

PIERŚCIEŃ, CIAŁA I HOMOMORFIZMY

Piotr M. Hajac
Uniwersytet Warszawski

Wykład 3, 16.10.2013

Typeset by Jakub Szczepanik.

Definicja pierścienia

Definition

Zbiór R wyposażony w dwa działania $R^2 \xrightarrow{+} R$, $R^2 \xrightarrow{\cdot} R$, nazywamy **pierścieniem** wtedy i tylko wtedy gdy

R1 $(R, +, 0)$ jest grupą abelową,

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

R3 $\forall x, y, z \in R : (x + y)z = xz + yz, \quad z(x + y) = zx + zy$
(obustronna rozdzielność mnożenia względem dodawania).

Pierścień nazywamy **przemiennym** wtedy i tylko wtedy gdy jego mnożenie jest przemienne.

Elementarne obserwacje:

- 1 Jeśli pierścień ma 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 $x + (-1) \cdot x = (1 - 1) \cdot x = 0 \cdot x = 0$.

Przykłady pierścieni

- ❶ **Pierścień liczb całkowitych** $(\mathbb{Z}, +, 0, \cdot, 1)$ jest pierścieniem przemennym. Dla dowolnego $N \in \mathbb{N}$, przemienne są pierścienie ilorazowe:

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

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

- ❷ Jeśli R jest pierścieniem i $X \neq \emptyset$, to $\text{Map}(X, R)$ jest pierścieniem ze względu na **działania punktowe** dane przez

$$\begin{aligned} \forall x \in X : \quad (f + g)(x) &:= f(x) + g(x), \\ (f \cdot g)(x) &:= f(x)g(x). \end{aligned}$$

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

Mnożenie spłotowe

Niech G będzie monoidem a R pierścieniem. Zdefiniujemy zbiór

$$R[G] := \left\{ \alpha \in \text{Map}(G, R) \mid \begin{array}{l} \alpha(g) \neq 0 \text{ dla} \\ \text{skończonej} \\ \text{ilości } g \in G \end{array} \right\}.$$

Odwzorowanie $R[G] \times R[G] \xrightarrow{*} R[G]$ zadane wzorem $\forall g \in G :$

$$(\alpha * \beta)(g) := \sum_{h, h' \in G, hh' = g} \alpha(h)\beta(h')$$

nazywamy **mnożeniem spłotowym**. Widać że jest ono dobrze określone. Można też sprawdzić że jest łączne. Jego elementem neutralnym jest funkcja δ_e dana przez

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

gdzie e jest elementem neutralnym działania w G . Zatem $(R[G], *, \delta_e)$ jest monoidem.

Pierścienie monoidalne i grupowe

Z drugiej strony, dodawanie punktowe i zerowa funkcja stała zadają na $R[G]$ strukturę grupy abelowej. Mnożenie punktowe jest obustronnie rozdzielne względem punktowego dodawania.

Definition

Zbiór $R[G]$ wraz z dodawaniem punktowym, stałą funkcją zerową, mnożeniem splotowym, i funkcją δ_e nazywamy **pierścieniem monoidalnym**. Jeśli G jest grupą, $(R[G], +, 0, *, \delta_e)$ nazywamy **pierścieniem grupowym**.

Jednym z najważniejszych przykładów pierścieni monoidalnych jest **pierścień wielomianów**. Wówczas naszym monoidem jest $(\mathbb{N}, +, 0)$, a wzór na mnożenie splotowe okazuje się być znanym wzorem na mnożenie wielomianów. A jeśli zamiast monoidu liczb naturalnych weźmiemy grupę liczb całkowitych, otrzymamy **wielomiany Laurenta**. Zaś jeśli zamiast funkcji zerujących się wszędzie poza skończoną ilością liczb naturalnych weźmiemy dowolne funkcje, otrzymamy **szeregi formalne**.

Definition

Ciałem nazywamy niezerowy przemienny pierścień którego każdy niezerowy element jest odwracalny. Najmniejszą liczbę naturalną n taką że

$$\overbrace{1 + \cdots + 1}^{n\text{-razy}} = 0$$

nazywamy **charakterystyką ciała**. Jeśli taka liczba nie istnieje, mówimy że ciało ma charakterystykę zero.

Elementarne obserwacje:

- 1 Niezerowy przemienny pierścień $(K, +, 0, \cdot, 1)$ jest ciałem $\Leftrightarrow K \setminus \{0\}$ jest grupą abelową.
- 2 Charakterystyka ciała jest albo zerem albo liczbą pierwszą.

Przykłady ciał

- 1 $\mathbb{Q}$ (ogólniej ciało ułamków),
- 2 $\mathbb{R}$ (ogólniej metryczne domknięcia ciał),
- 3 $\mathbb{C}$ (ogólniej algebraiczne domknięcia ciał),
- 4 $\mathbb{Q} + \sqrt{2}\mathbb{Q}$ (ogólniej rozszerzenia ciał przez pierwiastki wielomianu),
- 5 $\mathbb{Z}/p\mathbb{Z}$, gdzie p jest liczbą pierwszą (ogólniej ciała skończone i ich rozszerzenia algebraiczne).

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

Homomorfizmy

Definition

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).

Homomorfizmem grup nazywamy odwzorowanie pomiędzy grupami spełniające pierwszy z powyższych warunków. **Homomorfizmem pierścieni** (**ciał**) nazywamy odwzorowanie pomiędzy pierścieniami (ciałami) będące równocześnie homomorfizmem addytywnych grup jak i multiplikatywnych monoidów (grup).

Jeśli $\exists m^{-1}$ a f jest homomorfizmem monoidów, to $f(m^{-1}) = f(m)^{-1}$,
bo $e_N = f(e_M) = f(mm^{-1}) = f(m)f(m^{-1})$ i $e_N = f(m^{-1})f(m)$.

Jeśli $G \xrightarrow{f} H$ jest homomorfizmem grup, to $e_H = f(e_G)f(e_G)^{-1} = f(e_G e_G)f(e_G)^{-1} = f(e_G)f(e_G)f(e_G)^{-1} = f(e_G)$.

Jądra homomorfizmów i izomorfizmy

Definition

Jądrem homomorfizmu $M \xrightarrow{f} N$ monoidów, grup, pierścieni, ciał nazywamy

$$\boxed{\text{Ker } f := \{m \in M \mid f(m) = 0_N\}},$$

gdzie 0_N jest elementem neutralnym (addytywnej) struktury monoidalnej w N .

Homomorfizm grup $G \xrightarrow{f} H$ jest iniektywny $\Leftrightarrow \text{Ker } f = \{e_G\}$, bo $f(g) = f(g') \Leftrightarrow e_H = f(g)^{-1}f(g') = f(g^{-1})f(g') = f(g^{-1}g')$.

Definition

Izomorfizmem (monoidów, grup, pierścieni, ciał) nazywamy bijektywny homomorfizm (monoidów, grup, pierścieni, ciał).

Odwrotność izomorfizmu jest izomorfizmem:

$$\begin{aligned} f^{-1}(xy) &= f^{-1}\left(f(f^{-1}(x))f(f^{-1}(y))\right) = \\ f^{-1}\left(f\left(f^{-1}(x)f^{-1}(y)\right)\right) &= f^{-1}(x)f^{-1}(y), \text{ itd.} \end{aligned}$$

Przykłady homomorfizmów i podobiektu

- 1 $\forall X \xrightarrow{f} Y : 2^Y \xrightarrow{f^{-1}} 2^X, \boxed{f^{-1}(A) := \{x \in X \mid f(x) \in A\}},$
jest homomorfizmem monoidów dla $\cup$ i $\cap$. (Zbiór $f^{-1}(A)$ nazywamy **przeciwbrazem** A .)
- 2 Jedynym homomorfizmem grup $S_n \xrightarrow{f} \{\pm 1\}$ takim że $f(\tau_{ij}) = -1$ dla każdej transpozycji τ_{ij} jest znak permutacji.
- 3 $\forall$ pierścienia $R \exists!$ homomorfizm pierścieni $\mathbb{Z} \xrightarrow{f} R,$
 $f(m) = m \cdot 1_R.$
- 4 Można pokazać że wszystkie homomorfizmy ciał są injekcjami.

Jeżeli homomorfizm jest injektywny, to jego obraz jest “podobiektu”.

Definition

Podmonoidem, podgrupą, podpierścieniem, podciałem monoidu, grupy, pierścienia, ciała N nazywamy podzbiór $M \subseteq N$ do którego zawężają się działania w N , który zawiera elementy neutralne tych działań, i który z tą odziedziczoną strukturą jest monoidem, grupą, pierścieniem, ciałem.