

(Diskret matte D, ht16: F26, to 24 nov 2016)

Faktorsatsen: Om $f(x) \in F[x]$:

$$(x - \alpha) \mid f(x) \Leftrightarrow f(\alpha) = 0 \text{ i } F.$$

Så polynom av grad $n \geq 0$ i $F[x]$ har högst n nollställen i F .

Ett polynom $f(x) \in F[x]$, F en kropp, med $\deg f(x) \leq 3$ är irreducibelt omm det saknar nollställe i F (om $\deg f(x) > 3$ kan det ha faktorer av högre grad än 1).

Om F är en **ändlig kropp** är F 's **karakteristik** $p = o_+(1)$ (ordningen under addition), ett primtal. Då gäller för varje $a \in F, n \in \mathbb{Z}$ att $na = \underbrace{a + \dots + a}_{n \text{ st}} = 0$ omm $a = 0$ eller $p \mid n$, så xa är definierad för alla $x \in \mathbb{Z}_p$.

Det gäller

$$\begin{array}{ll} |F| = p^r & \text{något } r \geq 1 \\ (F, +) \approx C_p \times \dots \times C_p \quad (r \text{ st}) & r\text{-dimensionellt vektorrum över } \mathbb{Z}_p \\ (F \setminus \{0\}, \cdot) \approx C_{p^r-1} & \text{multiplikativa gruppen är cyklisk} \end{array}$$

För varje $r \geq 1$ och primtal p finns **precis en** kropp F med $|F| = p^r$

Ett **primitivt element** i F : $f \in F$ med $(F \setminus \{0\}, \cdot) = \langle f \rangle$, dvs ett genererande element i $(F \setminus \{0\}, \cdot)$

Om $k(x) \in F[x]$, $\deg k(x) = r$, fås en ekvivalensrelation $\sim$ i $F[x]$:

$$f(x) \sim g(x) \Leftrightarrow k(x) \mid (f(x) - g(x))$$

$|F|^r$ st ekvivalensklasser, bestående av de polynom som ger samma rest (av grad $< r$) vid division med $k(x)$. Klasserna identifieras ofta med denna rest,

$$F[x]/(k(x)) = \{[a_{r-1}x^{r-1} + \dots + a_1x + a_0] \mid a_i \in F \text{ för } i = 0, \dots, r-1\}.$$

Med $[f(x)] \circ [g(x)] = [f(x) \circ g(x)]$, $\circ = +, \cdot$

(dvs "räkna som vanligt och tag resten vid division med $k(x)$ ") är $F[x]/(k(x))$ en **ring**.

$F[x]/(k(x))$ är **en kropp** $\Leftrightarrow k(x)$ är **irreducibelt**.

"Man **utvidgar** F med α som uppfyller $k(\alpha) = 0$ "

(som kroppen $\mathbb{R}$ utvidgas med i (som uppfyller $i^2 + 1 = 0$) till kroppen $\mathbb{C} \approx \mathbb{R}[x]/(x^2 + 1)$.)

$k(x) \in F[x]$ är ett **primitivt irreducibelt polynom** om x (egentligen $[x]$) är ett primitivt element i $F[x]/(k(x))$.