T.C.
AKDENİZ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ARF SEMİGRUP VE CEBİRSEL EĞRİLERE UYGULAMALARI

Damla DEDE SİPAHİ

YÜKSEK LİSANS TEZİ

MATEMATİK ANABİLİM DALI

2013

T.C.
AKDENİZ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ARF SEMİGRUP VE CEBİRSEL EĞRİLERE UYGULAMALARI

Damla DEDE SİPAHİ

YÜKSEK LİSANS TEZİ

MATEMATİK ANABİLİM DALI

Bu tez TÜBİTAK tarafından "2210 Son Sınıf Lisans Öğrencileri İçin Yurt İçi Lisansüstü (Yüksek Lisans/Doktora) Burs" programı ile desteklenmiştir.

2013

T.C.
AKDENİZ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ARF SEMİGRUP VE CEBİRSEL EĞRİLERE UYGULAMALARI

Damla DEDE SİPAHİ

YÜKSEK LİSANS TEZİ

MATEMATİK ANABİLİM DALI

Bu tez ... / ... / 2013 tarihinde aşağıdaki jüri tarafından oybirliği / oyçokluğu ile kabul edilmiştir.

Doç. Dr. Mustafa ALKAN .....

Yrd. Doç. Dr. Nesrin TUTAŞ .....

Yrd. Doç. Dr. Sevda SEZER .....

ÖZET

ARF SEMİGRUP VE CEBİRSEL EĞRİLERE UYGULAMALARI

Damla DEDE SİPAHİ

Yüksek Lisans Tezi, Matematik Anabilim Dalı

Danışman: Yrd. Doç. Dr. Nesrin TUTAŞ

Haziran 2013, 55 sayfa

Nümerik semigruplarla ilgili çalışmaların önemli bir bölümü cebirsel geometride çalışılan cebirsel eğrilere dayanır. Nümerik semigruplar, kodlama teorisi ve cebirsel eğrilere uygulamaları nedeniyle önemlidir.

Bu tezde, öncelikle nümerik semigruplar ve genel özellikleri verilmiştir. Önemli cebirsel eğri sınıflarının bir Q Weierstrass noktasındaki semigrupları incelenmiş ve bu semigrupların Arf olma özelliği araştırılmıştır. Ayrıca, bir cebirsel eğri üzerinden yazılan tek noktalı cebirsel geometrik kodların, bir Arf semigrup üzerinden tanımlandığında kodun minimum mesafesi üzerinden Feng-Rao (order bound) sınırı Bras-Amoros (2000, 2005, 2007), Campillo ve diğerleri (2004) çalışmalarına göre hesaplanmıştır. Daha iyileştirilmiş parametrelere sahip kodlar kurulabileceği gözlemlenmiştir. İyi parametreli kodların yazılması açısından, Arf semigrupların kullanılmasının önemli katkılar ve yeni teknikler kazandıracağına inanıyoruz.

ANAHTAR KELİMELER: Arf semigrup, Feng-Rao sınırı, tek nokta kodları

JÜRİ: Doç. Dr. Mustafa ALKAN

Yrd. Doç. Dr. Nesrin TUTAŞ (Danışman)

Yrd. Doç. Dr. Sevda SEZER

ABSTRACT

ARF SEMIGRUP AND APPLICATIONS TO ALGEBRAIC CURVES

Damla DEDE SİPAHİ

MSc Thesis in Mathematics

Supervisor: Asst. Prof. Dr. Nesrin TUTAŞ

July 2013, 55 pages

An important part of the work on numerical semigroups are based on theory of algebraic curves. Numerical semigroups are important because of applications to coding theory and algebraic curves.

In this thesis, firstly we give general properties of a numerical semigrups. Numerical semigroups of some curve classes at a Weierstrass points Q are investigated and checked whether these are Arf numerical semigroup or not. Moreover, we compute the Feng-Rao (order bound) bound on the minimum distance of one point-algebraic geometric codes, when the numerical semigroup at the point Q is an Arf semigroup, via Bras-Amoros (2000,2005,2007), Campillo at all (2004). It has been observed that one can construct algebraic geometric codes with better parameters. We believe that Arf numerical semigroups may suggest new tecniques for the codes with better parameters.

KEYWORDS: Arf semigroup, Feng-Rao (order bound), one-point codes.

COMMITTEE: Assoc. Prof. Dr. Mustafa ALKAN

Asst. Prof. Dr. Nesrin TUTAŞ (Supervisor)

Asst. Prof. Dr. Sevda SEZER

ÖNSÖZ

Bu çalışma esas olarak iki bölümünden oluşmaktadır. İlk bölümde, nümerik semigrup kavramı tanıtılmış ve indirgenemez, simetrik, pseudo simetrik, akut, aralıkla üretilen semigruplar ile Arf nümerik semigrubun özellikleri ayrıntılı olarak incelenmiştir. Ayrıca, cebirsel fonksiyonlar cismi ve cebirsel kodların genel yapısı ifade edilmiştir.

İkinci bölümde ise, cebirsel eğrilerin nümerik semigruplarla ilişkilendirilmesi yapılmış, bazı cebirsel eğrilere karşılık gelen nümerik semigrup türleri incelenmiş, bunların özellikle Arf olma özelliğini sağlayıp sağlamadığı araştırılmıştır. Ayrıca, eğri üzerinde bir noktadaki semigrubun Arf olması halinde yazılan tek noktalı cebirsel geometrik kod için Feng-Rao (order bound) sınırı ile ilgili sonuçlar ifade edilmiştir.

Bu tez çalışması boyunca bilgisini ve desteğini esirgemeyen danışmanım Sayın Yard. Doç. Dr. Nesrin TUTAŞ'a (Akdeniz Üniversitesi Fen Fakültesi) , " 2210 Son Sınıf Lisans Öğrencileri İçin Yurt İçi Lisansüstü (Yüksek Lisans/Doktora) Burs" programı ile destek veren Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'na (TÜBİTAK), eşime ve ayrıca beni bugünlere getirmek için hiç bir şeyini esirgemeyen bu tezin gerçek yaratıcısı olan aileme sonsuz teşekkürlerimi sunarım.

İÇİNDEKİLER

1. GİRİŞ

Sylvester 1884'te " $obeb(a,b) = 1$ olacak şekilde verilen a, b pozitif tamsayıları için $n_1, n_2 \geq 0$ olmak üzere $N = n_1 + n_2$ biçiminde öyle N tamsayısı vardır ki her $m > N$ için $m = n_1 a + n_2 b$ biçiminde yazılabilirler. " iddiasını ortaya atmış ve bu problemi çözmüştür. Frobenius; Sylvester probleminin genellemesini yaparak $obeb(a_1, a_2, ..., a_n) = 1$, $n \geq 3$ olacak şekilde verilen pozitif tamsayılar için semigruba ait olmayan en büyük tamsayıyı bulma problemini ifade etmiş ve bu sayı için formül olup olmadığını ve böyle gösterime sahip olmayan kaç tane tamsayının olabileceği problemini ortaya atmıştır. Aslında bu problemlerin çalışılmasındaki asıl kaynak cebirsel geometride çalışılan cebirsel eğrilerdir.

Cahit Arf 1949'da tekil eğri dallanmalarının sınıflandırılması problemini onların katlılık dizisine bağlı olarak çözmüştür. Arf nümerik semigrup kavramı bu çalışmalarda ortaya çıkan önemli kavramlardan birisidir. Cebirsel eğriler üzerindeki ilginç nümerik semigruplardan bir diğeri de Weierstrass nümerik semigruplarıdır. Eğri üzerinde seçilen bir noktanın kutup noktaları kümesine karşılık gelen bu semigrup, sadece sonlu sayıda nokta için diğerlerinden farklanabilir.

Son yıllardaki çalışmalar ile nümerik semigruplar, cebirsel eğriler ve cebirsel kodlara uygulamalarıyla önemli yer edinmiştir. Özellikle, cebirsel eğriler üzerinde alınan Weierstrass noktalarına karşılık gelen nümerik semigruplar, daha iyi parametreli cebirsel kodların yazılmasına olanak sağlamıştır. Cebirsel geometrik kodları genelleştirmenin bir yolu Feng-Rao tarafından tanımlanmıştır. Bu genelleştirme, Arf semigrup kulllanıldığında önemli kolaylıklar sağlanmakta ve minimum uzaklık üzerindeki sınırlar daha iyi geliştirilebilmektedir.

Bu tezde, nümerik ve Arf nümerik semigrupların genel özellikleri incelenmiş, eğriler üzerindeki bazı Arf nümerik semigruplar ile kodlar üzerindeki iyileştirilmiş sınırlar, yukarıda sözü edilen çalışmalar ışığında, yeniden üretilmiş ve bazı örnekler sunulmuştur.

2. KURAMSAL BİLGİLER VE KAYNAK TARAMALARI

2.1. Nümerik Semigruplar ve Genel Özellikleri

Semigrup kavramı iyi bilinen cebirsel yapılardan birisidir ve aşağıdaki biçimde tanımlanabilir. Bu bölümde bahsedilen kavramlar hakkında ayrıntılı bilgi için (Arf 1949), (Rosales, Garcia-Sanchez, Garcia-Garcia, Branco 2004), (Amoros 2007), (Rosales ve Garcia-Sanchez 2009), (Lipman) kaynaklarına bakılabilir.

Tanım 2.1 *S bir küme, $+$, S üzerinde bir ikili işlem ve birleşme özelliğine sahip ise S'ye semigrup denir. S semigrubunun $+$ işlemine göre birimi $0 \in S$ ise S'ye monoid denir.*

Bu tez boyunca $\mathbb{N}$ ile negatif olmayan tamsayılar kümesini, $\mathbb{Z}$ ile de tamsayılar kümesini göstereceğiz. $\mathbb{N}$'nin $+$ işlemine göre bir monoid olduğu açıktır. $S \subseteqq \mathbb{N}$ ve $0 \in S$ ise S, $\mathbb{N}$'nin alt monoidi olarak adlandırılır. Alt monoidlerin kesişiminin yine bir alt monoid olduğu açıktır. $\{0\}$ aşikar monoid olarak adlandırılır. $\emptyset \neq A \subseteq S$ için A'yı kapsayan S'nin tüm alt monoidlerinin kesişimi, S'nin A'yı içeren en küçük alt monoididir, $< A >$ ile gösterilir ve A'nın ürettiği alt monoid olarak adlandırılır. Burada, A üreteç sistemi ve

$$< A >= \{\lambda_1 a_1 + \ldots + \lambda_n a_n \mid \lambda_i \in \mathbb{N}, a_i \in A, i \in \mathbb{N}\}$$

formundadır.

Tanım 2.2 *$S \subseteq \mathbb{N}$ bir alt monoid olsun. $\mathbb{N} \setminus S$ sonlu ise S'ye nümerik semigrup denir.*

$\mathbb{N}$ semigrubuna özel olarak aşikar nümerik semigrup denir.

Tanım 2.3 *S bir nümerik semigrup olsun. S'ye ait olmayan en büyük tamsayıya Frobenius sayısı ve her $n \in \mathbb{N}$ için $x + n \in S$ olacak şekilde en küçük x tamsayısına S'nin önderi (conductor) denir, sırasıyla $F(S)$ ve c ile gösterilir. $F(S) = c - 1$ dir. S'de olmayan elemanların kümesi $G(S)$ olmak üzere, kümenin eleman sayısına cins denir. S nümerik semigrubunun cinsi $g(S)$ ile gösterilir, kısaca cins için g gösterimi kullanılır. $g = \#(\mathbb{N} \setminus S)$ dir.*

Örnek 2.4 *$S = \langle 3, 4\rangle = \{0, 3, 4, 6, \longrightarrow\}$ dır. Burada $\longrightarrow$ sembolü c den sonraki elemanların kümeye ait olduğunu gösterir. $F(S) = 5$ ve $G(S) = \{1, 2, 5\}$ olmak üzere $g = 3$ tür.*

Tanım 2.5 *(H_n), semigruplar dizisi olsun. $H_1 = \mathbb{N}$ ve $n > 1$ için*

$$H_n = a_n H_{n-1} \cup \{m \in \mathbb{N} \mid m \geq a_n b_{n-1}\}$$

olacak şekilde (a_n) ve (b_n) pozitif tamsayılarının dizisi var ise (H_n), inductive semigrup dizisi olarak adlandırılır. İnductive semigrup dizisinin elemanı olan nümerik semigruba inductive denir.

Gözlem 2.6 *$a_n = 1$ ise $H_n = H_{n-1}$ olduğuna dikkat edelim. Böylece $n \geq 2$ için $a_n \geq 2$ kabul edebiliriz ve buradan b_n süper artan bir dizi olur. $n \geq 2$ için H_n'nin önderinin $a_n b_{n-1} = c_n$ olduğu açıktır.*

Bir S nümerik semigrubu için $\rho : \mathbb{N} \longrightarrow S$, $i \longmapsto \rho(i) = \rho_i$ ile belirlenen dönüşüm sayma dönüşümü olarak adlandırılır ve bire-bir, örten olacak şekildeki tek artan dönüşümdür.

$$S = \{\rho_0 = 0 < \rho_1 < \ldots\}$$

nümerik semigrubu, ρ sayma dönüşümü ile belirlenen nümerik semigrup olarak adlandırılır. S'nin önderi $c = \rho_r$ ise $g = c - r$ dir. $\rho \in S$ elemanlarına kutup ve $n \in \mathbb{N} \setminus S$ elemanlarına boşluk (gap) denir.

Nümerik semigrupların birkaç özelliğini aşağıdaki teoremle ifade edebiliriz.

Teorem 2.7 *A bir küme ve S bir nümerik semigrup olmak üzere,*
(a) $\emptyset \neq A \subseteq \mathbb{N}$ için; $< A >$'nın bir nümerik semigrup olması için gerekli ve yeterli koşul $obeb(A) = 1$ olmasıdır.
(b) $\emptyset \neq A \subseteq \mathbb{N}$ aşikar olmayan alt monoid ise $A, \mathbb{N}$'nin bir nümerik semigrubuna izomorftur.
(c) $S \subseteq \mathbb{N}$ alt monoid ve $S^* := S \setminus \{0\}$ olmak üzere

$$S^* + S^* := \{\rho_i + \rho_j \mid \rho_i, \rho_j \in S^*\}$$

tanımlayalım. $S^* \setminus (S^* + S^*)$, S'nin bir üreteç sistemidir ve her üreteç sistemi tarafından kapsanır.

İspat. *(a)* $(:\Longrightarrow)$ $< A >$ nümerik semigrup olsun. $obeb(A) = d$ ise $s \in A$ için $d \mid s$ dir. $< A >$ nümerik semigrup olduğundan tümleyeni sonludur. $< A >$'da öyle x elemanı vardır ki $d \mid x$ ve $d \mid x+1$ dir. Buradan $d \mid obeb(x, x+1)$ olduğu söylenebilir. Sonuç olarak $d = 1$ olmalıdır.
$(\Longleftarrow:)$ $obeb(A) = 1$ olsun. $< A >$ kümesinin nümerik semigrup olduğunu göstermek için $\mathbb{N} \setminus < A >$'nın sonlu olduğunu göstermek yeterlidir. $obeb(A) = 1$ olduğundan $a_i \in A$ $(i = 1, \ldots, n)$ için öyle $z_1, z_2, ..., z_n \in \mathbb{Z}$ vardır ki $z_1 a_1 + z_2 a_2 + \ldots + z_n a_n = 1$ dir. z_i'lerden negatif olanlar eşitliğin diğer tarafına geçirilirse $i_1, i_2, ..., i_k, j_1, ..., j_l \in \{1, 2, ..., n\}$ olmak üzere $z_{i_1} a_{i_1} + \ldots + z_{i_k} a_{i_k} = 1 - z_{j_1} a_{j_1} - \ldots - z_{j_l} a_{j_l}$ olur. Burada $-z_{j_1} a_{j_1} - \ldots - z_{j_l} a_{j_l} = s \in < A >$ olduğu görülür. Ayrıca, $z_{i_1} a_{i_1} + \ldots + z_{i_k} a_{i_k} \in < A >$ olduğundan $z_{i_1} a_{i_1} + \ldots + z_{i_k} a_{i_k} = s + 1 \in < A >$ ve sonuç olarak $s(s+1) \in < A >$ dır. $n \geq (s-1)s + (s-1)$ ise $n \in < A >$ olduğunu iddia edelim. q ve r pozitif tamsayıları için $0 \leq r < s$ olacak şekilde $n = qs + r$ olsun. $n \geq (s-1)s + (s-1)$ olduğundan $q \geq s - 1 \geq r$ dir. $n = qs + r + (rs) + ((-r)s) = (q - r)s + (s + 1)r \in < A >$ dır. Çünkü $(q - r)$, $r \in \mathbb{N}$ ve $s, s + 1 \in < A >$ dır. Bu durumda $(s - 1)s + (s - 1)$'den küçük elemanlar $\mathbb{N} \setminus < A >$'nın elemanıdır ve sonuç olarak $\mathbb{N} \setminus < A >$ sonludur.
(b) $d = obeb(A)$ olsun. $S = \langle \frac{m}{d} | m \in A \rangle \subseteq \mathbb{N}$, $obeb(S) = 1$ olduğundan (a) yardımıyla S bir nümerik semigruptur. $f : A \longrightarrow S$, $m \longmapsto \frac{m}{d}$ bir monoid izomorfizmidir, yani bire-bir, örten ve $f(a + b) = f(a) + f(b)$ dir.
(c) $\rho \in S^*$ için $\rho \notin S^* \setminus (S^* + S^*)$ ise öyle $x, y \in S^*$ vardır ki $\rho = x + y$ dir.

$x, y < \rho$ için de bu işlemler tekrarlanarak devam ettirildiğinde sonlu adım sonunda öyle $\rho_1, \ldots, \rho_n \in S^* \setminus (S^* + S^*)$ bulunabilir ki $\rho = \rho_1 + \rho_2 + \ldots + \rho_n$ dir. Buradan $S^* \setminus (S^* + S^*)$'nin üreteç sistemi olduğu ispatlanmış olur. Tanımdan her üreteç sistemi tarafından kapsandığı açıktır. ■

Örnek 2.8 (1) $A = \{3, 4, 11\}$ *olsun.* $obeb(A) = 1$ *olduğundan Teorem 2.7 (a)'dan* $< A >$ *bir nümerik semigruptur.*
(2) $A =< 6, 14, 22 >= \{6, 12, 14, 18, 20, 22, 24, 26, \longrightarrow\}$ *olsun.* $obeb(A) = 2$ *olduğundan A nümerik semigrup olmadığı halde, A Teorem 2.7 yardımıyla* $\mathbb{N}$ *'nin bir nümerik semigrubuna izomorftur. Bu nümerik semigrup* $S = \{3, 6, 7, 9, \longrightarrow\}$ *dur.*

Tanım 2.9 *S bir nümerik semigrup ve* $0 \neq n \in S$ *olsun. S'de n'nin Apéry kümesi*

$$Ap(S, n) = \{\rho \in S \mid \rho - n \notin S\} = \{0 = w(0), w(1), \ldots, w(n-1)\}$$

ile tanımlanır. Burada her $i \in \{0, 1, \ldots, n-1\}$ *için* $w(i) \equiv i \ (mod\ n)$ *olacak şekilde S'nin en küçük elemanı* $w(i)$ *dir.*

Gözlem 2.10 $\#Ap(S, n) = n$ *dir.*

Örnek 2.11 (1) $S = \langle 3, 7, 11\rangle = \{0, 3, 6, 7, 9, \longrightarrow\}$ *nümerik semigrubu için*

$$Ap(S, 10) = \{0, 11, 12, 3, 14, 15, 6, 7, 18, 9\}$$

ve $\#Ap(S, 10) = 10$ *dur.*
(2) $S =< 5, 7, 9 >= \{0, 5, 7, 9, 10, 12, 14, \longrightarrow\}$ *olsun.* $\mathbb{N} \setminus S = \{1, 2, 3, 4, 6, 8, 11, 13\}$ *olduğundan dolayı S'nin cinsi* $g = 8$*, Frobenius sayısı* $F(S) = 13$*,* $c = 14$ *ve*

$$Ap(S, 5) = \{0, 16, 7, 18, 9\}$$

dur.

Önerme 2.12 *S bir nümerik semigrup olsun. Her* $\rho \in S$ *için* $\rho = kn + w$ *olacak şekilde tek türlü belirli* $(k, w) \in \mathbb{N}\mathtt{x}Ap(S, n)$ *vardır.*

İspat. Varlık görmek kolaydır. Biz burada tekliği gösterelim. $\rho = k_1 n + w_1 = k_2 n + w_2$ şeklinde yazıldığını varsayalım. $(k_2 - k_1)n = w_2 - w_1$ olur. Buradan $n \mid w_2 - w_1$ ve $w_1 \equiv w_2 \ (mod\ n)$ dir. Burada $w(i)$'ler i kalanını veren S'nin en küçük elemanları olduğundan $w_2 = w_1$ ve $k_2 = k_1$ dir. ■

Örnek 2.13 $S = \langle 4, 7\rangle = \{0, 4, 7, 8, 11, 12, 14, 15, 16, 18, \longrightarrow\}$ *nümerik semigrubu için* $Ap(S, 8) = \{0, 25, 18, 11, 4, 21, 14, 7\} = \{0 = w(0), w(1), \ldots, w(7)\}$ *dir.* $\rho_1 = 33$ *ve* $\rho_2 = 44$ *elemanlarını alalım.* $\rho_1 = 33$ *için* $(1, 25) \in \mathbb{N}\mathtt{x}Ap(S, 8)$ *ve* $\rho_2 = 44$ *için* $(5, 4) \in \mathbb{N}\mathtt{x}Ap(S, 8)$ *dir.*

Lemma 2.14 *S bir nümerik semigrup ve* $n \in S$ *olsun.* $x, y \in S$ *ve* $x + y \in Ap(S, n)$ *ise* $\{x, y\} \subseteq Ap(S, n)$ *dir.*

İspat. $x, y \in S$ ve $x+y \in Ap(S,n)$ ise $x+y-n \notin S$ dir. Bu durumda, ya $y-n \notin S$ ya da $x-n \notin S$ dir. Dolayısıyla $\{x,y\} \subseteq Ap(S,n)$ dir. ■

Tanım 2.15 *Bir nümerik semigrubun üreteç sisteminin hiç bir özalt kümesi üreteç değilse o üreteç sistemine minimal üreteç sistemi denir.*

Teorem 2.16 *Her nümerik semigrup tek türlü belirli minimal üreteç sistemine sahiptir ve bu sistem sonludur.*

İspat. S bir nümerik semigrup olsun. Teorem 2.7 (c)'den $S^* \setminus (S^* + S^*)$ bir minimal üreteç sistemidir. $K := Ap(S,n) \cup \{n\}$ kümesini ele alalım. Önerme 2.12'den $S =< K >$ olur. K, S için bir üreteç sistemidir ve $S^* \setminus (S^* + S^*) \subseteq K$ dır. K sonlu olduğundan $S^* \setminus (S^* + S^*)$ de sonludur. ■

Tanım 2.17 *S bir nümerik semigrup ve $\{n_1 < n_2 < \ldots < n_p\}$, S'nin minimal üreteç sistemi olsun. n_1'e, S'nin katlılığı (multiplicity), minimal üreteç sisteminin kardinalitesi olan p sayısına S'nin gömülüş boyutu (embedding dimension) denir ve sırasıyla $m(S)$, $e(S)$ ile gösterilir.*

Önerme 2.18 *S bir nümerik semigrup olsun. Bu durumda*
(a) $m(S) = \min(S \setminus \{0\})$
(b) $e(S) \leq m(S)$
dir.

İspat. S'de en küçük pozitif tamsayının S'nin katlılığı olduğu açıktır. Diğer durumu ele alalım. Teorem 2.16'nın ispatından yararlanarak $\{m(S)\} \cup Ap(S, m(S)) \setminus \{0\}$, $m(S)$ elemanlı bir üreteç sistemidir ve minimal üreteç sisteminin eleman sayısı olan $e(S)$'den daha büyük veya eşittir. ■

Özel olarak $e(S) = m(S)$ ise nümerik semigrup maksimal gömülüş boyutuna (maximal embedding dimension) sahiptir denir.

$e(S) = 1$ olması için gerekli ve yeterli koşul $S = \mathbb{N}$ dir. $S = \{0, n, \longrightarrow\}$, n katlılığına sahip bir nümerik semigruptur.

Önerme 2.19 *S bir nümerik semigrup ve $0 \neq n \in S$ olsun. O zaman*
(a) $F(S) = (maks\ Ap(S,n)) - n$
(b) $g = \frac{1}{n}\left(\sum_{w \in Ap(S,n)} w\right) - \frac{n-1}{2}$
dır.

İspat. *(a)* Apéry kümesinin tanımından $(maks\ Ap(S,n)) - n \notin S$ olduğu açıktır. Eğer $x > (maks\ Ap(S,n)) - n$ ise $x + n > maks\ Ap(S,n)$ dir. $w \equiv x + n\ (mod\ n)$ olacak şekilde $w \in Ap(S,n)$ olsun. $w < x + n$ olduğundan uygun k pozitif tamsayısı için $x = w + kn$ olmasını gerektirir. Sonuç olarak $w \in Ap(S,n) \subseteq S$ olduğundan $x - n = w + (k-1)n \in S$ dir. O halde S'ye ait olmayacak şekilde en büyük seçim

$F(S) = (maksAp(S,n)) - n$ dir.
(b) Her $w \in Ap(S,n)$ için $i \in \{0,\ldots,n-1\}$ olmak üzere $w \equiv i \ (mod\ n)$ ise $w = k_i n + i$ olacak şekilde negatif olmayan k_i tamsayıları vardır. Tanım 2.9 daki notasyonları kullanarak

$$Ap(S,n) = \{0, w(1) = k_1 n + 1, w(2) = k_2 n + 2, \ldots, w(n-1) = k_{n-1} n + (n-1)\}$$

dir. $w(i) \equiv x \ (mod\ n)$ olmak üzere, $x \in S$ dir ancak ve ancak $w(i) \leq x$ dir.

$w(1) \in S$ iken $w(1) - n \notin S$, $w(1) - 2n \notin S$,..., $w(1) - k_1 n \notin S$ olduğundan $w(1)$ için k_1 tane boşluk vardır. Benzer şekilde $w(n-1) \in S$ iken $w(n-1) - n \notin S$, $w(n-1) - 2n \notin S$,..., $w(n-1) - k_{n-1} n \notin S$ olduğu görülür. O halde $w(n-1)$ için k_{n-1} tane boşluk vardır. Buradan

$$\begin{aligned} g &= k_1 + \ldots + k_{n-1} \\ &= \frac{1}{n}\left((k_1 n + 1) + \ldots + k_{n-1} n + (n-1)\right) - \frac{n-1}{2} \\ &= \frac{1}{n}\left(\sum_{w \in Ap(S,n)} w\right) - \frac{n-1}{2} \end{aligned}$$

elde edilir. ■

Örnek 2.20 (1) $S = \langle 4,5,7\rangle = \{0,4,5,7,\longrightarrow\}$ *nümerik semigrubu için* $F(S) = 6$ *ve* $G(S) = \{1,2,3,6\}$ *olduğundan* $g = 4$ *olduğu açıktır. Diğer taraftan* $n = 11$ *için*

$$Ap(S,11) = \{0,12,13,14,4,5,17,7,8,9,10\}$$

dir. Önerme 2.19'dan $F(S) = 17 - 11 = 6$ *ve* $g = \frac{1}{11}.99 - \frac{11-1}{2} = 4$ *olduğu elde edilmiş olur.*
(2) $b > a$ *ve* $obeb(a,b) = 1$ *olmak üzere* S, $\langle a,b\rangle$ *minimal üreteç sistemi ile üretilen nümerik semigrup olsun.*

$$S = \{0,a,b,a+b,2a,2b,2a+b,2b+a,2(a+b),\ldots\}$$

dır ve

$$Ap(S,a) = \{0,b,2b,\ldots,(a-1)b\}$$

dir. O halde Önerme 2.19 yardımıyla

$$F(\langle a,b\rangle) = maks\ Ap(S,a) - a = (a-1)b - a = ab - a - b$$

ve

$$g = \frac{1}{a}\left(\sum_{w \in Ap(S,a)} w\right) - \frac{a-1}{2} = \frac{1}{a}\left(\frac{a(a-1)b}{2}\right) - \frac{a-1}{2} = \frac{ab-a-b+1}{2}$$

dir. Buradan $g = \frac{F(S)+1}{2}$ *olduğu elde edilir.*

S bir nümerik semigrup ise $\rho \in S$ iken $F(S) - \rho \notin S$ olabilir. Buradan S bir nümerik semigrup ise $g \geq \frac{F(S)+1}{2}$ olduğu görülür.

Tanım 2.21 *S bir nümerik semigrup olsun. $x \notin S$ ve her $\rho \in S \setminus \{0\}$ için $x+\rho \in S$ ise x'e Pseudo-Frobenius sayısı denir. S'nin Pseudo-Frobenius sayılarının kümesi $PF(S)$ ve kümenin eleman sayısı $\#\ PF(S) = t(S)$ ile gösterilir ve S'nin tipi olarak adlandırılır.*

Örnek 2.22 (1) *$S = \langle 5,6,8\rangle = \{0,5,6,8,10,11,\longrightarrow\}$ nümerik semigrubu olsun. $PF(S)$ tanımından $3 \notin S$ için $3+6 \notin S$ olduğundan $3 \notin PF(S)$ dir. $4 \notin S$ için $4+5 \notin S$ olduğundan $4 \notin PF(S)$ dir. $PF(S) = \{7,9\}$ olduğu elde edilir.*
(2) *$S = \langle 4,5,7\rangle = \{0,4,5,7,\longrightarrow\}$ nümerik semigrubu için $PF(S) = \{3,6\}$ dır.*
(3) *$S = \langle 3,8\rangle = \{0,3,6,8,9,11,12,14,\longrightarrow\}$ nümerik semigrubu için $PF(S)$'nin elemanı sadece $F(S)$ dır.*

Tamsayılar kümesi üzerinde $b-a \in S$ olduğu durumda $a \leq_S b$ bağıntısını tanımlayalım. Bu bağıntı bir sıralama bağıntısıdır. Burada, $\mathbb{Z}\backslash S$'nin $\leq_S$ sıralamasına göre maksimal elemanlarıyla Pseudo-Frobenius sayıları elde edilir.

Önerme 2.23 *S bir nümerik semigrup ve $0 \neq n \in S$ olsun. Bu durumda*

$$PF(S) = \{w - n \mid w \in maks_{\leq_S} Ap(S,n)\}$$

olur.

İspat. $0 \neq n \in S$ ve $x \in PF(S)$ olsun. $x \notin S$ ve $x+n \in S$ dir, yani, $x+n \in Ap(S,n)$ dir. $x+n \leq_S w$ olacak şekilde uygun $w \in Ap(S,n)$ alalım. Böylece $w-(x+n) = (w-n)-x \in S$ dir. Bunun anlamı bazı $\rho \in S$ için $w-n = x+\rho$ dir. $w-n \notin S$ ve $x \in PF(S)$ olduğundan bu ρ'nun sıfır olması gerektiğini söyler ve böylece $w = x+n$ dir.

$w \in maks_{\leq_S} Ap(S,n)$ alalım. $w-n \notin S$ dir ve $0 \neq \rho \in S$ için $w-n+\rho \notin S$ ise $w+\rho \in Ap(S,n)$ olur. Bu w'nin maksimal olması ile çelişir. ■

Örnek 2.24 *$S = \langle 5,6,8\rangle = \{0,5,6,8,10,\longrightarrow\}$ nümerik semigrubunu alalım. $Ap(S,6) = \{0,13,8,15,10,5\}$ dir. $\leq_S$ sıralamasına göre $13-8 \in S$'den $8 \leq_S 13$, $13-5 \in S$'den $5 \leq_S 13$, $15-5 \in S$'den $5 \leq_S 15$ve son olarak $15-10 \in S$'den $10 \leq_S 15$ dir. $13-10 \notin S$ ve $15-13 \notin S$ olduğundan karşılaştırılamazlar. Buradan $maks_{\leq_S} Ap(S,6) = \{13,15\}$ dir ve buna göre Önerme 2.23'den $PF(S) = \{13-6, 15-6\} = \{7,9\}$ dur.*

$Ap(S,n)$'nin elemanlarında 0 elemanı hiç bir zaman maksimal olamayacağı için Önerme 2.23'den yararlanarak nümerik semigrubun tipi için bir üst sınır elde edilir.

Sonuç 2.25 *S bir nümerik semigrup ise $t(S) \leq m(S)-1$ dir.*

İspat. $t(S)$'nin tanımından açıktır. ■

Özel olarak $S = \langle m, m+1, \ldots, m+(m-1)\rangle$ ise $PF(S) = \{1, 2, \ldots, m-1\}$ dir.

Önerme 2.26 *S bir nümerik semigrup olsun. Bu durumda,*
(a) $maks_{\leq_S}(\mathbb{Z} \setminus S)$ dir.
(b) $x \in \mathbb{Z} \setminus S$ olması için gerek ve yeter koşul uygun $f \in PF(S)$ için $f - x \in S$ olmasıdır.

İspat. (a) $PF(S)$, $\mathbb{Z}\setminus S$'nin $\leq_S$ ye göre maksimal elemanları ile elde edilebildiğinden ispat açıktır.
(b) $(: \Longrightarrow)$ $x \notin S$ ve $n \in S \setminus \{0\}$ ise $x = w - kn$ olacak şekilde $w \in Ap(S, n)$ ve $k \in \mathbb{N} \setminus \{0\}$ vardır. $PF(S) = maks_{\leq_S} Ap(S, n) = \{w_{j_1}, \ldots, w_{j_t}\}$ ise $i \in \{1, \ldots, t\}$ için $w_{j_i} - w \in S$ olsun. $f = w_{j_i} - n$ tanımlarsak Önerme 2.23'den $f \in PF(S)$ olur. Bu durumda, $f - x = w_{j_i} - n - (w - kn) = (w_{j_i} - w) + (k-1)n \in S$ dır.
$(\Longleftarrow :)$ $f - x \in S$ ve $f \notin S$ olduğundan $x \in \mathbb{Z} \setminus S$ dir. ■

Önerme 2.27 *S bir nümerik semigrup olsun.*

$$N(S) = \{\rho \in S \mid \rho < F(S)\}$$

kümesi tamamıyla S ile belirlenir. $\#N(S) = n(S)$ ise $g + n(S) = F(S) + 1$ dir.

İspat. $N(S)$ ve $G(S)$ tanımından açıktır. ■

Önerme 2.26 (b)'den $x \notin S$ ise $x \leq_S f$ olacak şekilde $f \in PF(S)$ olduğu biliniyor.

$$f_x = \min \{f \in PF(S) \mid f - x \in S\}$$

tanımlayalım.

$$\Psi : G(S) \longrightarrow PF(S) \mathtt{x} N(S)$$

$\Psi(x) = (f_x, f_x - x)$ ile tanımlanan dönüşüm içine dönüşümdür ve $g \leq t(S)n(S)$ sınırını verir.

2.1.1. İndirgenemez nümerik semigrup

Tanım 2.28 *Bir nümerik semigrup, onu içeren nümerik semigrupların kesişimi olarak ifade edilemiyor ise indirgenemez nümerik semigrup olarak adlandırılır.*

İndirgenemez nümerik semigrupların, belirlenmiş bir sayı için o sayıyı Frobenius sayısı kabul eden nümerik semigrupların kümesinde maksimal olduğu gösterilecektir. Öncelikle bir nümerik semigruba Frobenius sayısını eklediğimizde yine bir nümerik semigrup olduğunu gösterelim.

Lemma 2.29 *$S \neq \mathbb{N}$ nümerik semigrubu olsun. O zaman $S \cup \{F(S)\}$ yine bir nümerik semigruptur.*

İspat. $\mathbb{N} \setminus S$ sonlu olduğundan $\mathbb{N} \setminus (S \cup \{F(S)\})$ sonludur. $a, b \in S \cup \{F(S)\}$ alalım. Bunlardan herhangi biri $F(S)$ ise $a + b \geq F(S)$ ve $a + b \in S \cup \{F(S)\}$ olur. a ve b, S'nin elemanı ise $a + b \in S \subseteq S \cup \{F(S)\}$ olur. Ayrıca $0 \in S \cup \{F(S)\}$ olduğu için $S \cup \{F(S)\}$'nin nümerik semigrup olduğu elde edilir. ■

Örnek 2.30 *Örnek 2.22 (3)'te verilen S nümerik semigrubu için $F(S) = 13$ olduğundan Lemma 2.29 yardımıyla $S \cup \{13\} = \{0, 3, 6, 8, 9, 11, \longrightarrow\}$ bir nümerik semigruptur.*

Teorem 2.31 *S bir nümerik semigrup olmak üzere aşağıdaki koşullar denktir:*
(a) S indirgenemezdir.
(b) S, $F(S)$ Frobenius sayısına sahip tüm nümerik semigrupların kümesinde maksimaldir.
(c) S, $F(S)$ Frobenius sayısını içermeyen tüm nümerik semigrupların kümesinde maksimaldir.

İspat. $(a \Longrightarrow b)$: T bir nümerik semigrup, öyle ki $S \subseteq T$ ve $F(T) = F(S)$ olsun. Bu durumda $S = (S \cup \{F(S)\}) \cap T$ dir. S indirgenemez olduğundan $S = T$ elde edilir.
$(b \Longrightarrow c)$: T bir nümerik semigrup, öyle ki $S \subseteq T$ ve $F(S) \notin T$ olsun. Bu durumda, $T \cup \{F(S) + 1, F(S) + 2, \longrightarrow\}$ kümesi $F(S)$ Frobenius sayısına sahip ve S'yi içeren bir nümerik semigruptur. $S = T \cup \{F(S) + 1, F(S) + 2, \longrightarrow\}$ ve $S = T$ olur.
$(c \Longrightarrow a)$: S_1 ve S_2, S'yi içeren iki nümerik semigrup olsun. Hipotezden $F(S) \in S_1$ ve $F(S) \in S_2$ olur. Böylece $S \neq S_1 \cap S_2$ dir. ■

Sonuç olarak, bir nümerik semigrup indirgenebilir ise $S \subseteq T$ ve $F(T) = F(S)$ olacak şekilde indirgenemez T nümerik semigrubu vardır. Aşağıdaki ifade bu indirgenemez nümerik semigrubun yapısını verir.

Lemma 2.32 *S bir nümerik semigrup ve*

$$h = maks\ \{x \in \mathbb{Z} \setminus S \mid F(S) - x \notin S\ ve\ x \neq F(S)/2\}$$

olsun. Bu durumda $S \cup \{h\}$, Frobenius sayısı $F(S)$ olan bir nümerik semigruptur.

İspat. S'nin nümerik semigrup olmasından yararlanarak $\mathbb{N} \setminus (S \cup \{h\})$'nın sonlu ve $0 \in S \cup \{h\}$ olduğu açıktır.

$$H = \{x \in \mathbb{Z} \setminus S \mid F(S) - x \notin S \text{ ve } x \neq F(S)/2\}$$

ve $x \in H$ ise $F(S) - x \in H$ olur. Buradan $h > F(S)/2$ elde edilir. $\rho \in S^*$ için $h + \rho \notin S$ ise h'nin maksimal olmasından dolayı $F(S) - (h + \rho) = t \in S$ ve böylece $F(S) - h = t + \rho \in S$ olur. Bu ise tanımla çelişir.

$2h \notin S$ ise tekrar h'nin maksimal olmasını kullanarak $F(S) - 2h = t \in S$ elde edilir. Benzer şekilde $h + t \in S$ olur. Ayrıca $h + t = F(S) - h \notin S$ elde edilir. Bu ise çelişkidir. ■

Örnek 2.33 *$S = \langle 3, 10, 11\rangle = \{0, 3, 6, 9, \longrightarrow\}$ semigrubu olsun. Lemma 2.29'dan $F(S) = 8$ için $S \cup \{8\}$'in nümerik semigrup olduğunu biliyoruz. $S \cup \{7\}$'nin de nümerik semigrup olduğunu iddia edelim. Lemma 2.32'den $4 \notin S$ için $4 = F(S)/2$ olduğundan Lemma 2.32'ün ispatındaki H kümesine dahil olamaz. Öte yandan $1 \notin S$ için $8 - 1 \notin S$ ve $7 \notin S$ için $8 - 7 \notin S$ dir. Maksimal eleman $h = 7$ olduğundan $S \cup \{7\}$ bir nümerik semigruptur.*

2.1.2. Simetrik nümerik semigrup

Tanım 2.34 *S bir indirgenemez nümerik semigrup olmak üzere $F(S)$ tek ise S'ye simetrik nümerik semigrup denir, kısaca S simetriktir diyeceğiz.*

Önerme 2.35 *S bir nümerik semigrup olsun.*
(a) S'nin simetrik olması için gerekli ve yeterli koşul $F(S)$ pozitif tek tamsayı ve $x \in \mathbb{Z} \setminus S$, $F(S) - x \in S$ olmasıdır.
(b) S'nin simetrik olması için gerekli ve yeterli koşul $g = \frac{F(S)+1}{2}$ olmasıdır.
(c) $e(S) = 2$ olan her nümerik semigrup simetriktir ve $t(S) = 1$ dir.
(d) S bir nümerik semigrup ve x, $\mathbb{N} \setminus S$'de olan tek pozitif tamsayı olsun. O zaman $S \subseteq \bar{S}$ ve $F(\bar{S}) = x$ olacak şekilde $\bar{S}$ simetrik nümerik semigrubu vardır.
(e) S bir nümerik semigrup ve x, S'de olmayan çift pozitif tamsayı olmak üzere aşağıdaki koşullar denktir:

(1) $S \subseteq \bar{S}$ ve $x \notin \bar{S}$ olacak şekilde bir $\bar{S}$ simetrik semigrubu vardır.

(2) $x + y \notin \langle S, y\rangle$ olacak şekilde y tek pozitif tamsayısı vardır.

(f) S bir nümerik semigrup ve $0 \neq n \in S$ olsun. $Ap(S, n) = \{a_0 < a_1 < \ldots < a_{n-1}\}$ olmak üzere, S simetriktir ancak ve ancak her $i \in \{0, 1, \ldots, n-1\}$ için $a_i + a_{n-1-i} = a_{n-1}$ dir.

İspat. $(a)(: \Longrightarrow)$ $F(S) - x \notin S$ olacak şekilde $x \in \mathbb{Z} \setminus S$ var olduğunu kabul edelim. İndirgenemez olmasından dolayı Lemma 2.32'den, öyle h tamsayısı vardır. Böylece $S \cup \{h\}$, $F(S)$ Frobenius sayısına sahip bir nümerik semigruptur. Bu ifade, S indirgenemez olduğundan S'nin $F(S)$ Frobenius sayısına sahip nümerik semigruplar kümesinde maksimal olmasıyla çelişir.
$(\Longleftarrow :)$ S'nin indirgenemez olduğunu göstermek yeterlidir. Bunun için, S'nin $F(S)$'yi içermeyen nümerik semigrupların kümesinde maksimal olduğunu göstermeliyiz. T nümerik semigrubu, $S \subsetneq T$ ve $F(S) \notin T$ olacak şekilde bir nümerik semigrup olsun. $x \in (T \setminus S) \subset (\mathbb{Z} \setminus S)$ elemanı göze alındığında hipotezden $F(S) - x \in S$ ve $F(S) - x \in T$ olur. Fakat bu $F(S) = x + (F(S) - x) \in T$ olmasını gösterir. Böylece, S, $F(S)$'yi içermeyen nümerik semigrupların kümesinde maksimaldir.
(b) g tane boşluk, $\{x_1, x_2, \ldots, x_g\}$ şeklinde olsun. $x_1 \notin S$ için simetrik nümerik semigrup tanımından hareket edersek $F(S) - x_1 \in S$ olur. Benzer şekilde S'nin $x_2, x_3, \ldots, x_g$ elemanları için $F(S) - x_2, F(S) - x_3, \ldots, F(S) - x_g \in S$ olur. Burada, $n(S) = g$ olduğundan Önerme 2.27'den yararlanarak $g = \frac{F(S)+1}{2}$ elde edilir.
(c) Örnek 2.20 (2)'den S nümerik semigrubu için $g = \frac{F(S)+1}{2}$ olduğundan, S nümerik

semigrubu simetriktir. Ayrıca $maks_{\leq_S} Ap(S,a) = \{(a-1)b\} = F(S)+a$ dır.

$$PF(S) = \{F(S)+a-a\} = \{F(S)\} = \{ab-a-b\}$$

olduğundan $t(S) = 1$ dir.
(d) $S' = S \cup \{x+1, x+2, \ldots\}$ olsun. S' bir nümerik semigrup ve $F(S') = x$ olduğu açıktır. $\bar{S}$, Frobenius sayısı x olan nümerik semigrupların kümesinde maksimal olsun. O halde $\bar{S}$ indirgenemez ve $F(\bar{S}) = x$ tek olduğundan $\bar{S}$ nümerik semigrubu, $S \subseteq \bar{S}$ olacak şekilde simetrik nümerik semigruptur.
(e) $(1 \Longrightarrow 2)$ $y = F(\bar{S}) - x$ olsun. x çift ve $F(\bar{S})$ tek olduğundan y tektir. Daha fazlası $x \notin \bar{S}$ ve $\bar{S}$ simetrik olduğundan $y = F(\bar{S}) - x \in \bar{S}$ dir. Buradan $\langle S, y\rangle \subseteq \bar{S}$ ve $x + y = F(\bar{S}) \notin \langle S, y\rangle$ olur.
$(2 \Longrightarrow 1)$ $S' = \langle S, y\rangle \cup \{x+y+1, x+y+2, \ldots\}$ olsun. S', $x+y$ tek Frobenius sayısı ile bir nümerik semigruptur ve (d) yardımıyla $S' \subseteq \bar{S}$ ve $F(\bar{S}) = x+y$ olacak şekilde $\bar{S}$ simetrik nümerik semigrubu vardır. O halde, $S \subseteq \bar{S}$ ve $x \notin \bar{S}$ dır. Aksi halde $y \in \bar{S}$ olduğundan $F(\bar{S}) = x + y \in \bar{S}$ elde edilir. Bu ise imkansızdır.
(f) Aşağıdaki ifade S nümerik semigrubu simetrik değilse $S \subseteq T$, $F(T)$ tek olacak şekilde öyle T simetrik nümerik semigrubunun varlığını söyler.
$(: \Longrightarrow)$ S'de n'nin Apéry kümesini dikkate alalım. Önerme 2.19'dan $F(S) = a_{n-1} - n$ dir. $a_i - n \notin S$ ve S simetrik olduğundan, $F(S) - (a_i - n) = a_{n-1} - a_i \in S$ dir. Lemma 2.14'den $a_{n-1} = a_i + a_j$ olacak şekilde $j \in \{0, 1, \ldots, n-1\}$ vardır ve $\{a_i, a_j\} \subseteq Ap(S,n)$ dir. Ayrıca $a_0 < a_1 < \ldots < a_{n-1}$ olduğundan $j = n-1-i$ olmalıdır.
$(\Longleftarrow :)$ Hipotez yardımıyla $\{a_{n-1}\} = maks_{\leq_S} Ap(S,n)$ dir. Önerme 2.23'den $PF(S) = \{F(S)\}$ ve Önerme 2.26'den $\{F(S)\} = maksimal_{\leq_S}(\mathbb{Z} \setminus S)$ olur. Özel olarak $x \in \mathbb{Z} \setminus S$ ise $F(S) - x \in S$ dir. Bunlara ek olarak $F(S)/2$ bir tamsayı ise $F(S)/2 \in \mathbb{Z} \setminus S$ dir. Bu, $F(S) - F(S)/2 = F(S)/2 \in S$ olmasını gerektirir ve çelişki elde edilir. $F(S)$ tek tamsayı ve (a) sağlandığından S simetriktir. ■

Örnek 2.36 (1) *$S = \langle 6, 9, 11\rangle$ olsun. $x = 13 \notin S$ tek tamsayısı için $F(S') = 13$ olacak şekilde $S' = S \cup \{14, 15, \longrightarrow\}$ nümerik semigrubunu alalım.*

$$\begin{aligned} Ap(S', 9) &= \{0, 19, 11, 12, 22, 14, 6, 16, 17\} \\ &= \{0 < 6 < 11 < 12 < 14 < 16 < 17 < 19 < 22\} \end{aligned}$$

ve Önerme 2.35 (f) yardımıyla en azından $i = 1$ için $a_1 + a_7 = 25 \neq 22 = a_8$ olduğundan S' simetrik değildir. Fakat $\bar{S} = \{0, 5, 6, 9, 10, 11, 12, 14, \longrightarrow\}$ nümerik semigrubu için

$$\begin{aligned} Ap(\bar{S}, 9) &= \{0, 10, 11, 12, 22, 5, 6, 16, 17\} \\ &= \{0 < 5 < 6 < 10 < 11 < 12 < 16 < 17 < 22\} \end{aligned}$$

ve Önerme 2.35 (f) yardımıyla $S' \subseteq \bar{S}$, $F(\bar{S}) = 13$ olacak şekilde simetrik nümerik semigruptur.
(2) *$S = \langle 5, 12, 19\rangle = \{0, 5, 10, 12, 15, 17, 19, 20, 22, 24, 25, 27, 29, 30, 31, 32, 34, \longrightarrow\}$ nümerik semigrubu olsun.*

$$\begin{aligned} Ap(S, 5) &= \{0, 31, 12, 36, 19\} \\ &= \{0 < 12 < 19 < 31 < 36\} \end{aligned}$$

ve Önerme 2.35 (f) yardımıyla S'nin simetrik nümerik semigrup olup olmadığı görülebilir. $8 \notin S$ çift tamsayısı ve 5 tek tamsayısı için $8+5 \notin \langle S, 5\rangle$ olduğundan Önerme 2.35 (e)'den $S \subseteq \bar{S}$ ve $8 \notin \bar{S}$ olacak şekilde $\bar{S}$ simetrik nümerik semigrubunun varlığı açıktır.

Sonuç 2.37 *S bir nümerik semigrup olsun.*
(a) Aşağıdaki koşullar denktir:

(1)*S simetriktir.*

(2) $PF(S) = \{F(S)\}$

(3) $t(S) = 1$ *dir.*

(b) $0 \neq n \in S$ olsun. S'nin simetrik olması için gerekli ve yeterli koşul

$$maks_{\leq_S} Ap(S, n) = \{F(S) + n\}$$

olmasıdır.

İspat. *(a)* $(1 \Longleftrightarrow 2)$ Önerme 2.35 (f)'nin ispatından, $(2 \Longleftrightarrow 3)$ tanımdan hareketle açıktır.
(b) $(:\Longrightarrow)$ S simetrik ise (a)'dan $PF(S) = \{F(S)\}$ dır ve böylece $maks_{\leq_S} Ap(S, n) = \{F(S) + n\}$ dir.
$(\Longleftarrow:)$ $maks_{\leq_S} Ap(S, n) = \{F(S)+n\}$ ise $PF(S) = \{(F(S)+n)-n\} = \{F(S)\}$ dir. Böylece (a)'dan S simetriktir. ■

Örnek 2.38 *$S = \langle 6, 9, 11\rangle$ simetrik nümerik semigrubu için $F(S) = 25$ ve Sonuç 2.37 (b)'den $maks_{\leq_S} Ap(S, 9) = F(S) + 9 = 34$ dür. Diğer taraftan,*

$$Ap(S, 9) = \{0, 6, 11, 12, 17, 22, 23, 28, 34\}$$

dir ve $maks_{\leq_S}\ Ap(S, 9) = 34$ dür.

Lemma 2.39 *(a) S, $m(S) \geq 3$ ile bir simetrik nümerik semigrup olsun. O zaman*

$$e(S) \leq m(S) - 1$$

dir.
(b) m ve q, $m \geq 2q + 3$ olacak şekilde pozitif tamsayılar ve S, $(\mathbb{N}, +)$'nın

$$\{m, m + 1, qm + 2q + 2, \ldots, qm + (m - 1)\}$$

ile üretilen alt monoidi olsun. S, katlılığı m ve gömülüş boyutu $e = m - 2q$ olan bir simetrik nümerik semigruptur. Ayrıca $F(S) = 2qm + 2q + 1$ dir.
(c) m ve q, $m \geq 2q + 4$ olacak şekilde negatif olmayan tamsayılar ve S, $(\mathbb{N}, +)$'nın

$$\{m, m + 1, (q + 1)m + q + 2, \ldots, (q + 1)m + m - q - 2\}$$

ile üretilen alt monoidi olsun. S, m katlılık ve $e = m-2q-1$ gömülüş boyutu ile bir simetrik nümerik semigruptur. Ayrıca $F(S) = 2(q + 1)m - 1$ dir.
(d) m ve e, $2 \leq e \leq m - 1$ olacak şekilde tamsayılar olsun. Katlılık $m(S) = m$ ve gömülüş boyutu $e(S) = e$ olacak şekilde bir simetrik nümerik semigrup vardır.

İspat. (a) $Ap(S, m(S)) = \{0 = a_0 < a_1 < \ldots < a_{m(S)-1}\}$ olsun. Önerme 2.35 (f) yardımıyla her $i \in \{0, 1, \ldots, m(S)-1\}$ için $a_{m(S)-1} = a_i + a_{m(S)-1-i}$ olur. $m(S) \geq 3$ ise $a_{m(S)-1}$ toplam şeklinde yazılabileceği için minimal üreteçin elemanı olamaz. O halde $i = 1$ seçebiliriz. $Ap(S, m(S))$'nin minimal üreteç olmayan sıfırdan farklı en az bir elemanı olduğundan $e(S) \leq m(S) - 1$ dir.
(b) (Rosales ve Garcia-Sanchez 2009).
(c) (Rosales ve Garcia-Sanchez 2009).
(d) $e = 2$ ise $S = \langle m, m+1 \rangle$, m katlılık ve e gömülüş boyutu ile bir simetrik nümerik semigruptur. Böylece $e \geq 3$ kabul edebiliriz. İki durumda inceleyelim:

$m - e$ çift ise $m - e = 2q$ olacak şekilde $q \in \mathbb{N} \setminus \{0\}$ vardır. Daha fazlası $e \geq 3$, $m \geq m - e + 3$ olmasını sağlar ve sonuç olarak $m \geq 2q + 3$ dir. Lemma 2.39 (b)'den m katlılık ve $e = m - 2q$ gömülüş boyutu ile bir simetrik nümerik semigrubun varlığı açıktır.

$m - e$ tek ise $m - e = 2q + 1$ olacak şekilde $q \in \mathbb{N}$ vardır. $e \geq 3$, $m \geq m - e + 3$ olmasını sağlar ve sonuç olarak $m \geq 2q + 4$ dür. Lemma 2.39 (c)'den m katlılık ve $e = m - 2q - 1$ gömülüş boyutu ile bir simetrik nümerik semigrubun varlığı açıktır. ■

Örnek 2.40 (1) *$m = 5$ ve $q = 1$ için $S = \langle 5, 6, 7 \rangle$ alt monoidi olsun. O zaman Lemma 2.39 (b) yardımıyla S, $m = 5$ katlılık ve $e = 3$ gömülüş boyutuna sahip bir simetrik nümerik semigruptur. Ayrıca $F(S) = 13$ tür.*
(2) *$m = 10$ ve $q = 3$ için S, $\{10, 11, 45\}$ ile üretilen alt monoid olsun. O zaman Lemma 2.39 (c)'den S, $m = 10$ katlılık ve $e = 3$ gömülüş boyutuna sahip bir simetrik nümerik semigruptur. Ayrıca $F(S) = 79$ dır.*

Önerme 2.35 (b)'nin bir sonucu olarak indirgenemez nümerik semigruplar $F(S)$ Frobenius sayısına sahip, en az olası cinse sahip nümerik semigruplardır. Ayrıca, S'nin maksimal gömülüş boyutuna sahip bir simetrik nümerik semigrup olması için gerek ve yeter koşul $m(S) = 2$ olmasıdır. Çünkü Lemma 2.39 (a) yardımıyla geriye kalan nümerik semigruplar için maksimal gömülüş boyutu olamaz.

2.1.3. Pseudo-simetrik nümerik semigrup

Tanım 2.41 *S bir indirgenemez nümerik semigrup olmak üzere $F(S)$ çift ise S'ye pseudo-simetrik nümerik semigrup denir, kısaca S pseudo-simetriktir diyeceğiz.*

Önerme 2.42 *(a) S'nin pseudo-simetrik olması için gerek ve yeter koşul $F(S)$ çift ve $x \in \mathbb{Z} \setminus S$ için, ya $F(S) - x \in S$ yada $x = F(S)/2$ olmasıdır.*
(b) S pseudo-simetriktir ancak ve ancak $g = \frac{F(S)+2}{2}$ dir.
(c) S pseudo-simetrik nümerik semigrup ve $n \in S$ olsun. $\frac{F(S)}{2} + n \in Ap(S, n)$ dır, diğer bir deyişle $\frac{F(S)}{2} \in PF(S)$ dir.
(d) S, çift Frobenius sayısı ile verilen bir nümerik semigrup ve $n \in S \setminus \{0\}$ olsun. S'nin pseudo-simetrik olması için gerek ve yeter koşul

$$Ap(S, n) = \{a_0 < a_1 < \ldots < a_{n-2} = F(S) + n\} \cup \{\frac{F(S)}{2} + n\}$$

ve her $i \in \{0, 1, \ldots, n-2\}$ *için* $a_i + a_{n-2-i} = a_{n-2}$ *olmasıdır.*

İspat. (*a*) Önerme 2.35 (a)'nın ispatına benzer şekilde gösterilir.
(*b*) $x \neq \frac{F(S)}{2}$ olacak şekilde her $x \in \mathbb{Z} \setminus S$ için $F(S) - x \in S$ ve $x = \frac{F(S)}{2} \in \mathbb{Z} \setminus S$ için $F(S) - x \notin S$ olduğundan $n(S) = g - 1$ dir. Önerme 2.27'den yararlanarak $F(S) + 1 = g + (g-1)$ olur. Böylece $g = \frac{F(S)+2}{2}$ dir.
(*c*) $\frac{F(S)}{2} \notin S$ olduğundan $\frac{F(S)}{2} + n \in S$ olduğunu ispatlamalıyız. Tersini iddia edelim. (a) yardımıyla $F(S) - (\frac{F(S)}{2} + n) = \frac{F(S)}{2} - n \in S$ dir. Bu $\frac{F(S)}{2} = \frac{F(S)}{2} - n + n \in S$ olmasını sağlar. Fakat bu imkansızdır.
(*d*) ($: \Longrightarrow$) (c) yardımıyla $\frac{F(S)}{2} + n \in Ap(S, n)$ dir. Önerme 2.19'dan

$$\frac{F(S)}{2} + n < maks_{\leq_S} Ap(S, n) = F(S) + n$$

dır. $w \in Ap(S, n) \setminus \{\frac{F(S)}{2} + n\}$ ise $w - n \notin S$ ve $w - n \neq \frac{F(S)}{2}$ dir. Önerme 2.35 (a)'dan $F(S) - (w - n) \in S$ ve böylece $maks_{\leq_S}\ Ap(S, n) - w = F(S) + n - w \in S$ dir. Daha fazlası, $maks_{\leq_S} Ap(S, n) - w \neq \frac{F(S)}{2} + n$ dir. Aksi halde $w = \frac{F(S)}{2}$ olur. İspatın geri kalanı Önerme 2.35 (f)'nin ispatından hareketle gösterilebilir.
($\Longleftarrow :$) $x \neq \frac{F(S)}{2}$ ve $x \notin S$ olacak şekilde bir x tamsayısı olsun. $F(S) - x \in S$ olduğunu gösterelim. $w \equiv x \ (mod\ n)$ olacak şekilde $w \in Ap(S, n)$ alalım. Uygun $k \in \mathbb{N} \setminus \{0\}$ için $x = w - kn$ olur. Bunu iki durumda inceleyebiliriz:

$w = \frac{F(S)}{2} + n$ ise $F(S) - x = F(S) - (\frac{F(S)}{2} + n - kn) = (\frac{F(S)}{2} + (k-1)n)$ olur. Ek olarak $x \neq \frac{F(S)}{2}$ ise bu $k \neq 1$ olmasına neden olur. Böylece $k \geq 2$ ve $F(S) - x \in S$ dir. Aksi halde, $a_{n-2} - w \in S$ olduğundan

$$F(S) - x = F(S) + n - w + (k-1)n = a_{n-2} - w + (k-1)n \in S$$

dir. ■

Örnek 2.43 (1) $S = \langle 3, 7, 11\rangle = \{0, 3, 6, 7, 9, \longrightarrow\}$ *olsun.* $F(S) = 8$ *çift ve* $2 \notin S$ *için* $8 - 2 \in S$, $4 \notin S$ *için* $4 = \frac{8}{2} = \frac{F(S)}{2}$, $5 \notin S$ *için* $8 - 5 \in S$ *olduğundan Önerme 2.42 (a)'dan S pseudo-simetrik nümerik semigruptur.*
(2) $S = \langle 6, 7, 11\rangle = \{0, 6, 7, 11, 12, 13, 14, 17, \longrightarrow\}$ *nümerik semigrubunun Frobenius sayısı* $F(S) = 16$ *dır. Fakat*

$$\begin{aligned} Ap(S, 11) &= \{0, 12, 13, 14, 26, 27, 6, 7, 19, 20, 21\} \\ &= \{0 < 6 < 7 < 12 < 13 < 14 < 20 < 21 < 26 < 27\} \cup \{\frac{F(S)}{2} + 11\} \end{aligned}$$

kümesinde en az bir $i \in \{1, \ldots, 9\}$ *için* $a_9 \neq a_i + a_{9-i}$ *olduğundan Önerme 2.42 (d) yardımıyla S pseudo-simetrik değildir.*

Önerme 2.44 *S bir nümerik semigrup ve* $0 \neq n \in S$ *olsun. S pseudo-simetriktir ancak ve ancak*

$$maks_{\leq_S} Ap(S, n) = \{\frac{F(S)}{2} + n, F(S) + n\}$$

dir.

İspat. Önerme 2.42 (d)'den, her $i \in \{0, 1, \ldots, n-2\}$ için $a_i + a_{n-2-i} = a_{n-2}$ olduğundan $a_i \leq_S a_{n-2}$ dir. Fakat $\frac{F(S)}{2} + n$, diğer elemanlar ile karşılaştırılamadığı için $maks_{\leq_S} Ap(S, n) = \{F(S) + n, \frac{F(S)}{2} + n\}$ dir. ■

Gözlem 2.45 *$PF(S)$ tanımı yardımıyla yukarıdaki önermenin sonucu olarak S nümerik semigrubu için aşağıdaki koşullar denktir:*
(1) S pseudo-simetriktir.
(2) $PF(S) = \{F(S), \frac{F(S)}{2}\}$
Ek olarak $t(S) = 2$ ise $PF(S) = \{F(S), \frac{F(S)}{2}\}$ sağlamayabilir.

Lemma 2.46 *$S = \{\rho_0, \rho_1, \ldots\}$ bir pseudo-simetrik nümerik semigrup, S'nin önderi c olsun. $\rho_1 + (c-1)/2$ den farklı herhangi bir $a \in Ap(S, \rho_1)$ için $\rho_1 + c - 1 - a \in Ap(S, \rho_1)$ dir.*

İspat. Öncelikle $\rho_1 + c - 1 - a \in S$ olduğunu gösterelim. $a \in Ap(S, \rho_1)$ olduğundan $a - \rho_1 \notin S$ dir ve hipotez yardımıyla $(c-1)/2$ den farklıdır. S pseudo-simetrik olduğundan $\rho_1 + c - 1 - a = c - 1 - (a - \rho_1) \in S$ olur.

Şimdi, $\rho_1 + c - 1 - a - \rho_1 = c - 1 - a \notin S$ olduğunu iddia edelim. Aksi halde $c - 1 \in S$ olmalıdır. Bu imkansız olduğundan, $\rho_1 + c - 1 - a \in Ap(S, \rho_1)$ olmalıdır. ■

Lemma 2.47 *(a) S, $m(S) \geq 4$ ile bir pseudo-simetrik nümerik semigrup olsun. $e(S) \leq m(S) - 1$ dir.*
(b) S nümerik semigrubu için aşağıdaki koşullar denktir:

(1) S, $e(S) = m(S) = 3$ ile bir pseudo-simetrik nümerik semigruptur.

(2) x, 3 ile bölünemeyen bir tamsayı olmak üzere $S = \langle 3, x+3, 2x+3 \rangle$ dir.
(c) $m \geq 4$ olacak şekilde m pozitif tamsayısı olsun. $F(S)$ çift ve $m(S) = m$, $e(S) = 3$ olacak şekilde bir S pseudo-simetrik nümerik semigrubu vardır.
(d) m ve q, $m \geq 2q + 5$ olacak şekilde negatif olmayan tamsayılar ve S, $(\mathbb{N}, +)$'nın

$$\{m, m+1, (q+1)m + q + 2, \ldots, (q+1)m + m - q - 3, (q+1)m + m - 1\}$$

ile üretilen alt monoidi olsun. S, m katlılık ve $e = m - 2q - 1$ gömülüş boyutu ile bir pseudo-simetrik nümerik semigruptur. Ayrıca $F(S) = 2(q+1)m - 2$ dir.
(e) $m \geq 2q + 4$ olacak şekilde $m \in \mathbb{N}$, $q \in \mathbb{N} \setminus \{0\}$ ve S, $(\mathbb{N}, +)$'nın

$$\{m, m+1, qm + 2q + 3, \ldots, qm + m - 1, (q+1)m + q + 2\}$$

ile üretilen alt monoidi olsun. S, m katlılık ve $e = m - 2q$ gömülüş boyutu ile bir pseudo-simetrik nümerik semigruptur. Ayrıca $F(S) = 2qm + 2q + 2$ dir.
(f) m ve e, $3 \leq e \leq m-1$ olacak şekilde pozitif tamsayılar olsun. Katlılık $m(S) = m$ ve gömülüş boyutu $e(S) = e$ olacak şekilde bir pseudo-simetrik nümerik semigrup vardır.

İspat. (a) Bir nümerik semigrup için $e(S) \leq m(S)$ olduğunu biliyoruz. $e(S) = m(S)$ ise S, $\{m(S), n_1, \ldots, n_{m(S)-1}\}$ minimal üreteç sistemi ile üretilmiştir ve

$$Ap(S, m(S)) = \{0 < n_2 < \ldots < n_{m(S)-1}\} \cup \{n_1 = \frac{F(S)}{2} + m(S)\}$$

dır. $m(S)-1 \geq 3$ olduğundan $n_{m(S)-1} - n_2 \in S$ olur. Bu ise $\{m(S), n_1, \ldots, n_{m(S)-1}\}$ kümesinın S'nin minimal üreteç sistemi olması ile çelişir.
(b) $(1 \implies 2)$ $e(S) = m(S) = 3$ ise $\{3, n_1, n_2\}$, S'nin minimal üreteç sistemidir. Önerme 2.42 (d) yardımıyla, $F(S)$ çift ve

$$Ap(S, 3) = \{0, n_1 = \frac{F(S)}{2} + 3, n_2 = F(S) + 3\}$$

dir. $x = \frac{F(S)}{2}$ alınırsa $n_1 = x + 3$ ve $n_2 = 2x + 3$ olur. $x = \frac{F(S)}{2} \notin S$ olduğundan x, 3'ün bir katı değildir.
$(2 \implies 1)$ $\{3, x+3, 2x+3\}$ kümesinin S'nin minimal üreteç sistemi olduğu açıktır ve $e(S) = m(S) = 3$ dir. Sonuç olarak $Ap(S, 3) = \{0, x+3, 2x+3\}$ dir. $2x+3 = F(S)+3$ ve buradan $\frac{F(S)}{2} + 3 = 2x + 3$ olur. Böylece S pseudo-simetriktir.
(c) m'ye bağlı olarak iki durumda inceleyelim:

m çift ise bazı $q \in \mathbb{N}$ için $m = 2q + 4$ dir.

$$S = \langle m, m + 1, (q + 1)m + (m - 1)\rangle$$

olsun. Burada $m(S) = m$ ve $e(S) = 3$ dür. Bu koşullar altında

$$Ap(S, m) = \{0, m + 1, 2(m + 1), \ldots, (m - 2)(m + 1)\} \cup \{(q + 1)m + (m - 1)\}$$

olur. Apéry küme yardımıyla $F(S) = (m-2)m-2$ çift ve $\frac{F(S)}{2}+m = (q+1)m+(m-1)$ dir. Böylece S'nin pseudo-simetrik nümerik semigrup olduğu açıktır.

m tek ise bazı $q \in \mathbb{N} \setminus \{0\}$ için $m = 2q + 3$ dir. S nümerik semigrubu

$$S = \langle m, m + 1, (q + 1)m + q + 2\rangle$$

olsun. $m(S) = m$ ve $e(S) = 3$ dür. $Ap(S, m)$ kümesi $\{0, m + 1, \ldots, q(m + 1), (q + 1)m+q+2, (m+1)+(q+1)m+q+2, \ldots, q(m+1)+(q+1)m+q+2\}\cup\{(q+1)(m+1)\}$ dir. Apéry kümesi yardımıyla $F(S) = 2(1+q+mq)$ çift ve $\frac{F(S)}{2}+m = (q+1)(m+1)$ dir. Böylece S'nin pseudo-simetrik nümerik semigrup olduğu açıktır.
(d) (Rosales ve Garcia-Sanchez 2009).
(e) (Rosales ve Garcia-Sanchez 2009).
(f) Lemma 2.47 (c)'den $e = 3$ ise semigrubun varlığı açıktır. Böylece $4 \leq e \leq m - 1$ kabul edebiliriz. İki durumda inceleyelim:

$m - e$ tek ise $m - e = 2q + 1$ olacak şekilde $q \in \mathbb{N}$ vardır. Daha fazlası $e \geq 4$ olduğundan $m \geq 2q + 5$ dir. Lemma 2.47 (d)'den m katlılık ve $e = m - 2q - 1$ gömülüş boyutu ile bir pseudo-simetrik nümerik semigrubun varlığı açıktır.

$m - e$ çift ise $m - e = 2q$ olacak şekilde $q \in \mathbb{N} \setminus \{0\}$ vardır. Daha fazlası $e \geq 4$ olduğundan $m \geq 2q + 4$ dir. Lemma 2.47 (e)'den m katlılık ve $e = m - 2q$ gömülüş boyutu ile bir pseudo-simetrik nümerik semigrubun varlığı açıktır. ■

Örnek 2.48 (1) $q = 2, m = 11$ *olsun. Lemma 2.47 (d)'den* $S = \langle 11, 12, 37, 38, 39, 43\rangle$ *nümerik semigrubu* $m(S) = 11$, $e(S) = 6$, $F(S) = 64$ *ile bir indirgenemez nümerik semigruptur. Ayrıca*

$$Ap(S, 11) = \{0, 12, 24, 36, 37, 38, 39, 51, 63, 75\} \cup \{43\}$$

dir.
(2) $q = 2, m = 11$ *olsun. Bu durumda, Lemma 2.47 (e)'den* $S = \langle 11, 12, 29, 30, 31, 32, 37\rangle$ *nümerik semigrubu* $m(S) = 11$, $e(S) = 7$, $F(S) = 50$ *ile bir indirgenemez nümerik semigruptur. Ayrıca*

$$Ap(S, 11) = \{0, 12, 24, 29, 30, 31, 32, 37, 49, 61\} \cup \{36\}$$

dir.

2.1.4. Aralıkla üretilen nümerik semigrup

Tanım 2.49 *S nümerik semigrubu, $i, j \in \mathbb{N}$, $i \leq j$ olacak şekilde*

$$S = \{n_i i + n_{i+1}(i + 1) + \ldots + n_j j \mid n_i, n_{i+1}, \ldots, n_j \in \mathbb{N}\}$$

ise S, $\{i, i+1, \ldots, j\}$ aralığı tarafından üretilen nümerik semigrup olarak adlandırılır.

Lemma 2.50 *$\{i, i + 1, \ldots, j\}$ tarafından üretilen nümerik semigrup $S_{\{i,i+1,\ldots,j\}}$ olmak üzere*

$$S_{\{i,i+1,\ldots,j\}} = \cup_{k\geq 0}\{ki, ki + 1, ki + 2, \ldots, kj\}$$

formundadır.

İspat. (Amoros 2004). ■

Önerme 2.51 *(a) $S_{\{i,i+1,\ldots,j\}}$ simetriktir ancak ve ancak $i \equiv 2$ mod $(j - i)$ dir.*
(b) Pseudo-simetrik olan ve aralıkla üretilen tek nümerik semigrup $\{0, 3, \longrightarrow\}$ dır.

İspat. *(a)* (Amoros 2004).
(b) Lemma 2.50 yardımıyla $\{i, \ldots, j\}$ tarafından üretilen aşikar olmayan $S_{\{i,\ldots,j\}}$ nümerik semigrubu $k = 0$ için $\{0, 1, 2, \ldots, j - i\}$, $k = 1$ için $\{i, i + 1, i + 2, \ldots, j\}$, $k = 2$ için $\{2i, 2i + 1, 2i + 2, \ldots, 2j\}$ ve $k \geq 3$ için benzer şekilde oluşan kümelerin birleşiminden meydana gelir. Kümelerin elemanları göz önüne alındığında ρ_1 ve önder arasındaki boşlukların aralıklarında, her bir aralığın uzunluğu ondan önceki uzunluktan $(j - i)$ kadar az olmasını sağlar. Başka bir deyişle, 1 ve $c - 1$ arasındaki kutupların aralıklarında, her bir aralığın uzunluğu ondan önceki uzunluktan $(j - i)$ kadar fazla olmasını sağlar. Şimdi, pseudo-simetrik tanımı yardımıyla, $(c - 1)/2$, ilk boşluk veya boşlukların aralığının son boşluğu olmalıdır. n boşluktan oluşan aralığın ilk boşluğunun $(c - 1)/2$ olduğunu varsayalım. Bunu iki kısımda inceleyelim:

$(c - 1)/2 = 1$ ise $c = 3$ ve $S = \{0, 3, \longrightarrow\}$ olur.

$(c-1)/2 \neq 1$ ise ρ sayma dönüşümü olmak üzere $(c-1)/2 > \rho_1$ dir. O halde, S pseudo-simetrik ise kutupların bir önceki aralığı $(n-1)$ uzunluktadır. S bir aralık tarafından üretildiğinden $(c-1)/2$'den sonraki kutupların ilk aralığının uzunluğu $(n-1)+j-i$ olmalıdır. Ayrıca, S pseudo-simetrik olduğundan $(c-1)/2$'den önceki boşlukların aralıkları aynı uzunlukta olmalıdır. Fakat, S aralıkla üretilen nümerik semigrup olduğundan $(c-1)/2$'den önceki boşlukların aralığının uzunluğu $n+j-i$ olmalıdır. Bu ise çelişkidir. O halde $(c-1)/2$ boşlukların aralığının en son boşluğu olamaz. Böylece, aralıkla üretilen pseudo-simetrik nümerik semigrup için tek olasılık $(c-1)/2 = 1$ olduğu durumdur. ■

2.1.5. Akut nümerik semigrup

Tanım 2.52 *$S \neq \mathbb{N}$, $\rho : \mathbb{N} \longrightarrow S$ sayma dönüşümüne, g cinsine ve c önderine sahip olan nümerik semigrup olsun. $\rho_{\rho^{-1}(c)-1}$ elemanı semigrubun dominantı olarak adlandırılır ve d ile gösterilir.*

$i \in \mathbb{N}$ için $g(i)$, ρ_i den küçük boşlukların sayısı olsun. $g(\rho^{-1}(c)) = g$ ve $g(\rho^{-1}(d)) = g' < g$ dir. i, $g(i) = g'$ olacak şekilde en küçük tamsayı ise ρ_i, S'nin alt önderi olarak adlandırılır ve c' ile gösterilir.

Gözlem 2.53 *$c' > 0$ ise $c' - 1 \notin S$ dir. Aksi halde $g(\rho^{-1}(c'-1)) = g(\rho^{-1}(c'))$ ve $c'-1 < c'$ elde edilir. c' ve d arasındaki tüm sayıların S'de olduğuna dikkat edelim. Aksi halde $g(\rho^{-1}(c')) < g'$ olur.*

Tanım 2.54 *Bir nümerik semigrup bir $c \in \mathbb{N}$ için $\{0\} \cup \{i \in \mathbb{N} \mid i \geq c\}$ kümesine eşit ise adi (ordinary) nümerik semigrup olarak adlandırılır, burada kısaca adi diyeceğiz.*

Adi nümerik semigruba örnek olarak $\mathbb{N}$ verilebilir.

Gözlem 2.55 *$S \neq \mathbb{N}$ nümerik semigrubu için aşağıdakiler denktir:*
(a) S adi nümerik semigruptur.
(b) S'nin dominantı 0 dır.
(c) S'nin alt önderi 0 dır.

Gerçekten, $a \iff b$ ve $b \implies c$ açıktır. Şimdi, (c)'nin sağlandığını varsayalım. Eğer $d \geq 1$ ise bunun anlamı $1 \in S$ dir ve böylece $S = \mathbb{N}$ olur, bu ise hipotezle çelişir.

Tanım 2.56 *S, ρ sayma fonksiyonu ve ρ_i alt önderi ile adi olmayan bir nümerik semigrup ise o zaman ρ_{i-1} elemanı alt dominant olarak adlandırılır ve d' ile gösterilir.*

Bu bölümde tanımlanan ifadeler sembolik olarak

$$d = maks\ \{\rho \in S \mid \rho < c\}$$

$$c' = \min \{\rho \in S \mid g(\rho) = g(d)\}$$

ve

$$d' = maks \{\rho \in S \mid \rho < c'\}$$

şeklinde ifade edilebilir.

Tanım 2.57 *Adi veya adi olmayan nümerik semigrubun önderi c, alt önderi c', dominantı d, alt dominantı d' iken $c - d \leq c' - d'$ sağlıyorsa akut nümerik semigrup olarak adlandırılır.*

Örnek 2.58 (1) $S = \langle 4, 7, 9\rangle = \{0, 4, 7, 8, 9, 11, \longrightarrow\}$ *nümerik semigrubunda* $c = 11$, $d = 9$, $c' = 7$ *ve* $d' = 4$ *dir. Burada* $c - d \leq c' - d'$ *sağladığından* S *nümerik semigrubu akuttur.*
(2) $S = \langle 3, 8\rangle = \{0, 3, 6, 8, 9, 11, 12, 14, \longrightarrow\}$ *nümerik semigrubunda* $c = 14$, $d = 12$, $c' = 11$ *ve* $d' = 9$ *dır. Burada* $c - d \leq c' - d'$ *sağladığından* S *nümerik semigrubu akuttur.*

Gözlem 2.59 *S nümerik semigrubunda, önderden önceki boşlukların aralıklarının son aralığı, ondan bir önceki boşluk aralığından daha küçük ise akut nümerik semigruptur.*

Önerme 2.60 *S bir nümerik semigrup olsun.*
(a) S simetrik ise akuttur.
(b) S pseudo-simetrik ise akuttur.
(c) S aralıkla üretilen nümerik semigrup ise akuttur.

İspat. S adi nümerik semigrup ise açıktır. S, g cinsi, c önderi, c' alt önderi, d dominantı, d' alt dominantı ile adi olmayan bir nümerik semigrup olsun.
(a) S simetrik semigrup varsayalım ve $F(S)$ yerine $c-1$ notasyonunu kullanalım. S simetrik nümerik semigruptur ancak ve ancak herhangi negatif olmayan i tamsayısı için $i \notin S$ ise $c - 1 - i \in S$ dir. Eğer S adi değilse $1 \notin S$ ve $c - 2 \in S$ sayısı S'nin dominantıdır. Buradan $c - d = 2$ dir. $c' - 1 \notin S$ olduğundan $c - d = 2 \leq c' - d'$ dır ve böylece S akuttur.
(b) S pseudo-simetrik nümerik semigrup varsayalım. $1 = (c - 1)/2$ ise $c = 3$ ve $S = \{0, 3, \longrightarrow\}$ nümerik semigrubu adidir. Aksi halde $1 \neq (c-1)/2$ ise (a)'da $1 \notin S$ için yapılan işlemlere denktir.
(c) S, $\{i, i + 1, \ldots, j\}$ aralığı ile üretilen nümerik semigrup olsun. O zaman Lemma 2.50 yardımıyla $c = ki$, $c' = (k - 1)i$, $d = (k - 1)j$ ve $d' = (k - 2)j$ olacak şekilde uygun k elemanı vardır. Böylece $c' - d' = k(i - j) - i + 2j$ iken $c - d = k(i - j) + j$ olur ve S akuttur. ■

Örnek 2.61 (1) $S = \langle 6, 9, 11\rangle = \{0, 6, 9, 11, 12, 15, 17, 18, 20, 21, 22, 23, 24, 26, \longrightarrow\}$ *simetrik nümerik semigrubunun Önerme 2.60 (a) yardımıyla akut nümerik semigrup olduğunu söyleyebiliriz. Şöyle ki,* $c = 26$, $d = 24$, $c' = 20$ *ve* $d' = 18$ *olduğundan* $c - d \leq c' - d'$ *dır.*

(2) $S = \langle 3, 8, 13\rangle = \{0, 3, 6, 8, 9, 11, \longrightarrow\}$ *pseudo-simetrik nümerik semigrubunun Önerme 2.60 (b) yardımıyla akut nümerik semigrup olduğunu söyleyebiliriz. Şöyle ki,* $c = 11$, $d = 9$, $c' = 8$ *ve* $d' = 6$ *olduğundan* $c - d \leq c' - d'$ *dir.*

Gözlem 2.62 *Akut olmayan nümerik semigruplar vardır. Örneğin,*

$$S = \{0, 6, 8, 9\} \cup \{i \in \mathbb{N} \mid i \geq 12\}$$

olduğu durumda, $c = 12$, $d = 9$, $c' = 8$ *ve* $d' = 6$ *dır.*

Diğer yandan simetrik semigrup, pseudo-simetrik semigrup, aralıkla üretilen semigrup olmadığı halde akut olan öyle nümerik semigruplar vardır.

Örnek 2.63 (1) $S = \langle 6, 7, 15\rangle = \{0, 6, 7, 12, 13, 14, 15, 18, 19, 20, 21, 22, 24, \longrightarrow\}$ *nümerik semigrubunu alalım.*

$$\begin{aligned} Ap(S, 13) &= \{0, 14, 15, 29, 30, 18, 6, 7, 21, 22, 36\} \\ &= \{0 < 6 < 7 < 14 < 15 < 18 < 21 < 22 < 24 < 25 < 29 < 30 < 36\} \end{aligned}$$

kümesinde Önerme 2.35 (f)'den en az bir $i \in \{0, 1, 2, \ldots, 12\}$ *için* $a_{12} \neq a_i + a_{12-i}$ *olduğundan* S *simetrik nümerik semigrup değildir. Fakat* $c = 24$, $d = 22$, $c' = 18$ *ve* $d' = 15$ *ile* $c - d \leq c' - d'$ *sağlandığı için* S *akut nümerik semigruptur. Böylece* S *simetrik olmadığı halde akuttur.*

2.2. Arf Nümerik Semigruplar

S, $\rho : \mathbb{N} \longrightarrow S$ sayma dönüşümü ile belirlenen nümerik semigrup olsun.

Tanım 2.64 $i \geq j \geq k$ *olacak şekilde her* $i, j, k \in \mathbb{N}$ *için* $\rho_i + \rho_j - \rho_k \in S$ *ise* S *nümerik semigrubu Arf nümerik semigrup olarak adlandırılır, burada kısaca Arf diyeceğiz.*

Gözlem 2.65 $\rho_i \geq c$ *ise* $i \geq j \geq k$ *olacak şekilde her* j, k *için* $\rho_i + \rho_j - \rho_k \in S$ *olduğu açıktır. Böylece tanımdaki koşul yerine* $c = \rho_r$ *olmak üzere,* $k \leq j \leq i < r$ *almak yeterlidir.*

Arf nümerik semigruplara örnek olarak $\{0, 3, 4, 5, \ldots\}$, $\{0, m, m+1, m+2, \ldots\}$ ve $\mathbb{N}$ verilebilir. Tanım 2.5'e göre $\mathbb{N}$ semigrubu inductive olduğundan herhangi bir inductive semigrup tümevarım yöntemi ile Arf nümerik semigruptur.

Önerme 2.66 S *Arf nümerik semigrup olsun. Bazı* $i, j \in \mathbb{N}$ *için* $i, i + j \in S$ *ise her* $k \in \mathbb{N}$ *için* $i + kj \in S$ *olur.* S *Arf ve* $i, i + 1 \in S$ *ise* $i \geq c$ *dir.*

İspat. k üzerinde tümevarım uygulayalım. $k = 0$ ve $k = 1$ için sonuç açıktır. $k > 0$ ve $i, i + j, i + kj \in S$ ise

$$(i + j) + (i + kj) - i = i + (k + 1)j \in S$$

dir. ■

Önerme 2.67 *S, ρ sayma dönüşümü ile belirlenen nümerik semigrup olsun. Aşağıdaki koşullar denktir:*
(a) S Arf nümerik semigruptur.
(b) $i \geq k$ koşulunu sağlayan her i, k pozitif tamsayısı için $2\rho_i - \rho_k \in S$ sağlanır.

İspat. Her Arf nümerik semigrubun (b) koşulunu sağladığı açıktır. Karşıt olarak (b) koşulunu kabul edelim. $k \leq j \leq i < r$ olacak şekilde i, j, k pozitif tamsayıları olsun. $m = \rho_i + \rho_j - \rho_k \in S$ olduğunu göstermeliyiz. Eğer $i = j$ veya $j = k$ ise bu açıktır. Aksi halde, $k < j < i$ ise $i_0 = i$, $j_0 = j$, $k_0 = k$ olsun ve

$$m = \rho_{i_0} + \rho_{j_0} - \rho_{k_0} = (2\rho_{j_0} - \rho_{k_0}) + \rho_{i_0} - \rho_{j_0}$$

şeklinde yazılsın. $(2\rho_{j_0} - \rho_{k_0}) \in S$ ve $(2\rho_{j_0} - \rho_{k_0}) > \rho_{j_0}$ olduğuna dikkat edelim. i_1, j_1, k_1

$$\rho_{i_1} = maks\ \{2\rho_{j_0} - \rho_{k_0}, \rho_{i_0}\}$$

$$\rho_{j_1} = \min\ \{2\rho_{j_0} - \rho_{k_0}, \rho_{i_0}\}$$

$$\rho_{k_1} = \rho_{j_0}$$

yardımıyla tanımlansın. Buradan $i_1 \geq j_1 > k_1$ ve $i_1 \geq i_0$, $j_1 \geq j_0$, $k_1 > k_0$ için $m = \rho_{i_1} + \rho_{j_1} - \rho_{k_1}$ olur. $i_1 = j_1$ ise (b) koşulu $m \in S$ olmasını gerektirir. Aksi halde, $i_t \geq j_t \geq k_t$ için $m = \rho_{i_t} + \rho_{j_t} - \rho_{k_t}$ olacak şekilde $(i_t), (j_t), (k_t)$ pozitif tamsayılarının üç artan dizisi elde edilir. Burada iki olasılık vardır: $i_h = j_h$ veya $j_h = k_h$ olacak şekilde bir h indeksi varsa $m \in S$ olmasıdır. Aksi halde, her t için $i_t > j_t > k_t$ ise o zaman yapısal olarak (j_t) dizisi kesin artan olur. Böylece $j_h \geq r$ olacak şekilde öyle h indeksi vardır ve yine $m \in S$ elde edilmiş olur. ■

Önerme 2.68 *S nümerik semigrubunun Arf olması için gerek ve yeter koşul herhangi bir $\rho \in S$ için $S(\rho) = \{l' - \rho \mid l' \in S,\ l' \geq \rho\}$ kümesinin bir nümerik semigrup olmasıdır.*

İspat. S'yi Arf nümerik semigrup varsayalım. O zaman $0 \in S(\rho)$ dur. l'', $l' \in S$ ve $l' \geq \rho$, $l'' \geq \rho$ iken $m_1 = l' - \rho$, $m_2 = l'' - \rho$ ise $m_1 + m_2 = l'' + l' - \rho - \rho$ olur. S Arf olduğundan $l'' + l' - \rho \in S$ dir ve bu eleman ρ'dan büyük veya eşittir. Böylece $m_1 + m_2 \in S(\rho)$ dir. ■

Önerme 2.69 *$S_1, S_2, ..., S_n$ Arf nümerik semigruplar ise $S = S_1 \cap S_2 \cap \ldots \cap S_n$ de Arf nümerik semigruptur.*

İspat. $i \geq j \geq k$ olacak şekilde her $t \in \{1, 2, \ldots, n\}$ için $\rho_i, \rho_j, \rho_k \in S_t$ olsun. ρ artan olduğundan $\rho_i \geq \rho_j \geq \rho_k$ dır. Böylece her $t \in \{1, 2, \ldots, n\}$ için $\rho_i + \rho_j - \rho_k \in S_t$ olduğundan $\rho_i + \rho_j - \rho_k \in S$ dir. ■

Tanım 2.70 *$A \subseteq \mathbb{N}$, $obeb(A) = 1$ olmak üzere A'yı içeren tüm Arf nümerik semigrupların kesişimine A tarafından üretilen Arf nümerik semigrup denir ve A'yı içeren en küçük Arf nümerik semigruptur, $Arf(A)$ ile gösterilir.*

Tanım 2.71 *S Arf nümerik semigrup ise $Arf(S) = S$ dir. $S = Arf(A)$ ise A'ya S'nin Arf üreteç sistemi denir. S bir nümerik semigrup ise $Arf(S)$'ye S'nin Arf kapanışı denir.*

Lemma 2.72 *$S \subseteq \mathbb{N}$ bir alt monoid olsun.*

$$S' = \{\rho_i + \rho_j - \rho_k \mid \rho_i, \rho_j, \rho_k \in S,\ \rho_i \geq \rho_j \geq \rho_k\}$$

de $\mathbb{N}$'nin alt monoidi olur ve $S \subseteq S'$ dir.

İspat. S' nın alt monoid olduğu açıktır. Ayrıca, $\rho \in S$ için $\rho = \rho + \rho - \rho \in S'$ olduğundan $S \subseteq S'$ elde edilir. ■

Bunu kullanarak $S \subseteq \mathbb{N}$ alt monoidi ve $n \in \mathbb{N}$ için S^n alt monoidini tanımlayalım:

$$\begin{aligned} S^0 &= S \\ S^{n+1} &= (S^n)' \end{aligned}$$

Lemma 2.73 *S bir nümerik semigrup ise öyle $k \in \mathbb{N}$ vardır ki $S^k = Arf(S)$ dir.*

İspat. n üzerinde tümevarım kullanarak her $n \in \mathbb{N}$ için $S^n \subseteq Arf(S)$'yi ispatlayalım. Şöyle ki; $n = 1$ için $S^1 = (S^0)' = S' \subseteq Arf(S)$ dir. $n-1$ için $S^{n-1} \subseteq Arf(S)$ olduğunu kabul edelim. n için

$$S^n = (S^{n-1})' \subseteq \{\rho_i + \rho_j - \rho_k \mid \rho_i, \rho_j, \rho_k \in Arf(S),\ \rho_i \geq \rho_j \geq \rho_k\} = Arf(S)$$

ile $S^n \subseteq Arf(S)$ olur ve böylece her $n \in \mathbb{N}$ için $S^n \subseteq Arf(S)$ olduğu gösterilmiş olur. Diğer yandan $S \subseteq S^n$, $S^n \subseteq S^{n+1} = (S^n)'$ olduğundan dolayı $S \subseteq S^1 \subseteq \ldots \subseteq S^n \subseteq S^{n+1} \ldots$ sonsuz dizisi oluşur. Fakat S bir nümerik semigrup olduğu için bu zincir sonlu olmalıdır. O halde, $S^k = S^{k+1}$ olacak biçimde uygun $k \in \mathbb{N}$ vardır. Bu koşul altında S^k Arf nümerik semigrup ve $S \subseteq S^k$ dır. Hatta, $S \subseteq Arf(S)$ ve $S \subseteq S^k$ iken S'yi kapsayan en küçük Arf nümerik semigrup S'nin Arf kapanışı olduğundan $Arf(S) \subseteq S^k$ olur. Burada, belirlenen k elemanı için de $S^k \subseteq Arf(S)$ olduğundan $S^k = Arf(S)$ elde edilmiş olur. ■

Lemma 2.74 *S Arf nümerik semigrup ve A, S'nin Arf üreteç sistemi olsun. Bu durumda*
(a) Minimal üreteç sisteminin en küçük elemanı $m(S) \in A$ dır.
(b) Her $\rho \in S$ için $B(\rho) = \{a \in A \mid a \leq \rho\}$ tanımlansın. Eğer $\rho \in < A >^n$ ise $\rho \in < B(\rho) >^n$ dir.
(c) A ve B minimal üreteç sistemi ise $A = B$ dir.

İspat. (a) $S \setminus m(S)$'nin Arf nümerik semigrup olduğunu gösterelim. $\rho_i \geq \rho_j \geq \rho_k$ olacak şekilde $\rho_i, \rho_j, \rho_k \in S \setminus m(S)$ olsun. $\rho_i, \rho_j, \rho_k \in S$ ve S Arf olduğundan $\rho_i + \rho_j - \rho_k \in S$ dir. $\rho_i + \rho_j - \rho_k \neq m(S)$ ise $\rho_i + \rho_j - \rho_k \in S \setminus m(S)$ olduğunu iddia edelim. $\rho_i, \rho_j, \rho_k \in S \setminus m(S)$ için $\rho_i \geq \rho_j \geq \rho_k > m(S)$ olduğundan $\rho_i + \rho_j - \rho_k > m(S)$ dir. Böylece $\rho_i + \rho_j - \rho_k \in S \setminus m(S)$ olduğundan $S \setminus m(S)$ Arf nümerik semigruptur. $m(S) \notin A$ olsa $A \subseteq S \setminus m(S)$, $Arf(A) \subseteq Arf(S \setminus m(S))$ ve $Arf(S \setminus m(S)) = S \setminus m(S)$ olduğundan $Arf(A) \subseteq (S \setminus m(S))$ olur. Bu ise A'nın Arf üreteç sistemi olmasıyla çelişir, $m(S) \in A$ olmalıdır.
(b) n üzerinden tümevarım uygulayalım. $n = 0$ için $\rho \in < A >^0$ ise $\rho \in < B(\rho) >^0$ dur. $n \in \mathbb{N}$ için $\rho \in < A >^n$ ise $\rho \in < B(\rho) >^n$'nin varlığını kabul edelim. Şimdi, $n+1 \in \mathbb{N}$ için $\rho \in < A >^{n+1}$ ise $\rho \in < B(\rho) >^{n+1}$ olduğunu iddia edelim. $\rho \in < A >^{n+1}$ olsun. O halde $x \geq y \geq z$ olacak şekilde öyle $x, y, z \in < A >^n$ için $\rho = x + y - z$ dir. Hipotezi kullanırsak $x \in < A >^n$ iken $x \in B(x)^n$; $y \in < A >^n$ iken $y \in B(y)^n$; $z \in < A >^n$ iken $z \in B(z)^n$ olur. $x \geq y \geq z$ için $\rho = x + y - z$ olduğundan $z \leq y \leq x \leq \rho$ ve $B(z) \subseteq B(y) \subseteq B(x) \subseteq B(\rho)$ dur. $x \geq y \geq z$ olacak şekilde x,y,$z \in < B(\rho) >^n$ iken $\rho = x + y - z \in < B(\rho) >^{n+1}$ olur.
(c) $A = \{0 = \rho_0 < \rho_1 < \ldots < \rho_p < \ldots\}$ ve $B = \{0 = \lambda_0 < \lambda_1 < \ldots < \lambda_q < \ldots\}$ olsun. (a)'dan $\rho_1 = m(S)$, $\rho_1 \in A$, $\lambda_1 = m(S)$ ve $\lambda_1 \in B$ dir. Buradan $\rho_1 = \lambda_1 = m(S)$ olur. $A \neq B$ olduğunu varsayalım. $\rho_r \neq \lambda_r$ olacak şekilde en küçük tamsayı r olsun. Hatta, $\lambda_r < \rho_r$ varsayalım. $\lambda_r \in S$ olduğundan $\lambda_r \in < A >^n$ vardır. $\lambda_r \in < A >^n$ ise $\lambda_r \in < B(\lambda_r) >^n = < \rho_1, \ldots, \rho_{r-1} >^n$ olur. Ayrıca her $k < r$ için $\rho_k = \lambda_k$ olduğundan $\lambda_r \in < \lambda_1, \ldots, \lambda_{r-1} >^n$ ve $\lambda_r \in Arf(B \setminus \lambda_r)$ dir. Böylece $S = Arf(B \setminus \lambda_r)$ olur. Fakat, bu B'nin minimal Arf üreteç sistemi olması ile çelişir. $A = B$ olmalıdır. ■

S nümerik semigrubunun minimal üreteç sisteminin kardinalitesine Arf-rank denir, $Arf - rank(S)$ ile gösterilir.

Lemma 2.75 *S bir Arf nümerik semigrup ve $m \in S$ olsun. $(m + S) \cup \{0\}$ da Arf nümerik semigruptur.*

İspat. $(m + S) \cup \{0\}$ nümerik semigruptur. $m + \rho_1$, $m + \rho_2$, $m + \rho_3 \in m + S$ ve $m + \rho_1 \geq m + \rho_2 \geq m + \rho_3$ olmak üzere $(m + \rho_1) + (m + \rho_2) - (m + \rho_3) \in m + S$ olduğunu iddia edelim. $m + \rho_1 \geq m + \rho_2 \geq m + \rho_3$ ise $\rho_1 \geq \rho_2 \geq \rho_3$ dır. S Arf nümerik semigrup olduğundan $\rho_1 + \rho_2 - \rho_3 \in S$ olur ve $(m + \rho_1) + (m + \rho_2) - (m + \rho_3) = m + (\rho_1 + \rho_2 - \rho_3) \in m + S$ dir. Böylece $(m + S) \cup \{0\}$ Arf nümerik semigruptur. ■

Lemma 2.76 *S Arf nümerik semigrup ve a, R keyfi pozitif tamsayılar olsun. O zaman*

$$\bar{S} = aS \cup \{m \in \mathbb{N} \mid m \geq R\}$$

Arf nümerik semigruptur.

İspat. $i \geq j \geq k$ olacak şekilde ρ_i,ρ_j,$\rho_k \in \bar{S}$ elemanları $\bar{S}$'nin önderinden küçük olsun. Böylece $R > \rho_i \geq \rho_j \geq \rho_k$ dir. $\alpha \geq \beta \geq \gamma$ olacak şekilde ρ_α,ρ_β,$\rho_\gamma \in S$ vardır ki $\rho_i = a\rho_\alpha$, $\rho_j = a\rho_\beta$, $\rho_k = a\rho_\gamma$ dir. O zaman $\rho_i + \rho_j - \rho_k = a(\rho_\alpha + \rho_\beta - \rho_\gamma) \in aS \subseteq \bar{S}$ olduğundan $\bar{S}$ Arftir. ■

Örnek 2.77 $S = \{0, 6, 7, 8, \longrightarrow\}$ *Arf nümerik semigrubunu ele alalım.* $7 \in S$ *için* $7 + S = \{7, 13, 14, \longrightarrow\}$ *Arf nümerik semigrup olmadığı halde Lemma 2.75'den* $(7 + S) \cup \{0\} = \{0, 7, 14, 20, 21, \longrightarrow\}$ *Arf nümerik semigruptur.*

Lemma 2.78 $m, r_1, r_2, \ldots, r_p \in \mathbb{N}$, *obeb*$(m, r_1, r_2, \ldots, r_p) = 1$ *olsun. Bu durumda*
(*a*) $m+ < m, r_1, r_2, \ldots, r_p >^n \subseteq Arf(m, m + r_1, m + r_2, \ldots, m + r_p)$
(*b*) $(m + Arf(m, r_1, r_2, \ldots, r_p)) \cup \{0\} = Arf(m, m + r_1, m + r_2, \ldots, m + r_p)$
(*c*) $m + F(Arf(m, r_1, r_2, \ldots, r_p)) = F(Arf(m, m + r_1, m + r_2, \ldots, m + r_p))$ *dır.*

İspat. (*a*) n üzerinden tümevarım uygulayalım. $n = 0$ için

$$m+ < m, r_1, r_2, \ldots, r_p > \subseteq Arf(m, m + r_1, m + r_2, \ldots, m + r_p)$$

olduğunu ispatlamalıyız. $i, j, k \in \{1, 2, ..., p\}$ olsun.
(1) $m + r_i$, $m + r_j$, $m \in Arf(m, m + r_1, m + r_2, \ldots, m + r_p)$ için $m + r_i + r_j = (m + r_i) + (m + r_j) - m \in Arf(m, m + r_1, m + r_2, \ldots, m + r_p)$ olur.
(2) $m+r_i+r_j$, $m+r_k$, $m \in Arf(m, m+r_1, m+r_2, \ldots, m+r_p)$ için $m+r_i+r_j+r_k = (m+r_i+r_j)+(m+r_k)-m \in Arf(m, m+r_1, m+r_2, \ldots, m+r_p)$ dir. Elemanların uygun katlarını alarak $\lambda m + \lambda_1 r_1 + \ldots + \lambda_p r_p \in Arf(m, m + r_1, m + r_2, \ldots, m + r_p)$ olur. $m + \lambda m + \lambda_1 r_1 + \ldots + \lambda_p r_p \in Arf(m, m + r_1, m + r_2, \ldots, m + r_p)$ dır. Bu formdaki elemanlar $m+ < m, r_1, r_2, \ldots, r_p >$'nın elemanları olduğundan $m+ < m, r_1, r_2, \ldots, r_p > \subseteq Arf(m, m + r_1, m + r_2, \ldots, m + r_p)$ olduğu görülür. $n \in \mathbb{N}$ için $m+(< m, r_1, r_2, \ldots, r_p >)^n \subseteq Arf(m, m+r_1, m+r_2, \ldots, m+r_p)$'nin varlığını kabul edelim. Şimdi, $n + 1 \in \mathbb{N}$ için

$$m+ < m, r_1, r_2, \ldots, r_p >^{n+1} \subseteq Arf(m, m + r_1, m + r_2, \ldots, m + r_p)$$

olduğunu gösterelim. $a \in m+ < m, r_1, r_2, \ldots, r_p >^{n+1}$ için $a = m + b$, $b \in < m, r_1, r_2, \ldots, r_p >^{n+1}$ dır. $b \in < m, r_1, r_2, \ldots, r_p >^{n+1}$ için $< m, r_1, r_2, \ldots, r_p >^n$ de $x \geq y \geq z$ olacak şekilde öyle x, y, z elemanları vardır ki $b = x + y - z$ dir. Buradan $(m + x)$, $(m + y)$, $(m + z) \in m+ < m, r_1, r_2, \ldots, r_p >^n$ olur. Yerine koyarsak $a = m + b = m + x + y - z = (m + x) + (m + y) - (m + z) \in Arf(m, m + r_1, m + r_2, \ldots, m + r_p)$ elde edilir ve her $n \in \mathbb{N}$ için $m + (< m, r_1, r_2, \ldots, r_p >)^n \subseteq Arf(m, m + r_1, m + r_2, \ldots, m + r_p)$ olduğu görülür.
(*b*) $m + (< m, r_1, r_2, \ldots, r_p >)^n \subseteq Arf(m, m + r_1, m + r_2, \ldots, m + r_p)$ olduğu (a)'da gösterilmiştir. Öyle $k \in \mathbb{N}$ vardır ki $< m, r_1, r_2, \ldots, r_p >^k = Arf(m, r_1, r_2, \ldots, r_p)$ dir. O halde, $m + Arf(m, r_1, r_2, \ldots, r_p) \subseteq Arf(m, m + r_1, m + r_2, \ldots, m + r_p)$ dır. $m, m + r_1, m + r_2, \ldots, m + r_p \in (m + Arf(m, r_1, r_2, \ldots, r_p)) \cup \{0\}$ olur ve buradan $m + Arf(m, r_1, r_2, \ldots, r_p) \cup \{0\}$ Arf nümerik semigruptur. Fakat bu elemanlara sahip en küçük Arf nümerik semigrup, $\{m, m + r_1, m + r_2, ..., m + r_p\}$ elemanlarının oluşturduğu nümerik semigrubun Arf kapanışı olduğundan, $Arf(m, m + r_1, m + r_2, \ldots, m + r_p) \subseteq (m + Arf(m, r_1, r_2, \ldots, r_p)) \cup \{0\}$ olur. Böylece $(m + Arf(m, r_1, r_2, \ldots, r_p)) \cup \{0\} = Arf(m, m + r_1, m + r_2, \ldots, m + r_p)$ elde edilir.
(*c*) (a) ve (b)'nin sonucu olarak elde edilir. ■

$X \subseteq \mathbb{N} \setminus \{0\}$ ve *obeb*$(X) = 1$ olmak üzere $\mathbb{N}$'nin bir alt kümeler dizisini

$$A_1 = X$$

$$A_{n+1} = (\{x - min\ A_n \mid x \in A_n\} - \{0\}) \cup \{min\ A_n\}$$

şeklinde tanımlayalım. Öklid algoritması fikri ile öyle bir negatif olmayan q tamsayısı vardır ki $q = min\ \{k \in \mathbb{N} \mid 1 \in A_k\}$ dır.

Önerme 2.79 *Yukarıdaki kabuller altında*

$$Arf(X) = \{0, min\ A_1, min\ A_1 + min\ A_2, \ldots, min\ A_1 + \ldots + min\ A_{q-1}, \longrightarrow\}$$

şeklindedir.

İspat. $1 \in A_q$ olduğundan $Arf(A_q) = \mathbb{N}$ dir.

$$Arf(A_{q-1}) = (min\ A_{q-1} + Arf(A_q)) \cup \{0\} = (min\ A_{q-1} + \mathbb{N}) \cup \{0\}$$

dır. Bu durumda $Arf(A_{q-1}) = \{0, minA_{q-1}, \longrightarrow\}$ dir. i üzerinden tümevarım kullanarak ispat yapalım. $Arf(A_{q-i})$'nın

$$\{0, min\ A_{q-i}, min\ A_{q-i} + min\ A_{q-i+1}, \ldots, min\ A_{q-i} + \ldots + min\ A_{q-1}, \longrightarrow\}$$

olduğunu kabul edelim. Şimdi $Arf(A_{q-i-1})$'in

$$\{0, min\ A_{q-i-1}, min\ A_{q-i-1} + min\ A_{q-i}, \ldots, min\ A_{q-i-1} + \ldots + min\ A_{q-1}, \longrightarrow\}$$

olduğunu iddia edelim.

$$Arf(A_{q-i-1}) = (min\ A_{q-i-1} + Arf(A_{q-i})) \cup \{0\}$$

eşitliğinde $Arf(A_{q-i})$'yi yerine koyalım böylece $Arf(A_{q-i-1})$ semigrubu

$$\{0, min\ A_{q-i-1}, min\ A_{q-i-1} + min\ A_{q-i}, \ldots, min\ A_{q-i-1} + \ldots + min\ A_{q-1}, \longrightarrow\}$$

kümesi olarak elde edilir ve ispat tamamlanmış olur. ■

Örnek 2.80 *$Arf(7, 24, 33)$'nın elemanlarını yukarıdaki algoritmayı kullanarak hesaplayalım. Burada $X = \{7, 24, 33\}$ dir.*
$A_1 = X,\ min\ A_1 = 7,$
$A_2 = (\{x - min\ A_1 \mid x \in A_1\} - \{0\}) \cup \{min\ A_1\} = \{7, 17, 26\},\quad min\ A_2 = 7$
$A_3 = (\{x - min\ A_2 \mid x \in A_2\} - \{0\}) \cup \{min\ A_2\} = \{7, 10, 19\},\quad min\ A_3 = 7$
$A_4 = (\{x - min\ A_3 \mid x \in A_3\} - \{0\}) \cup \{min\ A_3\} = \{7, 3, 12\},\quad min\ A_4 = 3$
$A_5 = (\{x - min\ A_4 \mid x \in A_4\} - \{0\}) \cup \{min\ A_4\} = \{3, 4, 9\},\quad min\ A_5 = 3$
$A_6 = (\{x - min\ A_5 \mid x \in A_5\} - \{0\}) \cup \{min\ A_5\} = \{1, 3, 6\}$ *elde edilir. Burada $q = 6$ ve $Arf(X) = \{0, 7, 14, 21, 24, 27, \longrightarrow\}$ dır.*

Önerme 2.81 *S Arf ise akuttur.*

İspat. S Arf nümerik semigrup olsun. $d \geq c' > d'$ olduğundan $d + c' - d' \in S$ ve $d + c' - d' > d$ dir. Böylece $d + c' - d' \geq c$ olur ve buradan S akuttur. ■

Örnek 2.82 *$S = \{0, 10, 11\} \cup \{i \in \mathbb{N} \mid i \geq 15\}$ olduğu durumda, $c = 15$, $d = 11$, $c' = 10$ ve $d' = 0$ dır. S, Arf nümerik semigrup olmadığı halde akut olan nümerik semigruba örnektir.*

Önerme 2.83 *Bir aralıkla üretilen ve Arf olan nümerik semigruplar, negatif olmayan uygun c tamsayıları için sadece $\{0\} \cup \{i \in \mathbb{N} \mid i \geq c\}$ formundaki nümerik semigruplardır.*

İspat. Lemma 2.50 ve Önerme 2.66'nın sonucu olarak elde edilir. ■

2.3. Cebirsel Fonksiyon Cisimleri

Bir projektif cebirsel eğri V, bir boyutlu projektif varyetedir. Bunun anlamı, V üzerindeki rasyonel fonksiyonlar cismi $K(V)$, bir değişkenli cebirsel fonksiyonlar cismidir. Bu bölümde cebirsel fonksiyon cisimlerinin genel özelliklerini vereceğiz. Bölüm boyunca K, herhangi bir cisim olacaktır. Ayrıntılı bilgi için (Stichtenoth 2009) bakılabilir.

2.3.1. Genel özellikler

Tanım 2.84 *F bir cisim ve $K \subseteq F$ cisim genişlemesi olsun. Eğer F, K üzerinde aşkın olan uygun $x \in F$ için $K(x)$ üzerinde bir sonlu genişleme ise F'ye K üzerinde bir değişkenli fonksiyon cismi denir, F/K ile gösterilir.*

Genel olarak F/K bir değişkenli fonksiyonlar cismi ise $F = K(x, y)$ olmak üzere öyle bir $\varphi(T) \in K(x)[T]$ indirgenemez polinomu vardır ki $\varphi(y) = 0$ dır.

Bu çalışma boyunca F, K üzerinde bir değişkenli fonksiyonlar cismini gösterecektir. $F = K(x)$ olacak şekilde $x \in F$, K üzerinde aşkın ise F/K fonksiyonlar cismine rasyonel fonksiyon cismi denir.

Örnek 2.85 *(1) $F = K(x)$ ve $x \in F$, K üzerinde aşkın olsun. F, $K(x)$ üzerinden sonlu genişleme olduğundan dolayı F/K bir fonksiyonlar cismidir.*
(2) $F = K(x, y)$ ve char $K \neq 2$ olsun. $y^2 = x(x-1)(x+1)$ polinomu için uygun $\varphi(T) \in K(x)[T]$ indirgenemez polinomu vardır ki $\varphi(y) = 0$ dır. O halde F/K bir fonksiyonlar cismidir.
(3) $F = \mathbb{R}(x, y)$ olsun. $x^2 + y^2 = -1$ polinomunu alalım. $\varphi(T) = x^2 + T^2 + 1$ indirgenemez polinomu için $\varphi(y) = 0$ olduğundan $\mathbb{R}(x, y)/\mathbb{R}$ bir fonksiyonlar cismidir.

F'nin K üzerinde cebirsel elemanları kümesi $\tilde{K}$, F'nin bir alt cismidir. $\tilde{K}$, F/K'nın sabitler cismi olarak adlandırılır ve $K \subseteq \tilde{K} \subsetneq F$ olur. Burada F, $\tilde{K}$ üzerinde fonksiyonlar cismidir. Ayrıca $K = \tilde{K}$ ise K'ya F'nin tüm sabitler cismi denir.

Örnek 2.86 (1) $F = K(x)$ *ise* $K = \tilde{K}$ *dır.*
(2) $F = \mathbb{R}(x, y)$ *ve* $x^6 + 2x^3y^2 + y^4 = -1$ *olsun.* $(x^3 + y^2)^2 = -1$ *için* $x, y \in F$ *olduğundan* $x^3 + y^2 = \alpha \in F$ *dir.* $\alpha^2 = -1$ *ve buradan* $\alpha = i$ *olmalıdır. O halde* $i \in F$ *dir. Fakat* $i \in \mathbb{C}$, $\mathbb{R}$ *üzerinden cebirsel olduğundan* $\mathbb{C} \subseteq F$ *olur. Böylece* $\tilde{K} = \mathbb{C}$ *dir.*

Tanım 2.87 F/K *bir değişkenli fonksiyon cismi ve* $\mathcal{O}$, F*'nin bir althalkası olsun.*
(a) $K \subsetneqq \mathcal{O} \subsetneqq F$
(b) *Her* $z \in F$ *için ya* $z \in \mathcal{O}$ *ya da* $z^{-1} \in \mathcal{O}$
koşulları sağlanıyorsa $\mathcal{O}$*'ya* F*'nin valuation halkası denir.*

F/K'nın bir $\mathcal{O}$ valuation halkası bir lokal halkadır, $\mathcal{O}$'nun maksimal idealine F/K fonksiyon cisminin bir noktası (place) denir. F/K'nın noktalar kümesi $\mathbb{P}_F$ ile gösterilir. $P \in \mathbb{P}_F$ ise $P = t\mathcal{O}$ olacak biçimde $t \in F$ vardır, bu t elemanına P'nin yerel parametresi denir. $\mathcal{O}$, F/K'nın valuation halkası ve P, onun maksimal ideali ise $\mathcal{O}$, P ile tek türlü belirlidir. Şöyle ki, $\mathcal{O} = \{z \in F \mid z^{-1} \notin P\}$ dir ve burada $\mathcal{O}$ halkasına P noktasında valuation halkası denir ve $\mathcal{O}_P$ ile gösterilir.

Tanım 2.88 F/K *fonksiyon cismi olsun.* $v : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ *fonksiyonu*
(a) $v(x) = \infty \iff x = 0$
(b) *Her* $x, y \in F$ *için* $v(xy) = v\ (x) + v(y)$ *dir.*
(c) *Her* $x, y \in F$ *için* $v(x + y) \geq \min\{v(x), v(y)\}$ *dir.*
(d) $v(z) = 1$ *olacak şekilde bir* $z \in F$ *vardır.*
(e) *Her* $0 \neq a \in K$ *için* $v(a) = 0$ *dır.*
koşullarını sağlarsa v*'ye bir ayrık değerlendirme (discrete valuation) denir, kısaca valuation diyeceğiz.*

F/K'nın bir v valuationı ve $v(x) \neq v(y)$ olacak şekilde $x, y \in F$ olsun. Bu durumda $v(x + y) = \min\{v(x), v(y)\}$ olur. $P \in \mathbb{P}_F$ ve t, P'nin yerel parametresi olmak üzere her $0 \neq z \in F$ elemanı $z = t^n u$ biçiminde tek türlü yazılabilir, burada u, $\mathcal{O}$'nun tersinir elemanı ve $n \in \mathbb{Z}$ dir. Bundan böyle $\mathcal{O}^*$ ile $\mathcal{O}$'nun tersinir elemanları kümesini göstereceğiz. $v_P : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ fonksiyonu $v_P(z) := n$, $v_P(0) := \infty$ ile tanımlanır.

Teorem 2.89 F/K *bir fonksiyon cismi olsun.*
(a) $P \in \mathbb{P}_F$ *için yukarıda tanımlanan* v_P *fonksiyonunun valuationdır. Üstelik,*

$$\begin{aligned} \mathcal{O}_P &= \{z \in F \mid v_P(z) \geq 0\}, \\ \mathcal{O}_P^* &= \{z \in F \mid v_P(z) = 0\}, \\ P &= \{z \in F \mid v_P(z) > 0\} \end{aligned}$$

dır. $x \in F$ *elemanı* P *için bir yerel parametredir ancak ve ancak* $v_P(x) = 1$ *dir. Tersine* v, F/K*'nın valuationı olsun.* F/K*'nın* $P := \{z \in F \mid v(z) > 0\}$ *noktasına karşılık gelen valuation halkası* $\mathcal{O}_P := \{z \in F \mid v(z) \geq 0\}$ *dır.*
(b) F/K*'nın her* $\mathcal{O}$ *valuation halkası* F*'nin maksimal althalkasıdır.*

İspat. (Stichtenoth 2009). ■

$\mathbb{P}_F$ noktalar kümesi, valuation halkaları kümesi ve valuation fonksiyonları kümesi arasında birebir eşleme vardır.

Tanım 2.90 *$P \in \mathbb{P}_F$ olsun.*
(a) $\mathcal{O}_P/P$'ye, P'nin kalan sınıflar cismi denir ve F_P ile gösterilir. $\mathcal{O}_P$ valuation halkası ve P onun maksimal ideali olduğundan $\mathcal{O}_P/P$ cisimdir. $F \longrightarrow F_P \cup \{\infty\}$, $x \longmapsto x(P)$ dönüşümüne P'ye göre kalan sınıflar dönüşümü denir. $x \in \mathcal{O}_P$ için $x + P := x(P)$ notasyonu kullanılır, $x \notin \mathcal{O}_P$ için $x(P) = \infty$ dur.
(b) P noktasının derecesi $[F_P : K]$ dır ve der P ile gösterilir. der $P = 1$ ise P, F/K'nın rasyonel noktası olarak adlandırılır.

P, F/K'nın bir noktası ve $0 \neq x \in P$ ise $\textit{der}\ P \leq [F : K(x)] < \infty$ dır. Sonuç olarak F/K'nın sabitler cismi $\tilde{K}$, K'nın bir sonlu genişlemesidir ve her noktanın derecesi sonludur.

Tanım 2.91 *$P \in \mathbb{P}_F$ ve $z \in F$ olsun. $v_P(z) > 0$ ise P'ye z'nin bir sıfırı, hatta $v_P(z) = m > 0$ ise P'ye z'nin m mertebeli bir sıfırı; $v_P(z) < 0$ ise P'ye z'nin bir kutbu, hatta $v_P(z) = -m < 0$ ise P'ye z'nin m mertebeli bir kutbu denir.*

Örnek 2.92 *$F = \mathbb{C}(x)$ ve $z = \frac{(x-2)^2}{(x-1)(x+3)^2}$ olsun. $P_1 = \langle (x-1) \rangle$, $P_2 = \langle (x-2) \rangle$, $P_3 = \langle (x+3) \rangle$ ve $v_{P_1}(z) = v_{P_1}\left(\frac{(x-2)^2}{(x-1)(x+3)^2}\right) = 2v_{P_1}(x-2) + v_{P_1}\left(\frac{1}{(x-1)(x+3)^2}\right) = 0 - v_{P_1}((x-1)(x+3)^2) = -v_{P_1}(x-1) - 2v_{P_1}(x+3) = -1 - 0 = -1$ olur. O halde P_1, 1 mertebeli kutup noktasıdır. Benzer şekilde P_2, 2 mertebeli sıfır noktası ve P_3, 2 mertebeli kutup noktasıdır.*

F/K bir fonksiyon cismi ve $x \in F$, K üzerinde aşkın eleman ise x'in en az bir sıfırı ve bir kutbunun olduğu kolayca görülebilir, dolayısıyla $\mathbb{P}_F \neq \emptyset$ dır.

2.3.2. Bölenler

F/K bir değişkenli cebirsel fonksiyonlar cismi ve K onun tüm sabitler cismi kabul edilecektir.

Tanım 2.93 *F/K'nın bölenler grubu $\mathbb{D}_F$,*

$$\mathbb{D}_F = \{D = \sum_{P \in \mathbb{P}_F} n_P P \mid \textit{hemen hemen her } P \in \mathbb{P}_F \textit{ için } n_P = 0, n_P \in \mathbb{Z}\}$$

dır. Bir $P \in \mathbb{P}_F$ ve D böleni için $v_P(D) = n_P$ tanımlanır.

Örnek 2.94 *$F = \mathbb{C}(x)$, $U = (x-3)^2(x+1)^3(x-2)^{-3}$ ifadesini bölen olarak ifade edersek $D = 2P_3 + 3P_1 - 3P_2 + 3P_\infty - 5P_\infty = 2P_3 + 3P_1 - 3P_2 - 2P_\infty$ olur. Özel olarak, P_3 noktasını alalım. $n_{P_3} = 2$ dir.*

$D = \sum_{P \in \mathbb{P}_F} n_P P$ böleni için destek kümesi *supp* $D = \{P \in \mathbb{P}_F \mid n_P \neq 0\}$ ile tanımlanır. $D = \sum_{P \in \mathbb{P}_F} n_P P$ ve $D' = \sum_{P \in \mathbb{P}_F} n'_P P$ olmak üzere iki bölenin toplamı

$$D + D' = \sum_{P \in \mathbb{P}_F} (n_P + n'_P) P$$

ve bölenin toplamsal tersi

$$-D = \sum_{P \in \mathbb{P}_F} -n_P P$$

dır. Ayrıca $\mathbb{D}_F$ bölen grubunun sıfırı

$$0 := \sum_{P \in \mathbb{P}_F} n_P P, \text{ her } n_P = 0$$

dir.

$$D_1 \leq D_2 \iff \text{Her } P \in \mathbb{P}_F \text{ için } v_P(D_1) \leq v_P(D_2)$$

$\mathbb{D}_F$ üzerinde kısmi sıralama bağıntısı tanımlar. Eğer $D_1 \leq D_2$ ve $D_1 \neq D_2$ ise $D_1 < D_2$ yazarız. Bir bölen $0 \leq D$ ise pozitif bölen olarak adlandırılır. Bir bölenin derecesi kavramı ise

$$der\ D = \sum_{P \in \mathbb{P}_F} n_P der\ P$$

ile tanımlıdır. Burada, $der : \mathbb{D}_F \longrightarrow \mathbb{Z}$ bir grup homomorfizmidir.

Tanım 2.95 *$0 \neq x \in F$, Z, x'in kutupları kümesi ve N, x'in sıfırları kümesi olmak üzere*

$$(x)_0 = \sum_{P \in N} v_P(x) P,\ (x)_\infty = \sum_{P \in Z} (-v_P(x)) P,\ (x) = (x)_0 - (x)_\infty$$

biçiminde tanımlanan bölenlere sırasıyla x'in sıfır böleni, kutup böleni ve esas böleni denir. $(x)_0 \geq 0$, $(x)_\infty \geq 0$ ve $(x) = \sum_{P \in \mathbb{P}_F} v_P(x) P$ olduğu açıktır. $0 \neq x \in F$ elemanı için

$$x \in K \iff (x) = 0$$

dır.

Tanım 2.96 *Bölenlerin*

$$\mathcal{P}(F) := \{(x) \mid 0 \neq x \in F\} \subseteq \mathbb{D}_F$$

kümesine F/K'nın esas bölenlerinin grubu denir.

$0 \neq x, y \in F$ için $(xy) = (x) + (y)$ ve $(x^{-1}) = -(x)$ olduğundan $\mathbb{D}_F$'nin bir alt grubudur. $\mathbb{D}_F/\mathcal{P}(\mathcal{F})$, F/K'nın bölen sınıfı grubu olarak adlandırılır. $D \in \mathbb{D}_F$ olmak üzere D'nin bölen sınıfı $[D]$ ile gösterilir. $[D_1] = [D_2]$ ise $D_1 + \mathcal{P}(\mathcal{F}) = D_2 + \mathcal{P}(\mathcal{F})$ alalım. $D_1 - D_2 \in \mathcal{P}(\mathcal{F})$ dir ancak ve ancak uygun $x \in F \setminus \{0\}$ için $D_1 - D_2 = (x)$ dır. Böylece $D_1 = D_2 + (x)$ olacak şekilde öyle $x \in F \setminus \{0\}$ vardır. $[D] = [D']$ ise $D, D' \in \mathbb{D}_F$'ye denk bölenler denir, $D \sim D'$ ile gösterilir.

Örnek 2.97 $u = \frac{(x-1)^2(x+3)^3}{(x-2)(x+4)^5}$ *ve* $v = \frac{(x-1)^4(x+3)^3}{(x-2)^2(x+4)^7}$ *olsun. Sırasıyla bölenler* $D = (u) = 2P_1 + 3P_3 - P_2 - 5P_4 - 5P_\infty + 6P_\infty = 2P_1 + 3P_3 - P_2 - 5P_4 + P_\infty$ *ve* $D' = (v) = 4P_1 + 3P_3 - 2P_2 - 7P_4 - 7P_\infty + 9P_\infty = 4P_1 + 3P_3 - 2P_2 - 7P_4 + 2P_\infty$ *şeklindedir.* $D' = D + 2P_1 - P_2 - 2P_4 + P_\infty = D + z$ *olacak şekilde uygun* $(z) = 2P_1 - P_2 - 2P_4 + P_\infty$ *böleni vardır. Sonuç olarak* $D \sim D'$ *dir.*

Tanım 2.98 $A \in \mathbb{D}_F$ *böleni için*

$$\mathcal{L}(A) := \{x \in F \mid (x) \geq -A\} \cup \{0\}$$

kümesine A ile oluşturulan Riemann-Roch uzayı denir.

$A = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j$, $n_i, m_j > 0$ olsun. $\mathcal{L}(A)$ kümesi, sıfırları Q_j noktasında $v_{Q_j}(x) \geq m_j > 0$ ve kutupları P_i noktalarında olma ihtimali olan $v_{P_i}(x) \geq -n_i$ $(i = 1, \ldots, r)$ olacak şekilde $x \in F$ elemanlarından oluşur.

Lemma 2.99 $A, B \in \mathbb{D}_F$ *olsun. Bu durumda*
(a) $x \in \mathcal{L}(A)$ *olması için gerekli ve yeterli koşul her* $P \in \mathbb{P}_F$ *için* $v_P(x) \geq -v_P(A)$ *olmasıdır.*
(b) $\mathcal{L}(A) \neq \{0\}$ *ancak ve ancak* $A' \geq 0$ *olacak şekilde bir* $A \sim A'$ *böleni vardır.*
(c) $\mathcal{L}(A)$, K *üzerinde bir vektör uzayıdır.*
(d) $A' \in \mathbb{D}_F$ *ve* $A \sim A'$ *ise* $\mathcal{L}(A)$ *ve* $\mathcal{L}(A')$ *izomorftur.*
(e) $\mathcal{L}(0) = K$ *dır.*
(f) $A < 0$ *ise* $\mathcal{L}(A) = \{0\}$ *dır.*
(g) $A \leq B$ *ise* $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ *ve* $boy_K\ (\mathcal{L}(B)/\mathcal{L}(A)) \leq der\ B - der\ A$ *dır.*

İspat. (Stichtenoth 2009). ■

Tanım 2.100 $A \in \mathbb{D}_F$ *böleni için* $l(A) := boy_K\ (\mathcal{L}(A))$ *tamsayısına A böleninin boyutu denir.*

Teorem 2.101 (a) *Her esas bölenin derecesi sıfırdır.*
(b) $x \in F \setminus K$ *için* $(x)_0, (x)_\infty$ *sırasıyla x'in sıfır böleni ve kutup böleni olsun.*

$$der\ (x)_0 = der\ (x)_\infty = [F : K(x)]$$

dir.
(c) $A, A' \in \mathbb{D}_F$ *olsun.*

(1) $A \sim A'$ *ise* $l(A) = l(A')$ *ve* $der\ A = der\ A'$

(2) $der\ A < 0$ *ise* $l(A) = 0$

(3) $der\ A = 0$ *olsun. Bu durumda,*
A *esas bölendir.* $\iff l(A) \geq 1 \iff l(A) = 1$ *olur.*

İspat. (Stichtenoth 2009). ■

Tanım 2.102 *F/K fonksiyonlar cismi olsun.*

$$g := maks\ \{der\ A - l(A) + 1 \mid A \in \mathbb{D}_F\}$$

tamsayısına F/K'nın cinsi denir.

Eğer $A = 0$ ise $der\ 0\ -l(0) + 1 = 0$ olduğundan $g \geq 0$ dır.

2.3.3. Riemann-Roch teoremi

Tanım 2.103 *$A \in \mathbb{D}_F$ böleni için,*

$$i(A) := l(A) - der\ A + g - 1$$

tamsayısına A'nın indeksi (index of speciality) denir.

A'nın derecesi yeterince büyük seçilir ise $i(A) = 0$ olur. Dolayısıyla $i(A)$ negatif olmayan bir tamsayıdır.

Tanım 2.104 *F/K fonksiyonlar cismi olsun.*

$$\alpha : \begin{cases} \mathbb{P}_F \longrightarrow F \\ P \longmapsto \alpha_P \end{cases}$$

fonksiyonunu ele alalım. Sonlu sayıda hariç her $P \in \mathbb{P}_F$ için $\alpha_P \in \mathcal{O}_P$ ise α'ya F/K'nın bir adeli denir. F/K'nın adeller kümesi $\mathcal{A}_F$ ile gösterilir.

Bir adel, $\prod_{P \in \mathbb{P}_F} F$ direk çarpımının bir elemanı olarak ifade edilebilir.

$$\mathcal{A}_F = \left\{ \alpha = (\alpha_P) \in \prod_{P \in \mathbb{P}_F} F \mid \text{sonlu sayıda hariç her } P \in \mathbb{P}_F \text{ için } v_P(\alpha_P) \geq 0 \right\}$$

dır. $\mathcal{A}_F$, K üzerinden vektör uzayıdır. $x \in F$ için $(x, x, ...) \in \mathcal{A}_F$ ile F, $\mathcal{A}_F$ içinde düşünülebilir.

Tanım 2.105 *(a) $A \in \mathbb{D}_F$ böleni için,*

$$\mathcal{A}_F(A) := \{\alpha \in \mathcal{A}_F \mid v_P(\alpha) \geq -v_P(A),\ her\ P \in \mathbb{P}_F\}$$

tanımlanır.
(b) F/K fonksiyonlar cismi ve $w : \mathcal{A}_F \longrightarrow K$, K üzerinde doğrusal bir dönüşüm olsun. Uygun bir $A \in \mathbb{D}_F$ böleni için $w(\mathcal{A}_F(A) + F) = 0$ ise w'ye F/K'nın Weil diferansiyeli denir. F/K'nın Weil diferansiyeli kümesi Ω_F ile gösterilir. $A \in \mathbb{D}_F$ böleni için,

$$\Omega_F(A) := \{w \in \Omega_F \mid w(\mathcal{A}_F(A) + F) = 0\}$$

tanımlanır.

$\mathcal{A}_F(A)$, $\mathcal{A}_F$'nin, $\Omega_F\ (A)$, Ω_F'nin K üzerinde alt vektör uzaylarıdır.

Önerme 2.106 *Ω_F, K üzerinden vektör uzayıdır. Hatta Ω_F , F üzerinde bir boyutlu vektör uzayıdır.*

İspat. (Stichtenoth 2009). ■

Tanım 2.107 *(a) $0 \neq w \in \Omega_F$, $A, B \in \mathbb{D}_F$ olsun. $w(\mathcal{A}_F(B)+F) = 0$ ve $w(\mathcal{A}_F(A)+F) = 0$ iken $A \leq B$ sağlanıyorsa B'ye w'nin böleni denir ve $B = (w)$ ile gösterilir.*
(b) $0 \neq w \in \Omega_F$ için $v_P(w)$, $v_P((w))$ ile tanımlanır.
(c) $w \in \Omega_F$ ve $P \in \mathbb{P}_F$ olmak üzere $v_P(w) > 0$ ise P'ye w'nin sıfırı, $v_P(w) < 0$ ise P'ye w'nin kutbu, $v_P(w) \geq 0$ ise w'ye P de düzenlidir denir.
(d) F/K'nın bir böleni uygun bir Weil diferansiyelinin bir böleni ise bu bölene kanonik bölen denir.

$0 \neq x \in F$ ve $0 \neq w \in \Omega_F$ için $(xw) = (x) + (w)$ dir. Böylece kanonik iki bölen denktir.

Teorem 2.108 *(a) (Duality Teoremi) $A \in \mathbb{D}_F$ ve $W = (w)$, F/K'nın bir kanonik böleni olsun. O halde*

$$\mu : \begin{cases} \mathcal{L}(W-A) \longrightarrow \Omega_F\ (A) \\ \qquad\qquad x \longmapsto xw \end{cases}$$

dönüşümü vektör uzayı olarak K-izomorfizmdir.
(b) (Riemann-Roch Teoremi) W, F/K'nın bir kanonik böleni ve cinsi g olsun. Her $A \in \mathbb{D}_F$ için

$$l(A) = der\ A + 1 - g + l(W-A)$$

dır.

İspat. (Stichtenoth 2009). ■

Sonuç 2.109 *(a) W kanonik böleni için $der\ W = 2g - 2$ ve $l(W) = g$ dir.*
(b) $A \in \mathbb{D}_F$ için $der\ A \geq 2g - 1$ ise $l(A) = der\ A + 1 - g$ dir.

İspat. (a) Riemann-Roch teoremi ve Lemma 2.99 (e)'den yararlanarak, $A = 0$ için

$$1 = l(0) = der0 + 1 - g + l(W - 0)$$

dır. Böylece $l(W) = g$ olur. Öte yandan Riemann-Roch teoreminde $A = W$ için

$$g = l(W) = derW + 1 - g + l(W - W) = derW + 2 - g$$

olur ve buradan $der\ W = 2g - 2$ dir.
(b) Riemann-Roch teoreminde W kanonik böleni için $l(A) = der\ A+1-g+l(W-A)$ dır. $l(W-A)$ için $der\ (W-A) = der\ (W)-der\ A = 2g-2-der\ A$ ve $der\ A \geq 2g-1$ olduğundan $der\ (W-A) < 0$ olur. Teorem 2.101 (c-2)'den $l(W-A) = 0$ dır. ■

Tanım 2.110 *$P \in \mathbb{P}_F$ olsun. $(x)_\infty = nP$ olacak şekilde bir $x \in F$ varsa $n \geq 0$ sayısına P'nin bir kutup sayısı (pole number) denir. Aksi halde P'nin boşluk sayısı (gap number) olarak adlandırılır.*

$n \in \mathbb{N}$, P'nin kutup sayısıdır ancak ve ancak $l(nP) > l((n-1)P)$ dir. Ayrıca, P'nin kutup sayılarının kümesi $\mathbb{N}$ toplamsal semigrubunun bir alt semigrubudur. Şöyle ki n_1, n_2 kutup sayısı ise $(x_1)_\infty = n_1 P$, $(x_2)_\infty = n_2 P$ ve buradan $(x_1 x_2)_\infty = (n_1 + n_2)P$ dir.

Önerme 2.111 *(a) F/K fonksiyonlar cismi için aşağıdaki ifadeler denktir:*

(1) F rasyonel fonksiyonlar cismidir, yani $F = K(x)$ dir.

(2) F/K fonksiyonlar cismi için $g = 0$ ve der $A = 1$ olacak şekilde uygun $A \in \mathbb{D}_F$ vardır.
(b) $P \in \mathbb{P}_F$ olsun. Bu durumda her $n \geq 2g$ için kutup böleni $(x)_\infty = nP$ olacak şekilde bir $x \in F$ vardır.

İspat. (Stichtenoth 2009). ■

Teorem 2.112 *(Weierstrass Boşluk Teoremi) F/K fonksiyonlar cismi, $g > 0$ ve $P \in \mathbb{P}_F$ derecesi bir olan bir nokta olsun. Bu durumda P'nin $i_1 < \ldots < i_g$ olacak şekilde tam g tane boşluk sayısı vardır. Üstelik, $i_1 = 1$ ve $i_g \leq 2g - 1$ dir.*

İspat. Önerme 2.111 (c)'den P'nin her boşluk sayısı $\leq 2g - 1$ dir ve 0 bir kutup sayısıdır. Boşluk sayıları için

$$i, P\text{'nin bir boşluk sayısıdır } \iff \mathcal{L}((i-1)P) = \mathcal{L}(iP)$$

karakterizasyonu vardır. Vektör uzaylarının

$$K = \mathcal{L}(0) \subseteq \mathcal{L}(P) \subseteq \mathcal{L}(2P) \subseteq \cdots \subseteq \mathcal{L}((2g-1)P) \subseteq \cdots$$

dizisini düşünürsek burada Sonuç 2.109 (b) yardımıyla $l(0) = 1$ ve $l((2g-1)P) = g$ dir. Lemma 2.99 (g)'den her i için

$$l(iP) \leq l((i-1)P) + 1$$

dir. $\mathcal{L}((i-1)P) \subsetneqq \mathcal{L}(iP)$ yardımıyla $1 \leq i \leq 2g-1$ için $g-1$ sayı vardır. g sayısı P'nin boşluklarıdır. Şimdi 1 sayısının boşluk olduğunu göstermeliyiz. Aksini varsayalım, 1 sayısı P'nin bir kutbu olsun. Kutup sayılarının kümesi toplamsal bir semigrup olduğundan, her $n \in \mathbb{N}$ sayısı bir kutup sayısıdır ve hiç bir boşluğa sahip değildir. Bu ise $g > 0$ ile çelişir. ■

Tanım 2.113 *$P \in \mathbb{P}_F$ olmak üzere P'deki kutup sayıları kümesine Weierstrass semigrup denir.*

Gözlem 2.114 $\mathcal{L}(0) \subseteq \mathcal{L}(P) \subseteq \mathcal{L}(2P) \subseteq \cdots \subseteq \mathcal{L}((2g-1)P) \subseteq \mathcal{L}(2gP) \subseteq \cdots$ *dizisinde sonlu sayıda hariç her P noktası için kutup sayıları kümesi aynıdır. Sadece sonlu sayıda nokta için farklanır. Bu tip noktalara Weierstrass noktası aksi halde adi (ordinary) nokta denir.*

F/K, F'/K' cebirsel fonksiyonlar cismi ve tüm sabitler cismi sırasıyla K, K' olsun. Burada K mükemmel cisim kabul edilecektir.

Tanım 2.115 *F'/K've F/K cebirsel fonksiyonlar cismi olsun. $K' \supseteq K$, $F' \supseteq F$ ve F'/F cebirsel genişleme ise F'/K'ya F/K'nın bir cebirsel genişlemesi denir. $[F' : F] < \infty$ ise F'/K'ya F/K'nın sonlu genişlemesi denir.*

F'/K', F/K'nın cebirsel genişlemesi olsun. K'/K cebirsel ve $F \cap K' = K$ dır.

Tanım 2.116 *F'/K', F/K'nın cebirsel genişlemesi ve $P \in \mathbb{P}_F$ olsun. $P' \in \mathbb{P}_{F'}$ için $P \subseteq P'$ ise P', P'nin bir genişlemesidir denir, $P'|P$ ile gösterilir.*

Önerme 2.117 *F'/K', F/K'nın cebirsel genişlemesi, P (veya P'), F/K'nın (F'/K''nın) bir noktası ve $Q_P \subseteq F$ ($Q_{P'} \subseteq F'$) karşılık gelen valuation halkası, v_P ($v_{P'}$) karşılık gelen valuation olsun. $P'|P$ ise, $P = P' \cap F$ ve $Q_P = Q_{P'} \cap F$ dir.*
$P'|P \iff Q_P \subseteq Q_{P'} \iff$ Her $x \in F$ için $v_{P'}(x) = e.v_P(x)$ olacak şekilde bir $e \geq 1$ tamsayısı vardır.

İspat. (Stichtenoth 2009). ■

Tanım 2.118 *Önerme 2.117'de bahsedilen $e := e(P'|P) \geq 1$ tamsayısına P' nün P üzerinde dallanma indeksi (ramification index) denir. $e(P'|P) = 1$ ise P', P üzerinde dallanmamış (unramified), aksi halde dallanmıştır (ramified) denir. $[F'_{P'} : F_P]$'ye P' nün P üzerinden relative derecesi denir ve $f(P'|P)$ ile gösterilir.*

Önerme 2.119 *$P'|P$ ve F'/K', F/K'nın cebirsel genişlemesi olsun.*
(a) $f(P'|P) < \infty \iff [F' : F] < \infty$
(b) F''/K'', F/K'nın cebirsel genişlemesi ve $P'' \in \mathbb{P}_{F''}$, P' nün genişlemesi ise

$$e(P''|P) = e(P''|P').e(P'|P) \text{ ve } f(P''|P) = f(P''|P').f(P'|P)$$

dir.
(c) Her $P' \in \mathbb{P}_{F'}$ için tam bir tane $P \in \mathbb{P}_F$ vardır ki $P'|P$, yani $P = P' \cap F$ dir.
(d) Her $P \in \mathbb{P}_F$ için en az bir, en çok sonlu sayıda $P' \in \mathbb{P}_{F'}$ genişlemesi vardır.

İspat. (Stichtenoth 2009). ■

Teorem 2.120 *F'/K', F/K'nın sonlu genişlemesi, $P \in \mathbb{P}_F$ ve $P_1, \ldots, P_m$, F'/K' de P'nin genişlemeleri olsun. $e_i = e(P_i|P)$, $f_i = f(P_i|P)$ ise*

$$\sum_{i=1}^{m} e_i.f_i = [F' : F]$$

dir.

İspat. (Stichtenoth 2009). ■

Bu çalışmada yararlanacağımız fonksiyon cismi genişlemelerinin önemli iki sınıfını oluşturan Kummer ve Artin-Schreier genişlemeleri hakkında detaylı bilgi için (Stichtenoth 2009)'a bakılabilir.

2.3.4. Cebirsel fonksiyon cismi örnekleri

Bu bölümde bazı cebirsel eğrileri fonksiyon cismi dilinde inceleyeceğiz. İlk örnek K üzerinde rasyonel fonksiyonlar cismi $K(x)$ dir ve cinsi $g = 0$ dır. Burada $g \geq 1$ olan bazı fonksiyon cisimlerini ifade edelim.

Tanım 2.121 *K, F'nin tüm sabitler cismi olmak üzere F/K fonksiyonlar cisminin cinsi, $g = 1$ ve der $A = 1$ olacak şekilde uygun $A \in \mathbb{D}_F$ var ise F/K'ya **eliptik fonksiyon cismi** denir.*

Önerme 2.122 *F, K üzerinde bir eliptik fonksiyon cismi olsun.*
(a) char $K \neq 2$ ise $F = K(x, y)$ ve

$$y^2 = f(x) \in K[x]$$

olacak şekilde uygun $x, y \in F$ vardır, burada $f(x)$ tam kare böleni olmayan polinom ve der $f(x) = 3$ dür.
(b) char $K = 2$ ise $F = K(x, y)$ ve

$$y^2 + y = f(x) \in K[x], \text{ der } f = 3$$

ya da

$$y^2 + y = x + \frac{1}{ax + b},\ a, b \in K \text{ ve } a \neq 0$$

olacak şekilde uygun $x, y \in F$ vardır.

İspat. (Stichtenoth 2009). ■

Tanım 2.123 *F/K cebirsel fonksiyon cismi olsun. $g \geq 2$, $[F : K(x)] = 2$ ve $K(x) \subseteq F$ ise F/K' ya **hipereliptik fonksiyonlar cismi** denir.*

Lemma 2.124 *(a) Cinsi $g \geq 2$ olan F/K cebirsel fonksiyonlar cismi hipereliptiktir ancak ve ancak der $A = 2$ ve $l(A) \geq 2$ olacak şekilde bir $A \in \mathbb{D}_F$ vardır.*
(b) $g = 2$ olan her F/K cebirsel fonksiyonlar cismi hipereliptiktir.

İspat. *(a)* F/K hipereliptik olsun. $[F : K(x)] = 2$ olacak şekilde $x \in F$ seçelim ve $A := (x)_\infty$ bölenini düşünelim. O halde *der* $A = 2$ ve $1, x \in \mathcal{L}(A)$ elemanları K üzerinde lineer bağımsızdır. Sonuç olarak $l(A) \geq 2$ dir.

Tersine, F/K'nın cinsi $g \geq 2$ ve $l(A) \geq 2$ ile *der* $A = 2$ olan A bölenini ele alalım. $A_1 \sim A$ olacak şekilde $A_1 \geq 0$ böleni vardır. Böylece *der* $A_1 = 2$ ve $l(A_1) \geq 2$ dir. $x \in \mathcal{L}(A_1) \setminus K$ olacak şekilde bir eleman bulabiliriz. O halde $(x)_\infty \leq A_1$ dir ve böylece $[F : K(x)] = der\ (x)_\infty \leq 2$ olur. F/K rasyonel olmadığından $[F : K(x)] = 2$ elde edilir.
(b) F/K'nın cinsi $g = 2$ olarak verilsin. Sonuç 2.109 (a)'dan her $W \in \mathbb{D}_F$ kanonik böleni için *der* $W = 2g - 2 = 2$ ve $l(W) = g = 2$ vardır. *(a)* yardımıyla F/K'nın hipereliptik olduğu görülür. ■

Örnek 2.125 *Öyle fonksiyon cisimleri vardır ki, bir P noktası için boşluk sayısı dizisi $1, 2, ..., g$ den farklıdır. Örneğin, $F = K(x, y)$, $y^3 + x^3y + x = 0$ ile tanımlı F'ye* ***Klein quartik fonksiyon cismi*** *denir.*

Örnek 2.126 *F_{q^2} üzerinde*

$$y^q + y = x^m$$

denklemiyle verilen $F = F_{q^2}(x, y)$ fonksiyon cismini dikkate alalım, burada q bir asal sayının kuvveti, m bir pozitif tamsayı ve $(q, m) = 1$ dir. Bu sınıf için cins $g = (q - 1)(m - 1)/2$ dir. Eğer $m = q + 1$ ise fonksiyon cismine ***Hermityen fonksiyon cismi*** *denir.*

Lemma 2.127 *F_{q^2} üzerinde Hermityen fonksiyon cismi*

$$H = F_{q^2}(x, y) \text{ ve } y^q + y = x^{q+1}$$

ile tanımlanabilir. O halde aşağıdaki özellikler sağlanır:
(a) H'nin cinsi $g = q(q - 1)/2$ dir.
(b) H, F_{q^2} üzerinde derecesi bir olan $q^3 + 1$ noktaya sahiptir. Yani,

(1) x ve y'nin ortak kutbu Q_∞ dur.

(2) Her $\alpha \in F_{q^2}$ için, $\beta^q + \beta = \alpha^{q+1}$ olacak şekilde q tane $\beta \in F_{q^2}$ vardır. Ayrıca her (α, β) ikilisi için, $x(P_{\alpha,\beta}) = \alpha$ ve $y(P_{\alpha,\beta}) = \beta$ olmak üzere derecesi bir olan sadece $P_{\alpha,\beta} \in \mathbb{P}_H$ noktasıdır.

İspat. Genelleşmiş Artin-Schreier genişlemesi yardımıyla ispatlanabilir. ■

Örnek 2.128 *Uygun pozitif n pozitif tamsayısı için $q_0 = 2^n$ ve $q = 2^{2n+1}$ olmak üzere,*

$$y^q - y = x^q(x^{q_0} - x)$$

denklemi ile belirlenen bir değişkenli cebirsel fonksiyonlar cismini $F := F_q(x, y)/F_q$ ile gösterelim. Bu fonsiyon cismine ***Suzuki fonksiyon cismi*** *denir. $q^2 + 1$ tane rasyonel noktası vardır.*

2.4. Cebirsel Kodlar

Bu bölümde kodun tanımı, sahip olduğu parametrelerin özellikleri ve ayrıca cebirsel geometrik kod ile duali olan kodun sahip olduğu parametrelerin özellikleri verilecektir.

2.4.1. Kodlar

q bir asal sayının kuvveti olmak üzere, $\mathbb{F}_q$ ile q elemanlı sonlu cisim ve $\mathbb{F}_q^n$ ile $\mathbb{F}_q$'nun n-defa kendisiyle kartezyen çarpımı gösterilecektir.

Tanım 2.129 *(a) $a = (a_1, a_2, ..., a_n)$, $b = (b_1, b_2, ..., b_n) \in \mathbb{F}_q^n$ olmak üzere a ve b'nin Hamming uzaklığı*

$$d(a, b) := \#\{i \mid a_i \neq b_i\},$$

$a \in \mathbb{F}_q^n$'nin ağırlığı ise

$$wt(a) := d(a, 0) = \#\{i \mid a_i \neq\neq 0\}$$

ile tanımlanır.
(b) $C \subseteq \mathbb{F}_q^n$, $\mathbb{F}_q^n$'nin bir alt vektör uzayı ise C'ye $\mathbb{F}_q$ üzerinde bir lineer kod, C'nin her bir elemanına ise bir kod kelime denir.
(c) C'nin $\mathbb{F}_q$ üzerinden vektör uzayı olarak boyutuna, C kodunun boyutu denir ve boy C ile gösterilir.
(d) $C \subseteq \mathbb{F}_q^n$ olduğundan n'ye C kodunun uzunluğu denir.
(e) C, $\mathbb{F}_q$ üzerinden bir lineer kod olmak üzere

$$d(C) := \min \{d(a, b) \mid a, b \in C; a \neq b\}$$

sayısına C kodunun Hamming uzaklığı ya da minimum uzaklığı denir.

Örnek 2.130 *$\mathbb{F}_q^n = \mathbb{Z}_5^4$ olsun. $wt(1, 3, 2, 4) = 4$, $wt(1, 4, 0, 0) = 2$, $wt(0, 3, 0, 0) = 1$, $wt(4, 3, 0, 1) = 3$ ve $d((4, 3, 0, 1), (1, 3, 2, 4)) = 3$, $d((1, 4, 0, 0), (0, 3, 0, 0)) = 2$ dır.*

Tanım 2.131 *Uzunluğu n, boyutu k, minimum uzaklığı d olan bir lineer koda $[n, k, d]$ kod ve n,k,d'ye bu kodun parametreleri denir.*

C kodunun minimum uzaklığı için

$$\begin{aligned} d(C) &= \min \{d(a, b) \mid a, b \in C, a \neq b\} = \min \{d(a - b, 0) \mid a, b \in C,\ a \neq b\} \\ &= \min \{wt(a - b) \mid 0 \neq a - b \in C\} \end{aligned}$$

dir.

Tanım 2.132 *(a) C, $\mathbb{F}_q$ üzerinden $[n, k, d]$ kod olsun. Satırları C'nin bir tabanı olan kxn matrisine C'nin bir üreteç matrisi denir.*
(b) $a = (a_1, a_2, ..., a_n)$, $b = (b_1, b_2, ..., b_n) \in \mathbb{F}_q^n$ için $\langle a, b\rangle := \sum_{i=1}^{n} a_i b_i$ ile tanımlanan ifadeye $\mathbb{F}_q^n$ üzerinde kanonik iç çarpım denir.
(c) $C \subseteq \mathbb{F}_q^n$ bir kod ise $C^{\perp} := \{u \in \mathbb{F}_q^n \mid \langle u, c\rangle = 0$ her $c \in C\}$ kümesine C'nin duali denir.

$\mathbb{F}_q^n = C \oplus C^\perp$ dir ve boyuta geçilirse $n = boy\ C + boy\ C^\perp$ dir.

Tanım 2.133 *$C^\perp$'in üreteç matrisine C'nin parite kontrol matrisi (eşitlik kontrol matrisi) denir.*

Bir $[n, k, d]$ lineer kodun kontrol matrisi H, $(n-k)$xn tipinde bir matristir ve $rank = n-k$ dır. u^t, u'nun devriği (transpoze) olmak üzere $C = \{u \in \mathbb{F}_q^n \mid H.u^t = 0\}$ dır. Böylece parite kontrol matrisi, bir $u \in \mathbb{F}_q^n$ vektörünün bir kod kelime olup olmadığını kontrol eder.

Önerme 2.134 *(Singleton Sınırı) C bir lineer $[n, k, d]$ kod olsun. Bu durumda*

$$k + d \leq n + 1$$

dir.

İspat. (Stichtenoth 2009). ■

C bir lineer $[n, k, d]$ kod olsun. $k + d = n + 1$ ise C lineer koduna maksimum uzaklıkta ayrılabilir kod (MDS) denir.

2.4.2. Cebirsel geometrik kodlar

V.D. Goppa tarafından tanımlandığı için bu kodlar geometrik Goppa kodlar olarak adlandırılır. Bu bölümde aşağıdaki gösterimleri kullanacağız.

$F/\mathbb{F}_q$ cinsi g olan cebirsel fonksiyonlar cismidir.

$P_1, P_2, ..., P_n$, $F/\mathbb{F}_q$'nun derecesi 1 olan, ikişerli birbirinden farklı bölenleridir.

$D = P_1 + P_2 + ... + P_n$.

G, $F/\mathbb{F}_q$'nın $Supp\ G \cap Supp\ D = \emptyset$ olacak şekilde bir böleni olsun.

Tanım 2.135 *$ev_D : \mathcal{L}(G) \to \mathbb{F}_q^n$ dönüşümü $ev_D(x) := (x(P_1), ..., x(P_n)) \in \mathbb{F}_q^n$ ile tanımlansın. D ve G bölenleri ile oluşturulan $C_\mathcal{L}(D, G) := ev_D(\mathcal{L}(G))$ cebirsel geometrik kodu*

$$C_\mathcal{L}(D, G) := \{(x(P_1), ..., x(P_n)) \mid x \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n$$

ile tanımlanır.

$Supp\ G \cap Supp\ D = \emptyset$ olduğundan $x \in \mathcal{L}(G)$ için $v_{P_i}(x) \geq 0$ $(i = 1, 2, ..., n)$ olur. x'in P_i moduna göre $x(P_i)$ kalan sınıfı, P_i'nin kalan sınıflar cisminin bir elemanıdır. P_i'nin derecesi 1 olduğundan kalan sınıflar cismi $\mathbb{F}_q$ ve böylece $x(P_i) \in \mathbb{F}_q$ dır.

Teorem 2.136 *$C_\mathcal{L}(D, G)$*

$$k = l(G) - l(G - D)\ ve\ d \geq n - der\ G$$

ile bir $[n, k, d]$ koddur .

İspat. Tanım 2.135 ile verilen ev_D dönüşümü örten bir lineer dönüşümdür ve

$$\text{Çek}(ev_D) = \{x \in \mathcal{L}(G) \mid v_{P_i}(x) > 0;\ i = 1, ..., n\} = \mathcal{L}(G - D)$$

dir. $k = boy\ C_{\mathcal{L}}(D, G) = boy\ \mathcal{L}(G) - boy\ \mathcal{L}(G - D)$ dir. $C_{\mathcal{L}}(D, G) \neq 0$ ise minimum uzaklık d kabul edilebilir. $wt(ev_D(x)) = d$ olacak şekilde $x \in \mathcal{L}(G)$ seçelim. D'nin destek kümesinde $P_{i_1}, ..., P_{i_{n-d}}$ olmak üzere tam $n - d$ nokta vardır. Böylece

$$0 \neq x \in \mathcal{L}(G - (P_{i_1} + ... + P_{i_{n-d}}))$$

olur. Teorem 2.101 (c-2) yardımıyla

$$0 \leq der\ (G - (P_{i_1} + ... + P_{i_{n-d}})) = der\ G - n + d$$

olur ve böylece $d \geq n - der\ G$ dir. ■

Sonuç 2.137 *der $G < n$ kabul edelim. O halde $ev_D : \mathcal{L}(G) \to C_{\mathcal{L}}(D, G)$ dönüşümü birebirdir ve bu durumda,*
(a) $C_{\mathcal{L}}(D, G)$ lineer kodu $d \geq n - der\ G$ ve $k = l(G) \geq der\ G + 1 - g$ ile bir $[n, k, d]$ koddur. Böylece

$$k + d \geq n + 1 - g$$

olur. Önerme 2.134 ile birleştirilirse $n + 1 - g \leq k + d \leq n + 1$ şeklinde $k + d$ için alt ve üst sınır belirlenmiş olur.
(b) $2g - 2 < der\ G < n$ ise $k = der\ G + 1 - g$ dir.
(c) $\{x_1, ..., x_k\}$, $\mathcal{L}(G)$'nin bir tabanı ise

$$M = \begin{pmatrix} x_1(P_1) & x_1(P_2) & \dots & x_1(P_n) \\ \vdots & \vdots & & \vdots \\ x_k(P_1) & x_k(P_2) & \dots & x_k(P_n) \end{pmatrix}$$

matrisi $C_{\mathcal{L}}(D, G)$'nin üreteç matrisidir.

İspat. (Stichtenoth 2009). ■

$g = 0$ ise $n + 1 = k + d$ olduğundan bu tür kodların MDS kod olduğuna dikkat edelim.

Tanım 2.138 *$d^* := n - der\ G$ tamsayısına $C_{\mathcal{L}}(D, G)$ kodunun atanmış uzaklığı denir.*

Tanım 2.139 *G ve D, bu bölüm başında verilen kabuldeki gibi olsun. Bu durumda, $C_{\Omega}(D, G)$ kodu*

$$C_{\Omega}(D, G) := \{(w_{P_1}(1), ..., w_{P_n}(1)) \mid w \in \Omega_F(G - D)\} \subseteq \mathbb{F}_q^n$$

ile tanımlanır.

Teorem 2.140 *$C_\Omega(D,G)$ bir $[n',k',d']$ kod olsun.*
(a) $k' = i(G-D) - i(G)$ ve $d' \geq der\ G - (2g-2)$ dir.
(b) $der\ G > 2g-2$ ise $k' = i(G-D) \geq n+g-1-der\ G$ dir.
(c) $2g-2 < der\ G < n$ ise $k' = n+g-1-der\ G = n+g-(der\ G+1)$ dir.
(d) $C_\Omega(D,G) = (C_\mathcal{L}(D,G))^\perp$ dir.

İspat. (Stichtenoth 2009). ■

Tanım 2.141 *$(d')^* = der\ G-(2g-2)$ ye $C_\Omega(D,G)$'nin atanmış uzaklığı denir.*

Önerme 2.142 *$v_{P_i}(\eta) = -1$ ve $\eta_{P_i} = 1$, $i = 1,...,n$ olacak şekilde bir η Weil diferansiyeli için $H := D - G + (\eta)$ olmak üzere*

$$(C_\mathcal{L}(D,G))^\perp = C_\Omega(D,G) = C_\mathcal{L}(D,H)$$

dir.

İspat. $(C_\mathcal{L}(D,G))^\perp = C_\Omega(D,G)$ eşitliği Teorem 2.140 (d)'de verilmişti. $i = 1,...,n$ için $v_{P_i}(\eta) = -1$ olduğundan $Supp\ (D-G+(\eta)) \cap Supp\ D = \emptyset$ olur. Buradan $C_\mathcal{L}(D, D-G+(\eta))$ tanımlıdır. Teorem 2.108 (a) yardımıyla $\mu(x) := x\eta$ ile tanımlanan $\mu : \mathcal{L}(D, D-G+(\eta)) \to \Omega_F(G-D)$ olacak şekilde bir izomorfizm vardır. $x \in \mathcal{L}(D, D-G+(\eta))$ için

$$(x\eta)_{P_i}(1) = \eta_{P_i}(x) = x(P_i).\eta_{P_i}(1) = x(P_i)$$

dir. Böylece $C_\Omega(D,G) = C_\mathcal{L}(D, D-G+(\eta))$ olur. ■

Sonuç 2.143 *Eğer*

$$2G - D \leq (\eta)\ ve\ i = 1,...,n\ için\ \eta_{P_i}(1) = 1$$

olacak şekilde bir η Weil diferansiyeli var ise $C_\mathcal{L}(D,G) \subseteq (C_\mathcal{L}(D,G))^\perp$ dir. Eğer

$$2G - D = (\eta)\ ve\ \eta_{P_i}(1) = 1,\ i = 1,...,n$$

ise $C_\mathcal{L}(D,G) = (C_\mathcal{L}(D,G))^\perp$ dir.

İspat. $2G - D \leq (\eta)$ ifadesi $G \leq D - G + (\eta)$ ifadesine denktir. Önerme 2.142'den

$$(C_\mathcal{L}(D,G))^\perp = C_\mathcal{L}(D, D-G+(\eta)) \supseteq C_\mathcal{L}(D,G)$$

elde edilir, böylece ilk koşul sağlanır. $2G - D = (\eta)$ yani $G = D - G + (\eta)$ ise

$$(C_\mathcal{L}(D,G))^\perp = C_\mathcal{L}(D, D-G+(\eta)) = C_\mathcal{L}(D,G)$$

dır. ■

3. BULGULAR

Bu bölümde nümerik semigrupların, cebirsel eğriler ve cebirsel kodlara bazı uygulamaları verilmiştir. Burada c, $S = \{\rho_0 = 0 < \rho_1 < \ldots\}$ nümerik semigrubunun önderi olmak üzere $c = \rho_r$ ile gösterilecektir.

3.1. Cebirsel Eğriler ile Nümerik Semigrupların İlişkileri

Örnek 3.1 (1) *Pseudo-simetrik olan ve aralıkla üretilen tek nümerik semigrup* $\{0, 3, \longrightarrow\}$ *olduğu Önerme 2.51 de gösterilmiştir.*
(2) *F bir hipereliptik fonksiyonlar cismi ve Q, F üzerinde rasyonel nokta olsun. Q'nun Weierstrass semigrubu hipereliptik olarak adlandırılır, yani, bazı $t \geq 3$ olan tek tamsayılar için $S =< 2, t >$ dir. (Eğer $t = 3$ semigrubu genel olarak eliptik olarak adlandırılır). Hipereliptik semigruplar $e(S) = 2$ olduğundan simetriktir. Üstelik, Arf nümerik semigruptur.*

Önerme 3.2 *Arf pseudo-simetrik olan nümerik semigruplar sadece* $\{0, 3, \longrightarrow\}$ *ve* $\{0, 3, 5, \longrightarrow\}$ *dır.*

İspat. S bir Arf pseudo-simetrik nümerik semigrup olsun. İlk olarak $Ap(S, \rho_1) = \{0, \rho_1+(c-1)/2, \rho_1+c-1\}$ olduğunu gösterelim. $\supseteq$ kapsaması açıktır. Ters kapsamayı göstermek için $l \in Ap(S, \rho_1), l \notin \{0, \rho_1 + (c-1)/2, \rho_1 + c - 1\}$ varsayalım. Lemma 2.46 yardımıyla $l \neq \rho_1 + c - 1$, $\rho_1 + c - 1 - l \geq \rho_1$ olduğundan $\rho_1 + c - 1 - l \in S$ dir. Başka bir deyişle, $l \neq 0$ ise o zaman $l \geq \rho_1$ olur. Burada Arf olma koşulundan dolayı $\rho_1 + c - 1 - l + l - \rho_1 = c - 1 \in S$ dir. Bu ise çelişkidir.

Şimdi, $\#Ap(S, \rho_1) = 1$ ise $\rho_1 = 1$ ve $S = \mathbb{N}$ dır. Fakat $\mathbb{N}$ pseudo-simetrik nümerik semigrup değildir.

$\#Ap(S, \rho_1) = 2$ ise Gözlem 2.10'dan $\rho_1 = 2$ dir. Bu durumda, S hipereliptik olmalıdır. Böylece, S pseudo-simetrik nümerik semigrup değildir.

Sonuç olarak, $\#Ap(S, \rho_1) = 3$ olmalıdır. Bu, Gözlem 2.10'dan $\rho_1 = 3$, 1 ve 2 nin boşluk olmasını sağlar. $(c-1)/2 = 1$ ise $c = 3$ olur ve $S = \{0, 3, \longrightarrow\}$'yi verir. Aksi halde, $(c-1)/2 = 2$ ise $c = 5$ olur ve $S = \{0, 3, 5, \longrightarrow\}$'yi verir. Son olarak $1 \neq (c-1)/2$ ve $2 \neq (c-1)/2$ ise S pseudo-simetrik nümerik semigrup olduğundan $c - 1$, $c - 3 \in S$ olur. Bu ise Lemma 2.66 ile çelişir. ■

Önerme 3.3 *Simetrik Arf nümerik semigruplar sadece hipereliptik semigruplardır.*

İspat. Öncelikle her hipereliptik semigrubun Arf nümerik semigrup olduğunu biliyoruz. Tersine, S Arf, $\rho \in S$ ve $\rho < c$ ise $\rho+1 \notin S$ dir. Aksi halde $2(\rho+1)-\rho = \rho+2 \in S$ olur. Benzer şekilde $\rho + 3, \rho + 4, ... \in S$ olduğu görülebilir ve bu $\rho < c$ ile çelişir. Buradan, $[0, c]$ aralığında ardışık iki tamsayının ikisinin birden kutup olamayacağı görülür. Eğer S simetrik ise boşluklar için aynı durum söz konusudur. (Eğer $l, l + 1$ boşluklar ise o zaman $c - l - 2, c - l - 1$ kutuplardır). 0 zaten kutup olduğundan, $[0, c] \cap S = [0, c] \cap 2\mathbb{N}$ elde edilir. Böylece S hipereliptiktir. ■

Örnek 3.4 (1) *Örnek 2.125 de verilen Klein quartik fonksiyon cismini* $K = F_8$ *üzerinden dikkate alalım. Denklemi* x^6 *ile çarpıp* $z = -yx^2$ *dönüşümü yapılırsa,* $x^7 = \frac{z^3}{1-z}$ *elde edilir. Bu durumda* F*'yi* $F_8(z)$*'nin bir genişlemesi olarak düşünebiliriz.* $F_8(z)$ *içinde* $(z) = P_0 - P_\infty$, $(1-z) = P_1 - P_\infty$ *olacaktır.* F *içinde ise cisim genişlemesinden kaynaklanan dallanma indeksi ile çarpılmak durumundadırlar. Bu indeks* P_0, P_1, P_∞ *için* 7 *diğer noktalarda ise* 1 *dir, ayrıca fonksiyon cisminin cinsi* 3 *tür.* F *içinde* P_∞*'un bir genişlemesi* Q_∞ *olsun. Bu durumda,*

$$v_{Q_\infty}(x^7) = v_{Q_\infty}(\frac{z^3}{1-z}) = 3.7.v_{P_\infty}(z) - 7.v_{P_\infty}(1-z) = -2.7$$

diğer yandan $v_{Q_\infty}(x^7) = 7.v_{Q_\infty}(x)$ *olduğundan* $v_{Q_\infty}(x) = -2$ *dir. Benzer şekilde,* $7.v_{P_\infty}(z) = v_{Q_\infty}(z) = v_{Q_\infty}(-yx^2) = 2.v_{Q_\infty}(x) + v_{Q_\infty}(y) = 2.(-2) + v_{Q_\infty}(y)$ *nedeniyle* $v_{Q_\infty}(y) = -3$ *elde edilir. Dolayısıyla,* Q_∞*'daki Weierstrass semigrup* $\{0, 3, 5, 6, 7, 8, 9, ...\}$ *dir.* $c = 5$ *ve* $(c-1)/2$*'den farklı boşluklar sadece* $l = 1$ *ve* $l = 4$ *dir. Her iki durumda da* $c - 1 - l \in S$ *olduğundan bu* S*'nin pseudo-simetrik olduğunu gösterir. Ayrıca* $c = 5$, $d = c' = 3$ *ve* $d' = 0$ *dır. Bu, Tanım 2.54 te verilen tanım yardımıyla adi olmayan akut nümerik semigrup için bir örnektir. Önerme 3.2 yardımıyla* S *bir Arf nümerik semigruptur.*
(2) *Örnek 2.126 de verilen Hermityen fonksiyon cismini alalım. Şimdi,* $P := P_{00}$ *ve* $Q := P_\infty$ *noktalarını alalım. Burada* P_∞ *sonsuzdaki noktayı and* P_{ab} *ise,* $x - a$ *ve* $y - b$ *nin ortak sıfırını göstermektedir. Bu durumda,* x *ve* y*'nin bölenlerinin*

$$(x) = \sum_{b^q + b = 0} P_{0b} - qP_\infty \quad ve \quad (y) = m(P_{00} - P_\infty)$$

ayrıca

$$(x^i y^j) = i \sum_{b^q + b = 0,\ b \neq 0} P_{0b} + (i + jm)P_{00} - (iq + jm)P_\infty$$

olduğu kolayca görülebilir. Hermityen fonksiyon cismi için $L(rP_\infty)$*'un,* $r \geq 0$, *bir tabanı*

$$\{x^i y^j : 0 \leq i\ ,\ 0 \leq j \leq q-1,\ \ iq + j(q+1) \leq r\}$$

dir. Q *noktasındaki Weierstrass semigrup* $S = \langle q, q+1 \rangle$ *dir. Bu durumda,* $q = 3$ *alınırsa Weierstrass semigrup* $\{0, 3, 4, 6, 7, 8, ...\}$, *boşluk sayıları* $\{1, 2, 5\}$ *olur. Benzer şekilde,* $\mathbb{F}_{16}$ *üzerinde* $y^4 + y = x^5$ *denklemi ile belirli Hermityen eğrisi için* Q *daki semigrup*

$$S = \langle 4, 5 \rangle = \{0, 4, 5, 8, 9, 10\} \cup \{i \in \mathbb{N} \mid i \geq 12\}$$

dir. Bu durumda $c = 12$, $d = 10$, $c' = 8$ *ve* $d' = 5$ *olduğundan* S *akuttur. Üstelik,* S *simetrik ve* $\{4, 5\}$ *aralığı ile üretilen nümerik semigruptur.*
(3) *Örnek 2.128 de verilen Suzuki fonksiyon cismini alalım. Her* $a, b \in F_q$ *için* $x - a$ *ve* $y - b$*'nin ortak noktası olan tek türlü belirli bir* $P_{ab} \in P_F$ *noktası vardır. Ek olarak, sonsuzda tek bir* P_∞ *noktası vardır.* F*'nin cinsi* $g = q_0(q-1)$ *dir.* F, $F_q(x)$ *fonksiyon cisminin bir genişlemesi olarak görülebilir ve* $[F : F_q(x)] = q$ *dur.* $Q_a \in P_{F_q(x)}$ *ile* $x - a$*'nın sıfırını* $Q_\infty \in P_{F_q(x)}$ *ile sonsuzdaki noktayı gösterelim ve*

$$x,\ y,\ v := y^{\frac{q}{q_0}} - x^{\frac{q}{q_0}+1},\ w := y^{\frac{q}{q_0}} x^{\frac{q}{q_0^2}-1} + v^{\frac{q}{q_0}}$$

fonsiyonlarını dikkate alalım. Bu durumda

$$(x)_\infty = qP_\infty, (y)_\infty = (q+q_0)P_\infty, (v)_\infty = (q+\frac{q}{q_0})P_\infty, (w)_\infty = (q+\frac{q}{q_0}+1)P_\infty$$

elde edilir. Her $b \in F_q$ *için* P_{0b} *,* Q_0*'ın bir genişlemesi ve* $F/F_q(x)$ *derecesi* q *olan bir genişleme olduğundan,* Q_0 *noktası* F*'de tam olarak parçalanır. Buradan*

$$(x) = \sum_{b\in F_q} P_{0b} - qP_\infty$$

elde ederiz. Böylece, $v_{P_{00}}(y) = v_{Q_0}(y)$ *,* $e(P_{00}|Q_0) = 1$ *dir. Hatta,* $y(y^{q-1}-1) = x^{q_0+1}\prod_{b\in F_q^*}(x-a)$ *ve*

$$v_{Q_0}(y) = (q_0+1)v_{Q_0}(x) + \sum_{b\in F_q^*} v_{Q_0}(x-a) - v_{Q_0}(y^{q-1}-1) = q_0+1$$

dir. Böylece, $v_{P_{00}}(y) = q_0+1$*,* $v_{P_{00}}(v) = \frac{q}{q_0}+1$ *ve* $v_{P_{00}}(w) = (q+\frac{q}{q_0}+1)$ *elde edilir.* w*'nın kutup böleninin derecesi* $(q+\frac{q}{q_0}+1)$ *dir. Bu durumda,* $(w) = (q+\frac{q}{q_0}+1)P_{00} - (q+\frac{q}{q_0}+1)P_\infty$ *dir.* F/F_q *Suzuki fonksiyonlar cismi ve* P*, bir rasyonel noktası olsun.* P *noktasındaki Weierstrass semigrup* $\left\langle q, q+q_0, q+\frac{q}{q_0}, q+\frac{q}{q_0}+1\right\rangle$ *dir.* $q_0 = 2$ *için semigrubun önderi, dominantı, alt önderi ve alt dominantı sırasıyla* $28, 26, 20$ *ve* 18 *olduğundan dolayı akut nümerik semigruptur.* $g = \frac{F(S)+1}{2}$ *olduğundan semigrup simetriktir.*

Örnek 3.5 $g = 2$ *olan hipereliptik fonksiyon cismi olsun. Weierstrass boşluk teoreminden* $1 \le i_j \le 2g-1$ *ve tam* g *tane boşluk sayısı vardır. Burada* $g = 2$ *olduğundan* $1 \le i_j \le 3$ *olur.* 1 *boşluktur. Diğer boşluk ya* 2 *yada* 3 *tür. Sırasıyla Weierstrass semigrup* $\{0, 3, \longrightarrow\}$ *ve* $\{0, 2, 4, \longrightarrow\}$ *olur.*

Tablo 1: Bazı fonsksiyon cisimlerinin semigrupları

	Simetrik	Pseudo-simetrik	Arf	Akut	Aralıkla Üretilen
Hermityen f. c.	x		x	x	x
Hipereliptik f. c.	x		x		
Klein quartik f. c.		x	x	x	
Suzuki f. c.	x			x	
Adi semigrup			x		x
{0,3,...,}		x	x		x
$S_{\{i,\ldots,\frac{(k+1)i-2}{k}\}}$	x				x
{0,3,5,...,}		x	x		

Burada x sembolü fonksiyon cisminin hangi nümerik semigruba dahil olduğunu belirtir.

Örnek 3.6 *$g = 2$ olan hipereliptik fonksiyon cismi olsun. Weierstrass boşluk teoreminden $1 \leq i_j \leq 2g-1$ ve tam g tane boşluk sayısı vardır. Burada $g = 2$ olduğundan $1 \leq i_j \leq 3$ dür ve 1 boşluktur. Diğer boşluk ya 2 ya da 3'tür. Sırasıyla $\{0, 3, \longrightarrow\}$ ve $\{0, 2, 4, \longrightarrow\}$ olur.*

3.2. $\oplus$ İşlemi ve v-Dizisi

S bir nümerik semigrup olsun. Sayfa 3'te ifade edilen $\rho : \mathbb{N} \longrightarrow S$ sayma dönüşümü ve S nümerik semigrubu için $\oplus$ işlemi

$$i \oplus j = \rho^{-1}(\rho_i + \rho_j)$$

ve $v = (v_i)_{i\in\mathbb{N}}$ dizisi $A[\rho_i] := \{\rho_j \in S \mid \rho_i - \rho_j \in S\}$ olmak üzere

$$v_i = \#A[\rho_i]$$

ile tanımlanır.

Örnek 3.7 *$S = \{0, 4, 5, 8, 9, 10, 12, \longrightarrow\}$ nümerik semigrubu için $1 \oplus 1 = \rho^{-1}(\rho_1 + \rho_1) = \rho^{-1}(4+4) = \rho^{-1}(8) = 3$, $3 \oplus 4 = \rho^{-1}(\rho_3 + \rho_4) = \rho^{-1}(8+9) = \rho^{-1}(17) = 11$ dir. $4 \oplus 3 = \rho^{-1}(\rho_4 + \rho_3) = \rho^{-1}(17) = 3 \oplus 4 = 11$ dir. Böyle devam edilirse $\oplus$'nin değişmeli olduğu ve ayrıca $\oplus$'nin, $\mathbb{N}$'nin doğal sıralamasına uyduğu kolayca görülebilir. Yani $a < b$ ise $a \oplus c < b \oplus c$ dir. v dizisi $1, 2, 2, 3, 4, 3, 4, 6, 6, 4, 5, 8, 9, 8, 9, 10, 12, 12, 13, 14, \ldots$ dir.*

Önerme 3.8 *(a) a, b pozitif tamsayılar, S, ρ sayma dönüşümü ile belirli nümerik semigrup, $d \in \mathbb{Z}$ ve $d \geq 2$ olsun. $S' = dS \cup \{i \in \mathbb{N} \mid i \geq d\rho_{a\oplus b}\}$ ile tanımlanmak üzere $\oplus_S$, $\oplus_{S'}$ sırasıyla S, S' ye bağlı $\oplus$ işlemleri olsun. Bu durumda, her $i \leq a$, her $j \leq b$ için $i \oplus_{S'} j = i \oplus_S j$ ve $S' \neq S$ dir.*
(b) k pozitif bir tamsayı ve S, ρ sayma dönüşümü ile belirli nümerik semigrup, $d \in \mathbb{Z}$ ve $d \geq 2$ olsun. $S' = dS \cup \{i \in \mathbb{N} \mid i \geq d\rho_k\}$ ile tanımlanmak üzere v^S, $v^{S'}$ sırasıyla S, S' ne ait v dizisi ise her $i \leq k$ için $v^S = v^{S'}$ ve $S \neq S'$ dir.

İspat. (a) $S' \neq S$ olduğu açıktır. ρ', S' nin sayma dönüşümü olsun. Her $k \leq a \oplus_S b$ için $\rho'_k = d\rho_k$ dır. Özel olarak, $i \leq a$ ve $j \leq b$ ise $\rho'_i = d\rho_i$ ve $\rho'_j = d\rho_j$ olur. Böylece $\rho'_{i\oplus_{S'}j} = \rho'_i + \rho'_j = d\rho_i + d\rho_j = d\rho_{i\oplus_S j}$ olur. Bu $i \oplus_{S'} j = i \oplus_S j$ yi sağlar.
(b) $S \neq S'$ olduğu açıktır. ρ', S' nin sayma dönüşümü olsun. Her $i \leq k$ için $\rho'_i = d\rho_i$ dir. Özel olarak $j \leq i \leq k$ ise $\rho'_i - \rho'_j = d(\rho_i - \rho_j) \in S'$ dır ancak ve ancak $\rho_i - \rho_j \in S$ dir. Buradan $v_i^S = v_i^{S'}$ olur. ■

Gözlem 3.9 *S, g cinsine, c önderine ve ρ sayma dönüşümüne sahip nümerik semigrup olsun. $g(i)$, ρ_i den daha küçük boşlukların sayısı ise o zaman $\rho_i = g(i)+i$ olduğu açıktır. Sonuç olarak*

$$\begin{aligned} \rho_i &= g + i, \text{ her } i \geq \rho^{-1}(c) \text{ ise} \\ \rho_i &< g + i, \text{ her } i < \rho^{-1}(c) \text{ ise} \end{aligned}$$

dir. Özel olarak $\rho^{-1}(c) = c - g$ dir.

Önerme 3.10 *S, c önderine ve ρ sayma dönüşümüne sahip nümerik semigrup olsun.*
(a) Her hangi bir $a \in \mathbb{N}$ ve her $b \in \mathbb{N}$ için

$$\rho_{a+b} \geq \rho_a + b$$

dir. $\rho_a \geq c$ ise eşitlik sağlanır.
(b) Her hangi bir $a, b \in \mathbb{N}$ için $a \oplus b \leq a + \rho_b$ dir. $\rho_a \geq c$ ise eşitlik sağlanır.
(c) S, $\oplus$ işlemi ile tek türlü belirli bir nümerik semigruptur.

İspat. (a) ρ_a ve ρ_{a+b} arasında boşluk olmayacak şekilde bir b elemanı varsa $\rho_{a+b} = \rho_a + b$ dir. Buna karşın ρ_a ve ρ_{a+b} arasında en az bir boşluk olacak şekilde bir b varsa $\rho_{a+b} > \rho_a + b$ dir. $\rho_a \geq c$ ise ρ_a'dan daha büyük bir boşluk olmayacaktır. Böylece her b için $\rho_{a+b} = \rho_a + b$ olur. Tersine $\rho_a < c$ ise $\rho_{a+b} \geq \rho_a + b$ söyleyebiliriz.
(b) $a \oplus b$'nin tanımından $\rho_{a \oplus b} = \rho_a + \rho_b$ ve $\rho_a \geq c$ ise (a) yardımıyla her b için $\rho_a + \rho_b \leq \rho_{a+\rho_b}$ dir. ρ dönüşümü bijektif ve artan olduğundan dolayı, bu $\rho_a \geq c$ ise $a \oplus b \leq a + \rho_b$ anlamına gelir.
(c) S'nin tek türlü belirli olduğunu ρ'nın her $i \in \mathbb{N}$ için $\oplus$ yardımıyla tek türlü belirli olmasından yararlanarak göstereceğiz. Burada, (b) yardımıyla

$$\begin{aligned} i \oplus j &\leq j + \rho_i, \text{ her } j \text{ için} \\ i \oplus j &= j + \rho_i, \ \rho_j \geq c \text{ olacak şekilde her } j \text{ için} \end{aligned}$$

dir. Böylece her i için $maks_j \{(i \oplus j) - j\}$ varlığı $\oplus$ yardımıyla tek türlü belirlidir ve bu kesinlikle ρ_i dir. ■

$v-$dizisi bir nümerik semigrup belirler. Burada, elemanların nasıl belirlendiğini gösterelim.

Önerme 3.11 *S, g cinsine, c önderine ve ρ sayma dönüşümüne sahip nümerik semigrup olsun. $g(i)$, ρ_i den daha küçük boşlukların sayısı olmak üzere*

$$D(i) := \{l \in \mathbb{N} \setminus S \mid \rho_i - l \in \mathbb{N} \setminus S\}$$

olsun. Bu durumda, her $i \in \mathbb{N}$ için

$$v_i = i - g(i) + \#D(i) + 1$$

dir. Özel olarak her $i \geq 2c - g - 1$ için (veya, denk olarak, $\rho_i \geq 2c - 1$ olacak şekilde her i için), $v_i = i - g + 1$ dir.

İspat. (Kırfel ve Pellikaan 1995). ■

Teorem 3.12 *(v_i), S nümerik semigrubuna ait dizi ise aynı (v_i) dizisine sahip başka bir nümerik semigrup yoktur.*

İspat. $S = \mathbb{N}$ ise (v_i) kesin artandır ve (v_i) dizisine sahip başka bir nümerik semigrup yoktur. $S \neq \mathbb{N}$ varsayalım. (v_i) dizisi yardımıyla g cinsi ve c önderi belirlenebilir. $k = 2c - g - 2$ olsun. Aşağıda c ve g bilinmeden k'nın nasıl belirleneceğini göreceğiz. $c \geq 2$ ve bu yüzden $2c - 2 \geq c$ dir. Bu $k = \rho^{-1}(2c-2)$ ve $g(k) = g$ sağlar. Önerme 3.11 yardımıyla $v_k = k - g + \#D(k) + 1$ olur. Ancak $D(k) = \{c-1\}$ dir. Sonuç olarak $v_k = k - g + 2$ olur. Önerme 3.11'dan her $i > k$ için $v_i = i - g + 1$ dir. Bu yüzden

$$k = maks\ \{i \mid v_i = v_{i+1}\}$$

dir. Cinsi

$$g = k + 2 - v_k$$

olarak, önderi

$$c = \frac{k + g + 2}{2}$$

şeklinde belirleyebiliriz.

$\{0\} \in S$ ve $\{i \in \mathbb{N} \mid i \geq c\} \subseteq S$ olduğu biliniyor. Üstelik , $\{1, c-1\} \subseteq \mathbb{N} \setminus S$ dir. Bu durumda, her $i \in \{2, \ldots, c-2\}$ için $i \in S$ olup olmadığını belirlemek kalır. $i \in \{2, \ldots, c-2\}$ varsayalım. $c - 1 + i - g > c - g$ ve buradan $\rho_{c-1+i-g} > c$ dir. Bu $g(c - 1 + i - g) = g$ anlamına gelir. Sonuç olarak

$$v_{c-1+i-g} = c - 1 + i - g - g + \#D(c - 1 + i - g) + 1$$

dir. Başka bir deyişle, eğer

$$\tilde{D}(i) := \{l \in \mathbb{N} \setminus S \mid c - 1 + i - l \in \mathbb{N} \setminus S,\ i < l < c - 1\}$$

şeklinde tanımlanırsa

$$D(c - 1 + i - g) = \begin{cases} \tilde{D}(i) \cup \{c-1, i\}, & i \in \mathbb{N} \setminus S \text{ ise} \\ \tilde{D}(i), & \text{aksi halde} \end{cases}$$

olur. Son iki eşitlikten

$$i \text{ boşluk değildir } \iff v_{c-1+i-g} = c + i - 2g + \#\tilde{D}(i)$$

olur. Bu tümevarımsal olarak $i = c - 2$ den $i = 2$ ye kadar azalan i'nin S'ye ait olup olmadığını verir. ■

Teorem 3.13 *S, c önderine, c' alt önderine, d dominantına ve ρ sayma dönüşümüne sahip adi olmayan akut nümerik semigrup olmak üzere*

$$m = \min\ \{\rho^{-1}(c + c' - 2), \rho^{-1}(2d)\}$$

olsun. Bu durumda,
(a) $v_m > v_{m+1}$ dir.
(b) Her $i > m$ için $v_i \leq v_{i+1}$ dir.

İspat. (Amoros 2004). ■

Sonuç 3.14 *S, c önderine, c' alt önderine ve ρ sayma dönüşümüne sahip adi olmayan akut nümerik semigrup olsun. $m = \min\{\rho^{-1}(c+c'-2), \rho^{-1}(2d)\}$ olmak üzere m tamsayısı, her $i \geq m$ için $\min\{v_j \mid \rho_j \in S,\ \rho_j \geq \rho_{i+1}\} = v_{i+1}$ olacak şekilde en küçük tamsayıdır.*

Örnek 3.15 *Klein quartik'in P_0 noktasındaki Weierstrass semigrubu Örnek 3.4'de verilmişti. S nümerik semigrubunun önderi 5, alt önderi 3 ve dominantı 3 tür. O halde, $\rho^{-1}(c+c'-2) = \rho^{-1}(2d) = 3$ ve böylece $m = \min\{\rho^{-1}(c+c'-2), \rho^{-1}(2d)\} = 3$ tür. $v_3 > v_4$ ve her $i > 3$ için $v_i \leq v_{i+1}$ olduğundan Teorem 3.13 sağlanmış olur. Ayrıca $\min\{v_j \mid \rho_j \in S,\ \rho_j \geq \rho_3\} \neq v_3$ iken her $i > 3$ için $\min\{v_j \mid \rho_j \in S,\ \rho_j \geq \rho_{i+1}\} = v_{i+1}$ dir.*

Önerme 3.16 *S, c önderine, c' alt önderine ve d dominantına sahip adi olmayan nümerik semigrup olsun.*
(a) S simetrik ise $\min\{c+c'-2, 2d\} = c+c'-2 = 2c-2-\rho_1$ dir.
(b) S pseudo-simetrik ise $\min\{c+c'-2, 2d\} = c+c'-2$ dir.
(c) S Arf ise $\min\{c+c'-2, 2d\} = 2d$ dir.
(d) S aralıkla üretilen nümerik semigrup ise $\min\{c+c'-2, 2d\} = c+c'-2$ dir.

İspat. *(a)* S simetrik ise $d = c-2$ olduğu Önerme 2.60'ın ispatında gösterilmişti. Böylece, $c' \leq d$ olduğundan $c+c'-2 = d+c' \leq 2d$ dir. Üstelik, $c-1 = F(S)$ alırsak Önerme 2.35 (a)'dan negatif olmayan herhangi x tamsayısı için $c-1-x \in S$ dir. $c'-1 = c-1-\rho_1$ olur ve böylece $c' = c-\rho_1$ dır. Sonuç olarak, $c+c'-2 = 2c-2-\rho_1$ dir.
(b) S adi olmayan pseudo-simetrik ise $1 \neq c-1/2$ boşluk olduğundan $d = c-2$ dir. Böylece, $c+c'-2 = d+c' \leq 2d$ olur.
(c) S Arf ise $c' = d$ dir. Şöyle ki, $c' < d$ ise $d-1 \in S$ ve S Arf olduğundan $d+1 = 2d-(d-1) \in S$ dir. Bu ise bir çelişkidir. O halde, $d \leq c-2$ olduğundan $2d \leq c+c'-2$ olur.
(d) S, $\{i, i+1, \ldots, j\}$ tarafından üretilen nümerik semigrup olsun. Lemma 2.50'den $c = ki$ ve $d = (k-1)j$ olacak şekilde k tamsayısı vardır. $c-d \leq j-i$ dir, aksi halde $(k+1)i-kj = c-d-(j-i) > 0$ olduğundan $kj+1$, c'den daha büyük boşluk olmalıdır. Diğer taraftan, $d-c' \geq j-i$ ve böylece $2d-(c+c'-2) = d-c+d-c'+2 \geq i-j+j-i+2 \geq 2$ dir. ■

Örnek 3.17 *Örnek 3.4'de verilen Hermityen eğrisi için önder 12, dominant 10 ve alt önder 8 dir. Teorem 3.13 ve Önerme 3.16 yardımıyla $\rho^{-1}(c+c'-2) = 12$ sayısı, $v_m > v_{m+1}$ olacak şekilde en büyük m tamsayısıdır. Böylece, her $i \geq m$ için $\min\{v_j \mid \rho_j \in S,\ \rho_j \geq \rho_{i+1}\} = v_{i+1}$ olacak şekilde en küçük tamsayıdır. Önerme 3.16'dan $c+c'-2 = 2c-2-\rho_1$ dir.*

S bir nümerik semigrup ve $v = (v_i)$, $v-$dizisini olmak üzere her $i \in \mathbb{N}$ için v-dizisi ve $\oplus$ işlemi arasındaki bağıntı

$$v_i = \#\{(j,k) \in \mathbb{N}^2 \mid j \oplus k = i\}$$

şeklindedir. v_i'yi hesaplamak için $\{j \oplus k \mid 0 \leq j, k \leq i\}$'ye bakmak yeterlidir. Sonuç olarak herhangi bir semigrup, onun $\oplus$ işlemiyle tamamen belirlenebilir. Başka bir deyişle Önerme 3.8 (a) ve (b)'nin bir sonucudur.

Önerme 3.18 *S bir nümerik semigrup olsun.*
(a) S, ρ sayma dönüşümüne sahip adi nümerik semigrup ise

$$v_i = \begin{cases} 1, & i = 0 \\ 2, & 1 \leq i \leq \rho_1 \\ i - \rho_1 + 2, & i > \rho_1 \end{cases}$$

olur.
(b) S nümerik semigrubu için (v_i) dizisi azalmayan ise S Arftir.

İspat. *(a)* $v_0 = 1$ ve $0 < \rho_i < 2\rho_1$ olduğu durumda $v_i = 2$ olduğu açıktır. O halde, $2\rho_1 = \rho_{\rho_1+1}$ olduğundan her $1 \leq i \leq \rho_1$ için $v_i = 2$ dir. Son olarak, $\rho_i \geq 2\rho_1$ ise ρ_i'nin yanısıra $\rho_i - \rho_1$'den büyük boşluk olmayan tüm elemanlar $A[\rho_i]$'ye aittir ve geriye kalan boşluk olmayan elemanlardan hiç birisi $A[\rho_i]$'ye ait değildir. S'nin cinsi g ise $v_i = \rho_i - \rho_1 + 2 - g$ ve $\rho_i = i + g$ dir. Böylece, $v_i = i - \rho_1 + 2$ dir.
(b) ρ, S'nin sayma dönüşümü olsun. Tümevarım yöntemi uygulayarak ispat yapalım. Herhangi negatif olmayan i tamsayısı için

(1) $A[\rho_{\rho^{-1}(2\rho_i)}] = \{j \in \mathbb{N} \mid j \leq i\} \sqcup \{\rho^{-1}(2\rho_i - \rho_j) \mid 0 \leq j < i\}$, burada $\sqcup$, ayrık kümelerin birleşimini göstermektedir.

(2) $A[\rho_{\rho^{-1}(\rho_i+\rho_{i+1})}] = \{j \in \mathbb{N} \mid j \leq i\} \sqcup \{\rho^{-1}(\rho_i + \rho_{i+1} - \rho_j) \mid 0 \leq j \leq i\}$

Eğer (1), her i için sağlanıyor ise $\{j \in \mathbb{N} \mid j \leq i\} \subseteq A[\rho_{\rho^{-1}(2\rho_i)}]$ olduğuna dikkat edelim. Bu durumda, Önerme 2.67'dan S Arftir. $i = 0$ durumunda (1) ve (2)'nin sağlandığı açıktır. $i > 0$ varsayalım. Tümevarım hipotezi yardımıyla, $v_{\rho^{-1}(\rho_{i-1}+\rho_i)} = 2i$ dir. Şimdi, (v_i) azalmayan bir dizi ve $2\rho_i > \rho_{i-1} + \rho_i$ olduğundan $v_{\rho^{-1}(2\rho_i)} \geq 2i$ dir. Diğer taraftan, $j, k \in \mathbb{N}$ için $j \leq k$ ve $\rho_j + \rho_k = 2\rho_i$ ise $\rho_j \leq \rho_i$ ve $\rho_k \geq \rho_i$ dir. Bu durumda,

$$\rho(A[\rho_{\rho^{-1}(2\rho_i)}]) \subseteq \{\rho_j \mid 0 \leq j \leq i\} \sqcup \{2\rho_i - \rho_j \mid 0 \leq j < i\}$$

olur. Böylece $v_{\rho^{-1}(2\rho_i)} \geq 2i$ olması için gerek ve yeter koşul

$$A[\rho_{\rho^{-1}(2\rho_i)}] = \{j \in \mathbb{N} \mid j \leq i\} \sqcup \{\rho^{-1}(2\rho_i - \rho_j) \mid 0 \leq j < i\}$$

olmasıdır. Bu (1)'i ispatlar. Son olarak, (1), $v_{\rho^{-1}(2\rho_i)} = 2i + 1$ olmasını gerektirir ve benzer şekilde (2) elde edilir. ■

Önermenin bir sonucu olarak, S adi nümerik semigrup ise (v_i) dizisi azalmayandır.

Teorem 3.19 *(a) (v_i) dizisi azalmayan tek nümerik semigrup adi nümerik semigruplardır.*
(b) (v_i) dizisi kesin artan olacak şekilde tek nümerik semigrup $\mathbb{N}$ dir.

İspat. *(a)* Önerme 3.18 (a) ve (b), Önerme 2.60, Önerme 2.81, Teorem 3.13'nin bir sonucu olarak elde edilir.
(b) (a) ve Önerme 3.18 (a)'nın bir sonucudur. ■

3.3. Cebirsel Geometrik Kodlar ve Arf Nümerik Semigruplarla İlişkisi

$\mathbb{F}_q$ sonlu bir cisim ve $F,\ \mathbb{F}_q$ üzerinde bir fonksiyon cismi olsun. Bir rasyonel Q noktası alalım ve $K_\infty(Q)$, Q dışında kutbu olmayan fonksiyonların kümesi (halkası) olsun.

$$S = S(Q) = \{-\upsilon_Q(f) \mid f \in K_\infty(Q)\} = \{\rho_1 = 0 < \rho_2 < \cdots\}$$

şeklinde ifade edilir. $\upsilon_Q(1) = 0$ ve her $f, g \in K_\infty(Q)$ için $\upsilon_Q(f.g) = \upsilon_Q(f) + \upsilon_Q(g)$ olduğundan $S = S(Q)$, Q da Weierstrass semigrubudur, burada S'nin önderi $c = \rho_r$ ile gösterilecektir. Bir m pozitif tamsayısı için, $\mathcal{L}(mQ) = \{f \in K_\infty(Q) \mid \upsilon_Q(f) \geq -m\}$ dir. F de $Q \notin \mathcal{P}$ olacak şekilde n faklı rasyonel noktanın kümesi $\mathcal{P} = \{P_1, \ldots, P_n\}$ olmak üzere $D = \sum_{i=1}^{n} P_i$ olsun.

$$ev_{\mathcal{P}} : \begin{cases} K_\infty(Q) \longrightarrow \mathbb{F}_q^n \\ f \longmapsto (f(P_1), \ldots, f(P_n)) \end{cases}$$

değerlendirme dönüşümünü alalım. Bir noktalı cebirsel geometrik kod $C_\Omega(D, \rho_l Q) = ev_{\mathcal{P}}(L(\rho_l Q))^\perp$ dir. Burada kısaca C_l diyeceğiz. $i = 1, 2, \cdots$ için $-\upsilon_Q(h_i) = \rho_i$ olacak şekilde $h_i \in K_\infty(Q)$ fonksiyonu seçilebilir. C_l'yi, $\mathbf{h}_j = ev_{\mathcal{P}}(h_j)$ olacak şekilde $\mathbf{h}_1, \ldots, \mathbf{h}_l$ parite kontrol sistemine göre tanımlayabiliriz.

$$C_l = \{\mathbf{c} \in \mathbb{F}_q^n \mid \mathbf{c}.\mathbf{h}_i = 0,\ \text{her } i = 1, .., l\}$$

C_l nin parametreleri şöyledir: uzunluğunun n olduğu açıktır. Ayrıca $\rho_l < n$ ise boyut en az $n - l$ dir. $\rho_l \geq n$ olduğu durumlarda ise, $\mathbf{h}_1, \ldots, \mathbf{h}_l$'nin bazıları bağımlı olabilir ve boyutun tam olarak değeri Teorem 2.108 (b) yardımıyla hesaplanabilir. $d(C_l)$, C_l kodunun minimum uzaklığını göstermek üzere, genel olarak $d(C_l)$ üzerinde alt sınır, $d(C_l) \geq d_G(l) := l + 1 - g$ olacak şekilde Goppa sınırı (Goppa atanmış minimum uzaklığı) ile verilir, (Hoholdt 1998).

Tanım 3.20 *$\rho_i \in S$ kutbu için $A[\rho_i] = \{p \in S \mid \rho_i - p \in S\}$ kümesini ele alalım. Bu durumda,*

$$d_{ORD}(l) = \min\ \{\#A[\rho_i] \mid \rho_i \in S,\ \rho_i \geq \rho_{l+1}\}$$

tamsayısına C_l'nin minimum uzaklığı üzerinde mertebe sınırı(veya Feng-Rao sınırı) denir.

Teorem 3.21 *$d_G(l) \leq d_{ORD}(l) \leq d(C_l)$ dir.*

İspat. (Hoholdt 1998). ■

Mertebe sınırının önemli özelliği sadece S'nin elemanları yardımıyla (yani, ne F ne de P ile ilişkisiz olarak) hesaplanabilir olmasıdır. Burada $d_{ORD}(l)$ minimum uzaklık üzerinde daha iyi bir sınırdır. Cebirsel geometrik kodların Feng-Rao tarafından tanımlanan bir genelleştirmesi aşağıdaki şekilde verilebilir.

Tanım 3.22 *Bir pozitif d tamsayısı için*

$$R_d = \{i \mid \#A[\rho_i] = v_i < d\}$$

olsun. R_d, $\{\rho \in S \mid \#A[\rho] < d\}$ ile denktir. Genelleştirilmiş geometrik Goppa kod

$$\check{C}(d) = \{\mathbf{c} \in \mathbb{F}_q^n \mid \mathbf{c}.\mathbf{h}_i = 0,\ her\ i \in R_d\}$$

ile tanımlanır.

$\check{C}(d)$'nin parametreleri şöyledir: $\check{C}(d)$'nin minimum uzaklığı en az d dir. Ayrıca, eğer $d = d_{ORD}(l)$ ise $C_l \subseteq \check{C}(d)$ dır. Dolayısıyla $\check{C}(d)$'nin boyutu en az C_l'nin boyutu kadardır. Tanımdan *boy* $\check{C}(d) \geq n - \#R_d$ dir. $c = \rho_r$, S'nin önderi olmak üzere, $2c \leq n$ ve $1 \leq d \leq 2r-2$ ise tüm $\mathbf{h}_i$'ler doğrusal bağımsızdır ve *boy* $\check{C}(d) = n - \#R_d$ dir. Böylece kodun bilinmeyen parametrelerini yine S'nin elemanları yardımıyla elde edebiliriz.

$C_\Omega(D, \rho_l Q)$ bir noktalı cebirsel geometrik kod ve S, Q noktasındaki Weierstrass semigrup olsun. Daha önce $C_\Omega(D, \rho_l Q)$'nın minimum uzaklığı üzerinde mertebe sınırının nasıl hesaplanacağını gösterilmişti. Bu hesaplamalar sadece S semigrubuyla alakalıdır. Daha fazlası v-dizisi kavramını gerektirir. Bu, çoğu semigruplar için genel olarak zordur. Arf nümerik semigruplar için $A[\rho]$'nın kardinalitesini hesaplamak daha kolay olacaktır. Burada $S \neq \mathbb{N}$ kabul edeceğiz.

$\rho \in S$ için $\{\rho_1, \ldots, \rho_j\} \subseteq A[\rho]$ olacak şekilde maximum j olsun. Bu durumda,

$$A[\rho] = \{\rho_1, \ldots, \rho_j, \rho - \rho_1, \ldots, \rho - \rho_j\}$$

olur. Çünkü $\{\rho_1, \ldots, \rho_j, \rho-\rho_1, \ldots, \rho-\rho_j\} \subseteq A[\rho]$ açıktır. Tersine, $k > j$ için $\rho_k \in A[\rho]$ ise $i \leq j$ olmak üzere $\rho - \rho_k = \rho_i$ olur. Aksi halde $\rho - \rho_{j+1} = \rho_i + \rho_k - \rho_{j+1} \in S$ olduğundan j'nin seçimiyle çelişir. Ama yine de $\{\rho_1, \ldots, \rho_j, \rho-\rho_1, \ldots, \rho-\rho_j\}$ kümesi birçok tekrarlayan elemanı içerebileceğinden $\#A[\rho] = 2j$ sağlanmayabilir. Buradan $\rho \in S$ için

$$\begin{aligned} \alpha(\rho) &= maks\ \{j \mid \rho_1, \ldots, \rho_j \in A[\rho]\} \\ \beta(\rho) &= maks\ \{j \mid \rho_1, \ldots, \rho_j \in A[\rho],\ \rho_j \leq \rho - \rho_j\} \\ &= maks\ \{j \mid \rho_j \in A[\rho],\ 2\rho_j \leq \rho\} \end{aligned}$$

tanımlayalım. Bu durumda, $\alpha(\rho) \geq \beta(\rho)$, $A[\rho] = \{\rho_1, \ldots, \rho_{\beta(\rho)}, \rho-\rho_1, \ldots, \rho-\rho_{\beta(\rho)}\}$ ve

$$\#A[\rho] = \begin{cases} 2\beta(\rho) - 1, & 2\rho_{\beta(\rho)=}\rho \text{ ise} \\ 2\beta(\rho)\ , & 2\rho_{\beta(\rho)\neq}\rho \text{ ise} \end{cases}$$

elde edilir.

Özellikle $\#A[\rho]$'nın tek olması için gerekli ve yeterli koşul $\rho \in 2S$ olmasıdır. Şimdi $\alpha(\rho)$ ve $\beta(\rho)$ sayıları hakkında ne söyleyebileceğimizi göreceğiz. İlk olarak $\#A[\rho]$'nın tek olduğu durumu ele alalım.

Önerme 3.23 *S Arf ise her $\rho_i \in S$ için $\beta(2\rho_i) = i$ dir. Sonuç olarak $\#A[2\rho_i] = 2i - 1$ dir.*

İspat. S Arf ise her $k \leq i$ için $2\rho_i - \rho_k \in S$ ve $\{\rho_1, \ldots, \rho_i\} \subseteq A[2\rho_i]$ olur. $\beta(2\rho_i) > i$ ise $\rho_j + \rho_k = 2\rho_i$ olacak şekilde $j, k > i$ vardır. Bu ise imkansızdır. ■

$\rho \in S \setminus 2S$ kutupları için, $\beta(\rho)$ hakkında genel olarak açık bir ifade veremeyiz. Ama yine de amacımız için yeterli olacak bazı sınırlamalar verebiliriz.

Bir i pozitif tamsayısı için $p_i = c + \rho_{i+1} - 1$ olsun. Her i için $p_i \geq c$ olduğundan p_i bir kutup sayısıdır. Daha fazlası, $p_i = \rho_r + \rho_{i+1} - 1 = \rho_{r+\rho_{i+1}-1}$ dir. Özellikle, $i \geq r-1$ için $t \geq 0$ olmak üzere $i = (r-1)+t$ yazılabilir. Buradan $\rho_{i+1} = \rho_{r+t} = c+t$ ve sonuç olarak $p_i = 2c + t - 1 = \rho_{c+i}$ dir.

Önerme 3.24 *(a) S bir nümerik semigrup olsun. Eğer $\rho \in S$ ve $\rho > p_{i-1}$ ise $\{\rho_1, \ldots, \rho_i\} \subseteq A[\rho]$ olur. Üstelik $i < r$ ise $\#A[\rho] \geq 2i$ dir.*
(b) S Arf nümerik semigrup ise $\alpha(p_i) = i$ olur. Üstelik, $i < r$ ise $\beta(p_i) = i$ ve $\#A[p_i] = 2i$ dir.

İspat. *(a)* $\rho > p_{i-1}$ ise $j = 1, \ldots, i$ için $\rho - \rho_j \geq c + \rho_i - \rho_j \geq c$ olur. Böylece $\rho - \rho_j \in S$ ve $\rho_j \in A[\rho]$ olur. Buradan $\{\rho_1, \ldots, \rho_i, \rho - \rho_1, \ldots, \rho - \rho_i\} \subseteq A[\rho]$ dir. $i < r$ ise $\rho_i < c$ olur. Böylece $2\rho_i \leq p_{i-1} < \rho$ ve $\rho_i < \rho - \rho_i$ dir. Sonuç olarak $\{\rho_1, \ldots, \rho_i, \rho - \rho_1, \ldots, \rho - \rho_i\}$ kümesindeki her eleman farklıdır.
(b) $p_i - \rho_{i+1} = c - 1 \notin S$ olduğundan $\rho_{i+1} \notin A[p_i]$ ve $\alpha(p_i) \leq i$ dir. S Arf ise $\rho > p_{i-1}$ olmak koşuluyla (a), $\alpha(\rho) \geq i$ anlamına gelir ve $i < r$ ise $\beta(p_i) \geq i$ dir. Buradan hareketle $i < r$ için $2\rho_i \leq p_i$'nin bir sonucu olarak istenen elde edilir. ■

Daha önce söylediklerimizden yola çıkarak $i \geq r-1$ olduğu durumda (p_i) dizisini gözden geçirirsek tüm kutuplar $\rho \geq p_{r-1} = 2c - 1$ dir, yani, $j \geq c + r - 1$ için $\rho_j = p_{j-c}$ dir. $\alpha(p_{j-c}) = j - c$ olduğundan

$$A[\rho_j] = \{\rho_1, \ldots, \rho_{j-c}, \rho_j - \rho_1, \ldots, \rho_j - \rho_{j-c}\}$$

elde edilir. Eğer $j \geq c+r$ ise $\rho_j - \rho_s > \rho_{j-c}$ olması için gerek ve yeter koşul $s \leq r-1$ olmasıdır. Ayrıca tekrarlamayan elemanların oluşturduğu

$$A[\rho_j] = \{\rho_1, \ldots, \rho_{j-c}, \rho_j - \rho_1, \ldots, \rho_j - \rho_{r-1}\}$$

elde edilir.

Önerme 3.25 *(a) $j \geq c + r$ için $\#A[\rho_j] = j - g$ dir.*
(b) $j < c + r$ ise $\beta(\rho_j) \leq r - 1$ ve $\#A[\rho_j] \leq 2r - 2 < \#A[\rho_{c+r}]$ dir.
(c) $\rho_{r-1} + r \leq j < c + r$ ise $\beta(\rho_j) = r - 1$ dir.

İspat. *(a)* Tanımdan hareketle gösterilebilir.
(b) $\beta(\rho_j) \leq r - 1$ göstermek yeterlidir. Aksi halde bazı $j < c + r$ için $\beta(\rho_j) \geq r$ ise $2\rho_r \leq \rho_j \leq \rho_{c+r-1}$ elde edilir. Fakat bu $2c \leq 2c - 1$ olmasına neden olur.
(c) $\rho_{r-1} + r \leq j$ ise $p_{r-2} < \rho_j$ olur. S Arf ise $\rho > p_{i-1}$ olmak koşuluyla $\alpha(\rho) \geq i$ ve $i < r$ ise $\beta(p_i) \geq i$ olduğu verilmişti. Bunun ve (b)'nin sonucu olarak istenen elde edilir. ■

Önerme (a)'nın özel bir durumu olarak $\#A[\rho_{c+r}] = c + r - g = 2r - 1$ dir. Bu sayı $j \leq c + r$ olduğu zaman $\#A[\rho_j]$'nın kardinalitesi üstten sınırlıdır.

Teorem 3.26 *S, cinsi g olan Arf nümerik semigrup ve $c = \rho_r$, S'nin önderi olsun. $i = 1, \ldots, r-1$ için $l_i = r + \rho_{i+1} - 2$ ve ek olarak $l_0 = 0$ olsun. O zaman, herhangi bir l pozitif tamsayısı için,*
(a) $l_{i-1} < l \leq l_i \leq l_{r-1}$ ise $d_{ORD}(l) = 2i$
(b) $c + r - 2 = l_{r-1} \leq l$ ise $d_{ORD}(l) = d_G(l) = l + 1 - g$ dir.

İspat. $l_{r-1} = c + r - 2$ olduğundan Önerme 3.25 den (b) açıktır. (a)'yı ispatlamak için, öncelikle $i = 1, \ldots, r-1$ için $p_i = \rho_{r+\rho_{i+1}-1} = \rho_{l_i+1}$ olduğunu dikkate alalım. Buradan, eğer $l_{i-1} < l \leq l_i$ ise $p_{i-1} < \rho_{l+1} \leq p_i$ elde edilmiş olur. Böylece Önerme 3.24 ve Önerme 3.25 (b)'ye göre

$$d_{ORD}(l) = \min \{\#A[\rho] \mid \rho \geq \rho_{l+1}\} = \#A[p_i] = 2i$$

elde edilmiş olur ve ispat tamamlanır. ■

3.4. Genelleştirilmiş Kodların Tekrar Oranı

Her S semigrubu için $d \geq 2r-1$ ise $\#R_d = d + g - 1$ ve $\#R_{2r-2} = \rho_{r-1} + r - 1$ dir. $d \geq 2r-2$ olmak şartıyla $\#R_d = \rho_{\lceil \frac{d}{2} \rceil} + \lfloor \frac{d}{2} \rfloor$ olarak yazılabilir, (Kırfel ve Pellikaan 1995, Hoholdt 1998).

Tanım 3.27 *Her $d > 1$ için $\#R_d = \rho_{\lceil \frac{d}{2} \rceil} + \lfloor \frac{d}{2} \rfloor$ formülünü sağlayan semigrup durağan (stable) olarak adlandırılır.*

Durağan semigrubun karakterizasyonu hala açık bir problemdir. Bu bölümde durağan semigrupların Arf nümerik semigrup olduğunu ispatlayacağız. Bunu göstermek için bazı notasyonlar tanımlayalım. d pozitif tamsayısı için

$$S_d := \{\rho \in S \mid \#A[\rho] = d\}$$

olsun. Böylece $\#R_{d+1} = \#R_d + \#S_d$ dır. Durağan semigrupları karakterize etmek için $1 \leq d \leq 2r-3$ aralığındaki d değerlerini incelemek yeterlidir. O zaman bir S semigrubun durağan olması için gerek ve yeter koşul $1 \leq d \leq 2r-3$ aralığındaki her d tek tamsayısı, $d = 2t+1$ olmak üzere

$$\begin{aligned} \#S_d &= 1 \\ \#R_d &= \rho_{t+1} + t \end{aligned}$$

olmasıdır.

Lemma 3.28 *S bir semigrup ve $\rho \in S$ olsun. O halde $\#A[\rho]$ tektir ancak ve ancak $\rho \in 2S$ dir. Bu durumda, $\rho = 2\rho_i$ ise $\#A[\rho] \leq 2i - 1$ dır.*

İspat. Her $p \in A[\rho]$ için $p' = \rho - p \in A[\rho]$ dir. Böylece, $p = p' = \rho - p$ olacak şekilde $p \in A[\rho]$ kutbuna sahip değilse $\#A[\rho]$ çifttir, yani, $\rho \in 2S$ dir. Bu durumda, $\rho = 2\rho_i$ ise $p + p' = \rho = 2\rho_i$ ile birlikte her $p, p' \in A[\rho]$ için ya $p \leq \rho_i$ yada $p' \leq \rho_i$ dir, böylece $\#A[\rho] \leq 2i - 1$ olur. ■

Önerme 3.29 *S bir semigrup olsun. Aşağıdaki koşullar denktir:*
(a) Her $\rho_i \in S$ *için* $\#A[2\rho_i] = 2i - 1$*dir.*
(b) Her tek d *için* $\#S_d = 1$ *dir.*
(c) S Arf'tir.

İspat. Lemma 3.28'e göre her tek d tamsayısı için, $\#S_d = 1$ olması için gerek ve yeter koşul her ρ_i için $\#A[2\rho_i] = 2i - 1$ dir. Bunun olması için gerek ve yeter koşul

$$A[2\rho_i] = \{\rho_1, \ldots, \rho_i, 2\rho_i - \rho_1, \ldots, 2\rho_i - \rho_i\}$$

olmasıdır, yani, $i \geq j$ olacak şekilde her i, j için $2\rho_i - \rho_j \in S$ dır. Önerme 2.67'e göre, bu S'nin Arf olmasına denktir. ■

Sonuç olarak, her durağan semigrup Arftir. Tersine, Arf nümerik semigrupların durağan olduğunu ispatlayalım. Burada, $1 \leq d \leq 2r - 3$ aralığındaki her d tek tamsayısı için gerçeklendiğini göstermek yeterlidir. $d = 2t+1$ ise o zaman $\#R_d = \rho_{t+1}+t$ olur.

Lemma 3.30 *S bir Arf nümerik semigrup ve d,* $1 \leq d \leq 2r - 3$ *aralığındaki tek tamsayılar olsun.* $p_i = c + \rho_{i+1} - 1$ *olmak üzere*
(a) $R_d \subseteq [0, p_t] \cap S$ *dir.*
(b) $\{\rho \in [0, p_t] \cap S \mid \beta(\rho) \geq t + 1\} = \{\rho_{t+1} + \rho_{t+1}, \ldots, \rho_{t+1} + \rho_{r-1}\}$ *dir.*

İspat. *(a)* $\#A[\rho] < d \leq 2r - 3$ ise Önerme 3.25 (b), $\rho \leq p_{r-1}$ olmasını gerektirir. Böylece Önerme 3.24 (a)'dan istenen sonuç elde edilir.
(b) $\alpha(\rho) \geq t + 1$ olacak şekilde $\rho \in [0, p_t] \cap S$ ise o halde bazı i'ler için $\rho = \rho_{t+1} + \rho_i$ olur. $2\rho_{t+1} \leq \rho$ olduğundan $i \geq t + 1$ sağlanır. Başka bir deyişle, $\rho \in [0, p_t]$ ve $\beta(p_t) = t$ olduğu için $\rho < \rho_t$ ve $i \leq r - 1$ dir. $\{\rho \in [0, p_t] \cap S \mid \beta(\rho) \geq t + 1\} \subseteq \{\rho_{t+1} + \rho_{t+1}, \ldots, \rho_{t+1} + \rho_{r-1}\}$ olur. Tersinin varlığı açıktır. ■

$\rho \in [0, p_t] \cap S$ olmak üzere $\rho \in R_d$ olması için gerek ve yeter koşul $\beta(\rho) \leq t$ olmasıdır.

Teorem 3.31 *S bir semigrup olsun. Aşağıdaki ifadeler denktir:*
(a) S Arftir.
(b) Her pozitif d tamsayısı için $\#R_d = \rho_{\lceil \frac{d}{2} \rceil} + \lfloor \frac{d}{2} \rfloor$ *dir.*

İspat. Eğer *(b)* sağlanır ise her d tek tamsayısı için $\#S_d = 1$ ve Önerme 3.29'dan dolayı S Arf semigrup olduğu açıktır. Tersine, S Arf ve $1 \leq d \leq 2r - 3$ aralığındaki bir d tek tamsayısı olsun. Önerme 3.29'dan $\#S_d = 1$ dir. $d = 2t + 1$ yazarsak o zaman Lemma 3.30 (b)'ye göre

$$\#R_d = \#([0, p_t] \cap S) - \#\{\rho_{t+1} + \rho_{t+1}, \ldots, \rho_{t+1} + \rho_{r-1}\}$$

olur. $p_t = \rho_r + \rho_{t+1} - 1 = \rho_{r+\rho_{t+1}-1}$ olduğundan $\#([0, p_t] \cap S) = r + \rho_{t+1} - 1$ elde edilir. Böylece, $\#R_d = (r + \rho_{t+1} - 1) - (r - t - 1) = \rho_{t+1} + t$ olur ve S, *(b)*'yi sağlar. ■

Şimdi C_l ve $\check{C}(d)$ kodlarının boyutlarını karşılaştıralım.

Önerme 3.32 *S Arf nümerik semigrup olsun. Pozitif bir l tamsayısı için $d = d_{ORD}(l)$ olduğunda C_l ve $\check{C}(d)$ kodlarını ele alalım. $l_0, \ldots, l_{r-1}$ Teorem 3.26 daki gibi olsun.*
(a) $i \leq r-1$ ve $2c \leq n$ ile $l_{i-1} < l \leq l_i$ ise boy $\check{C}(d)$ − boy $C_l = l - \rho_i - i$ dir.
(b) $l > l_{r-1} = c + r - 2$ ise $\check{C}(d) = C_l$ dir.

İspat. $2c \leq n$ ise $\check{C}(d)$ ve C_l içindeki tüm $\mathbf{h}_i$ kontrolleri lineer bağımsızdır. Böylece boy $C_l = n - l$, boy $\check{C}(d) = n - \#R_d$ ve boy $\check{C}(d)$ − boy $C_l = l - \#R_d$ olur. Şimdi, $l_{i-1} < l \leq l_i$ ise $d = 2i$ ve $\#R_d = \rho_i + i$ olduğundan $l - \#R_d = l - \rho_i - i$ dir. Bu (a)'yı ispatlar. $l \geq c + r - 1$ ise Teorem 3.26'ya göre $d = l + 1 - g \geq 2r - 1$ dir. Buradan $\#R_d = d + 1 - g = l$ olur, sonuç olarak $R_d = \{\rho_1, \ldots, \rho_l\}$ ve $\check{C}(d) = C_l$ dir. ■

4. KAYNAKLAR

AMOROS, M. B. June 2004. Acute semigroups. the Order Bound on The Minimum Distance, and the Feng-Rao Improvements. IEEE Transactions On Information Theory, 50: (6).

AMOROS, M. B. 2005. Addition Behavior of a Numerical Semigroup. Séminaries et Congrés 11, 21-28.

AMOROS, M. B. February 2007. A Note on Numerical Semigroups. IEEE Transactions On Information Theory, 53: (2).

ARF, C. 1949. Une interprétation algébrique de la suite des ordres de multiplicit´e d'une branche alg´ebrique. Proc. London Math. Soc. 50: (2), 256-287.

CAMPILLO, A., FARRAN, J.I. and MUNUERA, C. 2000. On The Parameters Of Algebraic Geometry Codes Related to Arf Semigroups. IEEE Transactions On Information Theory, 46: (7).

HOHOLDT, T., VAN LINT, J.H. and PELLIKAAN, R. 1998. Algebraic geometry codes. in Handbook of Coding Theory 1. pp. 871-961. Amsterdam, The Netherlands.

KIRFEL, C., PELLIKAAN, R. 1995. The minimum distance of codes in an array coming from telescopic semigroups. IEEE Transactions On Information Theory 1: (6), 1720-1732.

LIPMAN, J., Stable ideals and Arf rings. http://www.bilkent.edu.tr/ sertoz/depo/-lipman.pdf

PELLIKAAN, R., TORRES, F. 1999. On Weierstrass semigroups and the redundancy of improved geometric Goppa codes. IEEE Transactions On Information Theory 45. 1512-1520.

ROSALES, J.C., GARCIA-SANCHEZ, P.A., GARCIA-GARCIA, J.I. and BRANCO, M.B. 2004. Arf numerical semigroups. Journal of Algebra, 276, 3-12.

ROSALES, J.C. ve GARCIA-SANCHEZ, P.A. 2009. Numerical semigroups. pp. 5-44. Springer. New York.

SERTÖZ, S. http://www.bilkent.edu.tr/ sertoz/depo/sertoz1.pdf

STICHTENOTH, H. 2009. Algebraic function fields and codes. pp. 1-145. Springer. Berlin.

ÖZGEÇMİŞ

Damla DEDE SİPAHİ, 1987 yılında Antalya'da doğdu. İlk, orta ve lise öğrenimini Antalya'da tamamladı. 2005 yılında girdiği Ege Üniversitesi Fen Fakültesi Matematik Bölümü'nden 2010 yılında mezun oldu. Eylül 2010'da Akdeniz Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda Yüksek Lisans öğrenimine başladı.