T.C.
VAN YÜZÜNCÜ YIL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

GALOIS TEORİSİ, PALİNDROMİK POLİNOMLAR VE SIFIRLARININ BULUNUŞU İÇİN ALGORİTMALAR

YÜKSEK LİSANS TEZİ

HAZIRLAYAN: Fatma TUTAR
DANIŞMAN: Doç. Dr. Şenay BAYDAŞ

VAN-2018

T.C.
VAN YÜZÜNCÜ YIL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

GALOIS TEORİSİ, PALİNDROMİK POLİNOMLAR VE SIFIRLARININ BULUNUŞU İÇİN ALGORİTMALAR

YÜKSEK LİSANS TEZİ

HAZIRLAYAN: Fatma TUTAR

VAN-2018

KABUL VE ONAY SAYFASI

Matematik Anabilim Dalı'nda Doç. Dr. Şenay BAYDAŞ danışmanlığında, Fatma TUTAR tarafından sunulan "**Galois Teorisi, Palindromik Polinomlar ve Sıfırlarının Bulunuşu için Algoritmalar**" isimli bu çalışma Lisansüstü Eğitim ve Öğretim Yönetmeliği'nin ilgili hükümleri gereğince 07/06/2018 tarihinde aşağıdaki jüri tarafından **oy birliği** / ~~oy çokluğu~~ ile başarılı bulunmuş ve yüksek lisans tezi olarak kabul edilmiştir.

Başkan: Prof. Dr. Bülent KARAKAŞ

Üye: Doç. Dr. Şenay BAYDAŞ

Üye: Dr. Öğretim Üyesi Muhsin İNCESU

Fen Bilimleri Enstitüsü Yönetim Kurulu'nun …./..../…... tarih ve ..... sayılı kararı ile onaylanmıştır.

İmza

.....

Enstitü Müdürü

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

Fatma TUTAR

ÖZET

GALOIS TEORİSİ, PALİNDROMİK POLİNOMLAR VE SIFIRLARININ BULUNUŞU İÇİN ALGORİTMALAR

TUTAR, Fatma
Yüksek Lisans Tezi, Matematik Anabilim Dalı
Tez Danışmanı: Doç. Dr. Şenay BAYDAŞ
Haziran 2018, 61 sayfa

Bu tez yedi bölümden oluşmaktadır. Birinci ve ikinci bölümde giriş ve kaynak bildirişleri verilmiştir. Üçüncü bölümde temel kavramlar, dördüncü bölümde köklerle çözülebilirlikten bahsedilmiştir. Beşinci ve altıncı bölümlerde Galois grupları ve palindromik polinomların kökleri incelenmiştir. Yedinci bölümde ise sonuç ve tartışma ile tez sonlandırılmıştır.

Anahtar kelimeler: Cisim genişlemeleri, Galois grup, Palindromik polinomlar.

ABSTRACT

GALOIS THEORY, PALINDROMIC POLYNOMIALS AND ALGORITHMS FOR FINDING THE ROOTS OF PALINDROMIC POLYNOMIALS

TUTAR, Fatma
M. Sc. Thesis, Department of Mathematics
Supervisor: Assoc. Prof. Dr. Şenay BAYDAŞ
June 2018, 61 pages

This thesis consists of seven chapter. In the first and second chapters, introduction and literature were given. In the third chapter, basic concepts, in the fourth chapter, solubility with roots are mentioned. In the fifth and sixth chapters Galois groups and the roots of palindromic polynomials are investigated. In the seventh chapter, the thesis is terminated with conclusion and discussion.

Keywords: Field extension, Galois group, Palindromic polynomials.

ÖN SÖZ

Bu tez çalışmasında, her türlü ilgi ve yardımlarını esirgemeyen bana her zaman destek olan değerli hocalarım Sayın Doç. Dr. Şenay BAYDAŞ ve Sayın Prof. Dr. Bülent KARAKAŞ'a ayrıca verdikleri desteklerinden ötürü aileme ve arkadaşlarıma teşekkürlerimi borç bilirim.

2018

Fatma TUTAR

İÇİNDEKİLER

Sayfa

Sayfa

ŞEKİLLER LİSTESİ

Şekil **Sayfa**

1. GİRİŞ

Beş ve daha yüksek mertebeden polinomların genel çözümünün olmaması ilk olarak Abel tarafından ve sonrasında Galois teori simetri gruplarını inşa ederek ve kullanarak Galois tarafından ispat edilmiştir. Polinomlar halkasının özel altgrupları için çözüm teknikleri geliştirmek Abel ve Galois sonrasının önemli matematik araştırmaları arasındadır. Polinomların rasyonel sıfırlarının olmaması durumunda Evariste Galois'in öncülüğünü yaptığı cisim genişlemesinde polinom sıfırları hesaplanabilir. Beş ve daha yüksek mertebeden polinomların çözümü için bir genel kural verilememesi, beş ve beşten büyük mertebeli bütün polinomlar için geçerli değildir. Bu polinomlardan biri palindromik polinomlardır. Bu tez çalışmasında Galois teori, polinomların sıfırlarının bulunabilirliği, bağlı algoritmalar, köklerin bulunmasına dair algoritma verilemezliğinin mertebeye bağlı durumları, bazı özel polinomların katsayılara bağlı sıfırlarının bulunabilirliği ve özel olarak palindromik polinomlar incelenmiştir.

2. KAYNAK BİLDİRİŞLERİ

n. dereceden polinomların sıfırlarının araştırılması ilk olarak Harezmi'nin çalışmalarında yer alır (Rosen, 1831). Günümüz terminolojisi ile $ax^2 + bx + c = p(x)$ 2. dereceden polinomun sıfırları $x_{1,2} = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$ ile hesaplanabilir. 3. ve 4. dereceden polinomların sıfırlarının hesabı için dönüşüm formülleri ile hesap teknikleri mevcuttur (Süray, 1970).

Polinomların rasyonel sıfırlarının olmaması durumunda Galois'in öncülüğünü yaptığı cisim genişlemesinde polinomların sıfırları hesaplanabilir. Örneğin, $x^2 - 4$ polinomunun Q da sıfırları hesaplanabilirken, $x^2 + 4$ polinomunun sıfırları $\mathrm{Q}(i\sqrt{2})$ cisminde mevcuttur. Bu durum 3. ve 4. dereceden polinomlar için de söylenebilir.

Önemli olan $G(\mathrm{Q}(c_1, c_2, \dots, c_n)/\mathrm{Q}) \cong S_n$ e izomorf olmasıdır ve S_n, $n \leq 4$ için çözülebilirdir. Bir başka ifadeyle 2., 3. ve 4. dereceden polinomlar çözülebilirdir.

Beş ve beşten daha yüksek mertebeden polinomların çözümü için bir genel kural verilememesi, $n \geq 5$ için $P_n(x)$ polinomlarının tümünü içermez.

Simetrik polinomlar, palindromik polinomlar vs. genel çözümleri verilebilecek olan polinom tipleridirler. Bu tezde palindromik polinomlar ele alınacaktır.

Bir $P(x) = \sum_{n=0}^{k} a_n x^n$ polinomunda, $a_{n-k} = a_{k,} \forall k$ için sağlanıyor ise $P(x)$ e palindromik polinom adı verilir. Palindromik polinomların karakterizasyonu $P(x) = x^n P(\frac{1}{x})$ şeklindedir.

Palindromik ve antipalindromik polinomların kökleri çiftler halinde bulunur (λ, 1/λ) (Markovsky ve Rao, 2008).

$R(z) = 1 + \lambda(z + z^2 + \cdots + z^{n-1}) + z^n$ $\lambda \in \mathbb{R}$ palindromik polinomunun bütün sıfırlarının birim çember üzerinde olması için gerek ve yeter koşullar verildiğinde $S(z) = R(z) + \gamma z^n$ nin sıfırları kapalı birim disk içindedir (Botta ve ark., 2014).

Bir palindromik polinomunun matris formunun özdeğerlerinin hesaplanması için Ehrlich-Aberth kök bulma yöntemine dayanan bir algoritma mevcuttur (Gemignani ve Noferini, 2013).

α ∈ Q durumunda köklerin tümü gerçel sayı olan polinomların genel yapısı için Coulson tipi integral formülleri verilmiştir (Qiao ve ark., 2018).

Palindromik polinomların sıfırlarının aynı anda incelenmesi için Ehrlich-Aberth yönteminin bir varyasyonu verilmektedir (Brugiapaglia ve Gemignani, 2014).

Palindromik polinomlar ve Galois teori ile ilgili literatürde önemli çalışmalar mevcuttur (Joyner ve Shaska, 2000; Lindstorm, 2015).

3. TEMEL KAVRAMLAR

Bu bölümde tez için gerekli olan temel tanım ve teoremler aktarılacaktır.

Tanım 3.1. G boş olmayan bir küme ve G üzerinde bir $*$ ikili işlemi tanımlı olsun. Aşağıdaki şartlar sağlanıyor ise $(G,*)$ sıralı ikilisine bir grup denir.

(i) $*$ işlemi birleşme özelliğini sağlar ; yani, her $a, b, c \in G$ için

$$(a * b) * c = a * (b * c) \text{ ise}$$

(ii) Her $a \in G$ için

$$a * e = e * a = a$$

olacak biçimde bir $e \in G$ birim elemanı vardır.

(iii) Her $a \in G$ için

$$a * a' = a' * a = e$$

olacak biçimde bir $a' \in G$ vardır (a' ne a nın bir ters elemanı denir)

Ek olarak eğer $(G,*)$ grubunda her $a, b, c \in G$ için

$$a * b = b * a$$

ise bu gruba değişmeli ya da abelyan grup denir (Stewart, 1945).

Tanım 3.2. G bir grup olsun. G nin kardinalitesi $|G|$ ye G nin mertebesi denir. Eğer $|G|$ sonlu ise G ye sonlu grup ve sonsuz ise sonsuz grup denir (Fraleigh, 2006).

Böylece bir sonlu grubun mertebesi o grubun eleman sayısıdır.

Tanım 3.3. G bir grup ve H, G nin boş olmayan bir altkümesi olsun. Eğer H, G nin işlemine göre kapalı ve bu işleme göre bir grup ise o zaman H a G nin bir altgrubu denir ve $H \leq G$ ya da $G \geq H$ ile gösterilir (Asar ve Arıkan, 2011).

G ve {e}, G nin altgrupları olduğu açıktır. Bunlara G nin aşikar altgrupları denir.

Teorem 3.1. G bir grup ve $a \in G$ olsun. O zaman

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$$

dir (Fraleigh, 2006).

Tanım 3.4. G bir grup olsun. Eğer $G = \langle a \rangle$ olacak biçimde bir $a \in G$ varsa G ye a tarafından üretilen bir devirli grup denir (Asar ve Arıkan, 2011).

Tanım 3.5. A boştan farklı bir küme olsun. A üzerinde tanımlı birebir ve örten bir fonksiyona A üzerinde bir permütasyon denir.

Bir A kümesi üzerinde tanımlı bütün permütasyonların kümesi Sym(A) ile gösterilir. $I_n = \{1,2,\dots,n\}$ kümesi üzerinde tanımlı bütün permütasyonların kümesi ise S_n ile gösterilir.

Sym(A) grubuna A kümesi üzerindeki simetrik grup denir. Sym(A) nın her altgrubuna da A üzerinde bir permütasyon grubu denir (Artin, 1944).

Teorem 3.2. A , n elemanlı bir küme olsun. O zaman $|\mathrm{Sym}(A)| = n!$ dir (Hungerford, 1974).

Teorem 3.3. $n \geq 2$ olsun. O zaman A_n, S_n nin mertebesi $\frac{1}{2}n!$ olan bir altgrubudur. $|A_n| = \frac{1}{2}n!$ dir. A_n grubuna derecesi n olan alterne grup denir (Feyzioğlu, 1990).

Teorem 3.4. $G = \langle a \rangle$ devirli grubu verilsin. G nin her altgrubu devirlidir (Asar ve Arıkan, 2011).

Tanım 3.6. G ve H iki grup ve $\varphi: G \to H$ fonksiyonu verilsin. Eğer her $a, b \in G$ için

$$\varphi(ab) = \varphi(a)\varphi(b)$$

ise φ ye G den H ya bir grup homomorfizması denir.

Eğer ek olarak φ birebir ise φ ye bir grup monomorfizması; örten ise φ ye bir grup epimorfizması ve φ hem birebir ve hem de örten ise φ ye bir grup izomorfizması denir. φ bir izomorfizma ise G, H a izomorftur denir ve $G \cong H$ ile gösterilir. Ayrıca eğer $G = H$ ve φ, G den G ye tanımlı birim fonksiyon τ_G, G nin bir otomorfizması denir (Jacobson, 1910).

Tanım 3.7. $\varphi: G \to H$ bir grup homorfizması olsun.

$$Ker(\varphi) = \{g \in G: \varphi(g) = e_H\} \text{ ve } Im(\varphi) = \varphi(G) = \{\varphi(g): g \in G\}$$

kümelerine, sırasıyla, φ nin çekirdeği ve görüntüsü denir (Asar ve Arıkan, 2011).

Teorem 3.5. (Cayley Teoremi) Her grup bir permütasyon grubuna izomorftur (Asar ve Arıkan, 2011).

Tanım 3.8. G bir grup ve H, G nin bir altgrubu olsun. H ın G içindeki sol (sağ) kosetlerinin kardalitesine H ın G içindeki indeksi denir ve $|G:H|$ ile gösterilir (Hungerford, 1974).

Teorem 3.6. (Lagrange Teoremi) G bir sonlu grup ve H, G nin bir altgrubu olsun. O zaman H nın mertebesi G nin mertebesini böler (Dummit ve Foot, 2004).

Sonuç 3.1. G bir sonlu grup ve H, K, G nin altgrupları olmak üzere $K \leq H$ olsun. O zaman

$$|G:K| = |G:H||H:K|$$

olur (Asar ve Arıkan, 2011).

Sonuç 3.2. p bir asal sayı ve G mertebesi p olan bir grup olsun. O zaman G devirlidir ve $G \cong Z_p$ dir (Fraleigh, 2006).

Tanım 3.9. G bir grup olsun ve N, G nin bir altgrubu olsun. Eğer her $g \in G$ için

$$gNg^{-1} = N$$

ise N ye G nin bir normal altgrubu denir ve $N \lhd G$ ile gösterilir.

Her G grubunda G ve $\{e\}$ normal altgruplarıdır (Asar ve Arıkan, 2011).

Teorem 3.7. G bir grup ve N, G nin bir altgrubu olsun. Eğer $|G:N| = 2\ ise\ N \lhd G$ dir (Asar ve Arıkan, 2011).

Sonuç 3.3. $n \geq 2$ olsun. O zaman $A_n \lhd S_n$ dir (Hungerford, 1974).

Tanım 3.10. G bir grup ve $G \neq \{e\}$ olsun. Eğer G nin $\{e\}$ ve G den başka normal altgrubu yoksa G ye bir basit grup denir (Asar ve Arıkan, 2011).

Tanım 3.11. G bir grup ve $\{e\} = H_0 \leq H_1 \leq \cdots \leq H_n = G, G$ nin altgruplarının bir artan zinciri olsun. Eğer her $0 \leq i \leq n\ için\ H_i, H_{i+1}$ içinde normal ise;

$$\{e\} = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G$$

ise bu zincire G nin bir altnormal serisi denir. Her H_i ye altnormal serinin bir terimi ve H_{i+1}/H_i bölüm grubuna altnormal serinin bir bölüntüsü denir. Birbirinden farklı bölüntülerin sayısına altnormal serinin uzunluğu denir. Eğer $0 \leq i \leq n\ için\ H_i \lhd G$ ise seriye normal seri denir. H, G nin bir altgrubu olsun. Eğer

$H = H_0, H_1, \ldots, H_n = G, G$ nin altgrupları olmak üzere $H = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G$ ise H a G nin bir altnormal altgrubu denir (Asar ve Arıkan, 2011).

Tanım 3.12. G bir grup ve

$$\{e\} = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G$$

G nin bir altnormal serisi olsun. Eğer $0 \leq i \leq n\ için\ H_{i+1}/H_i$ bölüm grubu abelyan ise G ye çözülebilir grup denir (Asar ve Arıkan, 2011).

Örnek 3.1. $n \leq 4$ için S_n çözülebilirdir. $S_1\ ve\ S_2$ abelyan olduğundan çözülebilirdir. S_3 ün bir normal serisi

$$\{(1)\} \lhd A_3 \lhd S_3$$

Burada $A_3/\{(1)\}$ ile S_3/A_3 bölüm grubu abelyan olduğundan S_3 çözülebilirdir. S_4 ün bir normal serisi

$$\{(1)\} \lhd V_4 \lhd A_4 \lhd S_4$$

Burada V_4, Klein 4-grubudur. Açıkça görüldüğü gibi, $V_4/\{(1)\}, A_4/V_4, S_4/A_4$ bölüm grupları abelyan olduğundan S_4 çözülebilirdir (Asar ve Arıkan, 2011).

Sonuç 3.4. $n \geq 5$ olsun. O zaman S_n çözülebilir değildir (Asar ve Arıkan, 2011).

Tanım 3.13. R, boş olmayan bir küme olsun. R üzerinde her $a, b \in R$ için

$$+: (a, b) \to a + b, \qquad \cdot: (a, b) \to a \cdot b$$

biçiminde tanımlı ve sırasıyla, toplama ve çarpma denilen $''+''$ ve $''\cdot''$ ikili işlemleri verilsin. Eğer aşağıdaki şartları sağlarsa

(i) (R,+) bir abelyan gruptur,

(ii) Çarpma birleşme özelliğini sağlar; yani $a, b, c \in R$ için

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \text{ ise,}$$

(iii) $\cdot$ işlemi $+$ işlemi üzerinde dağılma özelliğine sahiptir; yani $a, b, c \in R$ için

$a \cdot (b + c) = a \cdot b + a \cdot c$ (sol dağılma özelliği)

$(a + b) \cdot c = a \cdot b + a \cdot c$ (sağ dağılma özelliği) ise,

$(R, +, \cdot)$ sıralı üçlüsüne bir halka denir. Eğer her $a, b \in R$ için $a \cdot b = b \cdot a$ ise halkaya bir değişmeli halka denir. R nin toplamsal birimi 0_R ile gösterilir ve buna R nin sıfırı denir. Eğer her $a \in R$ için $a \cdot 1_R = 1_R \cdot a = a$ olacak biçimde $1_R \in R$ varsa 1_R elemanına halkanın birim elemanı (birimi) ve halkaya da birimli halka denir. $R = \{0_R\}$ halkasının birimi $1_R = 0_R$ dir. $(R, +)$ grup olduğundan 0_R her zaman vardır fakat 1_R olmayabilir (Adamson, 1964).

Tanım 3.14. R bir halka ve $a, b \in R$ olsun. Eğer $a, b \neq 0_R$ $a \cdot b = 0_R$ ise a ya bir sol sıfır böleni ve b ye bir sağ sıfır böleni denir. Hem sol sıfır böleni hem de sağ sıfır böleni olan bir elemana sıfır böleni denir. Ne sol sıfır böleni ne de sağ sıfır böleni bulunan bir halkaya da sıfır bölensiz halka denir (Asar ve Arıkan, 2011).

Tanım 3.15. R birimli bir halka $(0_R \neq 1_R)$ ve $0_R \neq a \in R$ olsun. Eğer $a \cdot b = 1_R$ olacak biçimde $b \in R$ varsa b ye a nın sağ tersi ve $c \cdot a = 1_R$ olacak biçimde $c \in R$ varsa c ye a nın sol tersi denir. Eğer $d \in R$ olmak üzere $a \cdot d = d \cdot a = 1_R$ ise d ye a nın bir tersi ve a ya tersinir (birimsel) eleman denir (Asar ve Arıkan, 2011).

Tanım 3.16. R birimli değişmeli bir halka ve $0_R \neq 1_R$ olsun. Eğer R sıfır bölensiz ise R ye bir tamlık bölgesi denir (Fraleigh, 2006).

Tanım 3.17. R birimli değişmeli bir halka ve $0_R \neq 1_R$olsun. Eğer R nin sıfırdan farklı her elemanı tersinir ise R ye bir bölme halkası denir. Değişmeli bir bölme halkasına cisim denir (Hardy ve Wright, 1960).

Tanım 3.18. Eğer R halkasında her $r \in R$ için $nr = 0_R$ olacak biçimde bir pozitif n tamsayısı varsa bu n sayılarının en küçüğüne R nin karekteristiği denir. Eğer böyle bir pozitif tamsayısı yoksa R nin karakteristiği 0 olarak tanımlanır. R nin karakteristiği $kar(R)$ ile gösterilir (Asar ve Arıkan, 2011).

Tanım 3.19. R bir halka ve R nin boştan farklı bir altkümesi A olsun. Eğer A, R nin işlemlerine göre kapalı ve bu işlemlere göre bir halka ise A ya R nin bir althalkası denir. F bir cisim ve E, F nin bir althalkası olsun. Eğer E aynı zamanda bir cisim ise, E ye F nin bir altcismi denir.

Açıkça görüldüğü gibi, R ve $\{0_R\}$, R halkasının althalkalarıdır. $\{0_R\}$ ve R ye R nin aşikar althalkaları denir. R nin kendisinden farklı her althalkasına R nin bir öz althalkası denir (Hoffman ve Kunze, 1961).

Tanım 3.20. Bir cismin bütün altcisimlerinin kesişimine o cismin asal cismi denir (Asar ve Arıkan, 2011).

Tanım 3.21. R ve S iki halka ve $\varphi: R \to S$ fonksiyonu verilsin. Eğer her $a, b \in R$ için

$$\varphi(a+b) = \varphi(a) + \varphi(b) \; ve \; \varphi(ab) = \varphi(a)\varphi(b)$$

ise φ ye R den S ye bir halka homomorfizması denir. Eğer ek olarak φ birebir ise φ ye bir halka monomorfizması, örten ise bir halka epimorfizması ve birebir eşleme ise bir halka izomorfizması denir. R den R ye tanımlı bir homomorfizmaya endomorfizma ve bir izomorfizmaya otomorfizma denir (Dummit ve Foot, 2004).

3.1. Cisim Genişlemeleri

Tanım 3.1.1. E bir cisim ve F, E nin bir altcismi olsun. O zaman E ye F nin bir cisim genişlemesi denir. E bir cisim ve $E_1, E_{2,\ldots,} E_s, E$ nin altcisimleri olmak üzere her $0 \leq i \leq s$ için $E_i \leq E_{i+1}$ olsun. O zaman $E_1 \leq E_2 \leq \cdots \leq E_s$ yükselen zincirine bir cisim kulesi denir (Artin, 1944).

Örnek 3.1.1. Reel sayılar cismi $\mathbb{R}$, rasyonel sayılar cismi $\mathbb{Q}$, kompleks sayılar cismi $\mathbb{C}$ olmak üzere $\mathbb{C}$, hem $\mathbb{R}$ nin ve hem de $\mathbb{Q}$ nun birer cisim genişlemesidir. Böylece $\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ cisim kulesi elde edilir (Asar ve Arıkan, 2011).

Lemma 3.1.1. F bir cisim ve E, F nin bir cisim genişlemesi olsun. O zaman E, F üzerinde bir vektör uzayıdır (Asar ve Arıkan, 2011).

Tanım 3.1.2. F bir cisim ve E, F nin bir cisim genişlemesi olsun. O zaman E nin F-uzayı olarak boyutuna E nin F üzerindeki derecesi denir ve $[E:F]$ ile gösterilir. $[E:F]$ nin sonlu ya da sonsuz olmasına göre E ye F nin bir sonlu cisim genişlemesi ya da bir sonsuz cisim genişlemesi denir (Fraleigh, 2006).

Örnek 3.1.2. $\mathbb{R}$, $\mathbb{Q}$ nun bir sonsuz cisim genişlemesi ve $\mathbb{C}$, $\mathbb{R}$ nin bir sonlu cisim genişlemesidir.$\mathbb{C} = \{a + ib: a, b \in R\}$ ve $\{1, i\}$, $\mathbb{C}$ üzerinde lineer bağımsız olduğundan $[\mathbb{C}: \mathbb{R}] = 2$ dir. Öte yandan e sayısı sabit olmayan hiçbir $g(x) \in Q[x]$ polinomunun kökü değildir. Dolayısıyla $\{e^i: i \geq 0\}$ sonsuz kümesi $\mathbb{Q}$ üzerinde lineer bağımsızdır ve $[\mathbb{R}: \mathbb{Q}]$ sonsuzdur (Asar ve Arıkan, 2011).

Tanım 3.1.3. $p(x) \in F[x]$ olsun. Eğer

(i) $p(x)$ sabit değilse ve

(ii) $p(x)$, $F[x]$ içinde, her birinin derecesi $p(x)$ derecesinden daha küçük olan iki polinomun çarpımı olarak yazılamazsa o zaman $p(x)$ e $F[x]$ içinde bir indirgenemez polinom denir.

Böylece $p(x)$ in indirgenemez olması için gerek ve yeter şart $der(p(x)) \geq 1$ ve $p(x) = r(x)s(x)$ iken $r(x)$ ya da $s(x)$ in sabit olmasıdır.

Tanımdan görüldüğü gibi birinci dereceden her polinom indirgenemezdir (Asar ve Arıkan, 2011).

Teorem 3.1.1. (Eisenstein İndirgenemezlik Kriteri) p bir asal sayı ve $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in Z[x]$ olsun. Eğer

(i) $p|a_0, p|a_1, \ldots, p|a_{n-1}$ fakat $p \nmid a_n \; ve$

(ii) $p^2 \nmid a_o \; ise$

o zaman $f(x), Q[x]$ içinde indirgenemezdir (Asar ve Arıkan, 2011).

Teorem 3.1.2. (Kronecker Teoremi) $p(x) \in F[x]$ bir indirgenemez polinom olsun. F nin öyle bir cisim genişlemesi E vardır ki $p(x)$ in E içinde bir kökü vardır (Asar ve Arıkan, 2011).

Sonuç 3.1.1. $f(x) \in F[x]$ sabit olmayan bir polinom olsun. F nin öyle bir cisim genişlemesi E vardır ki E içinde $f(x)$ in bir kökü vardır (Asar ve Arıkan, 2011).

Teorem 3.1.3. F bir cisim ve E, F nin bir cisim genişlemesi olsun. Ayrıca $u \in E$, F üzerinde cebirsel, $\text{İ}nd(u,F) = p(x)$ ve $der(p(x)) = n$ olsun. Aşağıdakiler sağlanır (Fraleigh, 2006).

(i) $F(u) = F[u]$ ve $F(u) \cong F[x]/\langle p(x)\rangle$ tir.

(ii) $\{1, u, \dots, u^{n-1}\}, F(u)$ nun bir F-bazıdır.

(iii) $[F(u):F] = n$ dir.

3.2. Cebirsel Cisim Genişlemeleri

Tanım 3.2.1. E, bir F cisminin bir cisim genişlemesi olsun. Eğer E nin her elemanı F üzerinde cebirsel ise E ye F nin bir cebirsel genişlemesi denir (Asar ve Arıkan, 2011).

E, F nin bir cebirsel genişlemesi ise kısaca $F \leq E$ bir cebirsel genişleme denir. Her cisim kendisinin cebirsel genişlemesidir.

Örnek 3.2.1. $\mathbb{C}$, $\mathbb{R}$ nin bir cebirsel genişlemesidir. $a, b \in \mathbb{R}$ olmak üzere $z = a + ib$ olsun.

$g(x) = (x - z)(x - \bar{z}) = x^2 - 2ax + (a^2 + b^2) \in R[x]$ ve $g(z) = 0$ olduğundan z, $\mathbb{R}$ üzerinde cebirseldir (Asar ve Arıkan, 2011).

Teorem 3.2.1. Her sonlu cisim genişlemesi bir cebirsel genişlemedir (Asar ve Arıkan, 2011).

Teorem 3.2.2. $F \leq E \leq K$ cisim kulesi verilsin. Eğer E, F nin ve K, E nin sonlu genişlemeleri ise o zaman K, F nin bir sonlu cisim genişlemesidir ve

$$[K:F] = [K:E][E:F]$$

olur (Asar ve Arıkan, 2011).

Tanım 3.2.2. E bir F cisminin bir cisim genişlemesi olsun.

$$\overline{F_E} = \{c : c \in E \text{ ve } c, F \text{ üzerinde cebirseldir}\}$$

kümesine F nin E içindeki cebirsel kapanışı denir (Asar ve Arıkan, 2011).

Tanım 3.2.3. F bir cisim olsun. Eğer $F[X]$ in sabit olmayan her elemanının F içinde bir kökü varsa F ye cebirsel kapalı bir cisim denir (Fraleigh, 2006).

Tanım 3.2.4. Bir F cisminin cebirsel kapalı bir cebirsel genişlemesi varsa buna F nin bir cebirsel kapanışı denir (Asar ve Arıkan, 2011).

Teorem 3.2.3. Her cismin bir cebirsel kapanışı vardır (Fraleigh, 2006).

Teorem 3.2.4. F bir cisim olsun. F nin cebirsel kapalı olması için gerek ve yeter şart $F[x]$ in sabit olmayan her polinomunun $F[x]$ içinde lineer çarpanlara ayrılmasıdır (Fraleigh, 2006).

3.3. İzomorfizmaların Genişletilmesi ve Otomorfizma Grupları

Tanım 3.3.1. F bir cisim E, F nin bir cebirsel genişlemesi ve $u, v \in E$ olsun. Eğer $\text{İ}nd(u, F) = \text{İ}nd(v, F)$ ise u ile v, F üzerinde eşleniktir denir (Asar ve Arıkan, 2011).

Örnek 3.3.1. $z \in \mathbb{C}$ olsun. z nin $\mathbb{R}$ üzerindeki eşlenikleri $z \; ve \; \bar{z}$ dir. a,b reel sayılar olmak üzere $z = a + ib$ olsun. Eğer $b = 0 \; ise \; z = a \; ve \; \bar{z} = a$ dır. Ayrıca $\text{İ}nd(a, \mathbb{R}) = x - a$ olduğundan a nın tek eşleniği kendisidir. Şimdi $b \neq 0$ olsun. $p(x) = (x - z)(x - \bar{z}) = x^2 - 2ax + (a^2 + b^2)$ olsun. O zaman $p(x) \in R[x]$ tir. $p(x)$ in kökleri $z, \bar{z}$ reel olmadığından . $p(x), \mathbb{R}$ üzerinde indirgenemezdir. Dolayısıyla z nin eşlenikleri z , $\bar{z}$ dir (Asar ve Arıkan, 2011).

Tanım 3.3.2. $\varphi: R \to S$ bir halka homomorfizması ve A, R nin bir althalkası olsun. Her $a \in A$ için $\varphi(a) = a$ ise φ, A yı sabit bırakır denir. $\sigma: A \to S$ bir halka homomorfizması olsun. Eğer $\varphi|A = \sigma$ ise σ ya φ nin A ya kısıtlanışı ve φ ye σ nın $\mathbb{R}$ den S ye bir genişlemesi denir (Asar ve Arıkan, 2011).

Lemma 3.3.1. $\sigma: F \to F'$ bir cisim izomorfizması olsun. O zaman $\sigma^*: (a_0 + a_1x + \cdots + a_nx^n) \to \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n$ eşlemesi $F[x]$ ten $F'[x]$ e bir halka izomorfizmasıdır. Ayrıca $p(x) \in F[x]$, F üzerinde indirgenemez ise $\sigma^*\big(p(x)\big)$, F üzerinde indirgenemezdir (Fraleigh, 2006).

Teorem 3.3.1. $E = F(u) \; ve \; E' = F'(v)$ basit cebirsel genişlemeler ve $\sigma: F \to F'$ bir cisim izomorfizması olsun. Ayrıca $p(x) = \text{İ}nd(u, F) \; ve \; \sigma^*\big(p(x)\big) = \text{İ}nd(v, F')$ olsun. O zaman öyle bir $r: E \to E'$ cisim izomorfizması vardır ki, $r(u) = v \; ve \; r|F = \sigma$ dir. $F = F', \; E = E' \; ve \; \sigma = \tau$ ise o zaman $r: F(u) \to F(v)$ izomorfizması, $\psi_{u,v}$ ile gösterilir ve buna temel izomorfizma(monomorfizma) denir (Dummit ve Foot, 2004).

Sonuç 3.3.1. F ve F' iki cisim ve bunların birer cebirsel genişmeleri, sırasıyla, $E \; ve \; E'$ olsun. Ayrıca $\sigma: F \to F'$ bir cisim izomorfizması olsun. $p(x) \in F[x]$ bir indirgenemez polinom ve $p(x)$ in E içindeki bir kökü u olsun. O zaman σ nın $F(u)$ dan E' içine tanımlı her genişlemesi u yu $\sigma^*\big(p(x)\big)$ in bir köküne götürür. Dolayısıyla σ nın

genişlemelerinin sayısı $\sigma^*(p(x))$ in E' içindeki köklerinin sayısına eşittir (Fraleigh, 2006).

Sonuç 3.3.2. $E = F(u), F$ nin bir basit cebirsel genişlemesi , $p(x) =$ İ$nd(u, F)$ ve $der(p(x)) = n$ olsun. E nin F yi sabit bırakan bir homomorfizması r olsun. $p(x)$ in E içindeki bir kökü v olmak üzere $r = \psi_{u,v}$ dir. Dolayısıyla r, E nin F yi sabit bırakan otomorfizmalarının sayısı $p(x)$ in E içindeki köklerinin sayısına eşittir. Bundan başka her $b \in E$ için $c_0, c_1, \dots, c_{n-1} \in F$ olmak üzere

$b = c_0 + c_1u + \cdots + c_{n-1}u^{n-1}$ ve $r(b) = c_0 + c_1v + \cdots + c_{n-1}v^{n-1}$ dir (Fraleigh, 2006).

Örnek 3.3.2. $E = Q(\sqrt{2})$ cisminden C ye tanımlı bütün Q-monomorfizmalarını belirleyelim. İ$nd(\sqrt{2}, Q) = x^2 - 2$ olduğundan $\sqrt{2}$ nin Q üzerindeki eşlenikleri $-\sqrt{2}, \sqrt{2}$ dir. Dolayısıyla Sonuç 3.3.2 gereğince E nin Q yu sabit bırakan bütün monomorfizmaları $\psi_{\sqrt{2},\sqrt{2}}$ ve $\psi_{\sqrt{2},-\sqrt{2}}$ dir. E nin tipik elemanı $a, b \in Q$ olmak üzere $a + b\sqrt{2}$ biçimindedir ve $\psi_{\sqrt{2},-\sqrt{2}}(a + b\sqrt{2}) = a - b\sqrt{2}$ dir (Asar ve Arıkan, 2011).

Tanım 3.3.3. Bir E cisminden kendi üzerine tanımlı bir izomorfizmaya E nin bir otomorfizması denir. E nin bütün otomorfizmalarının kümesi $Aut(E)$ ile gösterilir (Dummit ve Foot, 2004).

Tanım 3.3.4. E bir cisim F, E nin bir altcismi ve H, $Aut(E)$ nin bir altgrubu olsun. O zaman E nin F yi sabit bırakan bütün otomorfizmalarının kümesi $G(E/F)$ ile ve E nin H tarafından sabit bırakılan elemanlarının kümesi E_H ile gösterilir. Böylece

$$G(E/F) = \{\sigma \in Aut(E) : \text{her } a \in F \text{ için } \sigma(a) = a\}$$

ve

$$E_H = \{a \in E : \text{her } \sigma \in H \text{ için } \sigma(a) = a\}$$

olur (Dummit ve Foot, 2004).

Teorem 3.3.2. E bir cisim ve $Aut(E)$ nin bir altgrubu H olsun. O zaman E_H kümesi E nin bir altcismidir (Asar ve Arıkan, 2011).

E_H cismine H nın E içindeki sabit cismi denir.

Teorem 3.3.3. F bir cisim, E, F nin bir cebirsel genişlemesi ve $E = F(u_1, u_2, \dots, u_k)$ olsun. O zaman $G(E/F)$ nin σ elemanı $u_1, u_2, \dots, u_k$ deki değerleriyle tam olarak belirlenir. Bundan başka eğer $G(E/F)$ nin her σ elemanı için

$$\sigma(\{u_1, u_2, \dots, u_k\}) \subseteq \{u_1, u_2, \dots, u_k\}$$

ise o zaman $G(E/F)$, $Sym(\{u_1, u_2, \dots, u_k\})$ nin bir altgrubuna izomorftur (Asar ve Arıkan, 2011).

Sonuç 3.3.3. F bir cisim, E, F nin bir cebirsel genişlemesi ve $E = F(u_1, u_2, \dots, u_k)$ olsun. Ayrıca $\sigma \in G(E/F)$ için

$$\sigma(\{u_1, u_2, \dots, u_k\}) \subseteq \{u_1, u_2, \dots, u_k\}$$

olsun. O zaman $G(E/F)$, S_k nın bir altgrubuna izomorftur ve böylece $|G(E/F)|\big|k!$ dir (Fraleigh, 2006).

Örnek 3.3.3. $G(\mathbb{C}/\mathbb{R})$ grubunu belirleyelim. $\mathbb{C} = \mathbb{R}(i)$ olduğundan. $\dot{I}nd(i, \mathbb{R}) = x^2 + 1$ olduğundan i nin $\mathbb{R}$ üzerindeki eşlenikleri $i, -i$ dir. Dolayısıyla Sonuç 3.3.2 gereğince $G(\mathbb{C}/\mathbb{R}) = \{\psi_{i,i}, \psi_{i,-i}\}$ dir. Ayrıca $G(\mathbb{C}/\mathbb{R})$ nin sabit cismi $\mathbb{R}$ dir (Asar ve Arıkan, 2011).

Örnek 3.3.4. $E = \mathbb{Q}(\sqrt{2})$ olsun. $G(E/\mathbb{Q})$ yu belirleyelim. Örnek 3.3.2 den dolayı

$$G(E/\mathbb{Q}) = \{\psi_{\sqrt{2},\sqrt{2}}, \psi_{\sqrt{2},-\sqrt{2}}\}$$

dir. Dolayısıyla $G(E/\mathbb{Q})$, mertebesi iki olan bir devirli gruptur. $E_{G(E/\mathbb{Q})} = \mathbb{Q}$ dur. E nin $\mathbb{Q}$ ve kendisinden başka altcismi ve $G(E/\mathbb{Q})$ nun birim ve kendisinden başka altgrubu yoktur (Asar ve Arıkan, 2011).

3.4. Parçalanma Cisimleri ve Normal Genişlemeler

Tanım 3.4.1. F bir cisim, $f(x) \in F[x]$ derecesi $n \geq 1$ olan bir polinom ve K, F nin bir cisim genişlemesi olsun. Eğer $f(x), K[x]$ içinde lineer çarpanlarına ayrılırsa; yani $a \in F$ ve $u_1, u_2, \dots, u_n \in K$ olmak üzere

$$f(x) = a(x - u_1)(x - u_2) \dots (x - u_n)$$

olarak yazılabilirse $f(x)$, K üzerinde parçalanır denir. Eğer $f(x)$, K üzerinde parçalanır fakat K nın hiçbir öz altcismi içinde parçalanmazsa; yani, $K = F(u_1, u_2, \dots, u_n)$ ise K ya, $f(x)$ in F üzerinde bir parçalanma cismi denir (Kaplansky, 1972).

Örnek 3.4.1. $f(x) = (x^2 - 5)(x^2 - 7) \in Q[x]$ polinomun Q üzerindeki parçalanma cismi $Q(\sqrt{5}, \sqrt{7})$ tür. $(x^2 - 5)(x^2 - 7)$, polinomunun kökleri $\pm\sqrt{5}, \pm\sqrt{7}$ olduğundan $f(x)$ polinomu $Q(\sqrt{5}, \sqrt{7})$ içinde çözülebilirdir. Ancak $f(x)$ polinomu $Q(\sqrt{5}, \sqrt{7})$ nin altcisimleri olan $Q(\sqrt{5})$, $Q(\sqrt{7})$ ve Q cisimlerinde parçalanmaz. Bu nedenle $Q(\pm\sqrt{5}, \pm\sqrt{7}) = Q(\sqrt{5}, \sqrt{7})$ parçalanma cismidir. $\left[Q(\sqrt{5}, \sqrt{7}) : \mathrm{Q}\right] = 4$ tür.

Teorem 3.4.1. $f(x) \in F[x]$ derecesi $n \geq 1$ olan bir polinom olsun. O zaman $f(x)$ in F üzerinde bir parçalanma cismi K vardır ve $[K:F] \leq n!$ dir (Fraleigh, 2006).

Teorem 3.4.2. F bir cisim ve K, F üzerinde derecesi $n \geq 1$ olan bir $f(x) \in F[x]$ polinomunun parçalanma cismi olsun. $f(x)$ in K içindeki birbirinden farklı kökleri $u_1, u_2, \dots, u_k$ olsun. O zaman $G(K/F)$, $Sym(\{u_1, u_2, \dots, u_k\})$ nın bir altgrubuna izomorftur ve $|G(K/F)||k!$ dir (Asar ve Arıkan, 2011).

Örnek 3.4.2. $x^3 - 2 \in Q[x]$ polinomunun Q üzerindeki parçalanma cismi K olsun. K yı ve $G(K/Q)$ grubunu belirleyelim. $x^3 - 2 \in Q[x]$ polinomunun Q üzerindeki parçalanma cismi $Q(\sqrt[3]{2}, i\sqrt{3})$ tür. $x^3 - 2$ nin bütün kompleks kökleri, $w = \frac{-1+i\sqrt{3}}{2}$ olmak üzere $\sqrt[3]{2}, \sqrt[3]{2}w, \sqrt[3]{2}w^2$olduğundan $x^3 - 2$ nin Q üzerindeki parçalanma cismi $K = Q(\sqrt[3]{2}, \sqrt[3]{2}w, \sqrt[3]{2}w^2) = Q(\sqrt[3]{2}, i\sqrt{3})$ tür. $\text{İ}nd(\sqrt[3]{2}, Q) = x^3 - 2$ olduğundan $Q(\sqrt[3]{2})$ nin bir Q-bazı $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ tür. Ayrıca $i\sqrt{3} \notin Q(\sqrt[3]{2})$ olduğundan K nın bir $Q(\sqrt[3]{2})$ bazı $\{1, i\sqrt{3}\}$ tür. Dolayısıyla K nın bir Q-bazı $\{1, \sqrt[3]{2}, \sqrt[3]{4}, i\sqrt{3}, i\sqrt{3}\sqrt[3]{2}, i\sqrt{3}\sqrt[3]{4}\}$ ve buradan $[K:Q] = 6$ dır. Şimdi $\sigma \in G(K/F)$ olsun.

Teorem 3.3.3'ten dolayı $\sigma, \sigma(\sqrt[3]{2})$ ve $\sigma(i\sqrt{3})$ değerleriyle tam olarak belirlenir. Ayrıca $\sigma(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \sqrt[3]{2}w, \sqrt[3]{2}w^2\}$ ve $\sigma(i\sqrt{3}) \in \{\pm i\sqrt{3}\}$ olduğundan , σ altı farklı biçimde belirlenir. Dolayısıyla 6 tane otomorfizma vardır ve böylece $|G(K/Q)| = [K:Q] = 6$ dır. Ayrıca Teorem 3.4.2'den dolayı $G(K/Q), Sym(\sqrt[3]{2}, \sqrt[3]{2}w, \sqrt[3]{2}w^2)$ nin ve o zaman S_3 ün bir altgrubuna izomorf olduğundan $G(K/Q) \cong S_3$ tür. $G(K/Q)$ un bütün elemanları aşağıda verilmiştir.

$$\begin{aligned}
\text{ı}: \sqrt[3]{2} &\to \sqrt[3]{2}, & i\sqrt{3} &\to i\sqrt{3} \\
\sigma_1: \sqrt[3]{2} &\to \sqrt[3]{2}w, & i\sqrt{3} &\to i\sqrt{3} \\
\sigma_2: \sqrt[3]{2} &\to \sqrt[3]{2}w^2, & i\sqrt{3} &\to i\sqrt{3} \\
\sigma_3: \sqrt[3]{2} &\to \sqrt[3]{2}, & i\sqrt{3} &\to -i\sqrt{3} \\
\sigma_4: \sqrt[3]{2} &\to \sqrt[3]{2}w, & i\sqrt{3} &\to -i\sqrt{3} \\
\sigma_5: \sqrt[3]{2} &\to \sqrt[3]{2}w^2, & i\sqrt{3} &\to -i\sqrt{3}
\end{aligned}$$

olmak üzere $G(K/Q) = \{\text{ı}, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$ tir. Burada $\sigma = \sigma_1$ ve $\tau = \sigma_3$ olsun. O zaman $\sigma^2: \sqrt[3]{2} \to \sqrt[3]{2}w^2$, $i\sqrt{3} \to i\sqrt{3}$ olduğundan $\sigma^2 = \sigma_2$ dir. Benzer biçimde $\sigma^3 = \tau^2 = \text{ı}$ dır. Ayrıca $\sigma\tau: \sqrt[3]{2} \to \sqrt[3]{2}w^2$, $i\sqrt{3} \to -i\sqrt{3}$ olduğundan $\sigma\tau = \sigma_5$ tir. Benzer biçimde $\sigma^2\tau = \sigma_4$ bulunur. Böylece $G(K/Q) = \{\text{ı}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ olur. Ayrıca

$\sigma\tau = \tau\sigma^2$ olduğundan $\langle\sigma\rangle \lhd G(K/Q)$ dir. Esasen $G(K/Q) \cong S_3$ tür. Bunun için $(a_1, a_2, a_3) = (\sqrt[3]{2}, \sqrt[3]{2}w, \sqrt[3]{2}w^2)$ ve $I_3 = \{1,2,3\}$ olsun. Her $\theta \in G(K/Q)$ için $\bar{\theta}: I_3 \to I_3$ fonksiyonu şöyle tanımlansın: $\theta(a_i) = a_j$ ise $\bar{\theta}(i) = j$ olsun. O zaman

$$\bar{\imath} = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, \bar{\sigma} = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \overline{\sigma^2} = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix},$$

$$\overline{\sigma\tau} = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}, \bar{\tau} = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}, \overline{\sigma^2\tau} = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$$

olur. Kolayca görüleceği gibi, $\theta \to \bar{\theta}$ eşlemesi $G(K/Q)$ dan S_3 e bir grup izomorfizmasıdır (Asar ve Arıkan, 2011).

Teorem 3.4.3. F bir cisim ve $f(x) \in F[x]$ olsun. $f(x)$ in F üzerindeki bir parçalanma cismi K *ve* $p(x)$, $F[x]$ in bir indirgenemez polinomu olsun. Eğer $p(x)$ in K içinde bir kökü varsa $p(x)$, K üzerinde parçalanır (Fraleigh, 2006).

Tanım 3.4.2. F bir cisim ve E, F nin bir cebirsel cisim genişlemesi olsun. Eğer E içinde bir kökü olan her $p(x) \in F[x]$ indirgenemez polinomu E üzerinde parçalanırsa E ye F nin bir normal genişlemesi denir (Fraleigh, 2006).

Teorem 3.4.4. $F \leq E \leq K$ bir cisim kulesi ve K, F nin bir sonlu normal genişlemesi olsun. O zaman E den K ya tanımlı F-monomorfizmalarının sayısı $\leq [E:F]$ dir. Bundan başka bu monomorfizmalarının sayısı K dan bağımsızdır; yani, yanlız E ve F ye bağlıdır (Asar ve Arıkan, 2011).

Tanım 3.4.3. $F \leq E \leq K$ bir cisim kulesi ve K, F nin bir sonlu normal genişlemesi olsun. O zaman E den K ya tanımlı F-monomorfizmalarının sayısına E nin F üzerindeki indeksi denir ve $\{E:F\}$ ile gösterilir (Asar ve Arıkan, 2011).

Teorem 3.4.4'ten dolayı $\{E:F\} \leq [E:F]$ dir.

Teorem 3.4.5. K, F nin bir sonlu cisim genişlemesi ve $F \leq E \leq K$ olsun. O zaman $\{K:E\}\{E:F\} = \{K:F\}$ dir (Fraleigh, 2006).

Teorem 3.4.6. F bir cisim ve E, F nin bir sonlu cisim genişlemesi olsun. Aşağıdakiler denktir (Fraleigh, 2006).

(i) E, F nin bir normal genişlemesidir.

(ii) $\{E:F\} = |G(E/F)|$ dir.

Örnek 3.4.3. $E = Q(\sqrt{2})$ olsun. $\{E:Q\}$ yu belirleyelim. E, Q üzerinde parçalanma cismi olduğundan Q nun bir normal genişlemesidir. Örnek 3.3.4'den dolayı

$G(E/Q) = \{\psi_{\sqrt{2},\sqrt{2}}, \psi_{\sqrt{2},-\sqrt{2}}\}$olduğundan $\{E:Q\} = 2$ dir (Asar ve Arıkan, 2011).

3.5. Ayrılabilir Genişlemeler

Tanım 3.5.1. $f(x) \in F[x]$ ve

$$f(x) = a_n x^n + a_{n-1}x^{n-1} \ldots + a_1 x + a_0$$

olsun. O zaman

$$f'(x) = na_n x^{n-1} + (n-1)a_n x^{n-2} + \cdots + a_1$$

polinomuna $f(x)$ in biçimsel türevi denir (Asar ve Arıkan, 2011).

Teorem 3.5.1. $f(x) \in F[x]$ in F nin bir cisim genişlemesi içindeki bir kökü u olsun. u nun çokkatlı kök olması için gerek ve yeter şart $f'(x)$ in bir kökü olmasıdır (Asar ve Arıkan, 2011).

Örnek 3.5.1: p bir asal sayı olmak üzere Z_p üzerinde bir belirsiz t olsun. $Z_p[t]$ polinom halkasının kesirler cismi $Z_p(t)$ ve $p(x) = x^p - t \in Z_p[t]$ olsun. O zaman $p(x)$ indirgenemezdir ve çokkatlı kökü vardır. $p(x)$ in $Z_p(t)$ nin bir cisim genişlemesi içindeki bir kökü u olsun. $u^p - t = \overline{0}$ ve buradan $t = u^p$ olduğundan

$$p(x) = x^p - u^p = (x-u)^p$$

olur. $\text{İnd}\left(u, Z_p(t)\right) = q(x)$ olsun. O zaman $q(x) \mid p(x)$ olduğundan $q(x) = (x-u)^s$ olacak biçimde $1 \leq s \leq p$ vardır. Mümkünse $s < p$ olsun. $q(x)$ in sabit terimi $(-1)^s u^s \in Z_p(t)$ olduğundan $u^s \in Z_p(t)$ olur. Ayrıca $(s,p) = 1$ olduğundan $ms + np = 1$ olacak biçimde m, n tamsayıları vardır. Buradan

$$u = u^{ms+np} = u^{sm}u^{pn} = u^{sm}t^n \in Z_p(t)$$

olduğundan $u \in Z_p(t)$ olur ki, bu çelişkidir; çünkü $u \notin Z_p(t)$ dir. Dolayısıyla $p(x)$, $Z_p(t)$ üzerinde indirgenemezdir. Ayrıca $p(x) = x^p - u^p = (x-u)^p$ olduğundan u çokkatlı köktür (Asar ve Arıkan, 2011).

Tanım 3.5.2. $p(x) \in F[x]$ bir indirgenemez polinom olsun. Eğer $p(x)$ in F üzerindeki bir parçalanma cismi içindeki her kökü basit kök ise $p(x)$ e F üzerinde bir ayrılabilir polinom denir. $f(x) \in F[x]$ sabit olmayan bir polinom olsun. Eğer $f(x)$ in her indirgenemez çarpanı F üzerinde ayrılabilir ise $f(x)$ e F üzerinde bir ayrılabilir polinom denir (Asar ve Arıkan, 2011).

Tanım 3.5.3. F bir cisim E, F nin bir cebirsel genişlemesi ve $u \in E$ olsun. Eğer $\text{İnd}(u, F)$ ayrılabilir ise u ya F üzerinde bir ayrılabilir eleman denir. Eğer E nin her

elemanı F üzerinde ayrılabilir ise E ye F nin bir ayrılabilir cisim genişlemesi denir (Asar ve Arıkan, 2011).

Teorem 3.5.2. F bir cisim ve $kar(F) = 0$ olsun. O zaman F nin her cebirsel genişlemesi ayrılabilir genişlemedir (Asar ve Arıkan, 2011).

Teorem 3.5.3. F bir cisim ve E, F nin bir sonlu cisim genişlemesi olsun. Aşağıdakiler denktir (Asar ve Arıkan, 2011).

(i) E, F nin bir ayrılabilir genişlemesidir.

(ii) $\{E:F\} = [E:F]$ olur.

Tanım 3.5.4. F bir cisim olsun. Eğer F nin her sonlu genişlemesi ayrılabilir genişleme ise F ye bir mükemmel cisim denir (Asar ve Arıkan, 2011).

Sonuç 3.5.1. Karakteristiği sıfır olan her cisim mükemmeldir (Asar ve Arıkan, 2011).

Teorem 3.5.4. $kar(F) = p$ olsun. F nin mükemmel olması için gerek ve yeter şart $F = F^p$ olmasıdır. Burada $F^p = \{a^p : a \in F\}$ (Fraleigh, 2006).

Sonuç 3.5.2. Her sonlu cisim mükemmeldir (Fraleigh, 2006).

Örnek 3.5.2: Örnek 3.5.1'de tanımlanan $Z_p(t)$ cismi mükemmel değildir. Çünkü $p(x) = x^p - t \in Z_p(t)$ üzerinde indirgenemezdir fakat $Z_p(t)$ nin bir cebirsel genişlemesi içinde çokkatlı bir kökü vardır. Dolayısıyla Teorem 3.5.4 gereğince $Z_p(t) \neq Z_p(t)^p$ dir (Asar ve Arıkan, 2011).

3.6. Sonlu Cisimler

Teorem 3.6.1. F bir sonlu cisim ve $kar(F) = p$ olsun. O zaman bir $n \geq 1$ için F, p^n elemanlı bir cisimdir (Fraleigh, 2006).

Sonuç 3.6.1. Bir sonlu cismin her sonlu genişlemesi bir basit genişlemedir (Fraleigh, 2006).

Teorem 3.6.2. F, p^n elemanlı bir cisim ise $1_F x^{p^n} - 1_F x \in \Delta(F)[x]$ polinomunun $\Delta(F)$ üzerindeki bir parçalanma cismidir. Ayrıca p^n elemanlı herhangi iki cisim birbirine izomorftur (Asar ve Arıkan, 2011).

Sonuç 3.6.2. Her sonlu cisim mükemmeldir (Fraleigh, 2006).

Teorem 3.6.3. Her p asal sayısı ve her $n \geq 1$ için p^n elemanlı bir cisim vardır.

Çoğunlukla, Z_p yi içeren p^n elemanlı bir cisim $GF(p^n)$ ile gösterilir ve bu cisme p^n elemanlı bir Galois cismi denir (Rotman, 1998).

Teorem 3.6.4. F bir sonlu cisim olsun. Her $n \geq 1$ için $F[x]$ içinde derecesi n olan bir indirgenemez polinom vardır (Asar ve Arıkan, 2011).

3.7. Galois Genişlemeleri

Tanım 3.7.1. F bir cisim ve E, F nin bir sonlu cisim genişlemesi olsun. Eğer E, F nin bir ayrılabilir normal genişlemesi ise E ye F nin bir Galois genişlemesi ve $G(E/F)$ grubuna da bu genişlemenin Galois grubu denir (Hungerford, 1974).

Örnek 3.7.1. $E = \mathbb{Q}(\sqrt{2})$ olsun. E, $\mathbb{Q}$ üzerinde $x^2 - 2$ nin parçalanma cismidir. Ayrıca Teorem 3.4.2'den dolayı E, $\mathbb{Q}$ nun bir ayrılabilir genişlemesi olduğundan $\mathbb{Q}$ üzerinde Galois dır $[E:\mathbb{Q}] = 2$ olduğu açıktır. Ayrıca Örnek 3.3.4'ten dolayı

$G(E/\mathbb{Q}) = \langle \psi_{\sqrt{2},-\sqrt{2}} \rangle = \{\iota, \psi_{\sqrt{2},-\sqrt{2}}\}$ olduğundan $[E:\mathbb{Q}] = |G(E/\mathbb{Q})|$ dur (Asar ve Arıkan, 2011).

Teorem 3.7.1. F bir cisim ve E, F nin bir sonlu cisim genişlemesi olsun. E nin F üzerinde Galois olması için gerek ve yeter şart $|G(E/F)| = [E:F]$ olmasıdır (Dummit ve Foot, 2004).

Lemma 3.7.1. F bir cisim E, F nin bir Galois genişlemesi ve $F \leq B \leq E$ olsun. O zaman E, B nin bir Galois genişlemesidir (Fraleigh, 2006).

Lemma 3.7.2. F bir cisim E, F nin bir Galois genişlemesi ve $F \leq B \leq E$ olsun. O zaman $E_{G(E/B)} = B$ (Fraleigh, 2006).

Lemma 3.7.3. F bir cisim E, F nin bir Galois genişlemesi, $G = G(E/F)$ ve H, G nin bir altgrubu olsun. O zaman $G(E/E_H) = H$ dır (Fraleigh, 2006).

Teorem 3.7.2. (Galois Teorisinin Temel Teoremi) F bir cisim E, F nin bir Galois genişlemesi ve $G = G(E/F)$ olsun. Ayrıca E nin F yi içeren bütün altcisimlerinin kümesi $Ara(E/F)$ ve G nin bütün altgruplarının kümesi $Alt(G)$ olsun. O zaman her $B \in Ara(E/F)$ için $\theta: B \to G(E/B)$ eşlemesi $Ara(E/F)$ den $Alt(G)$ üzerine bir bire bir eşlemedir. Ayrıca aşağıdakiler sağlanır (Dummit ve Foot, 2004).

(i) Her $B \in Ara(E/F)$ için $B = E_{G(E/B)}$ dir.

(ii) Her $H \in Alt(G)$ için $H = G(E/E_H)$ dir.

(iii) $[E:B] = |G(E/B)|$ ve $[B:F] = |G(E/F):G(E/B)|$ dir.

(iv) B nin F nin bir Galois genişlemesi olması için gerek ve yeter şart $G(E/B) \lhd G(E/F)$ olmasıdır. Bu durumda $G(B/F) \cong G(E/F)/G(E/B)$ dir.

Örnek 3.7.2. $E = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ ve $G = G(E/\mathbb{Q})$ olsun. G nin bütün altgruplarını ve E nin bütün altcisimlerini belirleyelim.

Örnek 3.4.2'de görüldüğü gibi $E, x^3 - 2$ nin $\mathbb{Q}$ üzerindeki parçalanma cismi olduğundan E, F üzerinde Galois dır. Ayrıca, $w = \frac{1}{2}(-1 + i\sqrt{3})$ olmak üzere

$$\sigma: \sqrt[3]{2} \to \sqrt[3]{2}w\,, i\sqrt{3} \to i\sqrt{3}\ ve\ r = \sqrt[3]{2} \to \sqrt[3]{2}\ , i\sqrt{3} \to -i\sqrt{3}$$

olarak tanımlanırsa, $G = \{\iota, \sigma, \sigma^2, r, \sigma r, \sigma^2 r\}$ olur. $\sigma^2, \sigma r, \sigma^2 r$ otomorfizmalarının $\sqrt[3]{2}, i\sqrt{3}$ üzerindeki etkileri aşağıda verilmiştir.

$$\sigma^2: \sqrt[3]{2} \to \sqrt[3]{2}w^2\ , \qquad i\sqrt{3} \to i\sqrt{3}$$
$$\sigma r: \sqrt[3]{2} \to \sqrt[3]{2}w^2\ , \qquad i\sqrt{3} \to -i\sqrt{3}$$
$$\sigma^2 r: \sqrt[3]{2} \to \sqrt[3]{2}w\ , \qquad i\sqrt{3} \to -i\sqrt{3}$$

Örnek 3.7.2'de görüldüğü gibi, $\sigma^3 = \sigma^2 = \iota$ ve $\sigma r = \sigma^2 r$ eşitlikleri sağlanır ve $G \cong S_3$ olur. Buradan sabit cisimlerini belirleyelim. $E_G = \mathbb{Q}\ ve\ E_\iota = E$ olduğu açıktır. Lemma 3.7.1 ve Lemma 3.7.2'den dolayı E, E_σ üzerinde Galois dır ve $[E: E_\sigma] = |\langle\sigma\rangle| = 3$ tür. Şimdi $\sigma(i\sqrt{3}) = i\sqrt{3}$ olduğundan $\mathbb{Q}(\sqrt[3]{2}) \leq E_\sigma$ dir. Ayrıca

$$6 = [E: \mathbb{Q}] = \left[E: \mathbb{Q}(i\sqrt{3})\right]\left[\mathbb{Q}(i\sqrt{3}): \mathbb{Q}\right] = \left[E: \mathbb{Q}(i\sqrt{3}\right] \times 2$$

olduğundan $\left[E: \mathbb{Q}(i\sqrt{3})\right] = 3$ olur. Dolayısıyla $E_\sigma = \mathbb{Q}(i\sqrt{3})$ tür. Benzer biçimde $E_r = \mathbb{Q}(i\sqrt{3})$ tür. Şimdi σr yu belirleyelim. $[E: E_{\sigma r}] = |\langle\sigma r\rangle| = 2$ olmalıdır.

$$\sigma r\left(\sqrt[3]{2}w^2\right) = \sigma\left(r\left(\sqrt[3]{2}w^2\right)\right) = \sigma\left(r\left(\sqrt[3]{2}\right)r(w^2)\right) = \sigma\left(\sqrt[3]{2}w\right) = \sigma\left(\sqrt[3]{2}\right)w = \sqrt[3]{2}w^2$$

olduğundan $\mathbb{Q}(\sqrt[3]{2}w^2) \leq E_r$ dur. Ayrıca $\dot{I}nd(\sqrt[3]{2}w^2, \mathbb{Q}) = x^3 - 2$ olduğundan $\left[\mathbb{Q}\left(\sqrt[3]{2}w^2\right): \mathbb{Q}\right] = 3$ ve buradan, yukarıda olduğu gibi, $E_{\sigma r} = \mathbb{Q}(\sqrt[3]{2}w^2)$ bulunur. Benzer biçimde $E_{\sigma^2 r} = \mathbb{Q}(\sqrt[3]{2}w)$ dir. G nin altgrupları ile E nin altcisimleri arasındaki Galois eşlemesi aşağıda gösterilmiştir (Asar ve Arıkan, 2011).

$$\mathbb{Q}\left(\sqrt[3]{2}, i\sqrt{3}\right) \leftrightarrow \{\iota\}, \qquad \mathbb{Q}\left(i\sqrt{3}\right) \leftrightarrow \langle\sigma\rangle$$
$$\mathbb{Q}\left(\sqrt[3]{2}\right) \leftrightarrow \langle r\rangle, \qquad \mathbb{Q}\left(w^2\sqrt[3]{2}\right) \leftrightarrow \langle\sigma r\rangle$$
$$\mathbb{Q}\left(w\sqrt[3]{2}\right) \leftrightarrow \langle\sigma^2 r\rangle, \qquad G \leftrightarrow \mathbb{Q}$$

Lemma 3.7.4. $s, t \in \mathbb{C}$ olmak üzere $f(x) = x^2 + sx + t$ olsun. $f(x), \mathbb{C}$ üzerinde parçalanır (Asar ve Arıkan, 2011).

Lemma 3.7.5. $f(x) \in R[x]$ ve $der(f(x)) = n$ bir tek tamsayı olsun. O zaman $f(x)$ in bir reel kökü vardır (Asar ve Arıkan, 2011).

Teorem 3.7.3. (Cebirin Temel Teoremi) $C[x]$ in sabit olmayan her polinomu C üzerinde parçalanır (Asar ve Arıkan, 2011).

4. KÖKLERLE ÇÖZÜLEBİLİRLİK

Bu bölümde 2, 3, 4. dereceden polinomlar için çözüm teknikleri aktarılacaktır.

4.1. 2. Dereceden Polinomların Sıfırlarının Bulunuşu

$ax^2 + bx + c = 0$, $a, b, c \in \mathbb{Q}$ ve $a \neq 0$ olsun. Gerekirse eşitliğin her iki yanı a ile bölünerek $a = 1$ alınabilir.

$$x^2 + bx + c = 0$$

denkleminde $x = y - \frac{b}{2}$ konulursa

$$(y - \frac{b}{2})^2 + b(y - \frac{b}{2}) + c = y^2 - by + \frac{b^2}{4} + by - \frac{b^2}{2} + c = y^2 - \frac{b^2}{4} + c = 0$$

elde edilir. Buradan $y^2 = \frac{b^2}{4} - c$ olduğundan kökler $y_{1,2} = \pm\frac{\sqrt{b^2-c}}{2}$ bulunur. Bu değerler x in eşitliğinde yerine konulursa

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

bulunur. Eğer $b^2 - 4c \geq 0$ ise kökler reel, $b^2 - 4c < 0$ ise kökler komplekstir (Asar ve Arıkan, 2011).

4.2. 3. Dereceden Polinomların Sıfırlarının Bulunuşu

$a, b, c \in \mathbb{Q}$ olmak üzere

$$x^3 + ax^2 + bx + c = 0 \tag{4.1}$$

olsun. Bu denklemde $x = y - \frac{a}{3}$ için, sadeleştirmelerden sonra,

$$y^3 + \left(-\frac{a^2}{3} + b\right)y + \left(\frac{2a^3}{27} - \frac{ab}{3} + c\right) = 0 \tag{4.2}$$

bulunur. Burada $p = -\frac{a^2}{3} + b, q = \frac{2a^3}{27} - \frac{ab}{3} + c$ için

$$y^3 + py + q = 0 \tag{4.3}$$

elde edilir. Bu Eş. 4.3 $y = u + v$ için,

$$y^3 = (u + v)^3 = u^3 + 3u^2v + 3uv^2 + v^3 = u^3 + v^3 + 3uvy \tag{4.4}$$

elde edilir. Bu değer Eş. 4.3 yerine konulursa

$$u^3 + v^3 + (3uv + p)y + q = 0$$

elde edilir. Şimdi $3uv + p = 0$ ve böylece $uv = -\frac{p}{3}$ olsun. O zaman

$$u^3 + v^3 = -q \; ve \; u^3v^3 = -\frac{p^3}{27} \tag{4.5}$$

eşitlikleri elde edilir. Dolayısıyla u^3 ve v^3

$$x^2 + qx - \frac{p^3}{27} = 0 \tag{4.6}$$

ikinci derece denkleminin kökleridir. Buradan

$$u^3 = \frac{1}{2}\left(-q + \sqrt{q^2 + \frac{4p^3}{27}}\right),\; v^3 = \frac{1}{2}\left(-q - \sqrt{q^2 + \frac{4p^3}{27}}\right) \tag{4.7}$$

bulunur. $u^3v^3 = -\frac{p^3}{27}$ denkleminin kökleri (u, v) sıralı ikilileri olmak üzere $(u, v), (u, wv), (u, w^2v), (wu, v), (wu, wv), (wu, w^2v), (w^2u, v), (w^2, wv)(w^2u, w^2v)$ olur. Burada $w = \frac{-1+i\sqrt{3}}{2}$ Bunlardan bileşenleri çarpımı $-\frac{p}{3}$ e eşit olanlar $(u, v), (wu, w^2v), (w^2u, wv)$ dir. Dolayısıyla $y^3 + py + q = 0$ denkleminin kökleri olarak $u + v$,$wu + w^2v, w^2u + wv$ bulunur. Buradan Eş. 4.1'in kökleri olarak

$$x_{1=}\, u + v - \frac{a}{3}, x_2 = wu + w^2v - \frac{a}{3}, x_3 = w^2u + wv - \frac{a}{3} \tag{4.8}$$

bulunur. Bu formüllere Cardano formülleri denir (Tignol, 2001).

4.3. 4. Dereceden Polinomların Sıfırlarının Bulunması

$a, b, c, d \in \mathbb{Q}$ olmak üzere

$$ax^4 + bx^3 + cx^2 + dx + e = 0 \tag{4.9}$$

şeklindedir. Bu denklemin köklerinin elde edilmesi üçüncü dereceden bir denkleme indirgemeyle elde edilir. Gerçekten Eş. 4.9'da $a \neq 0$ olduğu göz önüne tutularak,

$$x^4 + \frac{b}{a}x^3 = -\frac{c}{a}x^2 - \frac{d}{a}x - \frac{e}{a} \tag{4.10}$$

şeklinde yazıldıktan sonra eşitliğin iki tarafına $b^2x^2/4a^2$ ilave edilerek; birinci taraf bir tam kare olur, yani

$$(x^2 + \frac{b}{2a}x)^2 = \frac{b^2-4ac}{4a^2}x^2 - \frac{d}{a}x - \frac{e}{a} \tag{4.11}$$

elde edilir. Şimdi Eş. 4.11'de eşitliğinin iki tarafına $(x^2 + bx/2a)y + y^2/4$ ifadesini ilave edelim. Birinci taraf yine bir tam kare olup $(x^2 + bx/2a + 2)^2$ şeklindedir; böylece Eş. 4.1'i

$$(x^2 + \frac{b}{2a}x + \frac{1}{2}y)^2 = (y + \frac{b^2-4ac}{4a^2})x^2 + \left(\frac{b}{2a}y - \frac{d}{a}\right)x + (\frac{1}{4}y^2 - \frac{e}{a}) \tag{4.12}$$

şeklini alır. Eş. 4.11'de birinci taraf gibi ikinci tarafının da bir tam kare olması için

$$\left(\frac{b}{2a}y-\frac{d}{a}\right)^2-4(y+\frac{b^2-4ac}{4a^2})(\frac{1}{4}y^2-\frac{e}{a})=0 \tag{4.13}$$

elde edilmesi veya y nin kuvvetlerine göre sıralandıktan sonra

$$y^3-\frac{c}{a}y^2-\frac{bd-4ac}{a^2}y+\frac{4ace-b^2e-ad^2}{a^3}=0 \tag{4.14}$$

olmalıdır. Eş. 4.13'de Eş. 4.14'nin köklerinden biri alındığı taktirde bu eşitliğin ikinci tarafı $Ax+B$ gibi birinci dereceden bir ifadenin karesi olacaktır. Böylece, Eş. 4.12'i yerine buna eşdeğer olan

$$x^2+\frac{b}{2a}x+\frac{1}{2}y=\ Ax+B,\ x^2+\frac{b}{2a}x+\frac{1}{2}y=\ -(Ax+B) \tag{4.15}$$

denklemleri elde edilir. Bu Eş. 4.15'nin kökleri;

$$(x^2+\frac{b}{2a}x+\frac{1}{2}y)^2=(y+\frac{b^2-4ac}{4a^2})x^2+\left(\frac{b}{2a}y-\frac{d}{a}\right)x+(\frac{1}{4}y^2-\frac{e}{a}) \tag{4.16}$$

denkleminin ve dolayısıyla

$$u^3+v^3+(3uv+p)y+q=0 \tag{4.17}$$

denkleminin dört kökünden ibarettir (Süray, 1970).

Örnek 4.2.1: $f(x)=x^3-3x-1$ polinomunun köklerini Cardano formüllerini uygulayarak bulalım. $p=-3$ ve $q=-1$ dir. Bu değerler;

$$u^3=\frac{1}{2}\left(-q+\sqrt{q^2+\frac{4p^3}{27}}\right),\ v^3=\frac{1}{2}\left(-q-\sqrt{q^2+\frac{4p^3}{27}}\right)$$

eşitliklerinde yerine konulursa

$$u^3=\frac{1}{2}\left(1+\sqrt{1+\frac{4(-3)^3}{27}}\right)=\frac{(1+\sqrt{-3})}{2}=\frac{(1+i\sqrt{3})}{2}\text{ ve }\ v^3=\frac{(1-i\sqrt{3})}{2}$$

bulunur. Dolayısıyla $f(x)$ in kökleri $w=\frac{(-1+i\sqrt{3})}{2}$ olmak üzere,

$$x_1=\sqrt[3]{\frac{1}{2}(1+i\sqrt{3})}+\sqrt[3]{\frac{1}{2}(1-i\sqrt{3})}$$

$$x_2=\sqrt[3]{\frac{1}{2}(1+i\sqrt{3})}w+\sqrt[3]{\frac{1}{2}(1-i\sqrt{3})}w^2$$

$$x_3=\sqrt[3]{\frac{1}{2}(1+i\sqrt{3})}w^2+\sqrt[3]{\frac{1}{2}(1-i\sqrt{3})}w$$

olarak bulunur. Burada $\frac{(1+i\sqrt{3})}{2}=\cos\frac{\pi}{3}+i\sin\frac{\pi}{3}$ sayısının bir küp kökü,

$t = \cos\frac{\pi}{9} + i\sin\frac{\pi}{9}$ olduğundan $\sqrt[3]{u} = t$ ve $\sqrt[3]{v} = \bar{t}$. Buradan

$$\sqrt[3]{u} + \sqrt[3]{v} = t + \bar{t} = 2\cos\frac{\pi}{9},$$

$$(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3})(\cos\frac{\pi}{9} + i\sin\frac{\pi}{9}) = \cos\frac{7\pi}{9} + i\sin\frac{7\pi}{9}$$

olduğundan

$$\sqrt[3]{u}w + \sqrt[3]{v}w^2 = (\cos\frac{7\pi}{9} + i\sin\frac{7\pi}{9}) + (\cos\frac{7\pi}{9} - i\sin\frac{7\pi}{9}) = 2\cos\frac{7\pi}{9}$$

ve

$$(\cos\frac{2\pi}{3} - i\sin\frac{2\pi}{3})(\cos\frac{\pi}{9} + i\sin\frac{\pi}{9}) = \cos(-\frac{5\pi}{9}) + i\sin(-\frac{5\pi}{9})$$

olduğundan

$$\sqrt[3]{u}w^2 + \sqrt[3]{v}w = (\cos\frac{5\pi}{9} - i\sin\frac{5\pi}{9}) + (\cos\frac{5\pi}{9} + i\sin\frac{5\pi}{9}) = 2\cos\frac{5\pi}{9}$$

bulunur. Dolayısıyla

$$x_1 = 2\cos\frac{\pi}{9},$$

$$x_2 = 2\cos\frac{7\pi}{9},$$

ve

$$x_3 = 2\cos\frac{5\pi}{9}$$

olup bütün kökler reeldir (Asar ve Arıkan, 2011).

Örnek 4.3.2. $f(x) = x^4 - 3x - 2 = 0$ denkleminin köklerinin bulunuz.

$a = 1, b = 0, c = 0, d = -3, e = -2$ olduğundan denklemi $y^3 + 8y - 9 = 0$ şeklindedir. Bu denklemin köklerinden birinin $y = 1$ olduğu görülmektedir. Bu değer

$$(x^2 + \frac{b}{2a}x + \frac{1}{2}y)^2 = (y + \frac{b^2 - 4ac}{4a^2})x^2 + \left(\frac{b}{2a}y - \frac{d}{a}\right)x + (\frac{1}{4}y^2 - \frac{e}{a})$$

$$(x^2 + \frac{1}{2})^2 = x^2 + 3x + \frac{1}{4} + 2 = (x + \frac{3}{2})^2$$

veya

$$x^2 - x - 1 = 0\,, x^2 + x + 2 = 0$$

denklemleri elde edilir; bunlar sıra ile

$$x_1 = \frac{-1+i\sqrt{7}}{2}\,, x_2 = \frac{-1-i\sqrt{7}}{2}\,,\ x_3 = \frac{1+\sqrt{5}}{2}, x_4 = \frac{1-\sqrt{5}}{2}$$

köklerine sahiptirler. Verilen denklem x in ikisi kompleks ve ikisi reel olan bu dört değeri kök olarak kabul eder.

Tanım 4.1. F bir cisim ve E, F nin bir sonlu cisim genişlemesi olsun. Eğer F den E ye bir cisim kulesi

$$F = F_0 \leq F_1 \leq \cdots \leq F_t = E$$

varsa öyle ki; $1 \leq i \leq t$ için $F_i = F_{i-1}(u_i)$ ve ${u_i}^{n_i} \epsilon\, F_{i-1}$ olacak biçimde bir $u_i \in E$ ve $n_i \geq 1$ olsun, o zaman E ye F nin bir kök genişlemesi ve bu cisim kulesine de bir kök kulesi denir.

Yukarıdaki tanımda her $1 \leq i \leq t$ için ${u_i}^{n_i} = a_i$ konulursa o zaman $u_i, x^{n_i} - a_i = 0$ ın bir çözümü olur. Burada $u_i = \sqrt[n_i]{a_i}$ konulursa $E = F(\sqrt[n_1]{a_1}, \sqrt[n_2]{a_2}, \dots, \sqrt[n_t]{a_t})$ olur (Fraleigh, 2006).

Tanım 4.2: F bir cisim ve $f(x)$, $F[x]$ in sabit olmayan bir polinomu olsun. Ayrıca $f(x)$ in F üzerinde bir parçalanma cismi K olsun. Eğer F nin K yı içeren bir kök genişlemesi varsa $f(x) = 0_F$ denklemi F üzerinde köklerle çözülebilir denir.

$E = F(\sqrt[n_1]{a_1}, \sqrt[n_2]{a_2}, \dots, \sqrt[n_t]{a_t})$ olacak biçimde $a_1, \dots, a_t \in E$ vardır. Böylece $f(x) = 0_F$ denkleminin E içindeki çözümleri $\sqrt[n_1]{a_1}, \sqrt[n_2]{a_2}, \dots, \sqrt[n_t]{a_t}$ köklerinin monomlarının F-lineer kombinasyonları olur (Fraleigh, 2006).

Örnek 4.3. $f(x) = x^2 + bx + c \in Q[x]\ olsun.\ f(x)$ in kökleri

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

dir. Şimdi $Q \leq Q\left(\sqrt{b^2 - 4c}\right)$ ve $(\sqrt{b^2 - 4c})^2 = b^2 - 4c \in Q$ olduğundan $Q\left(\sqrt{b^2 - 4c}\right)$, Q nun bir kök genişlemesidir ve $x_1, x_2 \in Q(\sqrt{b^2 - 4c})$ olduğundan $f(x) = 0$ denklemi Q üzerinde köklerle çözülebilir (Asar ve Arıkan, 2011).

Lemma 4.1. $F \leq B \leq L$ bir cisim kulesi, $kar(F) = 0$, L, F nin bir sonlu cisim genişlemesi ve B, F nin bir normal genişlemesi olsun. Ayrıca bir $v \in L$ ve $k \geq 1$ için $L = B(v)$ ve $v^k \in B$ olsun. O zaman L nin öyle bir cisim genişlemesi N vardır ki N, B nin bir kök genişlemesi ve F nin bir normal genişlemesidir (Fraleigh, 2006).

Lemma 4.2. $F, kar(F) = 0$ olan bir cisim ve $f(x)$, $F[x]$ sabit olmayan bir polinom olsun. Eğer $f(x) = 0_F$ denklemi F üzerinde köklerle çözülebilirse o zaman F nin öyle bir normal kök genişlemesi N vardır ki N, $f(x)$ in F üzerindeki bir parçalanma cismini içerir (Fraleigh, 2006).

Lemma 4.3. $F, kar(F) = 0$ olan bir cisim olsun ve birimin bir ilkel n yinci kökünü içersin. Ayrıca $a \in F$ olmak üzere $x^n - a$ polinomunun F nin bir cisim genişlemesi içindeki bir kökü u olsun. Aşağadakiler sağlanır (Fraleigh, 2006).

(i) $F(u)$, F nin bir Galois genişlemesidir.

(ii) $G(F(u)/F)$ Galois grubu devirlidir.

Teorem 4.1. $F, kar(F) = 0$ olan bir cisim ve E, F nin bir normal kök genişlemesi olsun. O zaman $G(E/F)$ Galois grubu çözülebilirdir (Asar ve Arıkan, 2011).

Teorem 4.2. $F, kar(F) = 0$ olan bir cisim, $f(x), F[x]$ sabit olmayan bir polinom ve $f(x)$ in F üzerindeki bir parçalanma cismi K olsun. Eğer $f(x) = 0_F$ denklemi F üzerinde köklerle çözülebilirse o zaman $G(E/F)$ Galois grubu çözülebilirdir (Fraleigh, 2006).

Teorem 4.3. $F, kar(F) = 0$ olan bir cisim ve E, F nin bir Galois genişlemesi olsun. Eğer $G(E/F)$ Galois grubu çözülebilir ise o zaman F nin E yi içeren bir kök genişlemesi vardır (Fraleigh, 2006).

Teorem 4.4. Beşinci dereceden köklerle çözülemeyen bir $f(x) \in Q[x]$ polinomu vardır.

İspat:

$$f(x) = 2x^5 - 5x^4 + 5 \; olsun.$$

(a) $f(x) = 2x^5 - 5x^4 + 5$, Q üzerinde indirgenemezdir. Gerçekten $p = 5$ için Eisenstain indirgenemezlik kriterine göre $f(x)$ indirgenemezdir.

(b) $f(x)$ in üç reel kökü ve iki reel olmayan kökü vardır. $f(x)$ in türevi alınırsa

$$f'(x) = 10x^4 - 20x^3 = 0 \Rightarrow 10x^3(x-2) = 0 \Rightarrow x = 0 \text{ ve } x = 2$$

bulunur. Kolayca görülebileceği gibi, f fonksiyonu, $(-\infty, 0]$ aralığında artan, $[0, 2]$ aralığında azalan, ve $[2, \infty)$, aralığında artandır. $f(-1) = -2 < 0$ ve $f(0) = 5 > 0$ olduğundan bir $a_1 \in (-2, 0)$ için $f(a_1) = 0$ dır. $f(0) = 5 > 0$ ve $f(2) = -11 < 0$ olduğundan bir $a_2 \in (0, 2)$ için $f(a_2) = 0$ dır. Son olarak $f(2) = -11 < 0$ ve $f(3) = 86 > 0$ oduğundan bir $a_3 \in (2,3)$ için $f(a_3) = 0$ dır. Böylece $f(x)$ in bütün reel kökleri a_1, a_2 ve a_3 tür.

$f(x)$ in reel olmayan kompleks kökleri b_1 ve b_2 olsun. O zaman $f(x)$ in parçalanma cismi $K = Q(a_1, a_2, a_3, b_1, b_2)$ olur.$G = G(K/Q)$ olsun. Eğer G nin çözülebilir olmadığını gösterebilirsek Teorem 4.2 den dolayı , $f(x)$ köklerle çözülemez.

K, Q üzerinde Galois olduğundan , $[K:Q] = |G|$ dir. Ayrıca $[Q(a_1):Q] = 5$ olduğundan $5\big||G|$ dir. $\sigma \in G$ olsun. σ, $\{a_1, a_2, a_3, b_1, b_2\}$ kümesi üzerinde bir permütasyon tanımlar ve bu permütasyona karşılık $\{1,2,3,4,5\}$ üzerinde $\bar{\sigma}$ permütasyonu tanımlanır. Ayrıca $\sigma \to \bar{\sigma}$ eşlemesi $G\ den\ S_5$ içine bir monomorfizmadır. $G\ nin\ S_5$ içindeki görüntüsü $\bar{G}$ olsun. $5\big||G|$ olduğundan $\bar{G}$ nin mertebesi 5 olan bir elemanı vardır. $r = \{1,2,3,4,5\}$ olsun. S_5 içinde mertebesi 5 olan her eleman $5-$ devri olduğundan r ile eşleniktir. Dolayısıyla bir $s \in S_5$ için $srs^{-1} \in \bar{G}$ dır. Böylece $\{t_1, t_2, t_3, t_4, t_5\} = \{1,2,3,4,5\}$ olmak üzere $srs^{-1} = \{t_1, t_2, t_3, t_4, t_5\}$ tir. Öte yandan, $b_1, b_2 \notin \mathbb{Q}(a_1, a_2, a_3)$ olduğundan öyle bir $r \in G$ vardır ki,
$r(b_1) = b_2, r(b_2) = b_1$ ve $r, Q(a_1, a_2, a_3)$ ü sabit bırakır. Şimdi
$b_1 = a_4$ ve $b_2 = a_5$ olarak tanımlanırsa $\bar{r} = (4,5)$ olur. Ayrıca
$(srs^{-1})^k = \{4,5, c_1, c_2, c_3\}$ olacak biçimde $\{c_1, c_2, c_3\} = \{1,2,3\}$ ve $k \geq 1$ tamsayısı vardır.

$$(4,5, c_1, c_2, c_3)(4,5)(4,5, c_1, c_2, c_3)^{-1} = (5, c_1)$$

ve

$$(4,5, c_1, c_2, c_3)(5, c_1)(4,5, c_1, c_2, c_3)^{-1} = (c_1, c_2)$$

olduğundan $(5, c_1), (c_1, c_2) \in \bar{G}$ dır. Ayrıca $(4,5) \in \bar{G}$ olduğundan,$\langle (4,5), (c_1, c_2) \rangle$, $\bar{G}$ nin mertebesi 4 olan bir altgrubudur. Dolayısıyla $4\big||\bar{G}|$ dır. Ayrıca
$(4,5), (c_1, c_2) = (4,5, c_1) \in \bar{G}$ olduğundan, $3\big||\bar{G}|$ dır. Dolayısıyla $3\times 4 \times 5 = 60$ sayısı $|\bar{G}|$ sayısını böler. Öte yandan S_5 içinde mertebesi 60 olan tek altgrubu A_5 olduğundan, $A_5 \leq \bar{G}$ olmalıdır. Üstelik $(4,5) \in {}^{\bar{G}}/_{A_5}$ olduğundan $\bar{G} = S_5$ olmalıdır. Buradan

G $\cong S_5$ bulunur. Fakat Sonuç 3.4'ten dolayı S_5 çözülebilir olmadığından, G çözülebilir değildir. Dolayısıyla Teorem 4.2 gereğince, $f(x) = 2x^5 - 5x^4 + 5$ polinomu Q üzerinde köklerle çözülemez (Asar ve Arıkan, 2011).

4.4. Simetrik Fonksiyonlar ve N. Dereceden Genel Polinomların Galois Grubu

F bir cisim ve E, F nin bir cisim genişlemesi olsun. F üzerinde n tane belirsizin polinom halkası $F[x_1, x_2, \dots, x_n]$ ve $u_1, \dots, u_n \in E$ olsun.
$\emptyset_{u_1,\dots,u_n}: F[x_1, x_2, \dots, x_n] \to E$,
$\emptyset_{u_1,\dots,u_n}\big(F(x_1, x_2, \dots, x_n)\big) = F(u_1, \dots, u_n)$ ve $\emptyset_{u_1,\dots,u_n}|F = \tau_F$ biçiminde tanımlı

$\emptyset_{u_1,\dots,u_n}$ fonksiyonunu göz önüne alalım. Bir belirsizin polinom halkasında olduğu gibi $\emptyset_{u_1,\dots,u_n}$ bir halka homomorfizmasıdır ve buna da bir değer homomorfizması denir.

Şimdi $F[x_1, x_2, \dots, x_n]$ in kesirler cismi $F(x_1, x_2, \dots, x_n)$ yi $\sigma \in S_n$ olmak üzere $\emptyset_{x_{\sigma(1)},\dots,x_{\sigma(n)}}: F[x_1, x_2, \dots, x_n] \to F(x_1, x_2, \dots, x_n)$ değer homomorfizmasını göz önüne alalım. $\bar{\sigma} = \emptyset_{x_{\sigma(1)},\dots,x_{\sigma(n)}}$ ve $F(x_1, x_2, \dots, x_n) \in Ker(\bar{\sigma})$ olsun. O zaman $f\left(x_{\sigma(1)}, \dots, x_{\sigma(n)}\right) = 0_F$ dir. $F(x_1, x_2, \dots, x_n)$, $i_1, \dots, i_n$ doğal sayılar olmak üzere

$$a_{i_1 \dots i_n} x^{i_1} \dots x^{i_n}$$

tipindeki monomların bir sonlu toplamı olduğundan $f\left(x_{\sigma(1)}, \dots, x_{\sigma(n)}\right), \bar{\sigma}(a_{i_1 \dots i_2} x^{i_1} \dots x^{i_n}) = a_{i_1 \dots i_2} x_{\sigma(1)}^{i_1} \dots x_{\sigma(n)}^{i_n}$ tipindeki monomların bir sonlu toplamıdır. Üstelik $\left\{x_{\sigma(1)}, \dots, x_{\sigma(n)}\right\} = \{x_1, \dots, x_n\}$ olduğundan $j_1, \dots, j_n$ doğal sayılar olmak üzere

$$a_{i_1 \dots i_2} x_{\sigma(1)}^{i_1} \dots x_{\sigma(n)}^{i_n} = a_{i_1 \dots i_2} x^{j_1} \dots x^{j_n}$$

dir. $f\left(x_{\sigma(1)}, \dots, x_{\sigma(n)}\right) = 0_F$ demek $f\left(x_{\sigma(1)}, \dots, x_{\sigma(n)}\right)$ ın her teriminin $= 0_F$ olması demek her $a_{i_1 \dots i_n} = 0_F$ ve buradan $f(x_1, \dots, x_n) = 0_F$ bulunur. Böylece $\bar{\sigma}, F[x_1, \dots, x_n]$ den $F[x_1, \dots, x_n]$ ye F yi sabit bırakan bir monomorfizmadır. Dolayısıyla Sonuç 4.1 gereğince $\bar{\sigma}, f(x_1, \dots, x_n)$ nin bir otomorfizmasına genişler. Bu otomorfizma da $\bar{\sigma}$ ile gösterilsin. O zaman her $\frac{f(x_1,\dots,x_n)}{g(x_1,\dots,x_n)} \in F(x_1, \dots, x_n)$ için

$$\bar{\sigma}\left(\frac{f(x_1, \dots, x_n)}{g(x_1, \dots, x_n)}\right) = \frac{f\left(x_{\sigma(1)}, \dots, x_{\sigma(n)}\right)}{g\left(x_{\sigma(1)}, \dots, x_{\sigma(n)}\right)}$$

dir. Şimdi $\overline{S_n} = \{\bar{\sigma}: \sigma \in S_n\}$ olsun. Kolayca görülebilieceği gibi, $\bar{\sigma} \to \sigma$ eşlemesi $\overline{S_n}$ den S_n ye bir halka izomorfizmasıdır (Asar ve Arıkan, 2011).

Tanım 4.4.1. $\frac{f(x_1,\dots,x_n)}{g(x_1,\dots,x_n)} \in F(x_1, \dots, x_n)$ olsun. Her $\sigma \in S_n$ için

$$\bar{\sigma}\left(\frac{f(x_1, \dots, x_n)}{g(x_1, \dots, x_n)}\right) == \frac{f\left(x_{\sigma(1)}, \dots, x_{\sigma(n)}\right)}{g\left(x_{\sigma(1)}, \dots, x_{\sigma(n)}\right)} = \frac{f(x_1, \dots, x_n)}{g(x_1, \dots, x_n)}$$

ise $\frac{f(x_1,\dots,x_n)}{g(x_1,\dots,x_n)}$ ye F üzerinde $x_1, \dots, x_n$ nin bir simetrik fonksiyonu denir.

Böylece bütün simetrik fonksiyonlar $\overline{S_n}$ in $f(x_1, \dots, x_n)$ içindeki sabit cismini oluşturur. Bu cisim K olsun.

Şimdi $f(x_1, \dots, x_n)$ üzerinde bir t belirsizinin polinom halkası $f(x_1, \dots, x_n)[t]$ yi göz önüne alalım ve

$$f(t) = \prod_{i=1}^{n}(t - x_i)$$

olsun. $\bar{\sigma} \in \overline{S_n}$ ve $\bar{\sigma}$ nin $f(x_1, \dots, x_n)[t]$ ye

$$\frac{f\left(x_{\sigma(1)}, \dots, x_{\sigma(n)}\right)}{g\left(x_{\sigma(1)}, \dots, x_{\sigma(n)}\right)} = \frac{f(x_1, \dots, x_n)}{g(x_1, \dots, x_n)}$$

ise $\frac{f(x_1,\dots,x_n)}{g(x_1,\dots,x_n)}$ ye F üzerinde $x_1, \dots, x_n$ nin bir simetrik fonksiyonu denir.

Böylece bütün simetrik fonksiyonlar $\overline{S_n}$ in $f(x_1, \dots, x_n)$ genişlemesi $\overline{\sigma_t}$ olsun. O zaman

$$\overline{\sigma_t}(f(t)) = \overline{\sigma_t}(\prod_{i=1}^{n}(t - x_i)) = \prod_{i=1}^{n}(t - x_{\sigma(i)}) = \prod_{i=1}^{n}(t - x_i) = f(t)$$

olduğundan $\overline{\sigma_t}$, $f(t)$ nin katsayılarını sabit bırakır. Buradan $f(t) \in K[t]$ bulunur. Öte yandan $f(t)$ nin sağ yanı açılır ve t nin kuvvetlerine göre düzenlenirse

$$s_1 = \sum_{i=1}^{n} x_i \text{ ve her } i \geq 2 \text{ için } s_j = \sum_{1 \leq i_1 < \dots < i_j} x_{i_1} \dots x_{i_j}$$

olmak üzere $f(t) = t^n - s_1 t^{n-1} + \dots + (-1)^n s_n$ elde edilir. Her $\bar{\sigma} \in \overline{S_n}$ ve her $1 \leq i \leq n \, için \, \bar{\sigma}(s_i) = s_i$ olduğundan $s_i \in K$ dır (Stewart, 1945).

Tanım 4.4.2. Her $1 \leq i \leq n$ için s_i ye $x_1, \dots, x_n$ nin i yinci elemanter simetrik fonksiyonu denir (Stewart, 1945).

Kolayca görüldüğü gibi

$$s_1 = x_1 + x_2 + \dots + x_n \text{ ve } s_n = x_1 x_2 \dots x_n$$

olur.

$n = 2$ için elemanter simetrik fonksiyonlar

$$s_1 = x_1 + x_2, \qquad s_2 = x_1 x_2$$

ve $n = 3$ için elemanter simetrik fonksiyonlar

$$s_1 = x_1 + x_2 + x_3, \; s_2 = x_1 x_2 + x_1 x_3 + x_2 x_3, \; s_3 = x_1 x_2 x_3$$

olur.

Şimdi $E = f(s_1, \dots, s_n)$ olsun. O zaman $E \leq K$ dır. Ayrıca $f(t) \in E[t]$ olduğundan $f(x_1, \dots, x_n), f(t)$ nin E üzerindeki bir parçalanma cismidir ve $f(t)$ nin bütün kökleri birbirinden farklı olduğundan E nin bir ayrılabilir genişlemesidir. Böylece $f(x_1, \dots, x_n)$,E üzerinde Galois'dır. $G = G(F(x_1, \dots, x_n)/E)$ olsun. O zaman $[(F(x_1, \dots, x_n): E] = |G|$ dir. Ayrıca $E \leq K \leq F(x_1, \dots, x_n)$ olduğundan $F(x_1, \dots, x_n)$, K nın bir Galois genişlemesidir. Şimdi $\overline{S_n} \leq G(F(x_1, \dots, x_n)/K)$ ve Teorem 3.4.1 den

dolayı $[F(x_1,\dots,x_n):K] \le n!$ olduğundan $[F(x_1,\dots,x_n):K] = |\overline{S_n}| = n!$ dir. Buradan özel olarak $|G| \ge n!$ bulunur. Fakat $F(x_1,\dots,x_n)$, F üzerinde $f(t)$ nin bir parçalanma cismi olduğundan Teorem 3.4.2'den dolayı $|G| \le n!$ ve böylece $|G| = n!$ bulunur. Buradan $G = \overline{S_n}$ olur. Özel olarak $G \cong \overline{S_n}$ dir. Öte yandan $[F(x_1,\dots,x_n):K] = |\overline{S_n}|$ olduğundan $K = E$ dir. Böylece aşağıdaki sonuç elde edilir.

Teorem 4.4.1. (Simetrik Fonksiyon Teoremi) F bir cisim ve $x_1,\dots,x_n$, F tane belirsiz olsun. Ayrıca $x_1,\dots,x_n$ üzerinde tanımlı elemanter simetrik fonksiyonlar $s_1,\dots,s_n$ olsun. O zaman $F(s_1,\dots,s_n)$ bütün simetrik fonksiyonlar kümesidir. Ayrıca $F(x_1,\dots,x_n), F(s_1,\dots,s_n)$ nin bir Galois genişlemesidir ve

$$G(F(x_1,\dots,x_n)/F(s_1,\dots,s_n)) \cong S_n$$

dir (Asar ve Arıkan, 2011).

4.5. N. Dereceden Genel Polinom

F bir cisim, F üzerinde n tane $x_1,\dots,x_n$ belirsizinin rasyonel fonksiyonlar cismi $F(x_1,\dots,x_n)$ ve $F(x_1,\dots,x_n)$ üzerinde bir belirsiz t olsun. O zaman

$$g_n(t) = t^n - x_1 t^{n-1} + \cdots + (-1)^n x_n$$

polinomuna F üzerinde n yinci dereceden bir genel polinom denir. $g_n(t)$ ye genel polinom denilmesinin nedeni şöyle açıklanabilir.$F[t]$ içinde n yinci dereceden her monik polinom , $x_1,\dots,x_n$ yerine F nin uygun elemanları seçilerek $g_n(t)$ den elde edilir. Gerçekten $f(t) = t^n - a_1 t^{n-1} + \cdots + (-1)^n a_n \in F[t]$ olsun. O zaman her x_i yerine a_i konularak tanımlanan $\emptyset_{u_1,\dots,u_n}: F(x_1,\dots,x_n)[t] \to F[t]$ değer homomorfizması altında $g_n(t)$ nin görüntüsü $f(t)$ dir. Dolayısıyla eğer $g_n(t) = 0$ polinom denkleminin çözümleri için $x_1,\dots,x_n$ cinsinden formül varsa o zaman bu formülde $x_1,\dots,x_n$ yerine $a_1,\dots,a_n$ konularak $f(t) = 0$ polinom denkleminin çözümleri elde edilir. Örneğin $n = 2$ için $Q(x_1,\dots,x_n)[t]$ içindeki genel polinom $g_{2(t)} = t^2 - x_1(t) + x_2$ ve $g_{2(t)} = 0$ ın çözümleri $t_{1,2} = \frac{x_1 \pm \sqrt{x_1^2 - 4x_2}}{2}$ dir. Buradan $t^2 - 2t - 1 = 0$ ın çözümleri $t_{1,2} = \frac{2 \pm \sqrt{4+4}}{2} = 1 \pm \sqrt{2}$ bulunur (Fraleigh, 2006).

Teorem 4.5.1. F bir cisim, F üzerinde tanımlı bir genel polinom

$$g_n(t) = t^n - x_1 t^{n-1} + \cdots + (-1)^n x_n$$

ve $g_n(t)$ nin $F(x_1, \dots, x_n)$ üzerindeki parçalanma cismi K olsun. O zaman K, $F(x_1, \dots, x_n)$ üzerinde Galois'dır ve $G(K/F(x_1, \dots, x_n)) \cong s_n$ dir (Fraleigh, 2006).

Sonuç 4.5.1. F karakteristiği sıfır olan bir cisim olsun. $n \geq 5$ için n yinci dereceden bir genel polinom $g_n(t) = t^n - x_1 t^{n-1} + \cdots + (-1)^n x_n$, $F(x_1, \dots, x_n)$ üzerinde köklerle çözülemez.

İspat :

$g_n(t)$ nin $F(x_1, \dots, x_n)$ üzerindeki parçalanma cismi K ve

$$G(K/F(x_1, \dots, x_n))$$

olsun. Teorem 4.4.2'den dolayı $G \cong S_n$ dir. Sonuç 3.4'ten dolayı $n \geq 5$ için s_n çözülebilir olmadığından Teorem 4.2'den dolayı $g_n(t), F(x_1, \dots, x_n)$ üzerinde köklerle çözülemez (Fraleigh, 2006).

5. PALİNDROMİK POLİNOM

4. kesimde 5. dereceden polinomların sıfırlarının çözümü için bir genel formül verilemeyeceği gösterilmişti. Bir genel formül verilemeyeceği ifadesi özel durumlar için formüller verilebileceğine işaret eder. Bu tür polinomlardan biri palindromik polinomlardır ve yapısı gereği genel bir formül verilebilir.

Bu kesim palindromik polinomların sıfırlarının hesabı için genel çözümleri kapsar.

Tanım 5.1. $P(x) \in Q[x]$ polinomu

$$P(x) = a_n x^n + a_{n-1} x^n + \cdots + a_1 x + a_0$$

olarak verilsin. Eğer $i = 0,1, \dots, n$ için

$$a_{n-i} = a_i$$

ise $P(x)$ polinomuna Q üstünde palindromik polinom denir (Sun ve ark., 2015).

5.1. Palindromik Polinomların Kökleri

$$P(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_i x^{n-i} + \cdots + a_1 x + 1$$

palindromik polinomu verilsin. $P(x)$ in n-tane kökünün $\alpha_1, \alpha_2, \dots, \alpha_n$ olduğunu varsayalım. Bu durumda

$$P(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$$

yazılabilir.

Her monik palindromik polinom için sabit terim 1 olduğundan,

$$\begin{aligned} 1 &= (-\alpha_1)(-\alpha_2) \dots (-\alpha_n) \\ &= \alpha_1 . \alpha_2 \dots \alpha_n . (-1)^n \\ &= \alpha_1 . \alpha_2 \dots \alpha_n = (-1)^n \end{aligned}$$

yazılabilir.

$n = 2$ için, sıfırlar α_1 ve α_2 dir ve ayrıca, $\alpha_2 = \frac{1}{\alpha_1}$ ve $\alpha_1 = \frac{1}{\alpha_2}$

$P(x) = x^2 + bx + 1$ için,

$$\alpha_1 = \frac{-b + \sqrt{b^2 - 4}}{2}$$

$$\alpha_2 = \frac{-b - \sqrt{b^2 - 4}}{2}$$

olduğu bilinmektedir. $\alpha_2 = \frac{1}{\alpha_1}$ i irdelersek

$$\frac{1}{\alpha_1} = \frac{1}{\frac{-b + \sqrt{b^2 - 4}}{2}} = \frac{2}{-b + \sqrt{b^2 - 4}} = \frac{-b - \sqrt{b^2 - 4}}{2} = \alpha_2$$

elde edilir.

$n = 3$ için $P(x) = x^3 + ax^2 + ax + 1$ palindromik polinomların genel formudur. Sıfırlar

$\alpha_1, \alpha_2, \alpha_3$ ise,

$$\alpha_1 . \alpha_2 . \alpha_3 = (-1)^3 = -1$$

olur. -1, 3. dereceden palindromik polinomlar için sıfırdır. Şöyle ki;

$$P(-1) = (-1)^3 + a(-1)^2 + a(-1) + 1 = 0$$

$\alpha_1 = -1$ alırsak, $\alpha_2 . \alpha_3 = 1$ veya $\alpha_3 = \frac{1}{\alpha_2}$ olur. Buna ek olarak

$$P(x) = x^3 + ax^2 + ax + 1 = (x + 1)(x - \alpha_2)(x - \alpha_3)$$
$$= x^3 + (1 - \alpha_2 - \alpha_3)x^2 + (\alpha_2 . \alpha_3 - \alpha_3 - \alpha_2)x + \alpha_2 . \alpha_3$$
$$= x^3 + (1 - \alpha_2 - \alpha_3)x^2 + (1 - \alpha_3 - \alpha_2)x + 1$$

(burada $\alpha_1 = -1$ ve $\alpha_2 . \alpha_3$=1 olduğu kullanıldı). Bu nedenle $\alpha = 1 - \alpha_2 - \alpha_3$ olur) (Lindstorm, 2015).

Teorem 5.1.1. $P(x)$ tek sayı mertebeden bir palindromik polinom ise sıfırlarından biri -1 olur.

İspat:

$$P(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_2 x^2 + a_1 x + 1$$

tek sayı mertebeden bir polinom ve $n = 2m + 1$ olsun. P, $x = -1$ için

$$P(-1) = (-1)^n + a_1(-1)^{n-1} + a_2(-1)^{n-2} + \cdots + a_2(-1)^2 + a_1(-1) + 1$$
$$= -1 + a_1 - a_2 + \cdots + a_2 - a_1 + 1$$
$$= a_1 - a_2 + \cdots + a_2 - a_1$$
$$= 0$$

(Lindstorm, 2015).

Teorem 5.1.2. $P(x) \in Q[x]$, n-dereceden polinomun palindromik polinom olması için gerek ve yeter şart

$$P(x) = x^n P(\frac{1}{x})$$

olmasıdır.

İspat: $P(x)$ bir palindromik polinom olsun.

$$= P(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_2 x^2 + a_1 x + 1$$

$$= x^n . P\left(\frac{1}{x}\right) = x^n (\left(\frac{1}{x}\right)^n + a_1 \left(\frac{1}{x}\right)^{n-1} + \cdots + a_2 \left(\frac{1}{x}\right)^2 + a_1 (\frac{1}{x}) + 1)$$

$$= 1 + a_1 x^1 + a_2 x^2 + \cdots + a_1 x^{n-1} + x^n$$

$$= P(x)$$

Tersine;

$$P(x) = x^n P(\frac{1}{x})$$

olsun. Bu durumda;

$$x^n . P\left(\frac{1}{x}\right) = x^n (\left(\frac{1}{x}\right)^n + a_1 \left(\frac{1}{x}\right)^{n-1} + \cdots + a_2 \left(\frac{1}{x}\right)^2 + a_1 \left(\frac{1}{x}\right)$$

$$= a_n + a_{n-1} x + a_{n-2} x^2 + \cdots + a_1 x^{n-1} + a_0 x^n$$

$$= P(x)$$

$a_{n-i} = a_i$ karşılaştırmasıyla $P(x)$ palindromik polinomdur (Lindstorm, 2015).

Palindromik polinomlar fonksiyonların çarpma işlemine göre kapalıdır.

Teorem 5.1.3. İki palindromik polinomun çarpımı ve bölümü palindromik polinomdur.

İspat: $P(x)$ ve $Q(x)$ iki palindromik polinom olsun. Bu durumda

$P(x) = x^n P\left(\frac{1}{x}\right)$ ve $Q(x) = x^m Q(\frac{1}{x})$ eşitlikleri sağlanır.

$$R(x) = P(x).Q(x) \;\; R\left(\frac{1}{x}\right) = P\left(\frac{1}{x}\right).Q\left(\frac{1}{x}\right)$$

$$R(x) = P(x)Q(x)$$

$$= x^n P\left(\frac{1}{x}\right) x^m Q\left(\frac{1}{x}\right)$$

$$= x^{n+m} P\left(\frac{1}{x}\right) Q\left(\frac{1}{x}\right)$$

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

Benzer olarak $H(x) = \frac{P(x)}{Q(x)}$ ise,

$$H(x) = x^{n-m}H\left(\frac{1}{x}\right)$$

olur (Lindstorm, 2015).

Teorem 5.1.4. $P(x)$ bir palindromik polinom, $\alpha,\ P(x)$ in bir kökü olsun. Bu durumda $\frac{1}{\alpha}$ bir köktür.

İspat: $\alpha = 1$ için ispat aşikardır. $\alpha \neq 1$ olsun. α bir sıfır ise $P(\alpha) = 0$ dır. Ayrıca, $P(x) = x^n P\left(\frac{1}{x}\right)$ olduğu bilinmektedir. Buna göre,

$$P(\alpha) = 0 \Rightarrow \alpha^n . P\left(\frac{1}{\alpha}\right) = 0 \text{ ve } \alpha^n \neq 0 \text{ dan } P\left(\frac{1}{\alpha}\right) = 0$$

elde edilir (Lindstorm, 2015).

Lemma 5.1.1. Eğer α=1, bir palindromik polinomun bir sıfırı ise o zaman katlı köktür.

İspat: Teorem 5.1.4 ten $a_i \neq \pm 1,\ P$ nin bir sıfırı ise $\frac{1}{a_i}$ nin de bir sıfır olduğunu ve aynı katlı kök sayısına sahip olduğu bilinmektedir, $n_i.$ sıfırın (-1) katlı kökünün n_{-1} ve sıfırın katlı kökünü r olarak belirtirsek, P

$$P(x) = (x-1)^r (x+1)^{n-1} (x^2 - \left(a_1 + \frac{1}{a_1}\right)x + 1)^{n_1} \dots (x^2 - \left(a_m + \frac{1}{a_m}\right)x + 1)^{n_m}$$

olarak yeniden yazılır.

1 in katlı kökünün tek sayı olduğunu varsayarsak, $r = 2k + 1$ diyelim ve $(x-1)^2 = x^2 - 2x + 1$ in palindromik polinom

$$P(x) = (x-1)^{2k+1} (x+1)^{n-1} (x^2 - \left(a_1 + \frac{1}{a_1}\right)x + 1)^{n_1} \dots (x^2 - \left(a_m + \frac{1}{a_m}\right) + 1)^{n_m}$$

$$= (x-1)(x^2 - 2x + 1)^k (x+1)^{n-1} (x^2 - \left(a_1 + \frac{1}{a_1}\right)x + 1)^{n_1} \dots (x^2 - \left(a_m + \frac{1}{a_m}\right) + 1)^{n_m}$$

burada $(x^2 - 2x + 1)^k, (x+1)^{n-1}$ ve $(x^2 - \left(a_i + \frac{1}{a_i}\right)x + 1)^{n_i}\ \ i = 1, 2, \dots, m$ için palindromik polinomdur. Bu onların katlı kökünün palindromik polinom olduğu anlamına gelir. Bu nedenle, katlı kökün sabit terimi 1 dir. Ancak P nin son katlı kökü $(x-1)$ ile çarpıldığında sabit terimin -1 olduğunu görürüz. Dolayısıyla $P(x)$ palindromik polinom olamaz ki bu sıfır 1 in tek sayı olduğuna ilişkin varsayımımıza ters düşer (Lindstorm, 2015).

Teorem 5.1.5. $P(x)$ palindromik polinom ise aşağıdaki iki koşulu sağlar:

1) 1 katlı kök ise köktür.
2) α bir sıfır ise $\frac{1}{\alpha}$ da aynı zamanda katlı kökü olan bir sıfır olur.

Ayrıca (-1) bir palindromik polinomun bir sıfırı ise, polinomun derecesi tek sayıdır (Lindstorm, 2015).

5.2. Palindromik Polinomların Köklerini Bulmak

Bir $P(x)$ palindromik polinomun sıfırları $\left(\alpha_i, \frac{1}{\alpha_i}\right)$ formunda çiftlerden oluşur. $P(x) \in Q[x]$, n-dereceden monik polinom olsun. $\alpha_1, \alpha_2, \dots, \alpha_n$ $P(x)$ in sıfırları olsunlar. Eğer tüm sıfırların farklı olduğunu varsayılırsa ve bunların hiçbiri Q da değilse, P nin parçalanış cismi $Q(\alpha_1, \alpha_2, \dots, \alpha_n)$ olur ve P Galois grubu

$$G\,(Q(\alpha_1, \alpha_2, \dots, \alpha_n)/Q)$$

olur.

Niels Henrik Abel, mertebesi beş ve beşten daha yüksek olan polinomlar için sıfırların hesaplanması için bir formül bulunamayacağını kanıtladı. Aslında Galois 2., 3. ve 4. mertebeden polinomlarda Galois teorisini kullanarak çözülebilirliğini göstermiştir.

$$G\,(Q(\alpha_1, \alpha_2, \dots, \alpha_n)/Q) \cong S_n$$

S_n, $n \leq 4$ için çözülebilir, $n \geq 5$ için çözülemezdir. Bu demek oluyor ki mertebesi 2, 3 ve 4 olan polinomların sıfırları hesaplanabilir.

Her kök başka bir kökün tersidir, fakat bu sadece palindromik polinomlar için geçerlidir.

n nin bazı değerleri için palindromik polinomların sıfırları aşağıdaki gibi bulunur.

$n = 5$ için palindromik polinomların sıfırlarının hesabı:

$$P(x) = x^5 + a_1x^4 + a_2x^3 + a_2x^2 + a_1x + 1$$

$$P(-1) = 0$$

dır. Bu durumda $\frac{P(x)}{x+1}$ 4. dereceden bir polinomdur. $P(x) = (x+1)P_1(x)$ ve $P_1(x)$ 4. dereceden olduğundan sıfırları bulunabilir.

Sonuç olarak $P(x)$ in sıfırları hesaplanabilir.

$n = 6$ için palindromik polinomların sıfırlarının hesabı:

$P(x) = x^6 + a_1x^5 + a_2x^4 + a_3x^3 + a_2x^2 + a_1x + 1$ (5.1)

6. dereceden bir palindromik polinomdur ve $a_1, a_2, a_3 \in Q$ olsun. Bu polinomun sıfırları $\alpha_1, \alpha_2, \alpha_3, \frac{1}{\alpha_1}, \frac{1}{\alpha_2}$ ve $\frac{1}{\alpha_3}$ tür. $P(x)$ polinomu sıfırlar cinsinden yazılırsa,

$P(x) = (x - \alpha_1)\left(x - \frac{1}{\alpha_1}\right)(x - \alpha_2)\left(x - \frac{1}{\alpha_2}\right)(x - \alpha_3)(x - \frac{1}{\alpha_3})$ (5.2)

elde edilir. Gerekli işlem ve düzenlemeler yapılırsa;

$P(x) = (x^2 - \left(\alpha_1 + \frac{1}{\alpha_1}\right)x + 1)(x^2 - \left(\alpha_2 + \frac{1}{\alpha_2}\right)x + 1)(x^2 - \left(\alpha_3 + \frac{1}{\alpha_3}\right)x + 1)$ (5.3)

$\beta_i = \alpha_i + \frac{1}{\alpha_i}$ (5.4)

değişimiyle

$P(x) = (x^2 - \beta_1 x + 1)(x^2 - \beta_2 x + 1)(x^2 - \beta_3 x + 1)$ (5.5)

ve buradan;

$P(x) = x^6 - (\beta_1 + \beta_2 + \beta_3)x^5 + (3 + \beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3)x^4$ (5.6)

$+(2(\beta_1 + \beta_2 + \beta_3) + \beta_1\beta_2\beta_3)x^3 + (3 + \beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3)x^2 + (\beta_1 + \beta_2 + \beta_3 + 1$

ve

$S_1 = \beta_1 + \beta_2 + \beta_3$ (5.7)

$S_2 = \beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3$ (5.8)

$S_3 = \beta_1\beta_2\beta_3$ (5.9)

değişimiyle,

$S_1 = -a_1$ (5.10)

$S_2 = a_2 - 3$ (5.11)

$S_3 = -a_3 - 2S_1 = 2a_1 - a_3$ (5.12)

yazılabilir.

$\beta_1, \beta_2 \; ve \; \beta_3,$

$x^3 - S_1x^2 + S_2x - S_3 = 0$ (5.13)

$x^3 + a_1x^2 + (a_2 - 3)x - (2a_1 - a_3) = 0$ (5.14)

denklemin çözümüdür. β_1, β_2 ve β_3 hesaplandıktan sonra,

$$\beta_i = \alpha_i + \frac{1}{\alpha_i}$$

eşitliklerinden α_i ler,

$\alpha_i\beta_i = {\alpha_i}^2 + 1$

$$\alpha_i{}^2 - \alpha_i\beta_i + 1 = 0 \qquad (5.15)$$

denklemlerinden hesaplanır.

Örnek 5.2.1. $P(x) = x^6 - \frac{7}{12}x^5 - \frac{197}{4}x^4 - \frac{1067}{16}x^3 - \frac{197}{4}x^2 - \frac{7}{12}x + 1$

$$a_1 = -\frac{7}{12}, a_2 = -\frac{197}{4}, a_3 = \frac{1067}{16}$$

değerleri Eş. 5.10, Eş. 5.11, Eş. 5.12'lerde yerine yazılırsa

$$S_1 = \frac{7}{12}$$

$$S_2 = -\frac{209}{4}$$

$$S_3 = -\frac{3257}{48}$$

değerleri elde edilir. Bu değerler Eş. 5.13'de yerine yazılırsa

$$x^3 + \frac{7}{12}x^2 - \frac{209}{4}x + \frac{3257}{48} = 0$$

denklemi elde edilir. Buradan kökler

$$\beta_1 = \frac{5}{2}, \beta_2 = \frac{17}{4}, \beta_3 = -\frac{37}{6}$$

bulunur. Bu kökler Eş. 5.15'de yerine yazılırsa

$$\alpha_1{}^2 - \frac{5}{2}\alpha_1 + 1 = 0 \;\Rightarrow \alpha_1 = -2$$

$$\alpha_2{}^2 - \frac{17}{4}\alpha_2 + 1 = 0 \;\Rightarrow \alpha_2 = -4$$

$$\alpha_3{}^2 + \frac{37}{6}\alpha_3 + 1 = 0 \;\Rightarrow \alpha_3 = 6$$

Buradan

$$P(x) = (x+2)(x+4)(x-6)\left(x+\tfrac{1}{2}\right)(x+\tfrac{1}{4})(x-\tfrac{1}{6})$$

olur.

$n = 7$ için palindromik polinomların sıfırlarının hesabı:

-1 bir sıfır olduğundan bu durumda $\frac{P(x)}{x+1}$ 6. dereceden bir polinomdur.

$P(x) = (x+1)P_1(x) ve\ P_1(x)$ 6. dereceden olduğundan sıfırları bulunabilir. Sonuç olarak $P(x)$ in sıfırları hesaplanabilir.

$n = 8$ için palindromik polinomların sıfırlarının hesabı:

$$P(x) = x^8 + a_1x^7 + a_2x^6 + a_3x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + 1 \quad (5.16)$$

palindromik polinomunun sıfırlarını hesaplayalım. Sıfırlar $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \frac{1}{\alpha_1}, \frac{1}{\alpha_2}, \frac{1}{\alpha_3}$ ve $\frac{1}{\alpha_4}$ tür.

$$\beta_i = \alpha_i + \frac{1}{\alpha_i}$$

denirse,

$$\beta_1 = \alpha_1 + \frac{1}{\alpha_1}, \beta_2 = \alpha_2 + \frac{1}{\alpha_2}, \beta_3 = \alpha_3 + \frac{1}{\alpha_3}, \beta_4 = \alpha_4 + \frac{1}{\alpha_4}$$

$$P(x) = (x^2 - \beta_1x + 1)(x^2 - \beta_2x + 1)(x^2 - \beta_3x + 1)(x^2 - \beta_4x + 1) = x^8 - (\beta_1 + \beta_2 + \beta_3 + \beta_4)x^7 + (4 + \beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3 + \beta_1\beta_4 + \beta_2\beta_4 + \beta_3\beta_4)x^4 - (3(\beta_1 + \beta_2 + \beta_3) + \beta_1\beta_2\beta_3 + \beta_1\beta_2\beta_4 + \beta_1\beta_3\beta_4 + \beta_2\beta_3\beta_4)x^5 + (6 + 2\beta_1\beta_2 + 2\beta_1\beta_3 + 2\beta_2\beta_3 + 2\beta_1\beta_4 + 2\beta_2\beta_4 + 2\beta_3\beta_4 + \beta_1\beta_2\beta_3\beta_4)x^4 - (3(\beta_1 + \beta_2 + \beta_3) + \beta_1\beta_2\beta_3 + \beta_1\beta_2\beta_4 + \beta_1\beta_3\beta_4 + \beta_2\beta_3\beta_4)x^3 + (4 + \beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3 + \beta_1\beta_4 + \beta_2\beta_4 + \beta_3\beta_4)x^2 - (\beta_1 + \beta_2 + \beta_3 + \beta_4)x + 1 \quad (5.17)$$

ve

$$S_1 = \beta_1 + \beta_2 + \beta_3 + \beta_4 \quad (5.18)$$

$$S_2 = \beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3 + \beta_1\beta_4 + \beta_2\beta_4 + \beta_3\beta_4 \quad (5.19)$$

$$S_3 = \beta_1\beta_2\beta_3 + \beta_1\beta_2\beta_4 + \beta_1\beta_3\beta_4 + \beta_2\beta_3\beta_4 \quad (5.20)$$

$$S_4 = \beta_1\beta_2\beta_3\beta_4 \quad (5.21)$$

değişimiyle,

$$S_1 = -a_1 \quad (5.22)$$

$$S_2 = a_2 - 4 \quad (5.23)$$

$$S_3 = -a_3 - 3S_1 = 3a_1 - a_3 \quad (5.24)$$

$$S_4 = a_3 - 6 - 2S_2 = a_4 - 6 - 2(a_2 - 4) = a_4 - 2a_2 + 2 \quad (5.25)$$

yazılabilir.

$\beta_1, \beta_2, \beta_3$ *ve* β_4

$$x^4 - S_1x^3 + S_2x^2 - S_3x + S_4 = 0 \quad (5.26)$$

$$x^4 + a_1x^3 + (a_2 - 4)x^2 - (3a_1 - a_3)x + a_4 - 2a_2 + 2 = 0 \quad (5.27)$$

denklemin çözümüdür. $\beta_1, \beta_2, \beta_3$ ve β_4 hesaplandıktan sonra,

$$\beta_i = \alpha_i + \frac{1}{\alpha_i}$$

eşitliklerinden α_i ler,

$\alpha_i\beta_i = {\alpha_i}^2 + 1$

$${\alpha_i}^2 - \alpha_i\beta_i + 1 = 0 \qquad (5.28)$$

yazılabilir.

Örnek5.2.2. $P(x) = x^8 - \frac{137}{15}x^7 - \frac{9}{2}x^6 + \frac{2373}{20}x^5 + \frac{293}{5}x^4 - \frac{137}{15}x^3 - \frac{9}{2}x^2 + \frac{2373}{20}x + 1$

$$a_1 = -\frac{137}{6}, a_2 = -\frac{9}{2}, a_3 = \frac{2373}{20}, a_4 = \frac{293}{5}$$

Bu değerler Eş. 5.22, Eş. 5.23, Eş. 5.24, Eş. 5.25'lerde yerine yazılırsa

$$S_1 = \frac{137}{15}$$

$$S_2 = -\frac{17}{2}$$

$$S_3 = -\frac{2921}{20}$$

$$S_4 = \frac{348}{5}$$

değerleri elde edilir. Bu değerler Eş. 5.26'de yerine yazılırsa

$$x^4 - \frac{137}{5}x^3 - \frac{17}{2}x^2 + \frac{2921}{20}x + \frac{348}{5} = 0$$

denklemi elde edilir. Buradan kökler

$$\beta_1 = 2, \beta_2 = \tfrac{10}{3}, \beta_3 = \tfrac{26}{5}, \beta_1 = -\tfrac{17}{4}$$

bulunur. Bu kökler Eş. 5.28'de yerine yazılırsa

$${\alpha_1}^2 - 2\alpha_1 + 1 = 0 \;\Rightarrow \alpha_1 = -1$$

$${\alpha_2}^2 - \tfrac{10}{3}\alpha_2 + 1 = 0 \;\Rightarrow \alpha_2 = -3$$

$${\alpha_3}^2 - \tfrac{26}{5}\alpha_3 + 1 = 0 \;\Rightarrow \alpha_3 = -5$$

$${\alpha_4}^2 + \tfrac{17}{4}\alpha_4 + 1 = 0 \;\Rightarrow \alpha_3 = 4$$

Buradan

$$P(x) = (x+1)(x+3)(x+5)(x-4)(x+1)\left(x+\tfrac{1}{3}\right)(x+\tfrac{1}{5})(x+\tfrac{1}{4})$$

olur.

$n = 9$ için palindromik polinomların sıfırlarının hesabı:

-1 bir sıfır olduğundan bu durumda $\frac{P(x)}{x+1}$ 8.dereceden bir polinomdur.

$P(x) = (x+1)P_1(x) ve\ P_1(x)$ 8. dereceden olduğundan sıfırları bulunabilir. Sonuç olarak $P(x)$ in sıfırları hesaplanabilir.

5.3. Palindromik Polinomların Galois Teorisi

$P(x)$ bir palindromik polinom, $P(x)$ in parçalanış cismi F olsun. $P(x)$ in Galois grubu $G\,(F/Q)\,, Q$ yu sabit bırakan tüm $\emptyset: F \to F$ otomorfizmalarının grubudur. $P(x)$ in -1 hariç tüm sıfırları çiftler halindedir, Q dan ve $G\,(F/Q)$ nun elemanları grup izomorfizmleri olduklarından eğer $\alpha_2 = \frac{1}{\alpha_1}$ ve $\emptyset \in G\,(F/Q)\,,\ \emptyset(\alpha_1) = \alpha_2,$

$\emptyset(\alpha_2) = \alpha_1$ ise

$$\emptyset(\alpha_2) = \emptyset(\frac{1}{\alpha_1}) = \frac{\emptyset(1)}{\emptyset(\alpha_1)} = \frac{1}{\alpha_2} = \alpha_1$$

yazılabilir.

Teorem 5.3.1. $x_n + \frac{1}{x_n}$ ifadesi $x + \frac{1}{x}$ e göre rasyonel katsayılı bir polinom olarak verilebilir.

İspat: Yöntem olarak tümevarım yöntemini kullanılırsa;

$$n = 1 \text{ için } x^1 + \frac{1}{x^1} = x + \frac{1}{x} \text{ olduğu aşikardır.}$$

$$n = k \text{ için } P_k(x + \frac{1}{x}) = \ x^k + \frac{1}{x^k}$$

olsun.

$$x + \frac{1}{x}\, P_k(x + \frac{1}{x}) = (\, x^k + \frac{1}{x^k})(x + \frac{1}{x}) = \ x^{k+1} + \ x^{k-1} + \frac{1}{x^{k-1}} + \frac{1}{x^{k+1}}$$

$$= \ x^{k+1} + \frac{1}{x^{k+1}} + \ x^{k-1} + \frac{1}{x^{k-1}}$$

$$= P_k$$

Böylece;

$$x^{k+1} + \frac{1}{x^{k+1}} = (x + \frac{1}{x})\, P_k(x + \frac{1}{x}) - P_{k-1}(x + \frac{1}{x})$$

elde edilir ve bu ispat tamamlanır (Lindstorm, 2015).

$$P(x) = x^{2n} + a_1 x^{2n-1} + a_2 x^{2n-2} + \cdots + a_2 x^2 + a_1 x + 1$$

palindromik polinomunu ele alalım. $P(x)$ in $2n$ tane farklı $\alpha_1, \alpha_2, \dots, \alpha_n, \frac{1}{\alpha_1}, \frac{1}{\alpha_2}, \dots, \frac{1}{\alpha_n}$ sıfırları olsun. Bunların hiçbiri Q da olmasın. Bu durumda $P(x)$ in Q daki parçalanış cismi $F = Q(\alpha_1, \alpha_2, \dots, \alpha_n)$ dir.

Şimdi, $Q(x) = \frac{P(x)}{x^n}$ rasyonel fonksiyonunun hesaplanması durumunda

$$Q(x) = \frac{P(x)}{x^n} = \frac{x^{2n} + a_1 x^{2n-1} + a_2 x^{2n-2} + \cdots + a_2 x^2 + a_1 x + 1}{x^n}$$

$$Q(x) = x^n + a_1 x^{n-1} + \cdots + \frac{a_1}{x^{n-1}} + \frac{1}{x^n}$$

$$Q(x) = x^n + \frac{1}{x^n} + a_1\left(x^{n-1} + \frac{1}{x^{n-1}}\right) + a_2\left(x^{n-2} + \frac{1}{x^{n-2}}\right) + \cdots + a_{n-1}(x + \frac{1}{x}) + a_n$$

elde edilir. Böylece, $\frac{P(x)}{x^n}$ polinomu $Q_p\left(x + \frac{1}{x}\right)$ rasyonel katsayılı polinomu yazılabilir.

Genel olarak, $P(x)$ katsayıları bir E cisminden alınan bir polinom ise, $\frac{P(x)}{x^n}$ polinomu da katsayıları E de olan bir polinomdur ve ayrıca $Q_p\left(x + \frac{1}{x}\right) \in E\left(x + \frac{1}{x}\right)$ olur.

E bir cisim, $P(x)$ n-dereceden E-katsayılı bir palindromik polinom, sıfırları $\alpha_1, \alpha_2, \dots, \alpha_n, \frac{1}{\alpha_1}, \frac{1}{\alpha_2}, \dots, \frac{1}{\alpha_n}$ olsun. $Q_p\left(x + \frac{1}{x}\right) = \frac{P(x)}{x^n}$ polinomuna $E\left(x + \frac{1}{x}\right)$ −katsayılı, $P(x)$ in x^n ile türetilmiş polinomu adı verilir.

Özellik 5.3.1. $P(x)$ in bir sıfırının $\alpha, (\alpha \neq 0)$ olması için gerek ve yeter şart $\alpha + \frac{1}{\alpha}$ nın $Q_p\left(x + \frac{1}{x}\right)$ in bir sıfırı olmasıdır.

İspat:

($\Rightarrow$): $P(\alpha) = 0$ ve $\alpha^n \neq 0$ olsun.

$$= Q_p\left(x + \frac{1}{x}\right) = \frac{P(x)}{x^n} = 0$$

($\Leftarrow$): $\alpha + \frac{1}{\alpha} = 0$ olsun. $(\alpha^n \neq 0)$.

$$= P(x) = Q_p\left(x + \frac{1}{x}\right) x^n$$

$$= P(x) = Q_p\left(\alpha + \frac{1}{\alpha}\right) \alpha^n$$

$$= P(\alpha) = 0.\ \alpha^n$$

$$= P(\alpha) = 0$$

(Lindstorm, 2015).

6. GALOIS GRUP

α bir $p(x)$ palindromik polinomun bir sıfırı ise $\alpha + \frac{1}{\alpha}$ nın $Q_p(x + \frac{1}{x})$ nın sıfırı olduğu açıktır.

$$P(x) = x^{2n} + a_1x^{2n-1} + a_2x^{2n-2} + \cdots + a_2x^2 + a_1x + 1$$

alınırsa. Q_p nin parçalanış cismi

$$E = Q(\alpha_1 + \frac{1}{\alpha_1}, \alpha_2 + \frac{1}{\alpha_2}, \dots, \alpha_n + \frac{1}{\alpha_n})$$

ve Q_p nin katsayıları Q da olduğu için E, Q üzerinde bir parçalanış cismidir. Galois teorisine göre E, Q üzerinde bir parçalanış cismi olduğundan E, Q nun sonlu bir normal genişlemesidir. Teorem 3.7.2'de E, Q nun normal bir genişlemesi olduğundan G(F/E), G(F/Q) nun normal altgrubudur. Dolayısıyla

$$\mathrm{G}(E/Q) \cong \mathrm{G}(F/Q)\ /\mathrm{G}(F/E)$$

olur. G(F/Q) nun kaç elemanı olduğunu belirlemek kolay değildir. Gördüğümüz gibi Q yu sabit bırakan F nin tüm otomorfizmaları G(F/Q) da bulunmaktadır. Böylece F deki elemanların sayısı hakkında daha fazla bilgi edinmek için x^n ile türetilmiş Q_p polinomu ve G(F/E) nin Galois grubu göz önüne alınırsa.

Önce G(E/Q) yı düşünülürse;

G(E/Q), E nin Q yu sabit bırakan tüm otomorfizmalarının grubudur. Görüldüğü gibi bunlar Q_p nin sıfırlarını değiştiren E nin tüm otomorfizmalarıdır. Sıfırları n tane olduğundan G(F/Q) $\cong$ S_n olur.

Bu yüzden $|S_n| = n!$ olduğundan $|\mathrm{G}(E/Q)| = n!$ elde ederiz.

Sonra G(F/E) yi düşünülürse:

E nin F yi sabit bırakan tüm otomorfizmaların grubu, Yani α_i yi α_i ye yada $\frac{1}{\alpha_i}$ ye gönderen F nin otomorfizmi G(F/E) dir. Çünkü α_i yi ya α_j ye yada $\frac{1}{\alpha_i}$ ye gönderir. $j \neq i$ o zaman E yi sabit bırakmaz $\alpha_i + \frac{1}{\alpha_i}$ yi $\alpha_j + \frac{1}{\alpha_j}$ ya gönderir. Dolayısıyla;

$$|\mathrm{G}(F/E)| = 2^n$$

olmalıdır.

Galois teorisinden $\mathrm{G}(E/Q), \mathrm{G}(F/Q)$ nın $\mathrm{G}(F/E)$ ile

$$|\mathrm{G}(E/Q)| = |\mathrm{G}(F/Q)|/|\mathrm{G}(F/E)|$$
$$= |\mathrm{G}(F/Q)| = |\mathrm{G}(F/E)|.|\mathrm{G}(E/Q)|$$
$$= |\mathrm{G}(F/Q)| = 2^n.n!$$

(Lindstorm, 2015).

Örnek 6.1. Derecesi 4 olan bir palindromik polinom alalım.

$n = 2$ ve

$$p(x) = x^4 + ax^3 + bx^2 + ax + 1$$

olsun. Şimdi $\alpha_1, \alpha_2, \frac{1}{\alpha_1}$ ve $\frac{1}{\alpha_2}$ nin P nin sıfırları olduğunu ve parçalanış cisminin $F = Q(\alpha_1, \alpha_2)$ olduğunu varsayalım.

F nin maximum bir genişleme olması durumunda

$$|\mathrm{G}(F/Q)| = 2^n.n! = 2^2.2! = 4.2 = 8 \text{ olur.}$$

Basit olması için köklerimizi $\{\alpha_1, \alpha_2, \frac{1}{\alpha_1}, \frac{1}{\alpha_2}\}$={1, 2, 3, 4} olarak alınsın.

Örneğin $1 \to 3$ giderse $2 \to 4$ e gider. Yani (1342)$\in S_n$ permütasyonu $\mathrm{G}(F/Q)$ da değildir.

Mertebe 0: $\{e\}$

Mertebe 2: $\{(12), (34), (12)(34), (13)(24), (14)(23)\}$

Mertebe 3: yok

Mertebe 4: {(1324), (1423) }

Bu değişmeli olmayan bir gruptur, sadece $h = (34)$ ve $k = (13)(24)$, $\mathrm{G}(F/Q)$ dedir. O halde

$$hk = (34).(13)(24) = (1423)$$

iken

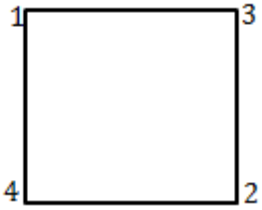
$$kh = (13)(24).(34) = (1324),$$

yani

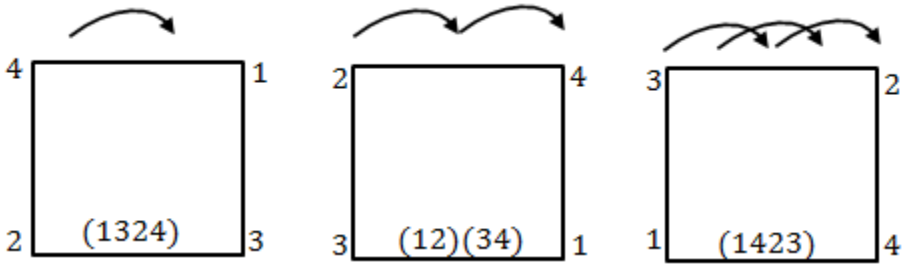
$$hk \neq kh.$$

D_4, değişmeli olmayan bir gruptur. Açıkça görülür ki $\mathrm{G}(F/Q) \cong D_4$ olur.

D_4, sekiz elemanlı dehidral grupları sıklıkla karenin simetrileri ile ilişkilendirilir. Eğer köşeler aşağıdaki gibi {1, 2, 3, 4} ile gösterilirse, her otomorfizma karenin bir simetrisi ile gösterebilir.

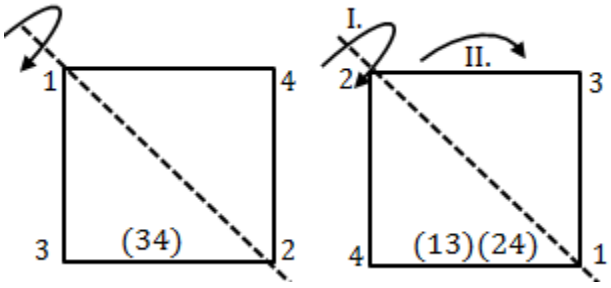


İlk olarak kare sağa 1, 2 ve 3 kez döndürülsün (Şekil 6.1).



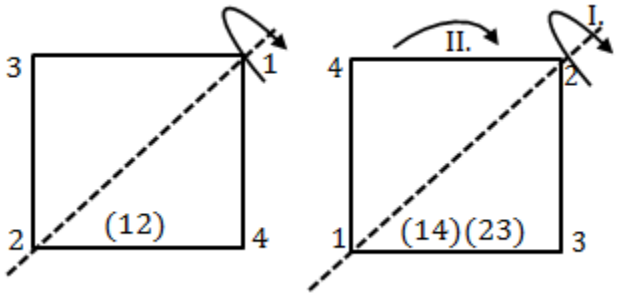
Şekil 6.1. Sağa bir, iki, üç kez döndürme.

Kare köşegenlerden birinin etrafında yansır. İlk önce yansır sonra döndürülür (Şekil6.2).



Şekil 6.2. Simetriye karşılık gelen permütasyonlar.

Son iki simetri, biri diyagonal etrafında yansıyan (birinci) daha sonra da (ikinci) yansıyan ve dönmeden oluşur (Şekil 6.3).



Şekil 6.3. Dönme ve yansımalara karşılık gelen permütasyonlar.

Son olarak otomorfizm birimdir, kenarları sabit bırakır (Şekil 6.4).

Şekil 6.4. Birim otomorfizm.

Buradan G(F/Q) $\cong D_4$ olur.

Aynı zamanda x^2 ile türetilmiş P polinomunun $Q_p(x+\frac{1}{x})$ Galois grubu düşünülürse. Önce $Q_p(x+\frac{1}{x})$ i hesaplayalım:

$$Q(x) = \frac{p(x)}{x^2} = x^2 + ax + b + \frac{a}{x} + \frac{1}{x^2}$$

$$=(x^2 + \frac{1}{x^2}) + a(x + \frac{1}{x}) + b$$

$$=(x + \frac{1}{x})^2\text{-}2+ a(x + \frac{1}{x}) + b$$

$$=Q_p\left(x + \frac{1}{x}\right) = (x + \frac{1}{x})^2 + \ a\left(x + \frac{1}{x}\right) + (b - 2).$$

Q_p nin sıfırlarının $\alpha_1 + \frac{1}{\alpha_1}$ ve $\alpha_2 + \frac{1}{\alpha_2}$ olduğu bilinmektedir, bu yüzden Q_p nin parçalanış cismi $E = Q(\alpha_1 + \frac{1}{\alpha_1}\ ,\ \alpha_2 + \frac{1}{\alpha_2})$ nin Q üzerinde de bir parçalanış cismi olduğu varsayılılırsa.

Şimdi hem G(F/E) yi hemde G(F/Q) yu düşünülürse:

G(E/Q), E nin Q yu sabit bırakan tüm otomorfizmalarının grubudur. G(E/Q) da ki tek otomorfizm $\alpha_1 + \frac{1}{\alpha_1}$ i $\alpha_2 + \frac{1}{\alpha_2}$ ye götüren birim dönüşümüdür. Dolayısıyla G(E/Q) nun mertebesi $|\mathrm{G}(E/Q)|$=2 olur.

G(F/E) , F nin E yi sabit bırakan otomorfizmalarının grubudur, bu nedenle $i = 1, 2$ için α_i yi α_i ye ve $\frac{1}{\alpha_i}$ ye gönderilebilir. Burada

$$|\mathrm{G}(F/E)| = 2^2 = 4$$

olur.

$$1 \to \mathrm{G}(F/E) \to \mathrm{G}(F/Q) \to \mathrm{G}(E/Q) \to 1,$$

dizisi G(F/E) nin G$(F/Q) \cong D_4$ un normal bir altgrubu olduğu anlamına gelir.

$$\mathrm{G}(F/E) = \{e, (12), (34), (12)(34)\}$$

olur. G$(F/E) \cong Z_2 \times Z_2 \subseteq D_4$ olduğu görülür.

Galois grubunun elemanları G(E/Q) den bir eleman ve G(F/E) den bir elemandan oluşan bir yapıdır. Permütasyon (1423)$\in$ G(F/Q) yani

$$\alpha_1 \to \frac{1}{\alpha_2} \to \frac{1}{\alpha_1} \to \alpha_2 \to \alpha_1$$

olsun.

G(E/Q) de $\alpha_1 + \frac{1}{\alpha_1}$ i $\alpha_2 + \frac{1}{\alpha_2}$ ye göndeririz $\alpha_1 + \frac{1}{\alpha_1}$, $\frac{1}{\alpha_1} + \alpha_1$ de herhangi bir fark görmediğimiz için bu (1324) e eşittir. Bu da

$$\alpha_1 \to \alpha_2 \to \frac{1}{\alpha_1} \to \frac{1}{\alpha_2} \to \alpha_1$$

olur. Öte yandan G(F/E) de $\alpha_1 + \frac{1}{\alpha_1}$ i ve $\alpha_2 + \frac{1}{\alpha_2}$ sabit tutulursa ve bu dönüşüm $\alpha_1 \to \frac{1}{\alpha_1}$ i $\alpha_2 \to \frac{1}{\alpha_2}$ ye yani permütasyon (12)(34) e eşittir.

Dolayısıyla G(F/Q) daki (1423) permütasyonu

(1423)=(12)(34)(1324)

çarpımına eşittir.

Düşük dereceli palindromik polinomların sıfırları için formül bulmak $x+\frac{1}{x}$ gibi polinom haline dönüşebileceğini kullanabiliriz (Lindstorm, 2015).

Örnek 6.2. 4. dereceden palindromik polinomun sıfırlarını hesaplamak için formül bulmak istiyoruz. $p(x)=x^4+ax^3+bx^2+ax+1$ varsayalım. Görüldüğü gibi eğer $\alpha+\frac{1}{\alpha}, Q_p$ nin bir sıfırı ise o zaman α, P nin bir sıfırı olacak şekilde $Q_p\left(x+\frac{1}{x}\right)$ polinomu bulabiliriz. $p(x)=x^4+ax^3+bx^2+ax+1$ polinomunda

$$Q(x)=\frac{p(x)}{x^2}=x^2+ax+b+\frac{a}{x}+\frac{1}{x^2}$$

$$=(x^2+\tfrac{1}{x^2})+a(x+\tfrac{1}{x})+b$$

$$=(x+\tfrac{1}{x})^2\text{-}2+a(x+\tfrac{1}{x})+b$$

$$=Q_p\left(x+\tfrac{1}{x}\right)=(x+\tfrac{1}{x})^2+a\left(x+\tfrac{1}{x}\right)+(b-2)$$

i buluyoruz. Basit olsun diye $y=x+\frac{1}{x}$ olsun

$$Q_p(y)=y^2+ay+(b-2)=0\Rightarrow y^2=-ay-b+2$$

çözebiliriz.

$$y=\frac{-a\pm\sqrt{a^2-4b+8}}{2}$$

Yani

$$x+\frac{1}{x}=y\Rightarrow x^2-yx+1=0$$

ve dolayısıyla

$$x=\frac{y\pm\sqrt{y^2-4}}{2}$$

$$\text{x}=\frac{\frac{-a\pm\sqrt{a^2-4b+8}}{2}\pm\sqrt{\frac{a^2\mp b\sqrt{a^2-4b+8}-2b+4-8}{2a}}}{2}$$

$$\text{x}=-\frac{a}{4}\pm\frac{\sqrt{a^2-4b+8}}{4}\pm\frac{1}{2\sqrt{2}}\sqrt{a^2\pm\sqrt{a^4-4a^2b+8a^2}-2b-4}$$

Şimdi $p(x)$ in dört kökü için bir formül bulunur.

Örnek 6.2 te görüldüğü gibi

$$y=\frac{-a\pm\sqrt{a^2-4b+8}}{2}$$

$$\Rightarrow x+\frac{1}{x}=y=\frac{-a\pm\sqrt{a^2-4b+8}}{2}$$

$\Rightarrow \alpha_1 + \frac{1}{\alpha_1} = -\frac{a}{2} + \frac{1}{2}\sqrt{a^2 - 4b + 8}$ ve $\alpha_2 + \frac{1}{\alpha_2} = -\frac{a}{2} + \frac{1}{2}\sqrt{a^2 - 4b + 8}$

olur (Lindstorm, 2015).

6.1. Polinom Sıfırlarının Karakterizasyonu

Bir polinomun sıfırları, Galois grubunun özellikleri kullanılarak bulunabilir. Ancak bu işlem bazen zor ve uzun zaman gerektirir. Sıfırları bulduğumuzu varsayarsak, sıfırlar arasındaki ilişkiyi veren önemli kavramlardan biri, bir polinomun diskriminantıdır (Lindstorm, 2015).

Tanım 6.1.1. $P(x) = \sum_{i=0}^{n} a_i x^i$ polinomu için , $\alpha_1, \alpha_2, \dots, \alpha_n$ $P(x)$ in sıfırları olmak üzere

$$\Delta = a_n^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2$$

değerine $P(x)$ in diskriminantı denir (Lindstorm, 2015).

Sıfırlardan biri katlı kök ise $\Delta = 0$ dır.

$n = 2$ için Δ yı hesaplansın.

$n = 2$ için $P(x) = ax^2 + bx + c$ dir.

Tanım gereği, $n = 2, a_2 = a, i = 1, j = 2,$ kökler α_1, α_2 alınırsa;

$$\Delta = a^{2.2-2}(\alpha_1 - \alpha_2)^2$$
$$= a^2(\alpha_1^2 - 2\alpha_1\alpha_2 + \alpha_2^2)$$

$P(x)$ sıfırlar cinsinden yazılırsa,

$$P(x) = a(x - \alpha_1)(x - \alpha_2)$$
$$= ax^2 - a(\alpha_1 + \alpha_2)x + a\alpha_1\alpha_2$$
$$\Rightarrow b = -a(\alpha_1 + \alpha_2)$$
$$c = a\alpha_1\alpha_2 \text{ alınırsa}$$
$$= b^2 = a^2(\alpha_1^2 + 2\alpha_1\alpha_2 + \alpha_2^2)$$

ve böylece;

$$\Delta = a^2\alpha_1^2 - 2a^2(\alpha_1 + \alpha_2) + \alpha_2^2$$
$$= b^2 - 4a^2\alpha_1\alpha_2$$
$$= b^2 - 4ac$$

benzer hesaplama $n = 3$ için yapılırsa,

$$P(x) = ax^3 + bx^2 + cx + d$$

için

$$\Delta = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd$$

elde edilir.

$n = 3$ için öyle ki

$$P(x) = x^3 + bx^2 + cx + d$$

$\Delta = 0$ olduğu kabul edilsin. Sıfırlar 2 ya da 3 ten çok ise P nin katsayılarını kullanarak bir şey söylenebilir mi ?

P nin 3 ün katı olan α gibi sadece bir sıfırı olsun.

$$P(x) = (x - \alpha)^3 = x^3 - 3\alpha x^2 + 3\alpha^2 x - \alpha^3$$

$$= b = -3\alpha, c = 3\alpha^2, d = -\alpha^3$$

$$= b^2 = 9\alpha^2 = 3c, b^3 = -27\alpha^3 = 27d, c^3 = 27\alpha^6 = 27d$$

Biz üç tane alt diskriminant tanımlanırsa

$$\Delta_1 := b^2 - 3c$$

$$\Delta_2 := b^3 - 27d$$

$$\Delta_3 := c^3 - 27d,$$

P için $\Delta_1 = 0, \Delta_2 = 0, \Delta_3 = 0$ dır.

Alt diskriminantları kullanarak diskriminant yeniden yazılabilir ($\alpha = 1$ alınsın)

$$\Delta = b^2c^2 - 4c^3 - 4b^3d - 27^2d^2 + 18bcd$$

$$= c^2(b^2 - 3c) - c^3 - 4b^3d + d(b^3 - 27d) - b^3d + 18bcd$$

$$= c^2(b^2 - 3c) - c^3 - 5b^3d + d(b^3 - 27d) + 6b^3d - 6bd(b^2 - 3c)$$

$$= (c^2 - 6bd)(b^2 - 3c) + d(b^3 - 27d) + b^3d - c^3$$

$$= (c^2 - 6bd)\,\Delta_1 + d\Delta_2 + b^3d - c^3$$

Kabul edilsin

$$b^3d - c^3 = d(b^3 - 27d) - (c^3 - 27d^2) = d\Delta_2 - \Delta_3$$

$$\Delta = (c^2 - 6bd)\,\Delta_1 + d\Delta_2 + b^3d - c^3$$

$$= (c^2 - 6bd)\,\Delta_1 + d\Delta_2 + d\Delta_2 - \Delta_3$$

$$= (c^2 - 6bd)\,\Delta_1 + 2d\Delta_2 - \Delta_3$$

Δ_1, Δ_2 ve Δ_3 alt diskriminantları kullanarak diskriminant için yeni bir ifade bulundu. Eğer Δ_1, Δ_2 ve $\Delta_3 = 0$ ise P nin 3 ün katı olan bir sıfırı vardır.

6.2. Palindromik Diskriminant

Bir polinomun palindromik diskriminantı şöyle tanımlanır.

Tanım 6.2.1. $P(x) = \sum_{i=0}^{n} a_i x^i$ polinomu için,

$$\Delta_p = a_n^{2n-n} \prod_{i \neq j} \left(\alpha_i - \frac{1}{\alpha_j} \right)$$

değerine $P(x)$ in palindromik diskriminantı denir (Lindstorm, 2015).

$n = 2$ için Δ yı hesaplayalım.

$n = 2$ için $P(x) = ax^2 + bx + c$ ve sıfırlar α_1, α_2 olsun. Bu durumda

$$\Delta_p = a^2 \left(\alpha_1 - \frac{1}{\alpha_2} \right) \left(\alpha_2 - \frac{1}{\alpha_1} \right)$$

$$= a^2 (\alpha_1 \alpha_2 - 2 + \frac{1}{\alpha_1 \alpha_2})$$

$$= a^2 \left(S_2 - 2 + \frac{1}{S_2} \right) = \frac{a^2}{S_2} \left({S_2}^2 - 2S_2 + 1 \right)$$

$$= \frac{a^2}{S_2} (S_2 - 1)^2 = \frac{a^2 (S_2 - 1)^2}{S_2},$$

ve buradan S_2, α_1 ve α_2, iki değişkenli temel simetrik polinomdur.

$$\Delta_p = \frac{a^2 (\alpha_1 \alpha_2 - 1)^2}{\alpha_1 \alpha_2}$$

elde edilir. 2. dereceden polinomlar için, $\alpha_1 \alpha_2 = \frac{c}{a}$ dan,

$$\Delta_p = \frac{a(c - a)^2}{c}$$

yazılır. Açıkça görülür ki, tüm palindromik polinomlar için $\Delta_p = 0$ dır.

7. TARTIŞMA VE SONUÇ

Galois tarafından beş ve beşten daha yüksek mertebeli polinomların çözümü için bir genel formül verilemeyeceği Galois teori temelli ispatlanmıştır. Ancak özel yapıya sahip bazı polinomlar için çözüm algoritmaları verilebilir. Simetrik polinomlar, palindromik polinomlar vs. bunlardan bazılarıdır. Bu tezde palindromik polinomlar için çözüm algoritmaları verildi ve örneklendirildi.

Palindromik polinomlar, kökler arasında $a_{n-i} = a_i$ ilgisi olan ve α bir kök iken $\frac{1}{\alpha}$ nın da kök olduğu özelliklerinden dolayı sıfırlarının bulunuşu için algoritma verilebilir tipten polinomlardır. Ayrıca tek sayı mertebeden palindromik polinomlar için -1 bir kök olduğundan tek sayı mertebeli bir $P(x)$ polinomu $P(x) = (x+1)Q(x)$ olarak yazılır. Burada $Q(x)$ çift mertebeli bir polinomdur. $Q(x)$ in mertebesi $2n$ ise $\alpha_1, \dots, \alpha_n$ ve $\frac{1}{\alpha_1}, \dots, \frac{1}{\alpha_n}$ ler ve -1 $P(x)$ in sıfırlarıdır. Sonuç olarak $2n+1$ mertebeden bir $P(x)$ polinomunun sıfırlarının bulunuşu algoritmik olarak n. mertebeden bir polinomun sıfırlarının bulunuşuna indirgenmiş olur.

KAYNAKLAR

Adamson, I. T., 1964. ***Introduction to Field Theory*.** Edinburgh: Oliver and Boyd, New York.

Artin, E., 1944. ***Galois theory*.** University of Notre Dame Press, London.

Asar, A.O., Arıkan, A., 2011. ***Sayılar Teorisi***. Gazi Kitapevi, Ankara.

Botta V., Marques L.F., Meneguette M., 2014. Palindromic and perturred polynomials: zeros locatıon. ***Acta Math. Hungar.*, 143**(1): 81-87.

Brugiapaglia, S., Gemignani L., 2014. On the simultaneous refinement of the zeros of H-palindromic polynomials. ***Journal of Computatiol and Aplied Mathematics* 272*:*** 293-303.

Dummit, D. S., Foot , R. M., 2004. Abstract Algebra Third Edition. John Wiley and Sons, Inc., USA.

Feyzioğlu, A., 1990. ***A Course on Algebra.*** Boğaziçi University Publication, İstanbul.

Fraleigh, J. B., 2006. ***A First Course in Abstract Algebra***. Pearson Education, New York.

Gemignani, L., Noferini, V., 2013. The Ehrlich–Aberth method for palindromic matrix polynomials represented in the Dickson basis. ***Linear Algebra and its Applications,* 438*:*** 1645-1666.

Hardy, G. H., Wright, E. M., 1960. ***An Introduction to the Theory of Numbers***. Oxford University Press, Ely House, London.

Hoffman, K., Kunze, R., 1961. ***Linear Algebra.*** Prentice Hall, Inc. Englewood Cliffs, London.

Hungerford, T.W., 1974. ***Algebra.*** Springer-Verlag, New York.

Jacobson, N., 1910. ***Lectures in Abstract Algebra.*** Springer Verlag, Berlin.

Joyner D., Shaska T., 2000. Self-inversive polynomials, curves, and codes. ***Contemporary Mathematics.*** 1-20.

Kaplansky, I., 1972. ***Fields and Rings***. The University of Chicago Press, London.

Lindstorm, P., 2015. ***Galois Theory of Palindromic Polynomials*** (Yüksek lisans tezi). Universty of Oslo, Oslo, Norveç.

Markovsky, I., Rao S., 2008. Palindromic polynomials, time-reversible systems, and conserced quantities. ***16 th Mediterranean Conference on Control and Automation Congress Centre, Ajaccio, France*** 25-27.

Qiao, L., Zhang, S., Li, J., 2018. Coulson-type integral formulas for the general energy of polynomials with real roots. ***Applied Mathematics and Computation,* 320*:*** 202-212.

Rosen, F., 1831. ***The Algebra of Mohammed Ben Musa***. The Oriental Translation Fund, London.

Rotman, J., 1998. ***Galois Theory***. Springer Verlag, New York.

Stewart, I., 1945. ***Galois Theory***. Chapman and Hall Ltd., London.

Sun H., Wang Y., Zhang H.X., 2015. Polynomials with palindromic and unimodal coefficients. ***Acta Matematica Sinica* 31**(4): 565- 575.

Süray, S., 1970. ***Umumi Matematik***, Çağlayan Kitapevi, İstanbul.

Tignol, J. P., 2001. ***Galois's Theory of Algebraic Equations***. World Scientific Publishing Co. Pte. Ltd., London.

ÖZ GEÇMİŞ

1993 yılında Mersin'de doğdu. İlk, orta ve lise eğitimini Mersin'de tamamladı. 2011 yılında Van Yüzüncü Yıl Üniversitesi, Fen Fakültesi, Matematik Bölümü'ne başladı ve 2015'de mezun oldu. Aynı yıl Van Yüzüncü Yıl Üniversitesi, Fen Bilimleri Enstitüsü, Matematik Anabilim Dalı'nda yüksek lisans eğitimine başladı.

T.C
VAN YÜZÜNCÜ YIL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
LİSANSÜSTÜ TEZ ORİJİNALLİK RAPORU

Tarih:27/06/2018

Tez Başlığı / Konusu:

Galois Teorisi,PalindromikPolinomlar ve Sıfırlarının Bulunuşu için Algoritmalar.....

.....

Yukarıda başlığı/konusu belirlenen tez çalışmamın Kapak sayfası, Giriş, Ana bölümler ve Sonuç bölümlerinden oluşan toplam 61+14 sayfalık kısmına ilişkin, 27/06/2018 tarihinde şahsım/tez danışmanım tarafından Turnitinintihal tespit programından aşağıda belirtilen filtreleme uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı % 3 (Üç) tür.
Uygulanan filtreler aşağıda verilmiştir:
- Kabul ve onay sayfası hariç,
- Teşekkür hariç,
- İçindekiler hariç,
- Simge ve kısaltmalar hariç,
- Gereç ve yöntemler hariç,
- Kaynakça hariç,
- Alıntılar hariç,
-Tezden çıkan yayınlar hariç,
- 7 kelimeden daha az örtüşme içeren metin kısımları hariç (Limit inatch size to 7 words)

Van Yüzüncü Yıl Üniversitesi Lisansüstü Tez Orijinallik Raporu Alınması ve Kullanılmasına İlişkin Yönergeyiinceledim ve bu yönergede belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihaliçermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabulettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini bilgilerinize arz ederim.

27.06.2018

Adı Soyadı: Fatma Tutar

Öğrenci No:159102003

Anabilim Dalı: Matematik

Programı: Matematik

Statüsü:Y.Lisans ■ Doktora □

DANIŞMAN ONAYI
UYGUNDUR

Doç. Dr. Şenay BAYDAŞ

ENSTİTÜ ONAYI
UYGUNDUR

(Unvan, Ad Soyadı, İmza)