PIERŚCIENIE, CIAŁA I HOMOMORFIZMY

Zbiór R wyposażony w dwa działania $+, \cdot : R^2 \to R$ nazywamy pierścieniem $\Leftrightarrow$

(R1) $(R, +, 0)$ jest grupą abelową,

(R2) $(R, \cdot, 1)$ jest monoidem,

(R3) $\forall x, y, z \in R: (x+y)z = xz + yz$,

$z(x+y) = zx + zy$

(dwustronna rozdzielność mnożenia względem dodawania).

Elementarne obserwacje:

(1) Jeśli pierścień posiada co najmniej 2 elementy, to $0 \neq 1$. Istotnie, $0 \cdot x = 0 \cdot x + 1 \cdot x - x = (0+1) \cdot x - x = 1 \cdot x - x = 0$. Zatem $0 = 1 \Rightarrow x = 1 \cdot x = 0 \cdot x = 0$.

(2) $(-1) \cdot x = -x$ bo $x + (-1) \cdot x = (1-1) \cdot x = 0 \cdot x = 0$

③ Jeśli R jest pierścieniem i $X \neq \emptyset$, to $\mathrm{Map}(X, R)$ jest pierścieniem ze względu na działania dane przez

$$(f+g)(x) := f(x)+g(x), \quad (f \cdot g)(x) := f(x)g(x),$$

$\forall x \in X$. Elementy neutralne to funkcje stałe: $x \mapsto 0$ (dla dodawania) i $x \mapsto 1$ (dla mnożenia).

Przykłady pierścieni:

① Niech G będzie grupą a R pierścieniem

Zbiór $R[G] := \left\{ \alpha \in \mathrm{Map}(G, R) \;\middle|\; \alpha(g) \neq 0 \text{ dla skończonej ilości } g \in G \right\}$

wyposażony w punktowe dodawanie i splotowe mnożenie

$$\forall g \in G: \quad (\alpha * \beta)(g) := \sum_{h \in G} \alpha(h)\beta(h^{-1}g)$$

nazywamy pierścieniem grupowym.

Elementy neutralne ze względu na $+$ i $*$ to odpowiednio funkcja stała $x \mapsto 0$ i funkcja δ_e dana przez

$$\delta_e(g) := \begin{cases} 0 & \text{dla } g \neq e \\ 1 & \text{dla } g = e \end{cases}.$$

(2) Pierścień nazywamy <u>przemiennym</u> $\Leftrightarrow$ jego mnożenie jest przemienne. Pierścień liczb całkowitych $(\mathbb{Z}, +, 0, \cdot, 1)$ jest pierścieniem przemiennym. Podobnie wszystkie pierścienie ilorazowe:

$$\mathbb{Z}/N\mathbb{Z} := \mathbb{Z}/R_N, \quad R_N := \{(m,n) \in \mathbb{Z}^2 \mid m-n \in N\mathbb{Z}\},$$

$N \in \mathbb{N}$. Dla $N=0$ otrzymujemy $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$, dla $N=1$ otrzymujemy $\mathbb{Z}/\mathbb{Z} = \{0\}$ (pierścień zerowy).

<u>Ćwiczenie</u>: Każdy niezerowy element pierścienia $\mathbb{Z}/N\mathbb{Z}$ jest odwracalny $\Leftrightarrow$ N jest liczbą pierwszą.

Ciałem nazywamy niezerowy przemienny pierścień którego każdy niezerowy element jest odwracalny. Innymi słowy, pierścień $(K, +, 0, \cdot, 1)$ jest ciałem $\Leftrightarrow$ $K \setminus \{0\}$ jest grupą abelową.

Przykłady ciał: $\mathbb{Q}$ (ogólniej ciało ułamków),

$\mathbb{R}$ (ogólniej metryczne domknięcia ciał, $\mathbb{C}$ (ogólniej algebraiczne domknięcia ciał)),

$\mathbb{Q} + \sqrt{2}\mathbb{Q}$ (ogólniej rozszerzenia ciał przez pierwiastki wielomianu),

$\mathbb{Z}/p\mathbb{Z}$, gdzie p jest liczbą pierwszą (ogólniej ciała skończone i ich rozszerzenia algebraiczne).

Uwaga: Moc elementów ciała skończonego jest zawsze postaci p^n, gdzie p jest liczbą pierwszą.

Charakterystyką ciała nazywamy liczbę (pierwszą) p taką że $p \cdot 1 = 0$. Jeśli taka liczba nie istnieje, mówimy że ciało ma charakterystykę zero.

Homomorfizmem monoidów nazywamy odwzorowanie pomiędzy monoidami $M \xrightarrow{f} N$ takie że:

① $\forall\, m, m' \in M : f(mm') = f(m)f(m')$,

② $f(e_M) = e_N$ (zachowywanie elementu neutralnego).

Obserwacja: Jeśli $\exists\, m^{-1}$ a f jest homomorfizmem monoidów, to $f(m^{-1}) = f(m)^{-1}$.
Istotnie, $e_N = f(e_M) = f(m m^{-1}) = f(m) f(m^{-1})$
oraz $e_N = f(e_M) = f(m^{-1}m) = f(m^{-1}) f(m)$.

Jądrem homomorfizmu monoidów $M \xrightarrow{f} N$ nazywamy $\operatorname{Ker} f := \{ m \in M \mid f(m) = e_N \}$.

Homomorfizmem grup nazywamy odwzorowanie pomiędzy grupami $G \xrightarrow{f} H$ takie że $\forall\, g, h \in G : f(gh) = f(g) f(h)$.

Obserwacja: $e_H = f(e_G) f(e_G)^{-1} = f(e_G e_G) f(e_G)^{-1}$
$= f(e_G) f(e_G) f(e_G)^{-1} = f(e_G)$.

Jądrem homomorfizmu grup $G \xrightarrow{f} H$ nazywamy
$\operatorname{Ker} f := \{ g \in G \mid f(g) = e_H \}$. ∎

Homomorfizmem pierścieni nazywamy odwzorowanie pomiędzy pierścieniami $R \xrightarrow{f} S$ będące równocześnie homomorfizmem addytywnych grup jak i multiplikatywnych monoidów: $\forall r,s \in R$:

① $f(r+s) = f(r) + f(s)$,

② $f(rs) = f(r)\,f(s)$,

③ $f(1_R) = 1_S$.

Jądrem homomorfizmu pierścieni $R \xrightarrow{f} S$ nazywamy $\ker f := \{r \in R \mid f(r) = 0_S\}$.

Izomorfizmem (monoidów, grup, pierścieni) nazywamy **bijektywny homomorfizm** (monoidów, grup, pierścieni)

Obserwacja: Odwrotność izomorfizmu jest izomorfizmem: $f^{-1}(xy) = f^{-1}(f(f^{-1}(x))f(f^{-1}(y))) = f^{-1}(x)f^{-1}(y)$, itd.

Przykłady homomorfizmów: ① $\forall X \xrightarrow{f} Y$: $2^Y \xrightarrow{f^{-1}} 2^X$, $f^{-1}(A) := \{x \in X \mid f(x) \in A\}$, jest homomorfizmem monoidów dla $\cup$ i $\cap$. ② Znak permutacji $S_n \xrightarrow{\text{sgn}} \{\pm 1\}$ jest jedynym homomorfizmem grup takim że $\text{sgn}(\tau_{ij}) = -1$ $\forall$ transpozycji τ_{ij}.

③ $\forall$ pierścienia R $\exists!$ homomorfizm pierścieni $\mathbb{Z} \xrightarrow{f} R$, $f(m) = m \cdot 1_R$.