$$f = 4x^7 + 17x^6 + 32x^5 + 39x^4 + 28x^3 + 13x^2 + 2x$$

$$f = x\underbrace{(4x^6 + \dots 2)}_{h}$$

$p \mid 2 \quad q \mid 4 \quad h$

$$\frac{p}{q} \in \{\pm 1, \pm 2, \pm \tfrac{1}{2}, \pm \tfrac{1}{4}\}$$

h nemá kladný kořen, protože má jen kladné koeficienty

	4	17	32	39	28	13	2
-1	4	13	19	20	8	5	-3
-2	4	9	14	11	6	1	0
$-\frac{1}{4}$	4	8	12	8	4	0	
	1	2	3	2	1		

$-3 \Rightarrow -1$ není kořen

$1\ 2\ 3\ 2\ 1$ nemá rac. kořeny

$$f = 4x(x+2)\left(x+\frac{1}{4}\right)(x^4+2x^3+3x^2+2x+1)$$

Hledáme násobné kořeny

$$g = x^4 + 2x^3 + 3x^2 + 2x + 1$$

$$g' = 4x^3 + 6x^2 + 6x + 2 = 2\left(2x^3 + 3x^2 + 3x + 1\right)$$

$\operatorname{nsd}(g, g')$

$$x^4 + 2x^3 + 3x^2 + 2x + 1 = \left(2x^3 + 3x^2 + 3x + 1\right)\cdot\left(\tfrac{1}{2}x + \tfrac{1}{4}\right) + \tfrac{3}{4}\left(x^2 + x + 1\right)$$

$$\begin{array}{l}
-\left(x^4 + \frac{3}{2}x^3 + \frac{3}{2}x^2 + \frac{1}{2}x\right) \\
\hline
\quad \frac{1}{2}x^3 + \frac{3}{2}x^2 + \frac{3}{2}x + 1 \\
\quad -\left(\frac{1}{2}x^3 + \frac{3}{4}x^2 + \frac{3}{4}x + \frac{1}{4}\right) \\
\hline
\qquad \frac{3}{4}x^2 + \frac{3}{4}x + \frac{3}{4}
\end{array}$$

$$2x^3 + 3x^2 + 3x + 1 = \boxed{\left(x^2 + x + 1\right)}\left(2x + 1\right) + 0$$

$$\begin{array}{l}
-\left(2x^3 + 2x^2 + 2x\right) \\
\hline
\quad x^2 + x + 1 \\
\quad -\left(x^2 + x + 1\right) \\
\hline
\qquad 0
\end{array}$$

je hledaný $\operatorname{nsd}(g, g')$

$$x^2 + x + 1 = 0$$

$$x_{1,2} = \frac{-1 \pm \sqrt{-3}}{2} = \begin{cases} \frac{-1 + i\sqrt{3}}{2} \\ \frac{-1 - i\sqrt{3}}{2} \end{cases}$$

$$f = x(x+2)(4x+1)\left(x + \frac{1 - i\sqrt{3}}{2}\right)^2\left(x + \frac{1 + \sqrt{3}\,i}{2}\right)^2 \quad \text{nad } \mathbb{C}$$

$$f = x(x+2)(4x+1)\left(x^2 + x + 1\right)^2 \quad \text{nad } \mathbb{R}, \mathbb{Q}.$$

$f = x(x^7 + x^3 + x^2 + 1)$

	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	1 není trojnásobný	

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

x^5+x^3+1 je buď ireducibilní, nebo lze rozložit na součin ired. stupňů 2 a 3

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

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

$$x^5+x^3+1 = (x^2+x+1)(x^3+x^2+x) + x+1$$

$$
\begin{array}{l}
x^5+x^3+1 \\
+(x^5+x^4+x^3) \\
\hline
x^4 \qquad +1 \\
x^4+x^3+x^2 \\
\hline
x^3+x^2+1 \\
x^3+x^2+x \\
\hline
x+1
\end{array}
$$

$\Downarrow$

x^5+x^3+1 je ireduc.

$f = x(x+1)^2(x^5+x^3+1)$ je rozklad f na ireducibilní polynomy

1) $a \cdot 0 = 0 \cdot a = 0$

$a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0 \quad / -a \cdot 0$

$\boxed{0 = a \cdot 0}$ $\quad 0 \cdot a = 0$ obdobně

2) $(-1) \cdot a = a \cdot (-1) = -a$

$0 = 0 \cdot a = (1 + (-1)) \cdot a = 1 \cdot a + (-1) a \quad / -a$

$\boxed{-a = (-1) a}$

$a \cdot (-1) = -a$ obdobně

3) $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$

$0 = 0 \cdot b = (a + (-a)) \cdot b = a \cdot b + (-a) \cdot b \quad / -(a \cdot b)$

$\boxed{-(a \cdot b) = (-a) b}$ obdobně i 2. rovnost

Název: III 19-8:48 (4 z 9)

$(R, +, \circ)$ $\quad a \circ b = a \cdot b + b \cdot a$

$$a \circ (b + c) = a \cdot (b + c) + (b + c) \cdot a =$$
$$= ab + ac + ba + ca =$$
$$= ab + ba + ac + ca =$$
$$= a \circ b + a \circ c$$

$(b + c) \circ a$ obdobně

Je $(R, \circ)$ monoid?

$$(a \circ b) \circ c = (a \cdot b + b \cdot a) \circ c =$$
$$= (a \cdot b + b \cdot a) c + c (a \cdot b + b \cdot a) = abc + bac +$$
$$+ cab + cba$$

$$a \circ (b \circ c) = a \circ (bc + cb) = a \cdot (bc + cb) +$$
$$+ (bc + cb) \cdot a = abc + acb + bca + cba$$

$\circ$ není asociativní $\Rightarrow (R, +, \circ)$ nemusí být okruh

e je neutr. prvek $(R, \circ)$

$$e \circ a = e \cdot a + a \cdot e = a$$

$(R, \cdot)$ komut. $\longrightarrow$ $\quad 2 \cdot a \cdot e = a$

$$2e = 1$$

Nechť $(R,+,\cdot)$ je okruh.

(Jak v $\mathbb{Z}$, tak v $\mathbb{Z}_n$ lze každý prvek vyjádřit jako součet několika 1, jinými slovy $(\mathbb{Z},+) = \langle 1 \rangle$, $(\mathbb{Z}_n,+) = \langle 1 \rangle$)

Uvažme podgrupu $\langle 1 \rangle \leq (R,+)$.

Nastávají 2 možnosti:

a) $ord_{(R,+)} 1 = n \in \mathbb{N} \Rightarrow |\langle 1 \rangle| = n$

$\langle 1 \rangle \cong \mathbb{Z}_n$

$1_R \mapsto [1]_n$

b) $ord_{(R,+)} 1 = \infty \Rightarrow |\langle 1_R \rangle| = \infty$

$\langle 1_R \rangle \cong \mathbb{Z}$

$1_R \mapsto 1_{\mathbb{Z}}$ je hledaný izo.

Zbývá dokázat, že $(\langle 1 \rangle, +, \cdot)$ je okruh

1) $(\langle 1 \rangle, +)$ je komutativní grupa ✓

2) $(\langle 1 \rangle, \cdot)$ je monoid

3) platí distributivita ... z obecného kvantifikátoru ✓

ad 2) jistě 1 je neutrální prvek $(\langle 1 \rangle, \cdot)$

je to asociativní (z ∀)

zbývá: $a, b \in \langle 1 \rangle \Rightarrow a \cdot b \in \langle 1 \rangle$

$a, b \in \langle 1 \rangle \quad \exists m, n \in \mathbb{Z}: a = m \cdot 1$

$b = n \cdot 1$

$$a \cdot b = (m \cdot 1) \cdot (n \cdot 1) = (\underbrace{1 + 1 + \ldots + 1}_{m\text{-krát}}) \cdot (\underbrace{1 + \ldots + 1}_{n\text{-krát}}) =$$

$$= \underbrace{1 + 1 + \ldots + 1}_{m \cdot n\text{-krát}} = (m \cdot n) \cdot 1 \in \langle 1 \rangle \quad \square$$

Název: III 19-9:05 (6 z 9)

$A = \{ \frac{p}{q} : p, q \in \mathbb{Z}, 3 \nmid p \}$

Je $(A, +, \cdot)$ podokruh $(\mathbb{Q}, +, \cdot)$?

$$\frac{1}{4} + \frac{2}{4} = \frac{3}{4} \notin A \Rightarrow \text{NO!}$$

$B = \{ \frac{r}{3^n} : r \in \mathbb{Z}, n \in \mathbb{N} \}$

uzavřenost na operace

$\frac{r}{3^n}, \frac{s}{3^m} \in B$, BÚNO $n \leq m$

$$\frac{r}{3^n} + \frac{s}{3^m} = \frac{r \cdot 3^{m-n} + s}{3^m} \in B \checkmark$$

$$\frac{r}{3^n} \cdot \frac{s}{3^m} = \frac{r \cdot s}{3^{m+n}} \in B \checkmark$$

neutr. prvky?

$0 = \frac{0}{3} \in B \checkmark$, $1 = \frac{3}{3} \in B \checkmark$

inverze vůči $+$ (opačné prvky):

$$\frac{r}{3^n} \in B \Rightarrow \frac{-r}{3^n} \in B \checkmark$$

$B^{\times} = \{ b \in B, \exists b^{-1} \in B : b \cdot b^{-1} = 1 \}$

$$0 \neq b = \frac{r}{3^m} \in B \Rightarrow b^{-1} = \frac{3^m}{r} \in B \Leftrightarrow r = \pm 3^m, m \in \mathbb{N}$$

$B^{\times} = \{ \pm 3^k, k \in \mathbb{Z} \}$

Název: III 19-9:20 (7 z 9)

$$\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$$

$$\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$$

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

$$(\mathbb{Z}_4[x])^\times \supseteq \{\cancel{[1]_4}, \cancel{[3]_4}, 2x+1, 2x^n+1\}$$

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

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

$\vdots$

$$(\mathbb{Z}[\sqrt{2}])^\times = \{1, -1,$$

$$(a+b\sqrt{2})(c+d\sqrt{2}) = 1$$

$$ac+2bd + (ad+bc)\sqrt{2} = 1$$

$$\Updownarrow$$

$$ac+2bd = 1 \quad /\cdot b$$
$$ad+bc = 0 \quad /\cdot a$$

$$abc+2b^2d = b$$
$$a^2d+abc = 0$$

$$(2b^2-a^2)\,d = b$$

$$d = \frac{b}{2b^2-a^2}$$

$$c = \frac{-a}{2b^2-a^2}$$

$$(a+b\sqrt{2}) \in (\mathbb{Z}[\sqrt{2}])^\times \Leftrightarrow 2b^2-a^2 = \pm 1$$

$$b=2 \quad a=3 \qquad 2\cdot 4-9=-1$$

$$3+2\sqrt{2} \in (\mathbb{Z}[\sqrt{2}])^\times$$

$$(\mathbb{Z}[\sqrt{2}])^\times \supseteq \{(3+2\sqrt{2})^k, k\in\mathbb{Z}\}$$

nekonečně mnoho