

# 1 Monoidové okruhy

## Definice 1.1 (Monoid)

Množina  $M$  s binární asociativní operací  $\cdot$  a neutrálním prvkem  $1$  se nazývá monoid. Značíme  $M(\cdot, 1) := (M, \cdot, 1)$ .

### Například

$R$  okruh  $(R, +, -, 0, \cdot, 1) \implies (R, \cdot, 1)$  monoid.  $(\mathbb{N}_0, +, 0)$  komutativní monoid.

### Poznámka (Řád)

Podobně jako pro grupy definujeme pro monoid  $M$  a  $a \in M$  řád prvku  $a$  jako  $\text{ord}_M(a) = |\langle a \rangle|$ , kde  $\langle a \rangle$  je nejmenší podmonoid obsahující  $a$ .

Pokud existuje  $n \in \mathbb{N}$ , že  $a^n = 1$ , pak nejmenší takové  $n$  je rovno  $\text{ord}_M(a)$ . (Pozor, opačně to neplatí, viz  $\mathbb{Z} \bmod 2$ , kde  $\text{ord}(0) = 2$  nebo  $\mathbb{Z} \bmod 8$ , kde  $\text{ord}(4) = 3$ ).

## Definice 1.2 (RM)

Nechť  $R$  okruh,  $M$  monoid. Definujme  $RM = R[M] := R^{(M)} := \{f : M \rightarrow R \mid f(m) = 0 \text{ pro skoro všechna } m\}$ .

Operace na  $R[M]$ :

- $0_{R[M]} = \text{nulové zobrazení}$ ;
- $1_{R[M]} = f$  takové, že  $f(1) = 1$  a  $f(m) = 0$  pro všechna  $m \in M \setminus \{1\}$ ;
- $(f \pm g)(m) = f(m) \pm g(m)$  ( $\forall m \in M$ );
- $(f \cdot g)(m) = \sum_{k, l \in M, k \cdot l = m} f(k) \cdot g(l)$ .

Pak  $R[M]$  je okruh.

### Poznámka

Prvek  $f \in R[M]$  se často zapisují jako formální suma  $\sum_{m \in M} f_m \cdot m$ , kde  $f_m := f(m)$ .

## Tvrzení 1.1

Pokud existuje  $a \in M$  a  $n \in \mathbb{N}$  takové, že  $a^n = 1$ , ale  $a \neq 1$ , pak  $R[M]$  není obor, tj. existují v  $R[M]$  netriviální dělitelé 0.

┌  
Důkaz

$$(a - 1) \cdot (a^{n-1} + a^{n-2} + \dots + a + 1) = a^n - 1^n = a^n - 1 = 0.$$

Ale jen tak to není definované, jelikož  $a$  je z  $M$  ale sčítání ne. Tedy počítáme nad  $R[M]$ , kde  $a = f$  takové, že  $f(a) = a$  a  $f(b) = 1$  pro všechna  $b \in M \setminus \{a\}$ .  $\square$

### Definice 1.3 (Kanonické vnoření do RM)

Kanonická vnoření  $R$  a  $M$  do  $R[M]$  definujeme jako:

$$\alpha : R \rightarrow R[M], r \mapsto f_r, \quad f_r(1) = r, f_r(k) = 0 \quad \forall k \in M \setminus \{1\},$$

$$\beta : M \rightarrow R[M], m \mapsto f_m, \quad f_m(m) = 1, f_r(k) = 0 \quad \forall k \in M \setminus \{m\},$$

kde  $f_r$  značíme často jen  $r$  a  $f_m$  často jen  $m$ .  $\alpha$  je okruhový monomorfismus (tj. injektivní okruhový homomorfismus) a  $\beta$  je injektivní homomorfismus monoidů.

Poznámka (Pozorování)

$$(\forall r \in R)(\forall m \in M) \alpha(r) \cdot \beta(m) = \beta(m) \cdot \alpha(r).$$

TODO?

### Tvrzení 1.2

Existuje vzájemně jednoznačná korespondence mezi strukturami pravých  $R$ -modulů na  $M$  a okruhovými homomorfiismy  $\psi : R \rightarrow \text{End}_Z(M)$ .

┌  
Důkaz

„ $\rightarrow$ “: definujeme  $\psi : R \rightarrow \text{End}_Z(M)$  jako  $r \mapsto (m \mapsto m \cdot r)$ .  $(m + n) \cdot r = mr + nr$ , tedy vhodně definované zobrazení.

$$\psi(1_R) = \text{id}_M = 1_{\text{End}_Z(M)}.$$

$$\psi(r + s) = \psi(r) + \psi(s), \quad m(r + s) = m \cdot r + m \cdot s.$$

$$\psi(r \cdot s) \stackrel{?}{=} \psi(r) \cdot \psi(s)$$

$$(m)(\psi(r \cdot s)) = m \cdot (r \cdot s) = (m \cdot r) \cdot s = ((m)\psi(r))\psi(s) = (m)(\psi(r) \circ \psi(s))$$

„ $\leftarrow$ “:  $\psi$  fixovaný, pro  $m \in M$ ,  $r \in R$  definujeme  $m \cdot r := (m)(\psi(r))$ .  $\square$

TODO!!!

Příklad (Pravé a levé ideály v  $M_n(T)$ )

$T$  komutativní těleso,  $n > 1$ . Mějme  $V$  vektorový podprostor v  $\mathbb{T}^n$ . Potom definujeme  $I_V = \{A \in M_n(T) \mid \text{každý sloupec z } A \text{ náleží do } V\}$ . Pak  $I_V$  je pravý ideál.

Naopak ať  $I$  je pravý ideál v  $M_n(T)$ . Položme  $V = \{a_0 \in T^n \mid a_n \text{ je sloupec v nějakém } A \in I\}$ .  
Ověříme, že  $V$  je vektorový podprostor v  $T$  a že  $I_V = I$ .

**Definice 1.4** ((Von–neumannovsky) regulární okruh, booleaovský okruh)

$R$  okruh nazveme regulární, pokud  $(\forall r \in R)(\exists s \in R)r \cdot s \cdot r = r$ .

$R$  nazveme booleovský, pokud  $(\forall r \in R)r \cdot r = r$ .

*Příklad*

Booleovský  $\implies$  komutativní:  $a + b = (a + b)^2 = aa + ab + ba + bb = a + ab + ba + b$ ,  
tj.  $ab = -(ba) = (-1) \cdot ba = (-1)^2 \cdot ba = ba$ .

TODO?

TODO!!!

TODO!!!

TODO!!!

TODO?