Mat624
Cebir II

Ders Notları

Bülent Saraç
Hacettepe University
Department of Mathematics
http://www.mat.hacettepe.edu.tr/personel/akademik/bsarac/

İçindekiler

Kısım 1

CİSİM TEORİSİ

BÖLÜM 1

Eşitliklerin Galois Teorisi

1.1. Giriş

Bu bölümde

(1) polinom eşitliklerinin yalnız köklü ifadeler ve cebirsel işlemler yardımıyla çözülmesi

ve

(2) işaretsiz cetvel ve pergel yardımıyla geometrik nesnelerin çizilmesi

problemleri üzerinde durulacaktır.

Bilindiği gibi $aX^2+bX+c=0$ $(a,b,c\in\mathbb{R})$ tipindeki bir kuadratik eşitliğin çözümü

$$\frac{-b\pm\sqrt{b^2-4ac}}{2a},$$

formülü ile verilebilir. Bu formül Babil dönemine kadar uzanmaktadır. Yukarıdaki (1) nolu problemle ilgili en temel katkılar, İtalyan Rönesansı döneminde, Scipione del Ferro ve Niccolo Tartaglia tarafından yapılmıştır. Tartaglia'nın sonuçları Geronimo Cardano'nun 1545'te yayınlanan ünlü Ars Magna'sında yer almıştır. Şimdi Tartaglia'nın $X^3+aX^2+bX+c=0$ şeklindeki bir eşitliğin çözümünü bulmak için ne yaptığına kısaca göz atalım. İlk adım olarak X yerine $X-\frac{1}{3}a$ yazarak eşitliği $X^3+pX+q=0$ tipindeki bir eşitliğe indirgeyelim. x_1, x_2 ve x_3 bu yeni denklemin tüm çözümleri ise

$$\begin{aligned}\delta &= -4p^3-27q^2\\ \zeta &= -\frac{1}{2}-\frac{1}{2}\sqrt{-3}\\ y_1 &= x_1+\zeta^2x_2+\zeta x_3\\ y_2 &= x_1+\zeta x_2+\zeta^2x_3\end{aligned}$$

için Cardano'nun formülleri

$$y_1=\sqrt[3]{-\frac{27}{2}q+\frac{3}{2}\sqrt{-3\delta}}$$
$$y_2=\sqrt[3]{-\frac{27}{2}q-\frac{3}{2}\sqrt{-3\delta}}$$

şeklinde verilmiştir. Ayrıca indirgenmiş denklemin yapısından dolayı $x_1+x_2+x_3=0$ eşitliği elde edilir. Buna göre

$$\begin{aligned} x_1 + \zeta^2 x_2 + \zeta x_3 &= y_1 \\ x_1 + \zeta x_2 + \zeta^2 x_3 &= y_2 \\ x_1 + x_2 + x_3 &= 0 \end{aligned}$$

eşitlikleri ortak çözülürse x_1, x_2 ve x_3 çözümleri elde edilir.

A. Ruffini (1813) ve N. H. Abel (1827) derecesi dörtten büyük olan eşitliklerin çözümlerini köklü ifadeler ve cebirsel işlemler ile vermenin mümkün olmadığını gösterdiler. Aslında Ruffini ve Abel'in kanıtları üstü kapalı idi ve tam değildi. Galois'nın çalışmaları, Ruffini–Abel Teoreminin kanıtını tamamlamakla kalmayıp aynı zamanda

$$X^n + a_1 X^{n-1} + \cdots + a_{n-1} = 0$$

tipindeki bir eşitliğin kökler ve cebirsel işlemler ile çözülmesi için bir kriter de sağlamıştır. (Galois bu çalışmalarını daha yirmili yaşlarına gelmeden önce tamamlamıştır.)

İkinci problem ise Yunan matematiğine kadar dayanmaktadır. Bu konu dahilinde en çok dikkati çeken problemler aşağıdaki gibidir:

(*a*) bir açının üç eş parçaya bölünmesi;

(*b*) bir küpün iki katının inşası; yani, bir küpün hacminin iki katı hacme sahip bir küp elde edilmesi;

(*c*) bir düzgün yedigen çizilmesi; ve

(*d*) bir çemberin kareleştirilmesi; yani, alanı bir çemberinkine eşit olan bir kare çizilmesi.

Geometrik çizimler ile ilgili problemlerde ele alınan geometrik nesnelerin elde edilmesi, sadece üzerinde hiçbir işaret ve ölçü aracı bulunmayan düz bir cetvel ile pergel kullanılarak mümkündür. Bu problem ile ilgili olan tüm tartışmalarda kısaca "*cetvel*" kelimesi ile üzerinde hiçbir işaretleme bulunmayan ve düz çizgi çizmeye yarayan bir çizim aracı kastedilecektir. Pergel ise iki ayağından birinde sabitlemek için kullanılmak üzere iğne, diğerinde ise işaretleme yapmak için kullanılmak üzere kalem bulunan ve yay çizmeye yarayan basit bir çizim aracı anlamına gelecektir. Bu konuya cisimleri ele aldığımız bir bölümde yer vermemizin nedeni herhangi bir geometrik çizim probleminin cisimler üzerinde bir cebirsel probleme dönüştürülebiliyor olmasıdır. Örneğin yukarıdaki (d) maddesinin olanaksız olması Lindemann'ın 1882 yılında gösterdiği gibi π sayısının bir transandant sayı olmasından ileri gelmektedir. Düzgün bir n–genin cetvel–pergel yardımıyla çizilmesinin mümkün olduğu n doğal sayılarının belirlenmesi genel problemi Gauss tarafından 1801 yılında çözülmüştür. Gauss'un sonucuna göre bu n sayıları ancak 17, 257 ve 65537 olmaktadır.

1.2. Önbilgiler ve Temel Sonuçlar

Herhangi bir R halkası için

$$\mathbb{Z}1 = \{m \cdot 1_R : m \in \mathbb{Z}\}$$

kümesi R'nin bir alt halkasıdır. Bu alt halkaya R'nin "asal halkası" adı verilir. Dikkat edilirse $\mathbb{Z}1 \cong \mathbb{Z}$ ya da $\mathbb{Z}1 \cong \mathbb{Z}/(k)$ $(k \neq 0)$ dır. Birinci durumda R'nin karakteristiği ($\operatorname{kar} R$ ile gösterilir) sıfırdır. İkinci durumda ise $\operatorname{kar} R = k$ olur. R bir tamlık bölgesi

ve $\operatorname{kar} R = k \neq 0$ ise o zaman k bir asal sayıdır. Şimdi $R = F$ bir cisim olsun. Bu durumda $\mathbb{Z}1$ alt halkası F'nin bir alt cismi olur. Bu alt cisme F'nin "asal cismi" denir. Eğer $\operatorname{kar} F = p \neq 0$ ise o zaman F'nin asal cismi $\mathbb{Z}/(p)$ cismine izomorftur. Aksine $\operatorname{kar} F = 0$ ise $\mathbb{Z} \to F$, $m \mapsto m \cdot 1$ şeklinde tanımlanan gömme dönüşümü (birebir halka homomorfizması, ya da monomorfizma) $\mathbb{Q} \to F$ gömme dönüşümüne genişler. Yani $\mathbb{Q}$ cismini F içine gömebiliriz. Sonuç olarak bir F cismi ya bir p asal sayısı için $\mathbb{Z}/(p)$ cismini ya da $\mathbb{Q}$ cismini içerir.

F bir cisim ve E F'nin bir genişlemesi (yani E ve F birer cisim ve F E'nin bir alt cismi) olsun. S, E'nin bir alt kümesi ise $F[S]$ ile E'nin F'yi ve S'yi içeren tüm alt cisimlerinin arakesiti gösterilecektir. Açıktır ki $F[S]$, E'nin $F \cup S$ kümesini içeren *en küçük* alt halkasıdır. $F[S]$ halkasına E'nin F–üzerinde S *tarafından üretilen alt halkası* ya da E/F'nin S *tarafından üretilen alt halkası* denir. Kolayca gösterilebilir ki

$$F[S] = \{ \sum_{(i_1,\ldots,i_n)\in\Lambda} c_{i_1,\ldots,i_n}\sigma_1^{i_1}\ldots\sigma_n^{i_n} : \Lambda \subseteq \mathbb{N}^n \text{ sonlu, her } (i_1,\ldots,i_n) \in \Lambda$$
$$\text{için } c_{i_1,\ldots,i_n} \in F \text{ ve } \sigma_1,\ldots,\sigma_n \in S\}$$

dir. Diğer taraftan E'nin $F \cup S$ kümesini içeren en küçük alt cismini $F(S)$ ile göstereceğiz. Bu alt cisme E/F'nin S *tarafından üretilen alt cismi* denir. Eğer T, E'nin başka bir alt kümesi ise o zaman $F(S)(T) = F(S \cup T)$ dir. Bir $u \in E$ için $F(\{u\})$ yerine $F(u)$ gösterimini tercih edeceğiz. Eğer $E = F(u)$ ise o zaman E'ye F'nin bir *basit genişlemesi* denir. Genel olarak $u_1, u_2, \ldots, u_n \in E$ ise $F(\{u_1, u_2, \ldots, u_n\})$ yerine daha basit olan $F(u_1, u_2, \ldots, u_n)$ ifadesini kullanacağız. Eğer $E = F(u_1, \ldots, u_n)$ ise E'ye F'nin bir sonlu genişlemesi denir.

Soru: E/F bir cisim genişlemesi ise bir $u \in E$ için $F(u)$ cismi neye benzemektedir?

F üzerinde birim olan ve X'i u'ya gönderen

$$\begin{aligned} \varphi_u : F[X] &\to E \\ g(X) &\mapsto g(u) \end{aligned}$$

değer homomorfizmasını düşünelim. Bu homomorfizmanın çekirdeği ($\operatorname{çek}\varphi_u$ ile gösterilir) sıfır ise $F[X] \cong F[u]$ olur. Bu durumda u'ya F üzerinde *transandant* denir. Aksi halde –yani $\operatorname{çek}\varphi_u \neq 0$ ise– o zaman $\operatorname{çek}\varphi_u = (f(X))$ olacak şekilde bir monik $f(X) \in F[X]$ polinomu bulunabilir. Dolayısıyla $F[X]/(f(X)) \cong F[u]$ olur. Bu durumda u'ya F üzerinde bir *cebirsel eleman* denir. Daha açık bir şekilde söylemek gerekirse u, F üzerinde cebirseldir ancak ve ancak u katsayıları F'nin elemanı olan sıfırdan farklı bir polinomun köküdür. $F[X]$ bir temel ideal bölgesi ve $f(X) \in F[X]$ bir asal eleman olduğundan $f(X) \in F[X]$ bir monik indirgenemez polinomdur. (Temel ideal bölgelerinde asal ve indirgenemez elemanlar çakışır.) Buradaki $f(X)$ polinomuna u'nun *minimal polinomu* adı verilir. Demek ki F üzerinde bir cebirsel eleman, $F[X]$ polinom halkasındaki bir monik indirgenemez polinomun köküdür ve bu monik indirgenemez polinoma o cebirsel elemanın minimal polinomu denir. Dikkat edilirse $F[X]$ bir temel ideal bölgesi ve $F[X]$'in sıfırdan farklı her öz idealinin bir ve yalnız bir tek monik üreteci bulunduğundan, bir cebirsel elemanın minimal polinomu ancak tek türlü belirlidir. Bir cebirsel $u \in E$ elemanının minimal polinomu $f(X)$ ise bu durumda $(f(X))$ temel ideali $F[X]$ halkasının bir maksimal ideali olacağından $F[u]$ bir cisim olur. Ayrıca $F \cup \{u\} \subseteq F[u] \subseteq F(u)$ ve $F(u)$, F ve u'yu içeren E'nin en küçük alt cismi olduğundan $F[u] = F(u)$ elde edilir. Diğer taraftan $F[X] \cong F[u]$ ise her $g(X) \in F[X]$ elemanını

$g(u) \in F[u]$ elemanına gönderen izomorfizma $F(X)$ cisminden ($F(X)$, $F[X]$'in kesirler cismi olan rasyonel polinomlar cismidir) $F(u)$ cismine tanımlı bir monomorfizmaya genişler. Dolayısıyla $F(u) \supsetneq F[u]$, $F(u) \cong F(X)$ elde edilir. Buna göre $F(u)$ cismi, $g(X), h(X) \in F[X]$ ve $h(x) \neq 0$ olmak üzere $g(u)h(u)^{-1}$ yapısındaki elemanlardan oluşur.

Açıklama. E/F bir cisim genişlemesi ve $u \in E$, F üzerinde cebirsel olsun. Buna göre $f(u) = 0$ ve $F(u) \cong F[X]/(f(X))$ olacak şekilde monik indirgenemez bir ve yalnız bir tek $f(X) \in F[X]$ polinomu vardır. Burada $f(X)$ polinomunun $f(u) = 0$ özelliğini sağlayan polinomlar arasında derecesi en küçük olan polinom olduğunu belirtmek gerekir. Aslında $f(x)$'in bu özelliği, "minimal polinom" ismini açıklayan özelliğidir. $f(x)$ polinomunun derecesine ($\operatorname{der} f(x)$ ile gösterilir) *u'nun F üzerindeki derecesi* denir.

E/F gibi bir cisim genişlemesini çalışırken E'yi F üzerinde bir vektör uzayı olarak düşünmenin faydası çok büyüktür. Gerçekten de E'nin zaten var olan toplamsal grup yapısına ek olarak yine zaten E'de bulunan çarpma işlemini kullanarak E'nin elemanları ile F'nin elemanları arasında skalerle çarpma işlemi tanımlanırsa E'yi Fcismi üzerinde bir vektör uzayı yapmış oluruz. Her vektör uzayının bir bazı olması gerektiğini ve herhangi iki bazın kardinalitelerinin aynı olması gerektiğini biliyoruz. Tüm bazların sahip olduğu bu ortak kardinaliteye vektör uzayının "boyutu" denir. Eğer V bir F–uzayı ise V boyutu $\operatorname{boy}_F V$ ya da üzerinde çalışılan cisim üzerinde hiçbir şüphe yoksa kısaca $\operatorname{boy} V$ şeklinde gösterilir. E/F cisim genişlemesi söz konusu olduğunda bu gösterimin dışına çıkarak E'nin F üzerindeki vektör uzayı boyutunu $[E : F]$ ile göstereceğiz. Eğer bir E/F genişlemesi için $[E : F] < \infty$ ise bu genişlemeye bir sonlu boyutlu genişleme; E'ye de F'nin bir sonlu boyutlu genişlemesi denir. Aşağıdaki önerme bir elemanın cebirsel olup olmadığını anlamak konusunda oldukça kullanışlıdır.

Önerme 1.1. *E/F bir cisim genişlemesi ve $u \in E$ olsun. u'nun F üzerinde cebirsel olması için gerek ve yeter koşul $[F(u) : F] < \infty$ olmasıdır.*

Kanıt. Önce $u \in E$ cebirsel olsun. u'nun minimal polinomu f ve $\operatorname{der} f = n$ olsun. $[F(u) : F] = n$ olduğunu göstereceğiz. u cebirsel ise $F(u) = F[u]$ olduğunu biliyoruz. $x \in F(u)$ olsun. O zaman $x = g(u)$ olacak şekilde $g(X) \in F[X]$ polinomu vardır. Bölme algoritması kullanılırsa $g(X) = f(X)q(X) + r(X)$ ve $r(X) = 0$ veya $\operatorname{der} r(X) < \operatorname{der} f(X)$ olacak şekilde $q(X), r(X) \in F[X]$ polinomları bulunabilir. Eşitliğin her iki tarafına φ_u değer homomorfizması uygulanırsa $g(u) = f(u)q(u)+r(u) = r(u)$ elde edilir. $r(X) = 0$ veya $\operatorname{der} r(X) < n$ olduğundan $r(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$ yazabiliriz. Buna göre $x = g(u) = r(u) = a_0 + a_1u + \cdots a_{n-1}u^{n-1}$ bulunur. Dolayısıyla $F(u)$, F üzerinde vektör uzayı olarak $\{1, u, \ldots, u^{n-1}\}$ kümesi tarafından gerilir. Şimdi de $\{1, u, \ldots, u^{n-1}\}$ kümesinin F üzerinde doğrusal bağımsız olması gerektiğini gösterelim. Aksini kabul edelim. Yani $b_0 + b_1u + \cdots + b_{n-1}u^{n-1} = 0$ olacak şekilde hepsi birden sıfır olmayan $b_0, b_1, \ldots, b_{n-1} \in F$ elemanları bulunsun. Buna göre u, sıfırdan farklı $b + b_1X + \cdots + b_{n-1}X^{n-1} \in F[X]$ polinomunun bir kökü olur. Fakat bu durum f'nin u'yu kök kabul eden en küçük dereceli polinom olması ile çelişir. Dolayısyla $\{1, u, \ldots, u^{n-1}\}$ kümesi E'nin$F$ üzerindeki bir bazı olur.

Diğer taraftan $[F(u) : F] = n < \infty$ olsun. O zaman $F(u)$'nun n'den fazla eleman içeren herhangi bir alt kümesi F üzerinde doğrusal bağımlı olur. Özel olarak $\{1, u, \ldots, u^n\}$ kümesini alırsak, bu küme de F üzerinde doğrusal bağımlı olacağından hepsi birden

sıfır olmayan $a_0, a_1, \ldots, a_n \in F$ elemanları için $a_0 + a_1u + \cdots + a_nu^n = 0$ olur. Dolayısıyla u, sıfırdan farklı $a_0 + a_1X + \cdots + a_nX^n \in F[X]$ polinomunun bir köküdür. Bu da kanıtı tamamlar. □

Açıklama. E/F bir cisim genişlemesi ve $u \in E$, F üzerinde cebirsel olsun. Buna göre u'nun F üzerinde minimum polinomu vardır. Bu polinom f olsun. Eğer bir $g(X) \in F[X]$ için $g(u) = 0$ ise $f(X) \mid g(X)$ dir. Aslında Bölme Algoritmasından $g(X) = f(X)q(X) + r(X)$ ve $r(X) = 0$ veya $\operatorname{der} r(X) < \operatorname{der} f(X)$ olacak şekilde $q(X), r(X) \in F[X]$ polinomları vardır. Her iki tarafa φ_u değer homomorfizması uygulanırsa $r(u) = 0$ bulunur. Eğer $r(X) \neq 0$ ise bu durum f'nin seçimi ile çelişir. Dolayısıyla $r(X) = 0$, yani $f \mid g$ olmak zorundadır. Eğer $F[X]$'in elemanları arasında

$$p(X) \preceq q(X) \iff p(X) \mid q(X)$$

şeklinde bir $\preceq$ bağıntısı tanımlanırsa, kolayca görülebilir ki $\preceq$ bir sıralama bağıntısı olur. İşte bu sıralama bağıntısına göre $f(X)$

$$\{g(X) \in F[X] : g(X) \text{ monik ve } g(u) = 0\}$$

kümesinin "en küçük" elemanıdır. Bu da $f(X)$'in minimalliğine başka bir açıdan bakış sunmaktadır.

Şu ana kadar söylediklerimizi aşağıdaki teorem ile toparlayabiliriz.

Teorem 1.2. *E/F bir cisim genişlemesi ve $u \in E$ olsun. Buna göre u, F üzerinde cebirseldir ancak ve ancak $F(u)$, F üzerinde sonlu boyutludur. Bu durumda $F(u)$ cismi $F[u] = \{g(u) : g(X) \in F[X]\}$ halkası ile çakışır.*

Teorem 1.3. *$K \supset E \supset F$ cisimler ise $[K : F]$ sonludur ancak ve ancak $[K : E]$ ve $[E : F]$ sonludur. Bu durumda aşağıdaki eşitlik sağlanır:*

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

Kanıt. Önce $[K : F]$ sonlu olsun. E, K'nın bir alt uzayı olduğundan $[E : F] < \infty$ olduğu açıktır. Ayrıca K'nın bir F–bazı alındığında bu baz K'yı E–üzerinde de gerer. Dolayısıyla K'nın her F–bazı, K'nın bir E–bazını içereceği için $[K : E] < \infty$ elde edilir.

Diğer taraftan $[K : E]$ ve $[E : F]$ sonlu olsun. Kabul edelim ki $\{\alpha_i\}_{i=1}^r$ K'nın bir E–bazı, $\{\beta_j\}_{j=1}^s$ ise E'nin bir F–bazı olsun. Göstereceğiz ki $\mathcal{B} = \{\alpha_i\beta_j : 1 \leq i \leq r, 1 \leq j \leq s\}$ kümesi K'nın bir F–bazıdır. Önce $\mathcal{B}$'nin K'yı F–üzerinde gerdiğini gösterelim. $x \in K$ olsun. Buna göre

$$x = \sum_{i=1}^{r} \epsilon_i\alpha_i$$

olacak şekilde $\epsilon_i \in E$ elemanları vardır. Ayrıca her $i = 1, \ldots, r$ için

$$\epsilon_i = \sum_{j=1}^{s} \phi_{ij}\beta_j$$

olacak şekilde $\phi_{ij} \in F$ elemanları bulunur. Dolayısıyla

$$x = \sum_{i=1}^{r} \epsilon_i\alpha_i = \sum_{i=1}^{r}\sum_{j=1}^{s} \phi_{ij}(\alpha_i\beta_j)$$

yazabiliriz. x elemanı keyfi olduğundan $\mathcal{B}$ kümesi K'yı F üzerinde gerer. Şimdi $\mathcal{B}$'nin F üzerinde doğrusal bağımsız olduğunu gösterelim. Kabul edelim ki bazı $\phi_{ij} \in F$ $(i = 1, \ldots, r,\ j = 1, \ldots, s)$ elemanları için

$$\sum_{i=1}^{r}\sum_{j=1}^{s} \phi_{ij}(\alpha_i\beta_j) = 0$$

olsun. Buna göre

$$\sum_{i=1}^{r}\left(\sum_{j=1}^{s} \phi_{ij}\beta_j\right)\alpha_i = 0$$

yazabiliriz. $\{\alpha_i\}_{i=1}^{r}$ kümesi K'nın bir E–bazı olduğundan her $i = 1, \ldots, r$ için

$$\sum_{j=1}^{s} \phi_{ij}\beta_j = 0$$

elde ederiz. Fakat $\{\beta_j\}_{j=1}^{s}$ kümesi de E'nin bir F–bazı olduğundan yukarıdakine benzer şekilde her $i = 1, \ldots, r$ ve her $j = 1, \ldots, s$ için $\phi_{ij} = 0$ elde ederiz. Bu da kanıtı tamamlar. □

Tanım 1.4. E/F bir cisim genişlemesi olsun. Eğer E'nin her elemanı F üzerinde cebirsel ise E'ye F'nin bir cebirsel genişlemesi (veya kısaca E, F üzerinde cebirseldir) denir. Eğer E, F üzerinde cebirsel ise E/F genişlemesine bir cebirsel genişleme adı verilir.

Alıştırma 1.5. E/F bir cisim genişlemesi ve $u_1, \ldots, u_n \in E$ elemanları F üzerinde cebirsel olsun. Buna göre gösteriniz ki
(i) $[F(u_1, \ldots, u_n) : F] < \infty$ ve
(ii) $F(u_1, \ldots, u_n) = F[u_1, \ldots, u_n]$ dir.

Önerme 1.6. *Her sonlu boyutlu cisim genişlemesi cebirseldir. Özel olarak eğer sonlu boyutlu bir E/F cisim genişlemesi için $[E : F] = n < \infty$ ise o zaman E'nin her elemanı F üzerinde derecesi en çok n olan bir cebirsel elemandır.*

Kanıt. Kabul edelim ki $[E : F] = n$ olsun. $u \in E$ alalım. Buna göre $[F(u) : F] \leq [E : F]$ olacağından kanıt tamamlanır. □

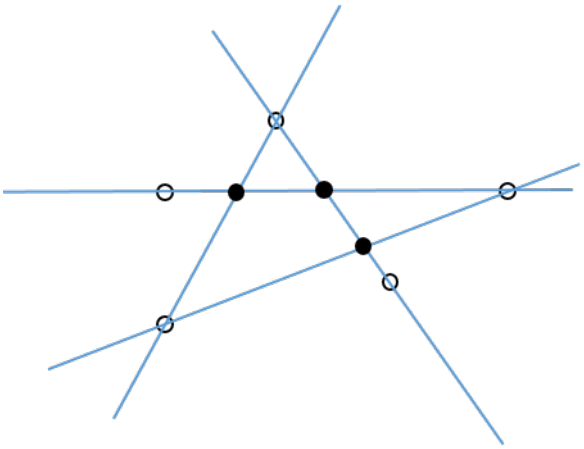
1.3. Geometrik Çizimler

Düzlemde noktaların sonlu bir $\mathcal{S} = \{P_1, P_2, \ldots, P_n\}$ kümesi verildiğinde tümevarım ile her m pozitif tamsayısı için $\mathcal{S}_m$ kümelerini şu şekilde inşa edelim: $\mathcal{S}_1 = \mathcal{S}$ ve $\mathcal{S}_{r+1}$ kümesi $\mathcal{S}_r$ ile aşağıdaki maddelerde tanımlanan kümelerin birleşimidir:

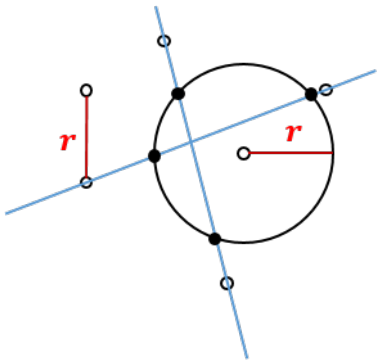
(1) $\mathcal{S}_r$'deki noktaları birleştiren doğru çiftlerinin kesişim noktalarının kümesi,

(2) $\mathcal{S}_r$'deki noktaları birleştiren doğrular ile merkezi $\mathcal{S}_r$'deki noktalar ve yarıçapı $\mathcal{S}_r$'deki iki noktayı birleştiren bir doğru parçası kadar olan çemberlerin kesişim noktalarının kümesi,

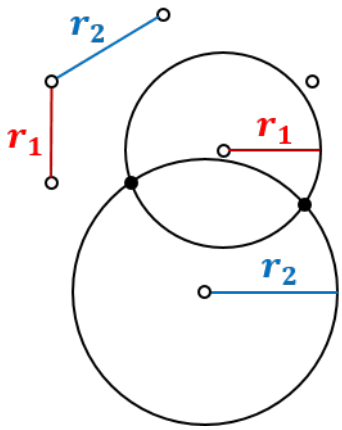
(3) Madde (2)'deki gibi tarif edilen çember çiftlerinin kesişim noktalarının kümesi. Örneğin, aşağıdaki şekillerde içi boş noktalar $\mathcal{S}_1$ kümesinde ise içi dolu olanlar $\mathcal{S}_2$'dedir.



Şekil 1.3.1. $\mathcal{S}_1$'deki noktaları birleştiren doğru çiftlerinin kesişim noktaları $\mathcal{S}_2$ kümesinin elemanlarıdır.



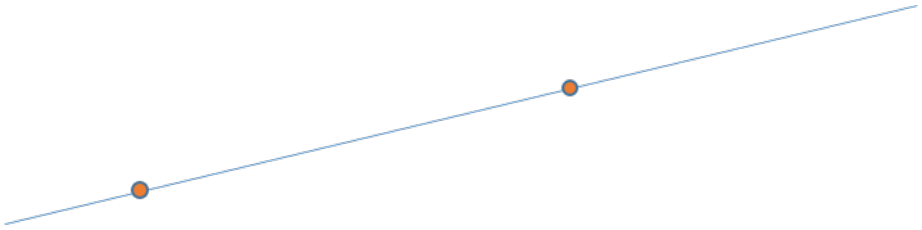
Şekil 1.3.2. $\mathcal{S}_1$'deki noktaları birleştiren doğrular ile merkezi $\mathcal{S}_1$'deki noktalar ve yarıçapı $\mathcal{S}_1$'deki iki noktayı birleştiren bir doğru parçası kadar olan çemberlerin kesişim noktaları $\mathcal{S}_2$'nin elemanlarıdır.



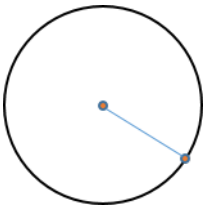
Şekil 1.3.3. Merkezi $\mathcal{S}_1$'deki noktalar ve yarıçapı $\mathcal{S}_1$'deki iki noktayı birleştiren bir doğru parçası kadar olan çember çiftlerinin kesişim noktaları $\mathcal{S}_2$'dedir.

$\mathscr{C}(P_1, P_2, \ldots, P_n) = \bigcup_{i=1}^{\infty} \mathcal{S}_i$ olsun. Buna göre $\mathscr{C}(P_1, P_2, \ldots, P_n)$'deki noktaları birleştiren doğruların kesim noktaları; $\mathscr{C}(P_1, P_2, \ldots, P_n)$'deki herhangi iki noktayı birleştiren bir doğru ile merkezi $\mathscr{C}(P_1, P_2, \ldots, P_n)$'de bir nokta, yarıçapı ise $\mathscr{C}(P_1, P_2, \ldots, P_n)$'deki iki noktayı birleştiren bir doğru parçasının uzunluğu kadar olan bir çemberin kesişim noktası ya da noktaları; merkezi $\mathscr{C}(P_1, P_2, \ldots, P_n)$'de bir nokta, yarıçapı ise $\mathscr{C}(P_1, P_2, \ldots, P_n)$'deki iki noktayı birleştiren bir doğru parçasının uzunluğu kadar olan iki çemberin kesişim noktası ya da noktaları tümüyle $\mathscr{C}(P_1, P_2, \ldots, P_n)$ kümesinin içine düşer. Eğer düzlemdeki bir P noktası için $P \in \mathscr{C}(P_1, P_2, \ldots, P_n)$ ise o zaman "P noktası cetvel–pergel yardımı ile $P_1, P_2, \ldots, P_n$ noktalarından elde edilebilir" diyeceğiz. Aksi halde P noktası P_i noktalarından elde edilemez.

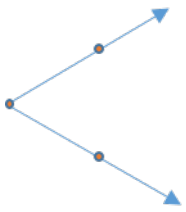
Öklid geometrisinin elemanları noktalar, doğrular, çemberler ve açılardır. Bu elemanlardan doğrular, çemberler ve açılar üzerlerinden seçilen bazı noktalar ile tam olarak belirlidir (bkz. Şekil 1.3.4, 1.3.5, 1.3.6). Dolayısıyla bu noktaların çizilebilir (yani $P_1, P_2, \ldots, P_n$ noktalarından elde edilebilir) olması doğru, çember ve açı gibi elemanların da çizilebilir olmasını gerektirir.



Şekil 1.3.4. Bir doğru, üzerindeki iki nokta ile belirlidir.



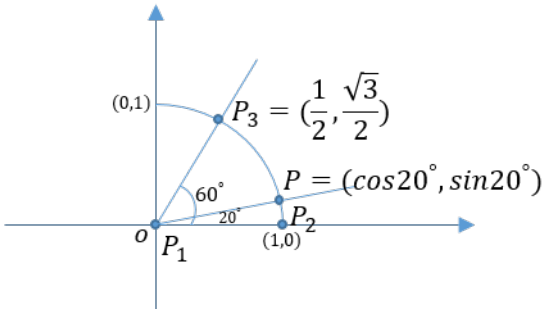
Şekil 1.3.5. Bir çember, merkezi ve üzerindeki bir nokta ile belirlidir.



Şekil 1.3.6. Bir açı, köşesi ve kolları üzerinde köşeye eşit uzaklıktaki iki nokta ile belirlidir.

Dikkat edilirse yukarıda tanımladığımız $\mathcal{S}_2, \mathcal{S}_3, \ldots$ kümelerindeki tüm noktalar, $\mathcal{S}_1$ kümesinden, yalnız cetvel ve pergel kullanılarak elde edilebilir. Aslında $\mathcal{S}_1 = \{P_1, \ldots, P_n\}$

kümesinden yalnız cetvel ve pergel kullanılarak elde edilebilen tüm noktaların kümesi $\mathscr{C}(P_1, P_2, \ldots, P_n)$ kümesidir.

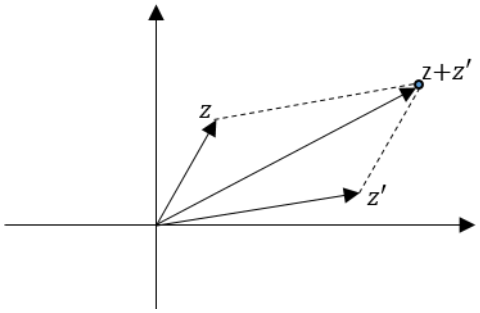


Şekil 1.3.7. 60°lik bir açının üçe bölünmesi problemi, $P = (\cos 20°, \sin 20°)$ noktasının $\mathscr{C}(P_1, P_2, P_3)$ kümesine ait olup olmadığının belirlenmesi problemidir.

Şimdi geometrik çizimler ile ilgili problemleri cebirsel olarak nasıl ele alabileceğimizi inceleyelim. $n \geq 2$ olarak kabul edeceğiz çünkü aksi halde $\mathscr{C}(P_1, P_2, \ldots, P_n) = \{P_1\}$ olur. Cartesian koordinat sistemimizi $P_1 = (0, 0)$ ve $P_2 = (1, 0)$ olacak şekilde seçeceğiz. $P = (x, y)$ şeklindeki bir nokta ile $x + iy$ karmaşık sayısını eşleştireceğiz. Buna göre $\{P_1, P_2, \ldots, P_n\}$ kümesi $z_1 = 0$ ve $z_2 = 1$ olmak üzere $\{z_1, z_2, \ldots, z_n\}$ karmaşık sayı kümesi olarak tanımlanmaktadır. Şimdi karmaşık sayıların $\mathscr{C}(z_1, z_2, \ldots, z_n)$ kümesinin neye benzediğini belirleyeceğiz. $\mathscr{C}(z_1, z_2, \ldots, z_n)$ kümesine $z_1, z_2, \ldots, z_n$ sayılarından (cetvel ve pergel ile) elde edilen karmaşık sayıların kümesi diyeceğiz.

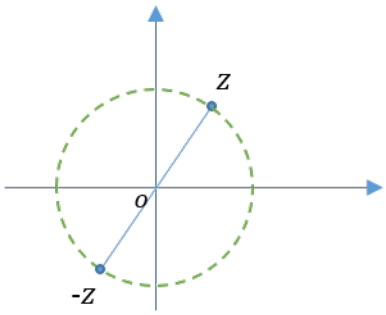
Teorem 1.7. *$\mathscr{C}(z_1, z_2, \ldots, z_n)$, karmaşık sayılar cisminin $z_1, z_2, \ldots, z_n$ sayılarını içeren ve karekök alma ile eşleniğe göre kapalı olan en küçük alt cismidir.*

Kanıt. Önce $\mathscr{C}(z_1, z_2, \ldots, z_n)$ kümesinin $\mathbb{C}$'nin bir alt cismi olduğunu ve karekök alma ile eşlenik işlemlerine göre kapalı olduğunu gösterelim. $z, z' \in \mathscr{C}(z_1, z_2, \ldots, z_n)$ olsun. $z + z'$ sayısı bilinen paralelkenar metoduna göre çizilebilir.



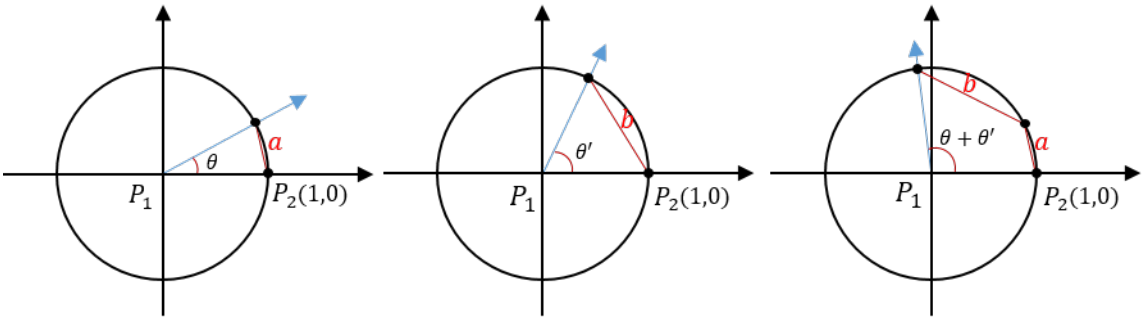
Şekil 1.3.8.

Böylece $z + z'$, merkezi z ve yarıçapı $|z'|$ olan çember ile merkezi z' ve yarıçapı $|z|$ olan çemberin kesişim noktasıdır. Bu da $z + z' \in \mathscr{C}(z_1, z_2, \ldots, z_n)$ olması demektir. Ayrıca orijin merkezli ve $|z|$ yarıçaplı çember ile $0z$ doğrusunun kesişimi $-z$ olduğundan $-z \in \mathscr{C}(z_1, z_2, \ldots, z_n)$ olur.



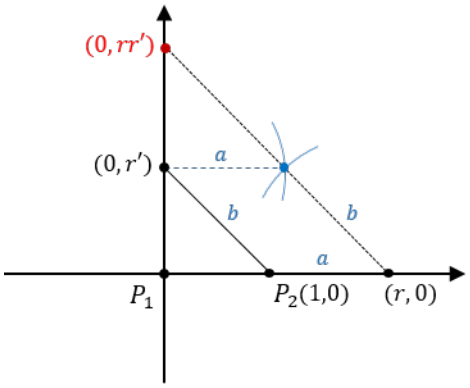
Şekil 1.3.9.

Şimdi $\mathscr{C}(z_1, z_2, \ldots, z_n)$ kümesinin çarpma işlemine ve çarpımsal ters ile kare kök alma işlemlerine göre kapalı olduğunu gösterelim. Bunun için karmaşık sayıların kutupsal gösterimlerini kullanacağız. Bir z karmaşık sayısı, θ, pozitif x–ekseni ile $0z$ vektörü arasında kalan yönlü açı ve $r = (x^2 + y^2)^{1/2}$ olmak üzere, $re^{i\theta}$ şeklinde yazılabilir. Bir karmaşık sayının bu biçimdeki gösterimine kutupsal gösterimi denir. $z = re^{i\theta}$ve $z' = r'e^{i\theta'}$olsun. Buna göre $zz' = rr'e^{i(\theta+\theta')}$ olur. Pozitif x–ekseni ile $\theta + \theta'$ kadar açı yapan bir ışını cetvel–pergel yardımıyla çizebiliriz (bkz. Şekil 1.3.10).



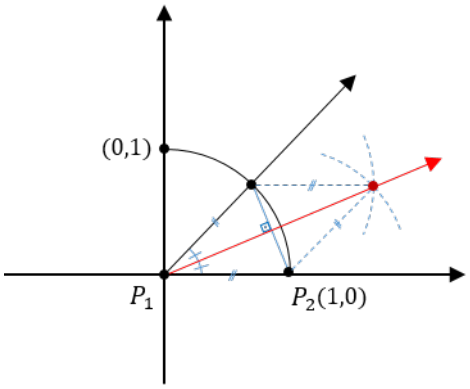
Şekil 1.3.10.

Dikkat edilirse iki açının farkı kadar ölçüye sahip bir açıyı da benzer yolla çizebiliriz. Öte yandan uzunluğu rr' olan bir doğru parçası da cetvel–pergel yardımıyla çizilebilir (bkz. Şekil 1.3.11).



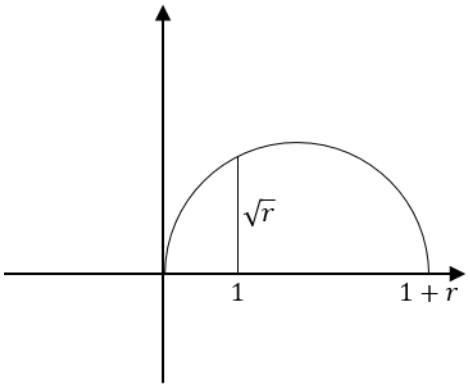
Şekil 1.3.11.

Yukarıdaki şekilde y–ekseni üzerindeki noktalar yukarıdan aşağı $(0, r)$ ve $(0, r')$ alınırsa x–ekseni üzerinde $(\frac{r}{r'}, 0)$ noktası elde edilir. Dolayısıyla zz' çarpımı ile $z' \neq 0$ iken $z(z')^{-1}$ çarpımı çizilebilirdir. Diğer taraftan bir açıyı yalnız cetvel ve pergel kullanarak ikiye bölmek çok zor değildir (bkz. Şekil 1.3.12).



Şekil 1.3.12.

Aşağıdaki şekil ise bir r sayısı için $\sqrt{r}$'nin nasıl çizilebileceğini açıklamaktadır.



Şekil 1.3.13.

Buna göre $z \in \mathscr{C}(z_1, z_2, \ldots, z_n)$ ise $z^{1/2} \in \mathscr{C}(z_1, z_2, \ldots, z_n)$ dir. Ayrıca $\bar{z}$ sayısını z'den x–eksenine dikme indirip orijin merkezli $|z|$ yarıçaplı çember ile kesiştirerek elde edebileceğimizden $z \in \mathscr{C}(z_1, z_2, \ldots, z_n)$ ise $\bar{z} \in \mathscr{C}(z_1, z_2, \ldots, z_n)$ olur. Böylece $\mathscr{C}(z_1, z_2, \ldots, z_n)$, $\mathbb{C}$'nin karekök ve eşlenik alma işlemlerine göre kapalı bir alt cismidir.

Şimdi $\mathscr{C}'$, $\mathbb{C}$'nin $z_1, \ldots, z_n$'i içeren ve karekök ile eşlenik alma işlemlerine göre kapalıbir alt cismi olsun. $\mathscr{C}(z_1, z_2, \ldots, z_n) \subseteq \mathscr{C}'$ olduğunu göstereceğiz. $\mathscr{C}(z_1, z_2, \ldots, z_n)$'in tanımlanma şeklinden dolayı

1. $\mathscr{C}'$ deki noktaları birleştiren doğru çiftlerinin kesişim noktalarının $\mathscr{C}'$ de olduğunu,
2. $\mathscr{C}'$ deki noktaları birleştiren doğrular ile merkezi $\mathscr{C}'$ deki noktalar ve yarıçapı $\mathscr{C}'$ deki iki noktayı birleştiren bir doğru parçası kadar olan çemberlerin kesişim noktalarının $\mathscr{C}'$ de olduğunu ve
3. merkezi $\mathscr{C}'$ deki noktalar ve yarıçapı $\mathscr{C}'$ deki iki noktayı birleştiren bir doğru parçası kadar olan çember çiftlerinin kesişim noktalarının $\mathscr{C}'$ de olduğunu

göstermek yeterlidir.

$\mathscr{C}'$ eşlenik alma işlemine göre kapalı ve $i = \sqrt{-1} \in \mathscr{C}'$ olduğundan her $x + iy \in \mathscr{C}'$ için $x, y \in \mathscr{C}'$ olur. Buna göre $\mathscr{C}'$ deki farklı iki noktayı birleştiren bir doğru, $\mathscr{C}'$ içindeki a, b, c reel sayıları için $ax + by + c = 0$ tipinde; merkezi $\mathscr{C}'$ deki bir nokta ve yarıçapı $\mathscr{C}'$ deki iki noktayı birleştiren bir doğru parçası kadar olan bir çember $\mathscr{C}'$ içindeki d, e, f reel sayıları için $x^2 + y^2 + dx + ey + f = 0$ tipindedir. $ax + by + c = 0$ ve $a'x + b'y + c' = 0$ tipindeki paralel olmayan iki doğrunun kesişim noktası Crammer yöntemi ile bu denklemleri ortak çözerek, yani a, b, c, a', b', c' reel sayılarının içinde bulunduğu bazı determinantları hesaplayarak elde edilebilir. Bu da kesişim noktasının a, b, c, a', b', c' sayılarından sadece cebirsel işlemler (toplama, çıkarma, çarpma, bölme) kullanılarak elde edilebileceği anlamına gelmektedir. Dolayısıyla koordinatları $\mathscr{C}'$ de olan noktaları birleştiren doğruların kesişim noktalarının da koordinatları $\mathscr{C}'$ de olur. $y = mx + b$ $(m \neq 0)$ doğrusu ile $x^2 + y^2 + dx + ey + f = 0$ çemberinin kesişim noktalarının apsisi $x^2 + (mx + b)^2 + dx + e(mx + b) + f = 0$ quadratik eşitliğini çözerek bulunabilir. Böyle bir quadratik eşitliğin çözümü yalnız cebirsel işlemler ile karekök alma işlemi kullanılarak yapılabildiğine göre eğer doğru ile çember kesişiyor ve m, b, d, e, f reel sayıları $\mathscr{C}'$ cisminde ise denklemin çözümleri de $\mathscr{C}'$ de bulunan reel sayılardır. $x = (y-b)/m$ olduğundan doğru ile çemberin kesişim noktasının koordinaları

$\mathscr{C}'$ cisminin elemanıdır. Ayrıca $x = a$ doğrusu ile $x^2 + y^2 + dx + ey + f = 0$ çemberinin kesişim noktaları için de aynı sonucu benzer şekilde elde edebiliriz. Diğer taraftan $\mathscr{C}'$ de bulunan d, e, f, d', e', f' reel sayıları için $x^2 + y^2 + dx + ey + f = 0$ ve $x^2 + y^2 + d'x + e'y + f' = 0$ çemberlerinin kesişim noktaları, $x^2 + y^2 + dx + ey + f = 0$ çemberi ile $(d - d')x + (e - e')y + f - f' = 0$ doğrusunun kesişim noktaları ile aynı olacağından yukarıdaki söylenenlerden dolayı bu çemberlerin kesişim noktaları da koordinatları $\mathscr{C}'$ cismine ait reel sayılar olacaktır. Böylece ispat tamamlanmış olur. □

NOT. $\mathscr{C}(z_1, z_2, \ldots, z_n)$ cismi, 1 ve i sayılarını içeren bir cisim olduğundan, $\mathbb{Q}(i) = \{p+iq : p, q \in \mathbb{Q}\}$ cismini kapsar. Dikkat edilirse $\mathbb{Q}(i)$, $\mathbb{C}$ içinde yoğundur; yani, $\mathbb{C}$'deki her dairesel komşuluk (dairesel bölge) $\mathbb{Q}(i)$'de bir nokta bulundurur.

$\mathscr{C}(z_1, z_2, \ldots, z_n)$'nin yukarıda verilen karakterizasyonundan faydalanarak aşağıdaki sonucu verebiliriz.

SONUÇ 1.8. $z_1, \ldots, z_n \in \mathbb{C}$ ve $F = \mathbb{Q}(z_1, \ldots, z_n, \bar{z}_1, \ldots, \bar{z}_n)$ olsun. Buna göre bir z karmaşık sayısı $z_1, \ldots, z_n$ sayılarından elde edilebilir ancak ve ancak
(1) $z \in F(u_1, \ldots, u_r)$,
(2) $u_1^2 \in F$ ve
(3) her $1 < i \leq r$ için $u_i^2 \in F(u_1, \ldots, u_{i-1})$
olacak şekilde $u_1, \ldots, u_r$ karmaşık sayıları vardır.

Yukarıdaki (2) ve (3) özelliğini sağlayan $F(u_1, \ldots, u_r)$ cismine F üzerinde bir *karekök kulesi* denir.

KANIT. $\mathscr{C}(z_1, \ldots, z_n)$, karekök ve eşlenik alma işlemlerine göre kapalı olduğundan, $\mathscr{C}(z_1, \ldots, z_n)$, F'yi ve F üzerindeki her karekök kulesini içerir. Dolayısıyla $\mathscr{C}'$, F üzerindeki karekök kulelerinin bileşimi ise $\mathscr{C}(z_1, \ldots, z_n) \supseteq \mathscr{C}'$ olur. $z, z' \in \mathscr{C}'$ olsun. $z \in F(u_1, \ldots, u_r)$ ve $z' \in F(u'_1, \ldots, u'_s)$ olacak şekilde F üzerinde $F(u_1, \ldots, u_r)$ ve $F(u'_1, \ldots, u'_s)$ gibi karekök kuleleri vardır. Dikkat edilirse $F(u_1, \ldots, u_r, u'_1, \ldots, u'_s)$ de F üzerinde bir karekök kulesidir. $z + z', zz' \in F(u_1, \ldots, u_r, u'_1, \ldots, u'_s)$ ve $z \neq 0$ iken $z^{-1} \in F(u_1, \ldots, u_r, u'_1, \ldots, u'_s)$ olacağından $\mathscr{C}'$ kümesi $\mathbb{C}$'nin bir alt cismidir. Öte yandan $\mathscr{C}'$ karekök alma işlemine göre kapalıdır. Bunu görmek için $u^2 \in \mathscr{C}'$ alalım. Buna göre $u^2 \in F(u_1, \ldots, u_r)$ olacak şekilde F üzerinde bir $F(u_1, \ldots, u_r)$ karekök kulesi vardır. Fakat bu durumda $F(u_1, \ldots, u_r, u)$ da F üzerinde bir karekök kulesi olacağından $u \in \mathscr{C}'$ bulunur. Ayrıca $\bar{F} = F$ ve $\overline{F(u_1, \ldots, u_r)} = F(\bar{u}_1, \ldots, \bar{u}_r)$ olduğundan $\mathscr{C}'$, eşlenik alma işlemine göre de kapalıdır. Böylece $\mathscr{C}' \supseteq \mathscr{C}(z_1, \ldots, z_n)$ elde edilir. Dolayısıyla $\mathscr{C}' = \mathscr{C}(z_1, \ldots, z_n)$ olur. Bu ise kanıtı tamamlar. □

SONUÇ 1.9. $F = \mathbb{Q}(z_1, \ldots, z_n, \bar{z}_1, \ldots, \bar{z}_n)$ olsun. Buna göre $z_1, \ldots, z_n$sayılarından elde edilebilen her z karmaşık sayısı, $\mathbb{C}$'nin F üzerinde derecesi 2'nin bir kuvveti olan cebirsel bir elemanıdır.

KANIT. F üzerindeki her karekök kulesinin F üzerindeki boyutu 2'nin bir kuvveti kadardır. Eğer z F'nin böyle bir genişlemesi içine düşerse $[F(z) : F]$ boyutu da 2'nin bir kuvveti olur. Böylece kanıt tamamlanır. □

Bir çok çizilebilme probleminde yalnız iki adet nokta (ya da denk olarak bir doğru parçası) verilmektedir. Uygun bir koordinat sistemi seçerek bu noktaları 0 ve 1 alabiliriz. Buna göre $F = \mathbb{Q}$ bulunur. Bu durumda $\mathscr{C} \equiv \mathscr{C}(z_1, z_2)$ cismine *çizilebilir (karmaşık) sayılar cismi* adı verilir.

Şimdi daha önce bahsi geçen klasik geometrik çizim problemlerine; yani,

(*a*) bir açının üç eş parçaya bölünmesi;

(*b*) bir küpün iki katının inşası; yani, bir küpün hacminin iki katı hacme sahip bir küp elde edilmesi;

(*c*) bir düzgün yedigen çizilmesi;

(*d*) bir çemberin kareleştirilmesi; yani, alanı bir çemberinkine eşit olan bir kare çizilmesi.

problemlerine yanıt vereceğiz.

BIR AÇININ ÜÇ EŞ PARÇAYA BÖLÜNMESI. *Yalnız cetvel ve pergel kullanarak her açıyı üç eş parçaya ayıramayız. Örneğin* $60°$*'lik ölçüye sahip bir açı üç eş parçaya bölünemez. Daha önce söylediğimiz gibi* $60°$*'lik bir açıdan* $20°$*'lik bir açıyı çizebilmek için* $P_1 = (0,0)$*,* $P_2 = (1,0)$ *ve* $P_3 = (\cos 60°, \sin 60°) = (\frac{1}{2}, \frac{\sqrt{3}}{2})$ *noktalarından* $P = (\cos 20°, \sin 20°)$ *noktasını çizebilmek gerekir. Eğer* P *noktası* P_1*,* P_2 *ve* P_3 *noktalarından elde edilebilir ise o zaman* P*'den* x*–eksenine inilen dikmenin ayağı, yani* $Q = (\cos 20°, 0)$ *noktası da* P_1*,* P_2 *ve* P_3 *noktalarından elde edilebilir. Dolayısıyla,* $z_1 = 0$*,* $z_2 = 1$ *ve* $z_3 = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ *için* $F = \mathbb{Q}(z_1, z_2, z_3, \bar{z}_1, \bar{z}_2, \bar{z}_3) = \mathbb{Q}(\sqrt{-3})$ *yazarsak,* $60°$*'lik açının üçe bölünebilmesi halinde* $\cos 20°$*'nin* F *üzerinde cebirsel olması ve* $\cos 20°$*'nin* F *üzerindeki derecesinin* 2*'nin bir kuvveti olması gerekir. Fakat* F*,* $\mathbb{Q}$ *üzerinde cebirsel ve* $[F : \mathbb{Q}] = 2$ *olduğundan* $\cos 20°$*,* $\mathbb{Q}$ *üzerinde de cebirsel ve* $\mathbb{Q}$ *üzerindeki derecesi de* 2*'nin bir kuvveti olmalıdır. Şimdi* $a = \cos 20°$ *olsun.* $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ *olduğundan* $4a^2 - 3a = \frac{1}{2}$ *bulunur. Buna göre* a*,* $4x^3 - 3x - \frac{1}{2} = 0$ *eşitliğinin bir köküdür. Fakat* $4x^3 - 3x - \frac{1}{2}$ *polinomu* $\mathbb{Q}$ *üzerinde indirgenemezdir çünkü*

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

polinomunun hiç tamsayı kökü yoktur. Dolayısıyla a*'nın* $\mathbb{Q}$ *üzerindeki derecesi* 3 *olur. Bu durumda yukarıda söylenenlerden dolayı* $\cos 20°$ z_1*,* z_2 *ve* z_3*'den elde edilemez.*

BIR KÜPÜN IKI KATININ INŞASI. *Bir küpün iki katı hacime sahip bir küp her zaman inşa edilemez. Bunu göstermek için* $\sqrt[3]{2}$*'nin çizilebilir bir sayı olmadığını göstermek yeterlidir. Aslında* $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ *olduğundan, Sonuç 1.9'dan dolayı* $\sqrt[3]{2}$ *çizilebilir değildir.*

p ASAL SAYISI IÇIN DÜZGÜN p–GEN INŞA ETME. *Bu problem* $z = \cos(2\pi/p) + i\sin(2\pi/p)$ *sayısının çizilebilir olması ile ilgilidir.* $z^p = 1$ *ve* $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + 1)$ *olduğundan* z*,* $z^{p-1} + z^{p-2} + \cdots + 1 = 0$ *olur.* $x^{p-1} + x^{p-2} + \cdots + 1$ *polinomu* $\mathbb{Q}[X]$ *içinde indirgenemez olduğundan* $[\mathbb{Q}(z) : \mathbb{Q}] = p - 1$ *olur. Buna göre Sonuç 1.9'dan, cetvel–pergel yardımıyla düzgün* p*–gen çizilebilmesi için* $p - 1 = 2^s$ *olacak şekilde bir* s *pozitif tamsayısının bulunması gerekir. Dolayısıyla* $p = 2^s + 1$ *tipindeki* p *asal sayıları için düzgün* p*–gen çizilebilmektedir.* 6*,* 2*'nin bir kuvveti olmadığından cetvel–pergel yardımıyla düzgün yedigen çizilemeyeceği sonucu hemen elde edilebilir.* $p = 2^s + 1$ *asal sayı ise* s *sayısı da* 2*'nin bir kuvveti olmalıdır. Aksi halde* $s = mn$ *ve* m *bir tek sayı ise* $p = 2^s + 1 = (2^n)^m + 1 = (2^n + 1)(2^{n(m-1)} - 2^{n(m-1)} + \cdots + 1)$ *olacağından bu durum* p*'nin asal olması ile çelişir. Buna göre düzgün* p*–gen çizilebilmesi için* p *asal sayısının* $2^{2^t} + 1$ *tipinde olması gerekir. Bu tipten bir asal sayıya Fermat asal sayısı denir. Pierre Fermat* $2^{2^t} + 1$ *tipindeki herhangi bir tamsayının asal olacağını düşünmüştü;*

ancak bu düşüncesinin doğru olmadığı Euler tarafından $2^{32}+1 = 641 \times 6700417$ *olduğu gösterilerek çürütülmüştür. Bilinen Fermat asalları* $t = 0, 1, 2, 3, 4$ *alınarak elde edilen* $p = 3, 5, 17, 257, 65537$ *sayılarıdır. Henüz kanıtlanamamış olmakla beraber bu listenin tüm Fermat asallarının listesi olduğu düşünülmektedir.*

BIR ÇEMBERIN KARELEŞTIRILMESI. *Yarıçapı* 1 *br olan bir çemberin alanı* π *br*^{2} *dir. Alanı* π *br*^{2} *olan bir karenin kenar uzunluğu da* $\sqrt{\pi}$ *br olur. Dolayısıyla bir çemberin kareleştirilmesi* π *sayısının çizilebilir olmasına bağlıdır. Fakat 1882'de Lindemann tarafından gösterildiği gibi* π *sayısı* $\mathbb{Q}$ *üzerinde cebirsel değildir. Buna göre Sonuç 1.9'dan dolayı yalnız cetvel ve pergel yardımıla bir çemberin alanına sahip bir kare çizilemez.*

1.4. Parçalanış Cisimleri

Bir F cismi üzerinde $p(X)$ polinomu verildiğinde, $p(X)$'in bütün köklerini içerecek şekilde F'nin bir E genişlemesinin bulunmasını istediğimiz durumlarla karşılaşırız. Eğer $\alpha \in E$ için $p(\alpha) = 0$ ise $X - \alpha \mid p(X)$ olduğunu biliyoruz. Buna göre $p(X)$ bir monik polinom ve $p(X)$'in bütün kökleri $\alpha_1, \ldots, \alpha_n \in E$ ise o zaman $E[X]$ içinde

$$p(X) = \prod_{i=1}^{n} (X - \alpha_i)$$

yazılabilir. Bu durumda "$p(X)$, E üzerinde tamamen çarpanlarına ayrılabilir" ya da kısaca "$p(X)$, E üzerinde parçalanabilir" denir. Eğer $\alpha \in E$, $p(X)$'in bir kökü ise $\prod_{i=1}^{n}(\alpha - \alpha_i) = p(\alpha) = 0$ olacağından uygun bir $i = 1, \ldots, n$ için $\alpha = \alpha_i$ olur. Öte yandan $p(X)$ polinomu $F(\alpha_1, \ldots, \alpha_n)$ cismi üzerinde de aynı biçimde çarpanlarına ayrılacaktır. Dolayısıyla E cismi yerine $F(\alpha_1, \ldots, \alpha_n)$ cismini düşünmek $p(X)$ polinomu üzerinde çalışırken gereksiz yere fazla eleman içeren bir cisim ile çalışmaktan daha iyi bir düşünce olacaktır.

TANIM 1.10. F bir cisim ve $p(X) \in F[X]$ bir monik polinom olsun. Kabul edelim ki E, F'nin bir genişlemesi olsun. Eğer

(i) $E[X]$ içinde $p(X) = (X-\alpha_1)\cdots(X-\alpha_n)$ yazılabiliyorsa, yani $p(X)$, E üzerinde parçalanabilir ise

ve

(ii) $E = F(\alpha_1 \ldots, \alpha_n)$ ise, yani E, F üzerinde $p(X)$'in tüm kökleri tarafından üretiliyorsa

o zaman E'ye $p(X)$ polinomunun F üzerindeki bir *parçalanış cismi* denir.

TEOREM 1.11. *F bir cisim olsun. F üzerindeki sabit olmayan her monik polinomun bir parçalanış cismi vardır.*

KANIT. $p(X) \in F[X]$, derecesi $n \geq 1$ olan bir monik polinom olsun. Kabul edelim ki $p_1(X), \ldots, p_k(X)$, F üzerinde (birbirinden farklı olmak zorunda olmayan) monik indirgenemez polinomlar olmak üzere $p(X) = p_1(X) \ldots p_k(X)$ olsun. ($p(X)$'i bu biçimde yazabileceğimizi $F[X]$'in bir tek türlü çarpanlara ayırma bölgesi oluşundan dolayı biliyoruz.) $k \leq n$ olduğu açıktır. $n - k$ üzerinde tümevarım uygulayacağız. $n - k = 0$ ise her i için $p_i(X)$ doğrusaldır ve bu durumda F'nin kendisi $p(X)$'in bir parçalanış cismi olur. Dolayısıyla $n - k > 0$ iddia $n - k$'dan küçük tüm negatif olmayan tamsayılar için doğru olsun. Buna göre en az bir i için $p_i(X)$'in derecesi 1'den büyüktür. Genelliği bozmadan bu polinomu $p_1(X)$ olarak alabiliriz. $K = F[X]/(p_1(X))$ yazalım. Buna

göre K bir cisimdir. Öte yandan her $a \in F$ için a'yı $a + (p_1(X)) \in K$ ile özdeş tutarsak F'yi K içine gömebiliriz; yani K'yı F'nin bir genişlemesi olarak görebiliriz. Hatta $u = X + p_1(X) \in K$ denirse $p_1(u) = 0$ ve $K = F(u)$ elde edilir. Dolayısıyla K, F'nin $p_1(X)$'in bir kökü tarafından üretilen bir basit genişlemesidir. Ayrıca her $i = 1, \ldots, k$ için $p_i(X)$'i $K[X]$ içinde indirgenemez çarpanlarına ayırırsak, $p(X)$'i $K[X]$ içindeki indirgenemez polinomların çarpımı şeklinde yazmış oluruz. Bu çarpımda l tane indirgenemez polinom yer alırsa, $K[X]$ içinde $p_1(X) = (X-u)p_1'(X)$ şeklinde yazılabileceğinden, $l > k$ olmak zorundadır. Buna göre $n - l < n - k$ dır. Tümevarım hipotezimizden dolayı K'nın bir genişlemesi $E = K(u_1, \ldots, u_n)$ için $p(X) = \prod_{i=1}^{n}(X - u_i)$ yazılabilir. $p_1(u) = 0$ ve $p_1(X) \mid p(X)$ olduğundan $p(u) = 0$ve böylece uygun bir i için $u = u_i$ olur. Dolayısıyla $E = K(u_1, \ldots, u_n) = F(u)(u_1, \ldots, u_n) = F(u, u_1, \ldots, u_n) = F(u_1, \ldots, u_n)$ elde edilir. Böylece E, $p(X)$'in F üzerindeki bir parçalanış cismi olur. □

Örnek 1.12. F bir cisim ve $a, b \in F$ olsun. Eğer $p(X) = X^2 + aX + b$, F üzerinde indirgenemez ise o zaman $E = F[X]/(p(X))$, $p(X)$'in F üzerindeki bir parçalanış cismi olur. $u = X + (p(X))$ olsun. $E = F(u)$ yazabiliriz. $p(u) = 0$ olduğundan $E[X]$ içinde $p(X) = (X - u)(X - u')$ olacak şekilde $u' \in E$ vardır. Buna göre $E = F(u) = F(u, u')$ olacağından E, F üzerinde $p(X)$'in tüm kökleri tarafından üretilen genişlemesidir. Ayrıca $[E : F] = 2$ dir.

Örnek 1.13. $F = \mathbb{Z}/2\mathbb{Z}$ olsun. $p(X) = X^3 + X + 1$ alalım. $p(X)$'in derecesi 3 olduğundan ve F içinde hiç kökü bulunmadığından $p(X)$, F üzerinde indirgenemezdir. $E = F[X]/(p(X))$ ve $u = X + (p(X)) \in E$ olsun. Buna göre $E = F(u)$, $p(X)$'in F üzerinde bir parçalanış cismidir. Dikkat edilirse $X^3+X+1 = (X+u)(X^2+uX+u^2+1)$ yazılabilir. Ayrıca E içinde $(u^2)^2+u(u^2)+u^2+1 = 0$ olduğundan $u^2 \in E$, X^2+uX+u^2+1 polinomunun bir köküdür. Dolayısıyla X^2+uX+u^2+1 polinomu $E[X]$ içinde tamamen çarpanlarına ayrılabilir. Böylece $E = F(u)$, $p(X)$'in F üzerinde bir parçalanış cismi olur.

Örnek 1.14. $F = \mathbb{Q}$ ve $p(X) = (X^2 - 2)(X^2 - 3)$ olsun. Buna göre $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $p(X)$'in $\mathbb{Q}$ üzerinde bir parçalanış cismidir.

Örnek 1.15. $F = \mathbb{Q}$, p bir asal sayı ve $p(X) = X^p - 1$ olsun. $X^p - 1 = (X - 1)(X^{p-1}+X^{p-2}+\cdots+1)$ ve $X^{p-1}+X^{p-2}+\cdots+1$ polinomunun $\mathbb{Q}$ üzerinde indirgenemez olduğunu biliyoruz. Şimdi $z = X + (X^{p-1} + X^{p-2} + \cdots + 1) \in \mathbb{Q}[X]/(X^{p-1} + X^{p-2} + \cdots + 1)$ olmak üzere $E = \mathbb{Q}(z)$ olsun. $z \neq 1$, $z^p = 1$ ve $X^{p-1} + X^{p-2} + \cdots + 1$, z'nin $\mathbb{Q}$ üzerindeki minimal polinomu olduğundan $1, z, \ldots, z^{p-1}$ elemanları birbirinden farklıdır. Öte yandan $(z^k)^p = (z^p)^k = 1$ olduğundan $1, z, \ldots, z^{p-1}$ elemanlarının her biri $X^p - 1$ polinomunun köküdür; yani, $X^p - 1 = \prod_{i=0}^{p-1}(X - z^i)$ olur. Böylece $\mathbb{Q}(z)$, $X^p - 1$ polinomunun $\mathbb{Q}$ üzerinde bir parçalanış cismidir.

Not 1.16. F bir cisim olsun. F üzerindeki her parçalanış cismi F üzerinde sonlu boyutludur. $p(X) \in F[X]$ ve $p(X)$'in F üzerindeki bir parçalanış cismi E olsun. Buna göre her $i = 1, \ldots, n$ için $p(u_i) = 0$ ve $E = F(u_1, \ldots, u_n)$ olacak şekilde $u_1, \ldots, u_n \in E$ elemanları vardır. Dikkat edilirse bu u_i elamanlarının her biri F üzerinde cebirsel olduğundan $F(u_1, \ldots, u_{i-1})$ cismi üzerinde de cebirseldir. Buna göre her $1 < i \leq n$ için

$$[F(u_1, \ldots, u_i) : F(u_1, \ldots, u_{i-1})] < \infty.$$

Dolayısıyla

$$[E : F] = \prod_{i=1}^{n} [F(u_1, \ldots, u_i) : F(u_1, \ldots, u_{i-1})] < \infty$$

olur. (Burada $i = 1$ iken $F(u_1, \ldots, u_{i-1}) = F$ olarak alınmaktadır.)

F ve F' iki cisim olmak üzere $\sigma : F \longrightarrow F'$ bir cisim homomorfizması (ya da denk olarak cisim monomorfizması) olsun. Eğer $p(X) = a_0 + a_1X + \cdots + a_nX^n \in F[X]$ ise o zaman $\sigma(a_0) + \sigma(a_1)X + \cdots + \sigma(a_n)X^n \in F'$ polinomunu $\sigma p(X)$ şeklinde göstereceğiz. Dikkat edilirse $f, g \in F[X]$ ise $\sigma(fg) = (\sigma f)(\sigma g)$ olur. Öyleyse $\sigma p(X)$, F' üzerinde indirgenemez ise $p(X)$ de F üzerinde indirgenemezdir. Eğer, ek olarak, σ bir cisim izomorfizması ise $p(X)$'in F üzerinde indirgenemez olması ile $\sigma p(X)$'in F' üzerinde indirgenemez olması denktir. Ayrıca her $a \in F$ için $\sigma(p(a)) = \sigma p(\sigma(a))$ olur. Dolayısıyla, $a \in F$, $p(X)$'in bir kökü ise $\sigma(a) \in F'$, $\sigma p(X)$'in bir köküdür.

LEMMA 1.17. *F ve F' birer cisim, $\sigma : F \longrightarrow F'$ bir cisim izomorfizması ve E ve E' sırasıyla F ve F' cisimlerinin birer genişlemesi olsun. Kabul edelim ki $u \in E$, minimal polinomu $p(X) \in F[X]$ olan E'nin F üzerindeki bir cebirsel elemanı olsun. Buna göre σ, $F(u) \xrightarrow{\bar{\sigma}} E'$ şeklinde bir monomorfizmaya genişler ancak ve ancak $\sigma p(X)$'in E' içinde bir kökü vardır. σ'nın $F(u) \xrightarrow{\bar{\sigma}} E'$ şeklindeki genişlemelerinin sayısı $\sigma p(X)$ polinomunun E' içindeki köklerinin sayısı kadardır.*

KANIT. Eğer σ'nın $\bar{\sigma} : F(u) \longrightarrow E'$ şeklinde bir genişlemesi varsa o zaman $\sigma p(\bar{\sigma}(u)) = \bar{\sigma} p(\bar{\sigma}(u) = \bar{\sigma}(p(u)) = \bar{\sigma}(0) = 0$ olacağından $\sigma p(X)$'in E' içindeki bir kökü $\bar{\sigma}(u)$ olur. Tersine $v \in E'$, $\sigma p(X)$'in bir kökü olsun. $F[X] \to E'$, $f(X) \mapsto \sigma f(v)$ şeklinde tanımlanan dönüşüm bir halka homomorfimasıdır. Bu homomorfizmanın çekirdeği $p(X)$'i içerdiği için $F[X]/(p(X)) \to E'$, $f(X) + (p(X)) \mapsto \sigma f(v)$ şeklinde bir homomorfizma elde edilir. Öte yandan $F(u) \to F[X]/(p(X))$, $f(u) \mapsto f(x) + (p(X))$ dönüşümünün bir izomorfizma olduğunu biliyoruz. Buna göre

$$\bar{\sigma} : F(u) \longrightarrow F[X]/(p(X)) \longrightarrow E'$$

$$f(u) \longrightarrow \sigma f(v)$$

bileşkesi σ'nın $F(u)$'ya bir genişlemesidir. $F(u)$'nun elemanları F üzerindeki u'ya bağlı polinomlar tipinde ifade edilebildiğinden $\bar{\sigma}$ u'yu v'ye götüren σ'nın tek genişlemesidir. Ayrıca σ bir izomomorfizma olduğundan σf F' üzerinde indirgenemezdir ve buradan da σf, v'nin F' üzerindeki minimal polinomudur. Dolayısıyla σ'nın genişlemelerinin sayısı σf polinomunun E' içindeki köklerinin sayısı kadardır. □

TEOREM 1.18. *F ve F' birer cisim, $\sigma : F \longrightarrow F'$ bir cisim izomorfizması ve $p(X) \in F[X]$ sabit olmayan bir polinom olsun. E ve E' sırasıyla $p(X)$ ve $\sigma p(X)$ polinomlarının F ve F' üzerindeki parçalanış cisimleri olsun. O zaman σ, E'den E''ye tanımlı bir $\bar{\sigma}$ izomorfizmasına genişletilebilir. Ayrıca σ'nın bu şekildeki genişlemelerinin sayısı en fazla $[E : F]$ kadardır ve eğer $\sigma p(X)$'in tüm kökleri farklı (yani tek katlı) ise o zaman genişlemelerin sayısı $[E : F]$'ye eşittir.*

KANIT. E, F üzerinde bir parçalanış cismi olduğudan $[E : F] < \infty$ olduğunu biliyoruz. $[E : F]$ üzerinde tümevarım uygulayacağız. Eğer $[E : F] = 1$ ise $E = F$

dir ve $F[X]$ içinde $p(X) = \prod(X - a_i)$ biçiminde yazılabilir. Dolayısıyla $F'[X]$ içinde $\sigma p(X) = \sigma \prod(X - a_i) = \prod(X - \sigma(a_i))$ yazılabilir. Buna göre $\sigma(a_i)$'ler $\sigma p(X)$'in kökleridir ve E', F' üzerinde bu kökler tarafından üretildiğinden $E' = F'$ bulunur. Dolayısıyla σ'nın yalnız $1 = [E : F]$ adet genişlemesi vardır; o da kendisidir. Şimdi kabul edelim ki $[E : F] > 1$ ve iddia $[E : F]$'den küçük boyutlu genişlemeler için doğru olsun. Bu durumda $E \neq F$ olacağından $p(X)$, $F[X]$ içindeki doğrusal polinomların çarpımı olarak yazılamaz. Dolayısıyla $p(X)$'in derecesi 1'den büyük olan monik ve F üzerinde indirgenemez bir böleni vardır. Bu bölen $q(X)$ olsun. Bun göre $F'[X]$ içinde $\sigma q(X) \mid \sigma p(X)$ olur. $p(X)$'in köklerini $E[X]$ içinde $p(X) = \prod_{i=1}^{n}(X - u_i)$ ve $q(X) = \prod_{i=1}^{m}(X - u_i)$ olacak şekilde yazalım. Buna göre $E'[X]$ içinde $\sigma p(X) = \prod_{i=1}^{n}(X - v_i)$ ve $\sigma q(X) = \prod_{i=1}^{m}(X - v_i)$ yazabiliriz. $K = F(u_1)$ olsun. $q(X)$, monik, F üzerinde indirgenemez ve $q(u_1) = 0$ olduğundan $q(X)$, u_1'in F üzerindeki minimal polinomunudur. Böylece $[K : F] = m$ olur. k, birbirinden farklı olan $v_1, \ldots, v_m$ elemanlarının sayısı olsun. Yukarıdaki lemmadan dolayı K'dan E' içine k tane σ'nın genişlemesi $\tau_1, \ldots, \tau_k$ vardır. Eğer $v_1, \ldots, v_m$ elemanlarının her biri farklı ise o zaman K'dan E' içine σ'nın $k = m$ tane genişlemesi vardır. Tanımdan açıkça görülebilir ki E, $p(X)$ polinomunun K üzerinde de bir parçalanış cismi, E' ise $\sigma p(X)$ polinomunun $\tau_i(K)$ $(i = 1, \ldots, k)$ üzerinde bir parçalanış cismidir. $[E : K] = [E : F]/[K : F] = [E : F]/m < [E : F]$ olduğundan tümevarım hipotezimizden dolayı her $i = 1, \ldots, k$ için τ_i, E'den E' üzerine bir izomorfizmaya genişletilebilir ve bu genişlemelerin sayısı en fazla $[E : K]$ kadardır; üstelik eğer $\sigma p(X)$'in tüm kökleri farklı ise genişlemelerin sayısı $[E : K]$'ya eşittir. Bu genişlemelerin herhangi biri aynı zamanda σ'nın da bir genişlemesidir. Özel olarak σ'nın $E \to E'$ şeklinde en az bir izomorfizmaya genişletilebileceğini söyleyebiliriz. Yani $E \cong E'$ olur. Öte yandan σ'nın E'den E' üzerine herhangi bir izomorfizma genişlemesinin K'ya kısıtlanışı σ'nın K'dan E' içine bir monomorfizma genişlemesidir ve dolayısıyla da τ_i'lerden birine eşittir. Böylece σ'nın E'den E' üzerine izomorfizma genişlemelerinin sayısı en fazla $m[E : K] = [E : F]$ kadardır ve eğer $\sigma p(X)$'in tüm kökleri farklı ise bu genişlemelerin sayısı $[E : F]$'ye eşittir. □

Yukarıdaki teoremde $F = F'$ ve σ da birim dönüşüm alınırsa $p(X)$'in F üzerindeki herhangi iki parçalanış cisminin izomorf olması gerektiği sonucunu elde edebiliriz. Aslında bu parçalanış cisimleri arasında F'ye kısıtlanışı birim olan bir izomorfizma bulunabilir. Böyle bir izomorfizmaya E'den E' üzerine F'yi sabit bırakan izomorfizma denir. Yukarıdaki teoremi $F = F'$ alarak uygularsak E üzerindeki F'yi sabit bırakan otomorfizmaların (ya da E'nin F üzerindeki otomorfizmalarının) sayısı en fazla $[E : F]$ kadardır ve eğer $p(X)$'in tüm kökleri farklı ise otomorfizmaların sayısı $[E : F]$'ye eşittir.

1.5. Katlı Kökler

$f(X) \in F[X]$ sabit olmayan bir monik polinom olsun. E, $f(X)$'in F üzerinde bir parçalanış cismi olsun. $E[X]$ içinde

$$f(X) = (X - u_1)^{k_1} \ldots (X - u_s)^{k_s}$$

yazalım. Kabul edelim ki $i \neq j$ ise $u_i \neq u_j$ olsun. Buradaki k_i pozitif tam sayısına u_i kökünün katı denir. Eğer $k_i = 1$ ise u_i'ye $f(X)$'in bir *basit kökü;* aksi halde ise *katlı kökü* denir. Eğer E', f'nin F üzerindeki başka bir parçalanış cismi ise o zaman F'yi sabit bırakan uygun bir izomorfizma altında u_i'ler ile eşleşen $u_i' \in E'$ elemanları için

$E'[X]$ içinde $f(X) = \prod(X - u_i')^{k_i}$ yazılabilir. Dolayısıyla k_i katları f'nin F üzerindeki parçalanış cisminin seçiminden bağımsızdır. Özel olarak bir kökün basit olması da bu seçimden bağımsızdır. Teorem 1.18'den dolayı tüm kökleri basit olan bir polinom ile çalışmak ayrı bir kolaylık sağlamaktadır. Çünkü böyle bir durumda E'nin F üzerindeki otomorfizmalarının sayısı $[E : F]$'ye eşittir.

Bu bölümde F'nin karakteristiği sıfırsa ya da F sonlu ise polinomun tüm köklerinin basit olduğunu varsaymanın genelliği bozmayacağını göstereceğiz. E, F'nin bir genişlemesi ve $p_1(X), \ldots, p_t(X)$, F üzerinde birbirinden farklı indirgenemez polinomlar olmak üzere $f(X) = p_1(X)^{l_1} \ldots p_t(X)^{l_t}$ ise, tanımdan kolayca görülebileceği gibi, E $f(X)$'in F üzerinde bir parçalanış cismidir ancak ve ancak E $f_0(X) = p_1(X) \ldots p_t(X)$ polinomunun F üzerinde bir parçalanış cismidir. Dolayısıyla $f(X)$'i F üzerinde indirgenemez olan birbirinden farklı polinomların çarpımı şeklinde kabul edebiliriz. Eğer $p(X)$ ve $q(X)$, F üzerinde iki farklı indirgenemez polinom ise $a(X)p(X) + b(X)q(X) = 1$ olacak şekilde $a, b \in F[X]$ vardır. Buna göre $p(X)$ ve $q(X)$ polinomlarının E içinde ortak bir kökünün olması mümkün değildir. Dolayısıyla $f(X)$ birbirinden farklı indirgenemez polinomların çarpımı ise $f(X)$'in tüm köklerinin basit olduğunu söylemek ile $f(X)$'in tüm indirgenemez çarpanları için aynı şeyi söylemek denktir.

Şimdi bir polinomun köklerinin basit olması ile ilgili kullanışlı bir kriter vereceğiz. Fakat bunun için türev adını verdiğimiz bir kavrama ihtiyacımız var. $F[X]$ halkasına h gibi bir değişken daha ekleyerek X ve h değişkenlerine bağlı $F[X, h]$ polinom halkasını yazalım. $F[X, h] = F[X][h]$ ve h, $F[X]$ üzerinde transandant olduğundan $F[X, h]$ içindeki her eleman, $f_i(X)$'ler $F[X]$ in elemanı olmak üzere, $f_0(X)+f_1(X)h+\cdots+f_n(X)h^n$ şeklinde tek türlü yazılabilir. Özel olarak $f(X) \in F[X]$ ise $f(X+h) = f_0(X)+f_1(X)h+\cdots+f_n(X)h^n$ şeklinde yazabiliriz. $h = 0$ alınırsa (yani $F[X, h] \to F[X]$, F'ye kısıtlanışı birim ve $X \mapsto X$, $h \mapsto 0$ olan değer homomorfizması uygulanırsa) $f(X) = f_0(X)$ elde edilir. Buna göre $h \mid f(X + h) - f(X)$ dir. $f(X + h) - f(X)$ polinomu h polinomuna bölersek $f_1(X) + f_2(X)h + \cdots + f_n(X)h^{n-1}$ buluruz. Buradan $h = 0$ alınırsa $f_1(X)$ elde edilir. İşte bu $f_1(X)$ polinomuna $f(X)$ polinomunun türevi denir ve $f_1(X) = f'(X)$ şeklinde yazılır. Buna göre tanımdan dolayı

$$(*) \qquad f(X + h) \equiv f(X) + f'(X)h \pmod{h^2}$$

olur. Ayrıca $f(X + h) \equiv f(X) + g(X)h \pmod{h^2}$ olacak şekilde bir $g(X) \in F[X]$ varsa o zaman $f'(X)h \equiv g(X)h \pmod{h^2}$ ve buradan da $f'(X) \equiv g(X) \pmod{h^2}$ yani $f'(X) = g(X)$ elde edilir. Dolayısıyla $f'(X)$ polinomu $(*)$ denkliği ile tek türlü belirlidir. Türevin bu karakterizasyonu aşağıdaki temel özellikleri elde etmemizi kolaylaştırır:

(1) $(f + g)' = f' + g'$,
(2) her $a \in F$ için $(af)' = af'$,
(3) $(fg)' = f'g + fg'$,
(4) $X' = 1$.

İlk iki özellik $(*)$ denkilğinden dolayı hemen elde edilir. Çarpım kuralı görmek için $(*)$ denkliğini $g(X + h)$ için yazılan denklik ile çarparız. Buna göre

$$\begin{aligned}(fg)(X + h) = f(X + h)g(X + h) &\equiv [f(X) + f'(X)h][g(X) + g'(X)h] \pmod{h^2} \\ &\equiv f(X)g(X) + [f'(X)g(X) \\ &\quad + f(X)g'(X)]h \pmod{h^2}\end{aligned}$$

bulunur. Dolayısıyla (3) özelliğini, $(*)$ denkliğini fg çarpımı için kullanarak elde edebiliriz. Ayrıca $X+h \equiv X+1\cdot h \pmod{h^2}$ olduğundan $X' = 1$ elde edilir. Bununla birlikte çarpım kuralı kullanılarak her $k > 0$ için $(X^k)' = kX^{k-1}$ yazabiliriz. Ek olarak $1^2 = 1$ olduğundan çarpım kuralı sayesinde $1'\cdot 1 + 1\cdot 1' = 1'$, buradan da $2(1') = 1'$ yani $1' = 0$ bulunur. Türevin doğrusallık özelliğinden (yukarıdaki (1) ve (2) özellikleri) herhangi bir $f(X) = a_0 + a_1X + \cdots + a_nX^n$ polinomu için Analiz derslerinde gördüğümüz

$$f'(X) = a_1 + 2a_2X + \cdots + na_nX^{n-1}$$

eşitliği elde edilir.

Teorem 1.19. *$f(X) \in F[X]$ sabit olmayan bir monik polinom olsun. Kabul edelim ki E, $f(X)$'in F üzerindeki herhangi bir parçalanış cismi olsun. O zaman $f(X)$'in E içindeki tüm kökleri basittir ancak ve ancak $f(X)$ ve $f'(X)$ polinomları aralarında asaldır.*

Kanıt. $F[X]$ içinde $(f(X), f'(X)) = d(X)$ olsun. Kabul edelim ki $f(X)$, E içinde u gibi bir çok katlı köke sahip olsun. Buna göre uygun bir $k > 1$ tamsayısı için $f(X) = (X-u)^k g(X)$ yazabiliriz. Her iki tarafın türevi alınırsa $f'(X) = (X-u)^k g'(X) + k\cdot (X-u)^{k-1}g(X)$ elde edilir. Buna göre $X-u$ polinomu $E[X]$ içinde $f(X)$ ve $f'(X)$ polinomlarının bir ortak bölenidir. Dolayısıyla $d(X) \neq 1$ dir. Tersine f'nin tüm kökleri basit olsun. O zaman $f(X) = \prod_{i=1}^{n}(X-u_i)$ ve $i \neq j$ iken $u_i \neq u_j$ olacak şekilde $u_1, \ldots, u_n \in E$ vardır. Her $i = 1, \ldots, n$ için $X - u_i \nmid f'(X)$ olduğunu gösterirsek $(f(X), f'(X)) = 1$ elde edilir. Kabul edelim ki $X - u_i \mid f'(X)$ olsun. $f(X) = (X-u_i)g_i(X)$ olacak şekilde $g_i(X) \in E[X]$ olduğundan $f'(X) = g_i(X) + (X-u_i)g_i'(X)$ olur. Kabulümüzden dolayı $X - u_i \mid g_i(X)$ yani $(X-u_i)^2 \mid f(X)$ olur. Bu ise bir çelişkidir. Dolayısıyla istenilen elde edilir. □

Not. (***i***) F bir cisim ve $f(X) \in F[X]$ olsun. Eğer $f(X)$, F üzerinde indirgenemez olduğu halde $(f, f') \neq 1$ ise $f \mid f'$ olur. Fakat $\deg(f') < \deg(f)$ olduğundan bu durum $f' = 0$ olmasını gerektirir. Yani bir indirgenemez polinomun (parçalanış cisminin içinde) katlı kökü varsa o zaman bu polinomun türevi sıfır olmalıdır. Eğer $\operatorname{kar} F = 0$ ise hiçbir indirgenemez polinomun türevi sıfır olamaz. Dolayısıyla karakteristiği sıfır olan bir halka üzerinde indirgenemez olan bir polinomun tüm kökleri tek katlıdır. Eğer $\operatorname{kar} F = p \neq 0$ ve $f(X) = a_0 + a_1X + \cdots + a_nX^n$ ise $f'(X) = \sum_{i=1}^{n} ia_iX^{i-1}$ olacağından $f'(X) = 0$ ancak ve ancak her $1 \leq i \leq n$ için $ia_i = 0$ olur. Böylece $f'(X) = 0$ olması ile

$$f(X) = b_0 + b_1X^p + b_2X^{2p} + \cdots + b_mX^{mp}$$

olacak şekilde $b_i \in F$ $(1 \leq i \leq n)$ olması denktir. Buna göre türevi sıfır olan bir $f(X)$ polinomu uygun bir $g(X) \in F[X]$ için $g(X^p)$ tipindedir.

(***ii***) F karakteristiği $p \neq 0$ olan bir cisim olsun. Çarpmanın değişmeli oluşundan dolayı her $a, b \in F$ için $(ab)^p = a^pb^p$ yazılabilir. Buna göre Binom Teoreminden

$$(a+b)^p = a^p + b^p + \sum_{i=1}^{p-1}\binom{p}{i}a^ib^{p-i}$$

yazılabilir. Her $1 \leq i \leq p-1$ için $\binom{p}{i} = p!/i!(p-i)! \in \mathbb{Z}$ ve p, (asal sayısı) bu rasyonel ifadede pay kısmında bulunduğu halde payda kısmında bulunmadığından her

$1 \leq i \leq p-1$ için

$$p \mid \binom{p}{i}$$

olur. Buradan $\sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} = 0$ ve böylece

$$(a+b)^p = a^p + b^p$$

elde edilir. Buna göre

$$\begin{array}{ccc} F & \longrightarrow & F \\ a & \longmapsto & a^p \end{array}$$

şeklinde tanımlanan dönüşüm bir endomorfizmadır. F bir cisim olduğundan bu endomorfizma özel olarak bir monomorfizmadır ve F^p şeklinde göstereceğimiz görüntüsü F'nin bir alt cismidir. Bu alt cisme F'nin p-yinci kuvveti adı verilir.

LEMMA 1.20. *F karakteristiği $p \neq 0$ olan bir cisim ve $a \in F$ ise $X^p - a$ polinomu ya F üzerinde indirgenemezdir ya da $X^p - a = (X-b)^p$ olacak şekilde $b \in F$ vardır.*

KANIT. Kabul edelim ki $X^p - a = g(X)h(X)$ olacak şekilde $g(X), h(X) \in F[X]$ monik polinomları vardır. $\text{der}(g) = k$ olsun. Buna göre $1 \leq k \leq p-1$ dir. E, $X^p - a$ polinomunun F üzerinde bir parçalanış cismi olsun. $b \in E$, $X^p - a$ polinomunun bir kökü olsun. Buna göre $b^p = a$ dır. Buradan $X^p - a = X^p - b^p = (X-b)^p = g(X)h(X)$ elde edilir. Dolayısıyla $g(X) = (X-b)^k$ bulunur. $k < p$ olduğundan $(k,p) = 1$ yani $uk + vp = 1$ olacak şekilde $u, v \in \mathbb{Z}$ vardır. Dolayısıyla $b = (b^k)^u (b^p)^v \in F$ elde edilir. Yani $F[X]$ içinde $X^p - a = (X-b)^p$ yazılabilir. □

ÖRNEK 1.21. p bir asal sayı ve t bir değişken olmak üzere $F = (\mathbb{Z}/(p))(t)$ olsun. Aslında F katsayıları $\mathbb{Z}/(p)$ cisminden gelen rasyonel polinomların cismi; ya da başka bir deyişle $(\mathbb{Z}/(p))[t]$ polinom halkasının kesirler cismidir. t bu cisim içinde hiçbir elemanın p–yinci kuvveti değildir. Aslında eğer $f(t) = \sum_{i=0}^{n} a_i t^i$ ve $g(t) = \sum_{j=1}^{m} b_j t^j \neq 0$ olmak üzere $t = (f(t)/g(t))^p$ ise $f(t)^p = a_0^p + a_1^p t^p + \cdots + a_n^p t^{np}$ ve $g(t) = b_0^p + b_1^p t^p + \cdots + b_m^p t^{mp}$ olacağından

$$(b_0^p + b_1^p t^p + \cdots + b_m^p t^{mp})t = a_0^p + a_1^p t^p + \cdots + a_n^p t^{np}$$

eşitliği elde edilir. $1, t, t^2, \ldots$ elemanları $\mathbb{Z}/(p)$ üzerinde doğrusal bağımsız olduğundan her i için $b_i = 0$ elde edilir ki bu durum $g(t) \neq 0$ olması ile çelişir. Buna göre yukarıdaki lemmadan dolayı $f(X) = X^p - t \in F[X]$ polinomu indirgenemezdir. Öte yadan eğer E, $f(X)$'in F üzerinde bir parçalanış cismi ise $f(X)$, $E[X]$ içinde bir polinomun p–yinci kuvvetidir. Dikkat edilirse $f'(X) = pX^{p-1} = 0$ olduğundan $f(X)$'in çok katlı kökü olduğu buradan da anlaşılabilir.

TANIM 1.22. F bir cisim ve $f(X) \in F[X]$ olsun. Eğer $f(X)$'in F üzerindeki her indirgenemez böleni farklı köklere sahip ise o zaman $f(X)$'ye F üzerinde *ayrılabilir polinom* denir.

Dikkat edilirse karakteristiği sıfır olan bir cisim üzerindeki her sabit olmayan polinom ayrılabilirdir. Ayrıca yukarıdaki örnek gösteriyor ki karakteristiği sıfırdan farklı olan bir cisim üzerinde ayrılabilir olmayan bir polinom bulmak mümkündür.

TANIM 1.23. F bir cisim olsun. Eğer F üzerindeki her polinom ayrılabilir ise F cismine bir *mükemmel cisim* denir.

Yukarıda elde edilenlerden dolayı karakteristiği sıfır olan her cisim mükemmeldir. Buna göre problemi sıfırdan farklı karakteristiğe sahip olan cisimler için ele almak daha ilgi çekicidir. Bu yönde aşağıdaki sonucu verebiliriz:

TEOREM 1.24. *F karakteristiği $p \neq 0$ olan bir cisim olsun. Buna göre F mükemmeldir ancak ve ancak $F = F^p$ dir.*

KANIT. Eğer $F^p \subsetneq F$ ise $a \in F \setminus F^p$ bulunabilir. Yukarıdaki lemmadan dolayı $X^p - a$ polinomu F üzerinde indirgenemezdir. Üstelik $(X^p - a)' = 0$ olduğundan $X^p - a$, F üzerinde ayrılabilir değildir. Dolayısıyla F mükemmel değildir. Şimdi kabul edelim ki $f(X) \in F[X]$, F üzerinde ayrılabilir olmayan bir indirgenemez polinom olsun. O zaman $(f, f') \neq 1$ dir. Dolayısıyla $f(X) = a_0 + a_1X^p + a_2X^{2p} + \cdots$ şeklinde yazılabilir. Buradaki a_i'lerden en az biri F'nin bir elemanının p–yinci kuvveti değildir. Aksi halde, eğer her i için $a_i = b_i^p$ olsaydı $F[X]$ içinde

$$f(X) = (b_o + b_1X + \cdots)^p$$

olurdu ki bu durum $f(X)$'in indirgenemez oluşu ile çelişir. Dolayısıyla $F \neq F^p$ dir. Yani F mükemmel değildir. □

SONUÇ 1.25. Her sonlu cisim mükemmeldir.

KANIT. F sonlu bir cisim ise F'nin karakteristiği bir asal sayıdır. Bu asal sayı p olsun. Buna göre her $a \in F$ için $a \mapsto a^p$ şeklinde tanımlanan monomorfizma bir izomorfizma olur. Böylece $F = F^p$ elde edilir. Yani F mükemmeldir. □

1.6. Galois Grupları ve Temel Teorem

E/F bir cisim genişlemesi olmak üzere E'nin F üzerindeki otomorfizmalarının kümesi bileşke işlemine göre bir gruptur. Bu grubu $\mathrm{Gal}(E/F)$ ile göstereceğiz.

ÖRNEK 1.26. F bir cisim ve $a \in F$ olsun. Kabul edelim ki $\mathrm{char}\, F \neq 2$ ve a, F'nin hiçbir elemanının karesi olmasın, yani $a \notin F^2$ olsun. $X^2 - a$ polinomunun F üzerindeki bir parçalanış cismi E olsun. O zaman $u^2 = a$ olacak biçimde $u \in E$ bulunabilir. Buna göre

$$X^2 - a = (X - u)(X + u)$$

olduğundan $E = F(u)$ yazılabilir. $\tau \in \mathrm{Gal}(E/F)$ olsun. τ, F'yi sabit bıraktığından, $X^2 - a$ polinomunun bir kökünü yine bu polinomun bir köküne götürmek zorundadır. Buna göre $\tau(u)$ ya u ya da $-u$ olmak zorundadır. Dikkat edilirse $E = F(u)$ olduğundan $\tau(u)$ değeri τ'yu tam olarak belirler. Eğer $\tau(u) = u$ ise $\tau = I_E$ olur. Böylece $\sigma : E \to E$, $\sigma(u) = -u$ şeklinde tanımlı F'yi sabit bırakan otomorfizma olmak üzere $\mathrm{Gal}(E/F) = \{I_E, \sigma\}$ bulunur.

ÖRNEK 1.27. $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ olsun. E, $\mathbb{Q}$ üzerinde $\sqrt{2}$ ve $\sqrt{3}$ tarafından üretildiğinden E'nin $\mathbb{Q}$ üzerindeki bir otomorfizması $\sqrt{2}$ ve $\sqrt{3}$'deki değerleri ile tam olarak belirlidir. Dikkat edilirse $\sqrt{2}$, $X^2 - 2 \in \mathbb{Q}[X]$ polinomunun bir kökü olduğundan, $\mathbb{Q}$'yu sabit bırakan her otomorfizma $\sqrt{2}$'yi ya $\sqrt{2}$'ye ya da $-\sqrt{2}$'ye götürür. $\sqrt{3}$ için de benzer

bir sonuç elde edilir. Buna göre her $a \in \mathbb{Q}$ için

$$\begin{array}{rccc} \tau_1: & E & \longrightarrow & E \\ & a & \longmapsto & a \\ & \sqrt{2} & \longmapsto & -\sqrt{2} \\ & \sqrt{3} & \longmapsto & \sqrt{3} \end{array} \qquad \begin{array}{rccc} \tau_2: & E & \longrightarrow & E \\ & a & \longmapsto & a \\ & \sqrt{2} & \longmapsto & \sqrt{2} \\ & \sqrt{3} & \longmapsto & -\sqrt{3} \end{array}$$

olmak üzere $\mathrm{Gal}(E/\mathbb{Q}) = \{I_E, \tau_1, \tau_2, \tau_1\tau_2\}$ bulunur.

Örnek 1.28. F karakteristiği p olan mükemmel olmayan bir cisim $a \in F \backslash F^p$ olsun. Buna göre Lemma 1.20'den dolayı $X^p - a$ polinomu F üzerinde indirgenemezdir. $X^p - a$ polinomunun F üzerindeki bir parçalanış cismi E olsun. Buna göre $u^p = a$ oacak biçimde bir $u \in E$ bulunabilir. Ayrıca $X^p - a = (X - u)^p$ olacağından $E = F(u)$ elde edilir. Dolayısıyla E'nin F üzerinde birimden başka bir otomorfizması yoktur. Yani $\mathrm{Gal}(E/F) = \{I_E\}$ dir.

Örnek 1.29. F bir cisim ve t, F üzerinde transandant olmak üzere $E = F(t)$ olsun. $f(t), g(t) \in F[t]$ ve $g(t) \neq 0$ olmak üzere

$$u = \frac{f(t)}{g(t)} \in E$$

alalım. Genelliği bozmadan $f(t)$ ve $g(t)$ polinomlarını aralarında asal; yani, $(f(t), g(t)) = 1$ olacak şekilde seçebiliriz. $\mathrm{der}\, u = \max\{\mathrm{der}\, f(t), \mathrm{der}\, g(t)\}$ olarak tanımlansın. Açıktır ki $\mathrm{der}\, u < 1$ ancak ve ancak $u \in F$ dir. Kabul edelim ki $u \notin E$; yani, $\mathrm{der}\, u \geq 1$ olsun. Öncelikle u'nun F üzerinde transandant olduğunu göstereceğiz. Bunun için aksini kabul edelim; yani,

$$u^n + c_{n-1}u^{n-1} + \cdots + c_1 u + c_0 = 0$$

olacak şekilde $n \in \mathbb{N}$, $c_0, \ldots, c_{n-1} \in F$ bulunsun. $g(t)u = f(t)$ olduğundan, yukarıdaki eşitliğin iki tarafını da $g(t)^n$ ile çarparsak

$$g(t)^n u^n + c_{n-1}g(t)[g(t)^{n-1}u^{n-1}] + \cdots + c_1 g(t)^{n-1}[g(t)u] + c_0 g(t)^n = 0,$$

ya da denk olarak

$$f(t)^n + c_{n-1}g(t)f(t)^{n-1} + \cdots + c_1 g(t)^{n-1}f(t) + c_0 g(t)^n = 0$$

bulunur. Buna göre son elde edilen eşitliğin ilk terimi sol kısımda yalnız bırakılırsa uygun bir $h(t) \in F[t]$ için

$$f(t)^n = g(t)h(t)$$

yazılabilir. Fakat $F[t]$ bir tek türlü çarpanlara ayırma bölgesi ve $(f(t), g(t)) = 1$ olduğundan bu durum imkansızdır. Dolayısıyla u, F üzerinde transandanttır. Buna göre u, F üzerinde bir değişken gibi davranır. Başka bir deyişle, $F[u]$ halkası F üzerinde tek değişkenli bir polinom halkasına izomorftur. $F[u]$ halkası üzerinde bir değişken X olmak üzere $F[u][X] = F[u, X]$ halkasını düşünelim. Bu halka F üzerinde iki değişkenli bir polinom halkası olarak görülebilir. $h = f(X) - ug(X) \in F[u, X]$ polinomunu ele alalım. bir indirgenemez polinom olur. Dolayısıyla h, $F[u]$ halkası üzerinde X değişkenine bağlı bir polinom olarak görüldüğü zaman da indirgenemez olur. Eğer $h = st$ olacak şekilde $s, t \in F[u][X]$ polinomları varsa aynı zamanda $h, s, t \in F[X][u]$ ve h, $F[X]$ halkası üzerinde u değişkenine bağlı bir polinom olarak görüldüğünde birinci dereceden bir polinom olacağından, s ya da t'den biri $F[X]$ üzerinde –u'ya bağlı bir polinom olarak–

sabit diğeri ise $F[X]$ üzerinde u'ya bağlı birinci dereceden bir polinom olmalıdır; yani s veya t den biri $F[X]$'in elemanı diğeri ise $f_1(X)+ug_1(X)$ formunda olmalıdır. Kabul edelim ki $s = s(X) \in F[X]$ ve $t = f_1(X) + ug_1(X)$ olsun. Buna göre

$$\begin{aligned} f(X) - ug(X) = st &= s(X)(f_1(X) + ug_1(X)) \\ &= s(X)f_1(X) + us(X)g_1(X) \end{aligned}$$

yazılabileceğinden $f(X) = s(X)f_1(X)$ ve $g(X) = -s(X)g_1(X)$ bulunur. Böylece $s(X) \mid (f(X), g(X)) = 1$ olacağından $s \in F$ elde edilir. Dolayısıyla h, $F[u]$ üzerinde X'e bağlı bir indirgenemez polinomdur. $F(u)$, $F[u]$ halkasının kesirler cismi olduğundan h, $F(u)$ üzerinde de indirgenemezdir. Öte yandan $h(t) = f(t) - ug(t) = 0$ olduğundan uygun bir $v \in F(u)$ için $vh(X)$, t'nin $F(u)$ üzerindeki minimal polinomu olur. Buna göre $[F(t) : F(u)] = 1$ ancak ve ancak $\operatorname{der} vh(X) = 1$ dir. Fakat

$$\operatorname{der} vh(X) = \operatorname{der} h(X) = \max\{\operatorname{der} f, \operatorname{der} g\} = \operatorname{der} u$$

olduğundan

$$\begin{aligned} E = F(u) &\iff \operatorname{der} u = 1 \\ &\iff u = \frac{at+b}{ct+d} \text{ ve } ad - bc \neq 0 \text{ olacak şekilde } a, b, c, d \in F \text{ vardır} \end{aligned}$$

denklikleri elde edilir. E üzerinde F'yi sabit bırakan her otomorfizma üreteçleri yine üreteçlere götüreceğinden bu otomorfizmalar $a, b, c, d \in F$ ve $ad - bc \neq 0$ olmak üzere

$$u \longmapsto \frac{at+b}{ct+d}$$

eşlemesi ile tam olarak belirlidirler. Böylece $\operatorname{Gal}(E/F)$'nin her elemanına F üzerinde determinantı sıfırdan farklı (ya da denk olarak tersinir) bir 2×2 kare matris karşılık gelir. Bu şekilde karşılık gelen matrisler

$$\begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix}, \ e \in F$$

tipindeki bir matrisle çarpılması farkı ile tektir. Yani F üzerindeki tersinir matrislerin çarpımsal grubunu $GL_2(F)$, F üzerindeki sıfırdan farklı skaler matrislerin alt grubunu F^* ve

$$u \longmapsto \frac{at+b}{ct+d}$$

eşlemesi ile tanımlanan otomorfizmayı

$$\tau_{a,b,c,d}$$

ile gösterirsek

$$\tau_{a,b,c,d} \longmapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} F^*$$

şeklinde tanımlanan dönüşüm $\operatorname{Gal}(E/F)$ ile $GL_2(F)/F^*$ grupları arasında bir izomorfizmadır.

E bir cisim olsun. Eğer G, E'nin otomorfizmalarının grubu Aut E 'nin bir alt grubu ise o zaman G'ye E'nin bir *otomorfizmalar grubu* diyeceğiz.

Kabul edelim ki bir E cismi için G, E'nin bir otomorfizmalar grubu olsun. O zaman

$$\mathrm{Sbt}(G) := \{a \in E : \text{her } \sigma \in G \text{ için } \sigma(a) = a\}$$

şeklinde tanımlanan küme E'nin bir alt cismidir. $\mathrm{Sbt}(G)$ cismine G'nin E içindeki *sabit cismi* denir.

Dikkat edilirse F, E'nin bir alt cismi ise $\mathrm{Gal}(E/F)$, E'nin bir otomorfizmalar grubudur. Bu durumda E'nin alt cisimleri ile E'nin otomorfizma gruplarını karşılık getiren aşağıdaki gibi eşlemeler yapılabilir:

$$G \longmapsto \mathrm{Sbt}(G)$$

$$F \longmapsto \mathrm{Gal}(E/F).$$

Bu şekilde tanımlanan eşlemelerin kolayca görülebilen temel bazı özellikleri şu şekilde sıralanabilir:

(1) $G_1 \supseteq G_2 \quad \Rightarrow \quad \mathrm{Sbt}(G_1) \subseteq \mathrm{Sbt}(G_2)$.

(2) $F_1 \supseteq F_2 \quad \Rightarrow \quad \mathrm{Gal}(E/F_1) \subseteq \mathrm{Gal}(E/F_2)$.

(3) $\mathrm{Sbt}(\mathrm{Gal}(E/F)) \supseteq F$.

(4) $\mathrm{Gal}\,(E/\,\mathrm{Sbt}(G)) \supseteq G$.

(5) $F = \mathrm{Sbt}(G) \quad \Rightarrow \quad \mathrm{Sbt}(Gal(E/F)) = F$.

(6) $G = \mathrm{Gal}(E/F) \quad \Rightarrow \quad \mathrm{Gal}(E/\,\mathrm{Sbt}(G)) = G$.

LEMMA 1.30. *E/F bir cisim genişlemesi olsun. Eğer E, F üzerinde ayrılabilir olan bir $f(X) \in F[X]$ polinomunun F üzerindeki bir parçalanış cismi ise o zaman*

$$|\mathrm{Gal}(E/F)| = [E : F]$$

olur.

KANIT. Kabul edelim ki $p_1, \ldots, p_n \in F[X]$ indirgenemez polinomlar ve $e_1, \ldots, e_n \in \mathbb{N}$ olmak üzere

$$f(X) = p_1(X)^{e_1} \ldots p_n(X)^{e_n}$$

olsun. Dikkat edilirse E,

$$f_1(X) = p_1(X) \ldots p_n(X)$$

polinomunun da F üzerinde bir parçalanış cismidir. Ayrıca $f(X)$, F üzerinde ayrılabilir olduğundan her $i = 1, \ldots, n$ için $p_i(X)$ polinomunun tüm kökleri E içinde ve basittir. Buna göre $f_1(X)$ polinomunun tüm kökleri basittir. Teorem 1.18'den dolayı istenilen elde edilir. □

LEMMA 1.31 (Artin). *G, E'nin bir sonlu otomorfizmalar grubu ve $F = \mathrm{Sbt}(G)$ olsun. Buna göre*

$$[E : F] \leq |G|$$

olur.

KANIT. Kabul edelim ki $|G| = n$ olsun. E'nin n'den fazla eleman içeren her alt kümesinin F üzerinde doğrusal bağımlı olduğunu göstermek yeterlidir. G=$\{\sigma_1$=1,σ_2,. . .,$\sigma_n\}$ olsun. $m > n$ olmak üzere E'nin $\{u_1, \ldots, u_n\}$ alt kümesini alalım. Buna göre $m > n$ olduğundan

$$(*) \qquad \sum_{j=1}^{m} \sigma_i(u_j)x_j = 0, \quad 1 \leq i \leq n$$

doğrusal denklem sisteminin aşikar olmayan bir çözümü vardır. Kabul edelim ki bu aşikar olmayan çözümler arasında en az sayıda sıfırdan farklı bileşene sahip çözüm $(b_1, \ldots, b_m)$ olsun. Gerekirse bilinmeyenleri yeniden sıralayarak, genelliği bozmadan, $b_1 \neq 0$ kabul edebiliriz. Ayrıca $b_1^{-1}(b_1, \ldots, b_m)$ sıralı m–lisi de $(*)$ sisteminin $(b_1, \ldots, b_m)$ çözümü ile aynı sayıda sıfır bileşeni içeren bir çözümü olacağından, yine genelliği bozmadan, $b_1 = 1$ kabul edebiliriz. Bu durumda her $j = 1, \ldots, m$ için $b_j \in F$ olduğunu göstereceğiz ki bu durumda $(*)$ eşitliğinin ilk denkleminden dolayı

$$u_1b_1 + \cdots + u_mb_m = 0$$

olacağından istenilen elde edilmiş olur.

Kabul edelim ki bir $j = 1, \ldots, m$ için $b_j \notin F$ olsun. Genelliği bozmadan $j = 2$ alabiliriz. Buna göre $\sigma_k(b_2) \neq b_2$ olacak şekilde $k = 2, \ldots, n$ vardır.

$$\sum_{j=1}^{m} \sigma_i(u_j)b_j = 0, \quad 1 \leq i \leq n$$

eşitliklerinin iki tarafına σ_k otomorfizması uygulanırsa

$$\sum_{j=1}^{m} (\sigma_k\sigma_i)(u_j)\sigma_k(b_j) = 0, \quad 1 \leq i \leq n$$

eşitlikleri elde edilir. Fakat G bir grup olduğundan $\sigma_kG = \{\sigma_k\sigma_1, \ldots, \sigma_k\sigma_n\} = G$ ve böylece

$$(\sigma_k\sigma_1, \ldots, \sigma_k\sigma_n)$$

sıralı n–lisi

$$(\sigma_1, \ldots, \sigma_n)$$

sıralı n–lisinin bir permütasyonundan başka birşey değildir. Dolayısıyla

$$\sum_{j=1}^{m} \sigma_i(u_j)\sigma_k(b_j) = 0, \quad 1 \leq i \leq n$$

eşitlikleri sağlanır. Buna göre $(1, \sigma_k(b_2), \ldots, \sigma_k(b_m))$ sıralı n–lisi $(*)$ sisteminin bir çözümüdür. Bu çözümü $(1, b_2, \ldots, b_m)$'den çıkarırsak başka bir çözüm olan

$$(0, b_2 - \sigma_k(b_2), \ldots, b_m - \sigma_k(b_m))$$

sıralı n–lisi elde edilir. Fakat bu son çözümün hem aşikar olmayan bir çözüm olması $(b_2 - \sigma_k(b_2) \neq 0)$ hem de $(1, b_2, \ldots, b_m)$ çzöümünden daha az sayıda sıfırdan farklı bileşen içermesi nedeniyle çelişki elde edilir. Dolayısıyla kanıt tamamlanır. □

TANIM 1.32. E/F bir cebirsel cisim genişleme (kısaca cebirsel genişleme) olsun.

(i) Eğer E'nin her elemanın F üzerindeki minimal polinomu ayrılabilir ise E/F'ye bir *ayrılabilir* (cebirsel) *genişleme* denir.

(ii) Eğer E'de en az bir kökü olan F üzerindeki her monik indirgenemez $p(X) \in F[X]$ polinomu, $E[X]$ içinde

$$p(X) = (X - u_1) \dots (X - u_n)$$

şeklinde doğrusal çarpanlarına ayrılabiliyorsa E/F'ye bir *normal* (cebirsel) *genişleme* denir.

NOT. (i)Tanımdan kolayca görülebilir ki, E/F'nin bir normal genişleme olması, E'nin her elemanının F üzerindeki minimal polinomunun bir parçalanış cisminin E tarafından içerilmesi anlamına gelir.

(ii) E/F normal ve ayrılabilir bir genişleme ise o zaman F üzerinde indirgenemez olan bir polinomun E'de bir kökü varsa bu polinom $E[X]$ içinde farklı doğrusal polinomların çarpımı şeklinde yazılır.

(iii) Önceki bölümde elde edilen sonuçlardan dolayı eğer $\operatorname{char} F = 0$ ya da $\operatorname{char} F = p \neq 0$ ve $F = F^p$ ise her cebirsel E/F genişlemesi ayrılabilirdir.

TEOREM 1.33. *E/F bir cisim genişlemesi olsun. Buna göre aşağıdakiler denktir:*

(i) E, F üzerinde ayrılabilir olan bir $f(X) \in F[X]$ polinomunun F üzerindeki bir parçalanış cismidir.

(ii) $F = \operatorname{Sbt}(G)$ olacak şekilde E'nin otomorfizmalarının sonlu bir G grubu vardır.

(iii) E/F sonlu boyutlu, normal ve ayrılabilir bir genişlemedir.

Ek olarak, eğer E ve F (i)'deki gibi ve $G = \operatorname{Gal}(E/F)$ ise $F = \operatorname{Sbt}(G)$ dir; eğer F ve G (ii)'deki gibi ise $G = \operatorname{Gal}(E/F)$ dir.

KANIT. $(i) \Rightarrow (ii)$: $G = \operatorname{Gal}(E/F)$ ve $F_1 = \operatorname{Sbt}(G)$ olsun. Buna göre F_1, E'nin F'yi içeren bir alt cismidir. Dolayısıyla E, F_1 üzerinde de $f(X)$ polinomunun bir parçalanış cismi olur. Üstelik $\operatorname{Gal}(E/F_1) = G$ dir. Dolayısıyla Lemma 1.30'dan,

$$[E : F] = |G| = [E : F']$$

ve böylece $F = F'$ elde edilir.

$(ii) \Rightarrow (i)$: Lemma 1.31'den dolayı $[E : F] \leq |G|$ olur. Buna göre E/F sonlu boyutludur. $f(X) \in F[X]$ monik indirgenemez polinomu için $f(r) = 0$ olacak şekilde bir $r \in E$ bulunsun.

$$G = \{\sigma_1 = 1, \sigma_2, \dots, \sigma_n\}$$

olsun. Kabul edelim ki

$$\{\sigma_1(r), \sigma_2(r), \dots, \sigma_n(r)\} = \{r_1 = r, r_2, \dots, r_m\}, \quad (m \leq n)$$

olsun. $\tau \in G$ ise $(\tau(r_1), \dots, \tau(r_m))$ sıralı m-lisi $(r_1, \dots, r_m)$ sıralı m-lisinin bir permütasyonudur. Dikkat edilirse $f(r) = 0$ ise $f(r_i) = 0$ $(1 \leq i \leq m)$ olur. Buna göre $f(X)$, $g(X) = \prod_{i=1}^{m}(X - r_i)$ tarafından bölünür. Fakat her $\tau \in G$ için $\tau g = g$ ve $F = \operatorname{Sbt}(G)$ olduğundan $g(X) \in F[X]$ olur. Fakat $f(X)$, F üzerinde monik indirgenemez olduğundan $f(X) = g(X) = \prod_{i=1}^{m}(X - r_i)$; yani, $f(X)$, $E[X]$ içinde farklı lineer polinomları çarpımıdır. Böylece E/F normal ve ayrılabilirdir.

$(iii) \Rightarrow (i)$: $[E : F] < \infty$ olduğundan $E = F(r_1, \dots, r_k)$ olacak şekilde $r_1, \dots, r_k \in E$ vardır. Her i için r_i'nin F üzerindeki minimal polinomu $f_i(X)$ olsun. Kabulümüzden

dolayı $f_i(X)$, $E[X]$ içinde farklı lineer polinomların çarpımı şeklinde yazılabilir. Buna göre $f(X) = \prod_{i=1}^{k} f_i(X)$ polinomu F üzerinde ayrılabilirdir ve $E = F(r_1, \ldots, r_k)$, $f(X)$'in F üzerindeki bir parçalanış cismidir.

E'nin otomorfizmalarının sonlu bir G grubu iççin $F = \mathrm{Sbt}(G)$ ise o zaman $\mathrm{Gal}(E/F) = G$ olacağını gösterelim. Lemma 1.31'den dolayı $[E : F] \leq |G|$ olduğunu biliyoruz. Ayrıca (i) koşulu da sağlanacağından Lemma 1.30'dan $|\operatorname{Gal}(E/F)| = [E : F]$ olur. $G \subseteq \mathrm{Gal}(E/F)$ ve

$$|G| \geq [E : F] = |\operatorname{Gal}(E/F)|$$

olduğundan $G = \mathrm{Gal}(E/F)$ olmak zorundadır. □

Teorem 1.34 (GALOIS TEORİSİNİN TEMEL TEOREMİ). *E/F yukarıdaki teoremin denk koşullarından birini (dolayısyla da tümünü) sağlayan bir cisim genişlemesi olsun. $G = \mathrm{Gal}(E/F)$ olsun. Γ, G'nin alt gruplarının kümesi ve Σ, E/F'nin alt cisimlerinin (yani E ile F arasında kalan cisimlerin) kümesi olsun. O zaman*

$$\begin{array}{ccc} \Gamma & \longrightarrow & \Sigma \\ H & \longmapsto & \mathrm{Sbt}(H) \end{array} \quad \textit{ve} \quad \begin{array}{ccc} \Sigma & \longrightarrow & \Gamma \\ K & \longmapsto & \mathrm{Gal}(E/K) \end{array}$$

fonksiyonları birbirlerinin tersidir ve böylece her ikisi de birer birebir eşlemedir. Ayrıca, aşağıdaki özellikler sağlanır:

(i) $H_1, H_2 \in \Gamma$ olmak üzere $H_1 \supseteq H_2$ ancak ve ancak $\mathrm{Sbt}(H_1) \subseteq \mathrm{Sbt}(H_2)$.

(ii) $H \in \Gamma$ için $|H| = [E : \mathrm{Sbt}(H)]$ ve $[G : H] = [\mathrm{Sbt}(H) : F]$.

(iii) $H \trianglelefteq G$ (yani H, G'nin bir normal alt grubudur) ancak ve ancak $\mathrm{Sbt}(H)/F$ normal genişlemedir. Bu durumda $\mathrm{Gal}(\mathrm{Sbt}(H)/F) \cong G/H$ olur.

Kanıt. $H \leq \mathrm{Gal}(E/F) = G$ olsun. Teorem 1.33'den $F = \mathrm{Sbt}(G)$ olur. Buna göre $F \subseteq \mathrm{Sbt}(H)$ ve böylece de $\mathrm{Sbt}(H)$, E'nin F'yi içeren bir alt cismi olur. Teorem 1.33'nın son kısmında ifade edilenlerin ikinci bölümünü G yerine H için uygularsak $\mathrm{Gal}(E/\operatorname{Sbt}(H)) = H$ elde edilir. Böylece Lemma 1.30 ve Teorem 1.33'ü de kullanarak

$$|H| = |\operatorname{Gal}(E/\operatorname{Sbt}(H))| = [E : \mathrm{Sbt}(H)]$$

eşitliklerini elde ederiz. Bu ise (ii) şıkkının ilk bölümünü verir. Şimdi K, E/F genişlemesinin bir alt cismi olsun. $H = \mathrm{Gal}(E/K)$ yazalım. Buna göre $H \subseteq G = \mathrm{Gal}(E/F)$ ve dolayısıyla $H \leq G$ dir. Ayrıca kolayca görülebilir ki E, K üzerinde de bir ayrılabilir polinomun parçalanış cismidir. Dolayısıyla, Teorem 1.33'ün son kısmının ilk bölümü E ve K cisimleri için uygulanırsa

$$K = \mathrm{Sbt}(H) = \mathrm{Sbt}(\mathrm{Gal}(E/K))$$

elde edilir. Böylece Γ ve Σ kümeleri arasında yukarıdaki gibi tarif edlien fonksiyonlar birbirlerinin tersidir. $H_1 \supseteq H_2$, G'nin alt grupları ise $\mathrm{Sbt}(H_1) \subseteq \mathrm{Sbt}(H_2)$ olacağını zaten biliyoruz. Diğer taraftan G'nin H_1 ve H_2 alt grupları için $\mathrm{Sbt}(H_1) \subseteq \mathrm{Sbt}(H_2)$ ise

$$H_1 = \mathrm{Gal}(E/\operatorname{Sbt}(H_1)) \supseteq \mathrm{Gal}(E/\operatorname{Sbt}(H_2)) = H_2$$

bulunur. Böylece (i) şıkkı elde edilmiş olur. (ii) şıkkının birinci bölümü yukarıda elde edilmişti.

$$|G| = [E : F] = [E : \mathrm{Sbt}(H)][\mathrm{Sbt}(H) : F] = |H|[\mathrm{Sbt}(H) : F]$$

ve

$$|G| = |H| \cdot |G : H|$$

olduğundan

$$[\mathrm{Sbt}(H) : F] = |G : H|$$

ele edilir. Böylece (ii) şıkkının tamamı elde edilmiş olur.

Gözlem: Şimdi $H \in \Gamma$ ve $K = \mathrm{Sbt}(H)$ olsun. Her $\sigma \in G$ için $\sigma H \sigma^{-1}$ eşlenik alt grubunun sabit cisminin $\sigma(K)$ olduğunu göstermek zor değildir. Buna göre $H \trianglelefteq G$ olması ile her $\sigma \in G$ için $\sigma(K) = K$ olması denktir. Ayrıca yukarıda söylenenlerden dolayı $H = \mathrm{Gal}(E/K)$ yazabiliriz.

Kabul edelim ki $H \trianglelefteq G$ olsun. Dolayısıyla her $\sigma \in G$ için $\sigma_{|_K} \in \mathrm{Aut}(K)$ olacağından

$$\sigma \longmapsto \sigma_{|_K}$$

şeklinde tanımlanan dönüşüm $G = \mathrm{Gal}(E/F)$'den $\mathrm{Gal}(K/F)$ içine bir grup homomorfizmasıdır. Bu homomorfizmanın görüntüsü G' olsun. Buna göre G', K'nın otomorfizmalarının bir grubu ve $\mathrm{Sbt}(G') = F$ dir. Dolayısıyla Teorem 1.33'den $G' = \mathrm{Gal}(K/F)$ elde edilir. Öte yandan $\sigma \mapsto \sigma_{|_K}$ homomorfizmasının çekirdeği E'nin K'yı sabbit bırakan otomorfizmalarından oluşur; yani $\mathrm{Gal}(E/K) = H$ dir. Böylece

$$G/H \cong G' = \mathrm{Gal}(K/F)$$

elde edilir. Ayrıca $F = \mathrm{Sbt}(G')$ olduğundan K/F normaldir.

Tersine, kabul edelim ki K/F normal olsun. $a \in K$ ve $f(X)$, a'nın F üzerindeki minimal polinomu olsun. O zaman $K[X]$ içinde $f(X) = (X - a_1)(X - a_2)\dots(X - a_m)$ şeklinde yazılabilir. Burada $a_1 = a$ alabiliriz. $\sigma \in G$ ise $f(\sigma(a)) = 0$, dolayısıyla da uygun bir i için $\sigma(a) = a_i$ yazabiliriz. Buna göre $\sigma(a) \in K$ elde edilir. $a \in K$ keyfi seçildiğinden, $\sigma(K) \subseteq K$ elde edilir. Daha önce yaptığımız gözlemi de kullanarak her $\sigma \in G$ için $\sigma H \sigma^{-1} \subseteq H$; yani, denk olarak, $H \trianglelefteq G$ elde edilir. □

Örnek 1.35. $F = \mathbb{Q}$ ve E, $X^{17} - 1$ polinomunun $\mathbb{Q}$ üzerindeki parçalanış cismi olsun. $(X^{17} - 1)' = 17X^{16}$ ile $X^{17} - 1$ polinomu aralarında asal olduğundan $X^{17} - 1$ polinomunun tüm kökleri farklıdır. Bunlar E'nin içinde çarpımsal devirli bir grup oluştururlar. Bugruba U diyelim. $U = \langle z \rangle$ olsun. $U = \{z, z^2, \dots, z^{17} = 1\}$ ve $E = \mathbb{Q}(z)$ olur. z'nin $\mathbb{Q}$ üzerindeki minimal polinomu $X^{16} + X^{15} + \dots + X + 1$ dir. Buna göre $|G| = 16$ olur. $\sigma \in G$ olsun. $\sigma(U) \subseteq U$ olduğundan $\sigma_{|_U}$, U grubunun bir otomorfizmasıdır.

$$\begin{array}{ccc} G & \longrightarrow & \mathrm{Aut}(U) \\ \sigma & \longmapsto & \sigma_{|_U} \end{array}$$

şeklinde tanımlanan dönüşüm bir grup homomorfizmasıdır. Eğer $\sigma_{|_U} = 1$ ise $\sigma(z) = z$, yani $\sigma = 1$ olacağından bu homomorfizma birebir olur. Öte yandan mertebesi n olan bir devirli grubun otomorfizmalar grubu $(\mathbb{Z}/n\mathbb{Z})^\times$ çarpımsal grubuna izomorf olduğundan

$$\mathrm{Aut}(U) \cong (\mathbb{Z}/17\mathbb{Z})^\times,$$

yani $|\mathrm{Aut}(U)| = 16$ olur. Buna göre mertebeleri karşılaştırırsak

$$\mathrm{Gal}(E/\mathbb{Q}) \cong (\mathbb{Z}/17\mathbb{Z})^\times$$

bulunur. $(\mathbb{Z}/17\mathbb{Z})^\times$ grubu $3 + 17\mathbb{Z}$ tarafından üretildiğine göre $\mathrm{Gal}(E/\mathbb{Q})$ grubu da

$$\eta : z \mapsto z^3$$

şeklinde tanımlanan otomorfizma tarafından üretilir. Böylece $G = \{\eta, \eta^2, \ldots, \eta^{16} = 1\}$ yazabiliriz. G'nin alt grubları aşağıdaki gibidir:

$$G = G_1 = \langle \eta \rangle \supset G_2 = \left\langle \eta^2 \right\rangle \supset G_3 = \left\langle \eta^4 \right\rangle \supset G_4 = \left\langle \eta^8 \right\rangle \supset G_5 = 1.$$

Bu alt gruplara karşılık her $i = 1, 2, 3, 4, 5$ için $F_i = \mathrm{Sbt}(G_i)$ olmak üzere E/F'nin alt cisimlerinin

$$F = F_1 \subset F_2 \subset F_3 \subset F_4 \subset F_5 = E$$

dizisi elde edilir. $x_1 = \sum_{i=1}^{8} \eta^{2i}(z)$ olsun. Buna göre $\eta^2(z) = z$ ve $\eta(z) \neq z$ olduğundan $x_1 \in F_2 \setminus F_1$ bulunur. Öte yandan $[G : G_2] = [G_1 : G_2] = 2$ olduğundan $[F_1 : F_2] = 2$ bulunur. Buna göre $F_2 = F_1(x_1) = F(x_1)$ elde edilir. Benzer şekilde

$$y_1 = \sum_{i=1}^{4} \eta^{4i}(z) \quad \text{ve} \quad z_1 = \sum_{i=1}^{2} \eta^{8i}(z)$$

denirse, $F_3 = F_2(y_1)$ ve $F_4 = F_3(z_1)$ bulunur. Böylece E/F'nin tüm alt cisimleri

$$F \subset F(x_1) \subset F(x_1, y_1) \subset F(x_1, y_1, z_1) \subset E$$

şeklinde listelenebilir. Ayrıca G grubu abelyan olduğundan tüm alt grupları normaldir. Buna göre E/F'nin her alt cismi F üzerinde normaldir.

1.7. Sonlu Grupların Bazı Özellikleri

G bir grup olsun. $H \trianglelefteq G$ ve $G \trianglerighteq H$ gösterimleri$H$'nin G içinde bir normal alt grup olduğunu belirtmek için kullanılacaktır. G'nin alt gruplarının

$$G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_s \trianglerighteq G_{s+1} = 1 \tag{1}$$

biçimindeki bir dizisine G grubu için bir "*normal seri*" denir. Buradan G_{i+1} grubunun G_i içinde normal olduğunu anlıyoruz; fakat dikkat edilmelidir ki bu durum, G_{i+1} in G içinde de normal olmasını gerektirmez.

$$S_3 \triangleright A_3 \triangleright 1 \tag{2}$$

ile

$$V = \{1, (12)(34), (13)(24), (14)(23)\}$$
$$W = \{1, (12)(34)\}$$

olmak üzere

$$S_4 \triangleright A_4 \triangleright V \triangleright W \triangleright 1 \tag{3}$$

dizileri normal serilere birer örnektir.

Yukarıdaki (1) serisi ile

$$G_1/G_2, G_2/G_3, \ldots, G_s/G_{s+1} \cong G_s$$

bölüm grupları ilişkilendirilebilir. Buna serinin *faktörler dizisi* adı verilir. Eğer bir G grubunun bölümler dizisi tümüyle abelyan olan bir normal serisi varsa G'ye bir *çözülebilir grup* denir. (2) ve (3) ile verilen normal serilerden dolayı S_3 ve S_4 gruplarının çözülebilir olduğunu söyleyebiliriz. Aslında S_3/A_3 mertebesi 2 olan bir devirli grup, A_3 mertebesi 3 olan bir devirli grup, S_4/A_4 mertebesi 2 olan bir devirli grup, A_4/V mertebesi 3 olan bir devirli grup ve V/W ile W ise mertebesi 2 olan birer devirli gruptur.

Dikkat edilirse her abelyan grup çözülebilirdir. Aşağıdaki teorem çözülebillir grupların başka önemli bir sınıfını sunmaktadır.

TEOREM 1.36. *Mertebesi bir asal sayının kuvveti olan her sonlu grup çözülebilirdir.*

KANIT. G mertebesi p^n (p asal ve $n \geq 1$) olan bir grup (yani kısaca bir p–grubu) olsun. Bu durumda $C(G) = \{a \in G : \text{her } g \in G \text{ için } ag = ga\}$ G grubunun merkezi olmak üzere $C(G) \neq 1$ dir. $C = C(G)$ diyelim. $G = C$ ise Gabelyan olacağından çözülebilir olur. $G \neq C$ ise $C = C_1$yazalım ve G/C_1 grubunu düşünelim. Bu grup da bir p–grubudur ve dolayısıyla da aşikar olmayan merkeze sahiptir. $C(G/C_1) = C_2/C_1$ olsun. Dikkat edilirse $C_2 \trianglelefteq G$ dir. $G \neq C_2$ ise G/C_2 grubunun merkezi C_3/C_2 olsun. Bu şekilde devam edilerek G'nin normal alt gruplarının

$$1 \subset C_1 \subset C_2 \subset C_3 \dots$$

şeklinde bir dizisi elde edilir. G sonlu olduğundan uygun bir s tamsayısı için $C_{s+1} = G$ olmak zorundadır. Buna göre

$$G = C_{s+1} \triangleright C_s \triangleright \cdots \triangleright C_1 \triangleright 1,$$

C_{i+1}/C_i faktörleri tümüyle abelyan olan bir normal seridir. Böylece G çözülebilir olur. □

Şimdi grupların çözülebilirliğini özel tipte bir normal seriden faydalanarak nasıl test edebileceğimizi göreceğiz. Bunun için önce komütatör adı verilen bir kavramı tanımlayacağız. G bir grup ve $g, h \in G$ olsun. g ve h elemanlarının komütatörü

$$[g, h] = g^{-1}h^{-1}gh$$

biçiminde tanımlanır. Buna göre $gh = hg[g, h]$ olur; yani g ve h'nin komütatörü bu elemanların değişmeli olmaktan ne denli uzak olduğunun bir ölçüsü olarak da görülebilir. G'nin her g, h eleman çifti için elde edilen $[g, h]$ komütatörlerinin ürettiği alt grubu G' ile göstereceğiz. Bu alt gruba G'nin komütatör alt grubu adı verilir. Dikkat edilirse $[g, h] = [h, g]^{-1}$ olduğundan G'

$$[g_1, h_1][g_2, h_2] \dots [g_k, h_k], \qquad g_i, h_i \in G\,(i = 1, \dots, k)$$

tipindeki çarpımların kümesine eşittir. $\sigma : G \to \overline{G}$ bir grup homomorfizması olsun. $\sigma([g, h]) = [\sigma(g), \sigma(h)]$ olacağından $\sigma(G') \subseteq \overline{G}'$ olur. Ayrıca, eğer σörten ise bu eşitlik $\overline{G}$ içindeki tüm komütatörleri ifade edebileceğinden $\sigma(G') = \overline{G}'$ olduğu görülür. Bu açıklamalar, özel olarak, $\overline{G} = G$ olduğunda da; yani, σ G üzerinde bir endomorfizma olduğu zaman da uygulanabilir.

Şimdi $K \trianglelefteq G$ olsun. Bu durumda G üzerinde

$$I_a : x \;\longmapsto\; axa^{-1}$$

biçiminde tanımlanan her iç otomorfizma K üzerinde bir otomorfizma tanımlayacağından, her $a \in G$ için $I_a(K') = K'$; yani $K' \trianglelefteq G$ elde edilir. Kısaca

$$K \trianglelefteq G \quad \Rightarrow \quad K' \trianglelefteq G$$

olur. Özel olarak $G \trianglelefteq G$ olduğundan $G' \trianglelefteq G$ bulunur.

$G'' = (G')'$ ve her $k > 1$ için $G^{(k)} = \left(G^{(k-1)}\right)'$ yazılarak yüksek mertebeden komütatör alt grupları tanımlayabiliriz. Tümevarım kullanılarak her $k \geq 1$ için $G^{(k)} \trianglelefteq G$ olması gerektiği gösterilebilir. Buna göre

$$G \trianglerighteq G' \trianglerighteq G'' \trianglerighteq \cdots$$

dizisi elde edilir. Aslında birazdan G'nin çözülebilir olması ile $G^{(k)} = 1$ olacak şekilde bir $k \geq 1$ tamsayısı bulunabilmesinin denk olduğunu göstereceğiz. Bunun için önce aşağıdaki lemmayı verelim.

LEMMA 1.37. *G/G' grubu abelyandır ve G' alt grubu G/K bölüm grubunun abelyan olduğu G'nin tüm normal K alt grupları tarafından içerilir.*

KANIT. Tanımdan açıkça görülebilir ki G abelyandır ancak ve ancak $G' = 1$ dir. $g, h \in G$ ve $K \trianglelefteq G$ ise o zaman

$$[gK, hK] = [g, h]K$$

ve böylece

$$[gK, hK] = 1_{G/K} \quad \Leftrightarrow \quad [g, h] \in K$$

olur. Dolayısıyla G/K abelyandır ancak ve ancak $K \supseteq G'$ bulunur. Bu ise lemmanın kanıtını tamamlar. □

TEOREM 1.38. *G bir grup olsun. G çözülebilirdir ancak ve ancak $G^{(k)} = 1$ olacak şekilde $k \geq 1$ tamsayısı vardır.*

KANIT. Eğer $G^{(k)} = 1$ olacak şekilde $k \geq 1$ tamsayısı varsa

$$G \trianglerighteq G' \trianglerighteq G'' \trianglerighteq \cdots \trianglerighteq G^{(k)} = 1$$

ve $G^{(i)}/G^{(i+1)}$ abelyan olacağından (Lemma 1.37) G çözülebilir olur.

Şimdi kabul edelim ki G çözülebilir olsun. Buna göre G'nin

$$G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_s \trianglerighteq G_{s+1} = 1$$

olacak şekilde tüm faktörleri abelyan olan bir normal serisi vardır. Yukarıdaki lemmadan $G_{i+1} \supseteq G_i'$ bulunur. Özel olarak $G_2 \supseteq G_1' = G'$ olur. Bir $k > 1$ için $G_k \supseteq G^{(k-1)}$ denirse

$$G_{k+1} \supseteq G_k' \supseteq \left(G^{(k-1)}\right)' = G^{(k)}$$

olacağından her i için $G_i \supseteq G^{(i)}$ elde edilir. $G_{s+1} = 1$ olduğundan $G^{(s+1)} = 1$ bulunur. □

TEOREM 1.39. *Bir çözülebilir grubun her alt grubu ve her homomorf görüntüsü çözülebilirdir. $K \trianglelefteq G$ için K ve G/K grupları çözülebilir ise G grubu da çözülebilirdir.*

KANIT. $H \leq G$ ise $H^{(i)} \subseteq G^{(i)}$ olacağından bir k için $G^{(k)} = 1$olması $H^{(k)} = 1$ olmasını gerektirir. Buna göre G'nin çözülebilir olması H'nin de çözülebilir olmasını gerektirir. Şimdi $\alpha : G \to H$ bir örten grup homomorfizması olsun. Bu durumda $\alpha(G') = (\alpha(G))' = H'$ olur. α'yı G' alt grubuna kısıtlarsak elde edilen grup homomorfizması G'''den H'''ye örten bir grup homomorfizması olacağından $\alpha(G'') = \alpha((G')') = (\alpha(g'))' = H''$ bulunur. Böyle devam edilirse her i için $\alpha(G^{(i)}) = H^{(i)}$ elde edilir. Buna göre eğer $G^{(k)} = 1$ ise $H^{(k)} = 1$ olacağından yukarıdaki teorem gereğince G çözülebilir ise H de çözülebilirdir.

Şimdi kabul edelim ki bir $K \trianglelefteq G$ için G/K çözülebilir olsun. $\nu : G \to G/K$ doğal homomorfizma olsun. ν örten olduğundan $\nu(G^{(i)}) = (G/K)^{(i)}$ olur. Buna göre uygun bir k için $\nu(G^{(k)}) = 1$ olur. Yani $G^{(k)} \subseteq K$ olur. Eğer K da çözülebilir ise uygun bir l için $K^{(l)} = 1$ olacağından $G^{(k+l)} \subseteq K^{(l)} = 1$ ve böylece G çözülebilir olur. □

Tanım 1.40. Bir G grubunun birim ve kendisinden başka normal alt grubu yoksa G'ye bir *basit grup* denir.

G abelyan ve basit bir grup ise mertebesi asal olan bir devirli gruptur. Aşağıdaki teorem abelyan olmayan basit grupların bir sınıfını vermektedir.

Teorem 1.41. *Her $n \geq 5$ için A_n basittir.*

Kanıt. $1 \neq K \trianglelefteq A_n$ olsun. $K = A_n$ olduğunu göstereceğiz. Bunun için K'nın herhangi bir 3–devirli permütasyonu - örneğin (123)'ü - içerdiğini göstermek yeterlidir. Aslında herhangi bir (ijk) 3–devirli permütasyonu için

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots \\ i & j & k & l & m & \cdots \end{pmatrix}$$

alınırsa γ'yı çift seçebileceğimizde (eğer tek ise γ yerine $(lm)\gamma$ permütasyonunu alırız) $(ijk) = \gamma(123)\gamma^{-1} \in K$ elde edilir. Bu durumda A_n 3–devirli permütasyonlar tarafından üretildiğinden $K = A_n$ olur. $1 \neq \alpha \in K$ alalım. Kabul edelim ki α, K'nın elemanları arasında maksimum sayıda elemanı sabit bırakan bir permütasyon olsun. (α'nın bir i'yi sabit bırakması $\alpha(i) = i$ olması anlamındadır.) α'nın bir 3–devirli permütasyon olduğunu göstereceğiz. Aksini kabul edelim. α'yı ayrık devirli permütasyonların çarpımı olarak yazdığımızda bu yazım ya

$$\alpha = (123\ldots)\ldots \tag{4}$$

yapısında ya da

$$\alpha = (12)(34)\ldots, \tag{5}$$

yani ayrık permütasyonların çarpımı şeklinde olacaktır.[1] Birinci durumda α, $(123k)$ şeklinde bir 'tek permütasyon' olamayacağından, en az iki elemanı daha, diyelim ki 4 ve 5'i harekete ettirir. $\beta = (345)$ ve $\alpha_1 = \beta\alpha\beta^{-1}$ olsun. α (4) deki gibi ise $\alpha_1 = (124\ldots)\ldots$ şeklindedir ve eğer α (5) deki gibi ise o zaman da $\alpha_1 = (12)(45)\ldots$ şeklindedir. Her iki durumda da $\alpha_1 \neq \alpha$ olur. $\alpha_2 = \alpha_1\alpha^{-1}$ olsun. Buna göre $\alpha_2 \neq 1$ dir. $i > 5$ için $\alpha(i) = i$ ise $\alpha_2(i) = i$ dir. Öte yandan eğer α (4) deki gibi ise o zama $\alpha_2(2) = 2$ ve böylece $1, 2, 3, 4$ ve 5'i hareket ettirdiğinden α_2 α'dan daha fazla eleman sabit bırakır. Bu ise α'nın seçimi ile seçilir. Eğer α (5) deki gibi ise $\alpha_2(1) = 1$ ve $\alpha_2(2) = 2$; yani, α 5'i sabit bıraksa ve α_2 hareket ettirse bile (ki hareket ettirir) α_2, α'dan daha fazla sayıda eleman sabit bırakır. Bu çelişki α'nın bir 3–devirli permütasyon olması gerektiğini gösterir. □

Doğal Sonuç 1.42. *$n \geq 5$ ise S_n grubu çözülebilir değildir.*

[1] Bu örnek yapılar işimizi görmek için yeterli ve kullanımı basit olduğundan tercih edilmiştir. Farklı alternatiflerin sadece paratezler içindeki sayıların seçimi ile ilgili olduğu ve diğer alternatiflerin seçilmesi halinde de kanıtın aynı yol izlenerek verilebildiği dikkate alınırsa genelliği bozmadığımız görülebilir.

KANIT. Eğer S_n çözülebilir ise bu durumda A_n de çözülebilir olur. O zaman $A_n' \subset A_n$ olur. Fakat $A_n' \trianglelefteq A_n$ ve A_n basit olacağından $A_n' = 1$; yani, A_n abelyan olur ki bu durum $n \geq 4$ için bile mümkün değildir. ((123) ve (234) permütasyonları değişmeli değildir.) □

G bir grup ve

$$G = G_1 \triangleright G_2 \triangleright \cdots \triangleright G_{s+1} = 1$$

G'nin bir normal serisi olsun. Eğer her $i = 1, \ldots, s$ için G_i'nin $G_i \supset H \supset G_{i+1}$ olacak şekilde bir normal alt grubu yoksa (yani denk olarak G_i/G_{i+1} basit grup ise) o zaman bu seriye G'nin bir *komposizyon serisi* denir. Buradaki G_i/G_{i+1} bölümlerine kompozisyon serisi tarafından belirlenen *kompozisyon faktörleri* denir.

G bir sonlu grup olsun. $G = G_1$ yazalım. G_1 bir maksimal normal alt grup içerir. Bu alt gruba G_2 diyelim. G_2 de sonlu olacağından, benzer şekilde, o da bir maksimal normal alt grup içerir. Bu alt gruba da G_3 diyelim. Bu şekilde devam edersek G'nin bir kompozisyon serisine ulaşırız. Dolayısıyla her sonlu grup bir kompozisyon serisine sahiptir.

TANIM 1.43. G bir grup olsun.

$$G = G_1 \triangleright G_2 \triangleright \cdots \triangleright G_{s+1} = 1 \tag{6}$$

ve

$$G = H_1 \triangleright H_2 \triangleright \cdots \triangleright H_{t+1} = 1 \tag{7}$$

G'nin iki kompozisyon serisi olsun. Eğer $s = t$ ve her $i = 1, \ldots, s$ için

$$G_i/G_{i+1} \cong H_{\sigma(i)}/H_{\sigma(i)+1}$$

olacak şekilde $\{1, \ldots, s\}$ kümesi üzerinde bir σ permütasyonu varsa (6) ve (7) serilerine denk kompozisyon serileri denir.

Tanımdan kolayca görülebilir ki iki kompozisyon serisinin denk olması bir denklik bağıntısı tanımlar. Aşağıdaki teorem, sabit bir sonlu grup için bu bağıntıya göre yalnız bir tek denklik sınıfı tanımlanabileceğini söylemektedir.

JORDAN-HÖLDER TEOREMI. *G bir sonlu grup ise G'nin herhangi iki kompozisyon serisi denktir.*

KANIT. Kabul edelim ki G'nin (6) ve (7) de verildiği gibi iki kompozisyon serisi olsun. $|G|$ üzerine tümevarım uygulayacağız. Kanıtı aşağıdaki gibi iki duruma ayıralım:

I. $G_2 = H_2$.
II. $G_2 \neq H_2$.

(I) durumunda

$$G_2 \triangleright \cdots \triangleright G_{s+1} = 1$$

ve

$$H_2 \triangleright \cdots \triangleright H_{t+1} = 1$$

serileri $G_2 = H_2$ grubu için kompozisyon serileri olur. $|G_2| < |G|$ olduğundan tümevarım hipotezimiz gereğince bu seriler denk olur. Ayrıca $G_1/G_2 = H_1/H_2$ olduğundan istenilen elde edilmiş olur. Şimdi (II) durumunu düşünelim. Yani $G_2 \neq H_2$ olsun. $G_2 \triangleleft G$ ve $H_2 \triangleleft G$ olduğundan $G_2H_2 \triangleleft G$ olur. $G_2 \subseteq G_2H_2$, $H_2 \subseteq G_2H_2$ ve $G_2 \neq H_2$ olduğundan

G_2'nin G içinde maksimal normal alt grup olması $G = G_2H_2$olmasını gerektirir. Buna göre

$$G/G_2 = G_2H_2/G_2 \cong H_2/(G_2 \cap H_2)$$

ve

$$G/H_2 = G_2H_2/H_2 \cong G_2/(G_2 \cap H_2)$$

elde edilir (2. İzomorfizma Teoremi). $K_3 = G_2 \cap H_2$ olsun. Buna göre K_3, G_2 ve H_2 içinde maksimal normaldir ve

$$G_1/G_2 \cong H_2/K_3, \quad H_1/H_2 \cong G_2/K_3$$

izomorfizmaları yazılabilir. Kabul edelim ki

$$K_3 \triangleright K_4 \triangleright \cdots \triangleright K_{u+1} = 1,$$

K_3'ün bir kompozisyon serisi olsun. Bu durumda aşağıdaki gibi dört adet komposizyon serisi elde edilir

(i) $$G = G_1 \triangleright G_2 \triangleright G_3 \triangleright \cdots \triangleright G_{s+1} = 1$$

(ii) $$G = G_1 \triangleright G_2 \triangleright K_3 \triangleright \cdots \triangleright K_{u+1} = 1$$

(iii) $$G = H_1 \triangleright H_2 \triangleright K_3 \triangleright \cdots \triangleright K_{u+1} = 1$$

(iv) $$G = H_1 \triangleright H_2 \triangleright H_3 \triangleright \cdots \triangleright H_{t+1} = 1.$$

(I) durumundan dolayı (i) ve (ii) serileri denktir. Benzer şekilde (iii) ve (iv) serileri de denk bulunur. Öte yandan

$$G_1/G_2 \cong H_2/K_3 \quad \text{ve} \quad H_1/H_2 \cong G_2/K_3$$

olduğundan (ii) ve (iii) serilerinin ilk iki kompozisyon faktörleri çapraz olarak izomorf olur. Bu iki serinin geriye kalan tüm kompozisyon faktörleri aynı olduğundan (ii) ve (iii) serileri de denk olur. Geçişme özelliğinden dolayı (i) ve (iv) serileri denk olur. □

Teorem 1.44. *G bi sonlu grup olsun. G çzöülebilirdir ancak ve ancak G'nin bir kompozisyon serisinde her kompozisyon faktörü mertebesi asal sayı olan bir devirli gruptur.*

Kanıt. G çözülebilir olsun.

$$G = G_1 \triangleright G_2 \triangleright \cdots \triangleright G_{s+1} = 1,$$

G'nin bir kompozisyon serisi olsun. Buna göre her $i = 1, \ldots, s$ için G_i/G_{i+1} kompozisyon faktörü çözülebilirdir. G_i/G_{i+1} ayrıca basit de olduğundan abelyan ve böylece de mertebesi asal olan bi devirli grup olur.

Tersine

$$G = G_1 \triangleright G_2 \triangleright \cdots \triangleright G_{s+1} = 1,$$

G'nin bir kompozisyon serisi ve her $i = 1, \ldots, s$ için G_i/G_{i+1} mertebesi asal olan bir devirli grup olsun. Buna göre G_i/G_{i+1} grupları abelyan olacağından G çözülebilir olur. □