Forelesning, 3 april 2024

Endelige kropper: - $|F| = p^n$
- Opp til iso; finnes én kropp av orden p^n
- F^*: syklisk gruppe

Ex. $F = \mathbb{F}_3$ $\mathbb{F}_3[X] \ni f(x)$ $\deg(f) = 2$

irreduserbel

x^2+1, ~~x^2+2~~, ~~x^2+x+1~~, x^2+x+2

~~x^2+2x+1~~, x^2+2x+2

$f(\alpha) = \alpha^2+1 = 0$ $\mathbb{F}_3(\alpha) = \mathbb{F}_3 + \alpha\mathbb{F}_3$

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

$= a^2+a+2-b^2 + (2a+1)b\alpha = 0$

$\overset{(a=1)}{=} 1-b^2 + 0\cdot\alpha = 0$ for $b=1,2$

x^2+x+2 har røtter $1 \pm \alpha$

x^2+1 har røtter $\pm\alpha$

x^2+2x+2 har røtter $2 \pm \alpha$

Thm 33.1

$F \leq E$

$[E:F] = n \Rightarrow |E| = q^n$ $\left(= |F \times F \times \cdots \times F| = |F|^n\right)$

$|F| = q$

Cor 33.2

E endelig kropp $\Rightarrow \mathbb{F}_p \leq E$ end.utv., $[E:\mathbb{F}_p] < \infty$

$\text{char}(E) = p$

$E^* \subset E$ (end. kropp)
$E : \mathbb{F}_p$
$|E| = p^n$

E^*: multiplikativ gruppe under multiplikasjon

$|E^*| = p^n - 1$.

Bevis: 1) For $\alpha \in E^*$ har vi $\langle \alpha \rangle \leq E^*$ og ved Lagrange's theorem har vi $|\alpha| \mid p^n - 1$

$$\Rightarrow \alpha^{p^n - 1} = 1$$

$$\Rightarrow \alpha^{p^n} = \alpha$$

dvs α er rot i $x^{p^n} - x \in \mathbb{F}_p[x]$

2) $x^{p^n} - x$ har p^n røtter, inkl. $x = 0$, dvs $p^n - 1$ røtter i E^*

$$\Rightarrow \quad \alpha \in E^* \iff \alpha \text{ er rot i } x^{p^n} - x \in \mathbb{F}_p[x]$$

— o — o — o —

E^*: syklisk gruppe (abelsk)

Bevis

Anta $E^* \cong \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}} = \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k}$

La $\mathbb{Z}_{d_1} = \langle \beta \rangle$. Hvis $\langle \beta \rangle = E^*$, så ok.

Anta $\langle \beta \rangle \neq E^*$ og la $\gamma \in E^* \setminus \langle \beta \rangle$. Anta $|\gamma| = m$ og la $\ell = \operatorname{lcm}(d_1, m)$.

Hvis $d_1 = \ell$ så må $m \mid d_1$ og derfor $\gamma^{d_1} = 1$

Motsigelse siden $x^{d_1} - 1$ har maksimalt d_1 røtter

Dvs $d_1 < \ell$. $(\beta\gamma)^t = 1$ betyr $t = 0$ eller $t = \ell$

$\Rightarrow \exists\, \beta_2 = \beta\gamma$ av orden $\ell > d_1$. Gjenta, siden $|E^*| < \infty$ vil dette stoppe og vi har funnet et element i E^* av orden $|E^*| \Rightarrow E^* \cong \mathbb{Z}_s$.

Cor. 33.6

$F \leq E$ (endelig kropp, end. utv.) $\Rightarrow$ $E = F(\alpha)$ hvor $E^* = \langle \alpha \rangle$

Ex. $\mathbb{F}_3 \leq E$ $\quad [E:\mathbb{F}_3] = 3$ $\quad$ Anta $E = \mathbb{F}_3(\alpha)$, $\text{irr}(\alpha, \mathbb{F}_3) = x^3 + x^2 + 2x + 1 = f(x)$

$f(0) = 1 \quad f(1) = 2 \quad f(2) = 2$

α

α^2

$\alpha^3 = 2\alpha^2 + \alpha + 2$

$\alpha^4 = 2\alpha^3 + \alpha^2 + 2\alpha = \alpha^2 + 2\alpha + 1 + \alpha^2 + 2\alpha = 2\alpha^2 + \alpha + 1$

$\alpha^5 = 2\alpha^2 + 1$

$\alpha^6 = \alpha^2 + 1$

$\alpha^7 = 2\alpha^2 + 2\alpha + 2$

$\alpha^8 = \alpha + 1$

$\alpha^9 = \alpha^2 + \alpha$

$\alpha^{10} = \alpha + 2$

$\alpha^{11} = \alpha^2 + 2\alpha$

$\alpha^{12} = \alpha^2 + \alpha + 2$

$\alpha^{13} = \alpha^3 + \alpha^2 + 2\alpha = (2\alpha^2 + \alpha + 2) + \alpha^2 + 2\alpha = 2 = -1$.

$\Rightarrow \alpha^{26} = 1$.

Lemma 33 8.

$F \leq \overline{F}$ alg. tillukning $\Rightarrow$ $x^{p^n} - x$ har p^n forskjellige røtter i $\overline{F}$.

$\text{char}(F) = p$

Bevis Anta $f(x) = x^{p^n} - x = (x-\alpha)^2 g(x)$

$\Rightarrow f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x)$

dvs $f'(\alpha) = f(\alpha) = 0$

For $f(x) = x^{p^n} - x$ har vi $f'(x) = p^n x^{p^n - 1} - 1 = -1$

$\Rightarrow$ Ingen multiple røtter

Alt. bevis $f(x) = (x-\alpha)\dfrac{x^{p^n} - x}{x-\alpha} = x(x-\alpha)\left(x^{p^n-2} + \alpha x^{p^n-3} + \alpha^2 x^{p^n-4} + \dots + \alpha^{p^n-2}\right)$

$\Rightarrow \dfrac{f(x)}{x(x-\alpha)} = g(x)$ og $g(\alpha) = (p^n - 1)\alpha^{p^n - 1} = \dfrac{p^n - 1}{\alpha} = -\dfrac{1}{\alpha} \neq 0$.

Lemma 33.9

$\text{char}(F) = p \Rightarrow (\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} \quad \forall \alpha, \beta \in F, n \geq 0$

Bevis

$$(\alpha+\beta)^p = \sum_{i=0}^{p} \binom{p}{i} \alpha^i \beta^{p-i} = \alpha^p + \beta^p$$

$$(\alpha+\beta)^{p^2} = ((\alpha+\beta)^p)^p = (\alpha^p + \beta^p)^p = \alpha^{p^2} + \beta^{p^2}$$

$$\vdots$$

etc

Thm 33.10

$\forall p^n \; \exists \; E = GF(p^n)$ s.a $|E| = p^n$

Bevis.

$\mathbb{F}_p \subseteq K$ inneholder alle røttene til $x^{p^n} - x$.

$\alpha, \beta \in K \quad (\alpha+\beta)^{p^n} - (\alpha+\beta) = (\alpha^{p^n} - \alpha) + (\beta^{p^n} - \beta) = 0$

$(\alpha\beta)^{p^n} = \alpha^{p^n} \cdot \beta^{p^n} = \alpha\beta$

$(-\alpha)^{p^n} = (-1)^{p^n} \alpha^{p^n} = (-1)^{p^n} \cdot \alpha = -\alpha$

(hvis p odd, ellers $p=2$)

$0^{p^n} - 0 = 0, \quad 1^{p^n} - 1 = 0$

$\left(\frac{1}{\alpha}\right)^{p^n} = \frac{1}{\alpha^{p^n}} = \frac{1}{\alpha}$

$\Rightarrow$ K kropp, $|K| = p^n$

Cor 33.11

F kropp, $|F| = p^r$, $n \geq 0$ $\exists$ $f(x) \in F[x]$ irredusibel, $\deg(f) = n$,

Bevis

Thm 33.10 $\Rightarrow \exists \; \mathbb{F}_p \leq K$, $|K| = p^{rn}$, K består av alle røttene til $x^{p^{rn}} - x$

$\alpha \in F$ er rot i $x^{p^r} - x$

$\Rightarrow \alpha^{p^{rn}} = (\alpha^{p^r})^{p^{r(n-1)}} = \alpha^{p^{r(n-1)}} = \cdots = \alpha^{p^r} = \alpha$

$\Rightarrow \alpha \in K$ dvs. $F \leq K$.

$[K:F] = h$ sida $p^{rn} = (p^r)^n$

K simpel/$_F$ $\Rightarrow K = F(\beta)$, $\beta \in K \Rightarrow \deg(\text{irr}(\beta, F)) = n$.

Thm 33.12

p primtall, $n \in \mathbb{Z}^+$ $\Rightarrow$ $E \simeq E'$

$|E| = |E'| = p^n$

kropper

Bevis

$\mathbb{Z}_p \leq E$, $\mathbb{Z}_p \leq E'$ (simple utvidelser av grad n) $\Rightarrow$ $\exists$ $f(x) \in \mathbb{Z}_p[x]$ irreduksibel, $\deg(f) = n$ og $E \simeq \mathbb{Z}_p[x]/(f(x))$

Alle elementer i E er røtter i $x^{p^n} - x$ $\Rightarrow$ $f(x) \mid x^{p^n} - x$

Alle elementer i E' er røtter i $x^{p^n} - x$

$\Rightarrow$ E' inneholder røttene til $f(x)$

$\Rightarrow$ E' inneholder alle elementer i E

Siden $|E| = |E'|$ $\Rightarrow$ $E \simeq E'$

— o — o — o —

$\mathbb{Z}_p \leq E$, $|E| = p^n$.

E kropp

$\Downarrow$ end. utv. av end. kropper er simple

$E = \mathbb{Z}_p(\alpha)$

$f(x) = \operatorname{irr}(\alpha, \mathbb{Z}_p) \in \mathbb{Z}_p[x]$

$\deg(f) = n$

$E \simeq \mathbb{Z}_p[x]/f(x)$

$\Downarrow$ $E^* \simeq \mathbb{Z}_{p^n - 1}$

Alle elementene β i E oppfyller $\beta^{p^n - 1} = 1$ eller $\beta^{p^n} - \beta = 0$ dvs rotte i $x^{p^n} - x$.

$\Longrightarrow$ Røttene til $f(x)$ er rotter i $x^{p^n} - x$

$x^{p^n} - x = f(x)\, g(x)$

$E \simeq E'$

$\Uparrow$

$\mathbb{Z}_p[x]/(f(x)) \xrightarrow{\sim} E'$

$\Uparrow$ $\mathbb{Z}_p[x]/f(x) \hookrightarrow E'$, $|\mathbb{Z}_p[x]/f(x)| = |E'|$

E' inneholder rotter til $f(x)$

$\Uparrow$ E' inneholder rotter til $x^{p^n} - x$

Ex.

$$\mathbb{F}_3[x]/(x^2+1) \longrightarrow \mathbb{F}_3[y]/(y^2+2y+2)$$

$$x \longmapsto y+1.$$

$$0 = x^2+1 \longmapsto (y+1)^2+1 = y^2+2y+2 = 0$$

Ex

$$\mathbb{F}_2[x]/(x^3+x+1) \longrightarrow \mathbb{F}_2[y]/(y^3+y^2+1)$$

$$x \longmapsto y^2+1$$

$$x^3+x+1 \longmapsto (y^2+1)^3+(y^2+1)+1 = y^6+y^4+y^2+1+y^2+1+1 = y^6+y^4+1$$

$$(y^3+y^2+1)^2 = y^6+y^4+1.$$

$(x \mapsto y^2+1)$

$$\mathbb{F}_2[x]/(x^3+x+1) \longrightarrow \mathbb{F}_2[y]/(y^3+y^2+1)$$

$y^3 = y^2+1$

$y^4 = (y^2+1)y = y^2+1+y$

$1 \longmapsto 1$

$x \longmapsto a_0 + a_1 y + a_2 y^2$

$x^2 \longmapsto (a_0 + a_1 y + a_2 y^2)^2$

$= a_0^2 + a_1^2 y^2 + a_2^2 y^4 + c$

$= (a_0^2 + a_2^2) + a_2^2 y + (a_1^2 + a_2^2) y^2$

$$a_1^3 + a_2^3 + a_1 a_2^2 = \begin{vmatrix} 1 & 0 & 0 \\ a_0 & a_1 & a_2 \\ a_0^2+a_2^2 & a_2^2 & a_1^2+a_2^2 \end{vmatrix}$$

$$x^3+x+1 \longmapsto \left((a_0^2+a_2^2) + a_2^2 y + (a_1^2+a_2^2)y^2\right)(a_0 + a_1 y + a_2 y^2) + a_0 + a_1 y + a_2 y^2 + 1$$

$$= a_0^3 + a_2^2 a_0 + a_0^2 a_1 y + a_2^2 a_1 y + a_0^2 a_2 y^2 + a_2^3 y^2 + a_0 a_2^2 y + a_1 a_2^2 y^2 + a_2^3(y^2+1) + a_1^2 a_0 y^2 + a_2^2 a_0 y^2 + a_1^3(y^2+1) + a_1 a_2^2 (y^2+1) + (a_1^2+a_2^2) a_2 (y^2+y+1) + a_0 + a_1 y + a_2 y^2 + 1$$

$$= (a_0^3 + a_0 a_2^2 + \cancel{a_2^3} + a_1^3 + a_1 a_2^2 + a_1^2 a_2 + \cancel{a_2^3} + a_0 + 1) + y(a_0^2 a_1 + a_2^2 a_1 + a_0 a_2^2 + a_1^2 a_2 + a_2^3 + a_1) + y^2(a_0^2 a_2 + \cancel{a_2^3} + \cancel{a_1 a_2^2} + a_2^3 + a_1^2 a_0 + a_2^2 a_0 + a_1^3 + \cancel{a_1 a_2^2} + a_1^2 a_2 + \cancel{a_2^3}) = 0$$

$+a_2$

$$a_0^3 + a_0 a_2^2 + a_1^3 + \cancel{a_1 a_2^2} + \cancel{a_1^2 a_2} + a_2 + 1 = 0$$

$$\cancel{a_2} + \cancel{a_0^2 a_2} + \cancel{a_2^3} + a_1^2 a_0 + \cancel{a_2^2 a_0} + a_1^3 + a_1^2 a_2 = 0$$

$$a_0^2 a_1 + \cancel{a_2^2 a_1} + a_0 a_2^2 + a_1^2 a_2 + a_2^3 + a_1 = 0$$

eller

$$a_0 + a_0 a_2 + a_1 + a_2 + 1 = 0$$

$$a_1 a_0 + a_1 + a_1 a_2 = 0 \iff a_1 = 0 \text{ eller } a_0 + a_2 + 1 = 0$$

$$a_0 a_1 + a_0 a_2 + a_2 + a_1 = 0$$

$a_1 = 0$; $a_0 = 1$, $a_2 = 1$ eller $a_0 = 1$, $a_2 = 0$, $a_1 = 0$

omvänt.

dvs $x \longmapsto y^2 + 1$ $\Rightarrow x^3 \longmapsto$

$x^3+x+1 \mapsto (y^2+1)^3 + (y^2+1) + 1$

$= y^6 + y^4 + y^2 + 1 + y^2 + 1 + 1$

$= (y^2+1)^2 + y^2 + y + 1 + 1$

$= y^2 + y + 1 + 1 + y^2 + y = 0$