T.C.
MİMAR SİNAN GÜZEL SANATLAR ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MİNİMAL OLMAYAN DEVİRLİ VE DEĞİŞMELİ KODLARIN KARŞILAŞTIRMASI

YÜKSEK LİSANS TEZİ

Emre OKUYUCU

Ana Bilim Dalı: MATEMATİK

Programı: MATEMATİK YÜKSEK LİSANS

Tez Danışmanı: Dr. Öğretim Üyesi İpek TUVAY

TEMMUZ 2021

T.C.
MİMAR SİNAN GÜZEL SANATLAR ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MİNİMAL OLMAYAN DEVİRLİ VE DEĞİŞMELİ KODLARIN KARŞILAŞTIRMASI

YÜKSEK LİSANS TEZİ

Emre OKUYUCU

Ana Bilim Dalı: MATEMATİK

Programı: MATEMATİK YÜKSEK LİSANS

Tez Danışmanı: Dr. Öğretim Üyesi İpek TUVAY

TEMMUZ 2021

..... tarafından hazırlanan .... adlı bu tezin .... tezi olarak uygun olduğunu onaylarım.

.....

Tez Danışmanı

Bu çalışma, jürimiz tarafından .....Anabilim Dalında ..... tezi olarak kabul edilmiştir.

Danışman : _____

Üye : _____

Üye : _____

Üye : _____

Üye : _____

Bu tez, Mimar Sinan Güzel Sanatlar Üniversitesi Lisansüstü Tez Yazım Kılavuzuna uygun olarak yazılmıştır.

Mimar Sinan Güzel Sanatlar Üniversitesi Lisansüstü Tez Yazım Kılavuzuna uygun olarak hazırladığım bu tez çalışmasında;

- Tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- Görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel etik kurallarına uygun olarak sunduğumu,
- Başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- Atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Ücret karşılığı başka kişilere yazdırmadığımı (dikte etme dışında), uygulamalarımı yaptırmadığımı,
- Bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

ÖNSÖZ

Öğrencisi olmakla kendimi şanslı hissettiğim, her konuda ilgi ve desteğiyle yardımlarını esirgemeyen ve kendilerinden çok şey öğrendiğim değerli hocam sayın Dr. Öğr. Üyesi İpek TUVAY'a sonsuz teşekkürlerimi sunarım.

Tez jürisinde bulunmayı kabul eden Dr. Öğr. Üyesi Fatma ALTUNBULAK AKSU ve Dr. Öğr. Üyesi Roghayeh HAFEZIEH'e teşekkür ederim.

Başarımda katkısı olan beni yetiştiren Mimar Sinan Güzel Sanatlar Üniversitesi Matematik bölümü hocalarına teşekkür ederim.

Bu tez "TÜBİTAK 2210-A Genel Yurt İçi Yüksek Lisans Burs Programı" tarafından desteklenmiştir. Yüksek lisans öğrenimim boyunca maddi desteklerinden dolayı TÜBİTAK'a teşekkür ederim.

Bu sürecin her aşamasında hep arkamda olan manevi desteklerini her zaman yanımda hissettiğim annem Penpe OKUYUCU, babam Hasan OKUYUCU, abim Adem OKUYUCU ve abim Ertuğrul OKUYUCU'ya sonsuz teşekkür ederim.

Emre OKUYUCU

MİNİMAL OLMAYAN DEVİRLİ VE DEĞİŞMELİ KODLARIN KARŞILAŞTIRMASI

ÖZET

Bu tezde, p^n uzunluklu devirli grup kodları ile devirli olmayan değişmeli grup kodlarının verimliliğinin kıyaslanması üzerinde durulmuştur. [1]'de $p > 3$ olduğunda p^2 uzunluğuna sahip devirli olmayan değişmeli grup kodlarının devirli grup kodlarından daha verimli olduğu gözlemlenmiştir. Biz de bu karşılaştırmayı n, 2'den büyük bir tamsayı olmak üzere p^n uzunluğuna sahip kodlar için yaptık. Sonuç olarak, minimal olmayan bazı değişmeli grup kodlarının minimal olmayan bütün devirli grup kodlarına göre daha verimli olduğunu gösterdik.

Anahtar Kelimeler : Devirli grup kod, Değişmeli grup kod, Verimlilik

COMPARISON OF NON-MINIMAL CYCLIC AND ABELIAN CODES

ABSTRACT

In this thesis, the convenience of cyclic and non-cyclic abelian group codes of length p^n has been studied. In [1], it has been observed that non-cyclic abelian group codes of length p^2 are more convenient than cyclic group codes of the same length, provided $p > 3$. We have studied some abelian group codes of length p^n where n is an integer greater than 2. In conclusion, we observe that there exist some non-minimal abelian group codes which are more convenient than all non-minimal cyclic group codes.

Key Words **:** Cyclic group code, Abelian group code, Convenience

İçindekiler

SEMBOLLER

$\mathbb{F}_q$: q elemanlı cisim

$\mathbb{F}_q^n$: $\mathbb{F}_q$ üzerinde n boyutlu vektör uzayı

$|C|$: C kodunun eleman sayısı

$\mathbb{F}_q G$: $\mathbb{F}_q$ cismi ile G grubunun oluşturuduğu grup cebiri

$\text{supp}(\alpha)$: α'nın destek kümesi

$w(\alpha)$: α'nın Hamming ağırlığı

$w(\mathfrak{J})$: $\mathfrak{J}$ idealinin minimum ağırlığı

$\dim(\mathfrak{J})$: $\mathfrak{J}$ idealinin boyutu

$w(C)$: C kodunun minimum ağırlığı

$\dim(C)$: C kodunun boyutu

$\text{conv}(C)$: C kodunun verimliliği

$\widehat{H}$: H grubunun elemanlarının toplamının $|H|$'ye bölümü

$S_{cc}(G)$: G grubunun tüm ko-devirli altgruplarını içeren küme

Bölüm 1

GİRİŞ

Kodlama teorisinin amacı, bilgilerin kaynağından hedefine eksiksiz bir şekilde aktarılmasını sağlamak ve bu aktarımda meydana gelen hataları tespit edip, hataları düzeltmektir. Bir kodun verimliliğini ölçen önemli parametreleri kodun uzunluğu, kod sözcüğü sayısı ve Hamming ağırlığıdır. Kodlama teorisinin temel problemlerinden birisi parametreleri iyi olan bir kod yazmaktır. Bir kodun Hamming ağırlığının büyük olması daha fazla hatanın tespitini ve düzeltmesini sağlar. Kodların Hamming ağırlığını hesaplamak her zaman kolay olmamaktadır.

Bazı kod aileleri diğer kod ailelerine kıyasla daha fazla cebirsel yapı içermektedir. Doğrusal kodlar ailesinin içerisinde yer alan grup kodları daha fazla cebirsel yapı barındırır. Biz, bazı grup kodlarının Hamming ağırlığını hesaplamaya çalışacağız.

Bu tez çalışmasında öncelikle, César Polcino Milies ve Fernanda Diniz de Melo'nun [1] numaralı kaynakta belirtilen makalesi incelenmiştir. Bu makalede uzunluğu p^2 olan minimal olmayan devirli grup kodları ile devirli olmayan değişmeli grup kodları karşılaştırılmıştır. Bunun sonucunda devirli olmayan değişmeli grup kodlarının daha elverişli olduğu görülmüştür. Bu

tezdeki amacımız, p^n uzunluğuna sahip minimal olmayan devirli ve değişmeli grup kodlarının hangisinin daha verimli bir kod olduğunu bulmak üzerinedir. Bunun için p^n uzunluğuna sahip devirli grup kodları ile devirli olmayan değişmeli grup kodlarının ağırlıkları ve boyutları hesaplanmıştır. Bu değerler sayesinde kodların verimliliği bulunarak bir karşılaştırılma yapılmıştır.

Bu tezin bölümleri şu şekilde planlanmıştır. İkinci bölümde tez için gerekli olan temel tanım ve teoremlerden bahsedilmiştir. Üçüncü bölümde César Polcino Milies ve Fernanda Diniz de Melo'nun [1] numaralı kaynakta belirtilen makalesi incelenmiş olup, p^2 uzunluğuna sahip bütün devirli grup kodları ile minimal olmayan değişmeli grup kodlarının verimliliği kıyaslanmıştır. Dördüncü bölümde p^2 uzunluğuna sahip kodlar için yapılan karşılaştırmanın, p^n uzunluklu kodlar için genellemesi üzerinde durulmuştur ve yapılan hesaplamaların sonucu Teorem 4.2.1'de gösterilmiştir.

Bölüm 2

TEMEL TANIM VE TEOREMLER

Bu bölümde, daha sonraki bölümlerde kullanılacak olan bazı temel tanım ve teoremlere değinilecektir. Tanım ve teoremler için ağırlıklı olarak [1], [3], [4], [5] numaralı kaynaklar kullanılmıştır.

2.1 Halkaların İdempotentleri

Tanım 2.1.1. *R birimli bir halka ve $e \in R$ olmak üzere*

(i) Eğer $e^2 = e$ sağlanıyor ise, e elemanına R halkasının ***idempotent*** *elemanı denir.*

(ii) Eğer e idempotent elemanı R halkasının merkezindeyse, e'ye ***merkezi idempotent*** *eleman denir.*

(iii) Diyelim ki e_1 ve e_2, R halkasının sıfırdan farklı olan idempotent elemanları olsun. Eğer $e_1e_2 = e_2e_1 = 0$ eşitlikleri sağlanıyorsa, e_1 ve e_2 birbirine **diktir** *denir.*

*(iv) Eğer sıfırdan farklı olan e idempotent elemanı için $e = e_1 + e_2$ eşitliğini sağlayan, birbirine dik olan sıfırdan farklı e_1, e_2 idempotentleri bulunamıyorsa, e elemanına R halkasının **ilkel idempotent** elemanı denir.*

Tanım 2.1.2. *R bir halka ve I, R halkasının bir sol ideali olsun. Eğer R halkasının $0 \subseteq J \subseteq I$ olacak şekildeki her J sol ideali için $J = \{0\}$ veya $J = I$ sağlanıyorsa, I idealine R halkasının **minimal sol ideali** denir.*

Aşağıdaki önerme literatürde Brauer'in önsavı olarak geçer.

Önerme 2.1.3. *R birimli bir halka olsun. Eğer I, R halkasının minimal sol ideali ise, ya $I^2 = \{0\}$ ya da öyle bir $e \in R$ ilkel idempotent elemanı vardır ki $I = Re$ sağlanır.*

Kanıt. İlk olarak $I^2 = \{x_1y_1 + \cdots + x_ny_n \mid x_i, y_i \in I\}$ kümesinin R halkasının bir sol ideali olduğunu gösterelim. $I \neq \emptyset$ olduğundan $I^2 \neq \emptyset$'dır. Diyelim ki $x, y \in I^2$ ve $r \in R$ olsun. Bu durumda $a_i, a_i^*, b_i, b_i^* \in I$ olmak üzere

$$x = \sum_{i=1}^{n} a_i b_i \text{ ve } y = \sum_{i=1}^{m} a_i^* b_i^*$$

olarak ifade edilebilir, üstelik

$$x - y = \sum_{i=1}^{n} a_i b_i - \sum_{i=1}^{m} a_i^* b_i^* = a_1 b_1 + \cdots + a_n b_n + (-a_1^*) b_i^* + \cdots + (-a_m^*) b_m^*$$

olduğundan, I^2 kümesinin tanımı dikkate alınırsa $x - y \in I^2$ olduğu görülür. Şimdi de

$$rx = r \sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n} r(a_i b_i) = \sum_{i=1}^{n} (ra_i) b_i$$

eşitliği dikkate alınırsa $rx \in I^2$ olduğu görülür. Dolayısıyla I^2, R halkasının sol ideali olur. I minimal sol ideal ve $I^2 \subseteq I$ olduğundan minimal ideal tanımından $I^2 = \{0\}$ ya da $I^2 = I$ olması gerekir. Son olarak eğer $I^2 \neq \{0\}$

ise uygun bir e idempotenti için $I = Re$ olduğunu göstermek istiyoruz. I idealinin sıfırdan farklı herhangi bir x elemanı için $Ix = \{tx \mid t \in I\}$ şeklinde tanımlanan küme R halkasının bir sol ideali olur. $Ix = I$ olduğundan I idealinde öyle bir e elemanı vardır ki $ex = x$ sağlanır. Bu eşitlikte her iki tarafı soldan e ile çarparsak

$$e(ex) = ex \Longrightarrow e^2x = ex \Longrightarrow e^2x - ex = 0 \Longrightarrow (e^2 - e)x = 0$$

elde ederiz. Ayrıca $J = \{r \in I \mid rx = 0\}$ şeklinde tanımlanan küme R halkasının bir sol ideali ve $J \subseteq I$ dir. I minimal ideal olduğundan $J = \{0\}$ ya da $J = I$ olması gerekir. Eğer $J = I$ eşitliği sağlanıyorsa $Jx = Ix$ olur. Buradan $\{0\} = Jx = Ix = I$ olması gerekir fakat $I \neq \{0\}$ olması ile çelişir. Dolayısıyla $J = \{0\}$ olması gerekir ve $e^2 - e \in J$ olduğundan dolayı $e^2 - e = 0$ eşitliğinden $e^2 = e$ elde ederiz. Sonuç olarak $I \neq \{0\}$ minimal sol ideali ve $e \in I$ için $\{0\} \neq Re \subseteq I$ olur. Ama I minimal ideal olduğunda, $I = Re$ sağlanır. Eğer $e = e_1 + e_2$ eşitliğini sağlayan, birbirine dik olan sıfırdan farklı e_1, e_2 idempotentleri bulunuyorsa, $Re = Re_1 \oplus Re_2$ şeklinde ifade edilebilir. Fakat bu durum Re'nin minimal ideal olması ile çelişir. Dolayısıyla $e = e_1 + e_2$ eşitliğini sağlayan, birbirine dik olan sıfırdan farklı e_1, e_2 idempotent elemanları bulunamaz, böylece e idempotent elemanı R halkasının ilkel idempotent elemanı olur. □

Tanım 2.1.4. *Eğer R halkasının kendisinden ve aşikar idealden başka ideali yoksa R halkasına* ***basit halka*** *denir. R basit olmayan birimli halkası için, eğer R halkası minimal sol ideallerin direkt toplamı olarak yazılabiliyorsa, R halkasına* ***basitimsi(semisimple) halka*** *denir.*

Not 2.1.5. *R basitimsi bir halka ise, her (sol) ideali minimal ideallerin direkt toplamı olarak yazılır ve bu minimal idealler Önerme* 2.1.3*'ten dolayı bir ilkel idempotent tarafından üretilirler.*

2.2 Grup Kodları

Tanım 2.2.1. [9] *$A = \{a_1, a_2, \cdots, a_q\}$ şeklinde q elemana sahip bir küme olsun.*

*(i) A kümesine **kod alfabesi**, A'nın elemanlarına ise **kod sembolleri** denir.*

*(ii) Her $i \in \{1, 2, \cdots, n\}$ için, $w_i \in A$ olmak üzere $w = w_1 w_2 \cdots w_n$ A üzerinde n uzunluğunda bir **q-lu sözcük** denir.*

*(iii) Aynı uzunluğa sahip q-lu sözcüklerin boş olmayan bir C kümesine **q-lu kod** denir.*

*(iv) C kümesinin her elemanına ise **kod sözcüğü** adı verilir.*

(v) C'deki kod sözcüklerinin sayısı, C'nin eleman sayısıdır ve $|C|$ olarak gösterilir.

Biz, alfabesi sonlu bir cisim olan kodlar ile ilgileneceğiz.

Tanım 2.2.2. [4] *$\mathbb{F}_q^n$ vektör uzayının bir C altuzayına, **doğrusal kod** denir.*

Tanım 2.2.3. [4] *Eğer C kodu doğrusal ve her $(a_0, a_1, \cdots, a_{n-1}) \in C$ için, $(a_{n-1}, a_0, a_1, \cdots, a_{n-2}) \in C$ oluyorsa C'ye **devirli kod** denir.*

Devirli kodlar, kodun iletimi için önemli bir husus olan hızlı kod çözme algoritmalarının oluşmasını sağlar.

Not 2.2.4. [4] *$R_n = \frac{\mathbb{F}_q[x]}{<x^n - 1>}$ bölüm halkasını ele alalım ve bu bölüm halkasının $f(x) \in R_n$ polinomunun sınıfını $[f(x)]$ ile gösterelim. Her $(a_0, a_1, \cdots, a_{n-1}) \in \mathbb{F}_q^n$ için $\varphi : \mathbb{F}_q^n \longrightarrow R_n$*

$$\varphi((a_0, a_1, \cdots, a_{n-1})) = [a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}]$$

olarak tanımlanan φ dönüşümü bir vektör uzayı izomorfizmasıdır. Bu izomorfizma sayesinde $\mathbb{F}_q^n$'deki doğrusal bir C altuzayının devirli kod olabilmesi için gerekli ve yeterli koşulun $\varphi(C)$'nin, R_n'nin bir ideali olması gerektiği görülür. Bu nedenle $\mathbb{F}_q^n$ üzerinde n uzunluğundaki devirli kodların incelenmesi ile R_n bölüm halkasının ideallerinin incelenmesi eşdeğerdir. Öte yandan, eğer C_n mertebesi n olan devirli bir grup ve $\mathbb{F}_qC_n$, $\mathbb{F}_q$ cismi üzerinde tanımlı grup cebiri ise

$$\frac{\mathbb{F}_q[x]}{< x^n - 1 >} \cong \mathbb{F}_qC_n$$

diye bir halka izomorfizması olduğu için $\mathbb{F}_q$ cismi üzerinde tanımlı n uzunluğundaki devirli kodlar $\mathbb{F}_qC_n$ grup cebirinin ideallerine karşılık gelmektedir.

Grup cebirleri, herhangi bir grup için herhangi bir cisim üzerinde tanımlanabilir. Kodlama teorisi sonlu cisimler üzerine tanımladığından aşağıdaki tanım ve sonuçları sonlu grup ve sonlu cisimler üzerine sınırlandırıyoruz.

Not 2.2.5. [4] *G bir sonlu grup ve $\mathbb{F}_q$ eleman sayısı q olan sonlu bir cisim olmak üzere*

$$\mathbb{F}_qG = \{\alpha = \sum_{g\in G} \alpha_g g \ : \alpha_g \in \mathbb{F}_q\}$$

kümesini dikkate alalım. Her $\alpha = \sum_{g\in G} \alpha_g g$, $\beta = \sum_{g\in G} \beta_g g \in \mathbb{F}_qG$ için

$$\alpha + \beta = \sum_{g\in G} \alpha_g g + \sum_{g\in G} \beta_g g = \sum_{g\in G} (\alpha_g + \beta_g) g$$

ve her $\lambda \in \mathbb{F}_q$ için

$$\lambda(\sum_{g\in G} \alpha_g g) = \sum_{g\in G} (\lambda\alpha_g) g$$

olarak tanımlanan işlemler ile birlikte $\mathbb{F}_qG$, $\mathbb{F}_q$ cismi üzerinde bir vektör uzayıdır. Ayrıca her $\alpha = \sum_{g\in G} \alpha_g g$, $\beta = \sum_{h\in G} \beta_h h \in \mathbb{F}_qG$ için

$$\alpha.\beta = (\sum_{g\in G} \alpha_g g)(\sum_{h\in G} \beta_h h) = \sum_{g,h\in G} (\alpha_g\beta_h)gh$$

olarak tanımlanan çarpma işlemi ile birlikte $\mathbb{F}_qG$, $\mathbb{F}_q$ cismi üzerinde ***grup cebiri*** *olur.*

Not 2.2.6. *Maschke Teoremi'nde, $\mathbb{F}_q$'nun karakteristiği $|G|$'yi bölmezse, $\mathbb{F}_qG$'nin basitimsi olduğunu ve dolayısıyla $\mathbb{F}_qG$'nin her (sol) idealinin minimal (sol) ideallerin direkt toplamı olarak yazılabileceği söylenir. Biz de ileryen bölümlerde bu duruma odaklanacağız.*

Tanım 2.2.7. [4] *$\mathbb{F}_q$ sonlu bir cisim ve C_m mertebesi m olan devirli grup olsun. $\mathbb{F}_qC_m$ grup cebirindeki herhangi bir ideale $\mathbb{F}_q$ cismi üzerinde* ***devirli grup kodu*** *denir.*

Devirli grup kodların bir genellemesi olarak, değişmeli grup kod tanımı aşağıdaki gibidir.

Tanım 2.2.8. *$\mathbb{F}_q$ sonlu bir cisim ve G sonlu değişmeli bir grup olsun. $\mathbb{F}_qG$ grup cebirindeki herhangi bir ideale $\mathbb{F}_q$ cismi üzerinde* ***değişmeli grup kodu*** *denir.*

Tanım 2.2.9. [1] *Herhangi bir $\alpha = \sum_{g\in G} \alpha_g g \in \mathbb{F}_qG$ için, $\mathrm{supp}(\alpha)$ ile gösterilen α'nın* ***destek kümesi***

$$\mathrm{supp}(\alpha) = \{g \in G \mid \alpha_g \neq 0\}$$

şeklinde tanımlanır.

Tanım 2.2.10. [1] *Herhangi bir* $\alpha \in \mathbb{F}_q G$ *için,* $w(\alpha)$ *ile gösterilen* α *elemanın* ***(Hamming) ağırlığı*** *adı verilen sayı,* α*'nın destek kümesinin kardinalitesi olarak tanımlanır, yani*

$$w(\alpha) = |\mathrm{supp}(\alpha)|$$

olur.

Tanım 2.2.11. [1] *Eğer* $\mathfrak{J}$*,* $\mathbb{F}_q G$*'nin bir ideali ise* $\mathfrak{J}$ *idealinin* ***minimum ağırlığı***

$$w(\mathfrak{J}) = \min\{\ |\mathrm{supp}(\alpha)| \mid \forall\ \alpha \in \mathfrak{J} \backslash \{0\}\}$$

şeklinde tanımlanır.

Bundan sonra G değişmeli grubunun belirli altgrupları ile $\mathbb{F}_q G$ grup cebirinin ilkel idempotent elemanları arasında bir ilişki kuracağız.

Önerme 2.2.12. [5, *Lemma* 3.6.6] G *sonlu bir grup ve* $H \leq G$ *olsun. Eğer* $\mathbb{F}_q$*,* $char(\mathbb{F}_q) \nmid |G|$ *olan bir cisim ise*

$$\widehat{H} = \frac{1}{|H|} \sum_{h \in H} h$$

$\mathbb{F}_q G$*'nin* **idempotent** *elemanı olur. Eğer* H*,* G *grubunun normal altgrubu ise* $\widehat{H}$*,* $\mathbb{F}_q G$*'nin* **merkezi idempotenti** *olur.*

Kanıt. Öncelikle, $\widehat{H}$'nin idempotent olduğunu gösterelim.

$$\begin{aligned}
\widehat{H}\widehat{H} &= \frac{1}{|H|}(\sum_{h\in H} h)\frac{1}{|H|}(\sum_{h\in H} h) \\
&= \frac{1}{|H|^2}(\sum_{h\in H} h)^2 \\
&= \frac{1}{|H|^2}|H|(\sum_{h\in H} h) \\
&= \frac{1}{|H|}\sum_{h\in H} h \\
&= \widehat{H}
\end{aligned}$$

olur. Son olarak, $H \trianglelefteq G$ ise $\widehat{H}$'nin merkezi idempotent olduğunu gösterelim. $H \trianglelefteq G$ olduğundan her $g \in G$ için $g^{-1}Hg = H$ sağlanır. Bu nedenle,

$$g^{-1}\widehat{H}g = \frac{1}{|H|}\sum_{h\in H} g^{-1}hg = \frac{1}{|H|}\sum_{h\in H} h = \widehat{H}$$

olur ve her $g \in G$ için $\widehat{H}g = g\widehat{H}$ sağlanır. Dolayısıyla, $\widehat{H}$ elemanı $\mathbb{F}_qG$'nin merkezi idempotenti olur. Sonuç olarak, $\mathbb{F}_qG.\widehat{H} = \widehat{H}.\mathbb{F}_qG$ sağlanır. □

Önerme 2.2.13. *H sonlu bir grup ve $K \leq H$ olmak üzere*

$$\widehat{H}\widehat{K} = \widehat{H}$$

sağlanır.

Kanıt. K, H'nin altgrubu olmak üzere

$$\begin{aligned}
\widehat{H}.\widehat{K} &= \frac{1}{|H|}(\sum_{h\in H} h)\frac{1}{|K|}(\sum_{k\in K} k) \\
&= \frac{1}{|H||K|}(\sum_{h\in H} h)(\sum_{k\in K} k) \\
&= \frac{1}{|H||K|}|K|(\sum_{h\in H} h) \\
&= \frac{1}{|H|}(\sum_{h\in H} h) \\
&= \widehat{H}
\end{aligned}$$

olur. □

Önsav 2.2.14. *G sonlu bir grup ve H, G grubunun altgrubu olsun. H altgrubunun G grubu içindeki sol kosetlerinin temsil kümesini ρ olarak adlandıralım. O zaman herhangi bir $\alpha \in \rho$ için*

$$\mathrm{supp}(\alpha\widehat{H}) = \alpha H$$

olur.

Kanıt. $\alpha \in \rho$ olmak üzere

$$\alpha\widehat{H} = \alpha(\frac{1}{|H|}\sum_{h\in H} h) = \frac{1}{|H|}\sum_{h\in H} \alpha h$$

için

$$\mathrm{supp}(\alpha\widehat{H}) = \{\alpha h \mid h \in H\} = \alpha H$$

olur. □

Önerme 2.2.15. [5, *Proposition* 3.6.7] *G sonlu bir grup ve H, G grubunun normal altgrubu olsun. $\mathbb{F}_q$, $\mathrm{char}(\mathbb{F}_q) \nmid |G|$ olan bir cisim olmak üzere aşağıdaki halka izomorfizması*

$$(\mathbb{F}_q G)\widehat{H} \cong \mathbb{F}_q(G/H)$$

vardır.

Kanıt. $(\mathbb{F}_qG)\widehat{H} \cong \mathbb{F}_q(G/H)$ olduğunu gösterebilmek için öncelikle $G/H \cong G\widehat{H}$ olduğunu göstereceğiz. Bunun için $G\widehat{H}$ yapısını inceleyelim. G bir grup olmak üzere

$$G\widehat{H} = \{g\widehat{H} \mid g \in G\}$$

kümesi, $g_1\widehat{H}g_2\widehat{H} := g_1g_2\widehat{H}$ şeklinde tanımlanan işlem ile bir gruptur. Gerçekten de $G \neq \emptyset$ olduğundan $G\widehat{H} \neq \emptyset$'dır. Bundan başka g_1, g_2, $g_3 \in G$ olmak üzere $g_1\widehat{H}$, $g_2\widehat{H}$, $g_3\widehat{H} \in G\widehat{H}$ için

$$((g_1\widehat{H})(g_2\widehat{H}))(g_3\widehat{H}) = (g_1\widehat{H})((g_2\widehat{H})(g_3\widehat{H}))$$

eşitliğini sağlandığından $G\widehat{H}$ kümesi üzerinde tanımlanan işleme göre birleşmelidir. Eğer 1_G, G'nin birim elemanı ise $1_G\widehat{H} = \widehat{H}$, $G\widehat{H}$'nin birim elemanıdır. Eğer $g\widehat{H} \in G\widehat{H}$ ise

$$g\widehat{H}g^{-1}\widehat{H} = gg^{-1}\widehat{H} = 1_G\widehat{H} = \widehat{H} \in G\widehat{H}$$

olduğundan $g\widehat{H} \in G\widehat{H}$ elemanın tersi $g^{-1}\widehat{H} \in G\widehat{H}$'dır.

Her $g \in G$ için $\theta : G \longrightarrow G\widehat{H}$, $\theta(g) = g\widehat{H}$ olarak tanımlanan θ dönüşümü bir grup epimorfizmasıdır. Bu epimorfizma, $\mathrm{Ker}(\theta) = H$ ve $\mathrm{Im}(\theta) = G\widehat{H}$ sağlar. Böylece Birinci İzomorfizma Teoremi gereği,

$$G/\mathrm{Ker}(\theta) = G/H \cong G\widehat{H} = \mathrm{Im}(\theta)$$

olur. $\mathbb{F}_q$ cismi üzerinde $G\widehat{H}$, $\mathbb{F}_qG\widehat{H}$ için bir baz olduğundan $(\mathbb{F}_qG)\widehat{H} \cong \mathbb{F}_q(G/H)$ sağlanır. □

Tanım 2.2.16. [4] *G değişmeli bir grup olsun. $H \leq G$ olmak üzere $G/H \neq \{1\}$ ve devirli ise, H altgrubuna G grubunun* **ko-devirli (co-cyclic)** *altgrubu denir. G grubunun tüm ko-devirli altgruplarını içeren küme*

$$\mathbf{S_{cc}(G)} = \{\ H \mid H,\ G \text{ grubunun ko-devirli altgrubu } \}$$

olarak tanımlanır.

Şimde de değişmeli bir G grubunun her bir ko-devirli H altgrubu için $\mathbb{F}_qG$'nin idempotent elemanlarını oluşturacağız.

Notasyon 2.2.17. [1] *G değişmeli bir p-grup olsun ve H, G'nin ko-devirli bir altgrubu olsun. G/H devirli bir p-grup olduğundan Eşleşme Teoreminden (Correspondence Theorem) dolayı $H < H^*$ ve $|H^*/H| = p$ sağlayan tek türlü belirli bir H^* vardır. Bu H altgrubu için $e_H = \widehat{H} - \widehat{H^*}$ olarak tanımlanır ve $e_H \neq 0$ olduğu açıktır.*

Not 2.2.18. *Yukarıda bahsedilen e_H elemanı $\mathbb{F}_qG$'nin idempotent elemanı olur. Gerçekten de*

$$e_He_H = (\widehat{H} - \widehat{H^*})(\widehat{H} - \widehat{H^*}) = \widehat{H}\widehat{H} - \widehat{H}\widehat{H^*} - \widehat{H^*}\widehat{H} + \widehat{H^*}\widehat{H^*}$$

eşitliği elde edilir ve Önerme 2.2.13'ten

$$e_He_H = \widehat{H} - \widehat{H^*} - \widehat{H^*} + \widehat{H^*} = \widehat{H} - \widehat{H^*} = e_H$$

olur.

Önsav 2.2.19. *H bir grup ve K, H'nin altgrubu olsun. Bu durumda*

$$\widehat{K}.e_H = e_H$$

sağlanır.

Kanıt. $K \leq H$ ise $K \leq H^*$ olur ve Önerme 2.2.13'ten

$$\begin{aligned} \widehat{K}.e_H &= \widehat{K}(\widehat{H} - \widehat{H^*}) \\ &= \widehat{K}\widehat{H} - \widehat{K}\widehat{H^*} \\ &= \widehat{H} - \widehat{H^*} \\ &= e_H \end{aligned}$$

sağlanır.

□

$\mathbb{F}_q G$'nin şu idempotent kümesini

$$\{e_G = \widehat{G}\} \cup \{e_H = \widehat{H} - \widehat{H^*} \mid H \in S_{cc}(G)\} \tag{2.2.1}$$

ele alalım. Şimdi bu idempotent kümesi ile ilgili önemli sonuçlar kanıtlayacağız.

Önerme 2.2.20. [3, *Lemma* 5] *Eğer p bir asal sayı, G eksponenti p^n olan bir değişmeli grup ise ve $\mathbb{F}_q$, $(p,q) = 1$ olacak şekilde eleman sayısı q olan cisim ise* (2.2.1)*'deki küme içindeki birbirinden farklı her idempotent birbirine diktir. Ayrıca,*

$$1 = \widehat{G} \ + \sum_{H \in S_{cc}(G)} e_H$$

sağlanır.

Kanıt. G grubunun birbirinden farklı ko-devirli altgrupları olan H ve K altgruplarını ele alalım. İlk olarak bu H ve K altgrupları için $e_H e_K = 0$ olduğunu gösterelim. Bu halde iki durum söz konusudur.

1.Durum: İlk önce $H \subset K$ olduğu durumu düşünelim. Bu durumda $H^* \subset K$ olur ve Önerme 2.2.13'ten

$$e_H e_K = (\widehat{H} - \widehat{H^*})(\widehat{K} - \widehat{K^*}) = \widehat{K} - \widehat{K^*} - \widehat{K} + \widehat{K^*} = 0$$

olur. Benzer şekilde $K \subset H$ için de yapılabilir.

2.Durum : Şimdi $H \not\subset K$ ve $K \not\subset H$ olsun. Bu durumda $H \subset H^*$ ve $K \subset K^*$ olduğu için $HK \subset H^*K^*$ olur. Diğer yandan $H \subset HK$, $K \subset HK$ olduğundan $H^* \subset HK$, $K^* \subset HK$ olur ve bunlardan dolayı $H^*K^* \subset HK$'dır.

Dolayısıyla $H^*K^* = HK$'dır. Ayrıca, $H \subset H^*$ ve $K \subset K^*$ olduğundan $HK \subset HK^* \subset H^*K^*$ ve $HK \subset H^*K \subset H^*K^*$ sağlanır. Fakat az önce $H^*K^* = HK$ olduğu gösterdik. O zaman $H^*K^* = HK^* = H^*K = HK$ olur. Sonuç olarak,

$$\begin{aligned} e_H e_K &= (\widehat{H} - \widehat{H^*})(\widehat{K} - \widehat{K^*}) \\ &= \widehat{H}\widehat{K} - \widehat{H}\widehat{K^*} - \widehat{H^*}\widehat{K} + \widehat{H^*}\widehat{K^*} \\ &= \widehat{HK} - \widehat{HK^*} - \widehat{H^*K} + \widehat{H^*K^*} \\ &= 0 \end{aligned}$$

olur. Eğer idempotent elemanlardan biri $e_G = \widehat{G}$ 'ya eşit ise benzer bir sonuç elde edilir.

Son olarak idempotentlerin toplamının 1'e eşit olduğunu gösterelim. $\mathcal{S}$, G/H devirli olacak şekilde G grubunun tüm H altgruplarını içeren küme olmak üzere $e = \sum_{H \in S} e_H$ olarak tanımlayalım ve $e = 1$ olduğunu iddia ediyoruz. Bunu kanıtlamak için $(\mathbb{F}_q G)e = \mathbb{F}_q G$ olduğunu göstermek yeterlidir. Daha önce gösterdik ki bu idempotent elemanlar birbirine diktir. Bu durumda

$$(\mathbb{F}_q G)e = \bigoplus_{H \in \mathcal{S}} (\mathbb{F}_q G)e_H$$

olur ve

$$\dim_{\mathbb{F}_q}((\mathbb{F}_q G)e) = \sum_{H \in \mathcal{S}} \dim_{\mathbb{F}_q}((\mathbb{F}_q G)e_H)$$

sağlanır. Ayrıca $\widehat{H} = \widehat{H^*} + e_H$ ve Önerme 2.2.13 gereği $\widehat{H^*}e_H = 0$ sağlandığından

$$(\mathbb{F}_q G)\widehat{H} = (\mathbb{F}_q G)\widehat{H^*} \oplus (\mathbb{F}_q G)e_H$$

olur. Böylece

$$\dim_{\mathbb{F}_q}((\mathbb{F}_q G)e_H) = \dim_{\mathbb{F}_q}((\mathbb{F}_q G)\widehat{H}) - \dim_{\mathbb{F}_q}((\mathbb{F}_q G)\widehat{H^*})$$

olur. Önerme 2.2.15 gereği $(\mathbb{F}_q G)\widehat{H} \cong \mathbb{F}_q(G/H)$, $(\mathbb{F}_q G)\widehat{H^*} \cong \mathbb{F}_q(G/H^*)$ sağlandığından

$$\dim_{\mathbb{F}_q}((\mathbb{F}_q G)e_H) = \dim_{\mathbb{F}_q} \mathbb{F}_q(G/H) - \dim_{\mathbb{F}_q} \mathbb{F}_q(G/H^*)$$

sonucunu elde ederiz.

G grubunun her devirli C altgrubu için C'yi üreten C'nin tüm elemanlarının kümesini $\mathcal{G}(C)$ ile gösterelim. $\mathcal{C}$, G grubunun tüm devirli altgruplarının ailesi olsun. Bu durumda $|G| = \sum_{C\in\mathcal{C}} |\mathcal{G}(C)|$ sağlanır. G bir sonlu p-grup ve G grubunun C devirli altgrubunun üreteç sayısı $\varphi(|C|)$ olduğundan $|\mathcal{G}(C)| = |C| - |C|/p$'dir. Ayrıca her $X \in \mathcal{C}$ için $\phi\colon \mathcal{C} \to \mathcal{S}$, $|X| = |G/\phi(X)|$ olacak şekilde iyi tanımlı birebir ve örten fonksiyon vardır. Bu sonlu değişmeli gruplar için karakter teorisinin bir sonucudur [8, Chapter 10]. $C \in \mathcal{C}$ için $\phi(C) = H$ olarak belirleyelim. Bu durumda

$$\dim_{\mathbb{F}_q} \mathbb{F}_q[G/H] = |C|$$

$$\dim_{\mathbb{F}_q} \mathbb{F}_q[G/H^*] = |G/H^*| = |G/H|/|H^*/H| = |C|/p$$

olur ve

$$\dim_{\mathbb{F}_q}((\mathbb{F}_q G)e_H) = |C| - |C|/p = |\mathcal{G}(C)|$$

dir. Bu durumda

$$\sum_{H\in\mathcal{S}} \dim_{\mathbb{F}_q}((\mathbb{F}_q G)e_H) = \sum_{C\in\mathcal{C}} |\mathcal{G}(C)| = |G|$$

olur. Sonuç olarak $(\mathbb{F}_q G)e = \mathbb{F}_q G$ eşitliği gösterilmiştir. Dolayısıyla $1 = \widehat{G} + \sum_{H\in S_{cc}(G)} e_H$ elde ederiz. □

Teorem 2.2.21. [3, *Theorem* 4.1] *p bir asal sayı olmak üzere G, eksponenti p^n olan değişmeli p-grup olsun. $\mathbb{F}_qG$ için (2.2.1)'deki dik idempotentler kümesinin ilkel idempotentler kümesi olabilmesi için gerekli ve yeterli koşul*

(i) $p^n = 2$ ve q tek sayı

(ii) $p^n = 4$ ve $q \equiv 3(mod 4)$

(iii) p tek asal sayı ve $U(\mathbb{Z}_{p^n})$'de $o(q) = \phi(p^n)$

durumlarından birinin sağlanmasıdır.

Not 2.2.22. *G bir grup ve H, G grubunun normal altgrubu olsun. τ, H altgrubunun G grubu içindeki sol kosetlerinin temsil kümesi olmak üzere*

$$G = \bigcup_{t \in \tau} tH$$

olarak ifade edebiliriz.

Önerme 2.2.23. [1] *G sonlu değişmeli bir grup ve H, G'nin altgrubu ve τ, H altgrubunun G içindeki sol kosetlerinin temsil kümesi olsun. $\mathbb{F}_q$, $\mathrm{char}(\mathbb{F}_q) \nmid |G|$ olan bir cisim olsun. Bu durumda;*

(i) Her $\alpha \in \mathbb{F}_qG$ için $\alpha_t \in \mathbb{F}_qH$ olmak üzere

$$\alpha = \sum_{t \in \tau} \alpha_t t$$

olarak ifade edilir.

(ii) Her $x \in H$ için $x\widehat{H} = \widehat{H}$ olur.

(iii) $\alpha_t \in \mathbb{F}_q H$ *olmak üzere,*

$$\alpha_t \widehat{H} = \epsilon(\alpha_t)\widehat{H}$$

eşitliği sağlanır.

(Burada $\epsilon(\alpha_t)$*,* α_t*'nin katsayılarının* $\mathbb{F}_q$ *üzerindeki toplamıdır.)*

Kanıt. (i) Not 2.2.22'den dolayı

$$\begin{aligned} \alpha &= \sum_{t\in\tau}(\sum_{h\in H}\alpha_{th}th) \\ &= \sum_{t\in\tau}(\sum_{h\in H}\alpha_{th}h)t \\ &= \sum_{t\in\tau}\alpha_t t \qquad\qquad (\alpha_t \in \mathbb{F}_q H) \end{aligned}$$

olur.

(ii) İlk olarak, $x \in H$ ise $xH = H$ dır. Böylece

$$x\widehat{H} = x(\frac{1}{|H|}\sum_{h\in H}h) = \frac{1}{|H|}(\sum_{h\in H}xh) = \frac{1}{|H|}(\sum_{h\in H}h) = \widehat{H}$$

eşitliği sağlanır.

(iii) $c_h \in \mathbb{F}_q$ olmak üzere $\alpha_t = \sum_{h\in H} c_h h$ olarak tanımlansın. İlk olarak $\alpha_t\widehat{H}$'yı inceleyelim.

$$\alpha_t\widehat{H} = (\sum_{h\in H}c_h h)\widehat{H} = \sum_{h\in H}c_h h\widehat{H} \overset{\text{(ii)}}{=} \sum_{h\in H}c_h\widehat{H}$$

olur. Diğer taraftan,

$$\epsilon(\alpha_t)\widehat{H} = \epsilon(\sum_{h\in H}c_h h)\widehat{H} = (\sum_{h\in H}c_h)\widehat{H} = \sum_{h\in H}c_h\widehat{H}$$

olur ve böylece eşitlik gösterilmiş olur.

□

Önerme 2.2.23'ün doğal bir sonucu olarak aşağıdaki sonucu elde ederiz.

Sonuç 2.2.24. [1] *Herhangi* $\alpha\widehat{H} \in (\mathbb{F}_q G)\widehat{H}$ *için,*

$$\alpha\widehat{H} = \sum_{t\in\tau} \alpha_t t\widehat{H} = \sum_{t\in\tau} \epsilon(\alpha_t) t\widehat{H}$$

olur. t_1 *ve* t_2, τ*'nun birbirinden farklı elemanları olmak üzere Önsav* 2.2.14 *gereği*

$$\mathrm{supp}(t_1\widehat{H}) \cap \mathrm{supp}(t_2\widehat{H}) = \emptyset$$

olur ve böylece $(\mathbb{F}_q G)\widehat{H}$*'nın her elemanının ağırlığı* $m \in \mathbb{Z}^+$ *olmak üzere* $m.|H|$ *formunda olması gerekir.*

Önerme 2.2.25. [7, *Proposition* 2.1] G *sonlu bir grup ve* $\mathbb{F}_q$, $\mathrm{char}(\mathbb{F}_q) \nmid |G|$ *olan bir cisim olsun.* H *ve* K, G *grubunun normal altgrupları olmak üzere* $H \subset K$ *olsun ve* $e = \widehat{H} - \widehat{K}$ *olarak tanımlansın. Bu durumda,*

(i) $dim_{\mathbb{F}_q}(\mathbb{F}_q G)e = |G/H| - |G/K|$

(ii) $w((\mathbb{F}_q G)e) = 2|H|$

(iii) A, K *altgrubunun* G *grubu içindeki sol kosetlerinin temsil kümesi ve* τ, H *altgrubunun* K *grubu içindeki sol kosetlerinin temsil kümesi olmak üzere*

$$\mathcal{B} = \{a(1-t)\widehat{H} \mid a \in A,\ t \in \tau\backslash\{1\}\}$$

kümesi $\mathbb{F}_q$ *cismi üzerinde tanımlı olan* $(\mathbb{F}_q G)e$ *için bir bazdır.*

Kanıt. (i) İlk olarak $e = \widehat{H} - \widehat{K}$ eşitliğinden $\widehat{H} = e + \widehat{K}$ olur. $e\widehat{K} = (\widehat{H} - \widehat{K})\widehat{K} = \widehat{H}\widehat{K} - \widehat{K}\widehat{K} = \widehat{K} - \widehat{K} = 0$ olduğundan $(\mathbb{F}_q G)\widehat{H} = (\mathbb{F}_q G)e \oplus (\mathbb{F}_q G)\widehat{K}$ olur ve dolayısıyla

$$\dim_{\mathbb{F}_q}(\mathbb{F}_q G)\widehat{H} = \dim_{\mathbb{F}_q}(\mathbb{F}_q G)e + \dim_{\mathbb{F}_q}(\mathbb{F}_q G)\widehat{K}$$

olur. $H, K \trianglelefteq G$ olduğundan Önerme 2.2.15'ten $(\mathbb{F}_q G)\widehat{H} \cong \mathbb{F}_q(G/H)$, $(\mathbb{F}_q G)\widehat{K} \cong \mathbb{F}_q(G/K)$ ve $\dim_{\mathbb{F}}(\mathbb{F}_q G)\widehat{H} = |G/H|, \dim_{\mathbb{F}_q}(\mathbb{F}_q G)\widehat{K} = |G/K|$ olur.

(ii) Sonuç 2.2.24'ten dolayı $(\mathbb{F}_q G)e$ 'nin her elemanının ağırlığı $m \in \mathbb{Z}^+$ olmak üzere $m|H|$ formunda olması gerekir. Ayrıca

$$e\widehat{H} = (\widehat{H} - \widehat{K})\widehat{H} = \widehat{H}\widehat{H} - \widehat{K}\widehat{H} = \widehat{H} - \widehat{K} = e \tag{2.2.2}$$

gözlemini yapalım. $\widehat{H} \notin (\mathbb{F}_q G)e$ olduğunu iddia ediyoruz. Bunun doğruluğunu göstermek için $\widehat{H} \in (\mathbb{F}_q G)e$ olduğunu kabul edelim. O zaman $(\mathbb{F}_q G)e$'nin birim elemanı olan e ile çarpımından $e\widehat{H} = \widehat{H}$ olması gerekirdi ama (2.2.2) eşitliği gereği $e\widehat{H} = e$ olur. Dolayısıyla çelişki elde etmiş olduk. Bu durumda $w((\mathbb{F}_q G)e) \geq 2|H|$ olur.
Diğer taraftan $h \in K \backslash H$ alalım ve

$$(1-h)e = (1-h)(\widehat{H} - \widehat{K}) = \widehat{H} - \widehat{K} - h\widehat{H} - h\widehat{K} = \widehat{H} - h\widehat{H}$$

için

$$\operatorname{supp}(\widehat{H}) \cap \operatorname{supp}(h\widehat{H}) = \emptyset$$

olduğundan $w((1-h)e) = 2|H|$'dır. Bu nedenle $w((\mathbb{F}_q G)e) = 2|H|$ olur.

(iii) Öncelikle $\mathcal{B}$ kümesinde bulunan elemanların $(\mathbb{F}_q G)e$ 'nin elemanları olduklarını gösterelim. Her $t \in \tau \backslash \{1\}$ için $(1-t)\widehat{K} = \widehat{K} - t\widehat{K} = \widehat{K} - \widehat{K} = 0$ eşitliği sağlanır ve

$$a(1-t)\widehat{H} = a(1-t)\widehat{H}(\widehat{H} - \widehat{K}) = a(1-t)\widehat{H}e \ \in (\mathbb{F}_q G)e$$

olur.

Şimdi de $\mathcal{B}$ kümesinin lineer bağımsız bir küme olduğunu gösterelim. Eğer

$$0 = \sum_{a\in A}\sum_{t\in\tau\setminus\{1\}} x_{at}(a(1-t))\widehat{H} = \sum_{a\in A}(\sum_{t\in\tau\setminus\{1\}} x_{at})a\widehat{H} - \sum_{a\in A}\sum_{t\in\tau\setminus\{1\}} x_{at}at\widehat{H}$$

ise her $a \in A,\ \ t \in \tau\setminus\{1\}$ için $x_{at} = 0$ olması gerekir. Gerçekten de $\{a\widehat{H}, at\widehat{H} \mid a \in A,\ t \in \tau\setminus\{1\}\}$ kümesindeki elemanlar birbirinden ayrık destek kümelerine sahip olduğundan $x_{at} = 0$ olur. Son olarak $\mathcal{B}$ kümesinin eleman sayısını hesaplayalım.

$$\begin{aligned} |\mathcal{B}| &= |A|(|\tau| - 1) \\ &= |\frac{G}{K}|(|\frac{K}{H}| - 1) \\ &= |\frac{G}{H}| - |\frac{G}{K}| \\ &= \dim_{\mathbb{F}_q}(\mathbb{F}_qG)e \end{aligned}$$

olur. Sonuç olarak $\mathcal{B}$ kümesi $\mathbb{F}_q$ cismi üzerinde tanımlı olan $(\mathbb{F}_qG)e$ için bir bazdır.

□

Bölüm 3

DEVİRLİ VE DEĞİŞMELİ KODLAR

Bu bölümdeki sonuçların hepsi ve kanıtları kaynakçada belirtilen [1] numaralı kaynaktan alınmıştır. İlk altbölümde p tek asal sayı olduğunda ve $\bar{q}$, $\mathbb{Z}_{p^n}$'nin birimlerinin kümesini üretecek şekilde olan q elemanlı $\mathbb{F}_q$ cismi üzerinde tanımlı p^n uzunluğuna sahip tüm devirli kodların minimum ağırlığı ve boyutu hesaplanmıştır. İkinci altbölümde $\mathbb{F}_q(C_p \times C_p)$'deki iki minimal kodun direkt toplamı olan kodların minimum ağırlık ve boyutları hesaplanmıştır. Üçüncü altbölümde p^2 uzunluğuna sahip devirli kodlar ile devirli olmayan değişmeli kodların verimliliği karşılaştırılmıştır.

3.1 Uzunluğu p^n Olan Devirli Kodlar

Bu altbölümde, $n \geq 1$, p tek asal sayı olmak üzere G mertebesi p^n olan devirli bir grup ve $\mathbb{F}_q$,

$$(q, p^n) = 1, \quad < \bar{q} >= U(\mathbb{Z}_{p^n})$$

koşulunu sağladığını kabul edeceğiz. Bu koşullar Teorem 2.2.21 (iii) durumunu sağlar.

Her $1 \leq i \leq n$ için $|G_i| = p^{n-i}$ olmak üzere

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$$

G grubunun altgrup zincirini oluşturalım. $\mathbb{F}_q G$'nin ilkel idempotentler kümesi $1 \leq i \leq n$ için

$$e_0 = \widehat{G} \;\; ve \;\; e_i = \widehat{G_i} - \widehat{G_{i-1}}$$

elemanları ile elde edilir. Bu durumda $\mathbb{F}_q$ cismi üzerinde uzunluğu p^n olan $\mathfrak{J}_i = (\mathbb{F}_q G)e_i$ idealleri Teorem 2.2.21'den ötürü minimal devirli grup kodlarımızdır. Bu minimal devirli grup kodların ağırlığı ve boyutunu hesaplamak için Önerme 2.2.15'ten

$$(\mathbb{F}_q G)\widehat{H} \cong \mathbb{F}_q[G/H] \;\; ve \;\; \dim(\mathbb{F}_q G(\widehat{H})) = [G : H]$$

olduğunu hatırlayalım.

Önerme 3.1.1. [1] *G bir sonlu devirli grup ve H, G grubunun altgrubu olsun. Eğer τ, H altgrubunun G grubu içindeki sol kosetlerinin temsil kümesi ise*

$$\mathfrak{B} = \{t\widehat{H} \mid t \in \tau\}$$

kümesi $\mathbb{F}_q$ cismi üzerinde $(\mathbb{F}_q G)\widehat{H}$ için bir bazdır.

Kanıt. Bu $\mathfrak{B}$ kümesinin $(\mathbb{F}_q G)\widehat{H}$ için bir baz olduğunu göstebilmek için lineer bağımsız üreteç kümesi olduğunu göstermemiz gerekir. Öncelikle her $t \in \tau$ için $t\widehat{H} \in (\mathbb{F}_q G)\widehat{H}$'dir. Diyelim ki $\sum_{t\in\tau} a_t t\widehat{H} = 0$ olsun. Bu eşitliğin sağlanabilmesi için her $t \in \tau$ için $a_t = 0$ olması gerekir. Çünkü Önerme 2.2.14 gereği her $t_1, t_2 \in \tau$ için $\mathrm{supp}(t_1\widehat{H}) \cap \mathrm{supp}(t_2\widehat{H}) = \emptyset$ olur ve böylece her $t \in \tau$ için $a_t = 0$ olur. Bu durumda bu küme lineer bağımsızdır. Ayrıca Önerme 2.2.15'ten $|\mathfrak{B}| = |\tau| = |G/H| = \dim((\mathbb{F}_q G)\widehat{H})$ olur. Sonuç olarak

boyutu $\dim((\mathbb{F}_qG)\widehat{H})$'ya eşit olan lineer bağımsız bir küme olduğu için $\mathbb{F}_q$ cismi üzerinde $(\mathbb{F}_qG)\widehat{H}$ için bir bazdır. □

Önerme 3.1.2. [1] *G mertebesi p^n olan devirli bir grup ve $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$ altgrup zinciri olsun.*

(i) $\dim(\mathbb{F}_qG)e_0 = 1 \;\; ve \;\; w((\mathbb{F}_qG)e_0) = |G| = p^n$

(ii) Her $1 \leq i \leq n$ için

$$\dim(\mathbb{F}_qG)e_i = |G/G_i| - |G/G_{i-1}| \;\; ve \;\; w((\mathbb{F}_qG)e_i) = 2|G_i| = 2.p^{n-i}$$

(iii) Eğer ρ, G_{i-1} altgrubunun G grubu içindeki sol kosetlerinin temsil kümesi ve τ, G_i altgrubunun G_{i-1} grubu içindeki sol kosetlerinin temsil kümesi ise

$$\mathfrak{B} = \{r(1-t)\widehat{G_i} \mid r \in \rho,\ t \in \tau\backslash\{1\}\}$$

kümesi $\mathbb{F}_q$ cismi üzerinde tanımlanan $(\mathbb{F}_qG)e_i$ için bir bazdır.

Kanıt. Önerme 2.2.25'ten iddiamız doğrudur. □

Herhangi bir C devirli grup kodu minimal devirli grup kodların direkt toplamı olarak yazılabildiğinden C devirli grup kodunun boyutu bu kodu oluşturan minimal devirli grup kodların boyutlarının toplamı olarak hesaplanır. Bu kodların minimum ağırlığının hesabı aşağıdaki sonuçta verilmiştir.

Önerme 3.1.3. [1, *Lemma II*.1] *G derecesi p^n olan devirli bir grup ve $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$, G'nin altgrup zinciri olsun. Eğer $\mathfrak{J} = \bigoplus_{i=0}^{s}(\mathbb{F}_qG)e_i$ ise bu durumda $\mathfrak{J} = (\mathbb{F}_qG)\widehat{G_s}$ olur ve*

$$w(\mathfrak{J}) = |G_s| = p^{n-s}$$

sağlanır.

Kanıt. İlk olarak

$$e_0 + e_1 + \cdots + e_s = \widehat{G} + (\widehat{G_1} - \widehat{G_0}) + \cdots + (\widehat{G_s} - \widehat{G_{s-1}}) = \widehat{G_s}$$

olduğunu gözlemleyelim. Bu durumda

$$\mathfrak{J} = \bigoplus_{i=0}^{s} (\mathbb{F}_q G) e_i = (\mathbb{F}_q G)(e_0 + e_1 + \cdots + e_s) = (\mathbb{F}_q G)\widehat{G_s}$$

ve $w(\mathfrak{J}) = w((\mathbb{F}_q G)\widehat{G_s})$ olur. Önerme 2.2.23 (i)'den dolayı verilen $\alpha \in \mathbb{F}_q G$ ve G_s altgrubunun G grubu içindeki sol kosetlerinin temsil kümesi τ için $\alpha_t \in \mathbb{F}_q G_s$ olmak üzere $\alpha = \sum_{t\in\tau} \alpha_t t$ olarak ifade edebiliriz. Önerme 2.2.23 (ii)'den her $g \in G_s$ için $g\widehat{G_s} = \widehat{G_s}$ olur ve Önerme 2.2.23 (iii)'den $\alpha_t\widehat{G_s} = \epsilon(\alpha_t)\widehat{G_s}$ sağlanır. Bu durumda herhangi $\alpha\widehat{G_s} \in (\mathbb{F}_q G)\widehat{G_s}$ için

$$\alpha\widehat{G_s} = \sum_{t\in\tau} \alpha_t t\widehat{G_s} = \sum_{t\in\tau} \epsilon(\alpha_t) t\widehat{G_s}$$

olur. t_1 ve t_2, τ birbirinden farklı elemanları olmak üzere $t_1\widehat{G_s}$ ve $t_2\widehat{G_s}$'nin destek kümeleri ayrıktır. Dolayısıyla

$$w(\alpha\widehat{G_s}) \geq w(\widehat{G_s}) = |G_s|$$

olur. Ayrıca $\widehat{G_s} \in (\mathbb{F}_q G)\widehat{G_s}$ olduğundan $w(\mathfrak{J}) = |G_s|$ olur.

□

Önerme 3.1.4. [1, *Lemma II.2*] *G derecesi p^n olan devirli bir grup ve $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$, G'nin altgrup zinciri olsun. $0 \leq i_1 \leq \cdots \leq i_t$ ve $e_{i_1} + \cdots + e_{i_t} \neq e_0 + \cdots + e_{t-1}$ olacak şekilde $\mathfrak{J} = \bigoplus_{k=0}^{t} (\mathbb{F}_q G) e_{i_k}$ tanımlansın. Bu durumda*

$$w(\mathfrak{J}) = 2|G_{i_t}| = 2p^{n-i_t}$$

olur.

Kanıt. İlk olarak $j \leq k$ olmak üzere

$$e_j\widehat{G_k} = (\widehat{G_j} - \widehat{G_{j-1}})\widehat{G_k} = \widehat{G_j} - \widehat{G_{j-1}} = e_j \tag{3.1.1}$$

olduğunu gözlemleyelim. Dolayısıyla $1 \leq k \leq t$ için

$$(\mathbb{F}_q G)e_{i_k} = (\mathbb{F}_q G)e_{i_k}\widehat{G_{i_t}} \subset (\mathbb{F}_q G)\widehat{G_{i_t}}$$

olur ve böylece $\mathfrak{J} \subset (\mathbb{F}_q G)\widehat{G_{i_t}}$'dir. Sonuç 2.2.24'ten $(\mathbb{F}_q G)\widehat{G_{i_t}}$'nin her elemanın ağırlığı $m \in \mathbb{Z}^+$ olmak üzere $m|G_{i_t}|$ formunda olduğunu biliyoruz. $\widehat{G_{i_t}} \notin \mathfrak{J}$ olduğunu iddia ediyoruz. Bunun doğruluğunu göstermek için $\widehat{G_{i_t}} \in \mathfrak{J}$ olduğunu kabul edelim. O zaman $(e_{i_1} + \cdots + e_{i_t})\widehat{G_{i_t}} = \widehat{G_{i_t}}$ olması gerekir ama (3.1.1) eşitliğinden $(e_{i_1} + \cdots + e_{i_t})\widehat{G_{i_t}} = (e_{i_1} + \cdots + e_{i_t})$ olması gerekir. Böylece $w(\mathfrak{J}) \geq 2|G_{i_t}|$'dir.

Şimdi $w(\mathfrak{J}) = 2|G_{i_t}|$ olduğunu gösterelim. Bir $g \in G_{i_{t-1}} \backslash G_{i_t}$ seçelim ve $\alpha = (1-g)e_{i_t}$ olsun. O zaman

$$(1-g)e_{i_t} = \widehat{G_{i_t}} - \widehat{G_{i_{t-1}}} - g\widehat{G_{i_t}} + g\widehat{G_{i_{t-1}}} = \widehat{G_{i_t}} - g\widehat{G_{i_t}}$$

olur. Bu durumda $w(\alpha) = 2|G_{i_t}|$ olur ve böylece $w(\mathfrak{J}) = 2|G_{i_t}|$'dir. □

Son iki önerme ışığında $\mathbb{F}_q$ cismi üzerinde p^n uzunluğuna sahip devirli grup kodların minimum ağırlığı $1 \leq i \leq n$ için p^{n-i} veya $2 \leq j \leq n$ için $2p^{n-j}$ formundadır. Olası her minimum ağırlık için $\mathbb{F}_q$ cismi üzerinde verilen ağırlığa ve maksimum boyuta sahip olan devirli grup kodları oluşturabiliriz. Yani verilen hata düzeltme kapasitesi için daha çok bilgi taşıyan devirli grup kodları belirleyebiliriz.

Teorem 3.1.5. [1, *Theorem II*.3] *G derecesi p^n olan devirli bir grup ve $\mathbb{F}_q$ cismi $(p^n, q) = 1$ ve $< \bar{q} >= U(\mathbb{Z}_{p^n})$ koşulunu sağlayan bir cisim olsun ve $0 \leq j \leq n$ olan her j tamsayısı için, $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$, G'nin altgrup zinciri olmak üzere*

1) Minimum ağırlığı p^{n-j}'ye eşit olan devirli grup kodları içinde maksimum boyuta sahip olan devirli grup kodu

$$\mathfrak{J} = (\mathbb{F}_q G)e_0 \oplus (\mathbb{F}_q G)e_1 \oplus \cdots \oplus (\mathbb{F}_q G)e_j$$

olur ve bu kodun boyutu p^j'dir.

2) Minimum ağırlığı $2p^{n-j}$'ye eşit olan devirli grup kodları içinde maksimum boyuta sahip olan devirli grup kodu

$$\mathfrak{J} = (\mathbb{F}_q G)e_1 \oplus (\mathbb{F}_q G)e_2 \oplus \cdots \oplus (\mathbb{F}_q G)e_j$$

olur ve bu kodun boyutu $p^j - 1$'dir.

3.2 Uzunluğu p^2 Olan Değişmeli Kodlar

Bu altbölümde $G =< a, b \mid a^p = b^p = 1,\ ab = ba >$ şeklinde belirlenmiş değişmeli grup ve

$$(q, p) = 1, \quad < \bar{q} >= U(\mathbb{Z}_p)$$

koşullarını sağlayan $\mathbb{F}_q$ sonlu cismini ele alalım. G grubunun tanımından dolayı $G =< a > \times < b >$ olarak ifade edebiliriz. Her $x \in G$ için $\widehat{x} = \widehat{< x >}$ olarak tanımlarsak Teorem 2.2.21'den dolayı $\mathbb{F}_q G$'nin ilkel idempotentler kümesi

$$e_0 = \widehat{G},\ e_1 = \widehat{a} - \widehat{G},\ e_2 = \widehat{b} - \widehat{G}$$

ve $1 \leq j \leq p-1$ için

$$f_j = \widehat{ab^j} - \widehat{G}$$

elemanları ile elde edilir. Böylece $\mathbb{F}_q G$'nin minimal idealleri $0 \leq i \leq 2$ için $(\mathbb{F}_q G)e_i$ ve $1 \leq j \leq p-1$ için $(\mathbb{F}_q G)f_j$ idealleridir.

Önerme 3.2.1. [1] *$G = C_p \times C_p$ olsun. Bu durumda*

(i) $\dim(\mathbb{F}_q G)e_0 = 1 \;\; ve \;\; w((\mathbb{F}_q G)e_0) = p^2$,

(ii) *$i = 1, 2$ ve $1 \leq j \leq p-1$ için*

$$\dim(\mathbb{F}_q G)e_i = \dim(\mathbb{F}_q G)f_j = p-1 \;\; ve \;\; w((\mathbb{F}_q G)e_i) = w((\mathbb{F}_q G)f_j) = 2p$$

olur.

Kanıt. Önerme 2.2.25'ten iddiamız doğrudur. □

Tanım 3.2.2. *I_1 ve I_2, $\mathbb{F}_q G$ grup cebirinin iki ideali olsun. Eğer $\mathbb{F}_q G$'ye lineer genişlemesi olan $\bar{\psi}$ için $\bar{\psi}(I_1) = I_2$ olan G'nin bir ψ otomorfizması varsa, I_1 ve I_2* ***G-denktir*** *denir.*

Not 3.2.3. [1, *Remark III*.1] *$i = 1, 2$ için $(\mathbb{F}_q G)e_i$ ve $1 \leq j \leq p-1$ için $(\mathbb{F}_q G)f_j$ minimal grup kodları ikili olarak birbirine G-denktir. Gerçekten de $\theta(a) = a$ ve $\theta(b) = ab^j$ şeklinde tanımlanan $\theta : G \longrightarrow G$ bir grup izomorfizması verir ve $\mathbb{F}_q G$'ye lineer genişlemesi olan $\bar{\theta} : \mathbb{F}_q G \longrightarrow \mathbb{F}_q G$ için her $\alpha \in \mathbb{F}_q G$ $w(\alpha) = w(\bar{\theta}(\alpha))$ koşulunu sağlar.*

Bundan sonra herhangi iki tane minimal değişmeli grup kodunun direkt toplamının tanımladığı kodun minimum ağırlığını hesaplamaya çalışacağız.

Önerme 3.2.4. [1] *G grubunun $< a >$, $< b >$ ve $1 \leq j \leq p-1$ için $< ab^j >$ altgruplarından herhangi ikisi olacak şekildeki H ve K altgruplarını ele alalım. Her seçim için de $G = H \times K$ eşitliği sağlanır. Kabul edelim ki $h \in H$ için $H =< h >$ ve $k \in K$ için $K =< k >$ olsun. Ayrıca $e = \widehat{H} - \widehat{G}$, $f = \widehat{K} - \widehat{G}$ olarak ayarlayalım ve*

$$\mathfrak{J} = (\mathbb{F}_q G)e \oplus (\mathbb{F}_q G)f$$

şeklinde tanımlansın. Bu durumda

$$\mathfrak{B} = \{(1-k^i)\widehat{H} \mid 1 \leq i \leq p-1\} \cup \{(1-h^j)\widehat{K} \mid 1 \leq j \leq p-1\}$$

kümesi $\mathbb{F}_q$ *cismi üzerinde* $\mathfrak{J}$ *için bir bazdır ve* $\dim(\mathfrak{J}) = 2(p-1)$ *olur.*

Kanıt. Önerme 2.2.25 $\mathfrak{B}$ kümesinin $\mathfrak{J}$'nin bir bazı olduğunu doğrular. □

Notasyon 3.2.5. [1] *Yukarıda tanımlanan* $\mathfrak{J}$ *ideali için* $\mathfrak{B}$ *kümesi bir baz olduğundan her* $\alpha \in \mathfrak{J}$ *için* x_i, $y_t \in \mathbb{F}_q$ *olmak üzere*

$$\alpha = \sum_{i=1}^{p-1} x_i(1-k^i)\widehat{H} + \sum_{t=1}^{p-1} y_t(1-h^t)\widehat{K}$$

şeklinde yazabiliriz. Daha sonra da

$$\alpha_1 = \left(\sum_{i=1}^{p-1} x_i + \sum_{t=1}^{p-1} y_t\right) 1, \qquad \alpha_2 = \sum_{i=1}^{p-1} \left(-x_i + \sum_{t=1}^{p-1} y_t\right) k^i$$

$$\alpha_3 = \sum_{t=1}^{p-1} \left(-y_t + \sum_{i=1}^{p-1} x_i\right) h^t, \qquad \alpha_4 = -\sum_{i,t=1}^{p-1} (x_i + y_t)\, k^i h^t$$

için

$$\alpha = \frac{1}{p}(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)$$

olarak ifade edilebilir.

Not 3.2.6. [1] *Notasyon* 3.2.5*'te tanımlanan* α_1, α_2, α_3, α_4 *elemanları ikili olarak ayrık destek kümesine sahiptirler. Bu nedenle*

$$w(\alpha) = w(\alpha_1) + w(\alpha_2) + w(\alpha_3) + w(\alpha_4)$$

eşitliği sağlanır ve $w(\alpha_1) \leq 1$, $w(\alpha_2) \leq p-1$, $w(\alpha_3) \leq p-1$, $w(\alpha_4) \leq (p-1)^2$*'dir.*

Not 3.2.7. [1] *Özel olarak*

$$x_1 = x_2 = \cdots = x_{p-1} = -y_1 = -y_2 = \cdots = -y_{p-1}$$

durumu sağlandığında $w(\alpha_1) = 0$, $w(\alpha_2) = p-1$, $w(\alpha_3) = p-1$, $w(\alpha_4) = 0$ *olur ve bu özel durum için* $w(\alpha) = 2p-2$*'dir.*

Bundan sonraki amacımız Önerme 3.2.4'te tanımlanan $\mathfrak{J}$ ideali için $w(\mathfrak{J}) = 2p-2$ olduğunu göstermek olup, bunun için de $0 < w(\alpha) < 2p-2$ olacak şekilde $\alpha \in \mathfrak{J}$ olduğunu kabul ederek bazı gözlemlerde bulunalım.

Notasyon 3.2.8. [1] $p > 3$ *olmak üzere* $\mathcal{A}$ *matrisi* $-\alpha_4$*'ün katsayılar matrisi olsun. Yani*

$$\mathcal{A} = \begin{bmatrix} x_1 + y_1 & x_1 + y_2 & \cdots & x_1 + y_{p-1} \\ x_2 + y_1 & x_2 + y_2 & \cdots & x_2 + y_{p-1} \\ \cdots & \cdots & \cdots & \cdots \\ x_{p-1} + y_1 & x_{p-1} + y_2 & \cdots & x_{p-1} + y_{p-1} \end{bmatrix}$$

şeklindedir ve $\mathcal{A}$ *matrisi en az dört tane sütun ve dört tane satırdan oluşmaktadır.*

Önerme 3.2.9. [1, *Remark III*.2] *Yukarıda tanımlanan* $\mathcal{A}$ *matrisi aynı anda üç tane girdisi sıfıra eşit olan*

$$\mathcal{A}' = \begin{bmatrix} a_{ij} & a_{ik} \\ a_{hj} & a_{hk} \end{bmatrix}$$

biçimindeki altmatrisleri içermez.

Kanıt. Kabul edelim ki $a_{ij} \neq 0$ ve $a_{ik} = a_{hk} = a_{hj} = 0$ olsun. Bu durumda

$$x_i + y_k = 0$$

$$x_h + y_k = 0$$

$$x_h + y_j = 0$$

olur ve böylece $x_i = -y_k = x_h = y_j$ eşitliklerinden $a_{ij} = x_i + y_j = 0$ olması gerekir. Fakat bu $a_{ij} \neq 0$ olması ile çelişir. O halde $\mathcal{A}'$ biçimindeki matrisin aynı anda üç tane girdisi sıfıra eşit olamaz. □

Eğer $w(\alpha) < 2p-2$ ise $w(\alpha_4) < 2p-2$ olur. Bu durumda göstereceğiz ki $p > 3$ olmak üzere $w(\alpha_4)$'ün alabileceği değerler $p-1$, $2p-3$ veya $2p-4$'tür.

Önerme 3.2.10. [1, *Lemma III*.3] *$p > 3$ için $w(\alpha_4) < 2p-2$ ise $\mathcal{A}$ matrisinin bir satırındaki ya da sütunundaki tüm girdilerin sıfıra eşit olması için gerekli ve yeterli koşul $w(\alpha_4) = p-1$ olmasıdır.*

Kanıt. Diyelim ki $\mathcal{A}$ matrisinin i_0. satırında bulunan tüm girdilerin sıfıra eşit olduğunu varsayalım. Bu durumda

$$-x_{i_0} = y_1 = y_2 = \ldots = y_{p-1}$$

eşitlikleri sağlanır. Eğer $\mathcal{A}$ matrisinde yukarıdaki girdiler dışında sıfıra eşit başka bir girdi daha bulunuyorsa i, t indeksleri için $-x_i = y_t$ olur. Her $1 \leq t \leq p-1$ için $-x_i = y_t$ ve $-x_{i_0} = y_1 = y_2 = \ldots = y_{p-1}$ eşitliklerinden dolayı i. satırda bulunan tüm girdiler sıfıra eşit olur. Her satırda $p-1$ tane girdi olduğundan ve yukarıdaki argümandan dolayı $\mathcal{A}$ matrisinde sıfıra eşit olan girdilerin toplam sayısının $(p-1)$'in bir katı olması gerekir.
Şimdi $w(\alpha_4) = 2p-k$ olarak belirleyelim. Eğer $w(\alpha_4) = 0$ ise $x_1 = x_2 = \ldots = x_{p-1} = -y_1 = -y_2 = \ldots = -y_{p-1}$ eşitlikleri sağlanır ve Not 3.2.7'de gösterildiği gibi $w(\alpha) = 2p-2$ olur. Bu nedenle $3 \leq k < 2p$ olduğunu kabul edelim ve α_4'ün

$$(p-1)^2 - (2p-k) = (p-1)^2 - 2(p-1) + k - 2$$

tane katsayısı sıfıra eşittir. Fakat $\mathcal{A}$ matrisinde sıfıra eşit olan girdilerin toplam sayısı $(p-1)$'in bir katı olduğundan

$$(p-1) \mid [(p-1)^2 - 2(p-1) + k - 2]$$

olur ve dolayısıyla $p-1 \mid k-2$'dir. Ama $1 \leq k-2 \leq 2p-3 < 2(p-1)$ olduğundan $k-2 = p-1$ olması gerekir ve bu nedenle $k = p+1$ olur. Sonuç olarak $w(\alpha_4) = 2p-k = 2p-(p+1) = p-1$'dir.

Şimdi diyelim ki $w(\alpha_4) = p-1$ olsun. Eğer $\mathcal{A}$ matrisi tüm girdileri sıfıra eşit olan bir satır içeriyorsa ispatımız biter. Varsayalım ki $\mathcal{A}$ matrisi her satırında en az bir tane sıfıra eşit olmayan girdiye sahip olan bir matris olsun. O zaman $w(\alpha_4) = p-1$ olması için her satırda sadece bir tane sıfırdan farklı girdi olması gerekir. Şimdi tüm bu girdilerin aynı sütunda olduğunu gösterelim. Birbirinden farklı olan j_1, j_2 sütunları için $i_1 \neq i_2$ olmak üzere $a_{i_1 j_1}$ ve $a_{i_2 j_2}$ girdilerinin sıfırdan farklı olduğunu kabul edelim. $p-1 > 3$ olduğundan üçüncü bir j sütununun varlığından söz edebiliriz. Bu j sütunu j_1 ve j_2'den farklı olduğu için ve her satırda sadece bir girdi sıfırdan farklı olduğundan $a_{i_1 j} = a_{i_2 j} = 0$ olması gerekir. Böylece

$$\begin{bmatrix} a_{i_1 j_1} & a_{i_1 j} \\ a_{i_2 j_1} & a_{i_2 j} \end{bmatrix}$$

altmatrisinde $a_{i_1 j_1}$ sıfırdan farklı olur ve diğer üç girdi sıfıra eşit olduğundan Önerme 3.2.9 ile çelişir. Bu durumda sıfıra eşit olmayan tüm girdilerin aynı sütunda olması gerekir ve diğer sütunlarda bulunan tüm girdiler sıfıra eşittir.

□

Önerme 3.2.11. [1, *Lemma III*.4] *Diyelim ki $p > 3$ için $w(\alpha_4) < 2p-2$ ve $w(\alpha_4) \neq p-1$ olsun. Bu durumda $\mathcal{A}$ matrisinde en az bir satır için bu satırda bulunan girdilerden sadece biri sıfırdan farklıdır.*

Kanıt. $w(\alpha_4) \neq p-1$ olduğundan Önerme 3.2.10 gereği $\mathcal{A}$ matrisi tamamı sıfıra eşit olan bir satır veya sütun içermez. $\mathcal{A}$ matrisinin her satırının en az iki tane sıfıra eşit olmayan girdiye sahip olduğunu varsayalım. $\mathcal{A}$ matrisi $(p-1)$ satırdan oluştuğundan dolayı en az $2(p-1)$ tane girdi sıfırdan farklı

olur. Dolayısıyla $w(\alpha_4) \geq 2(p-1)$ olur. Fakat bu durum $w(\alpha_4) < 2p-2$ olması ile çelişir. Bu çelişkiye her satırda en az iki tane sıfıra eşit olmayan girdi olduğunu varsayarak düştük. Böylece $\mathcal{A}$ matrisinde en az bir satırın sadece tek bir girdisi sıfırdan farklıdır. □

Önerme 3.2.12. [1, *Lemma III*.5] *$p > 3$ olmak üzere $\mathcal{A}$ matrisi Önerme* 3.2.11*'de belirtilen şekildeki gibi olan i_1, i_2 satırını içerdiğini kabul edelim ve $a_{i_1j_1}$, $a_{i_2j_2}$ sıfırdan farklı olan girdiler olsun. Bu durumda $j_1 = j_2$ olur.*

Kanıt. Eğer $j_1 \neq j_2$ ise kabulümüz gereği i_1 satırında sadece $a_{i_1j_1}$ sıfırdan farklı, i_2 satırında sadece $a_{i_2j_2}$ sıfırdan farklı olduğundan $a_{i_1j_2} = a_{i_2j_1} = 0$ olması gerekir.
$p-1 > 3$ olduğundan j_1 ve j_2 sütunlarından farklı olan bir j_3 sütunundan bahsedebiliriz. Bundan dolayı $a_{i_1j_3} = a_{i_2j_3} = 0$ olur. Böylece

$$\mathbf{A}' = \begin{bmatrix} a_{i_1j_1} & a_{i_1j_2} & a_{i_1j_3} \\ a_{i_2j_1} & a_{i_2j_2} & a_{i_2j_3} \end{bmatrix} = \begin{bmatrix} a_{i_1j_1} & 0 & 0 \\ 0 & a_{i_2j_2} & 0 \end{bmatrix}$$

altmatrisinde $a_{i_1j_1} \neq 0$, $a_{i_2j_2} \neq 0$ olduğundan Önerme 3.2.9 ile çelişir. Bu çelişkiye $j_1 \neq j_2$ olduğunu varsayarak düştük. O halde $j_1 = j_2$ olmalıdır. □

Önerme 3.2.13. [1, *Lemma III*.6] *$p > 3$ olmak üzere $\mathcal{A}$ matrisi i_1. satırında sadece $a_{i_1j_1}$ girdisi sıfırdan farklı olacak şekildeki bir matris olsun. Eğer i_2. satırda en az iki tane girdi sıfırdan farklı ise bu satırda ($a_{i_2j_1}$ hariç) tüm girdiler sıfırdan farklıdır.*

Kanıt. Bu ispatta iki durum söz konusudur.
1.Durum : $a_{i_2j_1} \neq 0$ olduğunu kabul edelim ve i_2 satırında bulunan diğer bütün girdilerin sıfırdan farklı olduklarını gösterelim. Şimdi $a_{i_2j_2}$ sıfırdan farklı olan bir diğer girdi olsun. $p-1 > 3$ olduğundan j_1 ve j_2 sütunlarından farklı

olan bir j sütunundan bahsedebiliriz. Bu durumda $a_{i_1 j} = 0$ olur ve eğer $a_{i_2 j} = 0$ eşitliği sağlanırsa

$$\begin{bmatrix} a_{i_1 j_2} & a_{i_1 j} \\ a_{i_2 j_2} & a_{i_2 j} \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ a_{i_2 j_2} & 0 \end{bmatrix}$$

altmatrisinde $a_{i_2 j_2} \neq 0$ olduğundan Önerme 3.2.9 ile çelişir. Bu çelişkiye $a_{i_2 j} = 0$ olduğunu kabul ederek düşeriz. Bu durumda i_2 satırında bulunan tüm girdiler sıfırdan farklı olur.

2.Durum : Şimdi $a_{i_2 j_1} = 0$ olarak kabul edelim ve i_2. satırda $a_{i_2 j_1}$ girdisi dışında tüm girdilerin sıfırdan farklı olduğunu gösterelim.

Eğer i_2. satırda $a_{i_2 j} = 0$ olacak şekilde başka bir girdi varsa bu durumda

$$\begin{bmatrix} a_{i_1 j_1} & a_{i_1 j} \\ a_{i_2 j_1} & a_{i_2 j} \end{bmatrix} = \begin{bmatrix} a_{i_1 j_1} & 0 \\ 0 & 0 \end{bmatrix}$$

altmatrisinde $a_{i_1 j_1} \neq 0$ olduğundan Önerme 3.2.9 ile çelişir. Böylece i_2 satırında $a_{i_2 j_1}$ dışında tüm girdiler sıfırdan farklı olur. □

Artık $w(\alpha_4)$ için olan iddiamıza hazırız.

Önerme 3.2.14. [1] *Eğer $w(\alpha_4) < 2p - 2$ ise $w(\alpha_4)$'ün alabileceği değerler $p - 1$, $2p - 3$ veya $2p - 4$'tür.*

Kanıt. İlk önce Önerme 3.2.10 ile $w(\alpha_4) = p - 1$ olması için gerek ve yeter koşulun $\mathcal{A}$ matrisinin tüm girdileri sıfıra eşit olan bir satır veya sütun içermesi olduğunu gösterdik.

Daha sonra $w(\alpha_4) \neq p - 1$ olduğunda Önerme 3.2.11'de en az bir satırda sadece bir tane girdinin sıfırdan farklı olduğunu gösterdik. Tüm satırlar böyle olsaydı $w(\alpha_4) = p - 1$ olurdu ve $w(\alpha_4) \neq p - 1$ olması ile çelişirdi. Bu nedenle $\mathcal{A}$ matrisinin en az bir satırı birden fazla girdisi sıfırdan farklı olacak şekildedir. Önerme 3.2.13 bu satırda bulunan girdilerin biri hariç hepsinin sıfırdan farklı olması gerektiğini gösterir. Bu son iki gözlem ışığı altında bize

minimum ağırlığı verecek olan matris

$$\mathcal{A} = \begin{bmatrix} 0 & \cdots & x_1 + y_j & \cdots & 0 \\ 0 & \cdots & x_2 + y_j & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & x_{k-1} + y_j & \cdots & 0 \\ x_k + y_1 & \cdots & x_k + y_j & \cdots & x_k + y_{p-1} \\ 0 & \cdots & x_{k+1} + y_j & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & x_{p-1} + y_j & \cdots & 0 \end{bmatrix}$$

formunda olup, Önerme 3.2.13 $x_k + y_j$ hariç bütün $x_i + y_j$'ler ve $x_k + y_t$'ler sıfırdan farklı olduğunu söyler. Sonuç olarak eğer $w(\alpha_4) \neq p-1$ ise $w(\alpha_4) = 2p-3$ veya $w(\alpha_4) = 2p-4$ değerlerinden biri olur.

□

Önerme 3.2.15. [1, *Lemma III*.7] *Eğer* $p > 3$ *ise* $w(\mathfrak{J}) = 2p-2$ *olur.*

Kanıt. Bu önermenin ispatını $w(\alpha_4)$'ün olası alabileceği değerler üzerine yapacağız.

Diyelim ki $w(\alpha_4) = p-1$ olsun. Bu durumda $-\alpha_4$'ün katsayılar matrisi olan $\mathcal{A}$, Önerme 3.2.10 gereği bir satırı ya da bir sütunu tamamen sıfıra eşittir. Kabul edelim ki i. satırda bulunan tüm girdiler sıfıra eşit olsun. Bu durumda $-x_i = y_1 = y_2 = \cdots = y_{p-1}$ eşitlikleri sağlanır. Eğer $\mathcal{A}$ matrisinde i. satır dışında başka bir girdi daha sıfıra eşit ise o satırda bulunan diğer girdiler de sıfıra eşit olması gerekir. O zaman $\mathcal{A}$ matrisinde sıfırdan farklı her girdinin aynı satırda olması gerekir. Diyelim ki bu satır j. satır olsun. O zaman $x_1 = x_2 = \cdots = x_{j-1} = x_{j+1} = \cdots = x_{p-1} = -y_1 = -y_2 = \cdots = -y_{p-1}$

eşitlikleri sağlanır. Bu durumda

$$\begin{aligned}
\alpha_2 &= \sum_{i=1}^{p-1}(-x_i + \sum_{t=1}^{p-1} y_t)k^i \\
&= (-x_1 + y_1 + \cdots + y_{p-1})k + \cdots + (-x_j + y_1 + \cdots + y_{p-1})k^j \\
&+ \cdots + (-x_{p-1} + y_1 + \cdots + y_{p-1})k^{p-1} \\
&= py_1k + \cdots + (-x_j + (p-1)y_1)k^j + \cdots + py_1k^{p-1}
\end{aligned}$$

olur. Eğer $y_1 = 0$ olursa $\alpha \neq 0$ olduğundan $x_j \neq 0$ olması gerekir. Bu durumda $\alpha_2 = (-x_j)k^j$ olur ve $w(\alpha_2) \geq 1$'dir. Bu özel seçim için, yine $y_1 = 0$ durumunda

$$\begin{aligned}
\alpha_3 &= \sum_{t=1}^{p-1}(-y_t + \sum_{i=1}^{p-1} x_i)h^t \\
&= (-y_1 + x_1 + \cdots + x_{p-1})h + \cdots + (-y_{p-1} + x_1 + \cdots + x_{p-1})h^{p-1} \\
&= x_jh + \cdots + x_jh^{p-1}
\end{aligned}$$

olur ve $w(\alpha_3) = p - 1$'dir. Böylece $w(\alpha) > 2p - 2$ olur. Eğer $y_1 \neq 0$ ise $w(\alpha_2) \geq p - 2$'dir. Eğer $w(\alpha_2) = p - 2$ olursa $\alpha_1 \neq 0$'dır ve böylece $w(\alpha_1) = 1$'dir. Sonuç olarak $w(\alpha) > 2p - 2$'dir.

Eğer $w(\alpha_4) = 2p - 3$ olursa $-\alpha_4$'ün katsayılar matrisi

$$\mathcal{A} = \begin{bmatrix}
0 & \cdots & x_1 + y_j & \cdots & 0 \\
0 & \cdots & x_2 + y_j & \cdots & 0 \\
\vdots & & \vdots & & \vdots \\
0 & \cdots & x_{k-1} + y_j & \cdots & 0 \\
x_k + y_1 & \cdots & x_k + y_j & \cdots & x_k + y_{p-1} \\
0 & \cdots & x_{k+1} + y_j & \cdots & 0 \\
\vdots & & \vdots & & \vdots \\
0 & \cdots & x_{p-1} + y_j & \cdots & 0
\end{bmatrix}$$

formundadır. Bu durumda $w(\alpha_2) \geq 1$ ve $w(\alpha_3) \geq 1$ olduğu gözlemlenir. Böylece $w(\alpha) \geq 2p - 2$ olur.

Son olarak $w(\alpha_4) = 2p-4$ olursa $-\alpha_4$'ün katsayılar matrisi

$$\mathcal{A} = \begin{bmatrix} 0 & \cdots & x_1+y_j & \cdots & 0 \\ 0 & \cdots & x_2+y_j & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & x_{k-1}+y_j & \cdots & 0 \\ x_k+y_1 & \cdots & 0 & \cdots & x_k+y_{p-1} \\ 0 & \cdots & x_{k+1}+y_j & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & x_{p-1}+y_j & \cdots & 0 \end{bmatrix}$$

formundadır. Bu durumda $w(\alpha_2) \geq 1$ ve $w(\alpha_3) \geq 1$ olduğu gözlemlenir. Sonuç olarak $w(\alpha) \geq 2p-2$ olur. □

Önerme 3.2.16. [1] *Eğer $p = 2$ ise $w(\mathfrak{J}) = 2$ olur.*

Kanıt. $H = \{1, h\}$, $K = \{1, k\}$ altgrupları için $e = \widehat{h} - \widehat{A}$, $f = \widehat{k} - \widehat{A}$ olarak ayarlayalım ve $\mathfrak{J} = (\mathbb{F}_q A)e \oplus (\mathbb{F}_q A)f$ şeklinde tanımlansın. Bu durumda $\mathfrak{B} = \{(1-k)\widehat{H}\} \cup \{(1-h)\widehat{K}\}$ kümesi $\mathbb{F}_q$ cismi üzerinde $\mathfrak{J}$ ideali için bir bazdır. O zaman $\alpha \neq 0 \in \mathfrak{J}$ için $x, y \in \mathbb{F}_q$ olmak üzere

$$\begin{aligned} \alpha &= x(1-k)\widehat{H} + y(1-h)\widehat{K} \\ &= \frac{1}{2}[(x+y)1 + (x-y)h + (y-x)k - (x+y)hk] \end{aligned}$$

olarak ifade edilir. Bu durumda $w(\alpha) \geq 2$ olur. Eğer $x = -y$ eşitliği sağlanırsa $w(\alpha) = 2$'dir ve böylece $w(\mathfrak{J}) = 2$ olur. □

Önerme 3.2.17. [1] *Eğer $p = 3$ ise $w(\mathfrak{J}) = 4$ olur.*

Kanıt. A grubunun $< a >$, $< b >$ ve $i = 1, 2$ için $< ab^i >$ altgruplarından herhangi biri olacak şekildeki H ve K altgruplarını ele alalım. Bu altgruplara karşılık gelen ilkel idempotent elemanlar $e = \widehat{H} - \widehat{A}$, $f = \widehat{K} - \widehat{A}$ dir ve $\mathfrak{J} = (\mathbb{F}_q A)e \oplus (\mathbb{F}_q A)f$ olarak tanımlansın. Herhangi bir $\alpha \in \mathfrak{J}$ için

$$\alpha_1 = \left(\sum_{i=1}^{2} x_i + \sum_{j=1}^{2} y_j\right) 1, \quad \alpha_2 = \sum_{i=1}^{2} \left(-x_i + \sum_{j=1}^{2} y_j\right) k^i$$
$$\alpha_3 = \sum_{j=1}^{2} \left(-y_j + \sum_{i=1}^{2} x_i\right) h^j, \quad \alpha_4 = -\sum_{i,j=1}^{2} (x_i + y_j)\, k^i h^j$$

elemanları için

$$\alpha = \frac{1}{3}(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)$$

olarak ifade edilir. Bu durumda $w(\mathfrak{J}) = 4$ olur. Bunu göstermek için öncelikle $-\alpha_4$'ün katsayıları matrisi olan

$$\mathcal{A} = \begin{bmatrix} x_1 + y_1 & x_1 + y_2 \\ x_2 + y_1 & x_2 + y_2 \end{bmatrix}$$

matrisini oluşturalım ve olabilecek tüm durumları inceleyelim. Eğer $w(\alpha_4) = 0$ olursa bu durumda $x_1 = x_2 = -y_1 = -y_2$ eşitlikleri gerçekleşir ve $w(\alpha) = 4$ olur. Eğer $w(\alpha_4) = 3$ sağlanırsa $w(\alpha_1) = 1$ dir ve böylece $w(\alpha) \geq 4$ olur. Son olarak $w(\alpha_4) = 2$ olduğunda $w(\alpha_2) \geq 1$, $w(\alpha_3) \geq 1$'dir ve böylece $w(\alpha) \geq 4$ olur. Sonuç olarak $w(\mathfrak{J}) = 4$ olur.

□

Önerme 3.2.15, Önerme 3.2.16, Önerme 3.2.17 birlikte bize aşağıdaki sonucu verir.

Teorem 3.2.18. [1, *Theorem III*.8] *Eğer p bir asal sayı, $A = C_p \times C_p$ olan bir grup, $\mathbb{F}_q$ cismi de $(p, q) = 1$ ve $< \bar{q} >= U(\mathbb{Z}_p)$ koşulunu sağlıyorsa A grubundaki indeksi p olan birbirinden farklı H ve K altgrupları için $e = \widehat{H} - \widehat{A}$, $f = \widehat{K} - \widehat{A}$ olarak belirleyelim ve $\mathfrak{J} = (\mathbb{F}_q A)e \oplus (\mathbb{F}_q A)f$ şeklinde tanımlandığında*

$$\dim(\mathfrak{J}) = w(\mathfrak{J}) = 2(p-1)$$

olur.

Örnek 3.2.19. [1, *Example III*.9] *A sonlu değişmeli grubu* $a^5 = b^5 = 1$ *için* $A =< a > \times < b >$ *olacak şekilde tanımlansın ve* $\mathbb{F}_2A$ *grup cebirini ele alalım. Bu durumda* $\mathbb{F}_2A$*'nın ilkel idempotentleri*

$$e_1 = \widehat{a} - \widehat{A},\ e_2 = \widehat{b} - \widehat{A},\ f_1 = \widehat{ab} - \widehat{A}$$

$$f_2 = \widehat{ab^2} - \widehat{A},\ f_3 = \widehat{ab^3} - \widehat{A},\ f_4 = \widehat{ab^4} - \widehat{A}$$

şeklindedir. Bu ilkel idempotentlerden yararlanarak $\mathbb{F}_2A$ *grup cebirinin birbirine izomorfik olmayacak şekildeki ideallerini inceleyelim. Bu idealleri* $I_1 = (\mathbb{F}_2A)e_1$
$I_2 = (\mathbb{F}_2A)e_1 \oplus (\mathbb{F}_2A)e_2$
$J_1 = (\mathbb{F}_2A)e_1 \oplus (\mathbb{F}_2A)e_2 \oplus (\mathbb{F}_2A)f_1$
$J_2 = (\mathbb{F}_2A)e_1 \oplus (\mathbb{F}_2A)e_2 \oplus (\mathbb{F}_2A)f_1 \oplus (\mathbb{F}_2A)f_2$
$J_3 = (\mathbb{F}_2A)e_1 \oplus (\mathbb{F}_2A)e_2 \oplus (\mathbb{F}_2A)f_1 \oplus (\mathbb{F}_2A)f_2 \oplus (\mathbb{F}_2A)f_3$
$J_4 = (\mathbb{F}_2A)e_1 \oplus (\mathbb{F}_2A)e_2 \oplus (\mathbb{F}_2A)f_1 \oplus (\mathbb{F}_2A)f_2 \oplus (\mathbb{F}_2A)f_3 \oplus (\mathbb{F}_2A)f_4$
olarak belirleyelim. Belirlenen her ideal için GAP(Groups, Algorithms Programming)[13] *yardımıyla*

$$w(I_1) = 10,\ w(I_2) = 8,\ w(J_1) = 6$$

$$w(J_2) = 4,\ w(J_3) = 2,\ w(J_4) = 2$$

olarak hesaplanmıştır.

Not 3.2.20. [1, *Remark III*.10] *A sonlu değişmeli grubu* $a^p = b^p = 1$ *için* $A =< a > \times < b >$ *olacak şekilde tanımlansın ve* $\mathbb{F}_qA$ *grup cebirini ele alalım.* $\mathbb{F}_qA$ *grup cebirinin birbirine izomorfik olmayan idealleri*

$$I_1 = (\mathbb{F}_qA)e_1,\ I_2 = (\mathbb{F}_qA)e_1 \oplus (\mathbb{F}_qA)e_2,$$

$$J_1 = (\mathbb{F}_qA)e_1 \oplus (\mathbb{F}_qA)e_2 \oplus (\mathbb{F}_qA)f_1$$

ve her $\leq i \leq p-1$ *için*

$$J_i = J_{i-1} \oplus (\mathbb{F}_q A) f_i$$

formundadırlar. Önerme 3.2.1*'den* $w((\mathbb{F}_q A)e_1) = 2p$ *ve Teorem* 3.2.18*'den* $w((\mathbb{F}_q A)e_1 \oplus (\mathbb{F}_q A)e_2) = 2p-2$ *olduğu hesaplanmıştır. Ayrıca* $w(J_{p-2}) = w(J_{p-1}) = 2$*'dir. Bu yüzden*

$$w(J_i) = w(J_{i-1}) - 2$$

eşitliği sağlanacak gibi duruyor. Fakat ispatı hem makalenin yazarları hem de bizim tarafımızdan yapılamamıştır.

Aşağıdaki örnek grup kodlarını kullanarak kod çözmenin nasıl yapılacağı hakkındadır.

Örnek 3.2.21. $G = C_3 \times C_3 =< a > \times < b >$ *ve* $q = 2$ *olmak üzere* $\mathbb{F}_2(C_3 \times C_3)$ *grup cebirini ele alalım ve*

$$\mathbb{F}_2(C_3 \times C_3) = \{1, a, a^2, b, b^2, ab, ab^2, a^2b, a^2b^2\}$$

olur. G'nin ko-devirli altgrubu olan $H =< a >$ *altgrubu ile* $\mathbb{F}_2(C_3 \times C_3)$*'ün*

$$e_H = \widehat{H} - \widehat{G} = \frac{1}{|H|}\sum_{h \in H} h - \frac{1}{|G|}\sum_{g \in G} g = b + b^2 + ab + ab^2 + a^2b + a^2b^2$$

ilkel idempotent elemanı elde edilir. Böylece,

$$\mathbb{F}_2(C_3 \times C_3)e_H = \{0, e_H, be_H, b^2e_H\}$$

$\mathbb{F}_2(C_3 \times C_3)$*'ün minimal ideali olur.* $E = \{e_1, \cdots, e_9\}$ *kümesi* $\mathbb{F}_2^9$*'un standart sıralı bazı olmak üzere*

$$\Phi : C_3 \times C_3 \longrightarrow E$$

$$1 \longmapsto e_1$$

$$a \longmapsto e_2$$

$$a^2 \longmapsto e_3$$

$$b \longmapsto e_4$$

$$b^2 \longmapsto e_5$$

$$ab \longmapsto e_6$$

$$ab^2 \longmapsto e_7$$

$$a^2b \longmapsto e_8$$

$$a^2b^2 \longmapsto e_9$$

şeklinde tanımlanan fonksiyonun lineer genişlemesi $\theta : \mathbb{F}_2(C_3 \times C_3) \longrightarrow \mathbb{F}_2^9$ *vektör uzayı izomorfizması sayesinde* $\mathbb{F}_2(C_3 \times C_3)$*'ün ideallerini,* $\mathbb{F}_2^9$*'un bir altuzayı olarak görebiliriz. Yani* $\mathbb{F}_2(C_3 \times C_3)e_H$ *minimal ideali için*

$$\theta : \mathbb{F}_2(C_3 \times C_3) \longrightarrow \mathbb{F}_2^9$$

$$0 \longmapsto 000000000$$

$$e_H \longmapsto 000111111$$

$$be_H \longmapsto 111010101$$

$$b^2e_H \longmapsto 111101010$$

olup, $C = \{000000000, 000111111, 111010101, 111101010\} \subseteq \mathbb{F}_2^9$ *olur. Diyelim ki alıcıya* $x = 111010100$ *sözcüğü ulaşmış olsun. Öncelikle* C*'nin bazı kosetlerini yazalım:*

$$000000000 + C = \{000000000, 000111111, 111010101, 111101010\}$$

$$000000001 + C = \{000000001, 000111110, 111010100, 111101011\}.$$

O zaman x kod sözcüğünün bulunduğu kosetteki en küçük ağırlığa sahip olan elemanı seçelim ve e olarak adlandıralım. Bu e elemanına hata dizgesi denir ve $e = 000000001$ olur. O zaman

$$v = x - e = 111010100 - 000000001 = 111010101$$

olarak çözülür.

3.3 Uzunluğu p^2 Olan Devirli Kodlar İle Değişmeli Kodların Karşılaştırılması

Bu altbölümde uzunluğu p^2 olan devirli grup kodları ile devirli olmayan değişmeli grup kodlarının kıyaslanması üzerinde durulacaktır.

Aşağıdaki önermeyi kıyaslayacağımız kodların ortak bir cisim kullanarak yazabilmek için kullanacağız.

Önsav 3.3.1. *Eğer p tek asal sayı ve $m \leq n$ ise $U(\mathbb{Z}_{p^m}) \leq U(\mathbb{Z}_{p^n})$ sağlanır. Ayrıca q, $U(\mathbb{Z}_{p^m})$ için bir üreteç ise q elemanı $U(\mathbb{Z}_{p^n})$ için de bir üreteç olur.*

Kanıt. Eğer $m \leq n$ ise $U(\mathbb{Z}_{p^m}) \leq U(\mathbb{Z}_{p^n})$ sağlanır. Gerçekten de $m \leq n$ ise, her $a \in U(\mathbb{Z}_{p^m})$ için $(a, p^m) = 1$ olduğundan $(a, p^n) = 1$ olur. Dolayısıyla $U(\mathbb{Z}_{p^m}) \subseteq U(\mathbb{Z}_{p^n})$ sağlanır.

Şimdi de $k \geq 2$ için q'nun $U(\mathbb{Z}_{p^k})$'nın bir üreteci olduğunu kabul edip, $U(\mathbb{Z}_{p^{k+1}})$ için de bir üreteç olduğunu gösterelim. Bunu göstermek için q'nun $U(\mathbb{Z}_{p^{k+1}})$'deki derecesinin h olduğunu kabul edelim. O zaman

$$q^h \equiv 1 \pmod{p^{k+1}}$$

sağlanır. Lagrange Teoremi gereğince $h \mid |U(\mathbb{Z}_{p^{k+1}})|$ olması gerekir, yani

$$h \mid (p^{k+1} - p^k) \tag{3.3.1}$$

olur. Ayrıca $q^h \equiv 1 \pmod{p^{k+1}}$ ise, $q^h \equiv 1 \pmod{p^k}$ sağlanır. Bu durumda $U(\mathbb{Z}_{p^k})$ içindeki q'nun derecesi olan $(p^k - p^{k-1})$'in h'yi bölmesi gerekir, yani

$$(p^k - p^{k-1}) \mid h \tag{3.3.2}$$

olur. Özel olarak h, p'nin bir katıdır. O zaman (3.3.1)'den $ha = (p^{k+1} - p^k)$ olacak şekilde pozitif a tamsayısı ve (3.3.2)'den dolayı $(p^k - p^{k-1})b = h$ olacak şekilde pozitif b tamsayısı vardır. Bu durumda

$$ab(p^k - p^{k-1}) = (p^{k+1} - p^k)$$

eşitliği sağlanır. Dolayısıyla $ab = p$ olması gerekir. Böylece $a = 1$ ya da $b = 1$ sağlanır. Bu nedenle $h = p^{k+1} - p^k$ ya da $h = p^k - p^{k-1}$ olması gerekir. Diyelim ki $h = p^k - p^{k-1}$ olsun. Şimdi, $U(\mathbb{Z}_{p^k})$ için q bir üreteç olduğundan

$$q^{p^{k-1}-p^{k-2}} \not\equiv 1 \pmod{p^k}$$

olur. Ayrıca $q \in U(\mathbb{Z}_{p^{k-1}})$ olduğu ve bu grubun eksponenti $p^{k-1} - p^{k-2}$ olduğu için

$$q^{p^{k-1}-p^{k-2}} \equiv 1 \pmod{p^{k-1}}$$

sağlanır. Son iki satırdaki matematiksel ifadeler p'nin bölmediği bir u tamsayısı için $q^{p^{k-1}-p^{k-2}} = 1 + up^{k-1}$ eşitliğinin sağlanması gerektiğini söyler. Dolayısıyla,

$$\begin{aligned}(q^{p^{k-1}-p^{k-2}})^p &= (1 + up^{k-1})^p \\ &= \binom{p}{0}1^p + \binom{p}{1}up^{k-1} + \binom{p}{2}(up^{k-1})^2 + \cdots + \binom{p}{p}(up^{k-1})^p\end{aligned}$$

olur. Dikkat edilirse her $1 \leq i \leq p-1$ için $\binom{p}{i}$, p'nin bir katıdır. Çünkü,

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p(p-1)\cdots(p-i+1)}{i(i-1)\cdots 2 \cdot 1}$$

$p \nmid i(i-1)\cdots 2\cdot 1$ ve $p \mid p(p-1)\cdots(p-i+1)$ olduğundan $p \mid \binom{p}{i}$ gerekir. Eğer $i = 2$ ise $\binom{p}{2}$, p'nin bir katı olduğundan $\binom{p}{2}(up^{k-1})^2$ terimi p^{k+1}'e bölünür. Çünkü, eğer $k = 2$ ise $p \cdot p^2 = p^3$ ifadesi p^3'e bölünür, $k \geq 3$ ise $2k-2 \geq k+1$ olduğundan $\binom{p}{2}(up^{k-1})^2$ terimi p^{k+1}'e bölünür. Ayrıca $2 < i \leq p$ sağlayan her i için $ik - i \geq k+1$ olur ve böylece p^{k+1} her $\binom{p}{i}(up^{k-1})^i$ terimini böler. Sonuç olarak,

$$(q^{p^{k-1}-p^{k-2}})^p \equiv 1 + up^k \pmod{p^{k+1}}$$

sağlanır. Böylece

$$(q^{p^{k-1}-p^{k-2}})^p \equiv 1 + up^k \pmod{p^{k+1}}$$

yani $q^{p^k-p^{k-1}} \equiv 1+up^k \pmod{p^{k+1}}$ sağlanır ve u, p'nin bir katı olmadığından $q^{p^k-p^{k-1}} \not\equiv 1 \pmod{p^{k+1}}$ olur. Bu da $U(\mathbb{Z}_{p^{k+1}})$'de q'nun derecesinin $h = p^k - p^{k-1}$ olması ile çelişir. Dolayısıyla $h = p^{k+1} - p^k$ olması gerekir. Sonuç olarak q, $U(\mathbb{Z}_{p^{k+1}})$ için bir üreteç olur. □

Uzunluğu p^2 olan devirli grup kodlarında grubun eksponenti p^2 olduğu için $\mathbb{F}_q$ cismi üzerindeki koşulumuz $(q, p^2) = 1$, $< \bar{q} >= U(\mathbb{Z}_{p^2})$ olduğunu ve uzunluğu p^2 olan değişmeli grup kodlarında grubun eksponenti p olduğu için $\mathbb{F}_q$ cismi üzerindeki koşulumuzun $(q, p) = 1$ ve $< \bar{q} >= U(\mathbb{Z}_p)$ olduğunu hatırlayalım. Dikkat edilirse p asal sayı olduğundan $(q, p) = 1$ ise $(q, p^2) = 1$ olur. Dolayısıyla bu altbölümde $\mathbb{F}_q$ cismi üzerindeki koşulumuzu, $(q, p) = 1$ ve Önsav 3.3.1'den dolayı $< \bar{q} >= U(\mathbb{Z}_p)$ olarak kabul edeceğiz.

İlk önce uzunluğu p^2 olan devirli grup kodlarını inceleyelim. Eğer A_1 mertebesi p^2 olan ve a ile üretilen sonlu devirli grup ise Bölüm 3.1'den hatırlanacağı üzere $\mathbb{F}_q A_1$'in ilkel idempotentleri

$$e_0 = \widehat{A_1},\ e_1 = \widehat{a^p} - \widehat{A_1} \text{ ve } e_2 = 1 - \widehat{a^p}$$

biçimindedirler ve bu ilkel idempotentler ile $i = 0, 1, 2$ için $\mathfrak{J}_i = (\mathbb{F}_q A_1)e_i$ minimal idealleri elde edilir ve bu minimal idealler için

$$w(\mathfrak{J}_0) = p^2,\ \dim(\mathfrak{J}_0) = 1$$

$$w(\mathfrak{J}_1) = 2p,\ \dim(\mathfrak{J}_1) = p - 1$$

$$w(\mathfrak{J}_2) = 2,\ \dim(\mathfrak{J}_2) = p^2 - p$$

olduğu görülür. Daha sonra da $\mathbb{F}_q A_1$'in minimal olmayan ideallerinden aynı ağırlığa sahip olanlar içinde bize maksimum boyutu verecek olan idealleri ele alalım. Bu idealler $\mathfrak{J}_0 \oplus \mathfrak{J}_1$, $\mathfrak{J}_1 \oplus \mathfrak{J}_2$ olup, Teorem 3.1.5'ten

$$w(\mathfrak{J}_0 \oplus \mathfrak{J}_1) = p,\ \dim(\mathfrak{J}_0 \oplus \mathfrak{J}_1) = p$$

$$w(\mathfrak{J}_1 \oplus \mathfrak{J}_2) = 2,\ \dim(\mathfrak{J}_1 \oplus \mathfrak{J}_2) = p^2 - 1$$

olduğu görülür.

Şimdi de mertebesi p^2 olan değişmeli A_2 grubunu ele alalım ve $a^p = b^p = 1$ için $A_2 =< a > \times < b >$ olsun. Bu durumda Bölüm 3.2'den hatırlanacağı üzere $\mathbb{F}_q A_2$'nin ilkel idempotentleri

$$e_0 = \widehat{A_2},\ e_1 = \widehat{a} - \widehat{A_2},\ e_2 = \widehat{b} - \widehat{A_2}$$

ve

$$f_j = \widehat{ab^j} - \widehat{A_2},\ 1 \leq j \leq p - 1$$

biçiminde olurlar ve bu ilkel idempotentler ile $i = 0, 1, 2$ için $\mathfrak{L}_i = (\mathbb{F}_q A_2)e_i$ ve $1 \leq j \leq p - 1$ için $\mathfrak{M}_j = (\mathbb{F}_q A_2)f_j$ minimal idealleri elde edilir ve bu minimal idealler için

$$w((\mathbb{F}_q A_2)e_0) = p^2,\ \dim(\mathbb{F}_q A_2)e_0) = 1$$

$$w(\mathfrak{L}_i) = 2p,\ \dim(\mathfrak{L}_i) = p - 1,\ i = 1, 2$$

$$w(\mathfrak{M}_j) = 2p,\ \dim(\mathfrak{M}_j) = p-1,\ 1 \leq j \leq p-1$$

olduğu görülür. Dolayısıyla ağırlığı $2p$'ye eşit olan minimal devirli grup kodları ile devirli olmayan minimal değişmeli grup kodlarının aynı boyuta sahip olduğu görülür ve boyutları $p-1$'e eşittir. Önerme 3.2.3'tekine benzer argüman kullanıldığında $i = 1, 2$ için $\mathfrak{L}_i$ ve $1 \leq j \leq p-1$ için $\mathfrak{M}_j$ idealleri birbirine A_2-denk olduğu görülür.

Şimdi A_2 grubunun C_p'ye izomorfik olan birbirinden farklı H ve K altgruplarını ele alalım. Bu altgrupların belirlediği idempotent elemanlar olan $e = \widehat{H} - \widehat{A_2},\ f = \widehat{K} - \widehat{A_2}$ için $\mathfrak{N} = (\mathbb{F}_q A_2)e \oplus (\mathbb{F}_q A_2)f$ olarak tanımlansın. Bu durumda

$$w(\mathfrak{N}) = 2(p-1),\quad \dim(\mathfrak{N}) = 2(p-1)$$

olduğu Teorem 3.2.18'de gözlemlenmiştir. $\mathbb{F}_q A_1$'de her olası ağırlık için bize maksimum boyutu verecek minimal olmayan idealler $\mathfrak{J}_0 \oplus \mathfrak{J}_1$ ve $\mathfrak{J}_1 \oplus \mathfrak{J}_2$ olup boyutları sırasıyla p ve p^2-1'dir. $\mathbb{F}_q A_2$'de her olası ağırlık için bize maksimum boyutu verecek minimal olmayan ideallerin boyutları $2 \leq m \leq p+1$ için $mp - m$'dir ya da $1 \leq m \leq p+1$ için $1 + mp - m$'dir. Bu nedenle uzunluğu p^2 olan minimal olmayan devirli grup kodları ile devirli olmayan değişmeli grup kodlarında boyutları eşit olan sadece

$$\Delta(A_1) = \mathfrak{J}_1 \oplus \mathfrak{J}_2 = (\mathbb{F}_q A_1)(1 - \widehat{A_1})$$

$$\Delta(A_2) = \sum_{j=1}^{p-1} (\mathbb{F}_q A_2) f_j \oplus \sum_{i=1}^{p-1} (\mathbb{F}_q A_2) e_i = (\mathbb{F}_q A_2)(1 - \widehat{A_2})$$

idealleri vardır. Bu ideallerin boyutu $p^2 - 1$'ye eşittir. Ayrıca bu ideallerin minimum ağırlıkları 2'dir. Gerçekten de, birim elemandan farklı olan $a_i \in A_i$ için $(a_i - 1)(1 - \widehat{A_i}) \in \Delta(A_i)$ olur ve

$$
\begin{aligned}
(a_i-1)(1-\widehat{A_i}) &= (a_i-1)(-\frac{1}{|A_i|}\sum_{a\in A_i\setminus\{1\}} a) \\
&= (-\frac{1}{|A_i|}\sum_{a\in A_i\setminus\{1\}} aa_i) + (\frac{1}{|A_i|}\sum_{a\in A_i\setminus\{1\}} a) \\
&= (-\frac{1}{|A_i|}\sum_{c\in A_i\setminus\{a_i\}} c) + (\frac{1}{|A_i|}\sum_{a\in A_i\setminus\{1\}} a) \\
&= \frac{1}{|A_i|}(a_i-1)
\end{aligned}
$$

olur. Bu elemanın ağırlığı 2'ye eşittir.

Dikkat edilirse, $\mathbb{F}_q A_1$'de boyutu p ve minimum ağırlığı p olan $\mathfrak{J}_0 \oplus \mathfrak{J}_1$ idealine, $\mathbb{F}_q A_2$'de yaklaşık olarak aynı boyutta ve minimum ağırlığı iki katı olan $\mathfrak{L}_i$, $\mathfrak{M}_j$ ideallerine sahibiz.

Genelde hata düzeltme kapasitesi iyi olan ve olabildiğince büyük boyuta sahip kodlar ele alınmak istenir. Bu değerlerden biri arttıkça diğeri azaldığından farklı ağırlığa ve boyuta sahip kodların verimliliğini karşılaştırmak için aşağıdaki tanım yapılabilir.

Tanım 3.3.2. [1] *Herhangi bir C kodunun* ***verimliliği(convenience)***

$$\mathrm{conv}(C) = \dim(C)w(C)$$

şeklinde ifade edilir.

Birbirine yakın boyuta veya ağırlığa sahip olan kodların karşılaştırılması durumunda bu kavramın daha anlamlı hâle geldiği görülür. Bununla birlikte parametrelerden herhangi birini diğerinden oldukça büyük olarak seçersek verimliliği büyük bir kod olabilir. Ancak bu kod kullanışlı olmaz. Çünkü C kodunun boyutu arttıkça C'deki eleman sayısı da hızla artacak ve üzerinde çalışılması zorlaşacaktır.

Minimal olmayan kodlardan aynı ağırlığa sahip olanlar içinde bize maksimum boyutu verecek olan devirli grup kodları için

$$\mathrm{conv}(\mathfrak{J}_0 \oplus \mathfrak{J}_1) = p^2 \quad \text{ve} \quad \mathrm{conv}(\mathfrak{J}_1 \oplus \mathfrak{J}_2) = 2(p^2-1)$$

olur. Ayrıca iki minimal devirli olmayan değişmeli grup kodunun direkt toplamı olan $\mathfrak{N} = (\mathbb{F}_q A_2)e \oplus (\mathbb{F}_q A_2)f$ kodu için

$$\mathrm{conv}(\mathfrak{N}) = 4(p-1)^2$$

olur.

Şimdiye kadar yapılan incelemelerin sonucunda aşağıdaki teoremi elde ederiz.

Teorem 3.3.3. [1] *$p > 3$ bir asal sayı ve $\mathbb{F}_q$, $(q,p) = 1$ ve $< \bar{q} >= U(\mathbb{Z}_p)$ koşulunu sağlayacak bir cisim ise $\mathbb{F}_q$ cismi üzerinde tanımlı p^2 uzunluğundaki minimal olmayan, devirli olmayan değişmeli grup kodları, aynı uzunluktaki bütün devirli grup kodlarından daha verimlidir.*

Örnek 3.3.4. [1] *Örnek* 3.2.19*'da $G = C_5 \times C_5$ için tanımlanan ideallerin*

$$\dim(I_1) = 4, \quad \dim(I_2) = 8, \quad \dim(J_1) = 12$$

$$\dim(J_2) = 16, \quad \dim(J_3) = 20, \quad \dim(J_4) = 24$$

olur ve böylece

$$\mathrm{conv}(I_1) = 40, \quad \mathrm{conv}(I_2) = 64, \quad \mathrm{conv}(J_1) = 72$$

$$\mathrm{conv}(J_2) = 64, \quad \mathrm{conv}(J_3) = 40, \quad \mathrm{conv}(J_4) = 48$$

olarak bulunur.

Örnek 3.3.5. [1] *$G = C_{25}$ mertebesi 25 olan devirli bir grup olsun ve G_1, G grubunun mertebesi 5 olan tek altgrubu olmak üzere $\mathbb{F}_2 G$'nin ilkel idempotentleri*

$$e_0 = \widehat{G}, \quad e_1 = \widehat{G_1} - \widehat{G} \quad ve \quad e_2 = 1 - \widehat{G_1}$$

şeklinde olup,

$$I_0 = (\mathbb{F}_2G)e_0, \quad I_1 = (\mathbb{F}_2G)e_1, \quad I_2 = (\mathbb{F}_2G)e_2$$

$\mathbb{F}_2G$*'nin minimal idealleri olur. Bölüm* 3.1*'den*

$$\dim(I_0) = 1, \quad \dim(I_1) = 4, \quad \dim(I_2) = 20$$

$$w(I_0) = 25, \quad w(I_1) = 10, \quad w(I_2) = 2$$

$$\mathrm{conv}(I_0) = 25, \quad \mathrm{conv}(I_1) = 40, \quad \mathrm{conv}(I_2) = 40$$

sonuçlarına ulaşırız.

Ayrıca Önerme 3.1.3 *ve Önerme* 3.1.4 *yardımıyla minimal olmayan idealle-rimiz için*

$$\dim(I_0 \oplus I_1) = 5, \quad \dim(I_0 \oplus I_2) = 21, \quad \dim(I_1 \oplus I_2) = 24$$

$$w(I_0 \oplus I_1) = 5, \quad w(I_0 \oplus I_2) = 2, \quad w(I_1 \oplus I_2) = 2$$

$$\mathrm{conv}(I_0 \oplus I_1) = 25, \quad \mathrm{conv}(I_0 \oplus I_2) = 42, \quad \mathrm{conv}(I_1 \oplus I_2) = 48$$

sonuçlarına ulaşırız.

Dolayısıyla, devirli durumda maksimum verimlilik 48 iken, devirli olmayan durumda maksimum verimlilik 72'dir. Yani devirli olmayan değişmeli grup kodları daha verimlidir.

Bölüm 4

p^n UZUNLUKLU DEVİRLİ VE DEĞİŞMELİ KODLARIN KARŞILAŞTIRILMASI

Bu bölümde p^n uzunluklu devirli ve değişmeli grup kodlarını karşılaştıracağız.

4.1 Minimal Olmayan Bazı Değişmeli Kodların Ağırlık Hesabı

Bu altbölümde minimal olmayan, devirli olmayan bazı değişmeli grup kodların ağırlık hesabını yapacağız. Bundan sonra bu bölümde G mertebesi p^n olan değişmeli grubu, $l \geq 2$ olmak üzere $k_1 \geq k_2 \geq \cdots \geq k_l$ ve $k_1+k_2+\cdots+k_l = n$ olacak şekilde

$$C_{p^{k_1}} \times C_{p^{k_2}} \times \cdots \times C_{p^{k_l}}$$

devirli grupların direkt çarpımı olsun. Ayrıca q,

$$(q, p^{k_1}) = 1 \quad ve \quad < \bar{q} >= U(\mathbb{Z}_{p^{k_1}})$$

koşulunu sağlayan $\mathbb{F}_q$ cismini ele alalım.

Önsav 4.1.1. *G grubunun ko-devirli altgrupları içinde G'deki indeksi p olacak şekildeki birbirinden farklı H ve K altgruplarını ele alalım ve*

$$T = H \cap K$$

olarak adlandıralım. Bu durumda

(i) $H/T \cong C_p$ *ve* $K/T \cong C_p$ *olur. Ayrıca* $H/T \neq K/T$*'dır.*

(ii) $G/T \cong C_p \times C_p$ *olur.*

(iii) $|T| = p^{n-2}$*'dir.*

Kanıt. (i) H ve K birbirinden farklı altgruplar ve her ikisinin de mertebesi p^{n-1} olduğundan $T \neq H$ ve $T \neq K$ olması gerekir. Her $g \in G$ için

$$\theta : G \longrightarrow G/H \times G/K, \quad \theta(g) = (gH, gK)$$

olarak tanımlanan θ bir homomorfizmadır. Gerçekten de her $g_1, g_2 \in G$ için

$$\theta(g_1 g_2) = (g_1 g_2 H, g_1 g_2 K) = (g_1 H, g_1 K)(g_2 H, g_2 K) = \theta(g_1)\theta(g_2)$$

sağlanır. Bu tanımlanan θ homomorfizması için

$$\mathrm{Ker}(\theta) = \{\ g \in G \mid \theta(g) = (gH, gK) = (H, K)\} = T$$

olur. Ayrıca $G/H \cong C_p$, $G/K \cong C_p$ ve $H \neq K$ olduğundan dolayı $G = HK$ eşitliği sağlanır. İkinci İzomorfizma Teoremi gereği

$$H/T = H/H \cap K \cong HK/K = G/K \cong C_p$$

olur, yani $H/T \cong C_p$'tir. Benzer şekilde K altgrubu içinde yapılırsa $K/T \cong C_p$ olur ve $H \neq K$ olduğundan $H/T \neq K/T$'dir.

(ii) Her $g \in G$ için

$$\theta : G \longrightarrow G/H \times G/K, \quad \theta(g) = (gH, gK)$$

olarak tanımlanan θ bir homomorfizma olduğunu göstermiştik ve bu θ homomorfizması için $\mathrm{Ker}(\theta) = T$'dir. Bu durumda G/T, $G/H \times G/K$'nın bir altgrubuna izomorfik olur. H ve T, G grubunun normal altgrupları ve $T < H$ olduğunu biliyoruz. O zaman Üçüncü İzomorfizma Teoremi gereği

$$(G/T)/(H/T) \cong G/H$$

olur. $G/H \cong C_p$ olduğundan

$$(G/T)/(H/T) \cong C_p$$

olur ve böylece $[G/T : H/T] = p$ olması gerekir. (i) şıkkından $H/T \cong C_p$ olduğundan $|H/T| = p$ olur ve böylece $|G/T| = p^2$ olması gerekir. Bu durumda $|G/T| = p^2$ ve G/T, $G/H \times G/K$'nın bir altgrubuna izomorfik olduğundan dolayı $G/T \cong C_p \times C_p$ olur.

(iii) G mertebesi p^n olan bir grup ve (ii)'den $|G/T| = p^2$ olduğundan $|T| = p^{n-2}$ olması gerekir.

□

Önsav 4.1.2. *G grubunun $|rT| = p$ ve $|sT| = p$ olacak şekilde öyle r ve s elemanları vardır ki*

$$G/T = < rT > \times < sT >$$

olur. T altgrubunun G grubu içindeki sol kosetlerinin temsil kümesi

$$\rho = \{1, r, \cdots, r^{p-1}, s, \cdots, s^{p-1}, rs, \cdots, rs^{p-1}, \cdots, r^{p-1}s, \cdots, r^{p-1}s^{p-1}\}$$

olmak üzere

$$\mathfrak{B} = \{\eta\widehat{T} \mid \eta \in \rho\}$$

kümesi $\mathbb{F}_q$ cismi üzerinde $(\mathbb{F}_qG)\widehat{T}$ için bir bazdır.

Kanıt. Önerme 3.1.1'den doğrudur. □

Önsav 4.1.3. *Herhangi $\alpha \in (\mathbb{F}_qG)\widehat{T}$ için*

$$\alpha = \sum_{l=0}^{p-1}\sum_{m=0}^{p-1} \alpha_{lm} r^l s^m \widehat{T}$$

şeklinde ifade edilir ve bu ifadede yer alan birbirinden farklı her elemanın destek kümesi ayrıktır.

Kanıt. Her $0 \leq l_1, l_2 \leq p-1$ ve $0 \leq m_1, m_2 \leq p-1$ için $(l_1, m_1) \neq (l_2, m_2)$ sağlanıyorsa

$$l_1 \not\equiv l_2 \ (mod\ p) \quad veya \quad m_1 \not\equiv m_2 \ (mod\ p)$$

olur ve Önsav 2.2.14'ten

$$\mathrm{supp}(r^{l_1} s^{m_1} \widehat{T}) \cap \mathrm{supp}(r^{l_2} s^{m_2} \widehat{T}) = \emptyset$$

olur. □

Önsav 4.1.4. *Her $0 \leq l \leq p-1$, $0 \leq m \leq p-1$ olacak şekildeki $\alpha_{lm} r^l s^m \widehat{T} \in (\mathbb{F}_qG)\widehat{T}$ için*

$$w(\alpha_{lm} r^l s^m \widehat{T}) = \begin{cases} 0, & \alpha_{lm} = 0 \\ |T|, & \alpha_{lm} \neq 0 \end{cases}$$

olur.

Yukarıdaki önsavın doğal bir sonucu olarak aşağıdaki sonucu elde ederiz.

Sonuç 4.1.5. *Herhangi $\alpha \in (\mathbb{F}_qG)\widehat{T}$'nın ağırlığı*

$$w(\alpha) = k|T|$$

olur. Burada k sayısı $\alpha = \sum_{l=0}^{p-1}\sum_{m=0}^{p-1}\alpha_{lm}r^l s^m\widehat{T}$ toplamındaki sıfırdan farklı olan α_{lm}'lerin sayısıdır.

Kanıt. Önsav 4.1.3'te her $0 \leq l, m \leq p-1$ için $\alpha_{lm}r^l s^m\widehat{T}$ elemanlarının ayrık desteğe sahip olduğunu göstermiştik. Bundan dolayı

$$w(\alpha) = w(\sum_{l=0}^{p-1}\sum_{m=0}^{p-1}\alpha_{lm}r^l s^m\widehat{T}) = \sum_{l=0}^{p-1}\sum_{m=0}^{p-1} w(\alpha_{lm}r^l s^m\widehat{T})$$

olur ve Önsav 4.1.4'ten $w(\alpha) = k|T|$'dir. □

Önerme 4.1.6. *G değişmeli bir grup ve Önsav 4.1.1'de tanımlanan T altgrubu için her $\eta\widehat{T} \in (\mathbb{F}_q G)\widehat{T}$ olmak üzere*

$$\psi_T : (\mathbb{F}_q G)\widehat{T} \longrightarrow \mathbb{F}_q(G/T), \quad \psi_T(\eta\widehat{T}) = \eta T$$

olarak tanımlanan ψ_T dönüşümü halka izomorfizmasıdır.

Kanıt. Önerme 2.2.15'ten doğrudur. □

Önerme 4.1.7. *$\alpha \in (\mathbb{F}_q G)\widehat{T}$'yı $\alpha = \sum_{l=0}^{p-1}\sum_{m=0}^{p-1}(\alpha_{lm}r^l s^m\widehat{T})$ olarak ifade edelim. O zaman k sayısı sıfırdan farklı olan α_{lm}'lerin sayısı ise*

$$k = w(\psi_T(\alpha))$$

sağlanır.

Kanıt. $\alpha \in (\mathbb{F}_q G)\widehat{T}$ elemanının ψ_T izomorfizması altındaki görüntüsü

$$\psi_T(\alpha) = \sum_{l=0}^{p-1}\sum_{m=0}^{p-1}(\alpha_{lm}r^l s^m T)$$

olur. Ayrıca

$$w(\alpha_{lm} r^l s^m T) = \begin{cases} 0, & \alpha_{lm} = 0 \\ 1, & \alpha_{lm} \neq 0 \end{cases}$$

olduğundan

$$w(\psi_T(\alpha)) = (\text{Sıfırdan farklı olan } \alpha_{lm}\text{'lerin sayısı}).1 = k$$

eşitliği elde edilir. □

Yukarıdaki önermelerin ışığı altında şu sonucu elde ederiz.

Sonuç 4.1.8. *Her* $\alpha \in (\mathbb{F}_q G)\widehat{T}$ *için*

$$w(\alpha) = w(\psi_T(\alpha))|T|$$

olur. Dolayısıyla $\mathfrak{J}$, $(\mathbb{F}_q G)\widehat{T}$*'nin bir ideali ise* $w(\mathfrak{J}) = w(\psi_T(\mathfrak{J}))|T|$*'dir.*

Şimdiki amacımız Önsav 4.1.1'de olduğu gibi G grubundaki indeksi p olan birbirinden farklı H ve K altgruplarının belirlediği minimal ideallerin direkt toplamı olan

$$(\mathbb{F}_q G)e_H \oplus (\mathbb{F}_q G)e_K$$

idealinin minimum ağırlığını hesaplamaktır.

Önsav 4.1.9. *H ve K, G'deki indeksi p olan altgruplar olmak üzere*

(i) $(\mathbb{F}_q G)e_H \subset (\mathbb{F}_q G)\widehat{T}$

(ii) $\psi_T(e_H) = e_{H/T}$

(iii) $\psi_T((\mathbb{F}_q G)e_H \oplus (\mathbb{F}_q G)e_K) = \mathbb{F}_q(G/T)e_{H/T} \oplus \mathbb{F}_q(G/T)e_{K/T}$

sağlanır.

Kanıt. (i) H, G grubunda indeksi p olan altgrup olduğu için $H^* = G$ eşitliği sağlanır ve

$$\widehat{H} = \frac{1}{|H|}(\sum_{h\in H} h) = \frac{1}{|H/T|}(\sum_{h\in H/T} h\widehat{T})$$

$$\widehat{H^*} = \widehat{G} = \frac{1}{|G|}(\sum_{g\in G} g) = \frac{1}{|G/T|}(\sum_{g\in G/T} g\widehat{T})$$

olur. Dolayısıyla, e_H idempotent elemanı

$$\begin{aligned} e_H &= \widehat{H} - \widehat{H^*} \\ &= \widehat{H} - \widehat{G} \\ &= \frac{1}{|H/T|}(\sum_{h\in H/T} h\widehat{T}) - \frac{1}{|G/T|}(\sum_{g\in G/T} g\widehat{T}) \end{aligned}$$

şeklindedir. Teorem 2.2.21'den e_H, $\mathbb{F}_qG$'nin ilkel idempotent elemanı olduğundan $(\mathbb{F}_qG)e_H$ minimal ideal olur. Ayrıca $(\mathbb{F}_qG)e_H \subset \mathbb{F}_qG$'dir. Daha sonra iki tarafı $\widehat{T}$ ile çarparsak $(\mathbb{F}_qG)e_H\widehat{T} \subset (\mathbb{F}_qG)\widehat{T}$ elde ederiz. Önsav 2.2.19'dan $e_H\widehat{T} = e_H$ eşitliği sağlandığı için $(\mathbb{F}_qG)e_H \subset (\mathbb{F}_qG)\widehat{T}$ olur.

(ii) e_H idempotent elemanının ψ_T izomorfizması altındaki görüntüsü

$$\begin{aligned} \psi_T(e_H) &= \psi_T(\widehat{H} - \widehat{G}) \\ &= \psi_T(\widehat{H}) - \psi_T(\widehat{G}) \\ &= \psi_T(\frac{1}{|H/T|}\sum_{h\in H/T} h\widehat{T}) - \psi_T(\frac{1}{|G/T|}\sum_{g\in G/T} g\widehat{T}) \\ &= \frac{1}{|H/T|}(\sum_{h\in H/T} hT) - \frac{1}{|G/T|}(\sum_{g\in G/T} gT) \\ &= \widehat{H/T} - \widehat{G/T} \\ &= e_{H/T} \end{aligned}$$

olur.

(iii) $(\mathbb{F}_qG)e_H \oplus (\mathbb{F}_qG)e_K$ idealinin ψ_T izmorfizmasındaki görüntüsü

$$\begin{aligned}\psi_T((\mathbb{F}_qG)e_H \oplus (\mathbb{F}_qG)e_K)) &= \psi_T((\mathbb{F}_qG)(e_H + e_K)) \\ &= \mathbb{F}_q(G/T)(e_{H/T} + e_{K/T}) \\ &= \mathbb{F}_q(G/T)e_{H/T} \oplus \mathbb{F}_q(G/T)e_{K/T}\end{aligned}$$

sağlanır.

□

Teorem 4.1.10. *G mertebesi p^n olan devirli olmayan bir değişmeli grup olsun. H ve K, G'deki indeksi p olan altgruplar olmak üzere $(\mathbb{F}_qG)e_H \oplus (\mathbb{F}_qG)e_K$ idealinin minimum ağırlığı*

$$w((\mathbb{F}_qG)e_H \oplus (\mathbb{F}_qG)e_K) = 2p^{n-1} - 2p^{n-2}$$

olur.

Kanıt. Sonuç 4.1.8'de $(\mathbb{F}_qG)\widehat{T}$'nin her idealinin minimum ağırlığını nasıl hesaplanacağını göstermiştik. Daha sonra Önsav 4.1.9'un (iii) şıkkında $(\mathbb{F}_qG)e_H \oplus (\mathbb{F}_qG)e_K$ idealinin ψ_T altındaki görüntüsünün $\mathbb{F}_q(G/T)e_{H/T} \oplus \mathbb{F}_q(G/T)e_{K/T}$ olarak bulmuştuk ve Teorem 3.2.18'den dolayı bu formda olan bir idealin minimum ağırlığı $2p-2$'dir. Sonuç olarak $(\mathbb{F}_qG)e_H \oplus (\mathbb{F}_qG)e_K$ idealinin ağırlığı

$$\begin{aligned}w((\mathbb{F}_qG)e_H \oplus (\mathbb{F}_qG)e_K)) &= w(\psi_T((\mathbb{F}_qG)e_H \oplus (\mathbb{F}_qG)e_K))|T| \\ &= (2p-2)p^{n-2} \\ &= 2p^{n-1} - 2p^{n-2}\end{aligned}$$

olur. □

4.2 Karşılaştırma

Bu altbölümde uzunluğu p^n olan minimal olmayan, devirli ve devirli olmayan bazı değişmeli grup kodlarının kıyaslaması üzerinde durulacaktır.

Bu kıyaslamayı yapabilmemiz için $\mathbb{F}_q$ cismi üzerindeki koşulumuzu tanımlamamız gerekir. Uzunluğu p^n olan devirli grup kodlarında grubun eksponenti p^n olduğu için $\mathbb{F}_q$ cismi üzerindeki koşulumuz $(q, p^n) = 1$, $< \bar{q} >= U(\mathbb{Z}_{p^n})$ olduğunu ve Bölüm 4.1'deki gibi tanımlanan uzunluğu p^n olan değişmeli grup kodlarında grubun eksponenti p^{k_1} olduğu için $\mathbb{F}_q$ cismi üzerindeki koşulumuzun $(q, p^{k_1}) = 1$ ve $< \bar{q} >= U(\mathbb{Z}_{p^{k_1}})$ olduğunu hatırlayalım. Dikkat edilirse p asal sayı olduğundan $(q, p^{k_1}) = 1$ ise $(q, p^n) = 1$ olur. Dolayısıyla bu altbölümde $\mathbb{F}_q$ cismi üzerindeki koşulumuzu, $(q, p^{k_1}) = 1$ ve Önsav 3.3.1'den dolayı $< \bar{q} >= U(\mathbb{Z}_{p^{k_1}})$ olarak kabul edeceğiz.

İlk önce uzunluğu p^n olan devirli grup kodlarını inceleyelim. Eğer A_1 mertebesi p^n olan ve a ile üretilen sonlu devirli grup ise Bölüm 3.1'den hatırlanacağı üzere $\mathbb{F}_q A_1$'in ilkel idempotentleri

$$e_0 = \widehat{A_1} \text{ ve } 1 \leq i \leq n \text{ için } e_i = \widehat{a^{p^i}} - \widehat{a^{p^{i-1}}}$$

biçimindedirler ve bu ilkel idempotentler ile $1 \leq i \leq n$ için $\mathfrak{J}_i = (\mathbb{F}_q A_1)e_i$ minimal idealleri elde edilir ve Önerme 3.1.2'den

$$w(\mathfrak{J}_0) = p^n \text{ ve } w(\mathfrak{J}_i) = 2p^{n-i}$$

olur. Şimdi de $\mathbb{F}_q A_1$'in minimal olmayan ideallerini düşünelim. Bu ideallerin minimum ağırlıkları hakkında Önerme 3.1.3'ten bir $1 \leq j \leq n$ için p^{n-j} olduğu veya Önerme 3.1.4'ten bir $2 \leq k \leq n$ için $2p^{n-k}$ olduğu gözlemlenmiştir. Daha sonra Teorem 3.1.5'ten p^{n-j} minimum ağırlığında ve maksimum boyuta sahip olan idealin $\mathfrak{J}_0 \oplus \mathfrak{J}_1 \oplus \cdots \oplus \mathfrak{J}_j$ olup, boyutunun p^j'e eşit olduğu

gözlemlenir. Yine Teorem 3.1.5'ten $2p^{n-k}$ minimum ağırlığında ve maksimum boyuta sahip olan idealin $\mathfrak{J}_1 \oplus \mathfrak{J}_2 \oplus \cdots \oplus \mathfrak{J}_k$ olup, boyutunun $p^k - 1$'e eşit olduğu gözlemlenir. Yani, her $1 \leq j \leq n$ için

$$w(\mathfrak{J}_0 \oplus \cdots \oplus \mathfrak{J}_j) = p^{n-j}$$

$$\dim(\mathfrak{J}_0 \oplus \cdots \oplus \mathfrak{J}_j) = p^j$$

ve her $2 \leq k \leq n$ için

$$w(\mathfrak{J}_1 \oplus \cdots \oplus \mathfrak{J}_k) = 2p^{n-k}$$

$$\dim(\mathfrak{J}_1 \oplus \cdots \oplus \mathfrak{J}_k) = p^k - 1$$

olur.

A_2 mertebesi p^n olan değişmeli grubu $l \geq 2$ ve $k_1 + \cdots + k_l = n$ olacak şekilde $C_{p^{k_1}} \times \cdots \times C_{p^{k_l}}$ devirli grupların direkt çarpımı olsun. A_2 grubunun içinde indeksi p olan H_1 ve H_2 ko-devirli altgruplarını düşünelim ve bunların tanımladığı ilkel idempotentler

$$e_1 = \widehat{H_1} - \widehat{A_2}, \quad e_2 = \widehat{H_2} - \widehat{A_2}$$

olup, minimal ideallerimiz $(\mathbb{F}_q A_2)e_1$ ve $(\mathbb{F}_q A_2)e_2$'dir. Bu minimal ideallerimiz için Önerme 2.2.25'ten

$$w((\mathbb{F}_q A_2)e_1) = w((\mathbb{F}_q A_2)e_2) = 2p^{n-1}$$

$$\dim((\mathbb{F}_q A_2)e_1) = \dim((\mathbb{F}_q A_2)e_2) = p - 1$$

olur. Ayrıca bu iki minimal idealin direkt toplamı için Teorem 4.1.10'dan

$$w((\mathbb{F}_q A_2)e_1 \oplus (\mathbb{F}_q A_2)e_2) = 2p^{n-1} - 2p^{n-2}, \quad \dim((\mathbb{F}_q A_2)e_1 \oplus (\mathbb{F}_q A_2)e_2) = 2p-2$$

olur.

Minimal olmayan devirli grup kodlarında aynı ağırlığa sahip olanlar içinde

bize maksimum boyutu verecek olan kodlar için her $1 \leq j \leq n$ olmak üzere

$$\begin{aligned} \mathrm{conv}(\mathfrak{J}_0 \oplus \cdots \oplus \mathfrak{J}_j) &= \dim(\mathfrak{J}_0 \oplus \cdots \mathfrak{J}_j)\mathrm{w}(\mathfrak{J}_0 \oplus \cdots \mathfrak{J}_j) \\ &= p^j p^{n-j} \\ &= p^n \end{aligned}$$

ve her $2 \leq k \leq n$ olmak üzere

$$\begin{aligned} \mathrm{conv}(\mathfrak{J}_1 \oplus \cdots \oplus \mathfrak{J}_k) &= \dim(\mathfrak{J}_1 \oplus \cdots \oplus \mathfrak{J}_k)\mathrm{w}(\mathfrak{J}_1 \oplus \cdots \oplus \mathfrak{J}_k) \\ &= (p^k - 1)2p^{n-k} \\ &= 2p^n - 2p^{n-k} \end{aligned}$$

olur. Şimdi de A_2 grubunda indeksi p olan ko-devirli altgrupların belirlediği minimal değişmeli kodları düşünelim. Bu şekildeki iki minimal değişmeli grup kodunun direkt toplamı olan $\mathfrak{M}$ kodu için

$$\begin{aligned} \mathrm{conv}(\mathfrak{M}) &= \dim(\mathfrak{M})\mathrm{w}(\mathfrak{M}) \\ &= (2p-2)(2p^{n-1} - 2p^{n-2}) \\ &= 4p^{n-2}(p-1)^2 \end{aligned}$$

olur.

Şimdiye kadar yapmış olduğumuz incelemeler sonucunda aşağıdaki teoremi elde ederiz.

Teorem 4.2.1. *$p > 3$ bir asal sayı ve $\mathbb{F}_q$, $(q, p^k) = 1$ ve $< \bar{q} >= U(\mathbb{Z}_{p^k})$ koşulunu sağlayacak bir cisim ise $\mathbb{F}_q$ cismi üzerinde tanımlı p^n uzunluğuna sahip devirli grup kodlarından daha verimli olan aynı uzunluğa sahip devirli olmayan değişmeli grup kodları vardır.*

Kanıt. Yukarıda yapılan gözlemler sonucunda p^n uzunluğuna sahip devirli grup kodlarının alabileceği maksimum verimlilik değeri p^n veya her $2 \leq k \leq n$

için $2p^n - 2p^{n-k}$ olduğunu, daha sonra da Teorem 4.1.10'daki gibi tanımlanan minimal olmayan değişmeli grup kodlarının $4p^{n-2}(p-1)^2$ verimlilik değerine sahip olduğunu gözlemledik. Bu durumda $p > 3$ olduğunda minimal olmayan değişmeli grup kodunun verimliliği daha büyük olur. Sonuç olarak devirli grup kodlarından daha fazla verimliliğe sahip devirli olmayan değişmeli grup kodu bulunmuştur. □

Not 4.2.2. *$p = 2$ veya $p = 3$ olduğunda p^n uzunluğuna sahip minimal olmayan devirli grup kodları Teorem 4.1.10'daki gibi tanımlanan devirli olmayan değişmeli grup kodlarına göre daha verimlidir. Biz bu tezde bazı p^n uzunluğuna sahip devirli olmayan değişmeli grup kodlarının verimliliğini hesapladığımızdan bu durumlar için tam olarak bir kıyaslama yapamamaktayız.*

Örnek 4.2.3. *G mertebesi 125 olan değişmeli bir grup olsun. Bu durumda G grubu C_{125}, $C_{25} \times C_5$, $C_5 \times C_5 \times C_5$ gruplarından birine izomorfiktir. Eğer $G \cong C_{125}$ ve bir a elemanı tarafından üretiliyorsa $\mathbb{F}_q G$'nin ilkel idempotentleri*

$$e_0 = \widehat{C_{125}}, \quad e_1 = \widehat{a^5} - \widehat{C_{125}}$$

$$e_2 = \widehat{a^{25}} - \widehat{a^5}, \quad e_3 = 1 - \widehat{a^{25}}$$

olup bu ilkel idempotentler ile $(\mathbb{F}qG)e_0$, $(\mathbb{F}qG)e_1$, $(\mathbb{F}qG)e_2$, $(\mathbb{F}qG)e_3$ minimal idealleri elde edilir. Daha sonra $\mathbb{F}_q G$'nin minimal olmayan ideallerini düşünelim ve aynı ağırlığa sahip olanlar içinde bize maksimum boyutu verecek olan idealleri ele alalım. Bu idealler $(\mathbb{F}qG)e_0 \oplus (\mathbb{F}qG)e_1 \oplus (\mathbb{F}qG)e_2$ ve $(\mathbb{F}qG)e_1 \oplus (\mathbb{F}qG)e_2 \oplus (\mathbb{F}qG)e_3$ olup, Teorem 3.1.5'ten

$$w((\mathbb{F}qG)e_0 \oplus (\mathbb{F}qG)e_1 \oplus (\mathbb{F}qG)e_2) = 5$$

$$\dim((\mathbb{F}qG)e_0 \oplus (\mathbb{F}qG)e_1 \oplus (\mathbb{F}qG)e_2) = 25$$

$$w((\mathbb{F}qG)e_1 \oplus (\mathbb{F}qG)e_2 \oplus (\mathbb{F}qG)e_3) = 2$$

$$\dim((\mathbb{F}qG)e_1 \oplus (\mathbb{F}qG)e_2 \oplus (\mathbb{F}qG)e_3) = 124$$

olarak hesaplanır. Dolayısıyla

$$\mathrm{conv}((\mathbb{F}qG)e_0 \oplus (\mathbb{F}qG)e_1 \oplus (\mathbb{F}qG)e_2) = 125$$

$$\mathrm{conv}((\mathbb{F}qG)e_1 \oplus (\mathbb{F}qG)e_2 \oplus (\mathbb{F}qG)e_3) = 248$$

olarak hesaplanır.

Şimdi de $G \cong C_{25} \times C_5$ olsun. G'de indeksi p olan H_1 ve H_2 ko-devirli altgruplarını ele alalım ve ilkel idempotentlerimiz

$$e_1 = \widehat{H_1} - \widehat{G}, \quad e_2 = \widehat{H_2} - \widehat{G}$$

olup, $(\mathbb{F}_qG)e_1$ ve $(\mathbb{F}_qG)e_2$ minimal ideallerdir. Önerme 2.2.25*'ten*

$$w((\mathbb{F}_qG)e_1) = w((\mathbb{F}_qG)e_2) = 50$$

$$\dim((\mathbb{F}_qG)e_1) = \dim((\mathbb{F}_qG)e_2) = 4$$

olur. Ayrıca bu iki minimal idealin direkt toplamını düşündüğümüzde Teorem 4.1.10*'dan*

$$w((\mathbb{F}_qG)e_1 \oplus (\mathbb{F}_qG)e_2) = 40$$

$$\dim((\mathbb{F}_qG)e_1 \oplus (\mathbb{F}_qG)e_2) = 8$$

olarak hesaplanır. Dolayısıyla

$$\mathrm{conv}((\mathbb{F}_qG)e_1 \oplus (\mathbb{F}_qG)e_2) = 320$$

olur.

Son olarak $G \cong C_5 \times C_5 \times C_5$ olsun. G'de indeksi p olan K_1 ve K_2 ko-devirli altgruplarını ele alalım ve ilkel idempotentlerimiz

$$f_1 = \widehat{K_1} - \widehat{G}, \quad f_2 = \widehat{K_2} - \widehat{G}$$

olup, $(\mathbb{F}_q G)f_1$ *ve* $(\mathbb{F}_q G)f_2$ *minimal ideallerdir. Önerme* 2.2.25*'ten*

$$w((\mathbb{F}_q G)f_1) = w((\mathbb{F}_q G)f_2) = 50$$

$$\dim((\mathbb{F}_q G)f_1) = \dim((\mathbb{F}_q G)f_2) = 4$$

olur. Ayrıca bu iki minimal idealin direkt toplamını düşündüğümüzde Teorem 4.1.10*'dan*

$$w((\mathbb{F}_q G)f_1 \oplus (\mathbb{F}_q G)f_2) = 40$$

$$\dim((\mathbb{F}_q G)f_1 \oplus (\mathbb{F}_q G)f_2) = 8$$

olarak hesaplanır. Dolayısıyla

$$\mathrm{conv}((\mathbb{F}_q G)f_1 \oplus (\mathbb{F}_q G)f_2) = 320$$

olur. Yani devirli olmayan değişmeli grup kodları daha verimlidir.

Kaynakça

[1] C. P. Milies ve F. D. Melo, *On Cyclic and Abelian Codes,* IEEE Transactions on Information Theory, vol.59, no.11, November 2013.

[2] S. D. Berman, *Semisimple cyclic and abelian code II,* Kibernetika, vol.3, pp. 17-23, 1967.

[3] R. A. Ferraz ve C. P. Milies, *Idempotents in group algebras and minimal abelian codes,* Finite Fields Appl., vol.13, pp.382-393, 2007.

[4] M. Guerreiro, *Group Algebras and Coding Theory,* São Paulo J. Math. Sci., September 7, 2015.

[5] C. P. Milies ve S. K. Sehgal, *An Introduction to Group Rings,* Dordrecht, The Netherlands:Kluwer, 2002.

[6] G. Chalom, R. A. Ferraz, M. Guerreiro, *Minimal ideals in finite abelian group algebras and coding theory*, São Paulo J. Math. Sci., 1 February, 2016.

[7] F. Dutra, R. A. Ferraz ve C. P. Milies, *Semisimple group codes and dihedral codes,* Algebra and Discrete Mathematics, vol.3, pp.28-48, 2009.

[8] J. J. Rotman, *An Introduction to the Theory of Group*, fourth ed., Grad. Texts in Math. , vol. 148, SpringerVerlag, New York, 1995.

[9] S. Ling, C. Xing *Coding Theory: A First Course,* First Edition, Cambridge University Press, New York, 2004.

[10] F. J. MacWilliams, *Codes and ideals in group algebras,* Combinatorial Mathematics and Its Applications, 317-328, 1969.

[11] F. J. MacWilliams, *Binary codes which are ideals in the group algebra of an abelian group,* Bell Syst. Tech. J., vol.49, pp.987-1011, 1970.

[12] S. D. Berman, *On the theory of group codes,* Kibernetika, vol.3, pp. 31-39, 1967.

[13] GAP, *Groups, Algorithms, and Programming The GAP Group*, 2012, Version 4.5.4 [Online].