NB! Alle irredusible polynomer vi har sett så langt har hatt distinkte røtter (altså: ingen røtter med høyere multiplisitet.

Vi skal se at dette alltid holder for kropper F med $\operatorname{char} F = 0$.

Formell derivasjon av polynomer

(fungerer over alle kropper, også endelige)

$$f(x) = a_n x^n + \dots + a_1 x + a_0$$

$$f'(x) := a_n n x^{n-1} + \dots + a_1 \qquad \deg f'(x) \leq \deg f(x) - 1$$

($=$ når $\operatorname{char} F = 0$)

Følgende regler holder: $(af+bg)' = af' + bg'$ $\qquad a,b \in F$

$(fg)' = f'g + fg'$ $\qquad f,g \in F[x]$

Eks. $\operatorname{char} F = 5$ $\quad (2x^5 + 3x)' = 3$

La $f(x) \in F[x]$, og E være rotkroppen til F

α rot av $f(x)$.

La m = max. heltall s.a. $(x-\alpha)^m$ er faktor. Da er m <u>multiplisiteten</u> til α (som rot i $F[x]$). Hvis $m=1$, kalles α simpel (enkel) rot

---

NB! Polynomer $\neq$ polynomielle funksjoner (likhet når $|F| = \infty$)

eks: over $\mathbb{Z}_2$: $\quad f(x) = x^2 + x$

$f(x) = 0$ $\qquad$ representerer samme funksjon

Teorem 3.3/3.4

La $f(x) \in F[x]$ ($\deg f(x) \geq 1$) og E rotkroppen til $f(x)$.

a) En rot $\alpha \in E$ er multippel $\Leftrightarrow f'(\alpha) = 0$ i E.

b) Hvis $f(x)$ irredusibel: $f(x)$ har en multippel rot $\Leftrightarrow f'(x) \equiv 0$.

Bevis: a) α rot: $f(x) = (x-\alpha)g(x)$ i $E[x]$

$$\Downarrow$$

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

Dermed α mult. rot $\Leftrightarrow g(\alpha) = 0 \Leftrightarrow f'(\alpha) = 0$.

b) Anta $\alpha \in E$ rot. $f'(x) = g(x) + (x-\alpha)g'(x)$

$\Leftarrow$) $f'(x) \equiv 0 \Rightarrow g(\alpha) = 0 \Rightarrow \alpha$ er multippel rot.

$\Rightarrow$) α multippel rot $\overset{(a)}{\Rightarrow} f'(\alpha) = 0$. Men: $\deg f'(x) < \deg f(x)$

og $f(x)$ er min. polynomet til α (egentlig $a f(x)$, s.a. $a f(x)$ monisk).

$\Rightarrow f'(x) \equiv 0$.

Kor. 3.5.

Et irredusibelt polynom $f(x) \in F[x]$ har

a) bare simple røtter når char $F = 0$

b) multiple røtter $\Leftrightarrow \exists g(x)$ s.a. $f(x) = g(x^p)$ når char $F = p \neq 0$.

Bevis:

La $f(x) = a_n x^n + \dots + a_1 x + a_0$

$f'(x) = a_n n x^{n-1} + \dots + a_1$

$f(x)$ har multiple røtter $\Leftrightarrow f'(x) \equiv 0 \Leftrightarrow i a_i = 0$ for $i = 1, \dots, n$.

Hvis char $F = 0$ $\quad ia_i = 0 \quad i = 1, \dots, n$

$\Leftrightarrow f(x) = a_0$ $\not\ast$ $(\deg f(x) \geq 1)$.

Altså: bare simple røtter når char $F = 0$.

Hvis char $F = p \neq 0$ $\quad ia_i = 0$ for $i = 1, \dots, n$

$\Updownarrow$

For hver i $\quad a_i = 0$ eller $p | i$ $\quad$ (altså $a_i = 0$ for $a_i x^i$ når $p \nmid i$)

$\Updownarrow$

$f(x) = g(x^p)$

Endelige kropper

Husk (fra TMA4150): Endelig kropp med p^n elementer $F \cong \mathbb{Z}_p[x]/(p(x))$

der $p(x)$ er irredusibelt polynom av grad n

Vi skal se: 1) $\exists$ unik kropp (opp til iso) med p^n elementer:

Kalles Galoiskroppen $GF(p^n)$, for hver p (primtall) og $n \geq 1$

2) og $GF(p^n)$ er en kroppsutvidelse av $\mathbb{Z}_p$.

3) Det finnes ingen andre endelige kropper.

(Husk $\mathbb{Z}_p$ kropp med p elementer og char $\mathbb{Z}_p = p$).

Teorem 4.2.

F endelig kropp

a) char F er et primtall p, og det finnes en innbedding $\mathbb{Z}_p \hookrightarrow F$.

b) $|F| = p^n$ for en $n \geq 1$.

Bevis:

a) Må ha char $F \geq 2$ (char $F = 0 \Rightarrow |F| = \infty$, char $F = 1 \Rightarrow 1 = 0$ ⚡)
$(\mathbb{Z} \hookrightarrow F)$
$1 \mapsto 1$

Anta $p = ab$ $1 < a, b < p$.

$0 \neq a = 1 + \dots + 1 \in F$

$0 \neq b = \underbrace{1 + \dots + 1}_{b \text{ ganger}} \in F$ $ab = p = 0$ ⚡

Betrakt

$\phi : \mathbb{Z} \to F$ $n \mapsto n \ (= n \cdot 1)$

ϕ er ringavbildning $\mathbb{Z}/\ker\phi \simeq \operatorname{Im}\phi$

$p \in \ker\phi \Rightarrow (p) \subseteq \ker\phi$. Men p prim $\Rightarrow (p)$ maximal.

så må ha $(p) = \ker\phi$.

$\operatorname{Im}\phi \simeq \mathbb{Z}/(p) \simeq \mathbb{Z}_p$.

b) F er da vektorrom over $\mathbb{Z}_p$ og siden $|F| < \infty$ $|F| = |\mathbb{Z}_p|^n = p^n$.

<u>Def.</u> En kropp F kalles en <u>primkropp</u> hvis den ikke har ekte underkropper. (Hver kropp inneholder en unik primkropp $= \bigcap$ alle underkropper)

<u>Teorem 4.1</u>

Alle primkropper er (opp til iso.) $\mathbb{Z}_p$ eller $\mathbb{Q}$.

Bevis: Kropper med char $F = p$ inneholder $\mathbb{Z}_p$ (se forrige bevis).

Kropper som har char $F = 0$, inneholder $\mathbb{Z}$, og dermed $\mathbb{Q}$.

(oppgave : vis at $\phi : \mathbb{Q} \to K$ ved $\phi\left(\frac{a}{b}\right) =$ $\phi\left(\frac{a}{b}\right) = a b^{-1}$

$\phi(1) = 1$ $\phi(a) = a \ (= a \cdot 1_K)$

det blir en veldefinert ring hom.

Teorem 4.3.

F endelig kropp med $|F| = p^n$ og $F_p \subseteq F$. (der $F_p \simeq \mathbb{Z}/p$)

Betrakt $x^{p^n} - x \in F_p[x]$.

F er rotkroppen til dette polynomet !

(NB! F består faktisk nøyaktig av røttene til dette polynomet).

Bevis: La $\alpha \in F$ $(\alpha \neq 0)$

Da er $F \setminus \{0\} = F^*$ en gruppe med $p^n - 1$ elementer (under multiplikasjon)

Ordenen til hvert element i F^* er da divisor i $p^n - 1$ (Lagrange). Så $\alpha^{p^n - 1} = 1 \Rightarrow \alpha^{p^n} = \alpha$ for alle α

(NB $0^{p^n} = 0$ også ok).

Altså: alle elementene i F er røtter til $h(x)$ $x^{p^n} - x \in F_p[x]$.

og $x^{p^n} - x$ kan ikke ha andre røtter, siden graden er p^n.

$\Rightarrow F$ er rotkroppen til $h(x)$ over F_p

Korollar F, F' endelige kropper med $|F| = |F'| \Rightarrow F \simeq F'$

Bevis: Anta $|F| = p^n = |F'|$

F, F' har da begge primkropper $\simeq \mathbb{Z}/p$ og er dermed begge isomorfe med rotkroppen til $h(x) = x^{p^n} - x \in F_p[x]$

Kalles: Galois-kroppen $GF(p^n)$