def.: <u>GRUPA</u> je čtveřice $\mathbf{G} = (G, *, ', e)$ kde

- G je množina
- $*$ je binární operace na G, $'$ je unární op. na G, $e \in G$
- $\forall a, b, c \in G$ $\quad a * (b * c) = (a * b) * c$

$$a * e = e * a = a$$
$$a * a' = a' * a = e$$

inverz jednotka

<u>ABELOVSKÁ</u> GRUPA : navíc $a * b = b * a$

def.: <u>OKRUH</u> je šestice $\mathbf{R} = (R, +, -, \cdot, 0, 1)$ kde

- R je množina, $+, \cdot$ binární op., $-$ unární op., $0, 1 \in R$
- $(R, +, -, 0)$ je abelovská grupa
- $\forall a, b, c \in R$ $\quad a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad , \quad a \cdot 1 = 1 \cdot a = a$

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad , \quad (b + c) \cdot a = b \cdot a + c \cdot a$$

<u>OBOR</u> : komutativní okruh, $0 \neq 1$, $\forall a, b \neq 0 \quad a \cdot b \neq 0$

<u>TĚLESO</u> : komutativní okruh, $0 \neq 1$, $\forall a \neq 0 \; \exists b \quad a \cdot b = 1$

Tvrzení ZV1: Buď $*$ asociativní operace na množině X, buď $a_1, \dots, a_n \in X$. Pak hodnota výrazu $a_1 * \dots * a_n$ nezávisí na uzávorkování.

Tvrzení ZV2: Buď $(G, *, ', e)$ grupa, $a, b, c \in G$. Pak

(1) $a * c = b * c \Rightarrow a = b$, $c * a = c * b \Rightarrow a \neq b$

(2) $a * u = a \Rightarrow u = e$, $u * a = a \Rightarrow u = e$

(3) $a * u = e \Rightarrow u = a'$, $u * a = e \Rightarrow u = a'$

(4) $(a')' = a$, $(a * b)' = b' * a'$!POZOR!

Tvrzení ZV3: Buď $(R, +, -, \cdot, 0, 1)$ okruh, $a, b, c \in R$. Pak

(1) $a \cdot 0 = 0$

(2) $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$, $(-a) \cdot (-b) = a \cdot b$

(3) Je-li R obor, pak $[a \cdot c = b \cdot c,\ c \neq 0] \Rightarrow a = b$

Tvrzení ZV4: Každé těleso je oborem.

Každý konečný obor je tělesem.

def: Buď $\mathbf{R}$ okruh a $S \subseteq R$ podmnožina t.ž.

$0, 1 \in S$; $a, b \in S \Rightarrow -a, a+b, a \cdot b \in S$ ["uzavřená na $+, \cdot, -$"]

Na množině S vezmeme restrikce operací okruhu R.

Dostaneme okruh, který značíme $\mathbf{S}$ a říkáme mu podokruh okruhu R.

terminologie: $\mathbf{R}$ obor $\rightsquigarrow$ říkáme podobor

$\mathbf{R}$ těleso, $\forall a \in S \setminus \{0\}$ $a^{-1} \in S$! $\rightsquigarrow$ říkáme podtěleso

def: Buď $\mathbf{R}, \mathbf{S}$ okruhy, $\varphi : R \to S$ bijekce. Nazýváme ji IZOMORFISMUS

pokud $\forall a, b \in R$
$$\varphi(a+b) = \varphi(a) + \varphi(b)$$
$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

Píšeme $\mathbf{R} \simeq \mathbf{S}$ pokud existuje izomorfismus $\varphi : R \to S$.

Buď $\mathbf{R}$ obor, $M \subseteq R$ multiplikativní množina.

Definujeme relaci $\sim$ na $R \times M$: $\boxed{(a,b) \sim (c,d) \iff ad = bc}$

☺ je to ekvivalence

Bloky ekvivalence $\sim$ nazýváme <u>zlomky</u> a značíme $\frac{a}{b} = [(a,b)]_\sim$.

Na množině Q všech zlomků definujeme operace:

$$\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd} \qquad -\frac{a}{b} := \frac{-a}{b} \qquad \frac{a}{b} \cdot \frac{c}{d} := \frac{a \cdot c}{b \cdot d}$$

a konstanty $0 := \frac{0}{1}$, $1 := \frac{1}{1}$.

☺ operace jsou dobře definované

Strukturu $\mathbf{Q} = (Q, +, -, \cdot, 0, 1)$ nazýváme <u>LOKALIZACE</u> oboru R podle M.

resp. <u>PODÍLOVÉ TĚLESO</u> pro případ $M = R \setminus \{0\}$

<u>Tvrzení:</u> $\mathbf{Q}$ je obor, v případě $M = R \setminus \{0\}$ to je těleso

množina $\{\frac{a}{1} : a \in R\}$ tvoří podobor, který je $\simeq \mathbf{R}$

Buď R komutativní okruh.

POLYNOM proměnné x nad R je VÝRAZ

$$a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$$

kde $n \in \mathbb{N} \cup \{0\}$
$a_0, \dots, a_n \in R$
$a_n \neq 0$

---

značení:
- zkratka $\sum_{i=0}^{n} a_i x^i$
- implicitně $a_m = 0 \ \forall m > n$

terminologie:
- stupeň $:= n$, píšeme $\deg(\dots)$
- $a_0 =$ absolutní člen
  $a_n =$ vedoucí koeficient
- $a_n = 1 \Rightarrow$ polynom je monický

Speciálně taky definujeme nulový polynom 0, $\deg 0 := -1$

Operace:

$$\left(\sum_0^m a_i x^i\right) + \left(\sum_0^n b_i x^i\right) = \sum_0^{\max(m,n)} (a_i + b_i) x^i$$

$$\left(\sum_0^m a_i x^i\right) \cdot \left(\sum_0^n b_i x^i\right) = \sum_{i=0}^{m+n} \left(\sum_{j+k=i} a_j b_k\right) x^i$$

Tvrzení: R obor, Q jeho podílové těleso, $f, g \in R[x]$, $g \neq 0$

$\Rightarrow \exists!\, q, r \in Q[x]$ t.ž. $\boxed{f = g \cdot q + r \quad \& \quad \deg r < \deg g}$

Značení: $q = f \operatorname{div} g$
$r = f \bmod g$

Pozn.: Je-li g monický, pak $q, r \in R[x]$.

Algoritmus dělení:

$$q_0 := 0, \quad r_0 := f$$

$$q_{i+1} := q_i + \frac{\ell(r_i)}{\ell(g)} \cdot x^{\deg r_i - \deg g}$$

$$r_{i+1} := r_i - \frac{\ell(r_i)}{\ell(g)} \cdot x^{\deg r_i - \deg g} \cdot g$$

kde $\ell(\cdots)$ značí vedoucí koeficient

$$\left[\begin{array}{l} \deg r_{i+1} < \deg r_i \quad \forall i \\ f = g \cdot q_i + r_i \quad \forall i \end{array}\right]$$, zastav se ve chvíli kdy $\deg r_{i+1} < \deg g$

def: $R \leq S$, $f \in R[x]$, $a \in S$ ... a je kořen f $\equiv$ $f(a) = 0$

Tvrzení: R obor, $f \in R[x]$, $a \in R$, pak

a je kořen f $\iff$ $x - a \mid f$.

Věta: R obor, $0 \neq f \in R[x]$, $\deg f = n$, pak

f má nejvýše n kořenů.

def: $R \leq S$ komutativní okruhy, $a_1, \dots, a_n \in S$

$R[a_1, \dots, a_n] :=$ nejmenší podokruh S obsahující $R \cup \{a_1, \dots, a_n\}$

"okruhové rozšíření"

def: $R \leq S$ tělesa, $a_1, \dots, a_n \in S$

$R(a_1, \dots, a_n) :=$ nejmenší podtěleso S obsahující $R \cup \{a_1, \dots, a_n\}$

"tělesové rozšíření"

Tvrzení: $R \leq S$ komut. okruhy, $a \in S$, pak

$$R[a] = \{ f(a) : f \in R[x] \} = \{ r_0 + r_1 a + \dots + r_n a^n : n \in \mathbb{N}, r_i \in R \}$$

Tvrzení: $R \leq S$ tělesa, $a \in S$, pak

$$R(a) = \left\{ \frac{f(a)}{g(a)} : f, g \in R[x], g(a) \neq 0 \right\}$$

Tvrzení: $R \leq S$ tělesa, $a \in S$ takový, že není kořenem žádného $f \in R[x]$, $f \neq 0$.

Pak $R[a] \neq R(a)$.

Norma v kvadratických rozšířeních $\mathbb{Z}[\sqrt{s}]$:

$$\nu : \mathbb{Z}[\sqrt{s}] \to \mathbb{N} \cup \{0\}$$
$$a + b\sqrt{s} \mapsto |a^2 - b^2 s|$$

Tvrzení: $\forall u, v \in \mathbb{Z}[\sqrt{s}]$

(1) $\nu(u) \cdot \nu(v) = \nu(u \cdot v)$

(2) $\nu(u) = 1 \iff u$ je invertibilní v $\mathbb{Z}[\sqrt{s}]$

(3) $\left.\begin{array}{l} u \mid v \\ v \nmid u \end{array}\right\} \Rightarrow \nu(u) \mid \nu(v)$ & $\nu(u) \neq \nu(v)$

Tvrzení: $\forall u, v \in \mathbb{Z}[i], v \neq 0 \quad \exists q, r \in \mathbb{Z}[i]$ t.ž.

$$u = v \cdot q + r \quad \& \quad \nu(r) < \nu(v)$$