümesine lineer bağımsızdır, denir.

Sonuç 2.2.7. $w_1, w_2, \ldots w_r \in W$ vektörlerinin tüm lineer kombinezonları kümesi W'nin bir alt uzayıdır.

Tanım 2.2.8. K cismi üzerinde bir W vektör uzayının boştan farklı bir alt kümesi $S = \{w_1, w_2, \ldots, w_k\}$ olsun. S'deki vektörlerin tüm lineer kombinezonlarının kümesine S tarafından gerilen küme denir ve

$$\langle S \rangle = \{\lambda_1 w_1 + \lambda_2 w_2 + \cdots + \lambda_k w_k \ : \ \lambda_i \in K, i = 1, 2, \ldots, k\}$$

şeklinde ifade edilir. $S = \emptyset$ ise $\langle S \rangle = \{0\}$ dır. $\langle S \rangle = W$ ise S kümesi W'yı gerer, denir.

Sonuç 2.2.9. $\langle S \rangle$ kümesi W vektör uzayının bir alt uzayıdır.

Sonuç 2.2.10. S kümesi W'nın bir alt uzayı ise $\langle S \rangle = S$'dir.

Tanım 2.2.11. K cismi üzerinde bir W vektör uzayının bir alt kümesi $B = \{w_1, w_2, \ldots, w_k\}$ kümesi olsun. B alt kümesi W vektör uzayını gererse (yani $W = \langle B \rangle$ ise) ve B kümesi lineer bağımsız ise B kümesine W vektör uzayının bir bazı (tabanı) denir.

Tanım 2.2.12. Bir W vektör uzayının bir bazının eleman sayısına W'nin boyutu denir ve $Boy(W)$ ile gösterilir.

Teorem 2.2.13. *$\mathbb{F}_q$ sonlu cismi üzerinde bir W vektör uzayının boyutu k ise W'nın q^k tane elemanı vardır.*

Tanım 2.2.14. W, K üzerinde bir vektör uzayı olsun. $u = (u_1, u_2, \ldots, u_n)$, $w = (w_1, w_2, \ldots, w_n) \in W$ olmak üzere u ile w'nın iç çarpımı (Euclidean iç çarpımı)

$$u \cdot w = u_1 w_1 + u_2 w_2 + \cdots + u_n w_n$$

şeklinde tanımlanan bir skalerdir. Özel olarak $u \cdot w = 0$ ise bu vektörlere ortogonal vektörler denir.

Örnek 2.2.15. $\mathbb{F}_2^4$'te $(1,1,0,1)$ ve $(1,0,1,0)$ vektörlerinin iç çarpımı

$$(1,1,0,1) \cdot (1,0,1,0) = 1$$

dır.

Lemma 2.2.16. *W, K üzerinde bir vektör uzayı olsun. Her $u, v, w \in W$ ve her $\lambda, \mu \in K$ elemanları için*

(i) $u \cdot v = v \cdot u$,

(ii) $(\lambda u + \mu v) \cdot w = \lambda (u \cdot w) + \mu (v \cdot w)$

dır.

Tanım 2.2.17. H bir halka ve M bir komütatif grup olsun. Her $h, h_1, h_2 \in H$ ve $m, m_1, m_2 \in M$ olmak üzere

$$H \times M \to M$$
$$(h, m) \mapsto hm$$

şeklinde tanımlanan dönüşüm ile

- $h_1(m_1 + m_2) = h_1 m_1 + h_1 m_2$
- $(h_1 + h_2)m_1 = h_1 m_1 + h_2 m_1$
- $(h_1 h_2)m_1 = h_1(h_2 m_1)$

koşulları sağlanıyorsa M'ye H üzerinde bir sol modül veya kısaca ifade edilerek sol H-modül denir. Eğer H birimli ve birimi 1_H ise $(1_H)m_1 = m_1$ koşulu da ilave edilir. Benzer şekilde $M \times H \to M$ için $(h, m) \mapsto hm$ dönüşümü ile de sağ modül tanımı yapılabilir, bu durumda M'ye H üzerinde bir sağ modül veya kısaca ifade edilerek sağ H-modül denir. Komütatif bir halka için $hm = mh$ olacağından bir sol modül aynı zamanda bir sağ modül olur.

Örnek 2.2.18. Her cisim aynı zamanda bir halka olduğundan bir K cismi üzerindeki W vektör uzayı bir K-modüldür.

Tanım 2.2.19. H bir halka olmak üzere M bir H-modül ve M'nin bir alt kümesi $S(\neq \emptyset)$ olsun. S alt kümesi bir H-modül ise bu S alt kümesine M'nin bir alt modülü denir.

Teorem 2.2.20. *H bir halka, M bir H-modül ve M'nin bir alt kümesi $S(\neq \emptyset)$ olsun. S alt kümesinin, M'nin bir alt modülü olması için g.y.k. her $h, h' \in H$ ve her $s, s' \in S$ için $hs + h's' \in S$ olmasıdır.*

Tanım 2.2.21. H birimli bir halka, M bir H-modül ve $x_1, x_2, \ldots, x_n \in M$ olsun. $a_1, a_2, \ldots, a_n \in H$ için her $x \in M$ elemanı

$$x = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n$$

biçiminde tek türlü yazılabiliyorsa M'ye bir serbest modül, $\{x_1, x_2, \ldots, x_n\}$'e M'nin bir serbest bazı denir.

2.3. KODLAMA TEORİSİ

Bu bölümde cebirsel kodlama teorisinin temel kavramları ve teoremleri sunulacaktır. Bu bölümün hazırlanmasında Hill [3], Ling ve Xing [4] ve Dougherty [6] kaynaklarından yararlanılmıştır.

q elemanlı $A = \{\alpha_1, \alpha_2, \cdots, \alpha_q\}$ kümesi ele alınsın. $i = 1, 2, \ldots, q$ için $\alpha_i \in A$ olmak üzere $a = \alpha_1\alpha_2 \ldots \alpha_n$ olacak şekilde tüm sıralı n-lilere uzunluğu n olan q-lu kelime denir ve bu kelimelerin kümesi A^n ile gösterilir. Burada tanımlanan A, kod alfabesi olarak adlandırılır. Bir $\mathfrak{C} \subseteq A^n$ alt kümesine q-lu blok kod denir. A^n kümesindeki her bir elemana kelime ve $\mathfrak{C}$ kümesindeki elemanlara ise kod kelimesi denir. Kodun içerdiği toplam kod kelimesi sayısına ise kodun büyüklüğü adı verilir ve bu büyüklük $\mid \mathfrak{C} \mid$ biçiminde gösterilir. Özellikle $q = 2$ olduğunda $\mathfrak{C}$ ikili kod (binary code) olarak adlandırılırken $q = 3$ olduğunda $\mathfrak{C}$ üçlü kod (ternary code) olarak adlandırılır.

Tanım 2.3.1. F_q^n vektör uzayının $x = x_1x_2 \ldots x_n$, $y = y_1y_2 \ldots y_n \in$ vektörleri arasında tanımlanan ve aynı konumdaki bileşenlerin farklılık sayısını ölçen fonksiyona Hamming uzaklığı denir. Bu uzaklık fonksiyonu genellikle d ile gösterilir ve şöyle tanımlanır:

$$d(x,y) = |\{k \in \{1,2,\ldots,n\} \mid x_k \neq y_k\}|.$$

Alternatif olarak, bileşen bazında aşağıdaki şekilde de ifade edilebilir:

$$d(x,y) = \sum_{i=1}^{n} \delta(x_i, y_i) \quad \text{burada} \quad \delta(a,b) = \begin{cases} 1, & \text{eğer } a \neq b \\ 0, & \text{eğer } a = b \end{cases}$$

Örnek 2.3.2. F_2^5 vektör uzayının $x = 01010$ ve $y = 01101$ vektörleri arasındaki Hamming uzaklık

$$d(x,y) = 3$$

dir.

Önerme 2.3.3. *Hamming uzaklık fonksiyonu bir metriktir.*

Tanım 2.3.4. Bir $\mathfrak{C}$ kodunun tüm ikişerli kod kelimelerinin Hamming uzaklıklarının en küçüğüne kodun minimum Hamming uzaklığı denir.

Teorem 2.3.5. *Bir $\mathfrak{C}$ kodunun minimum Hamming uzaklığı $d(\mathfrak{C})$ ise $\mathfrak{C}$ kodu bir kod kelimesindeki $d(\mathfrak{C})-1$ veya daha az hatayı tespit edebilir ve $\lfloor|\frac{d(\mathfrak{C})-1}{2}|\rfloor$ veya daha az hatayı düzeltebilir.*

Teorem 2.3.6 (Singleton Sınırı)**.** *$\mathfrak{C}$ bir $[n,k,d]$ kod için $n-k \geq d-1$'dır.*

Tanım 2.3.7. $x = x_1x_2\ldots x_n \in \mathbb{F}_q^n$ biçimindeki bir vektörün sıfır olmayan bileşenlerinin sayısına x vektörünün Hamming ağırlığı denir ve

$$w(x) = |\ \{x_i \neq 0 \mid 1 \leq i \leq n\}\ |$$

şeklinde ifade edilir. x vektörünün Hamming ağırlığı yerine kısaca x'in ağırlığı olarak da kullanılır.

Tanım 2.3.8. Bir $\mathfrak{C}$ kodundaki tüm kod kelimelerinin ağırlıklarından en küçüğü kodun minimum ağırlığı olarak adlandırılır ve değer $w(\mathfrak{C})$ sembolü ile ifade edilir.

Tanım 2.3.9. İki koddan biri diğerinin kod kelimelerinin bileşenlerinin bir permütasyonu ve/veya tüm kod kelimelerinde belirli bir bileşende sembol değiştirilmesi işlemleri ile elde edilebiliyorsa bu kodlara denk kodlar denir.

2.3.1 CİSİM ÜZERİNDEKİ LİNEER KODLAR

Lineer kodların tanımlanmasında genellikle sonlu cisimler (Galois cisimleri) kullanılır; çünkü sonlu cisimler, cebirsel işlemlerin kapalı ve iyi tanımlı olduğu yapılar sunar. Bu bölümde, ilk olarak sonlu cisimler üzerindeki lineer kodların temel tanımları, yapıları ve örnekleri ele alınarak, bu kodların özelliklerine dair genel bir çerçeve çizilecektir. Ardından özel olarak devirli kodlar incelenecektir. Tezin ilerleyen bölümlerinde, aksi belirtilmediği sürece tüm lineer kodların uzunluğunun n olduğu kabul edilecektir.

Tanım 2.3.10. $\mathbb{F}_q$, q elemanlı sonlu cisim ve n bir pozitif tam sayı olsun. $\mathbb{F}_q^n$'nin bir alt uzayına $\mathbb{F}_q$ üzerinde bir lineer kod denir. Dolayısıyla $\mathbb{F}_q$'nin bir $\mathfrak{C}$ alt kümesinin bir lineer

kod olması için g.y.k. $\mathfrak{C}$'nin toplama ve skaler çarpma işlemleri altında kapalı olmasıdır, yani,

$$u+v \in \mathfrak{C} \quad \text{ve} \quad \alpha v \in \mathfrak{C}$$

olmasıdır, burada her $u, v \in \mathfrak{C}$ ve $\alpha \in \mathbb{F}_q$ dır.

Teorem 2.3.11. *$\mathbb{F}_q$ üzerinde bir $\mathfrak{C}$ lineer kodu için $Boy(\mathfrak{C}) = k$ ise $\mid \mathfrak{C} \mid = q^k$'dır.*

Bir lineer kod genellikle üç parametre ile tanımlanır. Bu parametreler kod kelimelerinin uzunluğu, kodun eleman sayısı ve kodun minimum uzaklığıdır. Özel olarak, $\mathbb{F}_q$ üzerinde bir $\mathfrak{C}$ lineer kodu için $\mathfrak{C}$'nin boyutu k ($Boy(\mathfrak{C}) = k$) ve minimum uzaklığı d ise $\mathfrak{C}$ koduna $[n,k,d]$ kod denir. Bazı durumlarda yalnızca uzunluk ve boyut parametreleri verilerek $[n,k]$ kod gösterimi de kullanılabilir.

Tanım 2.3.12. Bir $[n,k]$ lineer $\mathfrak{C}$ kodunun duali $\mathfrak{C}$'deki her kod kelimesiyle ortogonal olan $\mathbb{F}_q^n$'in elemanlarının kümesi olarak tanımlanır ve

$$\mathfrak{C}^{\perp} = \{v \in \mathbb{F}_q^n \mid \text{her } u \in \mathfrak{C} \text{ için } u \cdot v = 0\}$$

şeklinde ifade edilir.

Teorem 2.3.13. *Herhangi bir $\mathfrak{C}$ kodu için $(\mathfrak{C}^{\perp})^{\perp} = \mathfrak{C}$'dir.*

Tanım 2.3.14. Bir $\mathfrak{C}$ lineer kodu için ortogonallik ilişkisi aşağıdaki şekilde sınıflandırılır:

- Eğer $\mathfrak{C}$ kodu, dualinin alt kümesi ise, $\mathfrak{C}$ kodu kendine-ortogonal (self-orthogonal) olarak adlandırılır. Bu durumda, her kod sözcüğü tüm diğer kod sözcükleriyle ortogonaldir.
- Eğer $\mathfrak{C}$ kodu, dualine eşit ise, $\mathfrak{C}$ kodu **kendine-dual** (self-dual) olarak adlandırılır. Bu, hem kendine-ortogonal hem de dual içeren olmanın özel bir durumudur.
- Eğer $\mathfrak{C}$ kodunun duali $\mathfrak{C}$'nin alt kümesi ise, $\mathfrak{C}$ kodu **dual içeren** (dual-containing) olarak adlandırılır. Bu, kodun dualinin kodun içinde yer aldığını belirtir.

Lemma 2.3.15. *$x, y \in \mathbb{F}_q^n$ elemanları için, iki vektör arasındaki uzaklık $d(x,y)$, $x-y$ vektörünün Hamming ağırlığına eşittir; yani $d(x,y) = w(x-y)$ şeklindedir.*

Tanım 2.3.16. G boyutu $k \times n$ olan bir matris olsun. G'nin satırları bir $[n,k]$ lineer kodun bazını oluşturuyorsa bu matrise üreteç matrisi denir.

Örnek 2.3.17. $\mathbb{F}_2$ üzerindeki $C = \{000, 011, 101, 110\}$ kodunun bir bazı $\{011, 101\}$'dir. O halde $\mathfrak{C}$ kodunun bir üreteç matrisi $G = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$ dır.

Teorem 2.3.18. *$\mathbb{F}_q^n$ üzerinde $k \times n$ tipinde iki matristen biri*

(R1) Satırların permütasyonu

(R2) Bir satırın sıfırdan farklı bir skalerle çarpılması

(R3) Bir satırın skalerle çarpımının başka bir satıra eklenmesi

(C1) Sütunların permütasyonu

(C2) Bir sütunun sıfırdan farklı bir skalerle çarpılması

işlemlerinin bir kombinasyonuyla diğer matristen elde edilebiliyorsa bu matrisler denk lineer kodları üretir.

Teorem 2.3.19. *Bir $[n,k]$-kodun üreteç matrisi G olsun. O halde (R1),(R2),(R3),(C1) ve (C2) işlemleri kullanılarak G üreteç matrisi $[I_k|A]$ şeklinde standart forma dönüştürülebilir, burada I_k, $k \times k$ tipinde birim matris ve A, $k \times (n-k)$ tipinde bir matristir.*

Örnek 2.3.20. Örnek 2.3.17'daki G üreteç matrisini Teorem 2.3.18'da verilen elementer satır işlemleriyle standart forma dönüştürmek için 1. satır ile 2. satırın yerini değiştirmek yeterlidir, böylece

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \xrightarrow{R_1 \leftrightarrow R_2} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

elde edilir, burada $I_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ ve $A = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ dir.

Lemma 2.3.21. *Bir $\mathfrak{C}$ lineer kodunun üreteç matrisi G olsun. $G^\intercal$, G'nin transpozunu göstermek üzere $v \in \mathfrak{C}^\perp$ olması için g.y.k. $vG^T = 0$ olmasıdır.*

Lemma 2.3.22. *$\mathfrak{C}$, $[n,k]$ parametrelerine sahip bir kod ise, $\mathfrak{C}^{\perp}$ ile gösterilen dual kod, $[n,n-k]$ parametrelerine sahip bir koddur.*

Tanım 2.3.23. $[n,k]$ parametrelerine sahip bir $\mathfrak{C}$ kodunun dualinin üreteç matrisi $(n-k)\times n$ tipindedir ve bu matrise $\mathfrak{C}$'nin parite kontrol matrisi denir.

Devirli kodlar (cyclic codes), lineer kodların önemli bir alt sınıfı olup zengin cebirsel özelliklere sahip olduğundan tüm kodlar arasında en çok çalışılanlardır. Devirli kodlar hata düzeltme amacıyla kullanılan ikili Hamming kodları, Reed-Solomon kodları veya BCH kodları gibi önemli kod ailelerini içerir. Devirli kodlar ile $\mathbb{F}_q[x]/\langle x^n-1\rangle$ polinom halkası arasındaki ilişki oldukça temeldir. Özellikle, uzunluğu n olan bir devirli kod, bu halkada bir ideal ile birebir karşılık gelmektedir. Bu bağlamda, devirli kodların yapısal özellikleri, söz konusu halkadaki ideallerin cebirsel özellikleri aracılığıyla incelenir. Özel olarak bu halka üzerindeki ideal teorisi, devirli kodların oluşturulması, sınıflandırılması ve analizinde merkezi bir rol oynamaktadır.

Tanım 2.3.24. $\mathbb{F}_q$ üzerinde bir $\mathfrak{C}$ lineer kodu tüm döngüsel kaydırmalarını içeriyorsa, yani $(\mathfrak{c}_0,\mathfrak{c}_1,\ldots,\mathfrak{c}_{n-2},\mathfrak{c}_{n-1})$ vektörü $\mathfrak{C}$ kodunun elemanı iken $(\mathfrak{c}_{n-1},\mathfrak{c}_0,\mathfrak{c}_1,\ldots,\mathfrak{c}_{n-2})$ vektörü de $\mathfrak{C}$ kodunun elemanı ise $\mathfrak{C}$ kodu devirli kod olarak adlandırılır. Bir $\mathfrak{c}\in\mathbb{F}_q^n$ kod kelimesi için i'inci döngüsel kaydırma $\mathfrak{c}^{(i)}$ ile gösterilecektir.

Örnek 2.3.25. $\mathfrak{C}=\{000,110,011,101\}$ ikili kodu devirlidir.

Tanım 2.3.26. $\mathfrak{C}$, $\mathbb{F}_q$ sonlu cisimi üzerinde bir lineer kod olsun. $u\in\mathbb{F}_q^*$ için her $(\mathfrak{c}_0,\mathfrak{c}_1,\ldots,\mathfrak{c}_{n-1})$ vektörü $\mathfrak{C}$ kodunun bir elemanı iken $(u\mathfrak{c}_{n-1},\mathfrak{c}_0,\ldots,\mathfrak{c}_{n-2})$ vektörü de $\mathfrak{C}$ kodunun elemanı oluyorsa $\mathfrak{C}$'ye $\mathbb{F}_q$ üzerinde bir u-sabit devirli (u-constacyclic) kod denir.

Tanım 2.3.27. $\mathfrak{C}$, $\mathbb{F}_q$ sonlu cisimi üzerinde bir lineer kod olsun. Bu durumda $\mathfrak{c}=(\mathfrak{c}_0,\mathfrak{c}_1,\ldots,\mathfrak{c}_{n-1})$ vektörü $\mathfrak{C}$ kodunun bir elemanı iken $(-\mathfrak{c}_{n-1},\mathfrak{c}_0,\ldots,\mathfrak{c}_{n-2})$ vektörü de $\mathfrak{C}$ kodunun elemanı oluyorsa $\mathfrak{C}$'ye $\mathbb{F}_q$ üzerinde bir negatif devirli (negacyclic) kod denir.

Devirli kodların en önemli özelliklerinden biri bu kodların cebirsel olarak da ifade edilebilmesidir. $\mathbb{F}_q^n$ vektör uzayının bir $(\mathfrak{c}_0,\mathfrak{c}_1,\ldots,\mathfrak{c}_{n-1})$ vektörü, $\mathbb{F}_q$ üzerinde modulo x^n-1'e göre $\mathfrak{c}(x)=\mathfrak{c}_0+\mathfrak{c}_1x+\cdots+\mathfrak{c}_{n-1}x^{n-1}$ polinomunun kalan sınıfı (residue class) ile tanımlanabilir. Bu ilişki

$$\begin{array}{rcl}\mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q[x]/\langle x^n-1\rangle \\ (\mathfrak{c}_0,\mathfrak{c}_1,\ldots,\mathfrak{c}_{n-1}) & \longmapsto & \mathfrak{c}_0+\mathfrak{c}_1x+\cdots+\mathfrak{c}_{n-1}x^{n-1}\end{array} \tag{2.3}$$

şeklinde ifade edilen birebir bir tasvir (bijeksiyon) ile sağlanır. Dolayısıyla, herhangi bir kod kelimesi hem bir vektör hem de bir polinom olarak göz önüne alınabilir. Bir $\mathfrak{c}$ kod kelimesinin polinom gösterimi için $\mathfrak{c}(x)$ kullanılır. Hem kod kelimesi hem de karşılık gelen polinom gösterimi için ayırt etmeksizin bir kod, $\mathfrak{C}$ ile gösterilecektir.

Bir $\mathfrak{C}$ devirli kodunun $\mathfrak{c}(x) = \mathfrak{c}_0 + \mathfrak{c}_1 x + \cdots + \mathfrak{c}_{n-1}x^{n-1}$ elemanı için

$$\begin{aligned} x\mathfrak{c}(x) = &\quad \mathfrak{c}_0 x + \mathfrak{c}_1 x^2 + \cdots + \mathfrak{c}_{n-1}x^n \\ = &\quad \mathfrak{c}_{n-1} + \mathfrak{c}_0 x + \mathfrak{c}_1 x^2 + \cdots + \mathfrak{c}_{n-2}x^{n-1} \in \mathfrak{C} \end{aligned}$$

olur. Dolayısıyla, bir $\mathfrak{c}(x)$ polinomunu x ile çarpmak, c vektörünün sağa doğru bir kaydırılmasına karşılık gelir. Genel olarak bir $\mathfrak{c}(x)$ polinomunu x^m ile çarpmak, $\mathfrak{c}$ vektörünün m'inci döngüsel kaydırmasına, yani $\mathfrak{c}^{(m)}$ kaydırmasına karşılık gelir. O halde (2.3)'deki tasvir ile $\mathbb{F}_q$ sonlu cismi üzerindeki devirli kodlar tam olarak $S_n := \mathbb{F}_q[x]/\langle x^n - 1\rangle$ halkasının idealleridir ve bunun tersi de geçerlidir. Bu nedenle, $\mathbb{F}_q$ üzerindeki devirli kodların incelenmesi, $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ halkasındaki ideallerin incelenmesine karşılık gelir.

Teorem 2.3.28. *S_n'de bir $\mathfrak{C}$ kodunun devirli kod olması için g.y.k. $\mathfrak{C}$'in $k(x)$, $l(x)$ kod kelimeleri ve S_n'in $r(x)$ vektörü için*

$$k(x) + l(x) \in \mathfrak{C} \quad ve \quad r(x)k(x) \in \mathfrak{C}$$

olmasıdır.

S_n halkası bir esas ideal halkası olduğundan, bu halkanın her ideali esas idealdir [2]. Dolayısıyla bir $\mathfrak{C}$ kodu bir tek eleman tarafından üretilir. $f(x) \in S_n$ polinomunun tüm katlarını içeren alt küme $\langle f(x)\rangle = \{f(x)r(x) \mid\ r(x) \in S_n\}$ şeklindedir.

Teorem 2.3.29. *S_n kümesinden seçilen herhangi bir $f(x)$ polinomunun oluşturduğu $\langle f(x)\rangle$ alt kümesi, bir devirli koddur ve bu koda $f(x)$ tarafından üretilen kod denir.*

Teorem 2.3.30. *$\mathfrak{C}$, $\mathbb{F}_q$ üzerinde sıfırdan farklı bir devirli kod olsun. O halde aşağıdaki ifadeler geçerlidir:*

(i) $\mathfrak{C}$'de derecesi en küçük olan ve baş katsayısı bir olan (monik) tek türlü belirli bir $g(x)$ polinomu bulunur.

(ii) $\mathfrak{C} = \langle g(x) \rangle$*'dir.*

(iii) $g(x)$ *monik polinomu* $x^n - 1$ *polinomunun bir çarpanıdır.*

Tanım 2.3.31. $\mathfrak{C}$ sıfırdan farklı bir devirli kod ise, Teorem 2.3.30'da verilen en küçük dereceli monik $g(x)$ polinomu $\mathfrak{C}$ kodunun üreteç polinomu olarak adlandırılır.

Lemma 2.3.32. *Bir devirli kodun üreteç polinomunda sabt terim sıfırdan farklıdır.*

Teorem 2.3.33. *Üreteç polinomu* $g(x) = g_0 + g_1 x + \cdots + g_r x^r$ *olan* $\mathfrak{C}$ *devirli kodunun üreteç matrisi*

$$\begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & g_r & 0 & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdots & g_r & \cdots & 0 \\ \vdots & \vdots & \vdots & & & \ddots & & & \vdots \\ 0 & 0 & 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_r \end{bmatrix}$$

biçimindedir. Burada $\mathfrak{C}$*'nin boyutu* $n - r$*'dir.*

$\mathfrak{C}$ lineer kodu üreteç polinomu $g(x)$ olan bir $[n,k]$ kod ise Teorem 2.3.30'a göre $g(x)$ monik polinomu $x^n - 1$'in bir çarpanıdır. O halde $x^n - 1 = g(x)\widehat{g}(x)$ koşulunu sağlayan bir $\widehat{g}(x)$ polinomu vardır. $g(x)$ monik polinom olduğundan $\widehat{g}(x)$ de monik polinomudur. Ayrıca Teorem 2.3.33'e göre $g(x)$ polinomunun derecesi $n-k$ olduğundan $\deg \widehat{g}(x) = k$'dır, burada $\widehat{g}(x)$ polinomu $\mathfrak{C}$ kodunun kontrol polinomu olarak adlandırılır. $\widehat{g}(x)$'in resiprokal polinomu $\widehat{g}^*(x)$, $\mathfrak{C}^\perp$'in üreteç polinomudur ve $\mathfrak{C}^\perp$ bir lineer $[n, n-k]$ koddur.

Teorem 2.3.34. $\mathfrak{C}$*,* S_n*'de üreteç polinomu* $g(x)$ *ve kontrol polinomu* $\widehat{g}(x)$ *olan bir devirli kod olsun. Bu durumda* $c(x) \in S_n$ *elemanının* $\mathfrak{C}$*'nin bir kod kelimesi olması için g.y.k.* $c(x)\widehat{g}(x) = 0$ *olmasıdır.*

Lemma 2.3.35. *Üreteç polinomu* $g(x)$ *olan ikili* $\mathfrak{C}$ *lineer devirli kodunun dualini içermesi için g.y.k.*

$$x^n - 1 \equiv 0 \ (mod\ g(x)g^*(x))$$

olmasıdır, burada $g^*(x)$*,* $g(x)$*'in resiprokal polinomudur [7].*

Lemma 2.3.36. *$\mathfrak{C}$, $\mathbb{F}_p$ üzerinde üreteç polinomu $g(x)$ olan bir devirli kod veya negatif devirli kod olsun. $g^*(x)$ polinomu, $g(x)$'in resiprokal polinomudur ve $\kappa = \pm 1$ olmak üzere $\mathfrak{C}$'nin dualini içermesi için g.y.k.*

$$x^n - \kappa \equiv 0 \pmod{(g(x)g^*(x))}$$

olmasıdır [8].

2.3.2 HALKA ÜZERİNDEKİ LİNEER KODLAR

Hammons *ve diğ.*[9], klasik lineer olmayan bazı ikili kodların, $\mathbb{Z}_4$ üzerindeki belirli lineer kodların ikili görüntüleri olarak elde edilebildiğini göstermiştir. Bu bulgu, kodlama teorisinde önemli bir değişimi beraberinde getirmiştir. Geleneksel olarak, ikili kodlar $\mathbb{F}_2$ üzerindeki vektör uzayı yapısı çerçevesinde incelenirken, $\mathbb{Z}_4$ gibi halka yapısına sahip cebirsel yapılara geçiş, kodların modül teorisi perspektifinden analiz edilmesine olanak tanımıştır.

Özellikle, $\mathbb{Z}_4$ üzerindeki lineer kodların *Gray dönüşümü* aracılığıyla ikili kodlara aktarılması, klasik lineer kodların kapsamını aşarak, Kerdock ve Preparata gibi iyi bilinen bazı doğrusal olmayan ikili kodların da cebirsel olarak yapılandırılabilmesini mümkün kılmıştır. Gray dönüşümü, $\mathbb{Z}_4$ kodlarının Lee ağırlığı ile ikili kodların Hamming ağırlığı arasında uzaklığı koruyan (izometrik) bir ilişki kurarak, bu geçişin tutarlı olmasını sağlamıştır.

Bu yeni yaklaşım, lineer olmayan kodların yapısal analizini kolaylaştırmakla kalmayıp, aynı zamanda farklı hata düzeltme yöntemlerinin geliştirilmesine de kapı aralamıştır. Halka-tabanlı yapılar, daha esnek uzaklık ve ağırlık tanımları ile klasik vektör uzayı teorisinin sınırlamalarını aşarak, daha geniş bir kod sınıfının sistematik olarak incelenmesine imkân tanımıştır.

Sonuç olarak, kodlama teorisinde sonlu halkalar, modüller ve alternatif cebirsel yapılar üzerinde kodların tanımlanması, hem teorik hem de uygulamalı araştırmalar açısından dinamik bir alan oluşturmuş; klasik kodlama teorisinin sınırlarının ötesine geçen yeni tekniklerin ve yapıların geliştirilmesini teşvik etmiştir.

Tanım 2.3.37. *R* bir halka ve *n* bir pozitif tam sayı olsun. *R^n*'in bir alt kümesine *R* üzerinde bir kod denir. Eğer bu alt küme aynı zamanda *R* üzerinde bir alt modül ise, buna *R* üzerinde

lineer kod adı verilir.

Halkalar üzerinde tanımlanan kodlar, çoğunlukla cisimler üzerindeki klasik kod teorisinin doğal bir genellemesi olarak ortaya çıkmaktadır. Ancak, bir cismin cebirsel özellikleri ile bir halkanın cebirsel özellikleri arasında temel farklar bulunduğundan, halka üzerindeki kodların incelenmesi, kimi durumlarda daha karmaşık bir matematiksel yapı gerektirmektedir. Örneğin, bir cisim üzerinde tanımlı her vektör uzayının bir bazı mevcutken, genel modüller için bu durum geçerli değildir; dolayısıyla halka tabanlı kodlarda üreteç matrislerinin tanımlanması özel bir önem kazanmaktadır.

Keyfi halkalar üzerinde yapılan kodlama çalışmaları, genellikle karmaşık yapılar ve zayıf cebirsel özellikler nedeniyle analitik zorluklar taşırken, sonlu zincir halkaları belirgin yapısal özellikleri sayesinde daha yönetilebilir bir çerçeve sunmaktadır. Sonlu zincir halkaları, iyi tanımlanmış ideal yapısına sahiptir; özellikle, bu halkalarda tüm idealler birbirini içerme ilişkisiyle sıralanır, yani, bir R halkasının eğer sonlu sayıda ideali mevcutsa ve bu idealler içerme sırasına göre

$$0 = I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n = R$$

şeklinde tam sıralanıyorsa, R'ye bir *sonlu zincir halkası* denir. Örneğin bir p asalı ve bir $k \geq 1$ tam sayısı için $\mathbb{Z}_{p^k}$ halkası bir sonlu zincir halkasıdır. Diğer bir örnek $u^2 = 0$ olmak üzere $\mathbb{F}_2 + u\mathbb{F}_2$ halkası bir sonlu zincir halkasıdır. Sonlu zincir halkalarının ideal yapısı, modül yapısının daha sistematik bir biçimde incelenmesine olanak tanır ve kodların özelliklerinin daha net bir biçimde belirlenmesine imkan verir.

Bu nedenle, sonlu zincir halkaları üzerindeki kodlar, yapı bakımından sonlu cisimler üzerindeki kodlara oldukça benzemekte ve klasik kod teorisinin bir tür doğal uzantısı olarak değerlendirilebilmektedir. Kodlama teorisinde en çok çalışılan halka sınıflarının başında sonlu zincir halkalarının gelmesi de, bu halkaların sahip olduğu cebirsel yapıdan kaynaklanmaktadır. Bir sonlu zincir halkası, sonlu değişmeli bir lokal halka olup, tüm idealleri bir zincir yapısı oluşturacak şekilde birbirine içerilir; bu da kodların analizi ve sınıflandırılması açısından büyük kolaylık sağlamaktadır.

Zincir halkası olmayan halkalar üzerinde tanımlanan kodlar daha karmaşık olmakla birlikte belirli uygulamalar ve teorik çalışmalar açısından değerlidir. Bu tür halkalarda kod

yapılarının incelenmesi daha fazla soyut cebirsel araç gerektirir. Klasik kod teorisindeki yapıların çoğu doğrudan uygulanmaz. Bu nedenle, genellikle daha özelleşmiş, teoreme dayalı bir çalışma yapılır.

Halkalar üzerindeki kodlar için iç çarpım ve dual kod tanımları, klasik cisim tabanlı kodlama teorisinde verilen tanımlara benzer şekilde genişletilebilmektedir. Ancak, halka yapısının cisim yapısına kıyasla daha genel bir cebirsel çerçeve sunması, dual ve ağırlık dağılımı gibi temel kavramların halka ortamına aktarılmasında dikkatli tanımlamalar gerektirmektedir.

Wood [10], sonlu cisimler üzerinde bilinen klasik MacWilliams teoreminin, yani bir lineer kod ile onun dual kodu arasındaki ağırlık dağılımı ilişkisinin, yalnızca belirli bir halka sınıfı üzerinde tam anlamıyla korunabildiğini göstermiştir. Bu bağlamda, Wood, MacWilliams tipi dualite sonuçlarının geçerli olduğu en geniş halka ailesinin *Frobenius halkaları* olduğunu ispatlamıştır. Frobenius halkaları, kendi karakter modülüne izomorf olan sonlu halkalar olarak tanımlanır ve bu özellikleri sayesinde kodların dualizasyonu ve ağırlık dağılımı ilişkilerinde cisim tabanlı yapıların doğal bir genellemesini sunarlar. Örneğin, $\mathbb{Z}_4$ halkası bir Frobenius halkadır. Bu halkada her modül, $\mathbb{Z}_4$'ün karakter modülüyle izomorftur. Dolayısıyla, $\mathbb{Z}_4$ üzerindeki doğrusal kodlar ve onların dual kodları, tıpkı sonlu cisimler üzerindeki kodlar gibi, MacWilliams teoreminin sunduğu ilişkiyi ve ağırlık dağılımını sağlayan bir yapıya sahiptir.

Bir R halkası üzerindeki devirli kod tanımı cisim üzerindeki devirli kod tanımı ile benzer şekilde verilir, yani, R halkası üzerinde uzunluğu n olan devirli kod herhangi bir kod kelimesinin döngüsel kaydırmasının yine bir kod kelimesi olması özelliğine sahip lineer kodlardır. Bu kodlar ayrıca, $R[x]/\langle x^n - 1\rangle$ halkasının idealleri ile de ilişkilendirilir. Bu sebeple, halkalar üzerinde devirli kodların üreteç polinomlarının bulunup bulunamayacağı doğal bir sorudur. Bu soruya cevap verebilmek için, öncelikle $x^n - 1$ polinomunun R üzerinde çarpanlarına ayrılışını incelemek gerekir.

Bu bağlamda, halka üzerindeki devirli kodların üreteç polinomlarının bulunup bulunamayacağı sorusu, önemli bir cebirsel soruyu gündeme getirmektedir. Bu soruya doğru bir şekilde cevap verebilmek için, öncelikle $x^n - 1$ polinomunun R üzerindeki çarpanlara ayrılabilirliğini incelemek gerekmektedir. Bu nedenle, bu çarpanlara ayırma işlemi, halka üzerindeki devirli kodlar için üreteç polinomlarının varlığını belirleyen temel faktörlerden biridir. Ancak $x^n - 1$ polinomunun bir halka üzerindeki çarpanlara ayrılması

işlemi, halkanın türüne, karakteristiğine ve polinomun derecesine bağlı olarak zorlu olabilir.

Bazı özellikler halkalar üzerinde geçerli olmayabilir. Örneğin, $\mathbb{Z}_{p^e}$ halkasında ($e > 1$) tek türlü çarpanlara ayrılma özelliği geçerli değildir. Bu durum, halkaların yapısal özelliklerinden kaynaklanır ve polinomların çarpanlara ayrılması işlemi genellikle daha karmaşık hale gelir. Örneğin, $\mathbb{Z}_6$ halkası üzerinde x^3-1 polinomu farklı şekillerde çarpanlara ayrılabilir:

$$x^3-1=(x-1)(x^2+x+1),$$

ancak bu aynı zamanda,

$$x^3-1=(x-1)(x+2)(x+3)$$

olarak da çarpanlara ayrılabilir. Bu örnek, çarpanların birbirinden farklı olabileceğini ve halkalar üzerindeki çarpanlara ayırma işlemlerinin cisimlere göre daha esnek ve bazen beklenmedik olabileceğini göstermektedir.

Bir diğer fark ise, polinomların çarpımının derecesinin, çarpanlarının derecelerinin toplamından daha küçük olabilmesidir. Bu durum, polinomların çarpanlara ayrılma özelliklerini ve halkalar üzerindeki yapılarını anlamada önemli bir noktadır. Örneğin, $\mathbb{Z}_6[x]$ üzerinde $(3x+2)^2=1$ eşitliği sağlanmaktadır. Bu eşitlik, halka üzerindeki bazı polinomların, derecelerinin toplamından farklı olabileceğini gösterir.

Sonuç olarak, bir halka üzerindeki bir polinomun indirgenemez olup olmadığını belirlemek oldukça zor bir işlemdir. Bu, özellikle daha genel halkalar üzerinde polinomların çarpanlara ayrılışının zorluğuna işaret eder. Bu nedenle, halkalar üzerindeki kodları çalışırken, tüm indirgenemez polinomlar yerine yalnızca belirli bir alt sınıfı, yani temel indirgenemez (basic irreducible) polinomlar çarpanlara ayırmaya odaklanılır . Bu alt sınıf, daha karmaşık yapıların analizini kolaylaştırır ve uygulamalarda daha verimli sonuçlar elde edilmesini sağlar.

Tanım 2.3.38. H bir sonlu komütatif Frobenius halka ve $f(x)\in H[x]$ olsun. H üzerinde bir $\mathfrak{C}$ devirli kodu $H[x]/\langle f(x)\rangle$ bölüm halkasının bir idealidir. Ayrıca

- $f(x)=x^n-1$ ise $\mathfrak{C}$ kodu bir devirli kod,

- $f(x) = x^n + 1$ ise $\mathfrak{C}$ kodu bir negatif devirli kod,
- λ, H'de bir aritmetik birim olmak üzere $f(x) = x^n + \lambda$ ise $\mathfrak{C}$ kodu λ-sabit devirli kod

olarak adlandırılır.

3. MALZEME VE YÖNTEM

Bu bölümde, bu tez çalışmasında göz önüne alınan cebirsel yapılar ve kullanılan yöntemler ile ilgili temel bilgiler verilecektir. Bu kapsamda ilk olarak döngüsel kosetler ile ilgili kavramlar ifade edilecektir. Daha sonra $\mathbb{F}_2 + v\mathbb{F}_2$ $(v^2 = v)$, $\mathbb{F}_p + u\mathbb{F}_p$ $(u^2 = 1)$, $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ $(u^2 = 0)$ ve son olarak $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + \cdots + u^k\mathbb{F}_{2^m}$ $(u^{k+1} = 0)$ halkasının cebirsel özellikleri ve bu halkalar üzerindeki lineer kodlar ile ilgili bilgiler verilecektir.

Boş kümeden farklı olan K ve L kümelerinin kartezyen çarpımı ve toplamı, sırasıyla,

$$K \otimes L = \{(k,l) \mid k \in K, l \in L\} \quad \text{ve} \quad K \oplus L = \{k+l \mid k \in K, l \in L\}$$

biçiminde tanımlanır.

3.1. DÖNGÜSEL KOSETLER

q bir asal sayının kuvveti olsun. Döngüsel kosetler, $x^n - 1$ polinomunun, $\mathbb{F}_q$ sonlu cismi üzerinde çarpanlara ayrılışı için kullanılan önemli bir araçtır. $x^n - 1$ polinomunun kökleri, genellikle bir primitif n-inci kök olan α'ya bağlı olarak tanımlanır. Bu köklerin üsleri mod n'ye göre devirli grup oluşturur ve bu gruplar döngüsel kosetler şeklinde sınıflandırılır. Her bir döngüsel koset, $x^n - 1$ polinomunun bir çarpanına karşılık gelir. Bu çarpanlar, devirli kodların *üreteç* (generator) veya *kontrol* (parity-check) polinomlarını oluşturur. Bu kısımda döngüsel kosetler hakkında genel bir bilgi verilecektir. Bu bölümün hazırlanmasında Ling ve Xing [4] ile MacWilliams ve Sloane [11] kaynaklarından yararlanılmıştır.

Bir $\mathbb{F}_q$ sonlu cisminin sıfırdan farklı elemanlarını içeren $\mathbb{F}_q^*$ kümesi bir çarpımsal grup oluşturur [12]. Bu çarpımsal grubun üreteci olan elemana *primitif eleman* denir. Primitif elemanın mertebesi $q-1$ dir. Bir sonlu cismin birden fazla primitif elemanı vardır. Euler'in ϕ fonksiyonu ile $\mathbb{F}_q^*$ çarpımsal grubunun primitif eleman sayısı $\phi(q-1)$'dir.

Tanım 3.1.1. $\alpha \in \mathbb{F}_{q^m}$ elemanını kök kabul eden $\mathbb{F}_q$ üzerindeki en küçük dereceli monik polinoma α'nın $\mathbb{F}_q$ üzerindeki minimal polinomu denir.

Teorem 3.1.2. *α, $\mathbb{F}_{q^m}$'in bir primitif elemanı olsun. O halde $\mathbb{F}_q$'da α^i'nin minimal polinomu*

$$M_i(x) = \prod_{j \in C_i} (x - \alpha^j)$$

dır, burada C_i, modülo $q^m - 1$'de q'nun i'yi içeren tek türlü belirli döngüsel kosetidir.

İspat. İspat üç adımda elde edilir:

i) $i \in C_i$ olduğundan α^i, $M_i(x)$'in bir köküdür.

ii) $M_i(x) = a_0 + a_1x_1 + \cdots + a_rx_r$ olsun. Burada $k = 0, 1, \ldots, r$ olmak üzere $a_k \in \mathbb{F}_{q^m}$ ve $r = \mid C_i \mid$'dir. $M_i(x) = a_0 + a_1x_1 + \cdots + a_rx_r$ polinomunda her katsayının q'nuncu kuvveti alınırsa

$$a_0^q + a_1^q x + \cdots + a_r^q x^r = \prod_{j \in C_i} (x - \alpha^{qj}) = \prod_{j \in C_{qi}} (x - \alpha^j) = \prod_{j \in C_i} (x - \alpha^j) = M_i(x)$$

elde edilir. Böylece her $0 \leq k \leq r$ için $a_k = a_k^q$ olur. Dolayısıyla a_k katsayılarının hepsi $\mathbb{F}_q$'nun elemanlarıdır. O halde $M_i(x)$, $\mathbb{F}_q$ üzerinde bir polinomdur.

iii) α bir primitif eleman olduğundan C_i'nin farklı j, k elemanları için $\alpha^j \neq \alpha^k$'dır. Yani $M_i(x)$'in katlı kökü yoktur.

Bir $f_k \in \mathbb{F}_q$ için $f(x) = f_0 + f_1x + \cdots + f_nx^n$ olsun. O halde her $j \in C_i$ için $j \equiv iq^l \pmod{q^m - 1}$ olacak şekilde bir l tam sayısı vardır. Böylece

$$\begin{aligned} f(\alpha^j) = f(\alpha^{iq^l}) &= f_0 + f_1\alpha^{iq^l} + \cdots + f_n\alpha^{niq^l} \\ &= f_0^{q^l} + f_1^{q^l}\alpha^{iq^l} + \cdots + f_n^{q^l}\alpha^{niq^l} \\ &= (f_0 + f_1\alpha^i + \cdots + f_n\alpha^{ni})^{q^l} = (f(\alpha^i))^{q^l} = 0 \end{aligned}$$

dır. O halde $M_i(x)$, $f(x)$'in bir çarpanıdır.

i), ii) ve iii)'den $M_i(x)$'in α^i'nin minimal polinomu olduğu elde edilir. □

Teorem 3.1.3. *n, $(q,n) = 1$ olacak şekilde bir pozitif tam sayı ve m, $n \mid q^m - 1$'i sağlayan bir pozitif tam sayı olsun. α, $\mathbb{F}_{q^m}$'in bir primitif elemanı ve $M_j(x)$, $\mathbb{F}_q$'da α^j'nin bir minimal polinomu olsun. Mod n'de q'nun döngüsel kosetlerinin bir tam temsilci kümesini*

$\{s_1, s_2, \ldots, s_t\}$ ile gösterelim. O halde $\mathbb{F}_q$ üzerinde $x^n - 1$'in indirgenemez monik çarpanlara ayrılışı

$$x^n - 1 = \prod_{i=1}^{t} M_{\frac{(q^m-1)s_i}{n}}(x)$$

şeklindedir.

İspat. $r = \frac{q^m-1}{n}$ olsun. O halde α^r birimin n. köküdür ve bu sebeple $x^n - 1$ polinomunun kökleri $1, \alpha^r, \alpha^{2r}, \ldots, \alpha^{(n-1)r}$ şeklindedir. Böylece Tanım 3.1.1'den, $0 \leq i \leq n-1$ olmak üzere $M_{ir}(x)$ polinomları $x^n - 1$'in çarpanlarıdır.

Sonuç olarak;

$$x^n - 1 = ekok(M_0(x), M_r(x), M_{2r}(x), \ldots M_{(n-1)r}(x))$$

elde edilir.

$x^n - 1$ polinomunu çarpanlarına ayırmak için $M_0(x), M_r(x), M_{2r}(x), \ldots M_{(n-1)r}(x)$ polinomları arasından farklı olanları belirlemek gerekir. Teorem 3.1.2'den ve Tanım 2.1.54'den $M_{ir}(x) = M_{jr}(x)$ olması için g.y.k. ir ve jr'nin modülo $q^m - 1 = rn$'de q'nun aynı döngüsel kosetlerinde olması gerektiği biliniyor. Bu da i ve j'nin modülo n'de q'nun aynı döngüsel kosetlerinde olmasına denktir. Buradan, $M_{s_1 r}(x), M_{s_2 r}(x), \ldots, M_{s_t r}(x)$'in $M_0(x), M_r(x), \ldots M_{(n-1)r}(x)$ arasındaki farklı polinomlardır. □

Sonuç 3.1.4. $(q, n) = 1$ olacak şekilde pozitif n tam sayısı için $x^n - 1$'in $\mathbb{F}_q$ üzerinde indirgenemez monik çarpanlarının sayısı modülo n'de q'nun döngüsel kosetlerinin sayısına eşittir.

Örnek 3.1.5. $\mathbb{F}_2$ üzerinde $x^{21} - 1$ polinomu alınsın. Örnek 2.1.57'den modülo 21'de 2'nin döngüsel kosetlerinin tam temsilci kümesi {0,1,3,5,7,9}'dur. $n \mid q^m - 1$ yani $21 \mid 2^6 - 1$ olduğundan $\mathbb{F}_{64}$ cismini alıyoruz. Böylece $n = 21, q = 2, m = 6$ olduğundan $r = \frac{q^m-1}{n} = 3$'tür

ve modülo 63'te 3'ün katlarını içeren 2-döngüsel kosetleri

$$C_0 = \{0\}$$
$$C_3 = \{3,6,12,24,48,33\}$$
$$C_9 = \{9,18,36\}$$
$$C_{15} = \{15,30,60,57,51,39\}$$
$$C_{21} = \{21,42\}$$
$$C_{27} = \{27,54,45\}$$

şeklindedir. Buradan

$$M_0(x) = 1+x$$
$$M_3(x) = \prod_{j\in C_3}(x-\alpha^j) = 1+x+x^2+x^4+x^6$$
$$M_9(x) = \prod_{j\in C_9}(x-\alpha^j) = 1+x^2+x^3$$
$$M_{15}(x) = \prod_{j\in C_{15}}(x-\alpha^j) = 1+x^2+x^4+x^5+x^6$$
$$M_{21}(x) = \prod_{j\in C_{21}}(x-\alpha^j) = 1+x+x^2$$
$$M_{27}(x) = \prod_{j\in C_{27}}(x-\alpha^j) = 1+x+x^3$$

elde edilir. Teorem 3.1.3'den

$$\begin{aligned} x^{21}-1 =& M_0(x)\,M_3(x)\,M_9(x)\,M_{15}(x)\,M_{21}(x)\,M_{27}(x) \\ =& (1+x)(1+x+x^2+x^4+x^6)(1+x^2+x^3)(1+x^2+x^4+x^5+x^6) \\ & (1+x+x^2)(1+x+x^3) \end{aligned}$$

elde edilir.

3.2. $\mathbb{F}_2+v\mathbb{F}_2$ HALKASI

$\mathbb{F}_2+v\mathbb{F}_2$ $(v^2=v)$ halkası kodlama teorisinde hem cebirsel özellikleri hem de uygulama açısından önemli bir yere sahip bir halkadır. Bu halkanın öne çıkan özelliklerinden biri parçalanabilir bir yapıya sahip olmasıdır. Yani $\mathbb{F}_2+v\mathbb{F}_2$ halkası iki farklı idealin doğrudan toplamı olarak ifade edilebilmekte ve $\mathbb{F}_2\times\mathbb{F}_2$ yapısı ile izomorfik olarak eşlenebilmektedir. Bu parçalanabilirlik özelliği sayesinde bu halkada tanımlanan lineer ve devirli kodların iki ayrı bileşene ayrılarak analiz edilmesini mümkün hale gelmektedir ve böylece her

kod, iki tane ikili kodun birleşimi gibi ele alınabilmektedir. Ayrıca bu halkada tanımlanan kodlar, Gray dönüşümü yoluyla ikili doğrusal kodlara dönüştürülebilmekte ve bu dönüşüm genellikle uzaklığı koruyan bir dönüşüm olmaktadır. Bu sayede, bu halka üzerinde elde edilen kodların minimum uzaklığı ve hata düzeltme kapasitesi yüksek yapılar üretilmektedir. Bu özellikleri sayesinde bu halka hem teorik açıdan hem de kod parametrelerinin belirlenmesinde önemli kolaylıklar sağlamaktadır. Tezin bu kısmında $\mathbb{F}_2 + v\mathbb{F}_2$ $(v^2 = v)$ halkasının bu özellikleri ayrıntılı olarak incelenecektir.

$\mathbb{F}_2 = \{0,1\}$ iki elemanlı sonlu cisim ve $v^2 = v$ olmak üzere

$$R_1 := \mathbb{F}_2 + v\mathbb{F}_2 = \{a + vb \mid a,b \in \mathbb{F}_2,\ v^2 = v\} = \{0,1,v,1+v\}$$

kümesi işlem tabloları

$+$	0	1	v	$1+v$
0	0	1	v	$1+v$
1	1	0	$1+v$	v
v	v	$1+v$	0	1
$1+v$	$1+v$	v	1	0

$\cdot$	0	1	v	$1+v$
0	0	0	0	0
1	0	1	v	$1+v$
v	0	v	v	0
$1+v$	0	$1+v$	0	$1+v$

şeklinde verilen işlemlere göre bir halkadır. İşlem tablolarından R_1 halkasının komütatif ve biriminin 1 olduğu görülür. R_1 halkasının karakteristiği 2'dir ve her elemanı idempotenttir. $v(1+v) = 0$ olduğundan v ile $1+v$ sıfır bölen çiftidir. Bu halkanın idealleri

$$\begin{aligned} \langle 0 \rangle &= \{0\} \\ \langle 1 \rangle &= \{0,1,v,1+v\} \\ \langle v \rangle &= \{0,v\} \\ \langle 1+v \rangle &= \{0,1+v\} \end{aligned}$$

şeklindedir ve sonlu zincir halkası değildir. R_1 halkasının iki maksimal ideali $\langle v \rangle$ ve $\langle 1+v \rangle$'dir. Üstelik

$$\langle v \rangle + \langle 1+v \rangle = R_1$$

olduğundan $\langle v \rangle$ ile $\langle 1+v \rangle$ komaksimal ideallerdir. $v(1+v) = 0$ ve $v^2 = v$, $(1+v)^2 =$

$1+v$ olduğundan v ile $1+v$ elemanları R_1 halkasının ortogonal idempotentleridir. Teorem 2.1.53'den

$$R_1 = vR_1 \oplus (1+v)R_1$$

dir. Üstelik Teorem 2.1.51'den

$$\phi : R_1 \to \mathbb{F}_2^2$$
$$a+vb \mapsto (a, a+b)$$

dönüşümü bir izomorfizmadır. Bu dönüşüm, bir n doğal sayısı olmak üzere $i = 1,2,\ldots,n$ ve $c_i = r_i + vq_i \in R_1$ olacak şekilde $c = (c_1, c_2, \ldots, c_n) \in R_1^n$ elemanı için

$$\Phi(c) = (r(c), r(c)+q(c))$$

şeklinde R_1^n'e genişletilebilir, burada $r(c) = (r_1, r_2, \ldots r_n) \in \mathbb{F}_2^n$ ve $q(c) = (q_1, q_2, \ldots, q_n) \in \mathbb{F}_2^n$'dir. R_1^n kümesinin boş olmayan her alt kümesine, R_1 üzerinde uzunluğu n olan bir kod denir. Eğer bu alt küme aynı zamanda R_1^n'nin bir R alt modülü ise, bu alt küme, R_1 üzerinde uzunluğu n olan bir lineer kod olarak adlandırılır. R_1 üzerindeki bir $\mathfrak{C}$ lineer kodu için

$$\mathfrak{C}_1 = \{a \in \mathbb{F}_2^n \mid a+vb \in \mathfrak{C},\ b \in \mathbb{F}_2^n\} \quad \text{ve} \quad \mathfrak{C}_2 = \{a+b \in \mathbb{F}_2^n \mid a+vb \in \mathfrak{C}\}$$

biçiminde tanımlanan $\mathfrak{C}_1$ ve $\mathfrak{C}_2$ kümeleri ikili lineer koddur.

Önerme 3.2.1. *R_1 üzerinde bir $\mathfrak{C} = (1+v)\mathfrak{C}_1 \oplus v\mathfrak{C}_2$ lineer kodunun devirli kod olması için g.y.k. $\mathfrak{C}_1$ ve $\mathfrak{C}_2$'nin ikili devirli kod olmasıdır [13].*

Önerme 3.2.2. *R_1 üzerinde uzunluğu n olan herhangi bir $\mathfrak{C} = (1+v)\mathfrak{C}_1 \oplus v\mathfrak{C}_2$ devirli kodu için $\mathfrak{C} = \langle (1+v)g_1(x), vg_2(x)\rangle$'dır, burada $g_1(x)$ ve $g_2(x)$, sırasıyla, $\mathfrak{C}_1$ ve $\mathfrak{C}_2$'nin üreteç polinomlarıdır. Üstelik $\mid \mathfrak{C} \mid = 2^{2n-deg(g_1(x))-deg(g_2(x))}$'dır [13].*

Önerme 3.2.3. *R_1 üzerinde uzunluğu n olan herhangi bir $\mathfrak{C}$ devirli kodu için $\mathfrak{C} = \langle g(x)\rangle$ ve $g(x) \mid x^n - 1$ olacak şekilde tek türlü belirli bir $g(x)$ polinomu vardır, burada $g(x) = (1+v)g_1(x) + vg_2(x)$'tir. Ayrıca eğer $g_1(x) = g_2(x)$ ise $g(x) = g_1(x)$'tir [13].*

Önerme 3.2.4. *R_1 üzerinde bir $\mathfrak{C} = (1+v)\mathfrak{C}_1 \oplus v\mathfrak{C}_2$ devirli kodunun duali $\mathfrak{C}^{\perp} = \langle\ (1+v)\widehat{g}_1^*(x) + v\widehat{g}_2^*(x)\rangle$'dır, burada $\widehat{g}_1^*(x)$ ve $\widehat{g}_2^*(x)$, sırasıyla $\widehat{g}_1(x)$ ve $\widehat{g}_2(x)$'in resiprokal*

polinomudur. Üstelik $|\mathfrak{C}^{\perp}| = 2^{deg(g_1(x))+deg(g_2(x))}$*'tir [13].*

3.3. $\mathbb{F}_p + u\mathbb{F}_p$ HALKASI

Bir p tek asal sayısı için p elemanlı sonlu cisim $\mathbb{F}_p$ olmak üzere

$$R_2 := \mathbb{F}_p + u\mathbb{F}_p = \{a+ub \mid a,b \in \mathbb{F}_p,\ u^2 = 1\}$$

kümesi

$$(a+ub)+(c+ud) = (a+c)+u(b+d) \quad \text{ve} \quad (a+ub)(c+ud) = ac+bd+u(ad+bc)$$

şeklinde tanımlanmış işlemlere göre bir halkadır, burada $a,b,c,d \in \mathbb{F}_p$'dir. $R_2 = \mathbb{F}_p[u]/\langle u^2-1\rangle$ olup idealleri $\{0\}, \langle u-1\rangle, \langle u+1\rangle$ ve R_2'dir ve bir zincir halkası değildir. R_2'nin $u^2 = 1$ elemanı için

$$\left(\frac{1+u}{2}\right)\left(\frac{1-u}{2}\right) = \frac{1-u^2}{4} = \frac{1-1}{4} = 0$$

ve

$$\left(\frac{1+u}{2}\right)^2 = \frac{1+u}{2}; \qquad \left(\frac{1-u}{2}\right)^2 = \frac{1-u}{2}$$

olduğundan $\frac{1+u}{2}$ ve $\frac{1-u}{2}$ elemanları R_2 halkasının ortogonal idempotentleridir. O halde Teorem 2.1.53'den

$$R_2 = \frac{1+u}{2}R_2 \oplus \frac{1-u}{2}R_2 = \frac{1+u}{2}\mathbb{F}_p \oplus \frac{1-u}{2}\mathbb{F}_p$$

elde edilir. Her $r \in R_2$ elemanı $r = \frac{1+u}{2}a + \frac{1-u}{2}b$ olacak şekilde tek türlü yazılabilir, burada $a,b \in \mathbb{F}_p$'dır.

R_2 halkasından $\mathbb{F}_p^2$'ye bir Gray dönüşüm

$$\begin{aligned} \Phi : R_2 &\to \mathbb{F}_p^2 \\ r &\mapsto (a-b, a+b) \end{aligned}$$

şeklinde tanımlanır. Bu dönüşüm, $\mathfrak{c} = (\mathfrak{c}_0, \mathfrak{c}_1, \ldots, \mathfrak{c}_{n-1}) \in R_2^n$ için

$$\phi(\mathfrak{c}) = (\Phi(\mathfrak{c}_0), \Phi(\mathfrak{c}_1), \ldots, \Phi(\mathfrak{c}_{n-1}))$$

şeklinde R_2^n'e genişletilebilir, burada n bir doğal sayıdır.

R_2^n'nin boştan farklı her alt kümesi R_2 üzerinde uzunluğu n olan bir kod olarak adlandırılır. R_2'nin elemanlarının özelliği ile bu $\mathfrak{C}$ kodu

$$\mathfrak{C} = \frac{1+u}{2}\mathfrak{C}_1 \oplus \frac{1-u}{2}\mathfrak{C}_2$$

biçiminde yazılabilir, burada

$$\mathfrak{C}_1 = \{a \in \mathbb{F}_p \mid \frac{1+u}{2}a + \frac{1-u}{2}b \in R_2\}$$

ve

$$\mathfrak{C}_2 = \{b \in \mathbb{F}_p \mid \frac{1+u}{2}a + \frac{1-u}{2}b \in R_2\}$$

şeklinde olup bu kümeler $\mathbb{F}_p$ üzerinde uzunluğu n olan kodlardır. R_2^n'nin bir R alt modülü R_2 üzerinde uzunluğu n olan bir lineer kod olarak adlandırılır. R_2 üzerinde uzunluğu n olan bir $\mathfrak{C}$ lineer kodu için $c = (\mathfrak{c}_0, \mathfrak{c}_1, \ldots, \mathfrak{c}_{n-1})$ vektörü $\mathfrak{C}$'de bir kod kelimesi iken $(\mathfrak{c}_{n-1}, \mathfrak{c}_0, \ldots, \mathfrak{c}_{n-2})$ vektörü $\mathfrak{C}$'de bir kod kelimesi ise $\mathfrak{C}$'ye devirli kod; $(-\mathfrak{c}_{n-1}, \mathfrak{c}_0, \ldots, \mathfrak{c}_{n-2})$ vektörü bir kod kelimesi ise $\mathfrak{C}$'ye negatif devirli kod ve $(u\mathfrak{c}_{n-1}, \mathfrak{c}_0, \ldots, \mathfrak{c}_{n-2})$ vektörü bir kod kelimesi ise $\mathfrak{C}$'ye R üzerinde bir u-sabit devirli kod, denir.

Lemma 3.3.1. *Bir $\mathfrak{C}$ lineer kodunun, R_2 üzerinde uzunluğu n olan bir u-sabit devirli kod olması için g.y.k. $\mathfrak{C}_1$ ve $\mathfrak{C}_2$'nin sırasıyla $\mathbb{F}_p$ üzerinde uzunluğu n olan devirli ve negatif devirli kod olmasıdır [8].*

R_2 halkası üzerinde tanımlı olan ve $u^2 = 1$ koşulunu sağlayan bir u-sabit devirli kodun polinom karşılığı aşağıdaki tasvir yardımıyla ifade edilmektedir.

$$\begin{aligned} R_2^n &\to R_2[x]/\langle x^n - u\rangle \\ (\mathfrak{c}_1, \mathfrak{c}_2, \ldots, \mathfrak{c}_n) &\mapsto (\mathfrak{c}_0 + \mathfrak{c}_1 x + \cdots + x^{n-1}) \end{aligned}$$

şeklinde tanımlanan tasvir bir R_2-modül izomorfizmasıdır. $\mathfrak{C}$'nin R_2 üzerinde u-sabit devirli kod olması için g.y.k. $\mathfrak{C}$'nin $R_2[x]/(x^n-u)$'nun bir ideali olmasıdır.

Lemma 3.3.2. *$\mathfrak{C}$, R_2 üzerinde bir u-sabit devirli kod olsun. O halde $\mathfrak{C} = \left\langle \frac{1+u}{2}g_1(x), \frac{1-u}{2}g_2(x) \right\rangle$'dir, burada $g_1(x)$ ve $g_2(x)$ polinomları $\mathfrak{C}_1$ ve $\mathfrak{C}_2$ kodlarının üreteç polinomlarıdır. Ayrıca $\mathfrak{C}^\perp = \frac{1+u}{2}C_1^\perp \oplus \frac{1-u}{2}\mathfrak{C}_2^\perp$, R_2 üzerinde bir u-sabit devirli koddur ve $\mathfrak{C}^\perp = \left\langle \frac{1+u}{2}\widehat{g}_1^*(x), \frac{1-u}{2}\widehat{g}_2^*(x) \right\rangle$'dır, burada $\widehat{g}_1^*(x)$ ve $\widehat{g}_2^*(x)$ polinomları, sırasıyla $\widehat{g}_1(x)$ ve $\widehat{g}_2(x)$'nin resiprokal polinomudur [8].*

3.4. $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ HALKASI

$\mathbb{F}_2 + u\mathbb{F}_2$ $(u^2 = 0)$ halkasının elemanları $a, b \in \mathbb{F}_2$ için $a + ub$ şeklinde tanımlıdır ve tanımı gereği dört elemana sahiptir. Bu halka kodlama teorisi alanında temel düzeyde teorik çalışmalar ve uygulama alanları açısından önem arz eden birçok kodun oluşturulmasına imkan sağlamıştır ancak gün geçtikçe uygulama alanlarının genişlemesi ve taşınacak bilgi kapasitesinin artmasıyla birlikte daha yüksek boyutlu kodlara ihtiyaç duyulmuştur. Sadece $\mathbb{F}_2 + u\mathbb{F}_2$ halkası ile sınırlı kalmak tanımlanacak kodların zenginliğini de sınırlayacağından bu halka daha fazla elemana sahip halkalara genelleştirilmiştir. Bu genellemelerden biri de $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ halkasına genellemedir. Böylelikle halkanın her $a + ub$ elemanı için a ve b elemanları $\mathbb{F}_2$'den değil $\mathbb{F}_{2^m}$'den alınır. Dolayısıyla halka 4 eleman değil 2^{2m} elemana sahip olur ve bu durumda m değeri arttıkça daha yüksek boyutlu kodlar oluşturulabilir ve bu kodların minimum uzaklığının yüksek olma ihtimali de artar. Yani bu genelleme kodlama teorisi açısından daha iyi parametrelere sahip kodların elde edilmesi için önemli bir genellemedir. Bu bölümde önce $\mathbb{F}_2 + u\mathbb{F}_2$ halkasının cebirsel yapısı kısaca tanıtılacak ardından $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ halkasının cebirsel özellikleri sunulacaktır.

$\mathbb{F}_2$ iki elemanlı sonlu cisim olmak üzere

$$\mathbb{F}_2 + u\mathbb{F}_2 = \{a + ub \mid a, b \in \mathbb{F}_2,\ u^2 = 0\} = \{0, 1, u, 1+u\}$$

şeklinde ifade edilen küme üzerinde tanımlanan

$$(a+ub)+(c+ud) = (a+c)+u(b+d) \quad \text{ve} \quad (a+ub)(c+ud) = ac+u(ad+bc),$$

sırasıyla, toplama ve çarpma işlemlerine göre bir halkadır, burada $a, b, c, d \in \mathbb{F}_2$'dir. İşlem

tabloları

$+$	0	1	u	$1+u$
0	0	1	u	$1+u$
1	1	0	$1+u$	u
u	u	$1+u$	0	1
$1+u$	$1+u$	u	1	0

$\cdot$	0	1	u	$1+u$
0	0	0	0	0
1	0	1	u	$1+u$
u	0	u	0	u
$1+u$	0	$1+u$	u	1

şeklinde olup $\mathbb{F}_2+u\mathbb{F}_2$ halkası komütatif bir halkadır ve birim elemanı 1'dir. $u \in \mathbb{F}_2+u\mathbb{F}_2$ elemanı nilpotent eleman olup halka sıfır bölenli bir halkadır. Bu halkanın idealleri

$$\begin{aligned}\langle 0\rangle &= \{0\}\\ \langle 1\rangle &= \{0,1,u,1+u\}\\ \langle u\rangle &= \{0,u\}\\ \langle 1+u\rangle &= \{0,1,u,1+u\}\end{aligned}$$

şeklindedir. $\mathbb{F}_2+u\mathbb{F}_2$, bir lokal halka olup maksimal ideali $\langle u\rangle$ idealidir ve $\langle 0\rangle \subset \langle u\rangle \subset \mathbb{F}_2+u\mathbb{F}_2$ olduğundan bir zincir halkasıdır. Bu halkanın bir genellemesi olarak $\mathbb{F}_{2^m}$, 2^m elemanlı sonlu cisim olmak üzere

$$R_3 := \mathbb{F}_{2^m}+u\mathbb{F}_{2^m} = \{a+ub \mid a,b \in \mathbb{F}_{2^m},\ u^2=0\}$$

kümesi her $a,b,c,d \in \mathbb{F}_{2^m}$ için sırasıyla

$$(a+ub)+(c+ud) = (a+c)+u(b+d) \quad \text{ve} \quad (a+ub)(c+ud) = ac+u(ad+bc)$$

şeklindeki işlemlere göre bir halkadır. Bu halka karakteristiği 2 olan birimli bir lokal halkadır. Üstelik $u^2=0$ olduğundan u nilpotent elemandır. $a,b,c,d \in \mathbb{F}_{2^m}$ elemanları ile

$$(a+ub)(c+ud) = ac+u(ad+bc) = 1$$

eşitliğinin sağlanması için $ac=1$ ve $ad+bc=0$ olması gerekir. $ac=1$ olduğundan $a \neq 0$ ve $c \neq 0$, yani a ve c elemanları tersinir olmak zorundadır. $\mathbb{F}_{2^m}$ cisminin aritmetik birimleri

kümesi $\mathbb{F}_{2^m}^* = \mathbb{F}_{2^m} \setminus \{0\}$ olduğundan, R_3 halkasının aritmetik birimleri kümesi

$$R_3^* = \{a + ub \in R_4 \mid a \in \mathbb{F}_{2^m}^*,\ b \in \mathbb{F}_{2^m}\}$$

dır. R_3 halkasının aritmetik birim olmayan elemanlarının kümesi ise halkanın $a = 0$ olan elemanlarıdır, yani

$$R_3 \setminus R_3^* = \{ub \in R_3 \mid b \in \mathbb{F}_{2^m}\}$$

şeklindedir. Burada tersinir olmayan elemanların kümesi

$$\{ub \in R_3 \mid b \in \mathbb{F}_{2^m}\} = \langle u \rangle$$

idealidir ve bu ideal maksimal idealdir. R_3 halkasının kalan cismi $R_3/ < u > \cong \mathbb{F}_{2^m}$'dir. $\langle 0 \rangle \subset \langle u \rangle \subset R_3$ olduğundan bir zincir halkasıdır.

$B = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ kümesi $\mathbb{F}_2$ üzerinde $\mathbb{F}_{2^m}$ için bir baz olsun. $0 \leq i \leq m-1$ için $x_i \in \mathbb{F}_2$ ve $x = x_0\alpha_1 + x_1\alpha_2 + \cdots + x_{m-1}\alpha_m \in \mathbb{F}_{2^m}$ olmak üzere bir Gray dönüşüm

$$\begin{aligned} \phi : \mathbb{F}_{2^m} &\to \mathbb{F}_2^m \\ x &\mapsto (x_0, x_1, \ldots, x_{m-1}) \end{aligned}$$

şeklinde tanımlanır. Bu dönüşüm

$$\begin{aligned} \Phi : \mathbb{F}_{2^m}^n &\to \mathbb{F}_2^{mn} \\ (r_0, r_1, \ldots, r_{n-1}) &\mapsto (\phi(r_0), \phi(r_1), \cdots, \phi(r_{n-1})) \end{aligned}$$

biçiminde $\mathbb{F}_{2^m}^n$'e genişletilir, burada $0 \leq i \leq n-1$ için $r_i \in \mathbb{F}_{2^m}$'dir. Her $c \in R_3^n$ elemanı, $r = (r_0, r_1, \ldots, r_{n-1})$ ve $q = (q_0, q_1, \ldots, q_{n-1}) \in \mathbb{F}_{2^m}^n$ elemanları ile $c = r + uq$ şeklinde yazılabilir. Böylece R_3^n'den $\mathbb{F}_2^{2mn}$'e bir Gray dönüşüm

$$\begin{aligned} \psi : R_3^n &\to \mathbb{F}_2^{2mn} \\ c &\mapsto (\phi(q), \phi(r+q)) \end{aligned}$$

şeklindedir. R_3^n'den $\mathbb{F}_2^{2mn}$'e tanımlanan ψ Gray tasviri $\mathbb{F}_2$-lineerdir.

R_3 üzerinde uzunluğu n olan bir $\mathfrak{C}$ kodunun devirli olması için g.y.k. $\mathfrak{C}$'nin $R_3[x]/\langle x^n+1\rangle$'in bir ideali olmasıdır. R_3 üzerinde uzunluğu n olan bir $\mathfrak{C}$ kodunun $(1+u)$-sabit devirli olması için g.y.k. $\mathfrak{C}$'nin $R_3[x]/\langle x^n+1+u\rangle$'nun bir ideali olmasıdır.

Teorem 3.4.1. *$\mathfrak{C}$, R_3 üzerinde uzunluğu n olan bir $(1+u)$-sabit devirli kod ise*

$$\mathfrak{C} = \langle f(x)h(x), uf(x)g(x)\rangle$$

olacak şekilde $R_3[x]$ üzerinde tek türlü belirli $f(x), g(x), h(x)$ monik polinomları vardır ve üstelik $|\,\mathfrak{C}\,| = 2^{m(2\deg(g(x))+\deg(h(x)))}$'dır, burada $f(x)g(x)h(x) = x^n+1+u$'dır. Ayrıca

$$\mathfrak{C}^{\perp} = \langle g^*(x)h^*(x), ug^*(x)f^*(x)\rangle$$

ve $|\,\mathfrak{C}^{\perp}\,| = 2^{m(2\deg(f(x))+\deg(h(x)))}$'dır, burada $g^*(x), h^*(x)$ ve $f^*(x)$ polinomları sırasıyla $g(x), h(x)$ ve $f(x)$ polinomlarının resiprokal polinomudur [14].

3.5. $\mathbb{F}_{2^m}+u\mathbb{F}_{2^m}+\cdots+u^k\mathbb{F}_{2^m}$ HALKASI

$\mathbb{F}_{2^m}$, 2^m elemanlı sonlu cisim olmak üzere

$$\begin{aligned} R_4 :&= \mathbb{F}_{2^m}+u\mathbb{F}_{2^m}+\cdots+u^k\mathbb{F}_{2^m} \\ &= \left\{ \sum_{i=1}^{k+1} u^{i-1}a_i \mid 1 \le i \le k+1 \text{ için } a_i \in \mathbb{F}_{2^m},\ u^{k+1}=0 \right\} \\ &\cong \mathbb{F}_{2^m}[u]/\langle u^{k+1}\rangle \end{aligned}$$

şeklinde tanımlı küme adi toplama işlemi ve adi çarpma işlemine göre komütatif ve karakteristiği 2 olan bir halkadır. Halkanın idealleri arasında

$$0 = u^{k+1}R_4 \subset u^kR_4 \subset \cdots \subset u^2R_4 \subset uR_4 \subset R_4$$

şeklinde bir zincir olduğundan R_4, maksimal ideali $\langle u\rangle$ olan bir zincir halkasıdır. R_4 halkasının kalan cismi $R_4/\langle u\rangle \cong \mathbb{F}_{2^m}$'dir. R_4 halkasının aritmetik birimleri $a \not\equiv 0 \pmod{u}$ koşulunu sağlayan $a \in R_4$ elemanlarıdır. Her $c \in R_4$ elemanı $i = 0,1,\ldots,k$ için $\delta_i(c) \in \mathbb{F}_{2^m}$

olmak üzere

$$c = \delta_0(c) + u\delta_1(c) + \cdots + u^k\delta_k(c)$$

biçiminde tek türlü yazılabilir. Bu halka için bir Gray dönüşüm

$$\Phi : R_4 \to \mathbb{F}_{2^m}^{k+1},$$
$$c \mapsto (\delta_k(c), \delta_k(c) + \delta_0(c), \delta_{k-1}(c) + \delta_0(c), \delta_{k-1}(c) + \delta_1(c), \ldots, e(c))$$

biçiminde tanımlanır, burada

$$e(c) = \begin{cases} \delta_{z+1}(c) + \delta_z(c), & k = 2z+1 \ (z \in \mathbb{Z}) \\ \delta_z(c) + \delta_{z-1}(c), & k = 2z \ (z \in \mathbb{Z}) \end{cases}$$

dir. Φ dönüşümü lineerliği korur. Ayrıca Φ dönüşümü R_4^n'e genişletilebilir. Genişletilmiş Φ dönüşümü R_4'ten $\mathbb{F}_{2^m}^{(k+1)n}$'e birebir ve örten bir dönüşümdür.

R_4 üzerinde uzunluğu n olan bir $\mathfrak{C}$ kodunun devirli olması için g.y.k. $\mathfrak{C}$'nin $R_4[x]/\langle x^n - 1\rangle$'in bir ideali olmasıdır.

Teorem 3.5.1. *R_4 üzerinde uzunluğu n olan bir devirli kod $\mathfrak{C}$ olsun. O halde $R_4[x]$'te $f_0(x)f_1(x)f_2(x)\cdots f_{k+1}(x) = x^n - 1$ olmak üzere*

$$\mathfrak{C} = \langle \widehat{f_1}(x),\ u\widehat{f_2}(x),\ u^2\widehat{f_3}(x),\ \cdots, u^k\widehat{f}_{k+1}(x)\rangle$$

olacak şekilde tek türlü belirli ikişerli aralarında asal olan $f_0(x), f_1(x), f_2(x), \cdots, f_{k+1}(x)$ monik polinomları vardır ve $|\ \mathfrak{C}\ | = 2^{m(\Sigma_{i=0}^{k}(k+1-i)\deg(f_{i+1}(x)))}$'dir. Üstelik

$$\mathfrak{C}^{\perp} = \langle \widehat{f_0}^{*}(x),\ u\widehat{f}_{k+1}^{*}(x),\ u^2\widehat{f}_k^{*}(x),\ \cdots, u^k\widehat{f}_2^{*}(x)\rangle$$

ve $|\ \mathfrak{C}^{\perp}\ | = 2^{m(\Sigma_{i=0}^{k+1} i\deg(f_{i+1}(x)))}$'dir, burada $i = 0, 1, \ldots, k+1$ için $\widehat{f}_i^{*}(x) = f_0^{*}(x)f_1^{*}(x)\ldots f_{i-1}^{*}(x)f_{i+1}^{*}(x)\ldots f_{k+1}^{*}(x)$'dir [15].

4. BULGULAR

Bu bölümdeki teoremler ve ispatlar genel olarak kodlama teorisinde önemli bir yere sahip olan resiprokal polinomlar yardımıyla verilmiştir. Resiprokal polinom kavramı, matematikte polinomların simetrik özelliklerini inceleme amacının bir sonucu olarak ortaya çıkmıştır. Kodlama teorisinde, özellikle devirli ve sabit devirli kodların analizinde, bu tür polinomların yapısal özellikleri kritik bir rol oynamaktadır. Halkalar üzerindeki devirli kodların üreteç polinomları genel itibariyle kodun yapısını belirler. Bir devirli kodun dual kodu da yine devirli olmaktadır ve bu dual kodun üreteç polinomu, çoğu zaman ana kodun üreteç polinomunun resiprokaliyle doğrudan ilişkili olmaktadır. Yani bir kodun yapısını anlamak için yalnızca üreteç polinomu değil aynı zamanda bu üreteç polinomunun resiprokali de dikkate alınmalıdır. Bu durum resiprokal polinomların kodlama teorisi literatüründe devirli kodların cebirsel yapısından kaynaklanan zorunlu bir yapı olduğunu ortaya koymaktadır. Resiprokal polinomların bu şekilde kullanılması yalnızca teknik bir hesaplama kolaylığı sunmakla kalmaz. Ayrıca bu dönüşüm, kodların yapısını ve davranış biçimlerini anlamamızı sağlar. Özellikle kendine dual, kendine ortogonal ve dual içeren kodların karakterizasyonu, resiprokal polinomlar aracılığıyla gerçekleştirilir. Bu tür kodlar, klasik hata düzeltme kodlarının ötesinde kuantum hata düzeltme kodları gibi ileri düzey uygulamalarda da temel bir rol oynar. Nitekim kuantum kodlarının inşasında kullanılan CSS (Calderbank–Shor–Steane) metodunda kodların dualini içermesi gerekliliği üreteç polinom ile onun resiprokali arasındaki ilişkiye doğrudan bağlıdır. Sonuç olarak, resiprokal polinomlar yalnızca cebirsel bir işlem olarak değil kodlama teorisinin hem yapısal hem de uygulamalı yönlerini kavramada kilit bir rol oynayan, çok yönlü ve vazgeçilmez bir araçtır. Bu yönüyle, resiprokal kavramı, kodlama teorisinin temel yapı taşlarından biri haline gelmiştir.

Bu bölümde, farklı cebirsel yapılar üzerindeki bir kodun dualini içermesi için gerek ve yeter koşullar incelenmiştir. Bu kapsamda, sırasıyla hem $\mathbb{F}_2$ cismi üzerinde hem de $R_1 = \mathbb{F}_2 + v\mathbb{F}_2$ $(v^2 = v)$, $R_2 := \mathbb{F}_p + u\mathbb{F}_p$ $(u^2 = 1)$, $R_3 := \mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ $(u^2 = 0)$ ve $R_4 := \mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + \cdots + u^k\mathbb{F}_{2^m}$ $(u^{k+1} = 0)$ halkaları üzerindeki devirli kodlar ele alınmıştır.

4.1. DÖNGÜSEL KOSETLERLE DUALİNİ İÇEREN İKİLİ DEVİRLİ KODLAR

Bu bölümde döngüsel kosetler yardımıyla bir ikili devirli kodun dualini içermesi için bir gerek ve yeter koşul verilecektir.

$(n,2)=1$ olsun ve $0 \leq s < n$ olacak şekilde bir s tam sayısı göz önüne alınsın. Simetrik kosetlerin sayısı $\varepsilon(n)$ ile, asimetrik koset çiftlerinin sayısı $\delta(n)$ ile gösterilsin. Eğer ξ, $\mathbb{F}_2$'nin bir cisim genişlemesinde birimin n inci dereceden bir primitif kökü ise ξ^s'in $\mathbb{F}_2$ üzerindeki minimal polinomu

$$M_i(x) = \prod_{i \in C_s} (x - \xi^i)$$

şeklindedir ve

$$x^n + 1 = \prod_{t=1}^{\varepsilon(n)} M_{i_t}(x) \prod_{l=1}^{\delta(n)} \left(M_{j_l}(x) M_{-j_l}(x) \right)$$

dir, burada $1 \leq t \leq \varepsilon(n)$ için C_{i_t}'ler tüm simetrik kosetler ve $1 \leq l \leq \delta(x)$ olmak üzere C_{j_l} ve C_{-j_l} asimetrik koset çiftleridir. $N = 2^\alpha n$ olsun. O halde

$$x^N + 1 = \prod_{t=1}^{\varepsilon(n)} M_{i_t}^{2^\alpha}(x) \prod_{l=1}^{\delta(n)} \left(M_{j_l}(x) M_{-j_l}(x) \right)^{2^\alpha}$$

dır. Eğer C_s simetrik ise $M_s^*(x) = M_s(x)$'tir. C_s ve C_{-s} asimetrik çiftler ise $M_s^*(x) = M_{-s}(x)$'dir.

Teorem 4.1.1. *$N = 2^\alpha n$ uzunluğunda ikili devirli iki kod $\mathfrak{C}$ ve $\mathfrak{C}'$ olsun. Eğer*

$$\mathfrak{C} = \left\langle \prod_{t=1}^{\varepsilon(n)} M_{i_t}^{a_t}(x) \prod_{l=1}^{\delta(n)} \left(M_{j_l}^{b_l}(x) M_{-j_l}^{c_l}(x) \right) \right\rangle$$

ve

$$\mathfrak{C}' = \left\langle \prod_{t=1}^{\varepsilon(n)} M_{i_t}^{a'_t}(x) \prod_{l=1}^{\delta(n)} \left(M_{j_l}^{b'_l}(x) M_{-j_l}^{c'_l}(x) \right) \right\rangle$$

ise $\mathfrak{C}^\perp \subset \mathfrak{C}'$ olması için g.y.k. $a'_t \leq 2^\alpha - a_t$, $b'_l \leq 2^\alpha - c_l$ ve $c'_l \leq 2^\alpha - b_l$ olmasıdır. Özel olarak $\mathfrak{C}^\perp \subset \mathfrak{C}$ olması için g.y.k. $\alpha_t \leq 2^{a-1}$ ve $b_l + c_l \leq 2^\alpha$ olmasıdır [16].

İspat. $\mathfrak{C}$ ve $\mathfrak{C}'$ kodlarının üreteç polinomları sırasıyla

$$f(x) = \prod_{t=1}^{\varepsilon(n)} M_{i_t}^{a_t}(x) \prod_{t=1}^{\delta(n)} \left(M_{j_l}^{b_l}(x) M_{-j_l}^{c_l}(x) \right)$$

ve

$$g(x) = \prod_{t=1}^{\varepsilon(n)} M_{i_t}^{a'_t}(x) \prod_{t=1}^{\delta(n)} \left(M_{j_l}^{b'_l}(x) M_{-j_l}^{c'_l}(x) \right)$$

şeklinde gösterilsin. $\mathfrak{C}^{\perp}$'in üreteç polinomu $\widehat{f}(x)$'in resiprokal polinomu olup

$$\widehat{f}^*(x) = \prod_{t=1}^{\varepsilon(n)} M_{i_t}^{2^\alpha - a_t}(x) \prod_{t=1}^{\delta(n)} \left(M_{j_l}^{2^\alpha - c_l}(x) M_{-j_l}^{2^\alpha - b_l}(x) \right)$$

şeklindedir. $\mathfrak{C}^{\perp} \subset \mathfrak{C}'$ olması için g.y.k. $g(x) \mid \widehat{f}^*(x)$ ve $\mathfrak{C}^{\perp} \subset \mathfrak{C}$ olması için g.y.k.$f(x) \mid \widehat{f}^*(x)$ olduğu biliniyor. Burada $g(x) \mid \widehat{f}^*(x)$ olması için g.y.k.

$$a'_t \leq 2^\alpha - a_t, \quad b'_l \leq 2^\alpha - c_l \quad \text{ve} \quad c'_l \leq 2^\alpha - b_l$$

olmasıdır. Ayrıca $f(x) \mid \widehat{f}^*(x)$ olması için g.y.k.

$$a_t \leq 2^\alpha - a_t \;\Rightarrow\; 2a_t \leq 2^\alpha \;\Rightarrow\; a_t \leq 2^{\alpha-1}$$

ve

$$b_l + c_l \leq 2^\alpha - c_l + 2^\alpha - b_l \;\Rightarrow\; 2(b_l + c_l) \leq 2(2^\alpha) \;\Rightarrow\; b_l + c_l \leq 2^\alpha$$

olmasıdır. □

4.2. $\mathbb{F}_2 + v\mathbb{F}_2$ HALKASI ÜZERİNDE DUALİNİ İÇEREN DEVİRLİ KODLAR

Qian [7] tarafından 2013 yılında yayınlanan çalışmada $\mathbb{F}_2 + v\mathbb{F}_2$ $(v^2 = v)$ halkası üzerinde tanımlı devirli kodlardan yola çıkılarak kuantum hata düzelten kodların inşası için yeni bir metot verilmiştir. Bu metot geliştirilirken $\mathbb{F}_2 + v\mathbb{F}_2$ $(v^2 = v)$ halkası üzerinde dualini içeren devirli kodların sağladığı koşulla ilgili bir teorem de sunulmuştur. Bu çalışmanın temelinde, $\mathbb{F}_2 + v\mathbb{F}_2$ $(v^2 = v)$ halkası üzerindeki bir devirli kodun bu halkadan $\mathbb{F}_2^2$'ye tanımlanan

Gray dönüşümü altındaki görüntüsünün birinci ve ikinci bileşeniyle ayrı ayrı oluşturulan kümelerin de dualini içeren ikili lineer kod olmaları durumu vardır. Qian'ın bu çalışması, yalnızca yapısal olarak dualini içeren kodların bir incelemesini yapmakla sınırlı kalmamış, aynı zamanda bu kodların Gray dönüşümleri üzerinden kuantum hata düzelten kodların nasıl elde edilebildiğini de göstermiştir. Bu bölümde, Qian'ın önerdiği yönteme dayanarak $\mathbb{F}_2 + v\mathbb{F}_2$ halkası üzerinde tanımlı devirli kodların dualini içermesi için gerek ve yeter koşul ayrıntılı biçimde ele alınmıştır. Ayrıca elde edilen sonuçları somutlaştırmak amacıyla bir örnek sunulmuştur. Kolaylık olması için ilgili halka $R_1 = \mathbb{F}_2 + v\mathbb{F}_2$ şeklinde gösterilecektir.

Teorem 4.2.1. *R_1 üzerinde uzunluğu n olan $\mathfrak{C} = \langle (1+v)g_1(x) + vg_2(x) \rangle$ bir devirli kodunun dualini içermesi için g.y.k.*

$$x^n - 1 \equiv 0 \ (mod\ g_1(x)g_1^*(x)) \quad ve \quad x^n - 1 \equiv 0 \ (mod\ g_2(x)g_2^*(x))$$

olmasıdır, burada $g_1^*(x)$ ve $g_2^*(x)$ sırasıyla $g_1(x)$ ve $g_2(x)$ polinomlarının resiprokal polinomlarıdır [7].

İspat. R_1 üzerinde uzunluğu n olan bir devirli kod $\mathfrak{C}$ ve $\mathfrak{C} = \langle g(x) \rangle = (1+v)\mathfrak{C}_1 \oplus v\mathfrak{C}_2$ olsun. O halde $\mathfrak{C} = \langle (1+v)g_1(x) + vg_2(x) \rangle$, $\mathfrak{C}_1 = \langle g_1(x) \rangle$ ve $\mathfrak{C}_2 = \langle g_2(x) \rangle$'dir, burada $\mathfrak{C}_1$ ve $\mathfrak{C}_2$ ikili lineer kodlardır. Eğer

$$x^n - 1 \equiv 0 \ (\text{mod}\ g_1(x)g_1^*(x)) \quad \text{ve} \quad x^n - 1 \equiv 0 \ (\text{mod}\ g_2(x)g_2^*(x))$$

ise Lemma 2.3.35'den

$$\mathfrak{C}_1^\perp \subseteq \mathfrak{C}_1 \quad \text{ve} \quad \mathfrak{C}_2^\perp \subseteq \mathfrak{C}_2$$

dir. $\mathfrak{C}_1^\perp$ ve $\mathfrak{C}_2^\perp$ ikili devirli kodlarının üreteç polinomları, sırasıyla $\widehat{g_1}(x)$ ve $\widehat{g_2}(x)$ polinomlarının resiprokal polinomları olduğundan $\langle \widehat{g_1}^*(x) \rangle \subseteq \langle g_1(x) \rangle$ ve $\langle \widehat{g_2}^*(x) \rangle \subseteq \langle g_2(x) \rangle$'dir. Böylece

$$\langle\ (1+v)\widehat{g_1}^*(x) + v\widehat{g_2}^*(x)\ \rangle \subseteq \langle (1+v)g_1(x) + vg_2(x) \rangle$$

elde edilir. Dolayısıyla $\mathfrak{C}$ kodu dualini içerir.

Diğer taraftan $\mathfrak{C}$ $\mathfrak{C}^\perp$ dual kodunu içersin. O halde $(1+v)\mathfrak{C}_1^\perp \oplus v\mathfrak{C}_2^\perp \subseteq (1+v)\mathfrak{C}_1 \oplus v\mathfrak{C}_2$'dir,

burada $\mathfrak{C}_1$ ve $\mathfrak{C}_2$ ikili devirli koddur. $\mathfrak{C} = (1+v)\mathfrak{C}_1 \oplus v\mathfrak{C}_2$ olduğundan

$$\mathfrak{C} \equiv (1+v)\mathfrak{C}_1 \pmod{v} \quad \text{ve} \quad \mathfrak{C} \equiv v\mathfrak{C}_2 \pmod{1+v}$$

dır, böylece

$$\mathfrak{C}_1^{\perp} \subseteq \mathfrak{C}_1 \quad \text{ve} \quad \mathfrak{C}_2^{\perp} \subseteq \mathfrak{C}_2$$

olur. Lemma 2.3.35'den

$$x^n - 1 \equiv 0 \pmod{g_1(x)g_1^*(x)} \quad \text{ve} \quad x^n - 1 \equiv 0 \pmod{g_2(x)g_2^*(x)}$$

elde edilir.

□

Sonuç 4.2.2. R_1 üzerinde uzunluğu n olan bir devirli kod $\mathfrak{C} = (1+v)\mathfrak{C}_1 \oplus v\mathfrak{C}_2$ olsun. $\mathfrak{C}^{\perp} \subseteq \mathfrak{C}$ olması için g.y.k.

$$\mathfrak{C}_1^{\perp} \subseteq \mathfrak{C}_1 \quad ve \quad \mathfrak{C}_2^{\perp} \subseteq \mathfrak{C}_2$$

olmasıdır [7].

Örnek 4.2.3. $x^7 - 1$ polinomu $\mathbb{F}_2[x]$ üzerinde

$$\begin{aligned} x^7 - 1 &= (x-1)(x^6 + x^5 + x^4 + x^2 + x^2 + x + 1) \\ &= (x-1)(x^3 + x^2 + 1)(x^3 + x + 1) \end{aligned}$$

şeklinde indirgenemez ve monik çarpanlarına ayrılır. $x - 1 \equiv x + 1 \pmod{2}$ olduğundan

$$x^7 - 1 = (x+1)(x^3 + x^2 + 1)(x^3 + x + 1)$$

şeklinde ifade edilebilir. Burada

$$\begin{aligned} f_1(x) &:= x^3 + x^2 + 1 \\ f_2(x) &:= x^3 + x + 1 \end{aligned}$$

olarak alınan polinomlar için $(1+v)f_1(x)$ ve $vf_2(x)$ polinomlarının toplamı ile üretilen $\mathfrak{C}$, R_1

üzerinde uzunluğu 7 olan bir devirli koddur. $f_1(x)$ ve $f_2(x)$'in resiprokal polinomları

$$f_1^*(x) = x^3(\tfrac{1}{x^3} + \tfrac{1}{x^2} + 1) = 1 + x + x^3 = f_2(x)$$
$$f_2^*(x) = x^3(\tfrac{1}{x^3} + \tfrac{1}{x} + 1) = 1 + x^2 + x^3 = f_1(x)$$

şeklinde elde edilir. Bu durumda

$$f_1(x)f_1^*(x) \mid x^7 - 1 \quad \text{ve} \quad f_2(x)f_2^*(x) \mid x^7 - 1$$

yani

$$x^7 - 1 \equiv 0 \pmod{f_1(x)f_1^*(x)} \quad \text{ve} \quad x^7 + 1 \equiv 0 \pmod{f_2(x)f_2^*(x)}$$

sağlanır. Dolayısıyla $\mathfrak{C}^{\perp} \subseteq \mathfrak{C}$'dir.

4.3. $\mathbb{F}_p + u\mathbb{F}_p$ HALKASI ÜZERİNDE DUALİNİ İÇEREN DEVİRLİ KODLAR

Gao ve Wang [8] tarafından 2018 yılında yayımlanan çalışmada $\mathbb{F}_p + u\mathbb{F}_p$ $(u^2 = 1)$ üzerinde tanımlı u-sabit devirli kodların yapısını detaylı biçimde inceleyerek, bu kodların klasik hata düzeltme alanındaki anlamını açıklamış ve aynı zamanda bu yapıların Gray dönüşüm ile elde edilen kodlar aracılığıyla yeni kuantum kodların inşasını da mümkün kılmıştır. Gao ve Wang'ın çalışmasında, u-constacyclic kodların $\mathbb{F}_p + u\mathbb{F}_p$ halkası üzerindeki tanımına ek olarak, bu kodların dual kodlarını içerme şartları detaylıca ortaya konmuş ve CSS (Calderbank–Shor–Steane) metodu ile yeni kuantum kodların nasıl inşa edilebileceği sunulmuştur. Bu bağlamda $\mathbb{F}_3$, $\mathbb{F}_5$ ve $\mathbb{F}_7$ üzerindeki bir kodun Gray dönüşümünün, kuantum kod parametrelerine nasıl dönüştüğü hesaplanarak elde edilen parametreler tablolar halinde verilmiştir. Bu kodların parametreleri literatürdeki mevcut kuantum kodlarla kıyaslanarak üstün yönleri ortaya konmuştur. Bu bağlamda, söz konusu çalışma, klasik kodların kuantum koda dönüştürülmesinde yeni bir yöntem sunmuş ve özellikle de halkalar üzerindeki lineer yapılar ile kuantum kodlama teorisi arasındaki bağı kuvvetlendirmiştir. Bu nedenle, bu çalışmada sunulan teknikler ve elde edilen sonuçlar, hem teorik kodlama çalışmaları hem de pratik kuantum bilgi işleme uygulamaları açısından önem arz etmektedir. Bu tezin bu bölümde, Gao ve Wang [8]'nın çalışmasının temel amacı için, $\mathbb{F}_p + u\mathbb{F}_p$ $(u^2 = 1)$ halkası üzerinde dualini içeren devirli kodların sağladığı koşulla ilgili ispatlanan teoreme yer

verilmiştir. Bu kısımda, kolaylık olması için ilgili halka $u^2 = 1$ olmak üzere $R_2 := \mathbb{F}_p + u\mathbb{F}_p$ olarak gösterilecektir, brada p bir asal sayıdır.

Teorem 4.3.1. *R_2 üzerinde uzunluğu n olan bir u-sabit devirli kod $\mathfrak{C} = \left\langle \frac{1+u}{2}g_1(x), \frac{1-u}{2}g_2(x) \right\rangle$'nin dualini içermesi için g.y.k.*

$$x^n - 1 \equiv 0 \pmod{g_1(x)\tilde{g}_1(x)} \quad ve \quad x^n + 1 \equiv 0 \pmod{g_2(x)\tilde{g}_2(x)}$$

olmasıdır, burada $\tilde{g}_1(x) = (g_1(0))^{-1}g_1^*(x)$ ve $\tilde{g}_2(x) = (g_2(0))^{-1}g_2^*(x)$'dir [8].

İspat. R_2 üzerinde bir u-sabit devirli kod

$$\mathfrak{C} = \frac{1+u}{2}\mathfrak{C}_1 \oplus \frac{1-u}{2}\mathfrak{C}_2 = \left\langle \frac{1+u}{2}g_1(x), \frac{1-u}{2}g_2(x) \right\rangle$$

olsun, burada $\mathfrak{C}_1 = \langle g_1(x) \rangle$ ve $\mathfrak{C}_2 = \langle g_2(x) \rangle$ $\mathbb{F}_p$ üzerinde uzunluğu n olan, sırasıyla devirli ve negatif devirli koddur. Eğer

$$x^n - 1 \equiv 0 \pmod{g_1(x)\tilde{g}_1(x)} \quad \text{ve} \quad x^n + 1 \equiv 0 \pmod{g_2(x)\tilde{g}_2(x)}$$

ise Lemma 2.3.36'dan $\mathfrak{C}_1^\perp \subseteq \mathfrak{C}_1$ ve $\mathfrak{C}_2^\perp \subseteq \mathfrak{C}_2$'dir. Buradan

$$\frac{1+u}{2}\mathfrak{C}_1^\perp \subseteq \frac{1+u}{2}\mathfrak{C}_1 \quad \text{ve} \quad \frac{1-u}{2}\mathfrak{C}_2^\perp \subseteq \frac{1-u}{2}\mathfrak{C}_2$$

dir. Böylece

$$\frac{1+u}{2}\mathfrak{C}_1^\perp \oplus \frac{1-u}{2}\mathfrak{C}_2^\perp \subseteq \frac{1+u}{2}\mathfrak{C}_1 \oplus \frac{1-u}{2}\mathfrak{C}_2$$

olur. Dolayısıyla $\mathfrak{C}$ kodu $\mathfrak{C}^\perp$ dual kodunu içerir.

Diğer taraftan $\mathfrak{C}$ kodu $\mathfrak{C}^\perp$ dual kodunu içersin. Bu durumda

$$\frac{1+u}{2}\mathfrak{C}_1^\perp \oplus \frac{1-u}{2}\mathfrak{C}_2^\perp \subseteq \frac{1+u}{2}\mathfrak{C}_1 \oplus \frac{1-u}{2}\mathfrak{C}_2$$

dir. $\mathfrak{C} = \frac{1+u}{2}\mathfrak{C}_1 \oplus \frac{1-u}{2}\mathfrak{C}_2$ olduğundan $\mathbb{F}_p$ üzerinde $\mathfrak{C} \equiv \frac{1-u}{2}\mathfrak{C}_2 \pmod{\frac{1+u}{2}}$ ve $\mathfrak{C} \equiv \frac{1+u}{2}\mathfrak{C}_1 \pmod{\frac{1-u}{2}}$'dir. Buradan hem $\mathfrak{C}_1$ kodu hem de $\mathfrak{C}_2$ kodu dualini içerir. Böylece

$$x^n - 1 \equiv 0 \pmod{g_1(x)\tilde{g}_1(x)} \quad \text{ve} \quad x^n + 1 \equiv 0 \pmod{g_2(x)\tilde{g}_2(x)}$$

dir. □

Örnek 4.3.2. $n = 12$ ve $p = 3$ olmak üzere $\mathbb{F}_3 + u\mathbb{F}_3$ $(u^2 = 1)$ halkası göz önüne alınsın. O halde $x^{12} - 1$ ve $x^{12} + 1$'in indirgenemez monik çarpanlara ayrılışı

$$x^{12} - 1 = (x+1)^3(x+2)^3(x^2+1)^3$$

ve

$$x^{12} + 1 = (x^2+2x+2)^3(x^2+x+2)^3$$

olarak bulunur. $g_1(x) = x+1$ ve $g_2(x) = x^2+x+2$ olmak üzere

$$\mathfrak{C} = \left\langle \frac{1+u}{2} g_1(x), \frac{1-u}{2} g_2(x) \right\rangle$$

$\mathbb{F}_3 + u\mathbb{F}_3$ halkası üzerinde uzunluğu 12 olan u-sabit devirli koddur. $g_1(x) = x+1$ ve $g_2(x) = x^2+x+2$ polinomlarının resiprokal polinomları sırasıyla

$$g_1^*(x) = x+1 \quad \text{ve} \quad g_2^*(x) = 2x^2+x+1$$

olur. Buradan

$$\tilde{g}_1(x) = (g_1(0))^{-1} g_1^*(x) = 1(x+1) = x+1$$

ve $2^{-1} \equiv 2 \pmod 3$ olduğundan

$$\begin{aligned} \tilde{g}_2(x) = (g_2(0))^{-1} g_2^*(x) &= 2^{-1}(2x^2+x+1) = 2(2x^2+x+1) \\ &= 4x^2+2x+2 \equiv x^2+2x+2 \pmod 3 \end{aligned}$$

dir.

$$g_1(x)\tilde{g}_1(x) = (x+1)^2$$

olduğundan $g_1(x)\tilde{g}_1(x) \mid x^{12} - 1$'dir. Ayrıca

$$g_2(x)\tilde{g}_2(x) = (x^2+x+2)(x^2+2x+2)$$

olur ve $g_2(x)\tilde{g}_2(x) \mid x^{12}+1$'dir. Böylece Teorem 4.3.1'den $\mathfrak{C}^{\perp} \subseteq \mathfrak{C}$'dir.

Örnek 4.3.3. $n = 20$ ve $p =$ olmak üzere $\mathbb{F}_5 + u\mathbb{F}_5$ $(u^2 = 1)$ halkası göz önüne alınsın. Bu halka üzerinde $x^{20}-1$ ve $x^{20}+1$ polinomlarının indirgenemez monik çarpanlara ayrılışı

$$x^{20}-1 = (x+1)^5(x+2)^5(x+3)^5(x+4)^5$$

ve

$$x^{20}+1 = (x^2+2)^5(x^2+3)^5$$

şeklindedir. $g_1(x) = (x+2)^2$ ve $g_2(x) = x^2+2$ olmak üzere

$$\mathfrak{C} = \left\langle \frac{1+u}{2}g_1(x), \frac{1-u}{2}g_2(x) \right\rangle$$

$\mathbb{F}_5 + u\mathbb{F}_5$ halkası üzerinde uzunluğu 20 olan u-sabit devirli koddur. $g_1(x) = (x+2)^2$ ve $g_2(x) = x^2+2$ polinomlarının resiprokal polinomları sırasıyla

$$g_1^*(x) = 4x^2+4x+1 \quad \text{ve} \quad g_2^*(x) = 2x^2+1$$

olur. Buradan $4^{-1} \equiv 4 \pmod 5$ olduğundan

$$\begin{aligned}\tilde{g}_1(x) = (g_1(0))^{-1}g_1^*(x) &= 4^{-1}(4x^2+4x+1) \\ &= 16x^2+16x+4 \equiv x^2+x+4 \equiv (x+3)^2 \pmod 5\end{aligned}$$

elde edilir. Böylece

$$g_1(x)\tilde{g}_1(x) = (x+2)^2(x+3)^2$$

olur ve $g_1(x)\tilde{g}_1(x) \mid x^{20}-1$'dir. Benzer şekilde $2^{-1} \equiv 3 \pmod 5$ olduğundan

$$\begin{aligned}\tilde{g}_2(x) = (g_2(0))^{-1}g_2^*(x) &= 2^{-1}(2x^2+1) \\ &= 6x^2+3 \equiv x^2+3 \pmod 5\end{aligned}$$

elde edilir. Buradan

$$g_2(x)\tilde{g}_2(x) = (x^2+2)(x^2+3)$$

olur ve $g_2(x)\tilde{g}_2(x) \mid x^{20}+1$'dir. Böylece Teorem 4.3.1'den $\mathfrak{C}^{\perp} \subseteq \mathfrak{C}$'dir.

Örnek 4.3.4. $n = 15$ ve $p = 7$ olmak üzere $\mathbb{F}_7 + u\mathbb{F}_7$ halkası göz önüne alınsın. Bu halka üzerinde $x^{15}-1$ ve $x^{15}+1$ polinomlarının indirgenemez monik çarpanlara ayrılışı

$$\begin{aligned} x^{15}-1 =& (x+3)(x+5)(x+6)(x^4+2x^3+4x^2+x+2) \\ & (x^4+x^3+x^2+x+1)(x^4+4x^3+2x^2+x+4) \end{aligned}$$

ve

$$\begin{aligned} x^{15}+1 =& (x+1)(x+2)(x+4)(x^4+3x^3+2x^2+6x+4) \\ & (x^4+6x^3+x^2+6x+1)(x^4+5x^3+4x^2+6x+2) \end{aligned}$$

şeklindedir. $g_1(x) = x+6$ ve $g_2(x) = x+1$ olmak üzere

$$\mathfrak{C} = \left\langle \frac{1+u}{2} g_1(x), \frac{1-u}{2} g_2(x) \right\rangle$$

$\mathbb{F}_7 + u\mathbb{F}_7$ halkası üzerinde uzunluğu 15 olan u-sabit devirli koddur. $g_1(x) = x+6$ ve $g_2(x) = x+1$ polinomlarının resiprokal polinomları sırasıyla

$$g_1^*(x) = 3x+1 \quad \text{ve} \quad g_2^*(x) = 2x+1$$

dir. $3^{-1} \equiv 5 \pmod 7$ olduğundan

$$\tilde{g}_1(x) = (g_1(0))^{-1} g_1^*(x) = 3^{-1}(3x+1) = 15x+5 \equiv x+5 \pmod 7$$

elde edilir. Buradan

$$g_1(x)\tilde{g}_1(x) = (x+3)(x+5)$$

olur ve $g_1(x)\tilde{g}_1(x) \mid x^{15}-1$'dir. Benzer şekilde $2^{-1} \equiv 4 \pmod 7$ olduğundan

$$\tilde{g}_2(x) = (g_2(0))^{-1} g_2^*(x) = 2^{-1}(2x+1) = 8x+4 \equiv x+4 \pmod 7$$

elde edilir. Buradan

$$g_2(x)\tilde{g}_2(x) = (x+2)(x+4)$$

olur ve $g_2(x)\tilde{g}_2(x) \mid x^{15}+1$'dir. Böylece Teorem 4.3.1'den $\mathfrak{C}^{\perp} \subseteq \mathfrak{C}$'dir.

4.4. $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ HALKASI ÜZERİNDE DUALİNİ İÇEREN DEVİRLİ KODLAR

Tang *ve diğ.*[14] tarafından 2020'de yapılan çalışmada, $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ halkası üzerinde tanımlı $(1+u)$-sabit devirli kodların Gray dönüşümleri aracılığıyla ikili lineer kodlara dönüştürüldüğü ve bu kodların kuantum kodlara uygulanabilirliği araştırılmıştır. Bu halka üzerinde tanımlanan $(1+u)$-sabit devirli kodların dualini içermesi durumu ele alınmış ve bu özelliğin sağlanması için gerek ve yeter koşul cebirsel olarak ifade edilmiştir. Bu çalışma sonucunda elde edilen dualini içeren kodların kuantum hata düzeltici kodlara geçişi için CSS (Calderbank-Shor-Steane) inşa metodu kullanılmış ve böylece halka üzerindeki kodlardan yola çıkılarak ikili kuantum kodlar elde edilmiştir. Çalışmanın son kısmında bir cebirsel hesap programı olan MAGMA aracılığıyla $\mathbb{F}_4 + u\mathbb{F}_4$ halkası üzerinde ayrı ayrı 85 ve 93 uzunluklu $(1+u)$-sabit devirli kodlardan iki farklı kuantum hata düzelten kod elde edilmiş ve kodların literatürde var olan örneklerden daha iyi paramaetrelere sahip olduğu belirtilmiştir. Bu çalışma, sonlu halkalar üzerinde tanımlı sabit devirli kodlar kullanılarak var olanlardan daha iyi parametrelere sahip lineer kodların ve ikili kuantum hata düzelten kodların inşa edilebileceğini göstererek literatüre anlamlı bir katkı sağlamıştır. Mevcut tezin bu kısmında, ilgili çalışmada ispatlanan, $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ halkası üzerinde tanımlı bir devirli kodun dualini içermesi için gerek ve yeter koşul verilmiştir. Bu kısımda kolaylık olması için ilgili halka $u^2 = 0$ olmak üzere $R_3 := \mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ şeklinde gösterilecektir.

Teorem 4.4.1. *$f(x), g(x)$ ve $h(x)$ polinomları $R_3[x]$ üzerinde $f(x)g(x)h(x) = x^n + 1 + u$ koşulunu sağlayan ikişerli aralarında asal monik polinomlar olmak üzere R_3 üzerinde uzunluğu n olan $(1+u)$-sabit devirli bir kod $\mathfrak{C} = \langle f(x)h(x), uf(x)g(x)\rangle$ olsun. O halde $\mathfrak{C}^{\perp} \subseteq \mathfrak{C}$ olması için g.y.k. $f(x) \mid g^*(x)$ olmasıdır [14].*

İspat. Teorem 3.4.1'den

$$\mathfrak{C}^{\perp} = \langle g^*(x)h^*(x), ug^*(x)f^*(x)\rangle$$

dir. $\mathfrak{C}^{\perp} \subseteq \mathfrak{C}$ olsun. Bu takdirde

$$g^*(x)h^*(x) = f(x)h(x)a(x)$$

olacak şekilde bir $a(x) \in R_3[x]$ vardır. Buradan

$$\begin{aligned} g^*(x)h^*(x)g(x) &= f(x)g(x)h(x)a(x) \\ &= (1+u)f^*(x)g^*(x)h^*(x)a(x) \end{aligned}$$

olur. O halde $f^*(x) \mid g(x)$'dır, böylece $f(x) \mid g^*(x)$ elde edilir.

Diğer taraftan $f(x) \mid g^*(x)$ olsun. Bu durumda

$$g^*(x) = f(x)l(x)$$

olacak şekilde bir $l(x) \in R_3[x]$ vardır. $b(x)$ kendine resiprokal polinomların çarpımı ve $r(x)$ kendine resiprokal olmayan polinomların çarpımı olmak üzere

$$h(x) = b(x)r(x)$$

biçiminde yazılabilir. O halde $f(x)g(x)h(x) = x^n + 1 + u$ olduğundan

$$(1+u)f^*(x)g^*(x)h^*(x) = f(x)g(x)h(x)$$

olur ki buradan $r(x) \mid f^*(x)g^*(x)h^*(x)$ elde edilir. ebob$(f^*(x), r(x)) = m(x)$ olsun. O halde $m(x) \mid f^*(x)$'tir. $f^*(x) \mid g(x)$ olduğundan $m(x) \mid g(x)$ olur. Benzer şekilde $m(x) \mid r(x)$ ve $r(x) \mid h(x)$ olduğundan $m(x) \mid h(x)$'dır. $g(x)$ ve $h(x)$ aralarında asal olduklarından $r(x)$ ile $f^*(x)$ aralarında asaldır. Aynı zamanda $r(x)$ ve $h^*(x)$ polinomları aralarında asaldır. Buradan $r(x) \mid f^*(x)g^*(x)h^*(x)$ olduğundan $r(x) \mid g^*(x)$ olur. Böylece $f(x)r(x) \mid g^*(x)$ olur. O halde

$$g^*(x) = f(x)r(x)k(x)$$

olacak şekilde $k(x) \in R_3[x]$ vardır. $g(x)$ ve $h(x)$ aralarında asal polinom olduğundan

$$g(x)s(x) + h(x)t(x) = 1$$

olacak şekilde $s(x), t(x) \in R_3[x]$ polinomları vardır. Böylece

$$\begin{aligned} uf^*(x)g^*(x) &= uf^*(x)f(x)r(x)k(x) \\ &= uf^*(x)f(x)r(x)k(x)(g(x)s(x) + h(x)t(x)) \\ &= uf^*(x)f(x)r(x)k(x)g(x)s(x) \\ &\qquad + uf^*(x)f(x)r(x)k(x)h(x)t(x) \\ &= uf^*(x)r(x)k(x)s(x)f(x)g(x) + uf^*(x)r(x)k(x)t(x)f(x)h(x) \in \mathfrak{C} \end{aligned}$$

elde edilir. Üstelik

$$\begin{aligned} g^*(x)h^*(x) &= f(x)r(x)k(x)b^*(x)r^*(x) \\ &= f(x)h(x)k(x)r^*(x) \in \mathfrak{C} \end{aligned}$$

olur. Böylece $\mathfrak{C}^{\perp} \subseteq \mathfrak{C}$ elde edilir. □

4.5. $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + \cdots + u^k\mathbb{F}_{2^m}$ HALKASI ÜZERİNDE DUALİNİ İÇEREN DEVİRLİ KODLAR

Tang *ve diğ.*[15] tarafından yapılan çalışmada, $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + \cdots + u^k\mathbb{F}_{2^m}$ $(u^{k+1} = 0)$ şeklindeki zincir halkalar üzerinde tanımlanan dualini içeren devirli kodlar kullanılarak yeni kuantum kod aileleri inşa edilmiştir. Tang *ve diğ.*[15] hem yeni bir Gray dönüşümü hem de klasik CSS (Calderbank–Shor–Steane) inşa metodunu kullanmış ve öncelikle bu halka üzerinde tanımlanan kodların dualini içermesi için bir gerek ve yeter koşul ortaya koymuş, ardından bu yapıları kuantum kod inşasında kullanmışlardır. Bu çalışmanın temelinde, klasik kodların dualini içeren bir kod olması durumunda, bu kodlardan kuantum hata düzeltici kodların elde edilebileceğine ilişkin teori yer almaktadır. Özellikle bu çalışma, bu biçimdeki halkalar üzerinde tanımlı devirli kodların kuantum kodlara uygulanmasında önemli bir boşluğu doldurmakta ve 2^m'li kuantum kodlar için bir inşa yöntemi sunmaktadır. Bu tezin bu kısmında, Tang *ve diğ.*[15]'ın çalışmasında ispatlanan, $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + \cdots + u^k\mathbb{F}_{2^m}$ $(u^{k+1} =$

0) halkası üzerinde tanımlı bir devirli kodun dualini içermesi için gerek ve yeter koşul verilmiştir. Ayrıca, elde edilen sonuçlara ilişkin bir örnek verilmiştir. Kolaylık olması için ilgili halka p bir asal sayı ve $u^{k+1}=1$ olmak üzere $R_4 := \mathbb{F}_{2^m}+u\mathbb{F}_{2^m}+\cdots+u^k\mathbb{F}_{2^m}$ şeklinde gösterilecektir.

Teorem 4.5.1. *$\mathfrak{C}$, R_4 üzerinde uzunluğu n olan bir devirli kod olsun. O halde $R_4[x]$ üzerinde $f_0(x)f_1(x)f_2(x)\cdots f_{k+1}(x)=x^n-1$ ve*

$$\mathfrak{C}=\langle \widehat{f_1}(x),\, u\widehat{f_2}(x),\, u^2\widehat{f_3}(x),\, \cdots, u^k\widehat{f_{k+1}}(x)\rangle$$

olacak şekilde ikişerli aralarında asal olan $f_0(x), f_1(x), f_2(x), \cdots, f_{k+1}(x)$ monik polinomları vardır. i=2, 3, …, k+1 olmak üzere $r_i(x)$, $f_i(x)$'in kendine resiprokal olmayan ve indirgenemez çarpanlarının çarpımı olsun. Bu takdirde $\mathfrak{C}^{\perp}\subseteq\mathfrak{C}$ olması için g.y.k.

$$f_0(x)r_2(x)r_3(x)\cdots r_{k+1}(x)|{f_1}^*(x) \tag{4.1}$$

olmasıdır [15].

İspat. $i=2,3,\ldots,k+1$ olmak üzere $r_i(x)$, $f_i(x)$'in indirgenemez kendine resiprokal olmayan çarpanlarının çarpımı olsun. $f_i(x)$ polinomu resiprokal olan ve resiprokal olmayan polinomların çarpımı olarak $f_i(x)=b_i(x)r_i(x)$ şeklinde yazılabildiğinden ve resiprokal polinom özelliğinden $\varepsilon_i\in\mathbb{F}_{2^m}$ aritmetik birim olmak üzere $b_i(x)=\varepsilon_i b_i^*(x)$ olduğundan $f_i(x)=\varepsilon_i b_i^*(x)r_i(x)$ yazılır. Dolayısıyla

$$f_i(x)^*=(\varepsilon_i b_i^*(x)r_i(x))^*=\varepsilon_i b_i(x)r_i^*(x)$$

olacak şekilde ifade edilebilir. Ayrıca Teorem 3.5.1'den

$$\mathfrak{C}^{\perp}=\langle \widehat{f_1^*}(x),\, u\widehat{f_2^*}(x),\, u^2\widehat{f_3^*}(x),\, \cdots, u^k\widehat{f_{k+1}^*}(x)\rangle$$

dir.

Gereklilik: $\mathfrak{C}^{\perp}\subseteq\mathfrak{C}$ olsun. O halde $\widehat{f_0^*}(x)\in\mathfrak{C}^{\perp}$ için

$$\widehat{f_0^*}(x)=\widehat{f_1}(x)a(x)$$

olacak şekilde $a(x) \in F_{2^m}[x]$ vardır, burada

$$\widehat{f_0^*}(x) = (f_1(x)f_2(x)\dots f_{k+1}(x))^* = f_1^*(x)f_2^*(x)\dots f_{k+1}^*(x)$$

ve

$$\widehat{f_1}(x) = f_0(x)f_2(x)\dots f_k(x)f_{k+1}(x)$$

dır. $i = 2,3,\dots,k+1$ için $b_i(x)$'ler $f_i(x)$'in kendine resiprokal çarpanları olduğu için $\varepsilon_i \in F_{2^m}^*$ olmak üzere $b_i(x) = \varepsilon_i b_i^*(x)$ şeklinde olup $f_i(x) = b_i(x)r_i(x)$ ve $f_i^*(x) = b_i^*(x)r_i^*(x)$ olarak yazılabilir. $\widehat{f_0^*}(x) = \widehat{f_1^*}(x)a(x)$ olduğundan

$$f_1^*(x)b_2^*(x)r_2^*(x)\dots b_{k+1}^*(x)r_{k+1}^*(x) = f_0(x)b_2(x)r_2(x)\dots b_{k+1}(x)r_{k+1}(x)a(x) \qquad (4.2)$$

elde edilir. $r_i(x)$'ler kendine resiprokal olmadığından $r_i(x)$ ve $b_i^*(x)r_i^*(x)$ polinomlarının ortak çarpanı yoktur. O halde (4.2) eşitliğinden $i = 2,3,\dots,k+1$ için $r_i(x) \mid f_1^*(x)$'dır. $j = 0,1,\dots,k+1$ için $f_j(x)$ fonksiyonları monik ikişerli aralarında asal polinomlar olduğundan $f_j(x)$ fonksiyonlarının çarpanları da birbirinden farklıdır. Dolayısıyla bu fonksiyonların resiprokal olmayan çarpanları da aralarında asaldır, yani $i = 2,3,\dots,k+1$ için $r_i(x)$'ler aralarında asaldır. Böylece $(r_2(x)r_3(x)\cdots r_{k+1}(x)) \mid f_1^*(x)$ olduğu elde edilir.

$f_0(x)f_1(x)f_2(x)\cdots f_{k+1}(x) = x^n - 1$ eşitliğinin her iki yanının resiprokalı alınırsa

$$\begin{aligned} f_0^*(x)f_1^*(x)f_2^*(x)\cdots f_{k+1}^*(x) &= -(x^n - 1) \\ &= -f_0(x)f_1(x)f_2(x)\cdots f_{k+1}(x) \end{aligned}$$

olduğundan

$$f_0^*(x)f_1^*(x)f_2^*(x)\cdots f_{k+1}^*(x)a(x) = -f_0^*(x)f_1^*(x)f_2^*(x)\cdots f_{k+1}^*(x)a(x)$$

dır. (4.2) eşitliğinden

$$f_1^*(x)f_2^*(x)\cdots f_{k+1}^*(x) = f_0(x)f_2(x)\cdots f_{k+1}(x)a(x)$$

olup bu eşitliğin her iki yanı $f_1(x)$ ile çarpılarak

$$\begin{aligned} f_1(x)f_1^*(x)f_2^*(x)\cdots f_{k+1}^*(x) &= f_1(x)f_0(x)f_2(x)\cdots f_{k+1}(x)a(x) \\ &= -f_0(x)f_1(x)f_2(x)\cdots f_{k+1}(x)a(x) \end{aligned}$$

elde edilir. O halde

$$f_1(x) = -f_0^*(x)a(x)$$

olup

$$f_1^*(x) = -f_0(x)a^*(x)$$

olduğundan $f_0(x) \mid f_1^*(x)$ elde edilir. $i = 1,2,3,\ldots,k+1$ için $f_i(x)$ polinomları aralarında asal ve $r_i(x)$ polinomları da $f_i(x)$ polinomlarının indirgenemez resiprokal olmayan çarpanlarının çarpımı olduğundan $i = 2,3,\ldots,k+1$ için $r_i(x)$ ile $f_0(x)$ aralarında asaldır. Dolayısıyla

$$f_0(x)_2(x)r_3(x)\cdots r_{k+1}(x) \mid f_1^*(x)$$

elde edilir.

Yeterlilik: $f_0(x)_2(x)r_3(x)\cdots r_{k+1}(x) \mid f_1^*(x)$ olsun. O halde

$$f^*(x) = f_0(x)r_2(x)r_3(x)\cdots r_{k+1}(x)m(x)$$

olacak şekilde bir $m(x) \in \mathbb{F}_{2^m}[x]$ vardır. $f_1(x)$ ile $f_{k+1}(x)$ aralarında asal olduklarından

$$f_1(x)s(x) + f_{k+1}(x)t(x) = 1$$

olacak şekilde $s(x),t(x) \in \mathbb{F}_{2^m}[x]$ vardır. Ayrıca $\widehat{f}_{k+1}(x) = f_0(x)f_1(x)f_2(x)\cdots f_k(x)$ olduğundan

$$\widehat{f}_{k+1}^*(x) = f_0^*(x)f_1^*(x)f_2^*(x)\cdots f_k^*(x)$$

dır. Buradan

$$\begin{aligned}
u^k\widehat{f_2^*}(x) &= u\widehat{f_{k+1}^*}(x)\cdot 1 = u\widehat{f_{k+1}^*}(x)(f_1(x)s(x)+f_{k+1}(x)t(x))\\
&= u^k f_0^*(x)f_1^*(x)f_3^*(x)\cdots f_{k+1}^*(x)f_1(x)s(x)\\
&\quad + u^k f_0^*(x)f_1^*(x)f_3^*(x)\cdots f_{k+1}^*(x)f_k(x)t(x)\\
&= u^k f_0^*(x)(f_0(x)r_2(x)r_3(x)\cdots r_{k+1}(x)m(x))f_3^*(x)\cdots f_{k+1}^*(x)f_1(x)s(x)\\
&\quad + u^k f_0^*(x)(f_0(x)r_2(x)r_3(x)\cdots r_{k+1}(x)m(x))f_3^*(x)\cdots f_{k+1}^*(x)f_k(x)t(x)\\
&= u^k f_0^*(x)(f_0(x)f_1(x)b_3(x)r_3(x)\cdots b_{k+1}(x)r_{k+1}(x))m(x)r_2(x)\cdots\\
&\qquad\qquad \varepsilon_3 r_3^*(x)\cdots\varepsilon_{k+1}r_{k+1}^*(x)s(x)\\
&\quad + u^k f_0^*(x)(f_0(x)b_2(x)r_2(x)r_3(x)\cdots f_k(x)b_{k+1}(x)r_{k+1}(x))m(x)r_k(x)\\
&\qquad\qquad \varepsilon_3 b_2(x)r_3^*(x)\cdots\varepsilon_{k+1}r_{k+1}^*(x)t(x)\\
&= u^k f_0^*(x)(f_0(x)f_1(x)f_3(x)\cdots f_{k+1}(x))\cdots\\
&\qquad\qquad \varepsilon_3\cdots\varepsilon_{k+1}r_2(x)r_2^*(x)\cdots r_{k+1}^*(x)m(x)s(x)\\
&\quad + u^k f_0^*(x)(f_0(x)f_2(x)f_3(x)\cdots f_{k+1}(x))\cdots\\
&\qquad\qquad \varepsilon_3\cdots\varepsilon_{k+1}r_2^*(x)\cdots r_{k+1}^*(x)m(x)t(x)\\
&= u^k\sigma_2\widehat{f_2}(x)+u^2\beta_2\widehat{f_1}\in\mathfrak{C}
\end{aligned}$$

olur. Benzer şekilde

$$u^{k-1}\widehat{f_3^*}(x),\cdots,u^3\widehat{f_{k-1}^*}(x),u^2\widehat{f_k^*}(x)\in\mathfrak{C}$$

olduğu gösterilebilir. Ayrıca

$$\widehat{f_0}(x)=f_1(x)f_2(x)\cdots f_{k+1}(x)$$

olduğundan

$$\widehat{f_0^*}(x)=f_1^*(x)(f_2(x)f_3(x)\cdots f_{k+1}(x))^*$$

olur. Buradan

$$\begin{aligned}\widehat{f_0}^*(x) &= (f_0(x)r_2(x)r_3(x)\cdots r_{k+1}(x)m(x))(b_2(x)r_2(x)\cdots b_{k+1}r_{k+1})^* \\ &= f_0(x)\varepsilon_2 b_2(x)r_2(x)\cdots\varepsilon_{k+1}b_{k+1}(x)r_{k+1}(x)m(x)r_2^*(x)\cdots r_{k+1}^*(x) \\ &= \varepsilon_2\cdots\varepsilon_{k+1}f_0(x)f_2(x)\cdots f_{k+1}(x)m(x)r_2^*(x)\cdots r_{k+1}^*(x) \in \mathfrak{C}\end{aligned}$$

dir. Böylece $\mathfrak{C}^{\perp} \subseteq \mathfrak{C}$ elde edilir.

□

Örnek 4.5.2. $n = 15$ ve $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2+u^3\mathbb{F}_2$ halkası göz önüne alınsın. $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2+u^3\mathbb{F}_2$ halkası üzerinde $x^{15}-1$ polinomu

$$x^{15}-1 = (x-1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$$

şeklinde indirgenemez ve monik çarpanlarına ayrılır.

$$\begin{aligned}f_0(x) &= 1 \\ f_1(x) &= (x^4+x+1)(x^4+x^3+x^2+x+1) \\ f_2(x) &= x^4+x^3+1 \\ f_3(x) &= x^2+x+1 \\ f_4(x) &= x-1\end{aligned}$$

şeklinde seçilirse

$$\begin{aligned}\widehat{f_0}(x) &= x^{15}-1 \\ \widehat{f_1}(x) &= (x-1)(x^4+x^3+1)(x^2+x+1) \\ \widehat{f_2}(x) &= (x-1)(x^2+x+1)(x^4+x+1)(x^4+x^3+x^2+x+1) \\ \widehat{f_3}(x) &= (x-1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1) \\ \widehat{f_4}(x) &= (x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)\end{aligned}$$

polinomları için

$$\mathfrak{C} = \left\langle \widehat{f_1}(x), u\widehat{f_2}(x), u^2\widehat{f_3}(x), u^3\widehat{f_4}(x) \right\rangle$$

$\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$ halkası üzerinde uzunluğu 15 olan bir devirli koddur. Böylece $i = 2,3,4$ için $r_i(x)$, $f_i(x)$'in indirgenemez ve kendine resiprokal olmayan çarpanlarının çarpımı olduğundan

$$r_2(x) = x^4 + x + 1$$
$$r_3(x) = 1$$
$$r_4(x) = 1$$

şeklindedir. Böylece

$$f_0(x)r_2(x)r_3(x)r_4(x) = 1 \cdot (x^4 + x^3 + 1) \cdot 1 \cdot 1 = x^4 + x^3 + 1$$

elde edilir. Dolayısıyla

$$f_1^*(x) = (x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$$

olduğundan

$$f_0(x)r_2(x)r_3(x)r_4(x) \mid f_1^*(x)$$

elde edilir. Teorem 4.5.1'den $\mathfrak{C}^{\perp} \subseteq \mathfrak{C}$'dir.

5. TARTIŞMA VE SONUÇ

Cebirsel kodlama teorisi, bilgi ve veri iletiminde güvenilirliği artırmak amacıyla geliştirilen matematiksel yöntemlerin temelini oluşturur. Modern iletişim sistemlerinde ve bilgi işlem teknolojilerinde karşılaşılan veri bozulmaları, iletim hataları ve dış etkenlere bağlı bilgi kayıpları gibi sorunların çözümünde kodlama teorisi önemli bir rol oynamaktadır. Bu bağlamda, cebirsel yapılarla temellendirilmiş kodlama yöntemleri, hem teorik sağlamlığı hem de uygulamadaki etkinliğiyle ön plana çıkmaktadır.

Özellikle sonlu cisimler ve halkalar gibi cebirsel yapıların, hata düzeltici kodların modellenmesinde ve analizinde kullanılması, kodlama teorisini yalnızca uygulamalı matematikle değil, aynı zamanda soyut cebirle de güçlü biçimde ilişkilendirmiştir. Cebirsel kodlama teorisi sayesinde, belirli hata modellerine karşı dayanıklı kodlar oluşturulabilmektedir. Bu kodların minimum uzaklıkları, dual yapıları ve devirli özellikleri matematiksel yöntemlerle analiz edilerek performansları hakkında yorum yapılabilmektedir. Bu tür matematiksel analizler, yalnızca teorik bilgi üretimi açısından değil, aynı zamanda yüksek hızlı veri iletimi, kriptografi, uydu haberleşmesi, kablosuz ağlar ve hatta biyolojik bilgi işleme sistemleri gibi çeşitli uygulama alanları açısından da büyük önem arz etmektedir.

Günümüzde gelişen teknolojiyle birlikte daha fazla veri daha hızlı bir şekilde iletilmekte ve daha düşük hata toleransları talep edilmektedir. Bu durum, daha güçlü, esnek ve optimize edilebilir kodlara olan ihtiyacı artırmaktadır. Bu durum cebirsel kodlama teorisinin hem akademik hem de endüstriyel açıdan stratejik bir alan olarak gelişimini sürdürmesini sağlamaktadır.

Cebirsel kodlama teorisinde, hata düzeltme ve tespit etme amacıyla çeşitli kod aileleri tanımlanmıştır. Bu kod aileleri, cebirsel yapıların kullanımıyla tanımlanır ve kodlama ile kod çözme işlemlerinde matematiksel etkinlik sağlar. En yaygın olarak incelenen kod aileleri arasında lineer blok kodlar, devirli kodlar, BCH kodları ve Reed–Solomon kodları yer alır. Lineer blok kodlar, vektör uzaylarında tanımlanan ve lineer cebir yöntemleriyle analiz edilebilen kodlardır. Devirli kodlar ise döngüsel özellikleri sayesinde hem kodlama hem de kod çözüm aşamasında hesaplama açısından pratiklik sağlar. BCH ve Reed–Solomon

kodları gibi daha genel yapılar ise çok daha yüksek hata düzeltme kapasiteleri sunarak özellikle dijital iletişim ve veri saklama sistemlerinde yaygın olarak kullanılmaktadır. Bu kodlar, cebirsel yapılar (örneğin sonlu cisimler) üzerinde inşa edilerek, yüksek doğrulukta bilgi iletimi için teorik ve pratik çözümler sunar. Bu örneklere benzer şekilde literatürde tanımlanmış ve farklı avantajlara sahip birçok kod ailesi vardır.

Cebirsel kodlama teorisinde dualini içeren devirli kodlar, hem zengin yapısal özellikleri hem de uygulamadaki etkinlikleri bakımından özel bir öneme sahiptir. Devirli kodlar, döngüsel özellikleri sayesinde hızlı algoritmalarla kodlama ve kod çözme olanağı sunar. Ayrıca dualini içeren devirli kodlar, kriptografi algoritmaları, kuantum hata düzeltme kodları ve simetrik veri iletimi gibi birçok uygulamada doğrudan kullanılabilecek avantajlı yapılardır. Bu kodlar, cebirsel yapılar üzerinde daha derin analizler yapılmasına olanak tanıdığı gibi, aynı zamanda güvenilir iletişim sistemleri tasarlamak için de sağlam bir matematiksel temel oluşturur. Bu nedenle, hem teorik inceleme hem de pratik uygulama açısından dualini içeren devirli kodlar kodlama teorisinin önemli yapı taşları arasında yer alırlar.

Bu tez çalışmasında, dualini içeren devirli kodlar çeşitli cebirsel yapılar üzerinde incelenmiş ve her bir cebirsel yapının söz konusu kodlara sağladığı yapısal avantajlar analiz edilmiştir. Bu inceleme, yalnızca kodlama teorisinin soyut yönleriyle sınırlı kalmayıp aynı zamanda cebirsel yapıların kodlama teorisi üzerindeki etkilerini de kapsamaktadır. Bir kodun dualini içermesi için gerekli ve yeterli koşulların belirlenmesi, çalışmada temel konu olarak ele alınmıştır. Bu koşullar, kullanılan alfabenin ait olduğu cebirsel yapıya (örneğin sonlu cisimler ya da sonlu halkalar) bağlı olarak önemli ölçüde farklılık göstermektedir. Bu bağlamda, literatürde daha önce yapılmış olan çalışmalar incelenmiş ve dualini içeren devirli kodların elde edilmesinde kullanılan yöntemler, çalışmanın dayandığı teorik zemini oluşturacak biçimde örneklendirilmiştir.

Bu çalışma çerçevesinde incelenen araştırmalar, dualini içeren devirli kodların varlığı ve yapısının, kullanılan kod alfabelerinin cebirsel özellikleriyle doğrudan ilişkili olduğunu ortaya koymaktadır. Bu açıdan değerlendirildiğinde, yalnızca klasik sonlu cisimler değil, aynı zamanda daha genel yapılar olan sonlu halkalar da dikkate alınmış, böylece kodlama teorisindeki yaklaşımın kapsamı genişletilmiştir.

Özellikle, ikili (binary) devirli kodların yanı sıra farklı sonlu komütatif halkalar ($v^2 = v$ olmak üzere $\mathbb{F}_2 + v\mathbb{F}_2$, $u^2 = 1$ olmak üzere $\mathbb{F}_p + u\mathbb{F}_p$, $u^2 = 0$ olmak üzere $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$

ve $u^{k+1} = 0$ olmak üzere $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + \cdots + u^k\mathbb{F}_{2^m}$) üzerinde tanımlanan devirli kodlar detaylı olarak ele alınmıştır. Bu sayede, göz önüne alınan cebirsel yapıların, kodların yapısı üzerindeki etkileri daha net biçimde analiz edilebilmiştir. Değişik halkalarda kodların dualini içerebilmesi için gereken yapısal koşulların analizi, çalışmanın temel taşlarından birini oluşturmaktadır.

Elde edilen sonuçlar, kodlama teorisinde halkalar üzerindeki kodlar dikkate alındığında, klasik cisimler üzerinden yapılan çalışmalara kıyasla daha esnek ve potansiyel olarak daha güçlü yapıların elde edilebileceğinin mümkün olduğunu göstermektedir. Bu durum, kodlama teorisinin hem teorik yönleri hem de pratik uygulamaları açısından önemli fırsatlar ortaya koyarak kodların tasarımı ve çözümlemesi bakımından farklı alfabelerin kullanımının daha elverişli olduğunu sunmaktadır. Özellikle, yeni nesil iletişim sistemleri, veri güvenliği uygulamaları ve hata düzeltme algoritmaları gibi alanlarda, halkalar üzerindeki devirli kodlar gelecekte önemli roller üstlenebilecektir.

Sonuç olarak, bu tez, dualini içeren devirli kodların yapısal özelliklerini detaylı biçimde inceleyerek, kodlama teorisinin gelişimine anlamlı katkılarda bulunmaktadır. Aynı zamanda, halkalara dayalı yaklaşımlar sayesinde kod tasarımının daha esnek hale getirilmesi ve farklı uygulama alanlarında kullanılabilirliğinin artırılması yönünde önemli fırsatlar sunmaktadır. Bu bağlamda, çalışma yalnızca mevcut literatüre katkı sağlamakla kalmayıp, ilerleyen dönemlerde yapılacak çalışmalara da ilham kaynağı olabilecek niteliktedir.

Bu tez çalışması literatürde dualini içeren devirli kodlarla ilgili bir derleme niteliğindedir. Bu kodların çeşitli sonlu halkalar üzerindeki yapısal özelliklerini inceleyerek kodlama teorisi alanına anlamlı katkılar sunmaktadır. Bununla birlikte, her bilimsel çalışmada olduğu gibi bu tez de belirli sınırlandırmalar ve kısıtlayıcı faktörler içermektedir. Bu faktörlerin farkında olmak, hem çalışmanın bulgularının yorumlanmasında hem de gelecekte yapılacak araştırmaların yönlendirilmesinde önem arz etmektedir. Örneğin tezde ele alınan halkalar birimli ve değişmeli halkalar olup bu halkalar, sonlu halkalar kümesinin yalnızca küçük bir alt kümesini temsil etmektedir. Birimli olmayan veya değişmeli olmayan halkalar gibi daha genel yapılar inceleme dışı bırakılmıştır. Diğer bir sınırlandırma kodların parametrelerinin göz önüne alınmamasıdır. Bu çerçevede kodların performansını doğrudan etkileyen parametrelerden biri olan minimum uzaklık, kod oranı ve hata düzeltme kapasitesi gibi ölçütler incelenmemiştir. Dolayısıyla gelecekte yapılacak çalışmalar, hem daha genel

cebirsel yapıları kapsamaya hem de kodların uygulamalardaki başarısını artıran faktörleri araştırmaya odaklanabilir.

KAYNAKLAR

[1]. Wan, Z., 2003, *Lectures on Finite Fields and Galois Rings*, World Scientific Publishing Company

[2]. Hungerford, T. W., 1980, *Algebra*,Springer-Verlag, New York

[3]. Hill, R., 1993, *A First Course in Coding Theory*, Oxford University Press, Oxford

[4]. Ling, S., Xing, C., 2004, *Coding Theory: A First Course*, Cambridge University Press, Cambridge

[5]. Ding, C., Pei, D., Salomaa, A., 1996, *Chinese Remainder Theorem, applications in computing, coding, cryptography*, World Scientific Publishing Co., Singapore

[6]. Dougherty, S. T., 1994, *Algebraic Coding Theory Over Finite Commutative Rings*, Springer International Publishing AG

[7]. Qian, J., 2013, *Quantum Codes from Cyclic Codes over* $F_2 + vF_2$, Journal of Information and Computational Science, vol. 10, pp. 1715-1722

[8]. Gao, J., Wang, Y., 2018 *u-Constacyclic codes over* $\mathbb{F}_p + u\mathbb{F}_p$ *and their applications of constructing new non-binary quantum code*, Quantum Information Processing, vol. 17, no. 4, pp. 1–9

[9]. Hammons, A. R., Kumar, P. V., Calderbank, A. R., Sloane, N. J. A., Sole, P., 1994, *The* $\mathbb{Z}_4$*-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Transactions on Information Theory, vol.40, no. 2, pp. 301-319

[10]. Wood, J. A., 1999, *Duality for modules over finite rings and applications to coding theory*, American Journal of Mathematics, vol. 121, no.3, pp. 555-575

[11]. MacWilliams, F. J., Sloane, N. J. A., 1977, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company

[12]. Lidl, R., Niederreiter, H., 1994, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, Cambridge

[13]. Zhu, S., Wang, Y., Shi, M., 2010, *Some Results on Cyclic Codes Over* $\mathbb{F}_2 + v\mathbb{F}_2$, IEEE Transactions on Information Theory, vol. 56, no. 4, pp. 1680-1684

[14]. Tang, Y., Yao, T., Zhu, S., Kai, X., 2020, *A Family of Constacyclic Codes over* $\mathbb{F}_{2^m} + u\mathbb{F}_{2^m}$ *and Its Application to Quantum Codes*, Chinese Journal of Electronics, vol. 29, no. 1, pp. 114-121

[15]. Tang, Y., Zhu, S., Kai, X., Ding, J., 2016, *New quantum codes from dual-containing cyclic codes over finite rings*, Quantum Information Processing, vol. 15, pp. 1489-1500

[16]. Li, R., Li, X., 2004, *Quantum codes constructed from binary cyclic codes*, International Journal of Quantum Information, vol. 2, no. 2, pp. 265-272

ÖZGEÇMİŞ

Kişisel Bilgiler	
Adı Soyadı	Ali SUBATAN
Doğum Yeri	
Doğum Tarihi	
Uyruğu	[X] T.C. [ ] Diğer:
E-Posta Adresi	
Web Adresi	

Eğitim Bilgileri	
Lisans	
Üniversite	İstanbul Üniversitesi
Fakülte	Fen Fakültesi
Bölümü	Matematik Bölümü
Mezuniyet Yılı	2022

Yüksek Lisans	
Üniversite	İstanbul Üniversitesi
Enstitü Adı	Fen Bilimleri
Anabilim Dalı	Matematik Anabilim Dalı
Programı	Matematik Programı
Mezuniyet Tarihi	