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

# DEĞİŞMELİ OLMAYAN HALKALAR ÜZERİNDE TANIMLI DEVİRLİ KODLAR

**FATMANUR GÜRSOY**

**YÜKSEK LİSANS TEZİ**
**MATEMATİK ANABİLİM DALI**

**DANIŞMAN**
**PROF. DR. İRFAN ŞİAP**
**EŞ DANIŞMAN DOÇ. DR. BAHATTİN YILDIZ**

**İSTANBUL, 2013**

Bu çalışma, TÜBİTAK BİDEB 2210 Burs Programı ve Yıldız Teknik Üniversitesi Bilimsel Araştırma Projeleri Koordinatörlüğü'nün 2012-01-03-YL01 numaralı projesi ile desteklenmiştir.

# ÖNSÖZ

Tez çalışmamın her aşamasında yakın ilgi ve desteğini gördüğüm; çalışmalarımın yönlendirilmesi ve sonuçlandırılmasında büyük emeği geçen saygıdeğer hocalarım Prof. Dr. İrfan ŞİAP ve Doç. Dr. Bahattin YILDIZ'a en içten teşekkürlerimi sunarım.

Değerli jüri üyeleri Prof. Dr. Fethi ÇALLIALP, Doç. Dr. Ünsal TEKİR ve Doç. Dr. Bayram Ali ERSOY'a fikir ve önerileriyle bu teze katkılarından ötürü ayrıca teşekkürlerimi sunarım.

Hayatım boyunca her konuda maddi ve manevi desteklerini esirgemeyen kıymetli anneme, babama ve kardeşlerime sonsuz teşekkürler.

Çalışmalarım sırasında bilgisayar programlama hususunda yardımlarından ötürü değerli arkadaşım Arş. Gör. Elif Segah ÖZTAŞ'a ve maddi manevi destekçim olan tüm arkadaşlarıma da ayrıca teşekkürler.

Son olarak tez süresince maddi destek sağlayan TÜBİTAK-Bilim İnsanı Destekleme Daire Başkanlığı'na ve Yıldız Teknik Üniversitesi BAP Birimi'ne teşekkür ederim.

Haziran, 2013

Fatmanur GÜRSOY

# İÇİNDEKİLER

Sayfa

## SİMGE LİSTESİ

| | |
|---|---|
| $F$ | Cisim |
| $M$ | Modül |
| $\mathbb{Z}$ | Tamsayılar kümesi |
| $\mathbb{Z}_p$ | Tamsayıların $\bmod p$ ye göre kalan sınıflarının kümesi |
| $F_q$ | $q$ elemanlı cisim |
| $Ann(M)$ | $M$ Modülünün sıfırlayıcısı |
| $A \cong B$ | $A$ ve $B$ kümeleri izomorftur. |
| $V$ | $F_q$ üzerinde tanımlı vektör uzayı |
| $F_q^n$ | Bileşenleri $F_q$ cisminin elemanı olan $n$ uzunluğundaki vektörlerin kümesi |
| $F^n$ | $F$'nin kendisi ile $n$ defa kartezyen çarpım kümesi |
| $\langle S \rangle$ | $S$ kümesi ile üretilen alt uzay |
| $boy(V)$ | $V$ vektör uzayının boyutu |
| $\langle \mathbf{u}, \mathbf{v} \rangle$ | $\mathbf{u}$ ile $\mathbf{v}$ vektörlerinin iç çarpımı |
| $S^{\perp}$ | $S$ kümesinin dik'i |
| $\lvert C \rvert$ | $C$ kodunun eleman sayısı |
| $C^{\perp}$ | $C$ kodunun duali |
| $wt(x)$ | $x$'in Hamming ağırlığı |
| $wt(C)$ | $C$ kodunun minimum Hamming ağırlığı |
| $d(x, y)$ | $x$ ile $y$ arasındaki Hamming uzaklığı |
| $d(C)$ | $C$ kodunun minimum Hamming uzaklığı |
| $(n, \mathrm{M})$ | $n$ uzunluğunda $\mathrm{M}$ elemanlı bir kod |
| $(n, \mathrm{M}, d)$ | $n$ uzunluğunda $\mathrm{M}$ elemanlı, $d$ minimum uzaklığına sahip kod |
| $[n, k]_q$ | $F_q$ üzerinde $n$ uzunluğunda boyutu $k$ olan lineer kod |
| $[n, k, d]_q$ | $F_q$ üzerinde $n$ uzunluğunda boyutu $k$ ve minimum uzaklığı $d$ olan lineer kod |
| $A_q(n, d)$ | $q$ elemanlı $A$ kümesi üzerinde $n$ uzunluğunda $d$ minimum uzaklığına sahip bir kodun eleman sayısının alabileceği en büyük değer |

| | |
|---|---|
| $B_q(n,d)$ | $F_q$ üzerinde $n$ uzunluğunda $d$ minimum uzaklığına sahip bir lineer kodun eleman sayısının alabileceği en büyük değer |
| $h_R(x)$ | $h(x)$ polinomunun ters sıralısı |
| $C=\langle g(x)\rangle$ | $g(x)$ tarafından üretilen $C$ devirli kodu |
| $(n,q)$ | $n$ ile $q$ sayılarının en büyük ortak böleni |
| $F_q[x]$ | Katsayıları $F_q$ cisminin elemanı olan polinom halkası |
| $\langle p\rangle$ | $p$ elemanı tarafından üretilen ideal |
| $GR(q^m)$ | Karakteristiği $q$, eleman sayısı $q^m$ olan Galois halkası |
| $\lvert\langle\theta\rangle\rvert$ | $\theta$ otomorfizmasının mertebesi |
| $F[x;\theta]$ | Katsayıları $F$ cisminin elemanı olan $\theta$ otomorfizması ile belirli skew polinom halkası |
| $F_4[x;\theta]$ | $F_4^*=\langle\alpha\rangle$ ve $\theta(a)=a^2$ ile belirli skew polinom halkası ($\alpha^2\equiv\alpha+1 \pmod 2$) |
| $F_9[x;\theta]$ | $F_9^*=\langle\gamma\rangle$ ve $\theta(a)=a^2$ ile belirli skew polinom halkası ($\gamma^2\equiv 2\gamma+1 \pmod 3$) |
| $der(f)$ | $f$ polinomunun derecesi |
| $Z(F[x;\theta])$ | $F[x;\theta]$ halkasının merkezi |
| $F_{q,n}$ | $F_q[x]\big/\langle x^n-1\rangle$ halkası |
| $R_{n,\theta}$ | $R$ bir skew polinom halkası olmak üzere $R\big/\langle x^n-1\rangle$ yapısı |
| $F_{p^m}+uF_{p^m}$ | $F_{p^m}[u]\big/\langle u^2\rangle$ halkası |
| $F_4+vF_4$ | $F_4[v]\big/\langle v^2-v\rangle$ halkası |
| $d_L(x,y)$ | $x$ ile $y$ arasındaki Lee ağırlığı |
| $w_L(x)$ | $x$'in Lee ağırlığı |

## ŞEKİL LİSTESİ

Sayfa

## ÇİZELGE LİSTESİ

Sayfa

# ÖZET

## DEĞİŞMELİ OLMAYAN HALKALAR ÜZERİNDE TANIMLI DEVİRLİ KODLAR

Fatmanur GÜRSOY

Matematik Anabilim Dalı

Yüksek Lisans Tezi

Tez Danışmanı: Prof. Dr. İrfan ŞİAP

Eş Danışman: Doç. Dr. Bahattin YILDIZ

Dijital bilgi transferinde ya da bilgi depolamasında kaynaktan kullanıcıya bilgi aktarılması esnasında dış etkenlerden ötürü bilgi mesajı değişikliğe uğrayabilir. Kodlama teorisi, haberleşme esnasında ya da bilgi depolamasında meydana gelebilecek hataları tespit etme ve düzeltme ile ilgilenir ve matematiğin farklı dallarıyla bağlantısı olan disiplinler arası bir alandır.

Kodlama teorisinin temel problemi ise orijinal bilgiye eklemeler yapılırken maliyetin minimumda tutulması ve aynı zamanda hata düzeltme kapasitesinin maksimum seviyede olmasını sağlamaktır. Bu alanda yapılan ilk çalışmalar cisimler üzerinde tanımlı lineer kodlar ve devirli kodlar üzerine yoğunlaşmıştır. Hamming kodlar, BCH kodlar, Golay kodları gibi bazı önemli kod aileleri elde edilmiştir. 70'lerin başından itibaren halkalar üzerinde kodlar çalışılmış, fakat bu alanda asıl ilerleme 1994 te Hammons vd. tarafından yapılan çalışma ile olmuştur. Bu çalışmada cebirsel bir yapıya sahip olmayan (lineer olmayan) Kerdock ve Preparata gibi bazı önemli kod aileleri $\mathbb{Z}_4$ üzerinde tanımlı lineer kodların Gray dönüşümü altındaki görüntüsü olarak elde edilmiştir. Böylece bu alanda yapılan çalışmalar farklı bir boyut kazanmış ve halkalar üzerinde kodlara yönelik birçok araştırma yapılmıştır.

Son altı yıldır ise değişmeli olmayan halkalar üzerinde kodlar tanımlanmış ve cebirsel özellikleri araştırılmıştır. Elde edilen bu yeni kod ailesi skew devirli kodlar olarak adlandırılmıştır. Skew devirli kodlar cebirsel yapıları nedeniyle oldukça önemlidir. Skew

polinom halkası tek türlü çarpanlarına ayrılabilen halka olmadığından devirli kodlara göre daha fazla üreteç polinomu ve böylece daha fazla sayıda kod elde etmek mümkündür. Dolayısıyla daha iyi parametrelere sahip kodların araştırılması açısından skew devirli kodlar daha avantajlı olabilir. En önemli özelliklerden biri ise lineer kodların daha zengin cebirsel yapılarda temsilinin elde edilmesidir.

Bu tezde skew devirli kodlarla ilgili literatürde mevcut olan çalışmalar irdelenmiş ve örneklendirilmiştir. Skew devirli kodların idempotent üreteçleri belirlenmiş ve idempotent üreteçlerin tek olmayabileceği gösterilmiştir. Karakteristiği 2 olan 16 elemanlı $F_4 + vF_4$ halkasının özellikleri çalışılmış ve bu halka üzerinde lineer kodlar belirlenmiştir. Ayrıca bu halka üzerinde Gray dönüşümü tanımlanarak $F_4$ üzerinde kodlar elde edilmiştir. Literatürde henüz çalışılmamış olan $F_4 + vF_4$ halkası üzerinde skew devirli kodlar tanımlanmış ve özellikleri belirlenmiştir. Bu kodların Gray dönüşümü altındaki görüntülerinden iyi parametrelere sahip kodlar elde edilmiştir.

**Anahtar Kelimeler:** Devirli kodlar, Galois halkaları, lineer kodlar, parçalı (quasi) devirli kodlar, skew devirli kodlar, skew polinom halkaları.

## ABSTRACT

### CYCLIC CODES OVER NONCOMMUTATIVE RINGS

Fatmanur GÜRSOY

Department of Mathematics

MSc. Thesis

Advisor: Prof. Dr. İrfan ŞİAP

Co-Advisor: Assoc. Prof. Dr. Bahattin YILDIZ

Coding theory is a field of research with a focus on detection and correction of errors that can occur during the transmission of data or data storing. It is a multi-disciplinary field with a lot of connections to different areas of mathematics.

One of the main tasks in coding theory is to encode messages with minimum cost and maximum error correction capability. Early studies in this area were concentrated on linear and cyclic codes over fields. Some of the important families of codes obtained in early stages were Hamming codes, BCH codes and Golay codes. Codes over rings had been considered by mathematicians from early seventies, but the breakthrough work was published in 1994 by Hammons et al. in which they showed that some important binary nonlinear codes such as Kerdock and Preparata codes can be obtained as Gray images of linear codes over $\mathbb{Z}_4$. The emergence of this paper brought a new direction to researchers working in coding theory. Since then a lot of research has been directed towards codes over rings.

In the last six years cyclic codes from noncommutative polynomial rings have been introduced and the algebraic structure of these codes has been examined. This new class of codes are named skew cyclic codes and they are important because of their algebraic structure. Since skew polynomial rings are not unique factorization rings there are many more generator polynomials leading to many more skew cyclic codes

compared to ordinary cyclic codes of the same lengths. Therefore skew cyclic codes are advantageous to search for codes with possible good parameters. Another important aspect of studying codes over such structures is the fact that one obtains a representation of linear codes over fields with a richer algebraic structure.

In this work, studies about skew cyclic codes in literature were examined and exemplified. Idempotent generators of skew cyclic codes are identified and it is shown that idempotent generator of a skew cyclic code may not be unique. The characteristic 2 ring $F_4 + vF_4$ of size 16 is considered. The properties of this ring are studied and linear codes over this ring are introduced. Also a Gray map is defined over this ring and codes over $F_4$ obtained as Gray images. Skew-cyclic codes over this ring are considered for the first time in the literature. The algebraic properties of these codes are examined and some good codes are obtained through the images of these codes.

**Keywords:** Cyclic codes, Galois rings, linear codes, quasi cyclic codes, skew cyclic codes, skew polynomial rings.

# BÖLÜM 1

# GİRİŞ

## 1.1 Literatür Özeti

Geçtiğimiz elli yıl içerisinde kodlama teorisi alanında yapılan çalışmaların önemli bir kısmı değişmeli olan halkalar ya da sonlu cisimler üzerinde tanımlı farklı tipteki kodların yapıları hakkındadır. Son zamanlarda yapılan çalışmalarda halkalar üzerinde tanımlanan kodlar yardımıyla daha iyi parametrelere sahip kodlar elde edilmiş ve lineer kodların farklı cebirsel yapılarda daha zengin temsillere sahip oldukları görülmüştür. Literatürde yeni olarak yer alan değişmeli olmayan halkalar üzerinde tanımlı kodlar yeni kodlar bulma ve hâlihazırda var olan kodların cebirsel yapılarının genelleştirilmesi açısından araştırmaya daha elverişli ve ehemmiyetlidir.

Değişmeli olmayan halkalar üzerinde tanımlı kodlar ilk olarak 2007 yılında Boucher vd. tarafından çalışılmıştır [3]. Bu çalışmada $F_q$ sonlu cismi üzerinde tanımlı $\theta$ otomorfizması ile belirli $F_q[x;\theta]$ skew polinom halkası kullanılarak devirli kodların genellemesi yapılmış ve elde edilen lineer kodlar skew devirli kodlar olarak adlandırılmıştır. $F_q[x;\theta]$ halkası tek türlü çarpanlarına ayrılabilen halka olmadığından devirli kodlara göre daha fazla üreteç polinomu ve böylece daha fazla sayıda kod elde etmek mümkündür. Dolayısıyla daha iyi parametrelere sahip kod elde etme ihtimali devirli kodlara nispeten daha yüksektir. Boucher vd. ([3]) bilinenden daha iyi parametrelere sahip kod örnekleri elde etmişlerdir. [8] nolu çalışmada skew devirli kodların dualleri üzerinde durulmuş ve bir skew devirli kodun dualinin de skew devirli kod olduğu gösterilmiştir. Fakat yukarıdaki iki çalışmada da skew devirli kodların uzunluğu için kısıtlama yapılmıştır. Şiap vd. tarafından herhangi bir $n$ uzunluğunda

skew devirli kod bulunabileceği gösterilmiştir [4]. Aynı çalışmada skew devirli kodlar ile devirli ve parçalı (quasi) devirli kodlar arasındaki ilişki incelenmiştir. 2010'da Abualrub vd. skew polinom halkalarını kullanarak skew parçalı devirli kodların inşası üzerine çalışmış ve bilinenden daha iyi parametrelere sahip kod örnekleri elde etmişlerdir [7].

2008'de Boucher vd. skew polinom halkasında katsayıları sonlu cisimler yerine Galois halkalarından alarak Galois halkaları üzerinde skew devirli kodları tanımlamışlardır [9]. Galois halkaları üzerinde tanımlı skew polinom halkaları sağ veya sol Öklidyen olmadığından bu çalışma monik üreteçli temel ideallerle belirlenen skew kodlar ile sınırlandırılmıştır. Daha sonra Bhaintwal 2010'da, [4] çalışmasındaki modül yaklaşımını kullanarak uzunluk için bir kısıtlama getirmeden Galois halkaları üzerinde skew parçalı devirli kodları tanımlamıştır [10].

2010'da Jitman vd. sonlu zincir halkaları üzerinde skew devirli kodları tanımlamışlardır [12]. Bu çalışmada $F_{p^m} + uF_{p^m}$ ($u^2 = 0$) halkası üzerinde tanımlı skew devirli kodlara ağırlık verilmiş ve bu halka üzerinde tanımlı tüm skew devirli kodların sınıflandırılması yapılmıştır.

### 1.2 Tezin Amacı

Literatürde yeni olarak yer alan skew devirli kodların cebirsel yapılarının incelenmesi, bu alanda yapılan çalışmaların örneklendirilmesi ve daha iyi parametrelere sahip kod bulmak için bilgisayar destekli araştırmalar yapılması amaçlanmıştır. Ayrıca skew devirli kodların farklı bir halka üzerinde tanımlaması yapılmıştır.

### 1.3 Orijinal Katkı

Skew devirli kodların diğer yapılarla ilişkisinden yararlanılarak Teorem 4.4 ve Teorem 4.5 elde edilmiştir. Ayrıca skew devirli kodların idempotent üreteçleri belirlenmiş ve birden fazla idempotent üreteç olabileceği gösterilmiştir.

$F_4 + uF_4$ üzerinde tanımlı skew devirli kodlardan lineer bir dönüşüm tanımlanarak $F_4$ üzerinde tanımlı lineer kodlar elde edilmiş ve optimale yakın kod örnekleri verilmiştir.

$F_4 + vF_4$ halkası üzerinde tanımlı lineer kodların yapısı incelenmiş ve bu halka üzerinde skew devirli kodlar tanımlanmıştır. Ayrıca $F_4 + vF_4$ halkası üzerinde tanımlı skew devirli kodların tek eleman tarafından üretildiği gösterilmiştir. Yine bu halka üzerinde tanımlı skew devirli kodların idempotent üreteçleri belirlenmiş ve optimal kod örnekleri verilmiştir.

# BÖLÜM 2

## TEMEL KAVRAMLAR

Bu bölümde, daha sonraki bölümlerde kullanılacak olan bazı temel tanım ve teoremlere değinilecektir. Tanım ve teoremler için ağırlıklı olarak [1], [11] ve [15] nolu kaynaklar kullanılacaktır.

### 2.1 Modül ve Alt Modüller

**Tanım 2.1** $(M,+)$ bir değişmeli grup ve $R$ bir halka olsun. $M$ deki elemanların, $R$ deki elemanlarla skaler çarpımı, $R\times M \to M$ fonksiyonu aşağıdaki koşulları sağlıyorsa, $M$ 'ye $R$ üzerinde bir sol modül veya kısaca sol $R$ -modül denir [21].

**i.** Her $r \in R$ ve her $m,m' \in M$ için $r(m+m') = rm + rm'$ ,

**ii.** Her $r,r' \in R$ ve her $m \in M$ için $(r+r')m = rm + r'm$ ,

**iii.** Her $r,r' \in R$ ve her $m \in M$ için $(rr')m = r(r'm)$ ,

**Not:** Bu işlemler sağ taraftan tanımlı olduğu durumda sağ modüldür. Bu tezde modüller sol modül olarak ele alınacaktır.

**Tanım 2.2** $R$ bir halka, $M$ bir $R$ -modül ve $N \subseteq M$ boş olmayan bir alt küme olsun. $N$ de kendi başına bir $R$ -modül ise $N$ 'ye $M$ 'nin bir alt modülü veya $R$ -alt modülü denir [21].

**Önerme 2.1** $R$ -modül $M$ 'nin boş olmayan bir $N \subseteq M$ alt kümesinin alt modül olması için gerek ve yeter koşul her $r,r' \in R$ ve her $m,m' \in N$ için $rm + r'm' \in N$ olmasıdır [21].

**Tanım 2.3** $M$ bir $R$ -modül ve $m \in M$ olsun. $\{m\}$ nin ürettiği alt modül

$$\langle m \rangle = Rm = \{rm : r \in R\}$$

şeklinde tanımlanır. Eğer $M = \langle m \rangle$ olacak şekilde bir $m \in M$ bulunabilirse, $M$ ye devirli modül denir [21].

**Tanım 2.4** $R$ bir halka ve $M$ bir $R$-modül olsun.

$$Ann(M) = \{r \in R \,|\, rM = 0\}$$

idealine $M$ modülünün sıfırlayıcısı (annihilator) denir [21].

**Tanım 2.5** $R$ bir halka, $M$ bir $R$-modül ve $S = \{y_\alpha\}_{\alpha \in I}$ de $M$ nin bir üreteç sistemi olsun. Her $m \in M$ elemanı, $r_\alpha \in R$, $y_\alpha \in S$ olmak üzere, $m = \sum_{\alpha \in I} r_\alpha y_\alpha$ şeklinde sonlu bir toplam olarak yazılabiliyor ve bu yazılış tek türlü oluyorsa, $S = \{y_\alpha\}_{\alpha \in I}$ ye $M$ nin bir tabanı denir. $M$ modülüne de bir serbest modül denir [21].

## 2.2 Cisimler

**Tanım 2.6** $F$ boş olmayan bir küme ve bu kümenin elemanları arasında "+" ve "." şeklinde iki tane ikili işlem tanımlanmış olsun. $(F,+,.)$ üçlüsü aşağıdaki şartları sağlıyorsa $F$ bir cisimdir. $a,b,c \in F$ olmak üzere

**i.** Kapalılık: $a+b \in F$ , $a.b \in F$

**ii.** Değişme özelliği: $a+b = b+a$ , $a.b = b.a$

**iii.** Birleşme özelliği: $(a+b)+c = a+(b+c)$ , $a.(b.c) = (a.b).c$

**iv.** Dağılma özelliği: $a.(b+c) = a.b + a.c$

**v.** Birim eleman:

**a)** Her $a \in F$ için $0_F \in F$ vardır öyle ki $a + 0_F = a$ eşitliğini sağlar.

**b)** Her $a \in F$ için $1_F \in F$ vardır öyle ki $a.1_F = a$ eşitliğini sağlar.

**vi.** Ters eleman:

**a)** Her $a \in F$ için $-a \in F$ vardır öyle ki $a + (-a) = 0_F$ eşitliğini sağlar.

**b)** Her $a \in F \setminus \{0\}$ için $a^{-1} \in F$ vardır öyle ki $a.a^{-1} = 1_F$ eşitliğini sağlar.

**Tanım 2.7** $F$ bir cisim olmak üzere $p.1_F = 0_F$ eşitliğini sağlayan en küçük pozitif $p$ tam sayısına $F$ cisminin karakteristiği denir. Böyle bir $p$ tam sayısı olmadığı durumlarda karakteristik $0$'dır [1].

**Teorem 2.1** Bir cismin karakteristiği ya sıfırdır ya da bir asal sayıdır [1].

**Teorem 2.2** $F$ sonlu bir cisim ve karakteristiği $p$ asalı ise $|F| = p^n$ olacak şekilde $n$ doğal sayısı vardır [1].

**Tanım 2.8** $F$ bir cisim ve $\theta : F \to F$ dönüşümü birebir ve örten bir homomorfizma ise $\theta$, $F$ üzerinde tanımlı bir otomorfizmadır, denir. Her $a \in F$ için $\theta^m(a) = a$ şartını sağlayan en küçük $m$ pozitif tam sayısına ise $\theta$ nın mertebesi denir ve kısaca $|\langle\theta\rangle| = m$ olarak gösterilir. $F$ cisminin $\theta$ tarafından sabit bırakılan elemanlarının kümesi $K = \{a \,|\, \theta(a) = a, a \in F\}$, $F$ nin bir alt cismidir [11].

**Tanım 2.9** $F$ cisminin karakteristiği $p$ olsun. $F$ üzerinde $\theta(a) = a^p$, $a \in F$ şeklinde tanımlanan $\theta$ otomorfizmasına Frobenius otomorfizması denir [11].

## 2.3 Sonlu Cisimler Üzerinde Tanımlı Vektör Uzayları

**Tanım 2.10** $F_q$, eleman sayısı $q$ olan bir sonlu cisim ve $V$ boş kümeden farklı bir küme olsun. $+ : V \times V \to V$ ve $. : F_q \times V \to V$ iki fonksiyon olmak üzere aşağıdaki koşullar sağlanıyorsa $V$ ye $F_q$ üzerinde tanımlı vektör uzayı denir [1].

Her $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ ve her $\alpha, \beta \in F_q$ için

**i.** $\mathbf{v} + \mathbf{w} \in V$,

**ii.** $\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v}$,

**iii.** $(\mathbf{v} + \mathbf{w}) + \mathbf{u} = \mathbf{v} + (\mathbf{w} + \mathbf{u})$,

**iv.** Her $\mathbf{v} \in V$ için $0 + \mathbf{v} = \mathbf{v} + 0 = \mathbf{v}$ olacak şekilde bir $0 \in V$ vardır,

**v.** Her $\mathbf{v} \in V$ için $(-\mathbf{v}) + \mathbf{v} = \mathbf{v} + (-\mathbf{v}) = 0$ olacak şekilde bir $-\mathbf{v} \in V$ vardır,

**vi.** $1_F \mathbf{v} = \mathbf{v}$,

**vii.** $(\alpha\beta)\mathbf{v} = a(\beta\mathbf{v})$,

**viii.** $\alpha(\mathbf{v}+\mathbf{u}) = \alpha\mathbf{v} + \alpha\mathbf{u}$,

**ix.** $(\alpha+\beta)\mathbf{v} = \alpha\mathbf{v} + \beta\mathbf{v}$.

Bileşenleri $F_q$ cisminin elemanlarından oluşan $n$ uzunluğundaki vektörlerin kümesi $F_q^n$ olarak gösterilir. Yani,

$$F_q^n = \left\{(v_1, v_2, ..., v_n) \middle| v_i \in F_q\right\}.$$

$\mathbf{v} = (v_1, v_2, ..., v_n) \in F_q^n$, $\mathbf{w} = (w_1, w_2, ..., w_n) \in F_q^n$ ve $\lambda \in F_q$ olmak üzere $F_q^n$ kümesi üzerinde vektörel toplam, $\mathbf{v} + \mathbf{w} = (v_1 + w_1, v_2 + w_2, ..., v_n + w_n) \in F_q^n$ ve skalerle çarpma işlemi, $\lambda\mathbf{v} = (\lambda v_1, \lambda v_2, ..., \lambda v_n) \in F_q^n$ olarak tanımlıdır. Tanımlanan işlemler altında $F_q^n$ bir vektör uzayı belirtir.

**Tanım 2.11** $V$, $F_q$ üzerinde bir vektör uzayı ve $\varnothing \neq C \subseteq V$ olsun. Aşağıdaki şartlar sağlanıyorsa $C$ kümesi $V$ nin bir alt vektör uzayıdır [1].

**i.** $\forall \mathbf{u}, \mathbf{v} \in C \Rightarrow \mathbf{u} + \mathbf{v} \in C$,

**ii.** $\forall \lambda \in F_q$ ve $\forall \mathbf{u} \in C \Rightarrow \lambda\mathbf{u} \in C$.

**Tanım 2.12** $V$, $F_q$ üzerinde bir vektör uzayı ve $\lambda_1, \lambda_2, ..., \lambda_r \in F_q$ olsun. $\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_r \in V$ vektörlerinin bir lineer kombinasyonu $\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + ... + \lambda_r\mathbf{v}_r$ şeklindedir [1].

**Tanım 2.13** $V$, $F_q$ üzerinde bir vektör uzayı olsun. $\lambda_1\mathbf{v}_1 + ... + \lambda_r\mathbf{v}_r = 0$ denkleminin tek çözümü $\lambda_1 = \cdots = \lambda_r = 0$ ise $\{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$ vektörler kümesi $V$ de lineer bağımsızdır [1].

**Örnek 2.1** $S = \{(0,0,0,1), (0,0,1,0), (0,1,0,0)\}$ kümesi herhangi bir $q$ pozitif tamsayısı için $F_q^4$ te lineer bağımsızdır [1].

**Tanım 2.14** $S = \{\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_n\}$, $V$ nin boştan farklı bir alt kümesi olsun. $S$ nin bütün lineer kombinasyonlarının kümesi $\langle S \rangle$ ile gösterildiğinde $\langle S \rangle$ uzayına, $S$ nin gerdiği (ürettiği) alt vektör uzayı denir. $S$ kümesi, $\langle S \rangle$ nin bir üreteç kümesidir [1].

**Önerme 2.2** $S$ kümesi $V$ nin bir alt vekör uzayı ise $\langle S \rangle = S$ dir [1].

**Örnek 2.2** $q = 2$ ve $S = \{0001, 0010, 0100\}$ ise $S$ nin gerdiği uzay;

$$\langle S \rangle = \{0000, 0001, 0010, 0100, 0011, 0101, 0110, 0111\} \text{ dir [1].}$$

**Tanım 2.15** $V$ , $F_q$ üzerinde bir vektör uzayı olsun.

**i.** $B = \{\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_n\}$, $B$ kümesi lineer bağımsız ve $V = \langle B \rangle$ ise $B$ ye $V$ vektör uzayının bir tabanı denir.

**ii.** $B$ tabanının eleman sayısına $V$ nin boyutu denir ve $boy(V)$ ile gösterilir. $B$ sonsuz elemanlı ise $boy(V) = \infty$ olarak gösterilir [1].

**Not:** $F_q$ üzerindeki sonlu boyutlu bir vektör uzayının birden fazla tabanı olabilir fakat bu tabanların tümü eşit sayıda eleman içerir.

**Teorem 2.3** $V$ , $F_q$ üzerinde bir vektör uzayı olsun. Eğer $boy(V) = k$ ise

**i.** $V$ nin eleman sayısı $q^k$ dır,

**ii.** $V$ nin $\frac{1}{k!}\prod_{i=0}^{k-1}\left(q^k - q^i\right)$ adet farklı tabanı vardır [1].

**Tanım 2.16** $\mathbf{v} = (v_1, v_2, ..., v_n) \in F_q^n$ ve $\mathbf{w} = (w_1, w_2, ..., w_n) \in F_q^n$ olsun.

**i.** $\mathbf{v}$ ile $\mathbf{w}$ nin skaler çarpımı (Öklid iç çarpım), $\langle \mathbf{v}, \mathbf{w} \rangle = v_1 w_1 + v_2 w_2, + ... + v_n w_n \in F_q^n$ şeklindedir.

**ii.** $\langle \mathbf{v}, \mathbf{w} \rangle = 0$ ise $\mathbf{v}$ ile $\mathbf{w}$ birbirine diktir denir.

**iii.** $S$ , $F_q^n$ nin bir alt kümesi olmak üzere $S^{\perp} = \{\mathbf{v} \in F_q^n \,|\, \langle \mathbf{v}, \mathbf{s} \rangle = 0,\ \forall \mathbf{s} \in S\}$ kümesine $S$ nin dik'i denir [1].

**Not:** $F_q^n$ nin herhangi $S$ alt kümesi için $S^{\perp}$ kümesi her zaman $F_q^n$ nin bir alt uzayıdır. Ayrıca $\langle S \rangle^{\perp} = S^{\perp}$ dir.

**Örnek 2.3** $q = 2$ ve $n = 4$ olsun. $\mathbf{u} = (1,1,1,1)$, $\mathbf{v} = (1,1,1,0)$ ve $\mathbf{w} = (1,0,0,1)$ olmak üzere

$$\langle \mathbf{u}, \mathbf{v} \rangle = 1\cdot 1+1\cdot 1+1\cdot 1+1\cdot 0 = 1,$$
$$\langle \mathbf{u}, \mathbf{w} \rangle = 1\cdot 1+1\cdot 0+1\cdot 0+1\cdot 1 = 0,$$
$$\langle \mathbf{v}, \mathbf{w} \rangle = 1\cdot 1+1\cdot 0+1\cdot 0+0\cdot 1 = 1.$$

Bu durumda $\mathbf{u}$ ile $\mathbf{v}$ vektörleri birbirine diktir [1].

**Teorem 2.4** $F_q^n$ nin her $S$ alt kümesi için $boy(\langle S \rangle) + boy(S^{\perp}) = n$ dir [1].

**Örnek 2.4** $q = 2$, $n = 4$ ve $S = \{0100, 0101\}$ olsun. Bu durumda $S$ nin gerdiği uzay;

$$\langle S \rangle = \{0000, 0100, 0001, 0101\} \text{ dir.}$$

$S$ lineer bağımsız bir küme olduğundan $boy(\langle S \rangle) = 2$ dir. $S$ nin dik'i $S^{\perp} = \{0000, 0010, 1000, 1010\}$ olarak bulunur. $\{0010, 1000\}$ kümesi $S^{\perp}$ için bir tabandır ve $boy(S^{\perp}) = 2$ dir. Dolayısıyla $boy(\langle S \rangle) + boy(S^{\perp}) = 2+2 = 4 = n$ eşitliği sağlanır [1].

## 2.4 Hata Düzelten Kodlarla İlgili Temel Bilgiler

Hata düzelten kodlar teorisi, dijital bilgi transferinde orijinal bilgiye eklemeler yapıp cebirsel bir yapı kazandırarak haberleşme esnasında ya da bilgi depolamasında meydana gelebilecek hataları düzeltme ve orijinal bilgiye yapılan ekleri optimize etmek ile ilgilenir [22]. Bu başlık altında kodlama teorisi ile ilgili bazı temel tanım ve teoremler verilecektir.

**Tanım 2.17** $A = \{a_1, a_2, ..., a_q\}$ şeklinde $q$ elemana sahip bir küme olsun.

**i.** Her $i \in \{1, 2, ..., n\}$ için $u_i \in A$ olmak üzere $\mathrm{u} = (u_1 u_2 ... u_n)$ elemanı $A$ üzerinde $n$ uzunluğunda bir $q$-lu sözdür. $\mathrm{u}$ elemanı aynı zamanda $\mathrm{u} = (u_1, u_2, ..., u_n)$ şeklinde bir vektör olarak da düşünülebilir.

**ii.** $C \subseteq A^n$ kümesi, $A$ üzerinde $n$ uzunluğunda bir $q$-lu blok koddur.

**iii.** $C$ deki bir elemana $C$'nin bir kodsözü denir.

**iv.** $C$ deki kodsözlerin sayısı, $C$ nin eleman sayısıdır ve $|C|$ olarak gösterilir.

**v.** Uzunluğu $n$ ve eleman sayısı $\mathrm{M}$ olan bir kod kısaca $(n, \mathrm{M})$ ile gösterilir.

**vi.** $A$ kümesine kod alfabesi, $A$ nın elemanlarına ise kod sembolleri denir [1].

**Örnek 2.5** $A=\{0,1\}$, $2$ elemanlı bir alfabe olsun. $C=\{00,10,01,11\}$ kümesi $A$ üzerinde $4$ elemanlı $2$ uzunluğunda ikili blok koddur [1].

**Tanım 2.18** $x=(x_1\dots x_n)$ ve $y=(y_1\dots y_n)$ $A$ alfabesi üzerinde $n$ uzunluğunda birer söz olsun. $d(x_i,y_i)$ fonksiyonu,

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

olmak üzere $x$ ile $y$ arasındaki Hamming uzaklığı $d(x,y)$ ile gösterilir ve $d(x,y)=d(x_1,y_1)+\dots+d(x_n,y_n)$ şeklinde tanımlanır. Diğer bir ifadeyle $d(x,y)=\left|\left\{i\,\middle|\,x_i\neq y_i, 1\le i\le n\right\}\right|$ dir [1].

**Örnek 2.6** $A=\{1,0\}$ ve $x=01010$, $y=01101$ olsun. Bu durumda $d(x,y)=3$ tür.

**Tanım 2.19** $C$, en az iki elemanlı bir kod olsun. $C$ kodunun minimum Hamming uzaklığı $d(C)$ ile gösterilir ve $d(C)=\min\left\{d(x,y)\,\middle|\,x,y\in C,\ x\neq y\right\}$ olarak tanımlıdır [1].

**Tanım 2.20** Uzunluğu $n$, eleman sayısı $\mathrm{M}$ ve minimum Hamming uzaklığı $d$ olan bir kod kısaca $(n,\mathrm{M},d)$-kod olarak gösterilir. $n$, $\mathrm{M}$ ve $d$ sayılarına kodun parametreleri denir [1].

**Örnek 2.7** $C=\{000000, 000111, 111222\}$, $F_3$ üzerinde bir kod olsun.

$$d(000000,000111)=3,$$
$$d(000000,111222)=6,$$
$$d(000111,111222)=6$$

olduğundan $d(C)=3$ tür. $C$ kodu $(6,3,3)$ parametrelerine sahip üçlü bir koddur [1].

**Tanım 2.21** $t>0$ olsun. Eğer $C$ kodundaki herhangi bir kodsözün en az 1, en fazla $t$ bileşeninde hata oluşmasıyla elde edilen söz $C$ nin kodsözü değilse $C$ kodu, $t$ hata fark edebilen bir koddur. Eğer $t$ hata fark edip $t+1$ hatayı fark edemiyorsa $C$ kodu tam olarak $t$ hata fark edebilen koddur [1].

**Teorem 2.5** Bir $C$ kodunun $t$ hata fark edebilmesi için gerek ve yeter koşul $d(C) \geq t+1$ olmasıdır. $d(C) = t$ ise $C$ kodu tam olarak $t-1$ hata fark edebilir [1].

**Tanım 2.22** $t > 0$ olsun. Eğer $C$ kodundaki herhangi bir kodsözün en az 1, en fazla $t$ bileşeninde hata oluşmasıyla elde edilen söz $C$ nin başka bir kodsözünden en az 1, en fazla $t$ bileşeninde hata meydana gelmesiyle elde edilemiyorsa $C$ kodu $t$ hata düzelten bir koddur. Eğer $C$ kodu $t$ hatayı düzeltebiliyor fakat $t+1$ hatayı düzeltemiyorsa tam olarak $t$ hata düzelten koddur [1].

**Teorem 2.6** Bir $C$ kodunun $t$ hata düzelten kod olması için gerek ve yeter koşul $d(C) \geq 2t+1$ olmasıdır. $d(C) = 2t+1$ ise $C$ kodu tam olarak $t$ hata düzelten koddur [1].

En iyi parametrelere sahip kodları bulma problemi kodlama teorisinin temel problemidir. Daha iyi kod bulmak için parametrelerden ikisi sabit iken diğeri optimize edilir.

**i.** $n$ uzunluğunda ve eleman sayısı $\mathrm{M}$ olan bir kod için olabilecek en büyük minimum Hamming uzaklığına,

**ii.** Eleman sayısı $\mathrm{M}$ ve minimum uzaklığı $d$ olan bir kod için olabilecek en küçük $n$ değerine veya

**iii.** $n$ uzunluğunda ve minimum uzaklığı $d$ olan bir kod için olabilecek en büyük $\mathrm{M}$ değerine sahip olan kodlar optimaldir.

**Tanım 2.23** $A$, $q$ elemanlı bir alfabe ve $A$ üzerinde $n$ uzunluğunda $d$ minimum uzaklığına sahip bir kodun eleman sayısının olabilecek en büyük değeri $A_q(n,d)$ ile gösterilsin. Bu durumda $A_q(n,d) = \max\left\{\mathrm{M} \middle| \mathrm{C} \subseteq \mathrm{A}^n \text{ ve C bir } (n,\mathrm{M},d)-\mathrm{kod}\right\}$ dur.

### 2.4.1 Lineer Kodlar

$F_q^n$ vektör uzayının bir $F_q$ alt vektör uzayına $n$ uzunluğunda lineer kod denir. Lineer kodlar vektör uzayı olduklarından tanımlanmaları ve kullanımları daha kolaydır. Lineer kodların lineer olmayanlara göre bazı avantajlarını şu şekilde sıralayabiliriz:

**i.** Lineer kod aynı zamanda bir vektör uzayı olduğundan bir taban kullanılarak daha basit ifade edilebilir.

**ii.** Bir lineer kodun minimum uzaklığı, sıfırdan faklı kodsözlerinin Hamming ağırlıklarının minimumuna eşittir.

**iii.** Lineer kodlar için geliştirilen kodlama ve dekodlama algoritmaları daha hızlı ve kolaydır.

**Tanım 2.24** $C$ , $F_q^n$ vektör uzayının bir alt vektör uzayı ve $boy(C)=k$ olsun. $C$ , $F_q$ üzerinde tanımlı $n$ uzunluğunda boyutu $k$ olan bir lineer koddur. Böyle bir kod kısaca $[n,k]_q$ -kod olarak ifade edilir. Özel olarak, $q=2$ iken ikili kod; $q=3$ iken üçlü kod denir [1].

**Örnek 2.8**

**i.** $C=\{(\lambda,\lambda,...,\lambda)\big|\lambda\in F_q\}\subseteq F_q^n$ bir lineer koddur.

**ii.** $C=\{0000,1100,2200,0001,0002,1101,1102,2201,2202\}\subseteq F_3^4$, üçlü $[4,2]$-lineer koddur [1].

**Teorem 2.7** $C$ , $F_q$ üzerinde $n$ uzunluğunda bir lineer kod olsun. Bu durumda

**i.** $|C|=q^{boy(C)}$ ,

**ii.** $C^{\perp}$ bir lineer koddur ve $boy(C)+boy(C^{\perp})=n$ ,

**iii.** $(C^{\perp})^{\perp}=C$ dir [1].

**Tanım 2.25** $C$ bir lineer kod olsun.

**i.** $C^{\perp}$ koduna $C$ kodunun duali denir.

**ii.** $C\subseteq C^{\perp}$ ise $C$ ye kendine dik (self ortogonal) kod denir.

**iii.** $C=C^{\perp}$ ise $C$ ye kendine dual kod denir [1].

**Önerme 2.3** Kendine dik $n$ uzunluğundaki bir kodun boyutu $k\le\frac{n}{2}$ ve kendine dual $n$ uzunluğundaki kodun boyutu ise $k=\frac{n}{2}$ dir [1].

**Tanım 2.26** $C$ , $n$ uzunluğunda bir kod ve $u=(u_1,u_2,...,u_n),\ v=(v_1,v_2,...,v_n)\in C$ olsun. $u$ kodsözü için Hamming ağırlığı $wt(u)=\left|\left\{i\,|u_i\neq 0\right\}\right|$ olarak tanımlıdır. Ayrıca $u$ ile $v$ arasındaki Hamming uzaklığı $d(u,v)=\sum_{i=1}^{n} wt(u_i-v_i)$ şeklinde hesaplanır [1].

**Örnek 2.9** $d(010101,111111)=3$ ve $d(010101,101010)=6$.

**Tanım 2.27** $C$ nin farklı kodsözleri arasındaki en küçük Hamming uzaklığına $C$ kodunun minimum Hamming uzaklığı denir ve $d(C)$ ile gösterilir. $C$ nin kodsözlerinin sıfırdan farklı en küçük Hamming ağırlığına $C$ kodunun minimum Hamming ağırlığı denir ve $wt(C)$ ile gösterilir [1].

**Tanım 2.28** $F_q$ üzerinde uzunluğu $n$ , boyutu $k$ ve minimum Hamming uzaklığı $d$ olan bir $C$ lineer kodu $[n,k,d]_q$-kod olarak gösterilir [1].

**Önerme 2.4** $u,v\in F_q^n$ ise $d(u,v)=wt(u-v)$ dir [1].

**Teorem 2.8** $C$ , $F_q$ üzerinde bir lineer kod ise $d(C)=wt(C)$ dir [1].

Yukarıdaki teoremden görüldüğü üzere lineer kodların minimum Hamming uzaklığının bulunması lineer olmayanlara göre daha kolaydır.

**Tanım 2.29** $q$ bir asalın kuvveti olmak üzere $F_q$ üzerinde $n$ uzunluğunda $d$ minimum uzaklığına sahip bir lineer kodun eleman sayısının olabilecek en büyük değeri $B_q(n,d)$ ile gösterilsin.

$$B_q(n,d)=\max\left\{q^k\,\middle|\,\mathrm{C}\subseteq F_q^n \text{ ve C bir } [n,k,d]-\mathrm{kod}\right\}$$

Bu durumda $C$ , $F_q$ üzerinde $[n,k,d]$-kod ve $q^k=B_q(n,d)$ ise $C$ koduna optimal kod denir [1].

### 2.4.2 Lineer Kodların Üreteç ve Kontrol Matrisleri

**Tanım 2.30**

**i.** Bir $C$ lineer kodunun, $F_q^n$ uzayının bir alt uzayı olduğundan, bir bazı vardır. $C$ nin baz vektörlerini satır kabul eden matrise $C$ nin üreteç matrisi denir.

**ii.** $\forall \overline{x} \in C$ için $H\overline{x}^T = 0$ eşitliğini sağlayan $H$ matrisi $C^{\perp}$ dual kodunun üreteç matrisidir. $H$ matrisi aynı zamanda $C$ lineer kodunun kontrol matrisidir [1].

**Not:**

**i.** $C$ bir $[n,k]$-lineer kod ise $G$ üreteç matrisi $k \times n$ ve $H$ kontrol matrisi $(n-k) \times n$ formundadır.

**ii.** $G$ ve $H$ matrislerinin satırları lineer bağımsızdır.

**iii.** $C = \{\overline{x} \in F_q^n \,|\, H\overline{x}^T = 0\}$.

**Önerme 2.5** $C$, $F_q$ üzerinde $[n,k]$-lineer kod ve $G$ bu kodun üreteç matrisi olsun. Bu durumda $v \in F_q^n$ nin $C^{\perp}$ dual kodun bir elemanı olması için gerek ve yeter koşul $vG^{\perp} = 0$ olmasıdır. Ayrıca $(n-k) \times n$ formunda bir $H$ matrisinin $C$ nin kontrol matrisi olması için gerek ve yeter koşul $H$ matrisinin satırlarının lineer bağımsız olması ve $HG^T = 0$ olmasıdır [1].

**Teorem 2.9** $C$ bir lineer kod ve $H$ matrisi $C$ nin bir kontrol matrisi olsun.

**i.** $C$ nin minimum uzaklığının $d$ den büyük veya $d$ ye eşit olması için gerek ve yeter koşul $H$ matrisinin herhangi $d-1$ tane sütununun lineer bağımsız olmasıdır.

**ii.** $C$ nin minimum uzaklığının $d$ den küçük veya $d$ ye eşit olması için gerek ve yeter koşul $H$ matrisinin en az $d$ tane sütununun lineer bağımlı olmasıdır [1].

**Sonuç 2.1** $C$ bir lineer kod ve $H$ matrisi $C$ nin bir kontrol matrisi olsun. Aşağıdaki ifadeler birbirine denktir [1].

**i.** $d(C) = d$;

**ii.** $H$ matrisinin herhangi $d-1$ tane sütunu lineer bağımsızdır ve $H$ matrisinde $d$ tane lineer bağımlı sütun vardır.

**Örnek 2.10** $C$, ikili bir lineer kod ve $C$ kodu için kontrol matrisi;

$$H=\begin{pmatrix}1&0&1&0&0\\1&1&0&1&0\\0&1&0&0&1\end{pmatrix}$$

olsun. $H$ matrisinin herhangi iki sütunu lineer bağımsız ve 1,3 ve 4 üncü sütunları lineer bağımlıdır. Bu durumda $C$ kodu için minimum uzaklık, $d(C)=3$ olur [1].

### 2.4.3 Devirli Kodlar

Devirli kodlar ilk olarak Eugene Prange (1957) tarafından çalışılmıştır. Bu çalışma hata düzelten kodlar teorisi alanında önemli gelişmelere yol açmıştır. Golay kodları, BCH kodlar ve Reed-Solomon kodları gibi bazı önemli kod aileleri devirli kodlardır. Devirli kodlar cebirsel yapıları sayesinde uygulama alanında daha avantajlıdır.

**Tanım 2.31** $C$ bir lineer kod ve her $c=(c_0,c_1,...,c_{n-1})\in C$ için $\psi(c)=(c_{n-1},c_0,...,c_{n-2})\in C$ ise $C$ ye devirli kod denir. $\psi$ dönüşümüne ise devirsel öteleme (cyclic shift) denir [1].

**Örnek 2.11**

$$C=\{0000000,1011100,0101110,0010111,1110010,0111001,1001011,1100101\}$$

ikili lineer kodu $7$ uzunluğunda devirli bir koddur.

**Önerme 2.6** Kodlar polinomlar cinsinden ifade edilebilir.

$$\pi: F_q^n \to F_q[x]\Big/\langle x^n-1\rangle, \quad c=(c_0,c_1,...,c_{n-1})\to c(x)=c_0+c_1x+...+c_{n-1}x^{n-1}$$

olarak tanımlanan $\pi$ fonksiyonu bir lineer dönüşümdür.

$c\in C$ kodsözünün devirsel ötelemesi $x.c(x)$'e tekabül eder. Yukarıdaki lineer dönüşüm vasıtasıyla devirli kodlar idealler cinsinden ifade edilebilir [1].

**Teorem 2.10** $C\subseteq F_q^n$ lineer kodunun devirli kod olması için gerek ve yeter koşul $\pi(C)$ nin $F_q[x]\Big/\langle x^n-1\rangle$ halkasının bir ideali olmasıdır [1].

**Örnek 2.12** $C=\{000,110,101,011\}$ kodu bir ikili devirli koddur. $C$ nin kod sözlerine karşılık gelen polinomların kümesi $\pi(C)=\{0,1+x,1+x^2,x+x^2\}$ dir. $\pi(C)$, $F_2[x]\big/\langle x^3-1\rangle$ halkasının bir idealidir.

**Teorem 2.11** $I$ , $F_q[x]\big/\langle x^n-1\rangle$ halkasının sıfırdan farklı bir ideali ve $g(x)$ polinomu da $I$ idealindeki sıfırdan farklı en küçük dereceye sahip monik polinom olsun. Bu durumda $g(x)$ polinomu $I$ idealinin bir üretecidir ve $x^n-1$'i böler [1].

**Teorem 2.12** $F_q[x]\big/\langle x^n-1\rangle$ halkasının sıfırdan farklı herhangi bir $I$ idealindeki sıfırdan farklı en küçük dereceli monik polinom tektir [1].

**Tanım 2.32** $F_{q,n}=F_q[x]\big/\langle x^n-1\rangle$ olmak üzere $C\subseteq F_q^n$ devirli kod ve $C$ ye karşılık gelen $\pi(C)$ idealindeki sıfırdan farklı en küçük dereceli monik polinom $g(x)$ olsun. Bu durumda $g(x)$ polinomuna $C$ nin üreteç polinomu denir ve $C=\langle g(x)\rangle=\{f(x)g(x)\,\big|\,f(x)\in F_{q,n}\}$ ile verilir [1].

**Örnek 2.13** $C=\{000,110,011,101\}$ devirli koduna karşılık gelen ideal

$$\pi(C)=\{0,1+x,x+x^2,1+x^2\}\subseteq F_2[x]\big/\langle x^3-1\rangle \text{ dir.}$$

Bu idealin içerisindeki en küçük dereceli monik polinom $1+x$, $\pi(C)$ idealini üretir aynı zamanda $C$ kodunun üreteç polinomudur.

**Teorem 2.13** $F_q[x]$ halkasında $x^n-1$ polinomunun her bir monik böleni $F_q$ üzerinde tanımlı bir devirli kod üretir [1].

**Teorem 2.14** $x^n-1$ polinomunun $F_q[x]$ halkasında asal çarpanlarına ayrılışı $x^n-1=\prod_{i=1}^{r}p_i^{e_i}(x)$ olsun. Bu durumda $F_q$ üzerinde $n$ uzunluğundaki devirli kodların sayısı $\prod_{i=1}^{r}(e_i+1)$ dir [1].

**Teorem 2.15** $g(x)\in F_q[x]$, $g(x)\,|\,x^n-1$ ve $der(g(x))=k$ olsun. Bu durumda $g(x)$ tarafından üretilen ideale karşılık gelen kod $n$ uzunluğunda boyutu $n-k$ olan devirli bir koddur [1].

**Örnek 2.14** $x^7-1=(1+x)(1+x^2+x^3)(1+x+x^3)\in F_2[x]$ indirgenemez çarpanlarının ayrışımıdır. Bu durumda $F_2$ üzerinde $n=7$ olan devirli kodların sayısı $(1+1)(1+1)(1+1)=8$ olarak bulunur. Burada $g(x)=(1+x)(1+x^2+x^3)=1+x+x^2+x^4$ polinomu $n=7$ uzunluğunda boyutu $n-k=7-4=3$ olan devirli bir kod üretir.

$\langle g(x)\rangle=\{0000000,1110100,0111010,0011101,1001110,0100111,1010011,1101001\}$.

**Teorem 2.16** $g(x)=g_0+g_1x+\ldots+g_{n-k}x^{n-k}\in F_q[x]$ ve $g(x)$, $x^n-1$ in bir böleni olsun. $C$ devirli bir kod ve $g(x)$ polinomu bu kodun üreteç polinomu ise

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

matrisi $C$ kodunun üreteç matrisidir [1].

**Tanım 2.33** $h(x)=\sum_{i=0}^{k}a_ix^i$, derecesi $k$ olan bir polinom olsun. $h(x)$ in ters sıralı polinomu $h_R(x):=x^kh(1/x)=\sum_{i=0}^{k}a_{k-i}x^i$ şeklinde tanımlıdır [1].

**Teorem 2.17** $C$, $F_q$ üzerinde tanımlı $[n,k]$ parametrelerine sahip bir devirli kod ve $g(x)$ polinomu $C$ nin üreteç polinomu olsun. $h(x)=(x^n-1)/g(x)$ ve $h(x)=h_0+h_1x+\ldots+h_kx^k$ olsun. Bu durumda $h_0^{-1}h_R(x)$ polinomu dual kodun ($C^{\perp}$) üreteç polinomudur ve $h_0^{-1}h_R(x)$ polinomuna $C$'nin kontrol polinomu denir. Ayrıca

$$H=\begin{pmatrix} h_R(x) \\ xh_R(x) \\ \vdots \\ x^{n-k-1}h_R(x) \end{pmatrix}=\begin{pmatrix} h_k & h_{k-1} & \ldots & \ldots & h_0 & 0 & 0 & \ldots & 0 \\ 0 & h_k & h_{k-1} & \ldots & \ldots & h_0 & 0 & \ldots & 0 \\ \vdots & & & \ddots & & & & & \vdots \\ 0 & 0 & \ldots & 0 & h_k & h_{k-1} & \ldots & \ldots & h_0 \end{pmatrix}$$

matrisi $C$'nin kontrol matrisidir [1].

**Örnek 2.15** Bir önceki örnekte $F_2$ üzerinde $g(x)=1+x+x^2+x^4$ tarafından üretilen devirli kod için üreteç matrisi,

$$G=\begin{pmatrix}1&1&1&0&1&0&0\\0&1&1&1&0&1&0\\0&0&1&1&1&0&1\end{pmatrix}$$

şeklindedir. $h(x)=(x^7-1)/g(x)=1+x+x^3$ ve $h_R(x)=1+x^2+x^3$ dir. Bu durumda $C$ nin kontrol matrisi,

$$H=\begin{pmatrix}1&0&1&1&0&0&0\\0&1&0&1&1&0&0\\0&0&1&0&1&1&0\\0&0&0&1&0&1&1\end{pmatrix}$$

şeklindedir. $h_0^{-1}h_R(x)=h_R(x)=1+x^2+x^3$ polinomu aynı zamanda $C$ nin kontrol polinomudur.

### 2.4.4 Devirli Kodların İdempotent Üreteçleri

$R$ bir halka ve $e\in R$ olsun. $e^2=e$ ise $e$ ye idempotent eleman denir.

Bir devirli kodu üreten birden fazla polinom olabilir.

**Teorem 2.18** $C$ , $F_q$ üzerinde uzunluğu $n$ olan bir devirli kod ve $g(x)$ polinomu $C$ nin üreteç polinomu olsun. $v(x)\in F_q[x]/\langle x^n-1\rangle$ olmak üzere $C=\langle v(x)\rangle$ olması için gerek ve yeter koşul $ebob(v(x),x^n-1)=g(x)$ olmasıdır.

$C$ , $F_q$ üzerinde devirli kod ve $e^2(x)=e(x)\pmod{x^n-1}$ şartını sağlayan $e(x)$ polinomu $C$ yi üretiyorsa $e(x)$ polinomuna $C$ nin idempotent üreteci denir [15].

**Teorem 2.19** $(n,q)=1$ ve $C$ , $F_q$ üzerinde $n$ uzunluğunda bir devirli kod olsun. Bu durumda $C=\langle e(x)\rangle$ olacak şekilde tek bir $e(x)\in C$ idempotent polinomu vardır [15].

$(n,q)=1$ ve $F_q$ üzerinde $n$ uzunluğunda bir $C$ devirli kodunun üreteç polinomu $g(x)$ biliniyorsa $C$ nin idempotent üreteci aşağıdaki gibi kolayca bulunabilir:

**i.** $(n,q)=1$ olduğundan $x^n-1$ polinomunun $F_q[x]$ te katlı kökü yoktur. Böylece $x^n-1=h(x)g(x)$ ise $ebob(h(x),g(x))=1$ olur.

**ii.** $1 = a(x)g(x) + b(x)h(x)$ olacak şekilde $a(x), b(x) \in F_q[x]$ vardır.

**iii.** $e(x) \equiv a(x)g(x) \pmod{x^n - 1}$ polinomu $C$ nin idempotent üretecidir.

Eğer aynı şekilde tanımlı $C$ devirli kodunun idempotent üreteci biliniyorsa üreteç polinomu aşağıdaki teorem yardımıyla bulunur .

**Teorem 2.20** $C$ , $F_q$ üzerinde devirli kod ve $e(x)$ $C$ nin idempotent üreteci olsun. Bu durumda $F_q[x]$ te $g(x) = ebob(e(x), x^n - 1)$ polinomu $C$ nin üreteç polinomudur [15].

**Örnek 2.16** $x^7 - 1 = (x^3 + x^2 + 1)(x^4 + x^3 + x^2 + 1) \in F_2[x]$. $g(x) = x^3 + x^2 + 1$ ve $C = \langle g(x) \rangle$ olsun. Bu durumda $C$ kodu $F_2$ üzerinde $n = 7$ uzunluğunda bir devirli koddur. Bölme algoritması uygulanarak $1 = x^3(x^3 + x^2 + 1) + (x^2 + 1)(x^4 + x^3 + x^2 + 1)$ elde edilir. Dolayısıyla $e(x) = x^3(x^3 + x^2 + 1) = x^6 + x^5 + x^3$ polinomu $C$ nin idempotent üretecidir.

### 2.4.5 Bazı Özel Devirli Kodlar

**Tanım 2.34** $\alpha$ , $F_{q^m}$ cisminin bir ilkel kökü ve $M^i(x)$ polinomu $\alpha^i$ nin $F_q[x]$ deki minimal polinomu olsun. $g(x) = ekok\{M^a(x), M^{a+1}(x), ..., M^{a+\delta-2}(x)\}$ polinomu tarafından üretilen devirli koda $n = q^m - 1$ uzunluğunda, $\delta$ minimum tasarlanmış uzaklığa sahip BCH kod denir ( $a > 0$ ) [1].

**Tanım 2.35** $C$ , $F_q^n$ uzayının bir alt uzayı olsun. Her

$$c = \left(c_{0,0}, c_{0,1}, ..., c_{0,l-1}, c_{1,0}, c_{1,1}, ..., c_{1,l-1}, ..., c_{s-1,0}, c_{s-1,1}, ..., c_{s-1,l-1}\right) \in C$$

için $T_{s,l}(c) = \left(c_{s-1,0}, c_{s-1,1}, ..., c_{s-1,l-1}, c_{0,0}, c_{0,1} ..., c_{0,l-1}, ..., c_{s-2,0}, c_{s-2,1}, ..., c_{s-2,l-1}\right) \in C$ oluyorsa $C$ ye uzunluğu $n = sl$ indeksi $l$ olan parçalı devirli kod veya $l$-parçalı devirli kod ($l$-quasi cyclic code ) denir.

### 2.4.6 Gray Dönüşümü

Hammons vd. tarafından 1994'te yapılan çalışmada $\mathbb{Z}_4$ halkasından $\mathbb{Z}_2$ üzerine bir dönüşüm tanımlanmış ve $\mathbb{Z}_2$ üzerinde tanımlı lineer olmayan bazı önemli kod aileleri $\mathbb{Z}_4$ üzerinde tanımlı lineer kodların bu dönüşüm altındaki görüntüsü olarak elde edilmiştir [16]. Bu çalışma sayesinde kodlama teorisinde halkalarla çalışmanın önemi ortaya çıkmış ve daha sonra yapılan çalışmalar halkalar üzerinde tanımlı kodlar üzerine yoğunlaşmıştır. [16] ve [17] nolu kaynaklardan yararlanılarak Gray dönüşümü ile $\mathbb{Z}_4$ üzerindeki lineer kodlardan ikili kod elde edilmesi hakkında bilgi verilecektir.

**Tanım 2.36**

$$\begin{aligned}\Phi : \mathbb{Z}_4 &\to \mathbb{Z}_2^2 \\ 0 &\to 00 \\ 1 &\to 01 \\ 2 &\to 11 \\ 3 &\to 10\end{aligned}$$

olarak tanımlanan $\Phi$ dönüşümü birebir ve örtendir. Bu dönüşüm Gray dönüşümü olarak adlandırılır. Herhangi $u, v \in \mathbb{Z}_2^2$ vektörleri için $w(v)$ ve $d(v)$ sırasıyla Hamming ağırlığını ve Hamming uzaklığını temsil etsin. Herhangi $x, y \in \mathbb{Z}_4$ için Lee ağırlığı ve Lee uzaklığı aşağıdaki gibi tanımlıdır.

$$\begin{aligned}w_L(x) &= w(\Phi(x)) \\ d_L(x, y) &= d(\Phi(x), \Phi(y))\end{aligned}$$

$\mathbb{Z}_4$ ün elemanları $\mathbb{Z}_2$ nin elemanları cinsinden tek türlü ifade edilebilir,

$$x = a + 2b \in \mathbb{Z}_4,\ a, b \in \mathbb{Z}_2 .$$

Bu yazıma elemanların 2-li (2-adic) temsili denir. Yukarıda tanımlı $\Phi$ dönüşümü aşağıdaki gibi elemanların 2-li temsili cinsinden ifade edilebilir.

$$\begin{aligned}\Phi : \mathbb{Z}_4 &\to \mathbb{Z}_2^2 \\ a + 2b &\to (b, a + b)\end{aligned}$$

$\Phi$ dönüşümünün $\mathbb{Z}_4$ üzerindeki lineer kodlara uygulanışı aşağıdaki gibidir. $x=(x_1,x_2,...,x_n)\in\mathbb{Z}_4^n$ ve $x_i=a_i+2b_i,\ a_i,b_i\in\mathbb{Z}_2$ olsun. $a=(a_1,a_2,...,a_n)\in\mathbb{Z}_2^2$ ve $a+b=(a_1+b_1,a_2+b_2,...,a_n+b_n)\in\mathbb{Z}_2^2$ olmak üzere $\Phi(x)=(b,a+b)$ dir [16].

**Örnek 2.17** $C=\{(0,0),(2,2)\}$ bir $\mathbb{Z}_4$-lineer koddur. $C$ nin kodsözlerinin Gray dönüşümü altındaki görüntüsü

$$\Phi(0,0)=(0,0,0,0)\ \text{ve}\ \Phi(2,2)=(1,1,1,1)$$

şeklindedir. Dolayısıyla $\Phi(C)=\{(0,0,0,0),(1,1,1,1)\}$ bu kodun Gray dönüşümü altındaki görüntüsüdür.

## 2.5 Galois Halkaları

Galois halkaları teorisi ilk olarak W. Krull (1924) tarafından ortaya atılmıştır. Bu başlık altında [11] nolu kaynaktan yararlanılarak Galois halkalarının tanımı ve bazı yapısal özellikleri hakkında bilgi verilecektir. Galois halkalarına geçmeden önce Galois halkalarının tanımında kullanılacak olan Hensel Lemma ve Hensel Lift konusuna değinilecektir.

### 2.5.1 Hensel Lemma ve Hensel Lift

$p$ bir asal sayı ve $s$ bir pozitif tamsayı olmak üzere $\mathbb{Z}_{p^s}=\{0,1,2,...,p^{s-1}\}$ kümesi tamsayıların $\bmod p^s$ ye göre kalan sınıflarının halkasıdır. $\mathbb{Z}_{p^s}$ halkasının birimselleri $p$ ile aralarında asal olan elemanlarıdır.

**Teorem 2.21** $\mathbb{Z}_{p^s}$ nin tüm idealleri temel idealdir ve $\langle 1\rangle,\langle p\rangle,\langle p^2\rangle,...,\langle p^{s-1}\rangle$ ve $\langle 0\rangle$ dan ibarettir. $\langle p\rangle$ ideali bu halkanın tek maksimal idealidir ve $\mathbb{Z}_{p^s}/\langle p\rangle\cong F_p$ dir [11].

$\mathbb{Z}_{p^s}$ halkasının elemanları, $c_i\in\mathbb{Z}_p$ olmak üzere, $c_0+c_1p+...+c_{s-1}p^{s-1}$ formunda tek türlü olarak ifade edilebilir.

$$-:\quad \mathbb{Z}_{p^s}\to F_p$$
$$c_0+c_1p+...+c_{s-1}p^{s-1}\to c_0$$

olarak tanımlı $-$ dönüşümü örten bir homorfizma ve bu homomorfizmanın çekirdeği $\langle p \rangle$ dir. $a \in \mathbb{Z}_{p^s}$ elemanının bu homorfizma altındaki görüntüsü $\overline{a} \in F_p$ olarak gösterilir. Bu homomorfizma $\mathbb{Z}_{p^s}$ halkasından $\mathbb{Z}_{p^s}[x]$ polinom halkasına genişletilebilir.

$$\begin{gathered} -: \mathbb{Z}_{p^s}[x] \to F_p[x] \\ a_0 + a_1 x + \ldots + a_n x^n \to \overline{a}_0 + \overline{a}_1 x + \ldots + \overline{a}_n x^n, \quad a_i \in \mathbb{Z}_{p^s} \end{gathered} \tag{2.1}$$

olarak tanımlı $-$ dönüşümü örten bir homomorfizmadır ve bu homomorfizmanın çekirdeği $\langle p \rangle$ dir. $f(x) \in \mathbb{Z}_{p^s}[x]$ elemanının görüntüsü $\overline{f}(x) \in F_p[x]$ dir.

$g_1, g_2 \in F_p[x]$ olsun. $F_p[x]$ te $g_1$ ve $g_2$ polinomlarının ortak böleni yoksa $g_1$ ve $g_2$ aralarında asaldır. Benzer şekilde $f_1, f_2 \in \mathbb{Z}_{p^s}[x]$ ve $\mathbb{Z}_{p^s}[x]$ te $\lambda_1 f_1 + \lambda_2 f_2 = 1$ olacak şekilde $\lambda_1, \lambda_2 \in \mathbb{Z}_{p^s}[x]$ polinomları varsa $f_1$ ve $f_2$ aralarında asaldır.

**Önerme 2.7** $f_1, f_2 \in \mathbb{Z}_{p^s}[x]$ olsun. $\mathbb{Z}_{p^s}[x]$ te $f_1$ ve $f_2$ polinomlarının aralarında asal olması için gerek ve yeter koşul $F_p[x]$ te $\overline{f_1}$ ve $\overline{f_2}$ polinomlarının aralarında asal olmasıdır [11].

**Önerme 2.8 (Hensel Lemma)** $f \in \mathbb{Z}_{p^s}[x]$ monik bir polinom ve $F_p[x]$ te $g_1$ ve $g_2$ aralarında asal monik polinomlar olmak üzere $\overline{f} = g_1 g_2$ olsun. Bu durumda $\mathbb{Z}_{p^s}[x]$ te $f = f_1 f_2$ ve $\overline{f_1} = g_1, \ \overline{f_2} = g_2$ olacak şekilde $f_1, f_2 \in \mathbb{Z}_{p^s}[x]$ polinomları vardır [11].

**Tanım 2.37** $f(x) \in \mathbb{Z}_{p^s}[x]$ monik polinom ve $\overline{f}(x)$ polinomu $F_p[x]$ te indirgenemez ise $f(x)$ polinomu $\mathbb{Z}_{p^s}[x]$ te monik temel indirgenemez polinomdur denir [11].

**Teorem 2.22** Herhangi bir $m \geq 1$ tamsayısı için $\mathbb{Z}_{p^s}[x]$ te derecesi $m$ olan monik temel indirgenemez polinom vardır ve bu polinom $\mathbb{Z}_{p^s}[x]$ te $x^{p^m - 1} - 1$ polinomunu böler [11].

**Tanım 2.38** $g(x) \in F_p[x]$ ve $f(x) \in \mathbb{Z}_{p^s}[x]$ monik polinomlar olsun. $\overline{f}(x) = g(x)$ ve $\mathbb{Z}_{p^s}[x]$ te $f(x) \mid (x^n - 1)$ olacak şekilde $p$ ile aralarında asal bir $n$ tamsayısı var ise $f(x)$ polinomuna $g(x)$ in $\mathbb{Z}_{p^s}[x]$ teki Hensel lifti denir [11].

**Teorem 2.23** $s$ bir tamsayı $s \geq 1$ ve $g(x) \in F_p[x]$ monik polinom olsun. $g(x)$ in $\mathbb{Z}_{p^s}[x]$ te Hensel lifti olması için gerek ve yeter koşul $x \nmid g(x)$ olması ve $F_p[x]$ te $g(x)$ in katlı kökü olmamasıdır [11].

**Teorem 2.24** $s$ bir tamsayı $s \geq 1$ ve $g(x) \in F_p[x]$ monik polinom olsun. $x \nmid g(x)$ ve $F_p[x]$ te $g(x)$ in katlı kökü yok ise $g(x)$ polinomunun $\mathbb{Z}_{p^s}[x]$ te Hensel lifti vardır ve tek türlüdür [11].

Graeffe metodu ile $\mathbb{Z}_2$ deki polinomların $\mathbb{Z}_4$ teki Hensel liftlerini bulmak mümkündür. Aşağıdaki teorem bu metodu açıklamaktadır.

**Teorem 2.25** $f_2(x)$ polinomu $\mathbb{Z}_2[x]$ te katlı kökü olmayan ve $x$ ile bölünemeyen bir polinom olsun.

- **i.** $f_2(x)$ polinomunun çift dereceli terimlerini içeren polinom $e(x)$ ve tek dereceli terimlerini içeren polinom $d(x)$ olmak üzere $f_2(x) = e(x) - d(x)$ olarak yazılabilir.
- **ii.** $\mathbb{Z}_4[x]$ te $e(x)^2 - d(x)^2$ polinomu derecesi $2der(f_2(x))$ olan ve sadece çift dereceli terimler içeren bir polinomdur.
- **iii.** $der(e(x)) > der(d(x))$ ise $+$, $der(d(x)) > der(e(x))$ ise $-$ olmak üzere $f(x^2) = \pm(e(x)^2 - d(x)^2)$ polinomu $f_2(x)$ in $\mathbb{Z}_4[x]$ teki Hensel liftidir [11].

**Örnek 2.18** $f_2(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$ olsun. $f_2(x) = e(x) - d(x)$ olarak düzenlendiğinde $e(x) = x^2 + 1$ ve $d(x) = -x$ dir. Bu durumda

$$e(x)^2 - d(x)^2 = x^4 + x^2 + 1 \in \mathbb{Z}_4[x] \text{ dir.}$$

Böylece $f(x)=x^2+x+1$ polinomu $\mathbb{Z}_4[x]$ te $f_2(x)=x^2+x+1$ polinomunun Hensel liftidir [11].

### 2.5.2 Galois Halkalarının İnşası ve Özellikleri

**Tanım 2.39** Birimli ve sonlu bir halkanın sıfır bölenleri ile sıfırından oluşan küme, $p$ asal sayı olmak üzere, $\langle p\rangle$ şeklinde bir temel ideal oluyorsa bu halka Galois halkası olarak adlandırılır [11].

**Örnek 2.19** $\mathbb{Z}_{p^s}$ halkası bir Galois halkasıdır. $\mathbb{Z}_{p^s}$ nin tüm sıfır bölenleri ve $0$ elemanından oluşan küme $\langle p\rangle$ idealidir [11].

Aşağıdaki örnekte $(p^s)^m$ elemalı bir Galois halkasının bulunuşunda izlenen yöntem gösterilecektir.

**Örnek 2.20** $h(x)\in\mathbb{Z}_{p^s}[x]$ polinomu derecesi $m$ olan monik temel indirgenemez polinom olsun. O halde $\mathbb{Z}_{p^s}[x]\big/\langle h(x)\rangle$ bir bölüm halkasıdır ve elemanları

$$a_0+a_1x+\ldots+a_{m-1}x^{m-1}+\langle h(x)\rangle,\quad a_i\in\mathbb{Z}_{p^s}\quad 0\le i\le m-1$$

şeklindedir. Dolayısıyla $\left|\mathbb{Z}_{p^s}[x]\big/\langle h(x)\rangle\right|=p^{sm}$ dir. $\mathbb{Z}_{p^s}[x]\big/\langle h(x)\rangle$ de $\langle p+\langle h(x)\rangle\rangle$ temel idealdir. $\langle p+\langle h(x)\rangle\rangle$ idealinin

$$\left[a_0+a_1x+\ldots+a_{m-1}x^{m-1}+\langle h(x)\rangle\right]\left[p+\langle h(x)\rangle\right],\ a_i\in\mathbb{Z}_{p^s}$$

şeklindeki herhangi bir elemanı için

$$\left[p^{s-1}+\langle h(x)\rangle\right]\left[a_0+a_1x+\ldots+a_{m-1}x^{m-1}+\langle h(x)\rangle\right]\left[p+\langle h(x)\rangle\right]=\langle h(x)\rangle$$

olduğundan $\langle p+\langle h(x)\rangle\rangle$ nin elemanları ya sıfır bölen ya da sıfırdır.

2.1 nolu denklemde verilen homomorfizma kullanılarak tanımlanan

$$-:\mathbb{Z}_{p^s}[x]\big/\langle h(x)\rangle\to F_p[x]\big/\langle\overline{h}(x)\rangle$$
$$a_0+a_1x+\ldots+a_{m-1}x^{m-1}+\langle h(x)\rangle\to\overline{a}_0+\overline{a}_1x+\ldots+\overline{a}_{m-1}x^{m-1}+\langle\overline{h}(x)\rangle,\quad a_i\in\mathbb{Z}_{p^s}$$

dönüşümü örten bir homomorfizmadır ve bu homomorfizmanın çekirdeği $\langle p+\langle h(x)\rangle\rangle$ olarak bulunur. Temel homomorfizma teoreminden

$$\left(\mathbb{Z}_{p^s}[x]/\langle h(x)\rangle\right)/\langle p+\langle h(x)\rangle\rangle \cong F_p[x]/\langle \overline{h}(x)\rangle$$

sonucu elde edilir. $h(x)$ polinomu $\mathbb{Z}_{p^s}[x]$ te temel indirgenemez olduğundan $\overline{h}(x)$ polinomu $F_p[x]$ te indirgenemezdir. Dolayısıyla $F_p[x]/\langle \overline{h}(x)\rangle$ cisimdir ve böylece $\langle p+\langle h(x)\rangle\rangle$ ideali $\mathbb{Z}_{p^s}[x]/\langle h(x)\rangle$ halkasının maksimal idealidir.

$a(x)+\langle h(x)\rangle \in \mathbb{Z}_{p^s}[x]/\langle h(x)\rangle$ ve $a(x)+\langle h(x)\rangle \notin \langle p+\langle h(x)\rangle\rangle$ olsun. $\langle p+\langle h(x)\rangle\rangle$ maksimal olduğundan $\langle a(x)+\langle h(x)\rangle, p+\langle h(x)\rangle\rangle$ ideali tüm halkayı üretir. O halde

$$1+\langle h(x)\rangle = \left[b(x)+\langle h(x)\rangle\right]\left[a(x)+\langle h(x)\rangle\right]+\left[c(x)+\langle h(x)\rangle\right]\left[p+\langle h(x)\rangle\right]$$

olacak şekilde $a(x), b(x) \in \mathbb{Z}_{p^s}[x]/\langle h(x)\rangle$ elemanları vardır ve böylece

$$1+\langle h(x)\rangle = b(x)a(x)+pc(x)+\langle h(x)\rangle$$

elde edilir. $1+\langle h(x)\rangle$ bu halkanın birimi olduğundan $1+\langle h(x)\rangle = \left(1+\langle h(x)\rangle\right)^{p^{s-1}}$ dir. Böylece

$$\begin{aligned} 1+\langle h(x)\rangle &= \left[b(x)a(x)\right]^{p^{s-1}}+\langle h(x)\rangle \\ &= \left[a(x)+\langle h(x)\rangle\right]\left[b(x)^{p^{s-1}}a(x)^{p^{s-1}-1}+\langle h(x)\rangle\right] \end{aligned}$$

elde edilir ve $a(x)+\langle h(x)\rangle$ elemanının birimsel olduğu görülür. Sonuç olarak bu halkada $\langle p+\langle h(x)\rangle\rangle$ idealinin dışında kalan tüm elemanlar birimsel olduğundan $\langle p+\langle h(x)\rangle\rangle$ ideali tüm sıfır bölenleri ve sıfırı içeren temel ideal aynı zamanda tek maksimal idealdir. Böylece $\mathbb{Z}_{p^s}[x]/\langle h(x)\rangle$ halkasının bir Galois halkası olduğu kanıtlanmış olur.

**Teorem 2.26** $h(x) \in \mathbb{Z}_q[x]$ polinomu derecesi $m$ olan monik ve temel indirgenemez bir polinom ve $q=p^s$ olsun. Bu durumda $\mathbb{Z}_q[x]/\langle h(x)\rangle$ halkası karakteristiği $q$, eleman

sayısı $q^m = p^{sm}$ olan bir Galois halkasıdır ve $GR(q^m)$ olarak gösterilir. $\mathbb{Z}_q$ bu halkanın bir alt halkasıdır [11].

**Teorem 2.27** $p$ bir asal sayı ve $s$ ve $m$ pozitif tam sayılar olmak üzere $R$, karakteristiği $q = p^s$ ve eleman sayısı $q^m = p^{sm}$ olan bir Galois halkası olsun. Bu durumda derecesi $m$ olan herhangi bir $h(x) \in \mathbb{Z}_q[x]$ monik ve temel indirgenemez polinomu için $R$ halkası $\mathbb{Z}_q[x]/\langle h(x)\rangle$ ye izomorftur [11].

$GR(q^m)$ halkasının elemanlarının farklı ifade şekilleri mevcuttur. $\xi = x + \langle h(x)\rangle$ olsun. Bu durumda $h(\xi) = 0$ ve böylece

$$\mathbb{Z}_q[x]/\langle h(x)\rangle = \mathbb{Z}_q[\xi]$$

elde edilir. $GR(q^m)$ halkasının tüm elemanları,

$$a = a_0 + a_1\xi + a_2\xi^2 + \ldots\ldots + a_{m-1}\xi^{m-1}, \quad a_i \in \mathbb{Z}_q \quad (0 \le i \le m-1)$$

şeklinde tek türlü olarak yazılabilir. $\tau_m = \{0, 1, \xi, \xi^2, \ldots, \xi^{p^m-2}\}$ kümesine $GR(q^m)$ halkasının Teichmüller kümesi denir. $GR(q^m)$ halkasının elemanları aynı zamanda

$$c = c_0 + c_1 p + \ldots + c_{s-1}p^{s-1}, \quad c_i \in \tau_m \ (0 \le i \le s-1)$$

olarak da tek türlü yazılabilir. Bu yazıma elemanların $p$ -li (p-adic) temsili denir [11].

$GR(q^m)$ halkası üzerinde Frobenius otomorfizması $\theta$

$$\theta(a) = a_0 + a_1\xi^p + a_2\xi^{2p} + \ldots\ldots + a_{m-1}\xi^{(m-1)p}, \quad a_i \in \mathbb{Z}_q \ (0 \le i \le m-1)$$

olarak tanımlıdır. $GR(q^m)$ halkasının otomorfizmalar grubu mertebesi $m$ olan devirli bir gruptur ve bu grup $\theta$ tarafından üretilir. $\sigma$, $GR(q^m)$ üzerinde tanımlı bir otomofizma ve $|\langle\sigma\rangle| = t$ ise $\sigma = \theta^d$ ve $m = td$ dir. $GR(q^m)$ halkasının alt halkası $GR(q^d)$ $\sigma$ altında sabittir [10].

**Örnek 2.21** $m=3$ ve $q=4$ olsun. $g(x)=x^3+x+1$ polinomu $\mathbb{Z}_2[x]$ te monik ve indirgenemezdir. $g(x)$ polinomunun $\mathbb{Z}_4[x]$ teki Hensel liftinin bulunuşu aşağıdaki gibidir.

$g(x)=e(x)-d(x)$ olarak düzenlendiğinde $e(x)=x^3+x$ ve $d(x)=-1$ dir.

$$h(x^2)=e(x)^2-d(x)^2=x^6+2x^4+x^2-1$$

elde edilir. Böylece $h(x)=x^3+2x^2+x-1$ polinomu $g(x)$ in $\mathbb{Z}_4[x]$ teki Hensel liftidir ve dolayısıyla $h(x)$ temel indirgenemezdir. $\xi=x+\langle h(x)\rangle$ olsun. Bu durumda $\mathbb{Z}_4[\xi]\cong GR(4^3)$ dir [17].

# BÖLÜM 3

## SKEW POLİNOM HALKASI

Değişmeli olmayan polinomlar teorisi ilk olarak Oystein Ore (1933) tarafından ortaya atılmış, Nathan Jacobson (1943) ve Bernard R. McDonald (1974) tarafından geliştirilmiştir. Bu bölümde skew polinom halkalarının tanımı ve temel özellikleri hakkında bilgi verilecektir.

$F$ ; karakteristiği $p$ olan sonlu bir cisim , $\theta$ ; $F$ üzerinde tanımlı bir otomorfizma ve $\theta$ nın mertebesi $\left|\langle\theta\rangle\right| = m$ olsun. $K$ , $\theta$ tarafından sabit bırakılan $F$ cisminin bir alt cismi olsun. Bu durumda $\left[F : K\right] = m$ dir. Ayrıca $K = F_{p^t}$ iken $F = F_q$ ise $q = p^{tm}$ olur. Her $a \in F$ için $\theta(a) = a^{p^t}$ şeklindedir. Bu başlık altındaki tanımlarda ve teoremlerde bu notasyonlar kullanılacaktır.

**Örnek 3.1** $\alpha^2 + \alpha + 1 = 0$ olmak üzere $F_4 = \left\{0, 1, \alpha, \alpha^2\right\}$ cismi üzerinde tanımlı Frobenius otomorfizması;

$$\theta : F_4 \to F_4$$
$$a \to a^2$$

şeklindedir. Bu durumda $\theta(0) = 0$, $\theta(1) = 1$, $\theta(\alpha) = \alpha^2$, $\theta(\alpha^2) = \alpha$ olacaktır. Dolayısıyla $F_2 = \left\{0, 1\right\}$ cismi $\theta$ tarafından sabit bırakılan alt cisimdir ve $\theta$ nın mertebesi 2 dir [7].

**Örnek 3.2** $F_9 = \left\{a + b\gamma \,\middle|\, a, b \in F_3,\ \gamma^2 = 2\gamma + 1\right\}$ cismi üzerinde tanımlı Frobenius otomorfizması $k \in F_9$ olmak üzere;

$$\theta : F_9 \to F_9$$
$$k \to k^3$$

şeklindedir. Bu durumda $\theta(0)=0$, $\theta(1)=1$, $\theta(2)=2$ ve $\theta(a+b\gamma)=(a+b\gamma)^3=a^3+2b^3+2b^3\gamma=a+2b+2b\gamma$ olacaktır. Dolayısıyla $F_3=\{0,1,2\}$ cismi $\theta$ tarafından sabit bırakılan alt cisimdir ve $\theta$ nın mertebesi 2 dir.

**Tanım 3.1** Skew polinomların kümesi;

$$F[x;\theta]=\left\{ f(x)=a_0+a_1x+...+a_n\,x^n \middle| a_i\in F, \forall i\in\{0,1,...,n\}\right\}$$

şeklindeki polinomlardan oluşur. Bu küme üzerinde toplama işlemi standart tanımlı olup çarpma işlemi ise

$$(ax^i)*(bx^j)=a\theta^i(b)x^{i+j}$$

kuralı ile belirlidir [2].

**Örnek 3.3** Örnek 3.1'deki otomorfizmayı kullanarak aşağıdaki çarpma işlemlerini inceleyelim;

$$(\alpha x)*(\alpha^2 x)=\alpha\theta(\alpha^2)x^2=\alpha^2x^2$$
$$(\alpha^2 x)*(\alpha x)=\alpha^2\theta(\alpha)x^2=\alpha x^2.$$

$F_4[x;\theta]$ kümesinin tanımlanan çarpma işlemine göre değişmeli olmadığı açıktır [7].

**Teorem 3.1** Toplama ve çarpma işlemlerinin yukarıdaki şekilde tanımlandığı $F[x;\theta]$ kümesi bir halka belirtir. $\theta$ birimden farklı ise $F[x;\theta]$ değişmeli olmayan bir halkadır. Bu halkaya skew polinom halkası denir ve aşağıdaki özellikleri sağlar [2].

- **i.** $F[x;\theta]$ halkasının sıfır böleni yoktur.
- **ii.** $F[x;\theta]$ halkasının birimselleri $F$ cisminin birimselleridir.
- **iii.** $der(f+g)\le \max\{der(f),der(g)\}$
- **iv.** $der(f*g)=der(f)+der(g)$

**Teorem 3.2** (Bölme Algoritması) $F[x;\theta]$ halkasındaki herhangi iki polinom $f\neq 0$ ve $g$ için

$$g = q * f + r \ , \ der(r) < der(f)$$

olacak şekilde $q, r \in F\left[x;\theta\right]$ vardır ve tek türlüdür [2].

Yukarıdaki teoremde $g$ polinomu $f$ polinomu ile sağdan bölünmüştür. Aynı teorem soldan bölme için de geçerlidir. Dolayısıyla $F[x;\theta]$ halkası için bölme algoritması sağdan ve soldan sağlanır.

**Not:** Bu tezde $\alpha^2 = \alpha + 1$, $F_4^* = \langle \alpha \rangle$ ve $\theta(a) = a^2$ ile belirli skew polinom halkası $F_4[x;\theta]$; $\gamma^2 = 2\gamma + 1$, $F_9^* = \langle \gamma \rangle$ ve $\theta(a) = a^3$ ile belirli skew polinom halkası $F_9[x;\theta]$ ile gösterilecektir.

**Örnek 3.4** $F_4[x;\theta]$ halkasında $x^2 - 1 = (x - \alpha)(x - \alpha^2)$ eşitliği sağlanır. Burada $x - \alpha$ polinomu $x^2 - 1$ polinomunun bir sol böleni ve $x - \alpha^2$, $x^2 - 1$ polinomunun bir sağ bölenidir. Fakat $\alpha$ ve $\alpha^2$ bu polinomun bir kökü değildir.

$$(\alpha)^2 - 1 = \alpha^2 - 1 = \alpha, \ (\alpha^2)^2 - 1 = \alpha - 1 = \alpha^2 .$$

Skew polinom halkalarında bir polinomun köklerini ve indirgenemez ayrışımını belirlemek değişmeli polinom halkalarında olduğu gibi kolay değildir. Literatürde bir skew polinomun çarpanlarına ayrılışı ile ilgili algoritmaların belirlendiği çalışmalar vardır [19,20]. Fakat bu çalışmalar da uygulama hususunda çok kolaylık sağlamadığından bu tezde örnekler oluşturmak için skew polinomların indirgenemez ayrışımları ve diğer işlemler C++ programı yardımıyla bulunmuştur.

### 3.1 $F[x;\theta]$ Halkasında İdeal Kavramı

$I$, $F[x;\theta]$ halkasının bir sol ideali ve $I$ idealindeki en küçük dereceli sıfırdan farklı polinom $f$ olsun. $g$ polinomu $I$ idealindeki herhangi bir polinom olmak üzere

$$g = q * f + r \ , \ \ der(r) < der(f)$$

sağlanır. Fakat $r = g - q * f \in I$ ve $f$ idealdeki en küçük dereceli polinom olduğundan $r = 0$ olmak zorundadır. Bu durumda

$$g = q * f \ , \quad \forall g \in I$$

sağlanır. Dolayısıyla $I$ ideali $F[x;\theta]$ halkasında temel sol idealdir. Benzer şekilde $F[x;\theta]$ halkasındaki tüm sağ idealler temel idealdir. Dolayısıyla $F[x;\theta]$ halkası değişmeli olmayan temel ideal bölgesidir [2].

**Tanım 3.2** $I \subseteq F[x;\theta]$ olsun.

$$I = F\left[x;\theta\right] * g$$
$$I = f * F\left[x;\theta\right]$$

olacak şekilde $f, g \in F[x;\theta]$ varsa $I$ ideali hem sağ hem de sol idealdir. Böyle bir $I$ idealine çift taraflı ideal veya kısaca ideal denir [2].

**Önerme 3.1** $I$ çift taraflı bir ideal olsun. $I$ idealinin sol üreteci aynı zamanda sağ üretecidir [2].

**İspat:** $I$ çift taraflı bir ideal olsun. Bu durumda $I = F\left[x;\theta\right] * g$ ve $I = f * F\left[x;\theta\right]$ olacak şekilde $f, g \in F[x;\theta]$ vardır. Böylece $fs = g$ eşitliğini sağlayan bir $s \in F[x;\theta]$ ve $tg = f$ eşitliğini sağlayan bir $t \in F[x;\theta]$ bulunabilir.

$tf \in I$ olduğundan $tf = ft'$ olacak şekilde $t' \in I$ vardır.

$f = tg = tfs = ft's$ ve $F[x;\theta]$ halkası sıfır bölensiz olduğu için $1 = t's$ olacaktır. Bu durumda $s$ elemanı birimseldir. Benzer şekilde $t$ elemanı da birimsel olarak bulunur. Dolayısıyla $f$ ile $g$ ilgilidir. ■

**Teorem 3.3** $\left|\langle\theta\rangle\right| = m$ ve $a_i \in K$ olsun. $F[x;\theta]$ halkasındaki herhangi bir çift taraflı idealin üreteci;

$$f(x) = (a_0 + a_1 x^m + a_2 x^{2m} + .... + a_r x^{mr}) * x^t \qquad (t \in \mathbb{Z}^+ \cup \{0\})$$

formundadır [2].

**İspat:** $f(x) = a_0 x^t + a_1 x^{t+1} + a_2 x^{t+2} + .... + a_r x^{t+r}$ polinomu bir idealin üreteci olsun. Herhangi $\beta \in F$ için $\beta x^t = x^t \delta$ eşitliğini sağlayan $\beta = \theta^t(\delta)$, $\delta \in F$ mevcuttur. Dolayısıyla $x^t$ tarafından üretilen ideal çift taraflıdır. $g(x) = a_0 + a_1 x + a_2 x^2 + .... + a_r x^r$, $a_0 \neq 0$ ve $g$ çift taraflı bir idealin üreteci olsun. Bu durumda herhangi $\beta \in F$ için $\beta g(x) = g(x)\delta$ olacak şekilde bir $\delta \in F$ mevcuttur.

$$g(x)\delta = (a_0 + a_1x + a_2x^2 + .... + a_rx^r)\delta$$
$$= a_0\delta + a_1\theta(\delta)x + a_2\theta^2(\delta)x^2 + .... + a_r\theta^r(\delta)x^r$$
$$\beta g(x) = \beta a_0 + \beta a_1x + \beta a_2x^2 + .... + \beta a_rx^r$$

Buradan $\beta = \delta,\ \beta = \theta(\delta),\ \beta = \theta^2(\delta), ...., \beta = \theta^r(\delta)$ elde edilir. Bu eşitlik ancak $x$ değişkenlerinin derecelerinin $m$ nin bir katı olması durumunda sağlanır.

**Sonuç 3.1** $x^s - 1$ polinomunun $F[x;\theta]$ halkasında ürettiği ideal $\langle x^s - 1\rangle$ olsun. $\langle x^s - 1\rangle$ idealinin çift taraflı bir ideal olması için gerek ve yeter koşul $m|s$ olmasıdır [7].

**Tanım 3.3** $R$ bir halka olsun.

$$Z(R) = \{a \,|\, ab = ba \ \forall b \in R\}$$

kümesine $R$ halkasının merkezi denir [18].

**Sonuç 3.2** $Z\left(F[x;\theta]\right) = \{f = a_0 + a_1x^m + ... + a_r\, x^{mr} \,|\, a_i \in K, \left|\langle\theta\rangle\right| = m\}$ kümesi $F[x;\theta]$ halkasının merkezidir [2].

**Önerme 3.2** $x^n - 1 \in Z\left(F[x;\theta]\right) \Leftrightarrow m|n$ [4].

**İspat:** $(\Leftarrow)$ $m|n$ ve $f(x) = a_0 + a_1x + ... + a_rx^r \in F[x;\theta]$ olsun. Bu durumda her $a \in F$ için $\theta^n(a) = a$ olur.

$$(x^n - 1) * f(x) = (x^n - 1) * (a_0 + a_1x + ... + a_rx^r)$$
$$= x^n * a_0 + x^n * a_1x + ... + x^n * a_rx^r - f(x)$$
$$= \theta^n(a_0)x^n + \theta^n(a_1)x^n.x + ... + \theta^n(a_r)x^n.x^r - f(x)$$
$$= a_0x^n + a_1x^n.x + ... + a_rx^n.x^r - f(x)$$
$$= a_0 * x^n + a_1x * x^n + ... + a_rx^r * x^n - f(x)$$
$$= (a_0 + a_1x + ... + a_rx^r) * x^n - f(x)$$
$$= f(x) * (x^n - 1).$$

Dolayısıyla $x^n - 1 \in Z\left(F[x;\theta]\right)$ dir.

$(\Rightarrow)$ $x^n - 1 \in Z\left(F[x;\theta]\right)$ olsun. Bu durumda her $f \in F[x;\theta]$ için $f(x)(x^n - 1) = (x^n - 1)f(x)$ olur. Özel olarak $f(x) = ax^m \in F[x;\theta]$ alındığında

$(x^n-1)*ax^m=\theta^n(a)x^{n+m}-ax^m$ ve $ax^m*(x^n-1)=ax^{n+m}-ax^m$ elde edilir. Buradan her $a\in F$ için $\theta^n(a)=a$ olacaktır, bu da ancak $m|n$ iken mümkündür. ■

**Örnek 3.5** $F_4[x;\theta]$ halkasında $\theta$ nın mertebesi $2$ olduğundan $n$ çift ise $x^n-1$ polinomu merkezdedir.

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

Fakat $(\alpha x^2+\alpha^2 x)(x^3-1)=\alpha x^5+\alpha^2 x^4-\alpha x^2-\alpha^2 x$ ve

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

olduğundan $x^3-1$ polinomu merkezde değildir.

**Önerme 3.3** $hg\in Z(F[x;\theta])$ ise $gh=hg$ sağlanır [8].

**Sonuç 3.3** Merkezdeki bir polinomun sol böleni aynı zamanda sağ bölenidir.

## 3.2 $F[x;\theta]\big/\langle x^n-1\rangle$ in Cebirsel Yapısı

$m|n$ ise $I=\langle x^n-1\rangle$ ideali $F[x;\theta]$ halkasında çift taraflı bir idealdir. $R=F[x;\theta]$ ve $R_{n,\theta}=R\big/\langle x^n-1\rangle$ olsun. $R_{n,\theta}$ kümesi üzerinde toplama işlemi iyi tanımlıdır. $R_{n,\theta}$ kümesi üzerinde çarpma işlemi ise

$$\begin{aligned}(f+I)*(g+I)&=f*g+f*I+I*g+I\\&=f*g+(f+g')*I+I\\&=f*g+I\end{aligned}$$

olarak iyi tanımlıdır. Dolayısıyla $R_{n,\theta}$ bir halkadır. $m\nmid n$ ise çarpma işlemi iyi tanımlı olmadığından $R_{n,\theta}$ halka olmayabilir. Dolayısıyla $R_{n,\theta}$ nın ideallerinden bahsedilemez. Fakat $R_{n,\theta}$ kümesi bir sol $F[x;\theta]$-modül olarak ele alınabilir ve bu küme üzerinde

$$r*(f+I)=r*f+I\quad\forall r\in F[x;\theta]$$

modül çarpımı tanımlanabilir [4].

**Örnek 3.6** $F_4[x;\theta]$ halkasında $\left|\langle\theta\rangle\right| = 2$ dir. $2 \nmid 3$ olduğundan $R_{3,\theta} = F_4[x;\theta] \Big/ \langle x^3 - 1 \rangle$ bir sol $F_4[x;\theta]$-modül olarak ele alınabilir. $F_4[x;\theta]$ halkasında $x^3 - 1 = (x+1)(x^2+x+1)$ dir. $I' = F_4[x;\theta] * (x+1) = \langle x+1 \rangle$, $R_{3,\theta}$ nın bir sol alt modülüdür. Bu alt modülün tüm elemanları ve elemanlarına karşılık gelen kodsözler ($c \in F_4^3$) aşağıda listelenmiştir. Örnek 4.4'te bu alt modüle karşılık gelen kodun devirli bir kod olduğu gösterilecektir.

Çizelge 3. 1 $I'$ nın elemanlarına karşılık gelen kodsözler

| $r(x) \in F_4[x;\theta]$ | $r(x) * (x+1) \in I'$ | kodsöz |
|---|---|---|
| $0$ | $0$ | $000$ |
| $1$ | $x+1$ | $110$ |
| $\alpha$ | $\alpha x + \alpha$ | $\alpha\alpha 0$ |
| $\alpha^2$ | $\alpha^2 x + \alpha^2$ | $\alpha^2\alpha^2 0$ |
| $x$ | $x^2 + x$ | $011$ |
| $\alpha x$ | $\alpha x^2 + \alpha x$ | $0\alpha\alpha$ |
| $\alpha^2 x$ | $\alpha^2 x^2 + \alpha^2 x$ | $0\alpha^2\alpha^2$ |
| $x+1$ | $x^2 + 1$ | $101$ |
| $\alpha x + 1$ | $\alpha x^2 + \alpha^2 x + 1$ | $1\alpha^2\alpha$ |
| $\alpha^2 x + 1$ | $\alpha^2 x^2 + \alpha x + 1$ | $1\alpha\alpha^2$ |
| $x + \alpha$ | $x^2 + \alpha^2 x + \alpha$ | $\alpha\alpha^2 1$ |
| $\alpha x + \alpha$ | $\alpha x^2 + \alpha$ | $\alpha 0\alpha$ |
| $\alpha^2 x + \alpha$ | $\alpha^2 x^2 + x + \alpha$ | $\alpha 1\alpha^2$ |
| $x + \alpha^2$ | $x^2 + \alpha x + \alpha^2$ | $\alpha^2\alpha 1$ |
| $\alpha x + \alpha^2$ | $\alpha x^2 + x + \alpha^2$ | $\alpha^2 1\alpha$ |
| $\alpha^2 x + \alpha^2$ | $\alpha^2 x^2 + \alpha^2$ | $\alpha^2 0\alpha^2$ |

# BÖLÜM 4

## SKEW DEVİRLİ KODLAR

Boucher vd. [3] tarafından devirli kodların üreteç polinomu değişmeli olmayan skew polinom halkalarından alınarak devirli kodların bir genellemesi elde edilmiştir. Bu yeni kod ailesi skew devirli kodlar olarak adlandırılmıştır. Daha sonra yapılan bazı çalışmalarda ise skew devirli kodlar yerine $\theta$-devirli kodlar ifadesi kullanılmıştır [6,8]. Skew polinom halkasında sağ ve sol bölme algoritması sağlandığı için bu halkalar vasıtasıyla elde edilen kodlar devirli kodlara benzer özellikler taşımaktadır.

**Tanım 4.1** $F$ sonlu bir cisim ve $\theta$, $F$ cismi üzerinde tanımlı bir otomorfizma olsun. $C$ $F^n$ uzayının bir alt kümesi olmak üzere

**i.** $C$, $F^n$ uzayının bir alt uzayı ve

**ii.** $\forall c=(c_0,c_1,....,c_{n-1})\in C$ için $\sigma(c)=\left(\theta\left(c_{n-1}\right),\theta\left(c_0\right),....,\theta\left(c_{n-2}\right)\right)\in C$

oluyorsa $C$ kümesine $n$ uzunluğunda skew devirli kod denir. $\sigma$ dönüşümüne skew devirsel öteleme (skew cyclic shift) denir [4].

$C$ kodunun kodsözleri aşağıdaki gibi polinom olarak ifade edebilir.

$$\pi:\ C\rightarrow\ F[x;\theta]\Big/\left\langle x^n-1\right\rangle$$
$$c=(c_0,c_1,.....,c_{n-1})\rightarrow c(x)=c_0+c_1x+.....+c_{n-1}x^{n-1}$$

olarak tanımlanan $\pi$ fonksiyonu bir izomorfizmadır. $c\in C$ kod sözünün $\sigma$ altındaki görüntüsü polinom yazılımında $x*c(x)=\theta(c_{n-1})+\theta(c_0)x+....+\theta(c_{n-2})x^{n-2}$ ye karşılık gelir.

$C$ , $F$ üzerinde tanımlı $n$ uzunluğunda devirli kod iken $\pi(C)$ nin $F[x]\Big/\langle x^n-1\rangle$ halkasının bir ideali olduğu gösterilmişti. Skew devirli kodlar tanımlanırken iki durum ile karşılaşılır.

$C$ , $F$ üzerinde tanımlı $n$ uzunluğunda skew devirli kod ve $|\langle\theta\rangle| = m$ olsun.

**i.** $m|n$ ise $F[x;\theta]\Big/\langle x^n-1\rangle$ bir halka belirtir. Bu durumda $\pi(C)$, $F[x;\theta]\Big/\langle x^n-1\rangle$ halkasının bir idealidir. Boucher vd. skew devirli kodların tanımını yaparken kodların uzunluğunu $m \mid n$ olarak kısıtlamıştır [3].

**ii.** $m \nmid n$ olması durumunda $F[x;\theta]\Big/\langle x^n-1\rangle$ halka belirtmez. Şiap vd. [4] te herhangi bir $n$ değeri için $\pi(C)$ yi $F[x;\theta]\Big/\langle x^n-1\rangle$ in bir sol alt modülü olarak ele almış ve uzunluk için bir önceki çalışmada verilen kısıtlamayı kaldırmışlardır.

**Teorem 4.1** $C$ , $F$ üzerinde tanımlı $n$ uzunluğunda bir lineer kod olsun. $C$ kodunun skew devirli kod olması için gerek ve yeter koşul $C$ nin $F[x;\theta]\Big/\langle x^n-1\rangle$ modülünün bir sol $F[x;\theta]$-alt modülü olmasıdır [4].

**İspat:** $C$ , $F$ üzerinde bir skew devirli kod ve $f(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1}$ polinomuna karşılık gelen kodsöz $(a_0, a_1, ..., a_{n-1}) \in C$ olsun. Bu durumda $(a_0, a_1, ..., a_{n-1})$ elemanının tüm skew devirsel ötelemeleri $C$ nin bir elemanıdır. Böylece

$$x * f(x) = \theta(a_{n-1}) + \theta(a_0)x + ... + \theta(a_{n-2})x^{n-1}$$
$$\vdots$$
$$x^i * f(x) = \theta^i(a_{n-i}) + \theta^i(a_{n-i+1})x + ... + \theta^i(a_{n-i-1})x^{n-1}$$

şeklindeki polinomlara karşılık gelen kodsözler $C$ nin elemanıdır. $C$ lineer olduğundan herhangi $r(x) \in F[x;\theta]$ için $r(x) * f(x) \in C$ olur. Dolayısıyla $C$ , $F[x;\theta]\Big/\langle x^n-1\rangle$ modülünün bir sol $F[x;\theta]$-alt modülüdür. ■

**Önerme 4.1** $C$ , $F[x;\theta]\Big/\langle x^n-1\rangle$ modülünün bir sol $F[x;\theta]$-alt modülü olsun. Bu durumda $C$ devirli alt modüldür ve $C$ deki sıfırdan farklı en küçük dereceli monik polinom tarafından üretilir [4].

**İspat:** $f(x)$ polinomu $C$ deki en küçük dereceli sıfırdan farklı monik polinom olsun. Eğer $C$ de $der(f(x)) = der(l(x))$ olacak şekilde monik $l(x)$ polinomu varsa $f(x) - l(x) \in C$ ve derecesi $f(x)$ den küçüktür. Bu ise $f(x)$ in en küçük dereceli oluşu ile çelişir. Bu durumda böyle bir $f(x)$ polinomu $C$ de tek türlüdür. $c(x) \in C$ olsun. Sağ bölme algoritmasından

$$c(x) = q(x) * f(x) + r(x),\ r(x) = 0 \text{ veya } der(r) < der(f)$$

olacak şekilde tek türlü belirli $q(x)$ ve $r(x)$ polinomları vardır. $C$ bir sol alt modül olduğundan $r(x) = c(x) - q(x) * f(x) \in C$ dir. Eğer $r \neq 0$ ise bu $f(x)$ in en küçük dereceli oluşu ile çelişir. O halde $r = 0$ ve $c(x) = q(x) * f(x)$ dir. Böylece $C$, $f(x)$ tarafından üretilen devirli alt modüldür, $C = \langle f(x) \rangle$ dir. ■

**Teorem 4.2** $C = \langle f(x) \rangle$, $F[x;\theta] \Big/ \langle x^n - 1 \rangle$ modülünün bir sol $F[x;\theta]$-alt modülü olsun. Bu durumda $f(x)$ polinomu $x^n - 1$ in bir sağ bölenidir [4].

**İspat:** $f(x)$ polinomu $C$ deki en küçük dereceli sıfırdan farklı monik polinom olsun. Sağ bölme algoritmasından

$$x^n - 1 = q(x) * f(x) + r(x),\ \ r(x) = 0 \text{ veya } der(r) < der(f)$$

olacak şekilde tek türlü belirli $q(x)$ ve $r(x)$ polinomları vardır. $f(x)$ ve $x^n - 1 = 0$, $C$ nin elemanları ve $C$ bir sol alt modül olduğundan $r(x) \in C$ dir. Eğer $r(x) \neq 0$ ise bu $f(x)$ in en küçük dereceli oluşu ile çelişir. O halde $r = 0$ ve $x^n - 1 = q(x) * f(x)$ dir. Dolayısıyla $f(x)$ polinomu $x^n - 1$'in bir sağ bölenidir. ■

Sonuç olarak; $x^n - 1$'in sağ bölenleri $F[x;\theta] \Big/ \langle x^n - 1 \rangle$ modülünde birer sol alt modül üretir ve $F[x;\theta] \Big/ \langle x^n - 1 \rangle$ modülünün sol alt modülleri birer skew devirli koda karşılık gelir. $x^n - 1$'in derecesi $n - k$ olan sağ böleni, $n$ uzunluğunda boyutu $k$ olan bir skew devirli kod üretir.

$\mathbb{Z}_p$ asal cisimlerinde aşikar olmayan $\theta$ otomorfizması yoktur. Aşikâr olmayan bir otomorfizmaya sahip en küçük cisim $F_4$ tür. $F[x;\theta]$ halkasında polinomların

çarpanlara ayrılışı tek türlü değildir. Çarpanların tek türlü olmaması daha fazla sayıda kod ve böylece daha iyi parametrelere sahip kod bulunması açısından avantajlıdır. Nitekim [3] te daha önce bilinenden daha iyi parametrelere sahip $F_4$ ve $F_9$ üzerinde tanımlı kod örnekleri bulunmuştur. Bunlardan bazıları $[30,16,9]_4$ , $[36,20,10]_4$ ve $[44,20,17]_9$ şeklindedir.

**Önerme 4.2** $g = g_r x^r + \ldots\ldots + g_1 x + g_0$ polinomu $F[x;\theta]$ halkasında $x^n - 1$ in bir sağ böleni olsun. Bu durumda $g$ polinomu $F$ üzerinde uzunluğu $n$, boyutu $n-r$ olan bir skew devirli kod üretir, $g$ polinomuna bu kodun üreteç polinomu denir [6].

$$G = \begin{bmatrix} g \\ xg \\ . \\ . \\ x^{n-r-1}g \end{bmatrix} = \begin{bmatrix} g_0 & \cdots & g_{r-1} & g_r & 0 & \cdots & 0 \\ 0 & \theta(g_0) & \cdots & \theta(g_{r-1}) & \theta(g_r) & \cdots & 0 \\ 0 & \ddots & & & & \ddots & \vdots \\ 0 & \ddots & & & & & 0 \\ 0 & \cdots & 0 & \theta^{n-r-1}(g_0) & \cdots & \theta^{n-r-1}(g_{r-1}) & \theta^{n-r-1}(g_r) \end{bmatrix}$$

$G$ matrisi bu kodun üreteç matrisidir.

**Örnek 4.1** $F_4$ üzerinde [4,2] parametrelerine sahip skew devirli kod bulmak için öncelikle $x^4 - 1 \in F_4[x;\theta]$ polinomunun derecesi 2 olan sağ böleni bulunmalıdır. $x^4 - 1$ in derecesi $2$ olan tüm sağ bölenleri aşağıdaki gibidir [3]:

$$\begin{aligned} x^4 - 1 &= (x^2+1)(x^2+1) \\ &= (x^2 + \alpha x + \alpha)(x^2 + \alpha x + \alpha^2) \\ &= (x^2 + \alpha^2 x + \alpha^2)(x^2 + \alpha^2 x + \alpha) \\ &= (x^2 + \alpha^2 x + \alpha)(x^2 + \alpha^2 x + \alpha^2) \\ &= (x^2 + x + \alpha^2)(x^2 + x + \alpha) \\ &= (x^2 + x + \alpha)(x^2 + x + \alpha^2) \\ &= (x^2 + \alpha x + \alpha^2)(x^2 + \alpha x + \alpha). \end{aligned}$$

$g_1 = x^2 + \alpha x + \alpha^2$ polinomu [4,2,3] parametrelerine sahip, üreteç matrisi $G_1 = \begin{pmatrix} \alpha^2 & \alpha & 1 & 0 \\ 0 & \alpha & \alpha^2 & 1 \end{pmatrix}$ olan skew devirli kod üretir. $F_4[x] \big/ \langle x^4 - 1 \rangle$ değişmeli polinom halkasında $x^4 - 1$ polinomunun derecesi $2$ olan böleni $g_2 = x^2 + 1$ dir. $g_2$ tarafından

üretilen ideal $F_4$ üzerinde $[4,2,2]$ parametrelerine sahip devirli bir koda karşılık gelir . $F_4[x]\Big/\langle x^4-1\rangle$ halkasında $x^4-1$'in ikinci dereceden başka böleni olmadığından $[4,2]$ parametrelerine sahip başka bir devirli kod yoktur. Brouwer'in tablosuna göre $F_4$ üzerinde $[4,2,3]$ parametrelerine sahip kodlar optimaldir [5]. Bu örnekte skew devirli kod ailesinin devirli kodlar ailesine göre daha iyi parametrelere sahip olduğu görülür.

**Örnek 4.2** $F_9$ üzerinde [4,2] parametrelerine sahip skew devirli kod örneği aşağıdaki gibi bulunur.

$$\begin{aligned} x^4-1 &= (x+1+\gamma)(x+1)(x^2+(1+2\gamma)x+2\gamma) \\ &= (x+2\gamma)(x+1)(x^2+(2+\gamma)x+1+\gamma) \\ &= (x+2+2\gamma)(x+1)(x^2+(\gamma)x+\gamma)\ . \end{aligned}$$

Yukarıdaki bölenler $x^4-1\in F_9[x;\theta]$ polinomunun tüm ikinci dereceden sağ bölenleri değildir. Bu şekilde toplamda 40 farklı faktorizasyonu mevcuttur. $g_1(x)=x^2+(1+2\gamma)x+2\gamma$ olarak alındığında $C=\langle g_1(x)\rangle$, $F_9$ üzerinde bir skew devirli koddur. $G_1=\begin{pmatrix} 2\gamma & 1+2\gamma & 1 & 0 \\ 0 & 1+\gamma & 2+\gamma & 1 \end{pmatrix}$ matrisi $C$ nin üreteç matrisidir. $C$ kodunun parametreleri $[4,2,3]_9$ dur. Bu parametrelere sahip bir kod [5] e göre optimal koddur.

Yukarıdaki iki örnekte de görüldüğü gibi bu kod ailesinden iyi kodlar elde edilmektedir.

**Önerme 4.3** $F[x;\theta]$ halkasında

$$g(x)=g_0+g_1x+....+g_rx^r,\ \ h(x)=h_0+h_1x+.....+h_{n-r}x^{n-r}$$

ve $x^n-1=h(x)g(x)$ olsun. $C$, $g$ polinomu tarafından üretilen $n$ uzunluğunda skew devirli kod ise

$$H=\begin{bmatrix} h_{n-r} & \theta(h_{n-r-1}) & \dots & \theta^{n-r-1}(h_1) & \theta^{n-r}(h_0) & 0 & \dots & 0 \\ 0 & \theta(h_{n-r}) & \cdots & \dots & \dots & \theta^{n-r+1}(h_0) & \dots & 0 \\ 0 & \ddots & \theta^2(h_{n-r}) & \ddots & & & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \dots & \ddots & 0 \\ 0 & \dots & \dots & 0 & \theta^{r-1}(h_{n-r}) & \dots & \theta^{n-2}(h_1) & \theta^{n-1}(h_0) \end{bmatrix}$$

matrisi $C$ kodu için kontrol matrisi ve $h_R(x) = h_{n-r} + \theta(h_{n-r-1})x + ..... + \theta^{n-r}(h_0)x^{n-r}$ kontrol polinomudur [6].

Bu önermede $h(x)$ polinomunun ters sıralısı olan $h_R(x)$ polinomu $\varphi(\sum_{i=0}^{n-r} a_i x^i) = \sum_{i=0}^{n-r} x^{-i} a_i$ fonksiyonu kullanılarak $h_R(x) = x^{n-r} * \varphi(h(x))$ eşitliğinden kolayca bulunabilir [8].

**Sonuç 4.1** $h(x)g(x) = x^n - 1 \in F[x;\theta]$ olsun. $C$, $g(x)$ tarafından üretilen skew devirli kod olmak üzere $g^{\perp}(x) = h_R(x) = h_{n-r} + \theta(h_{n-r-1})x + ..... + \theta^{n-r}(h_0)x^{n-r}$ polinomu, $C^{\perp}$ için üreteç polinomudur ve $C^{\perp}$ kodu bir skew devirli koddur [6].

**Örnek 4.3** $F_4[x;\theta]$ halkasında $x^6 - 1 = (x^2 + \alpha^2 x + 1)(x^4 + \alpha^2 x^3 + \alpha^2 x + 1)$ dir. $g(x) = x^4 + \alpha^2 x^3 + \alpha^2 x + 1$ ve $C = \langle g(x) \rangle$ olsun.

$$G = \begin{pmatrix} 1 & \alpha^2 & 0 & \alpha^2 & 1 & 0 \\ 0 & 1 & \alpha & 0 & \alpha & 1 \end{pmatrix}$$

matrisi $C$ kodu için bir üreteç matrisidir. $C$, $F_4$ üzerinde $[6,2,4]$ parametrelerine sahip skew devirli koddur. $C$ kodu Brouwer'in tablosuna göre optimal bir koddur [5]. $x^6 - 1 = h(x)g(x)$ eşitliğini sağlayan $h$ polinomu $x^2 + \alpha^2 x + 1$ dir. Bu durumda $h$ polinomunun ters sıralısı $h_R(x) = x^2(x^{-2} + x^{-1}\alpha^2 + 1) = x^2 + \theta(\alpha^2)x + 1 = x^2 + \alpha x + 1$ olarak bulunur. $h_R$ polinomu aynı zamanda $C$ nin kontrol polinomudur. Böylece

$$H = \begin{pmatrix} 1 & \alpha & 1 & 0 & 0 & 0 \\ 0 & 1 & \alpha^2 & 1 & 0 & 0 \\ 0 & 0 & 1 & \alpha & 1 & 0 \\ 0 & 0 & 0 & 1 & \alpha^2 & 1 \end{pmatrix}$$

matrisi $C$ nin kontrol matrisidir. Aynı zamanda $h_R$ polinomu $C^{\perp}$ için üreteç polinomu ve $H$ matrisi $C^{\perp}$ in üreteç matrisidir.

Abualrub vd. [7] nolu çalışmada parçalı devirli kodların genellemesi olarak skew parçalı devirli kodları tanımlamışlardır.

**Tanım 4.2** $C$, $F^n$ uzayının bir alt uzayı olsun. Her

$$c=\left(c_{0,0},c_{0,1},...,c_{0,l-1},c_{1,0},c_{1,1},...,c_{1,l-1},...,c_{s-1,0},c_{s-1,1},...,c_{s-1,l-1}\right)\in C$$

için

$$T_{\theta,s,l}(c)=\begin{pmatrix}\theta(c_{s-1,0}),\theta(c_{s-1,1}),...,\theta(c_{s-1,l-1}),\theta(c_{0,0}),\theta(c_{0,1}),\\ .....,\theta(c_{0,l-1}),...,\theta(c_{s-2,0}),\theta(c_{s-2,1}),...,\theta(c_{s-2,l-1})\end{pmatrix}\in C$$

oluyorsa $C$ ye uzunluğu $n=sl$ indeksi $l$ olan skew parçalı devirli kod veya $l$-skew parçalı devirli kod ($l$-quasi cyclic code ) denir [7].

$C'$, $F$ cismi üzerinde bir lineer kod ve $n=ms$ olmak üzere $c'=\left(c_1\left|c_2\right|...\left|c_s\right.\right)\in C'$, $c'$ kodsözünün $s$ eşit parçaya bölünmüş hali olsun. Bu durumda $\varphi_s(c')=\left(\sigma(c_1)\left|\sigma(c_2)\right|...\left|\sigma(c_s)\right.\right)\in C'$ oluyorsa $C'$ kodu, $F$ üzerinde uzunluğu $n$, indeksi $s$ olan skew parçalı devirli bir koda denktir. ($\sigma$; skew devirsel öteleme fonksiyonudur.)

### 4.1 Skew Devirli Kodların Diğer Yapılarla İlişkisi

Şiap vd. tarafından [4] te skew devirli kodların bazı şartlar altında devirli kodlar ve parçalı devirli kodlara denk oldukları bulgusuna ulaşılmıştır. Bu başlık altında ilgili teoremler örneklendirilecektir.

**Önerme 4.4** (Euclid Lemma) $a,b\in\mathbb{Z}$ ve $a$ ile $b$ nin en büyük ortak böleni $d$ olsun, $(a,b)=d$. Bu durumda $x,y\in\mathbb{Z}$ vardır öyle ki $ax+by=d$ eşitliği sağlanır.

Bu başlık altındaki teoremlerin ispatında yukarıdaki önerme kullanılacaktır.

**Teorem 4.3** $C$, $F$ üzerinde tanımlı $n$ uzunluğunda bir skew devirli kod ve $\left|\left\langle\theta\right\rangle\right|=m$ olsun. $(m,n)=1$ ise $C$ bir devirli koddur [4].

**İspat:** $g(x)\in F[x;\theta]\Big/\left\langle x^n-1\right\rangle$ ve $C=\left\langle g(x)\right\rangle$ olsun. $(m,n)=1$ iken $y_1m+y_2n=1$ eşitliğini sağlayan $y_1,y_2\in\mathbb{Z}$ vardır. $y_1m=1-y_2n$ eşitliğinde $y_2$ yi negatif tamsayı olarak alabiliriz, bu durumda $y_1m=1+Dn$ ve $D>0$ olur.

$c(x)=c_0+c_1x+...+c_{n-1}x^{n-1}\in C$ olsun. $C$ nin devirli kod olduğunu göstermek için $c_{n-1}+c_0x+...+c_{n-2}x^{n-1}\in C$ olduğunu göstermek yeterlidir.

$$x^{y_1 m} * c(x) = x^{1+Dn} * (c_0 + c_1 x + ... + c_{n-1} x^{n-1})$$
$$= \theta^{1+Dn}(c_0) x^{1+Dn} + ... + \theta^{1+Dn}(c_{n-2}) x^{1+Dn+n-2} + \theta^{1+Dn}(c_{n-1}) x^{1+Dn+n-1}$$
$$= \theta^{y_1 m}(c_0) x^{1+Dn} + ... + \theta^{y_1 m}(c_{n-2}) x^{1+Dn+n-2} + \theta^{y_1 m}(c_{n-1}) x^{1+Dn+n-1}.$$

$F[x;\theta] \Big/ \langle x^n - 1 \rangle$ halkasında $x^n = 1$ ve $a \in F$ için $\theta^{y_1 m}(a) = a$ olduğundan, $x^{y_1 m} * c(x) = c_{n-1} + c_0 x + ... + c_{n-2} x^{n-1} \in C$ dir. Böylelikle $C$, $n$ uzunluğunda bir devirli koddur. ■

**Örnek 4.4** $F_4[x,\theta]$ te $x^3 - 1$ polinomunun $x^3 - 1 = (x-1)(x^2 + x + 1)$ den başka indirgenemez ayrışımı yoktur. $g(x) = x - 1$ olarak alalım, bu durumda $C = \langle g(x) \rangle$, $F_4$ üzerinde uzunluğu $3$ boyutu $2$ olan skew devirli koddur ve $G = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ matrisi üreteç matrisidir. Bu kodun elemanları aşağıdaki gibidir:

$$C = \{000, 110, 011, 101, \alpha\alpha 0, 0\alpha\alpha, \alpha 0\alpha, \alpha^2\alpha^2 0, 0\alpha^2\alpha^2, \alpha^2 0\alpha^2,$$
$$\alpha\alpha^2 1, 1\alpha\alpha^2, \alpha^2 1\alpha, \alpha^2\alpha 1, 1\alpha^2\alpha, \alpha 1\alpha^2\}.$$

$C$, $F_4$ üzerinde $[3,2,2]$ parametrelerine sahip devirli bir koddur.

Bu tezde yukarıdaki teoremden yola çıkılarak yapılan araştırmalar neticesinde aşağıdaki teorem bulgusuna ulaşılmıştır.

**Teorem 4.4** $F_q[x;\theta]$ halkasında $g(x)$, $x^n - 1$ in bir sağ böleni ve $\theta$ altında sabit kalan alt cisim $K$ olsun. $(m,n) = 1$ ise $g(x) \in K[x]$ tir.

**İspat:** $g(x) = g_0 + g_1 x + ..... + g_{r-1} x^{r-1} + x^r$ ve $g(x)$, $x^n - 1$ in bir sağ böleni olsun. Bu durumda $C = \langle g(x) \rangle$, $F_q$ üzerinde $n$ uzunluğunda, boyutu $n - r$ olan bir skew devirli koddur.

$g(x)$, $C$ kodunun elemanları arasında en küçük dereceye sahip monik polinomdur. $(m,n) = 1$ ise $y_1 n + y_2 m = 1$ eşitliğini sağlayan $y_1, y_2 \in \mathbb{Z}$ vardır. $y_1 n = 1 - y_2 m$ eşitliğinde $y_2$ bir negatif tamsayı olarak alınabilir. Bu durumda $y_1 n = 1 + Dm$ ve $D > 0$ olur. $g(x) = g_0 + g_1 x + ..... + g_{r-1} x^{r-1} + x^r$ polinomuna karşılık gelen kodsöz $(g_0, g_1, ....., g_{r-1}, 1, 0, 0..., 0) \in C$ dir.

$$x^{y_1 n} * g(x) = \theta^{1+Dm}(g_0)x^{y_1 n} + \theta^{1+Dm}(g_1)x^{y_1 n+1} + ..... + \theta^{1+Dm}(g_{r-1})x^{y_1 n+r-1} + x^{y_1 n+r}$$
$$= \theta(g_0) + \theta(g_1)x + ..... + \theta(g_{r-1})x^{r-1} + x^r \in (g(x)).$$

Dolayısıyla $(-\theta(g_0), -\theta(g_1), ....., -\theta(g_{r-1}), -1, 0, 0, ....., 0) \in C$ dir.

Bu iki kodsözün toplamı yine $C$ nin bir kodsözüdür.

$c' = (g_0 - \theta(g_0), g_1 - \theta(g_1), ....., g_{r-1} - \theta(g_{r-1}), 0, 0, 0, ....., 0) \in C$, bu kod söze karşılık gelen polinom $c'(x) = g_0 - \theta(g_0) + (g_1 - \theta(g_1))x + ..... + (g_{r-1} - \theta(g_{r-1}))x^{r-1} \in \langle g(x) \rangle$ dir.

Bu durumda $\deg(c'(x)) < \deg(g(x))$ olur. Eğer $g_i \neq \theta(g_i)$ , $0 \leq i \leq r-1$ olacak şekilde bir $i$ varsa $g(x)$'in en küçük dereceli olması ile çelişir. O zaman her $i$; $0 \leq i \leq r-1$ için $g_i = \theta(g_i)$ olmalıdır. Bu da ancak $g(x) \in K[x]$ iken mümkündür. Dolayısıyla $(m,n)=1$ iken $x^n - 1$ in $F_q[x;\theta]$ daki indirgenemez ayrışımı tam olarak $x^n - 1$ in $K[x]$ halkasındaki indirgenemez ayrışımı olarak bulunur. ■

$F_q[x;\theta]$ skew polinom halkası tek türlü çarpanlarına ayrılabilen bir halka olmadığından $F_q$ üzerinde tanımlı skew devirli kodların sayısını tam olarak belirlemek zor bir problemdir. Fakat yukarıdaki teorem ve Teorem 4.4 sonucu olarak $(m,n)=1$ olduğu durumda skew devirli kodların sayısı belirlenebilir.

**Teorem 4.5** $(m,n)=1$ ve $x^n - 1 \in F_q[x;\theta]$ polinomunun indirgenemez çarpanlarının ayrışımı $x^n - 1 = \prod_{i=1}^{r} p_i^{s_i}(x)$ olsun. Bu durumda $F_q$ üzerinde tanımlı uzunluğu $n$ olan skew devirli kodların sayısı $\prod_{i=1}^{r}(s_i + 1)$ dir.

**Örnek 4.5** $\theta$, $F_9$ üzerinde tanımlı Frobenius otomorfizması olsun. Bu durumda $a \in F_9$ için $\theta(a) = a^3$, $\theta$ nın mertebesi $|\langle\theta\rangle| = 2$ ve $\theta$ altında sabit kalan alt cisim ise $F_3$ tür. $n = 3,5,7$ için $x^n - 1$ in $F_9[x;\theta]$ halkasındaki indirgenemez ayrışımları;

$$x^3 - 1 = (x-1)(x-1)(x-1)$$
$$x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$$
$$x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$$

şeklindedir. Her biri tam olarak $n=3,5,7$ için $x^n-1$ in $F_3[x]$ deki ayrışımıdır. Böylece $F_9$ üzerinde tanımlı $n=3$ olan skew devirli kodların sayısı $4$, $n=5$ olan skew devirli kodların sayısı $4$ ve $n=7$ olan skew devirli kodların sayısı $4$ olarak bulunur.

**Teorem 4.6** $C$, $F$ üzerinde tanımlı $n$ uzunluğunda bir skew devirli kod ve $\left|\langle\theta\rangle\right|=m$ olsun. $(m,n)=d$ ise $C$; uzunluğu $n$, indeksi $d$ olan bir parçalı devirli koddur [4].

**İspat:** $n=ds$ ve $c=\left(c_{0,0},c_{0,1},...,c_{0,d-1},c_{1,0},c_{1,1},...,c_{1,d-1},...,c_{s-1,0},c_{s-1,1},...,c_{s-1,d-1}\right)\in C$ olsun. $(m,n)=d$ olduğundan $y_1m=d+Jn$ eşitliğini sağlayan pozitif $J$ tamsayısı vardır. $x^{d+Jn}*c(x)$ e karşılık gelen kodsözü $\theta^{d+Jn}(c)$ ile gösterelim. Bu durumda

$$\theta^{d+Jn}\begin{pmatrix}c_{0,0},c_{0,1},...,c_{0,d-1},c_{1,0},c_{1,1},...,\\ c_{1,d-1},...,c_{s-1,0},c_{s-1,1},...,c_{s-1,d-1}\end{pmatrix}$$
$$=\begin{pmatrix}\theta^{d+Jn}(c_{s-1,0}),\theta^{d+Jn}(c_{s-1,1}),...,\theta^{d+Jn}(c_{s-1,d-1}),\theta^{d+Jn}(c_{0,0}),...,\\ \theta^{d+Jn}(c_{0,d-1}),...,\theta^{d+Jn}(c_{s-2,0}),\theta^{d+Jn}(c_{s-2,1}),...,\theta^{d+Jn}(c_{s-2,d-1})\end{pmatrix}$$

$a\in F$ için $\theta^{d+Jn}(a)=\theta^{y_1m}(a)=a$ olduğundan,

$$\theta^{d+Jn}(c)=\begin{pmatrix}c_{s-1,0},c_{s-1,1},...,c_{s-1,d-1},c_{0,0},c_{0,1},...,\\ c_{0,d-1},...,c_{s-2,0},c_{s-2,1},...,c_{s-2,d-1}\end{pmatrix}\in C$$

olarak elde edilir. Dolayısıyla $C$, $n$ uzunluğunda indeksi $d$ olan bir parçalı devirli koddur. ■

**Örnek 4.6** $x^4-1=(x^2+\alpha^2x+\alpha^2)(x^2+\alpha^2x+\alpha)\in F_4[x,\theta]$, $g(x)=x^2+\alpha^2x+\alpha$ olarak alalım. Bu durumda $C=\langle g(x)\rangle$, $F_4$ üzerinde uzunluğu $4$, boyutu $2$ olan skew devirli koddur ve $G=\begin{pmatrix}\alpha & \alpha^2 & 1 & 0\\ 0 & \alpha^2 & \alpha & 1\end{pmatrix}$ matrisi $C$ nin bir üreteç matrisidir. $\theta$ nın mertebesi $2$ ve $n=4$ olduğundan indeks $d=(4,2)=2$ olarak elde edilir.

$$C=\{000,1111,\alpha\alpha\alpha\alpha,\alpha^2\alpha^2\alpha^2\alpha^2,$$
$$\alpha\alpha^2 10,10\alpha\alpha^2,0\alpha^2\alpha 1,\alpha 10\alpha^2,$$
$$\alpha^2\alpha 01,01\alpha^2\alpha,1\alpha^2 0\alpha,0\alpha 1\alpha^2,$$
$$\alpha^2 01\alpha,1\alpha\alpha^2 0,\alpha^2 1\alpha 0,\alpha 0\alpha^2 1\}$$

$C$ nin elemanları incelendiğinde $F_4$ üzerinde $[4,2,3]$ parametrelerine sahip indeksi 2 olan parçalı devirli kod olduğu görülür.

$F_q[x;\theta]$ halkasında $x^n-1$ polinomunun bir sağ böleni olan ve katsayıları $\theta$ otomorfizması altında sabit kalan elemanlardan oluşan bir polinom tarafından üretilen kod devirli koddur. Aşağıdaki önerme, [8] nolu çalışmadaki Önerme 4'ün skew devirli kodlar için düzenlenmiş halidir.

**Önerme 4.5** $\theta$, $F_q$ cismi üzerinde tanımlı bir otomorfizma ve $\theta$ tarafından sabit bırakılan alt cisim $K$ olsun. $f(x)\in F_q[x;\theta]$ polinomu $x^n-1$'in bir sağ böleni olmak üzere $C=\langle f(x)\rangle$ kodunun bir devirli kod olması için gerek ve yeter koşul $f(x)$ polinomunun katsayılarının $K$ cisminin elemanı olmasıdır.

**Örnek 4.7** $F_4$ üzerinde tanımlı $\theta(a)=a^2$ otomorfizması altında sabit bırakılan alt cisim $F_2=\{0,1\}$ dir. $F_4[x;\theta]$ halkasında $x^4-1$'in katsayıları $F_2$ cisminin elemanı olan sağ böleni $x^2+1$ dir. Bu durumda $C=\langle x^2+1\rangle$, $F_4$ üzerinde 4 uzunluğunda bir devirli koddur.

$$\begin{aligned}C=\{&000,1111,\alpha\alpha\alpha\alpha,\alpha^2\alpha^2\alpha^2\alpha^2,\\ &1010,0101,\alpha0\alpha0,0\alpha0\alpha,\alpha^20\alpha^20,0\alpha^20\alpha^2,\\ &1\alpha1\alpha,\alpha1\alpha1,\alpha^21\alpha^21,1\alpha^21\alpha^2,\alpha\alpha^2\alpha\alpha^2,\alpha^2\alpha\alpha^2\alpha\}\end{aligned}$$

## 4.2 Skew Devirli Kodların İdempotent Üreteçleri

$F_q[x]$ değişmeli polinom halkasında $(n,q)=1$ ise $F_q$ üzerinde tanımlı $n$ uzunluğunda devirli bir kodun idempotent üreteci vardır ve tek türlüdür [15]. $F_q[x;\theta]$ skew polinom halkasında ise bir polinomun çarpanlarına ayrılışı tek türlü olmadığından idempotent üreteçlerin varlığını tespit etmek zor bir problemdir. Aşağıdaki teoremde bazı kısıtlamalar altında idempotent üreteçlerin varlığı gösterilecektir.

**Teorem 4.7** $g(x)\in F_q[x;\theta]$ polinomu $x^n-1$ in bir monik sağ böleni ve $C$, $g(x)$ tarafından üretilen $F_q$ üzerinde $n$ uzunluğunda bir skew devirli kod olsun. $|\langle\theta\rangle|=m$

olmak üzere $(m,n)=1$ ve $(n,q)=1$ ise $C=\langle e(x)\rangle$ olacak şekilde bir $e(x)\in F_q[x;\theta]\Big/\langle x^n-1\rangle$ idempotent polinomu vardır.

**İspat:** $F_q$ cisminin $\theta$ altında sabit kalan alt cismi $K$ olsun. $g(x)\in F_q[x;\theta]$ polinomu $x^n-1$ in bir monik sağ böleni ve $(m,n)=1$ ise Teorem 4.4 ten $g(x)\in K[x]$ dir. Bu durumda $g(x)$ polinomu $K$ üzerinde $n$ uzunluğunda bir devirli kod üretir, bu kod $C'=\langle g(x)\rangle\in K^n$ olsun. $C=\langle g(x)\rangle\in F_q^n$ kodu $F_q$ üzerinde $n$ uzunluğunda bir skew devirli koddur ve $C'\subseteq C$ olduğu açıktır. $(n,q)=1$ ise $C'$ devirli kodunun $e(x)\in F_q[x]\Big/\langle x^n-1\rangle$ şeklinde tek bir idempotent üreteci vardır. Aynı zamanda $e(x)\in C$ dir. O halde $C=\langle e(x)\rangle$ olduğu gösterilirse istenen elde edilir. $e(x)\in C$ olduğundan $e(x)=a(x)*g(x)$ olacak şekilde $a(x)\in F_q[x;\theta]$ vardır ve böylece $F_q[x;\theta]\Big/\langle x^n-1\rangle$ de $\langle e(x)\rangle\subseteq\langle g(x)\rangle=C$ dir. $C$ nin tüm kodsözleri $C'$ nün kodsözlerinin $F_q$-lineer kombinasyonu olarak yazılabilir. Dolayısıyla $F_q[x;\theta]\Big/\langle x^n-1\rangle$ de $\langle e(x)\rangle$ ve $\langle g(x)\rangle$ in boyutları eşittir. Böylece $C=\langle e(x)\rangle$ ve $e(x)$ polinomu $C$ nin bir idempotent üretecidir. ■

**Örnek 4.8** $x^9-1$ polinomunun $F_4[x;\theta]$ halkasında indirgenemez çarpanlarına ayrılışı $x^9-1=(x+1)(x^2+x+1)(x^6+x^3+1)$ dir. $F_4[x;\theta]\Big/\langle x^9-1\rangle$ deki tüm idempotent polinomlar;

1. $x^3+x^6$
2. $x+x^2+x^4+x^5+x^7+x^8$
3. $x+x^2+x^3+x^4+x^5+x^6+x^7+x^8$
4. $1$
5. $1+x^3+x^6$
6. $1+x+x^2+x^4+x^5+x^7+x^8$
7. $1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8$
8. $\alpha+\alpha x+\alpha x^2+(1+\alpha)x^3+\alpha x^4+\alpha x^5+(1+\alpha)x^6+\alpha x^7+\alpha x^8$
9. $\alpha+(1+\alpha)x+(1+\alpha)x^2+\alpha x^3+(1+\alpha)x^4+(1+\alpha)x^5+\alpha x^6+(1+\alpha)x^7+(1+\alpha)x^8$

10. $1+\alpha+\alpha x+\alpha x^2+(1+\alpha)x^3+\alpha x^4+\alpha x^5+(1+\alpha)x^6+\alpha x^7+\alpha x^8$

11. $1+\alpha+(1+\alpha)x+(1+\alpha)x^2+\alpha x^3+(1+\alpha)x^4+(1+\alpha)x^5+\alpha x^6+(1+\alpha)x^7+(1+\alpha)x^8$

olarak bulunur.

$C=\langle 1+x+x^2\rangle$, $F_4$ üzerinde $9$ uzunluğunda bir skew devirli kod ve $F_2$ üzerinde $x^2+x+1$ polinomu tarafından üretilen $9$ uzunluğundaki devirli kod $C'$ olsun. Bu durumda $e(x)=1+x+x^2+x^4+x^5+x^7+x^8$ polinomu $C'$ nün idempotent üretecidir. Dolayısıyla $C=\langle e(x)\rangle$ ve $e(x)$ polinomu $C$ nin bir idempotent üretecidir. Fakat

$$\begin{aligned} e'(x) &= \alpha+\alpha x+\alpha x^2+(1+\alpha)x^3+\alpha x^4+\alpha x^5+(1+\alpha)x^6+\alpha x^7+\alpha x^8 \\ &= (\alpha+(1+\alpha)x^3+x^4+\alpha x^6)(1+x+x^2) \end{aligned}$$

polinomu $C$ kodunun diğer bir idempotent üreteci olarak bulunur. Öyleyse $F_q$ üzerinde tanımlı skew devirli kodların idempotent üreteçleri vardır fakat tek türlü olmayabilir.

# BÖLÜM 5

## GALOİS HALKALARI ÜZERİNDE TANIMLI SKEW DEVİRLİ KODLAR

Bu bölümde [9] ve [10] nolu çalışmalardan yararlanılarak Galois Halkaları üzerinde tanımlı skew devirli kodlar incelenecektir. D. Boucher vd. [9] da skew polinom halkasında polinomların katsayılarını sonlu cisimler yerine Galois halkalarından alarak skew devirli kodları tanımlamış ve [3] nolu çalışmayı genelleştirmişlerdir. Galois halkaları üzerinde tanımlanan skew polinom halkaları sağ(sol) Öklidyen olmadığından bu halkanın idealleri temel ideal olmayabilir. Fakat sağ(sol) bölme algoritması bazı polinomlar için sağlanır. Bu yüzden [9] da sadece monik üreteçli temel ideallerle belirlenen skew devirli kodlar üzerinde durulmuştur.

M. Bhaintwal [10] çalışmasında $GR(q^m)$ üzerinde tanımlı skew parçalı devirli kodları incelemiştir. D. Boucher vd. [9] nolu çalışmalarında skew devirli kodları tanımlarken $GR(4^m)$ halkası üzerine yoğunlaşmışlardır. $GR(q^m)$ ve $GR(4^m)$ halkaları üzerinde skew devirli kodların tanımı farklılık arz etmediğinden bu bölümde tanımlamalar ve örneklemeler $GR(4^m)$ halkası kullanılarak yapılacaktır.

### 5.1 $GR(4^m)$ Üzerinde Tanımlı Skew Polinom Halkası

$GR(q^m)$ halkası Bölüm 2 de tanımlanmıştı. Bu kısımda $GR(4^m)$ halkası ve bu halka üzerinde tanımlı Frobenius otomorfizması hakkında kısaca bilgi verilecektir.

**Tanım 5.1** $g(x) \in \mathbb{Z}_2[x]$ polinomu, derecesi $m$ olan monik ve indirgenemez bir polinom olsun. $\mathbb{Z}_4[x]$ halkasında $\overline{h}(x) = g(x)$ olacak şekilde monik ve temel

indirgenemez $h(x)$ polinomunu vardır ve Hensel lift yöntemi ile bulunur. $\xi = x + \langle h(x) \rangle$ olsun. Bu durumda $h(\xi) = 0$ olur, yani $\xi$ $h$ polinomunun bir köküdür. Böylece

$$GR(4^m) \cong \mathbb{Z}_4[x] / \langle h(x) \rangle = \mathbb{Z}_4[\xi]$$

elde edilir. $GR(4^m)$ halkasının tüm elemanları

$$a = a_0 + a_1\xi + a_2\xi^2 + ..... + a_{m-1}\xi^{(m-1)}, \quad a_i \in \mathbb{Z}_4$$

şeklinde tek türlü yazılabilir. $\tau_m = \{0, 1, \xi, \xi^2, ..., \xi^{2^m-2}\}$ Teichmüller kümesidir. $GR(4^m)$ halkasının elemanları aynı zamanda;

$$a + 2b, \quad a, b \in \tau_m$$

olarak da tek türlü ifade edilebilir. Bu yazıma elemanların 2-li (2-adic)temsili denir. $GR(4^m)$ halkası üzerinde Frobenius otomorfizması olan $\theta$, Bölüm 2 de tanımlandığı üzere, $\theta(a) = a_0 + a_1\xi^2 + a_2\xi^4 + ..... + a_{m-1}\xi^{2(m-1)}$, $a_i \in \mathbb{Z}_4$ $(0 \le i \le m-1)$ şeklidedir. Aynı otomorfizmayı elemanların 2-li temsilinde aşağıdaki gibi ifade etmek mümkündür [17].

$$\theta : GR(4^m) \to GR(4^m)$$
$$a + 2b \to a^2 + 2b^2 \quad a, b \in \tau_m$$

$\theta$ nın mertebesi $|\langle \theta \rangle| = m$ ve $\mathbb{Z}_4$ halkasının elemanları $\theta$ altında sabittir.

$$GR(4^m)[x;\theta] = \{a_0 + a_1x + a_2x^2 + .... + a_nx^n \mid a_i \in GR(4^m), n \in \mathbb{N}\}$$

kümesi standart toplama işlemi ve $(ax^i)(bx^j) = a\theta^i(b)x^{i+j}$ $(a, b \in GR(4^m))$ kuralı ile belirli çarpma işlemi altında polinom halkasıdır. Bu halkaya $GR(4^m)$ üzerinde tanımlı skew polinom halkası denir. $GR(4^m)[x;\theta]$ halkası $\theta$ otomorfizması birimden farklı ise değişmeli olmayan bir halkadır.

**Örnek 5.1** $GR(4^2)$ halkasını oluşturmak için $\mathbb{Z}_4[x]$ te derecesi 2 olan monik ve temel indirgenemez polinom bulunmalıdır. $\mathbb{Z}_2[x]$ halkasında ikinci dereceden indirgenemez polinom $x^2 + x + 1$ dir.

$\overline{h}(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$ polinomunun Hensel lifti $h(x) = x^2 + x + 1 \in \mathbb{Z}_4[x]$ polinomudur. $\xi$, $h(x)$ in bir kökü olsun. Bu durumda $h(\xi) = 0$ ve $\xi^2 = 3\xi + 3$ dir. Böylece $GR(4^2) = \{a_0 + \xi b_0 \mid a_0, b_0 \in \mathbb{Z}_4\}$ elde edilir.

$\tau = \{0, 1, \xi, \xi^2\}$ kümesi $GR(4^2)$ nin Teichmüller kümesidir ve $GR(4^2)$ halkasının tüm elemanları $a + 2b,\ a, b \in \tau$ şeklinde tek türlü ifade edilebilir. $GR(4^2)$ üzerinde tanımlı Frobenius otomorfizması ise

$$\begin{aligned} \theta : GR(4^2) &\to GR(4^2) \\ a + 2b &\to a^2 + 2b^2 \end{aligned}$$

şeklindedir ve $\left|\langle\theta\rangle\right| = 2$ dir. $a_0, b_0 \in \mathbb{Z}_4$ ve $a_0 + b_0\xi$ elemanının 2-li temsili $a + 2b$ olsun. Bu durumda $\theta(a + 2b) = \theta(a_0 + b_0\xi) = a_0 + b_0\xi^2$, $a_0, b_0 \in \mathbb{Z}_4$ tür. Görüldüğü üzere $\mathbb{Z}_4$ ün elemanları $\theta$ altında sabittir.

**Örnek 5.2** $GR(4^2)$ halkasında $3 + 2\xi$ elemanının 2-li temsilini bulalım.

$$3 + 2\xi = 1 + 2(1 + \xi) = 1 + 2(3 + 3\xi) = 1 + 2\xi^2$$

Bu elemanların $\theta$ altındaki görüntüleri,

$$\begin{aligned} \theta(3 + 2\xi) &= 3 + 2\xi^2 = 3 + 2(3 + 3\xi) = 1 + 2\xi \\ \theta(1 + 2\xi^2) &= 1 + 2(\xi^2)^2 = 1 + 2(3\xi) = 1 + 2\xi \end{aligned}$$

olarak bulunur ve $\theta(1 + 2\xi^2) = \theta(3 + 2\xi)$ olduğu görülür.

**Önerme 5.1** $GR(4^m)[x;\theta]$ halkasının merkezi, $Z(GR(4^m)[x;\theta]) = \mathbb{Z}_4[x^m]$ dir [9].

$GR(4^m)[x;\theta]$ halkası sol veya sağ Öklidyen değildir. Fakat sağ ve sol bölme algoritması bazı polinomlar için tanımlıdır. $f, g \in GR(4^m)[x;\theta]$ sıfırdan farklı polinomları için özel olarak $g$ polinomunun baş katsayısı birimsel olduğu durumda

$$f = qg + r, \qquad der(r) < der(g)$$

olacak şekilde $q, r \in GR(4^m)[x;\theta]$ polinomları vardır ve tek türlüdür. $r = 0$ ise $g$ polinomu $f$ nin bir sağ bölenidir. Sol bölme algoritması da benzer şekilde tanımlıdır.

**Örnek 5.3** $GR(4^2)[x;\theta]$ halkasında $x^4-1$ polinomunun indirgenemez çarpanları

$$x^4-1=(x+1)(x+1)(x+2\xi+1)(x+2\xi+3)$$
$$=(x^2+2\xi+1)(x^2+2\xi+3)$$

şeklindedir. Görüldüğü üzere $GR(4^2)[x;\theta]$ halkasında bir polinomun indirgenemez çarpanlarının derecelerinin sıralanışı tek türlü değildir [9].

Önceki bölümde $F[x;\theta]$ skew polinom halkası sağ ve sol Öklidyen olduğundan $F[x;\theta]$ nın tüm ideallerinin temel ideal olduğu gösterilmişti. $GR(4^m)[x;\theta]$ halkası sağ veya sol Öklidyen olmadığından $GR(4^m)[x;\theta]$ halkasının tüm sol(sağ) idealleri temel ideal olmayabilir. Bu nedenle [9] ve [10] nolu çalışmalarda monik polinomlar tarafından üretilen temel ideallere karşılık gelen skew devirli kodlar üzerinde durulmuştur.

D.Boucher vd. [9] çalışmalarında uzunluğu $m|n$ olarak kısıtlamış ve $GR(4^m)[x;\theta]\Big/\langle x^n-1\rangle$ halkasının temel ideallerine karşılık gelen skew devirli kodları incelemişlerdir. $m\nmid n$ ise $GR(4^m)[x;\theta]\Big/\langle x^n-1\rangle$ halka belirtmez fakat bir sol $GR(4^m)[x;\theta]$-modüldür. M. Bhaintwal [10] çalışmasında uzunluk için bir kısıtlama getirmeden $GR(4^m)[x;\theta]\Big/\langle x^n-1\rangle$ modülünün serbest sol alt modüllerine karşılık gelen skew devirli kodları incelemiştir.

Bu kısımda öncelikle $m\mid n$ şartı altında skew devirli kodlar incelenecektir. Daha sonra [10] da verilen modül yaklaşımı açıklanacaktır.

## 5.2 $GR(4^m)$ Üzerinde Skew Devirli Kodlar

$\theta$, $GR(4^m)$ üzerinde tanımlı bir otomorfizma ve $C$ $GR(4^m)$ üzerinde tanımlı $n$ uzunluğunda bir lineer kod olsun. Herhangi $c=(c_0,c_1,...,c_{n-1})\in C$ için $(\theta(c_{n-1}),\theta(c_0),...,\theta(c_{n-2}))\in C$ oluyorsa $C$, $GR(4^m)$ üzerinde tanımlı bir skew devirli koddur.

**Önerme 5.2** $f\in\mathbb{Z}_4[x^m]$, $der(f)=n$ , ve $f$ bir monik polinom olmak üzere $GR(4^m)[x;\theta]$ halkasının $f$ tarafından üretilen herhangi bir sol veya sağ ideali çift

taraflı temel idealdir. $g \in GR(4^m)[x;\theta]$ polinomu $f$ polinomunun bir sağ böleni olsun. Bu durumda $g$ polinomu $GR(4^m)[x;\theta]/\langle f \rangle$ halkasında bir temel sol ideal üretir [9].

$m \mid n$ ise $x^n - 1 \in \mathbb{Z}_4[x^m]$ ve böylece $GR(4^m)[x;\theta]/\langle x^n - 1 \rangle$ bir halkadır. $I$, $GR(4^m)[x;\theta]/\langle x^n - 1 \rangle$ halkasının bir sol ideali ve $I$ idealine karşılık gelen kod $C$ olsun. Herhangi $a = (a_0, a_1, a_2, ...., a_{n-1}) \in C$ için $p = a_0 + a_1 x + a_2 x^2 + ..... + a_{n-1} x^{n-1} \in I$ ve $I$ bir sol ideal olduğundan $xp \in I$ dır.

$$\begin{aligned} xp &= x(a_0 + a_1 x + ... + a_{n-1} x^{n-1}) \\ &= \theta(a_0) + \theta(a_1)x + ... + \theta(a_{n-1})x^n \\ &= \theta(a_{n-1}) + \theta(a_0)x + ... + \theta(a_{n-2})x^{n-1} \in I; \end{aligned}$$

böylece $(\theta(a_{n-1}), \theta(a_0), ....., \theta(a_{n-2})) \in C$ elde edilir. Dolayısıyla $C$, $GR(4^m)$ üzerinde tanımlı bir skew devirli koddur. $GR(4^m)[x;\theta]/\langle x^n - 1 \rangle$ halkasının her bir sol idealine karşılık gelen bir skew devirli kod vardır. Fakat bu halkanın tüm idealleri temel ideal olmadığından skew devirli kodların tamamını belirlemek zor bir problemdir.

**Teorem 5.1** $m \mid n$ olmak üzere $g(x) \in GR(4^m)[x;\theta]$ polinomu $x^n - 1$ in bir monik sağ böleni olsun. Bu durumda $\langle g(x) \rangle$ sol idealine karşılık gelen $C$ kodu $GR(4^m)$ üzerinde tanımlı bir skew devirli koddur [9].

Herhangi bir $n$ tam sayısı için $GR(4^m)$ üzerinde tanımlı $n$ uzunluğundaki skew devirli kodlar [4] te olduğu gibi modüller cinsinden ifade edilebilir. $R = GR(4^m)[x;\theta]$ olsun. $R(x^n - 1)$, $R$ nin bir sol alt modülüdür ve $R_{n,\theta} = R/R(x^n - 1)$ bir sol $R$-modüldür. Skew devirli kodlar $R_{n,\theta}$ nın sol alt modülleri cinsinden ifade edilebilir.

$a(x) \in R$ ve herhangi $v(x) \in R_{n,\theta}$ için $a(x)v(x) = v_1(x)(x^n - 1)$ olacak şekilde $v_1(x) \in R$ polinomu varsa $a(x)$ polinomu $R_{n,\theta}$ nın bir sıfırlayıcısıdır (annihilator). Özel durumda $v(x) = 1$ olarak alındığında $a(x).1 = r(x)(x^n - 1)$ olacak şekilde $r(x) \in R$ vardır ve $a(x) \in R(x^n - 1)$ dir. $R_{n,\theta}$ nın tüm sıfırlayıcılarından oluşan küme $I$ olsun. Bu durumda $I$, $R$ nin bir sol ideali ve $I \subseteq R(x^n - 1)$ dir. $g(x) \in R_{n,\theta}$ ise $g(x)$ derecesi $n$ den küçük

olan $GR(4^m)$ üzerinde bir polinomdur. $a(x), b(x) \in R$ iki polinom ve bu polinomların dereceleri $n$ den küçük olsun. Her $r(x) \in R_{n,\theta}$ için $a(x)r(x) = b(x)r(x)$ sağlanıyorsa $a(x) - b(x) \in I$ olur ve böylece $a(x) - b(x)$ polinomu $x^n - 1$'in bir katıdır. Fakat dereceleri $n$ den küçük olduğundan $a(x) = b(x)$ elde edilir. Böylece $R.R_{n,\theta} = R_{n,\theta}.R_{n,\theta} = R_{n,\theta}$ olduğu görülür. Dolayısıyla $C$ nin $GR(4^m)$ üzerinde tanımlı $n$ uzunluğunda bir skew devirli kod olması için gerek ve yeter koşul $R.C = R_{n,\theta}.C = C$ olması başka bir deyişle $C$ nin $R_{n,\theta}$ nın bir sol alt modülü olmasıdır.[10]

**Teorem 5.2** $C$ , $g(x) \in GR(4^m)[x] \Big/ \langle x^n - 1 \rangle$ monik polinomu tarafından üretilen skew devirli kod olsun. $C$ nin serbest $GR(4^m)-$modül olması için gerek ve yeter koşul $g(x)$ polinomunun $x^n - 1$'in bir sağ böleni olmasıdır [10].

Yukarıdaki teoremde $der(g(x)) = r$ ise $\beta = \{g(x), x * g(x), ..., x^{n-r-1} * g(x)\}$ kümesi $C$'yi üreten minimal kümedir (bazıdır). Dolayısıyla [9] nolu kaynakta $m \mid n$ şartı ile verilen önerme herhangi bir $n$ uzunluğu için geçerlidir.

**Önerme 5.3** $g = x^r + g_{r-1}x^{r-1} + ..... + g_1 x + g_0 \in GR(4^m)[x;\theta]$ monik polinomu $x^n - 1$ in bir sağ böleni olsun. Bu durumda $g$ polinomu $GR(4^m)$ üzerinde $[n, n-r]$ parametrelerine sahip bir skew devirli kod üretir. Bu kod için üreteç matrisi;

$$G = \begin{pmatrix} g_0 & \cdots & g_{r-1} & 1 & 0 & \cdots & 0 \\ 0 & \theta(g_0) & \cdots & \theta(g_{r-1}) & 1 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & & & & & & \\ 0 & \cdots & 0 & \theta^{n-r-1}(g_0) & & \theta^{n-r-1}(g_{r-1}) & 1 \end{pmatrix}$$

şeklindedir [9].

**Önerme 5.4** $h, g \in GR(4^m)[x;\theta]$ ve $x^n - 1 = hg$ olsun. $GR(4^m)$ üzerinde $g$ monik polinomu tarafından üretilen skew devirli kod $C$ olsun. Bu durumda $a \in C$ olması için gerek ve yeter koşul $a(x)h(x) = 0 \ \in GR(4^m)[x;\theta] \Big/ \langle x^n - 1 \rangle$ olmasıdır. Ayrıca

$h(x) = h_o + h_1 x + .... + x^k$ ise

$$H=\begin{pmatrix} 1 & \theta(h_{k-1}) & \cdots & \theta^{k}(h_0) & 0 & \cdots & 0 \\ 0 & 1 & \theta^{2}(h_{k-1}) & \cdots & \theta^{k+1}(h_0) & \cdots & 0 \\ 0 & 0 & \cdots & \cdots & \cdots & \ddots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & \theta^{n-k}(h_{k-1}) & \cdots & \theta^{n-1}(h_0) \end{pmatrix}$$

matrisi $C$ kodu için kontrol matrisidir [9].

**Sonuç 5.1** $C$, $GR(4^m)$ üzerinde $g$ tarafından üretilen $n$ uzunluğunda bir skew devirli kod ve $x^n-1=hg$ olsun. $g=\sum_{i=0}^{r} g_i x^i$ ve $h=\sum_{i=0}^{n-r} h_i x^i$ iken $C$ nin duali, $C^{\perp}$ için üreteç polinomu $g^{\perp}$;

$$g^{\perp}=h_{n-r}+\theta(h_{n-r-1})x+....+\theta^{n-r}(h_0)x^{n-r} \text{ dir.}$$

$C^{\perp}$ kodu bir skew devirli koddur. $g^{\perp}$ polinomu aynı zamanda $C$ kodunun kontrol polinomudur [9].

**Örnek 5.4** $x^4-1\in GR(4^2)[x;\theta]$ polinomunun derecesi 2 olan sağ böleni $GR(4^2)$ üzerinde $n=4,\ k=2$ parametrelerine sahip bir skew devirli kod üretir.

$$x^4-1=(x^2+2\xi+1)(x^2+2\xi+3)\ \in GR(4^2)[x;\theta]$$

$g(x)=x^2+2\xi+3$ polinomu tarafından üretilen skew devirli kod $C$ olsun.

$3+2\xi$ elemanının 2-li temsili $1+2\xi^2$ şeklindedir.

$$G=\begin{pmatrix} 1+2\xi^2 & 0 & 1 & 0 \\ 0 & \theta\left(1+2\xi^2\right) & 0 & \theta(1) \end{pmatrix}=\begin{pmatrix} 1+2\xi^2 & 0 & 1 & 0 \\ 0 & 1+2\xi & 0 & 1 \end{pmatrix}$$

matrisi $C$ kodu için üreteç matrisidir. $h(x)=(x^4-1)/g(x)=x^2+1+2\xi$ olduğundan $C$ kodu için kontrol polinomu $g^{\perp}(x)=x^2(x^{-2}+1+2\xi)=1+\theta^2(1+2\xi)x^2=1+(1+2\xi)x^2$ olarak bulunur ve böylece

$$H=\begin{pmatrix} 1 & 0 & 1+2\xi & 0 \\ 0 & 1 & 0 & 1+2\xi^2 \end{pmatrix}$$

matrisi $C$ nin kontrol matrisidir.

## 5.3 $GR(4^2)$ Üzerinde Tanımlı Monik Üreteçli Skew Devirli Kodlardan $\mathbb{Z}_4$ Üzerinde Tanımlı Lineer Kodların Eldesi

D.Boucher vd.[9] da bir dönüşüm tanımlayarak $GR(4^2)$ üzerinde tanımlı skew devirli kodlardan $\mathbb{Z}_4$ üzerinde tanımlı lineer kodlar elde etmişlerdir.

$C$, $GR(4^2)$ üzerinde tanımlı bir skew devirli kod ve $G$ matrisi $C$ kodu için üreteç matrisi olsun. $GR(4^2)$ ten $\mathbb{Z}_4$ e tanımlanan dönüşüm aşağıdaki gibidir.

**i.** Üreteç matrisinin her bir satırını $\xi$ ile çarpıp yeni bir satır olarak üreteç matrisine eklenir,

**ii.** Üreteç matrisindeki $a+\xi b$ şeklindeki her bir eleman $3a$ ve $a+b$ şeklinde 2 eleman olarak değiştirilir.

Neticede elde edilen üreteç matrisi $G'$, $\mathbb{Z}_4$ üzerinde tanımlı bir lineer kod üretir [9].

**Örnek 5.5** Önceki örnekteki $GR(4^2)$ üzerinde tanımlı $C$ kodundan yukarıdaki dönüşümü kullanarak $\mathbb{Z}_4$ üzerinde tanımlı bir kod elde etmek için öncelikle $G$ matrisinin elemanları $a+b\xi$ olarak düzenlenmelidir.

$$G=\begin{pmatrix}1+2\xi^2 & 0 & 1 & 0\\ 0 & 1+2\xi & 0 & 1\end{pmatrix}=\begin{pmatrix}3+2\xi & 0 & 1 & 0\\ 0 & 1+2\xi & 0 & 1\end{pmatrix}.$$

**i.** $G$ matrisini tüm satırlarını $\xi$ ile çarpıp satır olarak eklendiğinde aşağıdaki genişletilmiş matris elde edilir.

$$G'=\begin{pmatrix}3+2\xi & 0 & 1 & 0\\ 2+\xi & 0 & \xi & 0\\ 0 & 1+2\xi & 0 & 1\\ 0 & 2+3\xi & 0 & \xi\end{pmatrix}.$$

**ii.** $G'$ matrisinin $a+\xi b$ şeklindeki her bir elemanı $3a$ ve $a+b$ şeklinde 2 eleman ile değiştirildiğinde bileşenleri $\mathbb{Z}_4$ te olan aşağıdaki matris elde edilir.

$$G'' = \begin{pmatrix} 1 & 1 & 0 & 0 & 3 & 1 & 0 & 0 \\ 2 & 3 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 3 & 0 & 0 & 3 & 1 \\ 0 & 0 & 2 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

$G''$ matrisi $\mathbb{Z}_4$ üzerinde uzunluğu $2n = 8$ ve boyutu $2k = 4$ olan bir lineer kod üretir. Daha sonra Bölüm 2 de tanımlanan Gray map kullanarak $\mathbb{Z}_4$ üzerindeki bu koddan üreteç matrisi $G_2$ olan ikili lineer kod elde edilir.

$$G_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & & & & & 1 & 0 & 1 & 1 & & & & \\ 0 & 1 & 0 & 0 & & & & & 0 & 1 & 1 & 1 & & & & \\ 0 & 0 & 1 & 0 & & & 0 & & 1 & 1 & 0 & 1 & & & 0 & \\ 0 & 0 & 0 & 1 & & & & & 1 & 1 & 1 & 0 & & & & \\ & & & & 1 & 0 & 0 & 0 & & & & & 0 & 1 & 1 & 1 \\ & & & & 0 & 1 & 0 & 0 & & & & & 1 & 0 & 1 & 1 \\ & & 0 & & 0 & 0 & 1 & 0 & & & 0 & & 1 & 1 & 1 & 0 \\ & & & & 0 & 0 & 0 & 1 & & & & & 1 & 1 & 0 & 1 \end{pmatrix}.$$

$G_2$ tarafından üretilen ikili lineer kod [16,8,4] parametrelerine sahiptir. Bu kod, kendine dual kodlar için bilinen en iyi parametrelere sahip bir kendine dual koddur.

# BÖLÜM 6

## $F_{p^m}+uF_{p^m}$ HALKASI ÜZERİNDE TANIMLI SKEW DEVİRLİ KODLAR

Jitman vd. [12] de skew polinom halkasında polinomların katsayılarını sonlu zincir halkalarından alarak sonlu zincir halkaları üzerinde skew devirli kodları tanımlamışlardır.

$R$ birimli, değişmeli ve sonlu bir halka ve $R$ nin idealleri birbirini kapsıyor ise $R$ ye sonlu zincir halkası denir. $R$ nin ideallerinin zinciri

$$\langle 0\rangle = \langle \gamma^e\rangle \underset{\neq}{\subset} \langle \gamma^{e-1}\rangle \underset{\neq}{\subset} \cdots \underset{\neq}{\subset} \langle \gamma\rangle \underset{\neq}{\subset} R$$

şeklindedir. Sonlu zincir halkasının tüm idealleri temel idealdir ve maksimal ideali tektir.

$p$ bir asal sayı, $m$ ve $n$ pozitif tamsayılar ve $q=p^e$ olsun. $\mathbb{Z}_{p^e}$, $GR(q^m)$ ve $F_{p^m}+uF_{p^m}+\ldots+u^{e-1}F_{p^m}$ ($u^e=0$) halkaları birer sonlu zincir halkasıdır. $\mathbb{Z}_{p^e}$ halkası Galois halkasının özel bir halidir. Önceki bölümde Galois halkaları üzerinde tanımlı skew devirli kodlar incelenmişti. Bu bölümde $F_{p^m}+uF_{p^m}$ halkası üzerinde tanımlı skew devirli kodlar üzerinde durulacak ve $F_{p^m}+uF_{p^m}$ üzerinde tanımlı skew devirli kodların sınıflandırılması verilecektir. Ayrıca $F_4+uF_4$ üzerinde tanımlı skew devirli kodlardan $F_4$ üzerinde lineer kodlar elde edilerek optimale yakın kod örnekleri verilecektir.

$F_{p^m}+uF_{p^m}=\{a+ub \,|\, a,b\in F_{p^m}\}$ kümesi standart toplama işlemi ve $u^2=0$ kuralı ile değişkeni $u$ olan polinomların çarpma işlemi altında bir halkadır ve $F_{p^m}[u]\big/\langle u^2\rangle$

halkasına izomorftur. $F_{p^m}+uF_{p^m}$ değişmeli ve birimli bir halkadır. Tüm idealleri temel idealdir ve $\langle u \rangle$ ideali bu halkanın tek maksimal idealidir.

$F_{p^m}+uF_{p^m}$ halkası üzerinde skew polinom halkasını oluşturmak için bu halka üzerinde otomorfizmalar grubu bulunmalıdır. [13] te sonlu zincir halkalarının otomorfizma grupları belirlenmiştir.

**Teorem 6.1** $\theta \in Aut(F_{p^m})$ ve $\beta \in F_{p^m}^*$ olsun.

$$\Theta_{\theta,\beta} : F_{p^m}+uF_{p^m} \to F_{p^m}+uF_{p^m}$$
$$\Theta_{\theta,\beta}(a+ub)=\theta(a)+\beta\theta(b)u$$

olarak tanımlanan $\Theta_{\theta,\beta}$ dönüşümü bir otomorfizmadır ve $F_{p^m}+uF_{p^m}$ in otomorfizmalar grubu $Aut(F_{p^m}+uF_{p^m})=\{\Theta_{\theta,\beta} \mid \theta \in Aut(F_{p^m}),\ \beta \in F_{p^m}^*\}$ dir [13].

Galois halkaları ve sonlu cisimler üzerinde tanımlı skew polinom halkalarına benzer şekilde $F_{p^m}+uF_{p^m}$ üzerinde skew polinom halkaları tanımlanabilir.

**Tanım 6.1** $\Theta$ , $F_{p^m}+uF_{p^m}$ üzerinde tanımlı bir otomorfizma olsun.

$$(F_{p^m}+uF_{p^m})[x;\Theta]=\{a_0+a_1x+\ldots+a_nx^n \mid a_i \in F_{p^m}+uF_{p^m},\ n \in \mathbb{N}\}$$

kümesi standart toplama işlemi ve $x\alpha=\Theta(\alpha)x$ ($\alpha \in F_{p^m}+uF_{p^m}$) kuralı ile belirli çarpma işlemi altında bir halkadır. Bu halkaya $F_{p^m}+uF_{p^m}$ üzerinde tanımlı skew polinom halkası denir. $\Theta$ birim otomorfizma değilse $F_{p^m}+uF_{p^m}[x;\Theta]$ halkası değişmeli olmayan bir polinom halkasıdır [12].

$(F_{p^m}+uF_{p^m})[x;\Theta]$ halkası tek türlü çarpanlarına ayrılabilen bir halka değildir. Ayrıca indirgenemez çarpanların dereceleri belli bir sıralamadan sonra tek türlü değildir.

**Örnek 6.1** $\Theta_{id,2}(a+bu)=a+2bu$ olarak tanımlı $\Theta_{id,2}$ dönüşümü $F_3+uF_3$ halkası üzerinde tanımlı bir otomorfizmadır. $x^6-1$ polinomunun $(F_3+uF_3)[x;\Theta_{id,2}]$ halkasındaki 2 indirgenemez ayrışımı;

$$x^6 - 1 = (x+1)^3 (x+2)^3$$
$$= (x^2 + ux + 2)^3$$

şeklindedir. İlk ayrışımda birinci dereceden $6$ indirgenemez çarpan mevcutken diğerinde ikinci dereceden $3$ indirgenemez çarpan mevcuttur [12].

### 6.1 $F_{p^m} + uF_{p^m}$ Üzerinde Tanımlı Skew Devirli Kodların Sınıflandırması

$\Theta$, $F_{p^m}$ üzerinde tanımlı mertebesi $m$ olan bir otomorfizma olsun. $m \mid n$ ise $x^n - 1$ polinomu $(F_{p^m} + uF_{p^m})[x;\Theta]$ halkasının merkezindedir ve $x^n - 1$ tarafından üretilen ideal çift taraflı bir idealdir. Dolayısıyla $(F_{p^m} + uF_{p^m})[x;\Theta] \Big/ \langle x^n - 1 \rangle$ üzerinde çarpma işlemi iyi tanımlıdır ve bir halka belirtir. [12] de skew devirli kodlar tanımlanırken uzunluk $m \mid n$ olarak kısıtlanmıştır. Fakat [4] te verilen modül yaklaşımı kullanılarak uzunluk için bir kısıtlama getirmeden skew devirli kodlar tanımlanabilir.

**Teorem 6.2** $C$, $F_{p^m} + uF_{p^m}$ üzerinde tanımlı $n$ uzunluğunda bir lineer kod olsun. $C$ kodunun skew devirli kod olması için gerek ve yeter koşul $C$ nin $(F_{p^m} + uF_{p^m})[x;\Theta] \Big/ \langle x^n - 1 \rangle$ modülünün bir sol $(F_{p^m} + uF_{p^m})[x;\Theta]$-alt modülü olmasıdır.

$(F_{p^m} + uF_{p^m})[x;\Theta]$ halkası sol veya sağ Öklidyen değildir. Fakat sağ ve sol bölme algoritması bazı polinomlar için sağlanır.

**Teorem 6.3** $f, g \in (F_{p^m} + uF_{p^m})[x;\Theta]$ olsun, $g$ polinomunun baş katsayısı birimsel ise

$$f = qg + r, \qquad der(r) < der(g)$$

olacak şekilde $q, r \in (F_{p^m} + uF_{p^m})[x;\Theta]$ polinomları vardır ve tek türlüdür [12].

$(F_{p^m} + uF_{p^m})[x;\Theta]$ halkasının tüm sol(sağ) idealleri temel ideal olmayabilir.

**Önerme 6.1** $g(x) \in (F_{p^m} + uF_{p^m})[x;\Theta]$ polinomu $x^n - 1$ in bir monik sağ böleni ve $C$, $g(x)$ tarafından üretilen bir skew devirli kod olsun. Bu durumda $C$ bir serbest $(F_{p^m} + uF_{p^m})[x;\Theta]$-modüldür ve $C$ nin boyutu $n - der(g(x))$ dir.

$g(x) = g_0 + g_1 x + ... + g_{k-1} x^{k-1} + x^k$ ise

$$G = \begin{pmatrix} g_0 & \cdots & g_{k-1} & 1 & 0 & \cdots & 0 \\ 0 & \Theta(g_0) & \cdots & \Theta(g_{k-1}) & 1 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & & & & & & \\ 0 & \cdots & 0 & \Theta^{n-k-1}(g_0) & & \Theta^{n-k-1}(g_{k-1}) & 1 \end{pmatrix}$$

matrisi $C$ kodunun bir üreteç matrisidir [12].

**Önerme 6.2** $h, g \in (F_{p^m} + uF_{p^m})[x;\Theta]$ ve $x^n - 1 = hg$ olsun. $F_{p^m} + uF_{p^m}$ üzerinde $g$ monik polinomu tarafından üretilen skew devirli kod $C$ olsun. Bu durumda $c \in C$ olması için gerek ve yeter koşul $(F_{p^m} + uF_{p^m})[x;\Theta] \Big/ \langle x^n - 1 \rangle$ de $c(x)h(x) = 0$ olmasıdır.

$h(x) = h_o + h_1 x + .... + x^k$ ise

$$H = \begin{pmatrix} 1 & \Theta(h_{k-1}) & \cdots & \Theta^k(h_0) & 0 & \cdots & 0 \\ 0 & 1 & \Theta^2(h_{k-1}) & \cdots & \Theta^{k+1}(h_0) & \cdots & 0 \\ 0 & 0 & \cdots & \cdots & \cdots & \ddots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & \Theta^{n-k}(h_{k-1}) & \cdots & \Theta^{n-1}(h_0) \end{pmatrix}$$

matrisi $C$'nin kontrol matrisidir [12].

**Teorem 6.4** $C$, $F_{p^m} + uF_{p^m}$ üzerinde $g$ tarafından üretilen $n$ uzunluğunda bir skew devirli kod ve $x^n - 1 = hg$ olsun. $\varphi$ fonksiyonu $\varphi(\sum_{i=0}^{n-r} a_i x^i) = \sum_{i=0}^{n-r} x^{-i} a_i$ olarak tanımlı ve $g = \sum_{i=0}^{r} g_i x^i$, $h = \sum_{i=0}^{n-r} h_i x^i$ olsun. Bu durumda aşağıdakiler sağlanır [12].

**i.** $h_R = x^{\deg(h(x))} \varphi(h(x)) = h_{n-r} + \Theta(h_{n-r-1})x + .... + \Theta^{n-r}(h_0)x^{n-r}$ polinomu $x^n - 1$ in bir sağ bölenidir.

**ii.** $h_R$ polinomu dual kodun ($C^\perp$) üreteç polinomudur ve $C^\perp$ bir skew devirli koddur.

**iii.** $h_R$ polinomu $C$ nin kontrol polinomudur.

Yukarıdaki tanım ve teoremlerde $x^n-1$ in monik sağ bölenleri tarafından üretilen skew devirli kodlara değinilmişti. Fakat $F_{p^m}+uF_{p^m}$ üzerinde tanımlı iki polinom tarafından ya da monik olmayan polinomlar tarafından üretilen kodlar da mevcuttur. [12] de $m|n$ şartı altında $(F_{p^m}+uF_{p^m})[x;\Theta]\Big/\langle x^n-1\rangle$ halkasının tüm idealleri sınıflandırılmıştır ve böylece $F_{p^m}+uF_{p^m}$ üzerinde tanımlı $n$ uzunluğundaki tüm skew devirli kodların yapısal özellikleri belirlenmiştir. [4] teki modül yaklaşımı kullanılarak uzunluk için belirtilen kısıtlama kaldırılabilir. Aşağıdaki teorem, [12] deki Teorem 4.1 in modül yaklaşımıyla düzenlenmiş halidir.

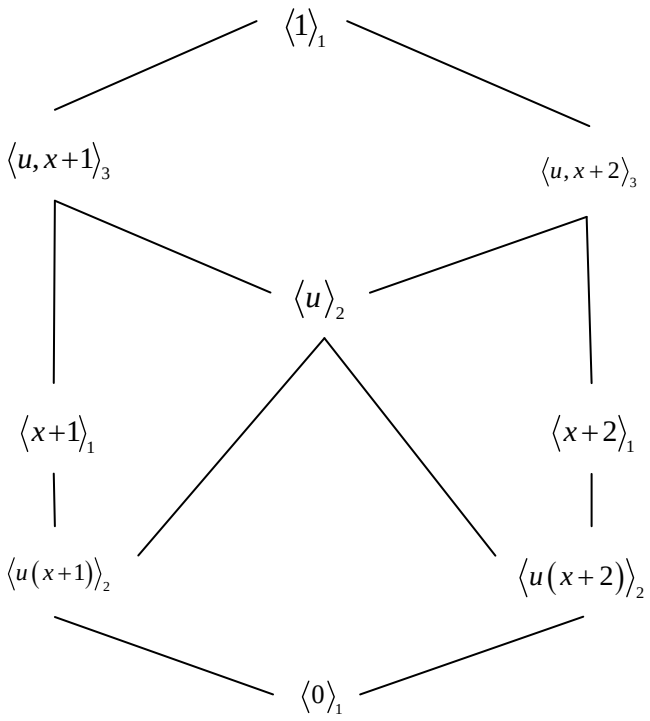
**Teorem 6.5** $C$ , $(F_{p^m}+uF_{p^m})[x;\Theta]\Big/\langle x^n-1\rangle$ modülünün sıfırdan farklı bir sol alt modülü ve $A$ kümesi $C$ deki en küçük dereceli sıfırdan farklı polinomların kümesi olsun.

- **i.** $A$ kümesinde bir $g(x)$ monik polinomu varsa tektir ve $C=\langle g(x)\rangle$ dir.
- **ii.** Eğer $C$ de monik polinom yoksa $A$ kümesinde baş katsayısı $u$ olan $g(x)=ug_1(x)$ şeklinde tek bir polinom vardır. Bu durumda $C=\langle g(x)\rangle$ dir.
- **iii.** $A$ kümesi monik polinom içermiyor, $C$ içeriyorsa $A$ kümesinde baş katsayısı $u$ olan $g(x)=ug_1(x)$ şeklinde tek bir polinom vardır. $C$ de $\deg(f_1(x))<\deg(g_1(x))$ olacak şekilde en küçük dereceli monik $f(x)=f_0(x)+uf_1(x)$ polinomu vardır ve tektir. Bu durumda $C=\langle g(x), f(x)\rangle$ dir.

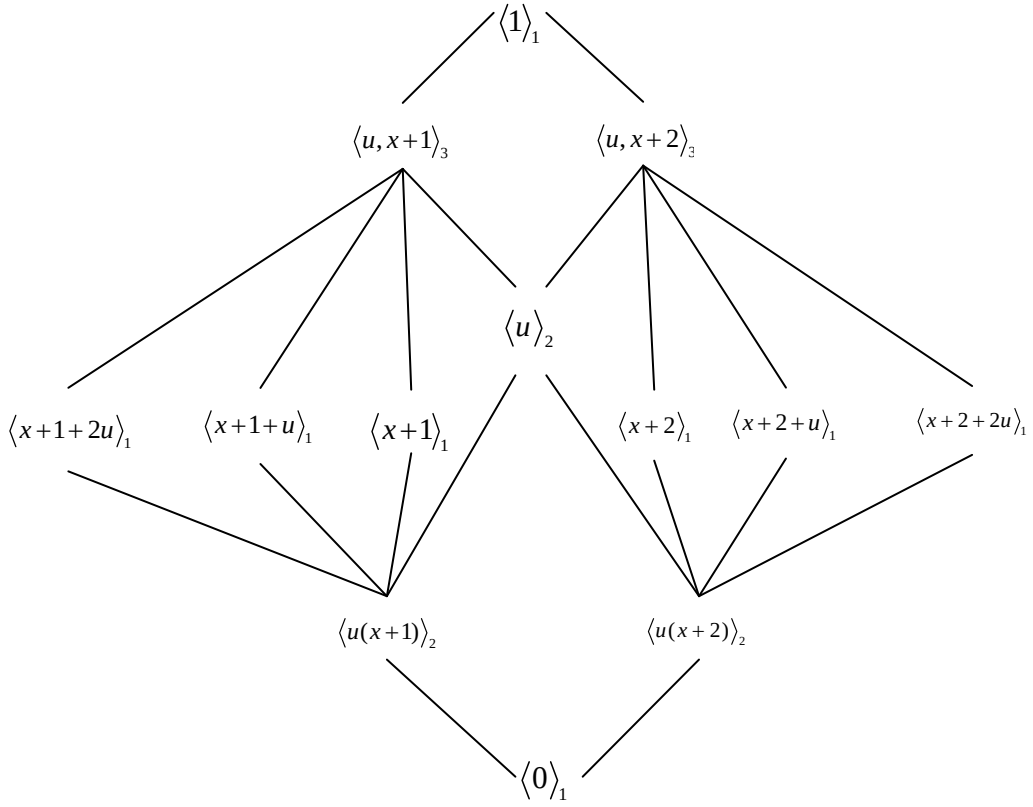
Yukarıdaki teoremde görüldüğü üzere $(F_{p^m}+uF_{p^m})[x;\Theta]\Big/\langle x^n-1\rangle$ modülünün sol alt modülleri üç farklı tiptedir. Teorem 6.5'te i şartını sağlayan alt modüller ve sıfır alt modülü SM-1, ii şartını sağlayan alt modüller SM-2 ve iii şartını sağlayan alt modüller SM-3 tipindeki sol alt modüller olarak adlandırılabilir.

**Örnek 6.2** Şekil 6.1 de $F_3+uF_3[x]\Big/\langle x^2-1\rangle$ halkasının ideallerinin latis şeması verilmiştir. $\Theta_{id,2}(a+ub)=a+2bu$ , $F_3+uF_3$ üzerinde mertebesi $2$ olan bir otomorfizmadır ($a,b\in F_3$). Şekil 6.2 de ise $F_3+uF_3[x;\Theta_{id,2}]\Big/\langle x^2-1\rangle$ halkasının

ideallerinin latis şeması verilmiştir. $1,2$ ve $3$ indisleri sırasıyla SM-1,SM-2 ve SM-3 tipindeki alt idealleri belirtmektedir [12].




Şekil 6. 1 $F_3 + uF_3[x] \Big/ \langle x^2 - 1 \rangle$ halkasının ideallerinin latis şeması




Şekil 6. 2 $F_3 + uF_3[x;\Theta_{id,2}]/\langle x^2-1\rangle$ halkasının ideallerinin latis şeması

## 6.2 $F_4 + uF_4$ Üzerinde Tanımlı Skew Devirli Kodlardan $F_4$ Üzerinde Lineer Kod Eldesi

Bu kısımda $F_4 + uF_4$ üzerinde tanımlı skew devirli kodlardan ağırlığı koruyan bir dönüşüm tanımlanarak $F_4$ üzerinde lineer kodlar elde edilecektir. Bu yaklaşımla optimal kodlara çok yakın kod örneklerinin elde edilebileceği gösterilecektir. $F_4 + uF_4$ üzerinde tanımlı 6 tane otomorfizma vardır. Fakat bu kısımda sadece aşağıdaki $\Theta$ otomorfizması kullanılacaktır.

$$\Theta : F_4 + uF_4 \to F_4 + uF_4$$
$$a + ub \to a^2 + ub^2 \qquad a, b \in F_4$$

$\Theta$ otomorfizmasının mertebesi $2$ dir. $F_4 + uF_4$ ün $\Theta$ altında sabit kalan alt halkası $F_2 + uF_2$ dir. Herhangi $a + ub \in F_4 + uF_4$ elemanı için Gray dönüşümü aşağıdaki gibidir.

$$\varphi : F_4 + uF_4 \to F_4^2$$
$$(a+ub) \to (b, a+b)$$

$\varphi$ dönüşümü $(F_4 + uF_4)^n$ için şu şekilde genişletilebilir: $c \in (F_4 + uF_4)^n$ ve $a, b \in F_4^n$ olmak üzere $c = a + ub$ ise $\varphi(c) = (b, a+b)$ dir.

$w_H$ , $F_4$ üzerindeki bir kodun Hamming ağırlığını, $w_L$ ise $F_4 + uF_4$ üzerindeki kodlar için tanımladığımız Lee ağırlığını temsil etsin. $F_4 + uF_4$ üzerindeki bir elemanın Lee ağırlığı aşağıdaki gibidir:

$$w_L(a+ub) = w_H(b, a+b).$$

$F_4 + uF_4$ üzerindeki bir kodsözün Lee ağırlığı koordinatlarının Lee ağırlıkları toplamına eşittir. Herhangi iki kodsöz arasındaki Lee uzaklığı ise

$$d_L(x, y) = w_L(x - y), \quad x, y \in (F_4 + uF_4)^n$$

olarak hesaplanır.

**Teorem 6.6** Yukarıda tanımlanan $\varphi : (F_4 + uF_4)^n \to F_4^{2n}$ dönüşümü lineer ve ağırlığı (uzaklığı) koruyan bir dönüşümdür.

**İspat:** Herhangi $x, y \in (F_4 + uF_4)^n$ için $\varphi(x+y) = \varphi(x) + \varphi(y)$ ve herhangi bir $s \in F_4$ için $\varphi(sx) = s\varphi(x)$ olduğu kolayca görülür. Dolayısıyla $\varphi$ lineer dönüşümdür. Lee ağırlığının tanımından

$$d_L(x, y) = w_L(x - y) = w_H(\varphi(x - y)) = w_H(\varphi(x) - \varphi(y)) = d_H(\varphi(x), \varphi(y))$$

elde edilir. ■

**Örnek 6.3** $(F_4 + uF_4)[x; \Theta]$ halkasında $x^6 - 1$ polinomunun derecesi $4$ olan monik sağ bölenlerinden bazıları aşağıdaki gibidir.

$$\begin{aligned} x^6 - 1 &= (1 + u + x + x^2)(1 + u + x + ux^2 + x^3 + x^4) \\ &= (1 + (\alpha^2 + \alpha^2 u)x + x^2)(1 + (\alpha^2 + \alpha^2 u)x + (\alpha^2 + \alpha^2 u)x^3 + x^4). \end{aligned}$$

$g(x) = 1 + u + x + ux^2 + x^3 + x^4$ tarafından üretilen skew devirli kod $C$ olsun.

$$G=\begin{pmatrix}1+u & 1 & u & 1 & 1 & 0\\ 0 & 1+u & 1 & u & 1 & 1\end{pmatrix}$$

matrisi $C$ nin bir üreteç matrisidir. $C$ kodunun uzunluğu $6$, boyutu ise $2$ dir. $C$ kodunun minimum Lee uzaklığı $d_L(C)=6$ dır. $C$ nin Gray görüntüsü $\varphi(C)$ $F_4$ üzerinde $[12,4,6]$ parametrelerine sahip bir lineer koddur. [5] e göre $F_4$ üzerinde $[12,4,7]$ parametrelerine sahip kodlar optimaldir.

$h(x)=(x^6-1)/g(x)=1+u+x+x^2$ ve $h(x)$ in ters sıralısı

$$\begin{aligned}h_R(x)&=x^2(x^{-2}+x^{-1}+1+u)\\&=\theta^2(1+u)x^2+x+1\\&=(1+u)x^2+x+1\end{aligned}$$

olarak bulunur. $h_R$ polinomu $C^{\perp}$ kodunun üreteç polinomu aynı zamanda $C$ nin kontrol polinomudur. Bu durumda

$$H=\begin{pmatrix}1 & 1 & 1+u & 0 & 0 & 0\\ 0 & 1 & 1 & 1+u & 0 & 0\\ 0 & 0 & 1 & 1 & 1+u & 0\\ 0 & 0 & 0 & 1 & 1 & 1+u\end{pmatrix}$$

matrisi $C$ nin bir kontrol matrisi ve $C^{\perp}$ kodunun üreteç matrisidir. $C^{\perp}$ kodu $6$ uzunluğunda boyutu $4$ olan bir skew devirli koddur. $C^{\perp}$ kodunun minimum Lee uzaklığı $d_L(C^{\perp})=3$ tür. $C^{\perp}$ kodunun Gray görüntüsü ise $F_4$ üzerinde $[12,8,3]$ parametrelerine sahip lineer koddur. Brouwer'in tablosuna göre $F_4$ üzerinde $[12,8,4]$ parametrelerine sahip bir kod optimaldir [5].

Aşağıdaki teoremde $F_4+uF_4$ üzerinde tanımlı skew devrili kodların Gray görüntülerinden $F_4$ üzerinde skew parçalı devirli kodlar elde edildiği gösterilecektir.

**Teorem 6.7** $C$, $F_4+uF_4$ üzerinde tanımlı $n$ uzunluğunda skew devirli kod ve $C$ nin Gray dönüşümü altıdaki görüntüsü $\varphi(C)$ olsun. Bu durumda $\varphi(C)$, $F_4$ üzerinde $2n$ uzunluğunda indeksi $2$ olan skew parçalı devirli bir koda denktir.

**İspat:** $c=(c_0,c_1,...,c_{n-1})\in C$, $c_i=a_i+ub_i$ ve $a_i,b_i\in F_4$ $(0\le i\le n-1)$ olsun.

$$\varphi(c) = (b_0, b_1, ..., b_{n-1}, a_0 + b_0, a_1 + b_1, ..., a_{n-1} + b_{n-1}) \in \varphi(C) \subseteq F_4^{2n}.$$

$b = (b_0, b_1, ..., b_{n-1}) \in F_4^n$ ve $a + b = (a_0 + b_0, a_1 + b_1, ..., a_{n-1} + b_{n-1}) \in F_4^n$ olsun. Böylece $\varphi(c) = (b, a + b)$ dir.

$C$ bir skew devirli kod olduğundan $c' = (\Theta(c_{n-1}), \Theta(c_0), ..., \Theta(c_{n-2})) \in C$ ve $\Theta(c_i) = a_i^2 + ub_i^2$ dir. Bu durumda

$$\varphi(c') = (b_{n-1}^2, b_0^2, ...b_{n-2}^2, a_{n-1}^2 + b_{n-1}^2, a_0 + b_0, ..., a_{n-2}^2 + b_{n-2}^2) \in \varphi(C) \subseteq F_4^{2n} \text{ ve}$$

$$\varphi(c') = (\sigma(b), \sigma(a + b)) \in \varphi(C)$$

elde edilir. Tanım 4.2'den $\varphi(C)$, $F_4$ üzerinde $n$ uzunluğunda indeksi $2$ olan skew parçalı devirli bir koda denktir. ■

## BÖLÜM 7

# $F_4 + vF_4$ HALKASI ÜZERİNDE TANIMLI SKEW DEVİRLİ KODLAR

Bu bölümde öncelikle $F_4[v]\Big/\langle v^2 - v\rangle = F_4 + vF_4$ halkasının yapısal özellikleri ve bu halka üzerinde tanımlı lineer kodların yapısı incelenecektir. Literatürde ilk olarak $F_4 + vF_4$ halkası üzerinde skew devirli kodlar tanımlanacaktır. Ardından $F_4 + vF_4$ halkası üzerinde tanımlı skew devirli kodların temel ideallere karşılık geldiği gösterilecek ve idempotent üreteçleri belirlenecektir. Ayrıca bu halka üzerinde tanımlı optimal kod örnekleri verilecektir.

$F_4 + vF_4 = \{a + bv \,|\, a, b \in F_4\}$ kümesi standart toplama işlemi ve $v^2 = v$ kuralı ile belirli değişkeni $v$ olan polinomların çarpma işlemi altında $16$ elemanlı bir halkadır. $\mathbb{Z}_{16}$ ve $F_4 + uF_4$ halkalarının aksine sonlu zincir halkası değildir. $F_4 + vF_4$ halkası, maksimal idealleri $\langle v\rangle$, $\langle 1+v\rangle$ olan yarı lokal bir halkadır.

$F_4 + vF_4$ halkası üzerinde tanımlı aşikar olmayan otomorfizmalar aşağıdaki gibidir.

$$\begin{aligned} \theta : F_4 + vF_4 &\to F_4 + vF_4 & \qquad \theta' : F_4 + vF_4 &\to F_4 + vF_4 \\ a + vb &\to a^2 + vb^2 & a + vb &\to a + (1+v)b \end{aligned}$$

$\theta$ ve $\theta'$ otomorfizmalarının mertebesi $2$ dir. $\theta$ altında sabit kalan alt halka $F_2 + vF_2 = \{0, 1, v, 1+v\}$ ve $\theta'$ altında sabit kalan alt halka ise $F_4$ tür. $\theta$ otomorfizması $F_4$ cisminin elemanları üzerinde $\theta(a) = a^2$ olarak etki etmektedir.

Bu bölümde sadece $\theta$ otomorfizması kullanılarak $(F_4+vF_4)[x;\theta]$ skew polinom halkası ve $F_4+vF_4$ halkası üzerinde tanımlı skew devirli kodlar irdelenecektir.

$(F_4+vF_4)[x;\theta]=\{a_0+..+a_nx^n \,|a_i\in F_4, n\in\mathbb{N}\}$ kümesi önceki bölümlerdeki tanımlara benzer olarak standart toplama işlemi ve $(ax^i)*(bx^j)=a\theta^i(b)x^{i+j}$, $(a,b\in F_4+vF_4)$ kuralı ile belirli çarpma işlemi altında değişmeli olmayan polinom halkasıdır. Bu halkaya $F_4+vF_4$ üzerinde tanımlı skew polinom halkası denir.

$(F_4+vF_4)[x;\theta]$ halkası sol(sağ) Öklidyen değildir. Fakat sağ ve sol bölme algoritması bazı polinomlar için tanımlıdır.

**Teorem 7.1** $f,g\in(F_4+vF_4)[x;\theta]$ olsun. $f\neq 0$ ve $g$ polinomunun baş katsayısı birimsel ise

$$f=qg+r,\qquad der(r)<der(g)$$

olacak şekilde $q,r\in(F_4+vF_4)[x;\theta]$ polinomları vardır ve tek türlüdür.

Yukarıdaki teoremde $r=0$ ise $g$ polinomu $f$ nin bir sağ bölenidir. Sol bölme algoritması da benzer şekilde tanımlıdır.

### 7.1 $F_4+vF_4$ Üzerinde Tanımlı Lineer Kodlar

[14] te $F_2+vF_2$ halkası üzerinde tanımlı devirli kodların yapısı ve özellikleri incelenmiş ve bu halka üzerinde tanımlı devirli kodların tek eleman tarafından üretildiği gösterilmiştir. Bu çalışmadaki bulgulardan yararlanarak $F_4+vF_4$ halkası üzerindeki lineer kodlar incelenecektir. [14] te tanımlanan Gray dönüşümüne benzer olarak $F_4+vF_4$ ten $F_4^2$ üzerine bir Gray dönüşümü tanımlanabilir. Bu dönüşüm aşağıdaki gibidir.

$$\begin{aligned}\Phi: F_4+vF_4 &\to {F_4}^2\\ a+bv &\to (a,a+b)\end{aligned}$$

$\Phi$ birebir ve örtendir. $\Phi$ dönüşümü $F_4+vF_4$ üzerindeki kodsözlere genişletilebilir. $c\in(F_4+vF_4)^n$ ve $a,b\in F_4^n$ olsun. $c=a+vb$ ise $\Phi(c)=(a,a+b)$ dir. $w_H$, $F_4$

üzerindeki bir kodun Hamming ağırlığını, $w_L$ ise $F_4 + vF_4$ üzerindeki kodlar için tanımladığımız Lee ağırlığını temsil etsin. $F_4 + vF_4$ ün bir elemanının Lee ağırlığı

$$w_L(a+vb) = w_H(a, a+b) \text{ dir.}$$

$F_4 + vF_4$ üzerindeki bir kodsözün Lee ağırlığı koordinatlarının Lee ağırlıkları toplamına eşittir. Herhangi iki kodsözün arasındaki Lee uzaklığı,

$$d_L(x, y) = w_L(x - y), \quad x, y \in (F_4 + vF_4)^n$$

olarak hesaplanır.

**Teorem 7.2** $\Phi : (F_4 + vF_4)^n \to F_4^{2n}$ dönüşümü lineer ve ağırlığı koruyan bir dönüşümdür.

**İspat:** Herhangi $x, y \in (F_4 + vF_4)^n$ için $\Phi(x+y) = \Phi(x) + \Phi(y)$ ve herhangi bir $s \in F_4$ için $\Phi(sx) = s\Phi(x)$ olduğu kolayca görülür. Dolayısıyla $\Phi$ lineer dönüşümdür. Lee ağırlığının tanımından

$$d_L(x, y) = w_L(x - y) = w_H(\Phi(x - y)) = w_H(\Phi(x) - \Phi(y)) = d_H(\Phi(x), \Phi(y))$$

elde edilir. ■

**Tanım 7.1** $A$ ve $B$ herhangi iki lineer kod olsun. $\otimes$ ve $\oplus$ işlemleri aşağıdaki gibi tanımlıdır.

$$A \otimes B = \{(a, b) \,|\, a \in A, b \in B\}$$
$$A \oplus B = \{a + b \,|\, a \in A, b \in B\}$$

$C$ , $F_4 + vF_4$ üzerinde tanımlı $n$ uzunluğunda bir lineer kod olsun. Bu durumda

$$C_1 = \{x \in F_4^n \,|\, x + vy \in C \ , \ y \in F_4^n\}$$
$$C_2 = \{x + y \in F_4^n \,|\, x + vy \in C\}$$

olarak tanımlanan $C_1$ ve $C_2$ kodları $F_4$ üzerinde lineer kodlardır. Bu bölümde yukarıdaki kümeler $C_1$ ve $C_2$ ile temsil edilecektir.

**Teorem 7.3** $C$, $F_4+vF_4$ üzerinde $n$ uzunluğunda bir lineer kod olsun. Bu durumda $\Phi(C)=C_1\otimes C_2$ ve $|C|=|C_1||C_2|$ dir. Ayrıca $\Phi(C)$ lineerdir.

**İspat:** $c=(c_1,c_2,...,c_n)\in C$ ve $c_i=r_i+v(r_i+q_i),\ 1\le i\le n$ olsun. $\Phi$ birebir ve örten olduğundan $(r_1,r_2...,r_n,q_1,q_2,...,q_n)\in\Phi(C)$ dir. Tanım gereği $(r_1,r_2,.....,r_n)\in C_1$ ve $(q_1,q_2,...,q_n)\in C_2$ olduğundan $(r_1,r_2...,r_n,q_1,q_2,...,q_n)\in C_1\otimes C_2$ dir. Dolayısıyla $\Phi(C)\subseteq C_1\otimes C_2$ dir.

Diğer yandan $r=(r_1,r_2,.....,r_n)\in C_1$ ve $q=(q_1,q_2,...,q_n)\in C_2$ olsun. Herhangi bir $(r_1,r_2...,r_n,q_1,q_2,...,q_n)\in C_1\otimes C_2$ için $a_i=r_i+vm_i$ ve $b_i=q_i+(1+v)n_i$ ($n_i,m_i\in F_4\quad 1\le i\le n$) olacak şekilde $a=(a_1,a_2,...,a_n)$, $b=(b_1,b_2,...,b_n)\in C$ vardır.

$C$ bir lineer kod olduğundan $c=(1+v)a+vb=r+v(r+q)\in C$ dir.

Buradan $\Phi(c)=(r_1,r_2...,r_n,q_1,q_2,...,q_n)$ olduğu görülür ve $C_1\otimes C_2\subseteq\Phi(C)$ elde edilir. Dolayısıyla $\Phi(C)=C_1\otimes C_2$ dir. $\Phi(C)$'nin lineer olduğu açıktır. ■

**Sonuç 7.1** $G_1$ ve $G_2$ sırasıyla $C_1$ ve $C_2$ kodlarının üreteç matrisleri olsun. Bu durumda

$$\begin{pmatrix}(1+v)G_1\\ vG_2\end{pmatrix}$$

matrisi $C$ kodunun bir üreteç matrisidir.

**İspat:** $\Phi(C)=C_1\otimes C_2$ lineer kodunun bir üreteç matrisi $\begin{pmatrix}G_1 & 0\\ 0 & G_2\end{pmatrix}$ şeklindedir. Teorem 7.3'ten $C$ nin üreteç matrisinin $\begin{pmatrix}(1+v)G_1\\ vG_2\end{pmatrix}$ olduğu görülür. ■

$C_1$ ve $C_2$ nin tanımından aşağıdaki sonuç elde edilir.

**Sonuç 7.2** $\Phi(C)=C_1\otimes C_2$ ise $C$ kodu $C=(1+v)C_1\oplus vC_2$ olarak tek türlü belirlidir.

**Önerme 7.1** $C$, $F_4+vF_4$ üzerinde tanımlı bir lineer kod olsun. $d_H$ ve $d_L$ sırasıyla minumum Hamming uzaklığı ve minimum Lee uzaklığını temsil etmek üzere $d_L(C)=d_H(\Phi(C))=\min\{d_H(C_1),d_H(C_2)\}$ dir.

**İspat:** $\Phi$, ağırlığı koruyan bir dönüşüm olduğundan,

$$d_L(C) = d_H(\Phi(C)) = d_H(C_1 \otimes C_2) = \min\{d_H(C_1), d_H(C_2)\} \text{ dir. } \blacksquare$$

$C$ bir lineer kod ve $G$ matrisi $C$ nin üreteç matrisi olsun. $G$ matrisine elementer satır ve sütun işlemleri uygulanarak aşağıdaki formda bir matris elde edilebilir.

$$G' = \begin{pmatrix} I_{k_1} & A & B & D_1 + vD_2 \\ 0 & vI_{k_2} & 0 & vC_1 \\ 0 & 0 & (1+v)I_{k_3} & (1+v)E \end{pmatrix}$$

$G'$ matrisi $C$ koduna denk bir kod üretir. Bu matriste $A, B, C_1, D_1, D_2, E$ alt matrislerin bileşenleri $F_4$ ün elemanlarından oluşur.

Bu matriste ikinci satırdaki elemanlar $v$ nin bir katı ve $v$ $F_4 + vF_4$ halkasında bir sıfır bölen olduğundan ikinci satırı $F_4 = \{0, 1, \alpha, \alpha^2\}$ ün elemanları ile çarpmak yeterlidir. Aynı şekilde üçüncü satırdaki elemanlar da $1+v$ nin bir katı ve $1+v$ bir sıfır bölen olduğundan $F_4$ ün elemanları ile çarpmak yeterlidir. Bir matriste birimsel eleman içermeyen satırlar serbest olmayan (non-free row) en az bir tane birimsel eleman içeren satırlar ise serbest satır (free row) olarak adlandırılır.

Dolayısıyla $C$ nin eleman sayısı $|C| = 16^{k_1} 4^{k_2} 4^{k_3}$ olarak elde edilir. Ayrıca, $C$ koduna $(k_1, k_2, k_3)$ tipindedir denir.

**Sonuç 7.3** $C = (1+v)C_1 \oplus vC_2$ kodu $F_4 + vF_4$ üzerinde uzunluğu $n$ olan bir lineer kod ve $C_1$ ve $C_2$ kodlarının boyutu sırasıyla $k_1$ ve $k_2$ olsun. Bu durumda $\Phi(C)$ kodu $F_4$ üzerinde $[2n, k_1 + k_2, \min\{d_H(C_1), d_H(C_2)\}]$ parametrelerine sahip bir lineer koddur.

**Önerme 7.2** $C$, $F_4 + vF_4$ üzerinde tanımlı bir lineer kod ve $C$ nin duali $C^\perp$ olsun. Bu durumda $\Phi(C^\perp) = \Phi(C)^\perp$ dir. $C$ kendine dual ise $\Phi(C)$ de kendine dualdir.

**İspat:** $c_1 = r_1 + vq_1 \in C$, $c_2 = r_2 + vq_2 \in C^\perp$ ve $r_1, q_1, r_2, q_2 \in F_4^n$ olsun. $\langle c_1, c_2 \rangle = 0$ ise

$$\langle c_1, c_2 \rangle = (r_1 + vq_1)(r_2 + vq_2) = r_1 r_2 + v(r_1 q_2 + q_1 r_2 + q_1 q_2) = 0 \text{ dır.}$$

Böylece $r_1r_2 = r_1q_2 + q_1r_2 + q_1q_2 = 0$ elde edilir. $\Phi(c_1) = (r_1, r_1 + q_1)$ ve $\Phi(c_2) = (r_2, r_2 + q_2)$ olduğundan

$$\langle \Phi(c_1), \Phi(c_2) \rangle = r_1r_2 + r_1r_2 + r_1q_2 + q_1r_2 + q_1q_2 = 0 \text{ dır.}$$

Dolayısıyla $\Phi(C^{\perp}) \subseteq \Phi(C)^{\perp}$ dir. $|C| = 16^{k_1}4^{k_2}4^{k_3}$ ve $C$ nin uzunluğu $n$ olsun. Bu durumda $\Phi(C)$ kodunun parametreleri $[2n, 2k_1 + k_2 + k_3]$ tür. $|\Phi(C)| = |C|$ olduğundan $|\Phi(C)^{\perp}| = 4^{2n-(2k_1+k_2+k_3)}$ dir.

Ayrıca $|\Phi(C^{\perp})| = |C^{\perp}| = 16^n / |C| = 16^{n-(k_1+k_2+k_3)}4^{k_2+k_3} = 4^{2n-(2k_1+k_2+k_3)}$ olduğundan $\Phi(C^{\perp}) = \Phi(C)^{\perp}$ olarak elde edilir. ■

**Teorem 7.4** $C$, $F_4 + vF_4$ üzerinde tanımlı $n$ uzunluğunda bir lineer kod ve $\Phi(C) = C_1 \otimes C_2$ olsun. Bu durumda $\Phi(C^{\perp}) = C_1^{\perp} \otimes C_2^{\perp}$ ve dolayısıyla $C^{\perp} = (1+v)C_1^{\perp} \oplus vC_2^{\perp}$ elde edilir.

**İspat:** Bir önceki önermeden $\Phi(C^{\perp}) = (C_1 \otimes C_2)^{\perp}$ olduğu görülür. O halde $C_1^{\perp} \otimes C_2^{\perp} = (C_1 \otimes C_2)^{\perp}$ olduğunu göstermek yeterli olacaktır. $C_1^{\perp} \otimes C_2^{\perp} \subseteq (C_1 \otimes C_2)^{\perp}$ olduğu açıktır. Diğer yandan $C_1 ve\, C_2$ nin parametreleri sırasıyla $[n, k_1]$ ve $[n, k_2]$ olsun. Bu durumda $|C_1^{\perp} \otimes C_2^{\perp}| = |C_1^{\perp}||C_2^{\perp}| = (C_1 \otimes C_2)^{\perp} = 4^{2n-k_1-k_2}$ elde edilir. Dolayısıyla $C_1^{\perp} \otimes C_2^{\perp} = (C_1 \otimes C_2)^{\perp}$ dir. Sonuç 7.2'den $C^{\perp} = (1+v)C_1^{\perp} \oplus vC_2^{\perp}$ olarak elde edilir. ■

## 7.2 $F_4 + vF_4$ Üzerinde Tanımlı Skew Devirli Kodlar

Önceki bölümlerde olduğu gibi skew devirli kodlar sol $(F_4 + vF_4)[x;\theta]$-alt modüller cinsinden ifade edilebilir. Aşağıdaki teorem, [4] nolu çalışmadaki Teorem 10 un bu halka üzerindeki kodlar için genellemesidir.

**Teorem 7.5** $C$, $F_4 + vF_4$ üzerinde tanımlı $n$ uzunluğunda bir lineer kod olsun. $C$ nin $F_4 + vF_4$ üzerinde bir skew devirli kod olması için gerek ve yeter koşul $C$ nin $(F_4 + vF_4)[x;\theta] / \langle x^n - 1 \rangle$ in bir sol $(F_4 + vF_4)[x;\theta]$-alt modülü olmasıdır.

$(F_4+vF_4)[x;\theta]$ halkası sol veya sağ Öklidyen olmadığından $(F_4+vF_4)[x;\theta]$ in tüm sağ veya sol idealleri temel ideal olmayabilir. Bu yüzden $F_4+vF_4$ üzerindeki skew devirli kodların sınıflandırılması zor bir problemdir. [14] nolu çalışmada $F_2+vF_2$ üzerindeki devirli kodlar değişmeli olan $(F_2+vF_2)[x]\Big/\langle x^n-1\rangle$ halkasının idealleri cinsinden belirlenmiştir ve bu halka üzerindeki devirli kodların tek bir polinom tarafından üretildiği gösterilmiştir. Bu bölümde [14] nolu çalışmada elde edilen bulgular $F_4+vF_4$ üzerinde tanımlı skew devirli kodlara uyarlanacaktır.

**Teorem 7.6** $C$, $F_4+vF_4$ üzerinde tanımlı bir lineer kod ve $C=(1+v)C_1\oplus vC_2$ olsun. $C$ nin $F_4+vF_4$ üzerinde bir skew devirli kod olması için gerek ve yeter koşul $C_1$ ve $C_2$ nin $F_4$ üzerinde birer skew devirli kod olmasıdır.

**İspat:** $c=(c_0,c_1,...,c_{n-1})\in C$ ve $c_i=r_i+vq_i,\ 0\le i\le n-1$ olsun.

$r=(r_0,r_1...,r_{n-1})$ ve $q=(q_0,q_1,...,q_{n-1})$ ise $r\in C_1$ ve $r+q\in C_2$ dir.

$C_1$ ve $C_2$ kodları $F_4$ üzerinde tanımlı birer skew devirli kod ise

$$\sigma(r)=(\theta(r_{n-1}),\theta(r_0),...,\theta(r_{n-2}))=(r_{n-1}^2,r_0^2,...,r_{n-2}^2)\in C_1 \text{ ve}$$

$\sigma(r+q)=(\theta(r_{n-1}+q_{n-1}),\theta(r_0+q_0),...,\theta(r_{n-2}+q_{n-2}))=(r_{n-1}^2+q_{n-1}^2,r_0^2+q_0^2,...,r_{n-2}^2+q_{n-2}^2)\in C_2$ dir.

Buradan $\sigma(c)=(1+v)\sigma(r)+v\sigma(r+q)\in C$ olarak elde edilir. Bu durumda $C$, $F_4+vF_4$ üzerinde tanımlı bir skew devirli koddur.

Diğer yandan herhangi $r=(r_0,r_1...,r_{n-1})\in C_1$ ve $q=(q_0,q_1,...,q_{n-1})\in C_2$ için $c_i=r_i+v(r_i+q_i),\ 0\le i\le n-1$ ise $c=(c_0,c_1,...,c_{n-1})\in C$ dir. $C$, $F_4+vF_4$ üzerinde tanımlı bir skew devirli kod ise

$$\sigma(c)=(\theta(c_{n-1}),\theta(c_0),...,\theta(c_{n-2}))=(r_{n-1}^2+vq_{n-1}^2,r_0^2+vq_0^2,...,r_{n-2}^2+vq_{n-2}^2)\in C$$

elde edilir. Neticede $\Phi(\sigma(c))=(\sigma(r),\sigma(q))\in C_1\otimes C_2$ olur. Öyleyse $\sigma(r)\in C_1$ ve $\sigma(q)\in C_2$ dir. Dolayısıyla $C_1$ ve $C_2$, $F_4$ üzerinde tanımlı birer skew devirli koddur. ■

**Sonuç 7.4** $C$ , $F_4+vF_4$ üzerinde tanımlı bir skew devirli kod ise $C$ nin dual kodu $C^{\perp}$ de bir skew devirli koddur.

**İspat:** Teorem 7.4'ten $C^{\perp}=(1+v)C_1^{\perp}\oplus vC_2^{\perp}$ dir. $F_4$ üzerinde tanımlı bir skew devirli kodun duali de skew devirli olduğundan $C_1^{\perp}$ ve $C_2^{\perp}$ de birer skew devirli koddur. Bu durumda Teorem 7.6'nın bir sonucu olarak $C^{\perp}$ kodu skew devirlidir. ■

**Sonuç 7.5** $C$ nin $F_4+vF_4$ üzerinde kendine dual bir skew devirli kod olması için gerek ve yeter koşul $C_1$ ve $C_2$ nin $F_4$ üzerinde kendine dual birer skew devirli kod olmasıdır.

**Sonuç 7.6** $C$ , $F_4+vF_4$ üzerinde $n$ uzunluğunda bir skew devirli kod olsun. Bu durumda $\Phi(C)$ , $F_4$ üzerinde $2n$ uzunluğunda indeksi $2$ olan bir skew parçalı devirli koddur.

**İspat:** Skew parçalı devirli kodların tanımı ve Teorem 7.3'ün bir sonucu olarak görülür.

**Teorem 7.7** $C=(1+v)C_1\oplus vC_2$ , $F_4+vF_4$ üzerinde $n$ uzunluğunda bir skew devirli kod olsun. $g_1$ ve $g_2$ polinomları sırasıyla $C_1$ ve $C_2$ kodlarının üreteç polinomları ise $C=\langle (1+v)g_1(x), vg_2(x)\rangle$ ve $|C|=4^{2n-der(g_1)-der(g_2)}$ dir.

**İspat:** $C_1=\langle g_1(x)\rangle$ , $C_2=\langle g_2(x)\rangle$ ve $C=(1+v)C_1\oplus vC_2$ olduğundan

$$C=\{c(x)=(1+v)r_1(x)g_1(x)+vr_2(x)g_2(x)\,|\,r_1(x),r_2(x)\in F_4[x;\theta]\}$$ dir.

Buradan $C\subseteq\langle (1+v)g_1(x), vg_2(x)\rangle\subseteq (F_4+vF_4)[x;\theta]\big/\langle x^n-1\rangle$ elde edilir.

Öte yandan $\langle (1+v)g_1(x), vg_2(x)\rangle$ nin bir elemanı $(1+v)k_1(x)g_1(x)+vk_2(x)g_2(x)$ ve $k_1(x),k_2(x)\in (F_4+vF_4)[x;\theta]\big/\langle x^n-1\rangle$ olsun. Bu durumda $(1+v)k_1(x)=(1+v)r_1(x)$ ve $vk_2(x)=vr_2(x)$ olacak şekilde $r_1(x),r_2(x)\in F_4[x,\theta]$ polinomları vardır. Dolayısıyla $\langle (1+v)g_1(x), vg_2(x)\rangle\subseteq C$ olur ve böylece $C=\langle (1+v)g_1(x), vg_2(x)\rangle$ eşitliği elde edilir. Ayrıca $|C|=|C_1||C_2|$ olduğundan $|C|=4^{2n-der(g_1)-der(g_2)}$ olarak bulunur. ■

**Teorem 7.8** $C_1$ ve $C_2$ , $F_4$ üzerinde tanımlı skew devirli kodlar, $g_1$ ve $g_2$ monik polinomları sırasıyla bu kodların üreteç polinomları ve $C=(1+v)C_1\oplus vC_2$ olsun. Bu

durumda $g(x)|(x^n-1)$ ve $C=\langle g(x)\rangle$ olacak şekilde bir $g(x)\in(F_4+vF_4)[x;\theta]$ polinomu vardır ve tek türlüdür. Ayrıca $g(x)=(1+v)g_1(x)+vg_2(x)$ dir.

**İspat:** Teorem 7.7'den $C=\langle(1+v)g_1(x),vg_2(x)\rangle$ dir. $g(x)=(1+v)g_1(x)+vg_2(x)$ ise $\langle g(x)\rangle\subseteq C$ olduğu açıkça görülür. Diğer yandan $(1+v)g_1(x)=(1+v)g(x)$ ve $vg_2(x)=vg(x)$ olduğundan $C\subseteq\langle g(x)\rangle$ elde edilir. Dolayısıyla $C=\langle g(x)\rangle$ dir.

$g_1$ ve $g_2$ polinomları $x^n-1$ in birer monik sağ böleni olduğundan $x^n-1=r_1(x)g_1(x)=r_2(x)g_2(x)$ eşitliğini sağlayan $r_1(x),r_2(x)\in F_4[x;\theta]\Big/\langle x^n-1\rangle$ vardır. Böylece

$$\begin{aligned}[(1+v)r_1(x)+vr_2(x)]g(x)&=[(1+v)r_1(x)+vr_2(x)][(1+v)g_1(x)+vg_2(x)]\\&=[(1+v)r_1(x)g_1(x)+vr_2(x)g_2(x)]\\&=[(1+v)(x^n-1)+v(x^n-1)]\\&=x^n-1\end{aligned}$$

elde edilir. Dolayısıyla $g(x)$ polinomu $x^n-1$ in bir sağ bölenidir. ■

**Sonuç 7.7** $(F_4+vF_4)[x;\theta]\Big/\langle x^n-1\rangle$ modülünün tüm sol alt modülleri devirlidir.

$F_4[x;\theta]$ halkasında $x^n-1=hg$ ve $C$, $g$ tarafından üretilen skew devirli kod ise $h_R$ polinomunun $C^\perp$ kodunun üreteç polinomu olduğu gösterilmişti. Bu kısımda $h$ polinomunun ters sıralısı olan $h_R$ polinomu kısaca $\tilde{h}$ ile gösterilecektir.

**Sonuç 7.8** $C_1$ ve $C_2$ $F_4$ üzerinde tanımlı skew devirli kodlar, $g_1$ ve $g_2$ monik polinomları sırasıyla bu kodların üreteç polinomları ve $F_4[x;\theta]$ te $x^n-1=h_1g_1$, $x^n-1=h_2g_2$ olsun. $C=(1+v)C_1\oplus vC_2$ ise $C^\perp=\langle(1+v)\tilde{h}_1(x)+v\tilde{h}_2(x)\rangle$ ve $|C^\perp|=4^{der(g_1)+der(g_2)}$ dir.

**İspat:** Teorem 7.4'ün sonucu olarak $C^\perp=(1+v)C_1^\perp\oplus vC_2^\perp$ dir. $C_1=\langle\tilde{h}_1\rangle$ ve $C_2=\langle\tilde{h}_2\rangle$ olduğundan $C^\perp=\langle(1+v)\tilde{h}_1(x)+v\tilde{h}_2(x)\rangle$ Teorem 7.8'in bir sonucu olarak elde edilir. ■

### 7.3 $F_4 + vF_4$ Üzerinde Tanımlı Skew Devirli Kodların İdempotent Üreteçleri

$C'$, $F_4$ üzerinde $n$ uzunluğunda bir skew devirli kod olsun. Teorem 4.7 den $(n,m)=(n,2)=1$ ve $(n,q)=(n,4)=1$ ise $C'$ kodunun bir idempotent üreteci vardır. O halde $n$ bir tek sayı ise $C'$ kodunun idempotent üreteci vardır.

**Teorem 7.9** $n$ bir pozitif tek tamsayı olmak üzere $C_1$ ve $C_2$, $F_4$ üzerinde $n$ uzunluğunda skew devirli kodlar olsun. $C=(1+v)C_1 \oplus vC_2$, $F_4+vF_4$ üzerinde tanımlı bir skew devirli kod ve $e_1(x)$ ve $e_2(x)$ polinomları sırasıyla $C_1$ ve $C_2$ nin idempotent üreteçleri olsun. Bu durumda $e(x)=(1+v)e_1(x)+ve_2(x)$ polinomu $C$ nin bir idempotent üretecidir.

**İspat:** Öncelikle $e(x)$ polinomunun $C$ nin bir idempotent elemanı olduğu gösterilmelidir.

$$\begin{aligned}(e(x))^2 &= ((1+v)e_1(x)+ve_2(x))^2 \\ &= (1+v)e_1(x)(1+v)e_1(x)+(1+v)e_1(x)(v)e_2(x) \\ &\quad +(v)e_2(x)(1+v)e_1(x)+(v)e_2(x)(v)e_2(x).\end{aligned}$$

$1+v, v \in Z((F_4+vF_4)[x;\theta])$ ve $(1+v)^2=1+v$ , $v^2=v$ olduğundan

$$(e(x))^2=(1+v)(e_1(x))^2+v(e_2(x))^2$$

elde edilir. $e_1(x)$ ve $e_2(x)$ $F_4[x;\theta]/(x^n-1)$ de idempotent ise $(F_4+vF_4)[x;\theta]/\langle x^n-1\rangle$'de de idempotenttir.

Dolayısıyla $(e(x))^2=(1+v)e_1(x)+ve_2(x)=e(x)$ ve $e(x)$ $C$ nin bir idempotent elemanıdır. $e_1(x)$ ve $e_2(x)$ polinomları sırasıyla $C_1$ ve $C_2$ nin üreteçleri olduğundan Teorem 7.8'in bir sonucu olarak $C=\langle e(x)\rangle$ dir. Böylece $e(x)$ polinomu $C$ nin bir idempotent üretecidir. ■

$n$ bir tek sayı ise $F_4$ üzerinde $n$ uzunluğundaki skew devirli kodların sayısı Teorem 4.5 de verilen formül yardımıyla hesaplanabilir. $F_4+vF_4$ üzerinde uzunluğu bir tek sayı olan skew devirli kodların sayısı aşağıdaki teorem yardımıyla hesaplanabilir.

**Teorem 7.10** $n$ bir tek sayı ve $x^n-1\in F_4[x;\theta]$ polinomunun indirgenemez çarpanlarına ayrılışı $x^n-1=\prod_{i=1}^{r} p_i^{s_i}(x)$ olsun. Bu durumda $F_4+vF_4$ üzerinde $n$ uzunluğundaki skew devirli kodların sayısı $\prod_{i=1}^{r}(s_i+1)^2$ dir

**İspat:** $n$ tek sayı ise Teorem 4.5 den $F_4$ üzerinde tanımlı skew devirli kodların sayısı $\prod_{i=1}^{r}(s_i+1)$ dir. Buradan $F_4+vF_4$ üzerinde $n$ uzunluğundaki skew devirli kodların sayısının $\prod_{i=1}^{r}(s_i+1)^2$ olduğu görülür. ■

**Örnek 7.1** $x^3-1$ polinomunun $F_4[x;\theta]$ daki indirgenemez çarpanlarına ayrılışı $x^3-1=(x-1)(x^2+x+1)$ dir. Bu durumda $F_4+vF_4$ üzerine $n=3$ uzunluğunda sıfırdan farklı $15$ adet skew devirli kod vardır.

$C_1$ ve $C_2$ $F_4$ üzerinde $n=3$ uzunluğunda skew devirli kodlar ve $C_1=\langle g_1(x)\rangle=\langle 1+x\rangle$ ve $C_2=\langle g_2(x)\rangle=\langle 1+x\rangle$ olsun. Bu durumda $C=(1+v)C_1\oplus vC_2$ kodu $F_4+vF_4$ üzerinde tanımlı $n$ uzunluğunda bir skew devirli kod ve $C=\langle (1+v)g_1(x)+vg_2(x)\rangle=\langle 1+x\rangle$ dir.

$$G=\begin{pmatrix}(1+v)G_1\\ vG_2\end{pmatrix}=\begin{pmatrix}1+v & 1+v & 0\\ 0 & 1+v & 1+v\\ v & v & 0\\ 0 & v & v\end{pmatrix}$$

matrisi $C$ nin bir üreteç matrisidir. $G$ matrisine elementer satır işlemleri uygulandığında $G'=\begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 1\end{pmatrix}$ olarak elde edilir. $G'$ matrisinin $2$ satırı da serbest olduğundan $|C|=16^2$ dir. $C$ kodunun Gray dönüşümü altındaki görüntüsü $\Phi(C)$ $F_4$ üzerinde $[6,4,2]$ parametrelerine sahip bir lineer koddur. [5] e göre $GF(4)$ üzerinde $[6,4,2]$ parametrelerine sahip bu kod optimaldir.

$C_1=\langle 1+x\rangle$ kodu için bir idempotent üreteç $e_1(x)=x+x^2$ ve $C_2=\langle 1+x\rangle$ kodu için bir idempotent üreteç $e_2(x)=x+x^2$ olarak bulunur. O halde $e(x)=(1+v)(x+x^2)+v(x+x^2)=x+x^2$ polinomu $C$ nin bir idempotent üretecidir.

Çizelge 7.1 de $F_4+vF_4$ üzerinde $n=3$ uzunluğunda sıfırdan farklı tüm skew devirli kodların üreteç matisleri, Hamming uzaklıkları ($d_H(C_i)$) ve $\Phi$ altındaki görüntülerinin parametreleri verilmiştir. Çizelgede verilen $[6,6,1]_4$ ve $[6,4,2]_4$ parametrelerine sahip bu kodlar optimaldir.

Çizelge 7. 1 $F_4+vF_4$ üzerinde $n=3$ uzunluğundaki skew devirli kodlar

| | Üreteç matrisi | $\lvert C_i\rvert$ | Üreteç polinomu | İdempotent üreteci | $d_H$ | $\Phi(C_i)$ |
|---|---|---|---|---|---|---|
| $C_1$ | $\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$ | $16^3$ | 1 | 1 | 1 | $[6,6,1]_4^*$ |
| $C_2$ | $\begin{pmatrix}1&1&0\\0&1&1\\0&0&v\end{pmatrix}$ | $16^2 4^1$ | $1+(1+v)x$ | $v+(1+v)x+(1+v)x^2$ | 1 | $[6,5,1]_4$ |
| $C_3$ | $\begin{pmatrix}1&1&1\\0&v&0\\0&0&v\end{pmatrix}$ | $16^1 4^2$ | $1+(1+v)x+(1+v)x^2$ | $1+(1+v)x+(1+v)x^2$ | 1 | $[6,4,1]_4$ |
| $C_4$ | $\begin{pmatrix}v&0&0\\0&v&0\\0&0&v\end{pmatrix}$ | $4^3$ | $v$ | $v$ | 1 | $[6,3,1]_4$ |
| $C_5$ | $\begin{pmatrix}1+v&0&0\\0&1+v&0\\0&0&1+v\end{pmatrix}$ | $4^3$ | $1+v$ | $1+v$ | 1 | $[6,3,1]_4$ |
| $C_6$ | $\begin{pmatrix}1&1&0\\0&1&1\\0&0&1+v\end{pmatrix}$ | $16^2 4^1$ | $1+v+vx$ | $1+v+vx+vx^2$ | 1 | $[6,5,1]_4$ |

| | | | | | | |
|---|---|---|---|---|---|---|
| $C_7$ | $\begin{pmatrix} 1 & 1 & 1 \\ 1+v & 0 & 0 \\ 0 & 0 & 1+v \end{pmatrix}$ | $16^1 4^2$ | $1+vx+vx^2$ | $1+vx+vx^2$ | 1 | $[6,4,1]_4$ |
| $C_8$ | $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ | $16^2$ | $1+x$ | $x+x^2$ | 2 | $[6,4,2]_4^*$ |
| $C_9$ | $\begin{pmatrix} 1 & 1 & v \\ 0 & 1+v & 1+v \end{pmatrix}$ | $16^1 4^1$ | $1+x+vx^2$ | $v+x+x^2$ | 2 | $[6,3,2]_4$ |
| $C_{10}$ | $\begin{pmatrix} 1 & 1 & 1+v \\ 0 & v & v \end{pmatrix}$ | $16^1 4^1$ | $1+x+(1+v)x^2$ | $1+v+x+x^2$ | 2 | $[6,3,2]_4$ |
| $C_{11}$ | $\begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$ | $16^1$ | $1+x+x^2$ | $1+x+x^2$ | 3 | $[6,2,3]_4$ |
| $C_{12}$ | $\begin{pmatrix} 1+v & 1+v & 1+v \end{pmatrix}$ | $4^1$ | $(1+v)+(1+v)x+(1+v)x^2$ | $(1+v)+(1+v)x+(1+v)x^2$ | 3 | $[6,1,3]_4$ |
| $C_{13}$ | $\begin{pmatrix} v & v & v \end{pmatrix}$ | $4^1$ | $v+vx+vx^2$ | $v+vx+vx^2$ | 3 | $[6,1,3]_4$ |
| $C_{14}$ | $\begin{pmatrix} 1+v & 1+v & 0 \\ 0 & 1+v & 1+v \end{pmatrix}$ | $16^1$ | $(1+v)+(1+v)x$ | $(1+v)x+(1+v)x^2$ | 2 | $[6,2,2]_4$ |
| $C_{15}$ | $\begin{pmatrix} v & v & 0 \\ 0 & v & v \end{pmatrix}$ | $16^1$ | $v+vx$ | $vx+vx^2$ | 2 | $[6,2,2]_4$ |

**Örnek 7.2** $x^5-1$ polinomunun $F_4[x;\theta]$ daki indirgenemez çarpanlarına ayrılışı $x^5-1=(1+x)(1+x+x^2+x^3+x^4)$ dir. Bu durumda $F_4+vF_4$ üzerinde $n=5$ uzunluğunda sıfırdan farklı $15$ adet skew devirli kod vardır. $g_1(x)=1+x+x^2+x^3+x^4$ ve $g_2(x)=1+x$ olsun.

Bu durumda $g(x)=(1+v)g_1(x)+vg_2(x)=1+x+(1+v)x^2+(1+v)x^3+(1+v)x^4$ ve $C=\langle g(x)\rangle$ $F_4+vF_4$ üzerinde uzunluğu $5$ olan bir skew devirli koddur.

$$G=\begin{pmatrix} 1+v & 1+v & 1+v & 1+v & 1+v \\ v & v & 0 & 0 & 0 \\ 0 & v & v & 0 & 0 \\ 0 & 0 & v & v & 0 \\ 0 & 0 & 0 & v & v \end{pmatrix}$$

matrisi bu kod için bir üreteç matrisidir. $G$ matrisine elementer satır işlemleri uygulanarak aşağıdaki matris elde edilir.

$$G'=\begin{pmatrix} 1 & 1 & 1+v & 1 & 1 \\ 0 & v & 0 & 0 & v \\ 0 & 0 & v & 0 & v \\ 0 & 0 & 0 & v & v \end{pmatrix}.$$

$G'$ matrisinin serbest olan bir satırı serbest olmayan $4$ satırı olduğundan $|C|=16^1 4^3=4^5$ tir. Böylece $C$ nin Gray dönüşümü altındaki görüntüsü $\Phi(C)$, $[10,5,2]_4$ parametrelerine sahip bir lineer koddur.

**Örnek 7.3** $F_4[x;\theta]$ da $x^4-1=(x^2+x+\alpha^2)(x^2+x+\alpha)$ dir.

$g_1(x)=x^2+x+\alpha^2$ ve $g_2(x)=x^2+x+\alpha$ olsun. Bu durumda $g(x)=x^2+x+\alpha^2+v$ ve $C=\langle g(x)\rangle$, $F_4+vF_4$ üzerinde uzunluğu $4$ olan bir skew devirli koddur.

$$G=\begin{pmatrix} \alpha^2+\alpha^2 v & 1+v & 1+v & 0 \\ 0 & \alpha+\alpha v & 1+v & 1+v \\ \alpha v & v & v & 0 \\ 0 & \alpha^2 v & v & v \end{pmatrix}$$

matrisi $C$ nin bir üreteç matrisidir. $G$ matrisine elementer satır işlemleri uygulanarak aşağıdaki matris elde edilir.

$$G' = \begin{pmatrix} \alpha^2+v & \alpha^2+v & 0 & 1 \\ 0 & \alpha+v & 1 & 1 \end{pmatrix}.$$

$G'$ matrisinin $2$ satırı da serbest olduğundan $|C| = 16^2 = 4^4$ tür. $\Phi(C)$, $[8,4,3]_4$ parametrelerine sahip bir lineer koddur.

**Örnek 7.4** $F_4[x;\theta]$ da $x^4 - 1 = (x^2 + \alpha x + \alpha^2)(x^2 + \alpha x + \alpha)$ dır.

$g_1(x) = x^2 + \alpha x + \alpha^2$ ve $g_2(x) = x^2 + \alpha x + \alpha$ olsun. Bu durumda $g(x) = x^2 + \alpha x + \alpha^2 + v$ ve $C = \langle g(x) \rangle$, $F_4 + vF_4$ üzerinde uzunluğu $4$ olan bir skew devirli koddur.

$$G = \begin{pmatrix} \alpha^2+\alpha^2 v & \alpha+\alpha v & 1+v & 0 \\ 0 & \alpha+\alpha v & \alpha^2+\alpha^2 v & 1+v \\ \alpha v & \alpha v & v & 0 \\ 0 & \alpha^2 v & \alpha^2 v & v \end{pmatrix}$$

matrisi $C$ nin bir üreteç matrisidir ve $G$ nin $4$ satırı da serbest olmadığından $|C| = 4^4$ tür Böylece $\Phi(C)$, $[8,4,3]_4$ parametrelerine sahip bir lineer koddur.

**Örnek 7.5** $F_4[x;\theta]$ da $x^4 - 1 = (x+1)(x+\alpha^2)(x+\alpha)(x+1)$ dır. $g_1(x) = x+1$ ve $g_2(x) = x+\alpha$ olsun. Bu durumda $g(x) = (1+v)g_1(x) + vg_2(x) = x+1+\alpha^2 v$ ve $C = \langle g(x) \rangle$, $F_4 + vF_4$ üzerinde tanımlı bir skew devirli koddur. $C_1 = \langle g_1(x) \rangle$, $F_4$ üzerinde boyutu $k_1 = 3$ ve $C_2 = \langle g_2(x) \rangle$, $F_4$ üzerinde boyutu $k_2 = 3$ olan skew devirli kodlardır. O halde $C$ nin Gray dönüşümü altındaki görüntüsü $\Phi(C)$ nin boyutu $k = k_1 + k_2 = 6$ dır. Dolayısıyla $\Phi(C)$, $[8,6,2]_4$ parametrelerine sahip bir lineer koddur. [5] e göre bu parametrelere sahip lineer kodlar optimaldir.

# BÖLÜM 8

## SONUÇ VE ÖNERİLER

Skew devirli kodlar cebirsel yapısı nedeniyle optimal kod elde etme açısından avantajlı ve araştırmaya açıktır. Bu tezde skew devirli kodlarla ilgili mevcut çalışmalar irdelenmiş ve örneklendirilmiştir. Skew devirli kodların bazı şartlar altında sayıları idempotent üreteçleri belirlenmiştir. Ayrıca $F_4 + vF_4$ halkası üzerinde skew devirli kodlar tanımlanmış ve bu halka üzerinde tanımlı skew devirli kodların tek bir eleman tarafından üretildiği gösterilmiştir.

$F_4 + vF_4$ halkasının daha genel hali olarak $F_{q^m} + vF_{q^m}$ halkası üzerinde skew devirli kodlar tanımlanabilir. Ayrıca bu yapılar üzerinde optimal kod bulma araştırmaya açık bir problemdir.

## KAYNAKLAR


[1] Ling, S. ve Xing, C. (2004). Coding Theory: A First Course, First Edition, Cambridge University Press, New York.

[2] McDonald, B.R., (1974). Finite Rings with Identity, Marcel Dekker Inc., New York.

[3] Boucher, D., Geiselmann, W. ve Ulmer, F., (2007). "Skew Cyclic Codes", Appl Algebr. Eng., 18:379-389.

[4] Siap, I., Abualrub, T., Aydin, N. ve Seneviratne, P., (2011). "Skew Cyclic Codes of Arbitrary Length", Int. J.Inform. Coding Theory, 2:10-20.

[5] Grassl, M., Bounds on the Minimum Distance of Linear Codes and Quantum Codes", http://www.codetables.de, 20 Nisan 2013.

[6] Boucher, D. ve Ulmer, F.,(2009). "Codes as Modules over Skew Polynomial Rings", Proceedings of the 12th IMA conference on Cryptography and Coding, Lecture Notes in Computer Science, 5921:38-55.

[7] Abualrub, T., Ghrayeb, A., Aydin, N. ve Siap, I., (2010). "On the Construction of Skew Quasi-Cyclic Codes", IEEE Trans. Inform. Theory, 56:2080-2090.

[8] Boucher, D. ve Ulmer, F., (2009). "Coding with Skew Polynomial Rings", Journal of Symbolic Computation, 44:1644-1656.

[9] Boucher, D., Solé P. ve Ulmer, F., (2008). "Skew Constacyclic Codes over Galois Rings", Adv. Math. Commun., 2:273-292.

[10] Bhaintwal, M.,(2012). "Skew Quasi-Cyclic Codes over Galois Rings", Des. Codes Cryptogr., 62:85-101.

[11] Wan, Z. X., (2003). Lectures on Finite Fields and Galois Theory, First Edition, World Scientific, Singapore.

[12] Jitman, S., Ling, S. ve Udomkavanich, P., (2010). "Skew Constacyclic Codes over Finite Chain Rings", Adv. Math. Commun., (submitted).

[13] Alkhamees, Y., (1990). "The Group of Automorphisms of Finite Chain Rings", Arab Gulf Journal of Scientific Research, 8:17-28.

[14] Zhu, S., Wang, Y. ve Shi, M., (2010). "Some Results on Cyclic Codes over $F_2 + vF_2$ ", IEEE Trans. Inform. Theory, 56:1680-1684.

[15] Huffman, W. C. ve Pless, V.,(2003). Fundamentals of Error Correcting Codes, First Edition, Cambridge University Press, New York

[16] Hammons, A.R. Jr., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A. ve Solé, P., (1994). "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and Related Codes", IEEE Trans. Inform. Theory, 40:301-319.

[17] Wan, Z. X., (1997). Quaternary Codes, First Edition, World Scientific, Singapore.

[18] Hungerford, T. W., (1974). Algebra, First Edition, Springer-Verlag, New York.

[19] Giesbrecht, M., (1998). "Factoring in Skew-polynomial Rings over Finite Fields", J. Symbolic Computation, 26:463-486.

[20] Lekic, N., (2011). Skew Coding and Skew Factorisation, Master Thesis, Instute of Science, University of Utrecht, Utrecht.

[21] Çallıalp, F. ve Tekir, Ü., (2009). Değişmeli Halkalar ve Modüller, 1. Baskı, Birsen Yayınevi, İstanbul.

[22] Özen, M., Hata Düzelten Kodlar Teorisine Bir Bakış, http://web.sakarya.edu.tr/~ozen/root/dusunce/dosyalar/9.doc, 20 Mayıs 2013.

# ÖZGEÇMİŞ

**KİŞİSEL BİLGİLER**


**Adı Soyadı** : Fatmanur GÜRSOY

**Doğum Tarihi ve Yeri** : 28.06.1989/ Denizli

**Yabancı Dili** : İngilizce

**E-posta** : fnurgursoy@hotmail.com


**ÖĞRENİM DURUMU**

| Derece | Alan | Okul/Üniversite | Mezuniyet Yılı |
|---|---|---|---|
| Lisans | Matematik(İng) | Fatih Üniversitesi | 2010 |
| Lise | Fen Bilimleri | Özel Yesevi Lisesi | 2006 |

**İŞ TECRÜBESİ**

| Yıl | Firma/Kurum | Görevi |
|---|---|---|
| 2011-2012 | İstanbul Medeniyet Üniversitesi | Araştırma Görevlisi |
| 2012-.. | Yıldız Teknik Üniversitesi | Araştırma Görevlisi |

**YAYINLARI**

**Bildiri**

1. “Skew Cyclic Codes over a Special Non-Chain Ring”, IWBCMS-I, 30 May-1 June 2013, Elbasan, Albania.

**Proje**

1. “Değişmeli Olmayan Halkalar Üzerinde Tanımlı Devirli Kodlar”, YTÜ BAP, Proje no: 2012-01-03-YL01.