6. Okruhy a dělitelnost

Definice: Okruh R je množina spolu se dvěma binárními operacemi, sčítáním a násobením takovými, že pro všechna $a, b, c \in R$ platí:

1. $a + b = b + a$
2. $(a + b) + c = a + (b + c)$
3. existuje prvek $0 \in R$ takový, že $a + 0 = a$
4. $a(bc) = (ab)c$
5. $a(b + c) = ab + ac$ a $(b + c)a = ba + ca$

Okruh je abelovskou grupou vzhledem ke sčítání spolu s násobením, které je distributivní zprava i zleva. Okruh nemusí mít jedničku vzhledem k násobení. Pokud ji má, říkáme, že je to okruh s jedničkou (identitou). Nenulový prvek s jedničkou nemusí mít inverzní prvek vzhledem k násobení. Pokud jej má, říkáme, že se jedná o jednotku okruhu.

Příklady:

1. Množina $\mathbb{Z}$ se sčítáním a násobením je komutativní okruh a identitou 1. Jednotky okruhu jsou 1 a -1.
2. Množina $\mathbb{Z}[x]$ polynomů s neznámou x a celými koeficienty se sčítáním a násobením je komutativní okruh s identitou $p(x) = 1$.
3. Množina $M_2(\mathbb{Z})$ matic řádu 2×2 s celými koeficienty je nekomutativní okruh s identitou $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
4. Množina všech reálných spojitých funkcí reálných neznámých, které prochází bodem $[0, 1]$ je komutativní okruh bez identity s bodovým sčítáním a násobením. $((f+g)(a) = f(a)+g(a), (fg)(a) = f(a)g(a))$

Říkáme, že a dělí b (nebo a je dělitel b) a zapisujeme $a|b$ pokud existuje prvek $c \in R$ takový, že $b = ac$.

Věta (pravidla násobení): Nechť $a, b, c \in R$. Potom:

1. $a0 = 0a = 0$
2. $a(-b) = (-a)b = -(ab)$
3. $(-a)(-b) = ab$
4. $a(b - c) = ab - ac$ a $(b - c)a = ba - ca$
   Navíc pokud má R identitu, tak platí
5. $(-1)a = -a$

6. $(-1)(-1) = 1$

Definice: Podmnožina $S \subset R$ je podokruh okruhu R, pokud je S okruh s operacemi R.

Věta: Neprázdná podmnožina S okruhu R je podokruh, pokud je S uzavřená vůči rozdílu a násobení. To znamená $a, b \in S \Rightarrow a - b \in S$, $ab \in S$.

Příklady:
1. 0 a R jsou podokruhy libovolného okruhu R. 0 je triviální podokruh.
2. $0, 2, 4$ je podokruh okruhu $\mathbb{Z}_6$ - celých čísel modulo 6.
3. Pro každé kladné n je množina $n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}$ podokruh celých čísel.
4. Množina $\left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \right\} a, b \in \mathbb{Z}$ diagonálních matic je podokruh okruhu všech matic řádu 2 s celými koeficienty.

Definice: Nenulový prvek a v komutativním okruhu R je dělitel nuly, pokud existuje nenulový prvek $b \in R$ takový, že $ab = 0$.

Definice: Komutativní okruh s nenulovou jedničkou je obor integrity, pokud nemá žádné dělitele nuly.

Příklady:
1. Okruh celých čísel je obor integrity.
2. Okruh $\mathbb{Z}[x]$ polynomů s celými koeficienty je obor integrity.
3. Okruh $\mathbb{Z}_p$ je obor integrity právě tehdy, když je p prvočíslo.
4. Okruh $M_2(\mathbb{Z})$ matic řádu 2 nad celými čísly není obor integrity.

Věta: Nechť a, b, c patří do oboru integrity. Pokud $a \neq 0$ a $ab = ac$, potom $b = c$.

Definice: Charakteristika okruhu R je nejmenší přirozené číslo n takové, že $nx = 0$ pro všechna $x \in R$. Pokud takové číslo neexistuje, říkáme, že R má charakteristiku 0.

Příklad: Okruh celých čísel má charakteristiku 0, $\mathbb{Z}_n$ má charakteristiku 0. Okruh $\mathbb{Z}_2[x]$ polynomů s celými koeficienty modulo 2 má charakteristiku 2.

Věta (charakteristika okruhu s identitou): Nechť R je okruh s jedničkou 1. Pokud má 1 nekonečný řád vzhledem ke sčítání, tak je charakteristika okruhu R rovna 0. Pokud má 1 řád n vzhledem ke sčítání, potom je charakteristika okruhu R rovna n.

Věta: Charakteristika oboru integrity je 0 nebo prvočíslo.