(F26, on 19 apr 2006)

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

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

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

$R[x]$ är en ring och kallas **polynomringen** över R.

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:

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

$U(F[x]) \approx F \setminus \{0\}$ (konstanta polynom)

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

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

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

Delbarhet i $F[x]$: $g(x) \mid f(x)$ betyder $f(x) = g(x)d(x)$, för något $d(x) \in F[x]$

Om $a(x), b(x) \in F[x]$ och

i) $d(x) \mid a(x)$, $d(x) \mid b(x)$

ii) $c(x) \mid a(x)$, $c(x) \mid b(x) \Rightarrow c(x) \mid d(x)$

så kallas $d(x)$ en största gemensam delare till $a(x)$ och $b(x)$. Om dessutom

iii) $d(x)$ är **monadiskt**, dvs högstagradskoefficienten är 1

kallas $d(x)$ den **monadiska största gemensam delaren** till $a(x)$ och $b(x)$, skrivs

$$d(x) = sgd\,(a(x), b(x)).$$

Sats: Om inte $a(x) = b(x) = 0$, existerar $sgd\,(a(x), b(x))$ entydigt och är $\lambda(x)a(x) + \mu(x)b(x)$, för några $\lambda(x), \mu(x) \in F[x]$

$d(x), \lambda(x), \mu(x)$ fås med **Euklides algoritm**:

$$\begin{aligned}
a(x) &= q_1(x)b(x) + r_1(x) & deg\, r_1(x) &< deg\, b(x) \\
b(x) &= q_2(x)r_1(x) + r_2(x) & deg\, r_2(x) &< deg\, r_1(x) \\
&\vdots & &\vdots \\
r_{k-3}(x) &= q_{k-1}(x)r_{k-2}(x) + r_{k-1}(x) & deg\, r_{k-1}(x) &< deg\, r_{k-2}(x) \\
r_{k-2}(x) &= q_k(x)r_{k-1}(x)
\end{aligned}$$

Då är $sgd\,(a(x), b(x)) = u \cdot r_{k-1}(x), \quad$ för något $u \in F \setminus \{0\}$.