

(Diskret matte D, ht16: F25, må 21 nov 2016)

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

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

Delbarhet i $F[x]$

$g(x) \mid f(x)$ betyder $f(x) = g(x)h(x)$, för något $h(x) \in F[x]$

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

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

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

iii) $d(x)$ är **moniskt**, dvs högstgradskoefficienten är 1

kallas $d(x)$ en (monisk) **största gemensam delare** till $a(x)$ och $b(x)$,
 $d(x) = \text{sgd}(a(x), b(x))$.

(Alla $d(x)$ som uppfyller i) och ii) kan kallas största gemensamma delare, då inte entydiga.)

Sats: För $a(x), b(x) \in F[x]$, existerar $d(x) = \text{sgd}(a(x), b(x))$ entydigt och
 $d(x) = \lambda(x)a(x) + \mu(x)b(x)$, för några $\lambda(x), \mu(x) \in F[x]$

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

$$a(x) = b(x)q_1(x) + r_1(x) \quad \deg r_1(x) < \deg b(x)$$

$$b(x) = r_1(x)q_2(x) + r_2(x) \quad \deg r_2(x) < \deg r_1(x)$$

$$\vdots \quad \quad \quad \vdots$$

$$r_{k-3}(x) = r_{k-2}(x)q_{k-1}(x) + r_{k-1}(x) \quad \deg r_{k-1}(x) < \deg r_{k-2}(x)$$

$$r_{k-2}(x) = r_{k-1}(x)q_k(x)$$

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

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

Irreducibla polynom i $F[x]$

Om F är en kropp och $f(x) \in F[x]$ säger vi att $f(x)$ är **irreducibelt** om

$$f(x) = g(x)h(x) \Rightarrow \text{precis en av } g(x) \text{ och } h(x) \text{ tillhör } U(F[x])$$

(Jämför $\pm$ primtal i $\mathbb{Z}$.)

Sats: Varje $f(x) \in F[x]$ är en produkt av irreducibla polynom, eller konstant.

Sats: Om $r(x) \in F[x]$ är irreducibelt och $r(x) \mid s_1(x) \dots s_k(x)$ så $r(x) \mid s_i(x)$,
något i , $1 \leq i \leq k$

Sats (Entydig faktorisering): Om $f(x) = g_1(x) \dots g_r(x) = h_1(x) \dots h_s(x)$
i $F[x]$, med $g_i(x), h_j(x)$ irreducibla, så är $r = s$ och $g_i(x) = u_i h_{\pi(i)}(x)$, där
 $u_i \in U(F[x])$, $\pi \in S_r$

Ring $\mathbb{Z}[i] = \{m + ni \mid m, n \in \mathbb{Z}\}$, de **gaussiska heltalen**, har entydig
faktorisering. De irreducibla elementen (”gaussiska primtal”) är precis element
med $m^2 + n^2$ antingen 2, primtal $p \equiv_4 1$ eller q^2 för primtal $q \equiv_4 3$, t.ex.
 $1 - i$, 11 , $2 + 3i$, $5965 + 4736i$.

Ringen $\mathbb{Z}[x]$ har också entydig faktorisering (trots att $\mathbb{Z}$ inte är en kropp). Vi visade att om $f(x) \in \mathbb{Z}[x]$ kan faktoriseras som $g(x)h(x)$ i $\mathbb{Q}[x]$, finns ett rationellt tal α sådant att $\alpha g(x), \alpha^{-1}h(x) \in \mathbb{Z}[x]$.

Ringen $\mathbb{Z}[i\sqrt{5}] = \{m + in\sqrt{5} \mid m, n \in \mathbb{Z}\}$ har **inte** entydig faktorisering. T.ex. är $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ och 2, 3, $1 + i\sqrt{5}$ och $1 - i\sqrt{5}$ är alla irreducibla.