Algebraiska strukturer, 4 mars

REDUCIBLA OCH IRREDUCIBLA POLYNOM

Låt K vara en kropp. Ett icke-konstant polynom $f(x) \in R[x]$ är **irreducibelt över** R eller **irreducibelt i** $R[x]$ om det inte finns polynom $g(x)$ och $h(x)$ i $R[x]$ av grad större än noll så att $f(x) = g(x)h(x)$. Om $f(x) \in R[x]$ är icke-konstant polynom som inte är irreducibelt över R så kallas det **reducibelt över** K eller **reducibelt i** $R[x]$.

Exempel. (a) Varje polynom av grad 1 i $K[x]$ är irreducibelt.

(b) $x^2 + 2$ är irreducibelt i $\mathbb{R}[x]$, men reducibelt i $\mathbb{C}[x]$, ty $x^2 + 2 = (x - i\sqrt{2})(x + i\sqrt{2})$.

(c) varje polynom av grad 2 och 3 är irreducibelt i $K[x]$, där K är en kropp, omm det saknar nollställe i K: om $f(a) = 0$ så är $f(x) = (x - a)g(x)$ och grad $g(x) \geq 1$ varav $f(x)$ är reducibelt, omvänt om $f(x) = g(x)h(x)$ är en faktoruppdelning av $f(x)$ i två icke-konstanta faktorer så måste någon av dessa ha grad 1 och om $g(x) = b_0 + b_1 x$ så är $a = -b_0 b_1^{-1}$ ett nollställe till $g(x)$ och därmed till $f(x)$.

(d) (**Eisensteins kriterium**) Låt $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ vara ett polynom med heltalskoefficienter och låt p vara ett primtal sådant att $p|a_0$, $p|a_1, \ldots, p|a_{n-1}$, p inte delar a_n och p^2 inte delar a_0. Då är $f(x)$ irreducibelt över $\mathbb{Q}$.

UNIK FAKTORISERING AV POLYNOM

Lemma. Om $a(x)$, $b(x)$, $p(x) \in K[x]$, där K är en kropp, och $p(x)$ är irreducibelt så

$$p(x)|a(x)b(x) \Rightarrow p(x)|a(x) \text{ eller } p(x)|b(x)$$

Sats. Varje moniskt icke-konstant polynom i $K[x]$, där K är en kropp, kan skrivas som en produkt av ireducibla moniska polynom. Faktorisering är unik förutom ordningen av faktorerna.

Satsen och lemman bevisas på exakt samma sätt som motsvarande sats och lemma för heltalen.

Exempel. $x^4 - 4 = (x^2 - 2)(x^2 + 2)$ i $\mathbb{Q}[x]$,
$x^4 - 4 = (x - \sqrt{2})(x + \sqrt{2})(x^2 + 2)$ i $\mathbb{R}[x]$,
$x^4 - 4 = (x - \sqrt{2})(x + \sqrt{2})(x + i\sqrt{2})(x - i\sqrt{2})$ i $\mathbb{C}[x]$.

UNIK FAKTORISERINGS OMRÅDE

$\mathbb{Z}$, $K[x]$, där K är en kropp, är standarta exempel på integritetsområde som har unik faktorisering: varje positivt heltal (moniskt polynom) kan skrivas som en produkt av primtal (respektive ireducibla moniska polynom) och sådan faktorisering är unik förutom ordningen av faktorerna.

I ett integritetsområde D säger vi att

- a **delar** b om det finns $c \in D$ så att $b = ac$
- a är en **enhet** om a delar 1 (a har en multiplikativ invers)

- $a \neq 0$ är irreducibelt om a ej är enhet och $a = bc$ innebär att antingen b eller c är en enhet.

Exempel. (a) Enheter i $\mathbb{Z}$ är ± 1. Irreducibla element är $\pm p$ där p är ett primtal.

(b) Enheter i en kropp K är $a \neq 0$, $a \in K$. Irreducibla element saknas.

(c) Enheter i $K[x]$ är konstanta polynom $\neq 0$. Irreducibla element är irreducibla polynom.

Vi säger att D har **unik faktorisering** om

- varje element $a \in D$ kan skrivas som en produkt av irreducibla element $a = p_1 p_2 \dots p_n$
- om $a \in D$ och $a = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t$, där p_i, q_j är irreducibla så är $s = t$ och $p_i = e_i q_i$, där e_i är enheter, vid lämligt numerering av faktorerna.

Exempel. (a) $\mathbb{Z}, K[x]$, där K är en kropp, har unika faktorisering. ($24 = 2 \cdot 2 \cdot 3 \cdot 2 = (-2) \cdot (-3) \cdot 2 \cdot 2$. Här är $-2 = (-1) \cdot 2$, $-3 = (-1) \cdot 3$ och -1 är en enhet i $\mathbb{Z}$.

(b) $\mathbb{Z}[\sqrt{-3}] = \{a + ib\sqrt{3} : a, b \in \mathbb{Z}\}$ saknar unik faktorisering (i är den imäginära enheten).

Bevis. $\mathbb{Z}[\sqrt{-3}]$ är ett integritetsområde (Varför?).

Definiera $N : \mathbb{Z}[\sqrt{-3}] \to \mathbb{Z}^+$ ($\mathbb{Z}^+$ är mängden av icke-negativa heltalen) genom

$$N(a + ib\sqrt{3}) = |a + ib\sqrt{3}|^2 = a^2 + 3b^2.$$

N kallas en norm på $\mathbb{Z}[\sqrt{-3}]$ och uppfyller

- $N(z) \geq 0$ då $z \in \mathbb{Z}[\sqrt{-3}]$,
- $N(z) = 0$ omm $z = 0$,
- $N(z_1 z_2) = N(z_1)N(z_2)$ då z_1, $z_2 \in \mathbb{Z}[\sqrt{-3}]$.

Enheter i $\mathbb{Z}[\sqrt{-3}]$ är lösningar till $zw = 1$, $z, w \in \mathbb{Z}[\sqrt{-3}]$. Vi har att $zw = 1 \Rightarrow N(zw) = 1 \Leftrightarrow N(z)N(w) = 1$ och eftersom $N(z)$ och $N(w)$ är icke-negativa heltal blir den senare ekvivalent med $N(z) = N(w) = 1$, dvs enheter har normen 1. Vidare,

$$N(a + ib\sqrt{3}) = 1 \Leftrightarrow a^2 + 3b^2 = 1 \Leftrightarrow a = \pm 1, b = 0.$$

Klart att ± 1 är enheter i $\mathbb{Z}[\sqrt{-3}]$ och ± 1 är de enda enheter som finns i $\mathbb{Z}[\sqrt{-3}]$.

I $\mathbb{Z}[\sqrt{-3}]$ gäller att

$$4 = 2 \cdot 2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$$

Om vi visar att 2 och $1 \pm i\sqrt{3}$ är irreducibla i $\mathbb{Z}[\sqrt{-3}]$ så visar vi att $\mathbb{Z}[\sqrt{-3}]$ saknar unik faktorisering.

Antag att $1 + i\sqrt{3} = xy$ där $x, y \in \mathbb{Z}[\sqrt{-3}]$. Då

$$4 = N(1 + i\sqrt{3}) = N(x)N(y)$$

vilket visar att $N(x) = 1, 2, 4$. Om $N(x) = 1$ så är x en enhet. Om $N(x) = 4$ så är $N(y) = 1$ och y är en enhet. Om $N(x) = 2$

och $x = a + ib\sqrt{3}$, $a, b \in \mathbb{Z}$, så är $a^2 + 3b^2 = 2$ vilket är omöjligt. Detta ger att $1 + i\sqrt{3} = xy$ gäller i $\mathbb{Z}[\sqrt{-3}]$ omm en av faktorerna är en enhet, dvs $1 + i\sqrt{3}$ är irreducibelt.

På ett liknande sätt visar man att $1 - i\sqrt{3}$ och 2 är irreducibla. Alltså saknar $\mathbb{Z}[\sqrt{-3}]$ unik faktorisering.

Varning! 13 är ej irreducibelt i $\mathbb{Z}[\sqrt{-3}]$ ty $13 = (1+i2\sqrt{3})(1-i2\sqrt{3})$, fast det är primtal och därmed är irreducibelt i $\mathbb{Z}$.

EUKLIDISKA OMRÅDEN

Ett integritetsområde D kallas Euklidiskt om det finns en funktion $d : D \setminus \{0\} \to \mathbb{Z}^+$ sådan att

- $d(\alpha\beta) \geq d(\alpha)$ då $\alpha \neq 0$, $\beta \neq 0$
- för α, $\beta \in D$ där $\beta \neq 0$ finns q och r så att

$$\alpha = q\beta + r \quad \text{med } d(r) < d(\beta) \text{ eller } r = 0$$

(Divisions algoritmen.)

Exempel. (a) $\mathbb{Z}$ är ett Euklidiskt område med $d(a) = |a|$.

(b) $K[x]$, där K är en kropp, är ett Euklidiskt område med $d(f(x)) = \text{grad } f(x)$.

Gaussiska heltalen. Låt $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, i är den imaginära enheten. Elementen i $\mathbb{Z}[i]$ kallas **Gaussiska heltalen**. $\mathbb{Z}[i]$ är ett integritetsområde.

Sats. $\mathbb{Z}[i]$ är ett Euklidisk område.

Bevis. Låt $d(a + bi) = |a + bi|^2 = a^2 + b^2$. Observera att för $z = a + bi \neq 0$ gäller att $d(a + bi) = a^2 + b^2 \geq 1$ och för z och w i $\mathbb{Z}[i]$ gäller

$$d(zw) = d(z)d(w) \geq d(z)$$

Det återstår att visa Divisions algoritmen. Låt α, $\beta \in \mathbb{Z}[i]$ med $\alpha = a_1 + a_2 i$, $\beta = b_1 + b_2 i$, $\beta \neq 0$. Vi måste hitta q och $r \in \mathbb{Z}[i]$ så att $\alpha = q\beta + r$ där $r = 0$ eller $d(r) < d(\beta)$. Vi skriver α/β på formen $\alpha/\beta = x + yi$, där x, $y \in \mathbb{Q}$. Låt q_1, q_2 vara heltal i $\mathbb{Z}$ så nära som möjligt till rationella talen x och respektive y. Låt $q = q_1 + q_2 i$ och $r = \alpha - q\beta$. Om $r = 0$ så är vi klara. Annars, har vi att $|x - q_1| \leq 1/2$ och $|y - q_2| \leq 1/2$ (enligt konstruktion av q). Detta ger

$$\begin{aligned}
&d(r) = d(\alpha - q\beta) = d(\beta(\alpha/\beta - q)) \leq \\
&d(\beta)d(\alpha/\beta - q) \leq d(\beta)d((x + yi) - (q_1 + iq_2)) \leq \\
&d(\beta)((x - q_1)^2 + (y - q_2)^2) \leq d(\beta)(1/4 + 1/4) < d(\beta).
\end{aligned}$$

Sats. Ett Euklidiskt område har unik faktorisering.
