Sist
F16

$(R, +, \times)$ är en ring om

1) $(R, +)$ är en kommutativ grupp, ident. el. 0

2) $(R, \times)$ sluten, associativ, identitetselement 1

3) distributiva lagar $a(b+c) = ab + ac$
$(a+b)c = ac + bc$

Ex. $\mathbb{Z}$, $\mathbb{Z}_m$, $M_n(\mathbb{R})$, $\mathbb{R}[x]$

$U(R)$: de inverterbara elementen i R

$(U(R), \times)$ är en grupp

Ex $U(\mathbb{Z}) = \{1, -1\}$

$U(\mathbb{Z}_m) = \{r \in \mathbb{Z}_m \mid \operatorname{sgd}(r, m) = 1\}$

$(F, +, \times)$ är en kropp om

1) $(F, +, \times)$ är en ring

2) $(F \setminus \{0\}, \times)$ är en kommutativ grupp

Ex $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}_p$

p primtal

Polynom över en ring R, $R[x]$

$f(x) = a_0 + a_1 x + \dots + a_n x^n$, $a_i \in R$

eller $f = (a_0, a_1, \dots, a_n, \dots)$, $a_i = 0$ om $i > n$

$f(x) + g(x)$, $f(x)g(x)$ "som vanligt"

eller $(a_0, a_1 \dots) + (b_0, b_1, \dots) = (a_0 + b_0, a_1 + b_1, \dots)$

$(a_0, a_1, \dots) \cdot (b_0, b_1, \dots) = (c_0, c_1, \dots)$

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

$f(x)$:s grad, $\deg f(x)$: största n med $a_n \neq 0$

(om alla $a_n = 0$: $-\infty$)

$\deg(f(x) + g(x)) \leq \max(\deg f(x), \deg g(x))$

$\deg(f(x)g(x)) \leq \deg f(x) + \deg g(x)$

$F[x]$ polynom över en kropp F :

$\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$

$R[x]$ och $F[x]$ är ringar

nollpolynomet

Sats: Om $a(x), b(x) \in F[x]$, $b(x) \neq 0$

finns $q(x), r(x) \in F[x]$, $\deg r(x) < \deg b(x)$

med $a(x) = q(x)\, b(x) + r(x)$ entydigt

kvot rest

Polynomdivision, "vanliga algoritmen"