"Det finns bare en kropp med p^n elementer."

Setning 94 (33.12)
La p være et primtall og n et heltall med $n \geq 1$. Hvis E og E' er to kropper med p^n elementer, da er $E \simeq E'$

Bevis: Setn 89:

$$\begin{array}{ccccc} \mathbb{Z}_p & \xrightarrow{\varphi \sim} & \operatorname{Im}\varphi = F & \hookrightarrow & E \\ \downarrow & & \downarrow & & \\ \mathbb{Z}_p[x] & \xrightarrow{\tilde{\varphi}} & F[x] & \xrightarrow{\varrho_\alpha} & E \\ a x^n & \longmapsto & \varphi(a) x^n & & \end{array}$$

hvor α er en generator av den sykliske gruppen $(E \setminus \{0\}, \cdot)$. La $\gamma = \varrho_\alpha \cdot \tilde{\varphi}$.
$\Rightarrow$ γ er på $\Rightarrow$

$$E \xleftarrow{\sim}{\gamma} \mathbb{Z}_p[x]/(p(x)) \text{ og}$$

$p(x)$ irred over $\mathbb{Z}_p$ av grad n.

Setn 82 (bevist) $\Rightarrow$ E er røttene i polynomet $x^{p^n} - x \in F[x]$.

Betrakt $x^{p^n} - x \in \mathbb{Z}_p[x]$. Har

$$\begin{aligned} \gamma(x^{p^n} - x) &= \varrho_\alpha \tilde{\varphi}(x^{p^n} - x) \\ &= \varrho_\alpha(\varphi(1_{\mathbb{Z}_p}) x^p - \varphi(1_{\mathbb{Z}_p}) x) \\ &= \varrho_\alpha(1_F x^{p^n} - 1_F x) \\ &= 1_F \alpha^{p^n} - 1_F \alpha = 0. \end{aligned}$$

$\Rightarrow x^{p^n} - x \in \ker\gamma = (p(x)) \Rightarrow p(x) \mid x^{p^n} - x \in \mathbb{Z}_p[x]$.

Tilsvarende som over

$$\begin{array}{ccccc} \mathbb{Z}_p & \xrightarrow{\varphi'} & \operatorname{Im}\varphi' = F' & \hookrightarrow & E' \\ \downarrow & & \downarrow & & \\ \mathbb{Z}_p[x] & \xrightarrow{\tilde{\varphi}'} & F'[x] & \xrightarrow{\varrho_{\alpha'}} & E' \end{array}$$

hvor α' er en generator for den sykliske gruppen $(E' \setminus \{0\}, \cdot)$. La $\gamma' = \varrho_{\alpha'} \tilde{\varphi}'$. Og E' er røttene i polynomet

$$x^{p^n} - x \in F'[x].$$

La β være en rot i $\tilde{\varphi}'(p(x))$.

$$\tilde{\varphi}'(p(x)) \mid \tilde{\varphi}'(\underbrace{x^{p^n} - x}_{\in \mathbb{Z}_p[x]}) = x^{p^n} - x \in F'[x]$$

Betrakt $\mathbb{Z}_p[x] \xrightarrow{\tilde{\varphi}'} F'[x] \xrightarrow{\varrho_\beta} E'$ og la $\delta = \varrho_\beta \tilde{\varphi}'$.

Her at

$$\delta(p(x)) = \varrho_\beta \tilde{\varphi}'(p(x)) = \tilde{\varphi}'(p(x))(\beta) = 0$$

$\Rightarrow p(x) \in \ker\delta \Rightarrow (p(x)) \subseteq \ker\delta \subseteq \mathbb{Z}_p[x]$

$(p(x))$ maksimalt $\Rightarrow \ker\delta = (p(x))$ eller $\ker\delta = \mathbb{Z}_p[x]$.

↑ umulig.

$$\Rightarrow \underbrace{\mathbb{Z}_p[x]/(p(x))}_{p^n \text{ elem.}} \cong \operatorname{Im}\delta \subseteq E'$$

likhet. ↑ p^n elem.

$\Longrightarrow E' \simeq \mathbb{Z}_p[x]/(\varphi(x)) \simeq E.$ $\square$