PİRİMİTİF KÖKLER
VE
PERİYODU VERİLEN EN KÜÇÜK MATRİS

Saadet ARSLAN

YÜKSEK LİSANS TEZİ

MATEMATİK ANABİLİM DALI

Konya,1994

T.C.
SELÇUK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

PRİMİTİF KÖKLER
VE
PERİYODU VERİLEN EN KÜÇÜK MATRİS

Saadet ARSLAN

YÜKSEK LİSANS TEZİ
MATEMATİK ANABİLİMDALI
KONYA - 1994

Selçuk Üniversitesi

Fen Bilimleri Enstitüsü

Primitif Kökler ve Periyodu Verilen En Küçük Matris

Saadet ARSLAN

Yüksek Lisans Tezi

Matematik Anabilimdalı

Bu tez 7 / 9 /1994 tarihinde aşağıdaki jüri tarafından kabul edilmiştir.

imza	imza	imza
Prof. Dr. Hasan ŞENAY	Doç. Dr. Saziye YÜKSEL	Yrd. Doç. Dr. Ferhat YILDIRIM
(Danışman)		

ABSTRACT

Master of Science Thesis

Primitive Roots and

The Smallest Matrix of Given Period

Saadet ARSLAN

Selçuk Üniversity

Science Institute

Mathematics Course

Supervisor : Prof. Dr. Hasan ŞENAY

Commitee : Doç. Dr. Saziye YÜKSEL

Yrd. Doç. Dr. Ferhat YILDIRIM

This work comprises four main chapters. In the first chapter, primitive roots were investigated in detail, and results of significant teorems about primitive roots were presented. In addition, applications of some simple problems were done in this chapter. In chapter two and three, main and significant terms and teorems related to field extension and polynom roots vere given, respectively. These two chapters help chapter four to be understood. In chapter four, the smallest dimension of a singular matrix of given period n. is discussed in terms of common degree of the irrediculble factors of cyclotomic polynoms. Finally, some observations about this work were explained at the end of this chapter.

ÖZET

Yüksek Lisans Tezi

Primitif Kökler ve

Periyodu Verilen En Küçük Matris

Saadet ARSLAN

Selçuk Üniversitesi

Fen Bilimleri Enstitüsü

Matematik Anabilimdalı

Danışman : Prof. Dr. Hasan ŞENAY

Jüri : Doç. Dr. Şaziye YÜKSEL

Yrd. Doç. Dr. Ferhat YILDIRIM

Bu çalışma dört bölümden oluşmaktadır. Birinci bölümde pirimitif kökler detaylı bir şekilde incelenmiş ve pirimitif köklerle ilgili önemli teoremlerin sonuçları verilmiştir. Ayrıca pirimitif köklerle ilgili bazı basit problemlerin uygulamaları da birinci bölümde sunulmuştur. İkinci ve üçüncü bölümde sırasıyla cisim genişlemeleri ve polinom kökleri ile ilgili temel ve önemli olan kavram ve teoremler verilmiştir. Bu iki bölüm dördüncü bölüm için bir ön hazırlık teşkil eder. Dördüncü bölümde ise periyodu n olarak verilen düzenli bir matrisin en küçük boyutu, cyclotomic polinomların indirgenemez çarpanlarının ortak derecelerinin bir fonksiyonu olarak verilmiştir. Bu bölüm sonunda konu ile ilgili elde edilmiş bazı gözlemler verildi.

İÇİNDEKİLER **Sayfa No:**

1. BÖLÜM

1.1. BİR TAM SAYININ MERTEBESİ

Euler teoreminden m pozitif bir tamsayı ve a, m ile aralarında asal bir tamsayı ise, bu taktirde $a^{\varphi(m)} \equiv 1 \pmod{m}$ dir. Dolayısıyle, $a^x \equiv 1 \pmod{m}$ kongrüansı en az bir x tamsayısı için sağlanır. Sonuç olarak, iyi sıralama özelliğinden bu kongrüansı sağlayan bir en küçük pozitif x tamsayısı mevcuttur.

Tanım 1: a ile m aralarında asal pozitif tamsayılar olsunlar. Bu taktirde $a^x \equiv 1 \pmod{m}$ olacak şekilde en küçük pozitif x tamsayısına m modülüne göre a nın mertebesi denir ve $\mathrm{ord}_m a$ biçiminde gösterilir [1].

Örnek: 7 modülüne göre 2 nin mertebesini bulmak için 7 modülüne göre 2 nin kuvvetlerinin kalanlarını buluruz:

$2^1 \equiv 2 \pmod{7}$, $2^2 \equiv 4 \pmod{7}$, $2^3 \equiv 1 \pmod{7}$.

Şu halde $\mathrm{ord}_7 2 = 3$ dür.

$a^x \equiv 1 \pmod{m}$ kongrüansının bütün çözümlerini düzenli bir şekilde bulmak için aşağıdaki teoremden yararlanılır.

Teorem 1 : n>0 olmak üzere a ile n aralarında asal tamsayılar ise, bu taktirde pozitif x tamsayının $a^x \equiv 1 \pmod{n}$ kongrüansının çözümü olabilmesi için gerek ve yeter şart $\mathrm{ord}_n a \mid x$ olmasıdır. [1]

İspat: Eğer $\mathrm{ord}_n a \mid x$ ise, bu taktirde $k \in Z^+$ olmak üzere $x = k.\mathrm{ord}_n a$ dır. Dolayısıyle

$$a^x = a^{k.\mathrm{ord}_n a} = \left(a^{\mathrm{ord}_n a}\right)^k \equiv 1 \pmod{n}$$

Karşıt olarak, eğer $a^x \equiv 1 \pmod{n}$ ise, bölme algortimasını kullanarak $x = q.\mathrm{ord}_n a + r$, $0 \le r < \mathrm{ord}_n a$ yazarız. Bu eşitlikten

$$a^x = a^{q.\mathrm{ord}_n a + r} = \left(a^{\mathrm{ord}_n a}\right)^q a^r \equiv a^r \pmod{n}$$

bulunur. $a^x \equiv 1 \pmod{n}$ olduğundan $a^r \equiv 1 \pmod{n}$ olur. $0 \le r < \mathrm{ord}_n a$ eşitsizliğinden r=0 sonucuna varırız. Çünkü,mertebe tarifinden, $y = \mathrm{ord}_n a$, $a^y \equiv 1 \pmod{n}$ olacak şekilde en küçük pozitif tamsayıdır. O halde r = 0 olduğundan $x = q.\mathrm{ord}_n a$ elde edilir. Dolayısıyle $\mathrm{ord}_n a \mid x$ dir.

Bu teoremden aşağıdaki sonuç elde edilir.

Sonuç 1: n>0 olmak üzere eğer a ve n aralarında asal tamsayılar ise, bu taktirde $ord_n a | \varphi(n)$ dir.

Mertebe hesaplarında sonuç 1'i kullanarak daha çabuk ve kolay bir şekilde sonucu elde edebiliriz. Şimdi bunu bir örnekle açıklayalım.

Örnek 2. 17 modülüne göre 5'in mertebesini bulalım. $\varphi(17) = 17 - 1 = 16$ dır. 16 nın pozitif bölenleri yalnızca 1, 2, 4, 8 ve 16 olduğundan, sonuç 1'den, $ord_{17} 5$ in mümkün olan değerleri yalnızca bunlardır.

$5^1 \equiv 5 \pmod{17}$ $\quad$ $5^4 \equiv 13 \pmod{17}$, $5^{16} \equiv 1 \pmod{17}$,

$5^2 \equiv 8 \pmod{17}$ $\quad$ $5^8 \equiv 16 \pmod{17}$ dir

O halde $ord_{17} 5 = 16$ dır.

Sonuç 2: a nın m modülündeki üssü t olsun. Bu durumda $a^j \equiv a^k \pmod{m}$ olması için gerek ve yeter şart $j \equiv k \pmod{t}$ olmasıdır.

Sonuç 3: Eğer a nın n modülündeki mertebesi k ise, bu taktirde $a, a^2, \ldots, a^k$ tamsayıları n modülüne göre kongrüent değildirler [7].

Sonuç 3 ten açıkça görülüyorki $k<\varphi(n)$ ise a nın kuvvetleri m modülüne göre indirgenmiş kalan sistemi oluşturmaz. Diğer yandan, eğer $k = \varphi(n)$ ise, yani a nın n modülüne göre mertebesi $\varphi(n)$ ise

$$1, a^2 a^3, \ldots, a^{\varphi(n)-1}$$

sayıları n modülüne göre bir indirgenmiş kalan sistemi oluştururlar.

Fermat Teoreminin karşıtı doğru değildir; yani eğer bazı a lar için $a^{n-1} \equiv 1 \pmod{n}$ ise o zaman n asaldır ifadesi doğru değildir. Sözgelimi (mod 91) e göre indirgenmiş kuvvetleri 3, 9, 27, 81, 61, 1 ve $ord_{91} 3 = 6$ dır. $6|90$ olduğundan $3^{90} \equiv 1 \pmod{91}$ dir. Fakat 91=7.13 olup asal değildir. Ancak daima $\varphi(n) \leq n-1$ olup ayrıca $\varphi(n)=n-1$ olması ancak ve ancak n nin asal olması durumunda söz konusu olduğundan, $ord_n a = n - 1$ olacak şekilde bir a varsa bu n nin kesinlikle asal olmasını gerektirecektir. Bu şekildeki gözlemlerden Fermat Teoreminin tam bir tersi aşağıdaki teoremle verilebilir.

Teorem 2: p, n-1 in asal bölenleri cümlesindeki bütün değerleri almak üzere $a^{(n-1)/p} \equiv 1 \pmod{n}$ kongrüanslarının hiçbirinin doğru olmamasına rağmen, eğer $a^{n-1} \equiv 1 \pmod{n}$ olacak şekilde bir a varsa n asaldır. [5]

İspat. Lemma 1 ve ilk hipoteze göre a nın n modülündeki mertebesi n-1 i böler. Öte yandan n-1 in her öz böleni aynı zamanda (n-1)/p sayılarının en az birinin böleni olduğundan ikinci hipotez ve lemma 1 e göre t, n-1 in bir öz böleni olamaz. Buradan t=n-1 dir. Sonuç 1 den $n-1 \mid \varphi(n)$ ve böylece $n-1=\varphi(n)$ olur ki bu, m nin asal olması demektir.

Aşağıdaki teorem asal modüllere göre ilkel köklerin varlığını ispat etmede kullanılacaktır. Böylelikle p modülüne göre ilkel köklerin sayısı tam olarak belirtilecektir.

Teorem 3: Eğer $\mathrm{ord}_m a = t$ ise $\mathrm{ord}_m a^n = t/(n,t)$ dir. [5]

İspat: (n,t)=d olsun. $a^t=1 \pmod{m}$ olduğundan

$$\left(a^t\right)^{n/d} = \left(a^n\right)^{t/d} = 1 \pmod{m}$$

dir. Öyleki eğer $\mathrm{ord}_m a^n = t'$ ise o zaman

$$t' \mid \frac{t}{d} \qquad (1)$$

olur. Öte yandan

$$\left(a^n\right)^{t'} \equiv 1 \pmod{m}$$

kongrüansından $t \mid nt'$ ya da

$$\frac{t}{d} \mid \frac{nt'}{d}$$

elde edilir. $\left(\frac{t}{d}, \frac{n}{d}\right) = 1$ olduğundan bu

$$\frac{t}{d} \mid t' \qquad (2)$$

sonucunu verir. (1) ve (2) den $t' = \frac{t}{d}$ elde edilir.

Sonuç 4: a nın n modülündeki üssü k olsun. Bu takdirde a^hın üssünün de k olması için gerek ve yeter şart (h,k) = 1 olmasıdır.

Örnek 3: Aşağıdaki tabloda 13 den küçük pozitif tamsayıların 13 modülüne göre mertebeleri gösterilmiştir.

Pozitif Tamsayı	1	2	3	4	5	6	7	8	9	10	11	12
Mertebe	1	12	3	6	4	12	12	4	3	6	12	2

$$\text{ord}_{13}2^2 = \frac{\text{ord}_{13}2}{(2,\text{ord}_{13}2)} = \frac{12}{(2,12)} = \frac{12}{2} = 6 \qquad \text{ord}_{13}2^3 = \frac{\text{ord}_{13}2}{(3,\text{ord}_{13}2)} = \frac{12}{(3,12)} = \frac{12}{3} = 4$$

Örnek 4: Eğer $\text{ord}_n a = hk$ ise $\text{ord}_n a^h = k$ dır. Gerçekten $\text{ord}_n a = hk$ ise $a^{hk} \equiv 1(\text{mod}\, n)$ dir. Buradan $(a^h)^k \equiv 1(\text{mod}\, n)$. Eğer $l<k$ için $(a^h)^l \equiv 1(\text{mod}\, n)$ olsaydı bu $\text{ord}_n a = hl$ olmasını gerektirirdi. O halde $\text{ord}_n a^h = k$ dir.

Örnek 5: $a \cdot b \equiv 1(\text{mod}\, m)$ ise a ile b nin m modülüne göre mertebeleri aynıdır. Gerçekten $\text{ord}_m a = k$ ve $\text{ord}_m b = l$ olsun. $a^k \equiv 1(\text{mod}\, m)$ ve $b^l \equiv 1(\text{mod}\, m)$ olur. Şimdi $k<l$ varsayalım. $a.b \equiv 1 \pmod m$ ise $(ab)^k \equiv (\text{mod}\, m)$ $\Rightarrow a^k b^k \equiv 1(\text{mod}\, m) \Rightarrow b^k \equiv 1(\text{mod}\, m)$ olur ki $\text{ord}_m b = l$ olması ile çelişir. $k>l$ varsayalım. Bu takdirde $(ab)^l = 1(\text{mod}\, m) \Rightarrow a^l.b^l \equiv 1(\text{mod}\, m) \Rightarrow a^l \equiv 1(\text{mod}\, m)$ olur ki bu da $\text{ord}_m a = k$ olması ile çelişir. Şu halde $k = l$ dir.

Örnek 6: $a^n - 1 \equiv 0(\text{mod}\, a^n - 1) \Rightarrow a^n \equiv 1(\text{mod}\, a^n - 1)$. $k<n$ için $a^k \equiv 1(\text{mod}\, a^n - 1)$ kabul edelim. Bu takdirde $a^k - 1 \equiv 0(\text{mod}\, a^n - 1) \Rightarrow a^n - 1 | a^k - 1$ olur ki $k<n$ olduğundan imkansızdır. O halde $\text{ord}_{a^n-1} a = n$ dir.

Örnek 7: $\text{ord}_p a = 2k$ ($p>2$, asal) ise $a^k \equiv -1(\text{mod}\, p)$ dir. $\text{ord}_p a = 2k$ ise $a^{2k} \equiv 1(\text{mod}\, p) \Rightarrow a^k.a^k \equiv 1(\text{mod}\, p)$. Bu durumda iki durum sözkonusudur.

i) $a^k \equiv 1(\text{mod}\, p)$ ki bu durum $\text{ord}_p a = 2k$ ile çelişir.

ii) $a^k \equiv -1(\text{mod}\, p)$ olmalıdır ki bu durum doğrudur.

Teorem 4: Eğer herhangi bir tamsayının, p asal olmak üzere p modülündeki üssü t ise birbirine kongrüent olmayan, p modülündeki üssü t olan tam $\varphi(t)$ tane sayı vardır [5].

İspat: $ord_p a = t$ olduğunu varsayalım. Sonuç 1'e göre t|p-1 olur. Bu durumda $x^t \equiv 1 \pmod p$ nin tam t sayıda kökü vardır. Öte yandan a, a^2, ... ,a^t sayılarının hepsi bu kongrüansın kökleridir ve bunlar p modülüne göre birbirlerine kongrüent olmadıklarından bunlardan başka kök bulunamaz. Teorem 3'e göre p mödülündeki üssü t olan a nın kuvvetleri (n,t)=1, $1 \le n \le t$ olan a^n sayılarıdır ve bunlardan φ fonksiyonunun tanımı gereği tam $\varphi(t)$ tane vardır.

Teorem 5: p tek asal ve t|p-1 ise p modülüne göre birbirine kongrüent olmayan, p modülündeki üssü t olan $\varphi(t)$ tane sayı vardır. Başka bir deyişle p-1'in her t böleni için,

$$x^t - 1 \equiv 0 \pmod p$$

kongrüansının p modülündeki üssü t olan $\varphi(t)$ kökü vardır [5].

İspat: p-1 in bölenleri cümlesindeki bütün değerleri alsın ve böyle her bir d için γ (d);1,2,...,p-1 tamsayıları arasından mertebesi d(mod p) olanların sayısını göstersin. Sonuç 1 ve Fermat Teoremine göre 1,2,...,p-1 tamsayılarının her birinin p modülündeki üssü tam tamına d lerden biridir. Buna göre

$$x^{p-1} - 1 \equiv \pmod p$$

nin kök sayısı p-1 olduğundan

$$\sum_{d|p-1} \gamma(d) = p - 1$$

dir. Öte yandan Euler'in φ fonksiyonunun özelliklerinden birinin

$$\sum_{d|p-1} \varphi(d) = p - 1$$

olduğunu bilmekteyiz. Böylece bu ikisinden

$$\sum_{d|p-1} \gamma(d) = \sum_{d|p-1} \varphi(d)$$

elde edilir. Teorem 4'e göre $\gamma(d)$ nin değeri her bir d için ya sıfır veya $\varphi(d)$ dir ve yukarıdaki son eşitlikten p-1 i bölen her bir d için $\gamma(d)=\varphi(d)$ sonucu elde edilir.

2. İLKEL KÖKLER

Tanım 1: Eğer a nın m modülündeki üssü $\varphi(m)$ ise yani $ord_m a = \varphi(m)$ ise a ya m nin ilkel kökü denir [8].

Bu kavram m modülüne göre asal kalan sınıfları sistemi elde etmede büyük kolaylık sağladığından önemlidir. Gerçekten g bir ilkel kök ise bunun m modülüne göre

$$g, g^2, \ldots, g^{\varphi(m)}$$

kuvvetleri sonuç 3'e göre birbirinden farklıdır. Ayrıca bunları sayısı $\varphi(m)$ kadar ve (g,m)=1 olduğundan bu sayılar m modülüne göre bir asal kalan sınıfları sistemi oluştururlar.

Örnek 1: $ord_7 3=6=\varphi(7)$ olduğundan 3, 7 mödülüne göre bir ilkel köktür. Benzer şekilde $ord_7 5=6=\varphi(7)$ olduğundan 5 de 7 modülüne göre bir köktür.

Göz önüne alınan herhangi bir tamsayının ilkel kökü bulunmayabilir de. Sözgelimi 8 modülüne göre hiç ilkel kök yoktur. Gerçekten de 8'den küçük ve 8 ile aralarında asal olan sayılar yalnızca 1, 3, 5 ve 7 dir. $ord_8 1 = 1$ ve $ord_8 3 = ord_8 5 = ord_8 7 = 2$ dir. $\varphi(8)=4$ olduğu için bunlardan hiçbiri 8 modülüne göre ilkel kök değildir.

Örnek 2: $F_n = 2^{2^n} + 1$, n>1 bir Fermat asalı ise bu taktirde 2, F_n nin ilkel kökü değildir. (F_1=5 $ord_5 2 = 4$ olduğundan 2, F_1 in ilkel köküdür).

$$2^{2^n+1} - 1 = \left(2^{2^n} + 1\right)\left(2^{2^n} - 1\right) \text{ olduğundan}$$

$$2^{2^n+1} \equiv 1 \pmod{F_n}$$

olur ki bu da 2 nin F_n modülüne göre mertebesinin 2^{n+1} den büyük olamıyacağını gösterir.

Gerçekten F_n ni asal bir sayı farzedersek $\varphi(F_n)=F_n-1=2^{2^n}$ dir. ve $2^{2^n} > 2^{n+1}$ (n>1) olduğu indüksiyonla görülür. Böylece F_n modülüne göre 2 nin mertebesi $\varphi(F_n)$ den küçüktür; tarif 1'den 2'nin F_n için bir pirimitif kök olamayacağı elde edilir.

Sonuç 1: Her asal sayının bir ilkel kökü vardır.

Şimdi bir p tek asalı için mevcut olan ilkel köklerin sayısını da tam olarak aşağıdaki teoremle verebiliriz.

Teorem 1: p tek asalının tam olarak $\varphi(\varphi(p))$ sayıda ilkel kökü vardır.

İspat: Teorem 3 den derhal p nin diğer ilkel köklerinin $(k, \varphi(p))=1$ olan g^k ler olduğunu söyleyebiliriz. Böylece $\varphi(p)$ yi geçmeyen ve $\varphi(p)$ ile aralarında asal olan $\varphi(\varphi(p))$ kadar sayı olacaktır.

Little Fermat Teoreminden eğer p bir asal ise, bu taktirde $h(x)=x^{p-1}-1$ polinomunun p modülüne göre birbirine kongrüent olmayan tam olarak p-1 tane kökü vardır. yani $x=1,2,3,...,p-1 \pmod p$ dir.

p bir asal olmak üzere p modülüne göre polinomların kökleri ile ilgili aşağıdaki önemli teoremi verelim.

Teorem 2. Lagrange Teoremi: $f(x)=a_n x^n + a_{n-1}x^{n-1}+...+a_1 x + a_0$ derecesi $n\geq 1$ olan, tamsayı katsayılı ve $p \nmid a_n$ olan bir polinom olsun. Bu takdirde f(x) polinomu p modülüne göre en çok n tane köke sahiptir [6].

Lagrange Teoremini aşağıdaki teoremi ispatlamak için kullanacağız.

Teorem 3: Eğer p asal ve d, p-1 in bir böleni ise $x^d - 1$ polinomunun p modülüne göre birbirine kongrüent olmayan tam tamına d tane kökü vardır [6].

İspat: $d|p-1$ ise $p-1=d.e$ olsun. Bu takdirde

$$x^{p-1}-1=\left(x^d-1\right)\left(x^{d(e-1)}+x^{d(e-2)}+...+x^d+1\right)$$
$$=\left(x^d-1\right)g(x)$$

Little Fermat teoreminden $x^{p-1}-1$ nin, p modülüne göre p-1 tane farklı kökü vardır. Üstelik $x^{p-1}-1$ in p modülüne göre herhangi bir kökü ya p modülüne göre $x^d - 1$ in bir kökü ya da p modülüne göre g(x) in bir köküdür.

Lagrange teoreminden g(x), p modülüne göre en çok $d(e-1)=p-d-1$ köke sahiptir. (mod p) ye göre g(x) in bir kökü olmayan $x^{p-1}-1$ in her kökü mod p ye göre x^d-1 in bir kökü olmak zorundadır. x^d-1 polinomunun mod p ye göre

en çok (p-1)-(p-d-1)=d farklı kökü vardır. Öte yandan, mod p ye göre en çok d tane farklı kökü vardır. Sonuç olarak $x^d - 1$, p modülüne göre d tane farlı kökü vardır.

3. PRİMİTİF KÖKLERİN VARLIĞI

Şimdi m nin hangi değerleri için ilkel köklerin mevcut olduğunu araştıralım. Öncelikle m nin her değeri için ilkel köklerin mevcut olmadığını ifade edelim. Şimdi yalnızca p tek asal olmak üzere m nin 2, 4, p^k ve $2p^k$ değerleri için ilkel köklerin bulunduğunu göstereceğiz. Ancak $k\geq 3$ için $m=2^k$ nın hiç bir ilkel kökünün bulunmadığını gösterdikten sonra diğer durumları ele alacağız.

Teorem 1: $k\geq 3$ ise tek x tamsayıları için

$$x^{\varphi(2^k)/2} \equiv 1 \pmod{2^k} \qquad (3)$$

dır. O halde 2^k modülüne göre hiç bir ilkel kök bulunamaz.

İspat: k=3 ise x tek tamsayıları için (3), $x^2\equiv 1 \pmod 8$ şekline indirgenir. Bu durumda iddianın doğruluğu;

$$(2m+1)^2 = 4m^2+4m+1 = 4m(m+1)+1$$

ve m(m+1) in çift olduğu göz önüne alınarak $(2m+1)^2\equiv 1 \pmod 8$ kongrüansından derhal elde edilir.

Şimdi teoremi k üzerinde indüksiyonla ispat edelim (3) ün k için doğru olduğunu kabul edip k+1 için doğru olduğunu gösterelim. İndüksiyon varsayımına göre q bir tam sayı olmak üzere.

$$x^{\varphi(2^k)/2} = 1+2^k q$$

olur. Her iki tarafın karesi alınır ve $2k\geq k+1$ olduğuna dikkat edilirse

$$x^{\varphi(2^k)} = 1+2^{k+1}q+2^{2k}q^2 \equiv 1 \pmod{2^{k+1}}$$

elde edilir. Burada (m,n)=d için $\varphi(mn)=d\varphi(m)\varphi(n)/\varphi(d)$ özelliğinden yararlana-rak $(2^k,2)=2$ olduğundan $\varphi(2^{k+1})=2\varphi(2^k)\varphi(2)/\varphi(2) \Rightarrow \varphi(2^{k+1})=2\varphi(2^k)$ $\Rightarrow \varphi(2^k)=\varphi(2^{k+1})/2$ bulunur. Bunun yukarıda kullanılmasıyla da teoremin k+1 için doğruluğu gösterilmiş olur.

Teorem 2: Herhangi bir p tek asalı ve m≥1 için m nin 1, 2, 4, p^k ve $2p^k$ biçiminde olmadığını varsayalım. Bu durumda (m,a)=1 olan herhangi bir a için

$$a^{\varphi(m)/2} \equiv 1 \pmod{m}$$

dir. O halde m modülüne göre hiç bir ilkel kök mevcut değildir.

İspat: n>2 için φ(n) çiftdir. Şimdi p_i ler farklı, tek asallar β≥0, α_i>0 ve r≥1 olmak üzere

$$m = 2^{\beta}\prod_{i=1}^{r} p_i^{\alpha_i}$$

Sayısını göz önüne alalım. Eğer (m,a)=1 ise Eular Teoremine göre

$$a^{\varphi(p_1^{\alpha_1})} \equiv 1\left(\text{mod } p_1^{\alpha_1}\right) \quad \text{ve} \quad a^{\varphi(m/p_1^{\alpha_1})} \equiv 1\left(\text{mod } m/p_1^{\alpha_1}\right)$$

elde edilir. Şimdi r≥2 veya β≥2 olduğunu varsayalım. Bu durumda hem $\varphi(p_1^{\alpha_1})$ ve hem de $\varphi(m/p_1^{\alpha_1})$ çift olup sonuçta

$$a^{\frac{1}{2}\varphi(p_1^{\alpha_1}).\varphi(m/p_1^{\alpha_1})} \equiv 1\left(\text{mod } p_1^{\alpha_1}\right)$$

ve

$$a^{\frac{1}{2}\varphi(p_1^{\alpha_1}).\varphi(m/p_1^{\alpha_1})} \equiv 1\left(\text{mod } m/p_1^{\alpha_1}\right)$$

ve bu ikisinden de

$$a^{\frac{1}{2}\varphi(p_1^{\alpha_1}).\varphi(m/p_1^{\alpha_1})} \equiv 1(\text{mod } m)$$

veya $\left(p_1^{\alpha_1}, m/p_1^{\alpha_1}\right)$=1 ve φ(n) çarpanlanabilir olduğundan

$$a^{\varphi(m)/2} \equiv 1 \pmod{m}$$

elde edilir ki bu sonuç r≥2 veya r=1 ve β≥2 olduğunda ilkel kökün bulunmadığını gösterir.

Şimdi p tek asal k≥2 olmak üzere $m=p^k$ durumu için ilkel köklerin varlığını tartışalım. p^k modülüne göre ilkel kökleri ararken p modülüne göre mevcu olan ilkel köklerin keza p^k modülüne göre bir ilkel kök olarak düşünülmesi doğal olacaktır. Artık g böyle bir illkel kök olmak üzere g nin p^2 modülüne göre bir ilkel kök olup olmayacağını araştıralım. $g^{p-1} \equiv 1 \pmod{p}$ ve

$\varphi(p^2)=p(p-1)>p-1$ olduğundan $g^{p-1}\equiv 1 \pmod{p^2}$ olması g nin p^2 modülüne göre bir ilkel kök olmayacağını gösterir. Buna göre

$$g^{p-1} \not\equiv 1 \pmod{p^2} \qquad (4)$$

bağıntısının g nin p^2 modülüne göre keza bir ilkel kök olması için gerek ve yeter şart olduğu aşağıdaki lemmalardan sonra vereceğimiz teoremle anlaşılacaktır.

Lemma 1: p tek asal olmak üzere p modülüne göre (4) ü gerçekleyen en az bir ilkel kök mevcut olup, $k\geq 2$ için p^k modülüne göre de en az bir ilkel kök vardır.

İspat: g, (mod p) ye göre bir ilkel kök olsun. Bu durumda eğer $g^{p-1}\not\equiv 1 \pmod{p^2}$ ise ispat tamamdır. Bunun yanı sıra eğer $g^{p-1}\equiv 1 \pmod{p^2}$ ise $g_1=g+p$ nin bu defa $g_1^{p-1} \not\equiv 1 (\mathrm{mod}\, p^2)$yi gerçekleyen p nin diğer ilkel kökü olduğunu gösterebiliriz. Gerçekten Binom Teoremine göre

$$g_1^{p-1} = (g+p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p + tp^2$$

ve g, p nin ilkel kökü olduğundan

$$g_1^{p-1} \equiv 1 - pg^{p-2} (\mathrm{mod}\, p^2)$$

olur. Burada $pg^{p-2} \equiv 0(\mathrm{mod}\, p^2)$ olamaz. Çünkü aksi halde bu, $g^{p-2} \equiv 0(\mathrm{mod}\, p)$ olmasını gerektirir ki bu sonuç g nin p modülüne göre bir ilkel kök olması ile çelişir. Böylece lemmanın ispatı tamamdır.

Lemma 2: g, p modülüne göre (4) ü gerçekleyen bir ilkel kök ise her $k\geq 2$ için

$$g^{\varphi(p^{k-1})} \not\equiv 1\left(\mathrm{mod}\, p^k\right) \qquad (5) \text{ dır.}$$

İspat: k üzerinde indüksiyonla ispatlayacağız. k=2 için (5) bağıntısı (4) e indirgenir ki bu durumda ispat tamamdır. Şimdi (5) in k için doğru olduğunu kabul edelim. Bu durumda Euler Teoremine göre

$$g^{\varphi(p^{k-1})} \equiv 1\left(\mathrm{mod}\, p^{k-1}\right)$$

olduğundan (5) e göre, $p \nmid q$ olduğu da göz önüne alınarak

$$g^{\varphi(p^{k-1})} = 1 + q\,p^{k-1}$$

yazılabilir. Bu son eşitliğin her iki yanının p. kuvveti alınır ve $\varphi(n)$ fonksiyonunun $\left[\varphi\left(p^{k-1}\right)\right]^p = \varphi\left(p^k\right)$ özelliği de gözönüne alınırsa Binom teoremine göre

$$g^{\varphi(p^k)} = \left(1 + q\,p^{k-1}\right)^p = 1 + q\,p^k + q^2\frac{p(p-1)}{2}p^{2(k-1)} + r\,p^{3(k-1)}$$

bulunur. $k\geq 2$ için $2k-2\geq k+1$ ve $3k-3\geq k+1$ olduğundan bu son eşitlikten $p\nmid q$ olmak üzere

$$g^{\varphi(p^k)} \equiv 1 + q\,p^k \pmod{p^{k+1}}$$

elde edilir. Bu son kongrüans da $k+1$ için $g^{\varphi(p^k)} \not\equiv 1 \pmod{p^{k+1}}$ olmasını gerektirir ki iddianın $k+1$ için doğruluğu gösterilmiş olur.

Teorem 3: g, p tek asalının bir ilkel kökü ise g nin $k\geq 1$ olmak üzere her p^k modülüne göre bir ilkel kök olması için gerek ve yeter şart (4) ün geçerli olmasıdır.

İspat: g, p nin bir ilkel kökü olsun. Eğer g, $k\geq 1$ olan her k için p^k nın da bir ilkel kökü ise bu durumda g özellikle p^2 nin de bir ilkel kökü olacaktır. Bu ise daha önce belirttiğimiz (4) ü gerektirecektir.

Karşıt olarak g nin p modülüne göre (4) ü gerçekleyen bir ilkel kök olduğunu kabul edelim. Her $k\geq 2$ için g nin keza p^k modülüne göre bir ilkel kök olacağını göstermeliyiz. g nin p^k modülündeki üssü t ise

$g^t \equiv 1 \pmod{p^k}$ olur.

Şimdi $t=\varphi(p^k)$ olduğunu gösterirsek ispat tamamlanır. $g^t\equiv 1 \pmod{p^k}$ $\Rightarrow g^t\equiv 1 \pmod{p}$ olup lemma 1 e göre $\varphi(p)|t$ olur. Buna göre $\exists c\in Z$ için $t=c.\varphi(p)$ dir. Öte yandan $g^t\equiv 1 \pmod{p^k}$ olduğundan $t|\varphi(p^k) \Rightarrow c.\varphi(p)|\varphi(p^k)\Rightarrow c.(p-1)|$ $p^{k-1}(p-1)\Rightarrow c|p^{k-1}$ bulunur. Böylece $j\leq k-1$ olmak üzere $c=p^j$ ve bunu t nin yukardaki ifadesinde kullanmakla da $t=p^j(p-i)$ bulunur. Eğer $j=k-1$ olduğunu gösterirsek o zaman $t=\varphi(p^k)$ olur ve istenen elde edilir. Şimdi bir an için $j<k-1$ olduğunu varsayalım. Bu durumda $j\leq k-2$ ve buradan da $t|\varphi(p^k)\Rightarrow t=p^j(p-1)|$ $p^{k-2}(p-1)=\varphi(p^{k-1})$ elde edilir ki bu $\varphi(p^{k-1})$ in t nin bir katı ve dolayısı ile

$g^{\varphi(p^{k-1})}\equiv 1 \pmod{p^k}$

olduğunu gösterir. Ancak bu sonuç lemma 2 e göre açık bir çelişki olup $j<k-1$ olamaz. Buna göre $j=k-1$ dir. Ve bu durumda $t=\varphi(p^k)$ olur. Bu g nin $k\geq 2$ için p^k modülüne göre bir ilkel kök olduğunu gösterir.

Son olarak $m=2p^k$ olması durumunda ilkel köklerin varlığını garanti eden aşağıdaki teoremi ispat edelim.

Teorem 4: p herhangi bir tek asal ve $k\geq 1$ ise p^k modülüne göre tek ilkel kökler mevcuttur. Böyle her g ilkel kökü aynı zamanda $2p^k$ nın da ilkel köküdür.

İspat: g, p^k nın bir ilkel kökü ise $g+p^k$ da ilkel köktür. Fakat g veya $g+p^k$ dan biri kesinlikle tek olup sonuçta p^k modülüne göre tek ilkel kök daima mevcut olacaktır. Şimdi $g_1=g$ veya $g+p^k$ diyelim. Bu durumda her h için

$$g_1^h \equiv 1 \pmod 2$$

ve aynı zamanda g, $g+p^k$ nın ikisi de p^k nin ilkel kökü olduğundan

$$g_1^h \equiv g^h \equiv 1 \pmod{p^k} \Leftrightarrow p^{k-1}(p-1)|h$$

elde edilir. Buradan g_1 in $2p^k$ nın bir ilkel kökü olduğu sonucuna varılır.

Teorem 5: (m,n)=1 ve m>2, n>2 ise, bu taktirde mn hiç bir ilkel kökü yoktur [7].

İspat: (a, mn)=1 olacak şekilde herhangi bir a tamsayısını gözönüne alalım; bu taktirde (a,n) = 1 ve (a, m)=1, $h=[\varphi(m), \varphi(n)]$ ve $d=(\varphi(m), \varphi(n))$ diyelim.

$\varphi(m)$ ve $\varphi(n)$ nin her ikisi de çift sayısı olduğundan kesinlikle $d\geq 2$ dir.

Sonuç olarak $h = \dfrac{\varphi(m).\varphi(n)}{d} \leq \dfrac{\varphi(m.n)}{2}$ dir.Euler Teoreminden $a^{\varphi(m)} \equiv 1 \pmod m$idi.Son eşitlikten $a^h = (a^{\varphi(m)})^{\varphi(n)/d} \equiv 1 \pmod m$.Benzer şekilde $a^h \equiv 1 \pmod n$ bulunur. Bu son iki ifade ve (m, n)=1 hipotezinden $a^h \equiv 1 \pmod{mn}$ dir. Şu halde mn ile aralarında asal olan herhangi bir tamsayının mertebesi $\varphi(mn)/2$ yi geçemez, dolayısıyle mn nin bir ilkel kökü yoktur.

Sonuç: yukarıda verilen teoremden aşağıdaki basit sonuçları elde ettik.

1) $2^{2^n+1}-1$ biçiminde ifade edilebilen sayıların hiç bir ilkel kökü yoktur.

Çözüm:

$2^{2^n-1}-1=(2^{2^n}+1)(2^{2^n}-1)$ yazılır. Halbuki $2^{2^n}+1$, $2^{2^n}-1$ ardışık iki tek sayıyı temsil ettiğinden $(2^{2^n}+1, 2^{2^n}-1)=1$, üstelik $2^{2^n}+1>$, $2^{2^n}-1>2$ olduğundan yukarıdaki teoreme göre $(2^{2^n}+1).(2^{2^n}-1)$ in hiç bir ilkel kökü yoktur.

2) Ardışık tek sayıların çarpımı biçiminde yazılabilen sayıların hiç bir ilkel kökü yoktur. Yani $m=(2k+1).(2k+3) \Rightarrow$ m nin hiç bir ilkel kökü yoktur.

3) $m>2$ ve $n>2$ ve $m=n+1$ ise m.n nin hiç bir ilkel kökü yoktur.

4) p tek sayı olmak üzere $m=p.2^k$ $k\geq 2$ nin hiç bir ilkel kökü yoktur.

2. BÖLÜM

CİSİM GENİŞLEMELERİ

Tarif 1: F bir cisim olsun. F i kapsayan her hangi bir K cismine F nin bir genişlemesi denir. Bununla özdeş olmak üzere, eğer F, K nın bir alt cismi ise o takdirde K ya F nin genişlemesi denir ve $F \subset K$ veya $\uparrow_F^K$ ile gösterilir [9].

Eğer K, F nin bir cisim genişlemesi ise K 'ya bilinen cisim işlerine göre F üzerinde bir vektör uzayı gibi bakılabilir.

Tarif 2: K nın F üzerinde derecesi, F üzerinde bir vektör uzayı olarak K nın boyutu olup, bu [K:F] biçiminde gösterilir [10].

Özel olarak, [K:F] sonlu olduğu durumda K nın F üzerinde sonlu boyutlu bir vektör uzayı olduğuna ilgi çekilmelidir. Bu durumda K ya F nin sonlu genişlemesi denir.

Teorem 1: L, K nın bir sonlu genişlemesi K da F nin bir sonlu genişlemesi ise L, F nin sonlu bir genişlemesidir. Ayrıca [L:F]=[L:K].[K:F] dir [9]

İspat: İspat için L nin F üzerinde bir bazı bulunduğunu ispat etmeliyiz. Böylece yalnızca L nin F nin sonlu bir genişlemesi olduğunu ispatlamakla kalmayıp aynı zamanda daha kuvvetli bir sonuç olan

$$[L:F]=[L:K].[K:F]$$

eşitliğini göstermiş oluruz.

[L:K]=n ve [K:F]=m olsun. Ayrıca $\{v_1, v_2, \ldots, v_m\}$ L nin K üzerinde bir bazı ve $\{\omega_1, \omega_2, \ldots, \omega_n\}$ de K nın F üzerinde bir bazı olsun. Şimdi i=1,2,...,m ve j=1,2,...,n için $v_i\omega_j$ elemanlarının F üzerinde L nin bir bazı olup olmadığını araştırabiliriz. İlk olarak L nin her elemanının katsayılar F den alınmak kaydıyla $v_i\omega_j$ lerin bir lineer bileşimi olduğunu daha sonra da m.n tane elemanında F üzerinde lineer bağımsız olduğunu göstermeliyiz.

Herhangi $t \in L$ alalım. Varsayıma göre L, K üzerinde bir vektör uzayı olduğundan $k_i \in K (i=1,\ldots,m)$ olmak üzere

$$t = k_1v_1 + k_2v_2 + \ldots + k_mv_m.$$

Bununla beraber yine varsayıma göre K da F üzerinde bir vektör uzayı olduğundan K nında her elemanı $f_j \in F$ (j=1,2,...n) olmak üzere.

$$f_1\omega_1 + f_2\omega_2 + \ldots + f_n\omega_n$$

biçiminde olacaktır. Şu halde

$$k_1 = f_1\omega_1 + \ldots + f_n\omega_n, \ldots, k_i = f_i,\omega_1 + \ldots + f_{in}\omega_n, \ldots, k_n = f_n,\omega_1 + \ldots + f_{mn}\omega_n$$

olur. Bunları t de yerine yazalım

$$t = (f_{11}\omega_1 + \ldots + f_{1n}\omega_n)v_1 + \ldots + (f_{m1}\omega_1 + \ldots + f_{mn}\omega_n)v_m$$

olur. Burada distrübitif ve birleşme özellikleri kullanılarak çarpma yapılacak olursa,

$$t = f_{11}\omega_1 v_1 + \ldots + f_{1n}\omega_n v_1 + \ldots + f_{ij}\omega_j v_i + \ldots + f_{mn}\omega_n v_m$$

elde edilir. Bu son ifade de bütün katsayılar F cisminde olduğundan t yi $\omega_j v_i$ elemanlarının F üzerinde bir lineer birleşimi olarak ifade etmiş olduk. Böylece gerçekten $\omega_j v_i$ elemanları F üzerinde L yi gererler ve bu da baz oluşturmak için ilk şart olur.

İkinci olarak, bu $v_i\omega_j$ elemanlarının F üzerinde lineer bağımsız olduğunu gösterelim. Bunun içinde $f_{ij} \in F$ olmak üzere

$$f_{ij}v_1\omega_1 + \ldots + f_{1n}v_1\omega_n + \ldots + f_{ij}v_i\omega_j + \ldots + f_{mn}v_m\omega_n = 0 \qquad (*)$$

olduğunu varsayalım. Burada her f_{ij} katsayısının sıfır olduğunu gösterirsek $v_i\omega_j$ elemanlarının lineer bağımsız olduğunu göstermiş oluruz. (*) ifadesini tekrar gruplayarak

$$(f_{11}w_1 + \ldots + f_{1n}\omega_n)v_1 + \ldots + (f_{i1}w_1 + \ldots + f_{in}\omega_n)v_i + \ldots + (f_{m1}\omega_1 + \ldots + f_{mn}\omega_n)v_m = 0$$

bulunur ω_j ler K da ve $K \supset F$ olduğunda bütün $k_i = f_i,\omega_1 + \ldots + f_{in}\omega_n$ katsayıları K da olacaktır

Artık $k_1v_1 + \ldots + k_mv_m = 0$ $(k_1, k_2, \ldots k_m \in F)$ dır. Kabülümüze göre v_i ler K üzerinde L nin bir bazı olduğundan özel olarak bunların K üzerindel lineer bağımsız olması gerekiyor. Yani, $k_1 = k_2 = \ldots = k_m = 0$ dır. $k_1, k_2, \ldots k_m$ lerin bu değeri yerine yazılırsa i = 1,2,...m için $f_{i1}\omega_1 + \ldots + f_{in}\omega_n = 0$ elde edilir. Öte yandan kabülümüze göre w lerde F üzerindel lineer bağımsız olduğundan $f_{ij} = 0$ olmasını gerektirir. Böylece $v_i\omega_j$ lerin F üzerinde lineer bağımsız olduğu gösterilmiş olur.

Bütün bunlardan $v_i\omega_j$ lerin L nin F üzerinde bir bazı olduğunu göstermiş oluruz. O halde [L:F] = m.n olmak zorundadır. Çünkü [L:F] = m ve [K:F] = n idi, böylece

$$[L:F] = [L:K].[K:F]$$

olduğunu göstermiş oluruz.

Sonuç 1: Eger L, F nin sonlu genişlemesi ve K da L nin F yi kapsayan bir alt cismi ise [K:F]|[L:F] dir.

İspat: $F \subset K \subset L$ ve [L:F] nin sonlu olduğunu varsayalım. Açık olarak L nin herhangi bir elemanı K üzerinde lineer bağımsız olup sonuçta F üzerinde lineer bağımsız olur. Böylece [L:F] nin sonlu olduğu kabülü [L:K] nın da sonlu olacağı sonucunu verir. Yine $K \subset L$ olduğundan [K:F] nin de sonlu olduğu sonucuna varılır. Bir önceki teoreme göre,

$$[L:F]=[L:K].[K:F]$$

eşitliği [K:F]|[L:F] olmasını gerektirir.

NOT: Eğer [L:F]=p (p bir asal) ise bu L ile F arasında $F \subset K \subset L$ olacak şekilde K cisminin bulunamayacağını gösterir. Bu sonuç pergel ve cetvel yardımıyla bazı çizimlerin yapılmasında fevkalade önemli rol oynar.

Tarif 3: F cisim ve $F \subset K$ olsun. Bir $a \in K$ için F de hepsi birden sıfır olmayan ve $\alpha_0 a^n + \alpha_1 a^{n-1} + \ldots + \alpha_n = 0$ olacak biçimde $\alpha_0, \alpha_1, \ldots, \alpha_n$ katsayıları varsa a ya F üzerinde cebirsel, aksi halde transandat denir [4].

Eğer $q(x) \in F[x]$ polinomu $q(x)=\beta_0 x^m + \beta_1 x^{m-1} + \ldots + \beta_m$ biçiminde ise, herhgangi bir $b \in K$ için

$q(b)=\beta_0 b^m + \beta_1 b^{m-1} + \ldots + \beta_m \in K$ anlaşılacaktır.

Yukarıdaki tarif, bu durumda $a \in K$, F üzerinde cebirsel ise $p(x) \in F[x]$ polinomu a tarafından sağlanıyor, p(a) = 0 oluyor şeklinde tekrar verilebilir.

$F \subset K$ ve $a \in K$ olsun $\mathcal{M}$ de K nın hem F yi hem de a yı kapsayan bütün altcisimlerin ailesi olsun. Öncelikle $\mathcal{M} \neq \phi$ olduğuna ilgi çekilmelidir.

Gerçekten K nın kendisi $\mathcal{M}$ dedir. Verilen herhangi bir K cisminin bütün alt cisimlerinin kesişimi yine K nın bir alt cismi olduğundan, K nın bütün alt

cisimlerinin kesişimi de $\mathcal{M}$ ailesindedir ve de K nın bir alt cismidir. Bu alt cismi F(a) İle gösterelim.

Şimdi bu alt cismin özelliklerini araştıralım:

Öncelikle bu alt cisim $\mathcal{M}$ ailesinin bir elemanı olmakla hem F yi hem de a'yı kapsar. Ayrıca kesişimin tanımına göre $\mathcal{M}$ ailesinde bulunan K nın her alt cismide F(a) yı kapsar. F(a) nın kendisi $\mathcal{M}$ ailesindedir. Böylece F(a), K nın hem F hem de a yı kapsayan en küçük alt cismi olur ki buna "F ye a yı katmakla elde edilen cisim" denir.

Şimdi F(a) nın değişik bir inşaasını yapalım. K da $\beta_0+\beta_1a+...+\beta_sa^s$ biçiminde ifade edilebilen bütün elemanları gözönüne alalım. Burada β_i ler F den alınmış olup s>0 olan bir tamsayıdır. K nın elemanları olarak $\beta_0+\beta_1a+...+\beta_sa^s$ biçimindeki elemanlar sıfır olmamak kaydıyla diğerleri tarafından bölünebilir. Şimdi U bu şekildeki bölümlerin cümlesi olsun. $U\subset K$ dır. Öte yandan bu şekilde tanımlanan U hem F yi hem de a yı kapsar. O halde $F(a)\subset U$ dır.

Karşıt olarak, K nın hem F hem de a yı kapsayan herhangi bir alt cismi $\beta_i\in F$ olmak üzere $\beta_0+\beta_1a+...+\beta_sa^s$ elemanlarını da kapsaması gerekir. Şu halde F(a) bütün elemanları kapsamalıdır. Keza F(a) bu tür elemanların bölümlerini de kapsamalıdır. Böylece $F(a)\supset U$ olup U = F(a) elde edilir.

Bu yolla F(a) nın içe ait bir yapısını elde ettik, açıkçası U gibi.

Teorem 2: $a\in K$ elemanının F üzerinde cebirsel olması için $\Leftrightarrow$ F(a) nın F nin sonlu bir genişlemesi olmasıdır [10].

İspat: $\Leftarrow$) F(a), F nin sonlu bir genişlemesi ve [F(a):F]=m olduğunu farzedelim. $1,a,a^2,...,a^m$ elemanlarını göz önüne alalım. Bu elemanların hepsi F(a) dadırlar ve sayıları m+1 dir. Lineer cebirden bilinen bir sonuca göre bu elemanlar lineer bağımlıdır. Böylece $\alpha_0 1+\alpha_1a+...+\alpha_ma^m=0$ olacak şekilde hepsi birden sıfır olmayan $\alpha_0,\alpha_1,...,\alpha_m\in F$ elemanları bulundu. O halde cebirsellik tarifine göre a elemanı F de cebirseldir ve böylece de dercesi en fazla m=[F(a):F] olan F[x] deki $p(x)=\alpha_0+\alpha_1x+...+\alpha_mx^m$ polinomunu sağlar.

$\Rightarrow$) Bunun için $a \in K$ nın F üzerinde cebirsel olduğunu varsaydım. Bu kabule göre a, F[x] de sıfır olmayan herhangi bir polinomu sağlar. p(x) bu şarta uyan yani p(a)=0 olan en küçük pozitif dereceli bir polinom olsun, $p(x) \in F[x]$ şimdi p(x) in F üzerinde indirgenemez olduğunu iddia ediyoruz. Gerçekten f(x), $g(x) \in F[x]$ olmak üzere p(x) = f(x).g(x) ise, o takdirde 0 = p(a) = f(a).g(a) dır ve f(a) ve g(a) K nın elemanları olduğundan bunların çarpımının sıfır olması ya f(a) = 0 veya g(a) = 0 olmasını gerektirir. p(x) polinomu p(a) = 0 şartını sağlayan en küçük dereceli polinom olduğundan derf(x)≥der p(x) veya derg(x)≥derp(x) olmalıdır. Bu ise p(x) in indirgenemez olduğunu ispatlar.

Şimdi $\psi: F[x] \xrightarrow{\text{içine}} F(a)$ dönüşümünü $\forall h(x) \in F[x]$ için $h(x)\psi = h(a)$ olacak şekilde tanımlayalım. Bu ψ dönüşümü bir halka homomorfizmidir. Şimdi ψ nin çekirdeğini bulalım. ψ nin tanımına göre

$$\text{Ker}\psi = V = \{h(x) \in F[x] \mid h(a) = 0\}$$

dir. V, F[x] in bir idealidir. o halde p(x), V idealinin keza en küçük dereceli bir polinomu olacaktır. Halka teoriden bilinen bir sonuca göre de p(x) indirgenemez olduğundan V maksimal idealdir ve $V=\langle p(x) \rangle$ dir . Çünkü polinomlar halkası bir öklit halkasıdır. Yine halka teoriden bilinen bir sonuca göre F[x]/V bir cisimdir. Şu halde temel halka homomorfizmine göre

$F[x]/V \cong F[x]$ dir.

O halde F[x] in ψ altındaki görüntüsünün F(a) nın alt cismi olduğunu gösterdik. Bu görüntü $x\psi = a$ ve de $\forall \alpha \in F$ için $\alpha\psi = \alpha$ yı da kapsar. Şu halde, F[x] in ψ altındaki görüntüsü hem F hemde a yı kapsayan F(a) nın bir alt cismi olur. F(a) tanımına göre de ψ altında F[x] in görüntüsünün F(a) nın tamamı olduğu görülür.

$F[x]/V \cong F(a)$.

Artık $V=\langle p(x) \rangle$ ideal olup buradan F[x]/V nin F üzerinde bir vektör uzayı olarak boyutunun tam tanımına derp(x) olduğunu söyleyebiliriz.

$F[x]/V \cong F(a)$, olduğundan [F(a):F]=derp(x) olur. Böylece [F(a):F] kesinlikle sonludur ve teorem ispat edilmiş olur.

p(x) polinomu, a tarafından sağlanan en küçük dereceli F üzerinde bir polinom olsun. Böyle bir polinoma F üzerinde a nın minimal polinomu denir. Burada x in en büyük kuvvetinin katsayısının 1 olduğunu varsayabiliriz. Yani F üzerinde a nın minimal polinomunun monik polinom olduğunu kabul etmekle genelliği bozmamış oluruz.

F üzerinde a nın herhangi iki monik miminal polinomunun eşit olduğu kolaylıkla gösterilebilir. olsun. Şu halde $\alpha_i \in F$ olmak üzere

$$p(x) = x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n$$

olacaktır. Eğer a nın minimal polinomu p(x) ise, o takdirde

$p(a) = a^n + \alpha_1 a^{n-1} + \ldots + \alpha_n = 0$ olur. Dolayısı ile $a^n = -\alpha_1 a^{n-1} - \ldots - \alpha_n$ olur. a^{n+1} ise

$$a^{n+1} = -\alpha_1 a^n - \alpha_2 a^{n-1} - \ldots - \alpha_n a$$

olur. a^n değerini a^{n+1} yerine yazacak olursak a^{n+1} i F üzerinde $1, a, \ldots a^{n-1}$ elemanlarının lineer kombinasyonu olarak ifade edebiliriz. Böylece devam ederek herhangi bir $k \geq 0$ için a^{n+k} yı yine F üzerinde $1, a, \ldots, a^{n-1}$ lineer kombinasyonu olarak ifade edebiliriz.

Şimdi $T = \{\beta_0 + \beta_1 a + \ldots + \beta_{n-1} a^{n-1} \mid \beta_0, \beta_1, \ldots, \beta_{n-1} \in F\}$ cümlesini göz önüne alalım. T cümlesi açık olarak yukarıda yaptığımız açıklamalar gereği toplamaya göre kapalıdır. T cümlesi keza çarpmaya göre de kapalıdır. T nin halka olduğu açıktır. Fazla olarak T nin hem F yi hem a yı kapsadığı açıktır. Şimdi T cümlesinin bir cisim olduğunu gösterelim.

$0 \neq \beta_0 + \beta_1 a + \ldots + \beta_{n-1} a^{n-1} = u \in T$ olsun.

$h(x) = \beta_0 + \beta_1 x + \ldots + \beta_{n-1} x^{n-1} \in F[x]$ alalım. $u \neq 0$ olduğundan yukarıdaki uyarılarımıza göre $u = h(a)$ olduğundan $h(a) \neq 0$ ve dolayısıyla $p(x) \nmid h(x)$ elde ederiz. p(x) indirgenemez olduğundan p(x) ve h(x) aralarında asaldır. O halde $p(x).s(x) + h(x).t(x) = 1$ olacak şekilde $s(x), t(x) \in F[x]$ polinomları bulunabilir. Fakat bu durumda da $p(a)=0$ olduğundan

$$1 = p(a)s(a) + h(a)t(a) = h(a)t(a)$$

elde edilir. Buradan da u=h(a) yazacak olursak

$$1 = u.t(a)$$

elde edilir ki bu u nun tersinin t(a) olduğunu gösterir. t(a) ifadesinde a nın n-1 den daha büyük bütün kuvvetleri F üzerinde $1,a,...,a^{n-1}$ elemanlarının lineer kombinasyonları ile değiştirilebilir. Dolayısı ile $t(a)\in T$ olur. O halde T bir cisimdir. Öte yandan F ve a nın her ikiside T cümlesinde kapsandığından $F(a)\subset T$ dır. T nin tanımına göre $T\subset F(a)$ olduğu açıktır. Dolayısı ile T=F(a) elde edilir. Böylece F(a) yı $\beta_0+\beta_1a+...+\beta_{n-1}a^{n-1}$ elemanlarının cümlesi olarak görebiliriz.

Buna göre T, F üzerinde $1,a,...,a^{n-1}$ elemanları tarafından gerildğinden $[T:F]\leq n$ olur. Bununla beraber $1,a,...,a^{n-1}$ elemanları F üzerinde lineer bağımsızdırlar. Gerçekten $\gamma_i\in F$ olmak üzere $\gamma_0+\gamma_0a+...+\gamma_{n-1}a^{n-1}$ biçimindeki herhangi bir bağıntı bizi a nın derecesi n den daha küçük olan F üzerinde $\gamma_0+\gamma_0x+...+\gamma_{n-1}x^{n-1}$ polinomunu sağladığı sonucuna götürür. Bu çelişki ise $1,a,...,a^{n-1}$ in lineer bağımsız olduğunu ispatlar ve dolayısıyla bunların F üzerinde T nin bir bazı olduğu sonucuna varılır. Böylece [T:F]=n ve T=F(a) olduğundan [F(a):F] = n elde edilir. Böylece aşağıdaki teoremi ispat etmiş oluruz.

Teorem 3: Eğer $a\in K$ elemanı F üzerinde n inci dereceden cebirsel ise o takdirde [F(a):F]=n dir [9].

Teorem 4: a,b elemanları F üzerinde cebirsel ($a,b\in K$) olsun. Bu takdirde $a\pm b$, a.b, $a/b(b\neq 0)$ elemanları da F üzerinde cebirseldir. Yani F üzerinde cebirsel olan K nın elemanları K nın bir alt cismini oluştururlar.

İspat: a nın F üzerinde m. dereceden ve b nin de F üzerinde n inci dereceden cebirsel olduğunu varsayalım. O takdirde önceki teoreme göre K nın T=F(a) alt cisminin F üzerinde derecesi m olur. b nin F üzerinde n inci dereceden cebirsel olması F yi kapsayan T üzerinde derecesinin en fazla n olmasını gerektirir. Şu halde $W = T(b)\subset K$ alt cismi yine önceki teoreme göre, T üzerinde n. dereceden bir genişlemesi olacaktır. Ancak [W:F]=[W:T].[T:F] olduğundan $[W:F]\leq m.n$ ve böylece W nin F nin bir sonlu genişlemesi olduğu görülür. Bununla beraber $a,b\in W$

ise o takdirde a±b, a.b, a/b elemanları da W dedir. [W:F] sonlu olduğundan bu elemanlar F üzerinde cebirsel olmalıdır.

Burada biraz daha fazlasını da ispat etmiş olduk. [W:F]≤m.n olduğundan W nin her elemanı F üzerinde derecesi en fazla m.n olan bir polinomu sağlayacağından aşağıdaki teoremin ispat etmiş oluruz.

Sonuç: a,b∈K elemanları F üzerinde sırası ile m. ve n. dereceden cebirsel iseler o takdirde a±b, a.b, a/b(b≠0) elemanları F üzerinde en fazla mn. dereceden cebirseldirler.

Tarif 4: K, F nin genişlemesi olmak üzere eğer K nın her elemanı F üzerinde cebirsel ise o takdirde K ya F nin cebirsel genişlemesi denir [9].

Teorem 5: L, K nın cebirsel genişlemesi ve K dan F nin cebirsel genişlemesi ise L, F nin cebirsel genişlemesidir [9].

İspat: u∈L keyfi bir eleman, burada u nun katsayıları F de olan trivial olmayan (sabitten farklı) polinomu sağladığını gösterirsek teoremi ispat etmiş oluruz.

$\sigma_1,\sigma_2,\ldots,\sigma_n$ K da olmak üzere L, K nın cebirsel genişlemesi olduğundan bu u elemanı $x^n+\sigma_1x^{n-1}+\ldots+\sigma_n$ şeklindeki bir polinomu sağlayacaktır. Fakat hipoteze göre K, F üzerinde cebirsel olduğundan, önceki teoremlerin arka arkaya uygulanmasıyla $M=F(\sigma_1,\ldots,\sigma_n)$ bir sonlu genişlemesi olur, u bu defa katsayıları M üzerinde olan $x^n+\sigma_1x^{n-1}+\ldots+\sigma_n$ polinomunu sağladığından u M üzerinde n. dereceden cebirseldir. Bu bize M(u) nun M nin bir sonlu genişlemesi olduğu sonucunu verir. O halde [M(u):F]=[M(u):M].[M:F] olup buradan M(u) nun F nin sonlu bir genişlemesi olduğu sonucu çıkar. Bu ise u nun F üzerinde cebirsel olmasını gerektirir ki, u,L nin keyfi elemanı olduğundan L,F nin bir cebirsel genişlemesi olur.

Tarif 5: Herhangi bir kompleks sayı rasyonel sayılar cismi üzerinde, cebirsel ise o takdirde buna cebirsel sayı denir. Cebirsel olmayan sayılara da transandat sayılar denir.

3. BÖLÜM

POLİNİMLARIN KÖKLERİ HAKKINDA

Tarif 1: $p(x)\in F[x]$ olmak üzere F nin herhangi bir cisim genişlemesinde bulunan bir a elemanı için eğer $p(a)=0$ oluyorsa a ya p(x) bir kökü denir [11].

Lemma 1: $p(x)\in F[x]$ ve $F\subset K$ olsun. O takdirde herhangi bir $b\in K$ için $q(x)\in K[x]$ ve $derq(x)=derp(x)-1$ olmak üzere

$$p(x)=(n-b).q(x)+p(b) \text{ dir [9]}$$

İspat : $F\subset K$ olduğundan $F[x]\subset K[x]$ dir. Dolayısıyla, p(x) polinomu K[x] de bir eleman olacaktır. K[x] deki polinomlar için bölme algoritmasına göre $q(x)\in K[x]$ ve $r=0$ veya $der r<der(x-b)=1$ olmak üzere $p(x)=(x-b)q(x)+r$ yazılabilir. Şu halde ya $r=0$ yada $der r=0$ olmak zorundadır. her iki durumdada r, K nın bir elemanı olur. Acaba bu r, K daki hangi elemandır?

$p(x) = (x-b)q(x)+r$ olduğundan $p(b) = (b-b)q(b)+r \Rightarrow p(b) = r$

olur ki böylece $p(x) = (x-b)q(x)+p(b)$ elde edilir. Burada yine bölme algoritmasına göre $derq(x) = derp(x)-1$ olduğu açıktır.

Sonuç 1: $F\subset K$ olmak üzere $p(x)\in F[x]$ in bir kökü $a\in K$ ise o takdirde K[x] de $(x-a)|p(x)$ dir.

İspat : Lemma 1 e göre p(x) i K[x] de

$$p(x) = (x-a)q(x)+p(a) = (x-a)q(x),\ p(a)=0$$

biçiminde yazılabilir. Buradan $(x-a)|p(x)$ elde edilir.

Tarif 2: $p(x)\in F[x]$ in $a\in K$ kökü için $(x-a)^m \mid p(x)$ fakat $(x-a)^{m+1} \nmid p(x)$ oluyorsa a ya p(x) in m katlı kökü denir.

Lemma 2: Bir cisim üzerinde derecesi n olan bir polinomun bu cismin herhangi bir genişlemesinde en fazla n tane kökü vardır.

İspat: n üzerinde indüksiyon ile, eğer p(x) in derecesi 1 ise o takdirde α, β bir F cisminde ve $\alpha\neq 0$ olmak üzere $\alpha x+\beta$ şeklinde olacaktır. $p(a)=0$ olacak şekilde herhangi bir a için $\alpha a+\beta = 0 \Rightarrow a = -\frac{\beta}{\alpha}$ sonucu elde edilir. Bu durumda p(x) in

$-\frac{\beta}{\alpha}$ gibi bir tek kökü olup Lemma nın iddiasi kesinlikle doğrudur. Şimdi Lemma nın iddiasının herhangi bir cisimdeki derecesi n den daha küçük olan polinomlar için doğru olduğunu kabul ederek p(x) in F üzerindeki derecesinin n olduğunu varsayalım. F⊂K olsun. Eğer p(x) in K da hiçbir kökü yoksa o takdirde ispat bitmiştir. Çünkü K daki köklerin sayısı (ki bu 0 dir) en fazla n olur. Öyleyse p(x) in en az a gibi bir kökünün (K da bulunan) bulunduğunu ve bunun katlılığının olduğunu varsayalım. Katlı kök tanımına göre, $(x-a)^m|p(x)$ olup buradan m<n elde edilir. Buna göre $p(x)=(x-a)^m.q(x)$ yazılabilir. (q(x)∈K[x] derq(x)=n-m). $(x-a)^{m+1}\nmid p(x)$ gerçeğinden $(x-a)\nmid q(x)$ dir. Dolayısı ile önceki sonuca göre a,q(x) in bir kökü olamaz. Eğer b≠a K daki bir diğer kök ise zaman $0=p(b)=(b-a)^m q(b)$ bulunur. Öte yandan b-a≠0 ve biz cisimde hesap yaptığımıza göre q(b)=0 elde edilir. Bu ise p(x) in a dan farklı K daki herhangi bir kökünün q(x) in bir kökü olması demektir. q(x) in derecesi n-m<n olduğundan indiksiyon varsayımına göre q(x) in K da en fazla n-m tane kökü bulunmalıdır. Bunlar öteki kök a ile birlikte m defa sayılmış olur ki buda bize p(x) in en fazla m+(n-m)=n tane kökünün K da bulunacağını gösterir ki bu da lemmayı ispatlar.

Teorem 2: p(x) derecesi ≥1 ve F üzerinde indirgenemez olan F[x] in polinomu olsun. O takdirde F nin öyle bir E cisim genişlemesi vardır, p(x) in E de bir kökü vardır ve [E:F]=n dir.

İspat: F[x], F üzerinde x in polinomlar halkası ve V=<p(x)> de p(x) in doğurduğu F[x] in bir ideali olsun. V maksimal idealdir. Dolayısı ile yine bilinen bir teoreme görede E=F[x]/V, bu E cisminin teoreminin idiasını gerçeklediğini göstereceğiz. Öncelikle E nin F nin bir cisim genişlemesi olduğunu gösterelim. Bunun içinde E nin bir alt cisminin F ile özdeşleştirebileceğimizi göstermeye çalışıyoruz. E, F nin gerçekte cisim genişlemesi olmadığından bu yola sapıyoruz.

$\overline{F}=\{\alpha+V|\alpha\in F\}$ olmak üzere $\overline{F}$ nin F ye izomorf bir cisim olduğunu iddia ediyoruz. Böylece $\overline{F}$, F nin E deki görüntüsü olacaktır. $\psi:F[x]\to F[x]/V=E$

$\forall f(x)\in F[x]$ için $f(x)\psi=f(x)+V$ ile tanımlanmış bir dönüşüm ise ψ nin F ye kısıtlanışı F den $\bar{F}$ üzerine bir izomorfizm üretir.

Bu izomorfizmi kullanarak, yukarda sözünü ettiğimiz şekilde F ve $\bar{F}$ cisimlerini biribirleriyle özdeşleştirmiş oluruz. Böylece, E yi F nin bir cisim genişlemesi olarak gözönüne alabiliriz.

Şimdi, E nin F nin derecesi n=degp(x) olan sonlu bir genişlemesi olduğunu görelim. Geçekten.

$$1+V,\ x+V,\ (x+V)^2=x^2+V,\ldots,(x+V)^i=x^i+V,\ldots,(x+V)^{n-1}=x^{n-1}+V$$

E nin F üzerinde bir bazını oluşturur. Notasyonun uygunluğu bakımından E cismindeki $x\psi=x+V$ elemanını a olarak gösterelim. Yani $a = x + V$ olsun. Herhangi bir $f(x)\in F[x]$ için $f(x)\psi$ ninde adeta f(a) olduğunu iddia ediyoruz. Gerçekten ψ homomorfizm olduğundan, eğer

$$f(x)=\beta_0+\beta_1x+\ldots+\beta_kx^k \Rightarrow f(x)\psi=\beta_0\psi+(\beta_1\psi)(x\psi)+\ldots+(\beta_k\psi)(x\psi)^k$$

olup, burada yukarıda belirtilen $\beta\psi$ yerine β yı alma özdeşleştirmesini kullanarak $f(x)\psi=f(a)$ olduğu görülür. Özel olarak $p(x)\in V$ olduğundan $p(x)\psi=0$ dır. Dolayısı ile $p(x)\psi=p(a)$ dır. Şu halde E nin $a = x\psi$ elemanı p(x) in bir köküdür. Bu da ispatı tamamlar.

Sonuç 2: $f(x)\in F[x]$ ise F nin E gibi öyle bir cisim genişlemesi vardır ki f(x) in E de bir kökü vardır. Ayrıca $[E:F]\leq degf(x)$.

Teorem 3: $f(x)\in F[x]$ derecesi ≥ 1 olan bir polinom olsun. Bu takdirde F nin derecesi en fazla n! olan ve f(x) in bütün köklerinin bulunduğu (katlılıkları dahil) bir E cisim genişlemesi vardır.

İspat: Teoremin ifadesinde katlılığı m olan bir kökü m tane kök olarak sayacağız. Yukarıdaki sonuca göre F nin $[E_0:F]\leq n$ ve f(x) in α gibi bir kökünün bulunduğu E_0 cisim genişlemesi vardır. Şu halde $E_0[x]$ de f(x) i, q(x) derecesi n-1 olan bir polinom olmak üzere $f(x)=(x-\alpha).q(x)$ biçiminde çarpanlara ayırabiliriz. Böyle devam ederek E_0 ın derecesi en fazla (n-1)! olan ve q(x) in (n-1) kökünün bulunduğu bir cisim genişlemesi vardır. f(x) in herhangi bir kökü ya α ya da q(x) in

bir kökü olduğundan f(x) in E deki n kökünün tamamını elde etmiş oluruz. Buradan $[E:F]=[E:E_0].[E_0:F]<n.(n-1)! = n!$ bulunur ki bu da ispatı tamamlar.

Teorem 3, F üzerinde derecesi n olarak verilen bir f(x) polinomunun n tane kökünün bulunduğu F nin E gibi bir sonlu genişlemesinin varlığını gösterir. Eğer $f(x)=a_0.x^n+a_1x^{n-1}+...+a_n$, $a_0\neq0$ ve bununE deki n tane kökü $\alpha_1,\alpha_2,...,\alpha_n$ ise lemma 1 i kullanarak f(x) polinomu E üzerinde $f(x)=a_0(x-\alpha_1)...(x-\alpha_n)$ şeklinde çarpanlara ayırabiliriz. Şu halde f(x) E üzerinde lineer çarpanların çarpımı olacak biçimde parçalanabilir. F ile E arasında $f(x)\in F[x]$ in lineer çarpanlara ayırabildiği başka bir cisim yoksa o zaman bununla ilgili olarak aşağıdaki tarifi verebiliriz.

Tarif 3: F bir cisim, E onun sonlu genişlemesi olsun. Eğer $f(x)\in F[x]$ polinomunun lineer çarpanların çarpımı olarak parçalanabildiği E nin F yi kapsayan herhangi bir alt cismi yoksa o takdirde E ye f(x) in F üzerinde parçalanış cismi denir.

NOT: Teorem 3, parçalanış cisminin varlığını garanti eder.

Gerçekten bu teorem; F üzerinde derecesi n olan bir polinom verildiğinde bu f(x) polinomunun n kökünün tamamının bulunduğu ve F üzerinde derecesi en fazla n! olan F nin bir genişlemesinin bulunduğunu ifade eder. Daha sonra n! in gerçekten bir üst sınır olduğunu yani verilen bir n için F üzerinde derecesi n olan f(x) polinomunun parçalanış cisminin F üzerindeki derecesinin n! olacak şekilde bir F cismi ile derecesi n olan $f(x)\in F[x]$ polinomunun bulunabileceğini göstereceğiz.

Yukarıdaki bu tanım aşağıdaki vereceğimiz ifadeye denktir.

F bir cisim ve f(x) de derecesi n olan F[x] in bir polinomu olsun. Eğer E f(x) in n kökünün tamamının bulunduğu F nin en küçük genişlemesi ise, o takdirde E ye F üzerinde f(x) in parçalanış cismi denir.

Bu aşamada aklımıza derhal şöyle bir soru gelir. F[x] in f(x) polinomunun E_1 ve E_2 gibi iki parçalanmış cismi verildiğinde bunlar arasındaki ilişki nedir? Kabaca bunların bütünüyle birbirlerine bağlı olduklarını kabul etmek için hiç bir hakkımız yoktur. Biraz sonraki gözlemlerimiz bunların gerçekten

biribirine bağlı olduğunu gösterecektir. Bu şekilde ki E_1 ve E_2 gibi iki parçalanış cismi F nin her elemanını sabit bırakan bir izomorfizmle birbirlerine izomorfdurlar.

Tarif 4: F ve F′ iki cisim τ da F den F′ üzerine bir izomorfizm olsun. Uygunluk için herhangi bir $\alpha \in F$ elemanının τ altındaki görüntüsünü α' ile gösterelim. O halde $\alpha\tau = \alpha'$ dür.

Şimdi acaba F ve F′ cisimleri arasında yukarıda verdiğimiz τ izomorfizmini F[x] ve F′[t] polinom halkaları arasında bir izomorfizm tesis edebilmek için kullanabilirmiyiz?

$$f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n \in F[x]$$

polinomu için τ^* dönüşümünü

$$f(x)\tau^* = (\alpha_0 x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n)\tau^* = \alpha_0' t^n + \alpha_1' t^{n-1} + \ldots + \alpha_n' \in F'[t]$$

şeklinde tanımlayalım.

Bu takdirde aşağıdaki lemmayı ispatsız olarak verebiliriz.

Lemma 3: Yukarıda sözünü ettiğimiz τ^* dönüşümü $\forall \alpha \in F$ için $\alpha\tau^* = \alpha'$ özelliği ile F[x] den F′[t] üzerine bir izomorfizmdir.

Eğer $f(x) \in F[x]$ ise o takdirde $f(x)\tau^*$, $f'(t)$ olarak yazacağız. Bu durumda Lemma 3 den derhal f(x) in F[x] deki parçalanışının f′(t) nin F′[t] deki parçalanışı ile aynı olduğunu veya bunun tersinin de doğru olduğu sonucunu çıkarabilirz. Buradan özel olarak; f(x) in F[x] de indirgenemez olması için gerek ve yeter şartın f′(t) nin de F′[t] de indirgenemez olmasıdır sonucunu çıkarabiliriz. Bununla beraber burada özel olarak polinom halkaları ile değil daha ziyade F nin genişlemeleri ile ilgileneceğiz. Gerçektin F nin uygun bir genişlemesinin elde etmek için polinom halkalarının bölüm halkalarını kullandığımızı hatırlayalım. Sonuç olarak $\langle f(x) \rangle$ ve $\langle f'(t) \rangle$ sırası ile F[x] ve F′[t] halkalarında f(x) ve f′(t) polinomlarının ürettiği idealler olmak üzere $F[x]/\langle f(x) \rangle$ ve $F'[x]/\langle f'(x) \rangle$ arasında mevcut bağıntı üzerinde çalışmak bizim için yerinde olacaktır.

Lemma 4: $\forall \alpha \in F$ için $\alpha\tau^{**} = \alpha'$ olacak biçimde

$$\tau^{**}: F[x]/\langle f(x) \rangle \xrightarrow{\text{üzerine}} F'[t]/\langle f'(t) \rangle$$ bir izomorfizm vardır.

İspat: İspata tam olarak başlamadan önce lemmanın son kısmındaki ifade ile neyin kastedildiğini açıklığa kavuşturmalıyız. Daha önce birçok defalar yaptığımız gibi F cismini; $\alpha \in F$ elemanını $F[x]/\langle f(x)\rangle$ in $\alpha+\langle f(x)\rangle$ kalan sınıfı ile özdeşliyerek $F[x]/\langle f(x)\rangle$ in içine yayılmış olarak gözönüne alabiliriz. Benzer şekilde F' cisminide $F'[t]/\langle f'(t)\rangle$ içinde kapsanmış olarak gözönüne alabiliriz. Bu durumda τ^{**} izomorfizminin $[\alpha+\langle f(x)\rangle]\tau^{**}=\alpha'+f'(t)$ eşitliğini sağladığını var sayabiliriz. Şimdi

$$\tau^{**}: F[x]/\langle f(x)\rangle \to F'[t]/\langle f'(t)\rangle$$

şeklinde bir izomorfizm arıyoruz. $\forall \rho(x) \in F[x]$ için

$$[\rho(x)+\langle f(x)\rangle]\tau^{**} = \rho'(t)+\langle f'(t)\rangle$$

şeklinde tanımlanan dönüşümün iyi tanımlı olduğu ve $F[x]/\langle f(x)\rangle$ den $F'[t]/\langle f'(t)\rangle$ üzerine bir izomorfizm olduğu kolaylıkla gerçeklenir.

Not: Parçalanış cisminin tekliğinin ispatı için aşağıdaki teoremi önceki Lemma dan ispatlayabiliriz.

Teorem 4: $p(x)$, $F[x]$ de indirgenemez ve v de $p(x)$ in bir kökü olsun. Bu takdirde ω, $p'(t)$ nin bir kökü olmak üzere $F(v) \cong F'(\omega)$ dir. Bundan başka bu σ izomorfizmi $v.\sigma = \omega$, $\forall \alpha \in F$ için $\alpha.\sigma = \alpha'$ olacak şekilde seçilebilir.

İspat: v, $p(x)$ indirgenemez polinomunun F nin K genişlemesindeki bir kökü olsun. $M = \{f(x) \in F[x] \mid f(v) = 0\}$ olsun. Aşikar olarak M, $F[x]$ in bir ideali ve $M \neq F[x]$ dir. $p(x) \in M$ ve $p(x)$ indirgenemez olduğundan $M = \langle p(x)\rangle$ yazarız. $\psi: F[x] \to F(v)$ dönüşümünü $F(v) < K$ içine $\forall q(x) \in F[x]$ için $\psi(q(x)) = q(v)$ olarak tanımlayalım. Kolayca görürüz ki ψ üzerinedir. Yine ψ nin çekirdeği M dir. Halkalar için temel homomorfizmden

$$\psi^*: F[x]/\langle f(x)\rangle \xrightarrow{\text{üzerine}} F(v)$$

bir izomorfizmdir.

$p(x)$, $F[x]$ de indirgenemez olduğundan $p'(t)$ de $F'(t)$ de indirgenemez ve bir θ^*, F' nün her elemanını sabit bırakan ve $\theta^*[t+\langle p'(t)\rangle]=w$ olan (w, $p'(t)$ nin bir kökü), $F[t]/\langle p'(t)\rangle \xrightarrow{\text{üzerine}} F'(w)$ bir izomorfizmdir.

Şimdi teoremin ispatı için parçaları birleştirilim. Lemma 4 den $x+<p(x)>$ i $t+<p'(t)>$ ye dönüştüren ve F de τ ile uyuşan $F[x]/<p(x)>$ i $F'[t]/<p'(t)>$ ye dönüştüren bir τ^{**} izomorfizmi vardır. Şimdi

$$\sigma = (\psi^*)^{-1}\tau^{**}\theta^*$$

olan $F(v) \xrightarrow{(\psi^*)^{-1}} F[x]/<p(x)> \xrightarrow{\tau^{**}} F'(t)/<p'(t)> \xrightarrow{\theta^*} F'(\omega)$ den hareketle)

$F(v)$ den $F'(\omega)$ üzerine dönüşümünü gözönüne alalım. Bu bütün ψ^*, τ^{**} ve θ^* dönüşümleri izomorfizm ve üzerine olduğundan $F(v) \xrightarrow{\text{üzerine}} F'(w)$ bir izomorfizmdir. Ayrıca,

$$v = \psi^*[x+<p(x)>]$$

$$(v)\sigma=(v)(\psi^*)^{-1}\tau^{**}\theta^*$$

$$= ([x+<p(x)>]\tau^{**})\theta^*$$

$$= (t+<p'(x)>)\theta^*$$

$$= w$$

dir. $\alpha \in F$ içinde $\alpha\sigma = (\alpha(\psi^*)^{-1}\tau^{**}\theta^* = (\alpha\tau^{**})\theta^* = \alpha'\theta^* = \alpha'$ dir. O halde, σ nın teoremi ifadesindeki izomorfizm için gerekli bütün şartları sağladığını gösterdik.

Sonuç: $p(x) \in F[x]$ indirgenemez ve a, b, $p(x)$ in iki kökü ise $F(a) \cong F(b)$ dir. Buradaki izomorfizm, F nin her elemanını sabit bırakıp a yı b ye dönüştüren bir izomorfizmdir.

Teorem 5: E ve E′ sırasıyla $f(x) \in F[x]$ ve $f'(t) \in F'[t]$ polinomlarının iki parçalanış cismi her $\alpha \in F$ için $\alpha\phi=\alpha'$ özelliğini sağlayan bir izomorfizmi ile izomorfiktirler. Yani $E \cong E'$ dür. (Özel olarak verilen bir F cismi üzerinde aynı polinomun herhangi iki parçalanış cismi F nin bütün elemanlarını sabit bırakan bir izomorfizmle izomorfiktirler).

İspat: Bu ispat içinde tümevarım metodunu kullanalım. Bunun için belli bir metodla arttırılabilen veya azaltılabilen bir indikatöre ihtiyacımız var. İndikatör olarak, ilk cisim üzerinde bir parçalanış cisminin derecesini kullanacağız. Bu yapay gibi görünebilir, fakat göreceğimiz gibi biz bunu kullanacağız.

[E:F]=1 ise E=F dir. Yani f(x), F nin kendi üzerinde çarpanlara ayrılmıştır. Lemma 3 den $f'(t)$ de $F'=E'$ üzerinde lineer çarpanlara ayrılmıştır. Fakat $\phi=\tau$, F üzerinde τ ya karşılık gelen E den E' üzerine izomorfizm ile gösterilir.

Herhangi bir F_0 cismi için bu sonucun doğruluğunu kabul edelim ve herhangi bir $f(x)\in F_0[x]$ polinomu F_0 üzerinde derecesi n den küçük olan f(x) in bir E_0 parçalanış cisminin derecesini sağlar. Yani $[E_0:F_0]<n$ dir.

Kabul edelim ki [E:F]=n>1 olsun. Burada E, F üzerinde f(x) in parçalanış cismidir. n>1 olduğundan f(x), r>1 dereceli p(x) indirgenemez çarpanına sahiptir. $p'(t)$, $f'(t)$ nin indirgenemez çarpanı olsun. E, f(x) in parçalanış cismi olduğundan f(x) in köklerinin tamamı ve p(x) in köklerinin biri E dedir. Böylece p(v)=0 olacak şekilde $v\in E$ vardır. Buradan [F(v):F]=r dir. Benzer şekilde, $p'(w)=0$, olacak şekilde bir $w\in E'$ vardır. Teorem 4 den $\forall\alpha\in F$ için $\alpha\sigma=\alpha'$ özelliğini sağlayan σ, F(v) den $F'(w)$ üzerine bir izomorfizmdir.

$$[F(v):F]=r>1 \text{ olduğundan } [E:F(v)]=\frac{[E:F]}{[F(v):F]}=\frac{n}{r}<n.$$

İddiamız E nin bir alt cismi olmayan F_0 ı kapsayan $F_0=F(v)$ üzerinde bir polinom olarak alının f(x) için E nin bir parçalanış cismi olduğudur ve E, F üzerinde f(x) in bir parçalanış cismi kabul edildiğinden F, f(x) in bir parçalanışı (ayrılışı) olabilir. Benzer şekilde, E', $F_0'=F'(w)$ üzerinde $f'(t)$ için bir parçalanış cismidir. Bizim tümevarım hipotezimizden $a\phi=a\sigma(\forall a\in F_0)$ olacak şekilde $\phi:E\xrightarrow{\text{üzerine}}E'$ izomorfizmi vardır. Fakat $\forall\alpha\in F$ için $\alpha\sigma=\alpha'$ olup, $\forall\alpha\in F\subset F_0$ için $\alpha\phi=\alpha\sigma=\alpha'$ olup bu da ispatı tamamlar.

$F=F'$ ve τ her $\alpha\in F$ için $\alpha\tau=\alpha$ özdeşlik dönüşümü olsun. Kabul edelim ki, E_1 ve E_2, $f(x)\in F[x]$ in iki parçalanış cismi olsunlar. $E_1=E\supset F$ ve $E_2=E'\supset F'=F$ gözönüne alalım ve hemen teoremin iddiasını uygularsak E_1 ve E_2 nin, F nin her elemanını sabit bırakan bir izomorfizm ile izomorf oldukları çıkar.

Gerçekten, F üzerinde aynı bir polinomun iki parçalanış cismi izomorfiktir ve bu izomorfizm F nin her elemanını sabit bırakır.

4. BÖLÜM

PERİYODU VERİLEN EN KÜÇÜK MATRİS

1. GİRİŞ

$o < k < n$ ve A düzenli bir matris olmak üzere eğer $A^k \neq I$ ve $A^n = I$ ise A nın periyodu n dir. Bu bölümde elemanları K cisminden alınan ve periyodu n olan r x r tipinde bir matris mevcut olacak şekilde ve r(n) ile göstereceğimiz en küçük r sayısı araştırılacaktır.

Tahmin edilebileceği gibi r(n) nin hesaplanması A nın R halkasından alınan elemanlarına bağlıdır. Eğer $z^n = 1$ ve $1 \leq m < n$ için $z^m \neq 1$ ise z kompleks sayısı birimin n. mertebeden ilkel köküdür. Dolayısıyle $e^{2\pi i/3}$ birimin pirimitif küp köküdür. Herhangi bir $n \geq 1$ sayısı için z birimin n. mertebeden ilkel kökü olsun. Bu takdirde periyodu n olan [z] matrisinin minimum boyutu yani r(n) = 1 dir.

1x1 tipindeki [1] matrisinin periyodu 1, [-1] ise 2 dir. Birimin k. mertebeden ilkel kökleri $k > 2$ için kompleks olduğundan 1x1 tipindeki hiçbir matrisin mertebesi 2 den daha büyük olamaz. O halde $R = \mathbb{R}$ ise $r(n) = \begin{cases} 1 & n = 1,2 \\ 2 & n \geq 3 \end{cases}$ dir.

Q rasyonel sayılar cismi ve Q[x] rasyonel katsayılı polinomlar halkası olsun. A elemanları Q dan alınan k x k tipinde bir matris olsun. Bu takdirde Cayley-Hamilton teoreminden A, $c(x) = |A - xI| = 0$ karakteristik polinomunu sağlar ve $c(x) \in Q[x]$ dir. A matrisinin minimum polinomu m(x) ise $m(x) \mid c(x)$ ve c(x) in derecesi A matrisinin boyutu olduğundan, A matrisinin boyutu minimum polinomunun derecesinden daha küçük olamaz.

A matrisinin periyodunun n olduğunu farzedelim. A, $x^n - 1$ polinomunu sağladığından $m(x) \mid x^n - 1$ dir. m(x) polinomunun özelliklerini ortaya koymak için $x^n - 1$ in, n nin her bir k böleni için cyclotomic polinomların $\prod c_k(x)$ biçimindeki çarpanlara ayrılışını göz önünde bulundurmalıyız.

k. cyclotomic polinom, kökleri tam olarak birimin k. mertebeden ilkel kökleri olan $c_k(x)$ polinomudur. Daha önceki bölümde gösterildiği gibi birimin k. mertebeden tam tamına $\varphi(k)$ tane pirimitif kökü vardır. Böylece

$$c_k(x) = \prod_{j=1}^{k-1} \left(x - e^{j2\pi i/k}\right) \quad (j,k) = 1$$

polinomunun derecesi $\varphi(k)$ olur. Üstelik $c_k(x)$ rasyonel sayılar cisminde indirgenemeyen, tam katsayılı monik bir polinomdur.

Ayrıca $t = 1,2,...,k-1$ için $c_t(x)$ biliniyor ise bu takdirde $c_k(x) = \dfrac{x^k - 1}{\prod_{d|k} c_d(x)}$ $d < k$ biçiminde de ifade edilebilir. $m(x) \mid x^n - 1 = \prod_{k|n} c_k(x)$ ve her bir $c_k(x)$ Q[x] de indirgenemez olduğundan

$$m(x) = c_{d_1}(x)...c_{d_k}(x) \qquad (d_t|n,\ t = 1,2,...,k)$$

yazılır. $d_1, d_2, ..., d_k$ nın en küçük ortak katı r olsun. Açık olarak $r \le n$ dir. Her bir d_i $(1 \le i \le k)$ r nin bir böleni ve $x^r - 1 = \prod_{k|r} c_k(x)$ olduğundan

$$x^r - 1 = m(x) \prod_{j|r} c_j(x) \qquad j \notin \{d_1,...,d_k\}$$

olur. Özellikle $m(x) \mid x^r - 1$ ve böylece $A^r = I$ dır. O halde r = n olup, m(x) in çarpanları indislerinin en küçük ortak katı n olacak biçimde seçilmek zorundadır. Bu şekildeki çarpımlar arasında, periyodu n olarak verilen ve aradığımız A matrisi için m(x) gibi minumum polinom olabilecek bir veya daha çok minumum dereceli polinom olacaktır. m(x) çarpanlarının indislerinin en küçük ortak katı n olan en küçük dereceli polinom olduğundan, $\deg m(x) \le \deg c_n(x) = \varphi(n)$ olur.

Minimum polinomu $m(x) = a_0 + a_1x + ,..., a_{k-}x^{k-1} + x^k$ olan bir matris

$$C = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ -a_0 & -a_1 & -a_2 & \dots & -a_{k-1} \end{bmatrix}$$

formundadır. Bu matrise m(x) in band matrisi denir. c kendi minimum polinomu m(x) sağladığından $c^n = I$ ve $t < n$ için $c^t \neq I$ dir. Böylece c nin periyodu (mertebesi) n dir. Ayrıca c nin boyutu minimumdur. Çünkü c nin boyutu minimum polinomu m(x) in derecesine eşittir. Dolayısıyle m(x) in mümkün olan her seçimi için c band matrisinin periyodu n ve minimum boyutu $r(n) \leq \varphi(n)$ dir.

Yukarıdaki metodla verilen her bir n için minimum boyutta n. mertebeden bütün matrisleri oluşturamayacağımıza dikkat edilmelidir. Sözgelimi, $\begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}$ yukardaki metodla elde edilen 3. mertebeden minimum boyuttaki matristir.

Halbuki $\begin{bmatrix} -\frac{2}{3} & 7/3 \\ -1/3 & -\frac{1}{3} \end{bmatrix}$ de minimum boyutta 3. mertebeden bir matris ama band matris değildir.

Örnek: Mertebesi (periyodu) 30 olan minimum boyuttaki matrisi bulalım:

$$x^{30} - 1 = c_1(x)c_2(x)c_3(x)c_5(x)c_6(x)c_{10}(x)c_{15}(x)c_{30}(x)$$

m(x) için mümkün çarpımlar ve dereceleri:

$c_{30}(x)$, derecesi 8,		$c_1(x)c_5(x)c_6(x)$, derecesi	7,
$c_1(x)c_{30}(x)$, derecesi 9,		$c_5(x)c_6(x)$, "	6,
$c_2(x)c_3(x)c_5(x)$ derecesi 7,		$c_3(x)c_{10}(x)$ "	6,
$c_6(x).c_{10}(x)$, derecesi 6.			

$m(x) = c_5(x)c_6(x)$ olarak alalım. ($c_3(x)c_{10}(x)$ çarpımı ile de çalışılabilir).

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

$$= x^6 + ox^5 + x^4 + x^3 + x^2 + ox + 1$$

Band matris $A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ -1 & 0 & -1 & -1 & -1 & 0 \end{bmatrix}$

Tamsayılar halkasında çalışıldığı zaman cyclotomic polinomlar tam katsayılı olduğundan rasyonel sayılarda elde edilen sonuçlar elde edilir. Yani

$d(n) = \min \left\{ \sum_{j \in} \varphi(j) : ekok(J) = n \right\}$ olmak üzere (Burada J pozitif tamsayıların sonlu bir cümlesidir) $r(n) = d(n)$ dir.

C, R, Q ve Z nin her biri birer tek çarpanlama bölgesi olduğu biliniyor. Bölümün 2. kısmı R nin herhangi bir tek çarpanlama bölgesi olması durumunda $c_j(x)$ in indirgenemez çarpanlarının ortak $\theta(j)$ dereceleri cinsinden r(n) nin hesaplanması ile ilgilidir.

2. r(n) NİN HESAPLANMASI

A, elemanları bir R tek çarpanlama bölgesinden alınan bir matris ve $f(x) \in R[x]$ olsun. Eğer $A^n = I$ olacak şekilde herhangi bir n varsa A nın periyodu en küçük pozitif n tamsayısıdır. Eğer $f(x) \mid x^n - 1$ olacak şekilde herhangi bir n varsa f(x) in üssü en küçük pozitif n tamsayısıdır. Bu tariflerden derhal A nın periyodunun (mertebesinin) n olması için gerek ve yeter şartın $m_A(x)$ minimum polinomunun üssünün n olması elde edilir. (Çünkü $f_A(x) = \det(xI-A)$ karekteristik polinomu R[x] de moniktir ve A nın $m_A(x)$ minimum polinomu R nin, K kesirler cismi üzerinde de moniktir ve $f_A(x)$ i böler.)

R[x] de derecesi r olan herhangi bir m(x) monik polinomu verildiğinde bunun r x r band matrisi, bütün m(x) minimum polinomları arasında en küçük r

büyüklüğüne sahiptir. Bundan dolayı, r(n) n üssüne sahip bir polinomun en küçük derecesidir; yani, r(n) herhangi bir $k < n$ için $x^k - 1$ in bir böleni olmayan, $x^n - 1$ in bir böleninin en küçük derecesidir.

Açıkca, R[x] üzerinde $x^n - 1$ in çarpanlara ayrılışı ile ilgileniyoruz. Gauss lammasından aralarında ilgililik hariç, çarpanlama K[x] de olduğu gibi R[x] de de aynıdır. Dolayısıyle, K üzerinde çalışma genelliği bozmaz.

Kar(K), K nın karakteristiğini göstersin. Eğer $kar(K) \nmid n$ ise bu takdirde n nin her d böleni için K nın bir genişletilmiş cisminde birimin d. mertebeden ilkel kökü vardır ve $x^n - 1$ polinomu $\prod_{d|n} c_d(x)$ şeklinde çarpanlara ayrılır. Burada, çarpım birimin bütün d. inci mertebeden a ilkel kökleri üzerinde yapılmak üzere $c_d(x)$ d. inci $\prod(x - a)$ cyclotomic polinomdur.

LEMMA 1: K bir cisim, n, $kar(K) \nmid n$ olacak biçimde bir pozitif tamsayı olsun ve $c_n(x)$ nin K[x] deki indirgenemez g_i çarpanlarına bir çarpanlaşının

$$c_n(x) = \prod g_i(x)$$

olduğunu varsayalım. Bu takdirde gi lerin hepsinin derecesi aynıdır.

İSPAT: F, K üzerinde g_i polinomlarının parçalanış cismi olsun. F, gi nin sıfırlarını kapsadığından birimin bir n. mertebeden pirimitif kökünü ihtiva eder. Dolayısıyle, F birimin bütün n. mertebeden pirimitif köklerini kapsar, böylece F, $x^n - 1$ in parçalanış cismi olur. Şu halde $\deg(g_i) = [F:K]$ i den bağımsızdır.

$\theta_K(n)$, K[x] deki $c_n(x)$ in indirgenemez çarpanlarının ortak derecesini göstersin [üzerinde çalıştığımız K cisminin vurgulanmasına ihtiyaç duyulması durumuna göre $\theta_K(n)$ ve $\theta(n)$ gösterimlerini birbirlerinin yerine kullanacağız.]

Teorem 2: Eğer K bir cisim ve n, $kar(K) \nmid n$ olacak şekilde bir tamsayı ise, bu takdirde

$$r(n) = \min\left\{\sum_{j\in J}\theta(j) : \text{ekok}(J) = n\right\}$$

dir.

K nın karekteristiği m yi böldüğü zaman r(m) nin hesaplanması o kadar açık değildir.

$\theta(n) = 1$ ise $\delta(n) = 0$ ve diğer durumlarda $\delta(n) = 1$ olsun.

Teorem 3: K karakteristiği pozitif p olan bir cisim ve n, $p \nmid n$ olacak şekilde bir pozitif tamsayı olsun. Bu takdirde, herhangi bir pozitif k tamsayısı için

$$r(np^k) = r(n) + p^{k-1} + \delta(n)$$

dir.

İspat: Aşağıda pek çok yerde herhangi u, $v \in K[x]$ ve p nin herhangi bir r. inci kuvvet için

$$(u+v)^r = u^r + v^r$$

gerçeğini kullanacağız.

Eğer $\theta(n) > 1$ ise bu takdirde f(x), derecesi r(n) ve üssü n olan bir polinom olmak üzere

$$m(x) = \left[(x-1)^{p^k-1}+1\right]f(x)$$

olsun. Diğer yandan, eğer $\theta(n) = 1$ ise bu takdirde $a \in K$ elemanı birimin n. inci mertebeden ilkel kökü ve $m(x) = (x-a)^{p^k-1}+1$ olsun. Her iki durumda da m(x) in derecesinin $r(n)+p^{k-1}+\delta(n)$ ve üssünün np^k olduğu açıktır. Bu suretle $r(np^k) \le r(n) + p^{k-1} + \delta(n)$ olduğu ispatlanır.

Karşıt eşitsizlik için m(x) in üssü np^k olan herhangi bir polinom olduğunu varsayalım. $\deg(m) \ge r(n) + p^{k-1} + \delta(n)$ olduğunu göstermeliyiz.

Her $e_j > 0$ olmak üzere m(x) in farklı indirgenemez g_j polinomların kuvvetlerine bir çarpanlanışı $m(x) = \prod g_j^{e_j}$ olsun. f(x) i de, $\prod g_j$ olarak tanımlayalım.

$m(x) \mid (x^{np^k}-1)$ ve $x^{np^k}-1 = (x^n-1)^{p^k}$ olduğundan her bir g_j, x^n-1 in bir bölenidir. Sonuç olarak, her bir $e_j \le p^k$ ve $f(x) \mid x^n-1$ dir. Tartışma açık olarak, $J(f) = \{d \in IN : e.b.o.b(f, c_d) \ne 1\}$ olmak üzere f nin üssünün L=e.k.o.k (J(f))

olduğunu gösterir. Şu halde $m(x) \mid f(x)^{p^k} \mid x^{Lp^k} - 1$ öyle ki $Lp^k \geq np^k$ dolayısıyle $L \geq n$ dir. Böylece f nin üssü $L = n$ olup $r(n) \leq \deg(f)$ olur.

Eğer her bir $e_j \leq p^{k-1}$ ise, bu takdirde $m(x) \mid (x^n - 1)^{p^{k-1}}$ olup, bu bir çelişkidir. Dolayısıyla $e_{j^*} > p^{k-1}$ olacak şekilde bir j^* indisi mevcuttur. Böylece $\deg(m) \geq \deg(f) + p^{k-1} \cdot \deg(g_{j^*}) \geq r(n) + p^{k-1}$ dir.

Eğer $\delta(n) = 0$ ise ispat tamamdır. Onun için $\delta(n) = 1$ farzedelim. Yukarıda $\deg(m) \geq \deg(f) + p^{k-1} \cdot \deg(g_{j^*})$ olduğunu gördük. İspatı tamamlamak için ya $\deg(f) > r(n)$ ya da $\deg(g_{j^*}) > 1$ olduğunu göstermek kafidir. Bunu sona erdirmek için

$$\mathcal{L}(n) = \left\{ J \subset \mathbb{N} : e.k.o.k(J) = n \text{ ve } \sum_{j \in J} \theta(j) = r(n) \right\}$$

olsun.

LEMMA 4: n, $kar(K) \nmid n$ olacak biçimde pozitif bir tamsayı olsun. O zaman $\theta(j)=1$ olacak şekilde bir $J \in \mathcal{L}(n)$ ve $j \in J$ olmasıdır.

$\deg(g_{j^*}) = 1$ olduğunu farzedelim. $g_{j^*} \mid f$ ve f nin üssü n olduğundan $\theta(n) > 1$ olup bu da Lemma 4 den $J(f) \notin \mathcal{L}(n)$ olmasını gerektirir. Böylece $\deg(f) > r(n)$ olur ki bu da istenendir. Şu halde Lemma 4 ispatlanınca teorem 3 ispatlanmış olacaktır.

Lemma 4 ve 5 in ispatında aşağıda ifade edilen gerçekleri kullanacağız:

Eğer $kar(K) \nmid rs$ ise bu takdirde

$$\theta(r) \mid \theta(rs) \qquad (1)$$

ve ebob $(r,s) = 1$ ise $\theta(rs) \mid \theta(r)\,\theta(s)$ (2) dir.

Lemma 4 ün ispatı: Eğer $\theta(n) = 1$ ve $j \mid n$ ise bu takdirde (1) den $\theta(j) \mid \theta(n)$ ve buradan $\theta(j) = 1$ elde edilir.Sonuç olarak eğer $j \in J$ ve $J \in \mathcal{L}(n)$ ise $j \mid n$ ve böylece $\theta(j) = 1$ dir. [Gerçekten $\theta(n) = 1$ olduğu zaman $r(n) = 1$, $\mathcal{L}(n) = \{(n)\}$ dir.]

$J \in \mathcal{L}(n)$ seçilmiş olsun, şöyle ki $\theta(j) = 1$ olacak şekilde bir $j \in J$ vardır ve böylece J ler arasında öyleleri vardır ki $\sum_{i \in J} t$ istenildiği kadar küçültülebilir.

İlk olarak her $i \in J$ için $\theta(i) = 1$ olduğunu göstereceğiz. Bir çelişkiye varmak için bazı i' ler için $\theta(i) > 1$ olduğunu varsayalım. Eğer (i, j) = 1 ise bu takdirde $J' = (J \setminus \{i,j\}) \cup \{i,j\}$ olsun. Açık olarak ekok (J') = ekok(J) = n dir. Üstelik (1) ve (2) den $\theta(i) \mid \theta(ij) \mid \theta(i)\,\theta(j)$ olup, $\theta(j) = 1$ olduğu için $\theta(ij) = \theta(i)$ olur. Dolayısıyla $\sum_{t \in J'} \theta(t) = \sum_{t \in J} \theta(t) - 1$ olup bu $J \in \mathcal{Y}(n)$ olması ile bir çelişir.

Diğer yandan eğer (i,j) > 1 ise, bu takdirde hem i hem de j yi bölen bir q asalı vardır. {h,k} = {i,j} ve[h/q,k] = [i,j] olacak şekilde h ve k seçilsin ve $J'=(J\setminus\{i,j\}) \cup \{h/q,k\}$ olsun. (1) den $\theta(h/q) + \theta(k) \le \theta(i) + \theta(j)$ ve h ve k nın seçilişinden ekok (J') = ekok(J) = n olur. Buradan $J' \in \mathcal{Y}(n)$ dir. Fakat $\sum_{t \in J'} t < \sum_{t \in J} t$, J nin seçilişi ile çelişir. Onun için her i elemanı için $\theta(i) = 1$ olmalıdır.

Buradan aşağıdaki Lemma gereğince $\theta(n) = 1$ elde edilir.

LEMMA 5: n, $\prod p_i^{\alpha_i}$ şeklinde asal çarpanlarına ayrılsın. Bu takdirde $\theta(n) = 1$ olması gerek ve yeter şart $\forall i$ için $\theta(p_i^{\alpha_i}) = 1$ olmasıdır.

Lemma 5, Lemma 4 ün ispatının tamamlandığını göstermek içindir. n, Lemma 5 de tanımlandığı gibi asal çarpanlarına ayrılsın ve J de yukarıdaki gibi seçilen bir cümle olsun. ekok (J) = n olduğundan her i için $p_i^{\alpha_i} \mid k_i$ olacak şekilde $k_i \in J$ bulunmalıdır. Fakat biraz önce belirttiğimiz gibi $\theta(k_i) = 1$ dir.

Buradan (1), $\theta(p_i^{\alpha_i}) = 1$ olmasını gerektirir. Her i için böyle olduğundan Lemma 5, $\theta(n) = 1$ olmasını gerektirir. Böylece Lemma 4 ün ispatı, Lemma 5 in ispatına dayanmaktadır.

Lemma 5 in İspatı:

$\Leftarrow$: (1) den derhal elde edilir.

$\Rightarrow$: $n_1 = p_1^{\alpha_1}$ ve i > 1 için $n_i = n_{i-1} p_i^{\alpha_i}$ ile pozitif tamsayıların bir dizisi tanımlansın. (2) yi kullanarak basit bir indüksiyonla her i için $\theta(n_i) = 1$ olduğu ispatlanır. n, son

n_i olduğundan $\theta(n) = 1$ elde edilir. Bu da Lemma 5 ve 4 ün dolaysıyle Teorem 3 ün ispatını tamamlar.

3. $\theta(n)$ NİN DEĞERLENDİRİLMESİ

r(n) nin değeri $\theta(j)$ nin değerleri ile tanımlanır. Bu kısımda $\theta(j)$ nin değerlendirilişi üzerinde durulacak ve cisim genişlemelerinin etkileriyle ilgili bazı gözlemler verilecektir.

Aşağıdaki teorem Lemma 1 ve $\theta_K(n)$ nin tarifinden derhal elde edilir.

Teorem 6: Eğer L, K nın bir genişlemesi ve kar(K) $\nmid$ n ise, bu takdirde $\theta_L(n) \mid \theta_K(n)$ dir.

Teorem 7: Eğer L, K nın saf transandat bir genişlemesi ve f, K[x] de indirgenemez ise, bu takdirde f, L[x] de de indirgenemezdir.

İspat:

1. Adım: t, K da transandat olmak üzere L = K(t) olsun. L[x] de $f = g_1 \cdot h_1$ olduğunu varsayalım. Bu takdirde R = K[t] olsun ve f = gh,

deg(g) = deg(g_1) ve deg(h) = deg(h_1) olacak şekilde R[x] de g ve h polinomlarının olduğu görülür. (Bu, R bir UFD ve L bir kesirler cismi olduğundan Gauss lemmasından çıkar.) Yani, S = K[x] olmak üzere K[t,x] = S[t] de f = gh dır. f nin t-derecesi sıfır olduğundan g ve h ın her ikisinin t derecesi de sıfırdır. Dolayısıyle, g, $h \in S = K[x]$ dir. Buradan f nin L[x] de indirgenir olması K[x] de de indirgenir olmasını gerektirir.

2. Adım: t_i ler K üzerinde transandat ve cebirsel olarak bağımsız olmak üzere $L=K(t_1,\ldots,t_s)$ nin, K nın bir transandat genişlemesi olduğunu varsayalım. 1. adımı kullanarak s üzerinde indüksiyonla f nin L[x] de indirgenemez olduğu görülür.

3. Adım: L,K nın herhangi bir tam transandat genişlemesi olsun. O zaman L=K(T), K üzerinde T nin elemanlarının bütün rasyonel fonksiyonlarının cismi olacak şekilde K üzerinde hem cebirsel hem de transandat olarak bağımsız elemanlarının T gibi bir cümlesi mevcuttur. Eğer L[x] de $f = g \cdot h$ ise, o takdirde g

ve h ın yalnızca sonlu sayıda katsayısı vardır ve bu katsayıların her biri T nin yalnızca sonlu sayıda, diyelim, $t_1,\ldots,t_s$ gibi elemanlarını kapsar. O zaman $K(t_1,\ldots,t_s)[x]$ de $f = gh$ dır.

Sonuç 7.1: Eğer L, K nın bir tam transandat gnişlemesi ise, bu takdirde $\theta_L = \theta_K$ dır.

Yukarıdaki sonuç, 2. adımdan elde edilir. Tespit edilmiş bir K cismi için $\theta = \theta_K$ fonksiyonunu ilgilendiren aşağıdaki elemanter bağıntılar, lemma 1 ispatında verilen bilgilerden elde edilir.

Teorem 8: K bir cisim, n,r ve s kar(K)$\nmid$ nrs olacak işekilde pozitif tamsayılar olsun ve a da birimin n. mertebeden ilkel kökü olsun. O takdirde

(1) $\theta(n) = [K(a):K]$

(2) $\theta(n) \mid \varphi(n)$

(3) $\theta(r) \mid \theta(rs)$

(4) Eğer $(r,s) = 1$ ise, o zaman $\theta(rs) \mid \theta(r)\,\theta(s)$ dir.

Teorem 9: Eğer p bir asal ve n kar(K)$\nmid$ pn olacak şekilde bir pozitif tamsayı ise, o zaman

(1) Eğer $p \nmid n$ ise $\theta(pn) \mid (p-1)\,\theta(n)$,

(2) Eğer $p \mid n$ ise $\theta(pn) \mid p\theta(n)$ dir.

İspat: a birimin n. mertebeden bir ikel kökü ve b de $x^p - a$ nın bir kökü olsun. O zaman $b^{np} = a^n = 1$ dir. Keza, eğer $b^k = 1$ ise $1 = b^{kp} = (b^p)^k = a^k$ ve böylece $n \mid k$ elde edilir. Buradan b, ya birimin n. inci mertebeden ilkel kökü ya da birimin pn. mertebeden bir ilkel köküdür.

(1): $p \nmid n$ olması durumunda, Z_n^* de $r = p^{-1}$ ve a birimin n. mertebeden ilkel kökü olsun. Buradan a^r nin birimi bir diğer n. mertebeden ilkel kökü olduğu kolaylıkla görülür. Böylece K(a) da $(x - a^r)$, $(x^p - a)$ nın bir lineer çarpanıdır. Bir önceki paragrafdan, $x^p - a$ nın diğer her bir kökü birimin pn. mertebeden bir ilkel köküdür. $x^p - a$ farklı köklere sahip olduğundan $(x^p - a) / (x - a^r)$ nin her bir indirgenemez çarpanı $c_{pn}(x)$ in bir indirgenemez çarpanıdır. Şu halde bu

çarpanların dereceleri $\theta_{K(a)}(pn)$ ve bunlardan k tane varsa o takdirde $k\theta_{K(a)}(pn) = p-1$ olur. Böylece $\theta_{K(a)}(pn) \mid p-1$ dir. Sonuç olarak $\theta_K(pn) = \theta_{K(a)}(pn)\,\theta_K(n)$ elde edilir.

(2) : (1) de yaptığımız gibi $x^p - a$ nın bütün köklerinden birimin pn. inci mertebeden ilkel köklerini hariç tutacağız. Böylece, $x^p - a$ nın indirgenemez her bir çarpanı, $c_{pn}(x)$ in indirgenemez bir çarpanıdır. Dolayısıyla $\theta_{K(a)}(pn) \mid p$ dir.

Teorem 10: K bir cisim ve p asal, kar(K) $\nmid$ pn olacak şekilde p ve n pozitif tamsayılar olsun. $p \mid n$ ve $\theta(pn) = p\theta(n)$ olduğunu varsayalım.

(1) Eğer p tek ise, o zaman $\theta(p^2 n) = p\theta(pn)$

(2) Eğer $p = 2$ ve $4 \mid n$ ise, o zaman $\theta(4n) = 2\theta(2n)$ dir.

İspat: Lang [5,p.210] da tarif edildiği gibi normu kullanmak en basittir.

a birimin n.mertebeden ilkel kökü olsun. Teorem 9 dan b ve c sırasıyla birimin pn. inci ve p^2n.inci mertebeden ilkel kökleridir. İspatı yapmak için Teorem 9 dan eğer $b \notin K(a)$ ise $c \notin K(b)$ olduğunu göstermek yeterlidir. Bir çelişkiye varmak için $b \notin K(a)$ ve $c \in K(b)$ olduğunu farzedelim. $b \notin K(a)$ olması $\theta_{K(a)}(pn) = p$ olmasını gerektirir. Böylece $[K(b):K(a)] = p$ dir. Norm $N: K(b)^* \to K(a)^*$ ye bir çarpımsal homomorfizmdir. Ayrıca $-a = (-1)^p N(b)$ dir [5, teorem 8, p.210].

Böylece $c \in K(b)$ olması $-a = (-1)^p \cdot N(b) = (-1)^p N(c^p) = (-1)^p [N(c)]^p$ olmasını gerektirir. Eğer p tek ise, o takdirde K(a) da $a = [N(c)]^p$ dir. Bu ise K(a) da $x^p - a$ polinomunun bir kökü bulunacağını gösterir. Çünkü teorem 9'dan böyle herhangi bir kök birimin pn. inci mertebeden ilkel köküdür, buradan K(a) = K(b) elde edilir ki bu bir çelişkidir.

Diğer yandan p = 2 ise, bu takdirde $4 \mid n$ olduğunu biliyoruz. Bu da birimin 4. üncü mertebeden köklerinin K(a) da kapsanmasını gerektirir. Eğer $x^2 = \alpha$, K(a) da bir çözüme sahipse bu takdirde $x^2 = -\alpha$ nın K(a) da çözümü olacağı sonucuna varılır. $-a = [N(c)]^2$ olduğundan K(a) da $a = x^2$ için bir çözüm vardır. Bu da bir önceki paragraftaki gibi aynı çelişkiyi verir.

4. CİSMİN SONLU OLDUĞU DURUM

K= GF(q), q elemandan oluşan sonlu bir cisim olduğu zaman, θ_K yı θ_q ile göstereceğiz. Eğer (n,q) = 1 ise

$$o_n(q) = \min\{k \in IN : q^k \equiv 1 (\mathrm{mod}\, n)\}$$

tanımlansın. Bu gösterim Z_n^* da q nun mertebesinin $o_n(q)$ olduğunu gösterir.

Teorem 11: Eğer q bir asal kuvvet ve (q,n) = 1 ise, bu takdirde $\theta_q(n)=o_n(q)$ olur.

İspat: GF(q) nun her sonlu genişlemesi $GF(q^k)$ biçimindedir. $GF(q^k)$ çarpımsal grubu q^k-1 mertebeli devirli gruptur ve dolayısıyla 1 in n.mertebeden bir ilkel kökünü kapsaması için gerek ve yeter şart $n|q^k-1$ olmasıdır. Teorem 8.(1) den

$$\theta_q(n) = \min\{k \in IN : n|q^k - 1\} = o_n(q)$$

elde edilir.

Sonuç 11.1: Eğer r,s ve q aralarında ikişer ikişer asal iseler, bu takdirde $\theta_q(rs) = [\theta_q(r), \theta_q(s)]$ dir.

İspat: U_n, n modülüne göre u nun kalan sınıfını göstersin. $Z_r^* \times Z_s^*$ de, $\theta_q(rs)$ nin mertebesi (q_r, q_s) olmak üzere $\theta_q(rs)$ nin Z_{rs}^* de mertebesi q_{rs} dir. Son ifade açık olarak $[o_r(q), o_s(q)] = [\theta_q(r), \theta_q(s)]$ dir.

Sonuç 11.2: p bir asal (veya bir asalın kuvveti) ve n ve k, (p, n) = 1 olacak şekilde pozitif tamsayılar olsun. Eğer $d = \theta_p(n)$ ve $q = p^k$ ise, bu takdirde $\theta_q(n) = d/(d,k)$ dir.

(q,n) = 1 olduğunda $\theta_q(n)$ yi hesaplamak için bu iki sonuç birleştirilir. $\theta_p(r^k)$ yı bütün ayrık r,p asalları ve pozitif k tamsayıları için hesaplamak yeterlidir. Teorem 10 açısından hesaplamayı daha da kolaylaştırabiliriz. x bir asal, $x^k|y$ ve $x^{k+1} \nmid y$ olması durumunda $x^k||y$ gösterimini kullanacağız.

Sonuç 11.3: p bir asal, q bir asalın kuvveti olsun.

(1) p nin tek olduğunu varsayalım ve s, $p^s \| q^{\theta_q(p)} - 1$ olacak şekilde bir tamsayı olsun. Bu takdirde $k \geq s$ için $\theta_q(p^k) = \theta_q(p) \cdot p^{k-s}$ dir.

(2) p = 2 olduğunu varsayalım ve s, $2^s \| q^{\theta_q(4)} - 1$ olacak şekilde tamsayı olsun. O takdirde $k \geq s$ için $\theta_q(2^k) = \theta_q(4) \cdot 2^{k-s}$ dir.

11.2 ve 11.3 sonuçları birleştirilerek, bir asal kuvvet q için hesap yapmak yerine p ve q asalları (p tek) ve $\theta_q(4)$ için yalnızca $\theta_q(p)$ yi hesaplamak gerekir.

Örnek: K = GF(27) cismi üzerinde periyodu 60 olan en küçük matrisin boyutunu, yani $r_{27}(60)$ in değerini hesaplayalım.

Teorem 3 den, $r_{27}(60) = r_{27}(20) + 3^\circ + \delta_{27}(20)$ dir. Sonuç 11.2 den 20 nin her bir d böleni için $\theta_{27}(d) = \theta_3(d)$ dir. Buradan $r_{27}(20) = r_3(20)$ olur. Teorem 11 ve sonuç 11.1 i kullanarak $\theta_3(20) = \theta_3(5) = 4$ bulunur. Sonuç olarak $\theta_{27}(20) > 1$ olduğundan $\delta_{27}(20) = 1$ olur. Bu ikisi birlikte yerine yazılarak

$$r_{27}(60) = 4 + 1 + 1 = 6$$

elde edilir.

Gerçekten periyodu 60 olan 6 x 6 tipinde bir matris bulmak için yukardaki sonuçları GF(3) üzerinde çalışarakda elde ederiz. Bu münasebetle GF(3) de böyle bir matris olduğunu göstermek yeterlidir. Teorem 3 ün ispatında $\delta = 1$ durumunu göz önüne alarak böyle bir matris için minimum polinom, f, $c_{20}(x) = x^8 + x^6 + x^4 + x^2 + 1$ cyclotomic polinomunun indirgenemez bir çarpanı olmak üzere $m(x) = (x-1)^2 \cdot f(x)$ dir.

f nin derecesinin $\theta_3(20) = 4$ olduğunu a, 1 in 20.inci mertebeden ilkel kökü olmak üzere f nin $(x-a)(x-a^3)(x-a^9)(x-a^{27})$ formunda olduğunu biliyoruz. Bu çözüm yolunu genişleterek ve $a^{20} = 1$ i kullanarak $f(x) = x^4 - cx^3 + cx + 1$ olduğunu görürüz. Ayrıca simetriden dolayı bu çalışma -a nın 20. inci mertebeden ilkel kökü içinde geçerlidir, böylece c_{20} nin bir diğer çarpanı $x^4 + cx^3 - cx + 1$ dir. Bu c nin 1 veya -1 olmasını gerektirir. Onun için $f(x) = x^4 - x^3 + x + 1$ alabiliriz. Dolayısıyle $m(x) = x^6 - x^2 - x - 2$ nin üssü 60 dır ve

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 2 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

band matrisinin hem GF(3) hem de GF(27) de periyodu 60 dır. Alternatif olarak, $(x-1)^2$ ve f(x) in band matrislerinin direk toplamının periyodu da 60 dır.

5. BAZI GÖZLEMLER

(1) GF(q) sonlu cismi üzerinde, $c_n(x)$ cyclotomic polinomunun herhangi bir indirgenemez g(x) çarpanının Galois grubunun basit bir tanımlamasının olduğuna ilgi çekilmelidir. Eğer r, q nun herhangi bir kuvveti ise, o zaman $a \to a^r$ tasviri q(x) in kökleri a nın bir permütasyonudur. Eğer a, q(x) in belirlenmiş herhangi bir kökü ise, o zaman bütün kökler $0 \le k < s = \min\{i \in IN: r = q^i \Rightarrow a^r = a\}$ için $r = q^k$ olmak üzere a^r biçimindedir. [Tabii ki a nın birimin n. mertebeden ilkel kökü olması $s = O_n(q)$ olmasını gerektirir]. Böylece, birimin bilinen herhangi bir n.inci mertebeden ilkel kökü $c_n(x)$ in indirgenemez çarpanlarından birinin bulunmasına imkan sağlar.

Eğer a birimin herhangi bir n.inci mertebeden ilkel kökü ve d, n nin herhangi bir böleni ise o zaman $a^{n/d}, c_d(x)$ in indirgenemez bir çarpanını bulmak için kullanılabilen birimin d. inci mertebeden bir ilkel köküdür. Eğer birimin herhangi bir n. inci mertebeden bir ilkel kökü bilinirse, o zaman üssü n ve derecesi r(n) olan polinomlar oluşturabiliriz. Bunların herhangi birinden periyodu n ve boyutu r(n) olan bir matris kurabiliriz.

Alternatif olarak, eğer a herhangi bir K cismi üzerinde birimin n.inci mertebeden bir ilkel kökü ise, o zaman $\{a^r: o \le r < n\}$ cümlesi, bir vektör uzayı

olarak K üzerinde K(a) yı geçer. Böylece, bu cümleden K üzerinde K(a) için sıralı B taban cümlesini seçebiliriz. $x \to ax$ lineer dönüşümünün B cümlesine göre A matrisinin periyodu n ve boyutu $\theta(n)$ dir. n nin her bir d böleni için bu işlem periyodu d, boyutu $\theta(d)$ olan A_d matrisini oluşturmak için birimin d. inci mertebeden ilkel kökü olan $a^{n/d}$ için de uygulanabilir. Eğer $J \in (n)$ ise, o zaman $d \in J$ olmak üzere A_d matrislerinin direk toplamı periyodu n; boyutu r(n) olan bir matristir.

(2) Eğer $n > 2$ ise, bu takdirde Q da r(n) çifttir. $n = 1, 2$ için rasyonel sayılarda $r(n) = 1$ olduğu açıktır.

İspat: $k > 2$ için $\varphi(k)$ çift olduğundan $m(x) = c_{d_1}(x)...c_{d_k}(x)$ nin derecesi tek olması için gerek ve yeter şart $c_1(x)$ veya $c_2(x)$ in çarpan olmasıdır. İddia ediyoruz ki ne $c_1(x)$ ne de $c_2(x)$, m(x) i bölmez; sonuç $r(n) = \deg m(x)$ den elde edilir.

İndislerinin en küçük ortak katı $c_{d2}(x)...c_{dk}(x)$ ile aynı olan ve daha küçük dereceli bir polinom $c_1(x)c_{d_2}(x)...c_{d_k}(x)$ dir. Böylece $c_1(x)$, m(x) in bir çarpanı değildir. Benzer şekilde $c_{d_2}(x)...c_{d_k}(x)$ ile $c_2(x)c_{d_2}(x)...c_{d_k}(x)$ in indislerinin en küçük ortak katı aynı ve eğer $d_2,...,d_k$ lardan en az biri 2 nin bir çarpanı ise ikinci ifadenin derecesi daha küçüktür. Eğer $d_2,...,d_k$ lardan hiçbiri 2 nin çarpanı değilse, bu takdirde $j = 2d_2$, o zaman c(x) in derecesi

$$\varphi(j) = \varphi(2d_2) = \varphi(2)\varphi(d_2) = 1\varphi(d_2) < 1 + \varphi(d_2) = \deg c_2(x) \cdot c_{d_2}(x) \text{dir.}$$

Böylece $c_j(x)c_{d_3}(x)...c_{d_k}(x)$ ile $c_2(x)c_{d_2}(x)...c_{d_k}(x)$ in indislerinin en küçük ortak katı eşit ve ikinci ifadenin derecesi daha küçüktür. Şu halde $c_2(x)$, m(x) in bir çarpanı değildir.

(3) Rasyonel sayılarda $r(n) = \varphi(n)$ olması için gerek ve yeter şart p asal olmak üzere $n = 1,2,12, p^k$ veya $2p^k$ $(p > 2)$ olmasıdır. Diğer bütün durumlarda $r(n) < \varphi(n)$ dir.

(4) Acaba boyutu n olarak verilen bir matris için mümkün olan en büyük $\alpha(n)$ nedir? Bu problem $\varphi(d_1) + \varphi(d_2) + ... + \varphi(d_k) = n$ olmak üzere

$\{d_1,...,d_k\}$ nın en küçük ortak katı maksimum olacak şekilde $d_1,...,d_k$ pozitif tamsayılarının bulunması ile ilgilidir. Söz gelimi n = 2 için mümkün olan durumlar

$$\varphi(1) + \varphi(2) = 2, \quad \varphi(3) = 2 \qquad \varphi(4) = 2, \quad \varphi(6) = 2$$

dir. Böylece maksimum en küçük ortak kat 6 olduğundan $\alpha(2) = 6$ dır.

$c_6(x) = x^2 - x + 1$ için $\begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}$ band matrisinin periyodu 6 dır.

KAYNAKLAR

[1] _ R. Hanson, Minimum dimension for a square matrix of order n, College Math. j.21:28-34 (1990)

[2] _ Richter, R. B. Wardlaw, W.P., The smallest matrix of given period and primitive roots of unity, Linear Algebra and its Applications 160:87-97 (1992).

[3] _ W.J. Guerrier, The factorization of cyclotomic polynomials modp, Amer. Math. Monthly 75:46 (1968).

[4] _ Artin, Michael, Algebra, Prentice Hall, Englewood cliffs, New Jersey (1991).

[5] _ Şenay, Hasan, Sayılar Teorisine Giriş, S.Ü. (1989).

[6] _ Rosen, K. H., Elementary Number Theory and its Applications, Addision - Wesley Publishing Company, New York, (1988).

[7] _ Burton, D., M., Elementary Number Theory, Revised Printing, London (1980).

[8] _ Gupto, H., Selected Topics in Number Theory, Abacus Press (1980).

[9] _ I. N. Herstein, Topics in Algebra, New Yorks: Blaisdell, 1964.

[10] _ J: B. Fraleigh, A First Course in Abstract Algebra, Addison - Wesley Publishing Company, London, 1977.

[11] _ Artin Emil, Galois Theory, University of Notre Dame Press, London, 1971.