E/F : cisim genişlemesi
$u \in E$: cebirsel

$$F \subseteq F(u) \subseteq E$$

$$der(Min_F(u)) = der_F(u) \Rightarrow [F(u):F] = der_F(u)$$

1. $F(u)$ nun her elemanı F üzerinde cebirsel mi?
2. $F \leq E \leq K$: cisim kulesi

E F üzerinde ve K E üzerinde cebirsel $\Rightarrow$ K F üz. cebirsel?

Cebirsel Cisim Genişlemeleri

Tanım. E/F bir cisim genişlemesi olsun. E nin bütün elemanları F üzerinde cebirsel ise bu genişlemeye bir cebirsel genişleme denir.

Örn. $\mathbb{C}$ $\mathbb{R}$ üzerinde cebirseldir.

$z = a+ib \in \mathbb{C}$ $\quad (x-z)(x-\bar{z}) = x^2 - \underbrace{(z+\bar{z})}_{\in \mathbb{R}}x + \underbrace{z\bar{z}}_{\in \mathbb{R}}$

TEOREM. Her sonlu cisim genişlemesi cebirseldir.

Kanıt. E, F nin bir sonlu genişlemesi olsun. $[E:F]=n$ o.ş. bir n tamsayısı vardır. $u \in E$ alalım.
$\{1, u, u^2, \ldots, u^n\}$ kümesi F üzerinde doğrusal bağımlıdır. Buna göre

$$a_0 + a_1 u + a_2 u^2 + \cdots + a_n u^n = 0$$

o.ş. hepsi birden sıfır olmayan $a_0, a_1, \ldots, a_n \in F$ bulunabilir

O zaman u, $p(x)=a_0+a_1x+\dots+a_nx^n \in F[x]\setminus\{0_F\}$ polinomunun bir köküdür.

$\therefore$ u F üzerinde cebirseldir.

$\therefore$ u keyfi old. E/F cebirsel genişleme olur. $\square$

TEOREM. $F \leq E \leq K$ cisim kulesi verilsin. Eğer $[K:E]<\infty$ ve $[E:F]<\infty$ ise o zaman $[K:F]<\infty$ olur ve $[K:F]=[K:E]\cdot[E:F]$ dir.

Kanıt. Kabul edelim ki $[K:E]=m$ ve $[E:F]=n$ olsun. $\{u_1,\dots,u_m\}\subseteq K$, K nın bir E-bazı ve $\{v_1,\dots,v_n\}\subseteq E$ E nin bir F-bazı olsun.

$$\begin{array}{l} K \\ \Big| \;\big\}\{u_i\} \\ E \\ \Big| \;\big\}\{v_j\} \\ F \end{array}$$

<u>İddia:</u> $\{u_iv_j : i=1,\dots,m,\ j=1,\dots,n\}$ kümesi K nın F üzerinde bir bazıdır.

$w\in K$ alalım. $w=\sum_{i=1}^{m} a_iu_i$ o.ş. $a_i\in E$ vardır. Her $i=1,\dots,m$ için

$$a_i=\sum_{j=1}^{n} b_{ij}v_j$$

o.ş. $b_{ij}\in F$ vardır.

$$\Rightarrow\quad w=\sum_{i=1}^{m}\Big(\sum_{j=1}^{n} b_{ij}v_j\Big)u_i=\sum_{i=1}^{m}\sum_{j=1}^{n} \underbrace{b_{ij}}_{\in F}u_iv_j$$

$\{u_iv_j\}$ kümesi K yı F üzerinde gerer.

$$\sum_{i,j} b_{ij} u_i v_j = 0 \Rightarrow \sum_i \Big(\underbrace{\sum_j b_{ij} v_j}_{E}\Big) u_i = 0$$

$$\Rightarrow \sum_j \underbrace{b_{ij}}_{F} v_j = 0 \quad \forall i = 1, \dots, m$$

$$\Rightarrow b_{ij} = 0 \quad \forall i, j.$$

$\therefore$ $\{u_i v_j\}$ kümesi F üzerinde doğrusal bağımsızdır. $\square$

Sonuç. $F = F_0 \leq F_1 \leq \dots \leq F_r = E$ bir cisim kulesi olsun. Eğer her $1 \leq i \leq r$ için $[F_i : F_{i-1}] < \infty$ ise

$$[E:F] = [F_r : F_{r-1}][F_{r-1} : F_{r-2}] \dots [F_1 : F_0]$$

ve böylece $[E:F] < \infty$ olur.

Kanıt taslağı: r üzerine tümevarım.

$$F \leq F_{r-1} \leq E \Rightarrow [E:F] = [E:F_{r-1}]\underbrace{[F_{r-1}:F]}_{\text{tümevarım}}$$

Sonuç. E/F bir cisim genişlemesi ve $u \in E$, F üzerinde cebirsel olsun. Eğer $v \in F(u)$ ise v F üzerinde cebirseldir ve $\operatorname{der}_F(v) \mid \operatorname{der}_F(u)$.

Kanıt.

$\operatorname{der}_F(u) = m$ olsun. O zaman $[F(u):F] = m < \infty$ old. $F(u)$ F üzerinde cebirsel $\Rightarrow v$ F üzerinde cebirsel

$v \in F(u)$ old. $F \leq F(v) \leq F(u)$

$$m = [F(u):F] = [F(u):F(v)]\overbrace{[F(v):F]}^{\operatorname{der}_F(v)}$$

Örnek. $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ cisminin bir $\mathbb{Q}$-bazını bulalım.

$$\begin{array}{ll} F = \mathbb{Q}(\sqrt{2})(\sqrt{3}) & \\ \quad | & \Big) \ ? \quad \{1, \sqrt{3}\} \\ \mathbb{Q}(\sqrt{2}) & \\ \quad | & \Big) \ \{1, \sqrt{2}\} \\ \mathbb{Q} & \end{array}$$

$\text{Min}_{\mathbb{Q}}(\sqrt{2}) = x^2 - 2 \Rightarrow \deg_{\mathbb{Q}}(\sqrt{2}) = 2 \Rightarrow \{1, \sqrt{2}\}$ $\mathbb{Q}$-bazı.

? : $\sqrt{3}$ ün $\mathbb{Q}(\sqrt{2})$ üzerindeki min. polinomu gereklidir.

$\text{Min}_{\mathbb{Q}}(\sqrt{3}) = x^2 - 3 \in \mathbb{Q}(\sqrt{2})[x]$

$\Rightarrow \text{Min}_{\mathbb{Q}(\sqrt{2})}(\sqrt{3}) \mid x^2 - 3 \Rightarrow \sqrt{3} \in \mathbb{Q}(\sqrt{2})$ veya

$\text{Min}_{\mathbb{Q}(\sqrt{2})}(\sqrt{3}) = x^2 - 3$.

$\sqrt{3} \in \mathbb{Q}(\sqrt{2})$ olsun. $\sqrt{3} = a + b\sqrt{2}$ o.ş. $a, b \in \mathbb{Q}$ vardır.

$\Rightarrow \underbrace{3}_{\mathbb{Q}} = \underbrace{a^2 + 2b^2}_{\mathbb{Q}} + 2ab\sqrt{2} \Rightarrow 2ab\sqrt{2} \in \mathbb{Q} \Rightarrow ab = 0$

$a = 0$: $\sqrt{3} = b\sqrt{2} \Rightarrow 3/2 = b^2$, çelişki

$b = 0$: $a = \sqrt{3} \in \mathbb{Q}$, çelişki.

$\therefore \sqrt{3} \notin \mathbb{Q}(\sqrt{2}) \Rightarrow \text{Min}_{\mathbb{Q}(\sqrt{2})}(\sqrt{3}) = x^2 - 3$.

$\therefore$ F in bir $\mathbb{Q}$-bazı $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ verilebilir.

$F = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$

$\sqrt{2}, \sqrt{3} \in F \Rightarrow \sqrt{2} + \sqrt{3} \in F \Rightarrow \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq F$.

$\mathrm{Min}_{\mathbb{Q}}(\sqrt{2}+\sqrt{3}) = x^4 - 10x^2 + 1$ old. $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}] = 4$

$$\underbrace{[F:\mathbb{Q}]}_{4} = \underbrace{[F:\mathbb{Q}(\sqrt{2}+\sqrt{3})]}_{1}\underbrace{[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]}_{4}$$

$\Rightarrow \; F = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Örnek $\mathbb{Q}(\sqrt[6]{2}) \supseteq \mathbb{Q}(\sqrt{2})$ dir çünkü

$$\sqrt{2} = (\sqrt[6]{2})^3 \in \mathbb{Q}(\sqrt[6]{2})$$

$\mathbb{Q}(\sqrt[6]{2})$ nin bir $\mathbb{Q}(\sqrt{2})$-bazını bulalım:

$$\begin{array}{c} \mathbb{Q}(\sqrt[6]{2}) = \mathbb{Q}(\sqrt{2})(\sqrt[6]{2}) \\ | \\ \mathbb{Q}(\sqrt{2}) \\ | \\ \mathbb{Q} \end{array} \Bigg\} \Rightarrow \underbrace{[\mathbb{Q}(\sqrt[6]{2}):\mathbb{Q}]}_{6} = [\mathbb{Q}(\sqrt[6]{2}):\mathbb{Q}(\sqrt{2})]\underbrace{[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]}_{2}$$

$\Rightarrow \; [\mathbb{Q}(\sqrt[6]{2}):\mathbb{Q}(\sqrt{2})] = 3$ olur.

$f(x) = x^3 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[x]$ ve $f(\sqrt[6]{2}) = 0$ old.
$\mathrm{Min}_{\mathbb{Q}(\sqrt{2})}(\sqrt[6]{2}) = x^3 - \sqrt{2}$.

$\{1, \sqrt[6]{2}, \sqrt[6]{4}\}$ $\mathbb{Q}(\sqrt[6]{2})$ nin bir $\mathbb{Q}(\sqrt{2})$-bazıdır.

TEOREM. E/F bir cisim genişlemesi olsun. Aşağıdakiler denktir:

(i) E, F nin bir sonlu genişlemesidir.

(ii) $E = F(u_1, \ldots, u_n)$ o.ş. F üzerinde cebirsel olan $u_1, \ldots, u_n$ elemanları vardır.

Kanıt.

(i) $\Rightarrow$ (ii) $[E:F] = n$ olsun $\{u_1, \ldots, u_n\}$, E nin F-bazı olsun. E nin tüm elemanları $u_1, \ldots, u_n$ nin lineer kombinasyonları old. $E = F(u_1, \ldots, u_n)$ yazılabilir.

(ii) $\Rightarrow$ (i) : $E = F(u_1, \ldots, u_n)$ olsun

$$\boxed{F = F_0 \leq F(u_1) \leq \underbrace{F(u_1, u_2)}_{F(u_1)(u_2)} \leq \ldots \leq F(u_1, \ldots, u_{n-1}) \leq E}$$

Her $i = 1, \ldots, n$ için u_i F üzerinde cebirsel old. $F(u_1, \ldots, u_{i-1})$ üzerinde de cebirseldir. Dolayısıyla

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

olur.

$$[E:F] = [E : F(u_1, \ldots, u_{i-1})] \ldots [F(u_1, u_2) : F(u_1)] [F(u_1) : F] < \infty$$

olur. E/F sonlu genişleme.

SONUÇ. $F \leq E \leq K$ bir cisim kulesi olsun. E F nin ve K da E nin cebirsel genişlemesi ise K, F nin bir cebirsel genişlemesidir.

Kanıt. $u \in K$ olsun. u E üzerinde cebirseldir. $p(x) = \mathrm{Min}_E(u)$ olsun. $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, $a_0, a_1, \ldots, a_n \in E$ yazabiliriz. $L = F(a_0, a_1, \ldots, a_n)$ olsun. E/F cebirsel old. her i için a_i F üzerinde cebirsel olur.

$\Rightarrow [L:F]$ sonludur.

u L üzerinde cebirsel old. ($p(x) \in L[x]$ ve $p(u) = 0$ old.) $[L(u):L]$ sonludur.

$$[F(u):F] \leq [L(u):F] = [L(u):L][L:F] < \infty$$

$\Rightarrow u$ F üzerinde cebirseldir.

Cebirsel Kapanış.

Tanım. E/F bir cisim genişlemesi olsun.

$$\overline{F}_E := \{ c \in E : c \ F \text{ üzerinde cebirsel} \}$$

kümesine F nin E içindeki cebirsel kapanışı denir.

TEOREM. E/F bir cisim genişlemesi ise $\overline{F}_E$ E nin F yi içeren bir alt cismidir.

Kanıt. $F \subseteq \overline{F}_E$ old. açıktır. $\overline{F}_E \neq \emptyset$ olur.

$a, b \in \overline{F}_E$ olsun.

a ve b F üzerinde cebirsel old. $F(a,b)$ F üzerinde cebirsel.

$$\overbrace{\underbrace{F \leq F(a)}_{\text{sonlu}} \leq F(a)(b)}^{\text{sonlu}}$$

$$F(a) \leq F(a)(b) \quad \text{sonlu}$$

$a-b,\ ab \in F(a,b)$ ve $b \neq 0_F$ ise $b^{-1} \in F(a,b)$.

$\Rightarrow a-b, ab, b^{-1} \in \overline{F}_E$ $(b \neq 0)$ olur.

$\therefore$ Alt cisim kriterinden $\overline{F}_E \leq E$ olur.

SONUÇ. Cebirsel sayıların kümesi $\mathbb{C}$ nin bir alt cismidir.

$$\mathbb{Q} \subseteq \overline{\mathbb{Q}}_{\mathbb{C}} \subseteq \mathbb{C}$$

TEOREM. $\overline{\mathbb{Q}}_{\mathbb{C}}$ $\mathbb{Q}$ nun bir sonsuz genişlemesidir.

Kanıt. $p(x) = x^n - 2$ polinomu Eisenstein kriteri gereğince $\mathbb{Q}$ üzerinde indirgenmezdir. $p(\sqrt[n]{2}) = 0$ old. $\sqrt[n]{2} \in \overline{\mathbb{Q}}_{\mathbb{C}}$ ve $[\overline{\mathbb{Q}}_{\mathbb{C}} : \mathbb{Q}] \geq [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$. Burada n keyfi seçildiğinden $[\overline{\mathbb{Q}}_{\mathbb{C}} : \mathbb{Q}] = \infty$ olur. $\square$

Tanım. F bir cisim olsun. $F[x]$ in sabit olmayan her elemanının F içinde bir kökü varsa F ye bir <u>cebirsel kapalı</u> cisim denir.

$\mathbb{C}$ bir cebirsel kapalı cisim (Cebirin Temel Teoremi)

TEOREM. F bir cisim olsun. F nin cebirsel kapalı olması için gerek ve yeter şart $F[x]$ deki sabit olmayan her polinomun tamamen lineer çarpanlarına ayrılmasıdır.

Kanıt. F cebirsel kapalı olsun. $f(x) \in F[x]$ alalım. $der(f(x)) = n$ olsun. n üzerine tümevarım uygulayalım. $n=1$ ise durum açık. $n>1$ ve iddia n den küçük pozitif tamsayılar için doğru olsun. F cebirsel kapalı old. $f(x)$ in en az bir kökü F de bulunur. Bu kök $a \in F$ olsun. $f(x) = c(x-a) f_1(x)$ o.ş $c \in F$ ve $f_1(x) \in F[x]$ vardır. der $f_1(x) < n$ old. tümevarım hipotezi gereğince $f_1(x)$ tamamen doğrusal çarpanlarına ayrılır. Dolayısıyla $f(x)$ de doğr. çarp. ayrılır.

Diğer yön açık olduğundan kanıt tamamlanır. $\square$

Tanım. Bir F cismininin cebirsel kapalı bir cebirsel genişlemesi varsa buna F nin bir cebirsel kapanışı denir.

E/F cebirsel ve E cebirsel kapalı $\Rightarrow$ E F nin bir cebirsel kapanışı.

$\mathbb{C}/\mathbb{R}$ cebirsel & $\mathbb{C}$ cebirsel kapalı $\Rightarrow$ $\mathbb{C}$ $\mathbb{R}$ nin bir cebirsel kapanışı.

TEOREM. Her cismin bir cebirsel kapanışı vardır.

SONUÇ. K bir cebirsel kapalı cisim ve $F \leq K$ olsun. O zaman $\overline{F}_K$ cebirsel kapalıdır.

Kanıt. $f(x) \in \overline{F}_K[x]$ sabit olmayan polinom $f(x) = a_0 + a_1 x + \dots + a_n x^n$ o.ş. $a_0, a_1, \dots, a_n \in \overline{F}_K$ vardır. $E = F(a_0, a_1, \dots, a_n)$ denirse $f(x) \in E[x]$ olur. a_i ler F üzerinde cebirsel old, $[E:F] < \infty$ olur.

K cebirsel kapalı old. $u \in K$ vardır öyle ki $f(u)=0$.
$f(x) \in E[x]$ old. u E üzerinde cebirsel. $\Rightarrow [E(u):E] < \infty$
$[E(u):F] < \infty \Rightarrow [F(u):F] < \infty \Rightarrow u \in \overline{F}_K$.
$\therefore$ $\overline{F}_K$ cebirsel kapalı.
$\square$