T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

# BAZI HALKALAR ÜZERİNDE TANIMLI ALT MODÜL KODLARI

FATİH TEMİZ

DOKTORA TEZİ
MATEMATİK ANABİLİM DALI
MATEMATİK PROGRAMI

DANIŞMAN
DOÇ. DR. E. MEHMET ÖZKAN

İSTANBUL, 2018

**T.C.**

**YILDIZ TEKNİK ÜNİVERSİTESİ**

**FEN BİLİMLERİ ENSTİTÜSÜ**

# BAZI HALKALAR ÜZERİNDE TANIMLI ALT MODÜL KODLARI

Fatih TEMİZ tarafından hazırlanan tez çalışması 05.09.2018 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda **DOKTORA TEZİ** olarak kabul edilmiştir.

**Tez Danışmanı**

Doç. Dr. Erdoğan Mehmet ÖZKAN

Yıldız Teknik Üniversitesi

**Jüri Üyeleri**

Prof. Dr. Bayram Ali ERSOY

Yıldız Teknik Üniversitesi _____

Doç. Dr. Erdoğan Mehmet ÖZKAN

Yıldız Teknik Üniversitesi _____

Doç. Dr. Uğur ŞENGÜL

Marmara Üniversitesi _____

Doç. Dr. Emre KOLOTOĞLU

Yıldız Teknik Üniversitesi _____

Dr. Öğr. Üyesi Elif Segah ÖZTAŞ

Karamanoğlu Mehmetbey Üniversitesi _____

Bu çalışma, Yıldız Teknik Üniversitesi Bilimsel Araştırma Projeleri Koordinatörlüğü'nün **FDK-2017-3037** numaralı projesi ile desteklenmiştir.

# ÖNSÖZ

Bu zorlu ve uzun yoldaki destekleri sebebiyle tez danışmanım Sayın Doç. Dr. Erdoğan Mehmet ÖZKAN'a teşekkürlerimi sunarım.

Tez dönemi boyunca gelişmeleri takip eden tez izleme komitesi üyeleri Sayın Prof. Dr. Bayram Ali ERSOY'a ve Sayın Doç. Dr. Uğur ŞENGÜL'e teşekkürler.

Bu tezi titizlikle okuyup, şekillenmesinde yardımcı olan jüri üyesi Sayın Doç. Dr. Emre KOLOTOĞLU'na ve bilgisayar programlama konusundaki önemli yardımları sebebiyle Sayın Dr. Öğr. Üyesi Elif Segah ÖZTAŞ'a çok teşekkürler.

Varlıklarıyla yaşamı benim için anlamlı kılan, tüm hayatım boyunca bana olan sevgilerini ve desteklerini bir an bile unutturmayan, emeklerinin karşılığını asla ödeyemeyeceğim sevgili anneme, babama, kardeşlerime ve tüm aileme sonsuz teşekkürler.

Hiçbir fedakârlık ve anlayışı benden esirgemeyen, bu zahmetli yolda daima yanımda olan, zor zamanlarımda bana umut veren, hayatımı güzelleştiren kıymetli eşim Nesrin'e sonsuz teşekkürler.

Eylül, 2018

Fatih TEMİZ

## İÇİNDEKİLER

## SİMGE LİSTESİ

| | |
|---|---|
| $\mathbb{Z}$ | Tam sayılar kümesi |
| $\mathbb{Q}$ | Rasyonel sayılar kümesi |
| $\mathbb{R}$ | Reel sayılar kümesi |
| $\mathbb{C}$ | Karmaşık sayılar kümesi |
| $(a,b)$ | $a$ ile $b$'nin en büyük ortak böleni |
| $C(n,r)$ | $n$'in $r$'li komibansyonu |
| $\lfloor a \rfloor$ | $a$'dan küçük ya da eşit, $a$'ya en yakın tam sayı |
| $\mathbb{F}_q$ | $q$ elemanlı cisim |
| $\mathbb{Z}_q$ | Modülo $q$ kalan sınıfı |
| $\mathcal{R}$ | $\mathbb{Z}_q + u\mathbb{Z}_q$ |
| $\mathfrak{R}_n$ | $(\mathbb{Z}_q + u\mathbb{Z}_q)[x]/\langle x^n - 1\rangle$ bölüm halkası |
| $C$ | Kod |
| $C^{\perp}$ | $C$ kodunun duali |
| $\lvert C \rvert$ | $C$ kodunun eleman sayısı |
| $\mathbb{F}_q^*$ | $\mathbb{F}_q - \{0\}$ |
| $\mathbb{Z}_n^*$ | $\mathbb{Z}_n$ halkasının birimsel elemanlarının kümesi |
| $der\left(f(x)\right)$ | $f(x)$ polinomunun derecesi |
| $(n,M)_q$ | $\mathbb{F}_q$ alfabesi üzerinde $n-$uzunluklu, $M$ elemanlı kod |
| $[n,k,d]_q$ | $\mathbb{F}_q$ alfabesi üzerinde $n-$uzunluklu, $q^k$ elemanlı lineer kod |
| $d(C)$ | $C$ kodunun minimum Hamming uzaklığı |
| $\mathbb{F}_q^n$ | $\mathbb{F}_q$ cismi üzerinde $n-$boyutlu vektör uzayı |
| $d_H(x,y)$ | $x$ ile $y$ vektörleri arasındaki Hamming uzaklığı |
| $w_H(x)$ | $x$ vektörünün Hamming ağırlığı |
| $\varphi(n)$ | $n$'den küçük ve $n$ ile aralarında asal olan sayıların sayısı |
| $C \oplus C^{\perp}$ | $C$ ile dualinin direkt toplamı |
| $\langle f(x) \rangle$ | $f(x)$ fonksiyonun ürettiği ideal |
| $\langle x,y \rangle$ | $x$ ile $y$ vektörlerinin iç çarpımı |

## KISALTMA LİSTESİ

| | |
|---|---|
| bkz. | bakınız |
| ISBN | International Standard Book Number |
| LFSR | Linear Feedback Shift Register |
| YTÜ | Yıldız Teknik Üniversitesi |
| vb. | ve benzeri |

## ŞEKİL LİSTESİ

Sayfa

# ÖZET

## BAZI HALKALAR ÜZERİNDE TANIMLI ALT MODÜL KODLARI

Fatih TEMİZ

Matematik Anabilim Dalı

Doktora Tezi

Tez Danışmanı: Doç. Dr. E. Mehmet ÖZKAN

20. yüzyılın ikinci yarısından bugüne dijital iletişim olağanüstü gelişerek verinin taşınması ve saklanmasının büyük önem kazanmasına neden oldu. Bu sebeple, veri kaybını önlemeyi veya kontrol edebilmeyi amaçlayan cebirsel kodlama teorisi ortaya çıktı ve hızla gelişti.

Lineer kodların önemli bir sınıfı olan devirli kodlar, matematiksel özellikleri ve bu özelliklerin elektronik devre yapılarına doğal uyumu sebebiyle haberleşme teorisi için hayati önemdedir.

Bazı lineer olmayan kodlar, hata düzeltme kapasitesi gibi daha iyi parametrelere sahip olabilse de, lineer kodlar gibi sistematik olmadıkları için üzerinde çalışılmaları ve bulunmaları daha zordur. Ne var ki, Hammons ve arkadaşları 1994'te yayımladıkları makalelerinde dörtlü lineer kodlar ve lineer olmayan ikili kodlar arasındaki ilişkiyi göstererek, nasıl lineer kodlar üzerinde çalışıp daha iyi parametreli lineer olmayan kodlar elde edilebileceğini gösterdiler. Pek çok çalışmaya ilham veren bu çalışmadan sonra birçok farklı halka üzerinde devirli kod yapıları ve bunların Gray fonksiyonları altındaki görüntüleri üzerine çalışmalar yapıldı.

Son zamanlarda, $q$ bir asalın kuvveti olmak üzere $\mathbb{Z}_q + u\mathbb{Z}_q$ üzerindeki devirli kodlar üzerine de çalışmalar yapıldı. Ne var ki, $R$ halkası üzerindeki $n$ uzunluklu bir lineer $C$ kodunun devirli olması için gerek ve yeter şartın kodsözlere karşılık gelen polinomların $R[x]/\langle x^n - 1\rangle$ halkasının bir ideali olması gerçeğine karşın, bu çalışmalar $(\mathbb{Z}_q + u\mathbb{Z}_q)[x]/\langle x^n - 1\rangle$ halkasının ideallerini belirleme problemi ile ilgilenmediler.

Bu tezde biz, $p$ bir asal ve $s$ pozitif bir tam sayı iken $q = p^s$ olmak üzere, $u^2 = 0$ için $\mathbb{Z}_q + u\mathbb{Z}_q$ halkalarının bütün ideallerini belirliyoruz. Sonrasında, bu ideallerin sayısını belirleyen bir formül veriyoruz. Daha sonra, $n$ ile $p$ aralarında asal olmak üzere, $(\mathbb{Z}_q + u\mathbb{Z}_q)[x]/ < x^n - 1 >$ halkasının ideal yapısını belirledikten sonra $n$ uzunluğundaki devirli kodları araştırıyoruz. Böylece, bir formül ile bu ideallerin sayısını vererek devirli kodların sayısını da belirliyoruz. Bazı sabit $q$ değerleri için özel kod aileleri üzerinde çalışıyoruz ve bu kodların eleman sayılarını belirliyoruz. Yine bu özel kod ailesinin dual kodları üzerinde çalışıyor ve eleman sayılarını belirliyoruz.

**Anahtar Kelimeler:** Lineer Kodlar, devirli kodlar, zincir olmayan halkalar, idealler, dual kodlar

## ABSTRACT

### SUBMODULE CODES OVER SOME RINGS

Fatih TEMİZ

Department of Mathematics

PhD Thesis

Advisor: Assoc. Prof. Dr. E. Mehmet ÖZKAN

Since the latter half of the $20^{th}$ century, the digital communication has been dramatically developed, and caused transmission and storing data to gain more importance. Hence algebraic coding theory which aims preventing or controlling the data loss arised and developed rapidly.

Cyclic codes, which are a significant class of linear codes, are vital for the communication theory, because of their mathematical properties and the natural adaption of these properties to electronic circuit structures and linear feedback shift registers (LFSR).

Although some non-linear codes may have better parameters, capability of error correcting for instance, they are more difficult to find and study since they are not as systematic as linear codes.

However, in 1994, Hammons et. al. presented how to obtain more acceptable non-linear codes via considering linear codes by showing the relation between quaternary linear codes and non-linear binary codes. After this work which inspired many works, the structure of cyclic codes and the Gray images of these codes have been studied over various rings.

Recently, cyclic codes over $\mathbb{Z}_q + u\mathbb{Z}_q$ where $q$ is a prime power and $u^2 = 0$ have been also considered. However, these studies do not deal with the ideal structure of the ring $(\mathbb{Z}_q + u\mathbb{Z}_q)[x]/ < x^n - 1 >$ in spite of the fact that a linear code $C$ of length $n$ over a

ring $R$ is cyclic if and only if the corresponding polynomials of its codewords form an ideal structure in the quotient ring $R[x]/<x^n-1>$.

In this thesis, we determine all the ideals of the rings $\mathbb{Z}_q+u\mathbb{Z}_q$, where $q=p^s$ , $p$ is any prime and $s$ is any positive integer with $u^2=0$. Next, we give a formula that enumerates the number of ideals of these rings. Afterwards, we investigate the cyclic codes of length $n$, where $n$ is relatively prime to $p$, considering the ideal structure of the quotient ring $(\mathbb{Z}_q+u\mathbb{Z}_q)[x]/<x^n-1>$. In this way, we determine the number of these ideals by giving a formula. We consider some special family of cyclic codes for some fixed values of $q$ and we find the size of these codes. We also consider dual codes of these special families and give the size of them.

**Keywords:** Linear codes, cyclic codes, non-chain rings, ideals, dual codes

# BÖLÜM 1

# GİRİŞ

## 1.1 Literatür Özeti

Kodlama teorisinin esas amacı, verinin (ses, görüntü, sinyal vb.) iletilmesi ve depolanması esnasında, verinin kanaldan geçerken gürültüye maruz kalması veya başka sebeplerle meydana gelebilecek veri kaybını ya da bozulmalarını düzeltmek ya da en azından hata meydana geldiğini tespit edebilmektir.

Claude Shannon'un 1948 yılında yayımladığı "A mathematical theory of communication" isimli çalışma [1], kodlama teorisinin doğmasına sebep oldu. Kısa sürede bilim insanlarının büyük ilgisini çeken bu alanda oldukça hızlı ilerlemeler kaydedildi. Kodlama teorisindeki problemler çoğunlukla mühendislik uygulamalarından ortaya çıksa da, bu alanın gelişimindeki kritik rolü matematiğin oynadığını belirtmek oldukça ilgi çekicidir [2]. Teori iletişim sistemleri, uydular, görüntü ve ses oynatıcılar, depolama sistemleri vb. gibi birçok yerde uygulama alanı buldu. Amaca uygun olarak etkili olması adına farklı kodlar inşa edildi. Bunlardan devirli kodlar, lineer (doğrusal) kodların oldukça önemli bir sınıfıdır. Lineer kodlar, cebirsel yapıda olmaları sebebiyle üzerinde çalışılması açısından önemli kolaylıklar sağlamaktadır. İnşaları, kodsözlerinin ve parametrelerinin belirlenmesi adına büyük avantaj sağlamaktadır. Bunlara ek olarak, lineer kodların önemli bir sınıfı olan devirli kodlar, kodlama ve dekodlama sürecinde ekstra kolaylık sağlar. Bunun sebebi, her bir kodsözün döngüsel olarak kaydırılmasıyla elde edilen vektörün yine bir kodsöz olmasıdır. Üstelik dijital devre yapılarındaki doğrusal geri beslemeli kaydırmalı yazdırgaç (linear feedback shift register) -kısaca LFSR- tasarımına doğal olarak adapte edilebilir ve dolayısıyla da teknolojide direkt

olarak kullanılabilirler. İlk kez 1957'de Prange tarafından çalışılan devirli kodlar [3], bahsedilen özellik ve avantajları sebebiyle kodlama teoriciler tarafından büyük bir ilgi görmüş ve geliştirilmiştir.

Lineer kodların sistematik yapıda olmasının yanı sıra, birçok lineer olmayan (nonlinear) kod, çok fazla elemana sahip olduğu için daha güçlü parametrelere sahiptir ve etkileri yüksektir. Hammons, Kumar, Calderbank, Sloane ve Sole 1994'teki çalışmalarında [4] Nordstrom-Robinson [5], Kerdock [6], Preparata [7], Goethals [8], ve Delsarte-Goethals [9] tarafından inşa edilen ve lineer olmayan ikili (binary) kodların, $\mathbb{Z}_4$ halkası üzerindeki lineer kodların Gray fonksiyonlar altındaki ikili görüntüleriyle basitçe inşa edilebildiğini gösterdiler. Ayrıca bu kodların polinom halkalarında uygun şekilde tanımlanarak yine $\mathbb{Z}_4$ halkası üzerinde devirli kodlara genişletilebileceğini ve dolayısıyla kodlama ve dekodlamalarının çok daha basitleştirilebileceğini gösterdiler. Pek çok çalışmaya ilham olan bu makeleden sonra değişik halkalar üzerinde devirli kod yapıları ve bunların değişik Gray fonksiyonları altındaki görüntüleri üzerine çalışmalar yapıldı.

Bu çalışmadan sonra Calderbank ve Sloane, 1995'te yayımlanan makalelerinde [10] $\mathbb{Z}_{p^n}$ halkası üzerinde $(n, p) = 1$ şartını sağlayan $n$ uzunluklu devirli kodların yapısını çalıştılar. Yine 1995'te Pless ve Qian, $\mathbb{Z}_4$ halkası üzerinde devirli kodlar ve kuadratik kalan kodlar üzerine çalışmalarını yayımladı [11]. Ardından lineer kodlar ailesinde önemli bir yeri olan kendine-dual kodlar, $\mathbb{Z}_4$ halkası üzerinde çalışıldı [12]. $\mathbb{F}_2 + u\mathbb{F}_2$ halkası, $\mathbb{Z}_4$ halkasının bazı iyi özelliklerini (eleman sayısı ve ideallerinin sayısı vb.) ve $\mathbb{F}_4$ cisminin bazı iyi özelliklerini (eleman sayısı ve karakteristik vb.) taşıdığı için üzerindeki devirli kod yapıları incelendi [13]. Bu halka üzerindeki lineer kodların tam ağırlık sayaçları 2002'de Şiap tarafından belirlendi [14]. Bundan sonra, $\mathbb{F}_q$ ve $\mathbb{Z}_2$ halkalarının farklı genişlemeleri üzerinde lineer kodlar ve devirli kodlar çokça çalışıldı [15] , [16], [17], [18], [19], [20], [21], [22]. Son zamanlarda, $u^2 = 0$ için $\mathbb{Z}_4 + u\mathbb{Z}_4$ halkası üzerindeki devirli kodlar ve bunların $\mathbb{Z}_4$ görüntüleri incelendi [23]. Ayrıca, $q$ bir asalın kuvveti olmak üzere $\mathbb{Z}_q + u\mathbb{Z}_q$ üzerindeki devirli kodların minimum üreteç kümeleri ele alındı [24]. Ne var ki, $R$ halkası üzerindeki $n$ uzunluklu bir lineer $C$ kodun devirli olması için gerek ve yeter şartın kodsözlere karşılık gelen polinomların $R[x]/ < x^n - 1 >$ halkasının

bir ideali olması gerçeğine karşın, bu çalışmalar $(\mathbb{Z}_q + u\mathbb{Z}_q)[x]/<x^n-1>$ halkasının ideallerini belirleme problemi ile ilgilenmediler. Bu güçlü ilişkinin kullanılabilmesi için bu tezde; $p$ bir asal ve $s$ pozitif bir tam sayı iken $q = p^s$ olmak üzere, $u^2 = 0$ için tüm $\mathbb{Z}_q + u\mathbb{Z}_q$ halkalarının bütün ideallerini belirliyoruz. Sonrasında, bu ideallerin sayısını belirleyen bir formül veriyoruz. Daha sonra, $n$ ile $p$ aralarında asal olmak üzere, $(\mathbb{Z}_q + u\mathbb{Z}_q)[x]/<x^n-1>$ halkasının ideal yapısını belirledikten sonra $n$ uzunluğundaki devirli kodları araştırıyoruz. Böylece, bir formül ile bu ideallerin sayısını vererek devirli kodların sayısını da belirliyoruz. Bazı sabit $q$ değerleri için özel kod aileleri üzerinde çalışıyoruz ve bu kodların eleman sayılarını belirliyoruz. Yine bu özel kod ailesinin dual kodları üzerinde çalışıyor ve eleman sayılarını belirliyoruz.

### 1.2 Tezin Amacı

Bu tezde, öncelikle $q$ bir asal sayının kuvveti ve $u^2 = 0$ olmak üzere $\mathbb{Z}_q + u\mathbb{Z}_q$ halkasının idealleri belirlenecek ve bu ideallerin sayısını veren bir formül elde edilecektir. Daha sonra $q$ ve $n$ aralarında asal olmak üzere $(\mathbb{Z}_q + u\mathbb{Z}_q)[x]/<x^n-1>$ halkasının ideallerinden faydalanılarak $\mathbb{Z}_q + u\mathbb{Z}_q$ halkası üzerindeki $n$ uzunluklu devirli kodların yapısı belirlenecek ve bunların sayısını veren bir formül elde edilecektir. Ayrıca bazı özel kod ailelerinin parametreleri ve duallerinin yapıları incelenecektir. Bu sayede daha önceden yapılmış olan çalışmaların genelleştirilmesi de amaçlanmaktadır.

### 1.3 Hipotez

$\mathbb{Z}_4$ halkasının ya da $\mathbb{Z}_q$ halkasının üzerindeki devirli kodların sayısı ile bu halkaların idealleri arasında birebir ilişki mevcutken $\mathbb{Z}_q + u\mathbb{Z}_q$ halkası üzerindeki devirli kodlar ile bu halkanın idealleri arasında böyle bir ilişki mevcut değildir. Üstelik zincir halkası olmayan bu $\mathbb{Z}_q + u\mathbb{Z}_q$ halkasının ideallerini belirlemek de çok basit değildir. $\mathbb{Z}_q + u\mathbb{Z}_q$ halkasının tüm ideallerini belirleyebilir ve sayısını verebiliriz. $q$ ile aralarında asal herhangi bir $n$ tam sayısı için de $(\mathbb{Z}_q + u\mathbb{Z}_q)[x]/<x^n-1>$ halkasının ideallerini ve bu

ideallerin sayısını belirleyerek, $\mathbb{Z}_q + u\mathbb{Z}_q$ halkası üzerindeki devirli kodların oldukça zengin olduğunu gösterebiliriz.

# BÖLÜM 2

## CEBİRSEL TEMEL KAVRAMLAR

Bu bölümde, tezin daha okunabilir olması için ileride kullanacağımız cebir bilgilerini mümkün olduğu kadar anlaşılır ve öz bir şekilde vereceğiz. Bölümün hazırlanmasında *A First Course In Abstract Algebra* [25] ve *Temel Grup Teorisi* [26] isimli eserlerden yararlanılmıştır.

Hayatımızın hemen her alanında kullandığımız toplama ve çarpma işlemleri, iki sayıyı işleme soktuğumuz için matematiksel olarak *ikili işlem* (*binary operation*) olarak adlandırılırlar. İkili işlemin matematiksel tanımı ise aşağıdaki gibidir:

**Tanım 2.1** $S \times S$ kartezyen kümeden $S$ üzerine tanımlanan fonksiyona, $S$ kümesi üzerinde ikili işlem denir.

**Örnek 2.2** Bilinen toplama "$+$" ve çarpma "$\cdot$" işlemleri $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ kümeleri üzerinde birer ikili işlemdir.

**Örnek 2.3** Bilinen bölme "$:$" işlemi ise sıfıra bölme işlemi tanımlı olmadığından yukarıdaki kümeler üzerinde bir ikili işlem değildir.

**Örnek 2.4** $M(\mathbb{R})$, girdileri (entry) reel sayılar olan tüm matrislerin kümesi olsun. Bilinen matris toplamı "$+$" da yine $M(\mathbb{R})$ kümesi üzerinde ikili işlem değildir. Çünkü farklı satır ve sütun sayılarına sahip matrislerin toplama işlemi tanımlı değildir.

## 2.1 Gruplar

Birinci derece denklem çözümlerinde kullandığımız birim ya da etkisiz (identity) eleman, ters (inverse) eleman ve birleşme (associativity) özelliği grup yapısının temelini oluşturur.

**Tanım 2.5** $G$ boş olmayan bir küme ve "$*$" işlemi $G$ üzerinde ikili işlem olsun. Aşağıdaki özellikler sağlanıyorsa $G$ kümesine "$*$" işlemi altında bir grup denir:

i. Her $a, b, c \in G$ için $(a*b)*c = a*(b*c)$ (birleşme)

ii. Her $x \in G$ için $e*x = x*e = x$ olacak şekilde bir $e \in G$ vardır (birim eleman)

iii. Her bir $a \in G$ için $a*a' = a'*a = e$ olacak şekilde bir $a' \in G$ vardır (ters eleman)

**Örnek 2.6** Bilinen toplama "$+$" işlemi altında $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ kümeleri birer gruptur.

**Örnek 2.7** Toplama işlemi altında $\mathbb{Z}^+$ kümesi grup değildir çünkü birim elemanı yoktur. Yine toplama işlemi altında $\mathbb{Z}^+ \cup \{0\}$ kümesi halen bir grup değildir. Çünkü birim eleman var olsa bile örneğin $5$'in tersi yoktur.

**Örnek 2.8** Bilinen çarpma işlemi altında $\mathbb{Z}^+$ grup değildir çünkü örneğin $2$'nin tersi yoktur. Fakat çarpma işlemi altında $\mathbb{Q}^+, \mathbb{R}^+, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ kümeleri birer gruptur.

**Tanım 2.9** Bir grubun ikili işlemi değişmeli ise yani her $a$ ve $b$ elemanı için $a*b = b*a$ oluyorsa o gruba *değişmeli grup* ya da *Abel grubu* denir. Şimdiye kadar verilen grup örneklerinin tümü değişmelidir.

**Örnek 2.10** Girdileri reel sayılar olan bütün $n \times n$'lik matrislerin kümesi $M_n(\mathbb{R})$, matris çarpımı altında grup değilken, bunlardan terslenebilir olan matrislerin oluşturduğu $S$ alt kümesi matris çarpımı altında bir gruptur.

**Tanım 2.11** Bir $G$ grubunun $H$ alt kümesi, $G$'nin ikili işlemi altında kapalıysa ve $G$'den kısıtlanmış ikili işlem altında kendisi bir grup ise $H$'ye $G$'nin altgrubu denir.

**Tanım 2.12** $G$ bir grup ve $H$ de $G$'nin bir altgrubu olsun. $a \in G$ için $aH = \{ah \mid h \in H\}$ kümesine, $H$'nin ($a$'yı kapsayan) *sol yankümesi* (left coset) ya da

*sol sınıfı*, *soldan ötelemesi* denir. $Ha$ kümesi de benzer şekilde tanımlanarak *sağ yanküme* olarak adlandırılır.

**Teorem 2.13** Bir altgrubun herhangi iki soldan ötelemesi ya aynıdır ya da ayrıktır.

Modern cebirin klasik cebirden en önemli farkı; klasik cebirde elemanlarla çalışılırken modern cebirde ise kümeler ve yapılar üzerinde çalışılır.

**Tanım 2.14** $G$ bir grup ve $H \leq G$ olsun. Sol ötelemeler kümesi $G/H$ aşağıdaki gibi tanımlanır:

$G/H = \{gH \mid g \in G\}$.

**Tanım 2.15** $G$ bir grup ve $H \leq G$ olsun. Eğer her $g \in G$ için $gH = Hg$ ise $H$'ye, $G$'nin normal altgrubu denir ve $H \lhd G$ ile gösterilir.

**Teorem 2.16** $H \lhd G$ olsun. Bu durumda $G/H$ bölüm kümesi

$(aH)(bH) = (ab)H$

işlemi altında bir grup yapısı oluşturur.

## 2.2 Halkalar

Şimdiye kadar kümeler üzerinde tek bir ikili işlemin tanımlandığı yapılar olan gruplarla ilgilendik. Fakat bir küme üzerinde iki tane ikili işlemle çalışmanın önemi ve gerekliliği halka kavramının tanımlanmasını gerektirir.

**Tanım 2.17** $R$ boş olmayan bir küme ve toplama "$+$" ile çarpma "$\cdot$" $R$ üzerinde tanımlı ikili işlem olsunlar. Eğer aşağıdaki özellikler sağlanıyorsa $(R,+,\cdot)$ bir *halka*dır.

i. $(R,+)$ bir gruptur.

ii. Çarpma işlemi birleşme özelliğini sağlar.

iii. Her $a,\ b,\ c \in R$ için *soldan dağılma özelliği*, $a\cdot(b+c) = (a\cdot b)+(a\cdot c)$ ve *sağdan dağılma özelliği*, $(a+b)\cdot c = (a\cdot c)+(b\cdot c)$ sağlanır.

Eğer $R$'nin boştan farklı bir $S$ alt kümesi, aynı işlemler ile bir halka yapısı oluşturuyor ise $(S,+,\cdot)$'ye $R$'nin alt halkası denir.

**Örnek 2.18** $(\mathbb{Z},+,\cdot),\ (\mathbb{Q},+,\cdot),\ (\mathbb{R},+,\cdot)$ ve $(\mathbb{C},+,\cdot)$ birer halkadır.

**Tanım 2.19** Bir halkadaki -varsa- çarpımsal etkisiz elemana (çarpımsal) *birim* denir ve $1_R$ ile gösterilir. Birimi olan halkaya birimli halka denir.

**Tanım 2.20** $a$ ve $b$ bir $R$ halkasının, $ab=0$ eşitliğini sağlayan sıfırdan farklı iki elemanı olsun. Bu durumda $a$'ya ve $b$'ye *sıfır bölen* (*zero divisor*) denir.

**Örnek 2.21** $\mathbb{Z}_{12}$ halkasındaki $2,\ 3,\ 4,\ 6,\ 8,\ 9$ ve $10$ elemanları sıfır bölendir.

**Tanım 2.22** Sıfır böleni olmayan birimli halkaya *tamlık bölgesi* (*integral domain*) denir.

**Örnek 2.23** $\mathbb{Z}$ tam sayılar halkası, $p$ asal sayı olmak üzere $\mathbb{Z}_p$ halkası tamlık bölgesidir.

Sadeleştirme kuralının geçerli olabilmesi için tamlık bölgelerine ihtiyaç duyulur ve bu açıdan tanımlanmaları önemlidir. Ayrıca, polinom çözümlerinde, sıfır bölenli halkalarda polinomun derecesinden daha fazla kök bulunabilmekte, bu da yine tamlık bölgesinin önemini göstermektedir.

Gruplardaki bölüm grubu yapısına benzer bir yapı halkalar için de tanımlıdır. Bölüm grubunu tanımlayabilmek için normal altgrupların tanımlanması gibi, bölüm halkasının tanımlanması için de *ideal* yapılarına ihtiyaç duyulur.

**Teorem 2.24** Bir $x$ belirsiziyle (değişken), katsayıları bir $R$ halkasından bütün polinomların kümesi $R[x]$, polinom toplamı ve çarpımı altında bir halkadır. Eğer $R$ birimli ise $R$'nin birimi aynı zamanda $R[x]$'in de birimidir.

**Tanım 2.25** $a^2=a$ eşitliğini sağlayan bir $R$ halkasının $a$ elemanına *idempotent* eleman, herhangi bir $n\in\mathbb{Z}^+$ için $b^n=0$ eşitliğini sağlayan $b$ elemanına *nilpotent* eleman denir.

**Tanım 2.26** $R$ bir halka ve $I$ da althalkası olsun. Eğer her $r\in R$ için $rI\subseteq I$ ve $Ir\subseteq I$ ise $I$'ya *ideal* denir.

**Teorem 2.27** $R$ bir halka ve $I$ da ideali olsun. Bu durumda $I$'nın toplamsal ötelemeleri $R/I$ aşağıdaki ikili işlemler altında bir halka yapısı oluşturur.

$$(a+I)+(b+I)=(a+b)+I$$
$$(a+I)(b+I)=ab+I$$

**Teorem 2.28** Yukarıda tanımlanan $R/I$ halkası *bölüm halkası* (*factor ring, quotient ring*) olarak adlandırılır.

**Tanım 2.29** Bir $R$ halkasının kendisinden farklı bir $M$ ideali, eğer $R$'nin bir öz $N$ ideali tarafından kapsanmıyorsa *maksimal ideal* olarak adlandırılır. Bir tane maksimal ideali olan halkalara *yerel* ya da *lokal halka* (local ring) denir.

**Tanım 2.30** Bir $R$ halkasının $P \neq R$ ideali, eğer $a,b \in R$ elemanları için $ab \in P$ olduğunda $a \in P$ veya $b \in P$ oluyorsa $P$'ye *asal ideal* denir.

**Tanım 2.31** Bir $R$ halkasının $P \neq R$ ideali, eğer $a,b \in R$ elemanları için $ab \in P$ olduğunda $a \in P$ veya bir $n > 0$ tam sayısı için $b^n \in P$ oluyorsa $P$'ye *asalımsı ideal* denir.

**Tanım 2.32** Bir $R$ halkasında, bütün $a \in R$ elemanları için $n \cdot a = 0$ eşitliğini sağlayan en küçük pozitif $n$ tam sayısına *karakteristik* denir. Eğer böyle bir sayı yoksa karakteristik $0$'dır.

## 2.3 Cisimler

**Tanım 2.33** $R$, birimi $1_R \neq 0$ olan bir halka olsun. Bir $a \in R$ elemanının *çarpımsal tersi*, $aa^{-1} = a^{-1}a = 1$ eşitliğini sağlayan $a^{-1} \in R$ elemanıdır. Çarpımsal tersi olan elemanlara *birimsel* eleman (unit) denir. Eğer değişmeli bir $F$ halkasının sıfırdan farklı her elemanı birimsel ise $F$'ye cisim (field) denir.

**Örnek 2.34** $\mathbb{Z}$ bir cisim değildir. Çünkü örneğin, $2$ elemanının çarpımsal tersi yoktur. Fakat $\mathbb{Q}$ ve $\mathbb{R}$ birer cisimdir. $p$ bir asal sayı olmak üzere $\mathbb{Z}_p$ de sonlu cisimdir.

**Teorem 2.35** Birimli ve değişmeli bir $R$ halkasının $M$ idealinin maksimal olması için gerek ve yeter koşul $R/M$'nin cisim olmasıdır.

**Teorem 2.36** Birimli ve değişmeli bir $R$ halkasının $P$ idealinin asal olması için gerek ve yeter koşul $R/P$'nin tamlık bölgesi olmasıdır.

Sonlu cisimlerin eleman sayısı $\mathbb{Z}_p$ ($p$ asal) örneğinde olduğu gibi ya asaldır ya da bir asalın kuvvetidir. Eleman sayısı asal olmayan cisimler, $\mathbb{Z}_p[x]$ polinom halkasının,

indirgenemez bir polinomun ürettiği maksimal ideale bölüm halkası ile elde edilirler ve $\mathbb{F}_q$ ile gösterilirler.

## 2.4 Vektör Uzayları

Kodlama teorisinin temellerini anlatacağımız kısımda kullanacağımız vektör uzaylarının, soyut cebirsel temel kavramlara aşina olmayan okuyucular için de anlaşılabilir olması için daha soyut bir tanım yerine aşağıdaki tanımı vermeyi daha uygun gördük.

**Tanım 2.37** [27] $V$ **,** üzerinde toplama ve skaler çarpım tanımlı olan bir küme olsun. Yani $V$'deki her $x$ ve $y$ çifti için, $V$'de tek bir $x+y$ elemanı, yine $V$'deki her $x$ elemanı ve skaler bir $\alpha$ için $V$'de tek bir $\alpha x$ elemanı elde edilsin. Bu durumda, aşağıdaki aksiyomlar sağlanıyorsa, toplama ve çarpım işlemleriyle birlikte $V$ bir *vektör uzayı*dır.

i. $V$'deki her $x$ ve $y$ için $x+y=y+x$

ii. $V$'deki her $x,y,z$ için $(x+y)+z=x+(y+z)$

iii. Her $x\in V$ için $x+0=x$ olacak şekilde bir $0\in V$ vardır

iv. Her $x\in V$ için $x+(-x)=0$ olacak şekilde bir $-x\in V$ vardır

v. Her $\alpha$ skaleri ve her $x,y\in V$ için $\alpha(x+y)=\alpha x+\alpha y$

vi. Her $\alpha,\beta$ skalerleri ve her $x\in V$ için $(\alpha+\beta)x=\alpha x+\beta x$

vii. Her $\alpha,\beta$ skalerleri ve her $x\in V$ için $(\alpha\beta)x=\alpha(\beta x)$

viii. Her $x\in V$ için $1\cdot x=x$

**Not:** Daha cebirsel bir ifade ile vektör uzayları, yukarıda tanımladığımız cisimler üzerinde tanımlıdır. Bahsi geçen skalerler, bu cismin elemanları ve skaler (dış) çarpım da cismin elemanı ile vektör uzayının elemanının çarpımıdır.

**Örnek 2.38** Bir kaç farklı vektör uzayı örneği verelim.

i. Her cisim, kendi üzerinde bir vektör uzayıdır: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_2$, $\mathbb{F}_{16}$

ii. $\mathbb{R}$ cismi üzerinde $\mathbb{R}^2=\{(a,b):a,b\in\mathbb{R}\}$

iii. Bir $\mathbb{F}_q$ cismi üzerinde $\mathbb{F}_q^n = \{(v_1, v_2, \ldots, v_n) \mid v_i \in \mathbb{F}_q\}$

iv. Bir $\mathbb{F}_q$ cismi üzerinde $\{(\alpha, \ldots, \alpha) \mid \alpha \in \mathbb{F}_q\}$

**Tanım 2.39** Bir $V$ vektör uzayının bir $C$ alt kümesi, aynı toplama ve skaler çarpım işlemleri ile vektör uzayı aksiyomlarını sağlıyorsa (kendisi de bir vektör uzayı ise) $V$'nin *alt uzayı* ya da *alt vektör uzayı* olarak adlandırılır.

**Örnek 2.40** Örnek 2.36'da (iv) şıkkında verilen vektör uzayı, (iii) şıkkında verilen vektör uzayının bir alt uzayıdır.

Kodlama teorisinde büyük önemi ve yeri olan lineer kodlar, vektör uzayları sayesinde tanımlanır. Lineer kodlar; teknolojiye uygulanabilirliği, üzerinde çalışmanın kolay olması ve sistematik yapıda olmalaları sebebiyle oldukça önemlidir.

**Tanım 2.41** $\mathbb{F}$ cismi üzerideki $V$ vektör uzayında, her bir $x$ ve $y$ vektör çiftini $\langle x, y \rangle \in \mathbb{F}$ skalerine götüren ve aşağıdaki özellikleri sağlayan işleme iç çarpım denir:

i. $\langle x, x \rangle \geq 0$ ve $\langle x, x \rangle = 0 \Leftrightarrow x = 0$

ii. Her $x, y \in V$ için $\langle x, y \rangle = \langle y, x \rangle$

iii. Her $x, y, z \in V$ ve her $\alpha, \beta \in \mathbb{F}$ için $\langle \alpha x + \beta y, z \rangle = \alpha \langle x, z \rangle + \beta \langle y, z \rangle$ dir.

## 2.5 Modüller

Bölüm 1'de bahsettiğimiz gibi yalnızca cisimler üzerindeki kodlar değil halkalar üzerindeki kodlar da etkili olabilmektedir. Cisimler üzerindeki lineer kodların matematiksel olarak vektör uzaylarına karşılık gelmesine benzer şekilde, halkalar üzerindeki lineer kodlar da, bir başka matematiksel yapı olan modüllere karşılık gelmektedir. Tanımı itibariyle vektör uzaylarına oldukça benzeyen modüller, halkalar üzerinde tanımlandığından yapısal olarak önemli farklılıklar göstermektedir.

**Tanım 2.42** $(R, +, \cdot)$ bir halka olsun.

$\odot : R \times M \to M$ skaler çarpımı ile birlikte aşağıdaki özellikleri sağlayan $(M, \oplus)$ abel grubu, sol $R$-modül olarak adlandırılır:

i. $r \odot (a \oplus b) = (r \odot a) \oplus (r \odot b)$, her $r \in R$ ve her $a, b \in M$ için

ii. $(r+s)\odot(a)=(r\odot a)\oplus(s\odot a)$, her $r,s\in R$ ve her $a\in M$ için

iii. $r\odot(s\odot a)=(rs)\odot a$, her $r,s\in R$ ve her $a\in M$ için

iv. Eğer halka birimli ise $1\odot a=a$, her $a\in M$ için.

**Örnek 2.43** Bir kaç farklı modül örneği verelim:

i. Her $R$ halkası kendi üzerinde bir modüldür: $\mathbb{Z}$-modül $\mathbb{Z}$ vb.

ii. Her toplamsal $G$ grubu bir $\mathbb{Z}$-modüldür: $\mathbb{Z}$-modül $\mathbb{Z}_n$ vb.

iii. Bir $\mathbb{F}$ cismi üzerindeki $V$ vektör uzayı, $\mathbb{F}$-modüldür.

# BÖLÜM 3

## HATA DÜZELTEN KODLAR

1948'de Shannon'un yayımladığı "A mathematical theory of communication" isimli çalışma [1] bir çığır açarak enformasyon teorisi ve kodlama teorisinin doğmasına sebep oldu. Bu çalışmasında Shannon, üzerinde taşınan bilgilerin bozulmaya uğrayabileceği gürültülü (noisy) bir iletişim kanalı için kanal kapasitesi ismini verdiği bir sayı tanımladı ve bu kapasitenin altındaki herhangi bir hızda (rate) güvenilir iletişimin mümkün olacağını gösterdi. Örneğin, uzak gezegenleri fotoğraflayıp bunları dünyaya gönderen bir uzay aracının, iletimde bir aksaklık olduğunda bu fotoğrafları yeniden göndermesi masraflı ve zaman alıcı, dolayısıyla da elverişsizdir. Bunun yerine, belirlenecek olan bir doğruluk oranında dekodlanması mümkün olacak biçimde, gönderilecek veri kodlanabilir. Aynı sebeplerle elektronik iletişim sistemlerinde, manyetik depolama sistemlerinde, CD'lerde cebirsel kodlama yapılmaktadır. Bir başka örnek olarak cep telefonlarını düşünebiliriz. İki cep telefonu arasındaki bir konuşmada, önce telefon sesimizi elektrik sinyaline dönüştürür. Daha sonra bu sinyaller, radyo dalgaları ile en yakındaki baz istasyonuna gönderilir. Baz istasyonları arasındaki iletişim ağı sayesinde karşıdaki telefona en yakın baz istasyonuna iletilen radyo dalgaları, buradan karşıdaki telefona iletilir ve tekrar sese dönüştürülür. Bu iletişim esnasında hava, iletişim kanalı olarak düşünülebilir. Yine iletişim anında meydana gelebilecek gürültüler (havadaki statik elektrik, termal sebepler, radyasyon, endüstriyel gürültü vb.) sebebiyle bilgiler kodlanır. Mesajın ses ya da görüntü, alıcının bu sesi ya da görüntüyü dinleyen/izleyen kişi ve kanalın ise bir CD olarak ele alınabileceği bir başka örnekte ise gürültü olarak CD üzerindeki çizikler ve parmak izleri düşünülebilir. Kısaca, alınan bilginin gönderilenle

her zaman aynı olmadığı iletişim sistemini gürültülü kanal olarak tanımlayabiliriz ve kodlamanın temel problemi, alınan bilgiden gönderilen bilgiyi elde etmektir.

Günlük hayatta sıkça karşılaştığımız bir başka kodlama örneği de barkod (barcode) sistemidir. Marketten aldığımız bir ürün kasada barkod okuyucu ile tanınır ve ücret ödeme işlemi gerçekleşir. Bu kodlama ve diğer kodlamalar *kaynak kodlaması* ve *kanal kodlaması* olmak üzere iki aşamada gerçekleşir. Kaynak kodlaması, mesajı kanaldan iletilebilecek uygun bir koda çevirmekten ibarettir. Kanal kodlaması ise, alıcının mesajda bir hata olup olmadığını anlamasını, hatta düzeltebilmesini sağlayacak şekilde mesaja fazlalıklar eklemektir ve bizim kodlama deyince ilgilendiğimiz ve kast ettiğimiz kodlama bu cebirsel kısım yani kanal kodlamadır. Barkod okuyucu, ürün üzerindeki kalın ve ince çizgileri (bar) okurken, ışık (düşük kontrast), yanlış okutma açısı veya barkod üzerindeki bir hasar sebebiyle hata meydana gelebilir ve farklı bir ürün olarak tanıyabilir. Bunu engellemek için hata tespiti yapan (kaynak) kodlama yapılır. Birçok benzer uygulama günlük hayatta sıkça karşımıza çıkar: ISSN kod, ISBN kod, QR kod vb. Yine kredi kartı numaraları, Türkiye Cumhuriyeti Kimlik Numarası gibi bilgilerde doğrulama yapma amacıyla kodlama yapılmaktadır.

Bu bölümde, hata düzelten kodlar hakkında temel kavramlar ve bilgiler verilecektir. Bölümün hazırlanmasında *Fundamentals of Error Correcting Codes* [28], *Coding Theory: A First Course* [2] ve *Quaternary codes* [29] isimli kaynaklardan yararlanılmıştır.

## 3.1 Temel Kavramlar

**Tanım 3.1** $A=\{a_1,a_2,\ldots,a_q\}$, elemanlarına *kod sembolleri* ve kendisine *kod alfabesi* diyeceğimiz, $q$ elemanlı bir küme olsun.

**i.** $A$ üzerinde, $n$ uzunluğunda, $q$-lu bir *söz*, tüm $i$'ler için her bir $w_i \in A$ olan bir $\mathbf{w}=w_1w_2\cdots w_n$ dizisidir. $\mathbf{w}$ aynı zamanda, $(w_1,w_2,\ldots,w_n)$ vektörü olarak da kabul edilebilir.

**ii.** $A$ üzerinde, $n$ uzunluğunda $q$-lu bir blok kod, aynı $n$ uzunluğuna sahip $q$-lu sözlerin boştan farklı bir $C$ kümesidir.

**iii.** $C$'nin bir elemanı, $C$'nin kodsözü olarak adlandırılır.

**iv.** $C$'deki kodsözlerin sayısına, $C$ kodunun eleman sayısı (size) denir ve $|C|$ ile gösterilir.

**v.** Uzunluğu $n$ olan ve eleman sayısı $M$ olan koda bir $(n,M)$-kod denir.

Birkaç özel örnek olarak, $\mathbb{F}_2=\{0,1\}$ alfabesi üzerindeki koda ikili (binary) kod, $\mathbb{F}_3=\{0,1,2\}$ alfabesi üzerindeki koda üçlü (ternary) kod denir. Dörtlü (quaternary) kod ise bazen $\mathbb{F}_4=\{0,1,\alpha,1+\alpha\}$ alfabesi üzerindeki koda bazen de $\mathbb{Z}_4=\{0,1,2,3\}$ alfabesi üzerindeki koda denir.

**Tanım 3.2** $x=(x_1,x_2,...,x_n)$ ve $y=(y_1,y_2,...,y_n)$ $A$ alfabesi üzerinde iki söz olsun. $x$ ile $y$ arasındaki (*Hamming*) *uzaklığı,* $x$ ve $y$ nin farklı olduğu koordinatların sayısıdır ve $d(x,y)$ ile gösterilir. Yani $d(x,y)=\left|\{i\mid x_i\neq y_i,\ i=1,2,\ldots,n\}\right|$.

**Örnek 3.3** $x=01010110$ ve $y=11010101$ ise $d(x,y)=3$ tür.

**Önerme 3.4** $d:A^n\times A^n\to\mathbb{N}\cup\{0\}$ uzaklık fonksiyonu bir metriktir. Yani $A$ alfabesi üzerinde, $n$ uzunluğundaki $x,y,z$ sözleri için

i. $0\le d(x,y)\le n$

ii. $d(x,y)=0$ ancak ve ancak $x=y$

iii. $d(x,y)=d(y,x)$

iv. $d(x,z)\le d(x,y)+d(y,z)$ (üçgen eşitsizliği)

**Tanım 3.5** En az iki kodsöze sahip bir $C$ kodunun *(minimum) uzaklığı* $d(C)=\min\{d(x,y)\mid x,y\in C, x\neq y\}$ olarak tanımlanır.

**Tanım 3.6** $n$ uzunluğunda, $M$ elemana sahip ve uzaklığı $d$ olan bir kod $(n,M,d)$-kod olarak gösterilir. $n,M,d$ sayıları da kodun *parametreleri* olarak adlandırılır.

**Örnek 3.7** $C=\{00000,10110,01110\}$ ikili bir kod olsun. Burada

$d(00000,10110)=3$, $d(00000,01110)=3$ ve $d(10110,01110)=2$ olduğu için $d(C)=2$ dir ve $C$ bir $(5,3,2)$-koddur.

Şimdi, bir kodun kaç hata tespit edebildiği ya da düzeltebildiğini açıklayan tanımları ve sonrasında kodun uzaklığı ile hata düzeltme ve hata tespit etme kapasitesi arasındaki yakın ilişkiyi gösteren teoremleri veriyoruz.

**Tanım 3.8** $t$ pozitif bir tam sayı olsun. Bir $C$ kodundaki bir kodsözde en az bir, en çok $t$ hata meydana geldiğinde oluşan söz eğer kodsöz değilse, bu koda $t$-hata tespit eden kod denir. Eğer $C$ kodu $t$-hata tespit eden kod ise ancak $(t+1)$-hata tespit eden kod değilse, $C$ ye tam $t$-hata tespit eden kod denir.

**Örnek 3.9** $C=\{000000,110101,011100\}$ ikili kodu $2$-hata tespit eden koddur. Çünkü kodsözlerden herhangi birinin iki koordinatını değiştirerek başka bir kodsöz elde etmek mümkün değildir.

$000000 \to 110101$ dönüşümü için 4 koordinatın değişmesi gerekir.

$000000 \to 011100$ dönüşümü için 3 koordinatın değişmesi gerekir.

$110101 \to 011100$ dönüşümü için 3 koordinatın değişmesi gerekir.

O halde $C$ tam $2$-hata tespit eden koddur. Çünkü $000000$ kodsözünün 2, 3 ve 4. koordinatları $0$'dan $1$'e değiştiğinde $011100$ kodsözü elde edilir. Yani $C$ kodu $3$-hata tespit eden kod değildir.

**Teorem 3.10** Bir $C$ kodunun $t$-hata tespit eden bir kod olması için gerek ve yeter koşul $d(C)\geq t+1$ olmasıdır. Diğer bir ifadeyle uzaklığı $d$ olan bir kod, tam $(d-1)$-hata tespit eden koddur.

**Tanım 3.11** $t$ pozitif bir tam sayı olsun ve iletişim için $C$ kodu kullanılsın. Eğer alınan bir söz, kendine en yakın uzaklıktaki kodsöze dekodlandığında $t$ veya daha az hata düzeltilebiliyorsa, yani $t$ ya da daha az sayıda koordinatı farklı olan ancak bir kodsöz varsa, $C$ kodu $t$-hata düzelten kod olarak adlandırılır. Eğer $C$ kodu $t$-hata düzelten bir kod ise ancak $(t+1)$-hata düzelten kod değilse, tam $t$-hata düzelten kod olarak adlandırılır.

**Örnek 3.12** $C=\{000000,110101,011100\}$ ikili kodu $2$-hata tespit eden koddur. Çünkü kodsözlerden herhangi birinin iki koordinatını değiştirerek başka bir kodsöz elde etmek mümkün değildir. Ayrıca $C$ kodu $1$-hata düzelten koddur:

• Eğer $000000$ kodsözü gönderilirse ve bir hata meydana gelirse, elde edilebilecek olan sözler $(100000, 010000, 001000, 000100, 000010$ ya da $000001)$ $000000$'a dekodlanacaktır.

• Eğer $110101$ kodsözü gönderilirse ve bir hata meydana gelirse, elde edilebilecek olan sözler $(010101, 100101, 111101, 110001, 110111$ ya da $110100)$ $110101$'e dekodlanacaktır.

• Eğer $011100$ kodsözü gönderilirse ve bir hata meydana gelirse, elde edilebilecek olan sözler $(111100, 001100, 011000, 010100, , 011110$ ya da $011101)$ $011100$'a dekodlanacaktır.

Tüm durumlarda, meydana gelen tek hata düzeltilir. Öyleyse $C$ kodu $1$-hata düzelten koddur.

Diğer taraftan, eğer iki adet hata meydana gelirse, yanlış kodsöze dekodlama yapılabilir. Örneğin, $110101$ kodsözü gönderilmiş ve $110000$ sözü alınmış (4. ve 6. koordinatlarda hata meydana gelmiş) olsun. Bu durumda, en yakın $110000$ sözü, en yakın kodsöze dekodlanacağı için ve hem $000000$ kodsözüne hem de $110101$ kodsözüne $2$-uzaklıkta olduğu için dekodlama yapılamaz. Öyleyse $C$ kodu tam $1$-hata düzelten koddur.

**Teorem 3.13** Bir $C$ kodunun $t$-hata düzelten kod olması için gerek ve yeter koşul $d(C) \geq 2t+1$ olmasıdır. Diğer bir ifadeyle, uzaklığı $d$ olan bir kod tam $\lfloor (d-1)/2 \rfloor$-hata düzelten koddur.

**Örnek 3.14** Yukarıdaki Örnek 3.12'de $C$ kodunun minimum uzaklığı 3 olduğu için, bir hata düzelttiği görülür.

### 3.2 Lineer Kodlar

Kodlama teorisinde büyük önemi ve yeri olan lineer kodlar, Tanım 2.36'da verdiğimiz vektör uzayları sayesinde tanımlanır. Lineer kodlar; teknolojiye uygulanabilirliği, üzerinde çalışmanın kolay olması ve sistematik yapıda olmaları sebebiyle oldukça önemlidir.

**Tanım 3.15** $\mathbb{F}_q$ üzerinde, $n$ uzunluklu bir $C$ *lineer kod*, $\mathbb{F}_q^n$ in bir alt uzayıdır.

**Not:** Bir kod için semboller sonlu sayıda olacağından lineer kodlar, sonlu cisimler üzerinde tanımlanmıştır.

**Örnek 3.16** Birkaç farklı lineer kod örneği verelim.

i. Bir $\mathbb{F}_q$ cismi üzerinde $\mathbb{F}_q^n = \{(\alpha,\ldots,\alpha) \mid \alpha \in \mathbb{F}_q\}$ (tekrarlı kod).

ii. $\mathbb{F}_2$ üzerinde $\{000,010,101,111\}$.

iii. $\mathbb{F}_2$ üzerinde $\{000000,010101,101010,111111\}$.

iv. $\mathbb{F}_3$ üzerinde $\{0000,0011,0022,2020,1010,2001,2012,1021,1002\}$.

**Tanım 3.17** $C$, $\mathbb{F}_q$ üzerinde $n$ uzunluğunda bir lineer kod olsun.

i. $C$'nin *dual kodu*, $\mathbb{F}_q^n$ vektör uzayında $C$'nin ortogonal tümleyeni (orthogonal complement) olarak tanımlanır ve $C^\perp$ ile gösterilir. Yani matematiksel ifadeyle, $C^\perp = \{x \in \mathbb{F}_q^n \mid \langle x,c\rangle = 0, \forall c \in C\}$.

ii. $C$ lineer kodunun boyutu, $\mathbb{F}_q$ üzerindeki alt uzay olarak boyutudur ve $\dim(C)$ ile gösterilir.

**Teorem 3.18** $C$, $\mathbb{F}_q$ üzerinde, $n$ uzunluğunda bir lineer kod olsun. Bu durumda;

i. $|C| = q^{\dim(C)}$.

ii. $C^\perp$ bir lineer koddur ve $\dim(C) + \dim(C^\perp) = n$.

iii. $(C^\perp)^\perp = C$.

**Not:** $\mathbb{F}_q$ üzerinde ve $n$ uzunluğunda bir $C$ lineer kodu genellikle $[n,k]_q$ kod ya da $q$-lu $[n,k]$ kod olarak, eğer bağlamdan $q$'nun ne olduğu belli ise $[n,k]$-kod olarak adlandırılır. Ayrıca, eğer $C$ kodunun minimum uzaklığı biliniyor ve bu uzaklık $d$ ise $[n,k,d]$-kod olarak adlandırılır.

**Tanım 3.19** $C$, $\mathbb{F}_q$ cismi üzerinde bir lineer kod olsun. Eğer $C \subseteq C^\perp$ ise $C$'ye *kendine dik kod*, eğer $C = C^\perp$ ise $C$'ye *kendine dual kod* denir.

**Tanım 3.20** $x \in \mathbb{F}_q^n$ bir söz (vektör) olsun. $x$'in (Hamming) ağırlığı, $x$'teki sıfırdan farklı koordinatların sayısı olarak tanımlanır ve $wt(x)$ ya da $w_H(x)$ olarak gösterilir. Yani

$w_H(x) = \left|\left\{ i \mid x_i \neq 0,\ x \in \mathbb{F}_q^n \right\}\right|$. Diğer bir ifadeyle $w_H(x) = d_H(x,0)$.

**Lemma 3.21** $x, y \in \mathbb{F}_q^n$ ise $d(x,y) = w(x-y)$ dir.

**Tanım 3.22** $C$ bir kod (lineer ya da lineer olmayan) olsun. $C$'nin (Hamming) ağırlığı, $C$'deki sıfırdan farklı kodsözlerin ağırlıklarının en küçüğü olarak tanımlanır ve $w(C)$ olarak gösterilir.

**Teorem 3.23** $C$, $\mathbb{F}_q$ üzerinde bir lineer kod olsun. Bu durumda $d(C) = w(C)$ dir.

**Not:** Lineer olmayan kodlar yerine, lineer kodların tercih edilme sebeplerinin bazıları şunlardır:

i. Lineer bir kod, vektör uzayı olduğu için, bir baz (taban) ile tamamen belirlenebilir.

ii. Lineer bir kodun uzaklığı, sıfırdan farklı kodsözlerin ağırlıklarının en küçüğüdür.

iii. Lineer kodların kodlama ve dekodlama işlemleri, lineer olmayan kodlara göre daha hızlı ve basittir.

**Tanım 3.24** $C$ bir $[n,k]_q$-kod olsun. Satırları $C$'nin bir bazından oluşan $G$ matrisine, $C$ lineer kodunun *üreteç matrisi* denir. Yani, $\{c_1, c_2, \ldots, c_k\}$ eğer $C$'nin bir bazı ise

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

matrisi, $[n,k]_q$-kod olan $C$'nin *üreteç matrisi*dir.

Üreteç matrisinin satırları, $C$ lineer kodunun (vektör uzayı) bazındaki vektörlerden oluştuğu için lineer bağımsızdırlar. Böylece $C$'nin kodsözleri, $G$ matrisinin satırlarının tüm olası lineer kombinasyonlarıdır.

**Tanım 3.25** $C$ bir $[n,k]_q$-lineer kod ve üreteç matrisi de $G=\left[I_k \middle| A\right]$ olsun. Bu şekilde sol tarafında $k\times k$ tipinde birim matris bulunan $G$ üreteç matrisi *standart formda*dır. Burada $A$ matrisi de $k\times(n-k)$ tipindedir.

**Tanım 3.26** Bir $C$ lineer kodunun (*parite) kontrol matrisi* $H$, $C^{\perp}$ dual kodun üreteç matrisidir. Bir lineer kodun dual kodu da lineer olduğu için ve kodsözleri lineer koddaki kodsözlere dik olduğu için $C=\{x\in\mathbb{F}_q^n \middle| Hx^T=0\}$ ile tanımlıdır.

**Örnek 3.27** Her ne kadar cisim üzerinde olmasa da, Hata Düzelten Kodlar bölümünün girişinde bahsettiğimiz gibi Türkiye Cumhuriyeti kimlik numaralarını belirleyen algoritmayı ve bunun üreteç matrisini verelim.

11 haneli T.C. kimlik numaralarının son iki hanesi kontrol amaçlı (parite) olup bilgi taşımaz ve bir algoritma ile ilk 9 hane kullanılarak elde edilir. Kimlik numarasıyla bir sisteme giriş yapıldığında, sistem kimlik numarasının ilk 9 hanesinden elde ettiği kontrol haneleri ile girilen kimlik numarsının son iki hanesini karşılaştırarak bir hata olup olmadığını kontrol eder.

T.C. kimlik numaralarının 10. hanesi; tek hanelerin yani 1., 3., 5., 7. ve 9. hanelerin toplamının 7 katı ile çift hanelerin yani 2., 4., 6. ve 8. hanelerin toplamının farklarının modülo 10'daki değeridir. T.C. kimlik numaralarının 11. hanesi ise ilk 10 hanenin toplamının modülo 10'daki değeridir. Bu algoritmayı sağlayan matris ise şöyledir:

$$G=\left[\begin{array}{c|cc} & 7 & 8\\ & 9 & 0\\ & 7 & 8\\ & 9 & 0\\ I_9 & 7 & 8\\ & 9 & 0\\ & 7 & 8\\ & 9 & 0\\ & 7 & 8 \end{array}\right]_{9\times 11}$$

Üreteç matrisine bakıldığında, kodlama işlemi sırasında ilk 9 hanenin değişmeyeceği açıktır. 10. hanenin de tek hanelerin 7 katı ile çift hanelerin 9 katının toplamının mod 10'daki değeri olduğunu görülür. Dikkat edilirse, $9\equiv -1(\mathrm{mod}\,10)$ denkliği bunun verilen

algoritma ile aynı olduğunu gösterir. 10. hane tek hanelerin 7'şer katlarıyla çift hanelerin -1'er katlarının toplamı olduğundan, ilk 10 hanenin toplamı aslında 9. haneye kadar tek hanelerin 8'er katlarının toplamının modülo 10'daki değeridir. Örneğin, Mustafa Kemal Atatürk'e tahsis edilen kodlanmamış 9 haneli kimlik numarası 100000001, kodlama işleminden sonra 10000000146 olarak son halini alır. Bu kodlama işlemi aşağıdaki matris çarpımı ile gerçekleşir:

$$[100000001]\cdot G=[100000001]\left[\begin{array}{c|c} & 7\ \ 8 \\ & 9\ \ 0 \\ & 7\ \ 8 \\ & 9\ \ 0 \\ I_9 & 7\ \ 8 \\ & 9\ \ 0 \\ & 7\ \ 8 \\ & 9\ \ 0 \\ & 7\ \ 8 \end{array}\right]_{9\times 11}=[10000000146]$$

**Örnek 3.28** Kitapların arkasında yer alan ve kitapları tanımlayan Uluslararası Standart Kitap Numarası (International Standard Book Number), kısaca ISBN kodu da günlük hayatta sıkça karşılaştığımız bir başka kodlama örneğidir. 2007 öncesi 10 haneden ve 2007 sonrası 13 haneden oluşan ISBN kodlarının algoritmaları şu şekildedir [30]:

ISBN-10 koda sahip bir kitabın $(x_1, x_2, \ldots, x_{10})$ şeklindeki numarasının 10. Hanesi şu eşitlikle belirlenir:

$$x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 + 8x_8 + 9x_9 + 10x_{10} \equiv 0 \pmod{11}$$

ISBN-13 koda sahip bir kitabın $(x_1, x_2, \ldots, x_{13})$ şeklindeki numarasının 13. Hanesi şu eşitlikle belirlenir:

$$x_1 + 3x_2 + x_3 + 3x_4 + x_5 + 3x_6 + x_7 + 3x_8 + x_9 + 3x_{10} + x_{11} + 3x_{12} + x_{13} \equiv 0 \pmod{10}$$

Bunlardan ISBN-10 kodun üreteç matrisi şu şekildedir:

$$G = \left[\begin{array}{c|c} & 1 \\ & 2 \\ & 3 \\ & 4 \\ I_9 & 5 \\ & 6 \\ & 7 \\ & 8 \\ & 9 \end{array}\right]_{9\times 10}.$$

**Teorem 3.29** $\mathbb{F}_q$ üzerindeki iki $(n, M)$-koddan biri diğerinden; kodsözlerinin sembollerine permütasyon uygulayarak ya da kodsözlerinin belirli bir pozisyondaki sembolü sıfırdan farklı bir skalerle çarparak elde ediliyorsa bu iki kod *denk*tir.

**Teorem 3.30** Her bir $C$ lineer kodu, üreteç matrisi standart formda olan bir $C'$ lineer koduna denktir.

### 3.3 Devirli Kodlar

İlk kez 1957 yılında Prange tarafından oraya atılan ve lineer kodların önemli bir sınıfı olan devirli (cyclic) kodlar, matematiksel yapılarının elektronik devre yapılarına doğal uyumunun bir sonucu olarak teknolojiye uygulanabilirliği sebebiyle haberleşme teorisi için hayati önemdedir.

**Tanım 3.31** $C \subseteq \mathbb{F}_q^n$ bir lineer kod olsun. Eğer $C$'nin kodsözlerinin devirsel olarak kaydırılmasıyla elde edilen vektörler de yine $C$'nin kodsözü oluyorsa, yani $c = (c_0, c_1, c_2, ..., c_{n-1}) \in C$ iken $c = (c_{n-1}, c_0, c_1, ..., c_{n-2}) \in C$ ise $C$'ye bir devirli kod denir.

**Not:** Devirli kodlar, cisimler üzerinde tanımlanmak zorunda olmayıp herhangi bir halka üzerinde de tanımlanabilir. Ancak henüz halkalar üzerindeki devirli kod tanımını vermediğimiz için şimdilik cisimler üzerindeki tanımını veriyoruz.

Geleneksel olarak, $\mathbb{F}_q$ cismi üzerindeki bir lineer kodun kodsözlerini, $\mathbb{F}_q[x]$ halkasındaki polinomlarla aşağıdaki gibi birebir olarak eşleriz

$$(c_0, c_1, \ldots, c_{n-1}) \leftrightarrow c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}.$$

Dikkat edilirse, kodsözlere uygulanacak olan kaydırma işlemi, polinomu $x$ ile çarpmaya denk gelir. Fakat bu kaydırma işlemi devirli olduğundan, $x^{n-1}$'in katsayısını sabitin yerine koymak için bu çarpma işlemi $x^n = 1$ denklik sınıfında yapılmalıdır. Bu da, bu polinomlarla $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ bölüm halkasında çalışmaya denk gelmektedir. Bu sayede kodların kombinatorik yapısını cebirsel bir yapıya çevirebilir ve sistematik bir biçimde işlem yapabiliriz. Bahsettiğimiz eşlemeyi matematiksel olarak bir dönüşümle aşağıdaki gibi ifade ederiz:

$$\varphi : C \to \mathbb{F}_q[x]/\langle x^n - 1\rangle,\ \varphi\left(c_0, c_1, \ldots, c_{n-1}\right) \mapsto c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \qquad (3.1)$$

**Teorem 3.32** $\varphi$, (2.1)'deki gibi tanımlanan bir lineer dönüşüm olsun. Bu durumda, $\mathbb{F}_q^n$'in boştan farklı bir $C$ alt kümesinin devirli kod olması için gerek ve yeter koşul $\varphi(C)$'nin, $\mathbb{F}_q[x]/\langle x^n - 1\rangle$'in bir ideali olmasıdır.

**İspat** [2] Kabul edelim ki $\varphi(C)$, $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ bölüm halkasının bir ideali olsun. Öyleyse, herhangi $\alpha, \beta \in \mathbb{F}_q \subset \mathbb{F}_q[x]/\langle x^n - 1\rangle$ için ve herhangi $a, b \in C$ için $\alpha\varphi(a), \beta\varphi(b) \in \varphi(C)$ dir. Kabul gereği, $\varphi(C)$ bir ideal olduğundan $\alpha\varphi(a) + \beta\varphi(b) \in \varphi(C)$ yani $\varphi(\alpha a + \beta b) \in \varphi(C)$ ve dolayısıyla da $\alpha a + \beta b$, $C$'nin bir kodsözüdür. Öyleyse $C$ bir lineer koddur.

Şimdi, $c = (c_0, c_1, \ldots, c_{n-1})$, $C$'nin bir kodsözü olsun. $\varphi(c) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ polinomu, $\varphi(C)$'nin bir elemanıdır. $\varphi(C)$ bir ideal olduğu için ve $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ halkasında $x^n - 1 = 0$ olduğu için

$$\begin{aligned} x\varphi(c) &= c_0 x + c_1 x^2 + \cdots + c_{n-2}x^{n-1} + c_{n-1}x^n \\ &= c_{n-1} + c_0 x + c_1 x^2 + \cdots + c_{n-2}x^{n-1} + c_{n-1}(x^n - 1) \\ &= c_{n-1} + c_0 x + c_1 x^2 + \cdots + c_{n-2}x^{n-1} \end{aligned}$$

polinomu da $\varphi(C)$'nin elemanıdır. Yani $(c_{n-1}, c_0, c_1, \ldots, c_{n-2})$, $C$'nin bir kodsözü ve dolayısıyla da $C$ bir devirli koddur.

Diğer taraftan, $C$'nin bir devirli kod olduğunu kabul edelim. Bu durumda, lineer kodun kapalılığı gereği, $\varphi(C)$'deki polinomların toplam ve farkları da $\varphi(C)$'nin elemanıdır. Ayrıca, $(f_0, f_1, \ldots, f_{n-1}) \in C$ kodsözü için yazılacak her

$$f(x) = f_0 + f_1 x + \cdots + f_{n-1}x^{n-1} = \varphi(f_0, f_1, \ldots, f_{n-1})$$

polinomu için,

$$xf(x) = f_{n-1} + f_0 x + f_1 x^2 + \cdots + f_{n-2}x^{n-1}$$

polinomu da, $C$ devirli olduğundan, $\varphi(C)$'nin elemanıdır. Benzer şekilde, $x^2 f(x) = x(xf(x))$ de yine $\varphi(C)$'nin elemanıdır. Tümevarımla, tüm $i \geq 0$ tam sayıları için, $x^i f(x)$ polinomunun $\varphi(C)$'de olduğunu görürüz. $C$ bir lineer kod olduğundan ve $\varphi$ de lineer dönüşüm olduğundan, $\varphi(C)$, $\mathbb{F}_q$ üzerinde bir lineer uzaydır. Öyleyse, herhangi bir $g(x) = g_0 + g_1 x + \cdots + g_{n-1}x^{n-1} \in \mathbb{F}_q[x]/\langle x^n - 1\rangle$ polinomu için

$$g(x)f(x) = \sum_{i=0}^{n-1} g_i (x^i f(x))$$

polinomu da $\varphi(C)$'dedir. Bu durumda, $\varphi(C)$, $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ bölüm halkasının bir idealidir.

**Örnek 3.33** Bir devirli kod ve buna karşılık gelen ideali, daha sonra da bir ideal ve karşılık gelen devirli kodu bulalım.

i. $C = \{0000, 1001, 1100, 0110, 0011, 0101, 1010, 1111\}$ kodu bir ikili (binary) devirli koddur. $\mathbb{F}_2[x]/\langle x^4 - 1\rangle$ halkasında buna karşılık gelen ideal ise $\varphi(C) = \{0, 1+x^3, 1+x, x+x^2, x^2+x^3, x+x^3, 1+x^2, 1+x+x^2+x^3\}$ dir.

ii. $I = \{0, 1+x+x^2+x^3, 2+2x+2x^2+2x^3\}$ kümesi $\mathbb{F}_3[x]/\langle x^4 - 1\rangle$ bölüm halkasının bir idealidir ve bu ideale karşılık gelen devirli kod $\varphi^{-1}(I) = \{0000, 1111, 2222\}$ olarak bulunur.

**Teorem 3.34** $I$, $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ bölüm halkasının sıfırdan farklı bir ideali ve $g(x)$, $I$'da sıfırdan farklı, en küçük dereceli monik (baş katsayısı 1) polinom olsun. Bu durumda $g(x)$ polinomu $I$'nın bir üretecidir ve $x^n - 1$'i böler.

**Örnek 3.35** Örnek 3.33'ün (i) şıkkında, $1+x$ polinomu en küçük dereceli monik polinomdur ve $\mathbb{F}_2$ üzerinde $x^4-1$'i böler; (ii) şıkkında $1+x+x^2+x^3$ polinomu en küçük dereceli monik polinomdur ve $\mathbb{F}_3$ üzerinde $x^4-1$'i böler.

**Not:** $\mathbb{F}_q[x]/\langle x^n-1\rangle$ esas ideal bölgesidir, yani her ideali bir eleman tarafından üretilir. O halde devirli bir $C$ kodu, $\varphi(C)$'nin üreteçlerinden herhangi biriyle belirlenebilir.

**Teorem 3.36** $\mathbb{F}_q[x]/\langle x^n-1\rangle$ bölüm halkasının sıfırdan farklı bir $I$ idealinin, en küçük dereceli tek bir monik polinomu vardır.

**Tanım 3.37** Teorem 3.34'de verilen $g(x)$ polinomuna $I$ idealinin ve $C$ devirli kodunun üreteç polinomu denir ve $C=\langle g(x)\rangle$ şeklinde gösterilir.

**Teorem 3.38** $g(x)$ polinomu $\mathbb{F}_q[x]/\langle x^n-1\rangle$ bölüm halkasının bir $I$ idealinin üreteci olsun. Bu durumda, eğer $g(x)$'in derecesi $n-k$ ise karşılık gelen $C$ kodunun boyutu $k$'dir.

**Tanım 3.39** $g(x)=g_0+g_1x+\cdots+g_{n-k}x^{n-k}$ polinomu, $\mathbb{F}_q^n$'deki bir $C$ devirli kodunun, derecesi $n-k$ olan üreteç polinomu olsun. Bu durumda

$$\begin{pmatrix} g(x) \\ xg(x) \\ . \\ . \\ . \\ x^{k-1}g(x) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & . & . & g_{n-k} & 0 & 0 & 0 & . & . & 0 \\ 0 & g_0 & g_1 & . & . & g_{n-k} & 0 & 0 & . & . & 0 \\ . & & & & & & & & & & . \\ . & & & & & & & & & & . \\ . & & & & & & & & & & . \\ 0 & 0 & . & . & g_0 & g_1 & . & . & . & . & g_{n-k} \end{pmatrix}$$

matrisi $C$ devirli kodunun bir üreteç matrisidir ve genellikle $G$ ile gösterilir.

**Tanım 3.40** $h(x)=\sum_{i=0}^{k}a_ix^i$, $\mathbb{F}_q$ üzerinde derecesi $k$ olan ($a_k\neq 0$) bir polinom olsun. Bu durumda $h(x)$'in *ters (reciprocal) polinomu* $h_R(x)$ aşağıdaki gibi tanımlanır

$$h_R(x)=x^k h(1/x)=\sum_{i=0}^{k}a_{k-i}x^i .$$

**Teorem 3.41** $g(x)$ polinomu, $\mathbb{F}_q$ üzerindeki bir $[n,k]$-devirli kodun üreteç polinomu ve $h(x)=(x^n-1)/g(x)$ olsun. Bu durumda $h_0$, $h(x)$ polinomunun sabit terimi olmak üzere, $h_0^{-1}h_R(x)$ polinomu $C^{\perp}$ dual kodun üreteç polinomudur.

## 3.4 $\mathbb{Z}_4$ Kodlar

**Tanım 3.42** $\mathbb{Z}_4=\{0,1,2,3\}$ modülo $4$ tam sayılar halkası ve $n$ bir pozitif tam sayı olmak üzere $\mathbb{Z}_4^n$, $\mathbb{Z}_4$ üzerinde $n$'lilerin kümesi yani $\mathbb{Z}_4^n=\{(x_1,x_2,\ldots,x_n)\mid x_i\in\mathbb{Z}_4\}$ olsun. $\mathbb{Z}_4^n$'in sıfırdan farklı herhangi bir $C$ alt kümesine *dörtlü kod (quaternary code)* ya da $\mathbb{Z}_4$-kod denir. Cisimler üzerindeki kodlarda olduğu gibi yine $\mathbb{Z}_4^n$ kümesindeki *söz*, $\mathbb{Z}_4$-kod olan $C$'nin elemanlarına *kodsöz* diyeceğiz.

Her $(x_1,x_2,\ldots,x_n)\in\mathbb{Z}_4^n$ ve $(y_1,y_2,\ldots,y_n)\in\mathbb{Z}_4^n$ için aşağıdaki gibi bileşen bileşene toplama işlemi tanımlanarak $\mathbb{Z}_4^n$, mertebesi $4^n$ olan bir değişmeli grup haline gelir.

$\mathbb{Z}_4^n$'in herhangi bir alt grubuna da $\mathbb{Z}_4$-*lineer kod* denir.

Her $(x_1,x_2,\ldots,x_n)\in\mathbb{Z}_4^n$ ve $(y_1,y_2,\ldots,y_n)\in\mathbb{Z}_4^n$ için aşağıdaki gibi bir *iç çarpım* tanımlanır

$x\cdot y=x_1y_1+\cdots+x_ny_n$.

Eğer $x\cdot y=0$ ise $x$ ve $y$ *ortogonal (orthogonal)* ya da *dik*tir denir.

$C$ bir $\mathbb{Z}_4$-lineer kod ve uzunluğu $n$ olsun. $C$'nin dual kodu şu şekilde tanımlanır:

$C^{\perp}=\{x\in\mathbb{Z}_4^n\mid \text{her } y\in C \text{ için } x\cdot y=0\}$.

Cisim üzerindeki kodlarda olduğu gibi $C^{\perp}$'in, $\mathbb{Z}_4^n$'ün bir alt grubu olduğu ve dolayısıyla da lineer kod olduğu kolayca gösterilebilir. $\mathbb{Z}_4$-kodlarda; kodların denkliği, kendine dual kod ve kendine dik kod tanımları cisim üzerindeki kodlar gibidir.

**Not:** Grup teoriden, $p$ asal ve $m>0$ olmak üzere mertebesi $p^m$ olan bir değişmeli grubun; mertebesi $p^{e_1}$ olan $m_1$ tane devirli grubun, mertebesi $p^{e_2}$ olan $m_2$ tane devirli grubun,..., mertebesi $p^{e_r}$ olan $m_r$ tane devirli grubun, burada $m_1,e_1,m_2,e_2,\ldots,m_r,e_r$ pozitif tam sayılar ve $e_1>\cdots>e_r$, direkt toplamı olarak tek türlü yazılabildiğini

biliyoruz. Böyle bir durumda gruba $(p^{e_1})^{m_1}(p^{e_2})^{m_2}\cdots(p^{e_r})^{m_r}$ tipinde denir. Elbette burada $m_1e_1+m_2e_2+\cdots+m_re_r$ dir. Ayrıca, yalnız birim elemandan oluşan gruba da $p^0$ tipinde denir. Bu sayede bir $\mathbb{Z}_4$-kodun tipini belirleyebiliriz. $\mathbb{Z}_4$'ün alt grupları; $\mathbb{Z}_4$, $\{0,2\}$ ve $\{0\}$ olduğu için herhangi bir $\mathbb{Z}_4$-kodun tipi $(2^2)^m$, $(2^2)^{m_1}2^{m_2}$, $2^m$ ya da $2^0$'dır. Kolaylık olması açısından $(2^2)^m$ yerine $4^m$ ve $(2^2)^{m_1}2^{m_2}$ yerine de $4^{m_1}2^{m_2}$ yazacağız [29].

**Teorem 3.43** Sıfırdan farklı herhangi bir $\mathbb{Z}_4$-lineer $C$ kodu, üreteç matrisi

$$\begin{pmatrix} I_{k_1} & A & B \\ 0 & 2I_{k_2} & 2D \end{pmatrix}$$

olan bir $\mathbb{Z}_4$-lineer koda permütasyon denktir. Burada $A$ ve $D$ matrislerinin elemanları $\{0,1\}$'lerden ve $B$ matrisinin elemanları $\mathbb{Z}_4=\{0,1,2,3\}$'lerden oluşmaktadır. Bu durumda $C$, tipi $4^{k_1}2^{k_2}$ olan bir değişmeli gruptur ve $2^{2k_1+k_2}$ kodsöze sahiptir. Ayrıca $k_1$ tam sayısına $C$ kodunun serbest kısmının boyutu ve $k_2$ tam sayısına da $C$ kodunun serbest olmayan kısmının boyutu denir.

### 3.5 Hensel Lemması ve Hensel Yükseltmesi (Lift)

$\mathbb{F}$ bir cisim olmak üzere, $\mathbb{F}[x]$ esas ideal bölgesi olduğundan $\mathbb{F}[x]/\langle x^n-1\rangle$'in her bir idealini üreten bir polinom vardır ve yine $\mathbb{F}[x]$ Öklid Bölgesi olduğundan bu üreteç polinom Euclid'in bölme algoritması ile bulunabilir. Bu yüzden cisim üzerindeki devirli kodlar sistemli bir şekilde belirlenebilir. Fakat $\mathbb{Z}_4$-kodlar gibi halka üzerindeki kodlar çalışılırken, $\mathbb{Z}_4[x]$ polinom halkası ne Öklid bölgesi ne de esas ideal bölgesi olduğundan bu şekilde bir yöntem mümkün değildir. Bu yüzden $\mathbb{Z}_4[x]/\langle x^n-1\rangle$ polinom halkasını, Çin Kalan Teoremi yardımıyla ayrıştırıp, her bir parçanın ideallerini belirleyip daha sonra bunların direkt toplamlarını elde etmek iyi bir fikirdir. Burada da yine $\mathbb{Z}_4[x]$ tek türlü çarpanlarına ayrılabilen bölge olmadığı için $x^n-1$'in çarpanlarına tek türlü ayrılamaması problemi vardır. Fakat bu problemi, cisimler üzerindeki indirgenemez polinom kavramının halkalar için temel indirgenemez polinom karşılığı tanımlanarak ve çarpanlara ayrılmanın bu temel indirgenemez polinomlar için tek türlü olması

belirlenmesi ile aşabiliriz. Bu yüzden Hensel'in lemması bu problemi çözmede oldukça önemli bir rol oynamaktadır.

Önce aşağıdaki homomorfizmayı tanımlayalım

$$\begin{aligned}\alpha &: \mathbb{Z}_4 \to \mathbb{Z}_2 \\ &0,2 \mapsto 0 \\ &1,3 \mapsto 1\end{aligned}$$

Kolaylık açısından $\alpha(0)=\alpha(2)=0$ ve $\alpha(1)=\alpha(3)=1$ yerine $\bar{0}=\bar{2}=0$ ve $\bar{1}=\bar{3}=1$ notasyonunu kullanalım. $\alpha$ homomorfizmasını basit ve doğal bir şekilde polinom halkaları arasındaki bir homomorfizmaya aşağıdaki gibi genişletebiliriz

$$\begin{aligned}\mathbb{Z}_4[x] &\to \mathbb{Z}_2[x] \\ a_0 + a_1x + \cdots + a_nx^n &\mapsto \bar{a}_0 + \bar{a}_1x + \cdots + \bar{a}_nx^n\end{aligned}.$$

Bu halka homomorfizmasının çekirdeğinin $\langle 2\rangle = \mathbb{Z}_4[x]2 = \{2f(x) \mid f(x) \in \mathbb{Z}_4[x]\}$ olduğunu görmek zor değildir. Bu fonksiyonu da "$-$" ile gösterelim ve $f(x) \in \mathbb{Z}_4[x]$ polinomunun "$-$" altındaki görüntüsünü $\overline{f}(x)$ ile gösterelim.

**Tanım 3.44** $\mathbb{Z}_4[x]$ üzerindeki $f_1(x)$ ve $f_2(x)$ için, eğer $\mathbb{Z}_4[x]$ halkasında

$$\lambda_1(x)f_1(x) + \lambda_2(x)f_2(x) = 1$$

olacak şekilde $\lambda_1(x)$ ve $\lambda_2(x)$ polinomları varsa, $f_1(x)$ ve $f_2(x)$ polinomları $\mathbb{Z}_4[x]$'te *aralarında asal*dır denir.

Şimdi, $\mathbb{Z}_4$ devirli kodlar için gerekli olan ve bizim de sonraki bölümde $\mathbb{Z}_q + u\mathbb{Z}_q$ halkası üzerindeki devirli kodları belirlerken bu halka üzerine taşıyacağımız bir dizi lemma ve teoremi [29] aşağıda veriyoruz. İspatlar için okuyucu [29]'a başvurabilir.

**Lemma 3.45** $f_1(x)$ ve $f_2(x) \in \mathbb{Z}_4[x]$ polinomlarının aralarında asal olması için gerek ve yeter koşul, $\overline{f}_1(x)$ ve $\overline{f}_2(x)$ polinomlarının $\mathbb{Z}_2[x]$'te aralarında asal olmasıdır.

**Lemma 3.46** $f(x) \in \mathbb{Z}_4[x]$ monik polinom ve $\overline{f}_1(x)$ ve $\overline{f}_2(x)$ polinomları $\mathbb{Z}_2[x]$'te aralarında asal olmak üzere $\overline{f}(x) = \overline{f}_1(x)\overline{f}_2(x)$ olsun. Bu durumda aşağıdaki özellikleri sağlayan $g_1(x), g_2(x) \in \mathbb{Z}_4[x]$ monik polinomları vardır:

i. $f(x) = g_1(x)g_2(x)$

ii. $\overline{g_1}(x) = \overline{f}_1(x)$, $\overline{g_2}(x) = \overline{f}_2(x)$

iii. $\text{der}\, g_1(x) = \text{der}\, \overline{f}_1(x)$, $\text{der}\, g_2(x) = \text{der}\, \overline{f}_2(x)$

iv. $g_1(x)$ ve $g_2(x)$ polinomları $\mathbb{Z}_4[x]$'te aralarında asaldır.

Yukarıda verilen Lemma 3.46 tümevarımla aşağıdaki gibi genellenebilir.

**Lemma 3.47** $f(x) \in \mathbb{Z}_4[x]$ monik polinom ve $\overline{f}_1(x), \overline{f}_2(x), \ldots, \overline{f}_r(x)$ polinomları $\mathbb{Z}_2[x]$'te ikili olarak aralarında asal olmak üzere $\overline{f}(x) = \overline{f}_1(x)\overline{f}_2(x)\cdots\overline{f}_r(x)$ olsun. Bu durumda aşağıdakileri özellikleri sağlayan $g_1(x), g_2(x), \ldots, g_r(x) \in \mathbb{Z}_4[x]$ monik polinomları vardır:

i. $f(x) = g_1(x)g_2(x)\cdots g_r(x)$

ii. $\overline{g_i}(x) = \overline{f}_i(x)$, $i = 1, 2, \ldots, r$

iii. $\text{der}\, g_i(x) = \text{der}\, \overline{f}_i(x)$, $i = 1, 2, \ldots, r$

iv. $g_1(x), g_2(x), \ldots, g_r(x)$ polinomları $\mathbb{Z}_4[x]$'te ikili olarak aralarında asaldır.

**Tanım 3.48** $f(x) \in \mathbb{Z}_4[x]$ derecesi $m \geq 1$ olan monik polinom olsun. Eğer $\overline{f}(x)$ polinomu $\mathbb{Z}_2$ üzerinde indirgenemez ise $f(x)$ polinomuna $\mathbb{Z}_4$ üzerinde $m.$ dereceden *temel indirgenemez polinom* denir. Eğer $\overline{f}(x)$ polinomu $\mathbb{Z}_2$ üzerinde ilkel ise $f(x)$ polinomuna $\mathbb{Z}_4$ üzerinde $m.$ dereceden *temel ilkel polinom* denir.

**Lemma 3.49** $f(x) \in \mathbb{Z}_4[x]$ ve $g(x) \in \mathbb{Z}_2[x]$ indirgenemez polinom, $e$ pozitif bir tam sayı olmak üzere $\overline{f}(x) = g(x)^e$ olsun. Bu durumda $f(x)$ polinomu $\mathbb{Z}_4[x]$'te asalımsıdır.

**Teorem 3.50** $f(x) \in \mathbb{Z}_4[x]$ derecesi $1$'den büyük olan monik polinom olsun. Öyleyse

i. $f(x) = g_1(x)g_2(x)\cdots g_r(x)$; $g_1(x), g_2(x), \ldots, g_r(x)$ polinomları ikili olarak aralarında asal monik asalımsı

ii. $f(x)$'in ikili aralarında asal monik asalımsı polinomlara ayrılışları $f(x) = g_1(x)g_2(x)\cdots g_r(x) = h_1(x)h_2(x)\cdots h_r(x)$ olsun. Bu durumda $r = s$ ve sıralandıktan sonra $i = 1, 2, \ldots, r$ için $g_i(x) = h_i(x)$ dir.

**Önerme 3.51** $n$ bir pozitif tek tam sayı olsun. Bu durumda $x^n - 1$ polinomu, $\mathbb{Z}_4$ üzerinde ikili olarak aralarında asal temel indirgenemez polinomların çarpımı olarak

$$x^n - 1 = g_1(x)g_2(x)\cdots g_r(x)$$

şeklinde yazılır ve bu çarpım tek türlüdür.

**Önerme 3.52** $n$ bir pozitif tek tam sayı ve $f_2(x) \in \mathbb{Z}_2[x]$ polinomu $x^n - 1$'in böleni olsun. Bu durumda $x^n - 1$ polinomunu $\mathbb{Z}_4[x]$'te bölen $\overline{f}(x) = f_2(x)$ olacak şekilde tek bir $f(x) \in \mathbb{Z}_4[x]$ polinomu vardır.

**Önerme 3.53** $n_1$ ve $n_2$ birer pozitif tek tam sayı ve $f_2(x) \in \mathbb{Z}_2[x]$ polinomu hem $x^{n_1} - 1$'in hem de $x^{n_2} - 1$'in böleni olsun. $\mathbb{Z}_4[x]$'teki monik $f^{(1)}(x)$ ve $f^{(2)}(x)$ polinomları da sırasıyla $x^{n_1} - 1$'i ve $x^{n_2} - 1$'i bölsün ve de $\overline{f}^{(1)}(x) = \overline{f}^{(2)}(x) = f_2(x)$ olsun. Bu durumda $f^{(1)}(x) = f^{(2)}(x)$.

**Sonuç 3.54** $n$ bir pozitif tek tam sayı ve $f_2(x) \in \mathbb{Z}_2[x]$ polinomu indirgenemez ve de $x^n - 1$'in böleni olsun. Bu durumda $\overline{f}(x) = f_2(x)$ olacak şekilde $x^n - 1$'i bölen bir tek temel indirgenemez $f(x) \in \mathbb{Z}_4[x]$ polinomu vardır. Üstelik $f(x)$, $n$'den bağımsızdır.

# BÖLÜM 4

## $\mathbb{Z}_q + u\mathbb{Z}_q$ DEVİRLİ KODLAR

Yıldız ve Aydın, $u^2 = 0$ olmak üzere $\mathbb{Z}_4 + u\mathbb{Z}_4$ halkası üzerindeki devirli kodları inceledikleri 2014 yılındaki çalışmalarında [23], elde ettikleri kodların $\mathbb{Z}_4$ üzerine görüntülerini alarak birçok yeni $\mathbb{Z}_4$-lineer kod elde ettiler. Bu çalışma [24]'te Gao ve arkadaşları tarafından $\mathbb{Z}_q + u\mathbb{Z}_q$ halkası üzerine genelleştirilmeye çalışılsa da, bu halka üzerindeki devirli kodların $(\mathbb{Z}_q + u\mathbb{Z}_q)[x]/ < x^n - 1 >$ bölüm halkasının bir ideali olmasına karşın, bu idealler şimdiye kadar belirlenememiştir. Bu amaca ulaşmak için öncelikle $p$ bir asal sayı ve $s$ pozitif bir tam sayı iken $q = p^s$ olmak üzere $\mathbb{Z}_q + u\mathbb{Z}_q$ halkasının ideal yapısını ve bu ideallerin sayısını belirliyoruz.

### 4.1 $\mathbb{Z}_q + u\mathbb{Z}_q$ Halkası

$p$ bir asal sayı ve $s$ bir pozitif tam sayı olmak üzere $q = p^s$ olsun. $u^2 = 0$ olmak üzere

$$\mathcal{R} = \mathbb{Z}_q + u\mathbb{Z}_q = \{a + bu \mid a, b \in \mathbb{Z}_q\}$$

halkası, $u$ değişkeniyle $\mathbb{Z}_q[u]/\langle u^2 \rangle$ bölüm halkasına izomorftur. Değişmeli bir halka olup karakteristiği $q$'dur. Bu halkadaki birimsel elemanlar $a \in \mathbb{Z}_q$ birimsel olmak üzere tüm $a + bu$ formundaki elemanlardır. Çünkü burada $u$, dolayısıyla da $bu$ nilpotent elemandır ve birimsel bir elemanla nilpotent elemanın toplamı yine birimseldir [31].

**Hatırlatma:** Bir $R$ halkasında birimsel $v$ ve herhangi bir $a \in R$ için $\langle v \rangle = R$, $\langle va \rangle = \langle a \rangle$ gerçeğini $\mathcal{R}$'nin ideallerini belirlediğimiz teoremin ispatında sıkça kullanacağız.

## 4.2 $\mathbb{Z}_q + u\mathbb{Z}_q$ Halkasının İdealleri

Aşağıdaki teorem ile $\mathbb{Z}_q + u\mathbb{Z}_q$ halkasının tüm ideallerini belirliyoruz.

**Teorem 4.1** $\mathbb{Z}_q + u\mathbb{Z}_q$ halkasının tüm idealleri aşağıdaki gibidir:

1. $\langle p^i \rangle$ ; $0 \le i \le s$

2. $\langle p^j u \rangle$ ; $0 \le j < s$

3. $\langle vp^i + p^j u \rangle$ ; $0 \le j < i < s$, $(p,v) = 1$ ve $1 \le v < p^{\min(i-j,s-i)}$

4. $\langle p^i, p^j u \rangle$ ; $0 \le j < i < s$

5. $\langle vp^i + p^j u, p^k \rangle$; $0 \le j < i < s$, $(p,v) = 1$, $1 \le v < p^{\min(i-j,s-i)-1}$ ve de $\lfloor \log_p v \rfloor + i < k < \min(i-j, s-i) + i$

**İspat** Önce bu halkanın esas idealleri belirleyelim. $\mathbb{Z}_q$ halkasında $v' = p^s - 1$ birimsel elemanı için

$$(a + (a+b)u)(1 + v'u) = a + bu$$

olacağı için $0 \le b \le a - 1$ iken $\langle a + (a+b)u \rangle = \langle a + bu \rangle$ eşitliğine dikkat edelim. O halde, $\langle a + bu \rangle$ ideallerini $a = 0$ ya da $0 \le b < a$ için araştırmamız yeterli olacaktır.

**I. Durum:** $a$, $\mathbb{Z}_q$ halkasında birimsel eleman olsun. Bu durumda $a + bu$ birimsel olduğu için $\langle a + bu \rangle = \mathbb{Z}_q + u\mathbb{Z}_q$ eşitliği açıktır.

**II. Durum:** $a = 0$ olsun. Eğer $b = 0$ ise aşikâr sıfır idealini elde ederiz. Eğer $b \neq 0$ ise $0 \le k \le s - 1$ tam sayı ve $v \in \mathbb{Z}_q$ birimsel olmak üzere $b = vp^k$ formundadır. Bu durumda $\langle a + bu \rangle = \langle vp^k u \rangle = \langle p^k u \rangle$ olur.

**III. Durum:** $k > 0$ bir tam sayı ve $v$, $\mathbb{Z}_q$ halkasında birimsel olmak üzere $a = vp^k$ olsun. Eğer $b = 0$ ise $\langle a + bu \rangle = \langle vp^k \rangle = \langle p^k \rangle$ olacağı açıktır. Eğer $v' \in \mathbb{Z}_q$ birimseli ve $0 \le l \le s - 1$ tam sayısı için $b = v' p^l$ formunda ise, $w \in \mathbb{Z}_q$, $v'$'nün çarpımsal tersi olmak üzere $w(a + bu) = wvp^k + p^l u$ olduğundan $\langle a + bu \rangle = \langle vwp^k + p^l u \rangle$ olur.

Böylece herhangi bir esas idealin; 1., 2. ya da 3. formda olacağı görülür.

3. tipteki tüm idealleri belirlemek için $v$'nin hangi değerleri için farklı ideal elde edileceğini de belirlememiz gerekir. $\overline{v} \in \mathbb{Z}_q$ birimseli için $v = p^{s-i} + \overline{v}$ iken $\langle vp^i + p^j u \rangle = \langle \overline{v}p^i + p^j u \rangle$ olduğu açıktır. $v = p^{i-j} + 1$ olduğunda $x = (p^{i-j} + 1)^{-1}$ ve $y = x^2$ olarak seçtiğimizde

$$
\begin{aligned}
&((p^{i-j}+1)p^i + p^j u)(x + yu) \\
&= ((p^{i-j}+1)p^i + p^j u)((p^{i-j}+1)^{-1} + (p^{i-j}+1)^{-2}u) \\
&= p^i + p^i(p^{i-j}+1)^{-1}u + p^j(p^{i-j}+1)^{-1}u \\
&= p^i + (p^{i-j}+1)^{-1}(p^i + p^j)u \\
&= p^i + (p^{i-j}+1)^{-1}p^j(p^{i-j}+1)u \\
&= p^i + p^j u
\end{aligned}
$$

eşitliğini elde ederiz ki $\langle vp^i + p^j u \rangle = \langle p^i + p^j u \rangle$ olduğunu görürüz. Bundan sonraki $v$ değerleri için döngüsel olarak daha önceki idealler üretilecektir. $v = p^{i-j} + \overline{v}$ iken $\langle vp^i + p^j u \rangle = \langle (p^{i-j} + \overline{v})p^i + p^j u \rangle = \langle p^{2i-j} + \overline{v}p^i + p^j u \rangle$ eşitliğini elde ederiz. Ancak $(\overline{v}p^i + p^j u)(\overline{v}^{-1}p^{i-j} - \overline{v}^{-2}u) = p^{2i-j}$ olduğundan $p^{2i-j} \in \langle \overline{v}p^i + p^j u \rangle$ olur ve dolayısıyla da $\langle p^{2i-j} + \overline{v}p^i + p^j u \rangle = \langle vp^i + p^j u \rangle = \langle \overline{v}p^i + p^j u \rangle$ ideallerin eşitliği elde edilir. Üstelik $(p^i + p^j u)(x + yu) = vp^i + p^j u$ eşitliğinin yalnızca $v > p^{\min(i-j, s-i)}$ iken çözümü vardır. Çünkü $p^i x = vp^i$ ise $k_1 \geq 0$ tam sayısı için $x = p^{s-i}k_1 + v$ ve $p^i y + p^j x = p^j$ ise $k_2 \geq 0$ tam sayısı için $x + p^{i-j}y = p^{s-j}k_2 + 1$ eşitliklerini elde ederiz. $x$'i yerine koyduğumuzda ise $v = k_2 p^{s-j} - yp^{i-j} - k_1 p^{s-i} + 1$ eşitliğini elde ederiz. Burada $s - i \leq i - j$ iken $v = p^{s-i}[-k_1 + k_2 p^{i-j} - yp^{2i-j-s}] + 1$ formunda olmak zorundadır ve $i - j < s - i$ iken de $v = p^{i-j}[-k_1 p^{s-2i+j} + k_2 p^{s-i} - y] + 1$ formunda olmak zorundadır. Buradan sonuç olarak her bir $v < p^{\min(i-j, s-i)}$ için $\langle vp^i + p^j u \rangle$ ideali diğerinden farklıdır.

Şimdi esas olmayan, iki eleman tarafından üretilen idealleri, 1., 2. ve 3. tip esas ideal üreteçlerinin kombinasyonları olarak elde edebiliriz.

1. ile 2.'nin kombinasyonundan, $j < i$ ise açıkça 4. tipteki ideali, $i \leq j$ ise $\langle p^i \rangle \supset \langle p^j u \rangle$ olacağı için 1. tipteki ideali elde ederiz.

1. ile 3.'nün kombinasyonundan, eğer $vp^i + p^j u \in \langle p^k \rangle$ ise $\langle vp^i + p^j u \rangle \subset \langle p^k \rangle$ olacağı için 1. tip ideal, eğer $p^k \in \langle vp^i + p^j u \rangle$ ise $\langle vp^i + p^j u \rangle \supset \langle p^k \rangle$ olacağı için 3. tip ideal aksi halde 5. tip ideal elde ederiz. $vp^i + p^j u \notin \langle p^k \rangle$ olması için $\lfloor \log_p v \rfloor + i < k$ şartının gerekliliği açıktır. Diğer taraftan, $p^k \in \langle vp^i + p^j u \rangle$ olabilmesi için $(vp^i + p^j u)(x + yu) = p^k$ eşitliğini sağlayan $x, y \in \mathbb{Z}_q$ elemanlarının bulunabilmesi gerekir. Ne var ki bu durumda $xvp^i = p^k$ ve $yvp^i + xp^j = 0$ dolayısıyla da $x = -yvp^{i-j}$ olacağından $p^k = -v^2 y p^{2i-j}$ formunda olmalıdır ve bu da ancak $2i - j \le k$ iken mümkündür. Öyleyse $\lfloor \log_p v \rfloor + i < k < \min(i - j, s - i) + i$ şartı sağlanmalıdır. Son olarak, $p^{\min(i-j,s-i)-1} \le v$ iken, $(p^{\min(i-j,s-i)-1}) p^i = p^{\min(2i-j,s)-1}$ olacağından yani $p^k$'nın alabileceği en büyük değere eşit olduğundan, 5. tipteki ideal için geçerli bir $k$ tam sayısının olamayacağını belirtelim. O halde 5. tip idealler için $1 \le v < p^{\min(i-j,s-i)-1}$ olmalıdır.

2. ile 3.'nün kombinasyonları için $\langle p^k u \rangle$ ile $\langle vp^i + p^j u \rangle$ ideallerini ele alalım. $k \le j$ ise $\langle vp^i + p^j u, p^k u \rangle = \langle p^i, p^k u \rangle$ olacağından 4. tip ideal, $i \le k$ ise $p^k u \in \langle vp^i + p^j u \rangle$ ve $\langle vp^i + p^j u, p^k u \rangle = \langle vp^i + p^j u \rangle$ olacağından 3. tip ideal elde edilir. $j < k < i$ olduğunda ise $[(vp^i + p^j u)p^{k-j} - p^k u]v^{-1} = p^{k-j+i}$ ve $(vp^i + p^j u)p^{k-j} - vp^{k-j+i} = p^k u$ olacağından $\langle vp^i + p^j u, p^k u \rangle = \langle vp^i + p^j u, p^{k-i+j} \rangle$ eşitliğinin gösterdiği gibi 5. tip ideal elde edilir.

**Teorem 4.2** $p$ bir asal sayı ve $s$ pozitif bir tam sayı olsun. $u^2 = 0$ olmak üzere $\mathbb{Z}_{p^s} + u\mathbb{Z}_{p^s}$ halkasının tüm ideallerinin sayısı $K_{p,s}$ aşağıdaki formül ile belirlenebilir:

$$K_{p,s} = \sum_{i=0}^{s} (i+1) p^{\lfloor (s-i)/2 \rfloor}.$$

Bu sayı aynı zamanda $K_{p,0} = 1$ ve $K_{p,1} = 3$ olmak üzere aşağıdaki yinelemeli bağıntı (recurrence relation) ile bulunabilir:

$$K_{p,s} = pK_{p,s-2} + 2s + 1.$$

**İspat** 1., 2. ve 4. tip ideallerin sayılarının sırayla $s+1$, $s$ ve $C(s,2)$ olduğu farklı $i$ ve $j$'leri sayarak kolayca görülür.

3. tip ideallerin sayısını belirlerken dikkat edelim ki, farklı idealler elde etmek için $v$ birimseli $\phi(p^{\min(i-j,s-i)})$ tane farklı değer alabilir. O halde $i-j$ ve $s-i$'nin birbirlerini $s-j$'ye tamamladıklarını göz önünde bulundurursak, herhangi bir $0 \le j \le s-2$ için, $s-j$ çift olduğunda

$$\phi(p)+\phi(p^2)+\cdots+\phi(p^{((s-j)/2)-1})+\phi(p^{(s-j)/2})+\phi(p^{((s-j)/2)-1})+\cdots+\phi(p^2)+\phi(p)$$

ideal vardır ve $s-j$ tek olduğunda

$$\phi(p)+\phi(p^2)+\cdots+\phi(p^{\lfloor (s-j)/2 \rfloor})+\phi(p^{\lfloor (s-j)/2 \rfloor})+\cdots+\phi(p^2)+\phi(p)$$

ideal vardır. Öyleyse bütün 3. tip ideallerin sayısı

$$\sum_{i=0}^{s-2}(i+1)\phi(p^{\lfloor (s-i)/2 \rfloor})=(p-1)\sum_{i=0}^{s-2}(i+1)p^{\lfloor (s-2-i)/2 \rfloor} \tag{4.1}$$

olur. Aynı metotla 5. tip ideallerin sayısını da belirleyebiliriz. Sabit birer $i$ ve $j$ için; $k=i+\min(i-j,s-i)-1$ olduğunda $\phi(p^{\min(i-j,s-i)-1})$ tane 5. tip ideal, $k=i+\min(i-j,s-i)-2$ olduğunda $\phi(p^{\min(i-j,s-i)-2})$ tane 5. tip ideal,..., $k=i+\min(i-j,s-i)-(\min(i-j,s-i)-1)=i+1$ olduğunda da $\phi(p^{\min(i-j,s-i)-(\min(i-j,s-i)-1)})=\phi(p)$ tane 5. tip ideal vardır. Öyleyse $1 \le v < p^{\min(i-j,s-i)-1}$ olduğunu göz önünde bulundurarak, her bir $0 \le j \le s-4$ için $s-j$ çift iken

$$\begin{aligned}
&\phi(p)+\phi(p^2)+\cdots+\phi(p^{((s-j)/2)-2})+\phi(p^{((s-j)/2)-1})+\phi(p^{((s-j)/2)-2})+\cdots+\phi(p^2)+\phi(p)\\
&+\phi(p)+\phi(p^2)+\cdots+\phi(p^{((s-j)/2)-3})+\phi(p^{((s-j)/2)-2})+\phi(p^{((s-j)/2)-3})+\cdots+\phi(p^2)+\phi(p)\\
&\vdots\\
&+\phi(p)+\phi(p^2)+\phi(p)\\
&+\phi(p)
\end{aligned}$$

tane ideal, ve $s-j$ tek iken

$$\begin{aligned}
&\phi(p)+\phi(p^2)+\cdots+\phi(p^{\lfloor (s-j)/2 \rfloor-1})+\phi(p^{\lfloor (s-j)/2 \rfloor-1})+\cdots+\phi(p^2)+\phi(p)\\
&+\phi(p)+\phi(p^2)+\cdots+\phi(p^{\lfloor (s-j)/2 \rfloor-2})+\phi(p^{\lfloor (s-j)/2 \rfloor-2})+\cdots+\phi(p^2)+\phi(p)\\
&\vdots\\
&+\phi(p)+\phi(p^2)+\phi(p^2)+\phi(p)\\
&+\phi(p)+\phi(p)
\end{aligned}$$

tane ideal vardır. O halde bütün 5. tip ideallerin sayısı, $s$ çift iken

$$\sum_{i=0}^{0}(i+1)\phi(p^{\lfloor(2-i)/2\rfloor})+\sum_{i=0}^{2}(i+1)\phi(p^{\lfloor(4-i)/2\rfloor})+\cdots+\sum_{i=0}^{s-4}(i+1)\phi(p^{\lfloor(s-2-i)/2\rfloor})$$

ve $s$ tek iken de

$$\sum_{i=0}^{1}(i+1)\phi(p^{\lfloor(3-i)/2\rfloor})+\sum_{i=0}^{3}(i+1)\phi(p^{\lfloor(5-i)/2\rfloor})+\cdots+\sum_{i=0}^{s-4}(i+1)\phi(p^{\lfloor(s-2-i)/2\rfloor})$$

dir. Burada, $p$ asal sayısı için $\phi(p)+\phi(p^2)+\cdots+\phi(p^n)=p^n-1$ eşitliğini hatırlayalım. Sonuçta 5. tip ideallerin sayısını

$$\sum_{i=0}^{s-4}(i+1)p^{\lfloor(s-2-i)/2\rfloor}-C(s-2,2)=\sum_{i=0}^{s-2}(i+1)p^{\lfloor(s-2-i)/2\rfloor}-C(s,2)$$

olarak buluruz. Dikkat edilirse bu ifade aynı zamanda

$\phi(p)[\sum_{i=0}^{s-4}(i+1)p^{\lfloor(s-4-i)/2\rfloor}+\sum_{i=0}^{s-6}(i+1)p^{\lfloor(s-6-i)/2\rfloor}+\cdots+\sum_{i=0}^{s(\mathrm{mod}\,2)}(i+1)p^{\lfloor(s-2-i)/2\rfloor}]$'dir.

Artık beş faklı tip idealin sayısını belirlediğimize göre, $\mathbb{Z}_{p^s}+u\mathbb{Z}_{p^s}$ halkasının ideal sayısı

$$(s+1)+s+(p-1)\sum_{i=0}^{s-2}(i+1)p^{\lfloor(s-2-i)/2\rfloor}+C(s,2)+\sum_{i=0}^{s-2}(i+1)p^{\lfloor(s-2-i)/2\rfloor}-C(s,2)$$

$$=p\sum_{i=0}^{s-2}(i+1)p^{\lfloor(s-2-i)/2\rfloor}+2s+1=\sum_{i=0}^{s-2}(i+1)p^{\lfloor(s-i)/2\rfloor}+\sum_{i=s-1}^{s}(i+1)p^{\lfloor(s-i)/2\rfloor}=\sum_{i=0}^{s}(i+1)p^{\lfloor(s-i)/2\rfloor}$$

olarak bulunur. Burada, eğer $\sum_{i=0}^{s}(i+1)p^{\lfloor(s-i)/2\rfloor}$ toplamını $K_{p,s}$ ile gösterecek olursak,

$\sum_{i=0}^{s-2}(i+1)p^{\lfloor(s-2-i)/2\rfloor}=K_{p,s-2}$ olacağından,

$$K_{p,s}=pK_{p,s-2}+2s+1$$

yinelemeli bağıntısı elde edilir. $K_{p,0}=1$ ve $\mathbb{Z}_p+u\mathbb{Z}_p$'nin ideallerinin $\langle 0\rangle$, $\langle u\rangle$ ve $\langle 1\rangle$ 'den ibaret olduğunu görmek zor değildir yani $K_{p,1}=3$'tür.

**Not:** $p=2$ için bu yinelemeli bağıntı [32]'de yer almaktadır ve aynı sonucu veren açık bir formül içermektedir. Biz de [32]'deki tam sayı dizileri ansiklopedisine, bu sayı

dizisinin aynı zamanda $\mathbb{Z}_{2^s}+u\mathbb{Z}_{2^s}$ halkasının ideallerinin sayısını verdiğine dair bir yorum ekledik.

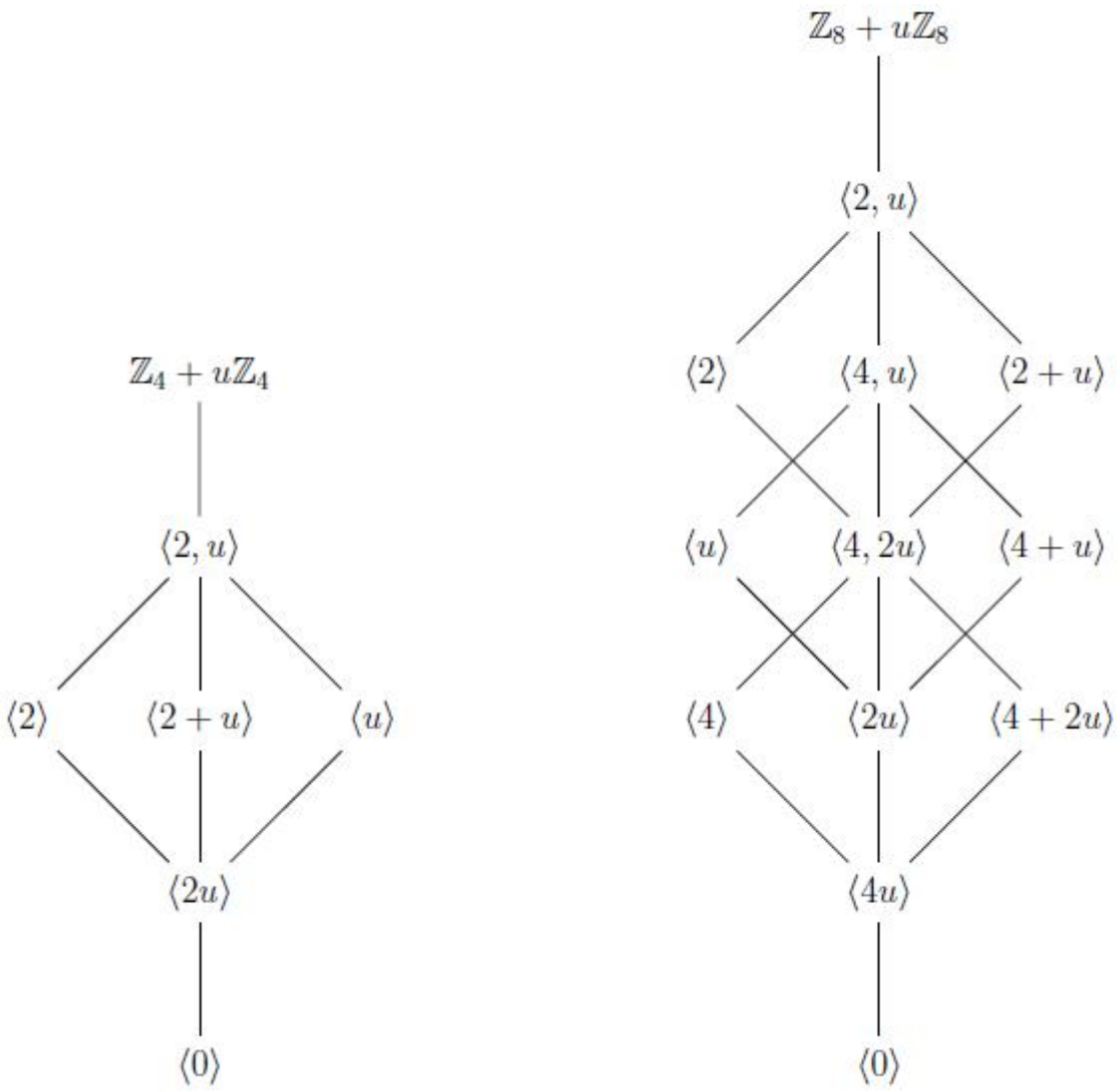
**Örnek 4.3** $\mathbb{Z}_{81}+u\mathbb{Z}_{81}$ halkasının 33 idealini üreteç tiplerine göre sınıflandırarak verelim:

- $\langle 0\rangle,\langle 1\rangle,\langle 3\rangle,\langle 9\rangle,\langle 27\rangle$
- $\langle u\rangle,\langle 3u\rangle,\langle 9u\rangle,\langle 27u\rangle$
- $\langle 3+u\rangle,\langle 6+u\rangle,\langle 9+u\rangle,\langle 18+u\rangle,\langle 36+u\rangle,\langle 45+u\rangle,\langle 63+u\rangle,\langle 72+u\rangle,\langle 27+u\rangle$
  $\langle 54+u\rangle,\langle 9+3u\rangle,\langle 18+3u\rangle,\langle 27+3u\rangle,\langle 54+3u\rangle,\langle 27+9u\rangle,\langle 54+9u\rangle$
- $\langle 3,u\rangle,\langle 9,u\rangle,\langle 27,u\rangle,\langle 9,3u\rangle,\langle 27,3u\rangle,\langle 27,9u\rangle$
- $\langle 9+u,27\rangle,\langle 18+u,27\rangle$

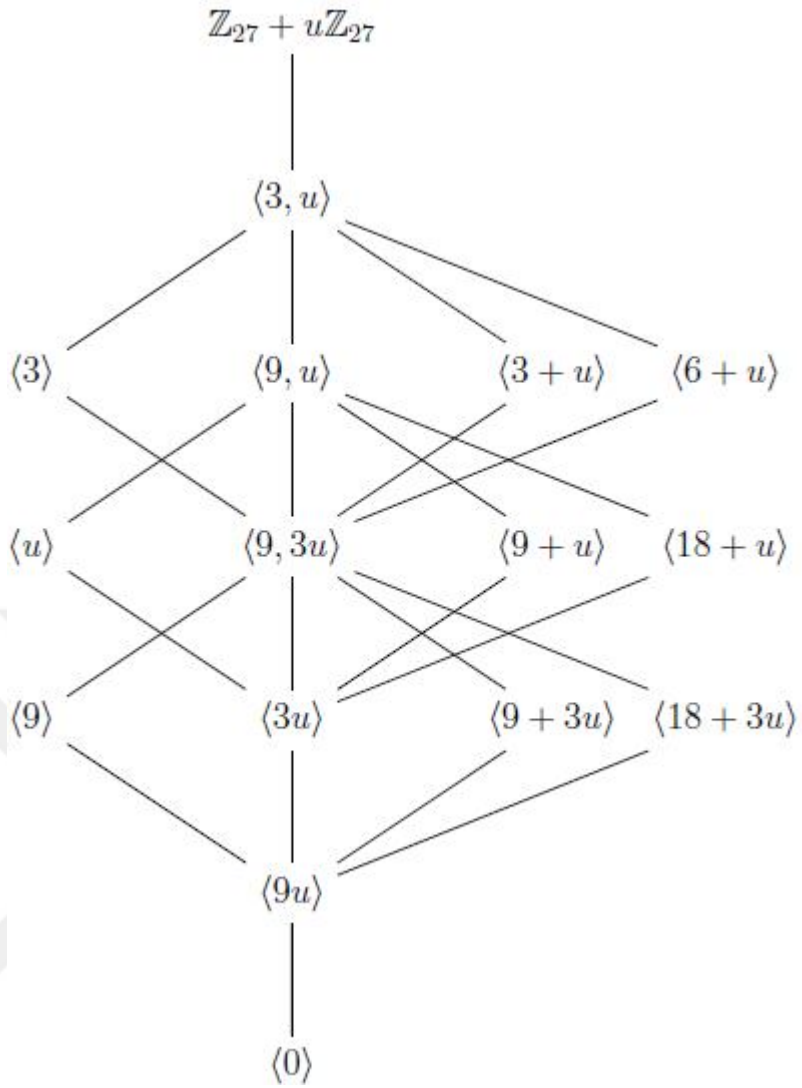
$\mathbb{Z}_{64}+u\mathbb{Z}_{64}$ halkasının 59 idealini üreteç tiplerine göre sınıflandırarak verelim:

- $\langle 0\rangle,\langle 1\rangle,\langle 2\rangle,\langle 4\rangle,\langle 8\rangle,\langle 16\rangle,\langle 32\rangle$
- $\langle u\rangle,\langle 2u\rangle,\langle 4u\rangle,\langle 8u\rangle,\langle 16u\rangle,\langle 32u\rangle$
- $\langle 2+u\rangle,\langle 4+u\rangle,\langle 12+u\rangle,\langle 8+u\rangle,\langle 24+u\rangle,\langle 40+u\rangle,\langle 56+u\rangle,\langle 16+u\rangle,\langle 48+u\rangle$
  $\langle 32+u\rangle,\langle 4+2u\rangle,\langle 8+2u\rangle,\langle 24+2u\rangle,\langle 16+2u\rangle,\langle 48+2u\rangle,\langle 32+2u\rangle,\langle 8+4u\rangle$
  $\langle 16+4u\rangle,\langle 48+4u\rangle,\langle 32+4u\rangle,\langle 16+8u\rangle,\langle 32+8u\rangle,\langle 32+16u\rangle$
- $\langle 2,u\rangle,\langle 4,u\rangle,\langle 8,u\rangle,\langle 16,u\rangle,\langle 32,u\rangle,\langle 4,2u\rangle,\langle 8,2u\rangle,\langle 16,2u\rangle,\langle 32,2u\rangle,\langle 8,4u\rangle,$
  $\langle 16,4u\rangle,\langle 32,4u\rangle,\langle 16,8u\rangle,\langle 32,8u\rangle,\langle 32,16u\rangle$
- $\langle 4+u,8\rangle,\langle 8+u,16\rangle,\langle 8+u,32\rangle,\langle 24+u,32\rangle,$
  $\langle 16+u,32\rangle,\langle 8+2u,16\rangle,\langle 16+2u,32\rangle,\langle 16+4u,32\rangle$

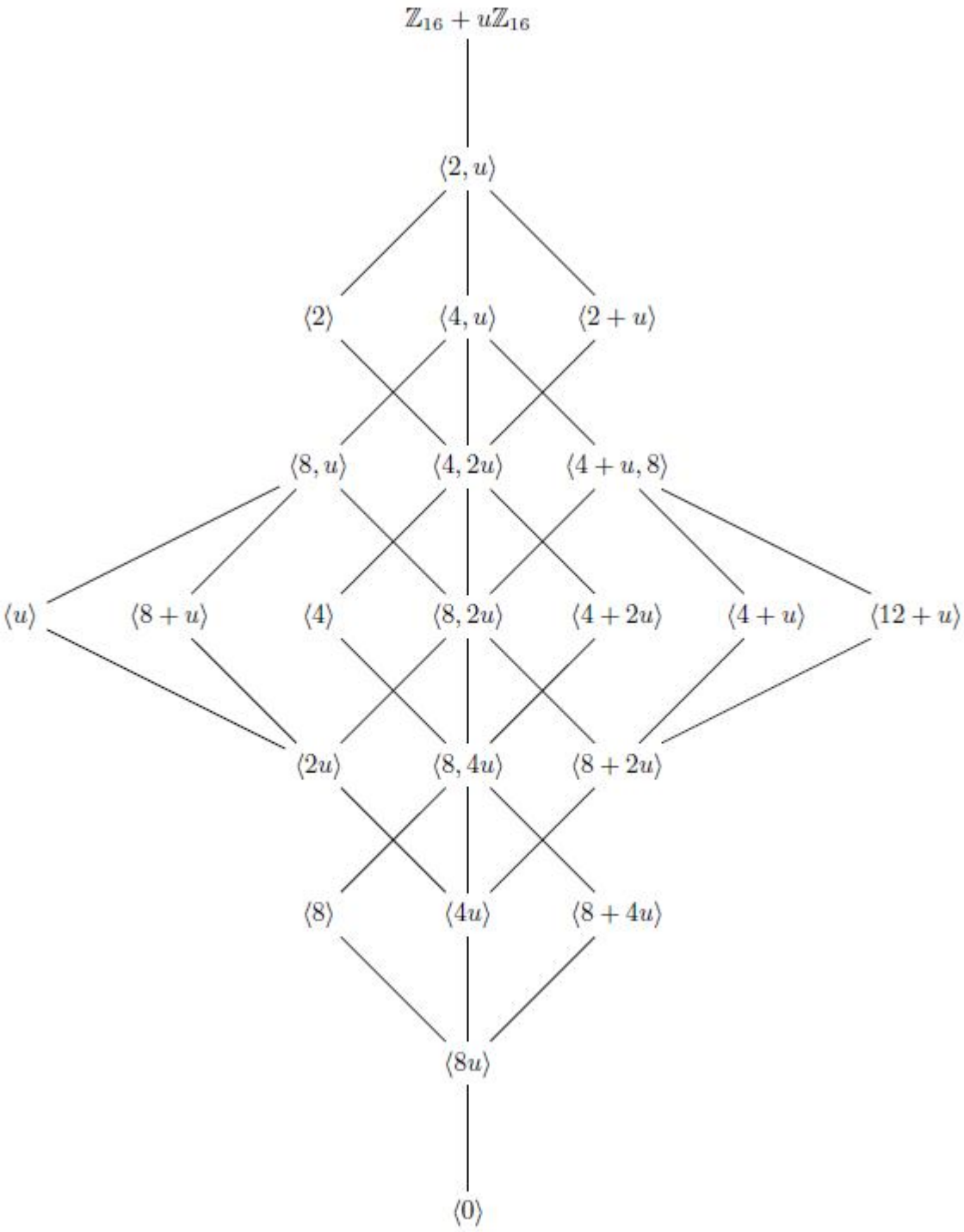
**Örnek 4.4** $\mathbb{Z}_4+u\mathbb{Z}_4$, $\mathbb{Z}_8+u\mathbb{Z}_8$, $\mathbb{Z}_{27}+u\mathbb{Z}_{27}$ ve $\mathbb{Z}_{16}+u\mathbb{Z}_{16}$ ve halkalarının ideallerini Hasse diyagramı ile gösterelim:



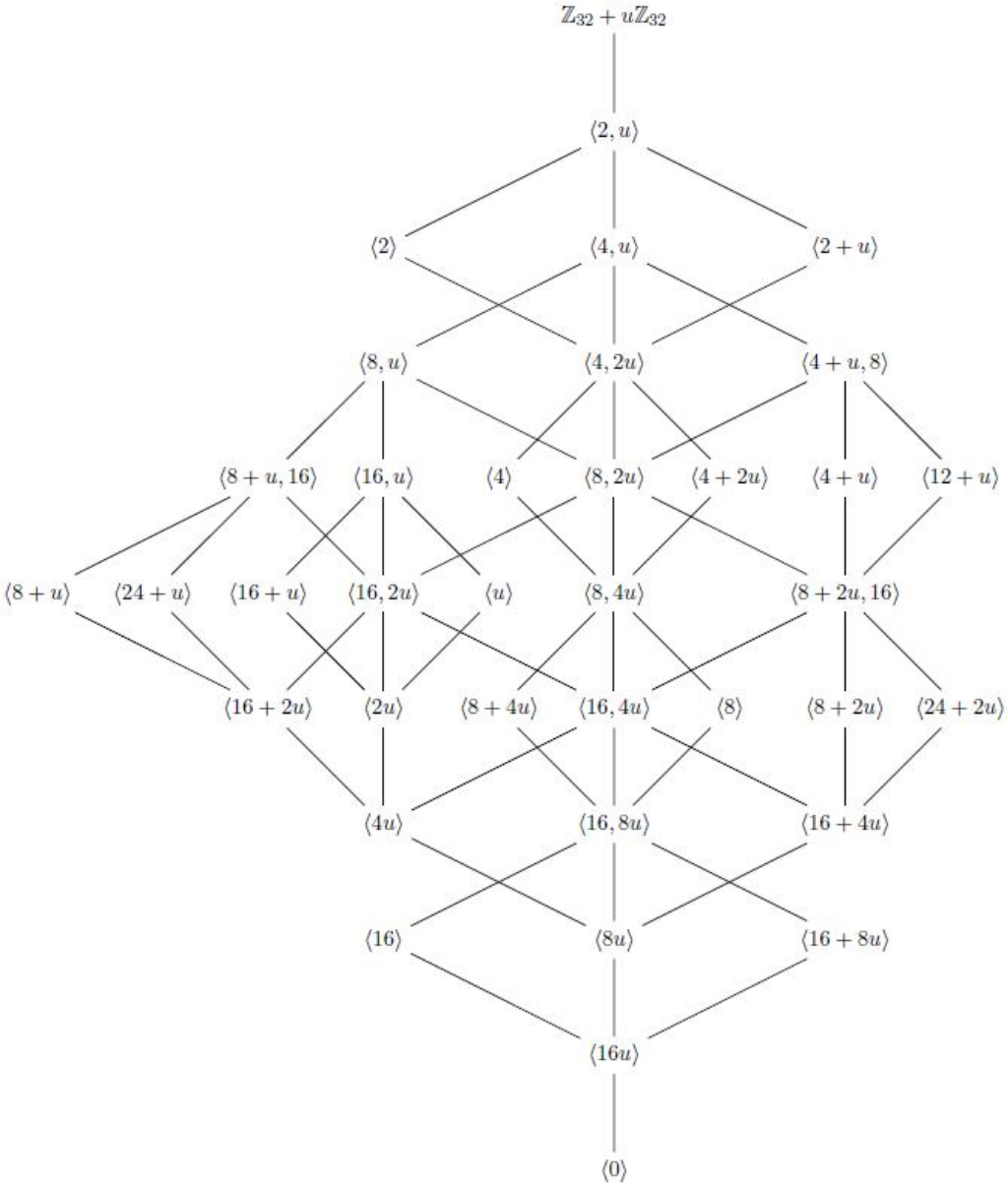

Şekil 4. 1 $\mathbb{Z}_4 + u\mathbb{Z}_4$ ve $\mathbb{Z}_8 + u\mathbb{Z}_8$ halkalarının idealleri için Hasse diyagramı




Şekil 4. 2 $\mathbb{Z}_{27} + u\mathbb{Z}_{27}$ halkasının idealleri için Hasse diyagramı




Şekil 4. 3 $\mathbb{Z}_{16} + u\mathbb{Z}_{16}$ halkasının idealleri için Hasse diyagramı




Şekil 4. 4 $\mathbb{Z}_{32} + u\mathbb{Z}_{32}$ halkasının idealleri için Hasse diyagramı

### 4.3 $\mathbb{Z}_q + u\mathbb{Z}_q$ Halkası Üzerinde Devirli Kodlar

**Tanım 4.5** $\mathbb{Z}_q + u\mathbb{Z}_q$ üzerinde bir $C$ lineer kodu, $\mathbb{Z}_q + u\mathbb{Z}_q$ kat sayılı bütün $n$'lilerin kümesi $(\mathbb{Z}_q + u\mathbb{Z}_q)^n = \{(c_0, c_1, \ldots, c_{n-1}) \mid \text{tüm } i = 0,1,\ldots,n-1 \text{ ler için } c_i \in \mathbb{Z}_q + u\mathbb{Z}_q\}$'in bir $(\mathbb{Z}_q + u\mathbb{Z}_q)$-alt modülüdür.

$\mathbb{Z}_q + u\mathbb{Z}_q$ halkası üzerindeki devirli kodlar da tıpkı cisimler üzerindeki devirli kodlar gibi tanımlanır ve kodsözlerle polinomlar aynı şekilde eşlenir.

**Tanım 4.6** $\mathbb{Z}_q + u\mathbb{Z}_q$ halkası üzerindeki bir $C$ lineer kodu, eğer her bir $c = (c_0, c_1, \ldots, c_{n-1})$ kodsözü için bu kodsözün koordinatlarının devirsel olarak kaydırılmasıyla elde edilen $(c_{n-1}, c_0, \ldots, c_{n-2})$ sözü de $C$ kodunun elemanı ise ya da diğer bir ifadeyle $C$ kodu kaydırma operatörü altında değişmez (invariant) ise, $C$ kodu bir devirli kod olarak adlandırılır.

Devirli Kodlar bölümünde bahsettiğimiz gibi $\mathbb{Z}_q + u\mathbb{Z}_q$ halkası üzerindeki $n$ uzunluklu $C$ lineer kodunun devirli olması için gerek ve yeter koşul, Eşitlik (3.1)'e benzer şekilde aşağıdaki gibi tanımlanan eşlemeyle kodsözlere karşılık gelen polinomların, $(\mathbb{Z}_q + u\mathbb{Z}_q)[x]/\langle x^n - 1\rangle$ halkasının bir ideali olmasıdır:

$$\varphi : C \to (\mathbb{Z}_q + u\mathbb{Z}_q)[x]/\langle x^n - 1\rangle,\ \varphi\left(c_0, c_1, \ldots, c_{n-1}\right) \mapsto c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}.$$

$(\mathbb{Z}_q + u\mathbb{Z}_q)[x]/\langle x^n - 1\rangle$ halkasının ideal yapısını belirlememizdeki temel motivasyon, bahsettiğimiz bu çift taraflı gerektirmedir. Bu amaç için, $\mathbb{Z}_4$-lineer kodlar bölümündekine benzer şekilde

$$\begin{aligned} &- : \mathbb{Z}_q + u\mathbb{Z}_q \to \mathbb{Z}_p \\ &a + bu \mapsto \bar{a} = a \pmod p \end{aligned}$$

fonksiyonunu tanımlamamız yararlı olacaktır. Bu fonksiyon, aşağıdaki gibi doğal bir yolla polinom halkaları arasındaki bir fonksiyona genişletilebilir.

$$\begin{aligned} &\psi : (\mathbb{Z}_q + u\mathbb{Z}_q)[x] \to \mathbb{Z}_p[x] \\ &f(x) = c_0 + c_1 x + \cdots + c_m x^m \mapsto \bar{f}(x) = \bar{c}_0 + \bar{c}_1 x + \cdots + \bar{c}_m x^m \end{aligned} \tag{4.2}$$

**Tanım 4.7** Eğer $a(x)f(x)+b(x)g(x)=1$ olacak şekilde $a(x),b(x)\in(\mathbb{Z}_q+u\mathbb{Z}_q)[x]$ polinomları varsa $f(x)$ ve $g(x)$ polinomları $\mathbb{Z}_q+u\mathbb{Z}_q$ halkası üzerinde *aralarında asaldır* denir.

**Lemma 4.8** $\mathbb{Z}_q+u\mathbb{Z}_q$ halkası üzerindeki $f_1(x)$ ve $f_2(x)$ polinomlarının aralarında asal olması için gerek ve yeter koşul, (4.2) fonskiyonu altındaki görüntüleri $\overline{f}_1(x)$ ve $\overline{f}_2(x)$ polinomlarının $\mathbb{Z}_p[x]$'te aralarında asal olmasıdır.

**İspat** $f_1(x)$ ve $f_2(x)$ aralarında asal olduğunda (4.2)'de verilen $\psi$ altındaki görüntüleri $\overline{f}_1(x)$ ve $\overline{f}_2(x)$'in de $\mathbb{Z}_p[x]$'te aralarında asal olduğu açıktır. Tersini göstermek için kabul edelim ki $\overline{f}_1(x)$ ve $\overline{f}_2(x)$ polinomları $\mathbb{Z}_p[x]$'te aralarında asal olsunlar. O halde $\overline{a}_1(x)\overline{f}_1(x)+\overline{a}_2(x)\overline{f}_2(x)=1$ olacak şekilde $a_1(x),\ a_2(x)\in(\mathbb{Z}_q+u\mathbb{Z}_q)[x]$ polinomları vardır. Öyleyse, $i=1,2,\ldots,s$ için $k_i(x)\in(\mathbb{Z}_q+u\mathbb{Z}_q)[x]$ olmak üzere

$$a_1(x)f_1(x)+a_2(x)f_2(x)=1+pk_1(x)+p^2k_2(x)+\cdots+p^{s-1}k_{s-1}(x)+uk_s(x) \tag{4.3}$$

eşitliği geçerlidir. Bu eşitliğin her iki tarafını $p^{s-1}k_{s-1}(x)+uk_s(x)$ ile çarptığımızda

$$\begin{aligned}&(p^{s-1}k_{s-1}(x)+uk_s(x))a_1(x)f_1(x)+(p^{s-1}k_{s-1}(x)+uk_s(x))a_2(x)f_2(x)\\&=p^{s-1}k_{s-1}(x)+up^{s-1}k_{s-1}(x)k_s(x)+uk_s(x)+puk_1(x)k_s(x)+\cdots+p^{s-1}uk_{s-1}(x)k_s(x)\end{aligned} \tag{4.4}$$

eşitliğini elde ederiz. (4.3)'ten (4.4)'ü taraf tarafa çıkardığımızda ise

$$\begin{aligned}&(1-p^{s-1}k_{s-1}(x)-uk_s(x))a_1(x)f_1(x)+(1-p^{s-1}k_{s-1}(x)-uk_s(x))a_2(x)f_2(x)\\&=1+(pk_1(x)+p^2k_2(x)+\cdots+p^{s-1}k_{s-1}(x))(1-uk_s(x))-p^{s-1}k_{s-1}(x)\end{aligned} \tag{4.5}$$

eşitliğini elde ederiz. Dikkat edilirse, Eşitlik (4.5)'in sol tarafı $f_1(x)$ ve $f_2(x)$'in lineer kombinasyonu ve sağ tarafı da birimsel elemandır. Öyleyse eşitliğin iki tarafını da sağ tarafın tersi ile çarparsak $f_1(x)$ ve $f_2(x)$'in aralarında asal olduğu görülür.

**Tanım 4.9** $\mathbb{Z}_q+u\mathbb{Z}_q$ halkası üzerindeki bir $f(x)$ polinomunun $\psi$ fonksiyonu altındaki görüntüsü $\psi(f(x))=\overline{f}(x)$, $\mathbb{Z}_p$ halkası üzerinde indirgenemez ise $f(x)$ polinomuna $\mathbb{Z}_q+u\mathbb{Z}_q$ üzerinde *temel indirgenemez polinom* denir. Eğer $\langle f(x)\rangle$ asalımsı idealse, $f(x)$ polinomuna da *asalımsı* denir.

**Lemma 4.10** Eğer $f(x)$ temel indirgenemez polinom ise aynı zamanda asalımsıdır.

**İspat** $g(x)h(x) \in \langle f(x) \rangle$ olsun. $\psi(f(x)) = \overline{f}(x)$ indirgenemez olduğu için $\text{ebob}(\overline{f}(x), \overline{g}(x))$ ya 1'dir ya da $\overline{f}(x)$'dir. Eğer $\text{ebob}(\overline{f}(x), \overline{g}(x)) = 1$ ise $f(x) \mid h(x)$. $\text{ebob}(\overline{f}(x), \overline{g}(x)) = \overline{f}(x)$ durumunda ise $g(x) = f(x)a(x) + pb(x)$ eşitliğini sağlayan $a(x), b(x) \in (\mathbb{Z}_q + u\mathbb{Z}_q)[x]$ polinomları vardır. Eşitlikte her iki tarafın $s$'inci kuvvetini alırsak $g(x)^s \in \langle f(x) \rangle$ kapsamasını elde ederiz.

Hensel'in Lemması'nın sonlu, yerel (lokal) değişmeli halkalarda geçerli olduğu [33]'te gösterilmiştir. Öyleyse $\mathbb{Z}_p$'nin genişlemesi olan $\mathbb{Z}_q + u\mathbb{Z}_q$ halkası için de geçerlidir:

**Lemma 4.11** $f(x) \in (\mathbb{Z}_q + u\mathbb{Z}_q)[x]$ monik polinom $\overline{f}_1(x), \overline{f}_2(x), \ldots, \overline{f}_r(x)$ polinomları $\mathbb{Z}_p[x]$'te ikişerli olarak aralarında asal olmak üzere $\overline{f}(x) = \overline{f}_1(x)\overline{f}_2(x)\ldots\overline{f}_r(x)$ olsun. Bu durumda aşağıdakileri özellikleri sağlayan $g_1(x), g_2(x), \ldots, g_r(x) \in (\mathbb{Z}_q + u\mathbb{Z}_q)[x]$ monik polinomları vardır:

i. $f(x) = g_1(x)g_2(x)\cdots g_r(x)$

ii. $\overline{g_i}(x) = \overline{f}_i(x)$, $i = 1, 2, \ldots, r$

iii. $der(g_i(x)) = der(\overline{f}_i(x))$, $i = 1, 2, \ldots, r$

iv. $g_1(x), g_2(x), \ldots, g_r(x)$ polinomları $(\mathbb{Z}_q + u\mathbb{Z}_q)[x]$'te ikişerli aralarında asaldır.

**Lemma 4.12** $n$ ile $p$ aralarında asal olmak üzere $n$ pozitif bir tam sayı olsun. $x^n - 1$ polinomu, ikişerli olarak aralarında asal, temel indirgenemez polinomların çarpımı olarak $x^n - 1 = f_1(x)f_2(x)\cdots f_r(x)$ biçiminde tek türlü yazılır.

**İspat** $R$ bir lokal halka olmak üzere $R[x]$'te sıfır bölen olmayan polinomlar regüler (regular polynomial) olarak adlandırılır ve çarpımları tek türlüdür [33]. Lokal halka olan $\mathbb{Z}_q + u\mathbb{Z}_q$ üzerindeki, sıfırdan farklı katsayılarının en az bir tanesi birimsel olan polinomlar ve özel olarak $x^n - 1$ polinomu regülerdir. Öyleyse, Hensel'in Lemması'ndan $x^n - 1$ temel indirgenemez polinomların çarpımı olarak yazılır. Üstelik Lemma 4.10'dan

bu polinomlar asalımsıdır. Çarpımın tek türlü olduğu da lokal halkalar için [33]'teki çarpanlarına ayırma (factoriaztion) teoreminde gösterilmiştir.

**Lemma 4.13** $f_1(x), f_2(x), \ldots, f_r(x)$ polinomları $\mathbb{Z}_q + u\mathbb{Z}_q$ üzerinde ikişerli olarak aralarında asal olsunlar ve $f_i(x)$ hariç bütün $f_j(x)$'lerin çarpımını $\hat{f}_i(x)$ ile gösterelim. Bu durumda $f_i(x)$ ile $\hat{f}_i(x)$ aralarında asaldır.

**İspat** Lemma 4.8'de gösterildiği gibi farklı $i$ ve $j$'ler için $f_i(x)$ ile $f_j(x)$'in aralarında asal olması ve $\overline{f}_i(x)$ ile $\overline{f}_j(x)$'nin aralarında asal olması birbirini gerektirir. $\mathbb{Z}_p$ üzerindeki $\overline{\hat{f}}_i(x) = \overline{f}_1(x)\cdots\overline{f}_{i-1}(x)\overline{f}_{i+1}(x)\cdots\overline{f}_r(x)$ ve $\overline{f}_i(x)$'nin aralarında asal olduğu açıktır. Öyleyse Lemma 4.8'den $f_i(x)$ ve $\hat{f}_i(x)$'nin de aralarında asal olduğu sonucuna varırız.

**Lemma 4.14** $f_1(x), f_2(x), \ldots, f_r(x)$ temel indirgenemez polinomları $\mathbb{Z}_q + u\mathbb{Z}_q$ halkası üzerinde ikişerli olarak aralarında asal olsunlar. Bu durumda

$$\langle f_1(x)f_2(x)\cdots f_r(x)\rangle = \langle f_1(x)\rangle \cap \langle f_2(x)\rangle \cdots \cap \langle f_r(x)\rangle \tag{4.5}$$

eşitliği geçerlidir.

**İspat** $\langle f_1(x)f_2(x)\cdots f_r(x)\rangle \subseteq \langle f_1(x)\rangle \cap \langle f_2(x)\rangle \cdots \cap \langle f_r(x)\rangle$ kapsaması zaten açıktır. Ters kapsamayı göstermek için de $r$ üzerinde tümevarım uygularız. $r=1$ için durum aşikardır. $r>1$ iken $r-1$ için Eşitlik (4.5)'in doğru olduğunu kabul edelim. Bu durumda $\langle f_1(x)f_2(x)\cdots f_{r-1}(x)\rangle = \langle f_1(x)\rangle \cap \langle f_2(x)\rangle \cdots \cap \langle f_{r-1}(x)\rangle$ eşitliği geçerli olacaktır. Şimdi Eşitlik (4.5)'in sağ tarafındaki idealden bir $g(x) \in \langle f_1(x)\rangle \cap \langle f_2(x)\rangle \cdots \cap \langle f_r(x)\rangle$ alalım, bu durumda kabul gereği $g(x) \in \langle f_1(x)f_2(x)\cdots f_{r-1}(x)\rangle \cap \langle f_r(x)\rangle$ olacaktır. Öyleyse $g(x) = g_1(x)f_1(x)f_2(x)\cdots f_{r-1}(x) = g_r(x)f_r(x)$ olacak şekilde $g_1(x), g_r(x) \in \mathcal{R}[x]$ polinomları vardır. Lemma 4.13'ten $f_1(x)f_2(x)\cdots f_{r-1}(x)$ ve $f_r(x)$ aralarında asaldır. O halde $h_1(x)f_1(x)f_2(x)\cdots f_{r-1}(x) + h_r(x)f_r(x) = 1$ olacak şekilde $h_1(x), h_r(x) \in \mathcal{R}[x]$ polinomları vardır. Bu eşitliğin her iki tarafını $g(x)$ ile çarparsak

$$\begin{aligned} g(x) &= g(x)h_1(x)f_1(x)f_2(x)\cdots f_{r-1}(x) + g(x)h_r(x)f_r(x) \\ &= \left(g_r(x)h_1(x) + g_1(x)h_r(x)\right)f_1(x)f_2(x)\cdots f_r(x) \\ &\in \langle f_1(x)f_2(x)\cdots f_r(x)\rangle \end{aligned}$$

içermesini elde ederiz ve göstermek istediğimiz de buydu.

**Teorem 4.15** [34] (Çin Kalan Teoremi) $A_1, A_2, \ldots, A_n$ bir $R$ halkasının, tüm $i$'ler için $R^2 + A_i = R$ ve tüm $i \neq j$'ler için $A_i + A_j = R$ şartını sağlayan idealleri olsun. Eğer $b_1, \ldots, b_n \in R$ ise

$b \equiv b_i (\mathrm{mod}\, A_i)$ $(i = 1, 2, \ldots, n)$

olacak şekilde $b \in R$ vardır ve $b$ elemanı $A_1 \cap A_2 \cap \cdots \cap A_n$ idealinin denklik sınıfında tek türlü belirlidir.

**Sonuç 4.16** [34] $A_1, A_2, \ldots, A_n$ bir $R$ halkasının idealleri olsun. Bu durumda

$\theta : R/(A_1 \cap A_2 \cap \cdots \cap A_n) \to R/A_1 \times R/A_2 \times \cdots \times R/A_n$

monomorfizması vardır. Eğer tüm $i$'ler için $R^2 + A_i = R$ ve tüm $i \neq j$'ler için $A_i + A_j = R$ ise $\theta$ bir izomorfizmadır.

**Not:** $\mathcal{R}$ birimli halka olduğu için ve birimli halkalarda $R^2 = R$ olacağı için $R^2 + A_i = R$ şartı otomatik olarak sağlanır.

**Sonuç 4.17** $(n, p) = 1$ olmak üzere $x^n - 1 = f_1(x)f_2(x)\cdots f_r(x)$ temel indirgenemez ve ikişerli olarak aralarında asal polinomların çarpımı olsun. Öyleyse Lemma (4.14)'ten

$$\mathfrak{R}_n = (\mathbb{Z}_q + u\mathbb{Z}_q)[x]/\langle x^n - 1\rangle = \mathcal{R}[x]/\langle f_1(x)\rangle \cap \langle f_2(x)\rangle \cdots \cap \langle f_r(x)\rangle$$

olur ve Çin Kalan Teoremini uyguladığımızda, Sonuç (4.16)'dan

$$\mathfrak{R}_n \cong \mathcal{R}[x]/\langle f_1(x)\rangle \oplus \mathcal{R}[x]/\langle f_2(x)\rangle \oplus \cdots \oplus \mathcal{R}[x]/\langle f_r(x)\rangle$$

izomorfizmasını elde ederiz. Dolayısıyla $I$, eğer $\mathfrak{R}_n$'in bir ideali ise, $i = 1, 2, \ldots, r$ için $I_i$'ler $\mathcal{R}[x]/\langle f_i(x)\rangle$'in idealleri olmak üzere aşağıdaki izomorfizmayı elde ederiz:

$$I \cong I_1 \oplus I_2 \oplus \cdots \oplus I_r \qquad (4.6)$$

Öyleyse şimdi, nihai amacımız olan $\Re_n = (\mathbb{Z}_q + u\mathbb{Z}_q)[x]/\langle x^n - 1\rangle$ bölüm halkasının ideallerini belirlemek için (4.6)'daki izomorfizmadan yararlanabilmek adına, $f(x)$ temel indirgenemez polinom olmak üzere $\mathcal{R}[x]/\langle f(x)\rangle$'in ideallerini belirleyelim.

Bir zincir halkası olan $\mathbb{Z}_4$ üzerindeki devirli kodlar belirlenirken de ihtiyaç duyulan $\mathbb{Z}_4[x]/\langle f(x)\rangle$'in idealleri ile $\mathbb{Z}_4$'ün idealleri arasında birebir ilişki varken, zincir halkası olmayan $\mathbb{Z}_q + u\mathbb{Z}_q$ için $(\mathbb{Z}_q + u\mathbb{Z}_q)[x]/\langle f(x)\rangle$'in idealleri ile $\mathbb{Z}_q + u\mathbb{Z}_q$'nun idealleri arasında böyle bir ilişki yoktur. $(\mathbb{Z}_q + u\mathbb{Z}_q)[x]/\langle f(x)\rangle$ bölüm halkası $\mathbb{Z}_q + u\mathbb{Z}_q$'dan çok daha zengin bir ideal yapısına sahiptir.

**Lemma 4.18** $f(x)$, $\mathbb{Z}_q + u\mathbb{Z}_q$ üzerinde, derecesi $m$ olan bir temel indirgenemez polinom olsun. Bu takdirde $(\mathbb{Z}_q + u\mathbb{Z}_q)[x]/\langle f(x)\rangle$ halkasının idealleri aşağıdaki gibidir.

1. $\langle p^i + \langle f(x)\rangle\rangle$ ; $0 \le i \le s$

2. $\langle p^j u + \langle f(x)\rangle\rangle$ ; $0 \le j < s$

3. $\langle v(x)p^i + p^j u + \langle f(x)\rangle\rangle$ ; $0 \le j < i < s$ ve her bir $l$ için $v_l < p^{\min(i-j,s-i)}$ olmak kaydıyla $v(x) = \sum_{l=0}^{m-1} v_l x^l$ birimsel

4. $\langle p^i + \langle f(x)\rangle, p^j u + \langle f(x)\rangle\rangle$ ; $0 \le j < i < s$

5. $\langle v(x)p^i + p^j u + \langle f(x)\rangle, p^k + \langle f(x)\rangle\rangle$ ; $0 \le j < i < s$, $1 \le \overline{v} < p^{\min(i-j,s-i)-1}$ ve $(p,\overline{v}) = 1$ olmak üzere $\lfloor \log_p \overline{v} \rfloor + i < k < \min(i-j, s-i) + i$ ve de her bir $l$ için $v_l < p^{k-i}$ olmak kaydıyla $v(x) = \sum_{l=0}^{m-1} v_l x^l$ birimsel

**İspat** Teorem 4.1'in ispatına benzer şekilde önce $(\mathbb{Z}_q + u\mathbb{Z}_q)[x]/\langle f(x)\rangle$ halkasının esas ideallerini belirleyeceğiz. İki üreteçli idealleri de bu esas ideallerin kombinasyonları ile belirleyeceğiz. Öncelikle bu halkanın birimsel elemanlarının

$$\left\{ \sum_{i=0}^{m-1} a_i x^i \mid a_i \in \mathbb{Z}_q + u\mathbb{Z}_q, \exists i \to a_i \text{ birimsel} \right\}$$

kümesinden ibaret olduğunu belirtelim. $\mathbb{Z}_q + u\mathbb{Z}_q$ halkasındaki birimsel olmayan sıfırdan farklı tüm elemanlar nilpotent olduğu için hiçbir katsayısı birimsel olmayan

polinomun da birimsel olmayacağı açıktır. Bununla birlikte bir tane katsayısı birimsel olan polinomun $\psi$ altındaki görüntüsü, temel indirgenemez olan $f(x)$'in $\psi$ altındaki görüntüsü $\overline{f}(x)$ ile aralarında asal olacağı için, bu polinom $\langle f(x)\rangle$ denklik sınıfında birimsel olacaktır. O halde, aşikâr olmayan $\langle g(x)\rangle$ esas, öz ideali için, üreteç polinom $g(x)$'in tüm katsayılarının $\mathbb{Z}_q + u\mathbb{Z}_q$ halkasında birimsel olmayan elemanlardan oluştuğunu söyleyebiliriz.

Eğer bir zincir halkası olan $\mathbb{Z}_q$ üzerindeki $a(x),\ b(x) \in \mathbb{Z}_q[x]$ polinomları için $g(x) = a(x) + ub(x)$ formunda ise $g(x)$ polinomunu; $a(x)$'in katsayılarının en büyük ortak böleni $p^i$ ve $b(x)$'in katsayılarının en büyük ortak böleni $p^j$ olmak üzere $g(x) = p^i a_1(x) + p^j u b_1(x)$ şeklinde ifade edebiliriz. Burada, $b_1(x)$ polinomu birimsel olacağı için $\langle g(x)\rangle = \langle a_1(x)b_1(x)^{-1}p^i + p^j u\rangle$ olur ki bu da 3. tipteki idealdir. Özel bir durum olarak $g(x)$'in tüm katsayıları $\mathbb{Z}_q$ ya da $u\mathbb{Z}_q$ halkasından gelirse, $g(x)$ tarafından üretilen esas ideal 1 ya da 2 tipinde olacaktır.

3. tipteki ideallerin birbirinden farklı olması için birimsel $v(x)$ polinomunun katsayılarının ($l = 1,2,\ldots,m-1$ için $v_l$'ler) $p^{\min(i-j,s-i)}$'den küçük olması gerekliliği Teorem 4.1'deki gibi gösterilebilir. Genelliği bozmadan, tam sayısı için, $(p^{s-i} + v_\alpha)p^i = p^i v_\alpha$ olacağından

$$\langle (v_0 + v_1 x + \cdots + v_\alpha x^\alpha + \cdots + v_{m-1}x^{m-1})p^i + p^j u\rangle$$
$$= \langle (v_0 + v_1 x + \cdots + (p^{s-i} + v_\alpha)x^\alpha + \cdots + v_{m-1}x^{m-1})p^i + p^j u\rangle$$

ideallerinin eşitliğini görmek zor değildir. O halde $v_l < p^{s-i}$'dir.

Yine genelliği bozmadan $0 \le \beta \le m-1$ tam sayısı için, $v(x) = v_0 + v_1 x + \cdots + v_{m-1}x^{m-1}$ olmak üzere $\langle (v_0 + v_1 x + \cdots + (v_\beta + p^{i-j})x^\beta + \cdots + v_{m-1}x^{m-1})p^i + p^j u\rangle$ idealini ele alalım. Bu idealin $\langle v(x)p^i + p^{2i-j}x^\beta + p^j u\rangle$ idealine eşit olduğu açıktır. Ancak dikkat edilirse, $(v(x)p^i + p^j u)(v(x)^{-1}p^{i-j} - v(x)^{-2}u) = p^{2i-j}$ eşitliğinden $p^{2i-j} \in \langle v(x)p^i + p^j u\rangle$ ve dolayısıyla da $p^{2i-j}x^\beta \in \langle v(x)p^i + p^j u\rangle$ olduğu görülür. Buradan sonuç olarak

$$\langle v(x)p^i + p^{2i-j}x^\beta + p^j u\rangle = \langle (v_0 + v_1 x + \cdots + (v_\beta + p^{i-j})x^\beta + \cdots + v_{m-1}x^{m-1})p^i + p^j u\rangle$$
$$= \langle v(x)p^i + p^j u\rangle$$

eşitliğini elde ederiz. Öyleyse $v_l < p^{i-j}$ olmalıdır.

1. tip ile 2. tip ideallerin kombinasyonundan $j < i$ ise açıkça 4. tipteki ideali, $i \le j$ ise $\langle p^i + \langle f(x)\rangle\rangle \supset \langle p^j u + \langle f(x)\rangle\rangle$ olacağı için 1. tipteki ideali elde ederiz.

1. tip ile 3. tip ideallerin kombinasyonundan, $\langle v(x)p^i + p^j u + \langle f(x)\rangle\rangle$ ile $\langle p^i + \langle f(x)\rangle\rangle$ ideal üreteçlerinin, birbirlerinin ürettiği ideallerde içerilme şartına göre 1. tip ideal, 3. tip ideal ya da 5. tip ideal elde edileceği görülür.

2. ile 3. tip ideallerin kombinasyonları için $\langle p^k u + \langle f(x)\rangle\rangle$ ile $\langle v(x)p^i + p^j u + \langle f(x)\rangle\rangle$ ideallerine baktığımızda $k < j$ iken $\langle v(x)p^i + p^j u + \langle f(x)\rangle, p^k u + \langle f(x)\rangle\rangle$ $= \langle p^i + \langle f(x)\rangle, p^k u + \langle f(x)\rangle\rangle$ olacağından 4. tip ideal elde edileceği açıktır. $j < k$ olduğunda ise 5. tip ideal elde edilecektir.

5. tip ideallerdeki $k$'nın sınırlarının belirlenmesi Teorem 4.1'deki gibidir. Diğer yandan genelliği bozmadan bir $0 \le \theta \le m-1$ tam sayısı için, $v(x) = v_0 + v_1 x + \cdots + v_{m-1}x^{m-1}$ olmak üzere $\langle (v_0 + v_1 x + \cdots + (v_\theta + p^{k-i})x^\theta + \cdots + v_{m-1}x^{m-1})p^i + p^j u, p^k\rangle$ ideali; $\langle v(x)p^i + p^k x^\theta + p^j u, p^k\rangle = \langle v(x)p^i + p^j u, p^k\rangle$ idealine eşit olacağı için, farklı ideal elde etmek için $v_l < p^{k-i}$ olmalıdır.

Şimdi, yukarıda belirlediğimiz idealleri, $\mathfrak{R}_n$ halkasının iç direkt toplananlarının ideallerine taşıyabilmek için aşağıdaki Lemma'yı veriyoruz.

**Lemma 4.19** $n$ ile $p$ aralarında asal olmak üzere $n$ pozitif bir tam sayı olsun. $(\mathbb{Z}_q + u\mathbb{Z}_q)[x]$ üzerinde $x^n - 1 = f_1(x)f_2(x)\cdots f_r(x)$ ikişerli aralarında asal, dereceleri $1$ ya da daha büyük monik polinomların çarpımı olsun. Bu durumda

**1.** $\mathfrak{R}_n$'de $1 = e_1 + e_2 + \cdots + e_r$ olacak şekilde $i = 1, 2, \ldots, r$ için $e_i$ idempotent elemanlar vardır. Üstelik $R_i = \mathfrak{R}_n e_i$, $\mathfrak{R}_n$'in bir ideali olur ve de $\mathfrak{R}_n$'in aşağıdaki gibi iç direkt toplam ayrışımını elde ederiz;

$$\mathfrak{R}_n = R_1 \oplus R_2 \oplus \cdots \oplus R_r \qquad (4.7)$$

**2.** Her bir $1 \le i \le r$ için aşağıda verilen fonksiyon bir izomorfizmadır

$$\begin{aligned}&(\mathbb{Z}_q + u\mathbb{Z}_q)[x]/\langle f_i(x)\rangle \to R_i = \mathfrak{R}_n e_i \\ &k(x) + \langle f_i(x)\rangle \mapsto (k(x) + \langle x^n - 1\rangle)e_i\end{aligned} \tag{4.8}$$

**İspat** $f_i(x)$ ile $\hat{f}_i(x)$'in aralarında asal olduğunu Lemma 4.13'ten biliyoruz. Öyleyse

$$u_i(x)\hat{f}_i(x) + v_i(x)f_i(x) = 1 \tag{4.9}$$

olacak şekilde $u_i(x)$ ve $v_i(x)$ polinomları vardır. Eğer $e_i = u_i(x)\hat{f}_i(x) + \langle x^n - 1\rangle$ olarak seçersek (4.7)'yi Çin Kalan Teoremi'nin doğal bir sonucu olarak elde ederiz.

(4.8)'de verilen fonksiyonun bir halka homomorfizması olduğu rutin bir şekilde gösterilebilir. Bu fonksiyonun bir monomorfizma olduğunu göstermek için çekirdeğinin $\{0\}$'dan ibaret olduğunu gösterelim.

(4.8) altındaki görüntüsü $0$ olan bir $k(x) + \langle f_i(x)\rangle$ alalım. Bu durumda $e_i$'yi yerine koyarsak

$$k(x)u_i(x)\hat{f}_i(x) \equiv 0 \pmod{x^n - 1}$$

denkliğini elde ederiz. Buradan da $x^n - 1 = f_i(x)\hat{f}_i(x)$ olduğu için

$$k(x)u_i(x)\hat{f}_i(x) \equiv 0 \pmod{f_i(x)}$$

denkliğini elde ederiz. Burada Eşitlik (4.9)'un her iki tarafını da $k(x)$ ile çarpıp modülo $f_i(x)$'teki değerini aldığımızda

$$k(x)u_i(x)\hat{f}_i(x) \equiv k(x) \pmod{f_i(x)}$$

denkliğini elde ederiz ki buradan da $k(x) \equiv 0 \pmod{f_i(x)}$ sonucuna varırız. Bu da (4.8)'in çekirdeğinin yalnızca $0 + \langle f_i(x)\rangle$ elemanından oluştuğunu ve dolayısıyla da birebir olduğunu gösterir.

Son olarak (4.8)'in örten olduğunu gösterelim. Görüntü kümesinden herhangi bir $(m(x) + \langle x^n - 1\rangle)e_i$ elemanı alalım. $f_i(x)$ monik polinom olduğu için $m(x)$'i, $f_i(x)$'e böldüğümüzde $q(x), r(x) \in \mathcal{R}[x]$ $der(r(x)) < der(f_i(x))$ olmak üzere $m(x) = f_i(x)q(x) + r(x)$ eşitliğini elde ederiz. Burada

$r(x)+\langle f_i(x)\rangle = m(x)+\langle f_i(x)\rangle \in \mathcal{R}[x]/\langle f_i(x)\rangle$ olduğu ve $r(x)+\langle f_i(x)\rangle$'in (4.8)'de verilen homomorfizma altındaki görüntüsününün $(m(x)+\langle x^n-1\rangle)e_i$ olduğu görülür. Öyleyse (4.8)'de verilen homomorfizma örtendir.

**Lemma 4.20** $n$ ile $p$ aralarında asal ve $x^n-1$'in $\mathbb{Z}_q+u\mathbb{Z}_q$ üzerinde temel indirgenemezlerin tek türlü çarpımına ayrılışı $x^n-1=f_1(x)f_2(x)\cdots f_r(x)$ olsun. Bu durumda $t=1,2,\ldots,r$ için Lemma 4.18'de belirlenen $(\mathbb{Z}_q+u\mathbb{Z}_q)[x]/\langle f_t(x)\rangle$ halkasının idealleri, Lemma 4.19'da (4.8) ile verilen izomorfizma ile $R_t$'nin ideallerine aşağıdaki gibi resmedilir:

1. $\langle p^i \hat{f}_t(x)+\langle x^n-1\rangle\rangle$ ; $0\le i\le s$

2. $\langle p^j u\hat{f}_t(x)+\langle x^n-1\rangle\rangle$ ; $0\le j< s$

3. $\langle (v(x)p^i+p^j u)\hat{f}_t(x)+\langle x^n-1\rangle\rangle$ ; $0\le j<i<s$, her bir $l$ için $v_l<p^{\min(i-j,s-i)}$ olmak kaydıyla $v(x)=\sum_{l=0}^{m-1}v_l x^l$ birimsel

4. $\langle p^i \hat{f}_t(x)+\langle x^n-1\rangle, p^j u\hat{f}_t(x)+\langle x^n-1\rangle\rangle$ ; $0\le j<i<s$

5. $\langle (v(x)p^i+p^j u)\hat{f}_t(x)+\langle x^n-1\rangle, p^k \hat{f}_t(x)+\langle x^n-1\rangle\rangle$ ; $0\le j<i<s$ $1\le \overline{v}<p^{\min(i-j,s-i)-1}$ ve $(p,\overline{v})=1$ olmak üzere $\lfloor \log_p \overline{v}\rfloor+i<k<\min(i-j,s-i)+i$ ve de her bir $l$ için $v_l<p^{k-i}$ olmak kaydıyla $v(x)=\sum_{l=0}^{m-1}v_l x^l$ birimsel

**Sonuç 4.21** $n$ ile $p$ aralarında asal ve $x^n-1$'in $\mathbb{Z}_q+u\mathbb{Z}_q$ üzerinde temel indirgenemezlerin tek türlü çarpımına ayrılışı $x^n-1=f_1(x)f_2(x)\cdots f_r(x)$ olsun. Öyleyse $\mathfrak{R}_n$'in idealleri, Lemma 4.20'de verilen bazı ideallerin bir iç direkt toplamıdır.

**Sonuç 4.22** $f(x)$, $\mathbb{Z}_q+u\mathbb{Z}_q$ üzerinde, derecesi $m$ olan bir temel indirgenemez polinom olsun. Bu takdirde $(\mathbb{Z}_q+u\mathbb{Z}_q)[x]/\langle f(x)\rangle$'in bütün ideallerinin sayısı;

$$K_{p,0}^m=1,\ K_{p,1}^m=3 \text{ ve } K_{p,s}^m=\sum_{i=0}^{s}(i+1)p^{\lfloor (s-i)/2\rfloor m}$$

olmak üzere

$K_{p,s} + (p^m - 1)(K^m_{p,s-2} + K^m_{p,s-4} + \cdots + K^m_{p,s \bmod 2}) - (K_{p,s-2} + K_{p,s-4} + \cdots + K_{p,s \bmod 2})$'dir.

**İspat** $\mathbb{Z}_q + u\mathbb{Z}_q$ halkasındaki tüm ideal üreteçlerinin, $(\mathbb{Z}_q + u\mathbb{Z}_q)[x] / \langle f(x) \rangle$ halkasında da ideal üreteci olacağı açıktır. O halde yapmamız gereken 3. ve 5. tip ideallerin sayısını belirlemektir. 1., 2. ve 4. tip ideallerin sayısı $\mathbb{Z}_q + u\mathbb{Z}_q$ halkasındakilerle aynı olacaktır. Önce, her $0 \le j < i < s$ için katsayıları $p^{\min(i-j,s-i)}$'den küçük olan birimsel $v(x)$ polinomlarının sayısını bulalım. Daha sade ifadeler için $l = \min(i-j, s-i)$ diyelim. Bahsettiğimiz gibi bir $v(x) = a_0 + a_1 x + \cdots + a_{m-1} x^{m-1}$ birimsel polinomu için $(p^l)^m - \left(p^l - \phi(p^l)\right)^m = (p^m - 1)(p^m)^{l-1}$ seçenek vardır. $l$ tam sayısı; $s-j$ çift olduğunda

$1, 2, \ldots, (s-j)/2, (s-j)/2 \ldots, 2, 1$

ve $s-j$ tek olduğunda,

$1, 2, \ldots, \lfloor (s-j)/2 \rfloor - 1, \lfloor (s-j)/2 \rfloor, \lfloor (s-j)/2 \rfloor - 1, \ldots, 2, 1$

değerlerinin tümünü aldığından, sabit bir $0 \le j \le s-2$ değeri için, $s-j$ çift iken

$(p^m - 1)[(p^m)^0 + (p^m)^1 + \cdots + (p^m)^{(s-j)/2-1} + \cdots + (p^m)^1 + (p^m)^0]$

tane birimsel polinom ve $s-j$ tek iken

$(p^m - 1)[(p^m)^0 + (p^m)^1 + \cdots + (p^m)^{\lfloor (s-j)/2 \rfloor - 1} + (p^m)^{\lfloor (s-j)/2 \rfloor - 1} + \cdots + (p^m)^1 + (p^m)^0]$

tane birimsel polinom vardır. Öyleyse toplamda $(p^m - 1)K^m_{p,s-2}$ tane polinom olduğunu (bkz. Eşitlik (4.1)) görürüz. Dikkat edelim ki, $v(x)$ birimseli bir sabit ise, zaten $K_s$ içerisinde sayılmış olacağından, $\mathbb{Z}_q + u\mathbb{Z}_q$'daki üreteçlerden farklı olarak $(p^m - 1)K^m_{p,s-2} - (p-1)K_{p,s-2}$ tane 3. tip ideal vardır.

$\mathbb{Z}_q + u\mathbb{Z}_q$ halkasının 5. tip ideallerinin sayısının $K_{p,s-4} + K_{p,s-6} + \cdots + K_{p,s \bmod 2}$ olduğunu hatırlatalım. Benzer şekilde 5. tip idealleri saydığımızda da, $\mathbb{Z}_q + u\mathbb{Z}_q$'daki üreteçlerden farklı olarak $(p^m - 1)(K^m_{p,s-4} + K^m_{p,s-6} + \cdots + K^m_{p,s \bmod 2}) - (K_{p,s-4} + K_{p,s-6} + \cdots + K_{p,s \bmod 2})$ tane olduklarını görürüz. Bu da ispatımızı tamamlar.

**Örnek 4.23** $(\mathbb{Z}_{64}+u\mathbb{Z}_{64})[x]/\langle x^2+31x+63\rangle$ bölüm halkasındaki tüm ideallerin sayısı $K_6+(2^2-1)(K_{2,4}^2+K_{2,2}^2+K_{p,0}^2)-(K_{2,4}+K_{2,2}+K_{2,0})=59+3(45+9+1)-(23+7+1)$ $=193$'tür.

**Teorem 4.24** $n$ ile $p$ aralarında asal ve $x^n-1$'in $\mathbb{Z}_q+u\mathbb{Z}_q$ üzerinde temel indirgenemezlerin tek türlü çarpımına ayrılışı $x^n-1=f_1(x)f_2(x)\cdots f_r(x)$ olsun. Bu durumda $\mathbb{Z}_q+u\mathbb{Z}_q$ üzerindeki $n$ uzunluklu devirli kodların sayısı, $\mathrm{der}(f_i(x))=m_i$ olmak üzere aşağıdaki gibidir:

$$\prod_{w=1}^{r}\left(K_{p,s}-\sum_{j=1}^{\lfloor s/2\rfloor}K_{p,s-2j}+(p^{m_w}-1)\sum_{k=1}^{\lfloor s/2\rfloor}K_{p,s-2k}^{m_w}\right)$$
$$=\sum_{i=0}^{r}\left(K_{p,s}-\sum_{j=1}^{\lfloor s/2\rfloor}K_{p,s-2j}\right)^{i}\sum_{1\le k_1<\cdots<k_{r-i}\le r}\prod_{l=m_{k_1}}^{m_{k_{r-i}}}(p^l-1)\left(\sum_{t=1}^{\lfloor s/2\rfloor}K_{p,s-2t}^{l}\right)$$

**İspat** $r$ tane çarpanın her bir terimi $w$'ye bağlı olan ve olmayan terimlerin toplamıdır. Dolayısıyla bu çarpım, binom açılımında olduğu gibi, her bir çarpandan bir toplam seçmek ve bunların çarpımlarını toplamaktır. Bunlardan $0\le i\le r$ tane $w$'ye bağlı olmayan terimi seçtiğimizde

$$\left(K_{p,s}-\sum_{j=1}^{\lfloor s/2\rfloor}K_{p,s-2j}\right)^{i}$$

elde edilirken, geriye kalan $r-i$ terim, $w$'ye bağlı olanların içinden olası tüm $r-i$'lilerin çarpımlarının toplamı olarak

$$\sum_{1\le k_1<\cdots<k_{r-i}\le r}\prod_{l=m_{k_1}}^{m_{k_{r-i}}}(p^l-1)\left(\sum_{t=1}^{\lfloor s/2\rfloor}K_{p,s-2t}^{l}\right)$$

biçiminde seçilir. Öyleyse sonuç, her bir $0\le i\le r$ için bu terimlerin çarpımlarının toplamıdır.

**Örnek 4.25** $\mathbb{Z}_8+u\mathbb{Z}_8$ üzerinde $7$ uzunluğundaki devirli kodların sayısını bulalım:

$$\prod_{i=1}^{r}\left(K_{2,3}-K_{2,1}+(2^{m_i}-1)K_{2,1}^{m_i}\right)=\left(K_{2,3}-K_{2,1}+K_{2,1}^{1}\right)\left(K_{2,3}-K_{2,1}+(2^3-1)K_{2,1}^{3}\right)^2=12493$$

## 4.4 $\mathbb{Z}_{p^2}+u\mathbb{Z}_{p^2}$ Halkası Üzerinde Bir Kod Ailesi

Şimdi $\mathbb{Z}_{p^2}+u\mathbb{Z}_{p^2}$ halkası üzerinde özel bir kod ailesinin üreteçlerini tek türlü olarak belirleyeceğiz ve eleman sayılarını bulacağız.

**Teorem 4.26** $n$ ile $p$ aralarında asal olsun. $I_i$'ler Lemma 4.20'de verilen formda idealler olsun ve eğer içlerinde 3. tipte ve 5. tipte olanlar varsa $v(x)=1$ alınsın. Bu durumda, $(\mathbb{Z}_{p^2}+u\mathbb{Z}_{p^2})[x]\big/\langle x^n-1\rangle$ bölüm halkasının $I=I_1\oplus I_2\oplus\cdots\oplus I_r$ şeklindeki bir ideali, $\mathbb{Z}_{p^2}+u\mathbb{Z}_{p^2}$ üzerindeki $g_1g_2\cdots g_r=x^n-1$ eşitliğini sağlayan $g_1,g_2,\ldots,g_r$ polinomları ile tek türlü olarak aşağıdaki gibi belirlenir

$$I=\langle g_1g_3\cdots g_r, ug_1g_2g_4\cdots g_{p+4}, pg_1g_2g_3g_5\cdots g_{p+4}, (p+u)g_1\cdots g_4g_6\cdots g_r,$$
$$(2p+u)g_1\cdots g_5g_7\cdots g_r,\ldots,((p-1)p+u)g_1\cdots g_{p+2}g_{p+4}g_r, pug_1\cdots g_{p+3}g_r\rangle$$

ve bu idealin eleman sayısı

$$|I|=\frac{(p^4)^{der(g_2)}(p^2)^{der(g_3g_r)+der(g_4g_r)+der(g_5)+der(g_6)+\cdots+der(g_{p+3})}p^{der(g_{p+4})}}{p^{der(g_r)}}$$ dir.

**İspat** $x^n-1$'in tek türlü temel indirgenemez çarpanlarına ayrılışı $f_1(x)f_2(x)\cdots f_r(x)$ olsun. Bu durumda Lemma 4.19'da gösterdiğimiz gibi aşağıdaki izomorfizmayı elde ederiz:

$$(\mathbb{Z}_{p^2}+u\mathbb{Z}_{p^2})[x]/\langle x^n-1\rangle\cong\langle\hat{f}_1+\langle x^n-1\rangle\rangle\oplus\langle\hat{f}_2+\langle x^n-1\rangle\rangle\oplus\cdots\oplus\langle\hat{f}_r+\langle x^n-1\rangle\rangle.$$

Burada, $\mathbb{Z}_{p^2}+u\mathbb{Z}_{p^2}$ halkasının Şekil 4.5'de verilen ideal yapısını göz önünde bulundursak, $f_1(x),f_2(x),\ldots,f_r(x)$ polinomlarını uygun şekilde yeniden sıralayarak, Sonuç 4.21'den, $I$ idealinin aşağıdaki gibi olduğunu kabul edebiliriz:

$$I = \langle \hat{f}_{k_1+1} \rangle + \cdots + \langle \hat{f}_{k_2} \rangle + \langle u\hat{f}_{k_2+1} \rangle + \cdots + \langle u\hat{f}_{k_3} \rangle + \langle p\hat{f}_{k_3+1} \rangle + \cdots + \langle p\hat{f}_{k_4} \rangle$$
$$+\langle (p+u)\hat{f}_{k_4+1} \rangle + \cdots + \langle (p+u)\hat{f}_{k_5} \rangle + \langle (2p+u)\hat{f}_{k_5+1} \rangle + \cdots + \langle (2p+u)\hat{f}_{k_6} \rangle$$
$$\vdots$$
$$+\langle ((p-1)p+u)\hat{f}_{k_{p+2}+1} \rangle + \cdots + \langle ((p-1)p+u)\hat{f}_{k_{p+3}} \rangle + \langle pu\hat{f}_{k_{p+3}+1} \rangle + \cdots + \langle pu\hat{f}_{k_{p+4}} \rangle$$
$$+\langle p\hat{f}_{k_{p+4}+1}, u\hat{f}_{k_{p+4}+1} \rangle + \cdots + \langle p\hat{f}_r, u\hat{f}_r \rangle$$

$$= \langle \hat{f}_{k_1+1} \rangle + \cdots + \langle \hat{f}_{k_2} \rangle + \langle u\hat{f}_{k_2+1} \rangle + \cdots + \langle u\hat{f}_{k_3} \rangle + \langle u\hat{f}_{k_{p+4}+1} \rangle + \cdots + \langle u\hat{f}_r \rangle$$
$$+\langle p\hat{f}_{k_3+1} \rangle + \cdots + \langle p\hat{f}_{k_4} \rangle + \langle p\hat{f}_{k_{p+4}+1} \rangle + \cdots + \langle p\hat{f}_r \rangle + \langle (p+u)\hat{f}_{k_4+1} \rangle + \cdots$$
$$+\langle (p+u)\hat{f}_{k_5} \rangle + \cdots + \langle (2p+u)\hat{f}_{k_5+1} \rangle + \cdots + \langle (2p+u)\hat{f}_{k_6} \rangle$$
$$\vdots$$
$$+\langle ((p-1)p+u)\hat{f}_{k_{p+2}+1} \rangle + \cdots + \langle ((p-1)p+u)\hat{f}_{k_{p+3}} \rangle + \langle pu\hat{f}_{k_{p+3}+1} \rangle \cdots + \langle pu\hat{f}_{k_{p+4}} \rangle.$$

Bu durumda

$$I = \langle f_1 \cdots f_{k_1} f_{k_2+1} \cdots f_r, uf_1 \cdots f_{k_2} f_{k_3+1} \cdots f_{k_{p+4}}, pf_1 \cdots f_{k_3} f_{k_4+1} \cdots f_{k_p+4}, (p+u)f_1 \cdots f_{k_4} f_{k_5+1} \cdots f_r$$
$$, (2p+u)f_1 \cdots f_{k_5} f_{k_6+1} \cdots f_r, \ldots, ((p-1)p+u)f_1 \cdots f_{k_{p+2}} f_{k_3+1} \cdots f_r, puf_1 \cdots f_{k_{p+3}} f_{k_{p+4}+1} \cdots f_r \rangle$$

eşitliğini elde ederiz. Şimdi $g_1 = f_1 \cdots f_{k_1}$, $2 \le m \le p+4$ iken $g_m = f_{k_{m-1}+1} \cdots f_{k_m}$ ve de $g_r = f_{k_{p+4}+1} \cdots f_r$ diyelim. Doğal olarak $k_1 = 0$ iken $g_1 = 1$, $k_m = k_{m-1}$ iken $g_m = 1$ ve de $r = k_{p+4} + 1$ olduğunda da $g_r = 1$ olarak tanımlayalım. Bu durumda

$$I = \langle g_1 g_3 \cdots g_r, ug_1 g_2 g_4 \cdots g_{p+4}, pg_1 g_2 g_3 g_5 \cdots g_{p+4}, (p+u)g_1 \cdots g_4 g_6 \cdots g_r,$$
$$(2p+u)g_1 \cdots g_5 g_7 \cdots g_r, \ldots, ((p-1)p+u)g_1 \cdots g_{p+2} g_{p+4} g_r, pug_1 \cdots g_{p+3} g_r \rangle$$

olduğunu görürüz. Son olarak, $p^4$ elemanlı $\mathbb{Z}_{p^2} + u\mathbb{Z}_{p^2}$ halkasındaki ideallerin eleman sayıları (bkz. Şekil 4.5)

$|\langle p \rangle| = |\langle p+u \rangle| = |\langle 2p+u \rangle| = \cdots = |\langle (p-1)p+u \rangle| = |\langle u \rangle| = p^2$ ve $|\langle pu \rangle| = p$ ' dir. Ayrıca

$$\langle pg_1 g_2 g_3 g_5 \cdots g_{p+4} \rangle \cap \langle ug_1 g_2 g_4 \cdots g_{p+4} \rangle = \langle pug_1 \cdots g_{p+4} \rangle$$

olduğuna ve $I$ 'nın üreteçlerinin tek başına üreteceği esas ideallerden, yukarıda arakesitlerini verdiğimiz ideallerden başka herhangi iki tanesinin arakesitinin aşikar olduğuna dikkat edelim.

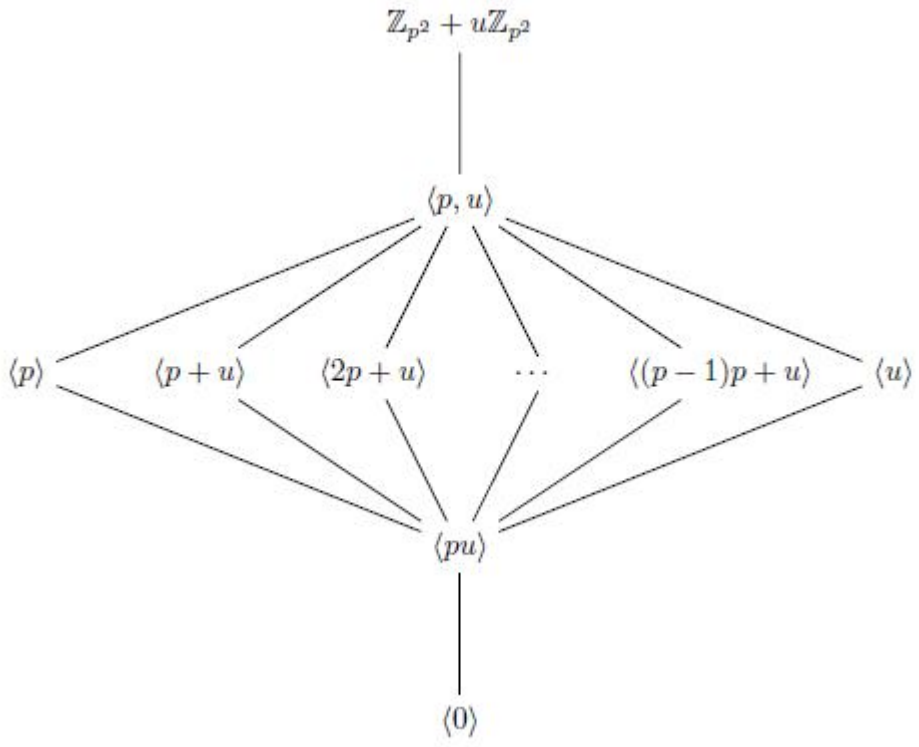
O halde,

$$|I| = \frac{|\langle g_1 g_3 \cdots g_r \rangle| \; |\langle u g_1 g_2 g_4 \cdots g_{p+4} \rangle| \; |\langle p g_1 g_2 g_3 g_5 \cdots g_{p+4} \rangle| \; |\langle pu g_1 \cdots g_{p+3} g_r \rangle|}{|\langle pu g_1 \cdots g_{p+4} \rangle|}$$

$$\times |\langle (p+u) g_1 g_2 g_3 g_4 g_6 \cdots g_r \rangle| \cdots |\langle ((p-1)p+u) g_1 \cdots g_{p+2} g_{p+4} g_r \rangle|$$

$$= \frac{(p^4)^{der(g_2)} (p^2)^{der(g_3 g_r)+der(g_4 g_r)+der(g_5)+der(g_6)+\cdots+der(g_{p+3})} p^{der(g_{p+4})}}{p^{der(g_r)}}$$

sonucuna varırız.




Şekil 4. 5 $\mathbb{Z}_{p^2} + u\mathbb{Z}_{p^2}$ halkasının idealleri için Hasse diyagramı

**Sonuç 4.27** $n$ ile $p$ aralarında asal ve $i = 1, 2, \ldots, r$ için $f_i$'ler $x^n - 1$'in monik bölenleri olsun. Bu durumda $(\mathbb{Z}_{p^2} + u\mathbb{Z}_{p^2})[x] / \langle x^n - 1 \rangle$'in, Teorem 4.26'da verilen tüm idealleri, $i = 1, 2, \ldots, p+3$ için $f_i \mid f_0$ ve $j = 0, 1, 2, 4, \ldots, p+4$ için $f_3 \mid f_j$ olmak üzere $I = \langle f_0, uf_1, pf_2, puf_3, (p+u)f_4, \ldots, ((p-1)p+u)f_{p+3} \rangle$ formundadır.

**İspat** Önce $\langle g_1 g_3 \cdots g_r, u g_1 g_2 g_4 \cdots g_{p+4} \rangle = \langle g_1 g_3 \cdots g_r, u g_1 g_4 \cdots g_{p+4} \rangle$ eşitliğini gösterelim. $\langle g_1 g_3 \cdots g_r, u g_1 g_2 g_4 \cdots g_{p+4} \rangle \subseteq \langle g_1 g_3 \cdots g_r, u g_1 g_4 \cdots g_{p+4} \rangle$ kapsaması açıkça görülebilir. O halde $u g_1 g_4 \cdots g_{p+4} \in \langle g_1 g_3 \cdots g_r, u g_1 g_2 g_4 \cdots g_{p+4} \rangle$ olduğunu göstermemiz yeterli olacaktır. $g_3 g_r$ ve $g_2$ polinomları aralarında asal oldukları için

$ug_1g_4\cdots g_{p+4}a(g_3g_r)+ug_1g_4\cdots g_{p+4}(bg_2)=ug_1g_4\cdots g_{p+4}$ eşitliğini sağlayacak olan $a,b\in(\mathbb{Z}_{p^2}+u\mathbb{Z}_{p^2})[x]$ polinomları bulunabilir. Bu durumda eşitliğin her iki tarafını $ug_1g_4\cdots g_{p+4}$ ile çarparak

$$ug_1g_4\cdots g_{p+4}a(g_3g_r)+ug_1g_4\cdots g_{p+4}(bg_2)=ug_1g_4\cdots g_{p+4}$$

eşitliğini elde ederiz ki buradan da

$$\langle g_1g_3\cdots g_r,ug_1g_2g_4\cdots g_{p+4}\rangle=\langle g_1g_3\cdots g_r,ug_1g_4\cdots g_{p+4}\rangle$$

eşitliği elde edilir. İzlediğimiz metodu, $I$'nın diğer üreteçleri için de kullanarak, $I$ idealini

$$I=\langle g_1g_3\cdots g_r,ug_1g_4\cdots g_{p+4},pg_1g_3g_5\cdots g_{p+4},pug_1g_{p+4},$$
$$(p+u)g_1g_3g_4g_6\cdots g_r,\ldots,((p-1)p+u)g_1g_3\cdots g_{p+2}g_{p+4}g_r\rangle$$

formuna getirebiliriz. Son olarak, üreteçteki polinomları yeniden adlandırırsak $i=1,2,\ldots,p+3$ için $f_i\mid f_0$ ve $j=0,1,2,4,\ldots,p+4$ için $f_3\mid f_j$ olmak üzere

$$I=\langle f_0,uf_1,pf_2,puf_3,(p+u)f_4,\ldots,((p-1)p+u)f_{p+3}\rangle$$

sonucuna varırız.

## 4.5 $\mathbb{Z}_{p^2}+u\mathbb{Z}_{p^2}$ Halkası Üzerindeki Kod Ailesinin Dual Kodları

**Tanım 4.28** $C$, $\mathbb{Z}_{p^2}+u\mathbb{Z}_{p^2}$ halkası üzerinde bir lineer kod olsun. Bu takdirde $C$'nin dual kodu

$$C^{\perp}=\{x\in(\mathbb{Z}_{p^2}+u\mathbb{Z}_{p^2})^n\mid \text{bütün } c\in C \text{ kodsözleri için } x\cdot c=0\}$$

olarak tanımlanır.

**Tanım 4.29** Bir $C$, $\mathbb{Z}_{p^2}+u\mathbb{Z}_{p^2}$-lineer kodu için eğer $C\subseteq C^{\perp}$ ise $C$ koduna kendine dik (self orthogonal) ve eğer $C=C^{\perp}$ ise $C$ koduna kendine dual (self dual) kod denir.

**Tanım 4.30** $\mathbb{Z}_{p^2}+u\mathbb{Z}_{p^2}$ halkası üzerindeki, derecesi $k$ olan bir $h(x)=\sum_{i=0}^{k}a_ix^i$ ($a_k\neq 0$) polinomunun "reciprocal" polinomu

$$\tilde{h}(x)=\sum_{i=0}^{k} a_{k-i}x^{i}$$

olarak tanımlanır.

**Teorem 4.31**

$$C=\langle g_1g_3\cdots g_r, ug_1g_2g_4\cdots g_{p+4}, pg_1g_2g_3g_5\cdots g_{p+4}, (p+u)g_1\cdots g_4g_6\cdots g_r,$$
$$(2p+u)g_1\cdots g_5g_7\cdots g_r,\ldots,((p-1)p+u)g_1\cdots g_{p+2}g_{p+4}g_r, pug_1\cdots g_{p+3}g_r\rangle$$

$(p,n)=1$ olmak üzere $n$ uzunluğunda bir $\mathbb{Z}_{p^2}+u\mathbb{Z}_{p^2}$-lineer kod ve $g_1,g_2,\ldots,g_r$ monik polinomları $\mathbb{Z}_{p^2}+u\mathbb{Z}_{p^2}$ üzerinde $x^n-1$'in çarpanları olsun. Bu takdirde $C$'nin dual kodu da $\mathbb{Z}_{p^2}+u\mathbb{Z}_{p^2}$ üzerinde bir devirli koddur ve şu şekilde üretilir

$$C^{\perp}=\langle\tilde{g}_2\tilde{g}_3\cdots\tilde{g}_r, u\tilde{g}_1\tilde{g}_2\tilde{g}_4\cdots\tilde{g}_{p+3}\tilde{g}_r, p\tilde{g}_1\tilde{g}_2\tilde{g}_3\tilde{g}_5\cdots\tilde{g}_{p+3}\tilde{g}_r, (p+u)\tilde{g}_1\cdots\tilde{g}_{p+2}\tilde{g}_{p+4}\cdots\tilde{g}_r$$
$$,(2p+u)\tilde{g}_1\cdots\tilde{g}_{p+1}\tilde{g}_{p+3}\cdots\tilde{g}_r,\ldots,((p-1)p+u)\tilde{g}_1\cdots\tilde{g}_4\tilde{g}_6\cdots\tilde{g}_r, pu\tilde{g}_1\tilde{g}_2\cdots\tilde{g}_{p+4}\rangle$$

ve bu kodun eleman sayısı

$$|C^{\perp}|=\frac{(p^4)^{der(g_1)}(p^2)^{der(g_4g_{p+4})+der(g_3g_{p+4})+der(g_{p+3})+der(g_{p+2})+\cdots+der(g_5)}p^{der(g_r)}}{p^{der(g_{p+4})}}$$

olur.

**İspat** Tam ve uzun bir ispat yerine taslağını vereceğiz. Tanım gereği $C^{\perp}$'in de bir $\mathbb{Z}_{p^2}+u\mathbb{Z}_{p^2}-$devirli kod olduğu kolaylıkla görülebilir. Yine, klasik bir metotla $\langle g_1\rangle^{\perp}=\langle\tilde{g}_2\tilde{g}_3\cdots\tilde{g}_r\rangle$ olduğu kolayca gösterilebilir [3,29]. Üstelik $C\subseteq\langle g_1\rangle$ kapsamasından dolayı $\langle\tilde{g}_2\tilde{g}_3\cdots\tilde{g}_r\rangle\subseteq C^{\perp}$ kapsamasını elde ederiz. Ayrıca $\langle p\tilde{g}_1\tilde{g}_2\tilde{g}_3\tilde{g}_5\cdots\tilde{g}_{p+3}\tilde{g}_r\rangle\subseteq\langle\tilde{g}_2\rangle=\langle g_1g_3\cdots g_r\rangle^{\perp}$ içermesine dikkat edelim. Yine $\langle p\tilde{g}_1\tilde{g}_2\tilde{g}_3\tilde{g}_5\cdots\tilde{g}_{p+3}\tilde{g}_r\rangle\subseteq\langle\tilde{g}_3\tilde{g}_r\rangle=\langle g_1g_2g_4\cdots g_{p+4}\rangle^{\perp}\subseteq\langle ug_1g_2g_4\cdots g_{p+4}\rangle^{\perp}$ olduğunu görüyoruz. Benzer şekilde $x^n-1=g_1g_2\cdots g_{p+4}g_r$ eşitliğini göz önünde bulundursak $\langle p\tilde{g}_1\tilde{g}_2\tilde{g}_3\tilde{g}_5\cdots\tilde{g}_{p+3}\tilde{g}_r\rangle,\langle(p+u)\tilde{g}_1\cdots\tilde{g}_{p+2}\tilde{g}_{p+4}\cdots\tilde{g}_r\rangle,\ldots,\langle((p-1)p+u)\tilde{g}_1\cdots\tilde{g}_4\tilde{g}_6\cdots\tilde{g}_r\rangle$ ve $\langle pu\tilde{g}_1\tilde{g}_2\cdots\tilde{g}_{p+4}\rangle$ ideallerinin tümü $C^{\perp}$'in alt kümesi olacaktır. Bu koddaki kodsözlerin sayısnı ise,

$$|C^{\perp}|=\frac{(p^4)^{der(g_1)}(p^2)^{der(g_4g_{p+4})+der(g_3g_{p+4})+der(g_{p+3})+der(g_{p+2})+\cdots+der(g_5)}p^{der(g_r)}}{p^{der(g_{p+4})}}$$

olarak buluruz. Teorem 4.26'dan

$$|C|=\frac{(p^4)^{der(g_2)}(p^2)^{der(g_3g_r)+der(g_4g_r)+der(g_5)+der(g_6)+\cdots+der(g_{p+3})}p^{der(g_{p+4})}}{p^{der(g_r)}}$$

olduğunu biliyoruz. O halde $|C||C^{\perp}|=(p^4)^n=|(\mathbb{Z}_{p^2}+u\mathbb{Z}_{p^2})^n|$. Bu durumda

$$C^{\perp}=\langle \tilde{g}_2\tilde{g}_3\cdots\tilde{g}_r, u\tilde{g}_1\tilde{g}_2\tilde{g}_4\cdots\tilde{g}_{p+3}\tilde{g}_r, p\tilde{g}_1\tilde{g}_2\tilde{g}_3\tilde{g}_5\cdots\tilde{g}_{p+3}\tilde{g}_r, (p+u)\tilde{g}_1\cdots\tilde{g}_{p+2}\tilde{g}_{p+4}\cdots\tilde{g}_r,$$
$$(2p+u)\tilde{g}_1\cdots\tilde{g}_{p+1}\tilde{g}_{p+3}\cdots\tilde{g}_r,\ldots,((p-1)p+u)\tilde{g}_1\cdots\tilde{g}_4\tilde{g}_6\cdots\tilde{g}_r, pu\tilde{g}_1\tilde{g}_2\cdots\tilde{g}_{p+4}\rangle$$

eşitliğini göstermiş oluruz.

# BÖLÜM 5

## SONUÇ VE ÖNERİLER

Bu tezde öncelikle, $p$ bir asal sayı ve $s$ pozitif bir tam sayı iken $q = p^s$ ve $u^2 = 0$ olmak üzere $\mathbb{Z}_q + u\mathbb{Z}_q$ halkasının bütün ideallerini belirledik. Ayrıca bu ideallerin sayısını bulan bir formül verdik. Daha sonra, bu halka üzerindeki devirli kodları belirlemek amacıyla $(\mathbb{Z}_q + u\mathbb{Z}_q)[x]/\langle x^n - 1\rangle$ bölüm halkasının ideallerini belirledik ve yine bu ideallerin sayısını veren bir formül bulduk. $\mathbb{Z}_q + u\mathbb{Z}_q$ halkası üzerindeki devirli kodlarla $(\mathbb{Z}_q + u\mathbb{Z}_q)[x]/\langle x^n - 1\rangle$ halkasının idealleri arasında bire bir eşleme olmasına karşın, bu ideallerin belirlenmesi şimdiye dek gerçekleştirilememişti. $\mathbb{Z}_4 + u\mathbb{Z}_4$ durumunun genel hali olan $\mathbb{Z}_{p^2} + u\mathbb{Z}_{p^2}$ halkası üzerindeki devirli kodların yapılarını ve bu kodların eleman sayılarını belirledik. Ayrca bu kodların duallerini ve bu dual kodların eleman sayılarını da belirledik. Bu zengin ideal yapısı sayesinde elde edilen devirli kodların, Gray fonksiyonu yardımıyla bilinen halkalar üzerine görüntülerinin alınmasıyla iyi parametrelere sahip kodların elde edilebileceğini öngörmekteyiz.

## KAYNAKLAR


[1] Shannon, C. E. (1948). "A mathematical theory of communication", Bell Syst. Tech. J., 27: 623-656.

[2] Ling, S. ve Xing, C. (2004). Coding theory: a first course, Cambridge University Press, New York.

[3] Prange, E. (1962). "The use of information sets in decoding cyclic codes", IRE Transactions on Information Theory, 8(5): 5-9.

[4] Hammons, A. R., Kumar, P. V., Calderbank, A. R., Sloane, N. J. ve Solé, P. (1994). "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes", IEEE Transactions on Information Theory, 40(2): 301-319.

[5] Nordstrom, A. W. ve Robinson, J. P. (1967). "An optimum nonlinear code", Information and Control, 11(5-6): 613-616.

[6] Kerdock, A. M. (1972). "A class of low-rate nonlinear binary codes", Information and control, 20(2): 182-187.

[7] Preparata, F. P. (1968), A class of optimum nonlinear double-error-correcting codes, Coordinated Science Laboratory Report no. R-389, https://www.ideals.illinois.edu/bitstream/handle/2142/74662/B6-389.pdf?sequence=2, 10 Nisan 2018.

[8] Goethals, J. M. (1974). "Two dual families of nonlinear binary codes", Electronics Letters, 10(23): 471-472.

[9] Delsarte, P. ve Goethals, J. M. (1975). "Alternating bilinear forms over $GF(q)$", Journal of Combinatorial Theory, Series A, 19(1): 26-50.

[10] Calderbank, A. R. ve Sloane, N. J. (1995). "Modular andp-adic cyclic codes", Designs, codes and Cryptography, 6(1): 21-35.

[11] Pless, V. ve Qian, Z. (1995). "Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$" IEEE Transactions on Information Theory, 42(5): 1594-1600.

[12] Pless, V., Solé, P. ve Qian, Z. (1997). "Cyclic Self-DualZ4-Codes", Finite fields and their applications, 3(1): 48-69.

[13] Bonnecaze, A. ve Udaya, P. (1999). "Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$" IEEE Transactions on Information Theory, 45(4): 1250-1255.

[14] Siap, I. (2002). "Linear codes over $\mathbb{F}_2 + u\mathbb{F}_2$ and their complete weight enumerators", In Codes and Designs, 10: 259-271.

[15] Qian, J. F., Zhang, L. N. ve Zhu, S. X. (2005). "Cyclic codes over $\mathbb{F}_p + u\mathbb{F}_p + \cdots + u^{k-1}\mathbb{F}_p$", IEICE transactions on fundamentals of electronics, communications and computer science, 88(3): 795-797.

[16] Abualrub, T. ve Siap, I. (2007). "Cyclic codes over the rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$", Designs, Codes and Cryptography, 42(3): 273-287.

[17] Ozen, M. ve Siap, I. (2006). "Linear Codes over $\mathbb{F}_q[u]/(u^s)$ with Respect to the Rosenbloom–Tsfasman Metric", Designs, Codes and Cryptography, 38(1): 17-29.

[18] Zhu, S. X., Wang, Y. ve Shi, M. J. (2010). "Some Results on Cyclic Codes Over $\mathbb{F}_2 + v\mathbb{F}_2$", IEEE Transactions on Information Theory, 56(4): 1680-1684.

[19] Kai, X., Zhu, S. ve Li, P. (2010). "(1+ λu)-Constacyclic codes over $\mathbb{F}_p[u]/ < u^m >$", Journal of the Franklin Institute, 347(5): 751-762.

[20] Mohammed, A. A. (2011). "Cyclic codes over $Z_2 + uZ_2 + u^2Z_2 + \cdots + u^{k-1}Z_2$", Turkish Journal of Mathematics, 35(4): 737-749.

[21] Siap, I., Abualrub, T. ve Yildiz, B. (2012). "One generator quasi-cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$", Journal of the Franklin Institute, 349(1): 284-292.

[22] Yildiz, B. ve Karadeniz, S. (2011). "Cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$", Designs, Codes and Cryptography, 58(3): 221-234.

[23] Yildiz, B. ve Aydin, N. (2014). "On cyclic codes over $\mathbb{Z}4+ u\mathbb{Z}4$ and their $\mathbb{Z}4$–images", International Journal of Information and Coding Theory, 2(4): 226-237.

[24] Gao, J., Fu, F. W., Xiao, L. ve Bandi, R. K. (2015). "Some results on cyclic codes over $\mathbb{Z}q+ u\mathbb{Z}q$", Discrete Mathematics, Algorithms and Applications, 7(4): 1550058-1:1550058-8.

[25] Fraleigh, J. B. (2003). A First Course in Abstract Algebra, Seventh Edition, Pearson Education India.

[26] Nesin, A. (2014). Temel grup teorisi, Nesin Yayınevi.

[27] Leon, S. J., Bica, I. ve Hohn, T. (1980). Linear Algebra with Applications, Seventh Edition, Macmillan, New York.

[28] Huffman, W. C. ve Pless, V. (2010), Fundamentals of Error-Correcting Codes, Cambridge University Press, New York.

[29] Wan, Z. X., (1997). Quaternary codes, World Scientific Publishing, Singapore.

[30] The International ISBN Agency, ISBN Bar Coding, https://www.isbn-international.org/content/what-isbn, 20 Nisan 2018.

[31] Dummit, D. S. ve Foote, R. M. (2004). Abstract Algebra, Third Edition, Wiley, New Jersey.

[32] J. W. Layman, (2000), A053599, The On-Line Encyclopedia of Integer Sequences, http://oeis.org/A053599, 20 Mayıs 2018.

[33] McDonald, B. R. (1974). Finite Rings With Identity, Marcel Dekker Incorporated, California.

[34] Hungerford, T. W. (1980). Algebra, Springer, New York.

# ÖZGEÇMİŞ

**KİŞİSEL BİLGİLER**

**Adı Soyadı** : Fatih TEMİZ

**Doğum Tarihi ve Yeri** : Erbaa, 1986

**Yabancı Dili** : İngilizce

**E-posta** : temizf@gmail.com

**ÖĞRENİM DURUMU**

| **Derece** | **Alan** | **Okul/Üniversite** | **Mezuniyet Yılı** |
|---|---|---|---|
| Yüksek Lisans | Matematik | Yıldız Teknik Üniversitesi | 2012 |
| Lisans | Matematik (İng) | Dokuz Eylül Üniversitesi | 2010 |
| Lise | Fen Bilimleri | Yılmaz Kayalar Anadolu Lisesi | 2004 |

**İŞ TECRÜBESİ**

| **Yıl** | **Kurum** | **Görevi** |
|---|---|---|
| 2011-2018 | Yıldız Teknik Üniversitesi | Araştırma Görevlisi |

**YAYINLARI**

**Makale**

**1.** Temiz, F., Şiap, İ., ve Akin, H., (2014). "On Pseudo Random Bit Generators via Two-Dimensional Hybrid Cellular Automata", Acta Physica Polonica A, 125(2): 534-537.

**2.** Temiz, F., ve Şiap, V., (2013). "Linear block and array codes correcting repeated CT burst errors", Albanian Journal of Mathematics, 7(2): 77-92.

**3.** Temiz F., Şiap İ., Akın H. ve Köroğlu M. E., (2012). "A Family of Two Dimensional Hybrid Cellular Automata and Its Applications to Pseudo Random Number Generators", Global Journal on Technology, 1: 1649-1655.

**4.** Köroğlu M. E., Şiap İ., Akın H. ve Temiz F., (2012). "Hybrid quadratic cellular automata and its applications to Pseudo random number generators", Global Journal on Technology, 1:1166-1171

**Bildiri**

**1.** Temiz, F. ve Özkan, E.M., (2018). "Structure of Cyclic Codes over Zq+uZq and Some Special Family of Them", International Conference on Mathematics and Mathematics Education, 27-29 Haziran 2018, Ordu.

**2.** Temiz, F. ve Özkan, E.M., (2017). "On Ideals of the ring $\mathbb{Z}_{p^s}+u\mathbb{Z}_{p^s}$", International Congress on Fundamental and Applied Sciences, 21-25 Ağustos 2017, Saraybosna.

**3.** Temiz F. ve Şiap İ., (2016). "On Cyclic Codes over $\mathbb{Z}_q+u\mathbb{Z}_q$", 16$^{th}$ International Conference Computational and Mathematical Methods in Science and Engineering, 4-7 Temmuz 2016, Cadiz.

**4.** Temiz F. ve Şiap V., (2014). "2-Repeated CT Burst Error Correcting Array Codes with respect to the Euclidean Weight", Karatekin Mathematics Days, 11-13 Haziran 2014, Çankırı.

**5.** Temiz F. ve Şiap V., (2012). "Homogenous metric block codes with respect to CT burst errors", International Congress in Honour of Professor Hari M. Srivastava, 23 - 26 Ağustos 2012, Bursa.

**6.** Temiz F. ve Şiap V., (2012). “Perfect codes in the Euclidean metric”, 1st International Eurasian Conference on Mathematics Sciences and Applications, 3-7 Eylül 2012, Prishtine.

**7.** Temiz F. ve Şiap V., (2012). “Bursts in Homogenous metric block codes”, International Conference on Applied Analysis and Algebra, 20-24 Haziran 2012, İstanbul.

**8.** Temiz F., Şiap İ., Akın H. ve Köroğlu M.E., (2011). “A Family of Two Dimensional Hybrid Cellular Automata and Its Applications to Pseudo Random Number Generators”, 2nd World Conference on Information Technology, 22-27Kasım 2011, Antalya.

**9.** Köroğlu M.E., Şiap İ., Akın H. ve Temiz F., (2011). “Hybrid Quadratic Cellular Automata and Its Applications to Pseudo Random Number Generators", 2nd World Conference on Information Technology, 22-27Kasım 2011, Antalya.

**Proje**

**1.** Yıldız Teknik Üniversitesi Bilimsel Araştırma Projeleri Koordinatörlüğü (FDK-2017-3037) Bazı Halkalar Üzerinde Tanımlı Altmodül Kodları (Araştırmacı)

**2.** Sır paylaşım Sistemleri Üzerine Bazı Çalışmalar, TÜBİTAK PROJESİ No: 114F388 (Bursiyer)