3 Ireducibilní rozklady polynomů v $T[x]$

- rozklady polynomů na ireducibilní (dále nerozložitelné) prvky v oboru integrity polynomů jedné neurčité x nad tělesem T.

Příklad 5. *Uvažujme polynom $x^5+2x^4-2x^3-11x^2-6x+8$ z oboru integrity $Q[x] \subseteq R[x]$. Potom jeho ireducibilní rozklady v oborech integrity $Q[x]$, $R[x]$ a $C[x]$ vypadají takto:*

$Q[x]:\ (x-2)(x^2+x-1)(x^2+3x+4)$,

$R[x]:\ (x-2)(x+\frac{1}{2}+\frac{1}{2}\sqrt{5})(x+\frac{1}{2}-\frac{1}{2}\sqrt{5})(x^2+3x+4)$,

$C[x]:\ (x-2)(x+\frac{1}{2}+\frac{1}{2}\sqrt{5})(x+\frac{1}{2}-\frac{1}{2}\sqrt{5})(x+\frac{3}{2}+\frac{1}{2}i\sqrt{7})(x+\frac{3}{2}-\frac{1}{2}i\sqrt{7})$.

Polynom nazýváme **ireducibilní** právě když má pouze nevlastní (samozřejmé) dělitele. **Nevlastními děliteli** polynomu $f(x)$ v $T[x]$ jsou:
1) Jednotky tělesa T, tj. všechny nenulové prvky tělesa $(T,+,\cdot)$.
2) Polynomy asociované s $f(x)$, tj. polynomy ve tvaru $c\cdot f(x), c \in T, c \neq 0$.

Poznámky. Jednotky a asociované prvky.
1) Jednotkou v oboru integrity I rozumíme každý prvek $i \in I$, k němuž v I existuje inverzní prvek. Mějme na paměti, že existence inverzních prvků není v oboru integrity zaručena.
2) Prvky a, b oboru integrity I jsou spolu asociované právě když lze jeden z nich vyjádřit jako násobek druhého jednotkou z I. Jedná se o symetrickou relaci, proto též říkáme, že a je asociován s b, případně naopak. Značíme

$$a\|b.$$

Důsledky.
1) Polynom $f(x)$ je **reducibilním polynomem** $T[x]$ právě tehdy, když má vlastního dělitele $g(x)$. Platí

$$0 < st[g(x)] < st[f(x)].$$

2) Polynomy prvního stupně jsou v oboru integrity $T[x]$ ireducibilními polynomy.

Příklad 6. *Polynom x^2+x-1 je ireducibilní v $Q[x]$, ale ne v $R[x]$. Tam jsou ireducibilní např. polynomy $x-2$ a x^2+3x+4. Posledně uvedený však není ireducibilní v $C[x]$. Tam jsou ireducibilní pouze polynomy prvého stupně.*

Věta 3.1. *Nechť $f(x)$ je* **ireducibilní** *polynom v $T[x]$ a $g(x)$ je libovolný polynom z $T[x]$. Potom platí:*

$$NSD(f(x), g(x)) = 1 \qquad \textit{nebo} \qquad f(x)|g(x) \ \textit{v} \ T[x].$$

Příklad 7. $R[x]: \ f(x) = x^2+1, \ g(x) = x^3+x+1.$

Věta 3.2. *Polynom $f(x) \in T[x]$ je ireducibilní polynom v $T[x]$, právě když platí implikace:*

$$\forall g(x), h(x) \in T[x]; \ f(x)|g(x)h(x) \ \Rightarrow f(x)|g(x) \vee f(x)|h(x).$$

Příklad 8. *V Z porovnejte* $6|(9\cdot 8)$ *a* $3|(9\cdot 8)$.

Příklad 9. *V $Z[x]$ porovnejte*

$$(x^3-x^2+x-1)|(x^2-1)(x^2+1) \text{ a } (x+1)|(x^2-1)(x^2+1).$$

Věta 3.3. *Každý polynom z $T[x]$ stupně alespoň 1 má za dělitele alespoň jeden ireducibilní polynom z $T[x]$.*

Příklad 10. *Několik příkladů dělitelů ireducibilních v daném $T[x]$:*

$Z[x]: \ (x+1)|(x+1), \ (x+1)|(5x+5),$

$R[x]: \ (x^2+x+1)|(x^3-1),$

$C[x]: \ (x-\frac{1}{2}-i)|(x^3-1).$

4 Eukleidovské obory integrity

V Eukleidovském oboru integrity můžeme provádět **dělení se zbytkem** a pomocí Eukleidova algoritmu **nalézt** NSD **konečné skupiny prvků**.

Příkladem Eukleidovského oboru integrity je $Q[x]$.

Příklad 11. *Určete největšího společného dělitele polynomů* $f(x), g(x) \in Q[x]: \ f(x) = x^4 + x^3 - 3x^2 - x + 2, \ g(x) = 2x^4 + 5x^3 + 2x^2 + x + 2.$

Příklad 12. *Dokažte, že zlomek*

$$\frac{n^3 + 2n}{n^4 + 3n^2 + 1}$$

nelze krátit pro žádné přirozené číslo n*.*

Příklad 13. *Za jakých podmínek je polynom* $x^3 + px + q$ *dělitelný polynomem* $x^2 + mx - 1$*?*

Příklad 14. *Najděte polynom* $P(x)$ *tak, aby* $P(x)$ *byl dělitelný* x^2+1 *a* $P(x) + 1$ *byl dělitelný* $x^3 + x^2 + 1$*.*

Definice 4.1 (Eukleidovský obor integrity). *Obor integrity* I *se nazývá eukleidovský obor integrity, právě když existuje zobrazení* v *množiny* $I - \{0\}$ *do* N *(tomuto zobrazení říkáme* <u>*norma*</u>*) takové, že pro libovolná* $f, g \in I - \{0\}$, $g \neq 0$, *platí současně:*

1) $f|g \Rightarrow v(f) \leq v(g)$,

2) $\exists s, r \in I; f = g \cdot s + r \ \wedge \ (r = 0 \vee v(r) < v(g))$.

Zajímají nás eukleidovské obory integrity polynomů. Platí v nich následující věty.

Věta 4.1. *Nechť* $I[x]$ *je eukleidovský obor integrity,* $f(x), g(x) \in I[x]$, $d(x) = NSD(f(x), g(x))$*. Potom existují polynomy* $u(x), v(x) \in I[x]$ *tak, že*

$$f(x) \cdot u(x) + g(x) \cdot v(x) = d(x).$$

Důkaz. Vyjdeme z Eukleidova algoritmu. □

Věta 4.2. *Nechť $I[x]$ je eukleidovský obor integrity, $f(x), g(x) \in I[x]$. Jestliže jsou $f(x), g(x)$ nesoudělné polynomy, potom existují $u(x), v(x) \in I[x]$ takové, že*

$$f(x) \cdot u(x) + g(x) \cdot v(x) = 1.$$

Důkaz. Důsledek předcházející věty. □

Příklad 15. *Najděte polynomy $F(x)$, $G(x)$ tak, aby*

$$(x^8 - 1)F(x) + (x^5 - 1)G(x) = x - 1.$$

Věta 4.3. *Nechť T je těleso. Potom obor integrity $T[x]$ polynomů nad T je eukleidovský obor integrity.*

Důkaz. První vlastnost přímo, druhou matematickou indukcí. □

Důsledek. Struktury $Q[x], R[x], C[x]$ jsou eukleidovské obory integrity. Normou je pak stupeň polynomu.

Poznámka. I když to z uvedené věty nevyplývá, stojí za zmínku, že $Z[x]$ není eukleidovským oborem integrity. Pozor však, struktura $(Z, +, \cdot)$ je eukleidovským oborem integrity.

Při studiu rozkladu polynomů (čísel) nás zajímají obory, v nichž jsou tyto rozklady jednoznačné, tzv. Gaussovy obory integrity.

5 Gaussovy obory integrity

Definice 5.1 (Gaussův obor integrity). *Obor integrity I se nazývá Gaussův obor integrity, resp.* **obor integrity s jednoznačným dělením**, *právě když pro každé $a \in I, a \neq 0, a \nparallel 1$ existuje rozklad v součin ireducibilních prvků a když libovolné dva rozklady prvku jsou spolu asociovány.*

5.1 Podmínka konečnosti řetězce dělitelů

Příklad 16. $24 = 2^3 \cdot 3$

$$\begin{array}{r|l} 24 & 2 \\ 12 & 2 \\ 6 & 2 \\ 3 & 3 \\ 1 & 1 \\ 1 & \end{array}$$

Příklad 17. $x^4 - 2x^3 - 11x^2 + 12x + 36 = (x+2)^2(x-3)^2$

$$\begin{array}{r|c} x^4 - 2x^3 - 11x^2 + 12x + 36 & x+2 \\ x^3 - 4x^2 - 3x + 18 & x+2 \\ x^2 - 6x + 9 & x-3 \\ x-3 & x-3 \\ 1 & 1 \\ 1 & \end{array}$$

Pro Gaussův obor integrity je klíčová **podmínka konečnosti řetězce dělitelů**, stručně „podmínka (D)“.

Definice 5.2. *Řekneme, že obor integrity I splňuje podmínku konečnosti řetězce dělitelů, právě když pro každou posloupnost prvků v I tvaru*

$$a_1, a_2, a_3, ... \in I, \quad a_{i+1} | a_i, i = 1, 2, 3, ...$$

platí

$$\exists n \in N, \forall r, s \in N_i (n \leq r \wedge n \leq s) \Rightarrow a_r \parallel a_s,$$

(Tj. existuje $n \in N$ tak, že $a_n \parallel a_{n+1}, a_{n+1} \parallel a_{n+2}, ...$).

Příklad 18. *Konečné řetězce dělitelů:*

a) $12, 6, 3, 1, 1, ...$

b) $x^4 - 1, x^2 - 1, x + 1, 1, \ldots$
c) $x^2 + 2x + 1, x + 1, 7x + 7, \frac{1}{3}x + \frac{1}{3}, 1, 1, \ldots$
d) $x - 1, 2x - 2, 3x - 3, 4x - 4, 5x - 5, \ldots$

Důsledky platnosti podmínky (D)

Věta 5.1. *V každém eukleidovském oboru integrity platí podmínka (D).*

Důkaz. Od posloupnosti dělitelů přejdeme k posloupnosti norem. □

Příklad 19. $x^8 - 1$

$$x^4 - 1 | x^8 - 1$$

$$x^2 - 1 | x^4 - 1$$

$$x + 1 | x^2 - 1$$

Tj. ireducibilní polynom $x + 1$ *dělí* $x^8 - 1$.

Věta 5.2. *Nechť obor integrity splňuje podmínku (D) a nechť* $x \in I$, $x \neq 0$, $x \nparallel 1$. *Potom* x *je dělitelný alespoň jedním prvkem ireducibilním v* I.

Věta 5.3. *Nechť obor integrity* I *splňuje podmínku (D) a nechť* $x \in I$, $x \neq 0$, $x \nparallel 1$. *Potom lze prvek* x *vyjádřit ve tvaru součinu konečně mnoha prvků ireducibilních v* I. *Jinak řečeno,* **lze provést rozklad** x **v součin ireducibilních prvků**.

Věta 5.4. *Je-li* T *těleso, je* $T[x]$ *Gaussovým oborem integrity.*

Důkaz. Dokážeme následující dvě vlastnosti:
1) Splnění podmínky (D).
2) Každý ireducibilní polynom je prvočinitelem, tj. platí:

$$i(x)|f(x) \cdot g(x) \wedge i(x) \nmid f(x) \Rightarrow i(x)|g(x).$$

□

Poznámky. K důkazu věty 5.4:
1) Druhá vlastnost (tzv. **prvočíselná vlastnost**) **vede k jednoznačnosti rozkladu**.
2) Při důkazu věty jsme mohli použít také následující větu:
„Věta: Každý eukleidovský obor integrity je rovněž Gaussovým oborem integrity“.
3) Pozor! Věta uvedená v poznámce 2 se nedá obrátit. Existují Gaussovy obory integrity, které nejsou eukleidovské. Například $Z[x]$.

Obory $C[x]$, $R[x]$, $Q[x]$ a $Z[x]$ mají **vlastnosti existence a jednoznačnosti rozkladu v součin ireducibilních prvků** (jsou to Gaussovy obory integrity). Zajímá nás, **jak ty rozklady vypadají**.

Příklad 20. *Rozložte polynom x^8-1 postupně v $Z[x]$, $Q[x]$, $R[x]$ a $C[x]$.*
$Z[x], Q[x] : x^8-1=(x+1)(x-1)(x^2+1)(x^4+1)$,
$R[x] : x^8-1=(x+1)(x-1)(x^2+1)(x^2+x\sqrt{2}+1)(x^2-x\sqrt{2}+1)$,
$C[x] : x^8-1=(x+1)(x-1)(x+i)(x-i)(x+\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2})(x+\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2})(x-\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2})(x-\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2})$,

5.2 Rozklad polynomů v $C[x]$

Připomeňme znění **základní věty algebry**:
„Věta: Každý polynom $p(x)\in C[x]$ stupně $n\geq 1$ má alespoň jeden kořen $c\in C$.“
Též říkáme, že těleso komplexních čísel C je **algebraicky uzavřené**.

Věta 5.5. *Pro těleso komplexních čísel platí následující tvrzení:*
i) Každý polynom z $C[x]$ stupně $n\geq 2$ je reducibilní v $C[x]$.
ii) Každý polynom $f(x)\in C[x]$ stupně $n\geq 1$ má v $C[x]$ rozklad tvaru:

$$f(x)=a(x-\alpha_1)(x-\alpha_2)...(x-\alpha_n).$$

Věta 5.6 (Kanonický rozklad polynomu). *Libovolný polynom $f(x) \in C[x]$ stupně $n \geq 1$ má v $C[x]$ rozklad tvaru:*

$$f(x) = a(x-\beta_1)^{k_1}(x-\beta_2)^{k_2}...(x-\beta_s)^{k_s},$$

kde $k_1 + k_2 + ... + k_s = n$ a $\beta_1, \beta_2, ..., \beta_s$ jsou navzájem různá čísla.

Příklad 21. $x^3-1 = (x-1)(x^2+x+1) = (x-1)(x+\frac{1}{2}+\frac{3}{2}i)(x+\frac{1}{2}-\frac{3}{2}i)$

Příklad 22. *Rozložte kvadratický trojčlen ax^2+bx+c v součin ireducibilních polynomů v $C[x]$.*

Věta 5.7. *Nechť $f(x) = a_nx^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \in R[x]$ je (reálným) polynomem stupně $n > 1$. Je-li $\beta = b_1 + ib_2$, $b_2 \neq 0$, $k-$násobným ($k \geq 1$) kořenem polynomu $f(x)$, je zároveň i číslo $\overline{\beta} = b_1 - ib_2$ $k-$násobným kořenem polynomu $f(x)$.*

Důkaz. Známe z ALG4. $\square$

ÚKOL: K důkazu věty pro $n = 2$ použijte Vietovy vztahy.

5.3 Rozklad polynomů v $R[x]$

Věta 5.8. *Každý polynom $f(x) \in R[x]$ stupně $n \geq 1$ lze nad R zapsat ve tvaru součinu ireducibilních polynomů takto:*

$$f(x) = a(x-\alpha_1)...(x-\alpha_r)(x^2+a_1x+b_1)...(x^2+a_sx+b_s),$$

kde $a, \alpha_1, ..., \alpha_r, a_i, b_i \in R$ pro všechna $i = 1, 2, ..., s$. Polynomy $x^2 + a_ix + b_i$, $i = 1, 2, ..., s$ mají za kořeny dvě čísla komplexně sdružená. Platí $n = r + 2s$.

Důsledek. Je-li stupeň $f(x) \in R[x]$ liché číslo, pak má polynom $f(x)$ vždy alespoň jeden reálný kořen.

Příklad 23. *Charakteristická rovnice shodnosti v* E_3 :

$$\begin{vmatrix} a_{11}-\lambda & a_{12} & a_{13} \\ a_{21} & a_{22}-\lambda & a_{23} \\ a_{31} & a_{32} & a_{33}-\lambda \end{vmatrix} = 0.$$