(normované)

Příklad 35. *Nalezněte všechny ireducibilní polynomy*

1. *stupně nejvýše 4 nad* $\mathbb{Z}_2$.
2. *stupně nejvýše 2 nad* $\mathbb{Z}_3$*, dále určete počet ireducibilních polynomů stupně 3 nad* $\mathbb{Z}_3$.

ad 1.

st. 1: x, $x+1$ - ireducibilní

st. 2: $\cancel{x^2}$, $\cancel{x^2+1} = (x+1)^2$, $\cancel{x^2+x}$, x^2+x+1

$(x^2+x+1)^2 = x^4+x^2+1$

st. 3: $\cancel{x^3}$, $\cancel{x^3+1}$, $\cancel{x^3+x}$, x^3+x+1, $\cancel{x^3+x^2}$, x^3+x^2+1, $\cancel{x^3+x^2+x}$, $\cancel{x^3+x^2+x+1}$

st. 4: $\cancel{x^4}$, $\cancel{x^4+1}$, $\cancel{x^4+x}$, x^4+x+1, $\cancel{x^4+x^2}$, $\cancel{x^4+x^2+1}$, $\cancel{x^4+x^2+x}$, $\cancel{x^4+x^2+x+1}$, $\cancel{x^4+x^3}$, x^4+x^3+1, $\cancel{x^4+x^3+x}$, $\cancel{x^4+x^3+x+1}$, $\cancel{x^4+x^3+x^2}$, $\cancel{x^4+x^3+x^2+1}$, $\cancel{x^4+x^3+x^2+x}$, $x^4+x^3+x^2+x+1$

13 red.

$\Downarrow$

3 ired.

red.: $f_1 \cdot f_1 \cdot f_1 \cdot f_1$ 5

$f_1 \cdot f_1 \cdot f_2$ 3

$f_1 \cdot f_3$ 4

$f_2 \cdot f_2$ 1

ad 2. vypíšeme pouze normované ired. polynomy

vždy dostaneme jejich vynásobením jednotkami

příklad $\mathbb{Z}_3$, jedn. $1, -1$

st. 1: $x,\ x+1,\ x-1$

st. 2: $\cancel{x^2},\ x^2+1,\ \cancel{x^2-1}$

$\cancel{x^2+x},\ \cancel{x^2+x+1},\ x^2+x-1$

$\cancel{x^2-x},\ x^2-x-1,\ \cancel{x^2-x+1}$

$-\ x^2-1$

$-\ x^2-x+1$

$-\ x^2+x+1$

st. 3: # normovaných $3^3 = 27$

normovaných reducibilních: $f_1 \cdot f_1 \cdot f_1$ $\quad \binom{5}{2} = 10$

$\bullet|\bullet|\bullet \qquad ||\bullet\bullet\bullet$

$f_1 \cdot f_2 \quad 3 \cdot 3 = 9$

normovaných ired. je $27 - (10+9) = 8$

všech ired. nad $\mathbb{Z}_3$ je $2 \cdot 8 = 16$

Příklad 36. *Polynom*

$$f(x) \quad x^8 + x^4 + x^3 + x \in \mathbb{Z}_2[x]$$

rozložte na součin ireducibilních polynomů.

1. určíme kořeny: $x = 0$ $\quad f(x) = x \cdot \underbrace{(x^7 + x^3 + x^2 + 1)}_{f_1}$

	1	0	0	0	1	1	0	1	
1	1	1	1	1	0	1	1	0	✓
1	1	0	1	0	0	1	0		✓
1	1	1	0	0	0	1			×

$\Rightarrow f(x) = x \cdot (x+1)^2 \cdot x^5 + x^3 + 1$

Vydělíme x^5+x^3+1 jediným ireducibilním st. 2, totiž x^2+x+1.

$$(x^5+x^3+1):(x^2+x+1) = x^3+x^2+x$$
$$-(x^5+x^4+x^3)$$
$$x^4+1$$
$$-(x^4+x^3+x^2)$$
$$x^3+x^2+1$$
$$-(x^3+x^2+x)$$
$$x+1 \longrightarrow \text{zbytek}$$

$\Downarrow$

x^5+x^3+1 je ireducibilní

Příklad 37. *Rozložte polynom*

$$x^7 + 2x^6 + 2x^5 + 2x^4 + 2x^3 + x + 2$$

nad $\mathbb{Z}_3$ *na součin ireducibilních polynomů.*

Příklad 38. *Rozhodněte, ve kterém případě jde o okruh (s obvyklým sčítáním a násobením) s jedničkou:*

a) *přirozená čísla,* NE $(\mathbb{N},+)$ není grupa

b) *celá čísla, která jsou násobkem 3,* NE nemá jedničku $(3a \cdot 3b = 3b$ $\nexists a \in \mathbb{Z})$

c) *polynomy nad* $\mathbb{R}$ *stupně nejvýše* n*,* NE $(st(f \cdot g)$ může být $> n)$

d) *polynomy s celočíselnými koeficienty,* ANO

e) *polynomy s celočíselnými koeficienty s nulovým absolutním členem,*

f) *polynomy* f *nad* $\mathbb{R}$ *splňující* $f(2) = 0$*,*

g) *nesingulární matice* 2×2 *nad* $\mathbb{R}$*,*

h) *lineární reálné funkce, tj. funkce tvaru* $f(x) = a \cdot x + b, a, b \in \mathbb{R}$. NE

ad e) je to okruh, ale ne s jedničkou

ad f) ||

ad g) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ NE grupa?

$a = 1$, $b = 0$: $f(x) = x$

ad h) $(f \cdot g)(x) = f(x) \cdot g(x)$ ...

$(f \cdot f)(x) = x^2$

Příklad 39. *Nechť* $(R, +, \cdot)$ *je okruh. Pak rovněž* $(R, +, \circ)$*, kde*

$$a \circ b = a \cdot b + b \cdot a\ ,$$

je okruh. Dokažte nebo vyvraťte.

$(R,+)$ je komutativní grupa

$(R,\circ)$ je grupoid

asociativita? $(a\circ b)\circ c \stackrel{?}{=} a\circ(b\circ c)$

$L = (a\cdot b + b\cdot a)\circ c = (a\cdot b+b\cdot a)\cdot c + c\cdot(a\cdot b+b\cdot a) =$

$= a\cdot b\cdot c + b\cdot a\cdot c + c\cdot a\cdot b + c\cdot b\cdot a$

$R = a\circ(b\cdot c + c\cdot b) = a\cdot(b\cdot c+c\cdot b) + (b\cdot c + c\cdot b)\cdot a =$

$= a\cdot b\cdot c + a\cdot c\cdot b + b\cdot c\cdot a + c\cdot b\cdot a$ obecně ne,

další požadavek na R je, že $(R,\cdot)$ je komutativní

$(R,\circ)$ má jednotku?

$\exists e?\quad e \circ a = a \circ e = a \quad \forall a \in R$

$e \circ a = e \cdot a + a \cdot e \overset{?}{=} a$

$\| $

$e \cdot a + e \cdot a \overset{?}{=} a$

$(e+e) \cdot a \overset{?}{=} 1 \cdot a$ | obecně nemůžeme krátit

$(e+e-1) \cdot a \overset{?}{=} 0$

R: obor integrity

$2e = 1$

nemusí existovat v obecném OI (v $\mathbb{Z}$ neexistuje, v $\mathbb{Z}_5$ existuje)

R není obor integrity

$\mathbb{Z}_9 \quad e = 5 \qquad$ v $\mathbb{Z}_4$ neexistuje

Příklad 40. *Určete jednotky a dělitele nuly v okruzích:*

a) *celých čísel* $(\mathbb{Z}, +, \cdot)$, $\mathbb{Z}^\times = \{1, -1\}$ je to obor integrity

b) *celočíselných polynomů* $(\mathbb{Z}[x], +, \cdot)$, $(\mathbb{Z}[x])^\times = \{1, -1\}$, — " —

c) *reálných polynomů* $(\mathbb{R}[x], +, \cdot)$, $(\mathbb{R}[x])^\times = \mathbb{R}^\times$, — " —

d) *zbytkových tříd* $(\mathbb{Z}_n, +, \cdot)$,

e) *polynomů nad* $\mathbb{Z}_5$, *tj.* $(\mathbb{Z}_5[x], +, \cdot)$,

f) *funkcí* $f : [0, 1] \to \mathbb{R}$.

ad d) $a \cdot x \equiv 1 \pmod{n}$ x existuje $\Leftrightarrow (a, n) = 1$

$\mathbb{Z}_n^\times = \{a + \mathbb{Z}_n; (a, n) = 1\}$

dělitelé nuly: $a \cdot x \equiv 0 \pmod{n} \Leftrightarrow n \mid a \cdot x$

$(\exists x \not\equiv 0 (n) ?)$

Odtud $(a, n) = 1 \Rightarrow \nexists x \Rightarrow a$ není dělitel 0

$(a, n) = d > 1$, $b := \frac{n}{d} \Rightarrow a \cdot b = \frac{a}{d} \cdot n \equiv 0 (n)$ $\Downarrow$

a je dělitel n

ad e) $\mathbb{Z}_5[x]$ je obor integrity

$$(\mathbb{Z}_5[x])^\times = (\mathbb{Z}_5)^\times = \{[1],[2],[3],[4]\}$$

ad f) $\underbrace{f:[0,1]\longrightarrow\mathbb{R}}_{\mathcal{F}}$

jednička je funkce

$$1_{\mathcal{F}}: x \longmapsto 1$$

$$\mathcal{F}^\times = \{f\in\mathcal{F} : \exists g : f\cdot g = 1_{\mathcal{F}}\}$$

$$\forall x\in[0,1]\ f(x)\cdot g(x) = 1$$

$$= \{f\in\mathcal{F} : \forall x\in[0,1] : f(x)\neq 0\}$$

<u>dělitelé nuly</u>: $f\neq 0\ \exists x\in[0,1] : f(x)=0$

$f\cdot g = 0$, kde $g(x) = \begin{cases} 0 & \text{pro } f(x)\neq 0 \\ 1 & \text{pro } f(x) = 0\end{cases}$

Příklad 41. *Určete, zda je okruh* $(\mathbb{Z}_2, +, \cdot) \times (\mathbb{Z}_3, +, \cdot)$ *oborem integrity a rozhodněte, zda je izomorfní s okruhem* $(Z_6, +, \cdot)$.

$\mathbb{Z}_2 \times \mathbb{Z}_3$

$0,0$
$0,1$
$0,2$
$1,0$
$1,1$
$1,2$

$\underline{(1,0)} \cdot \underline{(0,1)} = (0,0)$

dělitelé nuly $\Rightarrow$ není OI

$(\mathbb{Z}_6, +, \cdot)$

$0, 1, 2, 3, 4, 5$

homom. vz. + ✓ $(\mathbb{Z}_6, +) \to (\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +)$

$f(a \cdot b) = f(a) \cdot f(b)$

$f(n \cdot 1) = n \cdot (1,1) = (n,n)$ .. chceme $f((n \cdot 1) \cdot (m \cdot 1)) \overset{?}{=} n \cdot (1,1) \cdot m(1,1)$

$n \cdot m \cdot (1,1) \overset{?}{=} n \cdot (1,1) \cdot m(1,1)$ ✓

Příklad 42. *Rozhodněte, zda je zobrazení $f : \mathbb{C} \to \mathbb{R}$ definované předpisem $f(a+bi) = a+b$ homomorfismem okruhů.*

$$f : (\mathbb{C}, +, \cdot) \to (\mathbb{R}, +, \cdot)$$

$$(a+bi) + (c+di) \xmapsto{f} a+b + c+d$$

$$\| \qquad\qquad\qquad \|$$

$$(a+c) + (b+d)\cdot i \xmapsto{f} (a+c) + (b+d)$$

$$f(\alpha \cdot \beta) = f(\alpha) \cdot f(\beta)$$

$$(a+bi) \cdot (c+di) \xmapsto{f} (a+b) \cdot (c+d)$$

$$\| \qquad\qquad\qquad \not\|$$

$$(ac-bd) + (ad+bc)\, i \xmapsto{f} ac-bd + ad+bc$$

nejde o homomorfismus

Příklad 43. *1. Uvažme zobrazení* $f : \mathbb{C} \to \mathrm{Mat}_{2,2}(\mathbb{R})$ *definované předpisem* $f(a+bi) = \left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right)$. *Rozhodněte (a zdůvodněte), je-li* f *homomorfismus okruhu* $(\mathbb{C}, +, \cdot)$ *do okruhu* $(\mathrm{Mat}_{2,2}(\mathbb{R}), +, \cdot)$ *matic typu 2x2 nad* $\mathbb{R}$.

2. Uvažme zobrazení $g : \mathrm{Mat}_{2,2}(\mathbb{Q}) \to \mathbb{Q}$ *definované předpisem* $g\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\right) = ad - bc$. *Rozhodněte (a zdůvodněte), je-li* g *homomorfismus okruhu* $(\mathrm{Mat}_{2,2}(\mathbb{Q}), +, \cdot)$ *matic typu 2x2 nad* $\mathbb{Q}$ *do okruhu* $(\mathbb{Q}, +, \cdot)$.

ad 1) $+$ je homomorfismus $(\mathbb{C}, +) \to (\mathrm{Mat}, +)$

$\cdot$ $(a+bi)\cdot(c+di) \longmapsto \begin{pmatrix} a & b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ d & c \end{pmatrix}$

$$= (ac-bd) + (ad+bc)i \longmapsto \begin{pmatrix} ac-bd & ad+bc \\ ad+bc & ac-bd \end{pmatrix} \neq$$

ad 2) $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$ je homom. vzhledem k $\cdot$; není hom. k $+$: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Příklad 44. *Buď* $\mathbb{Q}[x]$ *okruh polynomů s racionálními koeficienty a* $\mathrm{Mat}_{2,2}(\mathbb{Q})$ *okruh matic typu 2x2 s racionálními prvky. Uvažte zobrazení:* $\varphi : \mathbb{Q}[x] \to \mathrm{Mat}_{2,2}(\mathbb{Q})$ *definované předpisem*

$$\varphi : f(x) \mapsto \begin{pmatrix} f(1) & \frac{1}{2}(f(1) - f(-1)) \\ 0 & f(-1) \end{pmatrix}$$

a rozhodněte, je-li φ *homomorfismus okruhů. Pokud ano, určete jeho jádro* $\ker \varphi$.

je to homomorfismus

$\ker \varphi = \{ p \in \mathbb{Q}[x] ;\ p(1) = p(-1) = 1 \}$