T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SONLU CİSİMLER ÜZERİNDEKİ POLİNOMLARIN ÇARPANLARA AYRILIŞI

BETÜL DUMAN

YÜKSEK LİSANS TEZİ
MATEMATİK ANABİLİM DALI
MATEMATİK PROGRAMI

DANIŞMAN
DOÇ. DR. MURAT ALAN

İSTANBUL, 2017

T.C.

YILDIZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

SONLU CİSİMLER ÜZERİNDEKİ POLİNOMLARIN ÇARPANLARA AYRILIŞI

Betül DUMAN tarafından hazırlanan tez çalışması 25.05.2017 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Tez Danışmanı

Doç. Dr. Murat ALAN

Yıldız Teknik Üniversitesi

Jüri Üyeleri

Doç. Dr. Murat ALAN

Yıldız Teknik Üniversitesi _____

Prof. Dr. Bayram Ali ERSOY

Yıldız Teknik Üniversitesi _____

Prof. Dr. Ünsal TEKİR

Marmara Üniversitesi _____

ÖNSÖZ

Araştırmalarımın her aşamasında desteğini hiçbir zaman esirgemeyen, engin bilgi ve düşünceleriyle çalışmamı başarıyla bitirmemi sağlayan çok değerli Hocam Doç. Dr. Murat ALAN' a sonsuz teşekkür ederim.

Bugüne kadar bana hep destek olan ailemin her bir ferdine, çok değerli arkadaşlarım Sümeyra YOKUŞ, Büşra KAZANCI ve Tuğba ARKAN' a çok teşekkür ederim.

Mayıs, 2017

Betül DUMAN

İÇİNDEKİLER

Sayfa

SİMGE LİSTESİ v

ÇİZELGE LİSTESİ vi

ÖZET vii

ABSTRACT viii

BÖLÜM 1

GİRİŞ 1

1.1 Literatür Özeti 1
1.2 Tezin Amacı 2
1.3 Hipotez 2

BÖLÜM 2

SONLU CİSİMLER 3

BÖLÜM 3

TRİNOMİALLERİN DİSKRİMİNANTI İLE İNDİRGENEMEZLİK 31

BÖLÜM 4

İNDİRGENEMEZ POLİNOMLARIN İNŞASI 44

KAYNAKLAR 54

ÖZGEÇMİŞ 55

SİMGE LİSTESİ

$degf$	f polinomunun derecesi
$D(f)$	f polinomunun diskriminantı
E^n	Birimin n. kökleri kümesi
$f\|g$	f fonksiyonu g fonksiyonunu böler
f^*	f fonksiyonunun reciprocalı
$\mathbb{F}$	Herhangi bir mertebeden cisim
$\mathbb{F}_q$	q mertebeli sonlu cisim
$\mathbb{F}_q^*$	$\mathbb{F}_q$ cisminin sıfırdan farklı elemanlarından oluşan çarpımsal grup
$\mathbb{F}[x]$	Polinom halkası
$I(q,n;x)$	$\mathbb{F}_q$ üzerinde derecesi n olan monik, indirgenemez polinomların çarpımı
$K^{(n)}$	n. cyclotomic cisim
$N_{F\|K}(\alpha)$	α elemanına ait norm
$N_q(d)$	$\mathbb{F}_q$ üzerinde derecesi n olan monik, indirgenemez polinomların sayısı
$ordf$	f polinomunun mertebesi
$Q_n(x)$	n. cyclotomic polinom
$R(f,g)$	f ve g polinomlarının resultantı
$Tr_{F\|K}(\alpha)$	α elemanına ait trace (iz)
$\mathbb{Z}$	Tam Sayılar Kümesi
μ	Moebius fonksiyonu

ÇİZELGE LİSTESİ

Sayfa

Çizelge 3. 1 39

ÖZET

SONLU CİSİMLER ÜZERİNDEKİ POLİNOMLARIN ÇARPANLARA AYRILIŞI

Betül DUMAN

Matematik Anabilim Dalı

Yüksek Lisans Tezi

Tez Danışmanı: Doç. Dr. Murat ALAN

Bu tez çalışması dört bölümden oluşmaktadır. Birinci bölüm giriş bölümüne ayrılmıştır. İkinci bölümde, çalışma için gerekli, ileride kullanılacak olan sonlu cisimler için temel tanım ve kavramlar verilmiştir. Üçüncü bölümde, trinomialler için diskriminant tanımından yola çıkarak polinomların indirgenemezliği araştırılmış, ilgili teoremler ispatlanmıştır. Son bölümde ise indirgenemez bir polinom inşa etmek için gerekli durumlar açıklanmaya çalışılmış ve örnekler verilerek çalışma sonlandırılmıştır.

Anahtar Kelimeler: sonlu cisim, indirgenemez polinom, birimin kökleri ve cyclotomic polinomlar, minimal polinom, trace ve norm, polinomun mertebesi, Berlekamp algoritması, primitif polinom, trinomial, trinomiallerin diskriminantı.

ABSTRACT

FACTORIZATION OF POLYNOMIALS OVER FINITE FIELDS

Betül DUMAN

Department of Mathematics

MSc. Thesis

Adviser: Doç. Dr. Murat ALAN

This thesis consist of four chapters. The first chapter is devoted to the introduction. The second chapter, the fundamental definitions and theorems about finite fields have been given as preliminary notification. The third chapter, irreducibility of polynomials has been examined by using discriminant of trinomials and relevant theorems have been proved. The last chapter, necessary conditons have been explained to construction irreducible polynomial and the thesis has been finished by giving some examples.

Keywords: finite field, irreducible polynomial, roots of unity and cyclotomic polynomials, minimal polynomial, trace and norm, order of polynomials, Berlekamp's algorithm, primitive polynomial, trinomial, discriminant of trinomials.

BÖLÜM 1

GİRİŞ

1.1 Literatür Özeti

Sonlu cisimler üzerindeki indirgenemez polinomlar kodlama teorisi, kriptografi gibi dijital iletişim sistemlerinin etkili uygulamalarında önemli bir yere sahiptir. Ayrıca doğrulama kodlarının hatalarının inşa edilmesinde de bu polinomların payı büyüktür.

Genel olarak bir polinomun ne zaman indirgenemez olduğu tam olarak bilinememektedir. Bu sebeple bazı polinomların indirgenemezliğini kontrol etmek için oluşturulan sonuçlar çok önemlidir. Bu alanda ilk çalışmayı Swan [1] de yapmıştır. Swan burada sonlu cisimler üzerindeki herhangi bir trinomialin diskriminantı için bir formül vermiş ve bu formülü $\mathbb{F}_2$ üzerinde uygulayarak $\mathbb{F}_2$ üzerindeki trinomiallerin indirgenemez çarpanlarının sayısının tek ya da çift olup olmadığını belirlemiştir. Daha sonra Brent ve Zimmerman [2] de, Swan'ın Teoremini çok büyük dereceli indirgenemez trinomialler için durum sayısını düşürmek için kullanmışlardır.

Güncel çalışmalar daha çok tek karakteristikli sonlu cisimler üzerindeki polinomların indirgenemezliği üzerine olmuştur. Von Zur Gathen [3] te $\mathbb{F}_q$ üzerindeki bir polinomun tek sayıda indirgenemez çarpana sahip bir tam kare bölensiz polinom olmasının sadece $m_2 = p(q-1)$ ve $m_1 = lcm(4, m_2)$ olmak üzere $n\,(mod\, m_1)$, $k(mod\, m_2)$ ve ${}^{k}/_{\gcd(n,k)}\,(mod\, q-1)$ değerlerine bağlı olduğunu göstermiştir. Daha sonra $\mathbb{F}_3$ üzerindeki trinomiallere ait özel bir durumu analiz etmiş ve tek sayıda indirgenemez çarpana sahip tam kare bölensiz bir trinomialin koşullarını içeren bir tablo vermiştir.

Polinomların indirgenemezliği üzerine başka bir çalışma da 2010 yılında Abrahamyan

tarafından yapılmıştır. Abrahamyan [4] te $\mathbb{F}_q$ üzerinde derecesi m olan indirgenemez bir polinomdan derecesi pm olan başka bir indirgenemez oluşturmak için teorem vermiş ve bu teoremi $\mathbb{F}_4$ üzerindeki bir polinomla örneklendirmiştir.

1.2 Tezin Amacı

İlk olarak sonlu cisimler üzerindeki polinomların ve indirgenemezlik durumlarını inceleyen çalışmalar ele alınmış ve daha sonra bu çalışmalar göz önünde bulundurularak bu durumlara ek teoremlerin oluşturulması amaçlanmıştır.

1.3 Hipotez

Sonlu cisimler üzerindeki trinomiallerin indirgenemezliği ile ilgili teoremler oluşturulmuş ve ispatlanmıştır. Daha sonra polinomların genel hali üzerinde durumlar incelenmiş ve örnekler verilmiştir.

BÖLÜM 2

SONLU CİSİMLER

Tanım 2.1 p bir asal sayı olmak üzere $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ kümesini alalım. $a = 0, 1, \dots, p-1$ için $\emptyset[a] = a$ olacak şekilde

$$\emptyset: \mathbb{Z}/(p) \to \mathbb{F}_p$$

fonksiyonu tanımlayabiliriz. O zaman $\emptyset$ ile $\mathbb{Z}_p$ cisim yapısı $\mathbb{F}_p$ üzerine taşınabilir. Burada $\mathbb{F}_p$ cismine p *mertebeli Galois cismi* denir.

Ayrıca, $\emptyset([a] + [b]) = \emptyset([a]) + \emptyset([b])$ ve $\emptyset([a].[b]) = \emptyset([a]).\emptyset([b])$ olduğundan $\emptyset$ bir izomorfizmadır. Böylece $\mathbb{F}_p$ sonlu cisminin sıfır elemanı 0, birim elemanı 1 dir ve yapısı $\mathbb{Z}/(p)$ şeklindedir. Yani, $\mathbb{F}_p$ nin elemanları p modülüne göre tamsayılardır [5].

Örnek 2.2 $\mathbb{F}_3$ cisminin elemanları 0, 1 ve 2 dir.

Tanım 2.3 Keyfi bir R halkasında, her $r \in \mathrm{R}$ için $nr = 0$ eşitliğini sağlayan en küçük n sayısına, R halkasının karakteristiği denir. Eğer böyle bir n yoksa R nin karakteristiği sıfırdır denir [5].

Sonuç 2.4 Sonlu bir cismin karakteristiği asal sayıdır [5].

Örnek 2.5 $\mathbb{Z}/(p)$ $(\mathbb{F}_p)$ cisminin karakteristiği p dir.

Teorem 2.6 R, karakteristiği p olan değişmeli bir halka olsun. O zaman, her $a, b \in R$ ve her $n \in \mathbb{N}$ için

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}$$

ve

$$(a-b)^{p^n} = a^{p^n} - b^{p^n}$$

dir [1].

Tanım 2.7 (İndirgenemez Polinom) $p, b, c \in \mathbb{F}[x]$ olmak üzere $p = bc$ olması için b veya c den en az birinin sabit olması gerekiyorsa p ye indirgenemez polinom denir. Aksi halde p ye indirgenebilir denir [5].

Teorem 2.8 $f \in \mathbb{F}[x]$ herhangi bir polinom olmak üzere f,

$$f = a{p_1}^{e_1}{p_2}^{e_2} \dots {p_k}^{e_k}$$

olacak şekilde tek türlü yazılabilir. Burada $a \in \mathbb{F}$, $e_1, e_2, \dots, e_k \in \mathbb{Z}^+$ ve $p_1, p_2, \dots, p_k$ polinomları $\mathbb{F}[x]$ te farklı, monik, indirgenemez polinomlardır [5].

Teorem 2.9 $f \in \mathbb{F}[x]$ için, $\mathbb{F}/< f >$ nin cisim olması için gerek ve yeter koşul f nin $\mathbb{F}$ üzerinde indirgenemez olmasıdır [5].

Tanım 2.10 Bir $a \in \mathbb{F}$ ve $f \in \mathbb{F}[x]$ için $f(a) = 0$ oluyorsa, a ya f polinomunun bir kökü denir [5].

Teorem 2.11 Bir $a \in \mathbb{F}$ elemanının $f \in \mathbb{F}[x]$ polinomunun kökü olması için gerek ve yeter koşul $(x-a) | f$ olmasıdır [5].

İspat $q \in \mathbb{F}[x]$ ve $r \in \mathbb{F}$ olmak üzere

$$f(x) = (x-a)q(x) + r$$

yazabiliriz. $x = a$ için $f(a) = r$ olur.

Buradan,

$$f(x) = (x-a)q(x) + f(a).$$

Tanım 2.12 $a \in \mathbb{F}$, $f \in \mathbb{F}[x]$ polinomunun bir kökü olsun. $k \in \mathbb{Z}^+$ olmak üzere $(x-a)^k \mid f$; ancak $(x-a)^{k+1} \nmid f$ oluyorsa k ya, a nın katlılığı denir. Eğer $k \geq 2$ ise o zaman a ya f nin katlı kökü denir [5].

Teorem 2.13 $a \in \mathbb{F}$ elemanının, $f \in \mathbb{F}[x]$ polinomunun katlı kökü olması için gerek ve yeter koşul a nın hem f nin hem de f' (f nin türevi) nin kökü olmasıdır [5].

Teorem 2.14 $\mathbb{F}$ bir cisim ve $f \in \mathbb{F}[x]$ derecesi n olan bir polinom olmak üzere $\mathbb{F}$ cismi, f polinomunun en fazla n tane kökünü içerir [5].

Tanım 2.15 $\mathbb{F}$ bir cisim olsun. $K \subseteq \mathbb{F}$, $\mathbb{F}$ deki işlemlere göre bir grup belirtiyorsa K ya, $\mathbb{F}$ nin bir *alt cismi* denir. Burada $\mathbb{F}$ ye, K nın bir cisim genişlemesi denir. Eğer, $K \neq \mathbb{F}$ ise K, $\mathbb{F}$ nin bir özalt cismidir [5].

Tanım 2.16 Özalt cismi olmayan cisme *asal cisim* denir [5].

Tanım 2.17 $\mathbb{F}$ bir cisim olmak üzere, $\mathbb{F}$ nin tüm alt cisimlerinin kesişimine *asal alt cisim* denir [5].

Teorem 2.18 Bir $\mathbb{F}$ cisminin asal alt cismi; $\mathbb{F}$ nin karakteristiği 0 ise $\mathbb{Q}$ ya, $\mathbb{F}$ nin karakteristiği p ise $\mathbb{Z}_p$ ye izomorftur [5].

Tanım 2.19 K, $\mathbb{F}$ nin bir alt cismi ve $\alpha \in \mathbb{F}$ olsun. Eğer en az bir $0 \neq a_i \in K$ için

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

oluyorsa α ya K üzerinde cebirseldir denir [5].

Eğer $\mathbb{F}$ nin her elemanı K üzerinde cebirselse o zaman $\mathbb{F}$ ye K üzerinde cebirseldir denir.

Tanım 2.20 $\alpha \in \mathbb{F}$, K üzerinde cebirsel olmak üzere, α yı kök kabul eden en küçük dereceli, monik, indirgenemez polinoma α nın K üzerindeki minimal polinomu denir. Bu polinom, $\mathbb{F}$ nin elemanları göz ardı edilirse tek türlüdür. Ayrıca bu polinomun derecesi α nın K üzerindeki derecesidir [5].

Teorem 2.21 $\alpha \in \mathbb{F}$, K üzerinde cebirsel ve f, α nın minimal polinomu olsun. O zaman

(i) f, $K[x]$ te indirgenemezdir.

(ii) $g \in K[x]$ olmak üzere $g(\alpha) = 0 \Leftrightarrow f \mid g$ dir.

(iii) f, α yı kök kabul eden en küçük dereceli monik polinomdur [5].

Teorem 2.22 $\mathbb{F}$, K nın bir cisim genişlemesi, $\alpha \in \mathbb{F}$, K üzerinde derecesi n olan cebirsel eleman ve f, α nın K üzerindeki minimal polinomu olmak üzere,

(i) $K(\alpha) \cong K[x]/< f >$;

(ii) $[K(\alpha):K] = n$ ve $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$, $K(\alpha)$ nın K üzerindeki bir tabanıdır.

(iii) Her $\beta \in K(\alpha)$, K üzerinde cebirseldir ve K üzerindeki derecesi n yi böler [5].

Teorem 2.23 $f \in K[x]$, K üzerinde indirgenemez bir polinom olsun. O zaman f polinomunun bir kökü ile K cisminin basit bir genişlemesi vardır [5].

Tanım 2.24 $\mathbb{F}$, K nın bir cisim genişlemesi ve $f \in K[x]$ pozitif dereceli bir polinom olsun. a, f nin başkatsayısı olmak üzere eğer

$$f = a(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$$

olacak şekilde $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{F}$ elemanları varsa f polinomuna $\mathbb{F}$ de parçalanış denir.

$\mathbb{F} = K(\alpha_1, \alpha_2, \dots, \alpha_n)$ iken f polinomu K üzerinde parçalanıyorsa, $\mathbb{F}$ cismine f polinomunun K üzerindeki *parçalanış cismi* denir [5].

Yani K üzerindeki bir f polinomunun parçalanış cismi, f polinomunun köklerini içeren en küçük cisim genişlemesidir [5].

Teorem 2.25 (Parçalanış Cisminin Varlığı ve Tekliği) K bir cisim ve $f \in K[x]$ herhangi bir polinom olmak üzere K üzerinde f polinomunun bir parçalanış cismi vardır. Bu parçalanış cismi tektir [5].

Lemma 2.26 $\mathbb{F}$ sonlu bir cisim ve K, $\mathbb{F}$ nin q elemanlı bir alt cismi olsun. O halde $[\mathbb{F}: K] = m$ ise $\mathbb{F}$ cismi q^m tane elemana sahiptir [5].

Teorem 2.27 p bir asal sayı olmak üzere $\mathbb{F}$, karakteristiği p olan sonlu bir cisim olsun. O halde $\mathbb{F}$ cisminin asal alt cismi üzerindeki derecesi n ise $\mathbb{F}$ cismi p^n tane elemana sahiptir [5].

Lemma 2.28 $\mathbb{F}$, q elemanlı sonlu bir cisim olmak üzere her $a \in \mathbb{F}$ için $a^q = a$ olur [5].

İspat $a = 0$ için $a^q = a$ olur. $\mathbb{F}$ cisminde sıfır olmayan tüm elemanlar birlikte çarpmaya göre $q-1$ elemanlı bir cisim oluştururlar. Sonlu bir G grubunun her a elemanı için $a^{|G|} = 1_G$ olduğundan tüm $0 \neq a \in \mathbb{F}$ için $a^{q-1} = 1$ dir. Buradan $a^q = a$ olur.

Örnek 2.29 $f(x) = x^4 + 2x^3 + x^2 + x + 2 \in \mathbb{F}_3[x]$ polinomu indirgenemez olduğuna göre $\mathbb{F}_9 \subset {}^{\mathbb{F}_3}/_{< f >}$ cismini oluşturalım.

α, $x^4 + 2x^3 + x^2 + x + 2$ polinomunun bir kökü olmak üzere,

$\mathbb{F}_{81} = \{\beta | \beta = a\alpha^3 + b\alpha^2 + c\alpha + d$ ve $a, b, c, d \in \mathbb{F}_3$ ve $\alpha^4 + 2\alpha^3 + \alpha^2 + \alpha + 2 = 0\}$

olur. Şimdi Lemma 2.28 e göre $\beta \in \mathbb{F}_9$ olması için gerek ve yeter koşul $\beta^9 = \beta$ olmasıdır. Buradan,

$$(a\alpha^3 + b\alpha^2 + c\alpha + d)^9 = a\alpha^3 + b\alpha^2 + c\alpha + d$$

$$a\alpha^{27} + b\alpha^{18} + c\alpha^9 + d = a\alpha^3 + b\alpha^2 + c\alpha + d$$

$$a(\alpha^2 + 2\alpha) + b(2\alpha^2 + 1) + c(2\alpha^3 + 2\alpha^2 + 1) + d = a\alpha^3 + b\alpha^2 + c\alpha + d$$

$$(2c)\alpha^3 + (a + 2b + 2c)\alpha^2 + (2a)\alpha + b + c + d = a\alpha^3 + b\alpha^2 + c\alpha + d$$

Böylece,

$2c = a$

$a + 2b + 2c = b \Longrightarrow b = 2c$

$2a = c$

$b + c + d = d$

Bu denklem sistemine göre c ve d keyfi sabitler olmak üzere $a = 2c$ ve $b = 2c$ dir.

O halde,

$$\mathbb{F}_9 = \{2c\alpha^3 + 2c\alpha^2 + c\alpha + d \text{ ve } c, d \in \mathbb{F}_3 \text{ ve } \alpha^4 + 2\alpha^3 + \alpha^2 + \alpha + 2 = 0\}$$

$$= \{0, 1, 2, 2\alpha^3 + 2\alpha^2 + \alpha, 2\alpha^3 + 2\alpha^2 + \alpha + 1, 2\alpha^3 + 2\alpha^2 + \alpha + 2,$$

$$\alpha^3 + \alpha^2 + 2\alpha,\ \alpha^3 + \alpha^2 + 2\alpha + 1, \alpha^3 + \alpha^2 + 2\alpha + 2\}$$

dir.

Lemma 2.30 $\mathbb{F}$, q elemanlı sonlu bir cisim ve K, $\mathbb{F}$ nin bir alt cismi olsun. O halde $x^q - x \in K[x]$ polinomu

$$x^q - x = \prod_{a \in \mathbb{F}} (x - a)$$

şeklinde yazılabilir. Burada $\mathbb{F}$, $x^q - x$ polinomunun K üzerindeki parçalanış cismidir [1].

Teorem 2.31 (Sonlu Cisimlerin Varlığı ve Tekliği) Her p asal sayısı ve n pozitif tamsayısı için p^n elemanlı bir cisim vardır. $q = p^n$ elemanlı herhangi bir cisim, $x^q - x$ polinomunun $\mathbb{F}_p$ üzerindeki parçalanış cismine izomorftur [5].

Teorem 2.32 (Alt Cisim Olma Kriteri) $\mathbb{F}_q$, $q = p^n$ elemanlı sonlu bir cisim olsun. $|K| = p^m$ olmak üzere K cisminin $\mathbb{F}$ nin bir alt cismi olması için gerek ve yeter koşul $m|n$ olmasıdır [1].

Teorem 2.33 $\mathbb{F}_q$ sonlu bir cisim olmak üzere $\mathbb{F}_q^*$ çarpımsal grubu devirlidir [5].

Tanım 2.34 $\mathbb{F}_q^*$ çarpımsal grubunun üretecine $\mathbb{F}_q$ cisminin *primitif elemanı* denir.

ϕ, Euler Fonksiyonu olmak üzere $\mathbb{F}_q$ cisminin primitif eleman sayısı $\phi(q-1)$ tanedir [5].

Örnek 2.35 $\mathbb{F}_5$ sonlu cisminin primitif elemanları 2 ve 3 olmak üzere $\phi(4) = 2$ tanedir.

Teorem 2.36 $\mathbb{F}_q$ sonlu bir cisim ve $\mathbb{F}_r$ bir cisim genişlemesi olsun. O zaman, $\mathbb{F}_r$ cismi $\mathbb{F}_q$ cisminin basit cebirsel genişlemesidir [5].

Sonuç 2.37 Her $\mathbb{F}_q$ sonlu cismi ve n pozitif tamsayısı için $\mathbb{F}_q[x]$ te derecesi n olan bir indirgenemez polinom vardır [5].

Lemma 2.38 $\mathbb{F}_q$ sonlu bir cisim olmak üzere $f \in \mathbb{F}_q[x]$ indirgenemez bir polinom ve α, f polinomunun $\mathbb{F}_q$ üzerindeki bir cisim genişlemesindeki kökü olsun. O zaman bir $h \in \mathbb{F}_q[x]$ için

$$h(\alpha) = 0 \Leftrightarrow f \mid h$$

[5].

Lemma 2.39 $f \in \mathbb{F}_q[x]$, derecesi m olan indirgenemez bir polinom olsun. O zaman

$$f \mid x^{q^n} - x \Leftrightarrow m \mid n$$

[5].

İspat ($\Rightarrow$) α, f polinomunun bir kökü olsun.

$$x^{q^n} - x = f(x)h(x) \Rightarrow \alpha^{q^n} - \alpha = 0$$

$$\Rightarrow \alpha^{q^n} = \alpha$$

$$\Rightarrow \alpha \in \mathbb{F}_{q^n}$$

$$\Rightarrow \mathbb{F}_q(\alpha) \subseteq \mathbb{F}_{q^n}$$

Ayrıca $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$ ve $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ olduğundan

$$\left[\mathbb{F}_{q^n}: \mathbb{F}_q\right] = \left[\mathbb{F}_{q^n}: \mathbb{F}_q(\alpha)\right]\left[\mathbb{F}_q(\alpha): \mathbb{F}_q\right]$$

ifadesinden $m|n$ olur.

($\Leftarrow$) $m|n$ olsun. O halde $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$ olur.

α, f polinomunun bir kökü olsun. Buradan $f(\alpha) = 0$ olur.

$$\left[\mathbb{F}_q(\alpha): \mathbb{F}_q\right] = m \Rightarrow \mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$$

$$\Rightarrow \alpha \in \mathbb{F}_{q^n}$$

$$\Rightarrow \alpha^{q^n} = \alpha$$

$$\Rightarrow f|x^{q^n} - x$$

Teorem 2.40 $f \in \mathbb{F}_q[x]$, derecesi m olan indirgenemez bir polinom olsun. f nin bir kökü α ise tüm kökleri;

$$\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}} \in \mathbb{F}_{q^m}$$

dir ve hepsi birbirinden farklıdır [5].

İspat α, f polinomunun $\mathbb{F}_q$ üzerindeki bir cisim genişlemesindeki kökü olsun. O zaman $\left[\mathbb{F}_q(\alpha): \mathbb{F}_q\right] = m$ olur ve buradan $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$, yani $\alpha \in \mathbb{F}_{q^m}$ dir.

$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$ olsun. O halde $f(\alpha) = 0$ dır.

$$f(\alpha^q) = a_0 + a_1\alpha^q + a_2\alpha^{2q} + \cdots + a_m\alpha^{mq}$$

$$= a_0^q + a_1^q\alpha^q + a_2^q\alpha^{2q} + \cdots + a_m^q\alpha^{mq}$$

$$= (a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_m\alpha^m)^q$$

$$= 0$$

$$\Rightarrow \alpha^q \text{ da } f \text{ polinomunun bir köküdür.}$$

Bu şekilde devam edersek $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}} \in \mathbb{F}_{q^m}$ elemanlarının f polinomunun kökü olduğunu kolayca görebiliriz. Ayrıca bir önceki teoremden;

$$f|x^{q^m} - x \Rightarrow x^{q^m} - x = f(x)h(x) \Rightarrow \alpha^{q^m} - \alpha = 0 \Rightarrow \alpha^{q^m} = \alpha$$

olur.

Şimdi $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}}$ köklerinin birbirinden farklı olduğunu gösterelim.

$\alpha^{q^k} = \alpha^{q^i}$ olsun $(0 \leq k < i \leq m-1)$. O zaman,

$$(\alpha^{q^k})^{q^{m-k}} = (\alpha^{q^i})^{q^{m-k}}$$

$$\Rightarrow \alpha^{q^m} = \alpha^{q^{m-k+i}} = \alpha$$

$$\Rightarrow \alpha^{q^{m-k+i}} - \alpha = 0$$

ve $f(x)$ minimal polinom olduğundan

$$f(x) | x^{q^{m-k+i}} - x$$

$$\Rightarrow m | m-k+i$$

$$\Rightarrow m | i-k$$

olur ki bu durum $i-k < m$ olduğundan çelişkidir.

Sonuç 2.41 $f \in \mathbb{F}_q[x]$, derecesi m olan indirgenemez bir polinom olsun. f nin $\mathbb{F}_q$ üzerindeki parçalanış cismi $\mathbb{F}_{q^m}$ dir [5].

Tanım 2.42 $\mathbb{F}_q$ sonlu bir cisim ve $\mathbb{F}_{q^m}$ cisim genişlemesi olsun. $\alpha \in \mathbb{F}_{q^m}$ olmak üzere α elemanının $\mathbb{F}_q$ üzerindeki eşlenikleri

$$\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}}$$

elemanlarıdır [5].

Teorem 2.43 $\alpha \in \mathbb{F}_q^*$ elemanının herhangi bir alt cisme göre eşleniklerinin mertebesi α nın mertebesine eşittir [5].

Teorem 2.44 (Trace) $F = \mathbb{F}_{q^m}$ ve $K = \mathbb{F}_q$ olmak üzere $\alpha \in F$ nin K üzerindeki izi (trace) $Tr_{F/K}(\alpha)$ ile gösterilir ve

$$Tr_{F/K}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}}$$

şeklinde tanımlanır. Yani $Tr_{F/K}(\alpha)$, α nın K üzerindeki eşleniklerinin toplamına eşittir [5].

Teorem 2.45 $\alpha \in F$ ve $f \in K[x]$, α nın K üzerindeki d. dereceden minimal polinomu ve $m = [F:K]$ olmak üzere $d|m$ olsun. O halde, $g = f^{m/d} \in K[x]$ polinomuna α nın K üzerindeki *karakteristik polinomu* denir.

$$g(x) = [f(x)]^{m/d} = (x-\alpha)(x-\alpha^q)\dots(x-\alpha^{q^{m-1}})$$

şeklinde idi. Eğer,

$$g(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$$

ise $Tr_{F/K}(\alpha) = -a_{m-1} \in K$ dır [5].

Teorem 2.46 $F = \mathbb{F}_{q^m}$ ve $K = \mathbb{F}_q$ olsun. O zaman, $Tr_{F/K}$ aşağıdaki özellikleri sağlar:

(i) $Tr_{F/K}(\alpha+\beta) = Tr_{F/K}(\alpha) + Tr_{F/K}(\beta), \quad \forall\, \alpha,\beta \in F$

(ii) $Tr_{F/K}(c\alpha) = cTr_{F/K}(\alpha), \quad \forall\, c \in K, \alpha \in F$

(iii) $Tr: F \longmapsto K$ bir lineer dönüşümdür ve örtendir.

(iv) $Tr_{F/K}(a) = ma, \quad \forall\, a \in K$

(v) $Tr_{F/K}(\alpha^q) = Tr_{F/K}(\alpha), \quad \forall\, \alpha \in F$ [5].

İspat

(i) $\alpha,\beta \in F$ olmak üzere,

$$\begin{aligned} Tr_{F/K}(\alpha+\beta) &= \alpha+\beta+(\alpha+\beta)^q+\cdots+(\alpha+\beta)^{q^{m-1}} \\ &= \alpha+\beta+\alpha^q+\beta^q+\cdots+\alpha^{q^{m-1}}+\beta^{q^{m-1}} \\ &= \alpha+\alpha^q+\cdots+\alpha^{q^{m-1}}+\beta+\beta^q+\cdots+\beta^{q^{m-1}} \\ &= Tr_{F/K}(\alpha)+Tr_{F/K}(\beta) \end{aligned}$$

(ii) $c \in K$ ve $\alpha \in F$ olmak üzere,

$$\begin{aligned} Tr_{F/K}(c\alpha) &= c\alpha+(c\alpha)^q+\cdots+(c\alpha)^{q^{m-1}} \\ &= c\alpha+c^q\alpha^q+\cdots+c^{q^{m-1}}\alpha^{q^{m-1}} \\ &= c\alpha+c\alpha^q+\cdots+c\alpha^{q^{m-1}} \\ &= cTr_{F/K}(\alpha) \end{aligned}$$

(iii) (i) ve (ii) den $Tr_{F/K}$ lineer dönüşümdür. Şimdi bu lineer dönüşümün örten olduğunu ispatlamak için $Tr_{F/K}(\alpha) \neq 0$ olacak şekilde en az bir $\alpha \in F$ olduğunu gösterelim.

$\alpha \in Ker(Tr) \Leftrightarrow Tr(\alpha) = 0 \Leftrightarrow \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}} = 0$

$\Leftrightarrow \alpha, x + x^q + x^{q^2} + \cdots + x^{q^{m-1}}$ polinomunun köküdür.

$\Leftrightarrow |Ker(Tr)| \leq q^{m-1}$

$F/_{Ker(Tr)} \cong Im(Tr) \subseteq K$ ve $\left|F/_{Ker(Tr)}\right| = \frac{q^m}{q^{m-1}} \geq q$ olduğundan $Im(Tr) = K$ olur. Buradan, $Tr_{F/_K}$ lineer dönüşümü örtendir.

(iv) $a \in K$ olmak üzere,

$$Tr_{F/_K}(a) = a + a^q + \cdots + a^{q^{m-1}}$$

$$= a + a + \cdots + a$$

$$= ma$$

(v) $\alpha \in F$ olmak üzere,

$$Tr_{F/_K}(\alpha^q) = \alpha^q + (\alpha^q)^q + (\alpha^q)^{q^2} + \cdots + (\alpha^q)^{q^{m-1}}$$

$$= \alpha^q + \alpha^{q^2} + \alpha^{q^3} + \cdots + \alpha$$

$$= Tr(\alpha)$$

Teorem 2.47 $F = \mathbb{F}_{q^m}$ ve $K = F_q$ olsun. $\beta \in F$ için $L_\beta: F \longmapsto K$, $\alpha \longmapsto Tr(\beta\alpha)$ bir lineer dönüşümdür. Eğer $L: F \longmapsto K$ herhangi bir lineer dönüşüm ise $L = L_\beta$ olacak şekilde bir $\beta \in F$ vardır [5].

Teorem 2.48 K sonlu bir cisim ve F, K nın bir cisim genişlemesi ve E de F nin bir cisim genişlemesi olsun. O zaman,

$$Tr_{E/_K}(\alpha) = Tr_{F/_K}\left(Tr_{E/_F}(\alpha)\right), \quad \forall\, \alpha \in E$$

dir [5].

Teorem 2.49 (Norm) $F = F_{q^m}$ ve $K = F_q$ olmak üzere $\alpha \in F$ nin K üzerindeki normu $N_{F/_K}(\alpha)$ ile gösterilir ve

$$N_{F/_K}(\alpha) = \alpha.\alpha^q.\alpha^{q^2} \ldots \alpha^{q^{m-1}}$$

$$= \alpha^{q^m-1/_{q-1}}$$

ile tanımlanır.

Eğer α nın K üzerindeki karakteristik polinomu

$$g(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$$

ise $N_{F/K}(\alpha) = (-1)^m a_0 \in K$ dır [5].

Teorem 2.50 $F = F_{q^m}$ ve $K = F_q$ olsun. O zaman, $N_{F/K}$ aşağıdaki özellikleri sağlar:

(i) $N_{F/K}(\alpha\beta) = N_{F/K}(\alpha)N_{F/K}(\beta), \quad \forall\, \alpha, \beta \in F$

(ii) $N_{F/K}: F \longmapsto K,\ N_{F/K}: F^* \longmapsto K^*$ fonksiyonları örten fonksiyonlardır.

(iii) $N_{F/K}(a) = a^m, \quad \forall\, a \in K$

(iv) $N_{F/K}(\alpha^q) = N_{F/K}(\alpha), \quad \forall\, \alpha \in F$ [5].

İspat

(i) $\alpha, \beta \in F$ olmak üzere,

$$\begin{aligned} N_{F/K}(\alpha\beta) &= (\alpha\beta).(\alpha\beta)^q \ldots (\alpha\beta)^{q^{m-1}} \\ &= \alpha.\beta.\alpha^q\beta^q \ldots . \alpha^{q^{m-1}}\beta^{q^{m-1}} \\ &= \alpha.\alpha^q.\alpha^{q^2} \ldots \alpha^{q^{m-1}}\beta.\beta^q\beta^{q^2} \ldots \beta^{q^{m-1}} \\ &= N_{F/K}(\alpha)N_{F/K}(\beta) \end{aligned}$$

(ii) $N_{F/K}: F^* \longmapsto K^*$ fonksiyonunu alalım.

$\alpha \in F^*$ olmak üzere $\alpha \in Ker(N) \Leftrightarrow N(\alpha) = 1$

$$\Leftrightarrow \alpha^{q^{m-1}/q-1} - 1 = 0$$

$\Leftrightarrow \alpha, x^{q^{m-1}/q-1} - 1$ polinomunun bir köküdür.

$$\Leftrightarrow |Ker(N)| \leq \frac{q^{m-1}}{q-1}$$

$\left|F^*/Ker(N)\right| = \frac{q^{m-1}}{\frac{q^{m-1}}{q-1}} \geq q-1$ ve $F^*/Ker(N) \cong Im(N) \subseteq K^*$ olduğundan $|Im(N)| \geq q-1$ olmalı. Buradan, $Im(N) = K^*$ olur ve N örtendir.

(iii) $a \in K$ olmak üzere,

$$N_{F/K}(a) = a.a^q \dots a^{q^{m-1}}$$

$$= \underbrace{a.a \dots a}_{m\ tane} = a^m$$

(iv) $\alpha \in F$ olmak üzere,

$$N_{F/K}(\alpha^q) = \alpha^q.(\alpha^q)^q \dots (\alpha^q)^{q^{m-1}}$$

$$= \alpha^q.\alpha^{q^2} \dots \underbrace{\alpha^{q^m}}_{\alpha}$$

$$= N_{F/K}(\alpha)$$

Teorem 2.51 K sonlu bir cisim ve F, K nın bir cisim genişlemesi ve E de F nin bir cisim genişlemesi olsun. O zaman,

$$N_{E/K}(\alpha) = N_{F/K}\left(N_{E/F}(\alpha)\right), \quad \forall\, \alpha \in E$$

[5].

Örnek 2.52 $x^4 + 2x^3 + x^2 + x + 2 \in \mathbb{F}_3[x]$ indirgenemez bir polinom ve $F = \mathbb{F}_{81}$, $L = \mathbb{F}_9$ ve $K = \mathbb{F}_3$ olduğuna göre,

(i) $Tr_{F|K}(\alpha^2 + 2\alpha + 2)$,

(ii) $Tr_{F|L}(\alpha^2 + \alpha + 1)$ ve

(iii) $N_{F|L}(\alpha^3)$ değerlerini hesaplayalım.

α, $x^4 + 2x^3 + x^2 + x + 2$ polinomunun kökü olmak üzere,

$\alpha^4 = \alpha^3 + 2\alpha^2 + 2\alpha + 1$

$\alpha^6 = \alpha^3 + \alpha$

$\alpha^9 = \alpha^6 + \alpha^4 = 2\alpha^3 + 2\alpha^2 + 1$

$\alpha^{18} = \alpha^9 + \alpha^3 = 2\alpha^2 + 1$

$\alpha^{27} = 2\alpha^9 + 2\alpha^6 + 1 = \alpha^2 + 2\alpha$

$\alpha^{54} = 2\alpha^6 + 1 = 2\alpha^3 + 2\alpha + 1$

(i) $Tr_{F|K}(\alpha^2 + 2\alpha + 2) = Tr_{F|K}(\alpha^2) + Tr_{F|K}(2\alpha) + Tr_{F|K}(2)$

$$= \alpha^2 + (\alpha^2)^3 + (\alpha^2)^{3^2} + (\alpha^2)^{3^3} + 2\left(\alpha + \alpha^3 + \alpha^{3^2} + \alpha^{3^3}\right) + 4.2$$

$$= \alpha^2 + \alpha^6 + \alpha^{18} + \alpha^{54} + 2\alpha + 2\alpha^3 + 2\alpha^9 + 2\alpha^{27} + 2$$

$$= \alpha^2 + \alpha^6 + \alpha^9 + \alpha^3 + 2\alpha^6 + 1 + 2\alpha + 2\alpha^3 + 2\alpha^9 + 2\alpha^{27} + 2$$

$$= \alpha^2 + 2\alpha + 2\alpha^2 + \alpha$$

$$= 0$$

(ii) $Tr_{F|L}(\alpha^2 + \alpha + 1) = Tr_{F|L}\left(\alpha^2\right) + Tr_{F|L}(\alpha) + Tr_{F|L}(1)$

$$= \alpha^2 + (\alpha^2)^9 + \alpha + \alpha^9 + 2.1$$

$$= \alpha^2 + \alpha^{18} + \alpha + \alpha^9 + 2$$

$$= \alpha^2 + 2\alpha^2 + 1 + \alpha + 2\alpha^3 + 2\alpha^2 + 1 + 2$$

$$= 2\alpha^3 + 2\alpha^2 + \alpha + 1$$

(iii) $N_{F|L}(\alpha^3) = (\alpha^3)^{\frac{9^2-1}{9-1}} = (\alpha^3)^{10} = \alpha^{30} = \alpha^3\alpha^{27} = \alpha^3(\alpha^2 + 2\alpha) = \alpha^5 + 2\alpha^4$

$$= \alpha^4 + 2\alpha^3 + 2\alpha^2 + \alpha + 2\alpha^4$$

$$= 2\alpha^3 + 2\alpha^2 + \alpha$$

Tanım 2.53 $F = \mathbb{F}_{q^m}$ ve $K = \mathbb{F}_q$ olsun. $\alpha \in F$ olmak üzere $\{1, \alpha, \alpha^2, \dots, \alpha^{m-1}\}$ kümesine F nin K üzerindeki bir *polinom tabanı* denir [5].

Tanım 2.54 $F = \mathbb{F}_{q^m}$ ve $K = \mathbb{F}_q$ olsun. Eğer bir $\alpha \in F$ için $\{\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}}\}$ kümesi F nin K üzerindeki bir tabanı ise bu tabana *normal taban* denir. $\alpha \in F$ elemanına da F nin K üzerindeki bir *normal elemanı* denir [5].

Teorem 2.55 (Normal Taban Teoremi) K herhangi bir sonlu cisim ve F de K nın cisim genişlemesi olmak üzere F nin K üzerinde bir normal tabanı mevcuttur [5].

Tanım 2.56 $n \in \mathbb{N}$ olsun. $x^n - 1$ polinomunun K üzerindeki parçalanış cismine *n. cyclotomic cisim* denir ve $K^{(n)}$ ile gösterilir. $x^n - 1 \in K[x]$ polinomunun köklerine ise *birimin n. kökleri* denir ve bu köklerin kümesi $E^{(n)}$ ile gösterilir [5].

Teorem 2.57 $n \in \mathbb{N}$ ve K, karakteristiği p (burada p 0 olabilir) olan sonlu bir cisim olsun. O zaman,

(i) $p \nmid n \Rightarrow E^{(n)}$, mertebesi n olan çarpımsal devirli bir gruptur.

(ii) $p \mid n \Rightarrow n = mp^e$ ve $p \nmid n$ olmak üzere $K^{(n)} = K^{(m)}$ ve $E^{(n)} = E^{(m)}$ dir [5].

Tanım 2.58 K, karakteristiği p olan bir cisim ve n, $p \nmid n$ olacak şekilde bir tamsayı olsun. $E^{(n)}$ devirli grubunun üretecine *birimin n. ilkel kökü* denir.

$E^{(n)}$ kümesinin tam olarak $\phi(n)$ tane üreteci vardır. $E^{(n)} =< \zeta >$ olmak üzere K üzerindeki tüm birimin n. ilkel köklerinin kümesi

$$\{\zeta^s : 1 \leq s \leq n, \gcd(s,n) = 1\}$$

ile gösterilir [5].

Tanım 2.59 K, karakteristiği p olan bir cisim, $p \nmid n$ ve de ζ, K üzerindeki birimin n. ilkel kökü olsun. O halde,

$$Q_n(x) = \prod_{\substack{s=1 \\ (s,n)=1}}^{n} (x - \zeta^s)$$

polinomuna K üzerinde *n. cyclotomic polinom* denir. Ayrıca bu polinomun derecesi $\phi(n)$ e eşittir [5].

Teorem 2.60 K, karakteristiği p olan bir cisim ve $p \nmid n$ olmak üzere

(i) $x^n - 1 = \prod_{d|n} Q_d(x)$;

(ii) $Q_n(x)$ polinomunun başkatsayısı K nın asal alt cisminin elemanıdır [5].

Örnek 2.61 p bir asal sayı ve $n \in \mathbb{N}$ olmak üzere

$$Q_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$$

$$Q_{p^2}(x) = 1 + x^p + x^{2p} + \cdots + x^{(p-1)p}$$

$$Q_{p^k}(x) = 1 + x^{p^{k-1}} + x^{2p^{k-1}} + \cdots + x^{(p-1)p^{k-1}}$$

dir.

Teorem 2.62 $K^{(n)}$ her zaman K cisminin bir basit genişlemesidir. Ayrıca,

(i) $K = Q$ ise $Q_n(x)$ polinomu her zaman K üzerinde indirgenemezdir ve $[K^n : K] = \phi(n)$ dir.

(ii) $K = \mathbb{F}_q$ ve $\gcd(q,n) = 1$ olmak üzere $q^d \equiv 1\ (mod\ n)$ ifadesini sağlayan en küçük pozitif tamsayı d olsun. O halde $Q_n(x)$ polinomu dereceleri d olan $\phi(n)/d$ tane farklı monik indirgenemez polinomun çarpımı şeklinde yazılır [5].

İspat Eğer ζ, K üzerinde $n.$ dereceden birimin ilkel kökü ise o zaman $K^{(n)} = K(\zeta)$ dir. Diğer taraftan, Teorem 2.57 (ii) ye göre $K^{(n)} = K^{(m)}$ dir. Kalan ifadeyi göstermek için (ii) yi ispatlamak yeterli olacaktır. Şimdi, $Q_n(x)$ polinomunun herhangi bir kökü α olsun. α nın minimal polinomunun derecesi ise k olsun. O halde $\alpha \in \mathbb{F}_{q^k}$ olur.

$\alpha \in \mathbb{F}_{q^k} \Rightarrow \alpha^{q^k} = \alpha \Rightarrow \alpha^{q^k-1} = 1 \Rightarrow n | q^k - 1$ (α, $Q_n(x)$ nın kökü olduğundan $\alpha^n = 1$)

$$\Rightarrow q^k \equiv 1\ mod\ n$$

$$\Rightarrow k = d$$

$$\Rightarrow \alpha \in \mathbb{F}_{q^d}$$

olur. Buradan α keyfi bir kök olduğundan α nın K üzerindeki minimal polinomunun derecesi d dir. Ayrıca, $Q_n(x)$ polinomunun derecesi $\phi(n)$ olduğundan bu polinomlar tam olarak $\phi(n)/d$ tanedir.

Örnek 2.63 $\mathbb{F}_2$ üzerinde $2 \nmid 15$ olduğundan $Q_{15}(x)$ polinomu tanımlıdır.

$$Q_{15}(x) = x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$= (x^4 + x^3 + 1)(x^4 + x + 1)$$

Burada, $2^d \equiv 1\ mod\ 15$ ifadesini sağlayan en küçük tamsayı $d = 4$ tür ve $\phi(15) = 8$ olduğundan $Q_{15}(x)$ polinomu dereceleri 4 olan $\phi(n)/d = 8/4 = 2$ tane monik indirgenemez polinomun çarpımı şeklinde yazılmıştır.

Teorem 2.64 $\mathbb{F}_q$ sonlu cismi her zaman herhangi bir alt cisminin $(q-1)$. cyclotomic cismidir [5].

Lemma 2.65 $f \in \mathbb{F}_q[x]$, derecesi $m \geq 1$ ve $f(0) \neq 0$ olan bir polinom olsun. O halde, $f(x) \mid x^e - 1$ olacak şekilde bir $e \leq q^m - 1$ sayısı vardır [5].

İspat $\mathbb{F}_q[x]/_{< f(x) >}$ bölüm halkası $I =< f(x) >$ olmak üzere $1 + I, x + I, x^2 + I, \dots, x^{q^m-1} + I$ şeklinde q^m tane sıfırdan farklı kalan sınıfı içerir. $\mathbb{F}_q[x]/_{< f(x) >}$ bölüm halkasında en fazla $q^m - 1$ tane sıfırdan farklı eleman olacağından $0 \leq i < j \leq q^m - 1$ ve $x^j \equiv x^i \, mod \, f(x)$ olacak şekilde i ve j tamsayıları vardır. x ve $f(x)$ aralarında asal olduğundan $x^{j-i} \equiv 1 \, mod \, f(x)$ olur. Buradan, $f(x) | \, x^{j-i} - 1$ ve $0 < j - i \leq q^m - 1$ dir.

Tanım 2.66 $0 \neq f \in \mathbb{F}_q[x]$ olsun. Eğer $f(0) \neq 0$ ise $f(x) \mid x^e - 1$ ifadesini sağlayan en küçük e tamsayısına $f(x)$ polinomunun *mertebesi* denir ve $ord(f) = ord(f(x))$ ile gösterilir. Eğer $f(0) = 0$ ise o zaman $h \in \mathbb{N}$, $g(0) \neq 0$ olmak üzere $f(x) = x^h g(x)$ şeklinde yazılabilir. Burada $ord(f) = ord(g)$ dir [5].

Teorem 2.67 $f \in \mathbb{F}_q[x]$, derecesi m ve $f(0) \neq 0$ olan indirgenemez bir polinom olsun. α elemanı f polinomunun bir kökü olmak üzere, f nin mertebesi α nın $\mathbb{F}_{q^m}^*$ daki mertebesine eşittir [5].

Sonuç 2.68 $f \in \mathbb{F}_q[x]$, derecesi m olan herhangi bir indirgenemez polinom olmak üzere

$$ord(f) \mid q^m - 1$$

dir [5].

Teorem 2.69 $\mathbb{F}_q$ üzerinde derecesi m ve mertebesi e olan monik indirgenemez polinomların sayısı;

(i) $e \geq 2$ ve $q^m \equiv 1 \, (mod \, n)$ ifadesini sağlayan en küçük tamsayı m ise $\phi(e)/_m$ tanedir.

(ii) $e = m = 1$ ise 2 tanedir.

(iii) diğer durumlarda 0 dır [5].

Lemma 2.70 $f \in \mathbb{F}_q[x]$ ve $f(0) \neq 0$ olsun. c bir pozitif tamsayı olmak üzere,

$$f(x) \mid x^c - 1 \Leftrightarrow ord(f) \mid c \text{ [5].}$$

İspat ($\Rightarrow$) $ord(f) = e$ ve $f(x) | x^c - 1$ olsun. O halde, $e \leq c$ olur.

$$e \leq c \Rightarrow c = eq + r, 0 \leq r < e \text{ ve } q \in \mathbb{N}$$

$$x^c - 1 = x^{eq}x^r - 1 + x^r - x^r$$

$$= x^r(x^{eq} - 1) + (x^r - 1)$$

$$\Rightarrow f(x) | x^r - 1$$

$$\Rightarrow r = 0$$

$$\Rightarrow e|c$$

($\Leftarrow$) $e \mid c$ olsun. O halde $c = et$ olacak şekilde bir $t \in \mathbb{Z}$ vardır. $ord(f) = e$ olduğundan $f(x) | x^e - 1$ dir. Buradan

$$f(x) | x^e - 1 \Rightarrow f(x) | x^{et} - 1 \Rightarrow f(x) | x^c - 1$$

olur.

Sonuç 2.71 e_1 ve e_2 pozitif tamsayılar ve $\gcd(e_1,\ e_2) = d$ olmak üzere

$$\gcd(x^{e_1} - 1, x^{e_2} - 1) = x^d - 1$$

dir [5].

Teorem 2.72 $g \in \mathbb{F}_q[x]$, $g(0) \neq 0$ ve $ord(g) = e$ olsun. $\mathbb{F}_q$ cisminin karakteristiği p olmak üzere $p^t \geq b$ ifadesini sağlayan en küçük tamsayı t ise $f(x) = g(x)^b$ polinomunun mertebesi ep^t dir [5].

İspat $ord(f) = ord(g^b) = c$ olsun. $c = ep^t$ olduğunu gösterelim.

$ord(f) = ord(g^b) = c \Rightarrow f | x^c - 1 \Rightarrow g^b \mid x^c - 1$

$\Rightarrow e \mid c$ (Lemma 2. 70)

Ayrıca $ord(g) = e$ olduğundan

$g \mid x^e - 1 \Rightarrow g^b \mid (x^e - 1)^b \Rightarrow g^b \mid (x^e - 1)^{p^t}$

$\Rightarrow g^b \mid x^{ep^t} - 1$

$\Rightarrow c \mid ep^t$ (Lemma 2.70)

$\Rightarrow c = ep^u, 0 \leq u \leq t$ (2.1)

Şimdi $u = t$ olduğunu gösterelim.

$$g^b \mid \left(x^{ep^u} - 1\right) \Rightarrow (x^e - 1)^{p^u} = g(x)^b h(x), \quad h(x) \in \mathbb{F}_q[x]$$

$$\Rightarrow p^u \geq b$$

$$\Rightarrow u \geq t \tag{2.2}$$

Buradan (2.1) ve (2.2) den $u = t$ dir ve $c = ep^t$ olur.

Teorem 2.73 $g_1, g_2, \dots, g_k \in \mathbb{F}_q[x]$ ikişer ikişer aralarında asal polinomlar olsun O zaman, $f = g_1 g_2 \dots g_k$ polinomunun mertebesi $ord(g_1), ord(g_2), \dots, ord(g_k)$ tamsayılarının en küçük ortak katına eşittir [5].

İspat $ord(f) = e$, $ord(g_i) = e_i$ ve $ekok(e_i) = c$ olsun. Şimdi $e = c$ olduğunu gösterelim.

$$\forall\, g_i \mid x^{e_i} - 1 \Rightarrow \forall\, g_i \mid x^c - 1$$

$$\Rightarrow g_1 g_2 \dots g_k \mid x^c - 1 \ (g_i \text{ ler aralarında asal idi})$$

$$\Rightarrow f \mid x^c - 1$$

$$\Rightarrow e \mid c \tag{2.3}$$

Ayrıca $ord(f) = e$ olduğundan $f \mid x^e - 1$ dir.

$$f \mid x^e - 1 \Rightarrow g_1 g_2 \dots g_k \mid x^e - 1$$

$$\Rightarrow \forall\, g_i \mid x^e - 1$$

$$\Rightarrow e_1 \mid e, e_2 \mid e, \dots, e_k \mid e$$

$$\Rightarrow ekok(e_i) \mid e$$

$$\Rightarrow c \mid e \tag{2.4}$$

(2.3) ve (2.4) ten $c = e$ dir yani $ord(f) = ekok(e_i)$ olur.

Örnek 2.74 $f = (x^2 + x + 1)^5 (x^3 + x + 1) \in \mathbb{F}_2[x]$ polinomunun mertebesini bulalım.

$x^2 + x + 1 \mid x^3 - 1$ ve $deg(x^3 - 1) = 3$ bu ifadeyi sağlayan en küçük tamsayı olduğundan $ord(x^2 + x + 1) = 3$ tür. Ayrıca, $2^3 \geq 5$ olduğundan Teorem 2.72 ye göre $ord(x^2 + x + 1) = 3.2^3 = 24$ tür.

Diğer taraftan, $x^3+x+1 \mid x^7-1$ ve $deg(x^7-1)=7$ bu ifadeyi sağlayan en küçük tamsayı olduğundan $ord(x^3+x+1)=7$ dir.

O halde Teorem 2.73 e göre $ord(f)=ekok(24,7)=168$ dir.

Tanım 2.75 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0 \in \mathbb{F}_q[x]$ ve $a_n \neq 0$ olsun. $f(x)$ polinomunun *reciprocalı* $f^*(x)$ ile gösterilir ve

$$f^*(x)=x^nf\left(\frac{1}{x}\right)=a_0x^n+a_1x^1+\cdots+a_{n-1}x+a_n$$

şeklinde tanımlanır. Özel olarak, $f^*(x)=f(x)$ ise $f(x)$ polinomuna *self-reciprocal* polinom denir [5].

Örnek 2.76 $f(x)=3x^4+x^3+2x^2+x+1 \in \mathbb{F}_5[x]$ polinomunun reciprocalı

$$f^*(x)=x^4f\left(\frac{1}{x}\right)=x^4\left(3\left(\frac{1}{x}\right)^4+\left(\frac{1}{x}\right)^3+2\left(\frac{1}{x}\right)^2+\left(\frac{1}{x}\right)+1\right)$$

$$=x^4+x^3+2x^2+x+3$$

dir.

Teorem 2.77 $0 \neq f \in \mathbb{F}_q[x]$ ve f^*, f polinomunun reciprocalı olmak üzere

$$ord(f)=ord(f^*)$$

dır [5].

İspat $f(0) \neq 0$ ve $degf=n$ olmak üzere $ord(f)=e$ olsun. O zaman

$$f \mid x^e-1 \Rightarrow x^e-1=f(x)g(x)$$

$$\Rightarrow x^e/\left(\frac{1}{x}\right)^e-1=f\left(\frac{1}{x}\right)g\left(\frac{1}{x}\right)$$

$$\Rightarrow 1-x^e=x^nf\left(\frac{1}{x}\right)x^{e-n}g\left(\frac{1}{x}\right)$$

$$\Rightarrow f^*(x) \mid x^e-1 \qquad (2.5)$$

Diğer taraftan,

$$f^*(x) \mid x^e-1 \Rightarrow (f^*(x))^* \mid x^e-1$$

$$\Rightarrow f(x) \mid x^e-1 \qquad (2.6)$$

(2.5) ve (2.6) dan f ve f^* ın mertebeleri eşittir.

Eğer $f(0) = 0$ ise $g(0) \neq 0$ olacak şekilde $f(x) = x^t g(x)$ yazılabiliyordu. Burada f nin mertebesi g nin mertebesine eşit idi. Buradan $ord(f) = ord(g) = ord(g^*) = ord(f^*)$ olur.

Teorem 2.78 $f \in \mathbb{F}_q[x]$, $f(0) \neq 0$ ve q bir tek tamsayı olsun. $ord\big(f(x)\big) = e$ ve $ord\big(f(-x)\big) = E$ olmak üzere;

(i) $4 \mid e \Rightarrow E = e$.

(ii) $e = 2k$, k tem tamsayı ve f nin her indirgenemez çarpanının mertebesi çift ise $E = {}^{e}/_{2} = k$ dır.

(iii) $e = 2k$, k tem tamsayı ve f nin her indirgenemez çarpanının mertebesi tek ise $E = e$ dir.

(iv) e tek tamsayı $\Rightarrow E = 2e$ [5].

Tanım 2.79 $f \in \mathbb{F}_q[x]$, derecesi m olan bir polinom olsun. $\alpha \in \mathbb{F}_q^*$ bir ilkel eleman olmak üzere f, α nın minimal polinomu ise f ye *ilkel polinom* denir [5].

Teorem 2.80 $f \in \mathbb{F}_q[x]$, derecesi m olan bir polinom olsun. f nin ilkel olması için gerek ve yeter koşul f nin monik, $f(0) \neq 0$ ve de $ord(f) = q^m - 1$ olmasıdır [5].

Lemma 2.81 $f \in \mathbb{F}_q[x]$, $f(0) \neq 0$ olmak üzere pozitif dereceli bir polinom olsun. $x^r \equiv a \, mod \, f(x)$, $a \in \mathbb{F}_q^*$ ifadesini sağlayan en küçük pozitif tamsayı r olmak üzere $ord(f) = hr$ dir. Burada h, a nın $\mathbb{F}_q^*$ üzerindeki mertebesidir [5].

İspat $ord(f) = e$ olsun. $x^r \equiv a \, mod \, f(x)$ olduğundan $e \geq r$ dir. Buradan,

$e = sr + t$, $s \in \mathbb{N}$ ve $0 \leq t \leq r$ yazabiliriz. Böylece

$$1 \equiv x^e \equiv x^{sr+t} \equiv a^s x^t \, mod \, f(x)$$

olur. Buradan $x^t \equiv a^{-s} \, mod \, f(x)$ dir ve r nin tanımından bu ifade yalnızca $t = 0$ iken sağlanır. O halde $a^s \equiv 1 \, mod \, f(x)$ olur ve $a^s = 1$ yani $s \geq h$ ve $e \geq hr$ dir. Diğer taraftan, $x^{hr} \equiv a^h \equiv 1 \, mod \, f(x)$ ve de $e = hr$ olur.

Teorem 2.82 $f \in \mathbb{F}_q[x]$, derecesi m olan bir monik polinom olsun. f nin ilkel olması için gerek ve yeter koşul $(-1)^m f(0)$ elemanının $\mathbb{F}_q$ da ilkel ve $x^r \equiv a \, mod \, f(x)$, $a \in$

$\mathbb{F}_q$ ifadesini sağlayan en küçük tamsayı r olmak üzere $r = {q^m - 1}/{q - 1}$ olmasıdır. Ayrıca, f ilkel ise $x^r \equiv (-1)^m f(0)\ mod\ f(x)$ dir [5].

Teorem 2.83 $\mathbb{F}_q$ sonlu bir cisim ve $n \in \mathbb{N}$ olsun. $\mathbb{F}_q$ üzerindeki derecesi n yi bölen tüm monik indirgenemez polinomların çarpımı $x^{q^n} - x$ dir [5].

İspat Lemma 2.39 a göre $\mathbb{F}_q$ üzerinde derecesi n yi bölen her indirgenemez polinom $x^{q^n} - x$ polinomunu böler. Ayrıca $x^{q^n} - x$ polinomunun türevi -1 olduğundan katlı kökü yoktur. Bu durumda derecesi n yi bölen tüm monik indirgenemez polinomların çarpımı $x^{q^n} - x$ dir.

Sonuç 2.84 $N_q(d)$, $\mathbb{F}_q$ üzerinde derecesi d olan tüm monik indirgenemez polinomların sayısı olmak üzere,

$$q^n = \sum_{d|n} dN_q(d), \quad \forall\, n \in \mathbb{N}$$

[5].

Tanım 2.85 μ Moebius Fonksiyonu

$$\mu(n) = \begin{cases} 1, & n = 1 \\ (-1)^k, & n = p_1 p_2 \dots p_k\ (p_i\ ler\ farklı\ asallardır) \\ 0, & n\ kare\ çarpan\ içerir \end{cases}$$

ile tanımlanır [1].

Lemma 2.86 $n \in \mathbb{N}$ için μ Moebius Fonksiyonu,

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1 \\ 0, & n > 1 \end{cases}$$

[1].

Teorem 2.87 (Moebius Terslik Formülü)

- Toplamsal Versiyon: G toplamsal değişmeli bir grup olmak üzere H ve h, $\mathbb{N} \longmapsto G$ iki fonksiyon olsun. O zaman

$$H(n) = \sum_{d|n} h(d), \qquad \forall\, n \in \mathbb{N}$$

$$\Leftrightarrow h(n) = \sum_{d|n} \mu\left({}^{n}/_{d}\right) H(d) = \sum_{d|n} \mu(d) H\left({}^{n}/_{d}\right), \quad \forall\, n \in \mathbb{N}$$

- Çarpımsal Versiyon: G çarpımsal değişmeli bir grup olmak üzere H ve h, $\mathbb{N} \longmapsto$G iki fonksiyon olsun. O zaman

$$H(n) = \prod_{d|n} h(d), \qquad \forall\, n \in \mathbb{N}$$

$$\Leftrightarrow h(n) = \prod_{d|n} H(d)^{\mu({}^{n}/_{d})} = \prod_{d|n} H({}^{n}/_{d})^{\mu(d)}, \quad \forall\, n \in \mathbb{N}$$

[5].

Teorem 2.88 $N_q(n)$, $\mathbb{F}_q$ üzerinde derecesi n olan tüm monik indirgenemez polinomların sayısı olmak üzere,

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu\left({}^{n}/_{d}\right) q^{d} = \frac{1}{n} \sum_{d|n} \mu(d)\, q^{{}^{n}/_{d}}$$

[5].

Teorem 2.89 K, karakteristiği p olan bir cisim ve $n \nmid p$ olmak üzere K üzerindeki n. dereceden cyclotomic polinom;

$$Q_n(x) = \prod_{d|n} (x^{d} - 1)^{\mu({}^{n}/_{d})} = \prod_{d|n} (x^{{}^{n}/_{d}} - 1)^{\mu(d)}$$

[5].

Örnek 2.90 K üzerinde tanımlı 12. dereceden cyclotomic polinom $Q_{12}(x)$ olmak üzere,

$$Q_{12}(x) = \prod_{d|12} (x^{{}^{12}/_{d}} - 1)^{\mu(12)}$$

$$\Rightarrow (x^{12} - 1)^{\mu(1)} (x^{6} - 1)^{\mu(2)} (x^{4} - 1)^{\mu(3)} (x^{3} - 1)^{\mu(4)} (x^{2} - 1)^{\mu(6)} (x^{1} - 1)^{\mu(12)}$$

$$\Rightarrow \frac{(x^{12} - 1)(x^{2} - 1)}{(x^{6} - 1)(x^{4} - 1)} = x^{4} - x^{2} + 1$$

Teorem 2.91 $\mathbb{F}_q$ üzerinde derecesi n olan tüm monik indirgenemez polinomların çarpımı

$$I(q,n,x)=\prod_{d|n}(x^{q^d}-x)^{\mu(n/d)}=\prod_{d|n}(x^{q^{n/d}}-x)^{\mu(d)}$$

şeklindedir [5].

Örnek 2.92 $\mathbb{F}_3$ üzerinde derecesi 3 olan monik indirgenemez polinomların çarpımı:

$$I(3,3,x)=\prod_{d|3}(x^{3^d}-x)^{\mu(3/d)}$$

$$\Rightarrow (x^{3^3}-x)^{\mu(1)}(x^3-x)^{\mu(3)}$$

$$\Rightarrow \frac{x^{27}-x}{x^3-x}$$

Teorem 2.93 $I(q,n,x)$, $\mathbb{F}_q[x]$ te derecesi n olan monik, indirgenemez polinomların çarpımı olsun. $q^n \equiv 1\ mod\ m$ ifadesini sağlayan q^n-1 in tüm m pozitif bölenleri için $Q_m(x)$, m. cyclotomic polinom olmak üzere

$$I(q,n;x)=\prod_{m} Q_m(x)$$

dir [5].

İspat $n>1$ için $S=\{\alpha|\ \alpha^n=1, \alpha\in\mathbb{F}_q\}$ olsun. Buradan $\alpha\in S$, $\mathbb{F}_q$ üzerinde derecesi n olan bir minimal polinoma sahiptir. Böylece α, $I(q,n;x)$ nin bir köküdür. Diğer taraftan eğer β, $I(q,n;x)$ nin bir kökü ise o zaman β, $\mathbb{F}_q$ üzerinde derecesi n olan indirgenemez bir polinomun köküdür. O halde $\beta\in S$ olur. Buradan

$$I(q,n;x)=\prod_{\alpha\in S}(x-\alpha).$$

Eğer $\alpha\in S$ ise $\alpha\in\mathbb{F}_{q^n}^*$ dir. O halde α nın mertebesi q^n-1 i böler. Buradan $ord(\alpha)=m$, en küçük n tamsayısı için $q^n\equiv 1\ mod\ m$ ifadesini sağlayan değerdir. $m\mid q^n-1$ için $S_m=\{\alpha|\ \alpha^m=1, \alpha\in\mathbb{F}_q\}$ olsun. O halde S kümesi ayrık S_m kümelerinin birleşimidir. Buradan

$$I(q,n;x)=\prod_{m}\prod_{\alpha\in S_m}(x-\alpha)$$

yazabiliriz. O halde S_m kümesi $\mathbb{F}_{q^n}^*$ de mertebesi m olan tüm elemanları içerir. Diğer bir ifadeyle S_m, $\mathbb{F}_q$ üzerinde m. dereceden birimin ilkel köklerinin kümesidir. Cyclotomic polinomun tanımından

$$\prod_{\alpha \in S_m} (x - \alpha) = Q_m(x)$$

olur ve buradan

$$I(q, n; x) = \prod_m Q_m(x).$$

Teorem 2.94 F_q bir cisim olsun. $f, h \in F_q[x]$ ve $h^q = h \bmod f$ olmak üzere $f(x) = \prod_{c \in F_q}(f(x), h(x) - c)$ dir [5].

İspat $(f(x), h(x) - c) \mid f(x)$ dir.

$h(x) \in F_q[x]$ ve her $c \in F_q$ için $h(x) - c$ aralarında asal polinomlardır. O halde $f(x)$ polinomu ile $h(x) - c$ polinomları da aralarında asaldır. Buradan her bir $c \in F_q$ için $(f(x), h(x) - c) \mid f(x)$ olduğundan

$$\prod_{c \in F_q} (f(x), h(x) - c) \mid f(x)$$

olur.

Diğer taraftan $h^q = h \bmod f$ olduğundan $f \mid h^q - h$ dir. Ayrıca $h^q(x) - h = \prod_{c \in F_q}(h(x) - c)$ olduğundan

$$f(x) \mid \prod_{c \in F_q} (f(x), h(x) - c)$$

Böylece, $f(x) = \prod_{c \in F_q}(f(x), h(x) - c)$ olur.

$(f(x), h(x) - c)$ bazen indirgenebilir çıkabileceğinden bu Teorem genel olarak f'nin tam olarak çarpanlara ayrılışını vermez.

Tanım 2.95 Teorem 2.94'te tanımlanan h, f'nin aşikar olmayan bir çarpanlara ayrılışını veriyorsa h ye bir *f-reducing* polinom denir [5].

$h^q = h \bmod f$, $degh < degf$ olmak üzere h, *f-reducing* polinomdur. Bu polinomları bulmak için aşağıda açıklayacağımız Berlekamp'ın Algoritmasını kullanacağız.

f'nin tekrar eden çarpanı olmasın, yani $(f(x), f'(x)) = 1$ olsun. $f = f_1 f_2 \dots f_k$ olmak üzere

$(c_1, c_2, \dots, c_k) \in F_q$ ise $h(x) = c_i mod f_i(x)$, $1 \le i \le k$, $degh < degf$ olacak şekilde tek bir h vardır.

Buradaki h için;

$$h(x)^q \equiv {c_i}^q \equiv c_i \equiv h(x) mod f_i(x), \ \ 1 \le i \le k$$

ve buradan

$$h(x)^q \equiv h(x) mod f(x), \ degh < degf \qquad (2.7)$$

Şimdi $degf = n$ olmak üzere nxn lik $B = \left(b_{ij}\right)$, $0 \le i \le n-1$ matrisi $x^{iq} mod f(x)$ polinomları hesaplanarak oluşturulur.

$$x^{iq} = \sum_{j=0}^{n-1} b_{ij} x^j mod f(x), \quad 0 \le i \le n-1$$

O zaman,

$h(x) = a_0 + a_1 x + \dots + a_{n-1} x^{n-1}$ (2.7)'nin bir çözümüdür.

$\Leftrightarrow (a_0, a_1, \dots, a_{n-1})\mathrm{B} = (a_0, a_1, \dots, a_{n-1})$

$\Leftrightarrow h(x) = \sum_{j=0}^{n-1} a_j x^j = \sum_{j=0}^{n-1} \sum_{i=0}^{n-1} a_i b_{ij} x^j = \sum_{i=0}^{n-1} a_i x^{iq} = h^q mod f(x)$.

Buradan,

$$(a_0, a_1, \dots, a_{n-1})(\mathrm{B} - \mathrm{I}) = 0$$

olur. Bu sistemin tam olarak q^k tane çözümü vardır. Buradan $(B - I)$ matrisinin sıfır uzayının boyutu olan k, f'nin farklı, monik, indirgenemez çarpanlarının sayısıdır ve $rank(B - I) = n - k$ dir.

$h_1(x) = 1$ için ${h_1}^q \equiv h \, mod f$ olduğundan $h_1 = 1$, (2.7)'nin aşikar çözümüdür. Ayrıca $degh_i \le n - 1$ olacak şekilde $h_2(x), h_3(x), \dots, h_k(x)$ *f-reducing* polinomları vardır ve bunlar $\mathrm{B} - \mathrm{I}$ matrisinin sıfır uzayının taban vektörlerine karşılık gelen polinomlardır.

$rank(B - I) = r$ olmak üzere $k = n - r$ idi.

$k = 1$ ise f indirgenemezdir.

$k \geq 2$ ise $h_2(x)$ *f-reducing* polinomu seçilir ve her $c \in F_q$ için $(f(x), h_2(x) - c)$ hesaplanır. Böylece,

$$f = \prod_{c \in F_q} (f(x), h_2(x) - c)$$

olur.

Eğer bu işlem sonunda k tane çarpan oluşmazsa her $c \in F_q$ için $(f(x), h_3(x) - c)$ hesaplanır. Bu işlem k tane çarpana ulaşılana kadar devam ettirilir. Sonlu cisimler üzerindeki polinomların indirgenemezliğini belirleme ve çarpanlarının bulunmasında kullanılan bu yönteme *Berlekamp Yöntemi* adı verilir.

Örnek 2.96 $f(x) = x^8 + x^6 + x^4 + x^3 + 1$ polinomunu F_2 üzerinde çarpanlarına ayıralım.

$f'(x) = 8x^7 + 6x^5 + 4x^3 + 3x^2 = 1$ olduğundan $(f(x), f'(x)) = 1$ dir. Buradan f'nin tekrar eden bir çarpanı yoktur.

Şimdi $x^{2i} mod f(x),\ 0 \leq i \leq n - 1 = 7$ polinomlarını bulalım.

$x^0 \equiv 1$

$x^2 \equiv x^2$

$x^4 \equiv x^4$

$x^6 \equiv x^6$

$x^8 \equiv 1 + x^3 + x^4 + x^6$

$x^{10} \equiv 1 + x^2 + x^3 + x^4 + x^5$

$x^{12} \equiv x^2 + x^4 + x^5 + x^6 + x^7$

$x^{14} \equiv 1 + x + x^3 + x^4 + x^5$

Şimdi $8x8$ lik B matrisini oluşturalım.

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix} \qquad B - I = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

$B - I$ matrisinin rankı 6'dır. Buradan

$k = n - r = 8 - 6 = 2$ olduğundan f, iki tane monik, indirgenemez polinomun çarpımı şeklinde yazılabilir.

$B - I$ matrisini eşelon forma getirmek için sütun işlemleri uygulandığında

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$ matrisi elde edilir.

Buradan;

$$[x_1 \ x_2 \ x_3 \ x_4 \ x_5 \ x_6 \ x_7 \ x_8] \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix} = 0$$

elde edilir.

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix} = x_1 \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + x_8 \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

Böylece $[1\ 0\ 0\ 0\ 0\ 0\ 0\ 0]$, $[0\ 1\ 1\ 0\ 0\ 1\ 1\ 1]$ vektörleri $B - I$'nın sıfır uzayının tabanı formundadır. Buradan, $h_1(x)$ ve $h_2(x)$ polinomları;

$h_1(x) = 1$ ve $h_2(x) = x + x^2 + x^5 + x^6 + x^7$ dir.

$(f(x), h_2(x) - 0) = x^6 + x^5 + x^4 + x + 1$

$(f(x), h_2(x) - 1) = x^2 + x + 1$

Buradan,

$$f(x) = (x^6 + x^5 + x^4 + x + 1)(x^2 + x + 1\,).$$

Örnek 2.97 Berlekamp Algoritmasını kullanarak $f(x) = x^6 - x^3 - x - 1 \in \mathbb{F}_3[x]$ polinomunun indirgenemez olduğunu gösterelim.

$f'(x) = 6x^5 - 3x^2 - 1 = 2$ olduğundan $\gcd(f(x), f'(x)) = 2$ dir. Buradan,

$f(x) = 2.(2x^6 + x^3 + x + 1)$ dir.

Şimdi $x^{3i} mod f(x),\ 0 \le i \le n - 1 = 5$ polinomlarını bulalım.

$x^0 \equiv 1$

$x^3 \equiv x^3$

$x^6 \equiv 1 + x + x^3$

$x^9 \equiv 1 + x + 2x^3 + x^4$

$x^{12} \equiv 2 + x^2 + 2x^4$

$x^{15} \equiv 2x + 2x^2 + 2x^3 + 2x^4 + x^5$

Şimdi $6x6$ lik B matrisini oluşturalım.

$$\mathrm{B} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 2 & 1 & 0 \\ 2 & 0 & 1 & 0 & 2 & 0 \\ 0 & 2 & 2 & 2 & 2 & 1 \end{bmatrix} \qquad \mathrm{B} - \mathrm{I} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 2 & 0 & 1 & 0 & 1 & 0 \\ 0 & 2 & 2 & 2 & 2 & 0 \end{bmatrix}$$

$\mathrm{B} - \mathrm{I}$ matrisinin rankı 5 dir. Buradan

$k = n - r = 6 - 5 = 1$ olduğundan $2x^6 + x^3 + x + 1$ indirgenemez bir polinomdur.

Böylece, $f(x) = 2.(\,2x^6 + x^3 + x + 1)$ polinomu da $\mathbb{F}_3$ üzerinde indirgenemez bir polinomdur.

BÖLÜM 3

TRİNOMİALLERİN DİSKRİMİNANTI İLE İNDİRGENEMEZLİK

Tanım 3.1 K bir cisim, $f \in K[x]$ derecesi $n \geq 2$ olan bir polinom ve $\alpha_1, \alpha_2, \ldots, \alpha_n$ ler f polinomunun K üzerindeki parçalanış cisminin elemanları olmak üzere

$$f(x) = a_0(x - \alpha_1) \ldots (x - \alpha_n)$$

olsun. O zaman, f polinomunun diskriminantı $D(f)$ olmak üzere;

$$D(f) = {a_0}^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$$

dir.

Örneğin $n = 2$ ve $f(x) = ax^2 + bx + c$ ise;

$$D(f) = a^2(\alpha_1 - \alpha_2)^2 = a^2((\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2) = a^2(b^2a^{-2} - 4ca^{-1})$$

Buradan,

$$D(f) = b^2 - 4ac$$

olur [5].

Teorem 3.2 $m, n \in \mathbb{N}$ olmak üzere $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in K[x]$ ve $g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_m \in K[x]$ iki polinom olsun. Bu iki polinomun *resultantı* şu şekilde tanımlanır:

$$R(f,g)=\begin{vmatrix} a_0 & a_1 & \dots & a_n & 0 & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_n & 0 & \dots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \dots & 0 & a_0 & a_1 & \dots & \dots & a_n \\ b_0 & b_1 & \dots & \dots & b_m & 0 & \dots & 0 \\ 0 & b_0 & b_1 & \dots & \dots & b_m & \dots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \dots & 0 & b_0 & b_1 & \dots & \dots & b_m \end{vmatrix}$$

Eğer $\deg(f)=n$ $(a_0 \neq 0)$ ve $f(x)=a_0(x-\alpha_1)\dots(x-\alpha_n)$ ise o zaman;

$$R(f,g)={a_0}^m\prod_{i=1}^{n} g(\alpha_i).$$

O halde $R(f,g)=0$ olması için gerek ve yeter koşul f ve g polinomlarının ortak köke sahip olmasıdır.

Şimdi $D(f)$ ile $R(f,g)$ arasında bağlantı kurabiliriz. $f \in K[x]$, $\deg(f)=n\geq 2$ ve başkatsayı a_0 olsun. O halde,

$$D(f)=(-1)^{n(n-1)/2}.{a_0}^{-1}.R(f,f')$$

Burada f', f polinomunun türevidir [5].

Teorem 3.3 $F[x]=\prod_1^n(x-\alpha_i)$, $\mathbb{Z}[x]$ te monik polinom olsun. O zaman;

$$D(f)=\prod_{1\leq i<j\leq n}(\alpha_i-\alpha_j)^2=(-1)^{n(n-1)/2}.{a_0}^{-1}.R(f,f')$$
$$=(-1)^{n(n-1)/2}\prod_{1\leq i<j\leq n}F'(\alpha_i)$$

dir [5].

Lemma 3.4

(i) $R(g,f)=(-1)^{\deg f.\deg g}R(f,g)$

(ii) g polinomunun başkatsayısı b olmak üzere,

$f=gq+r$ ise $R(f,g)=b^{\deg f-\deg r}R(r,g)$ dir.

(iii) a ve b sıfırdan farklı sabitler olmak üzere, $R(a,b)=1$ dir.

(iv) $R(f_1f_2,g)=R(f_1,g)R(f_2,g)$ [1].

İspat

(ii) $f = gq + r$ ve $degg = m$ olmak üzere,

$$R(gq + r, g) = b^{degf} \prod_{j=1}^{m} (gq + r)(\beta_j)$$

$$= b^{degf} \prod_{j=1}^{m} gq(\beta_j) + r(\beta_j)$$

$$= b^{degf} \prod_{j=1}^{m} r(\beta_j) = b^{degf} \frac{R(r, g)}{b^{degr}}$$

$$= b^{\deg f - \deg r} R(r, g)$$

(iii) a ve b sıfırdan farklı sabitler olmak üzere,

$R(a, b) = b^0 = 1$ dir.

(iv) $degg = m$ olmak üzere,

$$R(f_1 f_2, g) = b^{degf_1 f_2} \prod_{j=1}^{m} f_1 f_2(\beta_j)$$

$$= b^{degf_1 + \deg f_2} \prod_{j=1}^{m} f_1(\beta_j) \prod_{j=1}^{m} f_2(\beta_j)$$

$$= b^{degf_1} \prod_{j=1}^{m} f_1(\beta_j)\, b^{degf_2} \prod_{j=1}^{m} f_2(\beta_j)$$

$$= R(f_1, g) R(f_2, g)$$

Sonuç 3.5

(i) $R(f, g_1 g_2) = R(f, g_1) R(f, g_2)$

(ii) a sabit ise $R(f, a) = a^{degf} = R(a, f)$

(iii) $R(f, x^m) = R(f, x)^m = f(0)^m$ [1].

İspat

(i) $R(f, g_1 g_2) = (-1)^{\deg f . degg_1 g_2} R(g_1 g_2, f)$

$$= (-1)^{\deg f(deg g_1 + deg\ g_2)} R(g_1, f) R(g_2, f)$$

$$= (-1)^{\deg f . \deg g_1} R(g_1, f)(-1)^{\deg f . \deg g_2} R(g_2, f)$$

$$= R(f, g_1) R(f, g_2)$$

(ii) a sabit olmak üzere,

$$R(f, a) = a^{degf} = (-1)^{\deg f \overbrace{\deg a}^{0}} R(a, f) = R(a, f)$$

(iii) $R(f, x^m) = R\left(f, \underbrace{x . x \dots x}_{m\ tane}\right) = R(f, x) \dots R(f, x) = R(f, x)^m$

$$= (1^{degf} \prod_{j=1} f(0))^m = f(0)^m$$

Lemma 3.6 $d = \gcd(r, s)$ olsun ve $r = dr_1$ ve $s = ds_1$ alalım. O halde,

$$R(x^r - \alpha, x^s - \beta) = (-1)^s [\alpha^{s_1} - \beta^{r_1}]^d$$

dir [1].

Tanım 3.7 (Trinomialler İçin Diskriminant) $n > k \geq 1 \in \mathbb{Z}$ ve $q = p^t, t \in \mathbb{Z}$ ve de $a, b \in \mathbb{F}_q^*$ olmak üzere $f(x) = x^n + ax^k + b \in \mathbb{F}_q[x]$ polinomunun diskriminantı

$$D = (-1)^{n.(n-1)/2} b^{k-1} (n^{n_1} b^{n_1 - k_1} - (-1)^{n_1} (n-k)^{n_1 - k_1} k^{k_1} a^{n_1})^d$$

dir. Burada $d = \gcd(n, k)$, $n_1 = {}^{n}/_{d}$ ve $k_1 = {}^{k}/_{d}$ dir [1].

İspat

$$D(f) = (-1)^{n(n-1)/2} . R(f, f')$$

olduğunu biliyoruz. O halde,

$$D(x^n + ax^k + b) = (-1)^{n(n-1)/2} R(nx^{n-1} + kax^{k-1}, x^n + ax^k + b)$$

$$= (-1)^{n(n-1)/2} R(nx^{k-1}(x^{n-k} + n^{-1}ka), x^n + ax^k + b)$$

$$= (-1)^{n(n-1)/2} R(nx^{k-1}, x^n + ax^k + b) R(x^{n-k} + n^{-1}ka, x^n + ax^k + b)$$

$$= (-1)^{n(n-1)/2} R(n, x^n + ax^k + b) R(x^{k-1}, x^n + ax^k + b) R(x^{n-k} + n^{-1}ka, x^n + ax^k + b)$$

$= (-1)^{n(n-1)/2}\, n^n (-1)^{n(k-1)} R(\, x^n + ax^k + b, x^{k-1})(-1)^{n(k-1)} R(\, x^n + ax^k + b, x^{n-k} + n^{-1}ka)$

$= (-1)^{n(n-1)/2}\, n^n b^{k-1} R(x^n + ax^k + b, x^{n-k} + n^{-1}ka)\ (-1)^{n^2-n}$

$= (-1)^{n(n-1)/2}\, n^n b^{k-1} R(x^n + ax^k + b, x^{n-k} + n^{-1}ka)$

Lemma 3.4 (ii) ye göre

$= (-1)^{n(n-1)/2}\, n^n b^{k-1} R(a(1 - n^{-1}k)x^k + b, x^{n-k} + n^{-1}ka)$

$= (-1)^{n(n-1)/2}\, n^n b^{k-1} R\left(a(1 - n^{-1}k)\left(x^k + \frac{b}{a(1-n^{-1}k)}\right), x^{n-k} + n^{-1}ka\right)$

$= (-1)^{n(n-1)/2}\, n^n b^{k-1} R(a(1 - n^{-1}k), x^{n-k} + n^{-1}ka)\ R\left(\left(x^k + \frac{b}{a(1-n^{-1}k)}\right), x^{n-k} + n^{-1}ka\right)$

$= (-1)^{n(n-1)/2}\, n^n b^{k-1}\left(a(1 - n^{-1}k)\right)^{n-k} R\left(\left(x^k - \left(-\frac{b}{a(1-n^{-1}k)}\right)\right), x^{n-k} - (-n^{-1}ka)\right)$

Lemma 3.6 ya göre

$= (-1)^{n(n-1)/2}\, n^n b^{k-1} a^{n-k}(1 - n^{-1}k)^{n-k}(-1)^{n-k}\left[\left(-\frac{b}{a(1-n^{-1}k)}\right)^{n_1-k_1} - (-n^{-1}ka)^{k_1}\right]^d$

$= (-1)^{n(n-1)/2}\, b^{k-1}\left[(n^{n_1} a^{n_1-k_1}(1 - n^{-1}k)^{n_1-k_1}(-1)^{n_1-k_1})\left(\left(-\frac{b}{a(1-n^{-1}k)}\right)^{n_1-k_1} - (-n^{-1}ka)^{k_1}\right)\right]^d$

$= (-1)^{n(n-1)/2}\, b^{k-1}\left[n^{n_1} b^{n_1-k_1} + (-1)^{n_1-k_1+1+k_1} a^{n_1-k_1+k_1}\left(\frac{n-k}{n}\right)^{n_1-k_1} n^{n_1-k_1} k^{k_1}\right]^d$

$= (-1)^{n(n-1)/2}\, b^{k-1}[n^{n_1} b^{n_1-k_1} + (-1)^{n_1+1} a^{n_1}(n-k)^{n_1-k_1} k^{k_1}]^{\,d}$

$= (-1)^{n(n-1)/2}\, b^{k-1}[n^{n_1} b^{n_1-k_1} + (-1)^{n_1+1}(n-k)^{n_1-k_1} a^{n_1} k^{k_1}]^d$

Teorem 3.8 (Stickelberker, 1897) q asal olmak üzere, $f \in F_q[x]$ bir tam kare bölensiz polinom ve r, f nin birbirinden farklı indirgenemez çarpan sayısı olsun. $f = F(mod\ q)$ olmak üzere;

$(\deg(f) - r)$ nin çift olması için gerek ve yeter koşul $D(f)$ nin $(mod\ 4q)$ da bir tam kare olmasıdır [6].

Teorem 3.9 r, $F(mod\ 2)$ nin indirgenemez çarpan sayısı olsun.

- $D(f) \not\equiv 1{,}5\ (mod\ 8)$ olması için gerek ve yeter koşul $F(mod\ 2)$ nin katlı köke sahip olmasıdır.
- $D(f) \equiv 1(mod\ 8)$ ise $r \equiv n\ (mod\ 2)$ dir.
- $D(f) \equiv 5(mod\ 8)$ ise $r \not\equiv n\ (mod\ 2)$ dir [6].

Teorem 3.10 (Swan Teoremi) $f(x) = x^n + x^k + 1$ polinomu $\mathbb{F}_2$ üzerinde derecesi n olan bir tam kare bölensiz trinomial ve r de $f(x)$ in indirgenemez çarpanlarının sayısı olsun. O zaman,

(i) Eğer $n \equiv 0\ mod\ 8$ ise $r \equiv 0\ mod\ 2$ dir.

(ii) Eğer $n \equiv 4\ mod\ 8$ ise $r \equiv 1\ mod\ 2$ dir.

(iii) Eğer $n \equiv \pm 1\ mod\ 8$ ve k çift iken r nin çift olması için gerek ve yeter koşul $k \mid 2n$ olmasıdır.

(iv) Eğer $n \equiv \pm 3\ mod\ 8$ ve k çift iken r nin tek olması için gerek ve yeter koşul $k \mid 2n$ olmasıdır.

(v) Eğer $n \equiv \pm 2\ mod\ 8$ ve k tek iken r nin çift olması için gerek ve yeter koşul $n \neq 2k$ ve $^{nk}/_2 \equiv 1\ mod\ 4$ olmasıdır.

Burada n ve k nın her ikisi de çift ise o zaman $f(x)$ bir tam kare polinomdur [1].

Swan, daha sonra trinomialler üzerinde diskriminant hesaplamaları yaparak teoremini aşağıdaki şekle indirgemeyi başarmıştır.

Teorem 3.11 $f(x) = x^n + x^k + 1 \in \mathbb{F}_2[x]$ polinomu aşağıdaki koşullardan herhangi birini sağlıyor ise f nin indirgenemez çarpanlarının sayısı çifttir.

(i) n çift, k tek, $n \neq 2k$ ve $^{nk}/_2 \equiv 0\ mod\ 4$ ya da $^{nk}/_2 \equiv 1\ mod\ 4$ dir.

(ii) n tek, k çift, $k \nmid 2n$ ve $n \equiv \pm 3 \; mod \; 8$ dir.

(iii) n tek, k çift, $k \mid 2n$ ve $n \equiv \pm 1 \; mod \; 8$ dir

[7].

Steven Hayman [8] da Swan'ın bu teoremi ile $x^n + x^k + 1$ şeklindeki tüm trinomiallerin $5/8$ inin çift sayıda indirgenemez çarpana sahip olduğunu belirtmiştir. Bu durumda indirgenemezlik testi için sadece $3/8$ lük kısma bakmamız yeterli olacaktır.

Teorem 3.12 p asal olmak üzere $p \equiv 19 \; mod \; 24$ ya da $p \equiv 13 \; mod \; 24$ olsun. O zaman, $\mathbb{F}_2$ üzerinde derecesi p olan hiçbir indirgenemez trinomial yoktur [7].

Teorem 3.13 $n > 3$ olmak üzere $n \equiv 45 \; mod \; 56$ ya da $n \equiv 3 \; mod \; 56$ olsun. O zaman, $\mathbb{F}_2$ üzerinde derecesi n olan $f(x) = x^n + x^2 + 1$ şeklinde hiçbir indirgenemez trinomial yoktur.

İspat $f(x) = x^n + x^k + 1 \in \mathbb{F}_2[x]$ olmak üzere n tek, k çift, $n \equiv \pm 3 \; mod \; 8$ ve de $k \mid 2n$ alalım. Swan Teoreminin (iv) koşuluna göre f nin çift sayıda indirgenemez çarpanı yoktur. $k \mid 2n$, n tek, k çift olduğundan $k = 2$ aldığımızda aşağıdaki ifadeyi elde ederiz:

$x^3 + x^2 + 1$, $\mathbb{F}_2$ üzerinde indirgenemez bir polinom olmak üzere,

Eğer $n \equiv 3 \; mod \; 7$ ise $x^3 + x^2 + 1 \mid x^n + x^2 + 1$ olduğunu gösterelim.

$ord(x^3 + x^2 + 1) = 7$ olduğundan α, $x^3 + x^2 + 1$ polinomunun kökü olmak üzere $\alpha^7 = 1$ dir. Buradan $n = 7k + 3$ olmak üzere,

$$\alpha^{7k+3} + \alpha^2 + 1 = \alpha^{7k}\alpha^3 + \alpha^2 + 1 = \alpha^2 + 1 + \alpha^2 + 1$$

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

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

$$\Rightarrow x^3 + x^2 + 1 \mid x^n + x^2 + 1$$

$n \equiv 3 \; mod \; 7$ ve $n \equiv -3 \; mod \; 8$ için Çin Kalan Teoremi uygulanırsa,

$$8k - 3 \equiv 3 \; mod \; 7$$

$$k \equiv 6 \; mod \; 7$$

$n = 8k - 3 = 8.6 - 3 = 45 \; mod \; 56$ elde edilir.

Diğer taraftan, $n \equiv 3\ mod\ 7$ ve $n \equiv 3\ mod\ 8$ için Çin Kalan Teoremi uygulanırsa,

$$8k + 3 \equiv 3\ mod\ 7$$

$$k \equiv 0\ mod\ 7$$

$n = 8k - 3 = 8.0 + 3 = 3\ mod\ 56$ elde edilir.

Teorem 3.14 $n \equiv 17\ mod\ 24$ ya da $n \equiv 23\ mod\ 24$ olsun. O zaman, $\mathbb{F}_2$ üzerinde derecesi n olan $f(x) = x^n + x^4 + 1$ şeklinde hiçbir indirgenemez trinomial yoktur.

İspat $f(x) = x^n + x^k + 1 \in \mathbb{F}_2[x]$ olmak üzere n tek, k çift, $n \equiv \pm 1\ mod\ 8$ ve de $k \nmid 2n$ alalım. Swan Teoreminin (iii) koşuluna göre f nin çift sayıda indirgenemez çarpanı yoktur. $k \nmid 2n$, n tek, k çift olduğundan $k = 4$ aldığımızda aşağıdaki ifadeyi elde ederiz:

$x^2 + x + 1$, $\mathbb{F}_2$ üzerinde indirgenemez bir polinom olmak üzere,

Eğer $n \equiv 2\ mod\ 3$ ise $x^2 + x + 1 \mid x^n + x^4 + 1$ olduğunu gösterelim.

$ord(x^2 + x + 1) = 3$ olduğundan α, $x^2 + x + 1$ polinomunun kökü olmak üzere $\alpha^3 = 1$ dir. Buradan $n = 3k + 2$ olmak üzere,

$$\alpha^{3k+2} + \alpha^4 + 1 = \alpha^{3k}\alpha^2 + (\alpha^2)^2 + 1 = \alpha + 1 + (\alpha + 1)^2 + 1$$

$$= 2\alpha + 2 = 0$$

$$\Rightarrow \alpha^n + \alpha^4 + 1 = 0$$

$$\Rightarrow x^2 + x + 1 \mid x^n + x^4 + 1$$

$n \equiv 2\ mod\ 3$ ve $n \equiv -1\ mod\ 8$ için Çin Kalan Teoremi uygulanırsa,

$$8k - 1 \equiv 2\ mod\ 3$$

$$k \equiv 0\ mod\ 3$$

$n = 8k - 1 = 8.0 - 1 = 23\ mod\ 24$ elde edilir.

Diğer taraftan, $n \equiv 2\ mod\ 3$ ve $n \equiv 1\ mod\ 8$ için Çin Kalan Teoremi uygulanırsa,

$$8k + 1 \equiv 2\ mod\ 3$$

$$2k \equiv 1\ mod\ 3$$

$$k \equiv 2\ mod\ 3$$

$n = 8k + 1 = 8.2 + 1 = 17\ mod\ 24$ elde edilir.

Gathen, [3] te $\mathbb{F}_3$ üzerindeki indirgenemez trinomialleri incelemiş ve aşağıdaki tabloya ulaşmıştır.

Çizelge 3.1

$n\ mod\ 12$	$x^n + x^k + 1$	$x^n + x^k - 1$	$x^n - x^k + 1$	$x^n - x^k - 1$
0	–	2, 4	–	2, 4
1	**0**, **1**, **3**, **4**	0, **1**, **3**, 4	0, 1, 3, 4	**0**, 1, 3, **4**
2	**0**, **2**, **3**, **5**	1	0, 2, **3**, 4, 5	1
3	**4**, **5**	2, **5**	1, 2	1, **4**
4	–	0, 1, 3, 4(2; 01,10)	–	0, 1, 3, 4(2; 01,11)
5	–	4	1, 4	1
6	**1**, **2**, **4**, **5**	1, 5	**1**, 2, 4, 5	1, 5
7	–	2	2, 5	5
8	–	0, 2, 3, 5(4; 01,10)	–	0, 2, 3, 5(4; 01,11)
9	**1**, **2**	**1**, 4	4, 5	**2**, 5
10	**0**, **1**, **3**, **4**	5	0, **1**, 2, **3**, 4	5
11	**0**, **1**, **3**, **5**	0, 2, **3**, 5	0, 2, 3, 5	**0**, **2**, 3, 5

Bu tabloda **kalın** ile yazılan ifadeler o değerlere sahip trinomiallerin indirgenebilir; diğer değerlere sahip trinomiallerin ise indirgenemez olma ihtimallerinin olduğunu göstermektedir.

Teorem 3.15 $n \equiv 0\ mod\ 12$ olsun. O zaman, $n = 12t$ olacak şekilde $t \in \mathbb{Z}$ vardır. Eğer t tek tamsayı ise $\mathbb{F}_3$ üzerinde derecesi n olan $f(x) = x^n + x^4 - 1$ şeklinde hiçbir indirgenemez trinomial yoktur. Ayrıca bu polinomların ortak çarpanı $x^2 + x + 2$ dir.

İspat $f(x) = x^n + x^k - 1 \in \mathbb{F}_3$ olmak üzere Çizelge 3.1'e göre $n \equiv 0\ mod\ 12$ ve $k \equiv 4\ mod\ 6$ değerlerinde $f(x) = x^n + x^k - 1$ trinomialinin tek sayıda indirgenemez

çarpanı vardır. Yani f polinomunun indirgenemezlik ihtimali korunur. Burada k değerini 4 alırsak,

x^2+x+2, $\mathbb{F}_3$ üzerinde indirgenemez bir polinom olmak üzere, eğer $n=12t$ ve t tek tamsayı ise $x^2+x+2 \mid x^n+x^4-1$ olduğunu gösterelim.

$ord(x^2+x+2)=8$ olduğundan α, x^2+x+2 polinomunun bir kökü olmak üzere $\alpha^8=1$ dir. $n=12t$ ve $t=2k+1$, $k \in \mathbb{Z}$ olmak üzere;

$$\alpha^{12t}+\alpha^4-1=\underbrace{\alpha^{8t}}_{1}\alpha^{4t}+\alpha^4+2=\alpha^{8k+4}+\alpha^4+2$$

$$=\underbrace{\alpha^{8k}}_{1}\alpha^4+\alpha^4+2$$

$$=2(\alpha^2)^2+2=2(2\alpha+1)^2+2$$

$$=2(\alpha^2+\alpha+1)+2$$

$$=2(2\alpha+1+\alpha+1)+2$$

$$=6\alpha+6$$

$$=0$$

Buradan $x^2+x+2 \mid x^n+x^4-1$ olur.

Teorem 3.16 $n \equiv 5\ mod\ 13$ olsun. O zaman $\mathbb{F}_3$ üzerinde derecesi n olan $f(x)=x^n+x-1$ şeklinde hiçbir indirgenemez trinomial yoktur.

İspat x^3+x^2+2, $\mathbb{F}_3$ üzerinde indirgenemez bir polinom olmak üzere, eğer $n \equiv 5\ mod\ 13$ ise $x^3+x^2+2 \mid x^n+x-1$ olduğunu gösterelim.

$ord(x^3+x^2+2)=13$ olduğundan α, x^3+x^2+2 polinomunun bir kökü olmak üzere $\alpha^{13}=1$ dir. $n=13t+5$, $t \in \mathbb{Z}$ olmak üzere;

$$\alpha^{13t+5}+\alpha-1=\underbrace{\alpha^{13t}}_{1}\alpha^5+\alpha+2$$

$$=\alpha^3\alpha^2+\alpha+2=(2\alpha^2+1)\alpha^2+\alpha+2$$

$$=2\alpha^4+\alpha^2+\alpha+2=2(2\alpha^2+1)\alpha+\alpha^2+\alpha+2$$

$$=\alpha^3+2\alpha+\alpha^2+\alpha+2$$

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

$$= 0$$

Buradan $x^3 + x^2 + 2 \mid x^n + x - 1$ olur.

Sonuç 3.17 $n \equiv 18\, mod\ 156$ olsun. O zaman $\mathbb{F}_3$ üzerinde derecesi n olan $f(x) = x^n + x - 1$ şeklinde hiçbir indirgenemez trinomial yoktur.

İspat $f(x) = x^n + x^k - 1 \in \mathbb{F}_3$ olmak üzere Çizelge 3.1'e göre $n \equiv 6\, mod\ 12$ ve $k \equiv 1\, mod\ 6$ değerlerinde $f(x) = x^n + x^k - 1$ trinomialinin tek sayıda indirgenemez çarpanı vardır. Özel olarak k değerini 1 alırsak f polinomu Çizelge 3.1'de indirgenebilir trinomialler arasında değildir.

Teorem 3.16 ya göre $n \equiv 5\, mod\ 13$ olduğunda $f(x) = x^n + x^k - 1$ trinomiali indirgenebilir idi.

Şimdi, $n \equiv 5\, mod\ 13$ ve $n \equiv 6\, mod\ 12$ için Çin Kalan Teoremi uygulanırsa,

$$13k + 5 \equiv 6\, mod\ 12$$

$$k \equiv 1\, mod\ 12$$

$n = 13k + 5 = 13.1 + 5 = 18\, mod\ 156$ elde edilir.

Teorem 3.18 $n \equiv 3\, mod\ 13$ olsun. O zaman $\mathbb{F}_3$ üzerinde derecesi n olan $f(x) = x^n - x^2 + 1$ şeklinde hiçbir indirgenemez trinomial yoktur.

İspat $x^3 + 2x^2 + 2$, $\mathbb{F}_3$ üzerinde indirgenemez bir polinom olmak üzere, eğer $n \equiv 3\, mod\ 13$ ise $x^3 + 2x^2 + 2 \mid x^n + x^2 - 1$ olduğunu gösterelim.

$ord(x^3 + 2x^2 + 2) = 13$ olduğundan α, $x^3 + 2x^2 + 2$ polinomunun bir kökü olmak üzere $\alpha^{13} = 1$ dir. $n = 13t + 3$, $t \in \mathbb{Z}$ olmak üzere;

$$\alpha^{13t+3} - \alpha^2 + 1 = \underbrace{\alpha^{13t}}_{1}\alpha^3 + 2\alpha^2 + 1$$

$$= \alpha^2 + 1 + 2\alpha^2 + 1 = 3\alpha^2 + 3 = 0$$

Buradan $x^3 + 2x^2 + 2 \mid x^n + x^2 - 1$ olur.

Sonuç 3.19 $n \equiv 3\, mod\ 156$ olsun. O zaman $\mathbb{F}_3$ üzerinde derecesi n olan $f(x) = x^n - x^2 + 1$ şeklinde hiçbir indirgenemez trinomial yoktur.

İspat $f(x) = x^n - x^k + 1 \in \mathbb{F}_3$ olmak üzere Çizelge 3.1'e göre $n \equiv 3\, mod\ 12$ ve $k \equiv 2\, mod\ 6$ değerlerinde $f(x) = x^n - x^k + 1$ trinomialinin tek sayıda indirgenemez

çarpanı vardır. Özel olarak k değerini 2 alırsak f polinomu Çizelge 3.1'de indirgenebilir trinomialler arasında değildir.

Teorem 3.18 ya göre $n \equiv 3\, mod\, 13$ olduğunda $f(x) = x^n - x^2 + 1$ trinomiali indirgenebilir idi.

Şimdi, $n \equiv 3\, mod\, 13$ ve $n \equiv 3\, mod\, 12$ için Çin Kalan Teoremi uygulanırsa,

$$13k + 3 \equiv 3\, mod\, 12$$

$$k \equiv 0\, mod\, 12$$

$n = 13k + 3 = 13.0 + 3 = 3\, mod\, 156$ elde edilir.

Lemma 3.20 f, $\mathbb{F}_2$ üzerinde self-reciprocal indirgenemez bir polinom olsun. O halde f nin trinomialleri bölmesi için gerek ve yeter koşul f nin mertebesinin 3 ün katı olmasıdır [5].

İspat ($\Leftarrow$) $ordf = 3k, k \in \mathbb{Z}^+$ olsun. O halde

$f|x^{3k-1} - 1 \Rightarrow f|(x^k - 1)(x^{2k} + x^k + 1)$ dir, ayrıca $f \nmid x^k - 1$ ($ordf = 3k$ idi) olduğundan $f|x^{2k} - x^k + 1$ olur. Yani f polinomu bir trinomiali böler. Burada k keyfi sabit olduğundan f polinomu sonsuz çoklukta trinomiali böler.

($\Rightarrow$) $f|x^m + x^n + 1$ ve $ordf = e$ olsun. m ve n yi e ile kalanlı bölersek $m = eq + m'$, $n = eq' + n'$, $m, n < e$ olur. Şimdi α, f polinomunun bir kökü olsun. O zaman $\alpha^m + \alpha^n + 1 = 0$ dır ve f bir self-reciprocal polinom olduğundan $^1/_\alpha$ da f polinomunun bir köküdür. Böylece $\left(^1/_\alpha\right)^m - \left(^1/_\alpha\right)^n + 1 = 0$ olur. Denklemin her iki tarafını da α^m ile çarparsak $1 + \alpha^{m-n} + \alpha^m = 0$ elde ederiz. Şimdi, $1 + \alpha^{m-n} + \alpha^m = \alpha^m + \alpha^n + 1 = 0$ eşitliğinden

$$\alpha^{m-n} = \alpha^n \Rightarrow \alpha^{m-2n} = 1 \Rightarrow e \mid \underbrace{m}_{<e} - 2n \Rightarrow m - 2n = 0 \Rightarrow m = 2n.$$

Böylece $f|x^{2n} + x^n + 1 \Rightarrow f|(x^{2n} + x^n + 1)(x^n + 1) = x^{3n} + 1$ olur. Buradan $\alpha^{3n} = 1 \Rightarrow e \mid 3n$ olduğundan $e = 3n$, $n \in \mathbb{Z}^+$ dir. Aksi takdirde $e \mid 3n$ olabilmesi için $3n$ ifadesinin en az $2e$ olması gerekirdi; ancak $3n < {}^3/_2\, e$ ($2n < e \Rightarrow 3n < {}^3/_2\, e$).

Lemma 3.21 Mertebesi e olan indirgenemez bir f polinomu self-reciprocal $x^{2m} + x^m + 1$ trinomialini bölüyor ise o zaman derecesi e den küçük tek bir self-reciprocal trinomial vardır ve f polinomu bu trinomiali böler [9].

İspat α, f nin herhangi bir kökü olsun. O halde $\alpha^{2m} + \alpha^m + 1 = 0$ olur. Şimdi $m = eq + r,\ 0 < r < e$ yazalım. Eğer $2r < e$ ise $\alpha^{2r} + \alpha^r + 1$ istenen trinomialdir. $2r > e$ olduğunu kabul edelim. ($2r \neq e$ dir, çünkü $2r = e$ olsaydı $0 = \alpha^{2m} + \alpha^m + 1 = \alpha^{2r} + \alpha^r + 1 = \alpha^r + 1$ olurdu ki bu çelişkidir.)

$r_1 = 2r - e$ olsun. O zaman $0 < r - r_1 = e - r < r$ ve

$$0 = \alpha^{2m} + \alpha^m + 1 = \alpha^{e(2q+1)+r_1} + \alpha^{eq+r} + 1 = \alpha^r + \alpha^{r_1} + 1.$$

Diğer taraftan,

$$(\alpha^{-1})^{2m} + (\alpha^{-1})^m + 1 = \alpha^{-r} + \alpha^{-r_1} + 1 = 0$$

olur ve buradan

$$\alpha^r + \alpha^{r-r_1} + 1 = 0.$$

Burada $\alpha^r + \alpha^{r-r_1} + 1$ trinomiali $\alpha^r + \alpha^{r_1} + 1$ nin reciprocalıdır. O halde

$$\alpha^r + \alpha^{r-r_1} + 1 = \alpha^r + \alpha^{r_1} + 1.$$

$\alpha^{r-r_1} = \alpha^{r_1}$ dir. Böylece $\alpha^{|r-2r_1|} = 1$ dir öyle ki $e||r - 2r_1|$ olur.

$|r - 2r_1| < e$ olduğundan $r = 2r_1$ dir. Buradan $f|x^{2r_1} + x^{r_1} + 1$ olur. O zaman $\alpha^{3r} = 1$ $(\alpha^{3r_1} = 1)$ ve böylece $e \mid 3r\ (3r_1)$.

$2r\ (2r_1) < e$ olduğundan $e = 3r\ (3r_1)$. Eğer $\alpha^{2m_1} + \alpha^{m_1} + 1 = 0,\ 2m_1 < e$ olacak şekilde bir başka m_1 tamsayısı olsaydı o zaman $e = 3m_1$ ve buradan $m_1 = r(r_1)$ olurdu.

BÖLÜM 4

İNDİRGENEMEZ POLİNOMLARIN İNŞASI

$f(x), g(x) \in \mathbb{F}_q[x]$ ve $P(x) = \sum_{i=0}^{n} c_i x^i \in \mathbb{F}_q[x]$, n. dereceden indirgenemez bir polinom olsun. Bu durumda

$$P\left(f/g\right) = g^n(x) P\left(f(x)/g(x)\right) = \sum_{i=0}^{n} c_i f^i(x) g^{n-i}(x)$$

polinomu da $\mathbb{F}_q$ üzerinde bir polinomdur. $P\left(f/g\right)$ ye P nin f/g ile bileşkesi denir. Ayrıca, $P\left(f/g\right)$ polinomunun indirgenemez olması için öncelikle $P(x)$ in indirgenemez ve de $f(x)$ ve $g(x)$ in aralarında asal olmaları gerekir [10].

Teorem 4.1 $f(x), g(x) \in \mathbb{F}_q[x]$ ve $P(x) \in \mathbb{F}_q[x]$, n. dereceden indirgenemez bir polinom olsun. O halde, $P(f/g) = g^n(x) P(f(x)/g(x))$, $\mathbb{F}_q$ üzerinde indirgenemez olması için gerek ve yeter koşul λ, $P(x)$ in $\mathbb{F}_{q^n}$ deki bir kökü olmak üzere $f(x) - \lambda g(x) \in \mathbb{F}_{q^n}$ polinomunun $\mathbb{F}_{q^n}$ üzerinde indirgenemez olmasıdır [10].

İspat $P(x)$ in derecesi $n > 1$ olsun. O halde, $h = \max(\deg f, \deg g)$ olmak üzere $P(f/g)$ polinomunun derecesi hn dir. γ, $P(f/g)$ polinomunun bir kökü olsun. O zaman, λ, $P(x)$ in herhangi bir kökü olmak üzere $f(\gamma) = \lambda g(\gamma)$ dır. Buradan, $\mathbb{F}_q(\lambda) \subseteq \mathbb{F}_q(\gamma)$ ve de $[\mathbb{F}_q(\lambda): \mathbb{F}_q] = n$ dir. Şimdi,

$P(f/g)$, $\mathbb{F}_q$ üzerinde indirgenemez $\Leftrightarrow [\mathbb{F}_q(\gamma): \mathbb{F}_q] = hn$

$$\Leftrightarrow [\mathbb{F}_q(\gamma): \mathbb{F}_q(\lambda)] = h$$

$\Leftrightarrow f(x) - \lambda g(x)$, $\mathbb{F}_{q^n}$ üzerinde indirgenemezdir.

Lemma 4.2 $s, e \geq 2$, $(s, e) = 1$ ve s nin $mod\ e$ ye göre mertebesi m olsun. $t \geq 2$, her asal böleni e yi bölen ancak $s^m - 1/e$ yi bölmeyen bir tamsayı olsun. Ayrıca $t \equiv 0\ mod\ 4$ iken $s^m \equiv 1\ mod\ 4$ olduğunu kabul edelim. Bu durumda s nin $mod\ et$ deki mertebesi mt dir [1].

Teorem 4.3 $a \in \mathbb{F}_q^*$ elemanının mertebesi e olsun. $x^t - a$ polinomunun $\mathbb{F}_q$ üzerinde indirgenemez olması için $t \geq 2$ bir tamsayı olmak üzere aşağıdaki koşulların sağlanmasıdır.

(i) $\gcd\left(t, q - 1/e\right) = 1$,

(ii) t nin her asal böleni e yi bölmeli,

(iii) $4 \mid t \Rightarrow 4 \mid q - 1$

[10].

Sonuç 4.4 $P(x) \in \mathbb{F}_q[x]$, derecesi n ve mertebesi e olan indirgenemez bir polinom olsun. λ, $P(x)$ in $\mathbb{F}_{q^n}$ üzerindeki bir kökü olsun. O zaman,

$x^t - \lambda \in \mathbb{F}_{q^n}$ polinomu indirgenemez $\Leftrightarrow$ (i) $\gcd\left(t, q^n - 1/e\right) = 1$,

(ii) t nin her asal böleni e yi bölmeli,

(iii) $4 \mid t \Rightarrow 4 \mid q^n - 1$.

$\Leftrightarrow P(x^t)$ polinomu $\mathbb{F}_q$ üzerinde indirgenemez.

Teorem 4.5 $x^{2n} + x^n + 1$ trinomialinin $\mathbb{F}_2$ üzerinde indirgenemez olması için gerek ve yeter koşul $n = 3^k$, $k \in \mathbb{Z}$ olmasıdır [1].

İspat $P(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$ indirgenemez bir polinomdur. λ, $x^2 + x + 1$ polinomunun kökü olmak üzere λ elemanının mertebesi 3 tür. Şimdi,

(i) $\gcd\left(3^k, 2^2 - 1/3\right) = \gcd(3^k, 1) = 1$

(ii) 3^k nin her asal böleni $e = 3$ ü böldüğünden Sonuç 4.4'e göre $P\left(x^{3^k}\right) = x^{2.3^k} + x^{3^k} + 1$ polinomu indirgenemezdir. Buradan $n = 3^k$ dır.

Tanım 4.6 p bir asal sayı ve $q = p^m$ olmak üzere

$$L(x) = a_0 + a_1 x^p + a_2 x^{p^2} + \cdots + a_v x^{p^v} \in \mathbb{F}_q[x]$$

ile tanımlanan polinoma $\mathbb{F}_q$ üzerinde *lineerleştirilmiş polinom* denir [10].

Tanım 4.7 $b \in \mathbb{F}_q^*$ ve $L(x)$, $\mathbb{F}_q$ üzerinde lineerleştirilmiş polinom olmak üzere $L(x) - b$ polinomuna *affine polinom* denir [10].

Lemma 4.8 $L(x) \in \mathbb{F}_q[x]$ olsun. Eğer $L(x)$ polinomunun sıfırdan başka kökü yoksa her $b \in \mathbb{F}_q^*$ için $x - A \mid L(x) - b$ olacak şekilde bir $A \in \mathbb{F}_q$ vardır [10].

İspat $L(x): \mathbb{F}_q \longmapsto \mathbb{F}_q$ fonksiyonu tanımlayalım.

$L(\alpha) = L(\beta)$ olsun. O zaman,

$$L(\alpha) - L(\beta) = 0 \Rightarrow L(\alpha - \beta) = 0$$
$$\Rightarrow \alpha - \beta = 0$$
$$\Rightarrow \alpha = \beta$$
$$\Rightarrow L(x) \text{ fonksiyonu birebirdir.}$$

$L(x)$ fonksiyonu birebir ve $\mathbb{F}_q$ sonlu olduğundan $L(x)$ aynı zamanda örtendir. O halde, her $b \in \mathbb{F}_q^*$ için $L(A) = b$ olacak şekilde bir $A \in \mathbb{F}_q$ vardır. Böylece,

$$L(A) - b = 0 \Rightarrow x = A, L(x) \text{ in bir kökü}$$
$$\Rightarrow x - A \mid L(x) - b$$

olur.

Teorem 4.9 p bir asal sayı ve $q = p^m$ olmak üzere $b \in \mathbb{F}_q$ için $x^p - x - b$ trinomialinin $\mathbb{F}_q$ üzerinde indirgenemez olması için gerek ve yeter koşul $Tr_{\mathbb{F}_q|\mathbb{F}_p}(b) \neq 0$ olmasıdır [10].

İspat θ, $x^p - x - b$ trinomialinin bir kökü olsun. O halde $\theta^p - \theta - b = 0$ dır. Buradan,

$\theta^p = \theta + b$

$\theta^{p^2} = (\theta + b)^p = \theta^p + b^p = \theta + b + b^p$

$\theta^{p^3} = (\theta + b + b^p)^p = \theta^p + b^p + b^{p^2} = \theta + b + b^p + b^{p^2}$

$\vdots$

$\theta^{p^m} = (\theta + b + b^p + \cdots + b^{p^{m-2}})^p = \theta + b + b^p + \cdots + b^{p^{m-1}} = \theta + Tr_{\mathbb{F}_q|\mathbb{F}_p}(b)$

Buradan, $\theta^q - \theta = Tr_{\mathbb{F}_q|\mathbb{F}_p}(b)$ olur.

$Tr_{\mathbb{F}_q|\mathbb{F}_p}(b) = 0 \Rightarrow \theta^q = \theta$

$\Rightarrow \theta \in \mathbb{F}_q$

$\Rightarrow \theta, x^p - x - b$ nin bir köküdür

$\Rightarrow x - \theta \mid x^p - x - b$

$\Rightarrow x^p - x - b$ indirgenebilirdir.

Şimdi $Tr_{\mathbb{F}_q|\mathbb{F}_p}(b) \neq 0$ olsun. $x^p - x - b$ nin indirgenemez olduğunu gösterelim. θ yine $x^p - x - b$ trinomialinin bir kökü olsun.

$\theta^q - \theta = \underbrace{Tr_{\mathbb{F}_q|\mathbb{F}_p}(b)}_{\delta}$ idi.

$\theta^{q^2} = \theta^q + \delta^q = \theta + 2\delta \quad (\delta \in \mathbb{F}_p, \delta^q = \delta)$

$\theta^{q^3} = \theta + 3\delta$

$\theta^{q^m} = \theta + m\delta$

Şimdi θ nın minimal polinomunun derecesi m olsun. θ nın tüm eşlenikleri $\theta, \theta^q, \theta^{q^2}, \ldots, \theta^{q^{m-1}}$ dir.

$\theta^{q^m} = \theta + m\delta \Rightarrow m = 0 \equiv p$

$\Rightarrow \theta$ nın minimal polinomunun derecesi p dir.

$\Rightarrow$ minimal polinom $x^p - x - b$ ye eşittir.

$\Rightarrow x^p - x - b$ indirgenemez polinomdur.

Sonuç 4.10 $a, b \in \mathbb{F}_q^*$ olsun. $x^p - ax - b$ trinomialinin $\mathbb{F}_q$ üzerinde indirgenemez olması için gerek ve yeter koşul en az bir $A \in \mathbb{F}_q$ için $a = A^{p-1}$ ve $Tr_{\mathbb{F}_q|\mathbb{F}_p}\left(b/_{A^p}\right) \neq 0$ olmasıdır [10].

İspat $x^p - ax - b$ polinomunun $\mathbb{F}_q$ üzerinde indirgenemez olması için gerek ve yeter koşul $x^{p-1} - a$ polinomunun $\mathbb{F}_q$ üzerinde sıfırdan farklı bir köke sahip olmasıdır. $A \in \mathbb{F}_q$ için $a = A^{p-1}$ alalım. O halde,

$$x^p - ax - b = A^p \left(\left(\frac{x}{A}\right)^p - \left(\frac{x}{A}\right) - \frac{b}{A^p} \right)$$

Buradan, $y = \frac{x}{A}$ alırsak Teorem 3.8 e göre $y^p - y - \frac{b}{A^p}$ polinomunun indirgenemez olması için gerek ve yeter koşul $Tr_{\mathbb{F}_q|\mathbb{F}_p}\left(b/_{A^p}\right) \neq 0$ olmasıdır.

Teorem 4.11 $\mathbb{F}_q$ cisminin karakteristiği p olmak üzere, $P(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \in \mathbb{F}_q[x]$ indirgenemez bir polinom ve $b \in \mathbb{F}_q$ olsun. O halde,

$P(x^p - x - b)$ polinomu $\mathbb{F}_q$ üzerinde indirgenemezdir $\Leftrightarrow Tr_{\mathbb{F}_q|\mathbb{F}_p}(nb - c_{n-1}) \neq 0$

[10].

İspat α, $P(x)$ polinomunun bir kökü olmak üzere $P(x^p - x - b)$ polinomunun indirgenemez olması için gerek ve yeter koşul $x^p - x - b - \alpha$ polinomunun $\mathbb{F}_{q^n}$ üzerinde indirgenemez olmasıdır.

$x^p - x - b - \alpha$ polinomunu indirgenemezdir $\Leftrightarrow Tr_{\mathbb{F}_{q^n}|\mathbb{F}_p}(b + \alpha) \neq 0$

$$\Leftrightarrow Tr_{\mathbb{F}_{q^n}|\mathbb{F}_p}(b) + Tr_{\mathbb{F}_{q^n}|\mathbb{F}_p}(\alpha) \neq 0$$

$$\Leftrightarrow Tr_{\mathbb{F}_q|\mathbb{F}_p}(Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(b)) + Tr_{\mathbb{F}_q|\mathbb{F}_p}(Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha)) \neq 0$$

$$\Leftrightarrow Tr_{\mathbb{F}_q|\mathbb{F}_p}(nb) + Tr_{\mathbb{F}_q|\mathbb{F}_p}(-c_{n-1}) \neq 0$$

$$\Leftrightarrow Tr_{\mathbb{F}_q|\mathbb{F}_p}(nb - c_{n-1}) \neq 0$$

Teorem 4.12 $q = 2^m$ ve $P(x) = \sum_{i=0}^{n} c_i\, x^i$ derecesi n olan $\mathbb{F}_q$ üzerinde indirgenemez bir polinom olsun. O halde,

(i) $x^n P(x + x^{-1})$ polinomu $\mathbb{F}_q$ üzerinde indirgenemezdir $\Leftrightarrow Tr_{\mathbb{F}_q|\mathbb{F}_2}(c_1/c_0) \neq 0$.

(ii) $x^n P^*(x + x^{-1})$ polinomu $\mathbb{F}_q$ üzerinde indirgenemezdir $\Leftrightarrow Tr_{\mathbb{F}_q|\mathbb{F}_2}(c_{n-1}/c_n) \neq 0$

[10].

İspat

(i) α, $P(x)$ polinomunun bir kökü olmak üzere $x^n P(x+x^{-1}) = x^n P(\frac{x^2+1}{x})$ polinomunun indirgenemez olması için gerek ve yeter koşul $x^2+1-\alpha x$ polinomunun $\mathbb{F}_{q^n}$ üzerinde indirgenemez olmasıdır.

$x^2+1-\alpha x$ polinomu indirgenemezdir $\Leftrightarrow$ $\alpha = A^{p-1} = A^{2-1} = A \in \mathbb{F}_q$ ve $Tr_{\mathbb{F}_{q^{n_{|2}}}}(b/A^p) = Tr_{\mathbb{F}_{q^{n_{|2}}}}(1/\alpha^2) \neq 0$

$$\Leftrightarrow Tr_{\mathbb{F}_{q^{n_{|2}}}}(\alpha^{-2}) = [Tr_{\mathbb{F}_{q^{n_{|2}}}}(\alpha^{-1})]^2 \neq 0$$

$$\Leftrightarrow Tr_{\mathbb{F}_{q^{n_{|2}}}}(\alpha^{-1}) \neq 0$$

$$\Leftrightarrow Tr_{\mathbb{F}_q|\mathbb{F}_2}(Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha^{-1}) \neq 0$$

$$\Leftrightarrow Tr_{\mathbb{F}_q|\mathbb{F}_2}(-c_1/c_0) \neq 0$$

(ii) $P(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ olduğundan $P^*(x) = c_0 x^n + c_1 x^{n-1} + \cdots + c_{n-1}x + c_n$ olur. α, $P(x)$ polinomunun bir kökü olmak üzere $x^n P^*(x+x^{-1}) = x^n P^*(\frac{x^2+1}{x})$ polinomunun indirgenemez olması için gerek ve yeter koşul $x^2+1-\alpha x$ polinomunun $\mathbb{F}_{q^n}$ üzerinde indirgenemez olmasıdır.

$x^2+1-\alpha x$ polinomu indirgenemezdir $\Leftrightarrow$ $\alpha = A^{p-1} = A^{2-1} = A \in \mathbb{F}_q$ ve $Tr_{\mathbb{F}_{q^{n_{|2}}}}(b/A^p) = Tr_{\mathbb{F}_{q^{n_{|2}}}}(1/\alpha^2) \neq 0$

$$\Leftrightarrow Tr_{\mathbb{F}_{q^{n_{|2}}}}(\alpha^{-2}) = [Tr_{\mathbb{F}_{q^{n_{|2}}}}(\alpha^{-1})]^2 \neq 0$$

$$\Leftrightarrow Tr_{\mathbb{F}_{q^{n_{|2}}}}(\alpha^{-1}) \neq 0$$

$$\Leftrightarrow Tr_{\mathbb{F}_q|\mathbb{F}_2}(Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha^{-1}) \neq 0$$

$$\Leftrightarrow Tr_{\mathbb{F}_q|\mathbb{F}_2}(-c_{n-1}/c_n) \neq 0$$

Teorem 4.13 p asal olmak üzere $q = p^m$ ve $P(x) \in \mathbb{F}_q[x]$, derecesi n olan indirgenemez bir polinom olsun. O zaman, $x^n P(x+x^{-1})$ polinomu $\mathbb{F}_q$ üzerinde indirgenemez olması için gerek ve yeter koşul $P(2)P(-2)$ elemanının $\mathbb{F}_q$ da bir tam kare olmamasıdır [10].

İspat α, $P(x)$ polinomunun bir kökü olmak üzere $x^n P(x+x^{-1})$ polinomunun indirgenemez olması için gerek ve yeter koşul $x^2+1-\alpha x$ polinomunun $\mathbb{F}_{q^n}$ üzerinde indirgenemez olmasıdır. Bu koşul aşağıdaki ifadeye eşittir:

$x^2+1-\alpha x$ polinomu indirgenemez $\Leftrightarrow \Delta = \alpha^2-4$, $\mathbb{F}_{q^n}$ de bir tam kare değildir

$$\Leftrightarrow -1 = (\alpha^2-4)^{q^n-1/2}$$

Buradan,

$$(\alpha^2-4)^{q^n-1/2} = \left\{[(2-\alpha)(-2-\alpha)]^{q^n-1/q-1}\right\}^{q-1/2}$$

$$= \left\{\prod_{i=0}^{n-1}[(2-\alpha)(-2-\alpha)]^{q^i}\right\}^{q-1/2}$$

$$= \left\{\prod_{i=0}^{n-1}\left[\left(2-\alpha^{q^i}\right)\left(-2-\alpha^{q^i}\right)\right]\right\}^{q-1/2}$$

$$= \{P(2)P(-2)\}^{q-1/2}$$

O halde, $P(2)P(-2)$ elemanı $\mathbb{F}_q$ da bir tam kare değildir.

Örnek 4.14 $P(x) = x^3+2x+1 \in \mathbb{F}_3[x]$ indirgenemez bir polinomdur.

$P(2) = 2^3+2.2+1 = 13 \equiv 1 \; mod\; 3$

$P(-2) = (-2)^3+2.(-2)+1 = -11 \equiv 1 \; mod\; 3$

olmak üzere $P(2).P(-2) = 1.1 \equiv 2^2$ olduğundan Teorem 4.12'ye göre

$$x^n P\left(x+\frac{1}{x}\right) = x^3\left(\left(\frac{x^2+1}{x}\right)^3+2\left(\frac{x^2+1}{x}\right)+1\right)$$

$$= (x^2+1)^3+2x^2(x^2+1)+1$$

$$= x^6+2x^4+2x^2+2$$

polinomu $\mathbb{F}_3$ üzerinde indirgenebilir bir polinomdur. Gerçekten,

$$x^6+2x^4+2x^2+2 = (x^3+x^2+2)(x^3+x^2+1)$$

dir.

Sonuç 4.15 p asal olmak üzere $q = p^m$ ve $P(x) \in \mathbb{F}_q[x]$, derecesi n olan indirgenemez bir polinom olsun. O zaman, $2^n x^n P[(x + x^{-1})/2]$ polinomu $\mathbb{F}_q$ üzerinde indirgenemez olması için gerek ve yeter koşul $P(1)P(-1)$ elemanının $\mathbb{F}_q$ da bir tam kare olmamasıdır [3].

Teorem 4.16 $q = p^n$ ve $f(x) = x^m + a_1 x^{m-1} + \cdots + a_m$, $\mathbb{F}_q$ üzerinde indirgenemez bir polinom olsun. O halde,

$a_1 + {a_1}^p + \cdots + {a_1}^{p^{n-1}} \neq 0 \Longrightarrow {a_m}^{-1}(1 - x^{p-1})^m f^*\left(\frac{x^p}{1-x^{p-1}}\right)$, derecesi pm olan indirgenemez bir polinomdur [4].

İspat $\alpha \in \mathbb{F}_{q^m}$, $f(x)$ polinomunun bir kökü olsun. O halde, $\alpha^q, \ldots, \alpha^{q^{m-1}}$ elemanları da $f(x)$ polinomunun kökleridir. Buradan, $Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}} = -a_1$ ve $Tr_{\mathbb{F}_{q^m}|\mathbb{F}_p}(\alpha) = Tr_{\mathbb{F}_q|\mathbb{F}_p}(Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\alpha)) = Tr_{\mathbb{F}_q|\mathbb{F}_p}(-a_1) \neq 0$ olur. Böylece, Teorem 4.9'a göre $Tr_{\mathbb{F}_{q^m}|\mathbb{F}_p}(\alpha) \neq 0$ olduğundan $g(x) = x^p - x - \alpha$ polinomu $\mathbb{F}_{q^m}$ üzerinde indirgenemez bir polinomdur. O halde,

$$-\alpha^{-1} g^*(x) = -\alpha^{-1} x^p g\left(\frac{1}{x}\right) = -\alpha^{-1}(1 - x^{p-1} - \alpha x^p)$$

de $\mathbb{F}_{q^m}$ üzerinde indirgenemez bir polinomdur. $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ elemanları $f(x)$ polinomunun kökleri olduğundan $\alpha^{-1}, \alpha^{-q}, \ldots, \alpha^{-q^{m-1}}$ elemanları da $f^*(x)$ polinomunun kökleridir. Buradan,

$$-\alpha^{-1} g^*(x) = x^p - \alpha^{-1}(1 - x^{p-1})$$

polinomu indirgenemez olduğundan

$${a_m}^{-1}(1 - x^{p-1})^m f^*\left(\frac{x^p}{1 - x^{p-1}}\right)$$

polinomu da $\mathbb{F}_q$ üzerinde indirgenemez bir polinomdur.

Örnek 4.17 $x^2 + x + 1 \in \mathbb{F}_2[x]$ indirgenemez bir polinomdur. α, $x^2 + x + 1$ polinomunun bir kökü olmak üzere $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$ dir ve $f(x) = x^3 + \alpha x^2 + 1$ polinomu $\mathbb{F}_4$ üzerinde indirgenemez bir polinomdur. Buradan, Teorem 4.16'ya göre

$$g(x) = (1 - x)^3 f^*\left(\frac{x^2}{1 - x}\right) = (1 + x)^3 \left(\left(\frac{x^2}{1 - x}\right)^3 + \alpha\left(\frac{x^2}{1 - x}\right) + 1\right)$$

$$= x^6 + \alpha x^2(1+x)^2 + (1+x)^3$$

$$= x^6 + \alpha x^2 + \alpha x^4 + x^3 + x^2 + x + 1$$

$$= x^6 + \alpha x^4 + x^3 + (1+\alpha)x^2 + x + 1$$

polinomu $\mathbb{F}_4$ üzerinde indirgenemez bir polinomdur.

Örnek 4.18 $f(x) = x^3 + x^2 + 2 \in \mathbb{F}_3[x]$ indirgenemez bir polinomdur. Buradan, Teorem 4.16 ya göre $1 \neq 0$ olduğundan

$$g(x) = 2^{-1}(1-x^2)^3 f^*\left(\frac{x^3}{1-x^2}\right) = 2(1-x^2)^3\left(2\left(\frac{x^3}{1-x^2}\right)^3 + \left(\frac{x^3}{1-x^2}\right) + 1\right)$$

$$= 2(2x^9 + x^3(1-x^2)^2 + (1-x^2)^3)$$

$$= 2(2x^9 + x^3(1-2x^2+x^4) + 1 - x^6)$$

$$= 2(2x^9 + x^3 - 2x^5 + x^7 + 1 - x^6)$$

$$= x^9 + 2x^7 + x^6 + 2x^5 + 2x^3 + 2$$

polinomu $\mathbb{F}_3$ üzerinde indirgenemez bir polinomdur.

Teorem 4.19 $q = 2^n$ ve $f(x) = x^m + a_1 x^{m-1} + \cdots + a_{m-1}x + a_m$, $\mathbb{F}_q$ üzerinde indirgenemez bir polinom olsun. O halde

$a_1 + a_1^2 + \cdots + a_1^{2^{n-1}} \neq 0$ ve $Tr_{\mathbb{F}_q|\mathbb{F}_2}\left(\frac{a_{m-1}}{a_m}\right) \neq 0 \Longrightarrow x^{2m} f\left(\frac{x^4+x^3+x+1}{x^2}\right)$, $\mathbb{F}_q$ üzerinde indirgenemez bir polinomdur.

İspat $\alpha \in \mathbb{F}_{q^m}$, $f(x)$ polinomunun bir kökü olsun. O halde, $\alpha^q, \ldots, \alpha^{q^{m-1}}$ elemanları da $f(x)$ polinomunun kökleridir. Buradan, $Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}} = -a_1$ ve $Tr_{\mathbb{F}_{q^m}|\mathbb{F}_2}(\alpha) = Tr_{\mathbb{F}_q|\mathbb{F}_2}(Tr_{\mathbb{F}_{q^m}|\mathbb{F}_q}(\alpha)) = Tr_{\mathbb{F}_q|\mathbb{F}_2}(-a_1) \neq 0$ olur. Böylece, Teorem 4.9 a göre $Tr_{\mathbb{F}_{q^m}|\mathbb{F}_2}(\alpha) \neq 0$ olduğundan $g(x) = x^2 - x - \alpha$ polinomu $\mathbb{F}_{q^m}$ üzerinde indirgenemez bir polinomdur. Ayrıca, $Tr_{\mathbb{F}_q|\mathbb{F}_2}(\frac{a_{m-1}}{a_m}) \neq 0$ olduğundan Teorem 4.12 ye göre

$$x^2 g\left(x + \frac{1}{x}\right) = x^2\left(\left(x + \frac{1}{x}\right)^2 + \left(x + \frac{1}{x}\right) + \alpha\right)$$

$$= (x^2+1)^2 + (x^2+1)x + \alpha x^2$$

$$= x^4 + x^3 + x + 1 - \alpha x^2$$

polinomu $\mathbb{F}_{q^m}$ üzerinde indirgenemez bir polinomdur. Böylece Teorem 4.1'e göre

$$x^{2m} f\left(\frac{x^4 + x^3 + x + 1}{x^2}\right)$$

$\mathbb{F}_q$ üzerinde indirgenemez bir polinomdur.

Örnek 4.20 $f(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_8[x]$ indirgenemez bir polinomdur.

$1 + 1^2 + 1^{2^2} = 3 \neq 0$ ve $Tr_{\mathbb{F}_8|\mathbb{F}_2}(1) \neq 0$ olduğundan Teorem 4.19'a göre

$x^8 f\left(\frac{x^4+x^3+x+1}{x^2}\right) =$

$x^8 \left[\left(\frac{x^4+x^3+x+1}{x^2}\right)^4 + \left(\frac{x^4+x^3+x+1}{x^2}\right)^3 + \left(\frac{x^4+x^3+x+1}{x^2}\right)^2 + \left(\frac{x^4+x^3+x+1}{x^2}\right) + 1\right]$

$= (x^4 + x^3 + x + 1)^4 + x^2(x^4 + x^3 + x + 1)^3 + x^4(x^4 + x^3 + x + 1)^2 + x^4(x^4 + x^3 + x + 1) + x^8$

$= x^{16} + x^8 + x^7 + x^5 + x^3 + x^2 + 1$

fonksiyonu $\mathbb{F}_8$ üzerinde indirgenemez bir polinomdur.

KAYNAKLAR

[1] Swan, R.G., (1962). “Factorization of Polynomials Over Finite Fields”, Pacific Journal of Mathematics, 19: 1099-1106.

[2] Brent R., Zimmermann P., (2004). “Algorithms for Finding Almost Irreducible and Almost Primitive Trinomials”, Primes and Misdemeanours: Lectures in Honour of the Sixtieth Birthday of Hugh Cowie Williams, The Fields Institute, 91-102.

[3] Gathen, J. V. Z., (2003). “Irreducible Trinomials Over Finite Fields”, Mathematics of Computation, 244: 1987-2000.

[4] Abrahamyan, S., (2010). “Construction of Irreducible Polynomials over Finite Fields”, CASC 2010, LNCS 6244.

[5] Niederreiter, H. ve Lidl, R., (1986). Introduction of Finite Fields and Their Applications, Cambridge University Press, Cambridge.

[6] Stickelberger, L., (1897). “Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper”, Verhandlungen des ersten Internationalen Mathematiker-Kongresses, Zürich, 182-193.

[7] Ciet, M., Quisquarter, J.-J. ve Sica, F., (2002). “A Short Note on Irreducible Trinomials in Binary Fields”, Universite Catholique de Louvain, Belgium.

[8] Hayman, S., (2012). “Testing Irreducibility of Trinomials over $\mathbb{F}_2$”, Honor Projects, Bloomington.

[9] Koepf W., (2009). “Divisibility of Trinomials by Irreducible Polynomials over $\mathbb{F}_2$”, International Journal of Algebra, 4: 189-197.

[10] Menezez, A., Blake, I., Gao, X., Mullin, R., Vanstone, S. ve Yaghoobian, T., (1993). Applications of Finite Fields, Kluwer Academic Publishers, Boston.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : Betül DUMAN

Doğum Tarihi ve Yeri : 28.06.1990 – Of

Yabancı Dili : İngilizce

E-posta : betul.duman@outlook.com

ÖĞRENİM DURUMU

Derece	**Alan**	**Okul/Üniversite**	**Mezuniyet Yılı**
Lisans	Matematik	Yıldız Teknik Üniversitesi	2014
Lise	Fen Bilimleri	Bodrum Anadolu Lisesi	2009

İŞ TECRÜBESİ

Yıl	**Firma/Kurum**	**Görevi**
2013-2016	Devecioğlu Turab Yapı İnşaat San. Ltd. Şti.	Yönetici Asistanı
2016-Devam	Özel Kadıköy Kervan Mesleki ve Teknik Anadolu Lisesi	Matematik Öğretmeni

YAYINLARI

Bildiri

1. Ulusal Bildiri	**11. ANKARA MATEMATİK GÜNLERİ (2016 - ANKARA)** Sonlu Cisimler Üzerindeki İndirgenemez Trinomialler
2. Uluslararası Bildiri	**2nd INTERNATIONAL CONFERENCE ON ENGINEERING AND NATURAL SCIENCES (2016 – BOSNA HERSEK)** A Note On Construction of Irreducible Polynomials Over Finite Fields with Characteristic 2