T.C.

TRAKYA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

CEBİRSEL GEOMETRİK KODLAR VE BU KODLARIN OTOMORFİZMA GRUPLARI HAKKINDA

ENGİN ŞENEL

DOKTORA TEZİ

MATEMATİK ANABİLİM DALI

Tez Danışmanı: Prof. Dr. FİGEN ÖKE

EDİRNE-2022

Engin ŞENEL'in hazırladığı "**CEBİRSEL GEOMETRİK KODLAR VE BU KODLARIN OTOMORFİZMA GRUPLARI HAKKINDA**" başlıklı bu tez, tarafımızca okunmuş, kapsam ve niteliği açısından **Matematik** Anabilim Dalında bir **Doktora tezi** olarak kabul edilmiştir.

Jüri Üyeleri (Ünvan, Ad, Soyad): İmza

Prof. Dr. Figen ÖKE

Prof. Dr. Yasemin ÇENGELLENMİŞ

Prof. Dr. İlhan ERDOĞAN

Prof. Dr. Fırat ATEŞ

Prof. Dr. Sebahattin İKİKARDEŞ

Tez Savunma Tarihi: 06/12/2022

Bu tezin Doktora tezi olarak gerekli şartları sağladığını onaylarım.

İmza

Prof. Dr. Figen ÖKE
Tez Danışmanı

Trakya Üniversitesi Fen Bilimleri Enstitüsü onayı

Prof. Dr. Hüseyin Rıza Ferhat KARABULUT
Fen Bilimleri Enstitüsü Müdürü

T.Ü.FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI DOKTORA PROGRAMI
DOĞRULUK BEYANI

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

06/12/2022
Engin ŞENEL

Doktora Tezi
Cebirsel Geometrik Kodlar ve Bu Kodların Otomorfizma Grupları Hakkında
T.Ü. Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

ÖZET

Bu çalışma beş bölümden oluşmaktadır. İlk bölümde cebirsel geometrik (CG) kodlar, genelleştirilmiş cebirsel geometrik (GCG) kodlar ve bu kodların otomorfizma gruplarının literatürdeki öneminden bahsedildikten sonra bu tez boyunca uygulanacak yöntemler hakkında bilgi verilmiştir. İkinci bölümde, CG kodların ve GCG kodların matematiksel alt yapısını oluşturan fonksiyon cismi teorisi ve kodlama teorisinin temel tanım ve kavramları verildikten sonra bu kodlar sunulmuştur. Ardından fonksiyon cismi genişlemeleri ile ilgili tez boyunca ihtiyaç duyulacak temel tanım ve kavramlar verilmiştir.

Üçüncü bölümde, her bir koleksiyondaki noktaların derecesi aynı olmak üzere noktaların iki koleksiyonu tarafından oluşturulan GCG kodlar göz önüne alınıp, bu çalışmaya ait olan özgün sonuçlar sunulmaya başlanmıştır. Bu sınıftaki bir GCG kodun otomorfizma grubunun bir alt grubu olan N_1N_2-otomorfizma grubu kavramı tanımlanmıştır. Daha sonra, keyfi fonksiyon cismi durumunda N_1N_2-otomorfizma grubunun bir alt grubu ve rasyonel, hipereliptik ve Hermityan fonksiyon cismi durumlarında N_1N_2-otomorfizma grubunun kendisi belirlenmiştir. Rasyonel fonksiyon cismi durumunda N_1N_2-otomorfizma grubu uygulama anlamında yapısal olarak inşa edilmiştir. Bu bölümdeki sonuçların elde edilmesi için kullanılan yöntemler, yapısında aynı dereceden noktaların daha fazla koleksiyonunu içeren bir GCG kodun otomorfizma grubunun bir alt grubunun belirlenmesi için bir method sunmaktadır.

Dördüncü bölümde, belli şartlar altında bir GCG kodun izomorfizmalar gözetilmeksizin bir CG kod tarafından kapsandığı gösterilmiştir. Ardından üçüncü bölümde olduğu gibi aynı dereceden noktaların iki koleksiyonu tarafından oluşturulan GCG kodların bir sınıfı göz önüne alınıp, böyle bir kodun N_1N_2-otomorfizma grubunun,

ilgili CG kodun otomorfizma grubunun bir alt grubu olduğu gösterilmiştir. Böylece, bir CG kodun otomorfizma grubunun bir alt grubunu bulmak için bir yöntem sunulmuştur.

Son bölümde, bu çalışmada kullanılan yöntemler ve bulunan sonuçlar değerlendirilmiştir. Ayrıca devam çalışmaları konusunda çıkarımlarda bulunulmuştur.

Yıl : 2022
Sayfa Sayısı : 75
Anahtar Kelimeler : Cebirsel fonksiyon cisimleri, Fonksiyon cisimlerinin otomorfizma grupları, Kod otomorfizmaları, Genelleştirilmiş cebirsel geometrik kodlar, Cebirsel geometrik kodlar, Geometrik Goppa kodları

PhD Thesis

On Algebraic Geometry Codes and Their Automorphism Groups

Trakya University Institute of Natural Sciences

Department of Mathematics

ABSTRACT

This study consists of five chapters. In the first chapter, after mentioning the importance of algebraic geometry (AG) codes, generalized algebraic geometry (GAG) codes and automorphism groups of these codes in the literature, information is given about the methods to be applied throughout this thesis. In the second chapter, after giving the basic definitions and concepts of function field theory and coding theory, which constitute the mathematical substructure of AG codes and GAG codes, these codes are presented. Finally, in this chapter, basic definitions and concepts that will be needed throughout the thesis on function field extensions are given.

In the third chapter, with places of the same degree in each collection, the GAG codes constructed by two collections of places are considered and the original results of this study have begun to be presented. The concept of N_1N_2-automorphism group, which is a subgroup of the automorphism group of a GAG code in this class, is defined. Then, a subgroup of the N_1N_2-automorphism group in the case of an arbitrary function field and the N_1N_2-automorphism group itself in rational, hyperelliptic and Hermitian function field cases are determined. In the case of the rational function field, the N_1N_2-automorphism group is structurally constructed for application purposes. The techniques used to obtain the results in this chapter provide a method for determining a subgroup of the automorphism group of a GAG code that contains more collections of places of the same degree in its structure.

In the fourth chapter, it has been shown that under certain conditions a GAG code is contained (up to isomorphism) in an AG code. Then, as in the third chapter, GAG codes formed by two collections of places of the same degree is considered and it is shown that the N_1N_2-automorphism group of such a code is a subgroup of the

automorphism group of the corresponding AG code. Thus, a method is presented to find a subgroup of the automorphism group of an AG code.

In the last chapter, the methods used and the results obtained are evaluated. In addition, inferences are made for continuation studies.

Year : 2022
Number of Pages : 75
Keywords : Algebraic function fields, Automorphism groups of function fields, Code automorphisms, Generalized algebraic geometry codes, Algebraic geometry codes, Geometric Goppa codes

ÖNSÖZ

Edirne’de yaşamaya başladığım 2015 yılından bu yana bilgi ve tecrübeleriyle bana her türlü desteği sağlayan, öğrencisi olmaktan dolayı kendimi hep şanslı hissettiğim saygı değer hocam Prof. Dr. Figen Öke'ye (Trakya Üniversitesi, Fen Fakültesi, Matematik Bölümü, Cebir ve Sayılar Teorisi Anabilim Dalı) en içten teşekkürlerimi ve sevgilerimi sunarım.

Engin ŞENEL

İÇİNDEKİLER

ÖZET ..... **iv**
ABSTRACT ..... **vi**
ÖNSÖZ ..... **viii**
İÇİNDEKİLER ..... **ix**
SİMGELER VE KISALTMALAR DİZİNİ ..... **x**
BÖLÜM 1 - GİRİŞ **1**
BÖLÜM 2 - GENEL BİLGİLER **4**
2.1. Cebirsel Fonksiyon Cisimleri 4
2.2. Kodlar 9
2.3. Fonksiyon Cisimlerinin Cebirsel Genişlemeleri 17
BÖLÜM 3 - GCG KODLARIN OTOMORFİZMA GRUPLARI **21**
3.1. Keyfi Fonksiyon Cismi Durumu 21
3.2. Rasyonel Fonksiyon Cismi Durumu 34
3.3. Hipereliptik Fonksiyon Cismi Durumu 40
3.4. Hermityan Fonksiyon Cismi Durumu 49
BÖLÜM 4 - CG KODLAR VE GCG KODLAR **54**
4.1. CG Kodlar ve GCG Kodlar Arasındaki Bir İlişki 54
4.2. CG Kodlar ve GCG Kodların Otomorfizma Grupları Arasındaki Bir İlişki 57
BÖLÜM 5 - SONUÇLAR VE TARTIŞMA **60**
KAYNAKLAR **62**
ÖZGEÇMİŞ **64**
İLGİLİ TEZ KONUSUNA AİT BİLİMSEL FAALİYETLER **65**

SİMGELER VE KISALTMALAR DİZİNİ

Simgeler

$\mathrm{Aut}(C(\Phi;\mathrm{G}))$	: $C(\Phi;\mathrm{G})$ kodunun otomorfizma grubu
$\mathrm{Aut}(C(\Phi;\mathrm{G};\mathrm{n}))$	: $C(\Phi;\mathrm{G};\mathrm{n})$ kodunun otomorfizma grubu
$\mathrm{Aut}(C_{\mathcal{L}}(D,G))$	: $C_{\mathcal{L}}(D,G)$ kodunun otomorfizma grubu
$\mathrm{Aut}(F/K)$	: $F\ /\ K$ fonksiyon cisminin otomorfizma grubu
$C(\Phi;\mathrm{G})$	: Bir ϕ-divizörü Φ tarafından üretilen bir GCG kod
$C(\Phi;\mathrm{G};\mathrm{n})$	: Derecesi n olan noktalar tarafından üretilen bir GCG kod
$\mathrm{Con}_{F'/F}(P)$	: Bir P noktasının conorm'u
$\mathcal{H}(\Phi;\mathrm{G};\mathrm{n})$	: $C(\Phi;\mathrm{G};\mathrm{n})$ kodunun n-otomorfizma grubu
$\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$	: $C(\Phi;\mathrm{G})$ kodunun N_1N_2-otomorfizma grubu
$[n,k,d]$	: Uzunluğu n, boyutu k ve minimum uzaklığı n olan bir lineer kod
(P,ϕ_P)	: P noktası ile ilişkili bir ϕ-nokta
$\mathcal{S}_N$	: N-inci simetrik grup

Kısaltmalar

AG	: Algebraic geometry
CG	: Cebirsel geometrik
GAG	: Generalized algebraic geometry
GCG	: Genelleştirilmiş cebirsel geometrik

BÖLÜM 1

GİRİŞ

CG kodlar, 1981 yılında Goppa tarafından bulunmuştur (Goppa, 1981) ve asimptotik Gilbert-Varshamov sınırını aşmalarıyla bilinmektedirler. Bir CG kod oluşturulurken, bir fonksiyon cisminin derecesi bir olan noktaları kullanılmaktadır. Bu durum iyi CG kodların inşası için önemli bir kısıtlama meydana getirdiğinden, Xing, Niederreiter ve Lam tarafından daha genel bir kod yapısı oluşturulmuştur (Xing, Niederreiter & Lam, 1999b). Bu yeni kodlar, GCG kod olarak isimlendirilmektedir. Bu kodların yapısında yüksek dereceden noktaların kullanımı mümkün olduğundan, optimum kodların çoğu bu genelleme ile elde edilebilmektedir (Ding, Niederreiter & Xing, 2000; Jibril, Tomlinson, Ahmed & Tjhai, 2010).

Büyük otomorfizma gruplarına sahip kodlar ilgi çekicidir ve genel olarak kodlama teorisinde bir kodun otomorfizma grubunu bulmak önemli ve zor bir problemdir. Buna ek olarak, bu kodların yapısı hakkında bilgi sağladıklarından ve dekodlama algoritmaları için kullanıldıklarından dolayı, kodların otomorfizma grupları ve bu grupların alt grupları önemlidir (Hansen, 1987; Matsumoto & Oishi, 2001; Spera, 2005). Goppa, CG kodların otomorfizmalarının ilgili fonksiyon cisminin otomorfizmalarından elde edilebileceğini ortaya çıkarmıştır (Goppa, 1981). Goppa'nın makalesindeki bu sonuç tam olarak doğru değildi. Stichtenoth ilgili fonksiyon cisminin rasyonel olduğu durumda, bir CG kodun tüm otomorfizmalarının fonksiyon cisminin otomorfizmalarından elde edildiğini göstermiştir (Stichtenoth, 1990). Daha sonra, ilgili fonksiyon cisminin eliptik, hipereliptik, Hermityan ve diğer tipten olduğu durumlarda, bu iki grup arasındaki ilişkiyle ilgili birçok çalışma yapılmıştır (Joyner & Ksir, 2006; Wesemeyer, 1998; Xing, 1995a; Xing, 1995b). Bu çalışmaların temel hedefi, CG kodların otomorfizma grubunu belirlemekti.

CG kodların otomorfizma gruplarıyla ilgili bulunan bu sonuçlar esas alınarak, GCG kodların otomorfizma gruplarıyla ilgili benzer çıkarımlar yapılmıştır. Ancak, GCG kodların yapısında yüksek dereceden noktalar kullanılabildiğinden, CG kodlar için kullanılan metodlar bir GCG kodun otomorfizma grubunun tamamının belirlenmesinde kullanılamamıştır. Bir GCG kodun yapısında farklı dereceden noktaların kullanılabiliyor olması da önemli engellerden biri olmuştur. Bu nedenle, çalışmalar GCG kodların otomorfizma grubunun bir alt grubunu belirleme üzerine yoğunlaşmıştır. Bir GCG kodun otomorfizma grubunun bir alt grubu ve ilgili fonksiyon cisminin otomorfizma grubunun spesifik bir alt grubu arasındaki bir ilişki Spera tarafından verilmiştir (Spera, 2007). Bu çalışma, Stichtenoth'un sonucunun (Stichtenoth, 1990, Proposition 2.3) bir anlamda GCG kodlara bir genellemesi olarak düşünülebilir. Rasyonel, hipereliptik ve Hermityan fonksiyon cismi durumlarında, bir GCG kodun n-otomorfizma grubu kavramını tanımlayarak ve Wesemeyer'in metodunu (Wesemeyer, 1998) kullanarak, Picone ve Spera bir GCG kodun otomorfizma grubu ve ilgili fonksiyon cisminin otomorfizma grubunun aynı spesifik alt grubu arasında daha genel bir ilişki kurmuşlardır (Picone, 2016; Picone & Spera, 2009). (Picone, 2016; Picone & Spera, 2009; Spera, 2007) çalışmalarında aynı dereceden $n > 1$ noktalar tarafından üretilen GCG kodlar göz önüne alınmıştır. Bu çalışmada, her bir koleksiyondaki noktaların derecesi aynı olmak üzere noktaların iki koleksiyonu tarafından üretilen GCG kodlar göz önüne alınmış ve böyle bir GCG kod için N_1N_2-otomorfizma grubu kavramı tanımlanmıştır. GCG kodların daha büyük bir sınıfı için tanımlandığından N_1N_2-otomorfizma grubu, n-otomorfizma grubunun bir genellemesi olarak düşünülebilir. Daha sonra, ilgili fonksiyon cisminin otomorfizma grubunun $\mathrm{Aut}(F / \mathbb{F}_q)$ belli bir alt grubunun, belli şartlar altında N_1N_2-otomorfizma grubuna gömülebildiği gösterilmiştir. İlgili fonksiyon cisminin $F / \mathbb{F}_q$ rasyonel, hipereliptik ve Hermityan olduğu durumlarda fonksiyon cisminin otomorfizma grubunun aynı belli alt grubunun, N_1N_2-otomorfizma grubuna izomorf olabildiği gösterilmiştir. Böylelikle fonksiyon cisminin genel, rasyonel, hipereliptik ve Hermityan olduğu durumlarda, noktaların iki koleksiyonu tarafından üretilen bir GCG kodun otomorfizma grubunun bir alt grubu belirlenmiştir. Sonuç olarak (Picone, 2016; Picone & Spera, 2009; Spera, 2007) çalışmaları, GCG kodların daha büyük bir sınıfına genellenmiştir.

CG kodlar ve GCG kodlar arasındaki yapısal bir ilişki Picone tarafından verilmiştir (Picone, 2013, Section 3). Daha açık olarak, aynı dereceden $n > 1$ noktalar tarafından üretilen bir GCG kodun izomorfizmalar gözetilmeksizin uygun bir CG kod tarafından kapsandığı gösterilmiştir. Daha sonra, yine Picone tarafından bu şekildeki bir GCG kod için tanımlanan n-otomorfizma grubunun, ilgili CG kodun otomorfizma grubunun bir alt grubu olduğu gösterilmiştir (Picone, 2013, Section 3). Bu çalışmada öncelikle, noktaların derecesi üzerinde bir şart olmaksızın bir GCG kodun uygun bir CG kod tarafından kapsandığı gösterilmiştir. Daha sonra bu sonuçtan yararlanılarak, aynı dereceden noktaların iki koleksiyonu tarafından oluşturulan bir GCG kod için tanımlanan N_1N_2-otomorfizma grubunun, ilgili CG kodun otomorfizma grubunun bir alt grubu olduğu gösterilmiştir. Sonuç olarak (Picone, 2013, Section 3) çalışması GCG kodların daha büyük bir sınıfına ve GCG kodların otomorfizma gruplarının daha büyük alt gruplarına genellenmiştir.

İkinci bölümde, bu tezin yazımında kullanılacak olan temel tanım ve kavramlar verilmiştir. Üçüncü bölümde, bu çalışmada göz önüne alınacak olan GCG kodların sınıfı ve bu GCG kodların bu sınıfı için tanımlanan N_1N_2-otomorfizma grubu kavramı sunulmuştur. N_1N_2-otomorfizma grubu kavramı kullanılarak ve (Spera, 2007) çalışması bu tezde göz önüne alınan GCG kodların sınıfına genellenerek, bu tezin ana sonuçları elde edilmiştir. Daha sonra elde edilen bu sonuçlar, (Wesemeyer, 1998)'in yöntemi N_1N_2-otomorfizma grubuna uygulanarak rasyonel, hipereliptik ve Hermityan fonksiyon cismi durumlarına genişletilmiştir. Daha açık olarak, N_1N_2-otomorfizma grubunun her elemanının, sırasıyla rasyonel, hipereliptik ve Hermityan fonksiyon cisminin bir otomorfizması tarafından elde edildiği gösterilmiştir. Böylelikle N_1N_2-otomorfizma grubu belirlenmiştir. Ayrıca rasyonel fonksiyon cismi durumunda N_1N_2-otomorfizma grubu açık olarak inşa edilmiştir. Dördüncü bölümde, temel olarak fonksiyon cismi teorisi kullanılarak CG kodlar ve GCG kodlar arasındaki bir ilişki verilmiştir. Daha sonra bu ilişki kullanılarak, N_1N_2-otomorfizma grubunun ilgili CG kodun otomorfizma grubunun bir alt grubu olduğu gösterilmiştir. Son olarak beşinci bölümde, bulunan sonuçlar değerlendirilmiş ve gelecek çalışmaların neler olabileceği hakkında çıkarımlar yapılmıştır.

BÖLÜM 2

GENEL BİLGİLER

Bu bölümde öncelikle fonksiyon cismi teorisinin temel tanım ve kavramları verilecektir. Ardından kodlama teorisiyle ilgili genel tanım ve kavramlar verilecektir. Kodlama teorisiyle ilgili daha detaylı bilgi için (MacWilliams & Sloane, 1997)'a başvurulabilir. Cebirsel geometrik kodlar ve genelleştirilmiş cebirsel geometrik kodlar tanıtılacaktır. Genelleştirilmiş cebirsel geometrik kodların bu tez için önemli olan bir alt sınıfı ve bu alt sınıftaki kodların otomorfizma grubunun spesifik bir alt grubu sunulacaktır. Bu bölümde son olarak fonksiyon cisimlerinin cebirsel genişlemeleri ile ilgili temel tanım ve kavramlar verilecektir. Standart notasyonlar için (Stichtenoth, 2009; Şenel, 2017) kullanılacaktır.

Tüm bölüm boyunca aksi belirtilmedikçe, K keyfi bir cismi gösterecektir.

2.1. Cebirsel Fonksiyon Cisimleri

2.1.1. Tanım: K üzerinde transandant olan bir $x \in F$ için F, $K(x)$'in sonlu bir genişlemesi olmak üzere $K \subseteq F$ cisim genişlemesine K üzerinde tek değişkenli bir cebirsel fonksiyon cismi $F \,/\, K$ denir.

Sadelik açısından, $F \,/\, K$ fonksiyon cismi olarak isimlendirilecektir.

F cisminin K üzerindeki cebirsel elemanlarının kümesi $\widetilde{K}$, ilgili fonksiyon cisminin sabitlerinin cismi olarak isimlendirilir. $\widetilde{K} = K$ ise K, F'in tam sabit cismidir denir. Bu tez boyunca $F \,/\, K$, tam sabit cismi K olan bir fonksiyon cismini gösterecektir. (Stichtenoth, 2009, s. 15) gereğince bu varsayım genelliği kısıtlamaz.

2.1.2. Örnek: K bir cisim ve x, K üzerinde transandant olsun.

$$K(x) \coloneqq \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], g(x) \neq 0 \right\} \quad (2.1)$$

K'nın bir transandant genişlemesidir. Her cisim kendisinin bir sonlu genişlemesi olduğundan, $K(x) \,/\, K$ bir fonksiyon cismidir. Bu fonksiyon cismi, rasyonel fonksiyon cismi olarak isimlendirilir ve fonksiyon cisminin en basit örneklerindendir.

Herhangi bir fonksiyon cismi genellikle, indirgenemez bir polinom $\varphi(T) \in K(x)[T]$ için $\varphi(y) = 0$ olmak üzere, $K(x)$ rasyonel fonksiyon cisminin bir basit cebirsel cisim genişlemesi $F = K(x, y)$ olarak gösterilir. x ve y elemanları, F fonksiyon cisminin K cismi üzerinde üreteçleri olarak isimlendirilir.

2.1.3. Tanım: $F \,/\, K$ bir fonksiyon cismi olsun. Her $z \in F$ için $z \in \mathcal{O}$ veya $z^{-1} \in \mathcal{O}$ koşulunu sağlayan bir $K \subsetneq \mathcal{O} \subsetneq F$ halkasına, değerlendirme halkası denir.

Her değerlendirme halkasının teklikle belirli bir maksimal ideali vardır (Stichtenoth, 2009).

2.1.4. Tanım: $F \,/\, K$ fonksiyon cisminin bir değerlendirme halkası $\mathcal{O}$ göz önüne alınsın. $\mathcal{O}$ değerlendirme halkasının teklikle belirli maksimal idealine P, $F \,/\, K$ fonksiyon cisminin bir noktası (place) denir. $F \,/\, K$ fonksiyon cisminin bütün noktalarının kümesi $\mathcal{P}_F$ ile gösterilecektir.

2.1.5. Tanım: $F \,/\, K$ bir fonksiyon cismi olsun. Aşağıda verilen özellikleri sağlayan bir örten dönüşüme $v\colon F \longrightarrow \mathbb{Z} \cup \{\infty\}$ değerlendirme denir.

(1) $v(x) = \infty \Leftrightarrow x = 0$,

(2) Her $x, y \in F$ için $v(xy) = v(x) + v(y)$,

(3) Her $x, y \in F$ için $v(x + y) \geq \min\{v(x), v(y)\}$,

(4) Her $x \in K, x \neq 0$ için $v(x) = 0$.

Bir fonksiyon cisminin değerlendirme halkaları, noktaları ve değerlendirmeleri arasında birebir bir ilişki bulunmaktadır. Birbirine karşılık gelen değerlendirme halkası, nokta ve değerlendirmeyi göstermek için sırasıyla $\mathcal{O}_P$, P ve v_P notasyonu kullanılacaktır.

2.1.6. Tanım: P, F / K fonksiyon cisminin bir noktası olsun. $F_P \coloneqq \mathcal{O}_P / P$ cismine P'nin rezidü cismi denir. F_P cisminin bir elemanı sırasıyla $x \in \mathcal{O}_P$ için $x(P)$ ve $x \in F \setminus \mathcal{O}_P$ için $\varphi(x) = \infty$ şeklinde tanımlanır.

F / K fonksiyon cisminin bir noktası P göz önüne alınsın. İzomorfizmalar gözetilmeksizin, $K \subseteq F_P$ dir. Ayrıca bu sonlu bir cisim genişlemesidir. Bu nedenle sıradaki tanım anlamlıdır.

2.1.7. Tanım: Herhangi bir $P \in \mathcal{P}_F$ noktası göz önüne alınsın. $K \subseteq F_P$ cisim genişlemesinin derecesine, P noktasının derecesi denir ve $\deg P$ ile gösterilir. Derecesi bir olan bir noktaya, rasyonel nokta denir.

2.1.8. Tanım: P, F / K fonksiyon cisminin bir noktası olsun. Herhangi bir $z \in F$ elemanı için $v_p(z) > 0$ (sırasıyla $v_p(z) < 0$) ise P noktasına z'nin bir kökü (sırasıyla kutbu) denir. Ayrıca $v_p(z) \geq 0$ ise, $z \in F$ elemanına P noktasında regülerdir denir.

Bir fonksiyon cisminin sonsuz sayıda noktası vardır. Bu nedenle sıradaki tanımı yapmak mümkündür.

2.1.9. Tanım: F / K fonksiyon cisminin noktaları tarafından üretilen serbest abelian gruba, F / K'nın divizör grubu denir ve $\mathrm{Div}(F)$ ile gösterilir. Bu grubun bir elemanına F / K'nın bir divizörü denir. Diğer bir ifadeyle bir divizör, $n_P \in \mathbb{Z}$ ve sonlu sayıdaki hariç her bir $n_P = 0$ olmak üzere

$$D = \sum_{P \in \mathcal{P}_F} n_P P \tag{2.2}$$

şeklindedir. $\{ P \in \mathcal{P}_F \mid n_P \neq 0 \}$ kümesine D divizörünün support'u denir ve $\mathrm{supp}\, D$ ile gösterilir.

Değerlendirmeler, divizörler üzerinde sıradaki gibi tanımlanacaktır: Herhangi bir $Q \in \mathcal{P}_F$ noktası ve $A = \sum_{P \in \mathcal{P}_F} n_P P$ divizörü için $v_Q(A) \coloneqq n_Q$ yazılacaktır. Bu

tanımlama yardımıyla $\mathrm{Div}(F)$ üzerinde bir kısmi sıralama tanımlanabilir. $A, B \in \mathrm{Div}(F)$ olmak üzere, her $P \in \mathcal{P}_F$ noktası için $v_P(A) \leq v_P(B)$ ise $A \leq B$ yazılacaktır. 0, $\mathrm{Div}(F)$ grubunun birim elemanını göstermek üzere bir $D \in \mathrm{Div}(F)$ divizörü için $0 \leq D$ ise D divizörüne pozitif denilecektir.

2.1.10. Tanım: Bir $D = \sum_{P \in \mathcal{P}_F} v_P(D)P \in \mathrm{Div}(F)$ divizörünün derecesi,

$$\deg D = \sum_{P \in \mathcal{P}_F} v_P(D) \deg P \tag{2.3}$$

şeklinde tanımlanır.

Şimdi F / K fonksiyon cisminin bir elemanının divizörü tanımlanacaktır. Herhangi bir $x \in F$, $x \neq 0$ elemanının sonlu sayıda kökü ve kutbu vardır. Bu sebeple sıradaki tanım yapılabilir.

2.1.11. Tanım: Herhangi bir $x \in F$, $x \neq 0$ elemanının köklerinin (sırasıyla kutuplarının) kümesi $\mathcal{Z}$ (sırasıyla $\mathcal{N}$) olmak üzere, x elemanının kök divizörü, kutup divizörü ve esas divizörü sırasıyla

$$(x)_0 \coloneqq \sum_{P \in \mathcal{Z}} v_P(x)P, \tag{2.4}$$
$$(x)_\infty \coloneqq \sum_{P \in \mathcal{N}} (-v_P(x))P, \tag{2.5}$$
$$(x) \coloneqq (x)_0 - (x)_\infty = \sum_{P \in \mathcal{P}_F} v_P(x)P \tag{2.6}$$

şeklinde tanımlanır.

Tanımları gereğince bir $x \in F$, $x \neq 0$ elemanının kök divizörü ve kutup divizörü pozitiftir. Dahası, $(x) = 0$ olması için gerekli ve yeterli koşul $x \in K$ olmasıdır.

Şimdi tezin diğer bölümlerinde kullanılacak olan önemli bir teorem verilecektir.

2.1.12. Teorem: Bir $x \in F \setminus K$ elemanı için

$$\deg (x)_0 = \deg (x)_\infty = [F : K(x)] \tag{2.7}$$

eşitliği sağlanır.

Yukarıdaki teoremin bir sonucu olarak her $x \in F$, $x \neq 0$ elemanı için $\deg (x) = 0$ olduğu görülebilir.

Sıradaki tanım fonksiyon cismi teorisinde temel bir yer tutmaktadır.

2.1.13. Tanım: Bir $A \in \mathrm{Div}(F)$ divizörü için

$$\mathcal{L}(A) \coloneqq \{\, x \in F \mid (x) \geq -A \,\} \cup \{\, 0 \,\} \tag{2.8}$$

şeklinde tanımlı K-vektör uzayına A divizörünün Riemann-Roch uzayı denir. Bu vektör uzayının boyutu $\ell(A)$ ile gösterilir.

Bu kısmın geri kalanında fonksiyon cisimlerinin otomorfizmalarıyla ilgili sonraki bölümlerde kullanılacak olan birkaç sonuç verilecektir.

2.1.14. Tanım: Bir $F \,/\, K$ fonksiyon cismi için

$$\mathrm{Aut}(F/K) \coloneqq \{\, \sigma\colon F \longrightarrow F \mid \sigma, \text{her } k \in K \text{ için } \sigma(k) = k \text{ özelliğini sağlayan bir otomorfizmadır} \,\} \tag{2.9}$$

şeklinde tanımlı gruba, $F \,/\, K$ fonksiyon cisminin otomorfizma grubu denir.

Bir $\sigma \in \mathrm{Aut}(F/K)$ için $P \in \mathcal{P}_F$ olmak üzere $\sigma(P) \coloneqq \{\, \sigma(x) \mid x \in P \,\}$ şeklinde tanımlı küme de $F \,/\, K$ fonksiyon cisminin bir noktasıdır. Buna ek olarak $\sigma \in \mathrm{Aut}(F/K)$ yardımıyla tanımlanan,

$$\varphi\colon F_P \longrightarrow F_{\sigma(P)},\ z(P) \mapsto \sigma(z)(\sigma(P)) \tag{2.10}$$

dönüşümü P'nin rezidü cisminden, $\sigma(P)$'nin rezidü cismine tanımlı bir cisim izomorfizması olduğundan,

$$\deg \sigma(P) = \deg P \tag{2.11}$$

olur.

Bir $F \,/\, K$ fonksiyon cisminin otomorfizmalarının $\mathcal{P}_F$ üzerindeki eylemi, $\mathrm{Div}(F)$ grubu üzerine

$$\sigma\left(\textstyle\sum_{P \in \mathcal{P}_F} n_P P\right) \coloneqq \sum_{P \in \mathcal{P}_F} n_P \sigma(P) \tag{2.12}$$

şeklinde genişletilebilir. Ayrıca bir $D \in \mathrm{Div}(F)$ divizörü için (2.11) dikkate alınırsa $\deg \sigma(D) = \deg D$ olduğu görülebilir.

Verilen tanımlar ve sonuçlardan sonra, bir fonksiyon cismini $F \,/\, K$ karakterize eden en önemli kavramlardan biri verilebilecektir. Bir $\gamma \in \mathbb{Z}$ tamsayısı, her $A \in \mathrm{Div}(F)$ divizörü için

$$\deg A - \ell(A) \leq \gamma \tag{2.13}$$

eşitsizliğini sağlar. Bu nedenle sıradaki tanım anlamlıdır.

2.1.15. Tanım: Bir $F \,/\, K$ fonsiyon cismi göz önüne alınsın.

$$g \coloneqq \text{maks}\{\, \deg A - \ell(A) + 1 \mid A \in \text{Div}(F) \,\} \tag{2.14}$$

tamsayısına fonksiyon cisminin cinsi denir.

Bir fonksiyon cisminin cinsi negatif olmayan bir tamsayıdır.

Bu kısımda son olarak bir fonksiyon cisminin otomorfizmalarıyla ilgili sonraki bölümlerde kullanışlı olacak bazı sonuçlar verilecektir.

2.1.16. Teorem: (Picone, 2007) Cinsi g olan bir fonksiyon cismi $F \,/\, K$ ve bir $\sigma \in \text{Aut}(F/K)$ otomorfizması göz önüne alınsın.

(1) Bir $P \in \mathcal{P}_F$ rasyonel noktası için $x \in \mathcal{O}_P$ olmak üzere $\sigma(x)(\sigma(P)) = x(P)$ olur.

(2) Bir $A \in \text{Div}(F)$ divizörü için $\mathcal{L}(\sigma(A)) = \sigma(\mathcal{L}(A))$ dir.

(3) Eğer σ otomorfizması en az $2g + 3$ tane rasyonel noktayı sabit bırakıyorsa, birim dönüşümdür.

2.2. Kodlar

Kodlama teorisi çeşitli nedenlerden dolayı bozulan mesajların alıcıya hatasız bir şekilde ulaşmasıyla ilgilenir.

2.2.1. Tanım: Eleman sayısı q olan sonlu bir $\mathbb{F}_q$ cismi göz önüne alınsın. Bir n-boyutlu $\mathbb{F}_q^n$ vektör uzayının herhangi bir alt uzayına C, alfabesi $\mathbb{F}_q$ olan bir lineer kod denir. Bir kodun elemanına, kod sözcüğü denir.

Yukarıda verilen tanımdaki n pozitif tam sayısı, bu kodun uzunluğu olarak tanımlanır. Kodun C, bir vektör uzayı olarak $\mathbb{F}_q$ üzerindeki boyutuna kodun boyutu denir.

Herhangi iki $a, b \in \mathbb{F}_q^n$ elemanı için $\mathbb{F}_q^n$ üzerinde

$$d(a,b) \coloneqq |\{\, i \mid a_i \neq b_i \,\}| \tag{2.15}$$

şeklinde tanımlı metriğe, Hamming uzaklığı denir. Bir $a \in \mathbb{F}_q^n$ elemanının $0 \in \mathbb{F}_q^n$ vektörüne uzaklığına, a'nın ağırlığı denir ve bu değer $\mathrm{wt}(a)$ ile gösterilir.

(2.15)'de tanımlanan metrik yardımıyla, bir kodun en önemli parametrelerinden biri tanımlanacaktır.

2.2.2. Tanım: Bir C kodu için

$$d(C) \coloneqq \min\{\, d(a,b) \mid a, b \in C \text{ ve } a \neq b \,\} \tag{2.16}$$

şeklinde tanımlı pozitif tamsayıya, C kodunun minimum uzaklığı denir.

Uzunluğu n, boyutu k ve minimum uzaklığı n olan bir kod $[n, k, d]$ ile gösterilecektir.

İletilmek istenen bir mesajın, bir kod sözcüğüyle eşleştirilmesi işlemine enkodlama denir. Kodlama teorisinin temel prensibi bu kod sözcüğünü olası hataların olabileceği bir kanal boyunca iletmek, daha sonra elde edilen veriden iletilen kod sözcüğünü doğru olarak tahmin etmektir. Bu işlem dekodlama olarak isimlendirilir. Böylece iletilen mesaj elde edilmiş olur.

2.2.3. Tanım: Bir $C \subseteq \mathbb{F}_q^n$ kodu göz önüne alınsın. İletilmek istenen mesajın bir x kod sözcüğüyle eşleştirildiği varsayılsın. İletilen vektör $y \in \mathbb{F}_q^n$ olmak üzere,

$$e \coloneqq y - x \tag{2.17}$$

şeklinde tanımlı vektöre hata vektörü denir.

Dekodlama işlemi, temeli matematiksel yapılara dayanan çeşitli algoritmalarla yapılır. Sıradaki örnekte bu algoritmalardan biri sunulacaktır.

2.2.4. Örnek: Bir kod sözcüğünün bir kanal boyunca iletildiği varsayılsın. Alıcı çıktı olarak bir $y \in \mathbb{F}_q^n$ vektörü aldığında, bu vektöre (2.15)'de tanımlanan Hamming

uzaklığı anlamında en yakın kod sözcüğünün cevap olarak kabul edildiği dekodlama şekline en yakın komşu dekodlaması denir.

Yukarıdaki örnekte, ağırlığı en küçük olacak şekilde bir hata vektörünün seçilmesi gerektiğine dikkat edilmelidir. Yarıçapı t ve merkezi bir kod sözcüğü $c \in C$ olan bir kapalı yuvar

$$B_t(c) = \{\, u \in \mathbb{F}_q^n \mid d(c,u) \leq t \,\} \tag{2.18}$$

göz önüne alınsın. Herhangi iki kod sözcüğü $c_1, c_2 \in C$ için

$$t \coloneqq \lfloor (d-1)/2 \rfloor \tag{2.19}$$

olmak üzere $B_t(c_1) \cap B_t(c_2) = \emptyset$ olduğu görülebilir. Dolayısıyla eğer hata vektörü e, t ya da daha az hataya sahipse en yakın komşu dekodlaması gönderilmek istenen kod sözcüğünü doğru olarak iletebilecektir. Bu nedenle C lineer koduna, bir t-hata düzeltici kod denir.

Şimdi CG kodlar sunulacaktır. $F \,/\, \mathbb{F}_q$ fonksiyon cisminin bir rasyonel noktası $P \in \mathcal{P}_F$ göz önüne alınsın. 2.1.7 Tanım gereğince $z \in \mathcal{O}_P$ olmak üzere her $z(P) \in F_P$ elemanı, $\mathbb{F}_q$ sonlu cisminin bir elemanı olarak düşünülebileceğinden aşağıdaki tanım anlamlıdır.

2.2.5. Tanım: (Goppa, 1981) Bir fonksiyon cismi $F \,/\, \mathbb{F}_q$ göz önüne alınsın. $P_1, P_2, \dots, P_N \in \mathcal{P}_F$ ikili olarak birbirinden farklı rasyonel noktalar olmak üzere, $D \coloneqq P_1 + P_2 + \cdots + P_N$ divizörü ve $\operatorname{supp} G \cap \{P_1, P_2, \dots, P_N\} = \emptyset$ olacak şekilde bir $G \in \operatorname{Div}(F)$ divizörü göz önüne alınsın.

$$C_{\mathcal{L}}(D,G) \coloneqq \{\, (z(P_1), z(P_2), \dots, z(P_N)) \mid z \in \mathcal{L}(G) \,\} \subseteq \mathbb{F}_q^N \tag{2.20}$$

lineer koduna bir cebirsel geometrik kod denir.

$C_{\mathcal{L}}(D,G)$ CG kodunun uzunluğu N olduğundan, herhangi bir $(z(P_1), z(P_2), \dots, z(P_N)) \in C_{\mathcal{L}}(D,G)$ elemanının N-inci simetrik grup $\mathcal{S}_N$'in bir elemanı π altındaki görüntüsü

$$\pi(z(P_1), z(P_2), \dots, z(P_N)) \coloneqq (z(P_{\pi(1)}), z(P_{\pi(2)}), \dots, z(P_{\pi(N)})) \quad (2.21)$$

şeklinde tanımlanır. Bu nedenle $C_{\mathcal{L}}(D, G)$ CG kodunun otomorfizma grubu

$$\mathrm{Aut}(C_{\mathcal{L}}(D, G)) \coloneqq \{\, \pi \in \mathcal{S}_N \mid \pi(C_{\mathcal{L}}(D, G)) \subseteq C_{\mathcal{L}}(D, G) \,\} \quad (2.22)$$

şeklindedir. Ayrıca bir CG kodun boyutu ve minimum uzaklığı sırasıyla $k = \ell(G) - \ell(G - D)$ eşitliğini ve $d \geq N - \deg G$ eşitsizliğini sağlar.

GCG kodlar, yüksek dereceden noktalar kullanılarak CG kodların yapısının genelleştirilmesiyle benzer bir kod sınıfı inşa etmek amacıyla oluşturulmuştur. Concatenated kod kavramı, GCG kodların ortaya çıkmasında önemli bir rol oynamaktadır. Concatenated kodlar, Forney tarafından 1966 yılında bulunmuştur (Forney, 1966). Bir concatenated kod, iki kodun (Forney, 1966)'da verilen teknikle birleştirilmesiyle elde edilir. Concatenated kodların basit bir örneği aşağıdaki gibidir.

2.2.6. Örnek: (Ling & Xing, 2004) A, $\mathbb{F}_{q^m}$ üzerinde bir $[N, K, D]$ lineer kod ve B, $\mathbb{F}_q$ üzerinde bir $[n, m, d]$ lineer kod olsun. O zaman $\mathbb{F}_q$ üzerinde $d' = d(C) \geq dD$ olmak üzere $[nN, mK, d']$ parametrelerine sahip bir C lineer kodu vardır.

2.2.7. Tanım: (Ling & Xing, 2004) 2.2.6 Örnek'de elde edilen C koduna bir concatenated kod denir. 2.2.6 Örnek'deki A kodu dış kod, B kodu iç kod olarak isimlendirilir.

Bir fonksiyon cisminin yüksek dereceli noktalarından yararlanabilmek ve daha iyi parametrelere sahip CG kodlar elde edebilmek için çeşitli yöntemler kullanılarak 2.2.5 Tanım'da verilen kod yapısı genelleştirilmeye çalışılmıştır (Özbudak & Stichtenoth, 1999; Niederreiter, Xing & Lam, 1999; Xing, Niederreiter & Lam, 1999a; Xing vd., 1999b). Ancak elde edilen kodların parametre değerlerinin AG kodların parametre değerlerine benzer olması sebebiyle bu farklı yapılar arasında bazı ilişkiler olabileceği düşünülmüş, birinin diğerlerinden daha iyi olup olmadığı araştırılmıştır. Özbudak ve Stichtenoth (1999), diğer genellemelerin (Xing vd., 1999b)'de verilen yapının özel bir hali olduğunu ve bu yapının AG kodların en kapsamlı genellemesi olduğunu göstermişlerdir. Bu ön bilgiler ve sonuçlardan sonra GCG kodlar sunulabilecektir.

2.2.8. Tanım: (Xing vd., 1999b) Cinsi g olan bir fonksiyon cismi $F / \mathbb{F}_q$ göz önüne alınsın. $P_1, P_2, \dots, P_s \in \mathcal{P}_F$ ikili olarak birbirinden farklı noktalar olmak üzere $1 \leq i \leq s$ için $\deg P_i = k_i$ olsun. G, $F / \mathbb{F}_q$ fonksiyon cisminin $\operatorname{supp} G \cap \{P_1, P_2, \dots, P_s\} = \emptyset$ olacak şekilde bir divizörü ve $1 \leq i \leq s$ için C_i, parametreleri $[n_i, k_i, d_i]$ olan bir q-ary lineer kod olsun. $1 \leq i \leq s$ için π_i, $\mathbb{F}_{q^{k_i}}$'dan C_i'ye bir $\mathbb{F}_q$-lineer izomorfizma ve $\sum_{i=1}^{s} n_i = n$ olmak üzere,

$$C(P_1, \dots, P_s; G; C_1, \dots, C_s) \coloneqq \{ (\pi_1(z(P_1)), \dots, \pi_s(z(P_s))) \mid z \in \mathcal{L}(G) \} \subseteq \mathbb{F}_q^n \qquad (2.23)$$

lineer koduna bir genelleştirilmiş cebirsel geometrik kod denir.

GCG kodların parametreleri ile ilgili birkaç sonuç verilecektir.

2.2.9. Teorem: (Xing vd., 1999b) $\deg G < \sum_{i=1}^{s} k_i$ olsun. O zaman maksimum $\{1,2, \dots, s\}$ kümesinin tüm R alt kümeleri üzerinden alınmak üzere, $C(P_1, \dots, P_s; G; C_1, \dots, C_s)$ kodunun boyutu k ve minimum uzaklığı d aşağıdaki eşitsizlikleri sağlar:

$$k \geq \deg G - g + 1, \qquad (2.24)$$

$$d \geq \sum_{i=1}^{s} d_i - \deg G - \max_{R}\{ \textstyle\sum_{i \in R}(d_i - k_i) \}. \qquad (2.25)$$

Dahası $\deg G \geq 2g - 1$ ise $k = \deg G - g + 1$ olur.

2.2.10. Sonuç: (Xing vd., 1999b) $\deg G < \sum_{i=1}^{s} k_i$ koşuluna ek olarak $1 \leq i \leq s$ için $k_i \geq d_i$ koşulu sağlanıyorsa $C(P_1, \dots, P_s; G; C_1, \dots, C_s)$ kodunun minimum uzaklığı d için $d \geq \sum_{i=1}^{s} d_i - \deg G$ eşitsizliği sağlanır.

Küçük q değerleri için $\mathbb{F}_q$ sonlu cismi üzerinde en optimal parametrelere sahip lineer kodların çoğu 2.2.8 Tanım'daki yapıyla elde edilebilmektedir. Ancak Goppa'nın yapısıyla (1981), bu lineer kodlar elde edilememektedir. Bazı GCG kod örnekleri verilecektir. Verilecek örneklerde $i \geq 1$ olmak üzere $F / \mathbb{F}_q$ fonksiyon cisminin derecesi i olan nokta sayıları B_i ile gösterilecektir. Tüm örneklerde $F / \mathbb{F}_q$ fonksiyon cisminin ikili olarak birbirinden farklı s noktası, dereceleri azalmayan sıraya göre olmak üzere $P_1, P_2, \dots, P_s$ şeklinde verilecektir. Yeteri kadar büyük bir r pozitif tamsayısı için $F / \mathbb{F}_q$ fonksiyon cisminin dereceleri sırasıyla r ve $r + 1$ olan P ve Q noktaları vardır

(Xing vd., 1999b). Yeteri kadar büyük bir r pozitif tamsayısı için $\operatorname{supp} G \cap \{P_1, P_2, \dots, P_s\} = \emptyset$ olmak üzere, daima $G = m(Q - P)$ seçilecektir. Burada $\deg G = m$ dir. Tüm örnekler 2.2.9 Teorem ve 2.2.10 Sonuç'tan elde edilmiştir.

2.2.11. Örnek: (Xing vd., 1999b) $y^2 + xy = x^3 + x$ ile tanımlanan $F = \mathbb{F}_2(x, y)$ fonksiyon cismi göz önüne alınsın. Bu fonksiyon cismi için $B_1 = 4$, $B_2 = 2$, $B_3 = 0$ ve $B_4 = 2$ dir. Bu fonksiyon cisminin cinsi $g = 1$ dir.

$s = 6$ alınsın. $1 \le i \le 4$ için $[n_i, k_i, d_i] = [1, 1, 1]$ ve $i = 5, 6$ için $[n_i, k_i, d_i] = [3, 2, 2]$ olmak üzere parametreleri,

$1 \le m \le 4$ için $[10, m, 8 - m]$ (2.26)

olan ikili lineer kodlar elde edilir.

$s = 7$ alınsın. $1 \le i \le 4$ için $[n_i, k_i, d_i] = [1, 1, 1]$, $i = 5, 6$ için $[n_i, k_i, d_i] = [3, 2, 2]$ ve $[n_7, k_7, d_7] = [8, 4, 4]$ olmak üzere parametreleri,

$1 \le m \le 11$ için $[18, m, 12 - m]$ (2.27)

olan ikili lineer kodlar elde edilir.

$s = 8$ alınsın. $1 \le i \le 4$ için $[n_i, k_i, d_i] = [1, 1, 1]$, $i = 5, 6$ için $[n_i, k_i, d_i] = [3, 2, 2]$ ve $i = 7, 8$ için $[n_7, k_7, d_7] = [8, 4, 4]$ olmak üzere parametreleri,

$1 \le m \le 15$ için $[26, m, 16 - m]$ (2.28)

olan ikili lineer kodlar elde edilir.

2.2.12. Örnek: (Xing vd., 1999b) $y^2 + y = x^3$ ile tanımlanan $F = \mathbb{F}_2(x, y)$ fonksiyon cismi göz önüne alınsın. Bu fonksiyon cismi için $B_1 = 3$, $B_2 = 3$ ve $B_3 = 2$ dir. Bu fonksiyon cisminin cinsi $g = 1$ dir.

$s = 5$ alınsın. $1 \le i \le 3$ için $[n_i, k_i, d_i] = [1, 1, 1]$ ve $i = 4, 5$ için $[n_i, k_i, d_i] = [3, 2, 2]$ olmak üzere parametreleri,

$1 \le m \le 6$ için $[9, m, 7 - m]$ (2.29)

olan ikili lineer kodlar elde edilir.

$s = 6$ alınsın. $1 \leq i \leq 3$ için $[n_i, k_i, d_i] = [1, 1, 1]$ ve $4 \leq i \leq 6$ için $[n_i, k_i, d_i] = [3, 2, 2]$ olmak üzere parametreleri,

$1 \leq m \leq 8$ için $[12, m, 9 - m]$ (2.30)

olan ikili lineer kodlar elde edilir.

$s = 7$ alınsın. $1 \leq i \leq 3$ için $[n_i, k_i, d_i] = [1, 1, 1]$, $4 \leq i \leq 6$ için $[n_i, k_i, d_i] = [3, 2, 2]$ ve $[n_7, k_7, d_7] = [4, 3, 2]$ olmak üzere parametreleri,

$1 \leq m \leq 10$ için $[16, m, 11 - m]$ (2.31)

olan ikili lineer kodlar elde edilir.

$s = 8$ alınsın. $1 \leq i \leq 3$ için $[n_i, k_i, d_i] = [1, 1, 1]$, $4 \leq i \leq 6$ için $[n_i, k_i, d_i] = [3, 2, 2]$ ve $i = 7, 8$ için $[n_i, k_i, d_i] = [4, 3, 2]$ olmak üzere parametreleri,

$1 \leq m \leq 12$ için $[20, m, 13 - m]$ (2.32)

olan ikili lineer kodlar elde edilir.

$s = 8$ alınsın. $1 \leq i \leq 3$ için $[n_i, k_i, d_i] = [1, 1, 1]$, $4 \leq i \leq 6$ için $[n_i, k_i, d_i] = [3, 2, 2]$, $[n_7, k_7, d_7] = [4, 3, 2]$ ve $[n_8, k_8, d_8] = [6, 3, 3]$ olmak üzere parametreleri,

$1 \leq m \leq 13$ için $[22, m, 14 - m]$ (2.33)

olan ikili lineer kodlar elde edilir.

$s = 8$ alınsın. $1 \leq i \leq 3$ için $[n_i, k_i, d_i] = [1, 1, 1]$, $4 \leq i \leq 6$ için $[n_i, k_i, d_i] = [3, 2, 2]$ ve $i = 7, 8$ için $[n_i, k_i, d_i] = [6, 3, 3]$ olmak üzere parametreleri,

$1 \leq m \leq 14$ için $[24, m, 15 - m]$ (2.34)

olan ikili lineer kodlar elde edilir.

GCG kodların otomorfizma gruplarını belirlemek için kullanılan yöntemler, CG kodların otomorfizma gruplarını belirlemek için kullanılan yöntemlere dayanır. Ancak GCG kodların yapısında farklı dereceden noktaların ve bir dizi lineer kodun bulunması, CG kodların otomorfizma gruplarını belirlemek için kullanılan bu yöntemlerin en genel haliyle GCG kodlara uygulanmasına olanak vermemiştir. Bu nedenle çalışmalar GCG kodların aynı dereceden noktaları içeren daha elementer bir yapısını kullanarak, GCG

kodların otomorfizma gruplarının bir alt grubunu belirlemek üzerine yoğunlaşmıştır (Picone, 2016; Picone & Spera, 2009; Spera, 2007). Bu çalışmalarda göz önüne alınan GCG kodların bu alt sınıfı ve bu alt sınıftaki kodların otomorfizma grubunun yine bu çalışmalarda göz önüne alınan spesifik bir alt grubu sunulacaktır.

Öncelikle GCG kodların bu alt sınıfının yapısının daha kolay anlaşılmasını sağlayacak ve bulunan sonuçların uygulamalarında kullanışlı olacak ((Picone & Spera, 2009, s. 333-339)'e bakınız) bazı kavramlar ve notasyonlar verilecektir. Bir fonksiyon cismi $F \,/\, \mathbb{F}_q$ göz önüne alınsın. Derecesi n olan bir nokta $P \in \mathcal{P}_F$ için F_P rezidü cisminin $\mathbb{F}_{q^n}$ sonlu cismine $\mathbb{F}_q$-izomorf (burada iki cismin arasında $\mathbb{F}_q$ cisminin her elemanını sabit bırakan bir cisim izomorfizmasının olduğu kastedilmektedir) olduğu bilinmektedir. Bu şekildeki bir izomorfizma $\phi_P \colon F_P \longrightarrow \mathbb{F}_{q^n}$ olmak üzere, (P, ϕ_P) çiftine bir ϕ-nokta denir (Spera, 2007). Bir ϕ-divizör, ϕ-noktalar tarafından üretilen serbest abelyan grubunun bir elemanı olarak tanımlanır. Herhangi bir ϕ-divizör, $n_P \in \mathbb{Z}$ ve sonlu sayıdaki hariç her bir $n_P = 0$ olmak üzere $\Phi \coloneqq \sum_{P \in \mathcal{P}_F} n_P (P, \phi_P)$ şeklinde yazılır. Bir P noktasına karşılık gelen $\mathcal{O}_P$ değerlendirme halkasının bir z elemanı için $z(P, \phi_P) \coloneqq \phi_P(z(P))$ olarak tanımlanır.

$\mathbb{F}_q$ sonlu cismi üzerinde aynı boyuta sahip olan $\mathbb{F}_q^n$ ve $\mathbb{F}_{q^n}$ vektör uzayları birbirine izomorf olduğundan $z(P, \phi_P)$, $\mathbb{F}_q^n$ vektör uzayının bir elemanı olarak düşünülebilir. Daha açık olarak, $\mathbb{F}_q$ cisminin cebirsel kapanışının bir elemanı $\alpha \in \overline{\mathbb{F}_q}$ olmak üzere $\mathbb{F}_{q^n}$'in $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$ şeklinde yazılabileceği bilinmektedir. Böylece $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ kümesi, $\mathbb{F}_{q^n}$'in $\mathbb{F}_q$ üzerinde bir tabanıdır. Bu nedenle $\mathbb{F}_{q^n}$'in her elemanı $\sum_{i=0}^{n-1} a_i \, \alpha^i$, bir $(a_0, a_1, a_2, \dots, a_{n-1}) \in \mathbb{F}_q^n$ elemanı şeklinde düşünülebilir.

$(P_1, \phi_1), (P_2, \phi_2), \dots, (P_N, \phi_N) \in \mathcal{P}_F$ derecesi n olan ikili olarak birbirinden farklı ϕ-noktalar olmak üzere, $\Phi \coloneqq (P_1, \phi_1) + (P_2, \phi_2) + \cdots + (P_N, \phi_N)$ ϕ-divizörü ve $\operatorname{supp} G \cap \{P_1, P_2, \dots, P_N\} = \emptyset$ olacak şekilde bir $G \in \operatorname{Div}(F)$ divizörü göz önüne alınsın.

$$C(\Phi; \mathrm{G}; \mathrm{n}) \coloneqq \{ \, (z(P_1, \phi_1), \dots, z(P_N, \phi_N)) \mid z \in \mathcal{L}(G) \, \} \subseteq \mathbb{F}_q^{Nn} \simeq \prod_{i=1}^{N} \mathbb{F}_q^n \qquad (2.35)$$

lineer kodu, (2.23)'de tanımlanan GCG kodun özel bir halidir. Uygun bir G divizörü için $C(\Phi; \mathrm{G}; \mathrm{n})$ koduna basit olarak $P_1, P_2, \dots, P_N$ noktaları tarafından üretilmiştir

denilecektir. Burada her $i \in \{1, 2, \dots, N\}$ için C_i lineer kodunun $\mathbb{F}_q^n$ olarak alındığına dikkat edilmelidir.

Bu alt bölümde son olarak $C(\Phi; \mathrm{G}; \mathrm{n})$ kodunun otomorfizma grubunun spesifik bir alt grubu sunulacaktır. $C(\Phi; \mathrm{G}; \mathrm{n})$ kodunun otomorfizma grubu, bu kodun uzunluğu Nn olduğundan Nn-inci simetrik grup $\mathcal{S}_{Nn}$ olmak üzere

$$\mathrm{Aut}(C(\Phi; \mathrm{G}; \mathrm{n})) \coloneqq \{ \pi \in \mathcal{S}_{Nn} \mid \pi(C(\Phi; \mathrm{G})) \subseteq C(\Phi; \mathrm{G}) \} \tag{2.36}$$

şeklinde tanımlanır. Her $i \in \{1, 2, \dots, N\}$ için $z(P_i, \phi_i) \in \mathbb{F}_q^n$ olduğundan, $C(\Phi; \mathrm{G}; \mathrm{n})$ kodunun bir kod sözcüğünün N bloktan oluştuğu düşünülebilir. Bu N bloğun kendi arasında sıralanmasıyla Nn-inci simetrik grup $\mathcal{S}_{Nn}$'in bir elemanı elde edilir. $\mathrm{Aut}(C(\Phi; \mathrm{G}; \mathrm{n}))$ grubunun bu N bloğu kendi arasında sıralayan bir elemanına n-otomorfizma denir. Bu elemanların oluşturduğu alt gruba bir n-otomorfizma grubu denir ve bu grup $\mathcal{H}(\Phi; \mathrm{G}; \mathrm{n})$ ile gösterilir (Picone & Spera, 2009). Herhangi bir $(z(P_1, \phi_1), \dots, z(P_N, \phi_N)) \in C(\Phi; \mathrm{G}; \mathrm{n})$ elemanının, bir n-otomorfizma π altındaki görüntüsü

$$\pi(z(P_1, \phi_1), \dots, z(P_N, \phi_N)) \coloneqq (z(P_{\pi(1)}, \phi_{\pi(1)}), \dots, z(P_{\pi(N)}, \phi_{\pi(N)})) \tag{2.37}$$

şeklinde tanımlanır.

2.3. Fonksiyon Cisimlerinin Cebirsel Genişlemeleri

Bu alt bölümde, tez boyunca kullanılacak olan fonksiyon cisimlerinin cebirsel genişlemeleri ile ilgili temel tanımlar ve sonuçlar verilecektir. Alt bölüm boyunca K mükemmel bir cisim olmak üzere, $F \,/\, K$ tam sabit cismi K olan bir fonksiyon cismini gösterecektir.

2.3.1. Tanım: (Stichtenoth, 2009) $F \subseteq F'$ bir cebirsel cisim genişlemesi ve $K \subseteq K'$ ise $F' \,/\, K'$ fonksiyon cismine, $F \,/\, K$ fonksiyon cisminin bir cebirsel genişlemesi denir.

Fonksiyon cisimlerinin cebirsel genişlemelerinin özel durumları verilecektir.

2.3.2. Tanım: (Stichtenoth, 2009) F ve K' cisimlerinin bileşik cismi $F' = FK'$ olmak üzere, $F \,/\, K$ fonksiyon cisminin cebirsel genişlemesi $F' \,/\, K'$, bir sabit cisim genişlemesi olarak isimlendirilir.

2.3.3. Tanım: (Stichtenoth, 2009) $F \subseteq F'$ sonlu bir cisim genişlemesi ise, $F \,/\, K$ fonksiyon cisminin cebirsel genişlemesi $F' \,/\, K'$, bir sonlu genişleme olarak isimlendirilir.

$F \,/\, K$ ve $F' \,/\, K'$ fonksiyon cisimlerinin noktaları arasındaki ilişki incelenecektir.

2.3.4. Tanım: (Stichtenoth, 2009) $F \,/\, K$ fonksiyon cisminin bir cebirsel genişlemesi $F' \,/\, K'$ göz önüne alınsın. $P \in \mathcal{P}_F$ ve $P' \in \mathcal{P}_{F'}$ olmak üzere $P \subseteq P'$ ise P' noktası, P noktası üzerine uzanıyor denir. Ayrıca P' noktasına, P noktasının bir genişlemesi denir. Bu durum $P'|P$ ile gösterilir.

Bir $P' \in \mathcal{P}_{F'}$ noktası, $P \in \mathcal{P}_F$ noktası üzerine uzanıyorsa $\deg P \,|\, \deg P'$ dir (Tsfasman, Vladut & Nogin, 2019, s. 52).

2.3.5. Önerme: (Stichtenoth, 2009) $F \,/\, K$ fonksiyon cisminin bir cebirsel genişlemesi $F' \,/\, K'$ göz önüne alınsın. Bir $P \in \mathcal{P}_F$ noktasına karşılık gelen değerlendirme halkası ve değerlendirme sırasıyla $\mathcal{O}_P$ ve v_P ile gösterilsin. Benzer şekilde bir $P' \in \mathcal{P}_{F'}$ noktasına karşılık gelen değerlendirme halkası ve değerlendirme sırasıyla $\mathcal{O}_{P'}$ ve $v_{P'}$ ile gösterilsin. O zaman aşağıdaki ifadeler denktir:

(1) $P'|P$,

(2) $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$.

Dahası, eğer $P'|P$ ise $P = P' \cap F$ ve $\mathcal{O}_P = \mathcal{O}_{P'} \cap F$ olur. Bu sebeple P noktası, P' noktasının F cismine kısıtlaması olarak da isimlendirilir.

Fonksiyon cisim genişlemelerinde bir noktanın genişlemesinin varlığı ile ilgili bir önerme verilecektir.

2.3.6. Önerme: (Stichtenoth, 2009) $F \,/\, K$ fonksiyon cisminin bir cebirsel genişlemesi $F' \,/\, K'$ göz önüne alınsın.

(1) Her $P' \in \mathcal{P}_{F'}$ noktası için $P'|P$ olacak şekilde tam olarak bir tane $P \in \mathcal{P}_F$ noktası vardır.

(2) Tersine, her $P \in \mathcal{P}_F$ noktası için $P'|P$ olacak şekilde en az bir, fakat sonlu sayıda $P' \in \mathcal{P}_{F'}$ noktası vardır.

Bir noktanın genişlemelerini karakterize eden bazı tanımlamalar yapılacaktır.

2.3.7. Tanım: (Stichtenoth, 2009) $F\,/\,K$ fonksiyon cisminin bir cebirsel genişlemesi $F'\,/\,K'$ göz önüne alınsın ve bir $P' \in \mathcal{P}_{F'}$ noktası, bir $P \in \mathcal{P}_F$ noktasının üzerine uzansın. Bir $e \geq 1$ tamsayısı için $v_{P'}(x) = ev_P(x)$ eşitliği her $x \in F$ elemanı için sağlanır. $e(P'|P) \coloneqq e$ olmak üzere $e(P'|P) > 1$ ise $P'|P$ genişlemesine dallanmış, $e(P'|P) = 1$ ise $P'|P$ genişlemesine dallanmamış denir. $F\,/\,K$ fonksiyon cisminin bir sonlu genişlemesi $F'\,/\,K'$ durumunda $[F'\colon F] = n$ olmak üzere, $e(P'|P) = n$ ise $P'|P$ genişlemesine tamamen dallanmış denir.

2.3.8. Tanım: (Tsfasman vd., 2019, s. 52) $F\,/\,K$ fonksiyon cisminin bir sonlu genişlemesi $F'\,/\,K'$ göz önüne alınsın ve $[F'\colon F] = n$ olsun. Toplam herhangi bir $P \in \mathcal{P}_F$ noktasının üzerine uzanan noktalar üzerinden alınmak üzere, $\sum_{P'|P} \deg P' \leq n \deg P$ eşitsizliği sağlanır. $\deg P \mid \deg P'$ olduğundan P noktasının en fazla n genişlemesi vardır. P noktasının n genişlemesi varsa P noktasına parçalanmış denir. P noktasının tek bir genişlemesi var ve $\deg P' = n \deg P$ eşitliği sağlanıyorsa P noktasına durağan denir.

2.3.6 Önerme yardımıyla aşağıdaki tanım yapılabilecek ve $F\,/\,K$ fonksiyon cisminin $\mathrm{Div}\,(F)$ divizör grubundan $F'\,/\,K'$ fonksiyon cisminin $\mathrm{Div}\,(F')$ divizör grubuna bir homomorfizma tanımlamak mümkün olacaktır.

2.3.9. Tanım: (Stichtenoth, 2009) $F\,/\,K$ fonksiyon cisminin bir cebirsel genişlemesi $F'\,/\,K'$ göz önüne alınsın. Herhangi bir $P \in \mathcal{P}_F$ noktasının conorm'u $F'\,/\,K'$ fonksiyon cisminin

$$\mathrm{Con}_{F'/F}(P) \coloneqq \sum_{P'|P} e(P'|P\,)P' \tag{2.38}$$

şeklinde tanımlanan bir divizörüdür. Bu tanımlama yardımıyla,

$$\mathrm{Con}_{F'/F}\colon \mathrm{Div}(F) \longrightarrow \mathrm{Div}(F'),\ \mathrm{Con}_{F'/F}(\sum n_P P) \mapsto \sum n_P \mathrm{Con}_{F'/F}(P) \tag{2.39}$$

şeklinde bir homomorfizma tanımlanabilir.

BÖLÜM 3

GCG KODLARIN OTOMORFİZMA GRUPLARI

Bu bölümde öncelikle tez boyunca hakkında ilgili sonuçların bulunacağı, GCG kodların (2.35)'de verilen yapı anlamında farklı dereceye sahip noktalar tarafından üretilmesine izin veren daha genel bir alt sınıfı sunulacaktır. Ardından bu alt sınıftaki en fazla farklı iki dereceye sahip noktaların bir kümesi tarafından üretilen kodların N_1N_2-otomorfizma grubu $\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ tanımlanacaktır. Keyfi fonksiyon cismi durumda N_1N_2-otomorfizma grubu $\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$'ın bir alt grubu belirlendikten sonra, bu grubun kendisinin sırasıyla rasyonel, hipereliptik ve Hermityan fonksiyon cismi durumlarında hangi koşullar altında belirlenebildiği araştırılacaktır. Ayrıca rasyonel fonksiyon cismi durumunda böyle bir grup açık olarak inşa edilecektir.

3.1. Keyfi Fonksiyon Cismi Durumu

Bir fonksiyon cismi $F\,/\,\mathbb{F}_q$ için $(P_1,\phi_1),(P_2,\phi_2),\dots,(P_N,\phi_N)\in\mathcal{P}_F$ derecesi n_i olan ikili olarak birbirinden farklı ϕ-noktalar olmak üzere, $\Phi \coloneqq (P_1,\phi_1)+(P_2,\phi_2)+\cdots+(P_N,\phi_N)$ ϕ-divizörü ve $\operatorname{supp} G\cap\{P_1,P_2,\dots,P_N\}=\emptyset$ olacak şekilde bir $G\in \mathrm{Div}(F)$ divizörü göz önüne alınsın.

$$C(\Phi;\mathrm{G}) \coloneqq \{\,(z(P_1,\phi_1),\dots,z(P_N,\phi_N)) \mid z\in\mathcal{L}(G)\,\}\subseteq \mathbb{F}_q^{\sum_{i=1}^{N} n_i}\simeq \prod_{i=1}^{N}\mathbb{F}_q^{n_i} \qquad (3.1)$$

lineer kodu, dereceleri farklı olan noktalar tarafından üretilebildiğinden (2.35)'de tanımlanan $C(\Phi;\mathrm{G};\mathrm{n})$ lineer kodundan daha genel bir yapıya sahiptir. Burada her $i\in\{1,2,\dots,N\}$ için 2.2.8 Tanım'daki C_i lineer kodunun $\mathbb{F}_q^{n_i}$ olarak alındığına dikkat edilmelidir.

Aşağıdaki önerme $C(\Phi;\mathrm{G})$ kodunun parametreleriyle ilgilidir.

3.1.1. Önerme: $D = P_1 + P_2 + \cdots + P_N$ olsun. $k = \ell(G) - \ell(G-D)$ ve $d \geq N - \left\lfloor \frac{\deg G}{\min\{\, n_i \mid i\in\{1,2,\ldots,N\}\,\}} \right\rfloor$ olmak üzere $C(\Phi;\mathrm{G})$ bir $[\sum_{i=1}^{N} n_i\,, k, d]$ koddur.

Kanıt: $C(\Phi;\mathrm{G}) \subseteq \mathbb{F}_q^{\sum_{i=1}^{N} n_i}$ olduğundan, $C(\Phi;\mathrm{G})$ kodunun uzunluğu $\sum_{i=1}^{N} n_i$ dir. $C(\Phi;\mathrm{G})$ kodunun boyutunun $k = \ell(G) - \ell(G-D)$ olduğu gösterilecektir. $ev_\Phi\colon \mathcal{L}(G) \longrightarrow \mathbb{F}_q^{\sum_{i=1}^{N} n_i}$, $ev_\Phi(z) \coloneqq (z(P_1,\phi_1), z(P_2,\phi_2), \ldots, z(P_N,\phi_N))$ şeklinde tanımlı lineer dönüşüm için $ev_\Phi(\mathcal{L}(G)) = C(\Phi;\mathrm{G})$ dir. $\mathrm{Ker}(ev_\Phi) = \mathcal{L}(G-D)$ olduğunu göstermek yeterlidir. Herhangi bir $z \in \mathrm{Ker}(ev_\Phi)$ elemanı göz önüne alınsın. Her $i \in \{1,2,\ldots,N\}$ için $z(P_i,\phi_i) = 0$ olduğundan $v_{P_i}(z) \geq 1$ olur. Böylece her $P_i \in \mathrm{supp}\, D$ için $v_{P_i}(z) \geq v_{P_i}(D)$ olacağından $z \in \mathcal{L}(G-D)$ olur. Dolayısıyla $\mathrm{Ker}(ev_\Phi) \subseteq \mathcal{L}(G-D)$ bulunur. Benzer şekilde $\mathcal{L}(G-D) \subseteq \mathrm{Ker}(ev_\Phi)$ olduğu gösterilebileceğinden istenilen elde edilir.

$C(\Phi;\mathrm{G})$ kodunun minimum uzaklığının $d \geq N - \left\lfloor \frac{\deg G}{\min\{\, n_i \mid i\in\{1,2,\ldots,N\}\,\}} \right\rfloor$ eşitsizliğini sağladığı gösterilecektir. $z \in \mathcal{L}(G)$, $z \neq 0$ olacak şekildeki bir eleman için minimum ağırlığa sahip olacak şekildeki bir $(z(P_1,\phi_1), z(P_2,\phi_2), \ldots, z(P_N,\phi_N))$ kod sözcüğü göz önüne alınsın. $\{\, i \in \{1,2,\ldots,N\} \mid z(P_i,\phi_i) \neq 0 \,\}$ kümesinin eleman sayısı d' olsun. O halde genellik kaybına neden olmaksızın $i \in \{1,2,\ldots,N-d'\}$ için $z(P_i,\phi_i) = 0$ olduğu kabul edilebilir. Bu nedenle $i \in \{1,2,\ldots,N-d'\}$ için $v_{P_i}(z) \geq 1$ olacağından $z \in \mathcal{L}\big(G - \sum_{i=1}^{N-d'} P_i\big)$ ve dolayısıyla (Stichtenoth, 2009, Corollary 1.4.12) gereğince $\deg\big(G - \sum_{i=1}^{N-d'} P_i\big) \geq 0$ elde edilir. Böylece $\deg G \geq \sum_{i=1}^{N-d'} n_i \geq (N-d')\min\{\, n_i \mid i \in \{1,2,\ldots,N\}\,\}$ elde edileceğinden $d \geq d' \geq N - \left\lfloor \frac{\deg G}{\min\{\, n_i \mid i\in\{1,2,\ldots,N\}\,\}} \right\rfloor$ olur. ■

(3.1)'de yapılan tanımlama anlamında bu bölüm boyunca göz önüne alınacak olan GCG kodlar sunulacaktır. $\{P_1, P_2, \ldots, P_{N_1}\}$ derecesi n_1 olan ikili olarak birbirinden farklı noktalar ve $\{P_{N_1+1}, P_{N_1+2}, \ldots, P_{N_1+N_2}\}$ derecesi n_2 olan ikili olarak birbirinden farklı noktalar olsun. $\Phi = \sum_{i=1}^{N_1+N_2}(P_i,\phi_i)$ ϕ-divizörü ve $\mathrm{supp}\, G \cap \{P_1, P_2, \ldots, P_{N_1+N_2}\} = \emptyset$ olacak şekilde bir $G \in \mathrm{Div}(F)$ divizörü göz önüne alınsın. Aksi belirtilmediği sürece

bölüm boyunca $C(\Phi;\mathrm{G})$ GCG kodu için bulunacak olan tüm sonuçlar için Φ ϕ-divizörü ve G divizörü bu şekilde seçilecektir.

$C(\Phi;\mathrm{G})$ kodunun otomorfizma grubunun bir alt grubu sunulacaktır. Bir permütasyon $\pi \in \mathcal{S}_{N_1+N_2}$ ve bir kod sözcüğü $c \in C(\Phi;\mathrm{G})$ göz önüne alınsın. Tanım gereğince c kod sözcüğü, $1 \le i \le N_1$ için $a_i = z(P_i,\phi_i) = c_{i1}c_{i2}c_{i3}\dots c_{in_1},\ c_{ij} \in \mathbb{F}_q$, $1 \le j \le n_1$ ve $N_1+1 \le i \le N_1+N_2$ için $a_i = z(P_i,\phi_i) = c_{i1}c_{i2}c_{i3}\dots c_{in_2},\ c_{ij} \in \mathbb{F}_q$, $1 \le j \le n_2$ olmak üzere $c = (a_1, a_2, \dots, a_{N_1+N_2})$ şeklinde yazılabilir. $\mathcal{S}_{N_1+N_2}$ simetri grubu $C(\Phi;\mathrm{G})$ kodu üzerinde

$$\pi(c) \coloneqq (a_{\pi(1)}, a_{\pi(2)}, \dots, a_{\pi(N_1+N_2)}) \tag{3.2}$$

şeklinde tanımlanacaktır.

3.1.2. Tanım: $\pi(C(\Phi;\mathrm{G})) \subseteq C(\Phi;\mathrm{G})$ olacak şekildeki bir $\pi \in \mathcal{S}_{N_1+N_2}$ permütasyonuna, $C(\Phi;\mathrm{G})$ kodunun her kod sözcüğünün ilk N_1 ve diğer N_2 koordinatını kendi arasında sıralıyorsa bir N_1N_2-otomorfizma denir.

$C(\Phi;\mathrm{G})$ kodunun uzunluğu $n_1N_1 + n_2N_2$ olduğundan, otomorfizma grubu $\mathrm{Aut}(C(\Phi;\mathrm{G})) = \{\, \pi \in \mathcal{S}_{n_1N_1+n_2N_2} \mid \pi(C(\Phi;\mathrm{G})) \subseteq C(\Phi;\mathrm{G}) \,\}$ şeklindedir. $\mathcal{S}_{N_1+N_2}$ simetri grubunun her elemanı $\mathcal{S}_{n_1N_1+n_2N_2}$ simetri grubunun bir elemanı olarak düşünülebileceğinden her N_1N_2-otomorfizma, $\mathrm{Aut}(C(\Phi;\mathrm{G}))$ otomorfizma grubunun bir elemanıdır. Dahası N_1N_2-otomorfizmalar, $\mathrm{Aut}(C(\Phi;\mathrm{G}))$ grubunun bir alt grubunu oluşturur.

3.1.3. Tanım: $\mathrm{Aut}(C(\Phi;\mathrm{G}))$ grubunun N_1N_2-otomorfizmalardan oluşan alt grubu $\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ ile gösterilecek ve bu alt grup $C(\Phi;\mathrm{G})$ kodunun N_1N_2-otomorfizma grubu olarak isimlendirilecektir. Herhangi bir $(z(P_1,\phi_1), \dots, z(P_{N_1+N_2},\phi_{N_1+N_2})) \in C(\Phi;\mathrm{G})$ elemanının, bir N_1N_2-otomorfizma π altındaki görüntüsü

$$(z(P_{\pi(1)},\phi_{\pi(1)}), \dots, z(P_{\pi(N_1+N_2)},\phi_{\pi(N_1+N_2)})) \tag{3.3}$$

şeklinde tanımlanır.

$\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ grubu, $C(\Phi;\mathrm{G};\mathrm{n})$ kodundan daha genel bir yapıya sahip olan $C(\Phi;\mathrm{G})$ kodu için tanımlandığından $\mathcal{H}(\Phi;\mathrm{G};\mathrm{n})$ grubunun bir genellemesi olarak

düşünülebilir. Dahası, $C(\Phi; \mathrm{G})$ kodunu üreten noktaların dereceleri aynı olacak şekilde seçildiğinde bu iki grubun yapısının aynı olacağına dikkat edilmelidir.

Bir N_1N_2-otomorfizma, $\Phi = \sum_{i=1}^{N_1+N_2}(P_i, \phi_i)$ ϕ-divizörü üzerinde

$$\pi\Phi \coloneqq \sum_{i=1}^{N_1+N_2}(P_{\pi(i)}, \phi_{\pi(i)}) \tag{3.4}$$

şeklinde tanımlanacaktır. Aşağıdaki lemma, $P_1, P_2, \dots, P_{N_1+N_2}$ noktaları ve bu noktaların bir N_1N_2-otomorfizması altında sıralanışıyla elde edilen $P_{\pi(1)}, P_{\pi(2)}, \dots, P_{\pi(N_1+N_2)}$ noktaları tarafından üretilen GCG kodların aynı olduğunu göstermektedir.

3.1.4. Lemma: Herhangi bir $\pi \in \mathcal{H}_{N_1N_2}(\Phi; \mathrm{G})$ elemanı için $C(\Phi; \mathrm{G}) = C(\pi\Phi; \mathrm{G})$ dır.

Kanıt: Herhangi bir $(z(P_{\pi(1)}, \phi_{\pi(1)}), \dots, z(P_{\pi(N_1+N_2)}, \phi_{\pi(N_1+N_2)})) \in C(\pi\Phi; \mathrm{G})$ elemanı göz önüne alınsın. $z \in \mathcal{L}(G)$ olduğundan $c \coloneqq (z(P_1, \phi_1), \dots, z(P_{N_1+N_2}, \phi_{N_1+N_2})) \in C(\Phi; \mathrm{G})$ elde edilir. $\pi \in \mathcal{H}_{N_1N_2}(\Phi; \mathrm{G})$ olduğundan $\pi(c) \in C(\Phi; \mathrm{G})$ olur. $\pi(c) = (z(P_{\pi(1)}, \phi_{\pi(1)}), \dots, z(P_{\pi(N_1+N_2)}, \phi_{\pi(N_1+N_2)}))$ olduğuna dikkat edilirse $C(\pi\Phi; \mathrm{G}) \subseteq C(\Phi; \mathrm{G})$ olduğu görülür.

3.1.1 Önerme gereğince bu iki vektör uzayının $\mathbb{F}_q$ üzerindeki boyutu aynı olacağından $C(\Phi; \mathrm{G}) = C(\pi\Phi; \mathrm{G})$ olur. ■

2.1.16 Teorem (3) gereğince herhangi bir $\sigma \in \mathrm{Aut}(F \,/\, \mathbb{F}_q)$ otomorfizması en az $2g + 3$ rasyonel noktayı sabitliyorsa birim dönüşümdür. Aşağıdaki teoremde birden büyük olmak üzere aynı dereceden noktaları sabit bırakan bir $\sigma \in \mathrm{Aut}(F \,/\, \mathbb{F}_q)$ otomorfizmasının, hangi şartlar altında birim dönüşüm olduğu ile ilgili bazı sonuçlar verilmiştir.

3.1.5. Teorem: (Spera, 2007, Theorem 3.7) Cinsi g olan bir fonksiyon cismi $F \,/\, \mathbb{F}_q$ göz önüne alınsın. $\{P_1, P_2, \dots, P_N\}$ derecesi $n > 1$ olan ikili olarak birbirinden farklı noktalar olsun. Her $i \in \{1, 2, \dots, N\}$ için (P_i, ϕ_i) ϕ-noktasını sabit bırakan bir otomorfizma $\sigma \in \mathrm{Aut}(F \,/\, \mathbb{F}_q)$, sıradaki koşullardan en az birini sağlıyorsa birim dönüşümdür:

(1) $N - 1 > \frac{16(g+1)^2}{n}$;

(2) $F / \mathbb{F}_q$ fonksiyon cismi en az bir rasyonel noktaya sahiptir ve $N \geq \frac{4g+3}{n}$ eşitsizliği sağlanır;

(3) σ otomorfizması en az bir rasyonel noktayı sabit bırakır ve $N \geq \frac{2g+2}{n}$ eşitsizliği sağlanır.

Şimdi bir $\sigma \in \mathrm{Aut}(F / \mathbb{F}_q)$ otomorfizmasının farklı dereceden noktaları sabit bıraktığı durum göz önüne alınacak ve bu otomorfizmanın hangi koşullar altında birim dönüşüm olduğu araştırılacaktır.

3.1.6. Lemma: (Picone, 2007, Lemma 3.2.6) $F / \mathbb{F}_q$ fonksiyon cisminin bir (P, ϕ_P) ϕ-noktası göz önüne alınsın. Herhangi bir $\sigma \in \mathrm{Aut}(F / \mathbb{F}_q)$ otomorfizması (P, ϕ_P) ϕ-noktasını sabit bırakıyorsa, $v_P(x) \geq 0$ olacak şekildeki her $x \in F$ için $\sigma(x) - x \in P$ dir.

Aşağıdaki teorem bu çalışmanın ilk ana sonucu olup, aynı zamanda bu alt bölümde kanıtlanacak olan ikinci ana teorem için büyük bir öneme sahiptir ve (Spera, 2007, Theorem 3.7)'i genelleştirmektedir.

3.1.7. Teorem: Cinsi g olan bir fonksiyon cismi $F / \mathbb{F}_q$ göz önüne alınsın. $\{P_1, P_2, \dots, P_{N_1}\}$ derecesi n_1 olan ikili olarak birbirinden farklı noktalar ve $\{P_{N_1+1}, P_{N_1+2}, \dots, P_{N_1+N_2}\}$ derecesi n_2 olan ikili olarak birbirinden farklı noktalar olsun. Her $i \in \{1, 2, \dots, N_1 + N_2\}$ için (P_i, ϕ_i) ϕ-noktasını sabit bırakan bir otomorfizma $\sigma \in \mathrm{Aut}(F / \mathbb{F}_q)$, sıradaki koşullardan en az birini sağlıyorsa birim dönüşümdür:

(1) $n_1 N_1 + n_2 N_2 - 4g - 4 > 16(g+1)^2$;

(2) $F / \mathbb{F}_q$ fonksiyon cismi en az bir rasyonel noktaya sahiptir ve $n_1 N_1 + n_2 N_2 - 1 \geq 4g + 3$ eşitsizliği sağlanır;

(3) σ otomorfizması en az bir rasyonel noktayı sabit bırakır ve $n_1 N_1 + n_2 N_2 - 1 \geq 2g + 2$ eşitsizliği sağlanır.

Kanıt: (1) $n \geq 4g + 3$ ise derecesi n olan en az bir nokta vardır (Stichtenoth, 2009, s. 207). P ve P' sırasıyla dereceleri $4g + 3$ ve $4g + 4$ olan noktalar olmak üzere

(Spera, 2007, Theorem 3.7.)'ün kanıtındaki Adım 3 gereğince $F = \mathbb{F}_q(x, y)$, $(x)_\infty = (2g+1)P$ ve $(y)_\infty = 2P'$ olacak şekilde $x, y \in F \setminus \mathbb{F}_q$ elemanları vardır.

$F / \mathbb{F}_q$ fonksiyon cisminin $\Phi = \sum_{i=1}^{N_1+N_2}(P_i, \phi_i)$ ϕ-divizörü ve $\mathrm{D} = \sum_{i=1}^{N_1+N_2} P_i$ divizörü göz önüne alınsın. x ve y elemanları $\operatorname{supp} D$'nin en az $N_1 + N_2 - 1$ elemanında regülerdir. 3.1.6 Lemma gereğince, $\sigma(x) - x$ ve $\sigma(y) - y$ elemanları $\operatorname{supp} D$'de en az $N_1 + N_2 - 1$ köke sahiptir.

Öncelikle $\sigma(x) - x = 0$ olduğu gösterilecektir. $\sigma(x) - x \neq 0$ olduğu varsayılsın. Eğer $P \notin \operatorname{supp} D$ ise $\deg(\sigma(x) - x)_0 \geq n_1 N_1 + n_2 N_2$ olur. Eğer $P \in \operatorname{supp} D$ ise

$$\deg(\sigma(x) - x)_0 \geq n_1 N_1 + n_2 N_2 - 4g - 3 \tag{3.5}$$

olur. Böylece her durumda (3.5)'deki eşitsizlik sağlanır.

Şimdi $\deg(\sigma(x) - x)_\infty$'nin değeri incelenecektir. $v_P(\sigma(x)) = v_{\sigma^{-1}(P)}(x)$ (Wesemeyer, 1997, s. 50) ve değerlendirme tanımı gereğince $v_P(\sigma(x) - x) \geq \min\{v_P(\sigma(x)), v_P(x)\}$ olduğundan, $v_P(\sigma(x) - x) \geq \min\{v_{\sigma^{-1}(P)}(x), v_P(x)\}$ elde edilir.

Eğer $\sigma(P) = P$ ise $v_{\sigma^{-1}(P)}(x) = -(2g+1)$ olur. Böylece $\min\{v_{\sigma^{-1}(P)}(x), v_P(x)\} = -(2g+1)$ elde edilir. Diğer durumda, eğer $\sigma(P) \neq P$ ise $v_{\sigma^{-1}(P)}(x) \geq 0$ olacağından yine $\min\{v_{\sigma^{-1}(P)}(x), v_P(x)\} = -(2g+1)$ elde edilir. Böylece $v_P(\sigma(x) - x) \geq -(2g+1)$ olduğu görülür.

$Q = \sigma(P)$ ve $Q \neq P$ olsun. $v_Q(x) \geq 0$ ve $v_{\sigma^{-1}(Q)}(x) = -(2g+1)$ olduğundan $v_Q(\sigma(x) - x) \geq -(2g+1)$ olur.

Son olarak $Q \neq \sigma(P)$ ve $Q \neq P$ durumunda, $v_Q(x) \geq 0$ ve $v_Q(\sigma(x)) \geq 0$ olduğundan $v_Q(\sigma(x) - x) \geq 0$ olur.

$\sigma(x) - x$ elemanının muhtemel tüm kutupları belirlendiğinden, $(\sigma(x) - x)_\infty \leq (2g+1)P + (2g+1)\sigma(P)$ eşitsizliği sağlanır. Böylece $\deg(\sigma(x) - x)_\infty \leq 2(2g+1)(4g+3) < 16(g+1)^2$ olur. (1) koşulu sağlandığından $\deg(\sigma(x) - x)_\infty < n_1 N_1 + n_2 N_2 - 4g - 4$ elde edilir. Ancak (3.5) eşitsizliği sağlandığından, (Stichtenoth,

2009, Theorem 1.4.11) gereğince bu bir çelişkidir. Sonuç olarak $\sigma(x) - x = 0$ elde edilir.

Şimdi $\sigma(y) - y = 0$ olduğu gösterilecektir. $\sigma(y) - y \neq 0$ olduğu varsayılsın. Eğer $P' \notin \text{supp } D$ ise $\deg(\sigma(y) - y)_0 \geq n_1 N_1 + n_2 N_2$ olur. Eğer $P' \in \text{supp } D$ ise

$$\deg(\sigma(y) - y)_0 \geq n_1 N_1 + n_2 N_2 - 4g - 4 \tag{3.6}$$

olur. Böylece her durumda (3.6)'daki eşitsizlik sağlanır.

$\deg(\sigma(y) - y)_\infty$'nin değeri incelenecektir. $\sigma(P') = P'$ ise $v_{\sigma^{-1}(P')}(y) = -2$ olduğundan $\min\{v_{\sigma^{-1}(P')}(y), v_{P'}(y)\} = -2$ olur. Diğer durumda, $\sigma(P') \neq P'$ ise $v_{\sigma^{-1}(P')}(y) \geq 0$ olduğundan $\min\{v_{\sigma^{-1}(P')}(y), v_{P'}(y)\} = -2$ olur. O halde $v_{P'}(\sigma(y) - y) \geq -2$ olduğu görülür.

$Q = \sigma(P')$ ve $Q \neq P'$ olsun. $v_Q(y) \geq 0$ ve $v_{\sigma^{-1}(Q)}(y) = -2$ olduğundan $v_Q(\sigma(y) - y) \geq -2$ olur.

Son olarak, $Q \neq \sigma(P')$ ve $Q \neq P'$ ise $v_Q(y) \geq 0$ ve $v_Q(\sigma(y)) \geq 0$ olduğundan $v_Q(\sigma(y) - y) \geq 0$ olur.

$\sigma(y) - y$ elemanının muhtemel tüm kutupları belirlendiğinden, $(\sigma(y) - y)_\infty \leq 2P' + 2\sigma(P')$ eşitsizliği sağlanır. Böylece $\deg(\sigma(y) - y)_\infty \leq 2.2.(4g + 4) \leq 16(g + 1)^2$ olur. (1) koşulu sağlandığından $\deg(\sigma(y) - y)_\infty < n_1 N_1 + n_2 N_2 - 4g - 4$ elde edilir. Ancak (3.6) eşitsizliği sağlandığından, (Stichtenoth, 2009, Theorem 1.4.11) gereğince bu bir çelişkidir. Sonuç olarak $\sigma(y) - y = 0$ elde edilir.

$\sigma \in \text{Aut}(F / \mathbb{F}_q)$ otomorfizması $x, y \in F \setminus \mathbb{F}_q$ elemanlarını sabit bıraktığından $F = \mathbb{F}_q(x, y)$ cisminin her elemanını sabit bırakır. Bu nedenle σ birim dönüşümdür.

(2) Q, $F / \mathbb{F}_q$ fonksiyon cisminin herhangi bir rasyonel noktası olsun. (Spera, 2007, Theorem 3.7)'nin kanıtındaki Adım 1 gereğince, $(x)_\infty = 2gQ$ ve $(y)_\infty = (2g + 1)Q$ olacak şekilde $x, y \in F, x \neq 0, y \neq 0$ elemanları vardır. Dahası $(2g, 2g + 1) = 1$ olduğundan (Spera, 2007, Theorem 3.7)'nin kanıtındaki Adım 2 gereğince $F = \mathbb{F}_q(x, y)$ dir.

Eğer $Q \in \operatorname{supp} D$ ise x ve y elemanları $\operatorname{supp} D$'nin $N_1 + N_2 - 1$ elemanında regülerdir. 3.1.6 Lemma gereğince $\sigma(x) - x$ ve $\sigma(y) - y$ elemanları $\operatorname{supp} D$'de $N_1 + N_2 - 1$ köke sahiptir. Ayrıca (2)'de verilen eşitsizlik sağlandığından

$$\deg(\sigma(x) - x)_0 \geq n_1 N_1 + n_2 N_2 - 1 \geq 4g + 3, \tag{3.7}$$

$$\deg(\sigma(y) - y)_0 \geq n_1 N_1 + n_2 N_2 - 1 \geq 4g + 3 \tag{3.8}$$

olur. Eğer $Q \notin \operatorname{supp} D$ ise x ve y elemanları $\operatorname{supp} D$'nin $N_1 + N_2$ elemanında regülerdir. 3.1.6 Lemma gereğince $\sigma(x) - x$ ve $\sigma(y) - y$ elemanları $\operatorname{supp} D$'de $N_1 + N_2$ köke sahiptir. Ayrıca (2)'de verilen eşitsizlik sağlandığından

$$\deg(\sigma(x) - x)_0 \geq n_1 N_1 + n_2 N_2 \geq 4g + 3, \tag{3.9}$$

$$\deg(\sigma(y) - y)_0 \geq n_1 N_1 + n_2 N_2 \geq 4g + 3 \tag{3.10}$$

olur. Bu nedenle her durumda (3.7) ve (3.8)'deki eşitsizliklerin sağlandığı görülür.

Öncelikle $\sigma(x) - x = 0$ olduğu gösterilecektir. $\sigma(x) - x \neq 0$ olduğu varsayılsın. Eğer $\sigma(Q) = Q$ ise $v_{\sigma^{-1}(Q)}(x) = -2g$ olacağından $\min\{v_{\sigma^{-1}(Q)}(x), v_Q(x)\} = -2g$ olur. Diğer durumda, eğer $\sigma(Q) \neq Q$ ise $v_{\sigma^{-1}(Q)}(x) \geq 0$ olacağından $\min\{v_{\sigma^{-1}(Q)}(x), v_Q(x)\} = -2g$ olur. O halde $v_Q(\sigma(x) - x) \geq -2g$ olduğu görülür.

$P' = \sigma(Q)$ ve $P' \neq Q$ olsun. $v_{P'}(x) \geq 0$ ve $v_{\sigma^{-1}(P')}(x) = -2g$ olduğundan $v_{P'}(\sigma(x) - x) \geq -2g$ olur.

$P' \neq \sigma(Q)$ ve $P' \neq Q$ olsun. $v_{P'}(x) \geq 0$ ve $v_{P'}(\sigma(x)) \geq 0$ olduğundan $v_{P'}(\sigma(x) - x) \geq 0$ olur.

$\sigma(x) - x$ elemanının muhtemel tüm kutupları belirlendiğinden, $(\sigma(x) - x)_\infty \leq 2gQ + 2g\sigma(Q)$ eşitsizliği sağlanır. Böylece $\deg(\sigma(x) - x)_\infty \leq 4g$ elde edilir. Ancak (3.7) eşitsizliği sağlandığından, (Stichtenoth, 2009, Theorem 1.4.11) gereğince bu bir çelişkidir. Sonuç olarak $\sigma(x) - x = 0$ elde edilir.

Şimdi $\sigma(y) - y = 0$ olduğu gösterilecektir. $\sigma(y) - y \neq 0$ olduğu varsayılsın. Eğer $\sigma(Q) = Q$ ise $v_{\sigma^{-1}(Q)}(y) = -2g - 1$ olacağından $\min\{v_{\sigma^{-1}(Q)}(y), v_Q(y)\} = -2g - 1$ olur. Diğer durumda, eğer $\sigma(Q) \neq Q$ ise $v_{\sigma^{-1}(Q)}(y) \geq 0$ olacağından

$\min\{v_{\sigma^{-1}(Q)}(y), v_Q(y)\} = -2g-1$ olur. O halde $v_Q(\sigma(y)-y) \geq -2g-1$ olduğu görülür.

$P' = \sigma(Q)$ ve $P' \neq Q$ olsun. $v_{P'}(y) \geq 0$ ve $v_{\sigma^{-1}(P')}(y) = -2g-1$ olduğundan $v_{P'}(\sigma(y)-y) \geq -2g-1$ olur.

Son olarak $P' \neq \sigma(Q)$ ve $P' \neq Q$ durumu göz önüne alınsın. $v_{P'}(y) \geq 0$ ve $v_{P'}(\sigma(y)) \geq 0$ olduğundan $v_{P'}(\sigma(y)-y) \geq 0$ olur.

$\sigma(y)-y$ elemanının muhtemel tüm kutupları belirlenmiştir; o halde $(\sigma(y)-y)_\infty \leq (2g+1)Q + (2g+1)\sigma(Q)$ eşitsizliği sağlanır. Böylece $\deg(\sigma(y)-y)_\infty \leq 4g+2$ elde edilir. Ancak (3.8) eşitsizliği sağlandığından, (Stichtenoth, 2009, Theorem 1.4.11) gereğince bu bir çelişkidir. Dolayısıyla $\sigma(y)-y=0$ elde edilir.

Sonuç olarak $\sigma \in \mathrm{Aut}(F/\mathbb{F}_q)$ otomorfizması $x, y \in F \setminus \mathbb{F}_q$ elemanlarını sabit bıraktığından $F = \mathbb{F}_q(x,y)$ cisminin her elemanını sabit bırakır. Bu nedenle σ birim dönüşümdür.

(3) Q, $F/\mathbb{F}_q$ fonksiyon cisminin $\sigma(Q) = Q$ olacak şekildeki herhangi bir rasyonel noktası olsun. (Spera, 2007, Theorem 3.7)'nin kanıtındaki Adım 1 gereğince, $(x)_\infty = 2gQ$ ve $(y)_\infty = (2g+1)Q$ olacak şekilde $x, y \in F, x \neq 0, y \neq 0$ elemanları vardır. Dahası $(2g, 2g+1) = 1$ olduğundan (Spera, 2007, Theorem 3.7)'nin kanıtındaki Adım 2 gereğince $F = \mathbb{F}_q(x,y)$ dir. (3)'de verilen eşitsizlik sağlandığından (1) ve (2) durumlarına benzer bir şekilde

$$\deg(\sigma(x)-x)_0 \geq 2g+2, \tag{3.11}$$

$$\deg(\sigma(y)-y)_0 \geq 2g+2 \tag{3.12}$$

elde edilir.

Öncelikle $\sigma(x)-x=0$ olduğu gösterilecektir. $\sigma(x)-x \neq 0$ olduğu varsayılsın. $\sigma(Q)=Q$ olduğundan $v_{\sigma^{-1}(Q)}(x) = -2g$ elde edilir. Böylece $\min\{v_{\sigma^{-1}(Q)}(x), v_Q(x)\} = -2g$ olur. O halde $v_Q(\sigma(x)-x) \geq -2g$ eşitsizliği sağlanır.

$P' \neq Q$ durumunda $v_{P'}(x) \geq 0$ ve $v_{P'}(\sigma(x)) \geq 0$ olacağından $v_{P'}(\sigma(x)-x) \geq 0$ elde edilir.

$\sigma(x) - x$ elemanının muhtemel tek kutbu Q olduğundan, $(\sigma(x) - x)_\infty \leq 2gQ$ eşitsizliği sağlanır. Böylece $\deg(\sigma(x) - x)_\infty \leq 2g$ olur. Ancak (3.11) eşitsizliği sağlandığından, (Stichtenoth, 2009, Theorem 1.4.11) gereğince bu bir çelişkidir. Sonuç olarak $\sigma(x) - x = 0$ elde edilir.

Şimdi $\sigma(y) - y = 0$ olduğu gösterilecektir. $\sigma(y) - y \neq 0$ olduğu varsayılsın. $\sigma(Q) = Q$ olduğundan dolayı $v_{\sigma^{-1}(Q)}(y) = -2g - 1$ elde edilir. Dolayısıyla $\min\{v_{\sigma^{-1}(Q)}(y), v_Q(y)\} = -2g - 1$ olur. O halde $v_Q(\sigma(y) - y) \geq -2g - 1$ eşitsizliği sağlanır.

$P' \neq Q$ durumunda $v_{P'}(y) \geq 0$ ve $v_{P'}(\sigma(y)) \geq 0$ olacağından $v_{P'}(\sigma(y) - y) \geq 0$ elde edilir.

$\sigma(y) - y$ elemanının muhtemel tek kutbu Q olduğundan, $(\sigma(y) - y)_\infty \leq (2g + 1)Q$ eşitsizliği sağlanır. Böylece $\deg(\sigma(y) - y)_\infty \leq 2g + 1$ olur. Ancak (3.12) eşitsizliği sağlandığından, (Stichtenoth, 2009, Theorem 1.4.11) gereğince bu bir çelişkidir. Dolayısıyla $\sigma(y) - y = 0$ elde edilir.

Sonuç olarak $\sigma \in \mathrm{Aut}(F / \mathbb{F}_q)$ otomorfizması $x, y \in F \setminus \mathbb{F}_q$ elemanlarını sabit bıraktığından $F = \mathbb{F}_q(x, y)$ cisminin her elemanını sabit bırakır. Bu nedenle σ birim dönüşümdür. ■

Herhangi bir $\sigma \in \mathrm{Aut}(F / \mathbb{F}_q)$ otomorfizması ile aynı zamanda σ yardımıyla (2.10)'da tanımlanan cisim izomorfizması gösterilecektir. Derecesi n olan bir (P, ϕ_P) ϕ-noktası için $\phi_P \sigma^{-1}$ dönüşümü $F_{\sigma(P)}$ cisminden $\mathbb{F}_{q^n}$ cismine tanımlı bir cisim izomorfizmasıdır. Bu nedenle bir $\sigma \in \mathrm{Aut}(F / \mathbb{F}_q)$ otomorfizması için ϕ-noktalarının kümesi üzerinde $\sigma(P, \phi_P) \coloneqq (\sigma(P), \phi_P \sigma^{-1})$ şeklinde bir tanımlama yapılabilir. Bu tanım ϕ-divizör'lerin grubu üzerine $\sigma\left(\sum_{P \in \mathcal{P}_F} n_P (P, \phi_P)\right) \coloneqq \sum_{P \in \mathcal{P}_F} n_P (\sigma(P), \phi_P \sigma^{-1})$ şeklinde genişletilebilir (Spera, 2007).

Bir Φ ϕ-divizörü ve bir G divizörü göz önüne alınsın. $\mathrm{Aut}(F / \mathbb{F}_q)$ grubunun, Φ ϕ-divizörü ve G divizörünü sabitleyen otomorfizmaları bir alt grup oluşturur, bu alt grup $\mathrm{Aut}_{\Phi,\mathrm{G}}(F / \mathbb{F}_q)$ ile gösterilecektir.

$\mathrm{Aut}(F/\mathbb{F}_q)$ grubunu, $C(\Phi;\mathrm{G};\mathrm{n})$ kodunun $\mathcal{H}(\Phi;\mathrm{G};\mathrm{n})$ otomorfizma grubuyla ilişkilendiren bir teorem verilecektir. Bu teorem, $\mathcal{H}(\Phi;\mathrm{G};\mathrm{n})$ grubunun bir alt grubunun $\mathrm{Aut}(F/\mathbb{F}_q)$'ın bazı elemanlarıyla belirlenebileceğini ifade etmektedir. Aşağıdaki teorem en genel haliyle değil, bu çalışmanın sonuçlarının daha kolay anlaşılabilmesini sağlayacak şekliyle verilmiştir.

3.1.8. Teorem: (Spera, 2007, Theorem 3.9) Cinsi g olan bir fonksiyon cismi $F/\mathbb{F}_q$ göz önüne alınsın. $\{P_1, P_2, \dots, P_N\}$ derecesi $n > 1$ olan ikili olarak birbirinden farklı noktalar olsun. $\Phi = \sum_{i=1}^{N}(P_i, \phi_i)$ ϕ-divizörü ve $\mathrm{supp}\, G \cap \{P_1, P_2, \dots, P_N\} = \emptyset$ olacak şekilde bir $G \in \mathrm{Div}(F)$ divizörü göz önüne alınsın.

(1) Bir $\sigma \in \mathrm{Aut}_{\Phi,\mathrm{G}}(F/\mathbb{F}_q)$ otomorfizması $C(\Phi;\mathrm{G};\mathrm{n})$'nin kod sözcükleri üzerinde $x \in \mathcal{L}(G)$ olmak üzere

$$\sigma(x(P_1,\phi_1), \dots, x(P_N,\phi_N)) \coloneqq (x(\sigma(P_1,\phi_1)), \dots, x(\sigma(P_N,\phi_N))) \tag{3.13}$$

şeklinde tanımlansın. O zaman σ, $C(\Phi;\mathrm{G};\mathrm{n})$ kodunun bir n-otomorfizmasıdır.

(2) 3.1.5 Teorem'de verilen (1) ya da (2) koşulu sağlanıyorsa $\mathcal{H}(\Phi;\mathrm{G};\mathrm{n})$ grubu, $\mathrm{Aut}_{\Phi,\mathrm{G}}(F/\mathbb{F}_q)$ grubuna izomorf bir alt grup içerir.

(3) Q bir rasyonel nokta olmak üzere $G = rQ$ ve $2g + 2 \leq nN$ olsun. O zaman $\mathcal{H}(\Phi;\mathrm{G};\mathrm{n})$ grubu, $\mathrm{Aut}_{\Phi,\mathrm{G}}(F/\mathbb{F}_q)$ grubuna izomorf bir alt grup içerir.

Φ_1 ve Φ_2 ϕ-divizörleri ve bir G divizörü göz önüne alınsın. $\mathrm{Aut}(F/\mathbb{F}_q)$ grubunun, Φ_1 ve Φ_2 ϕ-divizörlerini ve G divizörünü sabitleyen otomorfizmaları bir alt grup oluşturur, bu alt grup $\mathrm{Aut}_{\Phi_1,\Phi_2,\mathrm{G}}(F/\mathbb{F}_q)$ ile gösterilecektir.

Şimdi bu çalışmanın ana sonuçlarından biri verilecektir. Aşağıdaki teorem $\mathrm{Aut}(F/\mathbb{F}_q)$ grubunu bir GCG kodun $\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ otomorfizma grubuyla ilişkilendirmektedir; $\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ grubunun bir alt grubunun $\mathrm{Aut}(F/\mathbb{F}_q)$'ın bazı elemanlarıyla belirlenebileceğini ifade etmektedir. Bu teorem, $C(\Phi;\mathrm{G};\mathrm{n})$ kodundan daha genel bir yapıya sahip olan $C(\Phi;\mathrm{G})$ kodu ve dolayısıyla $C(\Phi;\mathrm{G};\mathrm{n})$ kodunun $\mathcal{H}(\Phi;\mathrm{G};\mathrm{n})$ otomorfizma grubundan daha genel bir yapıya sahip olan $C(\Phi;\mathrm{G})$ kodunun $\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ otomorfizma grubu göz önüne alındığından (Spera, 2007, Theorem 3.9)'u genelleştirmektedir.

3.1.9. Teorem: Cinsi g olan bir fonksiyon cismi $F / \mathbb{F}_q$ göz önüne alınsın. $\{P_1, P_2, \dots, P_{N_1}\}$ derecesi n_1 olan ikili olarak birbirinden farklı noktalar ve $\{P_{N_1+1}, P_{N_1+2}, \dots, P_{N_1+N_2}\}$ derecesi n_2 olan ikili olarak birbirinden farklı noktalar olsun. $\Phi = \sum_{i=1}^{N_1+N_2}(P_i, \phi_i)$, $\Phi_1 = \sum_{i=1}^{N_1}(P_i, \phi_i)$, $\Phi_2 = \sum_{i=N_1+1}^{N_1+N_2}(P_i, \phi_i)$ ϕ-divizörleri ve $\operatorname{supp} G \cap \{P_1, P_2, \dots, P_{N_1+N_2}\} = \emptyset$ olacak şekilde bir $G \in \operatorname{Div}(F)$ divizörü göz önüne alınsın.

(1) Bir $\sigma \in \operatorname{Aut}_{\Phi_1,\Phi_2,\mathrm{G}}(F / \mathbb{F}_q)$ otomorfizması $C(\Phi; \mathrm{G})$'nin kod sözcükleri üzerinde $x \in \mathcal{L}(G)$ olmak üzere

$$\sigma(x(P_1, \phi_1), \dots, x(P_{N_1+N_2}, \phi_{N_1+N_2})) := (x(\sigma(P_1, \phi_1)), \dots, x(\sigma(P_{N_1+N_2}, \phi_{N_1+N_2}))) \quad (3.14)$$

şeklinde tanımlansın. O zaman σ, $C(\Phi; \mathrm{G})$ kodunun bir N_1N_2-otomorfizmasıdır.

(2) 3.1.7 Teorem'de verilen (1) ya da (2) koşulu sağlanıyorsa $\mathcal{H}_{N_1N_2}(\Phi; \mathrm{G})$ grubu, $\operatorname{Aut}_{\Phi_1,\Phi_2,\mathrm{G}}(F / \mathbb{F}_q)$ grubuna izomorf bir alt grup içerir.

(3) Q bir rasyonel nokta olmak üzere $G = rQ$ ve $2g + 2 \leq n_1N_1 + n_2N_2 - 1$ olsun. O zaman $\mathcal{H}_{N_1N_2}(\Phi; \mathrm{G})$ grubu, $\operatorname{Aut}_{\Phi_1,\Phi_2,\mathrm{G}}(F / \mathbb{F}_q)$ grubuna izomorf bir alt grup içerir.

Kanıt: (1) σ otomorfizması Φ_1 ve Φ_2 ϕ-divizörlerini sabitlediğinden, $\{(P_1, \phi_1), \dots, (P_{N_1}, \phi_{N_1})\}$ ve $\{(P_{N_1+1}, \phi_{N_1+1}), \dots, (P_{N_1+N_2}, \phi_{N_1+N_2})\}$ kümelerinin bir permütasyonunu oluşturur. Bu nedenle σ'nın bir N_1N_2-otomorfizma olduğunu göstermek için her $x \in \mathcal{L}(G)$ için $(x(\sigma(P_1, \phi_1)), \dots, x(\sigma(P_{N_1+N_2}, \phi_{N_1+N_2}))) \in C(\Phi; \mathrm{G})$ olduğunu göstermek yeterlidir. $\sigma(G) = G$ olduğundan, (Stichtenoth, 2009, s. 291) gereğince $\sigma(\mathcal{L}(G)) = \mathcal{L}(G)$ dır. Bu nedenle, $x = \sigma(y)$ olacak şekilde en az bir $y \in \mathcal{L}(G)$ elemanı vardır.

$\sigma(P_i, \phi_i) = (\sigma(P_i), \phi_i\sigma^{-1})$ olduğuna dikkat edilirse,

$$\begin{aligned}
&(x(\sigma(P_1, \phi_1)), \dots, x(\sigma(P_{N_1+N_2}, \phi_{N_1+N_2}))) = \\
&(x(\sigma(P_1), \phi_1\sigma^{-1}), \dots, x(\sigma(P_{N_1+N_2}), \phi_{N_1+N_2}\sigma^{-1})) = \\
&(\sigma(y)(\sigma(P_1), \phi_1\sigma^{-1}), \dots, \sigma(y)(\sigma(P_{N_1+N_2}), \phi_{N_1+N_2}\sigma^{-1})) \qquad (3.15)
\end{aligned}$$

elde edilir. (2.10) gereğince $\sigma(y(P_i)) = \sigma(y)(\sigma(P_i))$ olduğundan (3.15)'de elde edilen eşitliğin son ifadesinin $(y(P_1, \phi_1), \dots, y(P_{N_1+N_2}, \phi_{N_1+N_2}))$ kod sözcüğüne eşit olduğu görülür. $y \in \mathcal{L}(G)$ olduğundan $(y(P_1, \phi_1), \dots, y(P_{N_1+N_2}, \phi_{N_1+N_2})) \in C(\Phi; \mathrm{G})$ dır.

(2) (1)'de yapılan tanımlamayla $\mathrm{Aut}_{\Phi_1,\Phi_2,\mathrm{G}}(F / \mathbb{F}_q)$ grubundan $\mathcal{H}_{N_1N_2}(\Phi; \mathrm{G})$ grubuna bir homomorfizma elde edilir. Şimdi bu homomorfizmanın birebir olduğu gösterilecektir. Her $x \in \mathcal{L}(G)$ için

$$\sigma(x(P_1, \phi_1), \dots, x(P_{N_1+N_2}, \phi_{N_1+N_2})) = (x(P_1, \phi_1), \dots, x(P_{N_1+N_2}, \phi_{N_1+N_2})) \quad (3.16)$$

olacak şekildeki bir $\sigma \in \mathrm{Aut}_{\Phi_1,\Phi_2,\mathrm{G}}(F / \mathbb{F}_q)$ elemanı göz önüne alınsın. (1)'deki tanımlama kullanılarak

$$(x(\sigma(P_1, \phi_1)), \dots, x(\sigma(P_{N_1+N_2}, \phi_{N_1+N_2}))) = (x(P_1, \phi_1), \dots, x(P_{N_1+N_2}, \phi_{N_1+N_2})) \quad (3.17)$$

elde edilir. O halde her $i \in \{1, 2, \dots, N_1 + N_2\}$ elemanı için $x(\sigma(P_i, \phi_i)) = x(P_i, \phi_i)$ eşitliği sağlanır. Böylece $\sigma(P_i, \phi_i) = (P_i, \phi_i)$ olur.

3.1.7 Teorem gereğince σ birim dönüşümdür. $\mathrm{Aut}_{\Phi_1,\Phi_2,\mathrm{G}}(F / \mathbb{F}_q)$ grubunun farklı elemanları ile $\mathcal{H}_{N_1N_2}(\Phi; \mathrm{G})$ grubunun farklı elemanları elde edildiğinden kanıt tamamlanır.

(3) (2)'ye benzer şekilde, (1)'de yapılan tanımlamayla $\mathrm{Aut}_{\Phi_1,\Phi_2,\mathrm{G}}(F / \mathbb{F}_q)$ grubundan $\mathcal{H}_{N_1N_2}(\Phi; \mathrm{G})$ grubuna elde edilen homomorfizmanın birebir olduğu gösterilecektir. Her $x \in \mathcal{L}(G)$ için

$$\sigma(x(P_1, \phi_1), \dots, x(P_{N_1+N_2}, \phi_{N_1+N_2})) = (x(P_1, \phi_1), \dots, x(P_{N_1+N_2}, \phi_{N_1+N_2})) \quad (3.18)$$

olacak şekildeki bir $\sigma \in \mathrm{Aut}_{\Phi_1,\Phi_2,\mathrm{G}}(F / \mathbb{F}_q)$ elemanı göz önüne alınsın. (2)'de olduğu gibi her $i \in \{1, 2, \dots, N_1 + N_2\}$ için $\sigma(P_i, \phi_i) = (P_i, \phi_i)$ olduğu gösterilebilir.

σ otomorfizması Q rasyonel noktasını sabit bıraktığından ve $2g + 2 \leq n_1N_1 + n_2N_2 - 1$ eşitsizliği sağlandığından, 3.1.7 Teorem gereğince birim dönüşümdür. Böylece kanıt tamamlanır. ■

Bir sonraki alt bölümde, yukarıdaki teorem kullanılarak $\mathcal{H}_{N_1N_2}(\Phi; \mathrm{G})$ grubunun kendisi belirlenecektir.

3.2. Rasyonel Fonksiyon Cismi Durumu

Belli koşullar altında ve ilgili fonksiyon cismi özel olarak seçildiğinde, $\mathrm{Aut}_{\Phi_1,\Phi_2,\mathrm{G}}(F\,/\,\mathbb{F}_q)$ grubu $\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ N_1N_2-otomorfizma grubuna izomorf olabilmektedir. Bu alt bölümde bu durum incelenecektir. 3.1.9 Teorem'de $\mathrm{Aut}_{\Phi_1,\Phi_2,\mathrm{G}}(F\,/\,\mathbb{F}_q)$ grubundan $\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ grubuna bir grup monomorfizması olduğu gösterilmiştir. Bu nedenle, bu dönüşümün örten olduğunu göstermek yeterlidir.

Şimdi keyfi bir fonksiyon cismi $F\,/\,\mathbb{F}_q$ için $\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ grubunun herhangi bir elemanını $\mathrm{Aut}_{\Phi_1,\Phi_2,\mathrm{G}}(F\,/\,\mathbb{F}_q)$ grubunun bir elemanıyla eşlemede kullanışlı olacak bir $\mathbb{F}_q$-lineer dönüşüm tanımlanacaktır.

$\{P_1, P_2, \dots, P_{N_1}\}$ ve $\{P'_1, P'_2, \dots, P'_{N_1}\}$ derecesi n_1 olan ikili olarak birbirinden farklı noktaların iki kümesi olsun. Aynı şekilde, $\{P_{N_1+1}, P_{N_1+2}, \dots, P_{N_1+N_2}\}$ ve $\{P'_{N_1+1}, P'_{N_1+2}, \dots, P'_{N_1+N_2}\}$ derecesi n_2 olan ikili olarak birbirinden farklı noktaların iki kümesi olsun.

$$\Phi = \sum_{i=1}^{N_1+N_2}(P_i, \phi_i) \tag{3.19}$$

ve

$$\Psi = \sum_{i=1}^{N_1+N_2}(P'_i, \psi_i) \tag{3.20}$$

ϕ-divizörleri göz önüne alınsın.

$\mathrm{supp}\ G \cap \{P_1, P_2, \dots, P_{N_1+N_2}\} = \mathrm{supp}\ G \cap \{P'_1, P'_2, \dots, P'_{N_1+N_2}\} = \emptyset$ ve $\deg G < n_1N_1 + n_2N_2$ olacak şekilde bir G divizörü seçilsin. $\deg G < n_1N_1 + n_2N_2$ olduğundan (Stichtenoth, 2009, Corollary 1.4.12) gereğince $\ell(G - D) = 0$ dır. Bu nedenle 3.1.1 Önerme'nin kanıtında tanımlanmış olan ev_Φ ve ev_Ψ lineer dönüşümleri birebirdir. $C(\Phi;\mathrm{G}) = C(\Psi;\mathrm{G})$ olduğu varsayılırsa,

$$\lambda: \mathcal{L}(G) \longrightarrow \mathcal{L}(G),\ \lambda = ev_\Psi{}^{-1}\ o\ ev_\Phi \tag{3.21}$$

şeklinde tanımlı bir $\mathbb{F}_q$-lineer dönüşüm elde edilir. Burada her $z \in \mathcal{L}(G)$ için $\lambda(z) \in \mathcal{L}(G)$ elemanının her $i \in \{1, 2, \dots, N_1 + N_2\}$ için $\lambda(z)(P'_i, \psi_i) = z(P_i, \phi_i)$ olacak şekilde teklikle belirli olduğuna dikkat edilmelidir.

Φ ve Ψ divizörlerinin seçilişinden dolayı yukarıda tanımlanan λ $\mathbb{F}_q$-lineer dönüşümünün, benzer olmasına rağmen (Picone & Spera, 2009, s. 331)'de verilen lineer dönüşümden farklı olduğuna dikkat edilmelidir. Aşağıdaki lemma, (Picone & Spera, 2009, Lemma 3.3)'ün küçük bir düzenlemeyle λ için sağlandığını ve bu lineer dönüşümün bir cisim otomorfizması ile benzer özelliklere sahip olduğunu göstermektedir.

3.2.1. Lemma: G, herhangi bir $F \,/\, \mathbb{F}_q$ fonksiyon cisminin bir divizörü olsun.

(1) Eğer $\deg G < n_1N_1 + n_2N_2$ ve $1 \in \mathcal{L}(G)$ ise $\lambda(1) = 1$ dir.

(2) Eğer $G > 0$ ve $\deg G < \frac{n_1N_1+n_2N_2}{2}$ ise $f,\ g,\ fg \in \mathcal{L}(G)$ olmak üzere $\lambda(fg) = \lambda(f)\lambda(g)$ olur.

(3) Eğer $G > 0$ ve $\deg G < \frac{n_1N_1+n_2N_2}{2}$ ise herhangi bir $k \in \mathbb{Z}$, $k \geq 2$ için $f, f^k \in \mathcal{L}(G)$ olmak üzere $\lambda(f^k) = \lambda(f)^k$ ve $\deg(\lambda(f))_\infty \leq \frac{\deg G}{k}$ olur.

Kanıt: (Picone & Spera, 2009, Lemma 3.3)'ün kanıtına benzer bir şekilde elde edilir. ■

Aşağıdaki lemma, $\mathbb{F}_q(x,y) \,/\, \mathbb{F}_q$ şeklindeki bir fonksiyon cisminin bir (P, ϕ_P) ϕ-noktasının $x(P, \phi_P)$ ve $y(P, \phi_P)$ değerleri tarafından teklikle belirlendiğini göstermektedir. Bu lemma, sıradaki önermenin kanıtı için büyük bir öneme sahiptir.

3.2.2. Lemma: (Picone, 2007, Lemma 3.2.13) $\mathbb{F}_q(x,y) \,/\, \mathbb{F}_q$ şeklindeki bir fonksiyon cisminin iki ϕ-noktası (P_1, ϕ_1) ve (P_2, ϕ_2) göz önüne alınsın. x ve y elemanları P_1 ve P_2 noktalarında regüler olsun. Eğer $x(P_1, \phi_1) = x(P_2, \phi_2)$ ve $y(P_1, \phi_1) = y(P_2, \phi_2)$ ise $(P_1, \phi_1) = (P_2, \phi_2)$ dır.

Aşağıdaki önerme (3.21)'da verilen λ dönüşümünü, $\mathrm{Aut}(F \,/\, \mathbb{F}_q)$ grubunun bir elemanıyla ilişkilendirmektedir.

3.2.3. Önerme: $\mathbb{F}_q(x,y) \,/\, \mathbb{F}_q$ şeklinde bir fonksiyon cismi göz önüne alınsın ve $\sigma \in \mathrm{Aut}(\mathbb{F}_q(x,y) \,/\, \mathbb{F}_q)$ olsun. (3.19) ve (3.20)'de tanımlanan $\Phi = \sum_{i=1}^{N_1+N_2}(P_i, \phi_i)$ ve $\Psi = \sum_{i=1}^{N_1+N_2}(P_i', \psi_i)$ ϕ-divizörleri göz önüne alınsın. $\mathrm{supp}\, G \cap \{P_1, P_2, \dots, P_{N_1+N_2}\} =$

supp $G \cap \{P_1', P_2', \dots, P_{N_1+N_2}'\} = \emptyset$ olacak şekilde bir G divizörü seçilsin. $x,\ y \in \mathcal{L}(G)$ olsun ve $C(\Phi; \mathrm{G}) = C(\Psi; \mathrm{G})$ olduğu varsayılsın.

Eğer $\sigma(G) = G$ ve $\sigma|_{\mathcal{L}(G)} = \lambda$ ise, her $i \in \{1, 2, \dots, N_1 + N_2\}$ için $\sigma(P_i, \phi_i) = (P_i', \psi_i)$ olur.

Kanıt: $\sigma(G) = G$ olduğundan, 3.1.9 Teorem (1)'in kanıtında olduğu gibi $\sigma(\mathcal{L}(G)) = \mathcal{L}(G)$ elde edilir. Bu nedenle, $\sigma|_{\mathcal{L}(G)}: \mathcal{L}(G) \longrightarrow \mathcal{L}(G)$ olur. Dahası, $x \in \mathcal{L}(G)$ olduğundan $x = \lambda(f)$ olacak şekilde en az bir $f \in \mathcal{L}(G)$ elemanı vardır. Bu nedenle her $i \in \{1, 2, \dots, N_1 + N_2\}$ için

$$x(P_i', \psi_i) = \lambda(f)(P_i', \psi_i) = f(P_i, \phi_i) = \phi_i(f(P_i)) = \phi_i\sigma^{-1}(\sigma(f)(\sigma(P_i))) = \sigma(f)(\sigma(P_i), \phi_i\sigma^{-1}) = \lambda(f)(\sigma(P_i), \phi_i\sigma^{-1}) = x(\sigma(P_i), \phi_i\sigma^{-1}) \quad (3.22)$$

elde edilir. Benzer şekilde, her $i \in \{1, 2, \dots, N_1 + N_2\}$ için $y(P_i', \psi_i) = y(\sigma(P_i), \phi_i\sigma^{-1})$ olduğu görülebilir. Böylece 3.2.2 Lemma gereğince her $i \in \{1, 2, \dots, N_1 + N_2\}$ için $(P_i', \psi_i) = (\sigma(P_i), \phi_i\sigma^{-1})$ olacağından, $\sigma(P_i, \phi_i) = (P_i', \psi_i)$ olduğu gösterilmiş olur. ■

Bu alt bölümdeki ana teoremin ve bu bölümdeki diğer alt bölümlerin ana teoremlerinin kanıtı için gerekli olan birkaç lemma verilecektir. Öncelikle cisim genişlemeleri ile ilgili olan bir sonuç verilecektir.

3.2.4. Lemma: (Wesemeyer, 1998, Theorem 2.1) K bir cisim olmak üzere x, K cismi üzerinde transandant bir eleman olsun. Bir y elemanının $K(x)$ üzerindeki minimal polinomu $H(x, y) = 0$ olmak üzere $K(x, y) \,/\, K$ cisim genişlemesi göz önüne alınsın. $\tilde{x}$, $\tilde{y} \in K(x, y) \setminus K$ olmak üzere $H(\tilde{x}, \tilde{y}) = 0$ olsun. O zaman $K(x, y)$ cisminin,

$$\lambda: K(x, y) \,/\, K \longrightarrow K(x, y) \,/\, K,\ f(x, y) \mapsto f(\tilde{x}, \tilde{y}) \quad (3.23)$$

şeklinde tanımlı bir K-endomorfizması vardır. Dahası x ve y elemanları λ dönüşümünün görüntü kümesinde ise λ dönüşümü, $K(x, y) \,/\, K$ cisim genişlemesinin bir otomorfizmasıdır.

Aşağıdaki lemma, belli şartlar altında bir $\sigma \in \mathrm{Aut}(F \,/\, \mathbb{F}_q)$ otomorfizmasının ilgili fonksiyon cisminin bir divizörünün Riemann-Roch uzayını sabit bıraktığında, o divizörün kendisini sabit bıraktığını göstermektedir.

3.2.5. Lemma: (Wesemeyer, 1998, Lemma 2.9) Bir $F / \mathbb{F}_q$ fonksiyon cisminin $\deg G \geq 2g$ olacak şekilde bir $G > 0$ divizörü göz önüne alınsın. Bir $\sigma \in \mathrm{Aut}(F / \mathbb{F}_q)$ otomorfizması için $\sigma(\mathcal{L}(G)) = \mathcal{L}(G)$ ise $\sigma(G) = G$ olur.

Bu aşamadan sonra, bu alt bölüm boyunca $F / \mathbb{F}_q$ bir rasyonel fonksiyon cismi olacaktır.

3.2.6. Lemma: (Picone & Spera, 2009, s. 333) $\mathbb{F}_q(x) / \mathbb{F}_q$ bir rasyonel fonksiyon cismi olsun. $r \in \{0\} \cup \mathbb{Z}^+$, $r_i \in \mathbb{Z}^+$ ve her $i \in \{1, 2, \dots, m\}$ için P_{α_i} bir rasyonel nokta olmak üzere $G = rP_\infty + \sum_{i=1}^{m} r_i P_{\alpha_i}$ divizörü göz önüne alınsın. O zaman

$$B = \{ x^j \mid 0 \leq j \leq r \} \cup \left\{ \frac{1}{(x-\alpha_i)^j} \mid 1 \leq j \leq r_i \text{ ve } 1 \leq i \leq m \right\} \tag{3.24}$$

kümesi, $\mathcal{L}(G)$ Riemann-Roch uzayı için bir tabandır.

3.2.6 Lemma'daki gibi bir G divizörü seçilmesindeki ana sebep, $\mathcal{L}(G)$ Riemann-Roch uzayının bir tabanının belirlenebiliyor olmasıdır.

Aşağıdaki teorem belli şartlar altında, $\mathbb{F}_q(x) / \mathbb{F}_q$ rasyonel fonksiyon cisminin bir ϕ-divizörü Φ ve bir divizörü G olmak üzere, $C(\Phi; \mathrm{G}; \mathrm{n})$ kodunun $\mathcal{H}(\Phi; \mathrm{G}; \mathrm{n})$ otomorfizma grubunun 3.1.8 Teorem'de yapılan tanımlamayla $\mathrm{Aut}_{\Phi,\mathrm{G}}(\mathbb{F}_q(x) / \mathbb{F}_q)$ grubu tarafından belirlendiğini göstermektedir.

3.2.7. Teorem: (Picone & Spera, 2009, Theorem 3.6) $\mathbb{F}_q(x) / \mathbb{F}_q$ bir rasyonel fonksiyon cismi olsun. $\{P_1, P_2, \dots, P_N\}$ derecesi $n > 1$ olan ikili olarak birbirinden farklı noktalar olmak üzere $\Phi = \sum_{i=1}^{N} (P_i, \phi_i)$ ϕ-divizörü göz önüne alınsın. $r \in \{0\} \cup \mathbb{Z}^+$, $r_i \in \mathbb{Z}^+$ ve her $i \in \{1, 2, \dots, m\}$ için P_{α_i} bir rasyonel nokta olmak üzere $G = rP_\infty + \sum_{i=1}^{m} r_i P_{\alpha_i}$ olsun.

Eğer $\deg G < \frac{nN}{2}$ ve $nN \geq 3$ ise, $\mathrm{Aut}_{\Phi,\mathrm{G}}(\mathbb{F}_q(x) / \mathbb{F}_q)$ ve $\mathcal{H}(\Phi; \mathrm{G}; \mathrm{n})$ grupları izomorftur.

Şimdi bu çalışmanın ana sonuçlarından biri verilecektir. Aşağıdaki teorem rasyonel fonksiyon cismi durumunda Φ, Φ_1, Φ_2 ϕ-divizörleri ve G divizörü 3.1.9 Teorem'deki gibi olmak üzere, $C(\Phi; \mathrm{G})$ kodunun $\mathcal{H}_{N_1 N_2}(\Phi; \mathrm{G})$ $N_1 N_2$-otomorfizma grubunun 3.1.9 Teorem'de yapılan tanımlamayla $\mathrm{Aut}_{\Phi_1,\Phi_2,\mathrm{G}}(\mathbb{F}_q(x) / \mathbb{F}_q)$ grubu

tarafından belirlenebileceğini göstermektedir. Bu teorem, GCG kodların ve bu kodların otomorfizma gruplarının alt gruplarının daha büyük bir sınıfı göz önüne alındığından (Picone & Spera, 2009, Theorem 3.6)'yı genelleştirmektedir.

3.2.8. Teorem: $\mathbb{F}_q(x) \,/\, \mathbb{F}_q$ bir rasyonel fonksiyon cismi olsun. $\{P_1, P_2, \dots, P_{N_1}\}$ derecesi n_1 olan ikili olarak birbirinden farklı noktalar ve $\{P_{N_1+1}, P_{N_1+2}, \dots, P_{N_1+N_2}\}$ derecesi n_2 olan ikili olarak birbirinden farklı noktalar olmak üzere $\Phi = \sum_{i=1}^{N_1+N_2}(P_i, \phi_i)$, $\Phi_1 = \sum_{i=1}^{N_1}(P_i, \phi_i)$ ve $\Phi_2 = \sum_{i=N_1+1}^{N_1+N_2}(P_i, \phi_i)$ ϕ-divizörleri göz önüne alınsın. supp $G \cap \{P_1, P_2, \dots, P_{N_1+N_2}\} = \emptyset$, $r \in \{0\} \cup \mathbb{Z}^+$, $r_i \in \mathbb{Z}^+$ ve her $i \in \{1, 2, \dots, m\}$ için P_{α_i} bir rasyonel nokta olmak üzere $G = rP_\infty + \sum_{i=1}^{m} r_i P_{\alpha_i}$ olsun.

Eğer $\deg G < \frac{n_1N_1+n_2N_2}{2}$ ve $n_1N_1 + n_2N_2 \geq 4$ ise, $\mathrm{Aut}_{\Phi_1,\Phi_2,\mathrm{G}}(\mathbb{F}_q(x) \,/\, \mathbb{F}_q)$ ve $\mathcal{H}_{N_1N_2}(\Phi; \mathrm{G})$ grupları izomorftur.

Kanıt: 3.1.9 Teorem gereğince, $\mathcal{H}_{N_1N_2}(\Phi; \mathrm{G})$ grubu $\mathrm{Aut}_{\Phi_1,\Phi_2,\mathrm{G}}(\mathbb{F}_q(x) \,/\, \mathbb{F}_q)$ grubuna izomorf bir alt grup içermektedir. Burada bu alt grubun aslında $\mathcal{H}_{N_1N_2}(\Phi; \mathrm{G})$ grubunun kendisi olduğu gösterilecektir.

Herhangi bir $\pi \in \mathcal{H}_{N_1N_2}(\Phi; \mathrm{G})$ elemanı göz önüne alınsın. 3.1.4 Lemma gereğince $C(\Phi; \mathrm{G}) = C(\pi\Phi; \mathrm{G})$ olur. Bu nedenle (3.21)'de verilen ilgili $\lambda = \lambda_\pi$ dönüşümü göz önüne alınabilir.

3.2.6 Lemma gereğince (3.24)'de verilen B kümesi $\mathcal{L}(G)$ Riemann-Roch uzayı için bir tabandır. 3.2.1 Lemma gereğince her $j \in \{0, 1, \dots, r\}$ için $\lambda(x^j) = \lambda(x)^j$ olur. Yine 3.2.1 Lemma kullanılarak $1 = \lambda(1) = \lambda(\frac{1}{x-\alpha_i}(x - \alpha_i)) = \lambda(\frac{1}{x-\alpha_i})\lambda(x - \alpha_i)$ elde edilir. Böylece $\lambda(\frac{1}{x-\alpha_i}) = \frac{1}{\lambda(x-\alpha_i)} = \frac{1}{\lambda(x)-\alpha_i}$ olur. Dahası, 3.2.1 Lemma gereğince her $j \in \{1, 2, \dots, r_i\}$ elemanı için $\lambda((\frac{1}{x-\alpha_i})^j) = (\frac{1}{\lambda(x)-\alpha_i})^j$ elde edilir. Sonuç olarak, B kümesi $\mathcal{L}(G)$ Riemann-Roch uzayının bir tabanı olduğundan her $h(x) \in \mathcal{L}(G)$ elemanı için $\lambda(h(x)) = h(\lambda(x))$ olduğu gösterilmiş olur.

O halde 3.2.4 Lemma gereğince $\mathbb{F}_q(x) \,/\, \mathbb{F}_q$ fonksiyon cisminin,

$$\tilde{\lambda}\colon \mathbb{F}_q(x) \longrightarrow \mathbb{F}_q(x),\ h(x) \mapsto h(\lambda(x)) \tag{3.25}$$

şeklinde tanımlı bir $\mathbb{F}_q$-endomorfizması vardır. $\tilde{\lambda}$ dönüşümünün $\mathcal{L}(G)$ Riemann-Roch uzayına kısıtlaması λ dir. Dahası, x elemanı λ dönüşümünün görüntüsünde olduğundan $\tilde{\lambda}$ dönüşümünün de görüntüsündedir. Dolayısıyla 3.2.4 Lemma gereğince $\tilde{\lambda} \in \mathrm{Aut}(\mathbb{F}_q(x) \,/\, \mathbb{F}_q)$ olur. Böylece 3.2.5 Lemma gereğince $\tilde{\lambda}(G) = G$ olur.

$\tilde{\lambda}(G) = G$ ve $\tilde{\lambda}|_{\mathcal{L}(G)} = \lambda$ olduğundan, 3.2.3 Önerme gereğince her $i \in \{1, 2, \dots, N_1 + N_2\}$ için $\tilde{\lambda}(P_i, \phi_i) = (P_{\pi(i)}, \phi_{\pi(i)})$ elde edilir. Böylece $\tilde{\lambda}(\Phi_1) = \Phi_1$ ve $\tilde{\lambda}(\Phi_2) = \Phi_2$ olur. Sonuç olarak, her $\pi \in \mathcal{H}_{N_1 N_2}(\Phi; \mathrm{G})$ elemanı bir $\tilde{\lambda} \in \mathrm{Aut}_{\Phi_1, \Phi_2, \mathrm{G}}(\mathbb{F}_q(x) \,/\, \mathbb{F}_q)$ elemanı ile eşleştirildiğinden kanıt tamamlanır. ■

3.2.8 Teorem'in $\mathrm{supp}\, G \cap \{P_1, P_2, \dots, P_{N_1+N_2}\} = \emptyset$ ve $r \in \mathbb{Z}^+$ olmak üzere bir $G = rP_\infty$ divizörü için sağlandığına dikkat edilmelidir.

Bu alt bölümde son olarak elde edilen ana sonuçlar olan 3.1.9 Teorem ve 3.2.8 Teorem, bir örnekle sunulacak ve $N_1 N_2$-otomorfizma grubu $\mathcal{H}_{N_1 N_2}(\Phi; \mathrm{G})$ açık olarak inşa edilecektir.

3.2.9. Örnek: $\mathbb{F}_5(x) \,/\, \mathbb{F}_5$ rasyonel fonksiyon cismi ve $G = 2P_\infty$ divizörü göz önüne alınsın. $i = 1, 2, 3, 4$ için P_i noktası $x - 3^{i-1} \in \mathbb{F}_5[x]$ elemanının kökü olsun. $f(x),\ g(x) \in \mathbb{F}_5[x]$ polinomarı aralarında asal olmak üzere, (Stichtenoth, 2009, Proposition 1.2.1) gereğince $\phi_i\left(\frac{f(x)}{g(x)}(P_i)\right) = \frac{f(3^{i-1})}{g(3^{i-1})}$ olur. Burada P_1, P_2, P_3, P_4 noktalarının derecelerinin bir olduğuna dikkat edilmelidir. $\Phi_1 = \sum_{i=1}^{4}(P_i, \phi_i)$ olsun.

Şimdi

$$p_5(x) = x^5 + 4x^4 + 3x^3 + x^2 + 2x + 3, \tag{3.26}$$

$$p_6(x) = x^5 + 3x^4 + 2x^3 + 3x^2 + 2x + 1, \tag{3.27}$$

$$p_7(x) = x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 4, \tag{3.28}$$

$$p_8(x) = x^5 + x^4 + 3x^3 + 4x^2 + 2x + 2 \tag{3.29}$$

indirgenemez monik polinomlar ve α, $p_5(x)$ polinomunun bir kökü olmak üzere $\mathbb{F}_{5^5} = \mathbb{F}_5(\alpha)$ cismi göz önüne alınsın. Böylece (Stichtenoth, 2009, Proposition 1.2.1) gereğince derecesi 5 olan $P_{p_5(x)}, P_{p_6(x)}, P_{p_7(x)}, P_{p_8(x)}$ noktaları elde edilir. $i = 5, 6, 7, 8$

için $\phi_i\left(\frac{f(x)}{g(x)}\left(P_{p_i(x)}\right)\right)=\frac{f((i-4)\alpha)}{g((i-4)\alpha)}$ olur. $i=5,6,7,8$ için $P_i=P_{p_i(x)}$ olmak üzere $\Phi_2=\sum_{i=5}^{8}(P_i,\phi_i)$ olsun.

$\Phi=\sum_{i=1}^{8}(P_i,\phi_i)$ olmak üzere $C(\Phi;\mathrm{G})$ GCG kodu göz önüne alınsın. 3.1.1 Önerme gereğince $C(\Phi;\mathrm{G})$, $\mathbb{F}_5$ üzerinde $d\geq 6$ olmak üzere bir $[24,3,d]$ koddur. (Spera, 2007, s. 844) gereğince $\mathbb{F}_5(x)\,/\,\mathbb{F}_5$ fonksiyon cisminin Φ_2 ϕ-divizörünü ve G divizörünü sabit bırakan otomorfizmaları, $\sigma_1(x)=2x$, $\sigma_2(x)=4x$, $\sigma_3(x)=3x$ ve $\sigma_4(x)=x$ olmak üzere $\langle\sigma_1\rangle=\{\sigma_1,\sigma_2,\sigma_3,\sigma_4\}$ devirli grubunu oluşturur. Ayrıca Φ_1 ϕ-divizörünün, $\langle\sigma_1\rangle$ grubunun tüm elemanları tarafından sabit bırakıldığı görülebilir. Bu nedenle, $\mathrm{Aut}_{\Phi_1,\Phi_2,\mathrm{G}}(\mathbb{F}_5(x)/\mathbb{F}_5)=\langle\sigma_1\rangle$ olduğu görülür. $\deg G<12$ ve $n_1N_1+n_2N_2=1.4+5.4=24\geq 4$ olduğundan, 3.2.8 Teorem gereğince $\mathrm{Aut}_{\Phi_1,\Phi_2,\mathrm{G}}(\mathbb{F}_5(x)/\mathbb{F}_5)\simeq\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ elde edilir.

$\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ grubunun daha kapsamlı olarak anlaşılabilmesi için σ_1 otomorfizmasının $C(\Phi;\mathrm{G})$ kodunun kod sözcükleri üzerindeki etkisi incelenecektir.

$$\sigma_1(P_1,\phi_1)=(P_2,\phi_2),\sigma_1(P_2,\phi_2)=(P_3,\phi_3),\sigma_1(P_3,\phi_3)=(P_4,\phi_4),\sigma_1(P_4,\phi_4)=$$
$$(P_1,\phi_1),\sigma_1(P_5,\phi_5)=(P_7,\phi_7),\sigma_1(P_6,\phi_6)=(P_5,\phi_5),\sigma_1(P_7,\phi_7)=$$
$$(P_8,\phi_8),\sigma_1(P_8,\phi_8)=(P_6,\phi_6) \qquad (3.30)$$

olduğundan, 3.1.9 Teorem (1)'de yapılan tanımlama gereğince σ_1 otomorfizmasıyla $(1234)(5786)$ permütasyonu elde edilir. Ayrıca σ_2, σ_3 ve σ_4 otomorfizmalarıyla $(13)(24)(58)(67)$, $(5687)(1432)$ ve (1) permütasyonlarının elde edildiği görülebilir. Böylece

$$\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})=\{(1),(1234)(5786),(13)(24)(58)(67),(5687)(1432)\}\simeq\mathbb{Z}_4 \qquad (3.31)$$

olur.

3.3. Hipereliptik Fonksiyon Cismi Durumu

Bu alt bölümde hipereliptik fonksiyon cismi durumunda, bir önceki alt bölüme benzer bir şekilde $\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ N_1N_2-otomorfizma grubunun belirlenebileceği gösterilecektir. Daha açık olarak, $F\,/\,\mathbb{F}_q$ bir hipereliptik fonksiyon cismi olmak üzere

3.1.9 Teorem'de $\mathrm{Aut}_{\Phi_1,\Phi_2,\mathrm{G}}(F\ /\ \mathbb{F}_q)$ grubundan $\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ grubuna tanımlanan grup monomorfizmasının belli şartlar altında örten olduğu gösterilecektir. Eliptik fonksiyon cismi, hipereliptik fonksiyon cisminin özel bir durumu olarak görüldüğünden (Wesemeyer, 1998, s. 630), burada bulunacak sonuçlar eliptik fonksiyon cismi durumunda da geçerli olacaktır.

3.3.1. Tanım: (Stichtenoth, 2009, Definition 6.2.1) Cinsi $g \geq 2$ olan bir $F\ /\ K$ fonksiyon cismine, $[F:K(x)] = 2$ olacak şekilde bir rasyonel alt cisim içeriyorsa K üzerinde bir hipereliptik fonksiyon cismi denir.

Öncelikle hipereliptik fonksiyon cismine ait ön bilgiler verilecektir. Bu alt bölüm boyunca $F\ /\ \mathbb{F}_q$ şeklindeki bir hipereliptik fonksiyon cismi göz önüne alınacak ve kolaylık açısından $\mathrm{char}\ \mathbb{F}_q \neq 2$ olduğu varsayılacaktır.

3.3.2. Önerme: (Wesemeyer, 1997, Proposition 2.6.13) (1) Cinsi g olan bir $F\ /\ \mathbb{F}_q$ hipereliptik fonksiyon cismi göz önüne alınsın. $f(x) \in \mathbb{F}_q[x]$ derecesi $d = 2g + 1$ ya da $d = 2g + 2$ olan karesiz bir polinom olmak üzere, $F = \mathbb{F}_q(x, y)$ ve $y^2 - f(x) = 0$ olacak şekilde $x, y \in F$ elemanları vardır.

(2) Tersine, $f(x) \in \mathbb{F}_q[x]$ derecesi $d \geq 3$ olan karesiz bir polinom olmak üzere $y^2 = f(x)$ ve $F = \mathbb{F}_q(x, y)$ ise, $F\ /\ \mathbb{F}_q$ cinsi

$$g = \begin{cases} (d-1)/2, & d \equiv 1 \pmod 2 \\ (d-2)/2, & d \equiv 0 \pmod 2 \end{cases} \tag{3.32}$$

olan bir hipereliptik fonksiyon cismidir.

(3) $f(x) \in \mathbb{F}_q[x]$ derecesi $d = 2g + 1$ ya da $d = 2g + 2$ olmak üzere karesiz bir polinom, $F = \mathbb{F}_q(x, y)$ ve $y^2 = f(x)$ olsun. $F\ /\ \mathbb{F}_q(x)$ fonksiyon cisim genişlemesinde dallanmış noktalar $P \in \mathcal{P}_{\mathbb{F}_q(x)}$, $\deg f(x) \equiv 0 \pmod 2$ ise $f(x)$ polinomunun tüm kökleri, $\deg f(x) \equiv 1 \pmod 2$ ise $f(x)$ polinomunun tüm kökleri ve x elemanının kutbudur.

Bir önceki alt bölümde bir $C(\Phi;\mathrm{G})$ kodunun $\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ N_1N_2-otomorfizma grubunu belirlerken en önemli aşamalardan birinin (3.21)'de tanımlanan λ lineer

dönüşümünün, bir $\mathbb{F}_q(x) \,/\, \mathbb{F}_q$ rasyonel fonksiyon cisminin bir G divizörünün Riemann-Roch uzayı üzerinde her $h(x) \in \mathcal{L}(G)$ elemanı için $\lambda(h(x)) = h(\lambda(x))$ özelliğini sağlaması olduğu görülmüştü. Bu alt bölümde, buna benzer bir özelliğin bir $F \,/\, \mathbb{F}_q$ hipereliptik fonksiyon cisminin bir G divizörünün Riemann-Roch uzayı üzerinde sağlandığı gösterilecektir. Bu amaçla bir önceki alt bölümde olduğu gibi, uygun bir G divizörünün bir tabanı verilecektir. Bundan sonraki kısımda böyle bir G divizörünün tabanını belirtmek için gerekli olan, hipereliptik fonksiyon cismine ait bazı sonuçlar verilecektir.

Aşağıdaki önerme bir $\mathbb{F}_q(x, y) \,/\, \mathbb{F}_q$ hipereliptik fonksiyon cisminin x ve y üreteç elemanlarının tüm farklı durumlardaki kutup divizörlerini sunmaktadır.

3.3.3. Önerme: (Picone, 2007, Proposition 2.2.11) Bir hipereliptik fonksiyon cismi $F \,/\, \mathbb{F}_q$ göz önüne alınsın. $f(x) \in \mathbb{F}_q[x]$ derecesi $d = 2g + 1$ ya da $d = 2g + 2$ olmak üzere karesiz bir polinom, $F = \mathbb{F}_q(x, y)$ ve $y^2 = f(x)$ olsun.

x elemanının kutbu P_∞ üzerine uzanan nokta (ya da noktalar) Q_∞ (ya da parçalanmış durumda $Q_{\infty,1}$ ve $Q_{\infty,2}$) ile gösterilmek üzere,

$$(x)_\infty = \begin{cases} 2Q_\infty, & \text{x in kutbu } F/\mathbb{F}_q(x) \text{ da dallanmışsa} \\ Q_{\infty,1} + Q_{\infty,2}, & \text{x in kutbu } F/\mathbb{F}_q(x) \text{ da parçalanmışsa} \\ Q_\infty, & \text{x in kutbu } F/\mathbb{F}_q(x) \text{ da durağansa} \end{cases} \tag{3.33}$$

ve

$$(y)_\infty = \begin{cases} dQ_\infty, & \text{x in kutbu } F/\mathbb{F}_q(x) \text{ da dallanmışsa} \\ \frac{d}{2}Q_{\infty,1} + Q_{\infty,2}, & \text{x in kutbu } F/\mathbb{F}_q(x) \text{ da parçalanmışsa} \\ \frac{d}{2}Q_\infty, & \text{x in kutbu } F/\mathbb{F}_q(x) \text{ da durağansa} \end{cases} \tag{3.34}$$

olur.

Şimdi $F \,/\, \mathbb{F}_q$ hipereliptik fonksiyon cisminin bir divizörü ve bu divizör yardımıyla tanımlanan ve bu alt bölüm boyunca kullanılacak olan birkaç nokta kümesi tanımlanacaktır.

$$D_\infty := \begin{cases} Q_\infty, & \text{x in kutbu } F/\mathbb{F}_q(x) \text{ da dallanmışsa} \\ Q_{\infty,1} + Q_{\infty,2}, & \text{x in kutbu } F/\mathbb{F}_q(x) \text{ da parçalanmışsa} \\ Q_\infty, & \text{x in kutbu } F/\mathbb{F}_q(x) \text{ da durağansa.} \end{cases} \tag{3.35}$$

İlk durumda $d \equiv 1 \pmod 2$ olup D_∞ divizörünün derecesi 1, diğer iki durumda $d \equiv 0 \pmod 2$ olup D_∞ divizörünün derecesi 2'dir (Wesemeyer, 1998, s. 633).

$F \,/\, \mathbb{F}_q$ hipereliptik fonksiyon cismindeki derecesi bir olan tüm noktaların kümesi $\mathcal{P}_F^{(1)}$ olmak üzere

$$H(\mathbb{F}_q) \coloneqq \mathcal{P}_F^{(1)} \cup \text{supp}\,(D_\infty), \tag{3.36}$$

$$H_r(\mathbb{F}_q) \coloneqq \{\, P \in H(\mathbb{F}_q) \setminus \text{supp}\,(D_\infty) \mid P, F/\mathbb{F}_q(x) \text{ da dallanmışsa} \,\}, \tag{3.37}$$

$$H_s(\mathbb{F}_q) \coloneqq \{\, P \in H(\mathbb{F}_q) \setminus \text{supp}\,(D_\infty) \mid P, F/\mathbb{F}_q(x) \text{ da parçalanmışsa} \,\}. \tag{3.38}$$

Her $P \in \mathcal{P}_F^{(1)}$ için $x_P \coloneqq x(P)$ ve $y_P \coloneqq y(P)$ olsun. P bir rasyonel nokta olduğundan $x_P, y_P \in \mathbb{F}_q$ olduğuna dikkat edilmelidir. P noktası x_P ve y_P elemanları tarafından teklikle belirlendiğinden (Wesemeyer, 1998, s. 634), $P = (x_P, y_P)$ şeklinde bir tanımlama yapılabilir. $\bar{P}$ ile herhangi bir $P \in \mathcal{P}_F{}^{(1)}$ noktasının, $F/\mathbb{F}_q(x)$ cisim genişlemesinin $\xi(x) = x$ ve $\xi(y) = -y$ ile tanımlı aşikar olmayan ξ otomorfizmasına göre eşleneği $\xi(P)$ gösterilsin. Bu durumda $\bar{P} = (x_P, -y_P)$ olur.

Aşağıdaki lemma $x - x_P$ elemanının tüm farklı durumlardaki esas divizörünü sunmaktadır.

3.3.4. Lemma: (Picone, 2007, Lemma 2.2.12) $F \,/\, \mathbb{F}_q$ bir hipereliptik fonksiyon cismi olsun.

(1) $P \in H_r(\mathbb{F}_q)$ için

$$(x - x_P) = \begin{cases} 2P - 2D_\infty, & d \equiv 1 \pmod 2 \\ 2P - D_\infty, & d \equiv 0 \pmod 2 \end{cases} \tag{3.39}$$

olur.

(2) $P \in H_s(\mathbb{F}_q)$ için

$$(x - x_P) = \begin{cases} P + \bar{P} - 2D_\infty, & d \equiv 1 \pmod 2 \\ P + \bar{P} - D_\infty, & d \equiv 0 \pmod 2 \end{cases} \tag{3.40}$$

olur.

Aşağıdaki lemmada, bir $F\ /\ \mathbb{F}_q$ hipereliptik fonksiyon cisminin bu alt bölümün amaçlarına uygun bir G divizörünün, Riemann-Roch uzayının bir tabanını verebilmek için bazı elemanlar tanımlanmış ve bu elemanların özellikleri verilmiştir.

3.3.5. Lemma: (Picone, 2007, Lemma 2.2.13) $F\ /\ \mathbb{F}_q$ bir hipereliptik fonksiyon cismi olsun. Bir $P=(x_P,y_P)\in H_s(\mathbb{F}_q)$ elemanı göz alınsın. O zaman her $1\le i\le \left[\frac{d+1}{2}\right]=g+1$ elemanı için $\deg h_i(x)\le i-1$, $v_P(y-h_i(x))\ge i$ ve $v_{\bar{P}}(y-h_i(x))=0$ olacak şekilde bir $h_i(x)\in\mathbb{F}_q[x]$ polinomu vardır. Dahası $g_{i\bar{P}}:=\frac{y-h_i(x)}{(x-x_P)^i}$ olmak üzere, $v_{\bar{P}}(g_{i\bar{P}})=-i$ ve

$$v_\infty(g_{i\bar{P}})\ge\begin{cases}-(2g+1-2i), & d\equiv 1\ (\mathrm{mod}\ 2)\\ -(g+1-i), & d\equiv 0\ (\mathrm{mod}\ 2)\end{cases} \tag{3.41}$$

olur. Burada, x elemanının kutbu $F/\mathbb{F}_q(x)$'de dallanmışsa ya da durağansa $v_\infty=v_{Q_\infty}$ olur. Eğer x elemanının kutbu $F/\mathbb{F}_q(x)$'de parçalanmışsa v_∞, $v_{Q_{\infty,1}}$ ya da $v_{Q_{\infty,2}}$ değerlendirmesini temsil eder. Ayrıca $g_{0\bar{P}}:=1$ olarak tanımlanacaktır.

3.3.6. Önerme: (Wesemeyer, 1997, Proposition 5.2.6) $F\ /\ \mathbb{F}_q$ bir hipereliptik fonksiyon cismi ve $J\subseteq\mathcal{P}_F^{(1)}\setminus \mathrm{supp}\ (D_\infty)$ olsun. Her $Q\in J$ için $n_Q\ge 1$ ve

$$n_\infty\ge\begin{cases}2g+2, & d\equiv 1\ (\mathrm{mod}\ 2)\\ g+1, & d\equiv 0\ (\mathrm{mod}\ 2)\end{cases} \tag{3.42}$$

olmak üzere $G=n_\infty D_\infty+\sum_{Q\in J}n_Q Q$ divizörü göz önüne alınsın. Bu durumda $m:=g+1$ olmak üzere G divizörünün Riemann-Roch uzayının $\mathcal{L}(G)$ bir tabanı aşağıdaki elemanlarla verilebilir:

$$B=\{\,x^\alpha y^\beta\mid \alpha\ge 0,\ \beta\in\{0,1\}\text{ ve }x^\alpha y^\beta\in\mathcal{L}(n_\infty D_\infty)\,\}\cup\left\{\left(\frac{1}{x-x_Q}\right)^\alpha\left(\frac{y}{x-x_Q}\right)^\beta\mid 2\alpha+\beta\le n_Q,\alpha\ge 0,\beta\in\{0,1\}\text{ ve }Q\in J\cap H_r(\mathbb{F}_q)\right\}\cup\{\,(g_{mQ})^\alpha(g_{\beta Q})\mid m\alpha+\beta\le n_Q,\alpha\ge 0,0\le\beta<m\text{ ve }Q\in J\cap H_s(\mathbb{F}_q)\,\}. \tag{3.43}$$

Aşağıdaki teorem belli şartlar altında, $F\ /\ \mathbb{F}_q$ hipereliptik fonksiyon cisminin bir ϕ-divizörü Φ ve bir divizörü G olmak üzere, $C(\Phi;\mathrm{G};\mathrm{n})$ kodunun $\mathcal{H}(\Phi;\mathrm{G};\mathrm{n})$

otomorfizma grubunun 3.1.8 Teorem'de yapılan tanımlamayla $\mathrm{Aut}_{\Phi,\mathrm{G}}(F\,/\,\mathbb{F}_q)$ grubu tarafından belirlendiğini göstermektedir.

3.3.7. Teorem: (Picone & Spera, 2009, Theorem 3.5) $F\,/\,\mathbb{F}_q$ bir hipereliptik fonksiyon cismi olsun ve 3.3.6 Önerme'de verilen G divizörü göz önüne alınsın. $\{P_1, P_2, \dots, P_N\}$ derecesi $n > 1$ olan ve $\mathrm{supp}\, G \cap \{P_1, P_2, \dots, P_N\} = \emptyset$ olacak şekildeki ikili olarak birbirinden farklı noktalar olmak üzere $\Phi = \sum_{i=1}^{N}(P_i, \phi_i)$ ϕ-divizörü göz önüne alınsın. Eğer $\deg G < \frac{nN}{2}$ ve

(1) $nN > 16(g+1)^2 + n$;

(2) $F\,/\,\mathbb{F}_q$ en az bir rasyonel noktaya sahiptir ve $nN \geq 4g + 3$ eşitsizliği sağlanır.

koşullarından biri sağlanıyorsa $\mathrm{Aut}_{\Phi,\mathrm{G}}(F\,/\,\mathbb{F}_q)$ ve $\mathcal{H}(\Phi; \mathrm{G}; \mathrm{n})$ grupları izomorftur.

$\{P_1, P_2, \dots, P_{N_1}\}$ derecesi n_1 olan ikili olarak birbirinden farklı noktalar ve $\{P_{N_1+1}, P_{N_1+2}, \dots, P_{N_1+N_2}\}$ derecesi n_2 olan ikili olarak birbirinden farklı noktalar olsun. Aşağıdaki lemma, belli özelliklere sahip bir divizörün Riemann-Roch uzayından alınan iki elemanın, her $i \in \{1, 2, \dots, N_1 + N_2\}$ için P_i noktasının rezidü cisminde karşılık gelen denklik sınıflarının eşit olması halinde bu iki elemanın eşit olduğunu göstermektedir ve bu alt bölümdeki ana teorem için büyük bir öneme sahiptir. Bu lemma, herhangi bir fonksiyon cismi $F\,/\,\mathbb{F}_q$ için geçerlidir.

3.3.8. Lemma: $G_0, G_1 \geq 0$ olmak üzere herhangi bir divizör $G = G_0 - G_1$ göz önüne alınsın ve $u, v \in \mathcal{L}(G)$ olsun. $\deg G_0 < n_1N_1 + n_2N_2$ ve $\{P_1, P_2, \dots, P_{N_1+N_2}\}$ noktaları yukarıdaki gibi olmak üzere $\mathrm{supp}\, G_0 \cap \{P_1, P_2, \dots, P_{N_1+N_2}\} = \emptyset$ olsun. Her $i \in \{1, 2, \dots, N_1 + N_2\}$ için $u(P_i, \phi_i) = v(P_i, \phi_i)$ ise $u = v$ dir.

Kanıt: (Wesemeyer, 1997, Lemma 4.3.5)'in kanıtına benzer bir şekilde görülecektir. $u \neq v$ olsun. $u - v \in \mathcal{L}(G)$ olduğundan $(u-v) = (u-v)_0 - (u-v)_\infty \geq -G_0 + G_1$ olur. Böylece $(u-v)_\infty \leq G_0$ ve dolayısıyla $\deg (u-v)_\infty \leq \deg G_0 < n_1N_1 + n_2N_2$ elde edilir.

Diğer yandan her $i \in \{1, 2, \dots, N_1 + N_2\}$ için $u(P_i, \phi_i) = v(P_i, \phi_i)$ olduğundan $(u-v)(P_i, \phi_i) = 0$ olur. Burada $\mathrm{supp}\, G_0 \cap \{P_1, P_2, \dots, P_{N_1+N_2}\}$ olduğundan P_i

noktasının rezidü cisminin $(u-v)(P_i,\phi_i)$ elemanının tanımlı olduğuna dikkat edilmelidir. Dolayısıyla $\phi_i(u-v+P_i)=0$ olur. ϕ_i bir cisim izomorfizması olduğundan her $i\in\{1,2,\dots,N_1+N_2\}$ için $u-v\in P_i$ olur. Bu nedenle $u-v$ elemanının en az N_1+N_2 kökü vardır. Dolayısıyla $\deg(u-v)_0\geq n_1N_1+n_2N_2$ olur. (Stichtenoth, 2009, Theorem 1.4.11) gereğince çelişki elde edileceğinden $u=v$ dir. ■

Şimdi bu çalışmanın ana sonuçlarından biri verilecektir. Aşağıdaki teorem hipereliptik fonksiyon cismi durumunda Φ, Φ_1, Φ_2 ϕ-divizörleri 3.1.9 Teorem'deki gibi olmak üzere bazı ek koşullar altında, $C(\Phi;\mathrm{G})$ kodunun $\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ N_1N_2-otomorfizma grubunun 3.1.9 Teorem'de yapılan tanımlamayla $\mathrm{Aut}_{\Phi_1,\Phi_2,\mathrm{G}}(F/\mathbb{F}_q)$ grubu tarafından belirlenebileceğini göstermektedir. Bu teorem, hipereliptik fonksiyon cismi durumunda GCG kodların ve bu kodların otomorfizma gruplarının alt gruplarının daha büyük bir sınıfı göz önüne alındığından (Picone & Spera, 2009, Theorem 3.5)'i genelleştirmektedir.

3.3.9. Teorem: $F/\mathbb{F}_q$ bir hipereliptik fonksiyon cismi olsun ve 3.3.6 Önerme'de verilen G divizörü göz önüne alınsın. $\{P_1,P_2,\dots,P_{N_1}\}$ derecesi n_1 olan ikili olarak birbirinden farklı noktalar, $\{P_{N_1+1},P_{N_1+2},\dots,P_{N_1+N_2}\}$ derecesi n_2 olan ikili olarak birbirinden farklı noktalar ve $\mathrm{supp}\,G\cap\{P_1,P_2,\dots,P_{N_1+N_2}\}=\emptyset$ olmak üzere $\Phi=\sum_{i=1}^{N_1+N_2}(P_i,\phi_i)$, $\Phi_1=\sum_{i=1}^{N_1}(P_i,\phi_i)$ ve $\Phi_2=\sum_{i=N_1+1}^{N_1+N_2}(P_i,\phi_i)$ ϕ-divizörleri göz önüne alınsın. Eğer $\deg G<\frac{n_1N_1+n_2N_2}{2}$ ve

(1) $n_1N_1+n_2N_2-4g-4>16(g+1)^2$;

(2) $F/\mathbb{F}_q$ en az bir rasyonel noktaya sahiptir ve $n_1N_1+n_2N_2-1\geq 4g+3$ eşitsizliği sağlanır.

koşullarından biri sağlanıyorsa $\mathrm{Aut}_{\Phi_1,\Phi_2,\mathrm{G}}(F/\mathbb{F}_q)$ ve $\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ grupları izomorftur.

Kanıt: 3.2.8 Teorem'in kanıtına benzer bir şekilde $\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ grubunun her elemanı, $\mathrm{Aut}_{\Phi_1,\Phi_2,\mathrm{G}}(F/\mathbb{F}_q)$ grubunun en az bir elemanı ile eşleştirilecektir. Herhangi bir $\pi\in\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ elemanı için yine 3.2.8 Teorem'in kanıtında olduğu gibi ilgili $\lambda=\lambda_\pi$ dönüşümü göz önüne alınsın. Öncelikle her $h(x,y)\in\mathcal{L}(G)$ elemanının $\lambda(h(x,y))=h(\lambda(x),\lambda(y))$ özelliğini sağladığı gösterilecektir.

3.2.1 Lemma gereğince $x^{\alpha}y^{\beta} \in \mathcal{L}(G)$ için $\lambda(x^{\alpha}y^{\beta}) = \lambda(x)^{\alpha}\lambda(y)^{\beta}$ olur. Dahası, yine 3.2.1 Lemma kullanılarak $1 = \lambda(1) = \lambda\left(\frac{1}{x-x_Q}(x-x_Q)\right) = \lambda\left(\frac{1}{x-x_Q}\right)\lambda(x-x_Q) = \lambda\left(\frac{1}{x-x_Q}\right)(\lambda(x)-x_Q)$ elde edilir. Böylece $\lambda\left(\frac{1}{x-x_Q}\right) = \frac{1}{\lambda(x)-x_Q}$ olur. Benzer şekilde $\lambda\left(\frac{y}{x-x_Q}\right) = \lambda(y)\lambda\left(\frac{1}{x-x_Q}\right) = \frac{\lambda(y)}{\lambda(x)-x_Q}$ bulunur. O halde $2\alpha+\beta \leq n_Q$, $\alpha \geq 0$, $\beta \in \{0,1\}$ ve $Q \in J \cap H_r(\mathbb{F}_q)$ için $\lambda\left(\left(\frac{1}{x-x_Q}\right)^{\alpha}\left(\frac{y}{x-x_Q}\right)^{\beta}\right) = \left(\frac{1}{\lambda(x)-x_Q}\right)^{\alpha}\left(\frac{\lambda(y)}{\lambda(x)-x_Q}\right)^{\beta}$ bulunur.

Son olarak, herhangi bir $Q \in J \cap H_s(\mathbb{F}_q)$ noktası göz önüne alınsın. O zaman 3.3.5 Lemma gereğince her $1 \leq i \leq \min\{n_Q, g+1\}$ için 3.3.5 Lemma'daki özellikleri sağlayan bir $p_i(x) \in \mathbb{F}_q[x]$ polinomu vardır. (Wesemeyer, 1998, s. 636) gereğince $(x-x_Q)^i,\ y-p_i(x) \in \mathcal{L}(G)$ olduğundan, 3.2.1 Lemma gereğince $\lambda((x-x_Q)^i) = (\lambda(x-x_Q))^i = (\lambda(x)-x_Q)^i$ ve $\lambda(y-p_i(x)) = \lambda(y)-p_i(\lambda(x))$ olur. Ayrıca, $x_Q = x_{\bar{Q}}$ olduğundan $g_{iQ} = \frac{y-p_i(x)}{(x-x_Q)^i}$ yazılabilir. Bu nedenle $\lambda(g_{iQ}) = \frac{\lambda(y-p_i(x))}{\lambda((x-x_Q)^i)} = \frac{\lambda(y)-p_i(\lambda(x))}{(\lambda(x)-x_Q)^i}$ olacağından, 3.2.1 Lemma gereğince $m\alpha+\beta \leq n_Q,\ \alpha \geq 0,\ 0 \leq \beta < m$ ve $Q \in J \cap H_s(\mathbb{F}_q)$ için $\lambda\left(\left(g_{mQ}\right)^{\alpha}\left(g_{\beta Q}\right)\right) = \left(\frac{\lambda(y)-p_m(\lambda(x))}{(\lambda(x)-x_Q)^m}\right)^{\alpha}\left(\frac{\lambda(y)-p_\beta(\lambda(x))}{(\lambda(x)-x_Q)^\beta}\right)$ olur.

Sonuç olarak, her $h(x,y) \in \mathcal{L}(G)$ elemanı yukarıdaki elemanların bir lineer kombinasyonu olarak yazılabileceğinden $\lambda(h(x,y)) = h(\lambda(x),\lambda(y))$ olduğu kanıtlanmış olur.

Şimdi $f(x) \in \mathbb{F}_q[x]$ polinomu 3.3.2 Önerme (1)'deki gibi olmak üzere $\lambda(x)$ ve $\lambda(y)$ elemanlarının $(\lambda(y))^2 - f(\lambda(x)) = 0$ denklemini sağladığı gösterilecektir. Bu amaçla öncelikle $\lambda(y)^2,\ f(\lambda(x)) \in \mathcal{L}(2G)$ olduğu gösterilecektir. $x \in \mathcal{L}(G)$ ve (Wesemeyer, 1998, s. 636) gereğince $\deg f(x) = d$ olmak üzere $x^{\left\lfloor\frac{d+1}{2}\right\rfloor} \in \mathcal{L}(G)$ dır. $\left\lfloor\frac{d+1}{2}\right\rfloor = g+1$ olduğuna dikkat edilirse, 3.2.1 Lemma gereğince $\lambda(x^{g+1}) = \lambda(x)^{g+1}$ olacağından $\lambda(x)^{g+1} \in \mathcal{L}(G)$ elde edilir. $\frac{d}{2} \leq g+1$ olduğundan Riemann-Roch uzayı tanımı gereğince $\lambda(x)^d \in \mathcal{L}(2G)$ olur. Böylece $f(\lambda(x)) \in \mathcal{L}(2G)$ bulunur. $\lambda(y)^2 \in$

$\mathcal{L}(2G)$ olduğu gösterilecektir. $y \in \mathcal{L}(G)$ olduğundan $\lambda(y) \in \mathcal{L}(G)$ dir. Bu nedenle $(\lambda(y)) = (\lambda(y))_0 - (\lambda(y))_\infty \geq -G$ olacağından, $G > 0$ olduğu göz önünde bulundurulursa $-(\lambda(y))_\infty \geq -G$ elde edilir. Dolayısıyla $-(\lambda(y)^2)_\infty \geq -2G$ bulunur. Böylece $\lambda(y)^2 \in \mathcal{L}(2G)$ olduğu görülür.

Her $i \in \{1, 2, \dots, N_1 + N_2\}$ için $\lambda(y)^2(P_i, \phi_i) = f(\lambda(x))(P_i, \phi_i)$ olduğu gösterilecektir.

$$\lambda(y)^2\left(P_{\pi(i)}, \phi_{\pi(i)}\right) = \phi_{\pi(i)}\left(\lambda(y)^2\left(P_{\pi(i)}\right)\right) = \phi_{\pi(i)}\left(\left(\lambda(y)\left(P_{\pi(i)}\right)\right)^2\right) =$$

$$\left(\phi_{\pi(i)}\left(\lambda(y)\left(P_{\pi(i)}\right)\right)\right)^2 = \left(\lambda(y)\left(P_{\pi(i)}, \phi_{\pi(i)}\right)\right)^2 = \left(y(P_i, \phi_i)\right)^2 = y^2(P_i, \phi_i) =$$

$$f(x)(P_i, \phi_i) = \phi_i\left(f(x)(P_i)\right) = \phi_i\left(f\left(x(P_i)\right)\right) = f\left(\phi_i\left(x(P_i)\right)\right) = f\left(x(P_i, \phi_i)\right) =$$

$$f\left(\lambda(x)\left(P_{\pi(i)}, \phi_{\pi(i)}\right)\right) = f\left(\phi_{\pi(i)}\left(\lambda(x)\left(P_{\pi(i)}\right)\right)\right) = \phi_{\pi(i)}\left(f\left(\lambda(x)\left(P_{\pi(i)}\right)\right)\right) =$$

$$\phi_{\pi(i)}\left(f\left(\lambda(x)\right)\left(P_{\pi(i)}\right)\right) = f\left(\lambda(x)\right)\left(P_{\pi(i)}, \phi_{\pi(i)}\right) \tag{3.44}$$

ve $\deg G < \frac{n_1 N_1 + n_2 N_2}{2}$ olduğundan 3.3.8 Lemma gereğince $\lambda(y)^2 = f(\lambda(x))$ elde edilir.

O halde 3.2.4 Lemma gereğince $F \,/\, \mathbb{F}_q$ hipereliptik fonksiyon cisminin,

$$\tilde{\lambda}: F \longrightarrow F,\ h(x, y) \mapsto h(\lambda(x), \lambda(y)) \tag{3.45}$$

şeklinde tanımlı bir $\mathbb{F}_q$-endomorfizması vardır. $\tilde{\lambda}$ dönüşümünün $\mathcal{L}(G)$ uzayına kısıtlaması λ dönüşümü ile çakışmaktadır. x ve y elemanları λ dönüşümünün görüntüsünde olduğundan $\tilde{\lambda}$ dönüşümünün de görüntüsündedir. Dolayısıyla 3.2.4 Lemma gereğince $\tilde{\lambda}$ dönüşümü $F \,/\, \mathbb{F}_q$ hipereliptik fonksiyon cisminin bir otomorfizmasıdır. 3.2.5 Lemma gereğince $\tilde{\lambda}(G) = G$ olur.

Ayrıca 3.2.3 Önerme gereğince, $\tilde{\lambda}(G) = G$ ve $\tilde{\lambda}|_{\mathcal{L}(G)} = \lambda$ olduğundan her $i \in \{1, 2, \dots, N_1 + N_2\}$ için $\tilde{\lambda}(P_i, \phi_i) = (P_{\pi(i)}, \phi_{\pi(i)})$ olur. Bu nedenle $\pi \in \mathcal{H}_{N_1 N_2}(\Phi; \mathrm{G})$ elemanının tanımlanışı gereğince $\tilde{\lambda}(\Phi_1) = \Phi_1$ ve $\tilde{\lambda}(\Phi_2) = \Phi_2$ elde edilir. Sonuç olarak, her $\pi \in \mathcal{H}_{N_1 N_2}(\Phi; \mathrm{G})$ elemanı bir $\tilde{\lambda} \in \mathrm{Aut}_{\Phi_1, \Phi_2, \mathrm{G}}(\mathbb{F}_q(x) \,/\, \mathbb{F}_q)$ elemanı ile eşleştirildiğinden kanıt tamamlanır. ■

3.4. Hermityan Fonksiyon Cismi Durumu

Bu alt bölümde Hermityan fonksiyon cismi durumunda, önceki iki alt bölüme benzer bir şekilde $\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ N_1N_2-otomorfizma grubunun belirlenebileceği gösterilecektir. Bu amaçla öncelikle Hermityan fonksiyon cismi tanımını ve özelliklerini kapsamlı olarak belirtmek için gerekli olan bazı ön bilgiler ve sonuçlar verilecektir.

3.4.1. Tanım: (Garcia & Stichtenoth, 1991, s. 69) F karakteristiği $p > 0$ olan bir cisim olsun. Bir $E \,/\, F$ fonksiyon cisim genişlemesine, Galois grubu $\mathrm{Gal}\,(E \,/\, F)$ elementer abelyan p-grup olan bir Galois genişlemesi ise elementer abelyan p-genişleme denir.

Bir Hermityan fonksiyon cismi, K karakteristiği $p > 0$ olan bir cisim olmak üzere $K(x)$ rasyonel fonksiyon cisminin elementer abelyan p-genişlemeleri sınıfının özel bir durumudur. Bu tezin amaçları gereğince $\mathbb{F}_q(x)$ rasyonel fonksiyon cisim genişlemelerinin bu sınıfının bazı özellikleri verilecektir. Aşağıdaki önerme en genel haliyle (Stichtenoth, 2009, Proposition 6.4.1)'de bulunabilir.

3.4.2. Önerme: (Picone, 2016, Proposition 4.1) $\mathrm{Char}\,\mathbb{F}_q = p$, $m = p^s > 1$ ve $0 \neq \mu \in \mathbb{F}_q$ için $y^m + \mu y = f(x) \in \mathbb{F}_q[x]$ olmak üzere $F = \mathbb{F}_q(x,y)$ fonksiyon cismi göz önüne alınsın. $\deg f(x) =: d > 0$ ve p aralarında asal olmak üzere, $T^m + \mu T = 0$ polinomunun tüm kökleri $\mathbb{F}_q$ cisminde olsun. O zaman aşağıdakiler sağlanır:

a) $[F\colon \mathbb{F}_q(x)] = m$ ve $\mathbb{F}_q$, F'in tam sabit cismidir.

b) $F \,/\, \mathbb{F}_q(x)$ bir Galois genişlemesidir. $A := \{\, \gamma \in \mathbb{F}_q \mid \gamma^m + \mu\gamma = 0 \,\}$ kümesi $\mathbb{F}_q$ cisminin toplamsal grubunun m mertebeli bir alt grubudur. Her $\sigma \in \mathrm{Gal}\,(F \,/\, \mathbb{F}_q(x))$ otomorfizması için $\sigma(y) = y + \gamma$ olacak şekilde teklikle belirli bir $\gamma \in A$ elemanı vardır ve

$$\varphi\colon \mathrm{Gal}\,(F \,/\, \mathbb{F}_q(x)) \longrightarrow A,\ \sigma \mapsto \gamma \tag{3.46}$$

şeklinde tanımlı dönüşüm bir izomorfizmadır.

c) x elemanının $\mathbb{F}_q(x) \,/\, \mathbb{F}_q$ rasyonel fonksiyon cismindeki kutbu P_∞, teklikle belirli bir $Q_\infty \in \mathcal{P}_F$ genişlemesine sahiptir ve $Q_\infty | P_\infty$ tamamen dallanmıştır. Bu nedenle Q_∞, $F \,/\, \mathbb{F}_q$ fonksiyon cisminin birinci dereceden bir noktasıdır.

d) $\mathbb{F}_q(x) \,/\, \mathbb{F}_q$ rasyonel fonksiyon cisminin $F \,/\, \mathbb{F}_q(x)$'de dallanmış tek noktası P_∞ dır.

e) $F \,/\, \mathbb{F}_q$ fonksiyon cisminin cinsi $g = (m-1)(d-1) \,/\, 2$ dir.

f) $(x)_\infty = mQ_\infty$ ve $(y)_\infty = dQ_\infty$ dır.

g) $n_\infty \geq 0$ olsun. O zaman $\{ x^i y^j \mid i \geq 0, 0 \leq j \leq m-1, mi + dj \leq n_\infty \}$ kümesinin elemanları, $\mathcal{L}(n_\infty Q_\infty)$ Riemann-Roch uzayının $\mathbb{F}_q$ üzerinde bir tabanını oluşturur.

h) Her $\alpha \in \mathbb{F}_q$ elemanı için aşağıdaki durumlardan biri sağlanır:

Durum 1. $T^m + \mu T = f(\alpha)$ denklemi $\mathbb{F}_q$ cisminde m farklı köke sahiptir.

Durum 2. $T^m + \mu T = f(\alpha)$ denkleminin $\mathbb{F}_q$ cisminde kökü yoktur.

Durum 1 sağlandığında $\beta^m + \mu\beta = f(\alpha)$ olacak şekildeki her $\beta \in \mathbb{F}_q$ elemanı için $P_{\alpha,\beta} | P_\alpha$ ve $y(P_{\alpha,\beta}) = \beta$ olacak şekilde teklikle belirli bir $P_{\alpha,\beta} \in \mathcal{P}_F$ noktası vardır. Bu nedenle P_α, $F/\mathbb{F}_q\,(x)$'de derecesi bir olan m farklı genişlemeye sahiptir. Durum 2 sağlandığında P_α noktasının $\mathcal{P}_F$'deki tüm genişlemelerinin derecesi birden büyüktür.

(Wesemeyer, 1998, s. 637)'de olduğu gibi 3.4.2 Önerme'deki özellikleri sağlayan bir fonksiyon cismine geçerli denilecektir.

Hermityan fonksiyon cismi, birçok özelliğinin daha kolay ifade edilebilmesinden ve uygulamalarındaki kolaylıktan dolayı genellikle $\mathbb{F}_{q^2}$ cismi üzerinde tanımlanır.

3.4.3. Tanım: (Stichtenoth, 2009, Lemma 6.4.4) $y^q + y = x^{q+1}$ olmak üzere $\mathbb{F}_{q^2}(x, y) \,/\, \mathbb{F}_{q^2}$ fonksiyon cismine Hermityan fonksiyon cismi denir. Hermityan fonksiyon cismi aşağıdaki özelliklere sahiptir:

a) $g = q(q-1) \,/\, 2$.

b) $\mathbb{F}_{q^2}(x, y)$, $\mathbb{F}_{q^2}$ üzerinde birinci dereceden $q^3 + 1$ noktaya sahiptir. Bunlar:

1) x ve y elemanlarının ortak kutbu Q_∞,

2) Her $\alpha \in \mathbb{F}_{q^2}$ elemanı için $\beta^q + \beta = \alpha^{q+1}$ olacak şekilde q tane $\beta \in \mathbb{F}_{q^2}$ elemanı vardır. Ayrıca her (α, β) çifti için $x(P_{\alpha,\beta}) = \alpha$ ve $y(P_{\alpha,\beta}) = \beta$ olacak şekilde derecesi bir olan teklikle belirli bir $P_{\alpha,\beta} \in \mathcal{P}_{\mathbb{F}_{q^2}(x,y)}$ noktası vardır.

c) $\mathbb{F}_{q^2}(x, y) \,/\, \mathbb{F}_{q^2}$ bir maksimal fonksiyon cismidir.

d) $n_\infty \geq 0$ için $0 \leq i,\ 0 \leq j \leq q-1$ ve $iq + j(q+1) \leq n_\infty$ olmak üzere $x^i y^j$ şeklindeki elemanlar, $\mathcal{L}(n_\infty Q_\infty)$ Riemann-Roch uzayının $\mathbb{F}_q$ üzerinde bir tabanını oluşturur.

Hermityan fonksiyon cismi, 3.4.2 Önerme'de verilen fonksiyon cismi sınıfının özelliklerini sağladığından geçerlidir. Bu nedenle aşağıdaki sonuçlar Hermityan fonksiyon cismi durumunda da sağlanmaktadır.

Aşağıdaki teorem belli şartlar altında, $F \,/\, \mathbb{F}_q$ geçerli fonksiyon cisminin bir ϕ-divizörü Φ ve bir divizörü G olmak üzere, $C(\Phi; \mathrm{G}; \mathrm{n})$ kodunun $\mathcal{H}(\Phi; \mathrm{G}; \mathrm{n})$ otomorfizma grubunun 3.1.8 Teorem'de yapılan tanımlamayla $\mathrm{Aut}_{\Phi,\mathrm{G}}(F \,/\, \mathbb{F}_q)$ grubu tarafından belirlendiğini göstermektedir.

3.4.4. Teorem: (Picone, 2016, Theorem 4.5) $F \,/\, \mathbb{F}_q$ bir geçerli fonksiyon cismi olsun. $G = n_\infty Q_\infty$ divizörü ve $\{P_1, P_2, \ldots, P_N\}$ derecesi $n > 1$ olan ikili olarak birbirinden farklı noktalar olmak üzere $\Phi = \sum_{i=1}^{N} (P_i, \phi_i)$ ϕ-divizörü göz önüne alınsın. Eğer $2g + 2 \leq nN$ ve $\frac{nN}{m} > n_\infty \geq \left\lfloor \frac{d}{m} \right\rfloor m$ eşitsizlikleri sağlanıyorsa $\mathrm{Aut}_{\Phi,\mathrm{G}}(\mathbb{F}_q(x) \,/\, \mathbb{F}_q)$ ve $\mathcal{H}(\Phi; \mathrm{G}; \mathrm{n})$ grupları izomorftur.

Şimdi bu çalışmanın ana sonuçlarından biri verilecektir. Aşağıdaki teorem geçerli fonksiyon cismi durumunda Φ, Φ_1, Φ_2 ϕ-divizörleri 3.1.9 Teorem'deki gibi olmak üzere bazı ek koşullar altında, $C(\Phi; \mathrm{G})$ kodunun $\mathcal{H}_{N_1 N_2}(\Phi; \mathrm{G})$ $N_1 N_2$-otomorfizma grubunun 3.1.9 Teorem'de yapılan tanımlamayla $\mathrm{Aut}_{\Phi_1,\Phi_2,\mathrm{G}}(F \,/\, \mathbb{F}_q)$ grubu tarafından belirlenebileceğini göstermektedir. Bu teorem, geçerli fonksiyon cismi durumunda GCG kodların ve bu kodların otomorfizma gruplarının alt gruplarının daha büyük bir sınıfı göz önüne alındığından (Picone, 2016, Theorem 4.5)'i genelleştirmektedir.

3.4.5. Teorem: $F / \mathbb{F}_q$ bir geçerli fonksiyon cismi olsun ve $G = n_\infty Q_\infty$ divizörü göz önüne alınsın. $\{P_1, P_2, \dots, P_{N_1}\}$ derecesi n_1 olan ikili olarak birbirinden farklı noktalar, $\{P_{N_1+1}, P_{N_1+2}, \dots, P_{N_1+N_2}\}$ derecesi n_2 olan ikili olarak birbirinden farklı noktalar ve $\text{supp}\, G \cap \{P_1, P_2, \dots, P_{N_1+N_2}\} = \emptyset$ olmak üzere $\Phi = \sum_{i=1}^{N_1+N_2}(P_i, \phi_i)$, $\Phi_1 = \sum_{i=1}^{N_1}(P_i, \phi_i)$ ve $\Phi_2 = \sum_{i=N_1+1}^{N_1+N_2}(P_i, \phi_i)$ ϕ-divizörleri göz önüne alınsın. Eğer $2g + 2 \leq n_1 N_1 + n_2 N_2 - 1$ ve $\frac{n_1 N_1 + n_2 N_2}{m} > n_\infty \geq \left\lfloor \frac{d}{m} \right\rfloor m$ koşulları sağlanıyorsa $\text{Aut}_{\Phi_1,\Phi_2,\text{G}}(F / \mathbb{F}_q)$ ve $\mathcal{H}_{N_1 N_2}(\Phi; \text{G})$ grupları izomorftur.

Kanıt: 3.2.8 Teorem'in kanıtına benzer bir şekilde $\mathcal{H}_{N_1 N_2}(\Phi; \text{G})$ grubunun her elemanı, $\text{Aut}_{\Phi_1,\Phi_2,\text{G}}(F / \mathbb{F}_q)$ grubunun en az bir elemanı ile eşleştirilecektir. Herhangi bir $\pi \in \mathcal{H}_{N_1 N_2}(\Phi; \text{G})$ elemanı için yine 3.2.8 Teorem'in kanıtında olduğu gibi ilgili $\lambda = \lambda_\pi$ dönüşümü göz önüne alınsın. Öncelikle her $h(x, y) \in \mathcal{L}(G)$ elemanının $\lambda(h(x, y)) = h(\lambda(x), \lambda(y))$ özelliğini sağladığı gösterilecektir.

3.4.2 Önerme g) gereğince herhangi bir $h(x, y) \in \mathcal{L}(G)$ elemanı $i \geq 0, 0 \leq j \leq m - 1$ ve $mi + dj \leq n_\infty$ olmak üzere $x^i y^j$ elemanlarının bir lineer kombinasyonu olarak yazılabilir. 3.2.1 Lemma gereğince herhangi bir $x^i y^j \in \mathcal{L}(G)$ elemanı için $\lambda(x^i y^j) = \lambda(x)^i \lambda(y)^j$ olur. Dolayısıyla herhangi bir $h(x, y) \in \mathcal{L}(G)$ elemanı için $\lambda(h(x, y)) = h(\lambda(x), \lambda(y))$ dir.

Şimdi $f(x) \in \mathbb{F}_q[x]$ polinomu 3.4.2 Önerme'deki gibi olmak üzere $\lambda(x)$ ve $\lambda(y)$ elemanlarının $\lambda(y)^m + \mu\lambda(y) = f(\lambda(x))$ denklemini sağladığı gösterilecektir. Bu amaçla öncelikle $\lambda(y)^m + \mu\lambda(y), f(\lambda(x)) \in \mathcal{L}(mG)$ olduğu gösterilecektir. $x \in \mathcal{L}(G)$ dır. $\left\lfloor \frac{d}{m} \right\rfloor > 0$ ve hipotez gereğince $n_\infty \geq \left\lfloor \frac{d}{m} \right\rfloor m$ olduğundan $x^{\left\lfloor \frac{d}{m} \right\rfloor} \in \mathcal{L}(G)$ ve $G > 0$ olur. 3.2.1 Lemma gereğince $\lambda(x^{\left\lfloor \frac{d}{m} \right\rfloor}) = \lambda(x)^{\left\lfloor \frac{d}{m} \right\rfloor}$ olacağından $\lambda(x)^{\left\lfloor \frac{d}{m} \right\rfloor} \in \mathcal{L}(G)$ elde edilir. $\frac{d}{m} \leq \left\lfloor \frac{d}{m} \right\rfloor$ olduğundan Riemann-Roch uzayı tanımı gereğince $\lambda(x)^d \in \mathcal{L}(mG)$ olur. Böylece $f(\lambda(x)) \in \mathcal{L}(mG)$ bulunur. $\lambda(y)^m + \mu\lambda(y) \in \mathcal{L}(mG)$ olduğu gösterilecektir. $y \in \mathcal{L}(G)$ olduğundan $\lambda(y) \in \mathcal{L}(G)$ ve dolayısıyla $-(\lambda(y))_\infty \geq -G$ elde edilir. Bu nedenle $-(\lambda(y)^m)_\infty \geq -mG$ olacağından $\lambda(y)^m \in \mathcal{L}(mG)$ bulunur. $\mathcal{L}(mG)$ bir $\mathbb{F}_q$-vektör uzayı olduğundan $\lambda(y)^m + \mu\lambda(y) \in \mathcal{L}(mG)$ dır.

Şimdi her $i \in \{1, 2, \dots, N_1 + N_2\}$ için $(\lambda(y)^m + \mu\lambda(y))(P_i, \phi_i) = f(\lambda(x))(P_i, \phi_i)$ olduğu gösterilecektir.

$$\big(\lambda(y)^m + \mu\lambda(y)\big)\big(P_{\pi(i)}, \phi_{\pi(i)}\big) = \phi_{\pi(i)}\left(\big(\lambda(y)^m + \mu\lambda(y)\big)\big(P_{\pi(i)}\big)\right) =$$

$$\phi_{\pi(i)}\left(\lambda(y)^m\big(P_{\pi(i)}\big)\right) + \mu\phi_{\pi(i)}\left(\lambda(y)\big(P_{\pi(i)}\big)\right) = \left(\lambda(y)\big(P_{\pi(i)}, \phi_{\pi(i)}\big)\right)^m +$$

$$\mu\lambda(y)\big(P_{\pi(i)}, \phi_{\pi(i)}\big) = \big(y(P_i, \phi_i)\big)^m + \mu y(P_i, \phi_i) = (y^m + \mu y)(P_i, \phi_i) =$$

$$f(x)(P_i, \phi_i) = \phi_i\big(f(x)(P_i)\big) = f\left(\phi_i\big(x(P_i)\big)\right) = f\big(x(P_i, \phi_i)\big) =$$

$$f\left(\lambda(x)\big(P_{\pi(i)}, \phi_{\pi(i)}\big)\right) = f\left(\phi_{\pi(i)}\left(\lambda(x)\big(P_{\pi(i)}\big)\right)\right) = \phi_{\pi(i)}\left(f\left(\lambda(x)\big(P_{\pi(i)}\big)\right)\right) =$$

$$\phi_{\pi(i)}\left(f\big(\lambda(x)\big)\big(P_{\pi(i)}\big)\right) = f\big(\lambda(x)\big)\big(P_{\pi(i)}, \phi_{\pi(i)}\big) \qquad (3.47)$$

ve $\deg mG < n_1N_1 + n_2N_2$ olduğundan 3.3.8 Lemma gereğince $\lambda(y)^m + \mu\lambda(y) = f(\lambda(x))$ olur. Böylelikle istenilen kanıt, 3.3.9 Teorem'in kanıtına benzer bir şekilde elde edilebilir. ■

BÖLÜM 4

CG KODLAR VE GCG KODLAR

Bu bölümde öncelikle GCG kodlar ve CG kodlar arasındaki bir ilişki verilecektir. Daha açık olarak, bir GCG kodun izomorfizmalar gözetilmeksizin uygun bir CG kod tarafından kapsandığı gösterilecektir. Daha sonra bu ilişki kullanılarak N_1N_2-otomorfizma grubunun, bir CG kodun otomorfizma grubunun bir alt grubu olduğu gösterilecektir.

Bu bölümde genel olarak fonksiyon cisimlerinin cebirsel genişlemelerinin özellikleri kullanılacaktır. Bu nedenle öncelikle fonksiyon cisimlerinin cebirsel genişlemeleri ile ilgili bazı sonuçlar verilecektir. Bölüm boyunca K mükemmel bir cisim olmak üzere, $F\ /\ K$ tam sabit cismi K olan bir fonksiyon cismini gösterecektir.

4.1. CG Kodlar ve GCG Kodlar Arasındaki Bir İlişki

$F\ /\ K$ fonksiyon cisminin bir cebirsel genişlemesi $F'\ /\ K'$ olsun. $P \in \mathcal{P}_F$ ve $P' \in \mathcal{P}_{F'}$ olmak üzere $F_P = \mathcal{O}_P\ /\ P$ ve $F'_{P'} = \mathcal{O}_{P'}\ /\ P'$ rezidü cisimleri göz önüne alınsın. Eğer $P'|P$ ise 2.3.5 Önerme'nin bir sonucu olarak,

$$\varphi: F_P \longrightarrow F'_{P'},\ x(P) \mapsto x(P') \tag{4.1}$$

şeklinde bir doğal gömme dönüşümü tanımlanabilir (Stichtenoth, 2009, s. 70). Bu dönüşüm sayesinde F_P, $F'_{P'}$ cisminin bir alt cismi olarak düşünülebilecek ve $x \in \mathcal{O}_P$ olmak üzere $x(P) = x(P')$ yazılabilecektir.

Aşağıdaki önerme fonksiyon cisimlerinin sabit genişlemeleri durumunda bir $A \in \mathrm{Div}(F)$ divizörü ve onun conorm'u $\mathrm{Con}_{F'/F}(A) \in \mathrm{Div}(F')$ arasındaki ilişkiyi vermektedir ve bu bölümde bulunacak sonuçlar için büyük bir öneme sahiptir.

4.1.1. Önerme: (Stichtenoth, 2009, Theorem 3.6.3) $F \,/\, K$ fonksiyon cisminin bir sabit cisim genişlemesi $F' = FK'$ göz önüne alınsın.

(1) Herhangi bir $A \in \mathrm{Div}(F)$ divizörü için $\deg \mathrm{Con}_{F'/F}(A) = \deg A$ dır.

(2) Herhangi bir $A \in \mathrm{Div}(F)$ divizörü için

$$\ell(\mathrm{Con}_{F'/F}(A)) = \ell(A) \tag{4.2}$$

dır. Daha açık olarak, $\mathcal{L}(A)$ vektör uzayının her tabanı, $\mathcal{L}(\mathrm{Con}_{F'/F}(A))$ vektör uzayının da bir tabanıdır. Burada, $\mathcal{L}(A)$'nın bir K-vektör uzayı, $\mathcal{L}(\mathrm{Con}_{F'/F}(A))$'nın ise bir K'-vektör uzayı olduğuna dikkat edilmelidir.

Bu bölümdeki ilk ana sonuç için kullanılacak olan GCG kodların yapısı sunulacaktır. $\mathbb{F}_q(x, y) \,/\, \mathbb{F}_q$ fonksiyon cismi göz önüne alınsın. Derecesi $n_i \geq 1$ olan ikili olarak birbirinden farklı ve $x, y \in \mathcal{O}_{P_i}$ olacak şekildeki $P_1, P_2, \dots, P_N$ noktaları için $\Phi = \sum_{i=1}^{N} (P_i, \phi_i)$ olsun. supp $G \cap \{P_1, P_2, \dots, P_N\} = \emptyset$ olacak şekilde bir G divizörü için $C(\Phi; \mathrm{G})$ GCG kodu göz önüne alınsın.

Bu bölümdeki sonuçların elde edilmesinde kullanılacak olan bir $\mathbb{F}_q$-vektör uzayı ve bir $\mathbb{F}_q$-lineer izomorfizma sunulacaktır. $\deg P_i = n_i$ olduğundan her $i \in \{1,2, \dots, N\}$ için $z(P_i, \phi_i) \in \mathbb{F}_{q^{n_i}}$ olur. Böylece

$$\overline{C}(\Phi; \mathrm{G}) \coloneqq \{ \, (z(P_1, \phi_1), z(P_2, \phi_2), \dots, z(P_N, \phi_N)) \mid z \in \mathcal{L}(G) \, \} \subseteq \prod_{i=1}^{N} \mathbb{F}_{q^{n_i}} \tag{4.3}$$

şeklinde bir $\mathbb{F}_q$-vektör uzayı tanımlanabilir. $i \in \{1, 2, \dots, N\}$ için $\mathbb{F}_{q^{n_i}}$ ve $\mathbb{F}_q^{n_i}$ vektör uzayları arasındaki $\mathbb{F}_q$-lineer izomorfizma λ_i ile gösterilmek üzere

$$\varphi \colon \overline{C}(\Phi; \mathrm{G}) \longrightarrow C(\Phi; \mathrm{G})$$

$$(z(P_1, \phi_1), \dots, z(P_N, \phi_N)) \longmapsto (\lambda_1(z(P_1, \phi_1)), \dots, \lambda_N(z(P_N, \phi_N))) \tag{4.4}$$

şeklinde bir $\mathbb{F}_q$-lineer izomorfizma tanımlanabilir.

$\overline{C}(\Phi;\mathrm{G})$ $\mathbb{F}_q$-vektör uzayı kullanılarak, $C(\Phi;\mathrm{G})$ GCG kodunun bir CG koda gömülebileceği gösterilecektir. Bu amaçla öncelikle aşağıdaki önerme verilecektir.

4.1.2. Önerme: (Picone, 2013, Proposition 3.5) $F\,/\,\mathbb{F}_q$ bir fonksiyon cismi olsun. $f(X,Y)\in\mathbb{F}_q[X,Y]$ için $f(x,y)=0$ olmak üzere $F=\mathbb{F}_q(x,y)$ olsun. $F\,/\,\mathbb{F}_q$ fonksiyon cisminin, derecesi $n>1$ ve $x,y\in\mathcal{O}_P$ olacak şekildeki bir ϕ-noktası (P,ϕ) olsun. O zaman $\mathbb{F}_{q^n}(x,y)\,/\,\mathbb{F}_{q^n}$ sabit cisim genişlemesinin, (P,ϕ) üzerine uzanan ve herhangi bir $z\in\mathcal{O}_P$ için $z(P')=z(P,\phi)$ eşitliğini sağlayan bir P' rasyonel noktası vardır.

4.1.2 Önerme gereğince her $i\in\{1,2,\dots,N\}$ için $\mathbb{F}_{q^{n_i}}(x,y)\,/\,\mathbb{F}_{q^{n_i}}$ sabit cisim genişlemesinin, herhangi bir $z\in\mathcal{O}_{P_i}$ elemanı için $z(R_i)=z(P_i,\phi_i)$ eşitliğini sağlayacak şekilde (P_i,ϕ_i) üzerine uzanan bir R_i rasyonel noktası vardır. $n_1,n_2,\dots,n_N$ sayılarının en küçük ortak katı $\mathrm{ekok}\,(n_1,n_2,\dots,n_N)$ ile gösterilmek üzere $\mathbb{F}_{q^{n_i}}(x,y)\,/\,\mathbb{F}_{q^{n_i}}$ fonksiyon cisminin $\mathbb{F}_{q^{\mathrm{ekok}\,(n_1,n_2,\dots,n_N)}}(x,y)\,/\,\mathbb{F}_{q^{\mathrm{ekok}\,(n_1,n_2,\dots,n_N)}}$ sabit cisim genişlemesi göz önüne alınsın. 2.3.6 Önerme gereğince $\mathbb{F}_{q^{\mathrm{ekok}\,(n_1,n_2,\dots,n_N)}}(x,y)\,/\,\mathbb{F}_{q^{\mathrm{ekok}\,(n_1,n_2,\dots,n_N)}}$ fonksiyon cisminin R_i üzerine uzanan bir S_i noktası vardır. 4.1.1 Önerme (1) gereğince R_i rasyonel bir nokta olduğundan, S_i de rasyonel bir noktadır. Ayrıca, (4.1)'de tanımlanan gömme dönüşümü göz önüne alınırsa her $i\in\{1,2,\dots,N\}$ için $z\in\mathcal{O}_{P_i}$ olmak üzere

$$z(S_i)=z(R_i)=z(P_i,\phi) \tag{4.5}$$

olur.

Şimdi bu çalışmanın ana sonuçlarından biri verilecektir. Aşağıdaki teorem $\mathbb{F}_q$-izomorfizmalar gözetilmeksizin $C(\Phi;\mathrm{G})$ GCG kodunun, uygun bir CG kodun bir $\mathbb{F}_q$-alt vektör uzayı olduğunu ifade etmektedir. Bu teorem, $C(\Phi;\mathrm{G};\mathrm{n})$ kodundan daha genel bir yapıya sahip olan $C(\Phi;\mathrm{G})$ kodu göz önüne alındığından (Picone, 2013, Proposition 3.6)'yı genelleştirmektedir.

4.1.3. Teorem: Her $i\in\{1,2,\dots,N\}$ için S_i noktası yukarıdaki gibi olmak üzere, $D'=S_1+S_2+\cdots+S_N$ olsun. $G\in\mathrm{Div}(\mathbb{F}_q(x,y))$ divizörünün conorm'u $G'\in$

$\mathrm{Div}(\mathbb{F}_{q^{\mathrm{ekok}\,(n_1,n_2,\ldots,n_N)}}(x,y))$ olmak üzere, $C_{\mathcal{L}}(D',G')$ CG kodu göz önüne alınsın. O zaman

$$\overline{C}(\Phi;\mathrm{G}) \subseteq C_{\mathcal{L}}(D',G') \tag{4.6}$$

olur. Bu nedenle $C_{\mathcal{L}}(D',G')$ CG kodu, $C(\Phi;\mathrm{G})$ GCG koduna $\mathbb{F}_q$-izomorf bir alt uzay içerir.

Kanıt: Herhangi bir $z \in \mathcal{L}(G)$ elemanı göz önüne alınsın. Riemann-Roch uzayı tanımı gereğince her $i \in \{1,2,\ldots,N\}$ için $z \in \mathcal{O}_{P_i}$ olacağından (4.5) gereğince $z(S_i) = z(P_i,\phi)$ olur. Bu nedenle,

$$\overline{C}(\Phi;\mathrm{G}) = \{(z(S_1),z(S_2),\ldots,z(S_N)) \mid z \in \mathcal{L}(G)\} \tag{4.7}$$

yazılabilir. 4.1.1 Önerme (2) gereğince $\mathcal{L}(G) \subseteq \mathcal{L}(G')$ olduğundan $\overline{C}(\Phi;\mathrm{G}) \subseteq \{(z(S_1),z(S_2),\ldots,z(S_N)) \mid z \in \mathcal{L}(G')\} = C_{\mathcal{L}}(D',G')$ elde edilir. Dolayısıyla kanıt tamamlanır. ■

4.2. CG Kodlar ve GCG Kodların Otomorfizma Grupları Arasındaki Bir İlişki

Bu bölümdeki ikinci ana sonuç için kullanılacak olan GCG kodların yapısı sunulacaktır. $\mathbb{F}_q(x,y)\,/\,\mathbb{F}_q$ fonksiyon cismi göz önüne alınsın. $\{P_1,P_2,\ldots,P_{N_1}\}$ derecesi n_1 olan ikili olarak birbirinden farklı noktalar ve $\{P_{N_1+1},P_{N_1+2},\ldots,P_{N_1+N_2}\}$ derecesi n_2 olan ikili olarak birbirinden farklı noktalar olmak üzere $\Phi = \sum_{i=1}^{N_1+N_2}(P_i,\phi_i)$ olsun. $\mathrm{supp}\,G \cap \{P_1,P_2,\ldots,P_{N_1+N_2}\} = \emptyset$ olacak şekilde bir G divizörü için $C(\Phi;\mathrm{G})$ GCG kodu göz önüne alınsın. $\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ N_1N_2-otomorfizma grubunun, yalnızca bu şekildeki bir yapıya sahip olan GCG kodlar için tanımlandığına dikkat edilmelidir. Her $i \in \{1,2,\ldots,N_1+N_2\}$ için $\mathbb{F}_q^{n_i}$ ve $\mathbb{F}_{q^{n_i}}$ vektör uzayları birbirine izomorf olduğundan, $\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ N_1N_2-otomorfizma grubu $\overline{C}(\Phi;\mathrm{G})$ $\mathbb{F}_q$-vektör uzayı üzerinde aynı anlamda tanımlanacaktır.

4.1.3 Teorem'deki kabuller altında ve 4.1.3 Teorem'de verilen ilişki yardımıyla $C(\Phi;\mathrm{G})$ GCG ve $C_{\mathcal{L}}(D',G')$ CG kodlarının otomorfizma gruplarının aynı alt gruba sahip olduğu gösterilecektir. Daha açık olarak, $\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ N_1N_2-otomorfizma

grubunun, $C_{\mathcal{L}}(D', G')$ CG kodunun otomorfizma grubunun bir alt grubu olduğu gösterilecektir. Aşağıdaki teorem bu çalışmanın ana sonuçlarından biridir ve $\mathcal{H}(\Phi; \mathrm{G}; \mathrm{n})$ n-otomorfizma grubundan daha genel olan $\mathcal{H}_{N_1N_2}(\Phi; \mathrm{G})$ N_1N_2-otomorfizma grubu göz önüne alındığından (Picone, 2013, Proposition 3.7)'yi genelleştirmektedir.

4.2.1. Teorem: $\mathcal{H}_{N_1N_2}(\Phi; \mathrm{G})$ N_1N_2-otomorfizma grubu, $C_{\mathcal{L}}(D', G')$ CG kodunun otomorfizma grubunun bir alt grubudur.

Kanıt: Herhangi bir $\pi \in \mathcal{H}_{N_1N_2}(\Phi; \mathrm{G})$ otomorfizması göz önüne alınsın. π N_1N_2-otomorfizmasının $\overline{C}(\Phi; \mathrm{G})$ $\mathbb{F}_q$-vektör uzayı üzerindeki tanımı gereğince, $\frac{u(x,y)}{v(x,y)} \in \mathcal{L}(G)$ olmak üzere

$$\left(\frac{u(x,y)}{v(x,y)}\left(P_{\pi(1)}, \phi_{\pi(1)}\right), \dots, \frac{u(x,y)}{v(x,y)}\left(P_{\pi(N_1+N_2)}, \phi_{\pi(N_1+N_2)}\right)\right) \in \overline{C}(\Phi; G) \tag{4.8}$$

olur. $\overline{C}(\Phi; \mathrm{G})$ $\mathbb{F}_q$-vektör uzayı tanımı gereğince bir $\frac{u'(x,y)}{v'(x,y)} \in \mathcal{L}(G)$ elemanı için $\frac{u(x,y)}{v(x,y)}\left(P_{\pi(i)}, \phi_{\pi(i)}\right) = \frac{u'(x,y)}{v'(x,y)}(P_i, \phi_i)$ eşitliği her $i \in \{1, 2, \dots, N_1 + N_2\}$ için sağlanır. (4.5)'de verilen eşitlik kullanılarak her $i \in \{1, 2, \dots, N_1 + N_2\}$ için $\frac{u(x,y)}{v(x,y)}\left(S_{\pi(i)}\right) = \frac{u'(x,y)}{v'(x,y)}(S_i)$ elde edilir.

$B = \left\{\frac{u_1(x,y)}{v_1(x,y)}, \frac{u_2(x,y)}{v_2(x,y)}, \dots, \frac{u_r(x,y)}{v_r(x,y)}\right\}$ kümesi, $\mathcal{L}(G)$ $\mathbb{F}_q$-vektör uzayının bir tabanı olsun. O zaman $j \in \{1, 2, \dots, r\}$ olmak üzere bir $\frac{u'_j(x,y)}{v'_j(x,y)} \in \mathcal{L}(G)$ elemanı için $\frac{u_j(x,y)}{v_j(x,y)}\left(S_{\pi(i)}\right) = \frac{u'_j(x,y)}{v'_j(x,y)}(S_i)$ eşitliği her $i \in \{1, 2, \dots, N_1 + N_2\}$ için sağlanır.

4.1.1 Önerme (2) gereğince B kümesini oluşturan elemanlar $\mathcal{L}(G')$ $\mathbb{F}_{q^{\mathrm{ekok}\,(n_1,n_2)}}$-vektör uzayının da bir tabanı olduğundan herhangi bir $z \in \mathcal{L}(G')$ elemanı, $j \in \{1, 2, \dots, r\}$ için $a_j \in \mathbb{F}_{q^{\mathrm{ekok}\,(n_1,n_2)}}$ olmak üzere $z = \sum_{j=1}^{r} a_j \frac{u_j(x,y)}{v_j(x,y)}$ şeklinde yazılabilir. Bu nedenle her $i \in \{1, 2, \dots, N_1 + N_2\}$ için

$$z\left(S_{\pi(i)}\right) = \left(\sum_{j=1}^{r} a_j \frac{u_j(x,y)}{v_j(x,y)}\right)\left(S_{\pi(i)}\right) = \sum_{j=1}^{r} a_j \left(\frac{u_j(x,y)}{v_j(x,y)}\left(S_{\pi(i)}\right)\right) =$$

$$\sum_{j=1}^{r} a_j \left(\frac{u'_j(x,y)}{v'_j(x,y)}(S_i)\right) = \left(\sum_{j=1}^{r} a_j \frac{u'_j(x,y)}{v'_j(x,y)}\right)(S_i) \qquad (4.9)$$

elde edilir. Ayrıca $\sum_{j=1}^{r} a_j \frac{u'_j(x,y)}{v'_j(x,y)} \in \mathcal{L}(G')$ olduğuna dikkat edilirse, $\pi \in \mathrm{Aut}(C_{\mathcal{L}}(D', G'))$ olduğu görülür. Dolayısıyla $\mathcal{H}_{N_1 N_2}(\Phi; \mathrm{G}) \subseteq \mathrm{Aut}(C_{\mathcal{L}}(D', G'))$ elde edileceğinden kanıt tamamlanır. ■

BÖLÜM 5

SONUÇLAR VE TARTIŞMA

Bu çalışmanın üçüncü bölümünde, GCG kodların bir alt sınıfı göz önüne alınmıştır ve bu alt sınıftaki bir GCG kodun $\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ otomorfizma grubu kavramı tanımlanmıştır. Daha sonra, $\mathrm{Aut}(F\,/\,\mathbb{F}_q)$ grubunun $\mathrm{Aut}_{\Phi_1,\Phi_2,\mathrm{G}}(F\,/\,\mathbb{F}_q)$ altgrubunun, $\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ otomorfizma grubuna gömülebildiği gösterilmiştir. Dahası ilgili fonksiyon cismi rasyonel, hipereliptik ve Hermityan olduğunda $\mathrm{Aut}_{\Phi_1,\Phi_2,\mathrm{G}}(F\,/\,\mathbb{F}_q)$ ve $\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ gruplarının bazı şartlar altında izomorf olduğu gösterilmiştir. Böylece, (Picone, 2016; Picone & Spera, 2009; Spera, 2007) çalışmalarında göz önüne alınan GCG kodların daha büyük bir sınıfının otomorfizma grubunun bir altgrubu belirlenmiştir.

Bu çalışmanın dördüncü bölümünde, üreteç noktalarının derecesi üzerinde bir şart olmaksızın bir GCG kodun uygun bir CG kod tarafından kapsandığı gösterilmiştir. Ardından, ikinci bölümde göz önüne alınan GCG kodların bir alt sınıfı için tanımlanan $\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ otomorfizma grubunun, ilgili CG kodun otomorfizma grubunun bir alt grubu olduğu gösterilmiştir. Böylece, (Picone, 2013, Section 3) çalışmasında göz önüne alınan GCG kodların daha büyük bir sınıfının CG kodlarla ilişkisi gösterilmiş ve yapısal olarak farklı bu iki kod sınıfının otomorfizma grupları arasında (Picone, 2013, Section 3)'dan daha genel bir ilişki bulunmuştur.

Bu çalışmanın üçüncü bölümünde yer alan, 3.1 ve 3.2 alt bölümlerinde sunulan orijinal sonuçların bulunduğu, "On the automorphisms of generalized algebraic geometry codes" isimli makale, SCI ve SCI Expanded indekslerinde yer alan ve Q2 kategorisindeki Designs, Codes and Cryptography isimli dergide 10.1007/s10623-022-01043-1 DOI numarasıyla yayınlanmıştır. Bu çalışmanın dördüncü bölümünde yer alan,

4.1 ve 4.2 alt bölümlerinde sunulan orijinal sonuçların bulunduğu, "On a relation between GAG codes and AG codes" isimli makale, SCI Expanded indeksinde yer alan ve Q2 kategorisindeki Analele Stiintifice ale Universitatii Ovidius Constanta isimli dergi tarafından yayınlanmak üzere kabul edilmiştir.

$\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ grubu, ilgili fonksiyon cismi bu çalışmada göz önüne alınan fonksiyon cisimleri çeşidinden farklı seçildiğinde de bulunabilir. Bunun için teorik anlamda, ilgili fonksiyon cisminin bir G divizörünün Riemann-Roch uzayı $\mathcal{L}(G)$'ın bir tabanı üzerinde (3.21)'de tanımlanan λ lineer dönüşümünün gerekli özellikleri sağlaması gerekmektedir. Bu da fonksiyon cismi teorisindeki en önemli problemlerden biri olan, bir Riemann-Roch uzayının tabanını bulmayla ilişkilidir.

$\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ grubunun elemanları ilgili fonksiyon cisminin, verilen aynı dereceden noktaların iki koleksiyonu için her bir koleksiyondaki noktaları kendi arasında sıralayan otomorfizmaları tarafından elde edilmektedir. Uygulama anlamında, farklı fonksiyon cisimlerinin noktalarının yapısı ve özellikleri değişeceğinden bu otomorfizmaları elde etmek için yöntemler bulmak gerekmektedir.

Bu çalışmada CG kodların ve GCG kodların otomorfizma gruplarıyla ilgili elde edilen tüm sonuçlar $\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ grubunun yapısı ile ilgili gerekli düzenlemeler yapılarak, yapısında aynı dereceden noktaların daha fazla koleksiyonunu bulunduran GCG kodlara uygulanabilir. Ancak, koleksiyon sayısının artması uygulama anlamında fonksiyon cisminin istenilen özelliklere sahip otomorfizmalarını bulmayı zorlaştıracaktır. Bir GCG kodu üreten her noktanın derecesinin farklı olması durumunda ise $\mathcal{H}_{N_1N_2}(\Phi;\mathrm{G})$ grubu, $\mathcal{S}_{N_1+N_2}$ simetri grubunun yalnızca birim elemanını içereceğinden elde edilen sonuçlar aşikar olacaktır. Dolayısıyla bu durumda benzer sonuçları elde edebilmek için yeni yöntemler gerekmektedir.

KAYNAKLAR

Ding, C., Niederreiter, H. & Xing, C. P. (2000). Some new codes from algebraic curves. *IEEE Transactions on Information Theory, 46*(7), 2638-2642.

Forney, G. D. (1966). *Concatenated Codes*. Cambridge: MIT.

Garcia, A. & Stichtenoth, H. (1991). Elementary Abelian *p*-extensions of algebraic function fields. *Manuscripta Mathematica, 72*, 67-79.

Goppa, V. D. (1981). Codes on algebraic curves. *Soviet Mathematics – Doklady, 24*(1), 170-172.

Hansen, J. P. (1987). Codes on the Klein quartic, ideals, and decoding. *IEEE Transactions on Information Theory, 33*(6), 923-925.

Jibril, M., Tomlinson, M., Ahmed, M. Z. & Tjhai, C. (2010). *Good codes from generalised algebraic geometry codes.* Proceedings of 2010 IEEE International Symposium on Information Theory, 1130-1132.

Joyner, D. & Ksir, A. (2006). Automorphism groups of some AG codes. *IEEE Transactions on Information Theory, 52*(7), 3325-3329.

Ling, S. & Xing, C. P. (2004). *Coding Theory, A First Course.* Cambridge: Cambridge University.

MacWilliams, F. J. & Sloane, N. J. (1997). *The Theory of Error-Correcting Codes.* Amsterdam: North-Holland.

Matsumoto, R. & Oishi, M. (2001). Decoding method for generalized algebraic geometry codes. doi: 10.48550/arXiv.math/0104222

Niederreiter, H., Xing, C. P. & Lam, K. Y. (1999). A new construction of algebraic geometry codes. *Applicable Algebra in Engineering, Communication and Computing, 9*, 373-381.

Özbudak, F. & Stichtenoth, H. (1999). Constructing codes from algebraic curves. *IEEE Transactions on Information Theory, 45*(7), 2502-2505.

Picone, A. (2016). Automorphisms of Hermitian generalized algebraic geometry codes. *Journal of Pure and Applied Algebra, 220*(5), 1935-1945.

Picone, A. (2013). New lower bounds for the minimum distance of generalized algebraic geometry codes. *Journal of Pure and Applied Algebra, 217*, 1164-1172.

Picone, A. & Spera, A. G. (2009). Automorphisms of hyperelliptic GAG-codes. *Discrete Mathematics, 309*(2), 328-340.

Picone, A. (2007). *Automorphisms of Generalized Algebraic Geometry Codes*. Doktora tezi. Universita degli Studi di Palermo, Palermo. Erişim adresi: http://www.bdim.eu/item?fmt=pdf&id=tesi_2007_PiconeAlberto_1

Spera, A. G. (2007). On automorphisms of generalized algebraic-geometry codes. *Journal of Pure and Applied Algebra, 210*(3), 837-845.

Spera, A. G. (2005). Geometric Goppa codes on Fermat curves. *Matematiche, 1*, 3-12.

Stichtenoth, H. (2009). *Algebraic Function Fields and Codes*. Berlin: Springer-Verlag.

Stichtenoth, H. (1990). On automorphisms of geometric Goppa codes. *Journal of Algebra, 130*(1), 113-121.

Şenel, E. (2017). *Fonksiyon Cisimleri ve Kodlar Hakkında*. Yüksek lisans tezi. Trakya Üniversitesi, Edirne.

Tsfasman, M., Vladut, S. & Nogin, D. (2019). *Algebraic Geometry Codes: Advanced Chapters*. Providence: American Mathematical Society.

Wesemeyer, S. (1998). On the automorphism group of various Goppa codes. *IEEE Transactions on Information Theory, Vol. 44*(2), 630-643.

Wesemeyer, S. (1997). *On the Automorphism Group of Various Goppa Codes*. Doktora tezi. University of Exeter, Exeter. Erişim adresi: https://ore.exeter.ac.uk/repository/bitstream/handle/10871/8325/WesemeyerS.pdf

Xing, C. P. (1995a). Automorphism group of elliptic codes. *Communications in Algebra, 23*(11), 4061-4072.

Xing, C. P. (1995b). On automorphism groups of the Hermitian codes. *IEEE Transactions on Information Theory, 41*(6), 1629-1635.

Xing, C. P., Niederreiter, H. & Lam, K. Y. (1999a). Constructions of algebraic-geometry codes. *IEEE Transactions on Information Theory, 45*(4), 1186-1193.

Xing, C. P., Niederreiter, H. & Lam, K. Y. (1999b). A generalization of algebraic-geometry codes. *IEEE Transactions on Information Theory, 45*(7), 2498-2501.

ÖZGEÇMİŞ

28.11.1989 tarihinde İstanbul'un Beyoğlu ilçesinde doğdum. İlk ve orta öğrenimimi İstanbul'da tamamladım. Çanakkale Onsekiz Mart Üniversitesi, Fen-Edebiyat Fakültesi, Matematik Bölümü'nde 2006 yılında başladığım lisans eğitimini bölüm üçüncüsü olarak 2011 yılında tamamladım. 2012-2013 yılları arasında özel bir eğitim kurumunda matematik öğretmeni olarak çalıştım. 2015 yılında atandığım Milli Eğitim Bakanlığı'nda altı ay çalıştıktan sonra aynı yıl Trakya Üniversitesi, Fen Fakültesi, Matematik Bölümü'ne araştırma görevlisi olarak atandım. 2015 yılında Trakya Üniversitesi, Fen Fakültesi, Matematik Bölümü'nde başladığım yüksek lisans eğitimini 2017 yılında tamamladım.

İLGİLİ TEZ KONUSUNA AİT BİLİMSEL FAALİYETLER

SCI veya SCI Expanded Kapsamındaki Yayınlar

Şenel, E. & Öke, F. (2022). On the automorphisms of generalized algebraic geometry codes. *Designs, Codes and Cryptography*, *90*(6), 1369-1379.

Şenel, E. & Öke, F. (2022). On a relation between GAG codes and AG codes. *Analele Stiintifice ale Universitatii Ovidius Constanta* (Kabul edildi).

Uluslararası Bilimsel Toplantılarda Sunulan Bildiriler

Şenel, E. & Öke, F. (2020). *On the automorphisms of generalized algebraic geometry codes.* 3rd International Conference on Pure and Applied Mathematics, Türkiye, Van (Sözlü Bildiri).

Şenel, E. & Öke, F. (2022). *On a relation between GAG codes and AG codes.* 11th International Eurasian Conference on Mathematical Sciences and Applications, Türkiye, İstanbul (Sözlü Bildiri).