SAYILAR
TEORİSİ

Babamın Anısına...

Ve Aileme...

[redacted]

Erhan GÜLER

- BÖLÜM I -

2.10.96/Çarşamba

1. Cisim Genişlemeleri

TANIM : E bir cisim, F de bunun bir alt cismi olsun. Bu durumda E'ye F'nin bir genişlemesi denir. E/F ile gösterilir.

Örnek // $\mathbb{Q} \subset \mathbb{R}$ $\mathbb{Q}$, $\mathbb{R}$ nin bir alt cismidir. $\mathbb{R}/\mathbb{Q}$

$\mathbb{Q} \subset \mathbb{C}$ $\mathbb{Q}$, $\mathbb{C}$ nin bir alt cismidir. $\mathbb{C}/\mathbb{Q}$

TANIM : E, F nin bir genişlemesi (E/F) ve $S \subset E$ olsun. E'nin, F ve S yi kapsayan tüm alt cisimlerinin arakesiti F(S) ile gösterilir. F(S) cismine, F'ye S'nin elemanlarını katmakla elde edilen cisim denir.

F(S) cismi bu özellikteki en küçük cisimdir.

$$\left\{ \begin{array}{ll} \mathbb{R}/\mathbb{Q} & S=\{\sqrt{2}\} \subset \mathbb{R} \\ & \mathbb{Q}(\sqrt{2}) \end{array} \right\}$$

Örnek // $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$, $\mathbb{Q}$ ve $\sqrt{2}$ yi kapsayan en küçük cisimdir. $\mathbb{Q}(\sqrt{2}) \overset{\subset}{\underset{\supset}{=}} K$?

$K := \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$

$\subset$:
$$\left.\begin{array}{l} K \text{ cisimdir.} \\ \mathbb{Q} \subset K. \\ \sqrt{2} \in K \end{array}\right\} \mathbb{Q}(\sqrt{2}) \subset K \ \ldots (1)$$

$$\left.\begin{array}{l} \left.\begin{array}{l} - \ x-y \in K \\ - \ xy \in K \end{array}\right\} \Rightarrow \text{alt halka} \\ \text{- Sıfırdan farklı her elemanın tersi var.} \end{array}\right\} \Rightarrow \text{cisim.}$$

$\supset$: $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$
$b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$
$a+b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ $\in K \Rightarrow K \subset \mathbb{Q}(\sqrt{2}) \ldots (2)$

$\Rightarrow \mathbb{Q}(\sqrt{2}) = K = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$ $\sqrt{2}$ ve $\mathbb{Q}$ yü kapsayan en küçük cisimdir.

TANIM : E/F ve $a \in E$ olsun. Eğer $P(a)=0$ olacak şekilde bir $p(x) \in F[x]$ varsa a'ya (F-üzerinde) cebirsel eleman denir.

örnek// $c \in F$ için $P(X) = X - c \in F[X]$

$P(c) = 0$ c, cebirsel elemandır. //

{ Bir cismin elemanları kendi üzerinde cebirseldir. }

{ Ama cebirsel olmayan elemanlar vardır. }

$\mathbb{R}/\mathbb{Q}$, $\sqrt{2} \in \mathbb{R}$, $x^2 - 2 \in \mathbb{Q}[x] \Rightarrow \sqrt{2}$, $\mathbb{Q}$-cebirseldir.

$\mathbb{C}/\mathbb{Q}$, $i \in \mathbb{C}$, $x^2 + 1 \in \mathbb{Q}[x] \Rightarrow i$, $\mathbb{Q}$-cebirseldir.

$\mathbb{C}/\mathbb{R}$ cebirseldir. $\mathbb{Q} \subset \mathbb{R}$

$\pi \in \mathbb{R}$, e, π; $\mathbb{Q}$-cebirsel değildir.

Cebirsel olmayan elemanlara transandant denir.

$\pi + i\sqrt{2} \in \mathbb{C}$? $\{ \mathbb{Q}[x] \subset \mathbb{R}[x] \}$

$$[x - (\pi + i\sqrt{2})][x - (\pi - i\sqrt{2})] = x^2 - 2\pi x + \pi^2 + 2 \in \mathbb{R}[x]$$

Açıklama: E/F ve $a \in E$ cebirsel olsun.

$\Rightarrow \exists P(X) \in F[X] \underset{\text{öyleki}}{\exists} P(a) = 0$ dır.

$F[X]$, (E.B., T.Ü.İB) TAGB olduğundan $P(x) = q_1(x) q_2(x) \dots q_m(x)$ olacak şekilde $q_i(x) \in F[x]$ asal polinomları vardır. Bu yazılış tek türlüdür.

$P(a) = 0_E = q_1(a) q_2(a) \dots q_m(a)$ $\exists 1 \leq i \leq m$ için $q_i(a) = 0$.

Cisimde sıfır bölen yoktur.

(a'yı kök kabul eden asal polinomu buluyoruz. Asal değilse, asal çarpanlara ayırırız. Cebirsel elemanı kök kabul eden asal polinom bir tanedir. İlgililik farkıyla.)

$q(x), f(x) \in F[x]$ asal ve $\left.\begin{matrix} f(a) = 0 \\ q(a) = 0 \end{matrix}\right\}$ olsaydı;

$ebob(q(x), f(x)) = 1 = r(x) f(x) + s(x) q(x)$ o.ş. $\exists r(x), s(x) \in F[x]$.

$x = a$ alırsak; $1 = r(a) \underbrace{f(a)}_{0} + s(a) \underbrace{q(a)}_{0} = 0$ #

Cismin birimi sıfırına eşit olamaz.

O halde asal polinom bir tanedir.

$$q(x) = b_0 + b_1 x + b_2 x^2 + \dots + b_n x^n \in F[x] \text{ asal}, \quad q(a) = 0$$

$$\Rightarrow q(x) = \underset{\substack{\downarrow \\ \text{aritmetik birim}}}{b_n}\Big(\underbrace{\frac{b_0}{b_n} + \frac{b_1}{b_n}x + \frac{b_2}{b_n}x^2 + \dots + x^n}_{\text{monik polinom } !! \, k(x)}\Big) \quad \Rightarrow q(x) = b_n \cdot k(x)$$

$$\Rightarrow q(x) \approx k(x) \quad \Rightarrow k(x) \text{ asaldır.} \quad k(a) = 0$$

TANIM: F üzerinde cebirsel, $a \in E$ nin sağladığı asal ve monik polinoma, a'nın F üzerinde sağladığı (a'yı kök kabul eden) polinom veya a'nın minimal polinomu denir.

$P_F(a,x)$ ile gösterilir.

$d^\circ P_F(a,x) :=$ a'nın F üzerindeki derecesi. 8.10.96/SALI

Önerme: $\forall f(x) \in F[x]$ için $f(a) = 0 \Rightarrow P_F(a,x) \mid f(x)$.

(a, herhangi bir polinomun köküyse, minimal polinom onu böler.)

İspat// Kabul edelim ki, $P_F(a,x) \nmid f(x)$ olsun.

$\Rightarrow \text{ebob}(P_F(a,x), f(x)) = 1$ dir.

$1 = q(x) f(x) + r(x) P_F(a,x)$ o.ş. $\exists\, q(x), r(x) \in F[x]$.

$1 = q(a) \underbrace{f(a)}_{0} + r(a) \underbrace{P_F(a,a)}_{0}$ $(x = a$ alarak$)$

$1 = 0$ #

O halde kabulümüz yanlıştır. Yani $P_F(a,x) \mid f(x)$ olur.

TANIM: E/F olsun. E bir F-vektör uzayıdır.

$[E:F] := \text{Boy}_F E$ ifadesine, E'nin F üzerindeki boyutu, veya E/F genişlemesinin mertebesi (derecesi) denir.

1. **Önerme:** E/F ve $a \in E$ cebirsel ve $d^\circ P_F(a,x) = n \geq 1$ olsun.

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

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

Örnek// $[\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}] = 5$ tir. Çünkü:

$P_{\mathbb{Q}}(a,x) = x^5 - 2 \in \mathbb{Q}[x]$ monik polinomudur. Asallığına bakalım.

X^5-2 monik polinomu asaldır. Çünkü, Eisenstein kriterini uygularsak; $\mathbb{Q}$, TAGB ve polinomun katsayılarının ebob'u 1 dir. Yani $c(f)=1$ (ilkel) dir. $2\in\mathbb{Q}$ asal elemanı için,

i- $2 \mid a_0, a_1, a_2, a_3, a_4$ $\quad a_0=(-2) \quad a_1=0=a_2=a_3=a_4$

ii- $2 \nmid a_n$ $\quad a_n=1$

iii $2^2 \nmid a_0$ $\quad a_0=-2$

Eisenstein kriteri şartları sağlandığı için X^5-2 polinomu asaldır.

Ayrıca $\sqrt[5]{2}\in\mathbb{Q}(\sqrt[5]{2})$ cebirseldir. Teoreme göre, taban olarak;

$\{1, \sqrt[5]{2}, \sqrt[5]{4}, \sqrt[5]{8}, \sqrt[5]{16}\}$ alınabilir. //

Örnek // $a=\sqrt{2}+\sqrt{3} \Rightarrow P(a)=0$ polinomunu bulalım.

$a^2=(\sqrt{2}+\sqrt{3})^2=2+2\sqrt{6}+3$

$a^2-5=2\sqrt{6}$

$(a^2-5)^2=24 \Rightarrow a^4-10a^2+25=24$

$\Rightarrow a^4-10a^2+1=0 \Rightarrow P(X)=X^4-10X^2+1$ //

9.10.96/Çarşamba

İspat // $\{1, a, a^2, \dots, a^{n-1}\}$ lineer bağımlı olsaydı;

$\exists\, k_0, k_1, \dots, k_{n-1} \overset{\text{vardır ki}}{\exists} (k_0, k_1, \dots, k_{n-1})\neq(0,0,\dots,0)$ } hepsi sıfır değil bazıları sıfır.

$\Rightarrow k_0.1+k_1a+k_2a^2+\dots+k_{n-1}a^{n-1}=0$

$P(X)=k_0+k_1X+k_2X^2+\dots+k_{n-1}X^{n-1}\in F[X]$ $\quad P(a)=0$ dır.

Halbuki $\underset{d^\circ=n-1}{P_F(a,X)} \mid \underset{d^\circ=n}{P(X)}$ olamaz. #

O halde verilen taban lineer bağımsızdır.

E'nin, F ve a'yı kapsayan alt halkalarının arakesiti $F[a]$ olsun. Bu halka;

$F[a]=\{d_0+d_1a+d_2a^2+\dots+d_{n-1}a^{n-1} \mid d_i\in F, i=1,2,\dots,n-1\}$

şeklindedir. Şimdi bu eşitliği, kapsamalarla gösterelim.

$K:=\{d_0+d_1a+d_2a^2+\dots+d_{n-1}a^{n-1} \mid d_i\in F\}$

olsun.

$F[a] \underset{\supseteq}{\overset{\subseteq}{=}} K$?

$\subset$: $i-\ a\in K$
$ii-\ F\subset K$
$iii-\ K$, E'nin alt halkasıdır. $\left\{\begin{array}{l}\forall\alpha,\beta\in K,\\ \alpha-\beta\in K\\ \alpha.\beta\in K\end{array}\right\}$ $\Rightarrow F[a]\subset K$ arakesiti oluşturan her küme $F[a]$'yı kapsar.

$\supset$: $\forall\alpha=d_0+d_1a+d_2a^2+\dots+d_{n-1}a^{n-1}\in K$ elemanı $F[a]$'da olmalıdır.

$d_i\in F\subset F[a]\Rightarrow d_i\in F[a] \quad i=1,2,\dots,n-1$

$a\in F[a]\Rightarrow a,a^2,\dots,a^{n-1}\in F[a]$

$\Rightarrow \alpha\in F[a]$ (kapalılıktan dolayı) $\Rightarrow K\subset F[a]$

Bu ise, $F[a]=K$ demektir. $F[a]$ olarak gösterdiğimiz bu halkanın, aynı zamanda bir cisim olduğunu gösterelim.

$$\varphi : F[X]\longrightarrow F[a]$$
$$P(X)\longrightarrow \varphi(P(X)):=P(a)$$

φ dönüşümü bir epimorfizmadır. (örten, homomorfizma)

$F[X]/\text{çek}\,\varphi\cong F[a]$ olur. (homomorfizma teoreminden)

- $\forall p(x),q(x)\in F[x]$; $p(x)=q(x)\Rightarrow\varphi(p(x))=\varphi(q(x))$
$\Rightarrow p(a)=q(a)$ $\therefore \varphi$ iyi tanımlıdır.

- $\varphi(p(x)+q(x))=\varphi((p+q)(x))=(p+q)(a)=p(a)+q(a)$
$=\varphi(p(x))+\varphi(q(x))$

$\varphi(p(x).q(x))=\varphi((p.q)(x))=(p.q)(a)=p(a).q(a)$
$=\varphi(p(x)).\varphi(q(x))$ $\therefore \varphi$ homomorfizmadır.

- $a\in F[a]$ için $p(x)=a$ sabit polinomu alınırsa,

$\varphi(p(x))=p(a)=a$ olur. $\therefore \varphi$ örtendir.

$\Rightarrow \varphi$ bir epimorfizmadır. Şimdi çekφ'yi bulalım.

$P(X)\in \text{Çek}\varphi\Rightarrow\varphi(P(X))=P(a)=0$

$\Rightarrow P_F(a,X)\mid P(X)$ (teoremden)

$\Rightarrow P(X)=P_F(a,X).h(X)$ o.ş. $\exists\, h(X)\in F[X]$.

$\Rightarrow P(X)\in\langle P_F(a,X)\rangle$

$\Rightarrow \text{çek}\,\varphi=\underbrace{\langle P_F(a,X)\rangle}_{\text{minimal polinomun ürettiği ideal}}$.

Minimal polinom asaldır. Asal idealin ürettiği polinom da asaldır.

TÜİB de asal ideal maksimaldir.

$F[X]$ T.B idi. $\Rightarrow F[X]/<P_F(a,X)>$ cisim olur.

O halde buna izomorf olan $F[a]$ da cisimdir.

$$F(a) = F[a] = \{d_0 + d_1 a + d_2 a^2 + \dots + d_{n-1} a^{n-1} \mid d_i \in F\} \quad i=1,2,\dots,n-1$$

Bu $F(a)$ cismine, F'ye a katmakla elde edilen basit genişleme denir.

(Bir eleman katmakla elde edilen cisime basit genişleme denir.)

$\mathbb{Q}(\sqrt{2})$ basit cisim, $\mathbb{Q}(\sqrt{2}+\sqrt[3]{2})$ basit cisim

$\mathbb{Q}(\sqrt{2},\sqrt[3]{2})$ basit cisim değil.

TANIM: E/F olsun. E'nin her elemanı F üzerinde cebirsel ise bu genişlemeye cebirsel genişleme denir.

Örnek// $\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2} \mid a,b\in\mathbb{Q}\}$ için; $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ cebirsel genişlemedir.

$a=1+\sqrt{2}$ cebirseldir. $P(X)=X^2-2X-4$ ve $P(a)=0$ dır.

$\forall \alpha = a+b\sqrt{2}$, $\alpha^2-\underset{\in\mathbb{Q}}{2a}\alpha+\underset{\in\mathbb{Q}}{a^2-2b^2}=0$, $\forall\alpha\in\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}$ da cebirsel.

$x^2-2aX+(a^2-2b^2)\in\mathbb{Q}[X]$ olur.

2. Önerme: E/F olsun. $[E:F]=$ sonlu ise E, F'nin cebirsel genişlemesidir.

İspat// $[E:F]=n<\infty$ olsun.

$\Rightarrow$ E'nin en fazla n-tane lineer bağımsız elemanı vardır.

$\forall a\in E$ alalım. $1,a,a^2,\dots,a^n\in E$'nin $(n+1)$-tane elemanı olduğundan lineer bağımlıdır. Yani; (hepsi birden sıfır olmayan)

$\exists c_0,c_1,\dots,c_n \underset{\text{vardır}}{\exists}$ $(c_0,c_1,\dots,c_n)\neq(0,0,\dots,0)$ ki,

$c_0.1+c_1.a+c_2a^2+\dots+c_na^n=0$ dır.

$\Rightarrow P(X):=c_0+c_1X+c_2X^2+\dots+c_nX^n\in F[X]$, $P(a)=0$

$\therefore$ a, F-üzerinde cebirseldir.

Herhangi bir a elemanı F üzerinde cebirsel olduğundan, bunu her eleman için söyleyebiliriz. Yani her eleman F-cebirseldir.

★ (Sonlu genişlemeler cebirseldir.)

Önerme : $[E:F]=1 \iff E=F$ dir.

ispat// $\Rightarrow$: $\forall\, 0 \neq a \in E$ alalım. $\{a\}$, E'nin bir F-tabanıdır.

$\forall e \in E$, $e = c.a$ olacak şekilde $\exists c \in F$.

$1 = c_1.a$ o.ş. $\exists c_1 \in F$. $F \subset E$ ($E \subset F$ açık)

$\Rightarrow a = c_1^{-1} \in F$ olur. Buradan $E=F$ olur.

cisimde birim tektir.
Üst cismin birimiyle alt cismin birimi aynıdır.
Halkalarda ise farklıdır.

$\Leftarrow$: Açıktır.

3. Önerme : $E \subset F \subset G$ üç cisim olsun.

$[F:E]$ ve $[G:F]$ sonlu ise $[G:E]$ de sonludur.

Ve $[G:E] = [G:F].[F:E]$

dir.

$$\mathbb{Q} \subset \overset{\text{sonsuz}}{\cdots\cdots} \subset \mathbb{R} \underset{\neq}{\subseteq} \overset{\sim\text{yok}\sim}{K} \underset{\neq}{\subseteq} \mathbb{C}$$

$\mathbb{C} = \mathbb{R}(i)$, $P_{\mathbb{R}}(i,X) = X^2+1$ asal, monik

$[\mathbb{R}(i):\mathbb{R}] = 2$ $\{1,i\}$ tabandır.

$\mathbb{R}(i) = \{a+bi \mid a,b \in \mathbb{R}\} = \mathbb{C}$

$$[\mathbb{C}:\mathbb{R}] = 2 = \underbrace{[\mathbb{C}:K]}_{2}.\underbrace{[K:\mathbb{R}]}_{1}$$

önceki önermeden $K=\mathbb{R}$ olurdu

$\underbrace{\quad}_{1}$ $\underbrace{\quad}_{2}$ $\mathbb{C}=K$ olurdu.

$\Rightarrow$ $\mathbb{R}$ ile $\mathbb{C}$ arasında hiçbir cisim olamaz.

ispat// $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ G'nin bir F-tabanı,
$\{\beta_1,\beta_2,\ldots,\beta_m\}$ F'nin bir E tabanı, $\Rightarrow$

$\Rightarrow \{\alpha_i\beta_j \mid 1 \leq i \leq n,\ 1 \leq j \leq m\}$ kümesi de G'nin bir E-tabanıdır.

$\forall x \in G$ alalım. (lineer bağımsız ve G yi E üzerinde üretmeli)

$x = c_1\alpha_1 + c_2\alpha_2 + \ldots + c_n\alpha_n$ o.ş. $\exists c_i \in F$. $\forall i = 1,2,\ldots,n$ için

$c_i = a_{i1}\beta_1 + a_{i2}\beta_2 + \ldots + a_{im}\beta_m$ o.ş. $\exists a_{ij} \in E$ $(\forall j = 1,2,\ldots,m)$

$x = (a_{11}\beta_1 + a_{12}\beta_2 + \ldots + a_{1m}\beta_m)\alpha_1 + \ldots + (a_{n1}\beta_1 + a_{n2}\beta_2 + \ldots + a_{nm}\beta_m)\alpha_n$

$\Rightarrow$ (skalerler) $a_{ij} \in E$ ve x 'de $\alpha_i\beta_j$ şeklinde yazıldı.

$$x = \sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}\alpha_i\beta_j$$ G'yi E üzerinde üretir.

Şimdi lineer bağımsızlığı gösterelim.

$$\sum_{i=1}^{n}\sum_{j=1}^{m} c_{ij}\alpha_i\beta_j = 0 \Rightarrow \sum_{i=1}^{n}\Big(\underbrace{\sum_{j=1}^{m} c_{ij}\beta_j}_{A_i}\Big)\alpha_i = 0$$

$$\Rightarrow \sum_{i=1}^{n} A_i\alpha_i = 0 \quad \Rightarrow \forall i \text{ için } A_i = 0 \text{ dır.}$$

F'de lineer bağımsız. $\Rightarrow A_i = \sum_{j=1}^{m} c_{ij}\beta_j = 0 \Rightarrow \forall i,j,\ c_{ij} = 0.$

Sonuç: $[G:E] = n.m = [G:F].[F:E]$ dir.

Sonuç 1: α_1, α_2 F-cebirsel ise $F(\alpha_1,\alpha_2)$, F üzerinde sonlu ve cebirseldir.

1\. önermeden dolayı, α_1 cebirsel ise $[F(\alpha_1):F]$ = sonlu

$F[x] \subset F(\alpha_1)[x]$ olduğundan, α_2 F-cebirsel ise aynı zamanda
$\{F \subset F(\alpha_1)\}$
$F(\alpha_1)$-cebirseldir. Benzer şekilde;

$[F(\alpha_1,\underline{\alpha_2}):F(\alpha_1)] = \underset{\text{ön 1.}}{\underline{\text{sonlu}}}$ ve $\underset{\text{ön. 2}}{\underline{\text{cebirsel}}}$. $\quad F \subset F(\alpha_1) \subset F(\alpha_1,\alpha_2)$ olduğundan

{F(α₁)'e cebirsel eleman katarak}

önerme 3'den,

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

önerme 2 den, sonlu genişlemeler cebirseldir.

Sonuç 2: $\alpha_1, \alpha_2, \ldots, \alpha_n$ F-cebirsel iseler, $F(\alpha_1,\alpha_2,\ldots,\alpha_n)$'de F üzerinde sonlu ve cebirseldir.

Tümevarım ile ispatlayalım. n=1 ve n=2 için doğru olduğu biliniyor, n için doğru olduğunu kabul edelim. n+1 için de ifade doğru ise önerme doğru olur.

$F(\alpha_1,\alpha_2,\ldots,\alpha_n,\alpha_{n+1})$; F üzerinde sonlu ve cebirseldir ?

α_{n+1}; F-cebirsel ise $F[x] \subset F(\alpha_1,\alpha_2,\ldots,\alpha_n)[x]$ olduğundan α_{n+1}; $F(\alpha_1,\alpha_2,\ldots,\alpha_n)$-cebirseldir.

$F(\alpha_1,\alpha_2,\ldots,\alpha_n,\alpha_{n+1})$; $F(\alpha_1,\alpha_2,\ldots,\alpha_n)$ üzerinde sonludur.

$$\Rightarrow \underbrace{[F(\alpha_1,\alpha_2,\ldots,\alpha_{n+1}):F]}_{\text{sonlu cebirseldir.}} \Leftarrow \underbrace{[F(\alpha_1,\alpha_2,\ldots,\alpha_{n+1}):F(\alpha_1,\alpha_2,\ldots\alpha_n)]}_{\text{sonlu cebirsel}}.\underbrace{[F(\alpha_1,\ldots,\alpha_n):F]}_{\text{sonlu cebirsel}}$$

olur.

Sonuç 3: α ve β, F-cebirsel iseler;

$\alpha \mp \beta$, $\alpha . \beta$, $\frac{\alpha}{\beta}$ $(\beta \neq 0)$ F-cebirseldir.

{ $F(\alpha,\beta)$, F üzerinde cebirseldir. $\alpha \mp \beta$, $\alpha . \beta$, $\frac{\alpha}{\beta}$ $(\beta \neq 0) \in F(\alpha,\beta)$ F-cebirseldir. }

} $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5},\sqrt{7},\ldots)$ $\alpha+\beta$, $\alpha . \beta$, $\frac{\alpha}{\beta}$ Q-cebirseldir. }

1. Uygulama

1 - $F(a)$'nın F üzerinde sonlu olması için gerek ve yeter koşul, a'nın F üzerinde cebirsel olmasıdır. Gösteriniz.

Çözüm // $\Rightarrow$: $[F(a):F]=n$ (sonlu) olsun.

$1, a, a^2, \ldots, a^n$; $F(a)$'nın $n+1$ tane elemanı olduğundan, F üzerinde lineer bağımlı olurlar. O halde,

$$a_0 + a_1 a + a_2 a^2 + \ldots + a_n a^n = 0$$

olacak şekilde hepsi birden sıfır olmayan $a_i \in F$ $(i=0,1,\ldots,n)$ katsayıları bulunabilir. Bu ise a'nın sıfırdan farklı, $f(x)=a_0+a_1X+\ldots+a_nX^n \in F[X]$ polinomunun kökü olması demektir. Bu ise a'nın cebirsel olmasıdır.

$\Leftarrow$: a, F üzerinde cebirsel eleman olsun. Tanımdan, $f(a)=0$ olacak şekilde, sıfır polinomdan farklı bir,

$$\underline{f(x)=a_0+a_1X+a_2X^2+\ldots+a_nX^n} \in F[X]$$

polinomu bulunabilir. $F[X]$'de a'nın kök olduğu asal ve monik polinom (a'nın minimal polinomu) $P_F(a,X)$ alınırsa, $[F$ [illegible] $:F]=d^\circ P_F(a,X)$-in sonlu olduğu görülür. (Bak: 1. önerme)

2- a- $X^2-3 \in \mathbb{Q}(\sqrt{2})[X]$ polinomu asaldır. Gösterin.

Çözüm // $X=\mp\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ olduğundan bu polinom $\mathbb{Q}(\sqrt{2})[X]$ de asaldır.

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

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

$P_{\mathbb{Q}}(\sqrt{2},X)=X^2-2 \in \mathbb{Q}[X]$ de asal, monik $X=\mp\sqrt{2} \in \mathbb{Q}$

$d^\circ P_{\mathbb{Q}}(\sqrt{2},X)=2$

$P_{Q(\sqrt{2})}(\sqrt{3},X) = X^2-3$ monik, asal. $d^\circ P_{Q(\sqrt{2})}(\sqrt{3},X) = 2$

$\Rightarrow [Q(\sqrt{2},\sqrt{3}):Q] = 2.2 = 4$ bulunur.

c - $Q(\sqrt{2},\sqrt{3})$ ün Q tabanını bulun.

Çözüm// (Bk. Önerme 3. ispatı)

$E \subset F \subset G$ olsun.

$$\left.\begin{array}{l} \{\alpha_1,\alpha_2,\ldots,\alpha_n\} \text{ G'nin bir F-tabanı} \\ \{\beta_1,\beta_2,\ldots,\beta_m\} \text{ F'nin bir E-tabanı} \end{array}\right\} \Rightarrow \{\alpha_i\beta_j \mid 1\leq i\leq n, 1\leq j\leq m\}$$

kümesi, G'nin E-tabanıdır.

Buna göre; $Q \subset Q(\sqrt{2}) \subset Q(\sqrt{2},\sqrt{3})$ ve

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

$$\left.\begin{array}{l} \{1,\sqrt{3}\} \ Q(\sqrt{2},\sqrt{3})\text{'ün } Q(\sqrt{2})\text{-tabanı} \\ \{1,\sqrt{2}\} \ Q(\sqrt{2}) \text{ nin } Q\text{-tabanı} \end{array}\right\} \Rightarrow \{1,\sqrt{2},\sqrt{3},\sqrt{6}\} \text{ kümesi,}$$

$Q(\sqrt{2},\sqrt{3})$'ün Q tabanıdır.

3 - $n_1,n_2,\ldots,n_r$ farklı tamsayılar olsunlar.

a- $[Q(\sqrt{n_1},\sqrt{n_2},\ldots,\sqrt{n_r}):Q] \leq 2^r$ olduğunu gösteriniz. ($n_i \in N$, $1 \leq i \leq r$)

Çözüm// $[Q(\sqrt{n_1},\sqrt{n_2},\ldots,\sqrt{n_r}):Q] \leq 2^r$ için, tümevarımı kullanalım.

$r=1 \Rightarrow [Q(\sqrt{n_1}):Q] \leq 2$

$n_1 \neq a^2 \Rightarrow [Q(\sqrt{n_1}):Q] = 2 \leq 2$, $\{1,\sqrt{n_1}\}$ tabandır.

$n_1 = a^2 \Rightarrow [\underbrace{Q(\sqrt{n_1})}_{Q}:Q] = [Q:Q] = 1 < 2$

r için doğru olsun. $r+1$ için de doğru ise ispat biter.

$\Rightarrow [Q(\sqrt{n_1},\sqrt{n_2},\ldots,\sqrt{n_r}):Q] \leq 2^r$ için doğru olsun.

$[Q(\sqrt{n_1},\sqrt{n_2},\ldots,\sqrt{n_r},\sqrt{n_{r+1}}):Q] \leq 2^{r+1}$ olur mu bakalım.

$Q \subset Q(\sqrt{n_1},\sqrt{n_2},\ldots,\sqrt{n_r}) \subset Q(\sqrt{n_1},\sqrt{n_2},\ldots,\sqrt{n_r},\sqrt{n_{r+1}})$

$$[Q(\sqrt{n_1},\sqrt{n_2},\ldots,\sqrt{n_{r+1}}):Q] = \underbrace{[Q(\sqrt{n_1},\ldots,\sqrt{n_{r+1}}):Q(\sqrt{n_1},\ldots,\sqrt{n_r})]}_{2}.\underbrace{[Q(\sqrt{n_1},\ldots,\sqrt{n_r}):Q]}_{2^r}$$

$\leq 2.2^r = 2^{r+1}$

$\Rightarrow [Q(\sqrt{n_1},\sqrt{n_2},\ldots,\sqrt{n_r}):Q] \leq 2^r$ dir. //

b- Yukarıdaki eşitsizlik, kesin eşitsizlik olabilir mi?

Çözüm // $n_i, (1 \leq i \leq r)$ kare çarpanlı bir sayı ise bu eşitsizlik, kesin eşitsizlik olabilir.

4- birin sekizinci primitif kökü ($\xi = e^{\frac{2\pi i}{8}}$) olsun.

a- $(\xi + \xi^{-1})^2 = 2$ olduğunu gösterin.

Çözüm // $\alpha^n = 1, \quad 1 \leq k < n, \alpha^k \neq 1$

$$\alpha = e^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} \qquad (e^{i\theta} = \cos\theta + i\sin\theta)$$

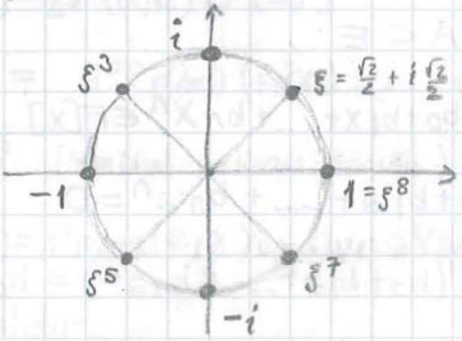
$$\xi = e^{\frac{2\pi i}{8}} = \cos\frac{2\pi}{8} + i\sin\frac{2\pi}{8} = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$$

$\xi^8 = 1$ dir.

$\xi^0 = 1, \xi = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}, \xi^2 = i$

$\xi^3 = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}, \xi^4 = -1$

$\xi^5 = -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}, \xi^6 = -i, \xi^7 = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$



$\xi^8 = 1$

$$\xi^2 = e^{2 \cdot \frac{2\pi i}{8}} = e^{\frac{\pi i}{2}} = \cos\frac{\pi}{2} + i\sin\frac{\pi}{2} = i$$

$$\xi^{-2} = e^{-2\frac{2\pi i}{8}} = e^{-\frac{\pi i}{2}} = \cos(-\tfrac{\pi}{2}) + i\sin(-\tfrac{\pi}{2}) = (-\sin\tfrac{\pi}{2})i = -i$$

$\Rightarrow (\xi + \xi^{-1})^2 = \xi^2 + 2\xi.\xi^{-1} + \xi^{-2} = i + 2 - i = 2$ bulunur.

b- $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\xi)$ olduğunu gösterin.

Çözüm // $(\xi + \xi^{-1})^2 = 2 \Rightarrow \xi + \xi^{-1} = \sqrt{2} \in \mathbb{Q}(\xi) \Rightarrow \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\xi)$ dir.

c- $[\mathbb{Q}(\xi) : \mathbb{Q}(\sqrt{2})] = ?$

Çözüm // $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\xi)$

$$[\underset{\smile}{\mathbb{Q}(\xi) : \mathbb{Q}}] = [\mathbb{Q}(\xi) : \mathbb{Q}(\sqrt{2})].[\underset{\sim}{\mathbb{Q}(\sqrt{2}) : \mathbb{Q}}]$$

$P_{\mathbb{Q}}(\sqrt{2}, X) = X^2 - 2$ monik, asal $\quad d^0 P_{\mathbb{Q}}(\sqrt{2}, X) = 2$

$\xi^8 = 1 \Rightarrow \xi^8 - 1 = 0$ olur. $\quad$ ($X^8 - 1$ monik, asal değil)

$X^8 - 1 = (X^4 - 1)(\underset{\sim}{X^4 + 1})$ $\quad \{(X^4+1)\ \mathbb{Q}[X]$ de asaldır.$\}$

$\Rightarrow X^8 - 1 = (X^2 - 1)(\underset{\sim}{X^2 + 1})(X^4 + 1)$ $\quad \{(X^2+1)\ \mathbb{Q}[X]$ de asaldır.$\}$

$\Rightarrow X^8 - 1 = (X-1)(X+1)(X^2+1)(\underset{\sim}{X^4+1})$

ξ, $X^4 + 1$ in bir köküdür. $\quad \xi^4 + 1 = 0$ dır.

$P_Q(\xi, X) = X^4+1$ $Q[X]$ de asal ve moniktir.

$d^\circ P_Q(\xi,X) = 4$

$$[Q(\xi):Q] = [Q(\xi):Q(\sqrt{2})].[Q(\sqrt{2}):Q]$$

$$4 = [Q(\xi):Q(\sqrt{2})].\ 2$$

$\Rightarrow [Q(\xi):Q(\sqrt{2})] = 2$ bulunur.

5- E/F cebirsel genişleme ve $F \subset A \subset E$ (A-alt halka) ise A cisimdir.

Çözüm // $\forall 0 \neq a \in A$ 'nın tersinin olduğunu göstermeliyiz.

$\forall 0 \neq a \in A \subset E$,

$\exists P(x) = b_0 + b_1 X + \ldots + b_n X^n \in F[X] \underset{\text{öyle ki}}{\ni} P(a) = 0$.

$\Rightarrow b_0 + b_1 a + \ldots + b_n a^n = 0$

$\Rightarrow b_0^{-1}(b_0 + b_1 a + \ldots + b_n a^n) = b_0^{-1}.0$ (b_0^{-1} ile çarparak) A alt halka olduğundan ters eleman vardır.

$\Rightarrow 1 + b_1 b_0^{-1} a + \ldots + b_n b_0^{-1} a^n = 0$

$\Rightarrow 1 = -(b_1 b_0^{-1} a + \ldots + b_n b_0^{-1} a^n)$ $\{\forall a \in A$ ve negatif kuvvetler cisim ise A'nın elemanıdır$\}$

$\Rightarrow a^{-1} = -(b_1 b_0^{-1} + \underbrace{b_2 b_0^{-1} a + \ldots + b_n b_0^{-1} a^{n-1}}_{\in A})$ $\{a^{-1}$ ile çarparak$\}$

$\Rightarrow A$ cisimdir. //

6- $E = F(\alpha, \beta)$, F'nin bir cebirsel genişlemesi ve α, β'nın minimal polinomları $f = P_F(\alpha, X)$, $g = P_F(\beta, X)$ olsun. $Ebob(d^\circ f, d^\circ g) = 1$ ise

a- $[E:F] = d^\circ f . d^\circ g$ olduğunu gösterin.

Çözüm // $F \subset F(\alpha) \subset F(\alpha,\beta) = E$

$$[E:F] = [\underbrace{F(\alpha,\beta):F(\alpha)}_{d^\circ h}].[\underbrace{F(\alpha):F}_{d^\circ f}] = [\underbrace{F(\alpha,\beta):F(\alpha)}_{d^\circ h}].d^\circ f \leq d^\circ f . d^\circ g \ldots (1)$$

$[F(\alpha,\beta):F(\alpha)] = d^\circ \overbrace{P_{F(\alpha)}(\beta,X)}^{h} = d^\circ h$

$h(\beta) = 0 \quad g(\beta) = 0 ;\ g = P_F(\beta, X)$

$\underline{d^\circ P_{F(\alpha)}(\beta,X)} \leq d^\circ g = \underline{d^\circ P_F(\beta,X)}$

$d^\circ h \leq d^\circ g$

$g = x^2 - 2 \in Q[X]$ asal

$g = (X-\sqrt{2})(X+\sqrt{2}) \in Q[\sqrt{2}][X]$

$P_{Q(\sqrt{2})}(\sqrt{2},X) = X - \sqrt{2} = h$

$d^\circ P_{Q(\sqrt{2})}(\sqrt{2},X) = 1 < 2 = d^\circ g$

$g(\sqrt{2}) = h(\sqrt{2}) = 0$

$[E:F]=[F(\alpha,\beta):F(\alpha)].[F(\alpha):F]$

$\Rightarrow d^\circ f \mid [E:F]$ ve $d^\circ g \mid [E:F]$ ve $ebob(d^\circ f, d^\circ g)=1$ ise

$\Rightarrow d^\circ f . d^\circ g \mid [E:F] \Rightarrow d^\circ f . d^\circ g \leqslant [E:F]$ ----- (2)

(1) ve (2) den dolayı ;

$[E:F]=d^\circ f . d^\circ g$ bulunur.

b- g(x) in $F(\alpha)[X]$ de asal olduğunu gösterin.

Çözüm // $\underline{[F(\alpha):F]}.[F(\beta):F]=[E:F]=\underline{[F(\alpha):F]}.[F(\alpha,\beta):F(\alpha)]$

$[F(\beta):F]=[F(\alpha,\beta):F(\alpha)]$

$d^\circ g = d^\circ P_{F(\alpha)}(\beta,X)$ ---- (1) } β'nın F(α) üzerindeki minimal polinomunun derecesi

$\Rightarrow P_{F(\alpha)}(\beta,X) \mid g(x)$ --- (2) (Minimal polinom tanımı)

(1) ve (2) den dolayı ; $g(x)=P_{F(\alpha)}(\beta,X)$ olur. Yani ;

g(x) polinomu, $F(\alpha)[X]$ de asaldır. //

7- $[Q(\sqrt{3},\sqrt[3]{3}):Q]=?$ ve $Q(\sqrt{3},\sqrt[3]{3})=Q(\sqrt[6]{3})$ olduğunu gösterin.

Çözüm // $[Q(\sqrt{3},\sqrt[3]{3}):Q]=[Q(\sqrt{3},\sqrt[3]{3}):Q(\sqrt{3})][Q(\sqrt{3}):Q]$

$P_{Q(\sqrt{3})}(\sqrt[3]{3},X)=X^3-3$ $P_Q(\sqrt{3},X)=X^2-3$

↓ monik, asal ve ↓ monik, asal

$m=d^\circ P_{Q(\sqrt{3})}(\sqrt[3]{3},X)=3$, $d^\circ P_Q(\sqrt{3},X)=2=n$

6/a 'dan dolayı $(m,n)=(3,2)=1$ aralarında asal ve

$[Q(\sqrt{3},\sqrt[3]{3}):Q]=m.n=3.2=6$ olur. //

Şimdi, $Q(\sqrt{3},\sqrt[3]{3})=Q(\sqrt[6]{3})$ olduğunu gösterelim.

$$\underbrace{Q\subset Q(\sqrt[6]{3})\subset Q(\sqrt{3},\sqrt[3]{3})}_{6}$$

$E=F \iff [E:F]=1$ idi. Buna göre ;

$P_Q(\sqrt[6]{3},X)=X^6-3$ 3 asalı için Eisenstein sağlanır.

$\sqrt{3},\sqrt[3]{3}\in Q(\sqrt{3},\sqrt[3]{3})$ ve $\frac{1}{\sqrt[3]{3}}=(\sqrt[3]{3})^{-1}\in Q(\sqrt{3},\sqrt[3]{3})$

$\Rightarrow \sqrt{3}.(\sqrt[3]{3})^{-1}=\underline{\sqrt[6]{3}\in Q(\sqrt{3},\sqrt[3]{3})}$ olduğundan

$Q(\sqrt{3},\sqrt[3]{3})=Q(\sqrt[6]{3})$ bulunur. //

8- $\sqrt{1+\sqrt{3}}$ ün Q üzerinde sağladığı polinomu bulunuz.

Çözüm // $a=\sqrt{1+\sqrt{3}} \Rightarrow a^2=1+\sqrt{3} \Rightarrow a^2-1=\sqrt{3}$

$$\Rightarrow a^4-2a^2+1=3$$

$$\Rightarrow a^4-2a^2-2=0$$

$\Rightarrow P_Q(a,X)=X^4-2X^2-2 \in Q[X]$ olur.

(18/11) 9- a- $[Q(\sqrt{3},\sqrt[3]{2}):Q]=?$

Çözüm // $[Q(\sqrt{3},\sqrt[3]{2}):Q]=[\underbrace{Q(\sqrt{3},\sqrt[3]{2}),Q(\sqrt{3})}][\underbrace{Q(\sqrt{3}):Q}]$.

$f=P_{Q(\sqrt{3})}(\sqrt[3]{2},X)=X^3-2 \qquad g=P_Q(\sqrt{3},X)=X^2-3$

$d^\circ f=3 \qquad d^\circ g=2$

$[Q(\sqrt{3},\sqrt[3]{2}):Q]=d^\circ f.\, d^\circ g=3.2=6$ //

b- $[Q(\underbrace{\sqrt{2}+\sqrt{3}}_{\alpha}):Q(\sqrt{2})]=?$

Çözüm // $P_{Q(\sqrt{2})}(\underbrace{\sqrt{2}+\sqrt{3}}_{\alpha},X)=?$ $\qquad \alpha=\sqrt{2}+\sqrt{3} \Rightarrow \alpha^2=2+2\sqrt{6}+3$

$$\Rightarrow \alpha^2-5=2\sqrt{6}$$

$$\Rightarrow \alpha^4-10\alpha^2+1=0$$

$\Rightarrow P_{Q(\sqrt{2})}(\sqrt{2}+\sqrt{3},X)=X^4-10X^2+1 \in Q(\sqrt{2})[X]$ asal, monik.

$\Rightarrow [Q(\sqrt{2}+\sqrt{3}):Q(\sqrt{2})]=4$ //

c- $[Q(\sqrt{2},\sqrt{3}):Q(\underbrace{\sqrt{2}+\sqrt{3}}_{\alpha})]=?$

Çözüm // $\sqrt{2}+\sqrt{3} \in Q(\sqrt{2},\sqrt{3}) \Rightarrow Q(\sqrt{2}+\sqrt{3}) \subset Q(\sqrt{2},\sqrt{3})$ olur.

$Q \subset Q(\sqrt{2}) \subset Q(\sqrt{2},\sqrt{3})$ ve $P_Q(\sqrt{3},X)=P_{Q(\sqrt{2})}(\sqrt{3},X)=X^2-3$ ve

$[Q(\sqrt{2},\sqrt{3}):Q(\sqrt{2})]=2$ olup, buradan;

$[Q(\sqrt{2},\sqrt{3}):Q]=[\underbrace{Q(\sqrt{2},\sqrt{3}):Q(\sqrt{2})}_{2}][\underbrace{Q(\sqrt{2}):Q}_{2}]=4$ olur.

O halde, $[Q(\sqrt{2},\sqrt{3}):Q] \leq 4$ olur.

$Q \subset Q(\sqrt{2}) \subset Q(\sqrt{2}+\sqrt{3})$ ve $\sqrt{2}+\sqrt{3} \notin Q(\sqrt{2})$ olur. Ve

$[Q(\sqrt{2}+\sqrt{3}):Q(\sqrt{2})] \geq 2$ olup, $[Q(\sqrt{2}+\sqrt{3}):Q] \geq 4$ olur.

Her iki eşitlikten; $[Q(\sqrt{2}+\sqrt{3}):Q]=4$ ve $Q \subset Q(\sqrt{2}+\sqrt{3})$'den

$Q(\sqrt{2}+\sqrt{3})=Q(\sqrt{2},\sqrt{3})$ olur.

O halde : $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2}+\sqrt{3})] = 1$ olur. //

22.10.96
SALI

(18/9) **10- a-** $\mathbb{R}$ gerçel (reel) sayılar cisminin $\dfrac{\mathbb{R}[X]}{\langle X^2+1\rangle \mathbb{R}[X]}$ cisminin bir alt cismine izomorf olduğunu gösterin.

Çözüm // $I = \langle X^2+1 \rangle \subset \underset{E.B.(TÜİB)}{\mathbb{R}[X]}$ $\left\{\begin{array}{l} Mat.3 - S:238 \\ R, E.B \Rightarrow R, TÜİB \Rightarrow R, \text{~~TAGB~~}. \end{array}\right\}$

$\Rightarrow \langle X^2+1\rangle$ asal ideal $\Rightarrow \langle X^2+1\rangle$ maksimal ideal

$\Rightarrow \mathbb{R}[X]/I$ cisimdir.

$f : \mathbb{R} \longrightarrow \mathbb{R}[X]/I$ 1:1, homomorfizma (monomorfizma) ise ispat biter.

$a \longrightarrow f(a) := a + I$

a = sabit polinom. $a+I$ = I idealine göre denklik sınıfı. $\forall a,b \in \mathbb{R}$;

- $a = b \Rightarrow a+I = b+I \Rightarrow f(a) = f(b)$ $\therefore f$, iyi tanımlıdır. //
- $f(a+b) = (a+b) + I = (a+I) + (b+I) = f(a) + f(b)$
  $f(a.b) = (a.b) + I = (a+I).(b+I) = f(a).f(b)$ $\Big\}$ $\therefore f$, homomorfizma. //
- $f(a) = f(b) \Rightarrow a+I = b+I \Rightarrow a-b \in I$
- $\therefore f$ örtendir. //

$\Rightarrow (a-b) = (X^2+1)\,P(X)$ o.ş. $P(X)$ yok.

$\Rightarrow a-b = 0$

$\Rightarrow a = b$ $\therefore f$, 1:1 dir. //

O halde, $\mathbb{R} \cong f(\mathbb{R}) \subset \mathbb{R}[X]/I$ olur. //

$f : \mathbb{R} \longrightarrow \mathbb{R}[X]/I = \{(aX+b)+I \,/\, a,b \in \mathbb{R}\}$.

$\Big\{ f(\mathbb{R}) = I \Rightarrow \text{çek} f \neq \{0\}$ dir.

$\Rightarrow f$ 1:1 değildir.

// müşö.

$\varphi : \overset{cisim}{F} \longrightarrow \overset{halka}{R}$

$\text{çek}\,\varphi \subset F$

$\Rightarrow \text{çek}\,\varphi = \{0\} \vee \text{çek}\,\varphi = F$

$\Rightarrow \varphi(F) = \{0_S\}$

her elemanın görüntüsü

b- $f : \mathbb{C} \longrightarrow \mathbb{R}[X]/I$

$(a+ib) \longrightarrow f(a+ib) := (a+bX) + I$ $\qquad I = \langle X^2+1\rangle$

dönüşümü altında $\mathbb{C} \cong \mathbb{R}[X]/I$ olduğunu gösterin.

Çözüm // $(a+bi), (c+di) \in \mathbb{C}$,

- $f[(a+bi)+(c+di)] = f[(a+c)+(b+d)i]$

$= [(a+c)+(b+d)X] + I = [(a+bX)+(c+dX)] + I$

$= [(a+bX)+I] + [(c+dX)+I]$

$= f(a+ib) + f(c+di)$

$$f[(a+ib).(c+di)] = f[(ac-bd)+(ad+bc)i]$$

$$= f[(ac+bdi^2)+(ad+bc)i]$$

$$= f[ac+(ad+bc+bdi)i]$$

$$= ac+(ad+bc+bdi)X + I$$

$$= f[(ac+adX+bcX)+(bdX)i]$$

$$= ac+adX+bcX+bdX^2 + I$$

$$= (a+bX)(c+dX)+I$$

$$= [(a+bX)+I][(c+dX)+I]$$

$= f(a+ib).f(c+id)$ ∴ f homomorfizmadır.

- $\forall\ (a+bX)+I \in \mathbb{R}[X]/I$ için $f(a+ib)=(a+bX)+I$ o.ş. $(a+ib)\in\mathbb{C}$ vardır.

  ∴ f, örtendir.

- ∴ f, 1:1 dir.

  $\Rightarrow \mathbb{C} \overset{\wedge}{=} \mathbb{R}[X]/I$ olur. f bir izomorfizmadır. //

11 - a - $\varphi : Q(x) \longrightarrow Q(\sqrt{2})$

$P(x) \longrightarrow \varphi(P(x)) = P(\sqrt{2})$ epimorfizmadır. Gösterin. (Mat.3-S:251)

Çözüm // • $\varphi(P(x) \dotplus q(x)) = \varphi((P\dotplus q)(x)) = (P\dotplus q)(\sqrt{2}) = P(\sqrt{2}) \dotplus q(\sqrt{2}) = \varphi(P(x)) \dotplus \varphi(q(x))$

$(\forall\ P(x), q(x) \in Q[X])$ ∴ φ homomorfizmadır.

• $\sqrt{2} \in Q(\sqrt{2})$ için, $P(x)=\sqrt{2}$ sabit polinomu alınırsa ;

$\varphi(P(x)) = P(\sqrt{2}) = \sqrt{2}$ ∴ φ örtendir.

$\Rightarrow \varphi$, epimorfizmadır. $\text{çek}\,\varphi = \langle X^2-2\rangle$ (Mat 3 - S:252)

Homomorfizma teoremi gereğince ; (Mat 3 - S:220)

$Q[X]/\langle X^2-2\rangle \overset{\wedge}{=} Q[\sqrt{2}]$ olur. //

$P(x) \in \text{çek}\,\varphi \Rightarrow \varphi(P(x)) = P(\sqrt{2}) = 0$

$\Rightarrow P_{Q}(\sqrt{2},x) \mid P(x)$

$\Rightarrow P(x) = P_{Q}(\sqrt{2},x)h(x)$ o.ş $\exists h(x) \in Q[X]$

$\Rightarrow P(x) \in \langle P_{Q}(\sqrt{2},x)\rangle \Rightarrow \text{çek}\,\varphi = \langle X^2-2\rangle$

2. Parçalanış Cisimleri ve Normal Genişlemeler

F cisim ⇒ F[x] E.B idi. (Mat-3. S:238) Bölme algoritması uygulayarak $f(x) \in F[x]$ polinomunun F cisminde en çok $d^o f = n$ tane sıfırı olabileceği gösterilebilir. Eğer f(x) asal ise f(x) in F de kökü yoktur. Çünkü $\alpha_1 \in F$, f(x) in bir kökü olsaydı ; $x - \alpha_1$ ile bölünürdü.

Bu bölümde ; F cismini, $\mathbb{Q}$ cisminin genişlemesi olarak alacağız.

$f(x) = (x^2-2) = \underbrace{(x-\sqrt{2})}_{\mathbb{Q}(\sqrt{2})[x]}(x+\sqrt{2})$ in polinomlarıdırlar.

Bir polinomu en küçük nerede parçalıyabiliyoruz. Bunu araştıracağız.

- F cisim ⇒ F[x] $\underset{\text{(zengin halka)}}{\text{E.B.}}$ dir.
- $p(x) \in F[x]$, $d^o p = n$ iken p(x)'in en fazla n-tane kökü vardır.
- $p(x) \in F[x]$'de asal ise F de hiçbir kökü yoktur. Lineer çarpanlara ayrılamaz. $\overset{\text{cisim}}{F}/\mathbb{Q}$ $F = \mathbb{Q}$ veya $\mathbb{Q} \subset F$ dir.

Teorem : $f(x) \in F[x]$ olsun. Bu taktirde f(x)'in bir kökünü bulunduran, F'nin bir E genişlemesi vardır. (Varlığı gösteren teorem).

$\exists E/F \underset{\text{öyle ki}}{\exists} f(a) = 0$ o.ş. $\exists a \in E$.

- F'yi kapsayan E cismi bulacağız.

- E'de bir eleman bulacağız ki, $f(x) \in F[x]$ kökü olacak.

İspat // $f(x) = p_1(x)\, p_2(x) \dots p_k(x)$ $\quad p_i(x) \in F[x]$

$f(x) \in F[x]$ asal alabiliriz. Çünkü $p_1(x)$, f(x)'in bir asal böleni ise, $p_1(x)$'in bir kökü f(x)'in de köküdür. Genelleştirme ile $p_i(x)$'ler asal olur. O halde f(x)'de asaldır.

$f(x)$ asal ⇒ $\langle f(x) \rangle$ asal idealdir.

⇒ $\langle f(x) \rangle$ maksimal idealdir (F[x] E.B ⇒ TÜİB. dir)

⇒ $F[x]/\langle f(x) \rangle$ cisimdir.

$$\varphi : F \longrightarrow F[x]/\langle f(x) \rangle$$
$$a \longrightarrow \varphi(a) := a + \langle f(x) \rangle$$

φ monomorfizmadır.

$F \cong \underset{\substack{\downarrow \text{cisim} \\ \text{hom. altında} \\ \text{görüntü.}}}{\varphi(F)} \subset F[x]/\langle f(x) \rangle =: E$ $\quad$ { F ile φ(F) nin elemanları farklıdır. }

⇒ E/F dir.

$$f(x) = a_0 + a_1X + a_2X^2 + \dots + a_mX^m \in F[x]$$

Diğer taraftan $\alpha := x + \langle f(x)\rangle \in E$ ve buradan ;

$$f(\alpha) = a_0 + a_1(X+\langle f(x)\rangle) + a_2(X+\langle f(x)\rangle)^2 + \dots + a_m(X+\langle f(x)\rangle)^m$$

$$= (a_0+\langle f(x)\rangle) + (a_1+\langle f(x)\rangle)(X+\langle f(x)\rangle) + (a_2+\langle f(x)\rangle)(X^2+\langle f(x)\rangle) + \dots$$

$$\dots + (a_m+\langle f(x)\rangle)(X^m+\langle f(x)\rangle)$$

$$\Rightarrow f(\alpha) = (a_0+a_1X+a_2X^2+\dots+a_mX^m)+\langle f(x)\rangle =$$

$$\Rightarrow f(\alpha) = f(x)+\langle f(x)\rangle = \langle f(x)\rangle$$

$\Rightarrow f(\alpha) = \langle f(x)\rangle$ olur. Yani; $\alpha \in E$, $f(x)$'in bir kökü olur.

1.Sonuç: $f(x) \in F[x]$ olsun.

$f(x) = \prod_{i=1}^{n}(X-\alpha_i)$; ($\alpha_i \in E$, $d^\circ f = n$) o.ş. F'nin E genişlemesi vardır.

{ $f(x) = (X-\alpha_1)(X-\alpha_2)\dots(X-\alpha_n)$ o.ş. lineer çarpanlara ayrılabilen F'nin bir E genişlemesi vardır. }

23.10.96 / Çarşamba

İspat // $f(x) = a_0 + a_1X + \dots + a_nX^n$

$$= a_n\underbrace{(a_0a_n^{-1} + a_1a_n^{-1}X + \dots + X^n)}_{g(x),\ \text{monik}}$$

$\Rightarrow f(x) = a_n g(x) \Rightarrow f \approx g \Rightarrow f$, monik alınabilir.

Teoremden, $f(x)$ in bir α_1 kökünü bulunduran F'nin bir E_1 genişlemesi vardır. (E_1/F)

$\Rightarrow f(x) = (x-\alpha_1)f_1(x)$, $f_1(x) \in E_1[x]$ olur.

Teoremi, $f_1(x)$'e uygularsak : $f_1(x)$ in bir α_2 kökünü bulunduran E_1'in bir E_2 genişlemesi vardır. (E_2/E_1)

$\Rightarrow f_1(x) = (X-\alpha_2)f_2(x)$, $f_2(x) \in E_2[x]$ olur. ----

--- Devam ederek ;

Çarpımın derecesi, dereceler toplamıdır.

$f(x) = (X-\alpha_1)(X-\alpha_2)\dots(X-\alpha_n)f_n(x)$ o.ş. $f_n(x) \in E_n[x]$ vardır.

$F \subset E_1 \subset E_2 \subset \dots \subset E_n =: E$

{ $d^\circ f = n + d^\circ f_n$, F cisim old.
$n = n + d^\circ f_n$
$0 = d^\circ f_n$
f monik $\Rightarrow f_n = 1$ dir. }

elde edilir.

$d^\circ f=n$, $f(x)$ monik olduğundan $d^\circ f_n=0$ ve $f_n=1$ sabit polinomdur.

O halde $E_n=:E$ genişlemesi f'nin tüm köklerini kapsar. ($\alpha_i\in E$) //

Örnek // $f(x)=4x^2-2\in Q[x]$; Q'nun bir genişlemesini bulalım.

Çözüm // $f(x)=4(x^2-\frac{1}{2})\in Q[x]$

$$=4\left(x-\frac{\sqrt{2}}{2}\right)\left(x+\frac{\sqrt{2}}{2}\right) \qquad \left\{Q\subset \overset{E}{\overset{\shortparallel}{Q(\sqrt{2})}}\right\}$$

$d^\circ f=2$, $\alpha_1=\frac{\sqrt{2}}{2}\in Q(\sqrt{2})$ ve $\alpha_2=-\frac{\sqrt{2}}{2}\in Q(\sqrt{2})$ olacak şekilde Q'nun bir $Q(\sqrt{2})$ genişlemesi vardır. //

TANIM: $f(x)\in F[x]$'in tüm köklerini F'ye katmakla elde edilen genişlemeye, f nin E üzerindeki parçalanış cismi denir. ($f(x)$'in parçalanış cismi.) ve E_f ile gösterilir.

{ Bir polinomun köklerini kapsayan, her zaman için bir cisim vardır. }

Önceki teorem, bu cismin varlığını göstermiş oldu.

$E_f=F(\alpha_1,\alpha_2,\dots,\alpha_n)$ tüm kökleri F'ye katmakla oluşan genişleme.

$\{P(x)=(x^2-2)=(x-\sqrt{2})(x+\sqrt{2})\in Q(\sqrt{2})\}$

2. Sonuç: $f_1(x),f_2(x),\dots,f_r(x)\in F[x]$ olsunlar. $\forall f_i(x)$ polinomu, $E[x]$'de lineer çarpanlara ayrılacak şekilde bir E/F genişlemesi vardır. (köklerini kapsayan, bir E genişlemesi vardır.)

{ x^2-2 , x^2-3 polinomlarının köklerini, $Q(\sqrt{2},\sqrt{3})$ genişlemesi kapsar. }

İspat // Tümevarımla gösterelim:

$r=1$ için doğrudur. (teoremden)

r için doğru olsun. yani ;

$f_1(x),f_2(x),\dots,f_r(x)\in F[x]$, E/F genişlemesi olsun.

1. Sonuç'tan ; $f_{r+1}(x)\in F[x]\subset E[x]$ 'in lineer çarpanlara ayrılacağı, E nin bir E' genişlemesi vardır. $E\subset E'$

$$F\subset \underset{\substack{\downarrow\\ f_r\\ \text{buradadır.}}}{E}\subset \underset{\substack{\downarrow\\ f_{r+1}\\ \text{buradadır.}}}{E'} \quad \Rightarrow E'/F \text{ genişlemesi vardır.}$$

$\Rightarrow r+1$ için de, doğru olduğu görülür. //

TANIM: K cisim olmak üzere, K[x] de sabitten farklı her polinom yine K[x]'de lineer çarpanlara ayrılabiliyorsa ; K cismine, cebirsel kapalı cisim denir.

Teorem: (GAUSS): ℂ, kompleks sayılar cismi, cebirsel kapalıdır.

(ispatı yapılmayacak.) (Dolayısıyla ℂ de asal polinomlar 1. derecedendir.)

{ $X^2+1 \in Q[\sqrt{2},\sqrt{3}]$'de cebirsel kapalı değil. Çünkü bu polinom, $Q[\sqrt{2},\sqrt{3}]$ de lineer çarpanlara ayrılamaz. }

$\forall f(x) \in F[x]$; $\mathbb{C}_f = \mathbb{C}$ dir. Yani ;

(Kompleks sayılar cismine göre) Her polinomun ℂ üzerindeki parçalanış cismi yine ℂ'dedir. ℂ'nin üzerinde cisim yoktur.

Örnek// $f(x) = x^3-2 \in Q[x]$ polinomunun, Q üzerindeki parçalanış cismini bulun. $Q_f = ?$, $[Q_f : Q] = ?$

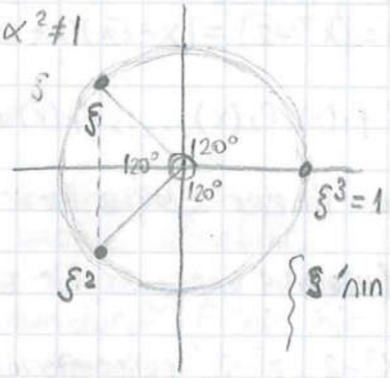
Çözüm// $\alpha^n = 1$, $1 \leq k < n$, $\alpha^k \neq 1$; $\left\{ \alpha = e^{\frac{k2\pi i}{n}} = \cos\frac{k2\pi}{n} + i\sin\frac{k2\pi}{n} \right\}$

$\alpha^3 = 1$ (Birin 3. primitif kökü) $\alpha \neq 1$, $\alpha^2 \neq 1$

$k = 0,1,2 \quad n = 3$

$\alpha^3 = 1 = e^{\frac{k2\pi i}{n}}$

$\alpha_k = \sqrt[3]{2}\, e^{\frac{k2\pi i}{3}} \qquad \xi = e^{\frac{2\pi i}{3}}$



{ξ'nın eşleniği, ξ^2 dir.}

$$\left.\begin{array}{l} \Rightarrow \alpha_0 = \sqrt[3]{2}\, e^0 = \sqrt[3]{2} \\ \Rightarrow \alpha_1 = \sqrt[3]{2}\, e^{\frac{2\pi i}{3}} = \sqrt[3]{2}.\xi \\ \Rightarrow \alpha_2 = \sqrt[3]{2}\, e^{\frac{4\pi i}{3}} = \sqrt[3]{2}.\xi^2 \end{array}\right\} \Rightarrow \{\sqrt[3]{2}, \sqrt[3]{2}\xi, \sqrt[3]{2}\xi^2\} \text{ köklerdir.}$$

$$Q_f = Q[\sqrt[3]{2}, \sqrt[3]{2}\xi, \sqrt[3]{2}\xi^2] \overset{\subset}{\underset{\supset}{=}} Q(\sqrt[3]{2}, \xi)$$

$\{\xi = \xi.\sqrt[3]{2}(\sqrt[3]{2})^{-1}\}$

$\Rightarrow Q_f = Q(\sqrt[3]{2}, \xi)$ olur.

$$[Q(\sqrt[3]{2},\xi) : Q] = [Q(\sqrt[3]{2},\xi) : Q(\sqrt[3]{2})].[Q(\sqrt[3]{2}) : Q]$$

$$\left.\begin{array}{l} f = P_{Q(\sqrt[3]{2})}(\xi, x) = x^2+x+1 \in Q(\sqrt[3]{2})[x] \\ g = P_Q(\sqrt[3]{2}, x) = x^3-2 \in Q[x] \end{array}\right\} (d^\circ f = 2,\ d^\circ g = 3)$$

$\Rightarrow [Q_f : Q] = 6$ dir. //

Örnek // $f(x) = x^n - 1 \in \mathbb{Q}[x]$ polinomunun $\mathbb{Q}$ üzerindeki parçalanış cismini bulun. $\mathbb{Q}_f = ?$ $[\mathbb{Q}_f : \mathbb{Q}] = ?$

Çözüm // $\xi = e^{\frac{2\pi i}{n}}$ olmak üzere $f(x)$ in kökleri ; $\{1, \xi, \xi^2, \dots, \xi^{n-1}\}$ dir.

Bu kökleri $\mathbb{Q}$ ya katarak elde edilen cisim $\mathbb{Q}_f$ dir.

$$\mathbb{Q}_f = \mathbb{Q}(1, \xi, \xi^2, \dots, \xi^{n-1}) \overset{\supseteq}{\underset{\subseteq}{=}} \mathbb{Q}(\xi)$$

$\forall \xi^i \; (i=1,2,\dots,n) \in \mathbb{Q}(\xi)$ olduğundan $\mathbb{Q}_f = \mathbb{Q}(\xi)$ olur.

Bu cisime n. daire bölümü cismi denir.

Şimdi $[\mathbb{Q}(\xi):\mathbb{Q}]$'yu bulalım. $P_{\mathbb{Q}}(\xi, x) = ?$

- $n=2 \Rightarrow \xi = e^{\pi i} = \cos\pi + i\sin\pi = -1 + 0i = -1 \Rightarrow \xi = -1$ olacağından, $\mathbb{Q}(\xi) = \mathbb{Q}$ olur. $\Rightarrow [\mathbb{Q}(\xi):\mathbb{Q}] = 1$ bulunur. $(P_{\mathbb{Q}}(\xi,x) = x+1)$
- $n=4 \Rightarrow \xi = e^{\pi i/2} = \cos\frac{\pi}{2} + i\sin\frac{\pi}{2} = 0 + 1.i = i \Rightarrow \xi = i$ olacağından, $x^4 - 1 = \underbrace{(x-1)}_{asal}\underbrace{(x+1)}_{asal}\underbrace{(x^2+1)}_{asal}$ asallarından yalnızca x^2+1 polinomu i'yi kök kabul eder. $\Rightarrow [\mathbb{Q}(\xi):\mathbb{Q}] = 2$ $(P_{\mathbb{Q}}(\xi,x) = x^2+1)$
- $n=5 \Rightarrow \xi = e^{2\pi i/5} = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5} \Rightarrow x^5 - 1 = \underbrace{(x-1)}_{asal}(\underbrace{x^4+x^3+x^2+x+1}_{asal\,.\,?})$

$\Rightarrow P_{\mathbb{Q}}(\xi,x) = x^4+x^3+x^2+x+1 \in \mathbb{Q}[x]$

polinomu ξ'yı kök kabul eder. Asal olup olmadığına bakalım:

$f(x)$ polinomu $\mathbb{Z}[x]$ de asal ise kesir cismi olan $\mathbb{Q}[x]$ de de asaldır.

$f(x+1)$ polinomu ~~$\mathbb{Z}[x]$ de~~ asal ise $f(x)$ de $\mathbb{Z}[x]$ de asal ve $\mathbb{Q}[x]$ de de asal olur. Buradan $x^4+x^3+x^2+x+1$ asal polinom olup,

$$P_{\mathbb{Q}}(\xi,x) = x^4+x^3+x^2+x+1 \; , \; [\mathbb{Q}(\xi):\mathbb{Q}] = 4 \text{ olur.}$$

- $n = p > 2$ asal olsun. $\xi = e^{\frac{2\pi i}{p}} \Rightarrow f(x) = x^p - 1 = (x-1)(x^{p-1} + \dots + x + 1)$

$\frac{x^{p}-1}{x-1} = x^{p-1} + \dots + x + 1$ $\quad \underset{monik}{f(\xi)} = 0$, $f(x)$ asal ? (Bk. Cebir 176/20)

$$f(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \dots + \binom{p}{p-2}x + \overset{\# p}{\binom{p}{p-1}}$$

$p \in \mathbb{Z}$ asal, $f(x+1)$ polinomunun katsayıları $\mathbb{Z}$ dedir. Kesir cismi de $\mathbb{Q}$ olur. $\underset{(1 \le i \le p-1)}{p \mid \binom{p}{i}}$, $p \nmid 1$, $p^2 \nmid p = \binom{p}{p-1}$ (Eisenstein sağlandı.)

$f(x+1)$ $\mathbb{Z}[x]$ de asal $\Rightarrow$ $\mathbb{Q}[x]$ de asal $\Rightarrow$ $f(x)$ de $\mathbb{Q}[x]$ de asaldır.

- $n=8$ olsun. (Asal olmasın) $\xi = e^{\frac{\pi i}{4}} = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$

$$X^8 - 1 = (X^4-1)(X^4+1) = (X^2-1)(X^2+1)(X^4+1)$$

$$= \underset{asal}{(X-1)}\underset{asal}{(X+1)}\underset{asal}{(X^2+1)}\underbrace{(X^4+1)}_{asal} \in \mathbb{Q}[X]$$

$X^4+1 \in \mathbb{Q}[X]$ polinomu ξ'yı kök kabul eder. Asallığını inceleyelim.

$f(X+1) = (X+1)^4+1 = X^4+4X^3+6X^2+4X+2$ $p=2$ asalı için;

$2|2$, $2\nmid 1$, $4\nmid 2$ Eisenstein $f(X+1)$ için sağlandı.

$f(X+1)$ $\mathbb{Z}[X]$ de asal $\Rightarrow$ $f(X+1)$ $\mathbb{Q}[X]$ de asal

$\Rightarrow f(X)$, $\mathbb{Z}[X]$ de, dolayısıyla $\mathbb{Q}[X]$ de asaldır.

Yani X^4+1 polinomu $\mathbb{Q}[X]$ de asaldır.

$d^\circ P_{\mathbb{Q}}(\xi, X) = [\mathbb{Q}(\xi):\mathbb{Q}] = 4$ bulunur.

Sonuç: $[\mathbb{Q}(\xi):\mathbb{Q}] = \varphi(n)$ Euler fonksiyonudur.

$$\left\{\begin{array}{ll} n=2 \Rightarrow \varphi(n)=1, & n=5 \Rightarrow \varphi(n)=4 \\ n=4 \Rightarrow \varphi(n)=2, & n=8 \Rightarrow \varphi(n)=4 \end{array}\right\} \quad n=p>1 \text{ asal} \Rightarrow \varphi(n)=p-1$$

TANIM: $P(X) = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n \in F[X]$ polinomunun türevi; formal (biçimsel) olarak;

$$P'(X) := a_1 + 2a_2X + 3a_3X^2 + \ldots + n a_n X^{n-1} \in F[X]$$

olarak tanımlanır.

$$na = \begin{cases} a+a+\ldots+a, & n>0 \\ 0_F, & n=0 \\ (-a)+(-a)+\ldots+(-a), & n<0 \end{cases} \text{ dir.}$$

$f: F \to F$

$x \to f(x) = (x^2+1)(x^5-2.1)^{-2}$

burada hangi topoloji üzerinde çalışıldığı belirtilmek zorundadır.

Biz burada türevi, biçimsel olarak ele alıyoruz.

Tanımı kullanarak, türevin şu özellikleri söylenebilir: $a,b \in F$, $g(x),h(x) \in F[X]$;

i - $[a.g(x)+b.h(x)]' = ag'(x)+b\,h'(x)$

ii - $[g(x).h(x)]' = g'(x)h(x)+g(x)h'(x)$

iii - $[(X\mp a)^n]' = n.(X\mp a)^{n-1}$, $(n \geq 2)$

iv - $d^\circ g(x) = d^\circ g'(x)+1$

$f(x)=(x-a)^n g(x)$, $(n\geq 2)$ şeklinde ise, a ya katlı kök denir.

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

İspat// a, $f(x)$'in katlı kökü $\Rightarrow f(X)=(X-a)^n g(X)$, $n>1$ dir.

Bu yazılış $E_F[X]$ veya $\mathbb{C}[X]$ de düşünülebilir.

$\Rightarrow f'(X)=\underbrace{n(X-a)^{n-1}}_{0}g(x)+\underbrace{(X-a)^n g'(X)}_{0}$ $(n>1$ old.)

$\Rightarrow f'(a)=0$ olur.

$f(x)$ ve $f'(x)$ in sabit olmayan bir ortak çarpanı olmasın. (Aksine iddia)

$\Rightarrow ebob(f(x),f'(x))=1$ dir.

$\Rightarrow 1=\alpha(x)f(x)\mp\beta(X)f'(X)$ o.ş. $\exists\alpha(x),\beta(x)\in F[X]$.

($F[X]$ EB $\Rightarrow F[X]$ TÜİB olur.) $F[X]$, TÜİB olduğundan;

$X=a$ yazılırsa,

$\Rightarrow 1=\alpha(a)\underbrace{f(a)}_{0}\mp\beta(a)\underbrace{f'(a)}_{0} \Rightarrow 1=0$ #

O halde $f(x)$ ve $f'(x)$'in sabit olmayan bir ortak çarpanı vardır.

Not: Tersine; a, $f(x)$ ve $f'(x)$'in bir ortak kökü ise, a, $f(x)$'in katlı bir köküdür. Çünkü;

a, $f(X)$ in kökü $\Rightarrow f(x)=(X-a)g(X)$ o.ş $\exists g(x)\in F[x]$.

$\Rightarrow f'(X)=g(x)+(x-a)g'(X)$

$\Rightarrow f'(a)=0$ olduğundan, $f'(a)=g(a)=0$ → hipotezden

$\Rightarrow g(X)=(X-a)h(X)$ o.ş $\exists h(X)\in F[x]$.

$\Rightarrow f(X)=(X-a)^2h(X)$

Önerme: $f(X)\in F[X]$ asal polinomunun tüm $\underbrace{\text{sıfırları}}_{\text{kökleri}}$ $\underbrace{\text{basittir.}}_{\text{katsız kök.}}$

İspat// $f(X)=a_0+a_1X+\ldots+a_nX^n$

$=a_n(\underbrace{a_0a_n^{-1}+a_1a_n^{-1}X+\ldots+X^n}_{g(x)})$

$\Rightarrow f(X)=a_n.\underset{\substack{\downarrow\\ \text{monik}}}{g(X)}$ $f(X)\approx g(x)$

$g(x)$ monik $\Rightarrow f(X)$ monik alınabilir.

Kabul edelim ki, $f(x)$'in katlı bir kökü olsun.

$\Rightarrow d^0 f \geqslant 2$ olur. $\{ f(x) = (x-a)^n g(x),\ n \geqslant 2$ idi.$\}$

Önceki önermeden, $f(x)$ ve $f'(x)$'in $F[x]$'de sabitten farklı bir ortak çarpanları (bölenleri) var idi. Fakat $f(x)$, $F[x]$ de asal olduğundan $f(x) \mid \underbrace{f'(x)}_{\text{monik.}}$ bulunur. #

Çünkü $d^0 f'(x) < d^0 f(x)$ olmak zorundadır.

O halde $f(x) \in F[x]$ asal polinomunun katlı kökü yoktur. //

$$\left\{ \begin{array}{l} \text{ebob}(\underbrace{f(x)}_{\text{asal}}, f'(x)) \neq 1 \Rightarrow \text{ebob}(f(x), f'(x)) = f(x) \text{ olur.} \\ \qquad\qquad\qquad\qquad \Rightarrow f(x) \mid f'(x) \ \# \qquad (d^0 f' < d^0 f) \\ \left\{ (\overset{\text{asal}}{\overset{\uparrow}{3}}, a) = 1 \vee 3 \right\} \end{array} \right\}$$

Örneğin; $(x^2-2) = (x-\sqrt{2})(x+\sqrt{2}) \Rightarrow x_1 = \sqrt{2},\ x_2 = -\sqrt{2}$ katlı kök değiller.

6.11.96/Çarşamba

Teorem: (İlkel Eleman Teoremi):

$E = F(\alpha, \beta)$, F nin cebirsel genişlemesi olsun.

$E = F(\gamma)$ olacak şekilde $\exists \gamma \in E$ vardır. (E, F nin basit genişlemesidir.)

$$\left\{ \overbrace{\underbrace{\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}+\sqrt{3})}_{4} \underbrace{\subset \mathbb{Q}(\sqrt{2},\sqrt{3})}_{1}}^{4} \quad \Rightarrow \mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3}) \right\}$$

İspat // $f(x) = P_F(\alpha, x)$, $g(x) = P_F(\beta, x)$ diyelim.

$f(x) = (x-\alpha_1)(x-\alpha_2) \dots (x-\alpha_n) \longrightarrow \alpha := \alpha_1$ (herhangi birini seçerek)

$g(x) = (x-\beta_1)(x-\beta_2) \dots (x-\beta_m) \longrightarrow \beta := \beta_1$ (herhangi birini seçerek)

$A := \left\{ \dfrac{\alpha_i - \alpha_1}{\beta_1 - \beta_j} \,\middle|\, 1 < i \leqslant n,\ 1 < j \leqslant m \right\}$ şeklinde tanımlayalım.

A kümesinin $(m-1).(n-1)$-tane elemanı vardır. $(i, j \neq 1)$

A kümesi bu nedenle sonlu elemanlı olur.

$\{$Burada, tüm cisimler $\mathbb{C}$ nin alt cismi olur.$\}$

$\exists t \in F$, $t \notin A$ olsun. Ve $\gamma := \underbrace{\underset{\in E}{\overset{}{\alpha}} + \underset{\in F}{t}\,\underset{\in E}{\beta}}_{\in E} \in E$ şeklinde tanımlayalım.

$\Rightarrow F(\gamma) \subset E = F(\alpha, \beta) \dots$ ①