Příklad 23. *Charakteristická rovnice shodnosti v* E_3 :

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

6 Ireducibilní rozklady polynomů v $Z[x]$

Obor integrity $Z[x]$ **není eukleidovským oborem integrity**.

Naším cíle je dokázat, že $Z[x]$ **je Gaussovým oborem integrity**, tj. existuje v něm jednoznačný rozklad v součin ireducibilních prvků.

Ireducibilní prvky v $Z[x]$
Ireducibilní prvek má pouze nevlastní dělitele (jednotky a polynomy s ním asociované).

Příklad 24.

$$2, \quad \pm 3, \quad x+1, \quad x^2+x+1, ...$$

Příklad 25. *Rozklad polynomu v* $Z[x]$:

a) $6x^5 + 6x^4 + 6x^2 + 6x + 12 = 2 \cdot 3 \cdot (x^2 + x + 1) \cdot (x^3 - x + 2)$.

b) $30x^4 - 13x^3 - 48x^2 + 7x + 12 = 30 \cdot (x - \frac{4}{3}) \cdot (x + \frac{1}{2}) \cdot (x - \frac{3}{5}) \cdot (x + 1) = (3x-4) \cdot (2x+1) \cdot (5x-3) \cdot (x+1)$.

Definice 6.1 (Primitivní polynom). *Nenulový polynom (zapsaný v normálním tvaru)*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 \in Z[x]$$

se nazývá primitivní polynom, právě když jeho koeficienty jsou nesoudělné, tj. když

$$\mathrm{NSD}(a_0, a_1, ..., a_{n-1}, a_n) = 1.$$

Příklad 26. *Primitivní polynomy:*

$$3x^3 - 4x^2 + 6x - 12, \quad -1, \quad x^3 + x^2 - 1.$$

Příklad 27. *Neprimitivní polynomy:*

$$8, \quad -56, \quad 4x^3 - 6x^2 + 4, \quad 4x^3 + 10x^2 - 6x + 4, \quad 3, \quad 2.$$

Lemma 6.1. *Součin dvou primitivních polynomů ze $Z[x]$ je opět primitivní polynom.*

Důkaz. Sporem. □

Lemma 6.2. *Každý nenulový polynom $f(x) \in Q[x]$ lze vyjádřit ve tvaru*

$$f(x) = a \cdot f_0(x),$$

kde $a \in Q$ a $f_0(x)$ je primitivní polynom ze $Z[x]$.

ÚKOL: Vyjádřete dané polynomy ve tvaru uvedenám v lemmatu 6.2:

a) $\frac{3}{2}x^5 - \frac{4}{7}x^3 + 9x^2 - \frac{1}{3}x + 1,$

b) $\frac{5}{2}x^2 + \frac{10}{3}x - \frac{15}{4},$

c) $-\frac{3}{4}.$

Lemma 6.3. *Nechť $f(x)$ a $g(x)$ jsou primitivní polynomy v $Z[x]$ a nechť platí*

$$a \cdot f(x) = b \cdot g(x);\ a, b \in Z.$$

Potom $a\|b$ (v Z) a zároveň $f(x)\|g(x)$ (v $Z[x]$).

Důkaz. $a|b \cdot g(x) \ \wedge \ b|a \cdot f(x).$ □

Věta 6.4. *Primitivní polynom $f(x) \in Z[x]$ je ireducibilní v $Z[x]$, právě když je ireducibilní v $Q[x]$.*

Příklad 28. *Rozložte na ireducibilní polynomy v* $Z[x]$:

a) $f(x) = 4x^2 - 8x + 3$,

b) $g(x) = x^2 - 2$,

c) $h(x) = 4x^2 - x - 18$.

Příklad 29. *Rozklad polynomu na ireducibilní prvky v* $Z[x]$:

$$12x^2 - 36x + 24 = 3 \cdot 4 \cdot (x-1) \cdot (x-2).$$

Věta 6.5. $Z[x]$ *je Gaussův obor integrity.*

Důkaz. $f(x) = d \cdot g(x)$, kde $g(x)$ je primitivní polynom. Potom využijeme rozklad $g(x)$ v $Q[x]$. □

Poznámka. Každý ireducibilní polynom v $Z[x]$ musí být primitivní.

6.1 Největší společný dělitel konečné množiny polynomů

Příklad 30. *Určete* $\mathrm{NSD}(f_1(x), f_2(x), f_3(x))$:

$f_1(x) = 12x^3 - 36x^2 - 156x + 180$,

$f_2(x) = 6x^2 - 6$,

$f_3(x) = 30x^2 + 60x - 90$.

Řešení: $\mathrm{NSD}(f_1(x), f_2(x), f_3(x)) = 6x - 6 = 6(x-1)$.

Věta 6.6 (O existenci NSD konečné množiny polynomů ze $Z[x]$). *Nechť je dáno r polynomů $f_1(x), f_2(x), ..., f_r(x)$, kde $f_i(x) = a_i g_i(x)$, $a_i \in Z$ a $g_i(x)$ jsou primitivní polynomy v $Z[x]$ pro $i = 1, 2, ..., r$. Nechť d je největší společný dělitel čísel a_i a $D(x)$ je největší společný dělitel polynomů $g_i(x)$ jakožto polynomů z $Q[x]$. Potom $D(x)$ můžeme volit tak, že je to primitivní polynom ze $Z[x]$ a výraz $d \cdot D(x)$ je největší společný dělitel polynomů $f_1(x), f_2(x), ..., f_r(x)$ v $Z[x]$.*

Poznámka. Polynom $D(x)$ jakožto NSD v $Q[x]$ je určen jednoznačně až na násobek. Potom existuje takový $D(x)$ v $Q[x]$, že je primitivní v $Z[x]$.

6.2 Posouzení ireducibility polynomu v $Z[x]$, resp. $Q[x]$

Věta 6.7 (Eisensteinovo kritérium ireducibility). *Nechť $f(x)$ je primitivní polynom $n-$tého stupně ze $Z[x]$ ve tvaru*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$$

a nechť existuje prvočíslo p tak, že platí současně:

$$\begin{aligned} &1)\ \ p \nmid a_n, \\ &2)\ \ p \mid a_i, \quad \text{pro všechna } i = 0, 1, ..., n-1, \\ &3)\ \ p^2 \nmid a_0. \end{aligned}$$

Potom je polynom $f(x)$ ireducibilní v $Z[x]$ i v $Q[x]$.

Důkaz. Sporem. □

Příklad 31. *Užitím Eisensteinova kriteria ireducibility rozhodněte, zda jsou dané polynomy ireducibilní v $Z[x]$:*

a) $x^4 - 8x^3 + 12x^2 - 6x + 2$,

b) $x^3 - 15x^2 + 45x + 75$,

c) $x^3 - 15x^2 + 45x + 54$.

Poznámka. Eisensteinovo kritérium má formu implikace. Pokud nenajdeme prvočíslo p, které splňuje stanovené podmínky, **nelze** pomocí tohoto kritéria **rozhodnout** o ireducibilitě daného polynomu v $Z[x]$.

Věta 6.8. *V $Q[x]$ existují ireducibilní polynomy libovolných stupňů.*

Důkaz. Důsledek Eisensteinova kritéria. □