Endelig kropper

Setning 89

La E være en endelig kropp.

(a) $\exists F \subseteq E$ underkropp med $F \simeq \mathbb{Z}_p$ for et primtall p. (p = karakteristikken til E (og F)).

(b) E vektorrom over $F \simeq \mathbb{Z}_p$.

(c) E har p^n elementer der $n = \dim_F E$.

(d) $E \simeq \mathbb{Z}_p[x]/(p(x))$ for et irredusibelt polynom $p(x)$ over $\mathbb{Z}_p$ av grad n.

Bevis: (a) Definer $\sigma : \mathbb{Z} \longrightarrow E$ gitt ved at

$$\sigma(z) = \begin{cases} \underbrace{1 + 1 + \cdots + 1}_{z \text{ ganger}}, & z > 0 \\ 0, & z = 0 \\ \underbrace{(-1) + (-1) + \cdots + (-1)}_{|z| \text{ ganger}}, & z < 0 \end{cases}$$

Oppgave: σ er en ringhomomorfi.

$\Rightarrow \ker \sigma = n\mathbb{Z}$ for en $n \in \mathbb{Z}$ og $\mathbb{Z}/\ker \sigma \simeq \operatorname{Im} \sigma \subseteq E$

$\operatorname{Im} \sigma$ underring av $E \Rightarrow \operatorname{Im} \sigma$ integritetsområde.

$$\begin{array}{c} \operatorname{Im}\sigma \\ \wr\wr \\ \mathbb{Z}/n\mathbb{Z} \quad \text{———— " ————} \end{array}$$

$\Rightarrow \mathbb{Z}/n\mathbb{Z}$ er en kropp.

Setn 60 $\Rightarrow n = p$ primtall $\Rightarrow \mathbb{Z}_p \simeq \operatorname{Im} \sigma = F \subseteq E$.

La sammensetningen $\mathbb{Z}_p \xrightarrow{\sim} \operatorname{Im} \sigma \hookrightarrow E$ betegnes med φ.

(b) Definer for $\alpha \in \mathbb{Z}_p$ og $x \in E$

$$\alpha \cdot x = \psi(\alpha) x \quad \text{(multiplikasjon i } E\text{)}.$$

<u>Oppgave:</u> E vektorrom over $\mathbb{Z}_p$.

(c) E endelig $\Rightarrow$ E har en endelig basis over $\mathbb{Z}_p$. La $\mathcal{B} = \{e_1, e_2, \ldots, e_n\}$ være en basis over $\mathbb{Z}_p$, $n = \dim_{\mathbb{Z}_p} E$. Ethvert element i E kan

skrives entydig på formen

$$\alpha_1 \cdot e_1 + \alpha_2 \cdot e_2 + \cdots + \alpha_n \cdot e_n, \quad \alpha_i \in \mathbb{Z}_p.$$

p valg

$\Rightarrow$ E har p^n elementer.

(d) E endelig kropp $\xRightarrow{\text{Setn 82}}$ $(E \setminus \{0\}, \cdot)$ syklisk gruppe. La $E \setminus \{0\} = \langle \alpha \rangle$ for en $\alpha \in E$. Definer

$$\gamma : \mathbb{Z}_p[x] \longrightarrow E$$

som sammensetningen $\mathbb{Z}_p[x] \xrightarrow{\tilde{\psi}} F[x] \xrightarrow{\varphi_\alpha} E$ der

$$a x^i \xrightarrow{\tilde{\psi}} \psi(a) x^i \xrightarrow{\varphi_\alpha} \psi(a) \alpha^i$$

<u>Oppgave:</u> γ er en ringhomomorfi.

Siden α er en generator for $E \setminus \{0\}$, så er γ på. Dette gir at

$$\mathbb{Z}_p[x] / \operatorname{Ker} \gamma \simeq \operatorname{Im} \gamma = E \leftarrow \text{kropp.}$$

Setn 87 $\Rightarrow$ $\operatorname{Ker} \gamma = (p(x))$ for et irredusibelt polynom $p(x)$ over $\mathbb{Z}_p$.

<u>Har:</u> $\dim_{\mathbb{Z}_p} E = \deg p(x) = n.$ $\square$