Setning 93 (33.10)

For hvert primtall p og heltall $n \geq 1$, så $\exists$ en kropp E med p^n elementer og $\mathbb{Z}_p \subseteq E$ er en underkropp.

Bevis: Betrakt $h(x) = x^{p^n} - x$ i $\mathbb{Z}_p[x]$, og la $\tilde{\mathbb{Z}}_p$ være en kropp som inneholder alle røttene til $h(x)$ og $\mathbb{Z}_p \subseteq \tilde{\mathbb{Z}}_p$ er en underkropp (Setn 91).

La $E \subseteq \tilde{\mathbb{Z}}_p$ være mengden av alle røttene av $h(x)$ i $\tilde{\mathbb{Z}}_p$

Påstår: $(E, +|_{E\times E}, \cdot|_{E\times E})$ er en kropp.

La $\alpha, \beta \in E$. Er $\alpha - \beta$, $\alpha\beta \in E$?

Lemma 92

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

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

$$= \begin{cases} \alpha - \beta, & p \text{ odde} \\ \alpha+\beta = \alpha-\beta, & p = 2 \end{cases}$$

$\Rightarrow \alpha - \beta \in E$

$$(\alpha\beta)^{p^n} = \underset{\alpha}{\alpha^{p^n}}\,\underset{\beta}{\beta^{p^n}} = \alpha\beta \Rightarrow \alpha\beta \in E$$

Har at $0, 1$ er røtter i $h(x) \Rightarrow 0, 1 \in E$.

$\Rightarrow E \subseteq \tilde{F}$ er en undering med 1.

La $0 \neq \alpha \in E$. Da $\exists\, \alpha^{-1} \in \tilde{\mathbb{Z}}_p$. Vi har

$$h(\alpha^{-1}) = (\alpha^{-1})^{p^n} - \alpha^{-1} = \underbrace{(\alpha^{p^n})^{-1}}_{\alpha} - \alpha^{-1} = \alpha^{-1} - \alpha^{-1} = 0.$$

$\Rightarrow \alpha^{-1} \in E$

$\Rightarrow E$ er en kropp.

<u>$\mathbb{Z}_p \subseteq E$:</u> $\alpha \in \mathbb{Z}_p$, $\alpha = 0$ er rot i $h(x)$

$\alpha \neq 0$: $\alpha^{p-1} = \overline{1} \Rightarrow \alpha^p = \alpha$

$$\alpha^{p^n} = (\alpha^p)^{p^{n-1}} = \alpha^{p^{n-1}} = \cdots = \alpha \Rightarrow h(\alpha) = 0.$$

$\Rightarrow \mathbb{Z}_p \subseteq E$ □

<u>Merk:</u> Fra Setning 89. vet vi at $\exists$ irred. polynom $q(x)$ over $\mathbb{Z}_p$ slikat

$$E \cong \mathbb{Z}_p[x]/(q(x))$$

Dvs. gitt $n \geq 1$, så $\exists$ irred. polynom $q(x)$ over $\mathbb{Z}_p$ med $\deg q(x) = n$.