PIERŚCIENIE $(\mathbb{Z}, +, \cdot)$

Def. Pierścieniem nazywamy trójkę $(P, \oplus, \odot)$ gdzie P - zbiór, $\oplus, \odot$ - działanie na P takie, że:
1. $(P, \oplus)$ jest grupą przemienną
2. $\odot$ jest łączne na P.
3. Rozdzielność mnożenia względem dodawania:
$$(\forall a, x, y \in P) \quad a \odot (x \oplus y) = a \odot x + a \odot y \quad \wedge$$
$$(x \oplus y) \odot a = x \odot a \oplus y \odot a$$

Przykłady:
- $(\mathbb{Z}, +, \cdot)$
- $(\mathbb{R}, +, \cdot)$
- $(\mathbb{R}[x], +, \cdot)$

} tu $\cdot$ jest przemienne.

zbiór wielomianów zmiennej x o współczynnikach z $\mathbb{R}$

- Istnieją pierścienie w których mnożenie $\cdot$ nie jest przemienne :(pierścień macierzy)

Notacja: $+, \cdot$ dodawanie i mnożenie

Podobne do oznaczeń $(\mathbb{Z}, +, \cdot)$

element neutralny dodawania nazywamy zerem, 0
element neutralny mnożenia, o ile ist. nazywamy 1.
element przeciwny do $x \in P$ wzgl $+$ oznaczamy $-x$
element pewny do $x \in P$ wzgl $\cdot$ oznaczamy x^{-1}

Fakt Podstawowe własności pierścieni.

Niech $(P, +, \cdot)$ pierścień. Wtedy:
1. $(\forall a \in P) \quad 0 \cdot a = a \cdot 0 = 0$.
2. $\forall a, b \in P \quad (-a) \cdot b = -(a \cdot b)$. $[a \cdot (-b) = -(a \cdot b)]$
3. $\forall a, b \in P \quad (-a) \cdot (-b) = a \cdot b$.
4. $\forall a \in P \quad -a = a \cdot (-1)$, o ile $1 \in P$

Dowód

rozdziel. mnożenie

1. $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$

$a \cdot 0 = a \cdot 0 + a \cdot 0 \quad | + -(a \cdot 0)$ zawsze ist.

$a \cdot 0 + -(a \cdot 0) \overset{\text{Ł}}{=} (a \cdot 0 + a \cdot 0) + -(a \cdot 0)$

$0 = a \cdot 0 + (a \cdot 0 + -(a \cdot 0))$

$0 = a \cdot 0 + 0$

$0 = a \cdot 0 \quad \square$

rozdziel mnożenie..

2. Zauważmy: $(-a) \cdot b + a \cdot b = (-a + a) \cdot b = 0 \cdot b \overset{1}{=} 0$

Zatem $(-a) \cdot b$ i $a \cdot b$ są wzajemnie przeciwne (względem $+$)

więc $-(a \cdot b) = (-a) \cdot b$.

3. Zauważmy $(-a) \cdot (-b) \overset{2}{=} -(a \cdot (-b)) \overset{2}{=} -(-(a \cdot b)) \overset{?!}{=} a \cdot b$.

ćw: w grupie G. $(g^{-1})^{-1} = g$.

4. ćw, wynika z 2 $\square$

PIERŚCIENIE $\mathbb{Z}_n$

Def: Niech $n \in \mathbb{N}^+$. Definiujemy działania na $\{0, 1, \ldots, n-1\}$

1. $+_n$, dla $a, b \in \{0, \ldots, n-1\}$ $a +_n b = (a + b) \pmod{n}$.
2. $\cdot_n$, dla $a, b \in \{0, \ldots, n-1\}$ $a \cdot_n b = (a \cdot b) \pmod{n}$

Fakt: Dla dowolnego $n \in \mathbb{N}^+$ trójka

$\mathbb{Z}_n \overset{\text{ozn}}{=} (\{0, 1, \ldots, n-1\}, +_n, \cdot_n)$ jest pierścieniem.

Przykładowe obliczenie:

- $\mathbb{Z}_{11} = (\{0, 1, 2, \ldots, 10\}, +_{11}, \cdot_{11})$

$8 +_{11} 9 = (8+9) \bmod 11 = 17 \bmod 11 = 6.$

$8 \cdot_{11} 9 = (8 \cdot 9) \bmod 11 = 72 \bmod 11 = 6$

$-8 : \quad 8 +_{11} \underline{3} = 0$

$-8 = 3$

$3^{-1} : \quad 3 \cdot_{11} x = 1 \quad$ tzn $\quad 3 \cdot \underline{x} = 11k + 1$

np: $3 \cdot \underline{4} = 11 \cdot \underline{1} + 1$

$x = 4$

$3^{-1} = 4$ w $\mathbb{Z}_{11}$.

- $3 \cdot_{11} (4 +_{11} 5) = 3 \cdot_{11} 9 = 27 (\bmod 11) = 5$
- $3 \cdot_{11} 4 +_{11} 3 \cdot_{11} 5 = 12 (\bmod 11) +_{11} 15 (\bmod 11) = 1 +_{11} 4 = 5$ $\quad \parallel$

Dowód Faktu: (szkic).

1. $(\mathbb{Z}_n, +_n) = C_n \leftarrow$ grupa.
2. Łączność. $\forall a,b,c \in \{0, \dots, n-1\}$

$$a \cdot_n (b \cdot_n c) = a \cdot_n (b \cdot c) \bmod n =$$
$$(a \cdot (b \cdot c) \bmod n) \bmod n \overset{!}{=} (a \cdot b \cdot c) \bmod n$$
$$(a \cdot_n b) \cdot_n c = \dots = (a \cdot b \cdot c) \bmod n \quad \text{//}$$

3. ćw $\square$

Homomorfizmy pierścieni.

Def. Niech $(P, +, \cdot)$, $(R, \oplus, \odot)$ pierścienie.
Funkcję $\varphi : P \to R$ nazywamy homomorfizmem pierścieni, gdy
1. $\forall a,b \in P \quad \varphi(a+b) = \varphi(a) \oplus \varphi(b)$
2. $\forall a,b \in P \quad \varphi(a \cdot b) = \varphi(a) \odot \varphi(b)$.

TW: Niech $n \in \mathbb{N}^+$. Funkcja $\varphi_n : \mathbb{Z} \to \{0, 1, \dots, n-1\}$
$$\varphi_n(k) = k (\bmod n)$$
jest homomorfizmem z pierścienia $(\mathbb{Z}, +, \cdot)$ w $\mathbb{Z}_n$ $+_n$ $\cdot_n$

D-d: Niech $n \in \mathbb{N}^+$. $a, b \in \mathbb{Z}$.

1. $\varphi_n(a+b) = (a+b) \bmod n = (a \pmod n + b \pmod n) \bmod n$
$= (\varphi_n(a) + \varphi_n(b)) \pmod n = \varphi_n(a) +_n \varphi_n(b)$

2. $\varphi_n(a \cdot b) = (a \cdot b) \bmod n = ((a \bmod n) \cdot (b \bmod n)) \bmod n =$
$(\varphi_n(a) \cdot \varphi_n(b)) \bmod n = \varphi_n(a) \cdot_n \varphi_n(b)$ $\square$

Fakt. Niech $(P, +, \cdot)$, $(R, \oplus, \odot)$ pierścienie, $\varphi: P \to R$ homomorfizm.
Wtedy:

1. $\varphi(0) = 0$
2. $\forall a \in P \quad \varphi(-a) = -\varphi(a)$.
3. $\varphi(1) = 1$ o ile $1 \in P$, $1 \in R$.
4. $\forall a \in P \quad \varphi(a^{-1}) = \varphi(a)^{-1}$ o ile $a^{-1} \in P$

D-d: ćw.

Zasady podzielności.

Fakt, Liczba (w systemie dziesiętnym) jest podzielna przez 3 $\Leftrightarrow$ suma jej cyfr jest podzielna przez 3

D-d. Rozważmy homomorfizm $\varphi_3: \mathbb{Z} \to \{0, 1, 2\}$.

Zauważmy, że $3 \mid n \Leftrightarrow \varphi_3(n) = 0$.

Notacja: dla cyfr $a_1, a_2, \ldots \in \{0, 1, \ldots 9\}$

$\overline{a_1 a_2 a_3} = 100 \cdot a_1 + 10 a_2 + a_3$

$\overline{231} = 100 \cdot 2 + 10 \cdot 3 + 1 = 231$.

Niech $k \in \mathbb{N}$. $k = \overline{a_n a_{n-1} \dots a_0}$. Wtedy

$3 \mid k \iff 3 \mid \overline{a_n a_{n-1} \dots a_0} \iff \varphi_3(\overline{a_n a_{n-1} \dots a_0}) = 0$

$\iff \varphi_3(10^n \cdot a_n + 10^{n-1} \cdot a_{n-1} + \dots + 10 a_1 + a_0) = 0$

φ_3 jest homomorfizmem,

$\iff \varphi_3(10^n \cdot a_n) +_3 \varphi(10^{n-1} \cdot a_{n-1}) +_3 \dots +_3 \varphi(10 a_1) +_3 \varphi(a_0) = 0$

φ_3 jest homomorf.

$\iff \varphi_3(10^n) \cdot_3 \varphi_3(a_n) +_3 \dots +_3 \varphi_3(10) \cdot \varphi_3(a_1) +_3 \varphi_3(a_0) = 0$

$\iff \varphi_3(10)^n \cdot_3 \varphi_3(a_n) +_3 \dots +_3 \cancel{\varphi_3(10)} \cdot_3 \varphi_3(a_1) +_3 \varphi_3(a_0) = 0$

$\iff [\varphi_3(10) = 1]$

$\varphi_3(a_n) +_3 \dots +_3 \varphi_3(a_1) +_3 \varphi_3(a_0) = 0$

$\iff$

$\varphi_3(a_n + \dots + a_1 + a_0) = 0$

$\iff 3 \mid (a_n + a_{n-1} + \dots + a_1 + a_0)$

$3 \mid \overline{a_n a_{n-1} \dots a_1 a_0} \iff 3 \mid a_n + a_{n-1} + \dots + a_1 + a_0$ $\square$