(Diskret matte D, ht13: F26, to 28 nov 2013)

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.

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 $na = \underbrace{a + \cdots + a}_{n \text{ st}} = 0$ omm $a = 0$ eller $p \mid n$, så xa är definierad för alla $x \in \mathbb{Z}_p$.

Det gäller

$\lvert F\rvert = p^r$	något $r \geq 1$
$(F,+) \approx C_p \times \ldots \times C_p \quad (r \text{ st})$	r-dimensionellt vektorrum över $\mathbb{Z}_p$
$(F \setminus \{0\}, \times) \approx C_{p^r-1}$	multiplikativa gruppen är cyklisk

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

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

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

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

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

$$F[x]/(k(x)) = \{[a_{r-1}x^{r-1} + \ldots + a_1 x + a_0] \mid a_i \in F \text{ för } i = 0, \ldots, r-1\}.$$

Med $[f(x)] \circ [g(x)] = [f(x) \circ g(x)]$, $\circ = +, \times$
(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 $\mathbb{C}$)

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

Att förstå **partialbråksuppdelning** "algebraiskt"

Låt F vara en kropp och $a(x), f(x), g(x) \in F[x]$, med $\deg a(x) < \deg(f(x)g(x))$ (så $f(x)g(x)$ kan inte vara nollpolynomet) och $\text{sgd}(f(x), g(x)) = 1$.

Då finns $\lambda(x), \mu(x) \in F[x]$ med $1 = \lambda(x)f(x) + \mu(x)g(x)$. Det ger
$a(x) = a(x)\lambda(x)f(x) + a(x)\mu(x)g(x) = (a(x)\lambda(x) + q(x)g(x))f(x) + r(x)g(x)$, där vi satt $a(x)\mu(x) = f(x)q(x) + r(x)$ med $\deg r(x) < \deg f(x)$ (division), så

$$a(x) = s(x)f(x) + r(x)g(x),$$

där $\deg a(x), \deg(r(x)g(x)) < \deg(f(x)g(x))$, så $\deg s(x) < \deg g(x)$.

Dividera med $f(x)g(x)$ (inte i $F[x]$, utan i $F(x)$, kroppen av kvoter av polynom i $F[x]$ (bildad analogt med kroppen $\mathbb{Q}$, kvoter av tal i $\mathbb{Z}$)), så fås

Sats (om partialbråk): Låt $f(x), g(x) \in F[x]$ vara relativt prima och dessutom $a(x) \in F[x]$ ha $\deg a(x) < \deg(f(x)g(x))$.
Då finns $r(x), s(x) \in F[x]$, $\deg r(x) < \deg f(x)$ och $\deg s(x) < \deg g(x)$ så att

$$\boldsymbol{\frac{a(x)}{f(x)g(x)} = \frac{r(x)}{f(x)} + \frac{s(x)}{g(x)}.}$$