def.: **multiplikativní množina** v oboru R:

$M \subseteq R$ t.ž. $0 \notin M$, $1 \in M$, $a, b \in M \Rightarrow a \cdot b \in M$

Konstrukce: Buď R obor, M mult. množina.

Def. relaci 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 $\sim$)

$\rightsquigarrow$ $(Q, +, -, \cdot, 0, 1)$ se nazývá LOKALIZACE oboru R podle M

resp. PODÍLOVÉ TĚLESO pro $M = R - \{0\}$

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

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

Tvrzení [kritérium existence racionálního kořene]

Buď 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]

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

Je-li f primitivní a $\exists p$ prvočinitel v R t.ž. $\boxed{p \mid a_i \;\; \forall i = 0, \dots, n-1}$, $\boxed{p^2 \nmid a_0}$

pak je f ireducibilní v $R[x]$.

Gaussovo lemma: Buď 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: Buď R gaussovský obor, Q jeho podílové těleso, $f, g \in R[x]$ primitivní.
Pak $\boxed{f \mid g \text{ v } R[x] \iff f \mid g \text{ v } Q[x].}$

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

(1) f je ireducibilní v $R[x] \iff$
- $\deg f = 0$, f je ired. v R
- $\deg f > 0$, f primitivní, ired. v $Q[x]$

(2) $\boxed{NSD_{R[x]}(f,g)}$ existuje a je $= c \cdot h$, kde

- $c = NSD_R(c(f), c(g))$
- $h = NSD_{Q[x]}(pp(f), pp(g))$, h primitivní z $R[x]$

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

Důkaz:

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

Čínská věta o zbytcích pro POLYNOMY:

Buď T těleso. Buď $m_1, \dots, m_n \in T[x]$ po dvou nesoudělné, $d := \sum \deg m_i$,
$u_1, \dots, u_n \in T[x]$ lib.

Pak $\exists!\, f \in T[x]$ stupně $< d$ splňující $f \equiv u_1 \pmod{m_1}$
$\vdots$
$f \equiv u_n \pmod{m_n}$

⊙ $m = x - a \Rightarrow f \equiv f(a) \pmod{m}$

⇝ speciálním případem je

Věta o interpolaci:

Buď T těleso. Buď $a_1, \dots, a_n \in T$ po dvou různé
$u_1, \dots, u_n \in T$ lib.

Pak $\exists!\, f \in T[x]$ stupně $< n$ splňující $f(a_1) = u_1$
$\vdots$
$f(a_n) = u_n$

Buď T těleso, $m \in T[x]$ stupně $n \geq 1$.

MODULÁRNÍ FAKTOROKRUH je algebraická struktura

$$T[x]/_{m(x)} = \left(\{f \in T[x] : \deg f < n\}, +, -, \odot, 0, 1\right)$$

kde $f \odot g = f \cdot g \bmod m$.

je to komutativní okruh

Tvrzení: Za uvedených předpokladů NTJE:

(1) $T[x]/(m)$ je těleso

(2) $T[x]/(m)$ je obor

(3) m je ireducibilní v $T[x]$

Buď T těleso, $f \in T[x]$ stupně $n \geq 1$. (ve všech Tvrzeních, definicích, ...)

Tvrzení 1: Pak existuje $S \geq T$ t.ž. f má kořen v S.

Tvrzení 2: Pak existuje $S \geq T$ t.ž. $f \mid (x-a_1) \cdots (x-a_n)$ v $S[x]$.

def.: KOŘENOVÝM NADTĚLESEM rozumíme $S \geq T$ t.ž.
f má v S kořen a & $S = T(a)$
ROZKLADOVÝM NADTĚLESEM rozumíme $S \geq T$ t.ž.
$f \mid (x-a_1) \cdots (x-a_n)$ v $S[x]$ & $S = T(a_1, \ldots, a_n)$.

Důsledek: $\forall T, f$ $\exists$ kořenové i rozkladové nadtěleso

Věta 1: (1) Buď T konečné těleso. Pak $|T| = p^k$, p prvočíslo.

(2) Buď p^k mocnina prvočísla. Pak $\exists T$ těleso t.ž. $|T| = p^k$.

Věta 2: (1) Buď T_1, T_2 konečná tělesa, $|T_1| = |T_2|$. Pak $T_1 \simeq T_2$.

(2) Buď p^k mocnina prvočísla. Pak $\exists m \in \mathbb{Z}_p[x]$ ireducibilní stupně k.

↪ čili $|T| = p^k \Rightarrow \exists m \; T \simeq \mathbb{Z}_p[x]/(m)$

⇝ značení: $\mathbb{F}_{p^k}$ (někdy také $GF(p^k)$)