(Diskret matte D, ht17: F18, on 4 okt 2017)

Ändliga kroppar

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 $\mathbb{Z}_p$
$(F \setminus \{0\}, \cdot) \approx C_{p^r-1}$	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: $\quad f \in F$ 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 $F[x]$:

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

$\lvert F\rvert^r$ 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 $[f(x)] \circ [g(x)] = [f(x) \circ g(x)]$, $\circ = +, \cdot$
(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 $\mathbb{C} \cong \mathbb{R}[x]/(x^2+1)$.)

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

En kropp med 9 element

Vi såg explicit att två "olika" kroppar av ordning $9 = 3^2$ är isomorfa,

$$\mathbb{Z}_3[x]/(x^2 + x + 2) \cong \mathbb{Z}_3[x]/(x^2 + 1).$$

Både x^2+x+2 och x^2+1 är irreducibla i $\mathbb{Z}_3[x]$, men av dem är bara x^2+x+2 primitivt irreducibelt.

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 $\deg s(x) < \deg g(x)$.

Divideras 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

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

Eisensteins kriterium

Vi har tidigare visat att om $f(x) \in \mathbb{Z}[x]$ och $f(x)$ är reducibelt i $\mathbb{Q}[x]$, så är $f(x)$ också reducibelt i $\mathbb{Z}[x]$. Så om ett polynom är irreducibelt i $\mathbb{Z}[x]$, så är det irreducibelt i $\mathbb{Q}[x]$.
Följande ger en metod att finna irreducibla polynom av godtycklig grad i $\mathbb{Q}[x]$.

Sats (Eisensteins kriterium): Om $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$ och p är ett primtal sådant att $p \mid a_i$ för $i = 0, 1, \ldots, n-1$, $p \nmid a_n$ och $p^2 \nmid a_0$, så är $f(x)$ irreducibelt i $\mathbb{Q}[x]$.

(Det betyder inte att $f(x)$ måste vara irreducibelt i $\mathbb{Z}[x]$. Av beviset följer att förutsättningarna bara ger att om $f(x) = g(x)h(x)$ med $g(x), h(x) \in \mathbb{Z}[x]$, måste en av $g(x)$ och $h(x)$ vara konstant (och därmed inverterbart i $\mathbb{Q}[x]$, men inte säkert i $\mathbb{Z}[x]$).)

Bl.a. såg vi att $x^{p-1} + \ldots + x + 1 = \frac{x^p - 1}{x - 1}$, p primtal, är irreducibla i $\mathbb{Q}[x]$.