2010-11-18

Kom ihåg: för alla polynom $f, g$, $g \neq 0$, existerar unika $q, r$ sådana att $f = q \cdot g + r$ och $\deg(r) < \deg(g)$.

$$\frac{f}{g} = q + \frac{r}{g} \qquad \frac{10}{4} = 2 + \frac{2}{4}$$

<u>Sats.</u> Låt $f$ vara ett polynom.

$$f(\alpha) = 0 \iff f(x) = (x-\alpha) \cdot g(x)$$

för något polynom $g$.

Faktorsatsen

OBS. "$\iff$". Ena påståendet är sant om det andra är det <u>och tvärtom.</u>

Bevis. "$\Rightarrow$". Antag att $f(\alpha) = 0$.

Dividera $f$ med $(x-\alpha)$:

$$f(x) = (x-\alpha) \cdot g(x) + r, \quad r \text{ konstant}$$

Sätt $x = \alpha$: $f(\alpha) = \underbrace{(\alpha-\alpha) \cdot g(\alpha)}_{=0} + r$

"$\Leftarrow$". Antag $f(x) = (x-\alpha) g(x)$.

Sätt $x = \alpha$: $f(\alpha) = (\alpha-\alpha) \cdot g(\alpha) = 0$.

$\square$

# Faktorisering

motiverande exempel: primtalsfaktorisering

$$195 = \left.\begin{matrix} 5 \cdot 39 \\ = 3 \cdot 65 \end{matrix}\right\} = 5 \cdot 3 \cdot 13$$

<u>Sats</u> (aritmetikens fundamentalsats)
Varje heltal $n > 1$ är på ett unikt sätt en produkt av primtal.

Bevis $\rightsquigarrow$ Övning.

Exempel: $f(x) = x^4 + 2x^3 - x - 2$
har rötterna $x = -2$, $x = 1$, $x = -\frac{1}{2} \pm \frac{\sqrt{3}}{2} i$
Använd faktorsatsen och liggande stolen för att faktoriser~~ing~~a:

$$f(x) = (x+2)(x-1)\left(x + \tfrac{1}{2} - \tfrac{\sqrt{3}}{2} i\right)\left(x + \tfrac{1}{2} + \tfrac{\sqrt{3}}{2} i\right)$$

<u>Sats</u> (algebrans fundamentalsats)
Varje moniskt polynom av grad $n$ kan skrivas på ett unikt sätt som $f(x) = (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$.

($f$ är moniskt om $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$)

Fråga: Om vi inte tilllåter alla komplexa tal som koefficienter i faktoriseringen utan bara t.ex. heltal, är då fortfarande faktoriseringen unik?

**Def** Låt $\mathbb{K} \subseteq \mathbb{C}$. Vi säger att $\mathbb{K}$ är en <u>delkropp</u> om (i) $0 \in \mathbb{K}$

(ii) $1 \in \mathbb{K}$

(iii) om $\forall x, y \in \mathbb{K}$ gäller $x+y \in \mathbb{K}$ och $xy \in \mathbb{K}$

(iv) om $x \in \mathbb{K}$, gäller $-x \in \mathbb{K}$

(v) om $0 \neq x \in \mathbb{K}$ gäller $\frac{1}{x} \in \mathbb{K}$

**Anm.** $x - y = x + (-y) \in \mathbb{K}$

$x/y = x \cdot \frac{1}{y} \in \mathbb{K}$

Dvs. $\mathbb{K}$ är en delmängd av $\mathbb{C}$ där alla fyra räknesätten fungerar.

**Ex** $\mathbb{K} = \mathbb{C}$, $\mathbb{K} = \mathbb{R}$, $\mathbb{K} = \mathbb{Q}$ (de rationella talen)

$\{x \in \mathbb{R} : x = \frac{p}{q} \text{ där } p, q \in \mathbb{Z}, q \neq 0\}$

är alla delkroppar

$\mathbb{K} = \mathbb{Z}$ (heltalen) är ingen delkropp

**Def.** Ett polynom $f$ sägs vara ett <u>polynom över $\mathbb{K}$</u> om dess koefficienter ligger i $\mathbb{K}$.

**Def.** Ett polynom $f$ över $\mathbb{K}$ sägs vara <u>irreducibelt över $\mathbb{K}$</u> om det inte går att skriva $f = g \cdot h$ där $\deg g < \deg f$ och $\deg h < \deg f$.

(för polynom $g, h$ över $\mathbb{K}$)

**Ex.** Om $\deg(f) \leq 1$ så är $f$ irreducibelt över varje $\mathbb{K}$.

Ty: $f = g \cdot h \Rightarrow \deg f = \deg g + \deg h$.

Ex. $f(x) = x^2 + 1. = (x+i)(x-i)$

$f$ är reducibelt över $\mathbb{C}$.

Dock: $f$ är irreducibelt över $\mathbb{R}$.

eftersom om $f$ vore reducibelt över $\mathbb{R}$

så måste $f(x) = (x-a)(x-b)$, $a,b \in \mathbb{R}$

dvs $f$ har minst en reell rot. ↯

$$f(a) = \underset{\substack{\vee\!\!\mid\\ 0}}{a^2} + 1 \geq 1 \neq 0$$

Hjälpsats. Låt $f, g$ vara polynom över $\mathbb{K}$, $g \neq 0$.

Skriv $f = q \cdot g + r$ där $\deg r < \deg g$

Då har även $q$ (och $r$) sina koefficienter i $\mathbb{K}$.

Mer allmänt: $f+g$, $f \cdot g$, $f-g$ har också koefficienter i $\mathbb{K}$.

Bevisskiss: Titta på liggande stolen.

Vi använder bara räknesätten $+, -, \cdot, /$.

Hjälpsats. Låt $f$ vara ett polynom över $\mathbb{K}$.

$f$ kan skrivas som en produkt av irreducibla polynom.

Bevis. Använd induktion.

Basfall: $\deg(f) \leq 1 \Rightarrow f$ är irreducibelt.

$\Rightarrow f = f$. OK.

Induktionssteg. Antag bevisat för alla polynom av grad $\leq n$. Låt $\deg(f) = n+1$.

Fall 1: $f$ irreducibelt över $\mathbb{K} \Rightarrow f = f$. OK.

Fall 2: $f$ reducibelt: $f = gh$, $g$ och $h$ polynom över $\mathbb{K}$

och $\deg g \leq n$, $\deg h \leq n$

$\Rightarrow$ $g$ är produkt av irreducibla polynom
och $h$ är produkt av irreducibla polynom
$\Rightarrow$ $f$ är produkt av irreducibla polynom $\square$

~~Prop~~ **Sats** Varje moniskt polynom $f$ över $\mathbb{K}$ kan skrivas unikt som en produkt av irreducibla polynom över $\mathbb{K}$.
moniska

Bevis. Tag $f = p_1 \cdots p_n = q_1 \cdots q_m$.
Om $p_1 = q_1$ så är $p_2 \cdots p_n = q_2 \cdots q_m$ och $\deg(p_1) = \deg(q_1) > 1$.

Induktion ger att $p_1 \cdots p_n$ och $q_1 \cdots q_m$ är samma faktorisering.

Om $p_1 \neq q_1$: Vi kan anta att $\deg(p_1) \leq \deg(q_1)$
Skriv $q_1 = a \cdot p_1 + b$ med $\deg b < \deg p_1$.

$\Rightarrow$ $p_1 \cdots p_n = (ap_1 + b) q_2 \cdots q_m$

$\Rightarrow$ $p_1(p_2 \cdots p_n - a q_2 \cdots q_m) = b \cdot q_2 \cdots q_m$

$\Rightarrow$ $p_1$ delar VL $\Rightarrow$ $p_1$ delar högerledet och högerledet har mindre grad än $f$ (kolla!)

Enligt induktion är $bq_2 \cdots q_m$ är unik produkt av irreducibla polynom. Denna faktorisering fås genom att faktorisera $b$.
Genom att faktorisera $p_1(p_2 \cdots p_n - a q_2 \cdots q_m)$ ses att $p_1$ ingår i faktoriseringen.
$\deg(p_1) > \deg(b)$ visar att $p_1$ inte fås genom faktorisering av $b$. $\square$