8. BÖLÜM
CİSİM

CİSİM KAVRAMI

8.1. Tanım: $A \neq \emptyset$ ve A kümesi üzerinde sırası ile $\bigstar$ ve $\square$ işlemleri tanımlansın. Eğer $(A, \bigstar, \square)$ sistemi üzerinde,

C1) $(A, \bigstar)$ sistemi değişmeli grup,
C2) $(A, \square)$ sisteminin etkisiz elemanı e olmak üzere $(A-\{e\}, \square)$ sistemi değişmeli grup,
C3) A kümesinde $\square$ işlemi $\bigstar$ işlemi üzerine sağdan ve soldan dağılma özelliği var,

C1, C2 ve C3 aksiyomlarını sağlıyorsa $(A, \bigstar, \square)$ sistemi bir cisimdir.

Örnek: $\mathbb{Q}$ rasyonel sayılar olmak üzere $(\mathbb{Q}, +, \cdot)$ sistemi cisimdir.

Çözüm: C1) $(\mathbb{Q}, +)$ bir grup mudur?

G1) Her $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$, $(b, d, f \neq 0)$ olmak üzere,

$$\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a \cdot d \cdot f + b \cdot c \cdot f + b \cdot d \cdot e}{b \cdot d \cdot f} = \left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f}$$

olup birleşme özelliği vardır.

G2) Her $\frac{a}{b} \in \mathbb{Q}$, $(b \neq 0)$ ve e_0 birim (etkisiz) eleman olmak üzere,

$$\frac{a}{b} + e_0 = \frac{a}{b} \text{ ise } e_0 = 0 \in \mathbb{Q}$$

elde edilir.

G3) Her $\frac{a}{b} \in \mathbb{Q}$, $(b \neq 0)$ ve $\frac{a}{b}$ sayısının x^{-1} ters eleman olmak üzere,

$$\frac{a}{b} + x^{-1} = 0 \text{ ise } x^{-1} = \frac{a}{b}$$

biçimindedir.

G4) Her $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$, $(b, d \neq 0)$ olmak üzere $\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d} = \frac{c}{d} + \frac{a}{b}$

O halde $(\mathbb{Q}, +)$ değişmeli bir gruptur.

C2) $(\mathbb{Q}, \cdot)$ bir grup mudur?

G1) Her $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$, $(b, d, f \neq 0)$ olmak üzere,

$$\frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right) = \frac{a \cdot c \cdot e}{b \cdot d \cdot f} = \left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f}$$

olup birleşme özelliği vardır.

G2) Her $\frac{a}{b} \in \mathbb{Q}$, $(b \neq 0)$ ve e_0 birim (etkisiz) eleman olmak üzere,

$$\frac{a}{b} \cdot e_0 = \frac{a}{b} \text{ ise } e_0 = 1 \in \mathbb{Q}$$

elde edilir.

G3) Her $\frac{a}{b} \in \mathbb{Q}$, $(b \neq 0)$ ve $\frac{a}{b}$ sayısının x^{-1} ters eleman olmak üzere,

$$\frac{a}{b} \cdot x^{-1} = 1 \text{ ise } x^{-1} = -\frac{b}{a}, (a \neq 0)$$

biçimindedir.

G4) Her $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$, $(b, d \neq 0)$ olmak üzere

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{c}{d} \cdot \frac{a}{b}$$

değişme özelliği vardır. O halde $(\mathbb{Q}, \cdot)$ değişmeli bir gruptur.

C3) Her $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}, (b, d, f \neq 0)$ olmak üzere

a) $\frac{a}{b} \cdot \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a \cdot c \cdot f + a \cdot e \cdot d}{b \cdot d \cdot f} = \frac{a \cdot c}{b \cdot d} + \frac{a \cdot e}{b \cdot f} = \left(\frac{a}{b} \cdot \frac{c}{d}\right) + \left(\frac{a}{b} \cdot \frac{e}{f}\right)$

b) $\left(\frac{a}{b} + \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{a \cdot d \cdot e + b \cdot c \cdot e}{b \cdot d \cdot f} = \frac{a \cdot e}{b \cdot f} + \frac{c \cdot e}{d \cdot f} = \left(\frac{a}{b} \cdot \frac{e}{f}\right) + \left(\frac{c}{d} \cdot \frac{e}{f}\right)$

olup çarpmanın toplama üzerine sağdan ve soldan dağılma özellikleri vardır.

C1, C2 ve C3 aksiyomlarını sağlandığından $(\mathbb{Q}, +, .)$ sistemi cisimdir.

8.1. Not: Bir R cisminde R\{0} kümesi bir grup olacağından $R = \{0\}$ halkası bir cisim olamaz. O halde "bir cisim en az 2 elemanlıdır" olur.

Örnek: i) $(\mathbb{R}, +, \cdot)$ sistemi cisimdir.
ii) $(\mathbb{C}, +, \cdot)$ sistemi cisimdir.
iii) $(\mathbb{Z}, +, \cdot)$ sistemi cisim değildir.

Bu örneğin çözümü okuyucuya bırakılmıştır.

Örnek: $H = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = ijk = -1\}$ kümesi olarak tanımlanan Hamilton sayılarının oluşturduğu $(H, +, \cdot)$ sistemi cisim değildir. Gerçekten;

$k = ij \neq ji = -k$

olacağından değişme özelliği yoktur. Şu halde cisim değildir.

CİSİMDE TAMLIK BÖLGESİ

8.1. Teorem: Her cisim bir tamlık bölgesidir.

İspat: F bir cisim, $a, b \in F$, $a \neq 0$ olsun. $b = 0$ olduğunu göstermemiz yeterlidir. F bir cisim olduğundan $a^{-1} \in F$ vardır.

$ab = 0 \Leftrightarrow a^{-1}(a\, b) = a^{-1}\, 0$

$\Leftrightarrow (a^{-1}\, a)b = 0$
$\Leftrightarrow 1 \cdot b = 0$
$\Leftrightarrow b = 0$

8.2. Teorem: Her sonlu tamlık bölgesi bir cisimdir.

İspat: $F = \{0, 1, a_1, a_2, \cdots, a_n\}$, $n + 2$ elemanlı sonlu bir tamlık bölgesi olsun. $G = F\backslash\{0\}$ diyelim. Her $x \in G$ nin çarpma işlemine göre bir tersinin olduğunu göstermemiz yeterlidir. 1'in tersi 1'dir. a_1 in tersinin olduğunu gösterelim.

$a_1G = \{a_1, a_1a_1, a_1a_2, \cdots, a_1a_n\}$ kümesine bakalım. Çarpma işlemi kapalı olduğundan ve F tamlık bölgesi olduğundan bu kümedeki elemanların hepsi G'nin elemanlarıdır. Ayrıca bu elemanların hepsi birbirinden farklıdır. Gerçekten;

i) $\exists$ i için $a_1 = a_1a_i$ olsaydı $a_i = 1$ olurdu.

ii) $\exists\, i \neq j$ ve $i \neq j$ için $a_1a_i = a_1a_j$ olsaydı $a_1a_i - a_1a_j = 0$ olup $a_1(a_i - a_j) = 0$ olurdu. F bir tamlık bölgesi olduğundan $a_i - a_j = 0$ olup $a_i = a_j$ olurdu.

Biz burada a_1 için gösterdik. Benzer şekilde diğerlerinin tersinin olduğu da gösterilir.

Sonuç olarak, her iki küme de $n + 1$ elemanlı olduğundan, $a_1G = G$ bulunur. $1 \in G$ olduğundan $\exists$ j için $a_ia_j = 1$ olmalıdır ki bu da $a_1^{-1} = a_j \in F$ olduğunu gösterir.

Örnek: $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, 2, \bar{3}, \bar{4}\}$ sonlu bir tamlık bölgesi olup bir cisimdir. Daha genel olarak p asal ise $\mathbb{Z}_p$ bir cisimdir, aksi halde değildir.

8.1. Sonuç: Tamlık özeliğine sahip bir sıralı cisim vardır.

8.2. Sonuç: Tamlık özeliğine sahip bütün sıralı cisimler birbirine izomorftur.

8.3. Teorem: Rasyonel sayılar kümesinin tamlık özeliği yoktur.

İspat: $S = \{x \in \mathbb{Q} : x^2 < 2\}$ kümesini göz önüne alalım. $S \subseteq \mathbb{Q}$ dür. $1^2 < 2$ olduğundan, $1 \in S$ dir. Öyleyse, $S \neq \emptyset$ dir. Ayrıca, 2 sayısı S'nin bir üst sınırıdır. $\mathbb{Q} \subseteq \mathbb{R}$ olduğundan, $S \subseteq \mathbb{Q}$ dir. Öyleyse, S'nin $\mathbb{R}$ içinde bir en küçük üst sınırı vardır. $\mathbb{R}$ kümesinin üst sınırlarının en küçüğünün $\sqrt{2}$ olduğu ispatlanabilir. $\sqrt{2} \notin \mathbb{Q}$ olduğundan, $\mathbb{Q}$ rasyonel sayılar kümesinin tamlık özeliğine sahip olmadığı anlaşılır.

CİSİMDE İDEALLİK

8.4. Teorem: R halkası birim elemanlı ve değişmeli olsun. Eğer R'nin {0} ve R olan sadece iki tane ideali var ise R'nin bir cisim olduğunu gösteriniz.

İspat: Her $0 \neq a \in R$ için $ba = 1$ olacak şekilde bir $b \in R$ elemanının varlığını göstermeliyiz.

$0 \neq a \in R$ verilsin. $Ra = \{xa : x \in R\}$ kümesini düşünelim. Ra nın bir ideal olduğunu gösterelim:

i) $0 \cdot a = 0$ olup $0 \in Ra$ dır. ($x = 0$ alınırsa)

ii) $xa, ya \in Ra$ ise $xa - ya = (x - y)a \in Ra$, $(x - y \in R)$

iii) $xa \in Ra$ ve $r \in R$ alalım. $r(xa) = (rx)a \in Ra$ dır, çünkü $rx \in R$ dir. Ayrıca R değişmeli olduğundan $(xa)r \in Ra$ dır.

Şu halde Ra bir idealdir. O zaman $Ra = \{0\}$ veya $Ra = R$ olmalıdır. $Ra = \{0\}$ olamaz, çünkü $1 \cdot a = a \in Ra$ ve $a \neq 0$ seçilmişti. O zaman $Ra = R$ olur. $1 \in R$ olduğundan $\exists\, b \in R$ için $ba = 1$ olmalıdır. O zaman $a^{-1} = b \in R$ olur.

Örnek: F bir cisim, R bir halka ve $\phi : F \to R$ bir halka homomorfizması olsun. ϕ'nin ya sıfır homomorfizması ya da 1-1 olduğunu gösteriniz.

Çözüm: Çek(ϕ) nin F'nin ideali olduğunu biliyoruz. F bir cisim olduğundan idealleri sadece {0} ve F dir. Çek(ϕ) = {0} ise ϕ, 1-1 dir. Çek(ϕ) = F ise ϕ sıfır homomorfizmasıdır.

8.5. Teorem: R değişmeli ve birim elemanlı bir halka, M'de onun bir ideali olsun. M maksimal ideal olması için gerek ve yeter şart R/M cisim olmasıdır.

İspat: $\Rightarrow$: M, R'nin maksimal ideali olsun. O halde $M \neq R$ olup R/M en az iki elemanlı bir halkadır. Ayrıca; R değişmeli ve birim elemanlı olduğundan R/M de değişmeli ve birim elemanlıdır (bkz halka). R/M nin cisim olduğunu göstermek için sıfır hariç (yani $M + 0$ hariç) her elemanın çarpma işlemine göre tersinin olduğunu göstermeliyiz. R/M halkasının sıfırı $M + 0 = M$ olduğundan $M \neq M + x \in R/M$ elemanını seçelim. Bu durumda $x \notin M$ olur. Şimdi

$$I = \{m + rx : m \in M, r \in R\}$$

kümesini düşünelim. Bu kümenin bir ideal olduğunu göstermek okuyucuya bırakalım. Her $m \in M$ için $m = m + o \cdot x \in I$ olduğundan ve $x = 0 + 1 \cdot x \in I$ fakat $x \notin M$ olduğundan $M \subsetneq I$ şartının sağlandığı görülür. M maksimal olduğundan $I = R$ olmalıdır. $1 \in R$ olduğundan $1 = m + ax$ olacak şekilde $m \in M$, $a \in R$ vardır. Buna göre $1 - ax \in M$ dir. Buradan

$$(M + a)(M + x) = M + ax = M + 1$$

sonucu bulunur. O halde $M + x$ in çarpma işlemine göre tersi $M + a$ dır.

$\Leftarrow$: M, R'nin bir ideali ve R/M bir cisim olsun. Bir cismin sıfırı ile birim elemanı farklı olduğundan $M \neq M + 1$ olup $1 \notin M$ dir. O halde $M \neq R$ dir. $M \subsetneq I \subsetneq R$ olacak şekilde bir I idealinin olduğunu kabul edelim. $x \in I \backslash M$ alalım. $x \notin M$ olduğundan $M + x \neq M$ olup $M + x$ in R/M içerisinde çarpma işlemine göre tersi vardır. $M + x$ in tersine $M + a$ diyelim. O halde

$$(M + x)(M + a) = M + xa = M + 1$$

olup $1 - xa \in M \subsetneq I$ olur. $x \in I$ ve I ideal olduğundan $xa \in I$ dır. Bu yüzden

$$1 = (1 - xa) + xa \in I$$

olur. Bu ise $I = R$ olduğunu gösterir. Buna göre M maksimal idealdir.

8.2. Tanım: $(F, +, \cdot)$ cismini göz önüne alalım. Her $x \in F$ için, $x \cdot n = 0$ eşitliğini gerçekleyen en küçük, n doğal sayısına $(F, +, \cdot)$ cismin karakteristiği denir. Bu şartı sağlayan böyle bir doğal sayı yoksa cismin karakteristiği sıfırdır denir.

Örnek: $(Z_{/6}, \oplus, \otimes)$ cisminde $\overline{3}$ sayısının karakteristiği $\overline{2}$ dir. Çünkü,

$$\overline{3} \otimes \overline{2} = \overline{0}$$

dır.

8.3. Tanım: (F , + , •) sıralı cisminde F ' nin boş olmayan her S alt kümesinin bir üst sınır varsa, S ' nin F içinde en küçük üst sınırı varsa S kümesine tam olması (ya da tamlık özeliğine sahip olması) denir.

CİSİM GENİŞLEMESİ

8.4. Tanım: E ve F birer cisim olsun. $F \subset E$ ve E'deki işlemlere göre F'de kendi başına bir cisim ise F'ye E'nin bir alt cismi ve bu durumda E'ye F'nin bir genişlemesi denir. Bu durum E/F ile gösterilir.

Örnek: $\mathbb{Q}$, $\mathbb{R}$'nin bir alt cismidir. Başka bir ifade ile $\mathbb{R}$, $\mathbb{Q}$'nun bir genişlemesidir.

8.6. Teorem: E, F'nin bir genişlemesi ve $S \subset E$ bir alt küme olsun. E'nin F ve S'yi kapsayan bütün alt cisimlerinin ara kesiti F(S) ile gösterilir ve bu cisme F'ye S'nin elemanları katılarak elde edilen cisim denir. Buna göre oluşan F(S) en küçük cisimdir.

Örnek: $\mathbb{Q}$ ve $\sqrt{2}$ yi kapsayan en küçük cisim

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

dir. Gerçekten, $\mathbb{Q}(\sqrt{2})$ nin $\mathbb{Q}$ ve $\sqrt{2}$ yi kapsayan cisim olduğunu göstermek okuyucuya bırakılmıştır. Ayrıca bir cisim $\mathbb{Q}$ ve $\sqrt{2}$ yi kapsarsa her $a, b \in \mathbb{Q}$ için $a + b\sqrt{2}$ nin de bu cisimde olacağı açıktır.

8.5. Tanım: E, F'nin bir genişlemesi ve $a \in E$ olsun. $f(a) = 0$ olacak şekilde bir $f(x) \in F[X]$ polinomu varsa a'ya F üzerinde cebirsel eleman denir.

Örnek: $a \in F$ ise a, F üzerinde cebirseldir. Çünkü a elemanı, $X - a \in F[X]$ polinomunun köküdür.

Örnek: $1 + i\sqrt{2} \in \mathbb{C}$ elemanı $\mathbb{Q}$ üzerinde cebirseldir. Çünkü $1 + i\sqrt{2}$, $x^2 - 2x + 3 \in \mathbb{Q}[X]$ polinomunun bir köküdür.

Örnek: π sayısı, $\mathbb{Q}$ üzerinde cebirsel değildir. Çünkü π sayısı irrasyonel sayı olup bir rasyonel polinomun kökü olamaz.

8.2. Not: $a \in E$, F üzerinde cebirsel olsun. Şu halde bir $f(x) \in F[X]$ için $f(a) = 0$ dir. F[X] bir tek türlü çarpanlara ayrılabilen bölge olduğu için $p_i(x)$ ler F[X] de asal polinomlar (çarpanlara ayrılamayan polinomlar) olmak üzere $f(x) = P_1(X)P_2(X) \dots P_r(X)$ şeklinde yazılabilir. $0 = f(a) = p_1(a)p_2(a) \dots p_r(a)$, $P_i(a) \in E$ ve E cisim olduğundan bir i indisi için $p_i(a) = 0$ olur. Genelliği bozmadan $p_i\langle X\rangle$ polinomlarını, monik polinom yani en büyük dereceli katsayısı 1 olan polinom olarak alabiliriz. Şu halde $a \in E$ cebirsel elemanı F[X] deki asal ve monik bir polinomunun kökü olur.

Gerçekten, S(X) başka bir asal ve monik polinom ve $S(a) = 0$ olsaydı; $\langle P(X), S(X)\rangle = 1$ olduğundan, $A(X)P(X) + B(X)S(X) = 1$ olacak şekilde $A(X), B(X) \in F[X]$ bulunabilirdi. Buradan

$1 = A(a)P(a) + B(a)S(a) = 0$

çelişkisi elde edilirdi.

8.6. Tanım: F üzerinde cebirsel, $a \in F$ nin sağladığı asal ve monik polinoma a'nın F üzerinde sağladığı polinom denir. $P_F(a, X)$ ile gösterilir. $d^0P_F(a, X)$ e de a'nın F üzerindeki derecesi denir.

8.7. Teorem: a, F üzerinde cebirsel ve için $f(x) = 0$ ise $P_F(a, X) \mid f(x)$ dir.

İspat: $P_F(a, X) \nmid f(x)$ olsaydı, aralarında $f(x) \in F[X]$ asal oluyorlardı. 8.2. Notta yapıla ispata benzer bir yolla bir çelişkiye varılır.

Örnek: $P_{\mathbb{Q}}(a, X) = x^2 - 2$

8.7. Tanım: E, F'nin bir genişlemesi ise E'ye F-vektör uzayı olarak bakabiliriz. $Boy_F E = [E: F]$ ye E'nin F üzerindeki boyutu veya E/F genişlemesinin mertebesi (derecesi) denir.

Örnek: $\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2$ dir. $\mathbb{Q}(\sqrt{2})$ nin $\mathbb{Q}$ üzerindeki bir tabanı olarak $\{1, \sqrt{2}\}$ alınabilir.

8.8. Teorem: $a \in E$, F üzerinde cebirsel ve $P_F(a,X)$ in derecesi $n \geq 1$ olsun. Bu takdirde;

i) $[F(a) : F] = n$

ii) F(a) nın bir F-tabanı $\{1, a, a^2, \dots, a^{n-1}\}$

dir.

İspat: (ii) gösterilirse (i) de ispatlanmış olur. Her $b \in F(a)$ nın $b_i \in F$ olmak üzere

$$b = b_0 + b_1\, a + b_2\, a^2 + \cdots + b_{n-1}a^{n-1}$$

şeklinde tek türlü olarak yazılabileceğini gösterelim.

b'nin bu yazılışının tekliğini gösterelim. Şöyle ki, başka bir yazılışı

$$b = b'_0 + b'_1\, a + b'_2\, a^2 + \cdots + b'_{n-1}a^{n-1}$$

olsun. Burada

$$0 = (b_0 - b'_0) + (b_1 - b'_1)\, a + (b_2 - b'_2\,)a^2 + \cdots + (b_{n-1} - b'_{n-1})a^{n-1}$$

bulunur. Bu ise a'nın F üzerinde derecesi $n-1$ den küçük olan bir polinomun kökü olması demektir. Bu ise $d^0P_F(a,X) = n$ ile çelişir. Buna göre her i için $b_i - b'_i$ olmalıdır.

Şimdi de yazılışın varlığını gösterelim;

$$P_F(a,X) = C^n + C_{n-1}a^{n-1} + \cdots + C_0$$

olsun. Buradan

$$a^n = -C_{n-1}a^{n-1} - \cdots - C_0$$

bulunur. Tümevarımla, her $r \in \mathbb{N}$ için

$$a^r = b_0 + b_1\, a + b_2\, a^2 + \cdots + b_{n-1}a^{n-1}$$

olduğu gösterilebilir. Şu halde F ve a'yı kapsayan en küçük halka,

$$F[a] = \{b_0 + b_1\, a + b_2\, a^2 + \cdots + b_{n-1}a^{n-1} : b_i \in F\}$$

dir. $F[a] \subset F(a)$ olduğu açıktır. Eğer F[a] nın cisim olduğunu gösterirsek eşitlik bulunur. $b \in F(a)$ alalım. $\varphi_a: F[a] \to F[a]$, $\varphi_a(f(x)) = f(a)$ dönüşümünün örten bir homorfizmadir. Bu dönüşümün örte ve homomorfizma olduğunu göstermeyi okuyucuya bırakıyoruz. F[X] in temel ideal bölgesi olduğu göz önünde tutarak, Çek $\varphi_a = (P_F(a,X))$ Bulunur. $P_F(a,X)$ asal olduğundan, Çek φ_a asal ideal, fakat temel ideal bölgesi de asal idealler maksimal olduğundan Çek φ_a maksimal idealdir. Şu halde F[a]/Çek $\varphi_a \cong F[a]$ cisimdir.

8.8. Tanım: F[a] cismine, F'ye a katmakla elde edilen basit genişleme denir.

8.9. Tanım: E, F'nin bir genişlemesi olsun. Her $a \in E$, F üzerinde cebirsel ise E'ye F'nin bir cebirsel genişlemesi denir.

8.9. Teorem: $[E : F] =$ sonlu ise E, F'nin cebirsel genişlemesidir.

İspat: $a \in E, [E : F] = n$ olsun. $1, a, a^2, \dots, a^n$; E'nin n+1 elemanı olduğundan, F üzerinde $c_0 + c_1 a + c_2 a^2 + \cdots + c_{n-1}a^{n-1} = 0$ olacak şekilde hepsi sıfır olmayan $c_i \in F$ ler bulunabilir. (Buna lineer cebir derslerinde lineer bağlıdır denecek.) Bu ise, a'nın

$c_0 + c_1 X + c_2 X^2 + \cdots + c_n X^n \in F[X]$

polinomunun bir kökü olması demektir. Yani a, F üzerinde cebirseldir.

8.10. Teorem: $[E : F] = 1$ olması için gerek ve yeter şart $E = F$ olmasıdır.

İspat: $\Rightarrow$: $\{\alpha\}$, E'nin F üzerindeki bir tabanı olsun. Şu halde her $b = a\alpha$, $(a \in F)$ şekilde yazılabilir. Özel olarak $b = 1$ için $1 = a_0\alpha$, $(a_0 \in F)$ olacağından $\alpha = a_0^{-1} \in F$ bulunur. Buradan $E = F$ çıkar.

$\Leftarrow$: Yeterlilik ispatı açıktır.

8.11. Teorem: $E \subset F \subset G$ üç cisim olsun. $[F : E]$ ve $[G : F]$ sonlu ise $[G : E]$ de sonlu ve $[G : E] = [G : F][F : E]$ dir. Ayrıca $\{\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n\}$, G'nin F tabanı ve $\{\beta_1, \beta_2, \beta_3, \dots, \beta_n\}$, F'nin E-tabanı ise $\{\alpha_i\beta_i : 1 \le i \le n, 1 \le j \le m\}$, G'nin E-tabanı olur.

İspat: $x \in G$ olsun. $x = \sum_{i=1}^{n} a_i\alpha_i$ olacak şekilde $a_i \in F$ ler bulunabilir. Diğer taraftan, her i için $a_i = \sum_{j=1}^{m} b_{ij}\beta_j$ olacak şekilde $b_{ij} \in E$ ler bulunabilir. Her iki eşitlikten, $x = \sum_{i=1}^{n}\sum_{j=1}^{m} b_{ij}\beta_j\alpha_i$ bulunur. Şu halde her $x \in G$, $\alpha_i\beta_j$ lerin bir doğrusal bileşenidir. Diğer taraftan $\alpha_i\beta_j$ lerin E üzerinde doğrusal bağımsız olduğunu gösterelim.

$$\sum_{i=1}^{n}\sum_{j=1}^{m} c_{ij}\alpha_i\beta_j = 0$$

$$\sum_{i=1}^{n}\left(\sum_{j=1}^{m} b_{ij}\beta_j\right)\alpha_i = 0\,,\ \{\alpha_i\}$$

doğrusal bağımsız olduğundan, her i için $\sum_{j=1}^{m} c_{ij}\beta_j = 0$, $\{\beta_j\}$ doğrusal bağımsız olduğundan, her i ve her j için $c_{ij} = 0$ bulunur.

8.12. Teorem: α_1 ve α_2, F üzerinde cebirsel iseler $F(\alpha_1, \alpha_2)$, F üzerinde sonlu cebirseldir.

İspat: α_1, F üzerinde cebirsel olduğundan $[F(\alpha_1) : F]$ sonludur. α_2, F üzerinde cebirsel olduğundan $F(\alpha_1)$ üzerinde de cebirseldir. Çünkü $F[X] \subset F(\alpha_1)[X]$ dir.

Şu halde $F(\alpha_1, \alpha_2)$, $F(\alpha_1)$ üzerinde sonlu ve $F(\alpha_1)$, F üzerinde sonlu olduğundan 8.11. teoreme göre $F(\alpha_1, \alpha_2)$, F üzerinde sonlu ve

$$[F(\alpha_1, \alpha_2): F] = [F(\alpha_1, F(\alpha_1)][F(\alpha_1) : F]$$

dir. Ayrıca sonlu bir genişlemenin cebirsel olduğunu 8.9. teoremden biliyoruz.

8.3. Sonuç: $\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n$; F üzerinde cebirsel iseler $F(\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n)$, F üzerinde sonlu ve cebirseldir.

8.13. Teorem: α ve β, F üzerinde cebirsel iseler $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta}$ $(\beta \neq 0)$ da F üzerinde cebirseldir.

İspat: $F(\alpha, \beta)$ nın F üzerinde cebirsel olduğunu 8.12. teoremden biliyoruz. $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta}$ $(\beta \neq 0)$, $F(\alpha, \beta)$ nın elemanları olduğundan bu elemanlar da F üzerinde cebirseldir.

PARÇALANIŞ CİSİMLERİ ve NORMAL GENİŞLEMELER

Bu kısımda F cismini, aksini ifade etmedikçe, $\mathbb{Q}$ rasyonel sayılar cisminin bir genişlemesi olarak alacağız.

8.14. Teorem: $f(x) \in F[X]$ olsun. Bu takdirde $f(x)$ in bir kökünü bulunduran F'nin bir E genişlemesi vardır.

İspat: f_1, f 'nin bir asal böleni ise f_1 in bir kökü f 'nin de bir kökü olur. Onun için, genelliği bozmadan f 'yi asal polinom olarak alabiliriz.

$$I = (f) = f \cdot F[X]$$

ideali asal, şu halde maksimal olacağından, çünkü F[X], temel ideal bölgesidir. Bu sebepten $F[X]/I$ cisimdir. $F \to F[X]/I, (a \to a^{+}I)$ dönüşümü 1-1 homomofizmadır. Şu halde $F[X]/I = E$ cisminin F'ye izomorf bir alt cismi vardır. Yani, E/F dir. Diğer taraftan $\alpha = X + I \in E$ dersek, $f(X) \in I$ olduğundan

$$f(\alpha) = f(X) + I = I$$

eşitliğinden $\alpha \in E$ nın, f(X) in bir kökü olduğu götürür.

8.15. Teorem: $f(x) \in F[X]$ olsun.

$$F(X) = \prod_{i=1}^{n} (X - \alpha_i) \qquad (\alpha_i \in E, d^0 f = n)$$

olacak şekilde F'nin bir E genişlemesi vardır.

İspat: F bir cisim ve f(X) i monik polinom olsun. 8.14. teoremden, f(X) in bir kökü $\alpha_1 \in E_1$ olacak şekilde bir E_1/F genişlemesi vardır.

$f(x) = (X - \alpha_1) f_1(X)$ ise teoremi $f_1(X)$ e uygulayarak, $f_1(X)$ in bir kökü $\alpha_2 \in E_2$ olacak şekilde bir E_2/F genişlemesi vardır ve $f_1(X) = (X - \alpha_2) f_2(X)$ olur. Benzer şekilde devam edilirse

$$f(x) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n) g_n(X), (\alpha_i \in E_n, g_n(X) \in E_n[X]$$

olacak şekilde $F \subset E_1 \subset E_2 \subset \cdots \subset E_n$ genişlemeler dizisi elde edilmiş olur. Fakat $d^0 f = n$ olduğundan $d^0 g_n = 0$ ve monik olduğundan, $g_n = 1$ dir. Şu halde $E_n = E$ genişlemesi f 'nin bütün köklerini ($d^0 f = n$ tane) kapsar.

8.10. Tanım: $f(X) \in F[X]$ in bütün köklerini F'ye katmakla elde edilen genişlemeye f 'nin F üzerindeki parçalanış cismi denir ve E_f ile gösterilir.//

Tanımdan hemen anlaşıldığı gibi, f 'nin parçalanış cismi E_f, F ve f'nin köklerini kapsayan en küçük cisimdir.

8.4. Sonuç: $f_1, f_2, f_3, \ldots, f_n$, F[X] de polinomlar olsunlar. Her f_i polinomu E[X] de lineer çarpanlara ayrılacak şekilde bire E/F genişlemesi vardır.

8.11. Tanım: F[X] de sabitten farklı her polinom F[X] de doğrusal çarpanlara ayrılabilirse F cismine cebirsel kapalı denir.//

XIX. yüzyılın başında Gauss'ın karmaşık sayılar cisminin önemli bir özelliğini işaretleyen şu teoremden $\mathbb{C}$ karmaşık sayılar kümesinin cebirsel kapalı bir cisim olduğu anlaşılır.

8.16. Teorem: C[X] deki sabit olmayan her polinom C[X] de doğrusal çarpanlara ayrılabilir.

Örnek: $f(X) = x^3 - 2$ polinomunun $\mathbb{Q}$ üzerindeki parçalanış cismini bulunuz.

Çözüm: $\mathbb{C}$ deki kökleri, $w = (-1 + i\sqrt{3})/2$ olmak üzere $\sqrt[3]{2}, \sqrt[3]{2}w, \sqrt[3]{2}w^2$ dir. Şu halde $E_{\mathbb{Q}} = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}w, \sqrt[3]{2}w^2)$ dir. Bu cismi biraz daha basit bir şekilde yazalım.

$\sqrt[3]{2}, \sqrt[3]{2}w \in E_{\mathbb{Q}}$ ise $w \in E_{\mathbb{Q}}$

$w, \sqrt[3]{2} \in E_{\mathbb{Q}}$ ise $\mathbb{Q}(\sqrt[3]{2}, w) \subset E_{\mathbb{Q}}$

dur. Tersine, $\sqrt[3]{2}, w \in \mathbb{Q}(\sqrt[3]{2}, w)$ olduğundan $\sqrt[3]{2}, \sqrt[3]{2}w, \sqrt[3]{2}w^2 \in \mathbb{Q}(\sqrt[3]{2}, w)$ ve $E_{\mathbb{Q}} = \mathbb{Q}(\sqrt[3]{2}, w)$ bulunur. Şu halde $E_{\mathbb{Q}} = \mathbb{Q}(\sqrt[3]{2}, w)$ dır. Şimdi de $[E_{\mathbb{Q}} : \mathbb{Q}]$ yi hesaplayalım.

$P_{\mathbb{Q}}(w, x) = x^2 + x + 1, P_{\mathbb{Q}}(\sqrt[3]{2}, x) = x^2 - 2$

olduğundan

$[\mathbb{Q}(w): \mathbb{Q}] = 2, \mathbb{Q}(\sqrt[3]{2}, \mathbb{Q}) = 3$

dür. $2 \mid [E_{\mathbb{Q}} : \mathbb{Q}]$ ve $3 \mid [E_{\mathbb{Q}} : \mathbb{Q}]$, $OBEB(2; 3) = 1$ olduğundan $6 \mid [E_{\mathbb{Q}} : \mathbb{Q}]$ bulunur. Fakat

$[E_{\mathbb{Q}} : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, w) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2},): \mathbb{Q}]$ ve $[\mathbb{Q}(\sqrt[3]{2}, w): \mathbb{Q}(\sqrt[3]{2})] \leq 2$

olduğundan $[E_{\mathbb{Q}} : \mathbb{Q}] \leq 6$ dır. Buradan $[E_{\mathbb{Q}} : \mathbb{Q}] = 6$ elde edilir.

Örnek: $f(x) = x^n - 1$ polinomunun $\mathbb{Q}$ üzerindeki parçalanış cismini bulunuz.

Çözüm: f 'nin kökleri $w = e^{2\pi i/n}$ olmak üzere, $1, w, w^2, \dots, w^{n-1}$ dirler. Her w^i $(i = 1,2, \dots, n)$ $\mathbb{Q}(w)$ de olduğu için $E_f = \mathbb{Q}(w)$ dir. Bu cisme n. daire bölümü cismi denir. Şimdi $[\mathbb{Q}(w) : \mathbb{Q}]$ yi bulalım.

$n = 2$ ise $w = -1$ olacağından $\mathbb{Q}(w) = \mathbb{Q}$ ve $[\mathbb{Q}(w) : \mathbb{Q}] = 1$ dir.

$n = p > 2$ olsun.

$x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$ ve $f(x) = x^{p-1} + \cdots + x + 1 \in \mathbb{Z}[x]$ de asal olduğundan $P_0(t, x) = f$ ve $d^0 f = p - 1$ olur. Şu halde $[\mathbb{Q}(w) : \mathbb{Q}] = p - 1$ dir. n herhangi bir tamsayı ise w'nin sağladığı asal polinomu bulmak biraz daha karışıktır. Genel halde $[\mathbb{Q}(w) : \mathbb{Q}] = \emptyset(n)$ dir. Bu eşitliği ispatlamadan, $n = 4$ için örnekle gösterelim. $x^4 - 1 = (x-1)(x+1)(x^2+1)$ olduğundan $w = e^{2\pi i/4} = i$ nin $\mathbb{Q}$ üzerinde sağladığı polinom, $P_{\mathbb{Q}}(i, x) = x^2 + 1$, şu halde $[\mathbb{Q}(w) : \mathbb{Q}] = \emptyset(4) = 2$ dir.

Örnek: p asal, $f(x) = x^p - a \in \mathbb{Q}[x]$ asal polinomunun $\mathbb{Q}$ üzerindeki parçalanış cismini bulalım ve $[E_f : \mathbb{Q}]$ yi hesaplayalım. $x^p - a$ nın kökleri;

$a^{1/p}, a^{1/p}w, \ldots, a^{1/p}w^2, (w = e^{2\pi i/p})$

dirler. Bu durumda $E_f = \mathbb{Q}(a^{1/p}, w)$ dir.

$[\mathbb{Q}(w) : \mathbb{Q}] = p - 1$ ve $\left[\mathbb{Q}\left(a^{1/p}\right) : \mathbb{Q}\right] = p$ dir, $\text{OBEB}(p, p-1) = 1$ olduğundan $[E_f : \mathbb{Q}] = p \cdot (p-1)$ elde edilir.

8.17. Teorem: f(x) in katlı bir kökü varsa f(x) ve $f'(x)$ in F[x] de sabit olmayan ortak bir çarpanları vardır.

İspat: $\Rightarrow$: a, f(x) in katlı bir kökü ise $f(x) = (x-a)^n g(x)$ şeklindedir. (Bu yazılış $E_f[x]$ de veya $\mathbb{C}[x]$ de düşünebiliriz.) Türev özelliklerinden,

$f'(x) = n(x-a)^{n-1} g(x) + (x-a)^n g'(x)$

olduğunu bildiğimizden, $n > 1$ olduğundan $f'(a) = 0$ elde edilir.

Eğer f ve f' nün F[x] de sabitten farklı ortak çarpanları yoksa, $1 = \alpha f(x) \pm \beta g(x)$ olacak şekilde $\alpha, \beta \in F[x]$ bulunabilir. Bu eşitlikte x yerine a yerleştirilirse $1 = 0$ bulunacağından bir çelişki elde edilir. Şu halde, F[x] de f ve f' nün sabit olmayan bir çarpanları vardır.

$\Leftarrow$: a, f ve f' nün bir ortak kökü ise a, f 'nin katlı bir köküdür.

8.18. Teorem: $f \in F[x]$ asal polinomunun bütün sıfırları sabittirler.

İspat: Genelliği bozmadan f 'yi monik polinom olarak alabiliriz. Kabul edelim ki, f 'nin katlı bir kökü var. Bu durunda $d^0 f \geq 2$ dir. Önceki önermeden f ve f' nün F[x] de sabitten farklı bir ortak bölenleri olduğu anlaşılır. Fakat f,

F[x] de asal olduğundan $f \mid f'$ bulunur. Bu ise $d^0 f' \leq d^0 f$ olduğundan bir çelişkidir. //

Bundan sonra, bütün cisimleri $\mathbb{C}$'nin alt cisimleri olarak alacağız.

8.19. Teorem (İlkel Eleman Teoremi): $E = F(\alpha, \beta)$, F'nin cebirsel bir genişlemesi olsun. Bu takdirde E, F'nin basit genişlemesidir. Yani, $E = F(\gamma)$ olacak şekilde $\gamma \in E$ bulunabilir.

İspat: $f = P_F(\alpha, x)$, $g = P_F(\beta, x)$ diyelim ve cebirsel kapalı bir cisim içinde f ve g'nin lineer çarpanlara ayrılışı

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

ve

$$g = (x - \beta_1)(x - \beta_2) \dots (x - \beta_n), (\beta = \beta_1)$$

olsun. $\mathbb{C}$ de $\frac{\alpha_i - \alpha_1}{\beta_1 - \beta_i}$, $(i \neq 1, j \neq 1)$ lerin kümesini göz önüne alalım. Bu küme sonlu elemanlıdır, $\mathbb{Q} \subset F$ olduğundan öyle bir $t \in F$ bulabiliriz ki, t bu kümenin elemanlarından farklı olur. $\gamma = \alpha + t\beta$ için $E = F(\gamma)$ olduğunu göstererek ispatı tamamlayacağız.

$\gamma = \alpha + t\beta \in E$ ise $F(\gamma) \subset E$ olduğu açıktır.

Ters kapsamayı göstermek için, $h(x) = f(\gamma - tx) \in F(\gamma)[x]$ polinomunu düşünelim. $h(\beta) = f(\gamma - t_\beta) = f(\alpha) = 0$ olduğundan, $\mathbb{C}[x]$ de $x - \beta \mid h(x)$ dir. Başka bir β_j $(j > 1)$ için $h(\beta_j) = 0$ olsa, buradan $f(\gamma - t\beta_j) = 0$, dolayısıyla bir $1 < i \leq n$ için $\gamma - t\beta_j = \alpha_i$ bulunurdu. $\gamma = \alpha_1 \pm \beta_1$ eşitliğini göz önüne alırsak, son eşitlikten $t = \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_i}$ olurdu. Bu ise t'nin seçimine ters düşer. Şu halde $x - \beta \mid h(x)$, fakat $j = 1$ için $x - \beta \nmid h(x)$ dir. Buradan $\mathbb{C}[x]$ de h(x) ve g(x) in obebleri $x - \beta$ olduğu görülür. $F(\gamma)[x]$ de h(x) ve g(x) in obeblerini 1 ya $x - \beta$ olabilir. $OBEB(h; g) = 1$ olsa $a(x)h(x) \pm b(x)g(x) = 1$ olacak şekilde $a(x), b(x) \in F(\gamma)[x]$ bulunabilirdi. Bu eşitlikte $x = \beta_1$ koyarak, $0 = 1$ çelişkisi elde edilirdi. Bu durumda

$$OBEB(h; g) = x - \beta_1 \in F(\gamma)[x]$$

dir. Özel olarak, $\beta = \beta_1 \in F(\gamma)$ ve $\gamma - t\beta = \alpha \in F(\gamma)$ elde edileceğinden, $F(\alpha, \beta) \subset F(\gamma)$ bulunmuş olur.

8.5. Sonuç: $E = F(\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n)$, F'nin cebirsel genişlemesi ise $F(\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n) = F(\gamma)$ olacak şekilde bir $\gamma \in E$ vardır.

8.12. Tanım: α, F üzerinde cebirsel ve $f = P_F(\alpha, x)$ olsun.

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

ise $\alpha_1, \alpha_2, \dots, \alpha_n$ ye $\alpha = \alpha_1$ nin F üzerindeki eşlenikleri denir.

Örnek: $\sqrt{5}$ nin $\mathbb{Q}$ üzerindeki eşlenikleri, $f = P_{\mathbb{Q}}(\sqrt{5}, x) = x^2 - 5$ olduğundan, $\pm\sqrt{5}$ diler.

Örnek: $2 + i$ nin $\mathbb{Q}$ üzerindeki eşlenikleri, $P_{\mathbb{Q}}(2 + i, x) = x^2 - 4x + 5$ olduğundan, $2 + i$ diler.

8.13. Tanım: E ve K bir F cisminin iki genişlemesi ve $\sigma : E \to K$ bir monomorfizma (1-1, homomorfizma) olsun. Eğer her $a \in F$ için $\sigma(a) = a$ ise σ'ya E'den K içine bir F-monomorfizma; eğer ayrıca σ örtense bir F-izomorfizma denir ve $E \cong K$ ile gösterilir.

8.3. Not: E cismine, $f : E \to K$ halka homomorfizmasının her zaman 1-1 olduğunu unutmayalım. Ayrıca E/F sonlu genişleme ise 8.9. teoremden cebirsel genişleme olacağını biliyoruz. Şu hadle $\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n \in E$ bulunabilir ki $E = F(\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n)$, ($\alpha_i$ lerin sayısı sonlu olmak zorunda çünkü, $[E : F] =$ sonlu) ve ilkel eleman teoremine göre E/F genişlemesi basit genişlemedir. Şu halde her E/F sonlu genişlemesi için, $E = F(\beta)$ olacak şekilde bir $\beta \in E$ vardır.

8.20. Teorem: $[E : F] = n$ ve $\beta \in E$ için $E = F(\beta)$ olsun. $\sigma : E \to C$ bir monomorfizma ise $\alpha(\beta) = \beta$ nın F üzerinde bir eşleniğidir. E'nin bütün F-monomorfizmalarının sayısı tam n tanedir ve β'nin eşlenikleri $\beta = \beta_1, \beta_2, \cdots, \beta_n$ iseler bunlar $\alpha_i(\beta) = \beta_i, (i = 1,2,3, \cdots, n)$ile belirlidirler.

İspat: Her $x \in E$, $x = a_0 + a_1\beta + \cdots + a_{n-1}\beta^{n-1}, (a_i \in F)$ şeklinde olduğundan ve σ, F'nin elemanlarını sabit bıraktığından

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

dir. Şu halde σ monomorfizması, β'da aldığı değer ile tamamen belirlidir. $f = P_F(\beta, x)$,

$f = b_0 + b_1x + \cdots + b_{n-1}x^{n-1} + x^n$

ise $0 = b_0 + b_1\beta + \cdots + b_{n-1}\beta^{n-1} + \beta^n$ eşitliğine σ'yı uygulayarak,

$$0 = \sigma(0) = b_0 + b_1\sigma(\beta) + \cdots + b_{n-1}\sigma(\beta)^{n-1} + \sigma(\beta)^n = f(\sigma(\beta))$$

bulunur. Şu hadle $\sigma(\beta)$ da f 'nin kökü, yani β'nin bir eşleniğidir. f asal polinom olduğundan, bütün farklı dolayısıyla β'nın eşlenikleri sayısı n tanedir. Bu eşlenikler $\beta = \beta_1, \beta_2, \cdots, \beta_n$ olsun. $\alpha_i(\beta) = \beta_i$ tanımlarsak, α_i $(i = 1,2,3, \cdots, n)$ lerin E'den C içine mümkün olan bütün monomorfizmalar olduğu gösterilmiş olur. α_i lerin herhangi bir $x \in E$ üzerindeki etkisini bulmak için

$$x = a_0 + a_1\beta + \cdots + a_{n-1}\beta^{n-1}, (a_i \in F)$$

şeklinde yazılır ve $\sigma(x) = a_0 + a_1\sigma(\beta) + \cdots + a_{n-1}\sigma(\beta)^{n-1}$ bulunur.

8.4. Not: 8.15 teoremde geçen, α_i $(i = 1,2,3, \cdots, n)$ F-monomorfizmalarının kümesi G(E/F) ile gösterilir.

Örnek: $E = Q(\sqrt{2})$ ise $G(E/F) = \{\sigma_1, \sigma_2\}$ dır. Burada σ_1 özdeşlik dönüşümünü $\sigma_1(\sqrt{2}) = \sqrt{2}$ ve $\sigma_2(\sqrt{2}) = -\sqrt{2}$ ile belirli monomorfizmayı göstermektedir.

Örnek: $E = Q(\sqrt[3]{2})$ ise $G(E/F) = \{\lambda_1, \lambda_2, \lambda_3\}$ dür. Bu dönüşümler $\lambda_1(\sqrt[3]{2}) = \sqrt[3]{2}$ (özdeşlik dönüşümü), $\lambda_2(\sqrt[3]{2}) = w\sqrt[3]{2}$ ve $\lambda_3(\sqrt[3]{2}) = w^2\sqrt[3]{2}$ ile belirlidir. ($w^3 = 1, w \neq 1$ olmak üzere)

8.5. Not: G(E/F) nin eleman sayısının $[E : F]$ olduğuna dikkat edelim. Ayrıca, G(E/F) nin elemanlarının E'den C içine birer dönüşüm olduklarını hazırlatalım. Örneğin, iki önceki örnekteki σ_1 ve σ_2 dönüşümleri E'den E'ye oldukları halde bir önceki örnekteki λ_2 ve λ_3 dönüşümleri E'den E'ye değildirler, çünkü $\lambda_2(\sqrt[3]{2}) \notin E$ ve $\lambda_3(\sqrt[3]{2}) \notin E$ dirler. Ayrıca belirtelim ki $\sigma \in G(E/F)$ için, $\sigma(E) \subset E$ ise $(E) = E$, yani σ örten olmak zorundadır. Çünkü $E \cong \sigma(E)$ olduğundan $[\sigma(E) : F] = [E : F]$ olur ve $F \subset \sigma(E) \subset E$ den $E = \sigma(E)$ çıkar. Bu uyarı ışığında şu tanımı yapmak yararlıdır:

8.14. Tanım: E, F'nin sonlu bir genişlemesi olsun. Eğer her $\sigma \in G(E/F)$ için $\sigma(E) = E$ ise E/F ye normal genişleme denir.

Aşağıdaki denklikler gösterilerek, normal genişleme tanımları söyle yapılabilir:

8.21. Teorem (Normal Genişleme Teoremi): E, F'nin sonlu bir genişleme olsun. Aşağıdaki ifadeler denktir.

1. E, bir $f \in F[x]$ polinomunun parçalanış cismidir.
2. E, sonlu sayıda $f_1, f_2, \cdots, f_n \in F[x]$ polinomlarının kökşleri F'ye katmakla elde edilir.
3. Her $\sigma \in G(E/F)$ için $\sigma(E) = E$ dir.
4. Her $x \in E$ için, x'in F üzerindeki bütün eşlenikleri de E'dedir.

İspat: $(1) \Rightarrow (2)$: Açık

$(2) \Rightarrow (3)$: E, F'ye sonlu sayıda $f_1, f_2, \cdots, f_n \in F[x]$ polinomunun kökleri katmakla elde edilsin. Bütün kökleri $\alpha_1, \alpha_2, \cdots, \alpha_s$ ile gösterirsek, $E = F(\alpha_1, \alpha_2, \cdots, \alpha_s)$ olur. $\alpha \in G(E/F)$ alalım. Her i için, $\sigma(\alpha_i), \alpha_i$ nin eşleniği olduğu için $\sigma(\alpha_i) \in \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ dir. Şu halde $F \subset \sigma(E) \subset E$ dir. Yukarıdaki notta da belirttiğimiz gibi, $[\sigma(E) : F] = [E : F]$ olduğundan $\sigma(E) = E$ bulunur.

$(3) \Rightarrow (4)$: Kabul edelim ki, her $\alpha \in G(E/F)$ için $\alpha(E) = E$ olsun. $x \in E$ ve x'in bir x' eşleniğini alalım. 8.20. teoreme göre $F(x) \to C$ ye $\sigma(x) = x'$ ile tanımlı dönüşüm F-monomorfizmadır. İlkel eleman tepreminden $E = F(x)(\beta)$ olacak şekilde bir $\beta \in E$ bulunabilir. $\sigma: F(x) \to C$, F-monomorfizmasını, $\eta: E \to C$ monomorfizmasına genişletebiliriz. Gerçekten bunun için $\eta(\beta)$ yi β'nın bir eşleniği olarak tanımlamak geter. Bu takdirde, her $\alpha \in E$,

$$\sigma = a_0 + a_1\beta + \cdots + a_{r-1}\beta^{r-1}, \ (a_i \in F(x), r = [E : F(x)])$$

şeklide yazılabileceği için

$$\eta(\sigma) = \sigma(a_0) + \sigma(a_1)\eta(\beta) + \cdots + \sigma(a_{r-1})\eta(\beta^{r-1})$$

olacağından $\eta: E \to C$ bir F-monomorfizma ve $F(x)$ e kısıtlanışı σ'dır. (3) aksiyomundan dolayı $\eta(E) = E$ kabul ettiğimizden, $x' = \eta(x) \in \eta(E) = E$ elde edilir.

$(4) \Rightarrow (1)$: Her $x \in E$ için x'in F üzerindeki her eşleniğinin E'de olduğunu kabul edelim. İlkel eleman teoreminden $E \in F(\beta), (\beta \in E)$ şeklindedir. β'nın F üzerindeki eşleniklerini $\beta = \beta_1, \beta_2, \cdots, \beta_n$ ile gösterelim. (4) den dolayı her $\beta_i \in E$ dir. Şu halde E, $f = P_F(\beta, x)$ polinomunun bütün sıfırlarını F'ye katmakla elde edilmiştir. Yani E, $f(x) \in F[x]$ polinomunun parçalanış cismidir.

Örnek: $Q(\sqrt[3]{2})/Q$ genişlemesi normal genişleme değildir. Çünkü $\sqrt[3]{2}$ nin bütün eşlenikleri Q'da değildir.

Örnek: $\zeta_m = e^{2\pi i/m}$, (birin m. Primitif kökü) olmak üzere, $Q(\zeta_m)/Q$ genişlemesi normaldir. Çünkü ζ_m nin eşlenikleri $\zeta_m, \zeta_m^2, \cdots, m-1$ lerin arasındadır ve bunların hepsi $Q(\zeta_m)$ dedirler.

GALOİS TEORİSİ

25 Ekim 1811, Bourg-la-Reine, Fransa - 31 Mayıs 1832, Paris, Fransa

8.15. Tanım: E, F'nin bir genişlemesi olsun. E'nin kendi üzerine bir F-monoformasına E'nin bir F-otomorfizması denir ve E'nin bütün F-otomorfizmaları kümesi Gal(E/F) ile gösterilir.

Açıktır ki $Gal(E/F) \subset G(E/F)$ dir. G(E/F) nin eleman sayısı $[E:F] = n$ olduğundan, Gal(E/F) nin eleman sayısı en çok n tanedir.

8.22. Teorem: $\sigma \in G(E/F)$ olsun. $\sigma \in Gal(E/F)$ olması için gerek ve yeter şart $\sigma(E) \subset E$ olmasıdır.

İspat: $\Rightarrow$: Açıktır.

$\Leftarrow$: $\sigma(E) \subset E$ olsun. Yukarıda $\sigma(E) \subset E$ ise $\sigma(E) = E$ olacağını göstermiştik. İspatı tekrarlayalım: $[E:F] = n$ ve E'nin F üzerindeki bir tabanı $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ olsun. σ bir F-monomorfizma olduğundan,

$\{\sigma(\alpha_1), \sigma(\alpha_2), \cdots, \sigma(\alpha_n)\}$

de nin F-üzerinde bir tabanı olur. Şu halde $[\sigma(E):F] = n$ dir. $\sigma(E) \subset E$ kabul ettiğimizden

$n = [\sigma(E):F] = [E : \sigma(E)] \cdot [\sigma(E):F]$

$[E : \sigma(E)] = 1$

$E = \sigma(E)$

bulunur.

8.23. Teorem: E/F, [E: F] = n ve E = F(β) olsun. β'nın F-üzerindeki eşleniklerini $\beta_1 = \beta, \cdots, \beta_n$ ile gösterelim. $\sigma_i \in G(E/F)$ ve $\sigma_i(\beta) = \beta_i$ ise

$\sigma_i \in Gal(E/F) \Leftrightarrow \beta_i \in E$

olmasıdır. Özel olarak E/F genişlemesi normal ise Gal(E/F) = G(E/F) dir. Yani Gal(E/F), n elemanlıdır.

İspat: 8.20. teoremde G(E/F) nin elemanlarının β'yı eşleniklerine götürdüklerini ve hepsinin bu şekildeki monomorfizmalar olduğunu göstermiştik.

8.22. teoreme göre,

$$\sigma_i \in Gal(E/F) \Leftrightarrow \sigma_i(E) \subset E \Leftrightarrow \sigma_i(\beta) \subset \beta_i \in E$$

elde edilir. //

Gal(E/F) üzerinde bir grup yapısı kuralım. $\sigma, \eta \in Gal(E/F)$ ise ησ yı bileşke işlemi olarak alabiliri. Yani $x \in E$ için, $(\eta\sigma)(x) = \eta(\sigma(x))$ dır. $\eta\sigma \in Gal(E/F)$ olduğunu açıktır. Örneğin, ησ nın F'nin elemanlarını sabit bıraktığını gösterelim. σ ve η, F-monomorfizma olduğundan, her $a \in F$ için $\sigma(a) = a$ ve $\eta(a) = a$ dır. Buradan

$(\eta\sigma)(a) = \eta(\sigma(a)) = \eta(a) = a$

elde edilir. Gal(E/F) nin bir grup olduğunu açıktır.

Örnek: $E = Q(\sqrt{2})$, Q nun normal genişlemesi olduğundan,

$$Gal(E/F) = G(E/F) = \{\sigma_1, \sigma_2\}$$

dir. Buradan $\sigma_1(\sqrt{2}) = \sqrt{2}$ ve $\sigma_2(\sqrt{2}) = -\sqrt{2}$ ile belirlidir. Şu halde $Gal(E/F) \cong Z_2$ dir.

Örnek: $E = Q(\sqrt[3]{2})$ için $G(E/Q) = \{\lambda_1 = 1, \lambda_2, \lambda_3\}$ olduğu yukarıdaki örneklerde göstermişti. E/Q genişlemesi normal olduğundan

$$Gal(E/Q) = \{\lambda_1 = 1, \} \neq G(E/Q)$$

dır.

Örnek: $E = Q(\sqrt[3]{2})$ için G(E/Q) yu bulalım. $\sqrt[3]{2}$ nin eşlenikleri $\sqrt[3]{2}, \sqrt[3]{2}w, \sqrt[3]{2}w^2$ olduğundan, E/Q genişlemesi normal değildir. $Gal(E/Q) \subsetneq G(E/Q)$ ve $Gal(E/Q) = \{\lambda_1\}$ dir. Burada λ_1, E'nin özdeşlik otomorfizmasıdır.//

Son örnekteki Galois grubu sadece birimden oluşmaktadır. Hâlbuki bu örnekte [E: Q] = 3 dür. E/Q genişlemesinin normal olmamasından dolayı böy-

le bir sonuca ulaştık. Örnek 1 ve 2 normal genişlemeler olduğundan, Gal(E/Q) nun mertebesi genişlemenin mertebesine eşittir.

8.16. Tanım: E/F sonlu ve normal genişlemesine Galois genişlemesi denir.

Galois teorisinin temel teoremi, E ve F arasındaki cisimlerle, $E = Gal(E/Q)$ grubunun alt grupları arasında birebir bir eşitlik kurmaktadır. Şimdi bu ilgiyi inceleyelim.

8.24. Teorem: H, $G = Gal(E/F)$ nin bir alt grubu olsun.

$$F(H) = \{x \in E : \sigma \in H \text{ için } \sigma(x) = x\}$$

ye E'nin F'ye, kapsayan bir alt cismidir. Bu cisme H'nın sabit cismi denir.

İspat: $F(H) \subset E$ olduğu açıktır. Her $\sigma \in H$ için σ bir F-otomorfizma olduğundan, her $a \in F$ için $\sigma(a) = a$ dır. Buradan $F \subset F(H)$ bulunur. Şimdi F(H) nin bir cismi olduğunu gösterelim.

$x, y \in F(H)$ ise her $\sigma \in H$ için $\sigma(x) = x$ ve $\sigma(y) = y$ olduğundan,

$$\sigma(x \pm y) = \sigma(x) \pm \sigma(y) = x \pm y \text{ ve } x, y \in F(H), y \neq 0$$

ise

$$\sigma(x\, y^{-1}) = \sigma(x)\, \sigma(y^{-1}) = \sigma(x)\, \sigma(y)^{-1} = x\, y^{-1}$$

olduğundan $x \pm y$ ve $xy^{-1} \in F(H)$ elde edilir. Şu halde F(H) bir cisimdir.

8.24. Teorem: E/F bir Galois genişlemesi ve H, Gal(E/F) nin bir alt grubu olsun. Bu takdirde E/F(H) bir Galois genişlemesidir ve $Gal(E/F(H)) = H$ dır.

İspat: E/F sonlu ve normal genişleme ise E/F(H) genişlemesi de sonlu ve normal genişlemedir. Şu halde Galois genişlemesi olur. Gal(E/F(H)), E'nin F(H)-otomorfizmalarıyla oluşur. $\sigma \in H$ elemanı, F(H) nın tanımından dolayı, F(H) nın elemanlarını sabit bıraktığından, $H \subset Gal(E/F(H))$ dır.

Kabul edelim ki H, s elemanlı ve Gal(E/F(H)), t elemanlı bir grup olsun. Yukarıdaki kapsamadan, $s \leq t$ dir. $s = t$ olduğunu gösterirsek, $H = Gal(E/F(H))$ ve böylece teoremin ispatı tamamlanmış olur. Kabul edelim ki $s < t$ olsun. $s + 1 < t$ olduğundan, $\alpha_1, \alpha_2, \cdots, \alpha_{s+1} \in E$ elemanlarını F(H) üzerinde doğrusal bağımsız olacak şekilde seçebiliriz.

$$\sum_{i=1}^{s+1}\sigma_j(\alpha_i)X_i = 0, \quad (j = 1,2,\cdots,s) \qquad (1)$$

homojen denklem sistemi, s denklem ve $s \pm 1$ bilinmeyenden oluşur. Şu halde E'de hepsi sıfır olmayan, $(c_1, c_2, \cdots, c_{s+1})$ çözümü bulunabilir. Gerçekten α_i leri yeniden sıralayarak, bu çözümü $(c_1, c_2, \cdots, c_r, 0, 0, \cdots, 0)$ $(1 \le i \le r$ için $c_i \neq 0)$ şeklinde alabiliriz. Ayrıca bu çözüm, sıfır olmayan c_i lerin sayısı r, minimum olacak şekilde seçilebilir ve denklem sistemi homojen olduğundan $c_r = 1$ yapılabilir. Gerçekten yukarıdaki çözüm yerine $(c_1c_r^{-1}, c_2c_r^{-1}, \cdots, 1, 0, 0, \cdots, 0)$ alanabilir. Her σ_i bir F(H)-otomorfizma ve her $c_i \in F(E)$ ise

$$\sum_{i=1}^{s+1}\sigma_j(\alpha_i)c_i = 0 \Leftrightarrow \sigma_j\left(\sum_{i=1}^{s+1}\alpha_i c_i\right) = 0 \Leftrightarrow \left(\sum_{i=1}^{s+1}\alpha_i c_i\right) = 0$$

bulunur. Bu ise σ_i lerin F(H) üzerinde doğrusal bağımsız olmaları ile çelişir. Şu halde c_i lerin hepsi F(H) de değildir. Genelliği bozmadan $c_i \notin F(H)$ alabiliriz. Buradan $\sigma(c_1) \neq c_1$ olacak şekilde bir $\sigma \in H$ nın varlığı çıkar. (1) denklem sisteminin her iki yanına bu σ'yı uygularsak;

$$\sum_{i=1}^{s+1}\sigma\sigma_j(\alpha_i)\sigma(c_i) = 0$$

bulunur. σ_j, H'da değişirken, $\sigma\sigma_i$ de H'da değişir. Buradan

$$(\sigma(c_1), \sigma(c_2), \cdots, \sigma(c_{r-1}), 1, 0, 0, \cdots, 0)$$

in de (1) in bir çözümü olduğu anlaşılır. Fakat bu iki çözümün farkı da bir çözüm olduğundan

$$(\sigma(c_1) - c_1, \sigma(c_2) - c_2, \cdots, \sigma(c_{r-1}) - c_{r-1}, 0, 0, \cdots, 0)$$

da (1) in bir çözümüdür. $\sigma(c_1) \neq c_1$ olduğundan, sıfır çözüm de değildir. Bu ise

$$(c_1, c_2, \cdots, c_r, 0, 0, \cdots, 0)$$

çözümünün seçimi ile (r'nin minimali ile) çelişir. Sonuç olarak $s = t$ olmalıdır.//

Böylece son iki teorem ile şunu göstermiş olduk: $H \to F(H)$ dönüşümü, Gal(E/F) nin H alt grununa, E/F genişlemesinin bir ara cismi F(H) yı karşılık getirmektedir. Bu tekabülü tersine de kurabiliriz. D, E/F nin bir ara cismi olsun.

$$g(D) = \{\sigma \in Gal(E/F) : \text{Her } x \in D \text{ için } \sigma(x) = x\}$$

diyelim. $g(D) = Gal(E/D)$ olduğu açıktır. 8.24 teoremden, H, Gal(E/F) nin herhangi bir alt grubu ise $g(F(H)) = H$ bulunur.

D herhangi bir ara cisim ise $g(F(H)) = H$ eşitliğini $H = g(D)$ için yazarsak $g(F(g(D))) = g(D)$ bulunur. Buradan mertebelerini hesaplayarak;

$$[E : (F(g(D)) = 0(g(D) = [E : D]$$

elde edilir. D, F(g(D)) olduğundan son eşitlik bize $D = F(g(D))$ yi verir. Bu ise her D ara cisminin F(H), $(H = g(D))$ şeklinde olması demektir. Bu bilgileri toplarsak şu temel teoremi elde ederiz.

8.25. Teorem (Galois Teorisinin Temel Teoremi): E/F bir Galois genişlemesi ve Galois grubu G olsun. $H \to F(H)$ dönüşümü G'nin alt grupları ile E/F nin ara cisimleri arasında 1-1 bir dönüşümdür. Üstelik bu dönüşüm altında, H'nın görüntüsü D ise E/D Galois genişlemesi ve $Gal(E/D) = H$ dır.

İspat: $H \to F(H)$ dönüşümünün 1-1 liği yukarıda $g(F(H)) = H$ olduğu gösterildiğinden bu elşitlikten elde edilir. Gerçekten,

$$F(H_1) = F(H_2) \Rightarrow g(F(H_1)) = g(F(H_2)) \Rightarrow H_1 = H_2$$

yi verir. Ayrıca her D ara cismi F(H) şeklinde olduğundan dönüşümün örtenliği elde edilr. Teoremin son ifadesini doğruluğu 8.24. teoremden görülür.

8.6. Sonuç: E/F Galois genişlemesi olsun. $F \subset D \subset E$ şeklide ancak sonlu sayıda D ara cismi vardır.

Gerçekten, Gal(E/F) sonlu grup olduğundan, sadece sonlu sayıda alt grubu vardır. Temel teoremden ara cisimlerin sayısının da sonlu olması gerekir.

Örnek: $F = Q, E = Q(\sqrt{2}, \sqrt{3})$ olsun. $G = Gal(E/F)$ nin mertebesi 4'dür ve elemanları şu şekilde belirlidir.

$$\sigma_1 : \begin{cases} \sqrt{2} \to \sqrt{2} \\ \sqrt{3} \to \sqrt{3} \end{cases} \quad \sigma_2 : \begin{cases} \sqrt{2} \to -\sqrt{2} \\ \sqrt{3} \to \sqrt{3} \end{cases} \quad \sigma_3 : \begin{cases} \sqrt{2} \to \sqrt{2} \\ \sqrt{3} \to -\sqrt{3} \end{cases} \quad \sigma_4 : \begin{cases} \sqrt{2} \to -\sqrt{2} \\ \sqrt{3} \to -\sqrt{3} \end{cases}$$

G'nin alt grupları: $H_1 = \{\sigma_1\}, H_2 = \{\sigma_1, \sigma_2\}, H_3 = \{\sigma_1, \sigma_3\}, H_4 = \{\sigma_1, \sigma_4\}$ ve $H_2 = G$ dir. Bu alt gruplara karşılık gelen ara cisimler

$$F(H_1) = Q(\sqrt{2}, \sqrt{3}) = E, \quad F(H_2) = Q(\sqrt{3}),$$
$$F(H_3) = Q(\sqrt{2}), \quad F(H_4) = Q(\sqrt{6}), \quad F(H_5) = Q$$

durlar. Şu halde E/Q nun 5 ara cismi vardır. Örnek olarak $F(H_4) = Q(\sqrt{6})$ olduğunu ispatlatalım:

$$\sqrt{6} = \sqrt{3} \cdot \sqrt{2} \in F(H_4) \Rightarrow Q(\sqrt{6}) \subset F(H_4)$$

dür. $Q(H_4) = 2$ olduğundan temel teorem göz önüne alınarak, $\left[Q(\sqrt{2}, \sqrt{3}) : F(H_4)\right] = 2$ bulunur. Ayrıca $\left[Q(\sqrt{2}, \sqrt{3}) : Q(\sqrt{6})\right] = 2$ olduğundan,

$$\left[F(H_4) : Q(\sqrt{6})\right] = 1 \Rightarrow F(H_4) = Q(\sqrt{6})$$

elde edilir.

Örnek: E, x^3-2 polinomunun Q üzerindeki parçalanış cismi olsun. Gal(E/Q) grubunu, alt gruplarını ve bunlara karşılık gelen ara cisimleri bulunuz.

Çözüm: $x^3-2=(x-\sqrt{2})(x^3+\sqrt[3]{2}x+\sqrt[3]{2^2})$ ve kökleri $\sqrt[3]{2}, \sqrt[3]{2}w, \sqrt[3]{2}w^2$ ($w=\frac{-1+\sqrt{3}i}{2}$ olduğundan, parçalanış cismi $E=Q(\sqrt[3]{2},\sqrt{3}i)$ dir. E/Q genişlemesi normal ve $[E:Q]=6$ dır. Gal(E/Q), 6 elemanlı bir gruptur. E'nin Q-otomorfizmaları $\sqrt[3]{2}$ ve $\sqrt{3}i$ ye olan etkileri ile tamamen belirlidir. Şu halde Gal(E/Q) nun 6 Q-otomotfizmasu şunlardır.

$$\sigma_1:\begin{cases}\sqrt[3]{2}\to\sqrt[3]{2}\\ \sqrt{3}i\to\sqrt{3}i\end{cases}\quad \sigma_2:\begin{cases}\sqrt[3]{2}\to\sqrt[3]{2}w\\ \sqrt{3}i\to\sqrt{3}i\end{cases}\quad \sigma_3:\begin{cases}\sqrt[3]{2}\to\sqrt[3]{2}w^2\\ \sqrt{3}\to\sqrt{3}i\end{cases}$$

$$\sigma_4:\begin{cases}\sqrt[3]{2}\to\sqrt[3]{2}w\\ \sqrt{3}i\to-\sqrt{3}i\end{cases}\quad \sigma_5:\begin{cases}\sqrt[3]{2}\to\sqrt[3]{2}w\\ \sqrt{3}i\to-\sqrt{3}i\end{cases}\quad \sigma_6:\begin{cases}\sqrt[3]{2}\to\sqrt[3]{2}w^2\\ \sqrt{3}\to-\sqrt{3}i\end{cases}$$

$\sigma_2\sigma_3=\sigma_5$, $\sigma_3\sigma_2=\sigma_4$, $\sigma_2\sigma_3\sigma_2=\sigma_6$ olduğu gösterilebilir. $\sigma_2=\sigma$, $\sigma_3=\tau$ yazarsak $G=Gal(E/Q)=\{\sigma_1,\sigma,\tau,\sigma\tau,\tau\sigma,\sigma\tau\sigma\}$ bulunur. G'nin alt grupları $\{\sigma_1\}$, $H_1=\{\sigma_1,\sigma\}$, $H_2=\{\sigma_1,\tau\}$, $H_3=\{\sigma_1,\sigma\tau\sigma\}$, $H_4=\{\sigma_1,\sigma_2\tau\sigma\}$ ve G dirler. Bu alt gruplarına karşılık gelen ara cisimler sırasıyla; E, $F(H_2)=Q(\sqrt[3]{2}w^2)$, $F(H_3)=Q(\sqrt[3]{2}w)$, $F(H_4)=Q(\sqrt[3]{2}i)$ ve Q olduğu gösterilebilir. Ayrıca şunu da belirtelim ki E/Q GAlois genişlemesi olduğu halde, $i=1,2,3$ için, $F(H_i)/Q$ genişlemesi normal değildir.

8.26. Teorem: E/F Galois genişlemesi ve Galois grubu olsun. H_1 ve H_2, G'nin alt grupları ve bunlara karşılık gelen ara cisimler D_1 ve D_2 iseler;

i) $H_1\subset H_2\Leftrightarrow D_1\supset D_2$

ii) $H_1\cap H_2$ ye karşılık gelen cisim, D_1 ve D_2 yi kapsayan E'nin en küçük alt cismidir. (Bu cisme D_1D_2 ile gösterilir.)

iii) H_1 ve H_2 yi kapsayan G'nin en küçük alt grubu $H_1\cup H_2$ ile gösterirsek, bu alt gruba karşılık gelen ara cisim $D_1\cap D_2$ dir.

İspat: Galois'in temel teoremden $D_1=F(H_1)$ ve $D_2=F(H_2)$ dir.

i) $H_1\subset H_2\Rightarrow F(H_1)\supset F(H_2)$ olduğu açıktır. Tersine

$F(H_1) \supset F(H_2) \Rightarrow g(F(H_1)) \subset g(F(H_2))$
ve yukarıda açıklanan $g(F(H)) = H$ izahı gereği $H_1 \subset H_2$ elde edilir.

ii) $H_1 \cap H_2$, G'nin H_1 ve H_2 de kapsanan en büyük alt grubudur. Şu halde (i) den ve Galois'in temel teoremden $F(H_1 \cap H_2)$, E'nin $F(H_1)$ ve $F(H_2)$ yi kapsayan en küçük alt cismidir.

iii) $H_1 \cup H_2$, G'nin H_1 ve H_2 yi kapsayan en küçük alt grubudur. Şu halde (i) den ve Galois'in temel teoreminden $F(H_1 \cup H_2)$, E'nin $F(H_1)$ ve $F(H_2)$ de kapsayan en büyük alt cismidir. Yani $F(H_1 \cup H_2) = F(H_1) \cap F(H_2)$ dir.

8.7. Sonuç: E/F Galois genişlemesi ve Galois grubu G ve $x \in E$ olsun. Eğer her $\sigma \in G$ için $\sigma(x) = x$ ise $x \in F$ dir.

Gerçekten, her $\sigma \in G$ için $\sigma(x) = x$ ise $x \in F(G)$ dir. G'nin tarafından $g(F) = G$ buradan $F(g(G)) = F(G)$ bulunur. Fakat yukarıda $F(g(G)) = F$ olduğu gösterildiğinden $x \in F$ elde edilir.

8.27. Teorem: E/F Galois genişlemesi ve $G = Gal(E/F)$ olsun. Ayrıca D bir ara cisim ve $H = g(D)$ olsun. Bu takdirde;

i) D/F normal genişleme $\Leftrightarrow H \lhd G$
ii) $H \lhd G \Rightarrow$ D/F Galois genişlemesi ve $Gal(D/F) \cong G/H$ dır.

İspat: $\sigma \in G$ olsun. Önce $g(\sigma D) = \sigma g(D)\sigma^{-1}$ olduğunu gösterelim. $\eta \in g(D)$ ise $\sigma\eta\sigma^{-1}$, σD yi sabit bırakır. Şu halde, $g(\sigma D) \supset \sigma g(D)\sigma^{-1}$ dir.

$\lambda \in g(\sigma D)$ ise $\sigma^{-1}\lambda\sigma$, D'yi sabit bırakır. Şu halde $\sigma^{-1}\lambda\sigma \in g(D)$ ve $\lambda \in \sigma g(D)\sigma^{-1}$ dir. Buradan $g(\sigma D) \subset \sigma g(D)\sigma^{-1}$ elde edilir. Her iki kapsamadan eşitlik çıkar.

i) D/F normal $\Leftrightarrow$ Her $\sigma \in Gal(E/F)$ için $\sigma D = D$
$\Leftrightarrow$ Her $\sigma \in Gal(E/F)$ için $g(\sigma D) = g(D)$ (8.26. teorem)
$\Leftrightarrow$ Her $\sigma \in Gal(E/F)$ için $\sigma H\sigma^{-1} = H$ (Yukarıdaki eşitlik)

ii) (i) den $H \lhd G$ ise D/F normal genişlemedir. D/F sonlu olduğundan Galois genişlemesi olduğu görülür.

$\psi : Gal(E/F) \to Gal(D/F)$ dönüşümü, $Gal(E/F)$ için $\psi(\sigma) = \sigma/D$ (σ'nın D'ye kısıtlanışı) olarak tanımlansın. ψ'nin bir homonorfizma olduğu gösterile-

bilir. D'nin her F-otomorfizması E'nin bir F-otomorfizmasına genişletilebildiğinden ψ örtendir.

Çek $\psi = \{\sigma \in Gal(E/F) : \sigma = D \text{ üzerinde özdeşlik}\} = H$

Şu halde homomorfizma teoreminden $Gal(D/F) \cong G/H$ dır.

ÇÖZÜMLÜ ALIŞTIRMALAR

1. R'de toplama ve çarpma,
$A + B = (A \cup B)\backslash(A \cap B)$ ve $A \cdot B = A \cap B$
olarak tanımlansın. $(R, +, \cdot)$ sistemi değişmeli ve birimli halka olduğu halka konusunda gösterilmiştir, ama bu $(R, +, \cdot)$ sistemi cisim değildir, gösteriniz.

Çözüm: Halka konusunda gösterilirken çarpma işleminde A kümesinin kendisi birim eleman olduğu gösterilmiştir.

$$A \cdot A^{-1} = A \cap A^{-1} = A$$

olacak şekilde $A^{-1} \in R$ bulunamaz. Şu halde $(R, +, \cdot)$ sistemi cisim değildir.

KAYNAKÇA

1. Doç. Dr. Fethi ÇALLIALP, Soyut Cebir e Sayılar Teorisi, Ondokuz Mayıs Üniversitesi, Fen Edebiyat Fakültesi, Samsun, 1986.
2. H. Hilmi Hacısalihoğlu, Lineer Cebir, Gazi Üniversitesi Yayınları, Ankara, 1975.