Forelesning 20. mars 2024

Repetisjon

$F \leq E \ni \alpha$

kropp utvidelse

$E = F(\alpha)$ simpel utvidelse

$\mathrm{irr}(\alpha, F) \in F[x]$

$\deg_F(F(\alpha)) = \deg(\mathrm{irr}(\alpha, F))$

$= [F(\alpha) : F]$.

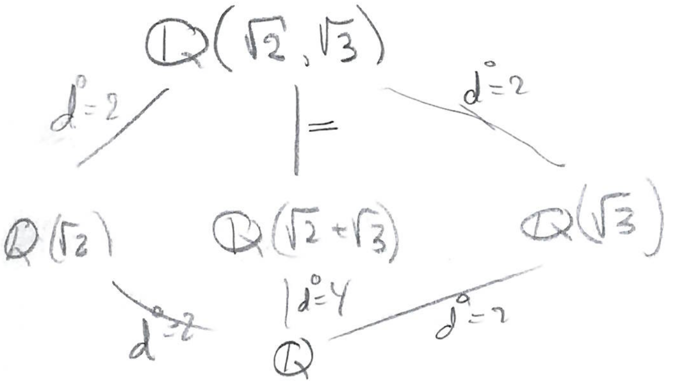
31,7

$F \leq F(\alpha) \leq E \ni \alpha$, $\beta \in F(\alpha)$

$\Rightarrow F \leq F(\beta) \leq F(\alpha) \Rightarrow [F(\alpha):F] = [F(\alpha):F(\beta)][F(\beta):\mathbb{Q}]$

$[F(\alpha):F] = \deg(F,\alpha)$, $[F(\beta):\mathbb{Q}] = \deg(F,\mathbb{Q})$

Ex



$\alpha^0 = 1 = 1$

$\alpha^1 = \sqrt{2}+\sqrt{3} = \sqrt{2}+\sqrt{3}$

$\alpha^2 = (\sqrt{2}+\sqrt{3})^2 = 5 + 2\sqrt{6}$

$\alpha^3 = (\sqrt{2}+\sqrt{3})^3 = 5\sqrt{2} + 5\sqrt{3} + 4\sqrt{3} + 6\sqrt{2} = 11\sqrt{2} + 9\sqrt{3}$

$\alpha^4 = (\sqrt{2}+\sqrt{3})^4 = 49 + 20\sqrt{6}$

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

$$\tfrac{1}{2}(\alpha^3 - 9\alpha) = \sqrt{2} \qquad -\tfrac{1}{2}(\alpha^3 - 11\alpha) = \sqrt{3}$$

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

Basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$:

$$\{1, \sqrt{2}\} \cdot \{1, \sqrt{3}\} = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$$

Ex $\mathbb{Q} \leq \mathbb{C} \ni \sqrt[3]{2} = \alpha$ $p(x) = \text{irr}(\alpha, \mathbb{Q}) = x^3 - 2$

Rødtene til $p(x)$: $x = \sqrt[3]{2}$, $x = \sqrt[3]{2}\cdot\xi$ $x = \sqrt[3]{2}\,\xi^2$ $\xi^3 = 1$

$$\mathbb{Q} \underset{d^\circ=3}{\leq} \mathbb{Q}(\sqrt[3]{2}) \underset{d^\circ=2}{\leq} \mathbb{Q}(\sqrt[3]{2}, \xi)$$

irreduserbel $\xi^2 + \xi + 1 = 0$

Ex $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2})$ $\text{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$

Ψ

$\alpha = a + b\sqrt{2}$

$\text{irr}(\alpha, \mathbb{Q})$:

$\alpha^0 = 1$

$\alpha^1 = a + b\sqrt{2}$

$\alpha^2 = (a^2 + 2b^2) + 2ab\sqrt{2}$

$$\alpha^2 - 2a\alpha + a^2 - 2b^2 = 0$$

$$\text{irr}(\alpha, \mathbb{Q}) = x^2 - 2ax + a^2 - 2b^2$$

$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\alpha)$ for $\alpha = a + b\sqrt{2}$, $b \neq 0$.

Thm 31.3 Enhver endelig utvidelse av F er algebraisk.

Thm 31.12

$F \leq E \ni \alpha, \beta$ algebraisk $\Rightarrow$ $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$, $\frac{\alpha}{\beta}$, $\beta \neq 0$ algebraiske.

$F(\alpha, \beta)$ endelig utvidelse $\Rightarrow$ $F(\alpha, \beta)$ algebraisk

Defn $F \leq E$ $\widetilde{F}_E = \{\alpha \in E \mid \alpha \text{ algebraisk over } F\}$

algebraisk tillukning av F i E (kropp)

Defn. 31.14

F algebraisk lukket $\iff \forall f(x) \in F[x]$, $\exists \alpha \in F$ s.a. $f(\alpha) = 0$

$\iff \forall f(x) \in F[x]$, $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$

Cor 31.16

$F \leq E \Rightarrow \alpha$ alg. over F, E algebraisk utvidelse $\Rightarrow irr(\alpha, F) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$

dvs $n=1$ siden $irr(\alpha, F)$ er irreduserbar

$\Rightarrow irr(\alpha, F) = x - \alpha$ og $\alpha \in F$.

$\Rightarrow F \leq E \Rightarrow F = E$

F alg. lukket, E alg. utv.

Eksistens av algebraisk avslutning

$$F \leq F(\alpha_1) \leq F(\alpha_1, \alpha_2) \leq \cdots \leq \bigcup_{n=1}^{\infty} F(\alpha_1, \ldots, \alpha_n) = G$$

1) G kropp siden $\alpha, \beta \in G$ betyr $\alpha, \beta \in F(\alpha_1, \ldots, \alpha_n)$

2) Zorns lemma: Enhver oppad begrenset kjede av inklusjoner har et maks element

3) $\Rightarrow \exists \bar{F}$ slik at $F(\alpha_1, \ldots, \alpha_n) \subset \bar{F}$. maks.

Konstruerbare tall (passer og linjal)

Thm 32.1 Konstruerbare tall er en kropp $\supseteq \mathbb{Q}$

Hva kan konstrueres

Linje med rasjonale koeff
Sirkel med rasjonalt sentrum og rasjonal diameter
skjæringer mellom disse

$\Rightarrow$ $\gamma \in \mathbb{R}$ konstruerbar betyr $\exists\ \alpha_1, \alpha_2, \dots, \alpha_n = \gamma$ slik at $\left[\mathbb{Q}(\alpha_1, \dots, \alpha_k) : \mathbb{Q}(\alpha_1, \dots, \alpha_{k-1})\right] = 2$.

$\Rightarrow \left[\mathbb{Q}(\gamma) : \mathbb{Q}\right] = 2^r$

Dobling av kube: innebærer å konstruere $\sqrt[3]{2}$

$\deg(\sqrt[3]{2}, \mathbb{Q}) = 3 \neq 2^r$.

Sirkelens kvadratur: innebære å konstruere π

$\deg(\pi, \mathbb{Q}) = \infty$.

Vinkelens tredeling: $\cos(3\theta) = 4\cos^3\theta - 3\cos\theta$

innebærer å konstruere α der

$4\alpha^3 - 3\alpha - \cos(3\theta) = 0$

irreduksibel for de fleste valg av θ

$x^3 - bx^2 + cx$
$-ax^2 + abx - ac$

f.eks $3\theta = \frac{\pi}{3}$, $\cos\left(\frac{\pi}{3}\right) = \frac{1}{2}$

$8x^3 - 6x - 1 = 0$

irreduksibel $/\mathbb{Q}$

$p(x) = 8x^3 - 6x - 1$ er irredusibel / $\mathbb{Q}$

1) $f(x) \in \mathbb{Z}[x] \iff f(x) = \sum_{i=0}^{n} a_i x^i$, $\gcd(a_0, \dots, a_n) = 1$.
primitiv

2) R integritetsområde $\Rightarrow$ $R[x]$ integritetsområde

3) $\mathbb{Z}[x] \xrightarrow{\psi_p} \mathbb{Z}_p[x]$ $\quad f(x) \longmapsto f(x) \pmod p$
Reduksjonshomomorf

4) $f(x), g(x) \in \mathbb{Z}[x]$ primitiv $\Rightarrow$ $f(x) \cdot g(x)$ primitiv.

Bevis: Anta $f(x)g(x)$ ikke primitiv $\Rightarrow \psi_p(f(x)g(x)) = 0$ for noen primtall p. Men

$$\psi_p(f(x)g(x)) = \psi_p(f(x))\,\psi_p(g(x))$$

og $\mathbb{Z}_p[x]$ integritetsområde

$\Rightarrow \psi_p(f(x)) = 0$ eller $\psi_p(g(x)) = 0$

Motsigelse siden f og g er primitive

5) Anta $p(x) = f(x)g(x) \in \mathbb{Q}[x]$. La d_1, d_2 være fellesnevner for koeffisientene i f, henholdsvis g.

$\Rightarrow d_1 f, d_2 g \in \mathbb{Z}[x]$

$\Rightarrow d_1 f = c_1 f'$, $d_2 g = c_2 g'$ hvor f', g' primitive

$\Rightarrow p(x) = f(x)g(x) = \frac{c_1 c_2}{d_1 d_2} f'(x) g'(x)$

Kan anta $\gcd(c_1 c_2, d_1 d_2) = 1$.

$$d_1 d_2 f(x) g(x) = c_1 c_2 f'(x) g'(x)$$

Siden f', g' er primitive og $\gcd(c_1 c_2, d_1 d_2) = 1$ må vi ha

$d_1 d_2 = 1 \Rightarrow f, g \in \mathbb{Z}[x]$

$\Rightarrow$ $p(x)$ er irredusibel over $\mathbb{Z}$ $\Rightarrow$ $p(x)$ irredusibel over $\mathbb{Q}$

$8x^3 - 6x - 1 = l(x)\,q(x)$

hvor $l(x) = x \pm 1$, $2x \pm 1$, $4x \pm 1$ eller $8x \pm 1$

dvs $x = 1, -1, \frac{1}{2}, -\frac{1}{2}, \frac{1}{4}, -\frac{1}{4}, \frac{1}{8}, -\frac{1}{8}$

Ingen av disse er røtter i $p(x)$

$p(1) = +1$ $\quad p(-1) = -3$

$p(\frac{1}{2}) = -3$ $\quad p(-\frac{1}{2}) = 1$

$p(\frac{1}{4}) = \frac{1}{8} - \frac{3}{2} - 1$ $\quad p(-\frac{1}{4}) = -\frac{1}{8} + \frac{3}{2} - 1$

$p(\frac{1}{8}) = \frac{1}{64} - \frac{3}{4} - 1$ $\quad p(-\frac{1}{8}) = -\frac{1}{64} + \frac{3}{4} - 1$