

(F24, må 24 feb)

Ringen $\mathbb{Z}[i] = \{m + ni \mid m, n \in \mathbb{Z}\}$, de gaussiska heltalen, har **entydig faktorisering**, men det har inte ringen $\mathbb{Z}[i\sqrt{5}]$.

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

Det gäller

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

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 $(F \setminus \{0\}, \times) = \langle f \rangle$, dvs ett genererande element i $(F \setminus \{0\}, \times)$

Om $k(x) \in \mathbb{Z}_p[x]$, $\deg k(x) = r$, fås en ekvivalensrelation $\sim$ i $\mathbb{Z}_p[x]$:

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

p^r st ekvivalensklasser, bestående av alla polynom som ger samma rest (av grad $< r$) vid division med $k(x)$. Ofta identifierar vi klasserna med denna rest.

$$\mathbb{Z}_p[x]/(k(x)) = \{[0], [1], \dots, [p-1], [x], [x+1], \dots, [(p-1)x^{r-1} + \dots + p-1]\}.$$

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

(dvs "räkna som vanligt och tag resten vid division med $k(x)$ "), blir $\mathbb{Z}_p[x]/(k(x))$ en **ring**.

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

"Man utvidgar $\mathbb{Z}_p$ med α som uppfyller $k(\alpha) = 0$ "

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