Forelesning 18. mars 2024

Defn. 29.1

$F \leq E$ — E kalles en kroppsutvidelse av F

kropper

Thm 29.3 Kronechers teorem:

$0 \neq f(x) \in F[x] \Rightarrow \exists\ F \leq E$ slik at $\exists\ \alpha \in E$ med $f(\alpha) = 0$.

kropp

Bevis.

1) Kan anta $f(x)$ er irreduserbelt.

2) $(f(x)) \subseteq F[x]$ siden f er irreduserbel (Thm 27.25)

maksimalt ideal

3) Definer

$$\psi : F \longrightarrow F[x]/(f(x))$$
$$a \longmapsto a + (f(x))$$

injektiv siden

$a + (f(x)) = b + (f(x))$

$\Downarrow$

$a - b \in (f(x))$

$\Downarrow$

$a - b = 0$

4) Setter $E = F[x]/(f(x))$ og $\alpha \in E$, $\alpha = x + (f(x))$

$$\Rightarrow \quad f(\alpha) = f(x + (f(x))) = f(x) + (f(x)) = (f(x))$$

Ex $\mathbb{R} \leq \mathbb{C} \ni i$ $\quad \mathbb{R} \leq \mathbb{R}[x]/(x^2+1)$ $\quad i = x + (x^2+1)$

$x^2+1 \in \mathbb{R}[x]$

$$\Rightarrow \quad \mathbb{R}[x]/(x^2+1) \leq \mathbb{C}.$$

Algebraens fundamentalsats sier $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$

Ex. $\mathbb{Q} \leq E = \mathbb{Q}[x]/(x^2-2) = \mathbb{Q}(\sqrt{2})$

$x^2 - 2$

$$\mathbb{Q} + \mathbb{Q}x \longrightarrow \mathbb{Q} + \mathbb{Q}\sqrt{2}$$

$x^2 = 2$ $\qquad$ $\sqrt{2}^2 = 2$.

Defn 29.6 $F \leq E \ni \alpha$

1) $\exists$ polynom $f(x) \in F[x]$ slik at $f(\alpha) = 0$
   $\Rightarrow$: α algebraisk over F
2) $\nexists$ — " —
   $\Rightarrow$: α transcendent over F

Ex. 1) $\sqrt{2}$, $\sqrt[3]{5}$, i, ... etc / $\mathbb{Q}$
2) π, e, π^2+1, ... / $\mathbb{Q}$

Df. 29.11

Algebraisk tall $\Leftrightarrow$ Algebraisk over $\mathbb{Q}$
Transcendent tall $\Leftrightarrow$ Transcendent over $\mathbb{Q}$

Thm. 29.12

$F \leq E \ni \alpha$

$\Phi_\alpha : F[x] \to E$
$f(x) \mapsto f(\alpha)$
evalueringshomomorf

α transcendent / F
$\Updownarrow$
Φ_α er injektiv

$\Phi_\alpha(f(x)) = 0$
$\Updownarrow$
$f(x) = 0$

Thm 29.13

$F \leq E \ni \alpha$ (α algebraisk/F) $\Rightarrow$ $\exists!$ irreduksibel $p(x) \in F[x]$ slik at $p(\alpha) = 0$.

Bevis. Evalueringshomomorfi $\Psi_\alpha : F[x] \to E$, $f(x) \to f(\alpha)$

α algebraisk $\Rightarrow \exists\, p(x) \in F(x)$ slik at $p(\alpha) = \Psi_\alpha(p(x)) = 0$
dvs. $\ker(\Psi_\alpha) \neq 0$.

$F[x]$ PID $\Rightarrow \ker(\Psi_\alpha) = (p(x))$.

Hvis $\Psi_\alpha(f(x)) = 0$ betyr det at $f(x) \in (p(x))$
dvs $p(x) \mid f(x)$.

Hvis $p(x) = r(x)s(x)$ så vil $\psi_\alpha(p(x)) = \psi_\alpha(r(x)\,s(x))$
$= r(\alpha)\cdot s(\alpha) = 0$

Siden E er en kropp og derfor et integritetsområde må vi ha $r(\alpha)=0$ eller $s(\alpha)=0$. (Anta $s(\alpha)=0$).
Det betyr $p(x) \mid s(x)$, men $p(x) = r(x)s(x)$, så $r(x) = C$ (konstant) og $p(x)$ er irreduserbel

Def. 29.14

$F \leq E \ni \alpha$

$p(x) \in F[x]$
irreduserbar
$p(\alpha)=0$

$\Rightarrow \quad p(x) = \mathrm{irr}(\alpha, F)$

Kalles det irreducible polynomet til α over F

Ex $\mathrm{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$ $\quad \mathrm{irr}(1+\sqrt{3}, \mathbb{Q}) = x^2 - 2x - 2$

$\mathrm{irr}(i, \mathbb{R}) = x^2 + 1$ $\quad \mathrm{irr}(\sqrt{2}+\sqrt{3}, \mathbb{Q}) = x^4 - 10x^2 + 1$

$1 = 1$

$x = \sqrt{2} + \sqrt{3}$

$x^2 = 5 + 2\sqrt{6}$

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

$x^4 = (5+2\sqrt{6})^2 = 25 + 20\sqrt{6} + 24 = 49 + 20\sqrt{6}$

$x^5 = (\sqrt{2}+\sqrt{3})(49+20\sqrt{6}) = 49\sqrt{2} + 40\sqrt{3} + 49\sqrt{3} + 60\sqrt{2}$
$= 109\sqrt{2} + 89\sqrt{3}$

$\Rightarrow \quad x^5 - 10x^3 + x = 109\sqrt{2} + 89\sqrt{3} - 110\sqrt{2} - 90\sqrt{3} + \sqrt{2} + \sqrt{3} = 0$

elle $x^4 - 10x^2 + 1 = 49 + 20\sqrt{6} - 50 - 20\sqrt{6} + 1 = 0$

dvs $\mathrm{irr}(\sqrt{2}+\sqrt{3}, \mathbb{Q}) = x^4 - 10x^2 + 1$

abc-formel: $x^2 = \frac{10 \pm \sqrt{100 - 4}}{2} = 5 \pm 2\sqrt{6}$

$F \leq E \ni \alpha$

$p(x) = \text{irr}(\alpha, F)$

$F(\alpha) = F[x]/(p(x))$

Minste kropp $F \leq E$ som inneholder α.

Defn 29.17

$F \leq E \ni \alpha \qquad E = F(\alpha)$: E er en simpel utvidelse av F

Thm 29.18

$F \leq E = F(\alpha)$

α algebraisk $\Rightarrow \forall \beta \in E = F(\alpha)$ har vi $\exists! b_0, \dots, b_{n-1} \in F$ slik at

$p(x) = \text{irr}(\alpha, F)$

$\deg p = n$

$$\beta = b_0 + b_1\alpha + \dots + b_{n-1}\alpha^{n-1}$$

Bevis

La $p(x) = a_0 + \dots + a_n x^n$, dvs $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$

Det betyr $\alpha^{n+1} = \frac{1}{a_n}\left(-a_0\alpha - a_1\alpha^2 - \dots - a_{n-1}\alpha^n\right)$

$$= \frac{1}{a_n}\left(-a_0\alpha - a_1\alpha^2 - \dots - a_{n-1}\left(\frac{1}{a_n}(-a_0 - \dots - a_{n-1}\alpha^{n-1})\right)\right)$$

Så alle elementer i $F(\alpha)$ kan skrives som en lineær kombinasjon av $1, \alpha, \dots, \alpha^{n-1}$.

Anta

$$\beta = b_0 + b_1\alpha + \dots + b_{n-1}\alpha^{n-1} = b_0' + b_1'\alpha + \dots + b_{n-1}'\alpha^{n-1}$$

$$\Rightarrow g(x) = (b_0 - b_0') + \dots + (b_{n-1} - b_{n-1}')x^{n-1} \in \ker(\Psi_\alpha)$$

Vi har $\ker(\Psi_\alpha) = (p(x))$, $\deg(p(x)) = n > \deg(g(x))$

$\Rightarrow g(x) = 0$.

Ex. $p(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$

irreducibelt siden $p(0) = 1$, $p(1) = 1$.

$$\mathbb{Z}_2 \in E = \mathbb{Z}_2[x]/(p(x)) = \mathbb{Z}_2(\alpha)$$

$$\mathbb{Z}_2(\alpha) = \{0, 1, \alpha, 1+\alpha\} \qquad \alpha^2 = 1+\alpha.$$

Kropp med 4 elementer

Addisjon: $\mathbb{Z}_2 \times \mathbb{Z}_2$

Multiplikasjon: $\mathbb{Z}_2(\alpha)^* \simeq \mathbb{Z}_3$.

Oppsummering

$p(x) = \mathrm{irr}(\alpha, F)$ $\alpha \in E$ alg. utv. delse

Endelig: $E = F(\alpha_1, \ldots, \alpha_n)$

VI

$$F(\alpha) \simeq F[x]/(p(x)) = \langle 1, \alpha, \alpha^2, \ldots, \alpha^{n-1} \rangle$$

basis for vektorrom/F

simpel VI

F

Def 31.1

$F \leq E \iff \forall \alpha \in E, \exists\ p(x) = \mathrm{irr}(\alpha, F)$, deg $p = n$

algebraisk utvidelse

dvs. alle elementer er algebraiske

Def 31.2

$F \leq E \iff [E : F] = \dim_F(E)$ (som vektorrom) $< \infty$.

endelig utvidelse

Thm. 31.3 En endelig utvidelse $F \leq E$ er algebraisk

Bevis La $\alpha \in E$ og anta $[E:F] = n$. Det betyr at

$\{1, \alpha, \ldots, \alpha^n\}$

lineært avhengig

$\Rightarrow \exists\, a_0, \ldots, a_n \in F$ slik at $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + a_n\alpha^n = 0$

dvs $f(\alpha) = 0$ for $f(x) = a_0 + a_1 x + \cdots + a_n x^n$

□.

Merk: En algebraisk utvidelse trenger ikke å være endelig

$\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots)$

algebraisk, men ikke endelig

Thm. 31.4

$$F \leq E \leq K \quad \Rightarrow \quad [K:F] = [K:E][E:F]$$

$\xRightarrow[\text{Cor 31.7}]{}$ $F \leq F(\alpha) \leq E \ni \alpha$ (β) $\Rightarrow \deg(\beta, F) \mid \deg(\alpha, F)$

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

Men $F \leq F(\beta) \leq F(\alpha)$ gir

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

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

$\Rightarrow \deg(\beta, F) \mid \deg(\alpha, F)$

Merk: $F \leq E \ni \alpha$

$F(\alpha)$ er den minste kroppen

- som inneholder F
- som inneholder α.

Thm 31.11

$F \leq E$ algebraisk $\qquad \dim_F(E) < \infty \iff E = F(\alpha_1, \ldots, \alpha_n)$

Bevis $\Leftarrow$ $\quad [E:F] = [E : F(\alpha_1, \ldots, \alpha_{n-1})]\,[F(\alpha_1, \ldots, \alpha_{n-1}) : F(\alpha_1, \ldots, \alpha_{n-2})]$

$\cdots \quad [F(\alpha_1) : F]$

Hver av faktorene representerer en algebraisk enkel utvidelse og er endelig $\Rightarrow [E:F) < \infty$

$\Rightarrow$ Anta $\dim_F(E) < \infty$ dvs $[E:F] < \infty$

Velg $\alpha_1 \in E$, $\alpha_1 \notin F$. Det gir $F \leq F(\alpha_1) \leq E$ og α_1 algebraisk

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

Hvis $[E : F(\alpha_1)] > 1$, gjenta prosessen. Siden $[E:F) < \infty$ får vi

$$E = F(\alpha_1, \ldots, \alpha_r)$$

Noen eksempler

$$\mathbb{Q} \leq \mathbb{Q}\left(\tfrac{-1+i\sqrt{3}}{2}\right) \leq \mathbb{Q}(i, \sqrt{3})$$

$$\left(\tfrac{-1+i\sqrt{3}}{2}\right)^2 = \frac{1 - 2i\sqrt{3} - 3}{4} = \frac{-1-i\sqrt{3}}{2} = -\left(\tfrac{-1+i\sqrt{3}}{2}\right) - 1$$

$\text{irr}\left(\tfrac{-1+i\sqrt{3}}{2}, \mathbb{Q}\right) = x^2 + x^2 + 1$

$$\left[\mathbb{Q}(i,\sqrt{3}) : \mathbb{Q}\left(\tfrac{-1+i\sqrt{3}}{2}\right)\right] = 2$$

$\mathbb{Q}(i,\sqrt{3}) = \mathbb{Q}\left(\tfrac{-1+i\sqrt{3}}{2}, i\right)$ og $\text{irr}\left(i, \mathbb{Q}\left(\tfrac{-1+i\sqrt{3}}{2}\right)\right) = x^2 + 1$

$$\left[\mathbb{Q}(i,\sqrt{3}) : \mathbb{Q}\right] = \left[\mathbb{Q}(i,\sqrt{3}) : \mathbb{Q}\left(\tfrac{-1+i\sqrt{3}}{2}\right)\right]\left[\mathbb{Q}\left(\tfrac{-1+i\sqrt{3}}{2}\right) : \mathbb{Q}\right]$$

$$= 2 \cdot 2 = 4.$$

$f(x) \in \mathbb{R}[x]$, $f(x) = a_0 + \cdots + a_n x^n$

$\Rightarrow \exists\, \beta \in \mathbb{C}$ slik at $f(\beta) = 0$

Bevis Hvis $a_0 = 0$ så er $f(0) = 0$.

Anta $a_0 \neq 0$. La $x \in re^{i\theta}$, $\theta \in [0, 2\pi\rangle$

$\Rightarrow f(x) = a_0 + a_1 r e^{i\theta} + \cdots + a_n r^n e^{in\theta}$

Velg r slik at $|a_1 r e^{i\theta} + \cdots + a_n r^n e^{in\theta}| < |a_0| \quad \forall\, \theta \in [0, 2\pi\rangle$

Det betyr at $f(re^{i\theta}) \neq 0 \quad \forall\, \theta \in [0, 2\pi\rangle$

Velg så r så stor at

$$|a_0 + a_1 r e^{i\theta} + \cdots + a_{n-1} r^{n-1} e^{i(n-1)\theta}| << |a_n r^n|$$

$\Rightarrow f(re^{i\theta})$ for $\theta \in [0, 2\pi\rangle$ beskriver n runder rundt Origo.

Ved skjæringssetningen må det finnes r og θ slik at $f(re^{i\theta}) = 0$.