

def.: multiplicativní množina v oboru R :

$$M \subseteq R \quad \text{t.č.} \quad 0 \notin M, \quad 1 \in M, \quad a, b \in M \Rightarrow a \cdot b \in M$$

Konstrukce: Bud' R obor, M mult. množina.

Def. relace na $R \times M$: $(a, u) \sim (b, v) \Leftrightarrow av = bu$

☺ je to ekvivalence

Bloky této ekvivalence se nazývají zlomky.

Na množině zlomků Q def. operace:

$$\frac{a}{u} + \frac{b}{v} = \frac{av + bu}{uv}, \quad -\frac{a}{u} = \frac{-a}{u}, \quad \frac{a}{u} \cdot \frac{b}{v} = \frac{ab}{uv}, \quad 0 = \frac{0}{1}, \quad 1 = \frac{1}{1}$$

☺ je to dobře definované (s ohledem na \sim)

$\Rightarrow (Q, +, -, \cdot, 0, 1)$ se nazývá **LOKALIZACE** oboru R podle M
resp. **PODÍLOVÉ TĚLESO** pro $M = R - \{0\}$

Trvzení: Je to obor, pro $M = R - \{0\}$ to je těleso.

$\left\{ \frac{a}{1} : a \in R \right\}$ tvoří podobor izomorfní R .

Tvrzení [kritérium existence racionálního kořene]

Bud' R gaussovský obor, Q jeho podílové těleso, $f = \sum_{i=0}^n a_i x^i \in R[x]$.

Má-li f kořen $\frac{r}{s}$ v Q (r, s nesoudělná), pak $\boxed{r \mid a_0, s \mid a_n}$.

def.: f se nazývá primitivní pokud nemá vlastního dělitele stupně 0.

Tvrzení [Eisensteinovo kritérium]

Bud' R obor, $f = \sum_{i=0}^n a_i x^i \in R[x]$.

Je-li f primitivní a $\exists p$ prvočíslo v R t.ž. $\boxed{\begin{array}{l} p \mid a_i \quad \forall i = 0, \dots, n-1 \\ p^2 \nmid a_0 \end{array}}$,
pak je f irreducibilní v $R[x]$.

Gaussova lemma: Bud' R gaussovský obor, $f, g \in R[x]$ primitivní.

Pak $f \cdot g$ je také primitivní polynom.

→ vztah dělitelnosti v $R[x]$ a $Q[x]$:

Tvrzení: Bude R gaussovský obor, Q jeho podílové těleso, $f, g \in R[x]$ primitivní.
Pak $f|g$ v $R[x] \Leftrightarrow f|g$ v $Q[x]$.

Tvrzení: Bude R gaussovský obor, Q jeho podílové těleso, $f, g \in R[x]$.

(1) f je ireducibilní v $R[x] \Leftrightarrow \begin{cases} \deg f = 0, f \text{ je } \underline{\text{ired. v } R} \\ \deg f > 0, f \text{ primitivní, } \underline{\text{ired. v } Q[x]} \end{cases}$

(2) $\underline{\text{NSD}_{R[x]}(f, g)}$ existuje a je $\underline{= c \cdot h}$, kde

- $c = \text{NSD}_R(c(f), c(g))$
- $h = \text{NSD}_{Q[x]}(pp(f), pp(g))$, h primitivní z $R[x]$

kde $c(f) = \text{NSD}$ koeficientů, $pp(f) = \frac{1}{c} \cdot f$

Důsledek:

Gaussova věta: Je-li R gaussovský obor,
pak $R[x]$ je také gaussovský obor.

Čínská věta o zbytcích pro POLYNOMY :

Bud' T těleso. Bud' $u_1, \dots, u_n \in T[x]$ po dvou nesoudělné, $d := \sum \deg u_i$,
 $u_1, \dots, u_n \in T[x]$ lib.

Pak $\exists!$ $f \in T[x]$ stupně $< d$ splňující

$$\begin{aligned} f &\equiv u_1 \pmod{u_1} \\ &\vdots \\ f &\equiv u_n \pmod{u_n} \end{aligned}$$

$$\textcircled{1} \quad m = x - a \Rightarrow f \equiv f(a) \pmod{m}$$

\leadsto speciálním případem je

Věta o interpolaci :

Bud' T těleso. Bud' $a_1, \dots, a_n \in T$ po dvou různé
 $u_1, \dots, u_n \in T$ lib.

Pak $\exists!$ $f \in T[x]$ stupně $< n$ splňující

$$\begin{aligned} f(a_1) &= u_1 \\ &\vdots \\ f(a_n) &= u_n \end{aligned}$$

