Algebra Komputerowa

Elementy Teorii Pierścieni [1, 2]

Filip Zieliński

2025

Spis Treści

Definicja

Zbiór R z dwoma działaniami $+, \cdot$ nazywamy **Pierścieniem**, jeżeli zachodzą następujące warunki

1. $(R, +)$ jest grupą abelową
2. $(R, \cdot)$ jest półgrupą
3. $\forall x, y, z \in R \quad x \cdot (y + z) = x \cdot y + x \cdot z \wedge$
   $(x + y) \cdot z = x \cdot z + y \cdot z$ *(rozdzielność mn. wzg. dod.)*

Definicja

Zbiór R z dwoma działaniami $+, \cdot$ nazywamy **Pierścieniem z jedynką**, jeżeli zachodzą następujące warunki

1. $(R, +)$ jest grupą abelową
2. $(R, \cdot)$ jest monoidem
3. $\forall x, y, z \in R \quad x \cdot (y + z) = x \cdot y + x \cdot z \wedge$
   $(x + y) \cdot z = x \cdot z + y \cdot z$ *(rozdzielność mn. wzg. dod.)*

Powtórka

Definicja

Zbiór R z dwoma działaniami $+, \cdot$ nazywamy **Pierścieniem przemiennym z jedynką**, jeżeli zachodzą następujące warunki

1. $(R, +)$ jest grupą abelową
2. $(R, \cdot)$ jest monoidem przemiennym
3. $\forall x, y, z \in R \quad x \cdot (y + z) = x \cdot y + x \cdot z \wedge$
   $(x + y) \cdot z = x \cdot z + y \cdot z$ *(rozdzielność mn. wzg. dod.)*

Definicja

Zbiór R z dwoma działaniami $+, \cdot$ nazywamy **Pierścieniem przemiennym z jedynką**, jeżeli zachodzą następujące warunki

1. $(R, +)$ jest grupą abelową
2. $(R, \cdot)$ jest monoidem przemiennym
3. $\forall x, y, z \in R \quad x \cdot (y + z) = x \cdot y + x \cdot z \wedge$
   $(x + y) \cdot z = x \cdot z + y \cdot z$ *(rozdzielność mn. wzg. dod.)*

Uwaga

Od tego momentu rozważamy jedynie pierścienie przemienne z jedynką. O ile nie jest powiedziane inaczej, gdy piszemy *pierścień* mamy na myśli *pierścień przemienny z jedynką.*

Kluczowe pierścienie

Z naszej perspektywy najistotniejszymi pierścieniami będą

- $\mathbb{Z}$ - pierścień liczb całkowitych.
- $R[x]$ - pierścień wielomianów jednej zmiennej o współczynnikach z pierścienia R.
- $R[x_1, \ldots, x_n]$ - pierścienie wielomianów wielu zmiennych.

Ideały

Definicja

Niepusty podzbiór I pierścienia R nazywa się **ideałem**, jeżeli zachodzi

$$\forall a, b \in I \quad a + b \in I \tag{1}$$

$$\forall a \in I \; \forall r \in R \quad r \cdot a \in I \tag{2}$$

Definicja

Niepusty podzbiór I pierścienia R nazywa się **ideałem**, jeżeli zachodzi

$$\forall a, b \in I \quad a + b \in I \tag{1}$$

$$\forall a \in I \; \forall r \in R \quad r \cdot a \in I \tag{2}$$

Konwencja

Fakt, że I jest ideałem pierścienia R oznaczamy przez $I \triangleleft R$.

Uwaga

Jeżeli potraktujemy R jako grupę z dodawaniem, to I jest podgrupą normalną grupy R.

Przykład

Ideałami są np.

1. Każdy pierścień R posiada ideał trywialny $\{\mathbf{0}\}$ oraz ideał niewłaściwy R.
2. W pierścieniu $\mathbb{Z}$ ideałami są zbiory postaci $n\mathbb{Z} = \{n \cdot k \mid k \in \mathbb{Z}\}$ - zbiory wielokrotności danej liczby.
3. W pierścieniu wielomianów $R[x]$ weźmy ustalony wielomian f. Zbiór $I = \{fg \mid g \in R[x]\}$ jest ideałem w $R[x]$.
4. W pierścieniu wielomianów $R[x_1, \dots, x_n]$ weźmy ustalone wielomiany f, g. Zbiór $I = \{a_1 f + a_2 g \mid a_1, a_2 \in R[x_1, \dots x_n]\}$ jest ideałem w pierścieniu $R[x_1, \dots, x_n]$.

Twierdzenie

Niech *R* będzie pierścieniem, a I ideałem tego pierścienia. Zachodzi

$$I = R \Leftrightarrow \mathbf{1} \in I$$

Twierdzenie

Niech R będzie pierścieniem, a I ideałem tego pierścienia. Zachodzi

$$I = R \Leftrightarrow \mathbf{1} \in I$$

Dowód.

($\Rightarrow$). Oczywiste.
($\Leftarrow$). Jeżeli $\mathbf{1} \in I$ to z definicji dla dowolnego $r \in R$ zachodzi $r \cdot \mathbf{1} \in I$, czyli $r \in I$. $\square$

Twierdzenie

Niech R będzie pierścieniem, a I ideałem tego pierścienia. Zachodzi

$$I = R \Leftrightarrow \mathbf{1} \in I$$

Dowód.

($\Rightarrow$). Oczywiste.
($\Leftarrow$). Jeżeli $\mathbf{1} \in I$ to z definicji dla dowolnego $r \in R$ zachodzi $r \cdot \mathbf{1} \in I$, czyli $r \in I$. $\square$

Twierdzenie

Jeżeli K jest ciałem, to jedynymi jego ideałami są $\{\mathbf{0}\}$ oraz K.

Twierdzenie

Jeżeli K jest ciałem, to jedynymi jego ideałami są $\{\mathbf{0}\}$ oraz K.

Dowód.

Niech $I \triangleleft K$. Jeżeli $I = \{\mathbf{0}\}$ to twierdzenie zachodzi. W innym przypadku istnieje $a \in K$ takie, że $a \neq \mathbf{0}, a \in I$. Z definicji dla dowolnego $r \in K$ mamy $r \cdot a \in K$. W szczególności dla $r = a^{-1}$ z czego wynika $a \cdot a^{-1} = 1 \in I$ zatem $I = K$. □

Twierdzenie

Jeżeli K jest ciałem, to jedynymi jego ideałami są $\{\mathbf{0}\}$ oraz K.

Dowód.

Niech $I \triangleleft K$. Jeżeli $I = \{\mathbf{0}\}$ to twierdzenie zachodzi. W innym przypadku istnieje $a \in K$ takie, że $a \neq \mathbf{0}, a \in I$. Z definicji dla dowolnego $r \in K$ mamy $r \cdot a \in K$. W szczególności dla $r = a^{-1}$ z czego wynika $a \cdot a^{-1} = 1 \in I$ zatem $I = K$. □

Twierdzenie

Jeżeli jedynymi ideałami pierścienia R są $\{\mathbf{0}\}$ oraz całe R, to R jest ciałem.

Twierdzenie

Niech będzie dany pierścień R oraz niepusty podzbiór T. Jeśli $I_t \triangleleft R$ dla każdego $t \in T$ to $\bigcap_{t \in T} I_t \triangleleft R$ (przecięcie ideałów jest ideałem).

Ideały generowane

Rozważmy pierścień R i element $a \in R$. Zdefiniujmy $I = \{r \cdot a \mid r \in R\}$. Zauważmy, że I jest ideałem R. Dodatkowo, zauważmy, że jest to najmnijeszy ideał zawierający a, to znaczy

$$\{r \cdot a \mid r \in R\} = \bigcap \{J \triangleleft R \mid a \in J\}.$$

Rozważmy pierścień R i element $a \in R$. Zdefiniujmy $I = \{r \cdot a \mid r \in R\}$. Zauważmy, że I jest ideałem R. Dodatkowo, zauważmy, że jest to najmnijeszy ideał zawierający a, to znaczy

$$\{r \cdot a \mid r \in R\} = \bigcap \{J \triangleleft R \mid a \in J\}.$$

Możemy to uogólnić:

Definicja

Niech R będzie pierścieniem, natomiast $A = \{a_1, \ldots, a_s\} \subseteq R$ skończonym jego podzbiorem. **Ideałem generowanym przez A** nazywamy zbiór

$$\langle A \rangle = \langle a_1, \ldots, a_s \rangle = \left\{ \sum r_i \cdot a_i \mid r_i \in R, a_i \in A \right\}$$

Ideały generowane

Twierdzenie

Ideał generowany przez zbiór jest ideałem.

Twierdzenie

Niech R będzie pierścieniem oraz $A = \{a_1, \dots, a_s\} \subseteq R$. Zachodzi

$$\langle A \rangle = \bigcap \{I \lhd R \mid A \subseteq I\}.$$

Twierdzenie

Ideał generowany przez zbiór jest ideałem.

Twierdzenie

Niech R będzie pierścieniem oraz $A = \{a_1, \ldots, a_s\} \subseteq R$. Zachodzi

$$\langle A \rangle = \bigcap \{ I \triangleleft R \mid A \subseteq I \}.$$

Konwencja

Jeżeli $I = \langle A \rangle = \langle a_1, \ldots, a_s \rangle \triangleleft R$, to A nazywamy *zbiorem generatorów* I, elementy $a_1, \ldots, a_s$ nazywamy *generatorami* I. Jeżeli da się zapisać ideał jako generowany przez skończony zbiór, to mówimy, że ideał jest *skończenie generowny*.

Uwaga

Jeżeli podzbiór A pierścienia R jest nieskończony, wszystkie definicje i twierdzenia wciąż zachodzą, tylko dokładamy do definicji jeden warunek

$$\langle A \rangle = \left\{ \sum r_i \cdot a_i \mid r_i \in R, a_i \in A \right\}$$

gdzie *prawie wszystkie* r_i są równe 0.

Ideały generowane

Uwaga

Jeżeli podzbiór A pierścienia R jest nieskończony, wszystkie definicje i twierdzenia wciąż zachodzą, tylko dokładamy do definicji jeden warunek

$$\langle A \rangle = \left\{ \sum r_i \cdot a_i \mid r_i \in R, a_i \in A \right\}$$

gdzie *prawie wszystkie* r_i są równe 0.

Uwaga

Dowodzi się, że każdy ideał w $\mathbb{Z}$ oraz $K[x_1, \ldots, x_n]$, gdzie K jest ciałem jest skończenie generowany.

Definicja

Niech R bedzie pierścieniem oraz $I, J \lhd R$. **Sumę ideałów I, J** definiujemy jako

$$I + J = \{a + b \mid a \in I, b \in J\}.$$

Suma Algebraiczna Ideałów

KOŁO NAUKOWE

Definicja

Niech R bedzie pierścieniem oraz $I, J \triangleleft R$. **Sumę ideałów I, J** definiujemy jako

$$I + J = \{a + b \mid a \in I, b \in J\}.$$

Twierdzenie

Jeżeli $I, J \triangleleft R$, gdzie R jest pierścieniem, to $I + J \triangleleft R$ (suma ideałów jest ideałem).

Definicja

Niech R bedzie pierścieniem oraz $I, J \lhd R$. **Sumę ideałów I, J** definiujemy jako

$$I + J = \{a + b \mid a \in I, b \in J\}.$$

Twierdzenie

Jeżeli $I, J \lhd R$, gdzie R jest pierścieniem, to $I + J \lhd R$ (suma ideałów jest ideałem).

Twierdzenie

Jeżeli $I = \langle a_1, \ldots, a_s \rangle$ oraz $J = \langle b_1, \ldots, b_r \rangle$ to

$$I + J = \langle a_1, \ldots a_s, b_1, \ldots, b_r \rangle.$$

Definicja

Mówimy, że dwa ideały I, J pierścienia *R* są **względnie pierwsze** jeśli zachodzi

$$I + J = R$$

Iloczyn algebraiczny Ideałów

Definicja

Niech R będzie pierścieniem oraz I, J ideałami w tym pierścieniu. **Iloczyn algebraiczny ideałów** I, J definiujemy jako

$$IJ = \left\{ \sum a_i \cdot b_i \mid a_i \in I, b_i \in J \right\}.$$

gdzie prawie wszystkie $a_i \cdot b_i$ są zerami (są to skończone sumy).

Definicja

Niech R będzie pierścieniem oraz I, J ideałami w tym pierścieniu. **Iloczyn algebraiczny ideałów** I, J definiujemy jako

$$IJ = \left\{ \sum a_i \cdot b_i \mid a_i \in I, b_i \in J \right\}.$$

gdzie prawie wszystkie $a_i \cdot b_i$ są zerami (są to skończone sumy).

Twierdzenie

Iloczyn algebraiczny ideałów jest ideałem.

Obserwacja

Jeśli $I_1, \ldots I_n$ to ideały pierścienia R, to zauważmy, że

$$I_1 \cdots I_n = \langle a_{i1} \cdots a_{in} \mid a_{ij} \in I_j \rangle$$

Iloczyn algebraiczny ideałów

Twierdzenie

Jeśli $I_1, \ldots I_n$ to ideały pierścienia R, to zachodzi

$$I_1 \cdots I_n \subseteq I_1 \cap \ldots \cap I_n$$

KOŁO NAUKOWE

Twierdzenie

Jeśli $I_1, \ldots I_n$ to ideały pierścienia *R*, to zachodzi

$$I_1 \cdots I_n \subseteq I_1 \cap \ldots \cap I_n$$

Twierdzenie

Niech *R* będzie pierścieniem oraz $I_1, \ldots I_n \triangleleft R$ będą ideałami (parami) względnie pierwszymi w *R*. Zachodzi

$$I_1 \cap \ldots \cap I_n = I_1 \cdot \ldots \cdot I_n$$

Definicja

Ideał I pierścienia R nazywamy **ideałem pierwszym**, jeżeli zachodzi

$$\forall a, b \in R \quad ab \in I \Rightarrow a \in I \vee b \in I.$$

Rozważmy pierścień R oraz jego ideał I.

Obserwacja

Ponieważ $(I, +)$ jest podgrupą (normalną) addytywną pierścienia, konstrukcja warstw oraz grupy ilorazowej ze względu na dodawanie jest w pełni poprawna.

Konwencja

Zwyczajowo warstwę elementu $a \in R$ względem ideału I oznaczamy jako $a + I$.

Twierdzenie

Jeśli I jest ideałem pierścienia *R* to wzór

$$(a + I) \odot (b + I) = ab + I$$

określa działanie w zbiorze warstw względem I nazywane mnożeniem warstw. Zbiór warstw z dodawaniem warstw i mnożeniem warstw tworzy pierścień.

KOŁO NAUKOWE

Definicja

Jeżeli I jest ideałem pierścienia *R* to pierścień warstw z dodawaniem warstw i mnożeniem warstw nazywamy **Pierścieniem Ilorazowym** *R* względem I i oznaczamy przez R/I.

Definicja

Jeżeli I jest ideałem pierścienia *R* to pierścień warstw z dodawaniem warstw i mnożeniem warstw nazywamy **Pierścieniem Ilorazowym** *R* względem I i oznaczamy przez R/I.

Konwencja

Warstwę $a + I$ nazywamy klasą reszt *a* albo klasą modulo *a* albo klasą abstrakcji *a*.
R/I czasem nazywane jest też pierścieniem reszt modulo I.
Działania w pierścieniu ilorazowym R/I oznacza się zwykle tak samo jak działania w pierścieniu *R*.

Twierdzenie

Niech R, R' będą pierścieniami. Jądro homomorfizmu $\varphi : R \to R'$ jest ideałem pierścienia R.

Twierdzenie

Niech R, R' będą pierścieniami. Jądro homomorfizmu $\varphi : R \to R'$ jest ideałem pierścienia R.

Twierdzenie

Niech R, R' będą pierścieniami, $\varphi : R \to R'$ homomorfizmem tych pierścieni oraz $J \triangleleft R'$. Zachodzi $\varphi^{-1}(J) \triangleleft R$ (przeciwobraz ideału jest ideałem).

Twierdzenie

Niech R, R' będą pierścieniami. Jądro homomorfizmu $\varphi : R \to R'$ jest ideałem pierścienia R.

Twierdzenie

Niech R, R' będą pierścieniami, $\varphi : R \to R'$ homomorfizmem tych pierścieni oraz $J \triangleleft R'$. Zachodzi $\varphi^{-1}(J) \triangleleft R$ (przeciwobraz ideału jest ideałem).

Uwaga

Obrazem homomorficznym ideału **nie zawsze** jest ideał.

KOŁO NAUKOWE

Twierdzenie

Jeśli I jest ideałem pierścienia R to odwzorowanie $\nu : R \to R/I$ zadane wzorem $\nu(a) = a + I$ jest homomorfizmem pierścieni $R, R/I$ oraz $\ker \nu = I$.

Twierdzenie

Jeśli I jest ideałem pierścienia R to odwzorowanie $\nu : R \to R/I$ zadane wzorem $\nu(a) = a + I$ jest homomorfizmem pierścieni $R, R/I$ oraz $\ker \nu = I$.

Konwencja

Homomorfizm $\nu : R \to R/I$ nazywamy homomorfizmem kanonicznym.

Twierdzenie

Jeśli I jest ideałem pierścienia R to odwzorowanie $\nu : R \to R/I$ zadane wzorem $\nu(a) = a + I$ jest homomorfizmem pierścieni $R, R/I$ oraz $\ker \nu = I$.

Konwencja

Homomorfizm $\nu : R \to R/I$ nazywamy homomorfizmem kanonicznym.

Wniosek

Ideały danego pierścienia i tylko one są jądrami homomorfizmów pierścieni.

Twierdzenie

Jeśli φ jest homomorfizmem pierścienia R na pierścień R', to istnieje izomorfizm $\psi : R' \to R/\ker\varphi$, dla którego przemienny jest diagram

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[dr, "\nu"'] & R' \arrow[d, "\psi"] \\ & R/\ker\varphi \end{tikzcd}$$

gdzie ν to homomorfizm kanoniczny.

KOŁO NAUKOWE

Twierdzenie

Jeśli φ jest homomorfizmem pierścienia R na pierścień R', to istnieje izomorfizm $\psi : R' \to R/\ker\varphi$, dla którego przemienny jest diagram

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[dr, "\nu"'] & R' \arrow[d, "\psi"] \\ & R/\ker\varphi \end{tikzcd}$$

gdzie ν to homomorfizm kanoniczny.

Twierdzenie

Jedynymi homomorfizmami ciała na ciało są izomorfizmy.

Definicja

Relacja równoważności $\sim$ określona na pierścieniu R nazywa się **kongruencją**, jeżeli

$$[(a \sim b) \wedge (c \sim d)] \Rightarrow [(a + c \sim b + d) \wedge (ac \sim bd)].$$

Kongruencje, to relacje równoważności, ktore można dodawać i mnożyc stronami.

Twierdzenie

Niech I będzie ideałem pierścienia *R*. Relacja przystawania elementów modulo I

$$a \equiv b \ (I) \Leftrightarrow a - b \in I$$

jest kongruencją w pierścieniu *R*.

Twierdzenie

Niech I będzie ideałem pierścienia R. Relacja przystawania elementów modulo I

$$a \equiv b \ (I) \Leftrightarrow a - b \in I$$

jest kongruencją w pierścieniu R.

Obserwacja

Kongruencje pierścieni można odejmować stronami.

Twierdzenie

Jeśli relacja równoważności $\sim$ określona na pierścieniu *R* jest kongruencją, to klasa abstrakcji I zbioru ilorazowego *R*/ $\sim$ która zawiera **0** pierścienia *R* jest ideałem pierścienia *R* oraz *R*$/\sim =$ *R*$/I$.

Źródła

[1] Bolesław Gleichgewicht. *Algebra : podręcznik dla kierunków nauczycielskich studiów matematycznych*. PWN, 1976.

[2] Łukasz Kubat. *Algebra Komutatywna - Notatki do wykładów prof. Kamila Ruska*.

Pytania, wątpliwości, uwagi ?