T.C.
KIRŞEHİR AHİ EVRAN ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

BİR POLİNOM ÖZDEŞLİĞİNİ SAĞLAYAN BİR DERİVASYONA SAHİP LİE CEBİRLERİNİN YAPISI

Hatice DİREMCİ NARİN

YÜKSEK LİSANS TEZİ

KIRŞEHİR
2026

T.C.
KIRŞEHİR AHİ EVRAN ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

BİR POLİNOM ÖZDEŞLİĞİNİ SAĞLAYAN BİR DERİVASYONA SAHİP LİE CEBİRLERİNİN YAPISI

Hatice DİREMCİ NARİN

YÜKSEK LİSANS TEZİ

DANIŞMAN
Doç. Dr. Nil MANSUROĞLU

KIRŞEHİR
2026

YÜKSEK LİSANS TEZ ONAYI

Bu Yüksek Lisans Tezi 14/05/2026 Tarihinde Aşağıdaki Jüri Üyeleri Tarafından Değerlendirilmiş ve Oy Birliği / Oy Çokluğu ile Kabul Edilmiştir.

Doç. Dr. Nil MANSUROĞLU (Danışman) .....

Doç. Dr. Gonca KIZILASLAN YILDIRIM (Jüri) .....

Dr. Öğr. Üyesi Emine ÖNAL KIR (Jüri) .....

Bu Tez Kırşehir Ahi Evran Üniversitesi, Fen Bilimleri Enstitüsü, Matematik Anabilim Dalında hazırlanmış ve onaylanmıştır.

Tez No:

Prof. Dr. Ümit DEMİRAL
Enstitü Müdürü

Not: Bu tezde kullanılan özgün ve başka kaynaktan yapılan bildirişlerin, tablo ve fotoğrafların kaynak gösterilmeden kullanımı, 5846 sayılı Fikir ve Sanat Eserleri Kanunundaki hükümlere tabidir.

KIRŞEHİR AHİ EVRAN ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZ ÇALIŞMASI

ETİK BEYANI

Kırşehir Ahi Evran Üniversitesi Bilimsel Araştırma ve Yayın Etiği Yönergesini okuduğumu ve anladığımı ve Kırşehir Ahi Evran Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde ve ortaya çıkan sonuçlarda herhangi bir değişiklik yapmadığımı,
- Tez olarak sunduğum bu çalışmanın özgün olduğunu,

bildirir, aksi bir durumda bu konuda hakkımda yapılacak tüm yasal işlemleri ve aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

14/05/2026

Hatice DİREMCİ NARİN

İÇİNDEKİLER DİZİNİ

Sayfa No

TEŞEKKÜR

Yüksek lisansa başladığım ilk andan son ana kadar bana karşı sabırlı ve sakin bir tutum sergileyen, yolumu aydınlatan ve başarıya ulaşmam için her adımda desteğini esirgemeyen saygıdeğer danışmanım Doç. Dr. Nil MANSUROĞLU'na teşekkürlerimi sunarım.

Bu zorlu süreçte danışmanımın yanı sıra bana en büyük desteği sağlayan sevgili eşime ve değerli aileme teşekkür ederim.

Tezimi kızım Laren NARİN'e ithaf ederim.

Mayıs, 2026 Hatice DİREMCİ NARİN

ÖZET

YÜKSEK LİSANS TEZİ

BİR POLİNOM ÖZDEŞLİĞİNİ SAĞLAYAN BİR DERİVASYONA SAHİP LİE CEBİRLERİNİN YAPISI

Hatice DİREMCİ NARİN

KIRŞEHİR AHİ EVRAN ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

MATEMATİK ANABİLİM DALI

Danışman: **Doç. Dr. Nil MANSUROĞLU**

Yıl: 2026 Sayfa: 47

Jüri: **Doç. Dr. Nil MANSUROĞLU**

Doç. Dr. Gonca KIZILASLAN YILDIRIM

Dr. Öğr. Üyesi Emine ÖNAL KIR

Bu çalışma dört bölümden oluşmaktadır. İlk bölümde Lie cebirleri hakkında ayrıntılı bir literatür taraması sunuldu. İkinci bölümde çalışma boyunca ihtiyaç duyulan temel tanımlar ve teoremlere yer verildi. Üçüncü bölümde aritmetik değişmezler tanımlandı ve bu değişmezler ile ilgili özellikler verildi. Ayrıca $f(x) = x^n - 1$ ve $g(x) = (x+1)^n - 1 \in \mathbb{Z}[x]$ polinomlarının ortak bölenlerinin en büyüğü ve bu polinomların resultantının bulunması için n nin bütün koşulları araştırıldı. Son bölümde polinom özdeşliğini sağlayan bir derivasyona sahip Lie cebirlerinin yapısı incelendi.

Anahtar Kelimeler: Lie Cebiri, Derivasyon, Resultant, Circulant matris, Polinom özdeşliği

ABSTRACT

MASTER'S THESIS

THE STRUCTURE OF LİE ALGEBRAS WİTH A DERİVATİON SATİSFYİNG A POLYNOMİAL İDENTİTY

Hatice DİREMCİ NARİN

KIRŞEHİR AHİ EVRAN UNIVERSITY

INSTITUTE OF NATURAL AND APPLIED SCIENCES

DEPARTMENT OF MATHEMATICS

Supervisor: **Assoc. Prof. Dr. Nil MANSUROĞLU**
Year: 2026 Pages: 47
Juries: **Assoc. Prof. Dr. Nil MANSUROĞLU**
Assoc. Prof. Dr. Gonca KIZILASLAN YILDIRIM
Assist. Prof. Dr. Emine ÖNAL KIR

This study includes four chapters. The first chapter one presents a detailed literature review on Lie algebras. In the second chapter, the definitions and theorems needed throughout the study are presented. In the third chapter, arithmetic invariants are defined and their specifications are discussed. Morever, the study investigates all possible conditions on n for determining the greatest common divisor and the resultant of the polynomials $f(x) = x^n - 1$ and $g(x) = (x+1)^n - 1 \in \mathbb{Z}[x]$. In the final chapter, the structure of Lie algebras with a derivation satisfying a polynomial identity is analyzed.

Keywords: Lie algebra, Derivation, Resultant, Circulant matrix, Polynomial identity

TABLOLAR DİZİNİ

Sayfa No

SİMGELER VE KISALTMALAR DİZİNİ

Simgeler	**Açıklama**
$\mathcal{C}(n)$	Circulant matris
K	Cisim
d	Derivasyon
$R(f,g)$	f ve g polinomlarının resultantı
$\mathbb{C}$	Kompleks sayılar
$\mathcal{G}$	Lie cebiri
$\mathbb{Q}$	Rasyonel sayılar
$\overline{\mathbb{Q}}$	Rasyonel sayıların cebirsel kapanışı
$\mathbb{R}$	Reel sayılar
$Syl(f,g)$	Sylvester matris
$\mathbb{Z}$	Tam sayılar
$\Phi_3(x)$	3. dereceden Sayklotomik polinom

1. GİRİŞ

Lie cebirleri, ilk olarak 1870 yılında M.S. Lie tarafından tanımlanmış ve matematik ile fiziğin birçok alanında temel bir yapı haline gelmiştir. Bu cebir yapıları hakkında literatürde pek çok çalışma mevcuttur. Bu çalışmada Lie cebirlerinin derivasyonları ve özellikle belli bir polinom özdeşliğini sağlayan derivasyona sahip Lie cebirlerinin yapısı incelendi.

Tekil olmayan derivasyonlar Lie cebirlerinde önemli bir yer almaktadır. N. Jacobson, [8] makalesinde tekil olmayan derivasyona sahip ve karakteristiği sıfır olan cisim üzerinde tanımlı Lie cebirlerinin nilpotent olduğunu gösterdi. Fakat bu durum karakteristiği asal bir p sayısı olan cisimlerde daha karışıktır. A.I. Kostrikin ve M.I. Kuznetsov, [11] çalışmasında tekil olmayan derivasyona sahip ve karakteristiği asal p sayısı olan cisim üzerinde tanımlı Lie cebirlerinin nilpotent olmadığını örnek vererek gösterdiler.

Bu çalışmanın amacı bir polinom özdeşliğini sağlayan bir derivasyona sahip ve karakteristiği sıfır olan cisim üzerinde tanımlı Lie cebirlerini incelemektir. K, karakteristiği sıfır olan bir cisim ve $\mathcal{G}$, K cismi üzerinde bir Lie cebir olsun. $r \in K[x]$ polinomu ele alınsın. Bu takdirde $d \in Der(\mathcal{G})$ derivasyonu, $r(d) = 0$ oluyorsa bu derivasyona r ile verilen bir polinom özdeşliğini sağlayan derivasyon denir. Bu çalışmada özel olarak $r = x^n - 1$ polinomu ele alındı. d derivasyonunun r ile verilen polinom özdeşliğinin sağlanabilmesi için gerek ve yeter koşulun d nin $n.$ mertebeden periyodik derivasyon olduğu, yani id birim dönüşüm olmak üzere $d^n = id$ olduğu gösterilmiştir. n nin 6 ile bölünüp bölünmeme durumları incelenerek $f(x) = x^n - 1$, $g(x) = (x+1)^n - 1 \in \mathbb{Z}[x]$ polinomlarının en büyük ortak böleni hesaplandı. Uzun yıllar boyunca f ve g polinomlarının resultantının bulunması üzerine birçok çalışma yapılmıştır. E. Wendt, [24] çalışmasında bu polinomların resultantının Circulant matris $\mathcal{C}(n)$ nin determinantına eşit olduğunu gösterdi. E. Lehmer de, [12] çalışmasında $\mathcal{C}(n)$ nin determinantının sıfır olması için gerek ve yeter koşulun n nin 6 ile tam bölünmesi olduğunu ispatladı.

Bu çalışma dört bölümden oluşmaktadır. İkinci bölümde çalışma boyunca ihtiyaç duyulacak temel tanımlar ve teoremlere yer verildi. Üçüncü bölümde aritmetik değişmezler tanımlandı ve bu değişmezler ile ilgili özellikler verildi. Son bölümde (D. Burde ve W. A. Moens, [4]) çalışmasında periyodik derivasyona sahip ve karakteristiği sıfır olan bir cisim üzerinde tanımlı Lie cebirleri ile ilgili elde edilen sonuçlar, karakteristiği sıfır olan bir cisim üzerinde belirli bir polinom özdeşliğini sağlayan derivasyona sahip Lie cebirleri için incelendi.

2. ÖNCEKİ ÇALIŞMALAR

Bu bölümde [1, 13] çalışmalarından yararlanılarak diğer bölümlerde ihtiyaç duyulacak olan temel tanımlar ve teoremler verildi.

2.1. Lie Cebirleri

Tanım 2.1. C, K cismi üzerinde bir vektör uzayı olmak üzere $(\kappa, \nu) \mapsto f(\kappa, \nu) := \kappa\nu$ şeklinde tanımlanan $f : C \times C \to C$ dönüşümü bilineerlik özelliğini sağlıyorsa C ye K-cebir denir ve (C, f) ile gösterilir.

Tanım 2.2. C, K cismi üzerinde bir cebir ve $\mathcal{N}$, C nin bir alt vektör uzayı olmak üzere her $\kappa, \nu \in \mathcal{N}$ için $\kappa\nu \in \mathcal{N}$ oluyorsa $\mathcal{N}$ ye C nin bir alt cebiri denir.

Tanım 2.3. C, K cismi üzerinde bir cebir ve $\mathcal{N}$, C nin alt vektör uzayı olsun. Her $\kappa \in C$ ve $\nu \in \mathcal{N}$ için $\kappa\nu, \nu\kappa \in \mathcal{N}$ ise $\mathcal{N}$ ye C nin bir ideali denir.

Uyarı 2.4. Her ideal bir alt cebirdir, fakat her alt cebir ideal değildir.

Tanım 2.5. C, K cismi üzerinde bir cebir olmak üzere her $\kappa, \nu, z \in C$ için

$$\kappa(\nu z) = (\kappa\nu)z$$

sağlanıyorsa C ye asosyatif (birleşmeli) cebir denir.

Tanım 2.6. C, K cismi üzerinde bir cebir olmak üzere her $\kappa, \nu \in C$ için

$$\kappa\nu = \nu\kappa$$

sağlanıyorsa C ye komütatif (değişmeli) cebir denir.

Tanım 2.7. C, K cismi üzerinde bir cebir olmak üzere her $\kappa \in C$ için

$$\kappa^2 = \kappa\kappa = 0$$

sağlanıyorsa C ye anti-komütatif cebir denir.

Tanım 2.8. C, K cismi üzerinde bir cebir olmak üzere her $\kappa, \nu, z \in C$ için

$$J(\kappa, \nu, z) = (\kappa\nu)z + (\nu z)\kappa + (z\kappa)\nu = 0$$

sağlanıyorsa C ye, Jacobi özdeşliğini sağlar denir.

Tanım 2.9. C, K cismi üzerinde bir cebir olmak üzere aşağıdaki iki koşulu

(L1) her $\kappa \in C$ için $\kappa\kappa = 0$ (anti-komütatiflik)

(L2) her $\kappa, \nu, z \in C$ için $(\kappa\nu)z + (\nu z)\kappa + (z\kappa)\nu = 0$ (Jacobi özdeşliği)

sağlıyorsa C ye Lie cebiri denir.

Tanım 2.10. $(C, .)$, K cismi üzerinde birleşmeli bir cebir olmak üzere C üzerinde

$$(\kappa, \nu) \mapsto [\kappa, \nu] = \kappa\nu - \nu\kappa$$

şeklinde tanımlanan $[,] : C \times C \to C$ yeni çarpıma Lie çarpımı denir.

Önerme 2.11. $(C, .)$, K cismi üzerinde herhangi bir birleşmeli cebir olsun. O zaman $(C, [,])$, bir Lie cebirdir.

Tanım 2.12. $\mathcal{G}$, K cismi üzerinde bir Lie cebir olmak üzere her $\kappa, \nu \in \mathcal{G}$ için $[\kappa, \nu] = 0$ ise $\mathcal{G}$ ye abelyen Lie cebir denir.

Tanım 2.13. M, $n \times n$ tipinde bir matris olsun. Bu matrisin köşegeni üzerindeki elemanlarının toplamına matrisin izi denir ve $iz(M)$ ile gösterilir.

Tanım 2.14. K cismi üzerindeki bütün $n \times n$ tipindeki matrislerin kümesi

$$\mathcal{M}_n(K) = \{M = [a_{ij}]_{n\times n} |\ a_{ij} \in K\}$$

matrislerde bilinen çarpma işlemi ile birlikte birleşmeli cebir olur. Önerme 2.11. den dolayı $(\mathcal{M}_n(K), [,])$ bir Lie cebirdir. Bu Lie cebirine matris Lie cebiri denir ve $gl(n, K)$ ile gösterilir.

Tanım 2.15. $sl(n, K) = \{M \in gl(n, K) |\ iz(M) = 0\}$ şeklinde tanımlanan küme $gl(n, K)$ nın bir alt uzayıdır. Ayrıca bu alt uzay, $gl(n, K)$ nın bir Lie alt cebiridir. Bu alt cebir özel lineer Lie cebiri olarak adlandırılır.

Tanım 2.16. $\mathcal{G}$, K cismi üzerinde bir Lie cebiri olmak üzere $C(\mathcal{G}) = \{\kappa \in \mathcal{G} |$ her $\nu \in \mathcal{G}$ için $[\kappa, \nu] = 0\}$ şeklinde tanımlanan kümeye $\mathcal{G}$ nin merkezi denir.

2.1.1. Nilpotent Lie cebirleri

Lemma 2.17. $\mathcal{G}, K$ cismi üzerinde bir Lie cebiri ve $\mathcal{S}$ ile $\mathcal{T}$, $\mathcal{G}$ nin idealleri olsun. O zaman

$$[\mathcal{T}, \mathcal{S}] = \text{Span}\{[\kappa, \nu] |\ \text{her } \kappa \in \mathcal{T}, \nu \in \mathcal{S} \text{ için}\}$$

çarpım uzayı $\mathcal{G}$ nin bir idealidir.

Tanım 2.18. $\mathcal{G}$, K cismi üzerinde bir Lie cebiri olmak üzere $\mathcal{G}$ nin kendisi ve $\{0\}$ dışında hiçbir ideali yoksa $\mathcal{G}$ ye basit Lie cebiri denir.

Tanım 2.19. $\mathcal{G}, K$ cismi üzerinde bir Lie cebiri olmak üzere $\mathcal{G}^1 = \mathcal{G}$ ve m pozitif tamsayısı için $\mathcal{G}^{m+1} = [\mathcal{G}^m, \mathcal{G}]$ şeklinde tanımlansın. O zaman her pozitif m tamsayısı için $\mathcal{G}^m$, $\mathcal{G}$ nin ideali ve $\mathcal{G}^{m+1} \subseteq \mathcal{G}^m$ olmak üzere $\mathcal{G}$ nin ideallerinin

$$\mathcal{G} = \mathcal{G}^1 \supseteq \mathcal{G}^2 \supseteq \ldots \supseteq \mathcal{G}^m \supseteq \mathcal{G}^{m+1} \supseteq \ldots$$

bir azalan serisi elde edilir. Bu seriye $\mathcal{G}$ nin alt merkezi serisi denir.

Tanım 2.20. Bir pozitif t tamsayısı için $\mathcal{G}^t = 0$ ise $\mathcal{G}$ ye nilpotent Lie cebiri denir. Bir s pozitif tamsayısı için eğer $\mathcal{G}^s \neq 0$ ve $\mathcal{G}^{s+1} = 0$ oluyorsa s ye $\mathcal{G}$ nin nilpotentlik sınıfı denir. Nilpotentlik sınıfı $c(\mathcal{G})$ ile gösterilir.

2.1.2. Derivasyonlar

Tanım 2.21. $\mathcal{G}_1$ ve $\mathcal{G}_2$, K cismi üzerinde iki Lie cebiri olsun. Eğer $d : \mathcal{G}_1 \to \mathcal{G}_2$ lineer dönüşümü her $\kappa, \nu \in \mathcal{G}_1$ için

$$[\kappa, \nu] \mapsto d([\kappa, \nu]) = [d(\kappa), d(\nu)]$$

eşitliğini sağlıyorsa d ye Lie cebir homomorfizması denir. d homomorfizması birebir ise monomorfizma, örten ise epimorfizma, hem birebir hem de örten ise d homomorfizmasına Lie izomorfizması denir ve $\mathcal{G}_1 \cong \mathcal{G}_2$ ile gösterilir. $\mathcal{G}$ bir Lie cebir olsun. $f : \mathcal{G} \to \mathcal{G}$ homomorfizmasına endomorfizma denir ve tüm endomorfizmaların kümesi $End(\mathcal{G})$ ile gösterilir.
$(End(\mathcal{G}), \circ)$, birleşmeli cebir olduğundan her $f, g \in End(\mathcal{G})$ için $[f, g] = f \circ g - g \circ f$ Lie çarpımı ile bir Lie cebir yapısı oluşturur. Dolayısıyla $gl(\mathcal{G}) = (End(\mathcal{G}), [,])$, bir Lie cebirdir.

Tanım 2.22. $\mathcal{G}$, bir Lie cebir olmak üzere $d : \mathcal{G} \to \mathcal{G}$ lineer dönüşümü her $\kappa, \nu \in \mathcal{G}$ için

$$d([\kappa, \nu]) = [d(\kappa), \nu] + [\kappa, d(\nu)]$$

koşulunu sağlarsa $d \in End(\mathcal{G})$ ye $\mathcal{G}$ nin bir derivasyonu denir.
$\mathcal{G}$ nin bütün derivasyonlarının kümesi $Der(\mathcal{G})$ ile gösterilir ve bu küme bir Lie cebir yapısı oluşturur.

Tanım 2.23. C, K cismi üzerinde $\{a_1, ..., a_n\}$ bazına sahip olan n boyutlu bir cebir ve d, C cebirinin bir derivasyonu olsun. Eğer $\{a_1, ..., a_n\}$ bazındaki bazı elemanlar için $d(a_i) \in Ka_i$ oluyorsa d derivasyonuna yarı basit denir.

Tanım 2.24. $\mathcal{G}$ bir Lie cebiri ve d, $\mathcal{G}$ nin bir derivasyonu olsun. Eğer d birebir ve örten ise d ye tekil olmayan derivasyon denir.

Tanım 2.25. $\mathcal{G}$ bir Lie cebir ve d, $\mathcal{G}$ nin derivasyonu olsun. id birim dönüşüm olmak üzere $d^n = id$ olacak şekilde n pozitif tamsayısı mevcutsa d ye n. mertebeden periyodik derivasyon denir.

2.2. Polinom Halkaları

2.2.1. Halkalar

Tanım 2.26. Boştan farklı $\mathcal{R}$ kümesi üzerinde toplama ve çarpma olarak tanımlanan iki tane işlem olsun. O zaman
(i) $\mathcal{R}$ kümesi toplama işlemine göre bir abelyen grup,
(ii) $\mathcal{R}$ kümesi çarpma işlemine göre kapalı ve birleşmeli,
(iii) her $\kappa, \nu, z \in \mathcal{R}$ için $\kappa(\nu + z) = \kappa\nu + \kappa z$ ve $(\nu + z)\kappa = \nu\kappa + z\kappa$ (dağılma özelliği) şartları sağlanıyorsa bu kümeye halka denir ve $(\mathcal{R}, +, .)$ ile gösterilir. $(\mathcal{R}, +, .)$ bir halka olmak üzere her $\kappa \in \mathcal{R}$ için

$$\varepsilon\kappa = \kappa\varepsilon = x$$

olacak şekilde $\varepsilon \in \mathcal{R}$ mevcutsa ε elemanına $\mathcal{R}$ halkasının birimi ve $\mathcal{R}$ ye de birimli halka denir. $\mathcal{R}$ nin toplamsal birimi $0_{\mathcal{R}}$ ve çarpımsal birimi $1_{\mathcal{R}}$ ile gösterilir.

Tanım 2.27. $\mathcal{R}$ bir halka olmak üzere her $\kappa, \nu \in \mathcal{R}$ için

$$\kappa\nu = \nu\kappa$$

ise $\mathcal{R}$ ye değişmeli halka denir.

Örnek 2.28. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ toplama ve çarpma işlemleriyle birimli ve değişmeli halkalardır.

Tanım 2.29. $\mathcal{R}$ bir halka olmak üzere $\kappa\nu = 0_{\mathcal{R}}$ şartını sağlayan her $\kappa, \nu \in \mathcal{R}$ için $\kappa = 0_{\mathcal{R}}$ veya $\nu = 0_{\mathcal{R}}$ ise $\mathcal{R}$ ye sıfır bölensiz halka denir.

Örnek 2.30. $(\mathbb{Z}, +, .)$ halkası sıfır bölensiz halkadır.

Tanım 2.31. $1_{\mathcal{R}} \neq 0_{\mathcal{R}}$ olacak şekilde $\mathcal{R}$ birimli, değişmeli bir halka olsun. Eğer $\mathcal{R}$ halkası sıfır bölensizse $\mathcal{R}$ ye tamlık bölgesi denir.

Örnek 2.32. $\mathbb{Z}, \mathbb{Q}$, $\mathbb{R}$ ve $\mathbb{C}$ halkaları birer tamlık bölgesidir.

Teorem 2.33. Her cisim bir tamlık bölgesidir.

Teorem 2.34. Her sonlu tamlık bölgesi bir cisimdir.

Tanım 2.35. $\mathcal{R}$ bir halka olmak üzere her $\kappa \in \mathcal{R}$ için $m\kappa = 0$ şartını sağlayan en küçük m pozitif tamsayısına $\mathcal{R}$ halkasının karakteristiği denir. Eğer bu koşulu sağlayan pozitif bir tamsayı mevcut değilse $\mathcal{R}$ nin karakteristiği sıfırdır. $\mathcal{R}$ halkasının karakteristiği $kar(\mathcal{R})$ ile gösterilir.

Örnek 2.36. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ve $\mathbb{C}$ halkalarının karakteristiği 0 dır. $(\mathbb{Z}_6, +, .)$ nin karakteristiği 6 dır.

Teorem 2.37. Bir tamlık bölgesinin karakteristiği sıfır ya da bir asal sayıdır.

Uyarı 2.38. Her cisim tamlık bölgesi olduğundan dolayı cismin karakteristiği sıfır ya da asal sayıdır.

Tanım 2.39. $\mathcal{R}$ bir tamlık bölgesi ve $\kappa \in \mathcal{R}$ olmak üzere κ tarafından üretilen

$$\langle \kappa \rangle = \{\kappa r \mid r \in \mathcal{R}\}$$

idealine esas ideal denir. $\mathcal{R}$ nin her ideali esas idealse $\mathcal{R}$ ye esas ideal bölgesi denir.

Örnek 2.40. $(\mathbb{Z}, +, .)$, esas ideal bölgesidir.

2.2.2. Polinom halkaları

Tanım 2.41. $\mathcal{R}$ bir birimli halka, x belirsiz ve her $i = 0, 1, 2, 3, \ldots, m$ için $\alpha_i \in \mathcal{R}$ olmak üzere

$$f(x) = a_0x^0 + a_1x^1 + \ldots + a_mx^m$$

şeklinde tanımlanan ifadeye $\mathcal{R}$ katsayılarından oluşan x e göre bir polinom denir. Bu şekilde tanımlanan bütün polinomların kümesi $\mathcal{R}[x]$ ile gösterilir.

Tanım 2.42. $\mathcal{R}$ bir halka ve x belirsiz olmak üzere $m, n \in \mathbb{N}$ için

$$f(x) = a_0x^0 + a_1x^1 + \ldots + a_mx^m \in \mathcal{R}[x]$$

$$g(x) = b_0x^0 + b_1x^1 + \ldots + b_nx^n \in \mathcal{R}[x]$$

olsun. $k = maks(m, n)$ ve $c_i = \sum_{j=0}^{i} a_jb_{i-j}$ olmak üzere

$$f(x) + g(x) = \sum_{i=0}^{k} (a_i + b_i)x^i$$

$$f(x).g(x) = \sum_{i=0}^{m+n} (c_ix^i)$$

şeklinde tanımlanan işlemlerle $(\mathcal{R}[x], +, .)$ birimli bir halka yapısına sahiptir. Bu halkaya $\mathcal{R}$ üzerinde tanımlı polinomlar halkası denir.

Tanım 2.43. $\mathcal{R}$ birimli bir halka olsun.

$$f(x) = a_0x^0 + a_1x^1 + \ldots + a_mx^m \in \mathcal{R}[x], \quad a_m \neq 0$$

olmak üzere m ye $f(x)$ polinomunun derecesi denir ve $derf(x)$ ile gösterilir.

Tanım 2.44. Başkatsayısı 1 olan polinoma monik polinom denir.

Tanım 2.45. $\mathcal{R}$ bir tamlık bölgesi, $f(x) \in \mathcal{R}[x]$ ve $c \in \mathcal{R}$ olsun. Eğer $f(c) = 0_{\mathcal{R}}$ ise c ye $f(x)$ polinomunun kökü ya da sıfırı denir.

Tanım 2.46. $\mathcal{R}$ bir tamlık bölgesi, $f(x) \in \mathcal{R}[x]$ sabit olmayan bir polinom ve $c \in \mathcal{R}$ olmak üzere $f(c) = 0_{\mathcal{R}}$ olsun. Eğer $(x-c)^s \mid f$ fakat $(x-c)^{s+1} \nmid f$ ise c ye f polinomunun s katlı bir kökü denir. Eğer $s = 1$ ise c ye basit kök denir.

Tanım 2.47. $f(x) = a_0x^0 + a_1x^1 + \ldots + a_mx^m \in \mathcal{R}[x]$ ve c_i ler bu polinomun kökleri olsun. O zaman bu polinomun diskriminantı

$$Disc(f) = a_m^{2m-2} \prod_{i<j}^{m} (c_i - c_j)^2$$

olarak tanımlanır.

Örnek 2.48. $f(x) = x^2 - 5x + 6$ polinomu $(x-2)(x-3)$ e eşittir. Böylece kökleri $c_1 = 2$ ve $c_2 = 3$ bulunur. $m = 2$ ve $a_2 = 1$ olmak üzere

$$\prod_{i<j}^{2} (c_1 - c_2)^2 = (2-3)^2 = 1^2 = 1$$

elde edilir. Dolayısıyla $Disc(f) = (-5)^2 - 4.1.6 = 25 - 24 = 1$ dir.

Uyarı 2.49. Eğer $\mathcal{R}$ tamlık bölgesi ise $\mathcal{R}[x]$ de tamlık bölgesidir. Ayrıca eğer $\mathcal{R}$ bir cisim ise $\mathcal{R}[x]$, bir esas ideal bölgesidir.

Aşağıdaki iki tanımda $\mathcal{R}$ cisim olarak kabul edilecektir.

Tanım 2.50. $f(x), g(x) \in \mathcal{R}[x]$ olmak üzere $f(x) = g(x).l(x)$ olacak şekilde bir $l(x) \in \mathcal{R}[x]$ varsa o zaman $f(x)$, $g(x)$ i böler ve $g(x)|f(x)$ şeklinde gösterilir.

Tanım 2.51. $f(x)$ ve $g(x)$, $\mathcal{R}[x]$ polinom halkasında sıfırdan farklı iki polinom olsun. O zaman
(i) $q(x)$ monik,
(ii) $q(x)|f(x)$ ve $q(x)|g(x)$,
(iii) $l(x)|f(x)$ ve $l(x)|g(x)$ iken $l(x)|q(x)$
şartlarını sağlayan $q(x)$ polinomuna, $f(x)$ ve $g(x)$ polinomlarının ortak bölenlerinin en büyüğü denir ve $q(x)$=$obeb(f(x), g(x))$ ile gösterilir.

Örnek 2.52. $f(x) = 3x^3 + 5x^2 + 6x \in \mathbb{Z}_7[x]$ ve $g(x) = 4x^4 + 2x^3 + 6x^2 + 4x + 5 \in \mathbb{Z}_7[x]$ olsun. O zaman $q(x) = obeb(f(x), g(x)) = x + 6$ dır.

Tanım 2.53. $\mathcal{R}$, birimli bir halka ve x belirsiz olmak üzere $f(x)$, $\mathcal{R}$ üzerinde tanımlı ve sabit olmayan polinom olsun. Eğer her $g(x), l(x) \in \mathcal{R}[x]$ için $f(x) = g(x).l(x)$ eşitliği sağlanıyorsa ve $g(x)$ veya $l(x)$ tersinir ise $f(x)$ polinomuna $\mathcal{R}$ üzerinde indirgenemez bir polinom denir.

Örnek 2.54. $f(x) = 2 + 4x \in \mathbb{Z}[x]$ olsun. $f(x) = 2 + 4x = 2(x + 2)$ deki çarpanların her ikisi $\mathbb{Z}[x]$ içinde tersinir olmadığından verilen polinom $\mathbb{Z}$ de indirgenemez değildir.

Örnek 2.55. $f(x) = x^2 + 1$ olsun. Bu polinom $\mathbb{C}$ de indirgenebilirdir fakat $\mathbb{R}$ de ve $\mathbb{Q}$ da indirgenemezdir.

2.2.3. İlkel kökler

Tanım 2.56. $n \in \mathbb{Z}^+$ ve K bir cisim olmak üzere $x^n - 1$ polinomunun K cismindeki köklerine birimin $n.$ kökleri denir.

Örnek 2.57. $x^n - 1$ polinomunun karmaşık sayılar içindeki kökleri $k = 0, 1, \ldots, n - 1$ için

$$w_k = e^{\left(\frac{2\pi k}{n}\right).i} = \cos\left(\frac{2\pi k}{n}\right) + i.\sin\left(\frac{2\pi k}{n}\right)$$

dir.

Tanım 2.58. Birimin $n.$ kökleri bir çarpım grubu oluşturur. Bu grup devirli ise üreteç elemanına birimin $n.$ ilkel kökü denir. $k = 0, 1, 2, \ldots, n-1$ için birimin $n.$ kökleri

$$\begin{aligned} w_k =& e^{\left(\frac{2\pi k}{n}\right).i} \\ =& \cos\left(\frac{2\pi k}{n}\right) + i.\sin\left(\frac{2\pi k}{n}\right) \\ =& \left(\cos\frac{2\pi}{n} + i.\sin\frac{2\pi}{n}\right)^k \\ =& w_1^k \end{aligned}$$

şeklinde ifade edilir. Böylece bu devirli grubun üreteci w_1 dir.

Örnek 2.59. $f(x) = x^5 - 1$ polinomunun kökleri $w = e^{\frac{2\pi i}{5}}$ olmak üzere $1, w, w^2, w^3, w^4$ tür.

Tanım 2.60. $t|n$ olacak şekilde $t, n \in \mathbb{Z}^+$ için $w_1, w_2, \ldots, w_k$ değerleri birimin $n.$ kökleri içerisinde $t.$ dereceden kökleri olsun. O zaman

$$\Phi_t(x) = (x - w_1)(x - w_2)\ldots(x - w_k)$$

polinomu, Sayklotomik polinom olarak adlandırılır.

Örnek 2.61. $t = 3$ ve $n = 6$ olsun. Birimin $6.$ kökleri kümesinden $3.$ dereceden kökleri w^0, w^2, w^4 şeklindedir. Bu kökler ile oluşturulan $3.$ dereceden Sayklotomik polinom

$$\Phi_3(x) = (x - w^2)(x - w^4) = x^2 + x + 1$$

dir.

Örnek 2.62. $x^n - 1$ polinomu çarpanlara ayrılışı

$$x^n - 1 = (x - w_1)(x - w_2)\ldots(x - w_k)\ldots(x - w_n)$$

şeklindedir. $1 < t$ ve $t \in \mathbb{Z}^+$ olmak üzere w, $t.$ dereceden bir kök ise $w^{\left(\frac{n}{t}\right)}$ de $t.$ dereceden bir kök olur. Dolayısıyla

$$x^n - 1 = \prod_{t|n} \Phi_t(x)$$

eşitliği elde edilir. Böylece $\Phi_1(x) = x - 1$ olduğu sonucuna ulaşılır. Genel olarak, $t < n$ ve $t|n$ için, $\Phi_n(x)$ Sayklotomik polinomunun tam katsayılı olduğu kabul edilir.

Buna göre,

$$\Phi_n(x) = \frac{x^n - 1}{\prod\limits_{\substack{t|n \\ t<n}} \Phi_t(x)}$$

olarak ifade edilir.

Şimdi Sayklotomik polinom $\Phi_n(x)$ ile ilgili bazı özellikler ve sonuçlar verilecektir.

Özellik 1 : $\Phi_n(x)$, $\mathbb{Q}[x]$ içinde indirgenemez bir polinomdur.

Sonuç 1 : w, birimin $n.$ ilkel kökü olmak üzere w nin indirgenemez polinomu $f(x)$ ise o zaman $f(x) = \Phi_n(x)$ dir.

Özellik 2 : $\Phi_n(x)$ polinomu $\mathbb{Z}_p[x]$ içinde çarpanlanabilirdir (indirgenebilirdir).

Özellik 3 : $\Phi_n(x)$ polinomunun derecesi Euler φ fonksiyonu olan $\varphi(n)$ ye eşittir. Yani $\varphi(n)$ değeri, n sayısından küçük olup n ile aralarında asal olan sayıların eleman sayısına eşittir.

3. MATERYAL VE METOT

3.1. Aritmetik Değişmezler

Bu bölümde [12, 24] çalışmalarından yararlanılarak bazı aritmetik değişmezler ve özellikleri verildi.

Lemma 3.1. $\alpha, \beta \in \mathbb{C}$ olmak üzere $|\alpha| = |\beta| = |\alpha + \beta| = 1$ olsun. O zaman w, birimin üçüncü ilkel kökü olmak üzere

$$\beta = w\alpha$$

veya

$$\beta = w^2\alpha$$

olur.

İspat: Verilen koşullardan

$$|0 - \alpha| = |\alpha - (\alpha + \beta)| = |0 - (\alpha + \beta)| = 1$$

elde edilir. Dolayısıyla

$$0,\ \alpha,\ \alpha + \beta$$

noktaları karmaşık düzlemde bir eşkenar üçgenin köşeleridir.
Şimdi

$$\gamma = -(\alpha + \beta)$$

olarak tanımlansın. O halde

$$\alpha + \beta + \gamma = 0$$

ve ayrıca

$$|\alpha| = |\beta| = |\gamma| = 1$$

eşitlikleri sağlanır. $|\beta| = |\alpha| = 1$ olduğundan bir $\lambda \in \mathbb{R}$ için

$$\beta = e^{i\lambda}\alpha$$

yazılabilir. Benzer şekilde bir $\mu \in \mathbb{R}$ için

$$\gamma = e^{i\mu}\alpha$$

olur.
Bu ifadeler

$$\alpha + \beta + \gamma = 0$$

eşitliğinde yerine yazılırsa

$$\alpha + e^{i\lambda}\alpha + e^{i\mu}\alpha = 0$$

elde edilir. $\alpha \neq 0$ olduğundan

$$1 + e^{i\lambda} + e^{i\mu} = 0$$

sonucuna ulaşılır.
Euler formülü kullanılarak

$$1 + \cos\lambda + \cos\mu + i(\sin\lambda + \sin\mu) = 0$$

elde edilir. Reel ve sanal kısımlar ayrı ayrı eşitlenirse

$$\cos\lambda + \cos\mu = -1$$

ve

$$\sin\lambda + \sin\mu = 0$$

olur.
Buradan

$$\sin\mu = -\sin\lambda$$

elde edilir. Ayrıca ilk denklem kullanılarak

$$\cos\mu = \cos\lambda$$

olduğu görülür. Dolayısıyla

$$\mu = -\lambda \pmod{2\pi}$$

elde edilir.
Böylece

$$2\cos\lambda = -1$$

olur ve buradan

$$\cos\lambda = -\frac{1}{2}$$

elde edilir. O halde

$$\lambda = \frac{2\pi}{3} \quad \text{veya} \quad \lambda = \frac{4\pi}{3}.$$

Dolayısıyla

$$e^{i\lambda} = w \quad \text{veya} \quad e^{i\lambda} = w^2,$$

burada

$$w = e^{2\pi i/3}$$

birimin üçüncü ilkel köküdür.
Sonuç olarak

$$\beta = w\alpha$$

veya

$$\beta = w^2\alpha$$

elde edilir.

Sonuç 3.2. $\alpha, \beta, \gamma, \alpha+\gamma, \beta+\gamma, \alpha+\beta+\gamma$ sayılarının tamamı birimin n. kökleri olamaz.

İspat: Aksi varsayılsın. Yani

$$\alpha, \beta, \gamma, \alpha+\gamma, \beta+\gamma, \alpha+\beta+\gamma$$

sayılarının tamamı birimin n. kökleri olsun.
Lemma 3.1. uygulanırsa,

$$|\alpha| = |\gamma| = |\alpha+\gamma| = 1$$

olduğundan birimin üçüncü ilkel kökü w için

$$\alpha = w^r\gamma$$

elde edilir; burada

$$r \in \{1, 2\}.$$

Benzer şekilde

$$|\beta| = |\gamma| = |\beta+\gamma| = 1$$

olduğundan yine Lemma 3.1. ile

$$\beta = w^s\gamma$$

elde edilir; burada

$$s \in \{1, 2\}.$$

Dolayısıyla

$$\alpha+\beta+\gamma = w^r\gamma + w^s\gamma + \gamma = (w^r + w^s + 1)\gamma.$$

Şimdi olasılıklar incelensin.
1. Durum: $r = s$.
Bu durumda

$$\alpha+\beta+\gamma = (1+2w^r)\gamma.$$

$r = 1$ için:

$$1 + 2w = 1 + 2\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = i\sqrt{3},$$

dolayısıyla

$$|1 + 2w| = \sqrt{3}.$$

Benzer şekilde $r = 2$ için de

$$|1 + 2w^2| = \sqrt{3}.$$

O halde

$$|\alpha + \beta + \gamma| = |1 + 2w^r||\gamma| = \sqrt{3}.$$

Fakat varsayıma göre

$$\alpha + \beta + \gamma$$

birimin kökü olduğundan normu 1 olmalıdır. Çelişki elde edilir.

2. Durum: $r \neq s$.

Bu durumda

$$\{r, s\} = \{1, 2\}$$

olur. Bilindiği gibi

$$1 + w + w^2 = 0.$$

Dolayısıyla

$$w^r + w^s + 1 = 0$$

ve böylece

$$\alpha + \beta + \gamma = 0$$

elde edilir.

Ancak 0, birimin kökü değildir. Bu da çelişkidir.

Her iki durumda da çelişki elde edildiğinden,

$$\alpha, \beta, \gamma, \alpha + \gamma, \beta + \gamma, \alpha + \beta + \gamma$$

sayılarının tamamı aynı anda birimin kökü olamaz.

Sonuç 3.3. $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ birimin $n.$ kökleri olsun. Eğer her farklı $i, j \in \{1, 2, 3, 4\}$ için

$$\alpha_i + \alpha_j$$

de birimin $n.$ kökü ise, böyle bir durum mümkün değildir.

İspat: Varsayılsın ki

$$\alpha_1, \alpha_2, \alpha_3, \alpha_4$$

birimin kökleri olsun ve ayrıca her farklı i, j için $\alpha_i + \alpha_j$ de birimin kökü olsun.
Lemma 3.1. uygulanırsa,

$$|\alpha_1| = |\alpha_2| = |\alpha_1 + \alpha_2| = 1$$

olduğundan

$$\alpha_2 = w^r \alpha_1$$

elde edilir; burada

$$r \in \{1, 2\}.$$

Benzer şekilde

$$\alpha_3 = w^s \alpha_1, \quad \alpha_4 = w^t \alpha_1$$

elde edilir; burada

$$r, s, t \in \{1, 2\}.$$

Şimdi üç sayı:

$$r, s, t$$

yalnızca iki farklı değer alabildiğinden, güvercin yuvası prensibine göre en az ikisi eşittir.
Dolayısıyla aşağıdaki durumlardan en az biri gerçekleşir:

$$r = s, \quad r = t, \quad s = t.$$

Genelliği bozmadan

$$r = s$$

olduğu varsayılsın. Bu durumda

$$\alpha_2 = \alpha_3 = w^r \alpha_1$$

olur.
Dolayısıyla

$$\alpha_2 + \alpha_3 = 2w^r \alpha_1.$$

Norm alınırsa:

$$|\alpha_2 + \alpha_3| = |2w^r \alpha_1| = 2|w^r||\alpha_1| = 2.$$

Ancak varsayıma göre

$$\alpha_2 + \alpha_3$$

birimin kökü olduğundan normunun 1 olması gerekir. Bu çelişkidir.
Dolayısıyla böyle bir durum mümkün değildir.

Tanım 3.4. $\mathcal{R}$ değişmeli bir halka ve

$$f(x) = a_0x^0 + a_1x^1 + \ldots + a_mx^m, \quad a_i \in \mathcal{R} \quad \text{ve} \quad a_m \neq 0$$

$$g(x) = b_0x^0 + b_1x^1 + \ldots + b_nx^n, \quad b_i \in \mathcal{R} \quad \text{ve} \quad b_n \neq 0$$

pozitif dereceye sahip $\mathcal{R}[x]$ üzerinde tanımlı iki polinom olsun. f polinomunun katsayıları her satırda n defa ve g polinomun katsayıları ise her satırda m defa kaydırılarak yazılmasıyla oluşturulan

$$Syl(f,g) = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_m & 0 & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_{m-1} & a_m & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & & \vdots & \vdots & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & a_0 & a_1 & \cdots & a_{m-1} & a_m \\ b_0 & b_1 & b_2 & \cdots & b_n & 0 & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_{n-1} & b_n & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & & \vdots & \vdots & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & b_0 & b_1 & \cdots & b_{n-1} & b_n \end{pmatrix}$$

matrisine Sylvester matrisi denir.

Örnek 3.5. $f(x) = x^2 + 3x + 2, g(x) = x + 1 \in \mathbb{Z}[x]$ olsun. O zaman Sylvester matrisi için gerekli katsayılar $f(x) = x^2 + 3x + 2$ polinomu için $[2, 3, 1]$ ve $g(x) = x + 1$ polinomu için ise $[1, 1]$ olarak bulunur. İlk olarak $f(x)$ in katsayıları $g(x)$ in derecesi kadar kaydırılarak yazılır. Daha sonra $g(x)$ in katsayıları $f(x)$ in derecesi kadar kaydırılarak satırlara yazılır. Böylece

$$Syl(f,g) = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

dir.

Tanım 3.6. Tanım 3.4. te verilen f ve g polinomlarının Sylvester matrisinin determinantına $\mathcal{R}$ üzerinde f ve g nin resultantı denir ve $R(f,g)$ ile gösterilir. α_i ler f nin β_j ler g nin kökleri olmak üzere f ve g nin resultantı

$$R(f,g) = a_m^n b_n^m \prod_{i,j} (\alpha_i - \beta_j) \tag{3.1}$$

ile de hesaplanır. Resultantın çarpım özelliği K cismi üzerinde

$$f(x) = a_m \prod_{i=1}^{m} (x - \alpha_i) \text{ ve } g(x) = b_n \prod_{j=1}^{n} (x - \beta_j)$$

olsun. Ayrıca

$$h(x) = c_t \prod_{k=1}^{t}(x - \gamma_k), \quad derh = t$$

olsun. Burada γ_k lar h nin kökleridir. (3.1) eşitliği kullanılarak

$$R(fg, h) = (a_m b_n)^t \prod_{k=1}^{t}(fg)(\gamma_k)$$

olur. Fakat $(fg)(\gamma_k) = f(\gamma_k)g(\gamma_k)$ olduğundan

$$R(fg, h) = (a_m b_n)^t \prod_{k=1}^{t} f(\gamma_k)g(\gamma_k)$$

dır. Çarpım ayrıştırıldığında

$$R(fg, h) = \left(a_m^t \prod_{k=1}^{t} f(\gamma_k)\right)\left(b_n^t \prod_{k=1}^{t} g(\gamma_k)\right)$$

olur. Dolayısıyla

$$R(f, h) = a_m^t \prod_{k=1}^{t} f(\gamma_k), \qquad R(g, h) = b_n^t \prod_{k=1}^{t} g(\gamma_k)$$

olduğundan

$$R(fg, h) = R(f, h)R(g, h)$$

şeklinde ifade edilir.

Örnek 3.7. $f(x) = x^2 - 5x + 6, g(x) = x - 1 \in \mathbb{Z}[x]$ olsun. O halde $f(x)$ in kökleri $\alpha_1 = 2$ ve $\alpha_2 = 3$ tür. $g(x)$ in kökü $\beta_1 = 1$ dir. Böylece

$$R(f, g) = \begin{vmatrix} 6 & -5 & 1 \\ -1 & 1 & 0 \\ 0 & -1 & 1 \end{vmatrix} = 7 - 5 = 2$$

dir. Ayrıca (3.1) formülü kullanılarak

$$R(f, g) = 1_1^1 . 1_1^2 \prod_{i,j}(\alpha_i - \beta_j) = (\alpha_1 - \beta_1)(\alpha_2 - \beta_1) = (2 - 1)(3 - 1) = 1.2 = 2$$

elde edilir. Sonuç olarak her iki yöntem ile $R(f, g) = 2$ dir.

Teorem 3.8. Katsayıları bir tamlık bölgesinden olan iki polinomun resultantının sıfır olması için gerek ve yeter koşul polinomların ortak bir köke sahip olmasıdır.

İspat: γ, f ve g polinomlarının ortak kökü olduğu kabul edilsin. Bu durumda çarpımın terimlerinden biri $(\gamma - \gamma) = 0$ olur. Dolayısıyla tüm çarpım sıfır olur.
Tersine $R(f,\ g) = 0$ olduğu kabul edilsin. O halde katsayıları tamlık bölgesinden dolayı sıfır bölen içermez, böyle çarpımın en az bir terimi sıfır olur. Bu terimin $(\alpha_k - \beta_l)$ olduğu varsayıldığında $\alpha = \beta$ elde edilir. Bu da f ve g polinomlarının ortak bir kökü olduğu anlamına gelir.

Lemma 3.9. $\Phi_3(x) = x^2 + x + 1 \in \mathbb{Z}[x]$, 3. dereceden Sayklotomik polinom ve $n \geq 1$ olmak üzere $f(x) = x^n - 1, g(x) = (x+1)^n - 1 \in \mathbb{Z}[x]$ in en büyük ortak böleni

$$obeb(f,g) = \begin{cases} 1, & \text{eğer } n \not\equiv 0 \pmod 6, \\ \Phi_3(x) = x^2 + x + 1, & \text{eğer } n \equiv 0 \pmod 6 \end{cases}$$

dır.

İspat: $h = obeb(x^n - 1, (x+1)^n - 1)$ olsun.
Karakteristik sıfır olduğundan

$$f(x) = x^n - 1$$

polinomunun türevi

$$f'(x) = nx^{n-1}$$

olur ve

$$obeb(f, f') = 1$$

elde edilir. Dolayısıyla f çok katlı kök içermez. Bu nedenle h de tekrarlı indirgenmez çarpan içermez.
Şimdi α, h nin bir kökü olsun. O halde

$$\alpha^n = 1$$

ve ayrıca

$$(\alpha + 1)^n = 1$$

olur. Dolayısıyla hem α hem de $\alpha + 1$ birimin n. kökleridir. Lemma 3.1. e göre

$$\alpha + 1 = w\alpha \quad \text{veya} \quad \alpha + 1 = w^2\alpha$$

olur.
Birinci durumda

$$1 = (w-1)\alpha$$

ve ikinci durumda

$$1 = (w^2-1)\alpha$$

elde edilir.
Her iki durumda da

$$\alpha^2 + \alpha + 1 = 0$$

sağlanır. Dolayısıyla

$$\Phi_3(\alpha) = 0.$$

Bu nedenle h nin tüm kökleri Φ_3 ün kökleridir. Ayrıca $\Phi_3(x) \mid x^n - 1$ ancak ve ancak $3 \mid n$ olduğundan,

$$h = \begin{cases} \Phi_3(x), & 3 \mid n, \\ 1, & 3 \nmid n. \end{cases}$$

İspat tamamlanmıştır.

Uzun yıllar boyunca $R(x^n-1, (x+1)^n-1)$ hesaplanması ile ilgili çeşitli çalışmalar yapılmıştır.

Tanım 3.10. $n \geq 1$ için sıfırdan farklı ρ_n tamsayısı

$$\rho_n = \begin{cases} R(x^n-1, (x+1)^n-1), & n \not\equiv 0 \pmod 6, \\ R\left(\frac{x^n-1}{\Phi_3}, \frac{(x+1)^n-1}{\Phi_3}\right), & n \equiv 0 \pmod 6 \end{cases}$$

şeklinde tanımlanır.

Tanım 3.11. $n \geq 1$ için

$$\mathcal{C}(n) = \begin{pmatrix} 1 & \binom{n}{1} & \binom{n}{2} & \cdots & \binom{n}{n-1} \\ \binom{n}{n-1} & 1 & \binom{n}{1} & \cdots & \binom{n}{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \binom{n}{1} & \binom{n}{2} & \binom{n}{3} & \cdots & 1 \end{pmatrix} \in \mathcal{M}_n(\mathbb{Z})$$

matrisine Circulant matrisi denir.

Tanım 3.12. Circulant matrisi $\mathcal{C}(n)$ nin determinantına Wendt determinantı denir.

Örnek 3.13. $n = 2$ için $2 \not\equiv 0 \pmod 6$ olduğundan Tanım 3.10. dan

$$\rho_2 = R(x^2 - 1, (x+1)^2 - 1)$$

elde edilir. O halde $f(x) = x^2 - 1$ in katsayıları $[-1, 0, 1]$, $g(x) = (x+1)^2 - 1 = x^2 + 2x$ nin katsayıları $[0, 2, 1]$ elde edilir. Sylvester matrisi

$$Syl(f, g) = \begin{pmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 1 \end{pmatrix}$$

olur. Bu matrisin determinantı -3 tür. Böylece $\rho_2 = -3$ tür.
$n = 6$ için $6 \equiv 0 \pmod 6$ olduğundan Tanım 3.10. ve Lemma 3.9. un ikinci durumu kullanılarak $\Phi_3(x) = x^2 + x + 1$ olmak üzere

$$\rho_6 = R\left(\frac{x^6 - 1}{\Phi_3}, \frac{(x+1)^6 - 1}{\Phi_3}\right) = -2^2 \cdot 3 \cdot 7^3$$

elde edilir. Böylece uzun bölme işlemi yapmak yerine Circulant matris kuralı kullanılarak

$$\mathcal{C}(6) = \begin{pmatrix} 1 & 6 & 15 & 20 & 15 & 6 \\ 6 & 1 & 6 & 15 & 20 & 15 \\ 15 & 6 & 1 & 6 & 15 & 20 \\ 20 & 15 & 6 & 1 & 6 & 15 \\ 15 & 20 & 15 & 6 & 1 & 6 \\ 6 & 15 & 20 & 15 & 6 & 1 \end{pmatrix}$$

elde edilir. Wendt determinant kuralından $det(\mathcal{C}(6)) = 0$ bulunur.

Önerme 3.14. $n \not\equiv 0 \pmod 6$ için ρ_n değişmezi Wendt determinantıdır. Ayrıca $\mathcal{C}(n)$, Circulant matris olmak üzere

$$det(\mathcal{C}(n)) = 0 \text{ olması için gerek ve yeter şart } n \equiv 0 \pmod 6$$

olmasıdır.

İspat: Fermat'ın Son Teoremi ile ilişkili olarak E. Wendt, [24] çalışmasında birinci satır binom katsayılarından oluşacak şekilde Circulant matris $\mathcal{C}(n)$ yi tanımladı. Wendt, $\mathcal{C}(n)$ matrisinin determinantının $R(x^n - 1, (x+1)^n - 1)$ e eşit olduğunu gösterdi. E. Lehmer, [12] çalışmasında $det(\mathcal{C}(n)) = 0$ olması için gerek ve yeter şartın $n \equiv 0 \pmod 6$ olması gerektiğini ispatladı.

$n \not\equiv 0 \pmod 6$ için yukarıda tanımlanan ρ_n literatürde incelenen benzer aritmetik değişmezlerle ilişkilidir. İlk on sayı ve bunların asal çarpanları aşağıda listelenmiştir.

Tablo 3.1. Bazı n değerleri için ρ_n ve asal çarpanları.

n	ρ_n	Asal çarpanlar
1	1	1
2	-3	-3
3	28	$2^2 \cdot 7$
4	-375	$-3 \cdot 5^3$
5	3751	$11^2 \cdot 31$
7	6 835 648	$2^6 \cdot 29^2 \cdot 127$
8	$-1\,343\,091\,375$	$-3^7 \cdot 5^3 \cdot 17^3$
9	364 668 913 756	$2^2 \cdot 7 \cdot 19^4 \cdot 37^2 \cdot 73$
10	$-210\,736\,858\,987\,743$	$-3 \cdot 11^9 \cdot 31^3$
11	101 832 157 445 630 503	$23^5 \cdot 67^2 \cdot 89 \cdot 199^2$

$n \equiv 0 \pmod 6$ durumu için sıralama mevcut değildir. Bu durumdaki bazı sayılar ve asal çarpanları aşağıda verilmiştir.

Tablo 3.2. Bazı $n \equiv 0 \pmod 6$ değerleri için ρ_n ve asal çarpanları.

n	ρ_n
6	$-2^2 \cdot 3 \cdot 7^3$
12	$-2^{10} \cdot 3 \cdot 5^3 \cdot 7^3 \cdot 13^9$
18	$-2^2 \cdot 3^{12} \cdot 7^3 \cdot 19^{15} \cdot 37^6 \cdot 73^3$
24	$-2^{30} \cdot 3^{31} \cdot 5^{21} \cdot 7^9 \cdot 13^9 \cdot 17^3 \cdot 73^6 \cdot 241^3$
30	$-2^{50} \cdot 3 \cdot 5^8 \cdot 7^3 \cdot 11^9 \cdot 31^{27} \cdot 61^{12} \cdot 151^3 \cdot 271^6 \cdot 331^3$
36	$-2^{10} \cdot 3^{12} \cdot 5^3 \cdot 7^3 \cdot 13^9 \cdot 17^6 \cdot 19^{15} \cdot 37^{33} \cdot 73^{15} \cdot 109^9 \cdot 181^6 \cdot 757^6$

Lemma 3.15. $m \mid n$ olacak şekilde m ve n pozitif tamsayılar olsun. O zaman $\mathbb{Z}$ de $\rho_m \mid \rho_n$ dir.

İspat:

1. Durum: $6 \nmid n$ olduğu kabul edilsin. O zaman $6 \nmid m$ dir. $\mathbb{Z}$ de $m \mid n$ olduğu için $\mathbb{Z}[x]$ de $(x^m - 1) \mid (x^n - 1)$ dir. O zaman $((x+1)^m - 1) \mid ((x+1)^n - 1)$ olur ve resultantların çarpım özelliği kullanılarak

$$\rho_m = R(x^m - 1, (x+1)^m - 1) \mid R(x^n - 1, (x+1)^n - 1) = \rho_n$$

elde edilir.
2. Durum: $6 \mid n$ ve $6 \mid m$ kabul edilsin. O zaman Φ_3, 3. dereceden Sayklotomik polinom olmak üzere $\mathbb{Z}[x]$ de $\frac{x^m-1}{\Phi_3} \mid \frac{x^n-1}{\Phi_3}$ ve $\frac{(x+1)^m-1}{\Phi_3} \mid \frac{(x+1)^n-1}{\Phi_3}$ elde edilir. Böylece $\rho_m \mid \rho_n$ dir.
3. Durum: $6 \mid n$ ve $6 \nmid m$ olsun. O zaman $\Phi_3 \nmid (x^m-1)$ ve $\Phi_3 \nmid ((x+1)^m-1)$, $\Phi_3 \mid (x^n-1)$ ve $\Phi_3 \mid ((x+1)^n-1)$ dir. O halde $(x^m-1) \mid \frac{x^n-1}{\Phi_3}$ ve $((x+1)^m-1) \mid \frac{(x+1)^n-1}{\Phi_3}$ olur. Böylece $\rho_m \mid \rho_n$ dir.

Örnek 3.16. $m = 2$ ve $n = 4$ olsun.
Tanım 3.10. gereği $n \not\equiv 0 \pmod 6$ olduğunda $R(x^n-1, (x+1)^n-1)$ alınır. Böylece

$$\begin{aligned}\rho_2 &= R(x^2-1,\ (x+1)^2-1) = R((x-1)(x+1),\ x^2+2x) = -3\\ \rho_4 &= R((x^4-1,\ (x+1)^4-1)\\ &= R\left((x^2-1)(x^2+1),\ x(x+2)(x^2+2x+2)\right) = -375\end{aligned}$$

sonuçları elde edilir. $-3 \mid -375$ olduğundan $\rho_2 \mid \rho_4$ tür.

Lemma 3.17. $\mathcal{R}$, karakteristiği $p \geq 0$ olan bir cisim olsun. $\alpha \in \mathcal{R}$, x^n-1 ile $(x+1)^n-1$ polinomlarının ortak bir kökü olduğu kabul edilsin. Eğer $6 \nmid n$ ise o zaman $p \mid \rho_n$ dir. Eğer $6 \mid n$ ise o zaman $p \mid \rho_n$ veya $\Phi_3(\alpha) = 0$ dır.

İspat:
1. Durum: $6 \nmid n$ olduğu kabul edilsin. O zaman $\rho_n = u.(x^n-1) + v.((x+1)^n-1)$ olacak şeklide $u, v \in \mathbb{Z}[x]$ polinomları vardır. x yerine α yazıldığında $\mathcal{R}$ de $\rho_n.\alpha = 0$ ifadesi elde edilir. Böylece $p \mid \rho_n$ olur.
2. Durum: $6 \mid n$ koşulu kabul edilsin. O zaman $\rho_n.\Phi_3 = u.(x^n-1) + v.((x+1)^n-1)$ olacak şekilde $u, v \in \mathbb{Z}[x]$ polinomları vardır ve α, x yerine yazıldığında $\mathcal{R}$ de $\rho_n.\Phi_3(\alpha) = 0$ ifadesi elde edilir. Böylece $p \mid \rho_n$ veya $\Phi_3(\alpha) = 0$ dır.

Tanım 3.18. $r \in \mathbb{Z}[x]$, başkatsayısı $a \in \mathbb{Z}$ ve derecesi s olan sıfırdan farklı bir polinom olsun. $\delta(r)$ değişmezi, $s = 0$ için $\delta(r) = r$ ve $s \geq 1$ için $\lambda_1, \ldots, \lambda_l$ çarpanları ile $\overline{\mathbb{Q}}$ ($\mathbb{Q}$ nun cebirsel kapanışı) de r nin farklı kökleri $m_1, \ldots, m_l$ ve $m = \max\{m_1, \ldots, m_l\}$ olmak üzere

$$\delta(r) = a^{1+2s^2}.(m-1)!. \prod_{\substack{1 \leq i,j \leq l \\ i \neq j}} (\lambda_i - \lambda_j)^m$$

olarak tanımlanır.

Örnek 3.19. $r = x^n - 1$ olsun. O halde $\delta(r)$, r nin genel diskriminantı ile çelişir ve w, birimin $n.$ ilkel kökü olmak üzere

$$\delta(r) = Disc(x^n - 1) = \left(\prod_{1 \le i < j \le n} (w^i - w^j) \right)^2 = (-1)^{\frac{n(n-1)}{2}} \cdot (-1)^{n-1} \cdot n^n$$

dir.

Tanım 3.20. $r \in \mathbb{Z}[x]$, başkatsayısı $a \in \mathbb{Z}$ ve derecesi s olan sıfırdan farklı bir polinom olsun. $\sigma(r)$ değişmezi, $s = 0$ için $\sigma(a) = 1$ ve $s \ge 1$ için $\lambda_1, \ldots, \lambda_l$ çarpanları ile $\overline{\mathbb{Q}}$ de r nin farklı kökleri $m_1, \ldots, m_l$ olmak üzere

$$\sigma(r) = a^{2s^3} \prod_{\substack{1 \le i,j \le l \\ a(\lambda_i + \lambda_j) \ne 0}} r(\lambda_i + \lambda_j) = a^{2s^3} \prod_{\substack{1 \le i,j,k \le l \\ r(\lambda_i + \lambda_j) \ne 0}} r(\lambda_i + \lambda_j - \lambda_k)^{m_k}$$

dır.

Önerme 3.21. $r = x^n - 1$ olsun. O zaman $\sigma(r)$ tamsayısı

$$\sigma(r) = \begin{cases} (-1)^n \rho_n^n, & \text{eğer } n \not\equiv 0 \pmod 6, \\ \left(\frac{n^2 \rho_n}{3} \right)^n, & \text{eğer } n \equiv 0 \pmod 6 \end{cases}$$

şeklindedir.

İspat: w, birimin $n.$ ilkel kökü olsun. O halde

$$r(x) = x^n - 1 = \prod_{i=0}^{n-1} (x - w^i)$$

olur.

1. Durum: $6 \nmid n$ olsun.

Sonuç 3.3. e göre iki $n.$ kökün toplamı tekrar bir $n.$ kök değildir. Bu nedenle Tanım 3.20. den

$$\sigma(r) = \prod_{i,j=0}^{n-1} ((w^i + w^j)^n - 1)$$

elde edilir.

Şimdi

$$w^i + w^j = w^j (w^{i-j} + 1)$$

ve $(w^j)^n = 1$ olduğundan

$$(w^i + w^j)^n = (w^j)^n(w^{i-j} + 1)^n = (w^{i-j} + 1)^n$$

eşitliği sağlanır. Böylece

$$\sigma(r) = \prod_{i,j=0}^{n-1}((w^{i-j} + 1)^n - 1)$$

olur.

Burada $k = i - j \pmod{n}$ alınırsa, her $k \in \{0, 1, \ldots, n-1\}$ değeri tam olarak n kez ortaya çıkar. Dolayısıyla

$$\sigma(r) = \prod_{k=0}^{n-1}((w^k + 1)^n - 1)^n$$

elde edilir.

Resultant tanımından

$$R((x+1)^n - 1, x^n - 1) = \prod_{k=0}^{n-1}((w^k + 1)^n - 1)$$

olduğundan

$$\sigma(r) = (R((x+1)^n - 1, x^n - 1))^n$$

yazılır.

Tanım 3.10. a göre $6 \nmid n$ durumunda

$$\rho_n = R(x^n - 1, (x+1)^n - 1)$$

dir. Resultantın simetri özelliğinden

$$R((x+1)^n - 1, x^n - 1) = (-1)^{n^2}\rho_n = (-1)^n\rho_n$$

olur. Böylece

$$\sigma(r) = ((-1)^n\rho_n)^n = (-1)^{n^2}\rho_n^n = (-1)^n\rho_n^n$$

elde edilir.

2. Durum: $6 \mid n$ olsun.

Lemma 3.9. a göre $x^n - 1$ ile $(x+1)^n - 1$ polinomlarının ortak böleni

$$\Phi_3 = x^2 + x + 1$$

dir.

Ayrıca iki n. kökün toplamının tekrar bir n. kök olması ancak bu köklerin oranının birimin 3. ilkel kökü olması durumunda mümkündür. Bu nedenle Tanım 3.20. den

$$\sigma(r) = \prod_{\Phi_3(w^k)\neq 0} ((w^k+1)^n - 1)^n$$

elde edilir.

Bu ifade resultant yardımıyla

$$\sigma(r) = \left(R\left((x+1)^n - 1, \frac{x^n-1}{\Phi_3} \right) \right)^n$$

şeklinde yazılır.

Resultantın çarpım özelliği kullanılırsa

$$R((x+1)^n - 1, x^n - 1) = R((x+1)^n - 1, \Phi_3) R\left((x+1)^n - 1, \frac{x^n-1}{\Phi_3} \right)$$

olur. Buradan

$$R\left((x+1)^n - 1, \frac{x^n-1}{\Phi_3} \right) = \frac{R((x+1)^n - 1, x^n - 1)}{R((x+1)^n - 1, \Phi_3)}$$

elde edilir.

Tanım 3.10. ve resultantın çarpım özelliği kullanılarak

$$R\left((x+1)^n - 1, \frac{x^n-1}{\Phi_3} \right) = (-1)^n \rho_n R\left(\Phi_3, \frac{x^n-1}{\Phi_3} \right)$$

elde edilir.

Şimdi

$$x^n - 1 = \prod_{t|n} \Phi_t(x)$$

olduğundan

$$R\left(\Phi_3, \frac{x^n-1}{\Phi_3} \right) = \prod_{\substack{t|n \\ t\neq 3}} R(\Phi_3, \Phi_t)$$

eşitliği elde edilir.

Apostol un Sayklotomik resultant formülüne göre ilgili durumlarda

$$R(\Phi_3, \Phi_t) = 1$$

olur; yalnızca

$$t = 1 \quad \text{ve} \quad t = 9$$

durumlarında trivial olmayan katkı elde edilir ve sonuç olarak

$$\prod_{\substack{t|n \\ t\neq 3}} R(\Phi_3, \Phi_t) = -\frac{n^2}{3}$$

şeklindedir.

Dolayısıyla

$$\sigma(r) = ((-1)^n \rho_n)^n \left(-\frac{n^2}{3}\right)^n$$

olur.

İspat tamamlanmıştır.

4. BULGULAR VE TARTIŞMA

4.1. Bir Polinom Özdeşliğini Sağlayan Bir Derivasyona Sahip Lie Cebirleri

Bu bölümde [4] çalışmasında karakteristiği sıfır olan bir cisim üzerinde periyodik derivasyona sahip Lie cebirleri ile ilgili elde edilen sonuçlar ve karakteristiği sıfır olan bir cisim üzerinde polinom özdeşliğini sağlayan derivasyona sahip Lie cebirleri incelenecektir.

K, karakteristiği sıfır olan bir cisim olsun. $\mathcal{G}$, K cismi üzerinde sonlu boyutlu bir Lie cebir olsun.

Tanım 4.1. $\mathcal{G}$, K cismi üzerinde bir Lie cebir ve d, $\mathcal{G}$ nin bir derivasyonu olsun. Eğer $d^n = id$ olacak şekilde n pozitif tamsayısı mevcut ise d ye $n.$ mertebeden periyodik derivasyon denir.

d periyodik derivasyonu $1.$ mertebeden olduğu zaman her $x, y \in \mathcal{G}$ için $[x, y] = d([x, y]) = 2[x, y]$ elde edilir. Dolayısıyla $[x, y] = 0$ eşitliğinden dolayı $\mathcal{G}$ abelyendir.

Tanım 4.2. $r \in K[x]$ bir polinom ve $d \in Der(\mathcal{G})$ olsun. Eğer $r(d) = 0$ ise o zaman d derivasyonu r ile verilen bir polinom özdeşliğini sağlayan derivasyon denir.

Özel olarak $r = x^n - 1$ polinomu, polinom özdeşliği için önemli bir örnektir. O zaman d, r ile verilen polinom özdeşliğini sağlaması için gerek ve yeter koşul d nin $n.$ mertebeden periyodik derivasyon olmasıdır, yani id birim dönüşüm olmak üzere $d^n = id$ dir.

Bir periyodik derivasyon tekil olmayandır. Bir tekil olmayan derivasyonun varlığı Lie cebir yapısı üzerinde güçlü bir etkiye sahiptir.

Teorem 4.3. [8] $\mathcal{G}$, karakteristiği sıfır olan bir cisim üzerinde tekil olmayan bir derivasyona sahip Lie cebiri olsun. O zaman $\mathcal{G}$ nilpotenttir.

Teorem 4.4. [11] $\mathcal{G}$, karakteristiği sıfır olan bir cisim üzerinde $6 \nmid n$ olacak şekilde $n.$ mertebeden periyodik derivasyona sahip bir Lie cebiri olsun. O zaman $\mathcal{G}$ abelyendir.

Önerme 4.5. $\mathcal{G}$, periyodik derivasyona sahip bir kompleks Lie cebiri olsun. O halde $\mathcal{G}$ nin nilpotent sınıfı $c(\mathcal{G}) \leq 2$ dir.

Cismin karakteristiği $p > 0$ olduğu durumlarda $\mathcal{G}$ nin nilpotentliği her zaman doğru değildir. Karakteristiği sıfırdan farklı olan cisim üzerinde periyodik derivasyona sahip nilpotent olmayan Lie cebirleri (Benkart, Kostrikin ve Kuznetsov, [3]) çalışmasında incelenmiştir.

Tanım 4.6. $\mathcal{G}$, K üzerinde sonlu boyutlu bir Lie cebiri olsun. Her $a \in \mathcal{G}$ için $ad_a : \mathcal{G} \longrightarrow \mathcal{G}$, $ad_a(b) = [a, b]$ lineer dönüşümü kendi karakteristik polinomunu sağlıyorsa yani $P_{ad_a}(ad_b) = 0$ oluyorsa bu Lie cebirine Hamilton Lie cebiri denir ve H ile gösterilir.

Tanım 4.7. K, karakteristiği $p > 0$ olan cebirsel kapalı bir cisim olsun. $\mathcal{G}$, K üzerinde sonlu boyutlu bir Lie cebiri ise $\mathcal{G}$ ye modüler Lie cebiri denir. Eğer $\mathcal{G}$ nin kendisi ve $\{0\}$ dışında başka ideali yoksa $\mathcal{G}$ ye basit modüler Lie cebiri denir.

Teorem 4.8. $\mathcal{G}$, karakteristiği $p > 7$ olan cebirsel kapalı bir cisim üzerinde basit modüler Lie cebiri olsun. O zaman aşağıdaki ifadeler birbirine denktir.
(i) $\mathcal{G},$ bir periyodik derivasyonu sağlar.
(ii) $\mathcal{G},$ tekil olmayan bir derivasyonu sağlar.
(iii) $\mathcal{G},$ (Benkart, [3]) çalışmasında yer alan özel Lie cebir $S(m; n, w_2)$ ya da Hamilton Lie cebiri $H(m; n, w_2)$ yi sağlar.

Teorem 4.9. $\mathcal{G}$, karakteristiği $p \geq 0$ olan K cismi üzerinde $n.$ mertebeden $p \nmid \rho_n$ olacak şekilde d periyodik derivasyonunu sağlayan bir Lie cebir olsun. O zaman $\mathcal{G}$ nin nilpotent sınıfı

$$c(\mathcal{G}) \leq \begin{cases} 1, & \text{eğer } n \not\equiv 0 \pmod 6, \\ 2, & \text{eğer } n \equiv 0 \pmod 6 \end{cases}$$

dır.

İspat: Nilpotentlik sınıfı skalerlerin genişlemesi altında korunduğundan dolayı K cebirsel kapalı kabul edilsin. Ayrıca, bir M yarı basit derivasyonu mevcut olur. $p = 0$ için $M = d$ dir. Eğer $p > 0$ ise $p^k | n$ ve $obeb(p, m) = 1$ ile $m = \frac{n}{p^k}$ olacak şekilde bir $k \geq 0$ tamsayısı mevcuttur. $M = d^{p^k}$ olsun. O zaman $M^m = d^{(m.p^k)} = d^n = 1$ olduğundan dolayı $m \mid n$ olacak şekilde M, m mertebeli bir periyodik derivasyondur. M, m mertebeli ve $obeb(p, m) = 1$ olduğundan dolayı M yarı basittir. K cebirsel kapalı olduğundan dolayı $\mathcal{G}$ için M ye bağlı bir özbaz bulunabilir. Bütün λ özdeğerleri $\lambda^m = 1$ koşulunu sağlar.
1. Durum: $6 \nmid m.$ $\mathcal{G}$, abelyen olmadığı kabul edilsin. O zaman $[a, b] \neq 0$ olacak şekilde özdeğerleri α, β olan özvektörleri $a, b \in \mathcal{G}$ vardır. $d(a) = \alpha a$, $d(b) = \beta b$ olsun. Dolayısıyla

$$\begin{aligned} d([a, b]) &= [d(a), b] + [a, d(b)] \\ &= [\alpha a, b] + [a, \beta b] \\ &= \alpha[a, b] + \beta[a, b] \\ &= (\alpha + \beta)[a, b] \end{aligned}$$

elde edilir. Böylece $[a, b]$, özdeğerleri $\alpha + \beta$ olan bir özvektör olduğunu görmek kolaydır. Buradan $\alpha^m = \beta^m = (\alpha+\beta)^m = 1$ bulunur. Böylece $\frac{\alpha}{\beta}$, x^m-1 ve $(x+1)^m-1$ polinomlarının ortak kökü olur. $p \mid \rho_m$ sonucuna ulaşılır. Ayrıca $m \mid n$ olduğundan Lemma 3.15. e göre

$\rho_m \mid \rho_n$ olur. Dolayısıyla $\rho \mid \rho_n$ elde edilir. Bu ise $\rho \nmid \rho_n$ kabul ile çelişmektedir. Sonuç olarak $\mathcal{G}$ abelyendir.

2. Durum: $6 \mid m$. O zaman Lemma 3.15. e göre $\rho_2 = 3$ ve $\rho_3 = 2^2.7$, ρ_m yi böler, dolayısıyla $6 \mid \rho_m$ elde edilir. Böylece kabulden dolayı $p > 3$ olur. $[[\mathcal{G}, \mathcal{G}], \mathcal{G}] \neq 0$ olduğu kabul edilsin. O zaman $[[a, b], c] \neq 0$ olacak şekilde özdeğerleri α, β, γ olan a, b, c özvektörleri vardır. $d(a) = \alpha a$, $d(b) = \beta b$, $d(c) = \gamma c$ olsun. Buradan $[x, y]$ özdeğeri $\alpha + \beta$ olan bir özvektördür. Ayrıca

$$\begin{aligned} d([[a, b], c]) &= [d([a, b]), c] + [[a, b], d(c)] \\ &= [(\alpha + \beta)[[a, b], c] + [[a, b], \gamma z] \\ &= (\alpha + \beta)[[a, b], c] + \gamma[[a, b], c] \\ &= (\alpha + \beta + \gamma)[[a, b], c] \end{aligned}$$

eşitliğinden $[[a, b], c]$ özvektörünün özdeğeri $\alpha + \beta + \gamma$ olarak bulunur. Jacobi özdeşliğinden yararlanarak da $[c, a]$ nın $\alpha + \gamma$ özdeğerlerine sahip özvektör olduğu görülür. O zaman $\frac{\alpha}{\beta}$, $\frac{\alpha}{\gamma}$ ve $\frac{\alpha+\beta}{\gamma}$ oranları $x^m - 1$ ve $(x + 1)^m - 1$ polinomlarının ortak kökleridir. Lemma 3.15. ten Φ_3 polinomunun kökleridir. Böylece bunların mertebesi 1 veya 3 olur. Fakat $p > 3$ olduğundan dolayı mertebe her zaman 3 olmalıdır. $w \in K$ mertebesi 3 olan bir eleman olsun. O zaman $\beta = \alpha w^i$, $\gamma = \alpha w^j$ ve $\alpha + \beta = \gamma w^k$ olacak şekilde $1 \leq i, j, k \leq 2$ vardır. Bu eşitlikler yerine konulduğunda

$$\alpha + \alpha w^i = (\alpha w^j) w^k = \alpha w^{j+k}$$

elde edilir. Her iki taraf α^{-1} ile çarpıldığında

$$1 + w^i - w^{j+k} = 0$$

bulunur. Böylece w, $1 + x + x^2$ ile $1 + x^i - x^{j+k}$ polinomlarının ortak bir köküdür. Bu iki polinomun resultantının K da sıfır olduğu anlamına gelir. Böylece

$$p \mid R(1 + x + x^2,\ 1 + x^i - x^{j+k})$$

olmalıdır. Bu resultant tüm i, j, k için $(1, 1, 1)$ veya $(2, 2, 2)$ olmadığı sürece 1 e eşittir. $(i, j, k) = (1, 1, 1)$ ve $(i, j, k) = (2, 2, 2)$ durumlarında 4 tür. Gerçekten de $f(x) = 1 + x + x^2$ polinomunun kökleri w ve w^2 dir. Ayrıca $f(x)$ monik polinom ve $R(f, g) = g(w).g(w^2)$ dir. $g(x) = 1 + x^i + x^{j+k}$ olduğundan dolayı $g(w) = 1 + w^i - w^{j+k}$, $g(w^2) = 1 + w^{2i} - w^{2(j+k)}$ olur. Resultant tanımından dolayı $R(1 + x + x^2,\ 1 + x^i - x^{j+k}) = 1 + w + w^2 + w^3$ sonucuna ulaşılır. Hesaplamalar yapılırken $w^3 = 1$ ve $w^2 + w = -1$ eşitliklerinden yararlanılacaktır.
(i) $(i, j, k) = (1, 2, 2)$ için

$$g(x) = 1 + x^1 - x^{2+2} = 1 + x - x^4 = 1 + x - x = 1$$

$R(f,g) = 1.1 = 1$ dir.
(ii) $(i,j,k) = (1,1,2)$ için

$$g(x) = 1 + x^1 - x^{1+2} = 1 + x - x^3 = 1 + x - 1 = x$$

$R(f,g) = w.w^2 = w^3 = 1$ dir.
(iii) $(i,j,k) = (2,2,2)$ için

$$g(x) = 1 + x^2 - x^{2+2} = 1 + x^2 - x^4 = 1 + x^2 - x = x$$

$R(f,g) = 1 - (-3) = 4$ tür.
(iv) $(i,j,k) = (2,1,1)$ için

$$g(x) = 1 + x^2 - x^{1+1} = 1 + x^2 - x^2 = 1$$

$R(f,g) = 1.1 = 1$ dir.
(v) $(i,j,k) = (1,1,1)$ için

$$g(x) = 1 + x^1 - x^{1+1} = 1 + x^1 - x^2 = 1$$

$R(f,g) = 1 - (-3) = 4$ tür.
$p = 2$ olduğundan dolayı bu bir çelişkidir. Dolayısıyla $c(\mathcal{G}) \leq 2$ dir.
Eğer $6 \nmid n$ ise $6 \nmid m$ de olur, böylece 1. durumdan $c(\mathcal{G}) \leq 1$ elde edilir.

Uyarı 4.10. $p = 0$ için ρ_n sıfırdan farklı olduğundan dolayı teoremdeki $p \nmid \rho_n$ varsayımı her zaman sağlanır. Bu sonuç, Önerme 4.5. i kompleks sayılardan karakteristiği sıfır olan herhangi bir cisme genelleştirilebilir. $p > 0$ durumunda $p \mid \rho_n$ olduğundan teoremden herhangi bir sonuç çıkarılamaz. Gerçekten de bazı n ve p değerleri için $p \mid \rho_n$ ile n mertebeli periyodik derivasyona sahip hem nilpotent olan hem de nilpotent olmayan Lie cebirleri vardır.

Tanım 4.11. Eğer p asal sayısı için $k = p^r$ ise $\mathbb{F}_k$ cismi üzerinde $W(1:k) = \langle e_\alpha : \alpha \in \mathbb{F}_k \rangle$ vektör uzayı, $[e_\alpha, e_\beta] = (\beta - \alpha)e_{\alpha+\beta}$ şeklindeki bilineer çarpım ile bir Lie cebiri yapısı oluşturur. Bu cebir yapısına Zassenhaus Lie cebir denir.

Örnek 4.12. $\mathcal{G} = W(1;m)$, $\mathbb{F}_2$ cismi üzerinde boyutu $2^m - 1$ olan Zassenhaus Lie cebir olsun. Bu cebirin mertebesi $(2^m - 1)$ sahip olduğu [2] çalışmasında gösterildi. Her $m \geq 2$ için $2 \mid \rho_{(2^m-1)}$ dir, böylece Teorem 4.9. dan herhangi bir sonuç elde edilemez. Bu durumda $\mathcal{G}$ basittir ve dolayısıyla nilpotent değildir.

Örnek 4.13. $\mathcal{G}$, $\mathbb{F}_3$ cismi üzerinde üç üreteçli ve nilpotentlik sınıfı 2 olan serbest nilpotent Lie cebiri olsun. Bu cebir mertebesi 6 olan bir periyodik derivasyona sahiptir. $3 \mid \rho_6$ olduğundan

dolayı Teorem 4.9. doğrudan uygulanamaz; fakat yine de bu durum sonucu etkilemez. Gerçekten $\mathcal{G}$ nin nilpotent sınıfı 2 dir.

Uyarı 4.14. Teorem 4.9., periyodik derivasyonlardan herhangi bir polinom özdeşliğini sağlayan derivasyonlara genelleştirilebilir. Bunun için [14, 15] deki yöntemler ve sonuçlar kullanılır. Burada [14] te tanımlandığı şekliyle genelleştirilmiş Higman dönüşümü kullanılmaktadır.

Tanım 4.15. X, $(\mathcal{T},+)$ alt kümesi olsun. Eğer X, $x,a \in X$ için $x, x+a, x+2a, \ldots$ formunda herhangi bir aritmetik işlem içermiyorsa aritmetik serbest olarak adlandırılır.

Tanım 4.16. $H_a(1,c)=1$, $H_a(b,0)=1$ sınır koşulları ve $b>1$, $c>0$ için

$$H_a(b,c) = max\{a.f(c, a+H_a(b-1, a.f(c-1, H_a(b,c-1))))+1, H_a(b-1,c), H_a(b,c-1)\}$$

olacak şekilde $H : \mathbb{N}\times\mathbb{N}\times\mathbb{N}_0 \longrightarrow \mathbb{N},\ (a,b,c) \longmapsto H_a(b,c)$ şeklinde tanımlansın. Özel olarak
(i) H: $\mathbb{N}\times\mathbb{N}_0 \longrightarrow \mathbb{N},\ (m,n) \longmapsto H_m(m,n)$ ve
(ii) H: $\mathbb{N} \longrightarrow \mathbb{N},\ n \longmapsto H_n(n,n) = H(n,n)$
dönüşümleri elde edilir. Buna genelleştirilmiş Higman dönüşümü denir.

Tanım 4.17. $r \in K[x]$ bir polinom olsun. r, $K[x]$ de x^m-1 i bölecek şekilde bir m pozitif tamsayısı mevcut ise bu m minimal pozitif tamsayısına r nin periyodu denir ve $per(r)$ ile ifade edilir. $K=\mathbb{F}_p$ için P_p ve B_p kümeleri
$P_p = \{\ per(h(x^p-1)) \mid h \in \mathbb{F}_p[t],\ h(0)\neq 0,\ der(h)\geq 1\}, \qquad B_p = \mathbb{N}.P_p$
şeklinde tanımlanır.

$\mathbb{F}_p[x]$ halkasında bir polinom r nin periyoda sahip olması için gerek ve gerek koşul $r(0)\neq 0$ olmasıyla mümkündür.

Örnek 4.18. Her p asal ve $k\geq 2$ için $p^k-1 \in P_p$ dir.

$$h(x) = 1 + x^{p-1} + x^{p^2-1} + x^{p^3-1} + \ldots + x^{p^{k-1}-1} \in \mathbb{F}_p[x]$$

olsun. $h(x)$, x^{-1} ortak paranteze alınarak

$$h(x) = 1 + x^{p-1} + x^{p^2-1} + \ldots + x^{p^{k-1}-1} = x^{-1}(x + x^p + x^{p^2} + \ldots + x^{p^{k-1}})$$

şeklinde ifade edilir. $S(x) = x + x^p + x^{p^2} + \ldots + x^{p^{k-1}}$ olsun. O zaman

$$x^{p^k} - x^p = (x^p - x)(x + x^p + \ldots + x^{p^{k-1}})$$

elde edilir. Ayrıca

$$x^{p^k} - x^p = (x^p - x)S(x) = (x^p - x)x\,h(x)$$

dolayısıyla her iki taraf x ile bölünerek

$$x^{p^k-1} - x^{p-1} = (x^p - x)h(x)$$

elde edilir. Böylece

$$h(x) = \frac{x^{p^k-1} - x^{p-1}}{x^p - x}$$

sonucuna ulaşılır. Sadeleştirildiğinde $h(x) = 1 + x^{p-1} + \ldots + x^{p^{k-1}-1}$ bulunur. Sonuç olarak $per\big(h(x)(x^p-1)\big) = p^k - 1$ olduğu ve dolayısıyla $p^k - 1 \in P_p$ olduğu görülür.

Düşük dereceli indirgenemez polinomlar $h(x) \in \mathbb{F}_p[x]$ için $h(x)(x^p - x)$ ifadelerinin periyotları hesaplanarak P_p kümesinde yer alan çeşitli elemanlar elde edilir.

Örnek 4.19. $p = 2$ ve $k = 3$ olsun. $h(x) = 1 + x^{2-1} + x^{2^2-1} = 1 + x + x^3$ ve $S(x) = x + x^2 + x^4 = x \cdot h(x)$ olur. O zaman $(x^2 - x)^3 = x^6 + x^5 + x^4 + x^3$ elde edilir. Buradan $h(x^2-x) = 1+(x^2-x)+(x^2-x)^3 = 1+x+x^2+x^3+x^4+x^5+x^6$ dır. $h(x^2-x) = \frac{x^7-1}{x-1}$ eşitliğinden periyodun 7 olduğu görülmektedir. $per(h(x^2 - x)) = 7 = 2^3 - 1$ dir. Böylece $2^3 - 1 \in P_2$ dir.

Örnek 4.20. $p = 3$ ve $k = 2$ olsun. $h(x) = 1 + x^{3-1} = 1 + x^2$ ve $S(x) = x + x^3 = x \cdot h(x)$ olur. Buradan $h(x^3 - x) = 1 + (x^3 - x)^2 = 1 + x^2 + x^4 + x^6$ eşitliği elde edilir. Ayrıca $(x^2 - 1)(1 + x^2 + x^4 + x^6) = x^8 - 1$ eşitliğinden periyodun 8 olduğu görülmektedir. $per(h(x^3 - x)) = 8 = 3^2 - 1$ dir. Böylece $3^2 - 1 \in P_3$ tür.

Örnek 4.21. $3, 7, 31, 73, 85, 127 \in P_2$ olsun. Aşağıdaki tabloda $p = 2$ için

Tablo 4.1. Polinomlara göre $h(x)(x^2 - x)$ ifadelerinin periyotları

$h(x)$	$per(h(x)(x^2 - x))$
$x + 1$	3
$x^3 + x + 1$	7
$x^4 + x^3 + x^2 + x + 1$	85
$x^5 + x^2 + 1$	31
$x^7 + x + 1$	127
$x^9 + x^4 + x^2 + x + 1$	73

bu sonuçlar elde edilir.

$r = x^n - 1$, $\mathbb{F}_p[x]$ için kök kümesine dair aşağıdaki sonuç ortaya çıkar. Bu sonuç [12] çalışmasının 4. Bölümünde dolaylı olarak belirtilmiştir.

Önerme 4.22. p bir asal sayı ve n pozitif bir tamsayı olsun. O zaman aşağıdaki ifadeler birbirine denktir.
(i) $X_{n,p} = \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^n = 1\}$
(ii) $\mathbb{F}_p[x]$ de $h_{n,p} = obeb(x^n - 1, (x+1)^n - 1, \ldots, (x+p-1)^n - 1) = 1$ dir.
(iii) $n \notin B_p$ dir.

İspat: (ii) $\Rightarrow$ (i) $X_{n,p}$ aritmetik serbest olmadığı kabul edilsin. $\alpha^n = (\alpha+\beta)^n = \ldots = (\alpha + (p-1)\beta)^n$ elemanlarının hepsi $X_{n,p}$ içerisinde olacak şekilde $X_{n,p}$ nin α, $\beta \neq 0$ elemanları vardır. Kısaca her $k = 0, 1, \ldots, p-1$ için $(\alpha + k\beta)^n = 1$ dir. $\gamma = \frac{\alpha}{\beta}$ olsun. $\gamma^n = (\frac{\alpha}{\beta})^n = \frac{\alpha^n}{\beta^n} = 1$ olur. Yani $\gamma \in X_{n,p}$ dir. Elde edilen eşitliklerden $(\alpha + k\beta) = 1$ deki ifadeleri $((\alpha + k)\beta)^n = 1$ şeklinde de yazılır. Buradan $\beta^n = 1$ olduğu için $(\alpha + k)^n = 1$ dir. $x^n - 1, (x+1)^n - 1, \ldots, (x + (p-1))^n - 1$ polinomlarının ortak kökü γ dır. Tüm polinomların ortak kökü olduğundan dolayı ortak bölenlerinin en büyüğü 1 olmaz. Yani $h_{n,p} \neq 1$ dir. Kabulden dolayı $h_{n,p} = 1$ fakat bu bir çelişkidir. Dolayısıyla $X_{n,p}$ aritmetik serbesttir.

(i) $\Rightarrow$ (ii) $h_{n,p} \neq 1$ olsun. $\gamma \in \overline{\mathbb{F}_p}[x]$ olduğundan dolayı $x^n - 1, (x+1)^n - 1, \ldots, (x + (p-1))^n - 1$ polinomlarının ortak köküdür. Yani $\gamma^n = (\gamma+1)^n = \ldots = (\gamma + (p-1))^n = 1$ dir. $\alpha = \beta = 1$ olsun. O zaman her $k = 0, 1, \ldots, p-1$ için $\gamma, \gamma+1, \gamma+2, \ldots, \gamma+(p-1)$ elemanları $X_{n,p}$ kümesindedir. Bu elemanlar $(\overline{\mathbb{F}_p}, +)$ kümesi içerisinde aritmetik dizi oluşturur. Dolayısıyla $X_{n,p}$ aritmetik serbest değildir.

(ii) $\Rightarrow$ (iii) $n \in B_p$ olsun. $h \in \mathbb{F}_p[x]$ olacak şekilde $h(0) \neq 0$, $der(h) \geq 1$ ve bir m için $n \mid m = per(h(x^p - x))$ bir polinom seçilebilir. Böylece $x^n - 1 \mid h(x^p - 1))$ dir. Fermat küçük teoremi gereği $(a+b)^p = a^p + b^p \pmod p$ ve $\mathbb{F}_p$ de $b^n = b$ dir. Bu nedenle her $l \in \mathbb{F}_p$ için $(x+l)^p - (x+l) = x^p - x$ doğrudur. Bu eşitlikte $h(x^p - x)$ yeniden yazılırsa $h(x^p - x) = h((x+l)^p - (x+l))$ elde edilir. Buradan $(x^n - 1) \mid h(x^p - x)$ olduğundan dolayı her $l = 0, 1, \ldots, p-1$ için $((x+l)^n - 1) \mid h(x^p - x)$ olur. $h(x^p - x)$ aynı anda $x^n - 1, (x+1)^n - 1, \ldots, (x+p-1)^n - 1$ polinomlarının her birini böler. Böylece $h(x^p - x)$ bu polinomların ortak kökü olan $h_{n,p}$ yi böler.

(iii) $\Rightarrow$ (ii) $h_{n,p} \neq 1$ olsun. Polinomlar tanımı $H_i \in \mathbb{F}_p[x]$ de $i \geq 1$ için

$$H_i = obeb(H_{i-1}(x), H_{i-1}(x+1)) \text{ ve } H_0 = x^n - 1$$

dir. O zaman her $k \in \mathbb{F}_p$ için $H_{i-1}(x+k), H_{i-1}(x+k+1))$ dir. Her $i \geq 0$ için

$$\begin{aligned} h_{n,p} &= obeb(H_i(x), H_i(x+1), \ldots, H_i(x+p-1)) \\ &= obeb(H_{i+1}(x), H_{i+1}(x+1), \ldots, H_{i+1}(x+p-1)) \end{aligned}$$

dir. Ayrıca her $i \geq 0$ için $der(H_i) \geq der(H_{i+1})$ öyle ki $l \geq 1$ olacak şekilde $der(H_l) \geq der(H_{l+1})$ vardır. $H_l(x)$ ve $H_l(x+1)$ aynı dereceye sahip monik polinomlar olup bunların ortak bölenlerinin en büyüğü ile de aynı dereceye sahip olduklarından $H_l(x) = H_{l+1}(x) = H_l(x+1)$ sonucuna varılır. Buna bağlı olarak $H_l(x), H_{l+1}(x+1), \ldots, H_l(x+p-1)$ dolayısıyla

$$h_{n,p}(x), h_{n,p}(x+1), \ldots, h_{n,p}(x+p-1)$$

dir. Böylece $h_{n,p}$ bazı $h \in \mathbb{F}_p[x]$ polinomu için $h(x^p - x)$ biçimindedir. $h_{n,p}$, $x^n - 1$ polinomunu böldüğünden $h_{n,p}(0) \neq 0$ olur ve dolayısıyla $h(0) \neq 0$ elde edilir. $h_{n,p}(0) \neq 1$ olduğu varsayıldığında h sabit olmayan bir polinomdur. Bu nedenle $per(h(x^p - x))$ sayısı n yi böler ve sonuç olarak $n \in B_p$ olur.

Örnek 4.23. Pozitif bir tamsayı $n \leq 12$ olacak şekilde belirlensin. Bu kadar küçük n değerleri için, hangi p asal sayıları için $n \in B_p$ eşitliğinin sağlandığı belirlenebilir. Aslında Örnek 4.21. e göre $n \in B_p$ olması $p \mid \rho_n$ olmasına eşdeğerdir. Dolayısıyla yalnızca n nin asal bölenleri olan p değerlerini

Tablo 4.2. $n \leq 12$ için ρ_n nin asal bölenleri ve $n \in B_p$ durumu

n	ρ_n nin asal bölenleri	$n \in B_p$
1	–	–
2	–	–
3	2	2
4	–	–
5	–	–
6	2	2
7	2	2
8	3	3
9	2	2
10	–	–
11	–	–
12	2	2

bu tabloda görmek mümkündür. [20] kaynağından elde edilen ilave sonuçlara göre

$$n \in B_p \text{ gerek ve yeter koşul } (n,p) \in \{(3,2),(6,2),(7,2),(8,3),(9,2),(12,2)\}$$

şeklindedir.

Dolayısıyla örneğin $2, 4, 5, 10, 11$ dereceli periyodik derivasyona sahip herhangi bir asal karakteristiği $p > 0$ için her modüler Lie cebirlerinin nilpotent olduğu bilinmektedir. $n = 3, 6, 7, 8, 9$ mertebesi için "kötü" asal sayıları $p = 2, 3$ tür. Yani n mertebeli karakteristiği $p > 0$ olan bir derivasyona sahip Lie cebiri zorunlu olarak nilpotent olmayabilir.

$p = 2$ için B_2 kümesi tamamen ρ_n cinsinden tanımlanabilir.

Örnek 4.24. $n \in B_2 \iff 2 \mid \rho_n$ dir. Karakteristiği 2 olan 3 boyutlu basit Lie cebiri $W(1;2)$, d bir derivasyon ve tüm n ile $2 \mid \rho_n$ için $d^n = id$ dür.
$W(1;2)$ nin bir bazı $\{x_1, x_2, x_3\}$ için $[x_1, x_2] = x_3$, $[x_2, x_3] = x_1$ ve $[x_1, x_3] = x_2$ olsun. $2 \mid \rho_n$ olduğu kabul edilsin. $\lambda^n = (1+\lambda)^n = 1$ olacak şekilde bir $\lambda \in \overline{\mathbb{F}}_2$ vardır. Tanım 2.25. den dolayı $d = \textit{köşeg}(1, \lambda, 1+\lambda)$ yani $d(x_1) = x_1, d(x_2) = \lambda x_2, d(x_3) = (1+\lambda)x_3$ tür. O zaman d, $d^n = id$ koşulunu sağlayan $W(1;2)$ nin bir derivasyonudur. $W(1;2)$ basit ve nilpotent olmayan bir Lie cebirdir. Bir d derivasyon var olduğu için $n \in B_2$ sonucu ortaya çıkar. Buna karşılık $n \in B_2$ yukarıdaki eşitlikten dolayı $2 \mid \rho_n$ anlamına gelmektedir.

5. SONUÇ VE ÖNERİLER

Bu çalışmada, birimin kökleri ile ilişkili aritmetik yapılar ve Lie cebirleri üzerindeki periyodik derivasyonlar sistematik olarak incelenmiştir. Üçüncü bölümde tanımlanan aritmetik değişmezler ve özellikle ρ_n, Wendt determinantı ile ilişkilendirilmiştir. $x^n - 1$ ve $(x+1)^n - 1$ polinomları arasındaki ortak kök yapısı, Sylvester matrisi ve resultant kavramları kullanılarak analiz edilmiştir. $\Phi_3(x)$ Sayklotomik polinomunun $n \equiv 0 \pmod 6$ durumunda özel etkisi vurgulanmıştır. ρ_n değişmezinin, $m \mid n$ olması durumunda $\rho_m \mid \rho_n$ olduğu gösterilmiştir. Ayrıca $\delta(r)$ ile $\sigma(r)$ değişmezleri kullanılarak polinom kökleri ve diskriminantları üzerinden yeni aritmetik ifadeler elde edilmiştir. Dördüncü bölümde ise karakteristiği sıfır ve pozitif olan cisimler üzerinde polinom özdeşliğini sağlayan derivasyonlar ve $r(x) = x^n - 1$ ile tanımlanan periyodik derivasyonlar incelenmiştir. Karakteristiği sıfır olan cisimlerde n. mertebeden periyodik derivasyona sahip Lie cebirlerinin nilpotent olduğu gösterilmiştir. Ayrıca $6 \nmid n$ koşulunu sağlayan periyodik derivasyonlara sahip Lie cebirlerinin ve kompleks Lie cebirlerinde periyodik derivasyonların nilpotent sınıfının en fazla 2 olduğu ortaya konmuştur. Pozitif karakteristiğe sahip cisimlerde ise $p \mid \rho_n$ durumunun bazı mertebelerde nilpotent olmayan Lie cebirlerine yol açabileceği, Zassenhaus ve serbest nilpotent Lie cebirleri örnekleri ile gösterilmiştir. Bu sonuçlar, periyodik ve polinom derivasyonların Lie cebirlerinin yapısal özellikleri üzerindeki etkilerini ortaya koymakta ve karakteristiğe bağlı yapısal farklılıkların sistematik olarak anlaşılmasına katkı sağlamaktadır.

KAYNAKLAR

[1] Arıkan, A., & Halıcıoğlu, S. (2021). Cebire Giriş, üçüncü baskı, Palme Yayınevi, 467 sayfa.

[2] Apostol, T. (1970). Resultants of cyclotomic polynomials, Proceedings of the American Mathematical Society, 24, 457-462.

[3] Benkart, G., Kostrikin, A. I., & Kuznetsov, M. I. (1995). Finite-dimensional simple Lie algebras with a nonsingular derivation, Journal of Algebra, 171(3), 894-916.

[4] Burde, D., & Moens, W. A. (2011). Periodic derivations and prederivations of Lie algebras, Journal of Algebra, 357, 208-221.

[5] Çevik, A. S. (2012). Soyut Cebir: Özel Konular, birinci basım, Nobel Yayınevi, 196-197, 210-212.

[6] Gezer, B., & Bizim, O. (2017). Soyut Cebir, birinci baskı, Dora Yayınevi, 662 sayfa.

[7] Govil, N. K., Rahman, Q. I., & Schmeisser, G. (1979). On the derivative of a polynomial, Illinois Journal of Mathematics, 23(2), 319-329.

[8] Jacobson, N. (1955). A note on automorphisms and derivations of Lie algebras, Proceedings of the American Mathematical Society, 6, 281-283.

[9] Judson, T. (2015). Abstract Algebra: Theory and Applications, Orthogonal Publishing, Ann Arbor, MI.

[10] Kostrikin, A. I., & Kuznetsov, M. I. (1996). Lie algebras with a nonsingular derivation, Algebra and Analysis (Kazan, 1994), de Gruyter, Berlin, 81-90.

[11] Kostrikin, A. I., & Kuznetsov, M. I. (1995). Two remarks on Lie algebras with a nonsingular derivation, Proceedings of the Steklov Institute of Mathematics, 208, 166-171.

[12] Lehmer, E. (1935). On a resultant connected with Fermat's last theorem, Bulletin of the American Mathematical Society, 41, 864-867.

[13] Mansuroğlu, N. (2022). Fundamentals of Lie Algebras, birinci basım, Gece Kitaplığı, 161 sayfa.

[14] Mattarei, S. (2002). The orders of nonsingular derivations of modular Lie algebras, Israel Journal of Mathematics, 132, 265-275.

[15] Mattarei, S. (2007). The orders of nonsingular derivations of Lie algebras of characteristic two, Israel Journal of Mathematics, 160, 23-40.

[16] Mattarei, S. (2009). A sufficient condition for a number to be the order of a nonsingular derivation of a Lie algebra, Israel Journal of Mathematics, 171, 1-14.

[17] Moens, W. A. (2017). Arithmetically-free group-gradings of Lie algebras: II, Journal of Algebra, 492, 457-474.

[18] Moens, W. A. (2020). The nilpotency of finite groups with a fixed-point-free automorphism satisfying an identity, arXiv:1810.04965v4.

[19] Parker, W. V. (1935). The degree of the highest common factor of two polynomials, American Mathematical Monthly, 42(3), 164-166.

[20] Shalev, A. (1999). The orders of nonsingular derivations, Journal of the Australian Mathematical Society Series A, 67(2), 254-260.

[21] Sylvester, J. J. (1851). On a remarkable discovery in the theory of canonical forms and of hyperdeterminants, London, Edinburgh and Dublin Philosophical Magazine and Journal of Science, 4, 391-410.

[22] Van der Waerden, B. L. (1949). Modern Algebra, Frederick Ungar Publishing Co., New York.

[23] Yaman, D., & Mansuroğlu, N. (2025). Periyodik derivasyona sahip sonlu boyutlu kompleks Lie cebirlerinin bazı özellikleri, Kırşehir Ahi Evran Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 3(1), 22-25.

[24] Wendt, E. (1894). Arithmetische Studien über den letzten Fermatschen Satz, welcher aussagt, dass die Gleichung $a^n + b^n = c^n$ für $n > 2$ in ganzen Zahlen nicht auflösbar ist, Journal für die reine und angewandte Mathematik, 113, 335-347.

[25] Woody, H. (2016). Polynomial Resultants, Department of Mathematics and Computer Science, University of Puget Sound.

EKLER

Ek 1. Kongre Katılım Belgesi

CERTIFICATE

OF PARTICIPATION

THIS CERTIFICATE IS PROUDLY PRESENTED TO

Hatice DİREMCİ NARİN

of participation in oral and technical presentation, recognition and appreciation of research contributions to
16th INTERNATIONAL MARDIN ARTUKLU SCIENTIFIC RESEARCHES CONFERENCE
held on February 8-10, 2026 / Mardin, Türkiye
with the an oral paper entitled

SOME PROPERTIES OF LIE ALGEBRAS WITH A DERIVATION SATISFYING A POLYNOMIAL IDENTITY

Prof. Dr. Salih ÖZTÜRK
Conference President

Ek 2. Kongre Katılım Belgesi

CERTIFICATE

OF PARTICIPATION

This Certificate Is Proudly Presented To

Hatice DİREMCİ NARİN

attended the 7th International Cappadocia Scientific Research Congress
held on August 02-04, 2025 / Cappadocia-Nevsehir, Türkiye, organised by IKSAD Institute
with an oral presentation entitled

SOME RESULTS ON RESULTANTS OF POLYNOMIALS

Dr. Mustafa Latif EMEK
President of IKSAD Institute

www.cappadociacongress.org
August 02-04, 2025 / Cappadocia-Nevsehir, Türkiye
7th International Cappadocia Scientific Research Congress

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER	
Adı Soyadı:	Hatice DİREMCİ NARİN
Uyruğu :	T.C.
Orcid Numarası:	0009-0008-0319-3916

EĞİTİM BİLGİLERİ	
Lisans	
Üniversite	Kırşehir Ahi Evran Üniversitesi
Fakülte	Fen Edebiyat Fakültesi
Bölüm	Matematik Bölümü
Mezuniyet Yılı	2018
Yüksek Lisans	
Üniversite	Kırşehir Ahi Evran Üniversitesi
Enstitü	Fen Bilimleri Enstitüsü
Anabilim Dalı	Matematik Anabilim Dalı
Mezuniyet Yılı	2026

Tezden Üretilen Makaleler ve Bildiriler
Diremci Narin, H. & Mansuroğlu, N. (2025). Polinomların Resultantları Üzerine Bazı Sonuçlar. 7. Uluslararası Kapadokya Kongresi, Nevşehir. (2-4 Ağustos)
Diremci Narin, H. & Mansuroğlu, N. (2026). Bir Polinom Özdeşliğini Sağlayan Bir Derivasyona Sahip Lie Cebirlerinin Bazı Özellikleri. 16. Uluslararası Mardin Artuklu Kongresi, Mardin. (8-10 Şubat)