

## Booleovy okruhy

Definice. Okruh  $(R, +, \cdot)$  se nazývá Booleův okruh, je-li idempotentní, tj. pro každé  $x \in R$  platí  $x \cdot x = x$ .

Příklad. Pro libovolnou množinu  $X$  tvoří  $(\mathcal{P}(X), \div, \cap)$ , kde  $\div$  značí symetrický rozdíl množin, tj.  $A \div B = (A - B) \cup (B - A)$ , Booleův okruh. Důkaz zanedlouho uvidíme, je to speciální příklad věty 9.2.

Věta 9.1. *Netriviální Booleův okruh je komutativní okruh charakteristiky 2.*

Důkaz. Z idempotentnosti plyne

$$1 + 1 = (1 + 1) \cdot (1 + 1) = 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 1 = 1 + 1 + 1 + 1.$$

Přičtením  $-(1 + 1)$  dostaneme  $1 + 1 = 0$ . Protože okruh není triviální, platí  $1 \neq 0$ , a tedy má charakteristiku 2.

Opět z idempotentnosti pro libovolné  $x, y \in R$  dostáváme

$$x + y = (x + y) \cdot (x + y) = x \cdot x + x \cdot y + y \cdot x + y \cdot y = x + x \cdot y + y \cdot x + y,$$

odkud  $x \cdot y = -y \cdot x = y \cdot x$ , což jsme měli dokázat.

## Booleův okruh vzniká z Booleovy algebry

Věta 9.2. *Nechť  $(G, \vee, \wedge)$  je Booleova algebra. Definujme na množině  $G$  operace  $+$  a  $\cdot$  takto: pro libovolné  $x, y \in G$  klademe*

$$x + y = (x \wedge y') \vee (x' \wedge y), \quad x \cdot y = x \wedge y.$$

*Pak  $(G, +, \cdot)$  je Booleův okruh.*

Důkaz. Obě operace jsou komutativní, násobení je i asociativní a idempotentní. Pro každé  $x \in G$  platí  $x + 0 = x$ ,  $x + x = 0$ ,  $x \cdot 1 = x$ . Je tedy  $(G, \cdot)$  je pogruba s neutrálním prvkem 1. Dokažme distributivní zákon, necht'  $x, y, z \in G$  jsou libovolné. Z definic a De Morganových zákonů plyne

$$\begin{aligned}x \cdot y + x \cdot z &= ((x \wedge y) \wedge (x \wedge z)') \vee ((x \wedge y)' \wedge (x \wedge z)) = \\&= (x \wedge y \wedge (x' \vee z')) \vee ((x' \vee y') \wedge x \wedge z) = \\&= (x \wedge y \wedge x') \vee (x \wedge y \wedge z') \vee (x' \wedge x \wedge z) \vee (y' \wedge x \wedge z) = \\&= (x \wedge y \wedge z') \vee (x \wedge y' \wedge z) = \\&= x \wedge ((y \wedge z') \vee (y' \wedge z)) = x \cdot (y + z),\end{aligned}$$

což jsme chtěli dokázat.

Zbývá ověřit asociativitu sčítání, necht'  $x, y, z \in G$  jsou libovolné.  
Z definice a De Morganových zákonů plyne

$$\begin{aligned}
 (x + y) + z &= (((x \wedge y') \vee (x' \wedge y)) \wedge z') \vee (((x \wedge y') \vee (x' \wedge y))' \wedge z) = \\
 &= (((x \wedge y') \vee (x' \wedge y)) \wedge z') \vee ((x' \vee y) \wedge (x \vee y') \wedge z) = \\
 &= (x \wedge y' \wedge z') \vee (x' \wedge y \wedge z') \vee \\
 &\quad \vee \left( ((x' \wedge x) \vee (x' \wedge y') \vee (y \wedge x) \vee (y \wedge y')) \wedge z \right) = \\
 &= (x \wedge y' \wedge z') \vee (x' \wedge y \wedge z') \vee \left( ((x' \wedge y') \vee (y \wedge x)) \wedge z \right) = \\
 &= (x \wedge y' \wedge z') \vee (x' \wedge y \wedge z') \vee (x' \wedge y' \wedge z) \vee (x \wedge y \wedge z).
 \end{aligned}$$

Poslední výraz se nezmění, provedeme-li s  $x, y, z$  jakoukoli permutaci. Proto

$$(x + y) + z = (y + z) + x = x + (y + z),$$

a tedy sčítání je asociativní, tudíž  $(G, +)$  je komutativní grupa.  
Ukázali jsme, že  $(G, +, \cdot)$  je Booleův okruh.

## Booleova algebra vzniká z Booleova okruhu

Věta 9.3. *Nechť  $(R, +, \cdot)$  je Booleův okruh. Definujme na množině  $R$  operace  $\vee$  a  $\wedge$  takto: pro libovolné  $x, y \in R$  klademe*

$$x \vee y = x \cdot y + x + y, \quad x \wedge y = x \cdot y.$$

*Pak  $(R, \vee, \wedge)$  je Booleova algebra, kde pro každé  $x \in R$  platí  $x' = x + 1$ .*

Důkaz. Operace  $\wedge$  je komutativní, asociativní a idempotentní a operace  $\vee$  komutativní a idempotentní. Pro libovolné  $x, y, z \in R$  platí

$$\begin{aligned}(x \vee y) \vee z &= (x \cdot y + x + y) \cdot z + (x \cdot y + x + y) + z = \\ &= x \cdot y \cdot z + x \cdot z + y \cdot z + x \cdot y + x + y + z = \\ &= x \cdot (y \cdot z + y + z) + x + y \cdot z + y + z = \\ &= x \vee (y \vee z),\end{aligned}$$

a tedy je  $\vee$  asociativní operace.

Protože

$$(x \vee y) \wedge x = (x \cdot y + x + y) \cdot x = x \cdot y \cdot x + x \cdot x + y \cdot x = x \cdot y + x \cdot y + x = x,$$

a také

$$(x \wedge y) \vee x = (x \cdot y) \cdot x + (x \cdot y) + x = x \cdot y + x \cdot y + x = x,$$

je  $(R, \vee, \wedge)$  svaz. Protože pro každé  $x \in R$  je  $x \wedge 0 = x \cdot 0 = 0$ , platí  $0 \leq x$ , podobně  $x \wedge 1 = x \cdot 1 = x$ , a tedy  $x \leq 1$ . Proto je 0 nejmenší a 1 největší prvek tohoto svazu.

Ověřme, že skutečně je  $x + 1$  komplementem prvku  $x$ :

$$x \wedge (x + 1) = x \cdot (x + 1) = x \cdot x + x = x + x = 0,$$

$$x \vee (x + 1) = x \cdot (x + 1) + x + (x + 1) = 0 + x + x + 1 = 1.$$

Je tedy  $(R, \vee, \wedge)$  komplementární svaz, zbývá ukázat, že je to též svaz distributivní. Platí

$$\begin{aligned}(x \wedge z) \vee (y \wedge z) &= (x \cdot z) \cdot (y \cdot z) + (x \cdot z) + (y \cdot z) = \\ &= x \cdot y \cdot z + x \cdot z + y \cdot z = (x \cdot y + x + y) \cdot z = \\ &= (x \vee y) \wedge z.\end{aligned}$$

Věta je dokázána.

# Korespondence Booleových algeber a Booleových okruhů

Věta 9.4. *Předchozí dvě věty nám dávají jednoznačnou korespondenci mezi Booleovými okruhy a Booleovými algebry.*

Důkaz. Ukážeme, že v předchozí konstrukci si Booleovy okruhy a Booleovy algebry navzájem odpovídají. Součiny a infima na sebe přecházely. Vyjděme z Booleova okruhu:

B. okruh  $(R, +, \cdot) \mapsto$  B. algebra  $(R, \vee, \wedge) \mapsto$  B. okruh  $(R, \oplus, \cdot)$ .

Pro libovolné  $x, y \in R$  tedy platí

$$\begin{aligned}x \oplus y &= (x \wedge y') \vee (x' \wedge y) = \\&= (x \cdot y') \cdot (x' \cdot y) + (x \cdot y') + (x' \cdot y) = \\&= x \cdot (x + 1) \cdot y \cdot (y + 1) + x \cdot (y + 1) + (x + 1) \cdot y = \\&= 0 + x \cdot y + x + x \cdot y + y = x + y.\end{aligned}$$

Nyní vyjděme z Booleovy algebry:

B. algebra  $(R, \vee, \wedge) \mapsto$  B. okruh  $(R, +, \cdot) \mapsto$  B. algebra  $(R, \sqcup, \sqcap)$ .

Pro libovolné  $x, y \in R$  tedy platí

$$\begin{aligned}x \sqcup y &= x \cdot y + x + y = x + y + (x \wedge y) = \\&= x + \left( (y \wedge (x \wedge y)') \vee (y' \wedge (x \wedge y)) \right) = \\&= x + \left( (y \wedge (x' \vee y')) \vee 0 \right) = \\&= x + ((y \wedge x') \vee (y \wedge y')) = x + ((y \wedge x') \vee 0) = \\&= x + (y \wedge x') = (x \wedge (y \wedge x')') \vee (x' \wedge (y \wedge x')) = \\&= (x \wedge (y' \vee x)) \vee (x' \wedge y) = \\&= x \vee (x' \wedge y) = (x \vee x') \wedge (x \vee y) = 1 \wedge (x \vee y) = x \vee y,\end{aligned}$$

což bylo třeba ověřit.

Poznámka. Podobné dvojí pohledy na jeden objekt bývají v matematice velmi cenné, neboť mnohdy ukáží nečekané souvislosti. Příkladem může být dualita, která je pro Booleovy algebry naprosto zřejmá. Výše uvedenou korespondencí se převádí též na Booleovy okruhy, kde už však není tak snadné si jí všimnout.