(Diskret matte D, ht17: F16, må 2 okt 2017)

Vi definierar två nya matematiska strukturer, med två operationer,

$(R, +, \cdot)$ är en **ring** om

1) $(R, +)$ är en **kommutativ grupp** med **identitetselement** 0
2) $(R, \cdot)$ är **sluten** och **associativ**, med **identitetselement** 1
3) $\cdot$ är **distributiv** m.a.p. $+$,

$$a(b+c) = ab + ac, \ (a+b)c = ac + bc \quad \text{för alla } a, b, c \in R$$

Exempel: $\mathbb{Z}$, $\mathbb{Z}_m$, $M_n(R)$, $R[x]$ (polynom med koefficienter i en ring R)

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

$(U(R), \cdot)$ är en **grupp**.

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

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

$(F, +, \cdot)$ är en **kropp** om

1) $(F, +, \cdot)$ är en **ring**
2) $(F \setminus \{0\}, \cdot)$ är en **kommutativ grupp**

Exempel: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}_p$ (p primtal)

$R[x]$, mängden av **polynom** över en ring R,

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, \quad a_i \in R$$

$f(x) + g(x)$, $f(x)g(x)$ definieras "som vanligt".
Det är viktigt att inte tänka på polynom som funktioner. T.ex. definierar x och x^2 i $\mathbb{Z}_2[x]$ samma funktion $\mathbb{Z}_2 \to \mathbb{Z}_2$, men de är olika polynom (två polynom är lika om och endast om motsvarande koefficienter är lika).

$f(x)$:s **grad**, $\deg f(x)$, är det **största** n med $a_n \neq 0$ (om alla $a_n = 0$, dvs $f(x)$ är **nollpolynomet**, kan vi låta $\deg f(x)$ vara $-\infty$ (eller odefinierad)).

Om $f(x), g(x) \in R[x]$ gäller

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

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

Om $f(x), g(x) \in F[x]$, polynom över en **kropp** F:

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

$R[x]$ och $F[x]$ är **ringar**.

Polynomdivision i $F[x]$, F en kropp, "vanliga algoritmen"

Sats: Om $a(x), b(x) \in F[x]$, $b(x) \neq 0$ (nollpolynomet),
finns entydigt bestämda $q(x), r(x) \in F[x]$, $\deg r(x) < \deg b(x)$ med

$$a(x) = b(x)q(x) + r(x)$$