KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MATEMATİK ANABİLİM DALI

DÜZGÜN ONYEDİ KÖŞELİNİN PERGEL VE CETVELLE İNŞASI

Bahaddin SİNSOYSAL

Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsünce
"Yüksek Lisans (Matematik)"
Ünvanının Verilmesi İçin Kabul Edilen Tezdir

Tezin Enstitüye Verildiği Tarih : 16.5.1995
Tezin Sözlü Savunma Tarihi : 30.6.1995

Tez Danışmanı : Prof.Dr.Ergün BAYAR
Jüri Üyesi : Doç.Dr.Ali PANCAR
Jüri Üyesi : Yrd.Doç.Dr.M.Sabri TERZİ

Enstitü Müdürü : Prof.Dr.Temel SAVAŞKAN

Mayıs 1995
TRABZON

ÖNSÖZ

Bu çalışmanın amacı, Galois teorisinin en önemli uygulama alanı olan geometride düzgün n-genlerden sadeve 17-genin yalnız pergel ve cetvelle nasıl inşa edilebileceğini, cebirsel ve geometrik yollarla incelemektir.

Gerek konu seçimi ve gerekse çalışmaların yürütülmesi sırasında ilgisini esirgemeyen Sayın Hocam Prof.Dr.Ergün BAYAR'a teşekkür eder, saygılarımı sunarım.

Yapıcı eleştirilerinden yararlandığım Sayın Hocam Yrd.Doç.Dr.M.Sabri TERZİ'ye ve yaptığı çevirilerden dolayı Sayın Hocam Prof.Dr.Ali BÜLBÜL'e teşekkür ederim.

Ayrıca çalışmalarım sırasında yardımlarını esirgemeyen Sayın Dr. Sultan YAMAK'a, Sayın Arş.Gör.A.Yaşar ÖZBAN'a ve tezin bilgisayarda yazılımını gerçekleştiren Sayın Saime KERİM'e teşekkürlerimi sunarım.

Trabzon, Mayıs 1995

Bahaddin SİNSOYSAL

İÇİNDEKİLER

ÖZET

"Düzgün 17-genin Pergel ve Cetvelle İnşası" adlı bu çalışma üç bölümden oluşmaktadır.

Birinci bölümde cisim genişlemeleri ve cisim izomorfilerine ait tanım ve teoremler (ispatsız) verilmiştir.

İkinci bölümde her sonlu, normal ve ayrılabilir bir cisim genişlemesinin tüm altcisimlerinin bir sonlu grubun altgrupları ile karakterize edilebileceği ve dolayısıyla sözü geçen cisim genişlemesinin tüm altcisimlerini belirleme probleminin bir sonlu grubun tüm altgruplarını belirleme problemine indirgenebileceği gösterilmiştir. Yine aynı bölümde, bir cisim genişlemesinin Galois grubunun nasıl bulunabileceği araştırılmıştır.

Üçüncü bölümde ise pergel-cetvel adımlarından ne kastedildiği ve bu adımlarla ne tür geometrik şekiller inşa edilebileceği üzerinde durulmuştur. Son olarak da düzgün 17-genin inşası probleminin, $\frac{2\pi}{17}$ açısının pergel ve cetvelle inşası problemine denkliği ele alınarak $\cos\frac{2\pi}{17}$ büyüklüğü ve dolayısıyla $\frac{2\pi}{17}$ açısı $Q^{(17)}$ cisminde inşa edilmiştir.

Anahtar Kelimeler: Cisim genişlemesi, ayrılabilir genişleme, çözülebilir grup, Galois genişlemesi, Fermat asalı, düzgün Poligon.

SUMMARY

Construction of A Regular 17-gon by Compass and Ruler

This study entitled "Construction of A Regular 17-gon by Compass and Ruler" consists of three chapters.

Some definitions and theorems related with field extensions and field isomorphisms are given in Chapter 1.

In Chapter 1, it has been shown that all subfields of every field extension which is finite, normal and seperable can be characterized by subgroups of a finite group and so the problem of determining all subfields extensions considered above is reduced to determining all subgroups of a finite group. In addition how Galois group of a field extension can be found is investigated in this chapter.

In Chapter 3, it has been discussed the meaning of ruler-compass steps and the type of geometric figures which can be constructed by those steps. Finally, the quantity $\cos\frac{2\pi}{17}$ and so the angle $\frac{2\pi}{17}$ is constructed in the field $Q^{(17)}$ by taking into consideration the equivalency of the problem of construction of a regular 17-gon to the construction of the angle $\frac{2\pi}{17}$ by compass and ruler.

Key Words: Field extension, seperable extension, solvable group, Galois extension, Fermat prime, regular Polygon.

ŞEKİL LİSTESİ

SEMBOL LİSTESİ

$\mathbf{N}$	Doğal sayılar kümesi
$\mathbf{N}_0$	$\mathbf{N} \cup \{0\}$
$\mathbf{Z}$	Tam sayılar kümesi
$\mathbf{Z}_n$	Modülo n kalan sınıflar kümesi
$\mathbf{Z}_n^*$	Modülo n asal kalan sınıflar kümesi
$\mathbf{P}$	Asal sayılar kümesi
$\mathbf{Q}$	Rasyonel sayılar kümesi
$\mathbf{R}$	Reel sayılar kümesi
$\mathbf{¢}$	Kompleks sayılar kümesi

Dönüşümler genel olarak küçük Grek harfleri ile gösterilecektir. Bir π dönüşümü altında bir g elemanının resmi için g^{π} (veya $(g)\pi$) yazılacaktır. Bu takdirde π ve ρ dönüşümlerinin bileşkesi

$$g^{\pi\rho} = (g^{\pi})^{\rho} \text{ veya } (g)\pi\rho = ((g)\pi)\rho$$

ile belirlenecektir. Bunun yanında bileşkesi yapılamayan bazı dönüşümler notasyon uygunluğu bakımından küçük veya büyük latin harfleri ile gösterilecek ve bu takdirde bir f (benzer şekilde F) dönüşümü altında a elemanının resmi f(a) (benzer şekilde F(a)) ile gösterilecektir.

1. GENEL BİLGİLER

1.1 Giriş

Tanım1: S bir cisim ve (V,+) bir Abel grubu olmak üzere

$$\sigma : S \times V \rightarrow V$$

dönüşümü her $a \in S$ ve $v \in V$ için

$$(a,v)^{\sigma} = av$$

olarak verilsin. σ dönüşümü aşağıdaki şartları gerçeklerse V ye S üzerinde bir vektör uzayı veya kısaca S-uzay denir.

(V.1). $(ab)v = a(bv)$, $a,b \in S$, $v \in V$

(V.2). $(a+b)v = av+bv$

$a(v+w) = av+aw$, $a,b \in S$, $v,w \in V$

(V.3). $1v = v$, $v \in V$.

Tanım 2: V S üzerinde bir vektör uzayı ve $U \subseteq V$ bir altküme olsun. U kümesi, V de tanımlanan vektör toplamına ve skalerle çarpıma göre bizzat S üzerinde bir vektör uzayı ise, U ya V nin bir altvektör uzayı denir.

Teorem 1: V S üzerinde bir vektör uzayı ve $U \subseteq V$ altküme olsun. U nun V nin bir altvektör uzayı olabilmesi için gerek ve yeter koşul,

$$U - U \subseteq U \ , \ SU \subseteq U$$

verilmesidir.

Teorem 2: S üzerindeki bir V vektör uzayının alt vektör uzaylarının keyfi bir ailesinin arakesiti de V nin S üzerindeki bir altvektör uzayıdır.

Tanım 3: V S üzerinde bir vektör uzayı olsun. Bir $v \in V$ vektörü, $a_1,...,a_n \in S$ ve $v_1,...,v_n \in V$ olmak üzere

$$v = a_1v_1 + ... + a_nv_n = \sum_{i=1}^{n} a_iv_i$$

şeklinde yazılabiliyorsa, v vektörüne $v_1,...,v_n$ vektörlerinin bir S- lineer kombinezonu denir.

$v_1,...,v_n \in V$ vektörlerinin tüm S-lineer kombinezonlarının kümesini

$$\langle v_1,...,v_n\rangle = \{ \sum_{i=1}^{n} a_i v_i \mid a_i \in S \}$$

$$= Sv_1+...+Sv_n$$

$$= \sum_{i=1}^{n} Sv_i$$

ile gösterelim.

Teorem 3: V S üzerinde bir vektör uzayı ve $v_1,...,v_n \in V$ sonlu sayıda vektörler olsun.

$$\langle v_1,...,v_n\rangle = \{ \sum_{k=1}^{n} a_k v_k \mid a_k \in S \}$$

dır.

Tanım 4: Bir $n \geq 0$ ve $v_1,...,v_n \in V$ vektörleri

$$\langle v_1,...,v_n\rangle = V$$

olacak şekilde mevcut iseler, V vektör uzayına sonlu üretenli ve $\{v_1,...,v_n\}$ kümesine de V nin S üzerindeki bir üretici sistemi denir.

Tanım 5: V S üzerinde bir vektör uzayı ve $v_1,...,v_n \in V$ $(n \geq 1)$ olsun.

$$\sum_{i=1}^{n} a_i v_i = 0 \ , \ a_i \in S$$

ifadesinden $a_1=...=a_n=0$ elde edilirse, $v_1,...,v_n$ vektörlerine S üzerinde lineer bağımsız (aksi takdirde lineer bağımlı) denir.

Bir $M \subset V$ altkümesinin sonlu sayıdaki vektöründen oluşan her $v_1,...,v_n$ $(n \geq 1)$ vektör takımı lineer bağımsız ise, M kümesine lineer bağımsız (akti takdirde lineer bağımlı) denir.

Tanım 6: V S üzerinde bir vektör uzayı ve $T=\{v_1,...,v_n\} \subset V$ $(n \geq 0)$ bir altküme olsun. $v_k \in T$ vektörleri S üzerinde lineer bağımsız ve V vektör uzayını üretiyorlarsa, T kümesine V nin S üzerindeki bir tabanı (veya bir S-tabanı) denir.

Teorem 4: V S üzerinde bir vektör uzayı ve $V= \langle v_1,...,v_n\rangle$ $(n \geq 1)$ olsun. Her $v \in V$ vektörünün v_k vektörlerinin tektürlü S-lineer kombinezonu olarak yazılabilmesi için gerek ve yeter koşul, $\{v_1,...,v_n\}$ kümesinin V nin bir S-tabanı olmasıdır.

Teorem 5: V S üzerinde sonlu üretenli bir vektör uzayı olsun. Bu takdirde V vektör uzayı en az bir S-tabana sahiptir. V nin herhangi iki S-tabanı aynı sayıda vektörden oluşur.

Tanım 7: V S üzerinde bir vektör uzayı olsun. V sonlu üretenli, T V nin bir S-tabanı ve |T|=n ise, bu n sayısına V vektör uzayının boyutu denir ve

$$n = [V:S]$$

yazılır. V vektör uzayı sonlu üretenli değilse, $[V:S] = \infty$ yazılır.

TEOREM 6: V S üzerinde bir vektör uzayı ve $[V:S] = n < \infty$ olsun. Bu takdirde V nin n+1 vektöründen meydana gelen her altkümesi S üzerinde lineer bağımlıdır ve V nin S üzerinde lineer bağımsız n vektöründen meydana gelen her küme V nin bir S-tabanını teşkil eder.

$[V:S] = \infty$ olabilmesi için gerek ve yeter koşul, V de keyfi sayıda lineer bağımsız vektörlerin mevcut olmasıdır.

Teorem 7: $V = \langle v_1,...,v_n \rangle$ S üzerinde sonlu üretenli bir vektör uzayı ve $u_1,...,u_r \in V$ S üzerinde lineer bağımsız vektörler olsun. Bu takdirde

$$\{u_1,...,u_r\} \subset T$$

olacak şekilde V nin bir T S-tabanı mevcuttur.

Teorem 8: V S üzerinde bir vektör uzayı ve $U \subseteq V$ bir alt vektör uzayı olsun.

(a). $[U:S] \leq [V:S]$ verilir.

(b). $[U:S] = [V:S] < \infty$ ifadesinden U=V elde edilir.

Teorem 9: (Boyut teoremi) L bir cisim, V L üzerinde bir vektör uzayı ve $S \subset L$ altcismi olsun.

(a). $[V:S] = [V:L]\,[L:S]$ verilir.

(b). $\{u_1,...,u_m\}$ L in bir S-tabanı ve $\{v_1,...,v_n\}$ V nin bir L-tabanı ise,

$$T = \{u_i v_j \mid i=1,...,m \; ; \; j=1,...,n\}$$

kümesi, V vektör uzayının bir S-tabanıdır.

İspat: $V \neq \{0\}$ olduğunu kabul edelim. $[V:L] < \infty$, $[L:S] < \infty$ olsun. Bu takdirde sadece (b) yi ispat etmek yeterlidir. Zira (b) ifadesinden

$$[V:S] = mn = [V:L]\,[L:S]$$

elde edilir. T kümesi, V vektör uzayının L üzerindeki bir üretici sistemidir. Zira keyfi bir $v \in V$ elemanına mukabil $a_1,...,a_n \in L$ elemanları

$$v=\sum_{i=1}^{n} a_i v_i$$

olacak şekilde mevcutturlar. Bunun yanında her a_i (i=1,...,n) elemanına mukabil $b_{ij}\in S$ elemanları

$$a_i=\sum_{j=1}^{m} b_{ij}u_j$$

olacak şekilde mevcutturlar. Dolayısıyla

$$v=\sum_{i=1}^{n}\sum_{j=i}^{m} b_{ij}u_j v_i$$

elde edilir. T kümesi S üzerinde lineer bağımsızdır. Zira $c_{ij}\in S$ olmak üzere

$$\sum_{i=1}^{n}\sum_{j=1}^{m} c_{ij}u_j v_i =0$$

olsun. Bu takdirde v_i vektörleri L üzerinde lineer bağımsız olduklarından

$$\sum_{j=1}^{m} c_{ij}u_j =0\ ,\ i=1,...,n$$

ve u_j elemanları S üzerinde lineer bağımsız olduklarından

$$c_{ij}=0\ ,\ i=1,...,n\ ;\ j=1,...,m$$

elde edilir.

$[V:L]=\infty$ olsun.

$$[V:S]\geq[V:L]$$

olduğundan $[V:S]=\infty$ olup, (a) ifadesi doğrudur.

$[L:S]=\infty$ olsun. Bu takdirde her $k\in\mathbb{N}$ sayısı için L in S üzerinde lineer bağımsız olan bir $\{u_1,...,u_k\}$ altkümesi mevcuttur. Her $v\in V-\{0\}$ için

$$\{u_1 v,...,u_k v\}$$

V nin S üzerinde lineer bağımsız bir altkümesidir. Dolayısıyla $[V:S]=\infty$ olup (a) ifadesi doğrudur.

1.2 Çözülebilir Gruplar ve Simetrik Polinomlar

Tanım 8: Bir G grubuna çözülebilirdir denir : $\Leftrightarrow$

(I) $N_i \trianglelefteq N_{i-1}$, i=1,2,...,n

(II) N_{i-1}/N_i Abel, i=1,2,...,n

koşullarını gerçekleyen G nin altgruplarının bir

$$G=N_0\supseteq N_1\supseteq\ldots\supseteq N_n=\{e\}$$

sonlu zinciri vardır.

Uyarı 1: Her Abel grubu çözülebilirdir.

Teorem 10: G sonlu bir grup olsun. G çözülebilirdir ancak ve ancak

(i) $N_i \lhd N_{i=1}$, $i=1,2,...,n$

(ii) N_{i-1}/N_i asal mertebeden devirli, $i=1,2,...,n$

koşullarını gerçekleyen G nin altgruplarının bir

$$G= N_0 \supseteq N_1 \supseteq ... \supseteq N_n = \{e\}$$

sonlu zinciri vardır.

Teorem 11: G bir grup, $H \leq G$ ve $N \trianglelefteq G$ olsun.

1. G çözülebilir ise H çözülebilirdir.
2. G çözülebilir ise G/N çözülebilirdir.
3. N ve G/N çözülebilir ise G çözülebilirdir.

Teorem 12: Her p-grup çözülebilirdir.

Tanım 9: Bir $f(x_1,...,x_n) \in R[x_1,...,x_n]$ polinomu, her $\pi = \begin{pmatrix} i \\ i^\pi \end{pmatrix} \in S_n$ permütasyonu için

$$f(x_{1\pi}, x_{2\pi}, ..., x_{n\pi}) = f(x_1, x_2, ..., x_n)$$

gerçeklenirse, $f(x_1,...,x_n)$ polinomuna simetrik denir.

Tanım 10: x $R[x_1,...,x_n]$ üzerinde bir belirsiz olmak üzere

$$g(x) = \prod_{i=0}^{n} (x-x_i)$$

polinomu gözönüne alınsın. Bu polinom

$$s_i = \sum_{\pi \in s_n} x_{1\pi} x_{2\pi} \cdots x_{i\pi} \quad , \quad i=1,...,\pi$$

$$1 \leq 1^\pi < ... < i^\pi \leq n$$

olmak üzere

$$g(x) = \sum_{i=o}^{n} (-1)^i s_i x^{n-i} \quad , \quad s_o = 1$$

şeklinde yazılabilir. Her $\pi \in S_n$ için

$$\prod_{i=1}^{n} (x-x_{\pi}) = \prod_{i=1}^{n} (x-x_i)$$

olduğundan $s_i(x_1,...,x_n)$ (i=1,...,n) ler simetrik polinomlardır. $s_i(x_1,...,x_n)$ polinomuna i inci elemanter simetrik polinom denir.

Teorem 13: Her $f(x_1,...,x_n) \in R[x_1,...,x_n]$ simetrik polinomuna mukabil

$$f(x_1,...,x_n) = g(s_1,...,s_n)$$

olmak üzere, tektürlü olarak belirli olan bir $g(s_1,...,s_n) \in R[s_1,...,s_n]$ polinomu mevcuttur.

1.3. Cisim Genişlemeleri

Tanım 11: L bir cisim, $K \subseteq L$ altcisim ise L ye K nın bir genişlemesi denir.

Tanım 12: K bir cisim, L K nın bir genişlemesi ve $T \subset L$ bir altküme olsun.

(a). L cisminde, K altcismini ve T altkümesini ihtiva eden tüm altcisimlerin arakesiti K(T) ile gösterilir. Açık olarak K(T), K altcismini ve T altkümesini ihtiva eden en küçük cisimdir:

$$K \subset K(T) \subset L.$$

K(T) ye, K ya T nin "katılması" ile elde edilen cisim denir. K(T) cisminin teşkil edilmesine de K cismine T kümesini "katma" denir.

(b). $T=\{t_1,...,t_n\}$ $(n<\infty)$ ise,

$$K(T) = K(t_1,...,t_n)$$

yazılır.

(c). Bir $t \in L$ için

$$K(t) = L$$

ise, L e K cisminin basit genişlemesi denir. Bu özelliğe sahip her $t \in L$ elemanına, L cisminin (K üzerindeki) bir primitif elemanı denir.

Tanım 13: K bir cisim, L K nın bir genişlemesi ve $t \in L$ olsun. K[x] polinomlar halkasında t yi kök kabul eden sıfırdan farklı f(x) polinomu varsa t ye K üzerinde cebirsel eleman denir. K üzerinde cebirsel olmayan bir elemana, K üzerinde transandant eleman denir.

Uyarı 2: Bundan böyle aksi belirtilmediği sürece, K bir cisim ve x K üzerinde bir belirsiz olsun. Bunun yanında K cisminin herhangi bir genişlemesi için, x aynı zamanda bu genişleme üzerinde de bir belirsiz olsun.

Tanım 14: t elemanı K üzerinde cebirsel olsun. Sıfır yerlerinden birisi t olan, K[x] halkasının en küçük dereceli monik polinomuna, t elemanının K üzerindeki minimal polinomu (veya indirgenemez polinomu) denir ve bu polinom

$$\text{İnd}\,(t,K)$$

ile gösterilir. İnd (t,K) minimal polinomunun derecesine, t elemanının K üzerindeki cebirsellik derecesi denir ve bu derece [t:K] ile gösterilir.

Teorem 14: t K üzerinde bir cebirsel eleman ve İnd (t,K) = g(x) olsun.

(a). Bir $f(x)\in K[x]$ polinomu için f(t)=0 olabilmesi için gerek ve yeter koşul, K[x] de

$$g(x) \mid f(x)$$

verilmesidir.

(b). Bir $f(x)\in K[x]$ polinomu için

$$f(x) = g(x)$$

olabilmesi için gerek ve yeter koşul, f(x) polinomunun K[x] de monik, indirgenemez ve f(t)=0 olmasıdır. Özellikle $g(x)\in K[x]$ polinomu t ve K ile tektürlü olarak belirlidir.

Teorem 15: t K üzerinde bir cebirsel eleman, İnd(t,K) = g(x) ve [t:K]=n olsun.

(a). K(t)=K[t] dir ve $\{1,t,...,t^{n-1}\}$ sistemi, K(t) nin bir tabanıdır:

$$K(t) = < 1,t,...,t^{n-1} > .$$

(Burada K(t) , K üzerinde bir vektör uzayı olarak gözönüne alınıyor).

Özellikle

$$[K(t) : K] = [t:K]$$

verilir.

(b). $K(t) \cong K[x] / < g(x) >$

verilir.

Teorem 16: t K üzerinde bir cebirsel eleman ve

$$\text{İnd}(t,K) = g(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1} + x^n$$

olsun. Bunun yanında $\bar{K}$ bir cisim ve $\bar{L}$, $\bar{K}$ nın bir genişlemesi olmak üzere bir $\alpha : K \to \bar{K}$ izomorfisi verilmiş olsun. y $\bar{K}$ üzerinde bir belirsiz olmak üzere

$$a_0^{\alpha} + a_1^{\alpha}\, y + ... + a_{n-1}^{\alpha} y^{n-1} + y^n = \bar{g}(y)\in\bar{L}$$

yazılsın.

(a). α izomorfisinin bir $\beta: K(t) \to \bar{L}$ genişletilmişinin mevcut olabilmesi için gerek ve yeter koşul, $\bar{g}(y)$ polinomunun $\bar{L}$ de en az bir sıfır yerine sahip olmasıdır.

(b). $s_1,...,s_r$ elemanları $\bar{g}(y)$ polinomunun $\bar{L}$ deki farklı sıfır yerleri olsunlar. Bu takdirde α izomorfisinin tam r tane genişletilmişi vardır ve bunlar $b_i \in K$ için

$$(\sum_i b_i t^i)^{\beta_j} = \sum_i b_i^{\alpha} s_j^i \ , \ j=1,...,r$$

ile belirlenen

$$\beta_j : K(t) \to \bar{K}(s_j) \ , \ j=1,...,r$$

dönüşümleridir. Özellikle α izomorfisinin $\beta_1 ,..., \beta_r$ genişletilmişleri, $\bar{g}(y)$ polinomunun $\bar{L}$ deki $s_1,...,s_r$ sıfır yerlerine tektürlü olarak tekabül ettirilebilir ve bu tekabül

$$t^{\beta_j} = s_j \ , \ j=1,...,r$$

ile belirlenir.

İspat: α izomorfisinin K(t) üzerine genişletilmişi $\beta:K(t) \to \bar{L}$ olsun. Bu takdirde $a_n=1$ olmak üzere

$$0=g(t)^{\beta} = (\sum_{i=0}^{n} a_i t^i)^{\beta} = \sum_{i=0}^{n} a_i^{\alpha} (t^{\beta})^i = \bar{g}(t^{\beta})$$

olduğundan, $t^{\beta} \in \bar{L}$ elemanı $\bar{g}(y)$ polinomunun bir sıfır yeridir. $t^{\beta} = s$ elemanının verilmesiyle β dönüşümü tektürlü olarak belirlenmiş olur. Zira keyfi bir $b \in K(t)$ elemanı, $b_i \in K$ olmak üzere

$$b = \sum_i b_i t^i$$

şeklinde olduğundan

$$b^{\beta} = (\sum_i b_i t^i)^{\beta} = \sum_i b_i^{\alpha} (t^{\beta})^i = \sum_i b_i^{\alpha} s^i$$

elde edilir.

Tersine olarak bir $s \in \bar{L}$ elemanı $\bar{g}(y)$ polinomunun bir sıfır yeri olsun. Keyfi bir $b \in K(t)$ elemanı $b_i \in K$ olmak üzere $b = \sum_i b_i t^i$ şeklinde yazılabilir.

$$b^{\beta} = \sum_i b_i^{\alpha} s^i$$

ile tanımlanan $\beta:K(t) \to \bar{K}(s)$ dönüşümünün bir izomorfi ve $\beta = \alpha \upharpoonright K(t)$ olduğu gösterilebilir. $b_i \in K$ olmak üzere

$$(\sum_i b_i x^i)^{\gamma} = \sum_i b_i^{\alpha} y^i$$

ile tanımlanan $\gamma:K[x] \to \bar{K}[y]$ dönüşümü bir izomorfidir.

$$g(x)^{\gamma} = \bar{g}(y)$$

olduğundan $\bar{g}(y) \in \bar{K}[y]$, indirgenemez bir monik polinomdur ve aynı zamanda

$$\bar{g}(y) = \text{İnd}(s,\bar{K})$$

verilir.

$$(\sum_i b_i x^i + < g(x) >)^{\theta} = \sum_i b_i^{\alpha} y^i + < \bar{g}(y) >$$

ile tanımlanan

$$\theta : K[x] / < g(x) > \rightarrow \bar{K}[y] / < \bar{g}(y) > ,$$

$$(\sum_i b_i t^i)^{\phi} = \sum_i b_i x^i + < g(x) >$$

ile tanımlanan

$$\phi : K(t) \rightarrow K[x] / < g(x) >$$

ve

$$(\sum_i b_i^{\alpha} s^i)^{\Psi} = \sum_i b_i^{\alpha} y^i + < \bar{g}(y) >$$

ile tanımlanan

$$\Psi : \bar{K}(s) \rightarrow \bar{K}[y] / < \bar{g}(y) >$$

dönüşümleri birer izomorfidir.

$$\phi\theta\Psi^{-1} : K(t) \rightarrow \bar{K}(s)$$

dönüşümü bir izomorfidir ve $\phi\theta\Psi^{-1} \downarrow K = \alpha$ dır. Dolayısıyla $\beta = \phi\theta\Psi^{-1}$ alınabilir.

Tanım 15: K üzerinde aynı minimal polinoma sahip cebirsel elemanlara, K üzerinde eşlenik veya kısaca K- eşlenik denir.

Teorem 17: s ve t K- eşlenik elemanlar ise, K(s) ve K(t) cisimleri K- izomorftur. Özellikle bu K- izomorfi

$$\sum_i b_i t^i \rightarrow \sum_i b_i s^i$$

ile verilir.

Teorem 18: $g(x) \in K[x]$ indirgenemez bir monik polinom olsun. Bu takdirde

$$g(x) = \text{İnd}(t,K)$$

olacak şekilde K üzerinde cebirsel olan bir t elemanı mevcuttur.

Tanım 16: L cismi K nın bir genişlemesi olsun.

(a). L cisminin her elemanı K üzerinde cebirsel ise, L e K cisminin bir cebirsel genişlemesi (veya K üzerinde cebirsel) denir.

(b). $[L:K] < \infty$ ise, L e K nın bir sonlu genişlemesi denir.

Teorem 19: Bir cismin her sonlu genişlemesi bir cebirsel genişlemedir.

Teorem 20: Bir K cisminin bir L genişlemesinin sonlu olabilmesi için gerek ve yeter koşul, K üzerinde cebirsel olan $t_1,...,t_n \in L$ elemanlarının

$$L = K(t_1,...,t_n)$$

olacak şekilde mevcut olmasıdır. Bu halde özellikle

$$L = K[t_1,...,t_n]$$

verilir.

Tanım 17: $f(x) \in K[x]$ sabit olmayan bir polinom olsun. K nın aşağıdaki özelliklere sahip bir L genişlemesine, f(x) polinomunun K üzerindeki bir parçalayıcı cismi denir.

(a). f(x) polinomu, L[x] halkasında lineer polinomların bir çarpımı şeklinde yazılabilir.

(b). L cismi K nın (a) özelliğine sahip en dar genişlemesidir. Diğer bir ifade ile $K \subset U$ olmak üzere her $U \subset L$ altcismi için f(x) polinomu U[x] halkasında lineer polinomların bir çarpımı şeklinde yazılamaz.

Teorem 21: $f(x) \in K[x]$ sabit olmayan ve baş katsayısı c olan bir polinom olsun. K nın bir L genişlemesinin f(x) polinomunun K üzerindeki bir parçalayıcı cismi olabilmesi için gerek ve yeter şart, $t_1,...,t_n \in L$ elemanlarının

$$f(x) = c \prod_{i=1}^{n} (x - t_i) \quad \text{ve} \quad L = K(t_1,...,t_n)$$

olacak şekilde mevcut olmasıdır.

Uyarı 3: L bir f(x) polinomunun K üzerindeki bir parçalayıcı cismi olsun. Bu takdirde teorem 21 ve teorem 20 ye göre, L K nın bir sonlu genişlemesidir. Bunun yanında $K \subset U$ olmak üzere, her $U \subset L$ altcismi için f(x) polinomunun U üzerindeki parçalayıcı cismi de L dir. Zira

$$L = U(t_1,...,t_n)$$

dir.

Teorem 22: $f(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$ n inci dereceden bir polinom ve $\alpha : K \to \bar{K}$ bir izomorfi olsun. y $\bar{K}$ üzerinde bir belirsiz olmak üzere

$$\sum_{i=0}^{n} a_i^{\alpha} y^i = \bar{f}(y) \in \bar{K}[y]$$

yazılsın. f(x) polinomunun K üzerindeki bir parçalayıcı cismi L ve $\bar{f}(y)$ polinomunun $\bar{K}$ üzerindeki bir parçalayıcı cismi $\bar{L}$ ise

$$\beta = \alpha \uparrow L$$

olacak şekilde bir $\beta : L \to \bar{L}$ izomorfisi mevcuttur.

Teorem 23: $f(x) \in K[x]$ sabit olmayan bir polinom olsun.

(a). $f(x)$ polinomunun K üzerinde en az bir parçalayıcı cismi mevcuttur.

(b). $f(x)$ polinomunun K üzerindeki iki parçalayıcı cismi daima K- izomorftur.

Tanım 18: t K üzerinde bir cebirsel eleman ve L, $İnd(t,K)$ polinomunun K üzerindeki bir parçalayıcı cismi olsun. Bu takdirde $t_1 = t$ olmak üzere

$$İnd(t,K) = \prod_{i=1}^{n} (x - t_i) \in L[x]$$

yazılabilir. $\{t_1,...,t_n\} \subset L$ alt kümesine, t elemanının K üzerindeki eşleniklerinin bir tam sistemi denir.

Tanım 19: L K cisminin bir cebirsel genişlemesi olsun. L cisminde en az bir sıfır yeri bulunan her indirgenemez $f(x) \in K[x]$ polinomu, L[x] halkasının lineer polinomlarının bir çarpımı şeklinde ise, L cismine K nın bir normal genişlemesi (veya K üzerinde normal) denir.

Teorem 24: K cisminin bir L genişlemesinin sonlu ve normal olabilmesi için gerek ve yeter koşul , L cisminin K[x] halkasının bir polinomunun K üzerindeki bir parçalayıcı cismi olmasıdır.

Teorem 25: L cismi K nın bir normal genişlemesi olsun. Bu takdirde L cismi, $K \subset U$ olmak üzere her $U \subset L$ altcisminin de bir normal genişlemesidir.

Teorem 26: L cismi K nın bir sonlu genişlemesi ve

$$L = K(t_1,...,t_n)$$

olsun. Bu takdirde

$$f(x) = \prod_{i=1}^{n} İnd(t_i,K) \in L[x]$$

polinomunun L üzerindeki her parçalayıcı cismi, L cisminin K üzerinde normal olan bir genişlemesidir.

Tanım 20: $x^n - 1 \in K[x]$ $(n \in \mathbf{N})$ polinomunun K üzerindeki bir parçalayıcı cismi $K^{(n)}$ ile gösterilsin. $K^{(n)}$ cismine K üzerinde bir n inci çember bölen cisim denir. $x^n - 1$ polinomunun

$K^{(n)}$ cismindeki sıfır yerlerine, birim elemanın (veya kısaca 1 in) K üzerindeki n inci kökleri denir. Bu köklerin kümesi B_n ile gösterilsin.

Teorem 27: $k(K)=p$ ve $n\in\mathbf{N}$ olsun.

(a). p|n veya $n=p^r m$, $(p,m)=1$ olacak şekilde $m,r\in\mathbf{N}$ sayıları mevcutsa, 1 in K üzerindeki her n inci kökü aynı zamanda 1 in K üzerindeki bir m inci köküdür.

(b). p/n ise, B_n kümesi $K^{(n)}$ cismindeki çarpma işlemine göre n inci mertebeden bir devirli gruptur.

Uyarı 4: $K^{(n)}$, $x^n-1\in K[x]$ polinomunun K üzerindeki bir parçalayıcı cismi olduğundan teorem 24 e göre, $K^{(n)}$ cismi K nın sonlu ve normal bir genişlemesidir ve özellikle

$$[K^{(n)} : K] \le \varphi(n)$$

verilir. Bunun yanında teorem 19 a göre $K^{(n)}$ cismi K nın bir cebirsel genişlemesidir ve 1 in K üzerindeki her primitif n inci kökü c için

$$K^{(n)} = K(c)$$

verilir. Özellikle K=Q için

$$[Q^{(n)} : Q] = \varphi(n)$$

verilir.

Tanım 21: $x^n-a\in K[x]$ $(n\in\mathbf{N})$ polinomunun K üzerindeki bir parçalayıcı cismindeki herhangi bir sıfır yerini $\sqrt[n]{a}$ ile gösterelim. $\sqrt[n]{a}$ elemanına, a nın K üzerindeki bir n inci kökü (veya a nın K üzerindeki n eksponentli bir radikali) denir. x^n-a polinomu K[x] halkasında indirgenemez ise, $\sqrt[n]{a}$ elemanına K üzerinde bir indirgenemez radikal denir.

Teorem 28: $k(K)=p>0$ olmak üzere $x^n-a\in K[x]$ $(a\neq 0,\ n\in\mathbf{N})$ polinomu gözönüne alınsın.

$$n=p^r m\ ,\ m\in\mathbf{N}\ ,\ r\in\mathbf{N}_0\ ,\ (p,m)=1$$

olsun. x^n-a polinomunun K üzerindeki bir parçalayıcı cismi L ve $\sqrt[n]{a}\in L$ tespit edilmiş bir radikal olsun. Bu takdirde L cismi 1 in K üzerindeki tüm m inci köklerini ihtiva eder ve a elemanının L cismindeki farklı n inci köklerinin tümü, c 1 in L deki bir primitif m inci kökü olmak üzere

$$\sqrt[n]{a}\ c^i\ ,\ i=0,1,\ldots,m-1$$

şeklindedir. Özellikle

$$L = K(\sqrt[n]{a}\ , c)$$

verilir.

Teorem 29: $p \in P$ olmak üzere $x^p - a \in K[x]$ polinomunun indirgenemez olabilmesi için gerek ve yeter koşul, bu polinomun K da bir sıfır yerine sahip olmamasıdır.

Tanım 22: $f(x) \in K[x]$ sabit olmayan bir polinom ve L f(x) polinomunun K üzerindeki bir parçalayıcı cismi olsun.

(a). f(x) polinomu L de sadece basit sıfır yerlerine sahip ise, f(x) e ayrılabilir polinom denir. Katlı sıfır yerlerine sahip bir polinoma ayrılamaz polinom denir.

(b). f(x) polinomunun L deki farklı sıfır yerlerinin sayısına, f(x) polinomunun indirgenmiş derecesi denir ve bu derece

$$d_i^o f(x)$$

ile gösterilir.

Teorem 30: $g(x) \in K[x]$ indirgenemez bir polinom olsun.

(a). $k(K)=0$ ise, g(x) polinomu ayrılabilirdir.

(b). $k(K)=p$ ise, g(x) polinomunun ayrılamaz olabilmesi için gerek ve yeter koşul, bir $h(x) \in K[x]$ polinomu için $g(x) = h(x^p)$ verilmesidir. r, bir $f(x) \in K[x]$ polinomu için

$$g(x) = f(x^{p^r})$$

olacak şekilde en büyük doğal sayı olsun. Bu takdirde

$$d_i^o g(x) = d^o f(x)$$

verilir ve g(x) polinomunun K üzerindeki bir parçalayıcı cismindeki her sıfır yerinin katlılığı p^r dir.

Tanım 23:

(a). t K üzerinde bir cebirsel eleman olsun. İnd(t,K) polinomu ayrılabilir ise, t ye K üzerinde ayrılabilir eleman ve İnd(t,K) polinomu ayrılamaz ise, t ye K üzerinde ayrılamaz eleman denir. İnd(t,K) polinomunun indirgenmiş derecesine t elemanının K üzerindeki indirgenmiş derecesi denir ve bu derece

$$[t : K]_i$$

ile de gösterilebilir.

(b). L K cisminin bir cebirsel genişlemesi olsun. L cisminin her elemanı K üzerinde ayrılabilir ise, L cismine K nın bir ayrılabilir genişlemesi (veya L cismi K üzerinde ayrılabilir) denir. L cisminin her elemanı K üzerinde ayrılabilir değil ise, L cismine K nın ayrılamaz genişlemesi (veya L cismi K üzerinde ayrılamaz) denir.

Teorem 31: L K cisminin bir ayrılabilir genişlemesi ve $K \subset U$ olmak üzere $U \subset L$ keyfi bir altcisim olsun. Bu takdirde L cismi U üzerinde de ayrılabilirdir.

Teorem 32: Bir L cisminin K nın bir cebirsel genişlemesi olabilmesi için gerek ve yeter koşul, $K \subset U \subset L$ olacak şekilde U cisimlerinin sayısının sonlu olmasıdır.

Teorem 3: (Primitif eleman teoremi) L cismi K nın sonlu bir genişlemesi ve

$$L = K(t_1,...,t_r)$$

olsun. $t_1,...,t_r \in L$ elemanları K üzerinde ayrılabilir iseler, L cismi K üzerinde bir primitif elemana sahiptir.

1.4. Cisim İzomorfileri

Teorem 34: $K \subset U \subset L$ cisim genişlemesi öyleki L K üzerinde sonlu ve normal olsun. U dan L nin bir genişlemesine her σ K- izomorfisi L nin bir K-otomorfisine genişletilebilir. Özellikle $U^\sigma \subset L$ verilir.

İspat: $u \in U$ keyfi bir eleman olsun. U cismi K üzerinde cebirsel olduğundan $\text{İnd}(u,K) \in K[x]$ polinomu mevcuttur.

$$\text{İnd}(u,K) = g(x) = \sum_{i=o}^{n} a_i x^i \ , \ a_n = 1$$

olsun. Bu takdirde

$$0 = g(u)^\sigma = (\sum_{i=o}^{n} a_i u^i)^\sigma = \sum_{i=o}^{n} a_i (u^\sigma)^i = g(u^\sigma)$$

olduğundan, u^σ elemanı da g(x) polinomunun bir sıfır yeridir. L cismi K üzerinde normal olduğundan g(x) polinomu L[x] halkasının lineer polinomlarının bir çarpımı şeklindedir. Buna göre $u^\sigma \in L$ dir ve dolayısıyla $U^\sigma \subset L$ elde edilir.

Teorem 24 e göre, L bir $f(x) \in K[x]$ polinomunun K üzerindeki bir parçalayıcı cismidir. teorem 22 ye göre, σ K-izomorfisi L cisminin bir K-otomorfisine genişletilebilir.

Teorem 35: $K \subset L \subset M$ cisim genişlemesi verilsin. Öyleki $|L:K| < \infty$ ve M K üzerinde normal olsun. L cisminin K üzerinde normal olabilmesi için gerek ve yeter koşul, L cismini M cismi içine resmeden her K- izomorfisinin L in bir K-otomorfisi olmasıdır.

İspat: L K üzerinde normal olsun. Bu takdirde teorem 34 e göre, L cismini M in içine resmeden her K-izomorfisi, L cisminin bir K- otomorfisidir.

L cismini M in içine resmeden her K-izomorfi, L in bir K-otomorfisi olsun. $g(x)\in K[x]$ bir indirgenemez monik polinom ve $a\in L$ bu polinomun bir sıfır yeri olsun. $[L:K]<\infty$ olduğundan teorem 20 ye göre, K üzerinde cebirsel olan sonlu sayıda $t_1,...,t_r\in L$ elemanları

$$L = K(t_1,...,t_r)$$

olacak şekilde mevcutturlar. M K üzerinde normal olduğundan, M cismi

$$g(x) = \left(\prod_{i=1}^{r} \text{İnd}(t_i,K)\right) \in K[x]$$

polinomunun K üzerindeki bir M_0 parçalayıcı cismini içerir. g(x) polinomunun M_0 da bulunan keyfi bir b sıfır yeri gözönüne alınsın. Teorem 16 ya göre, $a^\beta=b$ olacak şekilde bir

$$\beta : K(a) \to K(b)$$

K-izomorfisi mevcuttur. $K \subset K(a) \subset M_0$ dır ve M_0 cismi K üzerinde sonlu ve normal olduğundan teorem 34 e göre, β izomorfisi M_0 cisminin bir γ K-otomorfisine genişletilebilir. $\gamma\downarrow L$ dönüşümü L cismini M içine resmeden bir K-izomorfidir ve kabule göre L cisminin bir K-otomorfisidir. Dolayısıyla

$$b = a^\gamma \in L$$

elde edilir. Buna göre g(x) polinomu L[x] halkasının lineer polinomlarının bir çarpımı şeklinde yazılabilir. Dolayısıyla L, g(x) polinomunun K üzerindeki bir parçalayıcı cismi olduğundan teorem 24 e göre, L cismi K üzerinde normaldir.

Teorem 36: L cismi K nın sonlu bir genişlemesi ve

$$L = K(t_1,...,t_r)$$

olsun.

$$d_j^0 \text{ İnd}(t_j , K(t_1,...,t_{j-1})) = [t_j:K(t_1,...,t_{j-1})]_i=m_j \ , \ j=1,...,r$$

ve L cismini L in bir M genişlemesi içine resmeden tüm K-izomorfilerin sayısı m ise

$$m \le \prod_{j=1}^{r} m_j$$

verilir. Bu ifadedeki eşitlik, M cisminin K üzerinde normal olması halinde verilir.

İspat: İspat r üzerinden tümevarımla yapılacaktır. r=0 için L=K olduğundan iddia doğrudur. r>0 ve iddianın r-1 için doğru olduğu kabul edilsin. Bu takdirde

$$L' = K(t_1,...,t_{r-1})$$

cismini M genişlemesinin içine resmeden $\sigma_1,...,\sigma_{m'}$, K izomorfileri mevcut ve

$$m' \le \prod_{j=1}^{r-1} m_j \qquad (1)$$

olsun. $L=K(t_1,...,t_{r-1},t_r) = L'(t_r)$ cismini M cismi içine resmeden K- izomorfileri, σ_j dönüşümlerinin L üzerine genişletilmişleri arasında aranır.

$$\sigma \in \{\sigma_1,...,\sigma_{m'}\}$$

böyle bir K-izomorfi olsun:

$$\sigma\uparrow L : L = L'(t_r) \rightarrow M.$$

Bunun yanında

$g(x)=\text{İnd}(t_r,L') = \sum_i a_i x^i \in L'[x]$ ve $\bar{g}(x) = \sum_i a_i^{\sigma} x^i \in L'^{\sigma}[x]$ olmak üzere, $g(x)$ polinomunun L' üzerindeki bir parçalayıcı cismi F ve $\bar{g}(x)$ polinomunun L'^{σ} üzerindeki bir parçalayıcı cismi G olsun. Bu takdirde teorem 22 ye göre, σ izomorfisi F cismini G cismine resmeden bir K-izomorfiye genişletilebilir. Dolayısıyla $g(x)$ ve $\bar{g}(x)$ polinomlarının indirgenmiş dereceleri eşittir:

$$d_i^0 g(x) = d_i^0 \bar{g}(x).$$

Bu ortak indirgenmiş derece m_r ve $\bar{g}(x)$ polinomunun M cismindeki farklı sıfır yerlerinin sayısı m" olsun. Bu takdirde

$$m'' \leq m_r \qquad (2)$$

dir. $L'(t_r) = L$ cismini M cismi içine resmeden ve σ dönüşümünün genişletilmişi olan K-izomorfilerinin sayısı, teorem 16 (b) ye göre m" dir. σ dönüşümü için m' sayıda seçenek mümkün olduğundan (1) ve (2) ifadeleri yardımıyla L cismini M cismi içine resmeden en fazla

$(m_1 \ldots m_{r-1})\, m_r$ sayıda K-izomorfinin mevcut olduğu elde edilir.

M cismi K üzerinde normal olsun. Bu takdirde

$$m = \prod_{i=1}^{r} m_i$$

ifadesi r e göre tümevarımla ispatlanır. r-1 için iddia doğru olsun.

$$m' = \prod_{i=1}^{r-1} m_i .$$

M cismi

$$\prod_{i=1}^{r} \text{İnd}(t_i,K) \in K[x]$$

polinomunun K üzerindeki bir M_0 parçalayıcı cismini ihtiva eder. L'[x] halkasında

$$g(x) \mid \text{İnd}(t_r,K)$$

olduğundan g(x) polinomu $M_0[x]$ halkasının lineer polinomlarının bir çarpımı şeklindedir. M_0 cismi K üzerinde sonlu ve normal olduğundan teorem 34 e göre, σ dönüşümü M_0 cisminin bir τ K-otomorfisine genişletilebilir. Teorem 16 (b) ye göre, τ dönüşümü g(x) polinomunun sıfır yerlerini $\bar{g}(x)$ polinomunun sıfır yerlerine resmettiğinden, $\bar{g}(x)$ polinomu M cisminde en az m_r farklı sayıda sıfır yerine sahiptir. Bunun yardımıyla (2) ifadesine göre

$$m'' = m_r$$

ve dolayısıyla

$$m = \prod_{j=1}^{r} m_j$$

elde edilir.

Uyarı 5: Uyarı 2 deki L cismini M cismi içine resmeden tüm K-izomorfiler, teorem 16 yardımıyla şu şekilde bulunur: Önce $K(t_1)$ cismini M içine resmeden tüm K- izomorfiler bulunur. Bu izomorfilerin her birisi mümkün olan tüm haller için

$$K(t_1)(t_2) = K(t_1,t_2)$$

üzerine genişletilir. Bu genişletilmiş izomorfilerin her birisi mümkün olan tüm haller için

$$K(t_1,t_2)(t_3) = K(t_1,t_2,t_3)$$

üzerine genişletilir ve bu işleme devam edilerek r adım sonunda

$$L = K(t_1,...,t_r)$$

cismini M içine resmeden tüm K--izomorfiler elde edilmiş olur.

Tanım 24: Teorem 26 ya göre

$$L = K(t_1,...,t_r)$$

cisminin en az bir M genişlemesi, M K üzerinde normal olacak şekilde mevcuttur. L cismini M içine resmeden tüm K-izomorfilerin sayısı, teorem 36 ya göre

$$m = \prod_{j=1}^{r} m_j$$

dir ve bu sayı, L cisminin K üzerindeki $t_1,...,t_r$ üretici elemanlarına bağlı değildir. K ve L ile tektürlü olarak belirli olan bu m sayısına, L cisminin K üzerindeki indirgenmiş derecesi (veya ayrılabilirlik derecesi) denir ve bu derece

$$[L : K]_i$$

ile gösterilir.

Teorem 37: K cisminin her L sonlu genişlemesi için

$$[L : K]_i \leq [L : K]$$

verilir. Bu ifadedeki eşitlik, ancak ve ancak L cisminin K üzerinde ayrılabilir olması halinde verilir.

İspat: $L= K(t_1,...,t_r)$ ve $[t_j : K(t_1...,t_{j-1})]=n_j$, $[t_j : K(t_1,...,t_{j-1})]_i = m_j$, $j=1,...,r$ olsun. Bu takdirde teorem 9 (a) yardımıyla

$$[K(t_1) : K]\,[K(t_1,t_2) : K(t_1)] \ldots [K(t_1,...,t_r) : K(t_1,...,t_{r-1})] = [L:K] = \prod_{j=1}^{r} n_j \quad (3)$$

elde edilir.

L cismi K üzerinde ayrılamaz olsun. Bu takdirde K üzerinde ayrılamaz olan bir $t \in L$ elemanı mevcuttur. $L = K(t,t_1,...,t_r)$ olduğundan, örneğin $t=t_1$ seçilebilir. $m_1<n_1$ ve $j>1$ için $m_j \leq n_j$ olduğundan (3) ifadesi ve teorem 36 yardımıyla

$$[L:K]_i = \prod_{j=1}^{r} m_j < \prod_{j=1}^{r} n_j = [L:K]$$

elde edilir.

L cismi K üzerinde ayrılabilir olsun. Bu takdirde teorem 31 e göre, her t_j elemanı $K(t_1,...,t_{j-1})$ üzerinde ayrılabilir olduğundan $j=1,...,r$ için $m_j = n_j$ ve (3) ifadesi ve teorem 36 yardımıyla

$$[L:K] = [L:K]_i$$

elde edilir.

Teorem 38: t_j elemanı $K(t_1,...,t_{j-1})$ $(j=1,...,r)$ üzerinde ayrılabilir ise $K(t_1,...,t_r)$ cismi K üzerinde ayrılabilirdir.

İspat: İddianın ispatı teorem 37 den elde edilir.

Tanım 25: L K cisminin bir genişlemesi ve L cisminin K üzerindeki ayrılabilir elemanlarının tümü L_a ile gösterilsin. L_a cismine K nın L deki ayrılabilir kapanışı denir.

Teorem 39: $k(K)=p>0$ ve L cismi K nın bir cebirsel genişlemesi olsun. Bu takdirde $b \in L$ için daima

$$L(\sqrt[p]{b})_a = L_a$$

verilir.

İspat: $\sqrt[p]{b} \notin L$ olduğu kabul edilebilir. Her $t \in L(\sqrt[p]{b}) - L$ elemanının K üzerinde ayrılamaz olduğunu göstermek, iddianın ispatı için yeterlidir. $x^p - b \in L[x]$ polinomu teorem 29 a göre indirgenemezdir ve teorem 30 (b) ye göre ayrılamazdır. Özellikle

$$\text{İnd}\,(\sqrt[p]{b}, L) = x^p - b \quad \text{ve} \quad [L(\sqrt[p]{b}) : L] = [\sqrt[p]{b} : L] = p$$

dir. $t \notin L$ olduğundan $[L(t) : L] > 1$ dir ve teorem 9 (a) ya göre

$$[L(\sqrt[p]{b}) : L] = [L(\sqrt[p]{b}) : L(t)]\,[L(t) : L]$$

olduğundan

$$[L(t) : L] \mid p$$

verilir. Dolayısıyla

$$[L(t) : L] = p \quad \text{ve} \quad L(t) = L(\sqrt[p]{b})$$

elde edilir. t elemanının K üzerinde ayrılabilir olduğu kabul edilsin. Bu takdirde teorem 31 e göre, t elemanı L üzerinde de ayrılabilirdir. Dolayısıyla teorem 38 e göre, L(t) cismi L in ayrılabilir bir genişlemesidir. Bu sonuç , $\sqrt[p]{b}$ elemanının L üzerinde ayrılamaz olmasına aykırıdır.

Bir L cismini diğer bir M cismine resmeden tüm dönüşümlerin kümesini D(L,M) ile gösterelim. $\sigma, \rho \in D(L,M)$ ve $m \in M$ olmak üzere her $a \in L$ için

$$a^{\sigma+\rho} = a^\sigma + a^\rho \quad \text{ve} \quad a^{m\sigma} = ma^\sigma$$

yardımıyla tanımlanan işlemlere göre, D(L,M) M üzerinde bir vektör uzayıdır. Aşağıdaki teorem yardımıyla, L cismini M içine resmeden sonlu ve ikişer tarzda farklı izomorfilerden oluşan her sistemin M üzerinde lineer bağımsız olduğu elde edilir.

Teorem 40: (Dedekind) L ve M iki cisim ve $\sigma_1,\ldots,\sigma_n \in D(L,M)$ sonlu sayıda ve ikişer tarzda farklı izomorfiler olsunlar. Bu takdirde $a_i \in M$ $(i=1,\ldots,n)$ ler hepsi birden sıfır olmayan elemanlar olmak üzere, her $(a_1,\ldots,a_n)$ n- sıralısına mukabil bir $t \in L$ elemanı

$$\sum_{i=1}^{n} a_i t^{\sigma_i} \neq 0$$

olacak şekilde mevcuttur.

İspat: İddianın doğru olmadığı kabul edilsin. Bu takdirde σ_i izomorfileri uygun bir şekilde numaralanarak $r \leq n$ olmak üzere bir $r \in N$ sayısı ve hepsi birden sıfır olmayan $a_1,\ldots,a_r \in M$ elemanları, her $t \in L$ için

$$\sum_{i=1}^{r} a_i t^{\sigma_i} = 0 \qquad (4)$$

olacak şekilde mevcutturlar. r sayısı, (4) ifadesini gerçekleyen minimal sayı olarak seçilsin. $r>1$ dir. Zira, $r=1$ halinde (4) ifadesinden $1^{\sigma_1}=0$ elde edilir. $\sigma_1 \neq \sigma_r$ olduğundan bir $s \in L$ elemanı $s^{\sigma_1} \neq s^{\sigma_r}$ olacak şekilde mevcuttur. (4) ifadesinde t yerine st yazılırsa

$$\sum_{i=1}^{r} a_i s^{\sigma_i} t^{\sigma_i} = 0 \qquad (5)$$

elde edilir. (1) ifadesi s^{σ_r} ile çarpılır ve (5) ifadesinden çıkarılırsa, her $t \in L$ için

$$a_1(s^{\sigma_1} - s^{\sigma_r}) t^{\sigma_1} + \ldots + a_{r-1} (s^{\sigma_{r-1}} - s^{\sigma_r}) t^{\sigma_{r-1}} = 0 \qquad (6)$$

elde edilir.

$$a_1(s^{\sigma_1} - s^{\sigma_r}) \neq 0$$

olduğundan, (6) ifadesi r sayısının minimal oluşuna aykırıdır.

2. TEORİK ÇALIŞMALAR (Galois Teorisi)

2.1 Galois Genişlemeleri

Tanım 26:

(a). L cismi K nın bir genişlemesi olsun. $K \subset U$ olmak üzere, bir $U \subset L$ altcismine L cisminin K üzerindeki bir aracismi denir.

(b). U, L cisminin K üzerindeki bir aracismi olsun. L cisminin tüm U-otomorfilerinin kümesini

$$G(\frac{L}{U})$$

ile gösterelim.

Uyarı 6: Bir L cisminin tüm U-otomorfilerinin kümesi $G(\frac{L}{U})$, otomorfilerin çarpımı (bileşkesi) işlemine göre bir gruptur.

Tanım 27:

(a). Bir $H \subset G(\frac{L}{K})$ kompleksi gözönüne alınsın. H kompleksinin her K-otomorfisi için sabit kalan $a \in L$ elemanlarının kümesini S(H) ile gösterelim.

$$S(H) = \{a | a \in L, \forall \sigma \in H \text{ için } a^{\sigma} = a\}.$$

L cisminin K üzerinde bir aracismi olan S(H) cismine, L cisminde H kompleksine göre sabit kalan cisim denir.

(b). $G(\frac{L}{K})$ grubuna L cisminin K-otomorfiler grubu denir.

Uyarı 7: U L cisminin K üzerindeki bir aracismi olsun. Bu takdirde her

$$\sigma \in G(\frac{L}{U})$$

için $\sigma \in G(\frac{L}{K})$ olduğundan

$$G(\frac{L}{U}) \leq G(\frac{L}{K})$$

dır. O halde L cisminin K üzerindeki her U aracismine $G(\frac{L}{K})$ grubunun bir $G(\frac{L}{U})$ altgrubu tekabül ettirilebilir. Tersine olarak $G(\frac{L}{K})$ grubunun her H altgrubuna, L cisminin K üzerindeki bir S(H) aracismi tekabül ettirilebilir. L cisminin K üzerindeki aracisimleri ile $G(\frac{L}{K})$ grubunun altgrupları arasında tesis edilen bu tekabülün bire-bir olabilmesi için

$$S(G(\frac{L}{K})) = K$$

şartı gereklidir.

Tanım 28: L cismi K nın sonlu bir genişlemesi olmak üzere

$$S(G(\frac{L}{K})) = K$$

gerçeklenirse, L cismine K nın bir Galois genişlemesi denir. $G(\frac{L}{K})$ grubuna da L cisminin K üzerindeki Galois grubu denir.

Teorem 41: L cismi K nın bir genişlemesi olsun. Bu takdirde aşağıdaki ifadeler birbirlerine denktirler:

(a). L cismi, K nın bir Galois genişlemesidir.

(b). L cismi, K nın sonlu, normal ve ayrılabilir bir genişlemesidir.

(c). L, K[x] halkasının bir ayrılabilir polinomunun K üzerindeki bir parçalayıcı cismidir.

(d). $|G(\frac{L}{K})| = [L : K] < \infty$ verilir.

İspat:

(a). ⇒ (b). $t \in L$ ve

$$\text{İnd}(t,K) = g(x) \in K[x]$$

olsun. g(x) polinomunun ayrılabilir olduğunu ve bu polinomun L[x] halkasının lineer polinomlarının bir çarpımı şeklinde yazılabildiğini göstermek, iddianın ispatı için yeterlidir. Her $\sigma \in G(\frac{L}{K})$ için t^σ resim elemanları arasında farklı olanlar $t_1,...,t_r \in L$ olsunlar. Bu takdirde

$$t_1^\sigma, t_2^\sigma, \dots, t_r^\sigma \in L$$

elemanları, $t_1,...,t_r$ elemanlarının farklı bir sırada yazılışından ibarettir. Dolayısıyla bir

$$\pi = \begin{pmatrix} i \\ i\pi \end{pmatrix} \in S_r$$

için

$$t_i^\sigma = t_{i\pi} \quad , \quad i=1,...,r$$

yazabiliriz. $t_1 = t$ olmak üzere

$$h(x) = \prod_{i=1}^{r} (x - t_i) = \sum_{i=0}^{r} a_i x^{r-i} \in L[x] \ , \ a_0 = 1$$

polinomunu teşkil edelim. Her $\pi \in S_r$ için

$$\prod_{i=1}^{r} (x - t_{i\pi}) = \prod_{i=1}^{r} (x - t_i)$$

olup,

$$s_i = s_i(t_1,...,t_r) \ , \ i=1,...,r$$

elemanter simetrik polinomlar olmak üzere

$$a_i = (-1)^i s_i \ , \ i=1,...,r$$

dir. Dolayısıyla $\sigma \in G(\frac{L}{K})$ için

$$a_i^{\sigma} = a_i \ , \ i=1,...,r$$

verilir. Buradan

$$a_i \in S(G(\frac{L}{K})) = K \ , \ i=1,...,r$$

ve dolayısıyla $h(x) \in K[x]$ elde edilir. h(x) ayrılabilir bir polinom ve t elemanı h(x) polinomunun bir sıfır yeri olduğundan teorem 14 (a) ya göre, K[x] halkasında

$$g(x) \mid h(x)$$

verilir. Buna göre g(x) ayrılabilir bir polinomdur ve bu polinom, L[x] halkasının lineer polinomlarının bir çarpımı şeklindedir.

(b). ⇒ (c). Teorem 24 e göre, L bir $f(x) \in K[x]$ polinomunun K üzerindeki bir parçalayıcı cismidir. f(x) polinomunun K[x] halkasındaki farklı ve indirgenemez monik bölenlerinin bir çarpımı şeklinde olan bir $g(x) \in K[x]$ polinomunu gözönüne alalım. L cismi K üzerinde ayrılabilir olduğundan, g(x) polinomu ayrılabilirdir ve L cismi aynı zamanda g(x) polinomunun K üzerindeki bir parçalayıcı cismidir.

(c). ⇒ (d). L ayrılabilir bir polinomun K üzerinde bir parçalayıcı cismi olduğundan teorem 21, 24 ve 38 e göre, L cismi K nın sonlu, normal ve ayrılabilir bir genişlemesidir. Teorem 36 da M = L alınarak teorem 37 yardımıyla

$$\mid G(\frac{L}{K}) \mid = [L : K]_i = [L : K]$$

elde edilir.

(d). ⇒ (a). $K \subseteq S(G(\frac{L}{K}))$ dır. $S(G(\frac{L}{K})) \subseteq K$ olduğunu görmek için şu yol izlenir: M cismi L in bir genişlemesi ve M K üzerinde normal olsun. L cismini M cismi içine resmeden K- izomorfilerinin sayısı teorem 36 ve tanım 24 e göre $[L : K]_i$ dir. teorem 37 ye göre

$$[L : K]_i \geq \mid G(\frac{L}{K}) \mid = [L : K] \geq [L : K]_i$$

olduğundan

$$[L : K]_i = [L : K]$$

elde edilir. Buna göre L cismini M içine resmeden her K- izomorfi, L cisminin bir K- otomorfisidir ve L cismi K nın ayrılabilir bir genişlemesidir. Teorem 35 e göre, L cismi K üzerinde normaldir. $t \in S(G(\frac{L}{K}))$ olmak üzere

$$g(x) = \text{İnd}(t,K) \in K[x]$$

ve $s \in L$ elemanı $g(x)$ polinomunun L deki keyfi bir sıfır yeri olsun. Teorem 17 ye göre $t^{\sigma} = s$ ile belirlenen bir

$$\sigma : K(t) \rightarrow K(s)$$

K- izomorfisi mevcuttur. Teorem 34 e göre σ K- izomorfisi L cisminin bir $\tau \in G(\frac{L}{K})$ K- otomorfisine genişletilebilir. Dolayısıyla

$$t = t^{\tau} = s$$

elde edilir. L cismi K üzerinde ayrılabilir olduğundan g(x) ayrılabilir bir polinomdur. L cismi K üzerinde normal olduğundan g(x) polinomu L[x] halkasının lineer polinomlarının bir çarpımı şeklindedir. Buna göre

$$g(x) = x - t \in K[x]$$

ve dolayısıyla $t \in K$ dır. Bunun yardımıyla

$$S(G(\frac{L}{K})) \subseteq K$$

elde edilir.

$$S(G(\frac{L}{K})) = K$$

olduğundan L cismi K nın bir Galois genişlemesidir.

Teorem 42: L cismi K nın bir Galois genişlemesi ve $U \subset L$, K üzerinde bir aracisim olsun. Bu takdirde L cismi aynı zamanda U aracisminin de bir Galois genişlemesidir:

$$S(G(\frac{L}{U})) = U .$$

İspat: L cismi U aracisminin sonlu, normal ve ayrılabilir bir genişlemesi olduğundan teorem 41 e göre, L cismi U nun bir Galois genişlemesidir.

Teorem 43: (Galois teorisinin esas teoremi) L cismi K nın bir Galois genişlemesi, L cisminin K üzerindeki tüm aracisimlerinin kümesi **U** ve $G(\frac{L}{K})$ Galois grubunun tüm altgruplarının kümesi **H** olsun.

(a). $U \in \mathbf{U}$ için

$$U \rightarrow G(\frac{L}{U})$$

tekabülü, **U** kümesini **H** kümesine resmeden bir bire-bir ve örten dönüşümdür.

(b). $H \in \mathbf{H}$ için

$$H \rightarrow S(H)$$

tekabülü, **H** kümesini **U** kümesine resmeden bir bire-bir ve örten dönüşümdür ve bu dönüşüm (a) daki dönüşümün inversidir.

(c). Her $U \in \mathbf{U}$ ve her $H \in \mathbf{H}$ için

$$|G(\frac{L}{U})| = [L : U] \ , \ [S(H) : K] = [G(\frac{L}{K}) : H]$$

verilir.

İspat: $U \in \mathbf{U}$ olsun. Teorem 42 ye göre, L cismi U aracisminin bir Galois genişlemesi olduğundan

$$S(G(\frac{L}{U})) = U$$

verilir. Dolayısıyla teorem 41 e göre

$$|G(\frac{L}{U})| = [L : U]$$

elde edilir.

$H \in \mathbf{H}$ olsun. Teorem 41 ve 33 e göre, bir $t \in L$ elemanı

$$L = K(t)$$

olacak şekilde mevcuttur. $H = \{\sigma_1 , ..., \sigma_n\}$ $(\sigma_1 = \varepsilon)$ olsun ve

$$t^{\sigma_i} = t_i \ , \ i=1,...,n$$

olmak üzere

$$f(x) = \prod_{i=1}^{n} (x - t_i) = \sum_{i=0}^{n} a_i x^{n-i} \in L[x] \ , \ a_0 = 1$$

polinomunu teşkil edelim. H bir grup olduğundan keyfi bir $\sigma \in H$ için $\pi = \begin{pmatrix} i \\ i\pi \end{pmatrix} \in S_n$ olmak üzere

$$\sigma_i \sigma = \sigma_{i\pi} \ , \ i=1,...,n$$

yazılabilir. Her $\pi \in S_n$ için

$$\prod_{i=1}^{n} (x - t_i^{\sigma}) = \prod_{i=1}^{n} (x - t_{i\pi}) = \prod_{i=1}^{n} (x - t_i)$$

olup,

$$s_i = s_i(t_1 , ..., t_n) \ , \ i=1,...,n$$

elemanter simetrik polinomlar olmak üzere

$$a_i = (-1)^i s_i \ , \ i=1,...,n$$

dir. Dolayısıyla her $\sigma \in H$ için

$$a_i^{\sigma} = a_i \ , \ i=1,...,n$$

verilir. Buna göre

$$a_i \in S(H) \ , \ i=1,...,n$$

ve dolayısıyla

$$f(x) \in S(H)[x]$$

elde edilir. Teorem 41 yardımıyla

$$n = |H| = d^0 f(x) \geq d^0 \text{ ind}(t, S(H)) = [S(H)(t) : S(H)]$$
$$= [L : S(H)] = |G(\frac{L}{S(H)})|$$

yazılabilir. Buna göre

$$G(\frac{L}{S(H)}) \leq H$$

verilir. Diğer taraftan

$$H \leq G(\frac{L}{S(H)})$$

olduğundan

$$G(\frac{L}{S(H)}) = H$$

elde edilir.

$$S(G(\frac{L}{U})) = U \text{ ve } G(\frac{L}{S(H)}) = H$$

ifadelerinden teoremin (a) ve (b) şıklarında sözü geçen tekabüllerden birisinin diğerinin inversi olduğu elde edilir. Dolayısıyla bu tekabüller bire-bir ve örten dönüşümlerdir.

Her $H \in \mathbf{H}$ için teorem 9 (a) ve teorem 41 yardımıyla

$$[S(H) : K] = [L : K]\,[L : S(H)]^{-1} = |G(\frac{L}{K})|\,|G(\frac{L}{S(H)})|^{-1}$$
$$= |G(\frac{L}{K})|\,|H|^{-1} = [G(\frac{L}{K}) : H]$$

elde edilir.

Teorem 44: L cismi K nın bir Galois genişlemesi, U ve V L cisminin K üzerindeki iki aracismi ve $G(\frac{L}{U}) = H$, $G(\frac{L}{V}) = F$ olsun.

(a). $U \subseteq V$ ile $F \leq H$ denktir.

(b). $G(\frac{L}{U \cap V}) = \langle H \cup F \rangle$.

(c). $G(\frac{L}{U(V)}) = H \cap F$.

İspat:

(a). $U \subseteq V$ den

$$F = G(\frac{L}{V}) \leq G(\frac{L}{U}) = H$$

elde edilir. Tersine olarak $F \leq H$ dan

$$U = S(H) \subseteq S(F) = V$$

elde edilir.

(b). $H \leq \langle H \cup F \rangle$ ve $F \leq \langle H \cup F \rangle$ ifadelerinden (a) ya göre

$$S(\langle H \cup F \rangle) \subseteq U \quad ve \quad S(\langle H \cup F \rangle) \subseteq V$$

ve dolayısıyla

$$S(\langle H \cup F \rangle) \subseteq U \cap V$$

yazılabilir. Bunun yardımıyla

$$G(\frac{L}{U \cap V}) \leq G(\frac{L}{S(\langle H \cup F \rangle)}) = \langle H \cup F \rangle$$

elde edilir. Diğer taraftan $\langle H \cup F \rangle$ grubunun otomorfileri $U \cap V$ cisminin elemanlarını da sabit bıraktığından $U \cap V \subseteq S(\langle H \cup F \rangle)$ ve bunun yardımıyla

$$\langle H \cup F \rangle = G(\frac{L}{S(\langle H \cup F \rangle)}) \leq G(\frac{L}{U \cap V})$$

elde edilir.

(c). $H \cap F \leq H$ ve $H \cap F \leq F$ ifadelerinden (a) ya göre

$$U = S(H) \subseteq S(H \cap F) \quad ve \quad V = S(F) \subseteq S(H \cap F)$$

ve bu ifadeler yardımıyla da

$$U(V) \subseteq S(H \cap F)$$

yazılabilir. Bunun yardımıyla

$$H \cap F = G(\frac{L}{S(H \cap F)}) \leq G(\frac{L}{U(V)})$$

elde edilir. Diğer taraftan $U \subseteq U(V)$ ve $V \subseteq U(V)$ ifadelerinden (a) yardımıyla

$$G(\frac{L}{U(V)}) \leq G(\frac{L}{U}) = H \quad ve \quad G(\frac{L}{U(V)}) \leq G(\frac{L}{V}) = F$$

yazılabilir. Buradan

$$G(\frac{L}{U(V)}) \leq H \cap F$$

elde edilir.

Teorem 45: L cismi K nın bir Galois genişlemesi olsun. L cisminin K üzerindeki her U aracismi için aşağıdaki ifadeler gerçeklenir.

(a). Her $\sigma \in G(\frac{L}{K})$ için

$$G(\frac{L}{U^{\sigma}}) = \sigma\, G(\frac{L}{U})\sigma^{-1}$$

verilir.

(b). U aracisminin K nın bir Galois genişlemesi olabilmesi için gerek ve yeter koşul,

$$G(\frac{L}{U}) \trianglelefteq G(\frac{L}{K})$$

olmasıdır. Bu halde

$$G(\frac{U}{K}) \cong G(\frac{L}{K}) / G(\frac{L}{U})$$

verilir.

İspat:

(a). Her $\sigma \in G(\frac{L}{K})$ için

$$G(\frac{L}{U^\sigma}) = \{ \tau \mid \tau \in G(\frac{L}{K}) \ , \ \text{her } u \in U \text{ için } (u^\sigma)^\tau = u^\sigma \}$$

$$= \{ \tau \mid \tau \in G(\frac{L}{K}) \ , \ \text{her } u \in U \text{ için } u^{\sigma\tau\sigma^{-1}} = u \}$$

$$= \{ \sigma\tau\sigma^{-1} \mid \tau \in G(\frac{L}{K}) \text{, her } u \in U \text{ için } u^\tau = u \}$$

$$= \{ \sigma\tau\sigma^{-1} \mid \tau \in G(\frac{L}{U}) \}$$

$$= \sigma \, G(\frac{L}{U}) \sigma^{-1}$$

elde edilir.

(b). L cismi K üzerinde ayrılabilir olduğundan, teorem 31 e göre U aracismi de K üzerinde ayrılabilirdir. O halde U aracisminin K nın bir Galois genişlemesi olabilmesi için gerek ve yeter koşul, teorem 41 e göre U aracisminin K üzerinde normal olmasıdır. Diğer taraftan teorem 35 e göre U aracisminin K üzerinde normal olabilmesi için gerek ve yeter koşul, U cismini L cismi içine resmeden her σ K- izomorfinin U cisminin bir K- otomorfisi olmasıdır. Bu gerek ve yeter koşul, $U^\sigma = U$ olmasına denktir. Diğer taraftan teorem 34 e göre σ K- izomorfisi L üzerine genişletilebileceğinden, σ K- izomorfisi $G(\frac{L}{K})$ grubunun bir elemanı olarak ele alınabilir. (a) ya göre, her $\sigma \in G(\frac{L}{K})$ için

$$\sigma \, G(\frac{L}{U}) \, \sigma^{-1} = G(\frac{L}{U})$$

gerçeklendiğinden

$$G(\frac{L}{U}) \trianglelefteq G(\frac{L}{K})$$

elde edilir. Teorem 35 e göre U aracismini L cismi içine resmeden her K- izomorfi, U aracisminin bir K- otomorfisi olduğundan her $\sigma \in G(\frac{L}{K})$ için $\sigma\downarrow U \in G(\frac{U}{K})$ dır. Buna göre her $\sigma \in G(\frac{L}{K})$ için

$$f(\sigma) = \sigma\downarrow U$$

ile belirlenen bir

$$f: G(\frac{L}{K}) \rightarrow G(\frac{U}{K})$$

dönüşümü tanımlanabilir. Teorem 34 e göre $G(\frac{U}{K})$ nın her otomorfisi L in bir K- otomorfisine genişletilebileceğinden, f örten bir dönüşümdür. Her $\sigma,\tau \in G(\frac{L}{K})$ için

$$f(\sigma\tau) = \sigma\tau\downarrow U = (\sigma\downarrow U)\,(\tau\downarrow U) = f(\sigma)\, f(\tau)$$

olduğundan f bir homomorfidir.

$$\text{Çek } f = \{ \sigma \mid \sigma \in G(\frac{L}{K}) \ , \ f(\sigma) = \sigma\downarrow U = \varepsilon \}$$

$$= \{ \sigma \mid \sigma \in G(\frac{L}{K}) \text{ , her } u \in U \text{ için } u^{\sigma} = u \}$$

$$= G(\frac{L}{U})$$

olduğundan grupların homomorfi teoremine göre

$$G(\frac{U}{K}) \cong G(\frac{L}{K}) / G(\frac{L}{U})$$

elde edilir.

Teorem 46: L cismi K nın bir Galois genişlemesi olsun. L cisminin bir K- tabanı $\{t_1,....,t_m\}$ ve bir $H \leq G(\frac{L}{K})$ altgrubu verilmiş olsun. Bu takdirde H altgrubuna tekabül eden aracisim

$$B_H(t) = \sum_{\sigma \in H} t^{\sigma} \text{ , } t \in L$$

olmak üzere

$$S(H) = \sum_{i=1}^{m} K B_H(t_i) = K(B_H(t_1) ,...., B_H(t_m))$$

şeklindedir.

İspat: $M = \{B_H(t) \mid t \in L\} \subset L$ kümesini gözönüne alalım. Her $\tau \in H$ ve $t \in L$ için

$$B_H(t)^{\tau} = \sum_{\sigma \in H} t^{\sigma\tau} = \sum_{\sigma \in H} t^{\sigma} = B_H(t)$$

olduğundan $B_H(t) \in S(H)$ ve dolayısıyla

$$M \subseteq S(H)$$

elde edilir. Diğer taraftan teorem 40 a göre $B_H(s) \neq 0$ olacak şekilde bir $s \in L$ elemanı mevcuttur. Bu takdirde her $u \in S(H)$ için

$$B_H(B_H(s)^{-1} us) = \sum_{\sigma \in H} (B_H(s)^{-1} us)^{\sigma} = \sum_{\sigma \in H} B_H(s)^{-1} us^{\sigma} = uB_H(s)^{-1} \sum_{\sigma \in H} s^{\sigma} = u$$

olduğundan $u \in M$ ve dolayısıyla

$$S(H) \subseteq M$$

elde edilir. O halde M = S(H) dır. Bunun yanında

$$L = \sum_{i=1}^{n} Kt_i = \{ \sum_{i=1}^{m} a_i t_i \mid a_i \in K \}$$

olduğundan

$$S(H) = M = \{ B_H(t) \mid t \in L\} = \{ B_H(\sum_{i=1}^{m} a_i t_i) \mid a_i \in K\}$$

$$= \{ \sum_{i=1}^{m} a_i B_H(t_i) \mid a_i \in K\}$$

$$= \sum_{i=1}^{m} KB_H(t_i)$$

$$= K(B_H(t_1), \ldots, B_H(t_m))$$

elde edilir.

2.2 Galois Grubunun Belirlenmesi

Teorem 47: L cismi K nın bir Galois genişlemesi, t L cisminin K üzerinde bir primitif elemanı ve t elemanının K üzerindeki eşlenik elemanlarının bir tam sistemi $\{t_1,\ldots,t_m\}$, $t_1=t$ olsun. Bu takdirde σ_i ler

$$t^{\sigma_i} = t_i \ , \ i = 1,\ldots,m$$

ile belirlenen dönüşümler olmak üzere

$$G(\frac{L}{K}) = \{\sigma_1, \ldots, \sigma_m\}$$

dir.

İspat: Teorem 16 ya göre, L cismini kendi içine resmeden tam m tane K- izomorfi vardır. Bu izomorfiler

$$t^{\sigma_i} = t_i \ , \ i = 1,\ldots,m$$

ile belirlenir. Zira her $a \in L$ elemanı, x K üzerinde bir belirsiz olmak üzere bir $f(x) \in K[x]$ için $a=f(t)$ şeklinde olduğundan

$$a^{\sigma_i} = f(t)^{\sigma_i} = f(t^{\sigma_i}) = f(t_i) \ , \ i=1,\ldots,m$$

elde edilir. Teorem 35 e göre $\sigma_i \in G(\frac{L}{K})$ $(i=1,\ldots,m)$ olduğundan

$$G(\frac{L}{K}) = \{\sigma_1, \ldots, \sigma_m\}$$

elde edilir.

Teorem 48: $n \in N$ ve $k(K) \nmid n$ olmak üzere, K üzerindeki n inci çember bölen cisim $K^{(n)}$ K nın bir Galois genişlemesidir ve

$$G(\frac{K^{(n)}}{K})$$

Galois grubu Z_n^* grubunun bir altgrubuna izomorftur. K = Q halinde

$$G(\frac{Q^{(n)}}{Q}) \cong Z_n^*$$

verilir.

İspat: $K^{(n)}$, x^n-1 polinomunun K üzerindeki bir parçalayıcı cismi olduğundan, $K^{(n)}$ cismi K nın bir Galois genişlemesidir ve 1 in $K^{(n)}$ cismindeki her c primitif n inci kökü olmak üzere

$$K^{(n)} = K(c)$$

dir. c elemanının K üzerindeki eşlenikleri, c elemanının belli K- izomorf resimleri olduğundan, c elemanının her eşleniği de 1 in K üzerindeki bir primitif n inci köküdür. Dolayısıyla

$$c^{\sigma_i} = c^{k_i} \ , \ k_i \in N \ , \ (k_i,n) = 1 \ , \ i=1,...,m$$

olmak üzere

$$G(\frac{K^{(n)}}{K}) = \{\sigma_1 \ , ... , \ \sigma_m\}$$

elde edilir.

$$(\sigma_i)\pi = \bar{k}_i \ , \ i=1,...,m$$

ile belirlenen

$$\pi : G(\frac{K^{(n)}}{K}) \rightarrow Z_n^*$$

dönüşümünü gözönüne alalım.

$$c^{\sigma_i\sigma_j} = (c^{\sigma_i})^{\sigma_j} = (c^{k_i})^{\sigma_j} = (c^{\sigma_j})^{k_i} = c^{k_ik_j}$$

olduğundan

$$(\sigma_i\sigma_j)\pi = \bar{k}_i\bar{k}_j = \bar{k}_i\bar{k}_j = (\sigma_i)\pi\,(\sigma_j)\pi$$

elde edilir. Dolayısıyla π dönüşümü bir homomorfidir.

$$\text{çek}\,\pi = \{\sigma_i \mid \sigma_i \in G(\frac{K^{(n)}}{K}) \ , \ (\sigma_i)\pi = \bar{k}_i = \bar{1} \ , \ i\in\{1,...,m\}\} = \{\varepsilon\}$$

olduğundan grupların homomorfi teoremine göre, π bir monomorfidir.

K = Q için uyarı 4 e göre

$$[Q^{(n)} : Q] = \varphi(n) = |Z_n^*| = |G(\frac{Q^{(n)}}{Q})|$$

olduğundan

$$G(\frac{Q^{(n)}}{Q}) \cong Z_n^*$$

elde edilir.

Teorem 49: $n\in N$ ve $k(K) \mid n$ olmak üzere $B_n \subset K$ olsun.

(a). L cismi, bir $a\in K$ için

$$L = K(\sqrt[n]{a})$$

şeklinde olsun. Bu takdirde L cismi K nın bir Galois genişlemesidir ve $G(\frac{L}{K})$ Galois grubu m n sayısının bir böleni olmak üzere, m inci mertebeden bir devirli gruptur. m=n olabilmesi için gerek ve yeter koşul, $\sqrt[n]{a}$ radikalinin K üzerinde indirgenemez olmasıdır.

(b). L cismi K nın bir Galois genişlemesi ve $G(\frac{L}{K})$ Galois grubu n inci mertebeden bir devirli grup ise,

$$L = K(\sqrt[n]{a})$$

olacak şekilde bir $a \in K$ elemanı mevcuttur.

İspat: $c \in K$ elemanı 1 in primitif n inci kökü olsun.

(a). $a \neq 0$ kabul edilebilir. Teorem 28 e göre

$$x^n - a = \prod_{i=1}^{n} (x - \sqrt[n]{a}\, c^{i-1}) \in L[x]$$

olduğundan $x^n - a$ ayrılabilir bir polinomdur. L cismi bu polinomun K üzerindeki bir parçalayıcı cismidir. Teorem 41 e göre, L cismi K nın bir Galois genişlemesidir. $\sqrt[n]{a} \in L$ elemanının K üzerindeki eşlenikleri, $x^n - a$ polinomunun sıfır yerleri olduğundan, $c_j \in K$ $(j=1,...,m)$ elemanları 1 in farklı n inci kökleri olmak üzere

$$(\sqrt[n]{a})^{\sigma_j} = \sqrt[n]{a}\, c_j \,, \quad j=1,...,m$$

ile belirlenen σ_j dönüşümleri $G(\frac{L}{K})$ Galois grubunu oluşturur:

$$G(\frac{L}{K}) = \{\sigma_1, ..., \sigma_m\} \,.$$

$$(\sigma_j)\pi = c_j \,, \quad j=1,...,m$$

ile belirlenen

$$\pi : G(\frac{L}{K}) \to B_n$$

dönüşümü gözönüne alınsın.

$$(\sqrt[n]{a})^{\sigma_j\sigma_k} = ((\sqrt[n]{a})^{\sigma_j})^{\sigma_k} = (\sqrt[n]{a}\, c_j)^{\sigma_k} = c_j\, (\sqrt[n]{a})^{\sigma_k} = \sqrt[n]{a}\; c_j c_k$$

olduğundan

$$(\sigma_j\sigma_k)\pi = c_j c_k = (\sigma_j)\pi\,(\sigma_k)\pi$$

elde edilir. Dolayısıyla π dönüşümü bir homomorfidir. Grupların homomorfi teoremine göre $G(\frac{L}{K})$ Galois grubu, n inci mertebeden bir devili grup olan B_n nin bir altgrubuna izomorftur. Dolayısıyla min elde edilir. m=n olabilmesi için gerek ve yeter koşul,

$$[L : K] = n$$

olmasıdır. Bu şart ise

$$x^n - a = \text{İnd}\,(\sqrt[n]{a}\,, K)$$

veya $\sqrt[n]{a}$ radikalinin K üzerinde indirgenemez olmasına denktir.

(b). L cismi K nın bir Galois genişlemesi ve

$$G(\frac{L}{K}) = \langle \sigma \rangle \,, \quad |\sigma| = n$$

olsun. Bir $u \in L$ elemanı için

$$t = \sum_{i=1}^{n} c^{i-1} u^{\sigma^{i-1}}$$

ifadesini teşkil edelim. Teorem 40 a göre, u elemanı $t \neq 0$ olacak şekilde seçilebilir. Bu takdirde

$$t^{\sigma} = \sum_{i=1}^{n} c^{i-1} u^{\sigma^i} = c^{-1} \sum_{i=1}^{n} c^i u^{\sigma^i} = c^{-1}(cu^{\sigma} + c^2 u^{\sigma^2} + \ldots + c^{n-1} u^{\sigma^{n-1}} + u)$$

$$= c^{-1} \sum_{i=1}^{n} c^{i-1} u^{\sigma^{i-1}} = c^{-1} t$$

olduğundan her $r \in N$ için

$$t^{\sigma^r} = c^{-r} t$$

elde edilir. Buna göre, $G(\frac{L}{K})$ Galois grubunda t elemanını sabit bırakan biricik eleman $\sigma^0 = \varepsilon$ dır. Dolayısıyla

$$K(t) = S(<\varepsilon>) = L$$

elde edilir. Bunun yanında $a = t^n$ olmak üzere, $r \in N$ için

$$a^{\sigma^r} = (t^n)^{\sigma^r} = (t^{\sigma^r})^n = (c^{-r} t)^n = (c^n)^{-r} t^n = t^n = a$$

olduğundan

$$a \in S(G(\frac{L}{K})) = K$$

ve buna göre

$$L = K(\sqrt[n]{a})$$

elde edilir.

Teorem 50: $m \in N$, $k(K) \mid m$ ve $B_m \subset K$ olmak üzere L cismi K nın bir Galois genişlemesi olsun. $\{t_1, \ldots, t_r\}$ bir $t \in L$ elemanının K üzerindeki eşleniklerinin bir tam sistemi olsun. Bu takdirde

$$M = L\left(\sqrt[m]{t_1}, \ldots, \sqrt[m]{t_r}\right)$$

cismi K nın bir Galois genişlemesidir.

İspat: İddianın ispatı için teorem 41 e göre M cisminin, K[x] halkasının bir ayrılabilir polinomunun K üzerindeki bir parçalayıcı cismi olduğunu göstermek yeterlidir.

$$h(x) = \prod_{i=1}^{r} (x^m - t_i) \in L[x]$$

polinomu gözönüne alınsın. Her $x^m - t_i$ polinomunun sıfır yerleri, teorem 28 e göre c 1 in bir primitif m inci kökü olmak üzere

$$\sqrt[m]{t_i}\,\sigma^{j-1} \ , \ j=1,...,m$$

şeklinde olup, bu sıfır yerleri birbirlerinden farklıdırlar. Dolayısıyla h(x) ayrılabilir bir polinomdur ve M bu polunomun L üzerindeki bir parçalayıcı cismidir. $s_i(t_1,...,t_r)$ (i=1,...,r) elemanter simetrik polinomlar olmak üzere

$$h(x) = \sum_{i=0}^{r} (-1)^i s_i (x^m)^{r-i} \ , \ s_0=1$$

yazılabilir. Bunun yanında

$$\text{İnd}(t,K) = \prod_{i=1}^{r} (x - t_i) = \sum_{i=0}^{r} (-1)^i s_i x^{r-i} \in K[x]$$

olduğundan

$$h(x) \in K[x]$$

elde edilir. Diğer taraftan teorem 41 e göre L ayrılabilir bir $f(x)\in K[x]$ polinomunun K üzerindeki bir parçalayıcı cismidir. $f(x)h(x)\in K[x]$ polinomunun K[x] halkasındaki farklı indirgenemez monik bölenlerinin çarpımı $g(x)\in K[x]$ olsun. g(x) ayrılabilir bir polinomdur ve M, teorem 21 e göre g(x) polinomunun K üzerindeki bir parçalayıcı cismidir.

Tanım 29: $f(x)\in K[x]$ sabit olmayan bir polinom ve L f(x) polinomunun K üzerindeki bir parçalayıcı cismi olsun. f(x) polinomunun her sıfır yeri, K nın aynı bir genişlemesinde (K üzerinde) radikallerle gösterilebilir ise, f(x) polinomuna K üzerinde radikallerle çözülebilir (veya kısaca K üzerinde çözülebilir) denir. Diğer bir ifade ile L cisminin bir M genişlemesi, $m_i\in N$ ve $t_i\in M_i$ için

$$M_{i+1} = M_i\left(\sqrt[m_i]{t_i} \right) \ , \ i=0,1,...,r-1$$

olacak şekilde, M cisminin M_i altcisimlerinden oluşan ve K ile başlayıp M ile biten bir

$$K \subset M_0 \subset M_1 \subset \ ... \ \subset M_r = M$$

sonlu cisim serisi mevcut olacak şekilde elde edilebiliyor ise, f(x) polinomu K üzerinde çözülebilir denir. Her i için $\sqrt[m_i]{t_i}$ radikali M_i üzerinde indirgenemez ise, f(x) polinomu K üzerinde indirgenemez radikallerle çözülebilir denir.

Teorem 51: Bir ayrılabilir $f(x)\in K[x]$ polinomu K üzerinde çözülebilir ise, f(x) polinomunun K üzerindeki Galois grubu da çözülebilir bir gruptur.

İspat: $k(K) = p$ ve L f(x) polinomunun K üzerindeki bir parçalayıcı cismi olsun.

I. f(x) polinomu K üzerinde çözülebilir olduğundan L cisminin bir M genişlemesi ve

$$M_{i+1} = M_i\left(\sqrt[m_i]{t_i}\right),\ t_i \in M_i,\ m_i \in \mathbf{N}\quad (i=0,1,\ldots,r-1)$$

olmak üzere bir

$$K = M_0 \subset M_1 \subset \ldots \subset M_r = M \qquad (7)$$

cisim serisi mevcuttur. Burada m_i sayılarının asal olduğu kabul edilebilir. Zira $m_i = n_i k_i$ ise

$$\sqrt[n_i k_i]{t_i} = \sqrt[k_i]{\sqrt[n_i]{t_i}}$$

olduğundan $M_i\left(\sqrt[n_i]{t_i}\right)$ cismi, M_i ile M_{i+1} cisimleri arasına sıkıştırılarak tekrar (7) şeklindeki bir cisim serisi elde edilir:

$$M_i \subset M_i\left(\sqrt[n_i]{t_i}\right) \subset M_i\left(\sqrt[n_i]{t_i}\right)\left(\sqrt[k_i]{\sqrt[n_i]{t_i}}\right) = M_{i+1}\ .$$

II. (7) cisim serisinde $m_i \neq p$ $(i=0,1,\ldots,r-1)$ kabul edilebilir. Gerçekten, $p=0$ için iddia doğrudur. $p>0$ olmak üzere, bir

$$i \in \{0,1,\ldots,r-2\}$$

için $q \in \mathbf{P}$ olmak üzere

$$m_i = p \quad \text{ve} \quad m_{i+1} = q \neq p$$

olsun. Bu takdirde (7) cisim serisinde

$$M_i \subset M_{i+1} = M_i\left(\sqrt[p]{t_i}\right) \subset M_{i+2} = M_i\left(\sqrt[p]{t_i}\ ,\ \sqrt[q]{t_{i+1}}\right)$$

altserisi yerine

$$M_i \subset M_i\left(\sqrt[q]{t_{i+1}^p}\right) \subset M_i\left(\sqrt[q]{t_{i+1}^p}\right)\left(\sqrt[p]{t_i}\right) \subset$$

$$\subset M_i\left(\sqrt[q]{t_{i+1}^p}\ ,\ \sqrt[p]{t_i}\right)\left(\sqrt[p]{\sqrt[q]{t_{i+1}^p}}\right) = M_{i+2}$$

altserisi yazılsın.

$$t_{i+1} \in M_i\left(\sqrt[p]{t_i}\right)$$

olduğundan

$$t_{i+1}^p \in M_i(t_i) = M_i$$

dir ve dolayısıyla elde edilen yeni seri (7) serisinin özelliklerine sahip olan bir inceltilmiş cisim serisidir. Bu yeni seride M_i cismine katılan radikalin eksponenti q olup, p den farklıdır. Bu işleme devam edilerek sonlu adım sonunda elde edilen inceltilmiş serinin eksponenti p den farklı radikalli terimleri M_o dan itibaren ardarda sıralanmışlardır. Yeni cisim serisindeki katılan radikallerin eksponentleri tekrar m_i ler ile gösterilirse $0 \le i < r_o$ için $m_i \neq p$ ve $r_o \le j < r$ için $m_j = p$ olacak şekilde bir r_o sayısı mevcuttur. K cisminin M deki ayrılabilir kapanışı olan M_a cismi gözönüne alınsın.

$$K \subset L \subset M_a \subset M$$

dir. Teorem 39 a göre

$$(M_{r_o})_a = (M_{r_o+1})_a = \dots = (M_r)_a = M_a$$

olduğundan

$$M_a = (M_{r_o})_a \subset M_{r_o}$$

elde edilir. Buna göre yukarıda sözü geçen inceltilmiş cisim serisinde M_r yerine M_{r_o} alınabilir. O halde (7) cisim serisindeki terimlere ait m_i (i=0,1,...,r-1) eksponentlerin p den farklı olduğu kabul edilebilir.

III. Teorem 49 (a) nın tatbiki için (7) serisinin terimlerine 1 in gerekli olan kökleri katılır.

$$m = \prod_{i=0}^{r-1} m_i$$

ve c 1 in M üzerindeki bir primitif m inci kökü olsun.

$$M_i(c) = L_i \ , \quad i=0,1,\dots,r$$

olmak üzere (7) serisinden

$$K \subset L_o \subset L_1 \subset \dots \subset L_r \qquad (8)$$

cisim serisi teşkil edilebilir. Burada

$$L_o = K(c) \ , \ L_{i+1} = L_i\left(\sqrt[m_i]{t_i}\right) \ , \ t_i \in L_i \quad (i=0,1,\dots,r-1)$$

dir.

IV. (8) cisim serisi, mevcut özellikleri korunarak sonuncu terimi K nın bir Galois genişlemesi olacak şekilde inceltilir. Bir $i \ge 0$ için L_i cismi K nın bir Galois genişlemesi olsun. t_i elemanının K üzerindeki eşleniklerinin bir tam sistemi $t_{i1} = t_i$ olmak üzere

$$\{t_{i1}, \ldots, t_{in_i}\}$$

olsun. Bu takdirde

$$\sqrt[m_i]{t_{ij}}\ ,\ j=1,\ldots,n_i$$

radikalleri L_i cismine ardarda katılarak $L_i \subset L_{i+1}$ aralığından

$$L_i \subset L_{i+1} = L_i\left(\sqrt[m_i]{t_{i1}}\right) \subset L_i\left(\sqrt[m_i]{t_{i1}}, \sqrt[m_i]{t_{i2}}\right) \subset$$

$$\subset \ldots \subset L_i\left(\sqrt[m_i]{t_{i1}}, \ldots, \sqrt[m_i]{t_{in_i}}\right) = L'_{i+1}$$

cisim serisi elde edilir. Bu serinin sonuncu terimi olan L'_{i+1} cismi teorem 50 ye göre K nın bir Galois genişlemesidir. Aynı işlem L'_{i+1} cismine tatbik edilebilir.

$$\sqrt[m_{i+1}]{t_{i+1,j}}\ ,\ j=1,\ldots,n_{i+1}$$

radikalleri ardarda L'_{i+1} cismine katılarak K nın bir L''_{i+2} Galois genişlemesi elde edilir. Bu işleme devam edilerek ((8) cisim serisinin belli aralıkları genişletilerek ve dolayısıyla (8) serisi inceltilerek) sonlu adım sonunda sonuncu terimi L_r, K nın bir Galois genişlemesi olacak şekilde bir cisim serisi elde edilmiş olur. O halde L_r cisminin K nın bir Galois genişlemesi olduğu kabul edilebilir. Bu takdirde (8) den

$$G\left(\frac{L_r}{K}\right) > G\left(\frac{L_r}{L_o}\right) > \ldots > G\left(\frac{L_r}{L_{r-1}}\right) > G\left(\frac{L_r}{L_r}\right) = \{\varepsilon\} = E \qquad (9)$$

elde edilir. Teorem 48 e göre, L_o cismi K nın bir Galois genişlemesidir ve $G\left(\frac{L_o}{K}\right)$ grubu Abel'dir. Bunun yanında teorem 45 (b) ye göre

$$G\left(\frac{L_r}{L_o}\right) \lhd G\left(\frac{L_r}{K}\right) \quad \text{ve} \quad G\left(\frac{L_r}{K}\right) / G\left(\frac{L_r}{L_o}\right) \cong G\left(\frac{L_o}{K}\right)$$

olduğundan

$$G\left(\frac{L_r}{K}\right) / G\left(\frac{L_r}{L_o}\right)$$

bölüm grubu Abel'dir. Teorem 49 (a) ya göre her i $(0 \le i \le r-1)$ için L_{i+1} cismi L_i nin bir Galois genişlemesidir ve $G\left(\frac{L_{i+1}}{L_i}\right)$ asal mertebeli bir devirli gruptur. Dolayısıyla teorem 45 (b) ye göre

$$G\left(\frac{L_r}{L_{i+1}}\right) \lhd G\left(\frac{L_r}{L_i}\right) \text{ ve } G\left(\frac{L_r}{L_i}\right) / G\left(\frac{L_r}{L_{i+1}}\right) \simeq G\left(\frac{L_{i+1}}{L_i}\right), \quad i=0,1,\ldots,r-1$$

olduğundan her i $(0 \le i \le r-1)$ için

$$G\left(\frac{L_r}{L_i}\right) / G\left(\frac{L_i}{L_{i+1}}\right)$$

bölüm grubu da asal mertebeli bir devirli gruptur. Buna göre (9) ifadesi $G\left(\frac{L_r}{K}\right)$ grubunun faktörleri asal mertebeli devirli gruplar olan bir kompozisyon serisidir. Dolayısıyla $G\left(\frac{L_r}{K}\right)$ çözülebilir bir gruptur. Diğer taraftan teorem 45 (b) ye göre

$$G\left(\frac{L_r}{K}\right) / G\left(\frac{L_r}{L}\right) \simeq G\left(\frac{L}{K}\right)$$

dır ve $G\left(\frac{L_r}{K}\right)$ grubu çözülebilir olduğundan

$$G\left(\frac{L_r}{K}\right) / G\left(\frac{L_r}{L}\right)$$

grubu da çözülebilirdir ve bu bölüm grubuna izomorf olan $G\left(\frac{L}{K}\right)$ grubu çözülebilirdir.

3. BULGULAR

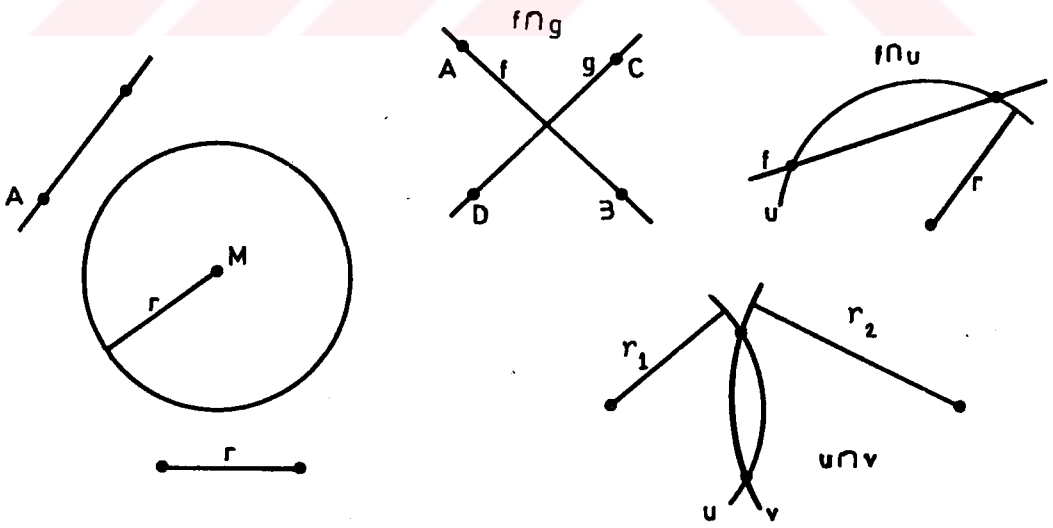
3.1. Pergel ve Cetvelle Geometrik İnşalar

Galois teorisinin uygulama alanlarından biri de geometridir. Geometride gözönüne alınan şekiller genellikle sonlu sayıda noktalar yardımıyla belirlenir. Örneğin bir doğru iki noktası ile, bir çember merkezi ve bir noktası ile, bir konik odak noktaları ve bir noktası ile v.b. belirlenir. Dolayısıyla düzlemde verilen bir takım şekiller (noktalar, doğrular veya çemberler) yardımıyla başka bir takım şekillerin inşası problemi, verilen sonlu sayıda noktalar yardımıyla belli şartları gerçekleyen sonlu sayıda yeni noktaların bulunması problemine denktir.

Diğer taraftan geometride, yalnız pergel ve cetvel kullanılarak inşa edilen şekillerin ayrı bir önemi vardır. Örneğin, yalnız pergel ve cetvel kullanılarak üç noktadan geçen çemberin, üç yüksekliği bilinen üçgenin, üç iç açı ortayı bilinen üçgenin v.b. bulunması problemleri. Bu problemlerden ilk ikisinin çözümlerinin mümkün olması yanında üçüncü problemin çözümü mümkün değildir [3].

Burada, düzlemde verilen sonlu sayıda noktalar yardımıyla belli şartları gerçekleyen sonlu sayıdaki yeni noktaların, sonlu adımda ve her adımda yalnız pergel ve cetvel kullanılarak nasıl elde edilebileceği cebirsel metodlar yardımıyla araştırılacaktır.

Yukarıda sözü geçen pergel ve cetvelle yapılan adımlar (veya kısaca pergel - cetvel adımları), aşağıda belirtilen dört tipte olabilir. A,B ve C,D verilen farklı iki nokta çifti olsun.



Şekil 1. Pergel- cetvel adımları

1. A ve B noktalarından geçen doğru ile C ve D noktalarından geçen doğrunun kesişme noktasının (mevcut olması halinde) belirlenmesi.

2. A ve B noktalarından geçen doğru ile merkezi C de olan ve D noktasından geçen çemberin kesişme noktalarının belirlenmesi.

3. Merkezi A da olan ve B noktasından geçen çember ile merkezi C de olan ve D noktasından geçen çemberin kesişme noktalarının belirlenmesi.

4. Belli yardımcı noktaların seçilmesi. Bu noktalar düzlemde keyfi olarak seçilir ve geometrik inşada temel rol oynamazlar. Ancak bu noktalar geometrik inşa için diğer noktalar gibi hizmet ederler.

Yukarıdaki geometrik ifadelerin cebirsel karşılıklarını elde etmek için düzlemde kartezyen koordinat sistemini gözönüne alalım. Analitik geometriden bilinen kurallar yardımıyla pergel-cetvel adımları, ilgili noktaların koordinatları arasında belli cebirsel ifadelerle belirlenebilir ve daha sonra bu cebirsel ifadelerin cisim teorisindeki karşılıkları verilebilir.

Düzlemde bir kartezyen koordinat sistemi tespit edilmiş ve koordinat sisteminin eksenleri üzerinde l doğru parçası (uzunluğu birim olan doğru parçası) belirlenmiş olsun.

A, B, C, D noktalarının koordinat gösterimleri

$$A = (a_1,a_2)\ ,\ B = (b_1,b_2)\ ,\ C = (c_1,c_2)\ ,\ D = (d_1,d_2)$$

olsun.

I. A ve B noktalarından geçen f doğrusu

$$f: ax + by = c\ ,\ a = a_2 - b_2\ ,\ b = b_1 - a_1\ ,\ c = a_2b_1 - a_1b_2$$

şeklindeki bir lineer denklemle belirlenir. Özellikle a, b ve c katsayıları $Q(a_1, a_2, b_1, b_2)$ cisminde bulunur. Benzer şekilde C ve D noktalarından geçen g doğrusu

$$g : a'x + b'y = c'\ ,\ a' = c_2 - d_2\ ,\ b' = d_1 - c_1\ ,\ c' = c_2d_1 - c_1d_2$$

şeklindeki bir lineer denklem ile belirlenir. a', b' ve c' katsayıları $Q(c_1, c_2, d_1, d_2)$ cisminde bulunurlar. f ve g doğrularının paralel olmadığı kabul edilebilir. Bu takdirde f ve g doğrularının kesişme noktalarının koordinatları Q(a, b, c, a', b', c') cisminde ve özellikle

$$K_0 = Q(a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2)$$

cisminde bulunurlar.

II. Merkezi C olan ve D noktasından geçen u çemberi

$$u: (x - c_1)^2 + (y - c_2)^2 = r_1^2\ ,\ r_1^2 = (d_1 - c_1)^2 + (d_2 - c_2)^2$$

şeklinde bir kuadratik denklem ile belirlenir. f doğrusu ile u çemberinin kesişmesi halinde, herbir kesişme noktasının x_0 , y_0 koordinatlarını hesaplayalım. $a \neq 0$ olsun. f in denklemi x e göre çözülür ve elde edilen ifade u nun denkleminde yerine yazılarak y için bir kuadratik denklem elde edilir ve bu denklem y ye göre çözülerek

$$y_0 \in Q(a, b, c, c_1, c_2, r_1)(\sqrt{d})$$

elde edilir. Burada d, y ye göre kuadratik denklemin diskriminantıdır. Sonuç olarak $d \in K_o$ olmak üzere

$$x_0, y_0 \in K_o(\sqrt{d})$$

elde edilir.

III. Merkezi A olan ve B noktasından geçen v çemberi

$$v: (x - a_1)^2 + (y - a_2)^2 = r_2^2 \ , \ r_2^2 = (b_1 - a_1)^2 + (b_2 - a_2)^2$$

şeklinde bir kuadratik denklem ile belirlenir. u ve v çemberlerinin kesişmesi halinde herbir kesişme noktasının koordinatları u ve v nin kuadratik denklemlerinden II. dekine benzer şekilde hesaplanabilir. Herbir kesişme noktasının koordinatları, bir $d \in K_o$ için $K_o(\sqrt{d})$ cisminde bulunur.

IV. Yardımcı noktalar keyfi seçilebileceğinden bu noktaların koordinatları rasyonel seçilebilir. Dolayısıyla yardımcı noktaların koordinatlarının daima K_o cisminde bulunduğunu kabul edebiliriz.

Yukarıda I, II, III ve IV de elde edilen sonuçlar, aşağıdaki teoremin (a) şıkkının ispatını teşkil eder.

Teorem 52:

(a). $A_1, \ldots, A_m$ keyfi ve sonlu sayıda noktalar, $\{a_1, \ldots, a_n\}$ bu noktaların koordinatlarının kümesi ve A $A_1, \ldots, A_m$ noktalarından pergel ve cetvelle inşa edilebilen bir nokta olsun. Bu takdirde A noktasının koordinatları, $Q(a_1, \ldots, a_n)$ cisminden sonlu sayıda 2 eksponentli radikallerin (kareköklerin) ardarda katılmasıyla elde edilen L cisminde bulunurlar. Diğer bir ifade ile sonlu sayıda $d_1, \ldots, d_r$ kompleks sayıları

$$d_i \in Q(a_1, \ldots, a_n, \sqrt{d_1}, \ldots, \sqrt{d_{i-1}}) \ , \ i=1,\ldots,r$$

ve

$$L = Q(a_1, \ldots, a_n, \sqrt{d_1}, \ldots, \sqrt{d_r})$$

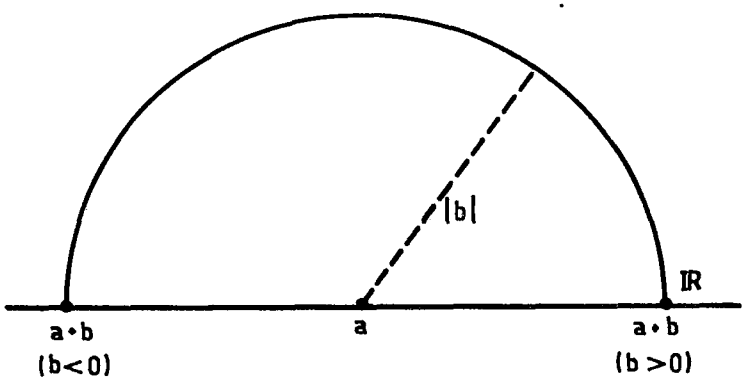
olmak üzere mevcutturlar.

(b). Tersine olarak koordinatları, $Q(a_1, ..., a_n)$ cisminin (a) daki gibi bir genişlemesinde bulunan her nokta, $A_1, ..., A_n$ noktalarından pergel ve cetvelle inşa edilebilir.

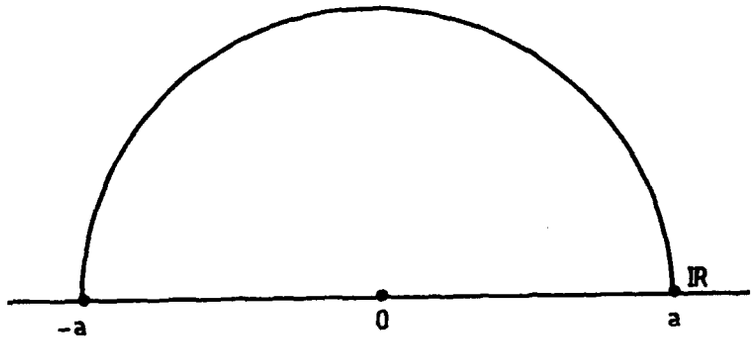
İspat: Bilindiği gibi, her kompleks sayı, reel ve sanal kısımları koordinatlar alınarak düzlemde bir nokta ile gösterilebilir. O halde kompleks sayılar cisminde iki kompleks sayıdan rasyonel işlemlerle elde edilen kompleks sayıya ve bir kompleks sayının karekökü alınarak elde edilen kompleks sayıya düzlemde tekabül eden noktaların pergel ve cetvelle inşa edilebildiğini göstermek, iddianın ispatı için yeterlidir. İki kompleks sayının toplamına (bzş. farkına) düzlemde vektör toplamı (bzş. farkı) tekabül eder. İki kompleks sayının çarpımında argümanlar toplanır ve modüller çarpılır. Kompleks sayılardaki bölmede argümanların farkı alınır ve modüller arasında bölme yapılır. Bir kompleks sayının karekökünün teşkilinde argümanın yarısı alınır ve modülün karekökü teşkil edilir. $a,b \in \mathbb{R}$ olsun. Bu takdirde

$$a + b,\ -a(a>0),\ ab,\ \frac{1}{a}\ (a \neq 0)\ \text{ve}\ \sqrt{r}\ (r>0)$$

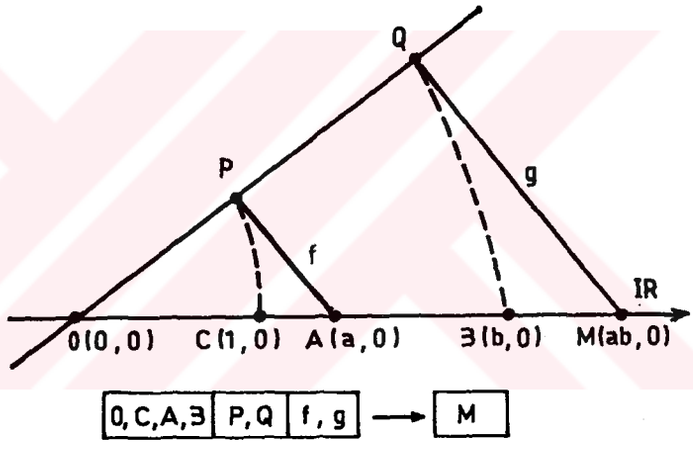
reel sayıları pergel ve cetvelle inşa edilebilirler:



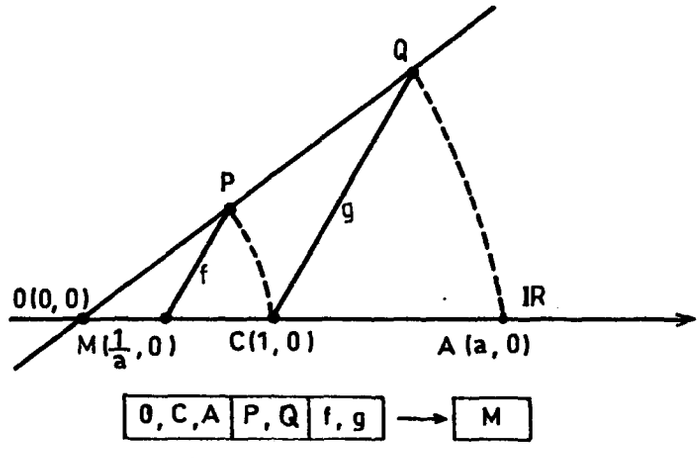
Şekil 2. a + b sayısının inşası.



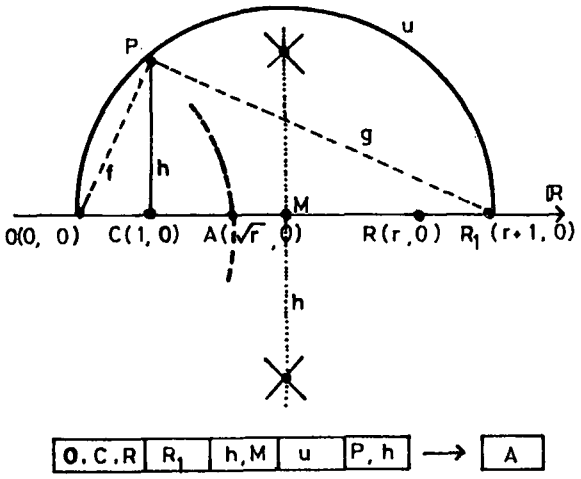
Şekil 3. - a sayısının inşası.



Şekil 4. ab sayısının inşası.



Şekil 5. $\frac{1}{a}$ $(a \neq 0)$ sayısının inşası.



Şekil 6. $\sqrt{r}$ (r>0) sayısının inşası.

Teorem 53: A_1 ,..., A_m sonlu sayıda noktalar ve $\{a_1$,..., $a_n\}$ bu noktaların koordinatlarının kümesi olsun. Bir A noktasının A_1 ,..., A_m noktalarından pergel ve cetvelle inşa edilebilmesi için gerek ve yeter koşul, A noktasının koordinatlarının

$$[L: Q(a_1, ..., a_n)] = 2^k, \quad k \in \mathbf{N}$$

olacak şekilde $Q(a_1$,..., $a_n)$ cisminin bir L Galois genişlemesinde bulunmalarıdır.

İspat: A noktası A_1 ,..., A_m noktalarından pergel ve cetvelle inşa edilsin. Bu takdirde teorem 52 ye göre, A noktasının koordinatları $K= Q(a_1$,..., $a_n)$ cisminin aşağıdaki özelliğe sahip bir L genişlemesinde bulunurlar.

$$L_{i+1} = L_i(\sqrt{d_i}), \quad d_i \in L_i \qquad (i=0,1,...,r-1)$$

olacak şekilde bir

$$K = L_0 \subset L_1 \subset ... \subset L_r = L$$

cisim serisi mevcuttur. Bu cisim serisi sonuncu terimi L_r cismi, K nın bir Galois genişlemesi olacak şekilde inceltilebilir. Bir $i \geq 0$ için L_i cismi K nın bir Galois genişlemesi olsun. d_i elemanının K üzerindeki eşleniklerinin bir tam sistemi $d_{i1} = d_i$ olmak üzere $\{d_{i1},...,d_it_i\}$ olsun. Bu takdirde

$$\sqrt{d_{ij}}, \quad j= 1,...,t_i$$

radikalleri L_i cismine ardarda katılarak $L_i \subset L_{i+1}$ aralığından

$$L_i \subset L_{i+1} = L_i(\sqrt{d_{i1}}) \subset L_i(\sqrt{d_{i1}}, \sqrt{d_{i2}}) \subset ... \subset L_i(\sqrt{d_{i1}}, ..., \sqrt{d_it_i})$$

cisim serisi elde edilir. Bu serinin sonuncu terimi olan L'_{i+1} cismi teorem 50 ye göre K nın bir Galois genişlemesidir. Aynı işlem L'_{i+1} cismine tatbik edilebilir.

$$\sqrt{d_{i+1,j}} \quad , \quad j=1,\ldots,t_{i+1}$$

radikalleri ardarda L'_{i+1} cismine katılarak K nın bir L''_{i+2} Galois genişlemesi elde edilir. Bu işleme devam edilerek sonlu adım sonunda sonuncu terimi L_r, K nın bir Galois genişlemesi olacak şekilde bir cisim serisi elde edilmiş olur.

$$[L_{i+1} : L_i] = 1 \text{ veya } 2 \quad , \quad i=0,1,\ldots,r-1$$

olduğundan boyut teoremine göre $k \in \mathbf{N}$ olmak üzere

$$[L_r : K] = 2^k$$

elde edilir.

A noktasının koordinatları , $k \in \mathbf{N}$ olmak üzere

$$[L : K] = 2^k$$

olacak şekilde K nın bir L Galois genişlemesinde bulunsun.

$$| G(\frac{L}{K}) | = 2^k$$

olduğundan $G(\frac{L}{K})$ grubu bir 2-grup olup, çözülebilirdir [2]. Dolayısıyla

$$G(\frac{L}{K}) = G_0 \rhd G_1 \rhd \ldots \rhd G_s = E$$

kompozisyon serisinin tüm faktörlerinin mertebesi 2 dir. İlgili cisim serisi

$$K = K_0 \subset K_1 \subset \ldots \subset K_s = L$$

olsun. Teorem 45 (b) ye göre bu cisim serisindeki K_{i+1} cismi K_i nin bir Galois genişlemesidir. Teorem 49 (b) ye göre

$$K_{i+1} = K_i (\sqrt{d_i}) , \; d_i \in K_i \quad (i=0,1,\ldots,s-1)$$

elde edilir. Buna göre L cismi K dan sonlu sayıda kareköklerin ardarda katılması ile elde edilir. Dolayısıyla teorem 41 e göre, A noktası A_1 ,..., A_m noktalarından pergel ve cetvelle inşa edilebilir.

Teorem 54: $n \in \mathbf{N}$ olmak üzere her açının n e bölünebilmesi için gerek ve yeter koşul

$$n = 2^k \quad , \quad k \in \mathbf{N}$$

olmasıdır.

İspat: $n = 2^k$, $n \in \mathbf{N}$ olsun. Bu takdirde verilen t açısı pergel ve cetvelle k defa ikiye bölünerek, $\frac{t}{2^k}$ açısı pergel ve cetvelle inşa edilebilir.

n sayısının 2 nin bir kuvveti şeklinde olmadığını kabul edelim. Her a açısı için cosna cosa ya göre Z üzerinde n inci dereceden bir polinomdur. Dolayısıyla $\cos\frac{t}{n}$

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

şeklinde bir n inci dereceden polinomun bir sıfır yeridir. Burada $a_i \in Z$ (i=0,...,n) ve x, Q(cost) üzerinde bir belirsizdir. cost sayısını mutlak değeri 1 den küçük olan bir transandant sayı olarak seçelim. Zira, böyle en az bir transandant u sayısı mevcuttur ve

$$\frac{u}{[|u|]+1}$$

transandant sayısının mutlak değeri 1 den küçüktür. h(x), cost belirsizine göre Z[x] üzerinde bir primitif lineer polinomdur. Buna göre h(x) polinomu Z[cost,x] halkasının bir asal elemanıdır ve dolayısıyla h(x) polinomu Q(cost)[x] halkasında indirgenemezdir. Özellikle

$$[Q(\cos t, \cos\frac{t}{n}) : Q(\cos t)] = n$$

olduğundan teorem 53 e göre, $(\cos\frac{t}{n}, 0)$ noktası (cost, 0) noktasından pergel ve cetvelle inşa edilemez.

Tanım 30: Bir $m \in N_0$ için

$$p = 1 + 2^{(2^m)}$$

şeklinde yazılabilen bir $p \in P$ sayısına, Fermat asal sayısı denir. m= 0, 1, 2, 3, 4 için yukarıdaki formda yazılan sayılar, sırasıyla 3, 5, 17, 257, 65537 olup tümü asaldırlar. Ancak, yukarıdaki formda yazılan her sayı asal değildir. Örneğin

$$1 + 2^{(2^5)}$$

sayısı 641 ile bölünür [5].

Teorem 55: n>2 olmak üzere bir $n \in N$ için düzgün n köşelinin pergel ve cetvelle inşa edilebilmesi için gerek ve yeter koşul, $m \in N_0$ ve $p_1, \ldots, p_k$ farklı Fermat asal sayıları olmak üzere

$$n = 2^m \prod_{i=1}^{k} p_i$$

olmasıdır.

İspat: n>2 olmak üzere bir $n \in N$ için düzgün n köşelinin pergel ve cetvelle inşası problemi, $\frac{2\pi}{n}$ açısının pergel ve cetvelle inşası problemine denktir. Buna göre $(\cos\frac{2\pi}{n}, 0)$

noktasının (1,0) noktasından pergel ve cetvelle inşa edilebilmesi için gerek ve yeter koşul araştırılır. Araştırılan cisim,

$$c = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

olmak üzere

$$U = Q(\cos\frac{2\pi}{n}) = Q(c + c^{-1})$$

olup, bu cisim Q(c) n inci çember bölen cisminin bir altcismidir. Uyarı 4 ve teorem 48 e göre, $Q(c) = Q^{(n)}$ cismi Q nun bir Galois genişlemesidir.

$$[Q^{(n)} : Q] = \varphi(n)$$

verilir ve

$$G\left(\frac{Q^{(n)}}{Q}\right)$$

Galois grubu Abel'dir. Dolayısıyla teorem 45 (b) ye göre U cismi Q nun bir Galois genişlemesidir. Diğer taraftan x U üzerinde bir belirsiz olmak üzere

$$\text{İnd}(c,U) = x^2 - (c + c^{-1})x + 1 \in U[x]$$

olduğundan

$$2 = [U(c) : U] = [Q(c) : U]$$

dır. Boyut teoremine göre verilen

$$[Q(c) : Q] = [Q(c) : U]\,[U : Q]$$

ifadesinden

$$[U : Q] = \frac{\varphi(n)}{2}$$

elde edilir. O halde düzgün n köşelinin pergel ve cetvelle inşa edilebilmesi için gerek ve yeter koşul, teorem 53 e göre $\varphi(n)$ sayısının 2 nin bir kuvveti şeklinde olmasıdır. $p_1, \ldots, p_r \in P$ ikişer tarzda farklı asal sayılar olmak üzere,

$$n = \prod_{i=1}^{r} p_i^{n_i}\ ,\ (n_1>0, \ldots, n_r>0)$$

olsun. Bu takdirde

$$\varphi(n) = \prod_{i=1}^{r} (p_i - 1)\, p_i^{n_i-1}$$

dir. $\varphi(n)$ sayısının 2 nin bir kuvveti olabilmesi için gerek ve yeter koşul, her tek asal faktör p_j için $n_j = 1$ ve bir $s \in \mathbf{N}$ için

$$p_j = 1 + 2^s$$

olmasıdır. Böyle bir s sayısı da 2 nin bir kuvvetine eşit olmalıdır. Zira $2 \nmid b$, $b>1$ olmak üzere $a,b \in \mathbf{N}$ için $s = ab$ olduğunu kabul edelim. Bu takdirde

$$p_j = 2^{ab} + 1 = (2^a + 1)(2^{ab-a} - 2^{ab-2a} + - \ldots + 1)$$

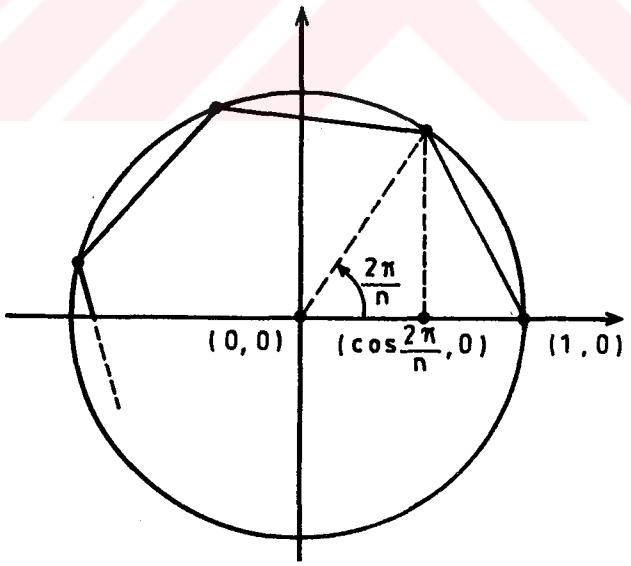
olduğundan

$$1 + 2^a \mid p_j$$

elde edilir. Bu sonuç p_j nin bir asal sayı olmasına aykırıdır. Dolayısıyla

$$n = 2^m \prod_{i=2}^{r} p_i$$

elde edilir. Burada p_i ler Fermat asal sayılarıdır.



Şekil 7. Düzgün n köşelinin inşası.

3.2. Düzgün 17 Köşelinin İnşası

$$c = \cos\frac{2\pi}{17} + i\sin\frac{2\pi}{17}$$

olmak üzere

$$\cos\frac{2\pi}{17} = \frac{1}{2}(c + c^{-1}) = d$$

büyüklüğünü 17 inci çember bölen $Q^{(17)} = Q(c)$ cisminde pergel ve cetvelle inşa edelim.

$$G\left(\frac{Q^{(17)}}{Q}\right) = G$$

grubunun kompozisyon serisinin faktörleri 2. mertebeden altgruplardır. Teorem 48 e göre

$$G \simeq Z_{17}^{*}$$

dır ve bu izomorfi $\sigma_i \in G$ olmak üzere

$$\sigma_i \rightarrow \bar{i} \ , \quad \bar{i} \in Z_{17}^{*}$$

ile belirlenir ve

$$c^{\sigma_i} = c^{i} \ , \quad i=1,\ldots,16$$

verilir. $Z_{17}^{*} = \langle\bar{3}\rangle$ grubu devirli olduğundan G grubu da devirli olup $\sigma_3 = \sigma$ olmak üzere

$$G = \langle\sigma\rangle \ , \quad |\sigma| = 16$$

dır. Bu takdirde G nin altgrupları

$$H_i = \langle\sigma^{i}\rangle \ , \quad i=1, 2, 4, 8, 16$$

şeklindedir [4]. Dolayısıyla G grubunun kompozisyon serisi

$$G = H_1 > H_2 > H_4 > H_8 > H_{16} = E$$

şeklindedir. İlgili cisim serisi

$$Q = K_1 \subset K_2 \subset K_4 \subset K_8 \subset K_{16} = Q^{(17)}$$

olsun. Bu seri K_1 cisminden itibaren ardarda karekök katılması ile inşa edilir. Teorem 55 in ispatında olduğu gibi

$$d^{o}\text{ind}\,(c, Q(d)) = 2$$

olduğundan

$$[Q(c) : Q(d)] = [Q(d)(c) : Q(d)] = 2$$

dır ve bunun yardımıyla

$$16 = [Q(c) : Q] = [Q(c) : Q(d)]\,[Q(d)] : Q]$$

ifadesinden

$$[Q(d) : Q] = 8$$

elde edilir. Bunun yanında $[K_8 : Q] = 8$ olduğundan teorem 8 (b) ye göre $Q(d) = K_8$ elde edilir. Dolayısıyla sadece K_2 ve K_4 aracisimlerini belirlemek yeterlidir.

$$Q \subset K_2 \subset K_4 \subset Q(d) \subset Q(c)$$

teorem 46 ya göre

$$K_i = Q(B_{H_i}(c),\ B_{H_i}(c^2),\ldots,\ B_{H_i}(c^{16}))\ ,\quad i=2,4$$

ve $B_{H_i} = B_i$ olmak üzere

$$B_i(c^j) = \sum_{k=1}^{\frac{16}{i}} (c^j)^{\sigma^{ik}} = \sum_{k=1}^{\frac{16}{i}} c^{j3^{ik}}\ ,\quad i=2,4$$

verilir. Bunun yardımıyla

$$\begin{aligned}
B_2(c) &= B_2(c^2) = B_2(c^4) = B_2(c^8) = B_2(c^9) = B_2(c^{13}) = B_2(c^{15}) = B_2(c^{16}) \\
&= c + c^{-1} + c^2 + c^{-2} + c^4 + c^{-4} + c^8 + c^{-8} \\
B_2(c^3) &= B_2(c^5) = B_2(c^6) = B_2(c^7) = B_2(c^{10}) = B_2(c^{11}) = B_2(c^{12}) = B_2(c^{14}) \\
&= c^3 + c^{-3} + c^5 + c^{-5} + c^6 + c^{-6} + c^7 + c^{-7} \\
B_4(c) &= B_4(c^4) = B_4(c^{13}) = B_4(c^{16}) = c + c^{-1} + c^4 + c^{-4} \\
B_4(c^2) &= B_4(c^8) = B_4(c^9) = B_4(c^{15}) = c^2 + c^{-2} + c^8 + c^{-8} \\
B_4(c^3) &= B_4(c^5) = B_4(c^{12}) = B_4(c^{14}) = c^3 + c^{-3} + c^5 + c^{-5} \\
B_4(c^6) &= B_4(c^7) = B_4(c^{10}) = B_4(c^{11}) = c^6 + c^{-6} + c^7 + c^{-7}
\end{aligned}$$

yazabiliriz. Bunlar yardımıyla

$$K_2 = Q(B_2(c)\ ,\ B_2(c^3))\ ,\quad K_4 = Q(B_4(c)\ ,\ B_4(c^2)\ ,\ B_4(c^3)\ ,\ B_4(c^6))$$

elde edilir.

$B_2(c)^{\sigma^j}$ resim elemanları arasında farklı olanlar $B_2(c)$ ve $B_2(c^3)$ olduğundan

$$\sum_{i=1}^{16} c^i = -1 \qquad (10)$$

olduğu gözönünde bulundurularak

$$\text{İnd}(B_2(c)\ ,\ Q) = (x - B_2(c))\ (x - B_2(c^3)) = x^2 + x - 4$$

elde edilir. Diğer taraftan

$$B_2(c) = 2(\cos\frac{2\pi}{17} + \cos\frac{4\pi}{17} + \cos\frac{8\pi}{17} + \cos\frac{16\pi}{17}) > 0$$

olduğundan $B_2(c)$ sayısı , x^2+x-4 polinomunun pozitif sıfır yeridir. Dolayısıyla

$$B_2(c) = -\frac{1}{2} + \frac{\sqrt{17}}{2} \quad , \quad B_2(c^3) = -\frac{1}{2} - \frac{\sqrt{17}}{2}$$

dır ve buradan da

$$K_2 = Q(B_2(c))$$

elde edilir.

Her $\tau \in G\left(\frac{Q(c)}{K_2}\right) = H_2$ için $B_4(c)^\tau$ resim elemanları arasında farklı olanlar $B_4(c)$ ve $B_4(c^2)$ olduğundan (10) ifadesi gözönünde bulundurularak

$$\text{İnd}(B_4(c), K_2) = (x - B_4(c))(x - B_4(c^2)) = x^2 - B_2(c)x - 1$$

elde edilir. Diğer taraftan

$$B_4(c) = 2\cos\frac{2\pi}{17} + 2\cos\frac{8\pi}{17} > 0$$

olduğundan $B_4(c)$ sayısı, $x^2 - B_2(c)\,x - 1$ polinomunun pozitif sıfır yeridir:

$$B_4(c) = \frac{B_2(c)}{2} + \frac{1}{2}\sqrt{B_{2(c^2)} + 4} \quad \text{ve} \quad B_4(c^2) = \frac{B_2(c)}{2} - \frac{1}{2}\sqrt{B_2(c^2) + 4}\,.$$

Benzer şekilde, $B_4(c^3)$ ve $B_4(c^6)$ da $x^2 - B_2(c^3) - 1$ polinomunun sıfır yerleri olup

$$B_4(c^3) = \frac{B_2(c^3)}{2} + \frac{1}{2}\sqrt{B_2(c^3)^2 + 4}\ ,\ B_2(c^6) = \frac{B_2(c^3)}{2} - \frac{1}{2}\sqrt{B_2(c^3)^2 + 4}$$

elde edilir.

Bunun yanında

$$[K_2(B_4(c)) : K_2] = 2 = [K_4 : K_2]$$

olduğundan

$$K_4 = K_2(B_4(c))$$

elde edilir.

Son olarak $\text{İnd}(d, K_4)$ polinomu belirlenir. Her $\rho \in G\left(\frac{Q(c)}{K_4}\right) = H_4$ için d^ρ resim elemanları arasında farklı olanlar d ve $c^4 + c^{-4}$ dır. Dolayısıyla

$$\text{İnd}(d,K_4) = (x-d)\,(x-(c^4 + c^{-4})) = x^2 - B_4(c)x + B_4(c^3)$$

elde edilir. Diğer taraftan

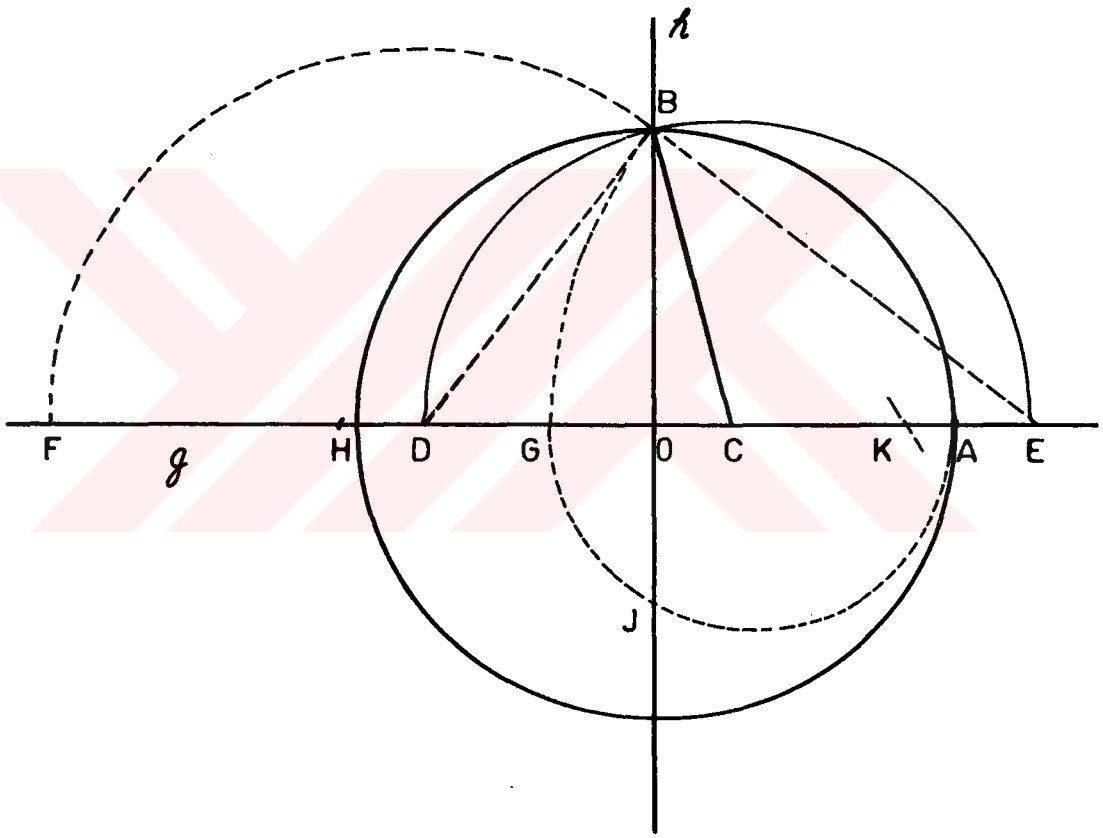
$$d = 2\cos\frac{2\pi}{17} > 2\cos\frac{8\pi}{17} = c^4 + c^{-4}$$

olduğundan d sayısı $\text{İnd}(d,K_4)$ polinomunun maksimum sıfır yeridir. Dolayısıyla

$$\cos\frac{2\pi}{17} = \frac{1}{4}\,(B_4(c) + \sqrt{B_4(c)^2 - 4B_4(c^3)}\,)$$

elde edilir.

Sonuç olarak düzgün 17-genin cetvel ve pergelle inşası bu şekilde elde edilen formüllerden çıkarılır:



Şekil 8. $\cos \frac{2\pi}{17}$ büyüklüğünün pergel ve cetvelle inşası

Birbirine dik g ve h doğrusu ve onların kesim noktası olan O merkezli keyfi seçilmiş $\overline{OA} = \overline{OB}$ birim yarıçaplı çemberi gözönüne alalım.

$B_2(c)$ ve $B_2(c^3)$ ü inşa etmek için öncelikle $\sqrt{17}$ uzunluğunda bir doğru parçasına ihtiyaç vardır. Bunun için $\overline{OA}$ doğru parçası 4 e bölünerek bir C noktası ve böylece uzunluğu

$$\sqrt{1^2 + (\frac{1}{4})^2} = \frac{1}{4}\sqrt{17}$$

olan bir $\overline{BC}$ doğru parçası elde edilir. C merkezli $\overline{BC}$ yarıçaplı çember yayı g doğrusunu D ve E noktalarında keser. Buna göre $\overline{OD}$ ve $\overline{OE}$ nin uzunlukları

$$-\frac{1}{4} + \frac{\sqrt{17}}{4} = \frac{B_2(c)}{2} \text{ ve } \frac{1}{4} + \frac{\sqrt{17}}{4} = -\frac{B_2(c^3)}{2}$$

dır.

$B_4(c)$ ve $B_4(c^3)$ ün inşasında öncelikle

$$\sqrt{\left(\frac{B_2(c)}{2}\right)^2 + 1} \text{ ve } \sqrt{\left(\frac{B_2(c^3)}{2}\right)^2 + 1}$$

köklü ifadelerine ihtiyaç vardır. Gerçekte bu köklü ifadeler OBD ve OBE dik üçgenlerinden $\overline{BD}$ ve $\overline{BE}$ doğru parçalarının uzunlukları olarak bulunur. D merkezli ve $\overline{BD}$ yarıçaplı çember g doğrusunu F noktasında keser. Buradan $\overline{OF} = \overline{OD} + \overline{DF}$ doğru parçası

$$\frac{B_2(c)}{2} + \sqrt{\left(\frac{B_2(c)}{2}\right)^2 + 1} = B_4(c)$$

uzunlukludur.

Buna paralel yolla E merkezli $\overline{BE}$ yarıçaplı çember g doğrusunu G noktasında keser. $\overline{OG} = \overline{EG} - \overline{EO}$ doğru parçasının uzunluğu

$$\sqrt{\left(\frac{B_2(c^3)}{2}\right)^2 + 1} - \left(\frac{B_2(c^3)}{2}\right) = B_4(c^3)$$

dır.

Son olarak d nin inşası için

$$\sqrt{\left(\frac{B_2(c^3)}{2}\right)^2 - B_4(c^3)} = \sqrt{\left(\frac{B_4(c)}{2}\right)^2 - \left(\sqrt{B_4(c^3)}\right)^2}$$

köklü ifadesine ihtiyaç vardır. Bunun için $\overline{OF}$ doğru parçası iki eşit parçaya bölünerek uzunlukları $\frac{B_4(c)}{2}$ olan $\overline{OH}$ ve $\overline{HF}$ doğru parçaları elde edilir. Diğer yandan $\overline{AG}$ doğru parçası üzerinde Tales çemberi oluşturularak GJA dik üçgenindeki $\overline{OJ}$ yüksekliğinin uzunluğu $\sqrt{1.B_4(c^3)} = \sqrt{B_4(c^3)}$ olarak elde edilir.

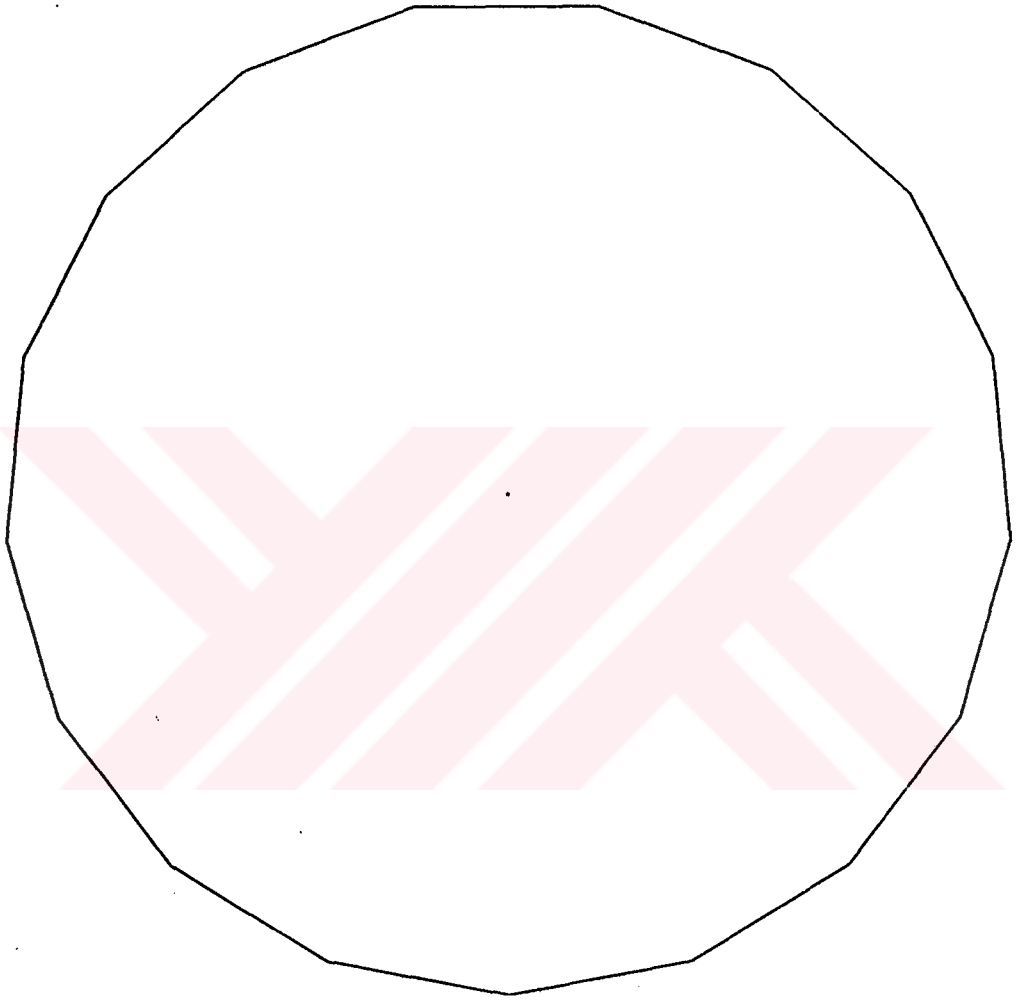
J merkezli ve $\overline{OH} = \overline{HF}$ yarıçaplı çember yayı g doğrusunu K noktasında keser. $\overline{OK}$ doğru parçası JOK dik üçgeninde uzunluğu

$$\sqrt{\left(\frac{B_4(c)}{2}\right)^2 - B_4(c^3)}$$

olan bir dik kenardır. $\overline{HK}$ doğru parçası için $\overline{HK} = \overline{HO} + \overline{OK}$ sağlanır ve bunun uzunluğu

$$\frac{B_4(c)}{2} + \sqrt{\left(\frac{B_4(c)}{2}\right)^2 - B_4(c^3)} = c + c^{-1} = 2\cos\frac{2\pi}{17}$$

dır. Bunun yarısı, uzunluğu $\cos\frac{2\pi}{17}$ olan aranan doğru parçasını verir.



Şekil 9. Düzgün 17- gen.

4. İRDELEME

K bir cisim, L K nın bir genişlemesi ve $T \subset L$ bir altküme olsun. L nin hem K hem de T yi içine alan en küçük altcismine yeni L nin $K \cup T$ yi kapsayan bütün altcisimlerinin arakesiti olan altcisme K ya T kümesini katarak elde edilen genişleme denir ve K(T) ile gösterilir.

T nin tek α öğesinden oluşması durumunda K(T) yerine $K(\alpha)$ gösterimi kullanılarak buna K ya α yı katmakla elde edilen genişleme denilir.

Bu katmalar yardımıyla pergel ve cetvel adımları arasındaki ilişki aşağıdaki şekilde verilir:

1. Çakışık olmayan doğruların kesim noktası (varsa) bu noktayı elde edinceye kadar kullanılan noktaların koordinatlarını içine alan en küçük cisim K_o, bunlarla birlikte kesim noktasının koordinatlarını da içine alan en küçük cisim K_1 ise $K_o=K_1$ yani

$$[K_1 : K_o] = 1 = 2^o$$

dır.

2. Bir doğruyla bir çemberin kesim noktaları elde edilinceye kadar kullanılan noktaların koordinatlarını içine alan en küçük cisim K_o ve bunlarla birlikte kesim noktalarının koordinatlarını da içine alan en küçük cisim K_1 ise

$$K_1 = K_o(\sqrt{\Delta})$$

olup $\sqrt{\Delta} \in K_o$ iken $[K_1:K_o]=1=2^o$ ve $\sqrt{\Delta} \notin K_1$ iken $[K_1:K_o]=2$ elde edilir.

3. Pergel ve cetvel adımlarından olan iki çemberin kesim noktalarının belirlenmesi problemlerinde de durum aynıdır.

Daha da genel olarak şu temel teorem verilerek katmalar yardımıyla bir noktanın yalnız pergel ve cetvel kullanılarak elde edilebilmesi aşağıdaki şekilde ifade edilir:

$A_1, ..., A_m$ keyfi ve sonlu sayıda noktalar, $\{a_1, ..., a_n\}$ bu noktaların koordinatlarının kümesi ve A $A_1, ..., A_m$ noktalarından pergel ve cetvelle inşa edilebilen bir nokta olsun. Bu taktirde A noktasının koordinatları, $Q(a_1, ..., a_n)$ cisminden sonlu sayıda 2 eksponentli radikallerin (karaköklerin) ardarda katılmasıyla elde edilen L cisminde bulunurlar. Diğer bir ifade ile sonlu sayıda $d_1, ..., d_r$ kompleks sayıları

$$d_i \in Q(a_1,...,a_n, \sqrt{d_1}, ..., \sqrt{d_{i-1}}), \quad i=1,...r$$

ve

$$L = Q(a_1, ..., a_n, \sqrt{d_1}, ..., \sqrt{d_r})$$

olmak üzere mevcutturlar.

Tersine olarak koordinatları, $Q(a_1,...,a_n)$ cisminin yukarıdaki gibi bir genişlemesinde bulunan her nokta, $A_1,...,A_n$ noktalarından pergel ve cetvelle inşa edilebilir.

5. SONUÇLAR

(1) Bir K cisminin verilen bir sonlu genişlemesinin tüm K-izomorfileri belirlenmeye çalışıldı. Önce normal genişlemeler gözönüne alınarak, bir normal genişlemenin bir K-otomorfisinin, bu genişlemenin bir altcisminin bir K-izomorfisinin genişletilmişi olarak elde edilebileceği gösterildi.

(2) Her sonlu, normal ve ayrılabilir bir cisim genişlemesinin tüm altcisimlerinin belli bir sonlu grubun altgrupları ile karakterize edilebileceği ve dolayısıyla sözü geçen cisim genişlemesinin tüm altcisimlerini belirleme probleminin bir sonlu grubun tüm altgruplarını belirleme problemine indirgenebileceği gösterildi.

(3) Bir Galois grubunun altgruplarına tekabül eden aracisimlerin nasıl bulunabileceği gösterildi.

(4) K cisim ve L cismi K nın bir Galois genişlemesi olmak üzere

a) L cisminin K üzerindeki bir primitif elemanının verilmesi,

b) L cisminin K üzerindeki bir üretici sisteminin verilmesi,

c) L cisminin bir ayrılabilir polinomun K üzerindeki bir parçalayıcı cismi olarak verilmesi hallerinde $G(\frac{L}{K})$ Galois grubunun nasıl bulunabileceği araştırıldı.

(5) Pergel ve cetvel kullanmanın ne demek olduğu üzerinde durularak pergel ve cetvel adımları sonucu üretilen yeni noktaların koordinatları ile eskilerin koordinatları arasındaki bağıntı cebirsel ifadelerle belirlenerek daha sonra bu cebirsel ifadelerin cisim teorisindeki karşılıkları verildi.

(6) $n>2$ olmak üzere $n \in \mathbf{N}$ için düzgün n köşelinin pergel ve cetvelle inşa edilebilmesi için gerek ve yeter koşullar ispatlandı. Bu koşullar altında düzgün 17-gen pergel ve cetvelle inşa edildi.

6. ÖNERİLER

(Richolet (1832) tarafından "De resolutine algebraica aequationis $x^{257}=1$, sive de divisione circuli per bisectionam anguli septies repetitam in partes 257 inter se aequales commentatio coronata" başlığı altında Crelle's Journal da düzgün 257-genin bir inşası yayınlanmıştır. Fakat 65537 genin inşası hakkında herhangi bir belgeye rastlanılmamasına rağmen Profesör Hermes'in on yılını bu probleme harcadığı ve dökümanları Göttingen de sakladığı ileri sürülmektedir [7]. Bu konu üzerinde çalışmalar yapılabilir.

7. KAYNAKLAR

1. BAYAR,E., Soyut Cebir, Karadeniz Üniversitesi, Fen-Edebiyat Fakültesi, Genel Yayın No. 102, Fakülte Yayını No. 41, Trabzon 1986.

2. BHATTACHARYA, P.B., JAIN, S.K. ve NAGPAUL, S.R., Basic Abstract Algebra, Cambridge University Press 1986.

3. GARLING, D.J.H., A Course In Galois Theory, Cambridge University Press 1986.

4. HUNGERFORD , J.W., Algebra, Hot, Rinehart-Winston 1973.

5. KANAGASABAPATHY, P., A New Proof of the Compositeness of F_5, Mathematical Gazette, 42 (1958) 310

6. LUGOWSKI, H. ve WEINERT, H.J., Grundzüge der Algebra, Teil III: B.G. Teubner Verlagsgesellschaft, Leipzig 1967.

7. STEWART, I., Galois Theory, Chapman and Hall, New York 1989.

8. ÖZGEÇMİŞ

Bahaddin SİNSOYSAL, 2.3.1969 da İstanbul'da doğdu. 1980 yılında Çamaltı İlkokulu'ndan, 1983 yılında Kavacık Ortaokulu'ndan, 1986 yılında Üsküdar Halide Edip Adıvar Lisesi'nden mezun oldu.

1986 yılında kazandığı K.T.Ü. Fen-Edebiyat Fakültesi matematik Bölümü'nden 1991 yılında mezun oldu. Aynı yıl, aynı Üniversitede Fen Bilimleri Enstitüsü Yüksek Lisans (Matematik) programına başladı.

Nisan 1994 tarihinden itibaren K.T.Ü. Fen-Edebiyat Fakültesi Matematik Bölümü'nde Araştırma Görevlisi olarak görev yapmaktadır. Bildiği yabancı dil ise İngilizce'dir.