(F28, on 26 apr 2006)

Megasatsen för ändliga kroppar
Om F är en ändlig kropp gäller

$\lvert F\rvert = p^r$	något primtal p och något $r \geq 1$
$(F, +) \approx C_p \times \cdots \times C_p \quad (r \text{ st})$	
$(F \setminus \{0\}, \times) \approx C_{p^r-1}$	multiplikativa gruppen är cyklisk

För varje $r \geq 1$ och primtal p finns **precis en** kropp F med $\lvert F\rvert = p^r$. Den kallas **Galoiskroppen** med p^r element, skrivs ofta $GF(p^r)$.

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

Om $k(x) \in \mathbb{Z}_p[x]$, $\;deg\, k(x) = r$, låter vi $\mathbb{Z}_p[x]/(k(x))$ beteckna alla polynom i $\mathbb{Z}_p[x]$ av grad högst $r-1$ där räkningar utförs **modulo** $k(x)$. D.v.s vi inför räkneregeln att $k(x) = 0$.

Ytterligare ett sätt att beskriva samma sak är att i $\mathbb{Z}_p[x]/(k(x))$ räknar vi som i $\mathbb{Z}_p[x]$ och tar sedan resten vid division med $k(x)$.

$\mathbb{Z}_p[x]/(k(x))$ blir en **ring** med p^r element.

$\mathbb{Z}_p[x]/(k(x))$ är **en kropp** $\;\Leftrightarrow\;$ $k(x)$ är **irreducibelt i** $\mathbb{Z}_p[x]$.

På så sätt kan $GF(p^r)$ konstrueras för alla primtal p och $r \geq 1$.

$k(x) \in \mathbb{Z}_p[x]$ är ett **primitivt irreducibelt polynom** om x är ett primitivt element i $\mathbb{Z}_p[x]/(k(x))$.