Algebra Komputerowa

Pierścienie z jednoznacznością rozkładu [2, 1]

Filip Zieliński

2025

Spis Treści

Założenia

KOŁO NAUKOWE

Uwaga

Przypominam, że mówiąc pierścień mamy na myśli pierścień przemienny z jedynką.

Założenia

KOŁO NAUKOWE

Uwaga

Przypominam, że mówiąc pierścień mamy na myśli pierścień przemienny z jedynką.

Uwaga

Dodatkowo, w tym rozdziale zawężamy nasze rozważania do pierścieni całkowitych. Mówiąc pierścień, mamy na myśli pierścień całkowity przemienny z jedynką.

Niech R będzie pierścieniem oraz a, b elementami tego pierścienia.

Definicja

Mówimy, że element a *dzieli* b, jeśli istnieje taki element $c \in R$, że $ac = b$. Tak więc

$$a \mid b \Leftrightarrow \exists c \in R : b = ac$$

Gdy $a \mid b$ mówimy, że "a jest dzielnikiem elementu b" lub "b jest podzielne przez a" lub "b jest wielokrotnością a". Jeśli a nie dzieli b to piszemy $a \nmid b$.

Własności podzielności

KOŁO NAUKOWE

Obserwacja

Relacja $|$ określona na pierścieniu R jest relacją zwrotnią i przechodnią.

Twierdzenie

Dla dowolnych $a, b, c, d \in R$ zachodzi

1. $\mathbf{1} \mid a$
2. $a \mid b \Rightarrow a \mid bc$
3. $a \mid b \wedge a \mid c \Rightarrow a \mid b \pm c$
4. $a \mid b \Rightarrow ac \mid bc$
5. $a \mid b \wedge c \mid d \Rightarrow ac \mid bd$

Relacja stowarzyszenia

KOŁO NAUKOWE

Definicja

Mówimy, że elementy $a, b \in R$ są stowarzyszone, co zapisujemy $a \sim b$, jeśli $a \mid b \wedge b \mid a$.

Obserwacja

Relacja stowarzyszenia, jest relacją równoważności.

Relacja stowarzyszenia
Podzielność

KOŁO NAUKOWE

Definicja

Mówimy, że elementy $a, b \in R$ są stowarzyszone, co zapisujemy $a \sim b$, jeśli $a \mid b \wedge b \mid a$.

Obserwacja

Relacja stowarzyszenia, jest relacją równoważności.

Definicja

Element u pierścienia R nazywamy jednością, jeżeli istnieje w pierścieniu R do niego element odwrotny.

Definicja

Zbiór wszystkich jedności w pierścieniu R nazywamy *zbiorem elementów odwracalnych* i oznaczamy przez U_R.

Zbiór jedności

Obserwacja

Zbiór elementów odwracalnych pierścienia R jest grupą względem ich mnożenia.

Zbiór jedności

Obserwacja

Zbiór elementów odwracalnych pierścienia R jest grupą względem ich mnożenia.

Obserwacja

Zachodzi $U_R = \{a \in R : a \sim \mathbf{1}\}$, czyli jednoścu to dokładnie elementy stowarzyszone z jedynką.

Zbiór jedności

KOŁO NAUKOWE

Obserwacja

Zbiór elementów odwracalnych pierścienia R jest grupą względem ich mnożenia.

Obserwacja

Zachodzi $U_R = \{a \in R : a \sim \mathbf{1}\}$, czyli jednoścu to dokładnie elementy stowarzyszone z jedynką.

Twierdzenie

Jeśli a, b są elementami pierścienia R, to

$$a \sim b \Leftrightarrow \exists \varepsilon \in U_R : b = a\varepsilon.$$

Definicja

Niech $a \in R \setminus \{\mathbf{0}\}$. Rozkładem elementu a na czynniki nazywamy każde przedstawienie go w postaci iloczynu $a = a_1 a_2 \dots a_n$.

Definicja

Niech $a \in R \setminus \{\mathbf{0}\}$. Rozkładem elementu a na czynniki nazywamy każde przedstawienie go w postaci iloczynu $a = a_1 a_2 \ldots a_n$.

Definicja

Różny od zera element a pierścienia R nazywamy **rozkładalnym**, jeśli da się go przestawić jako iloczyn a_1, a_2 gdzie a_1 oraz a_2 są elementami nieodwracalnymi.
Jeżeli element nie jest zerem, nie jest jednością oraz nie jest rozkładalny to nazywamy go **nierozkładalnym.**

Definicja

Niech R będzie pierścieniem.

- Pierścień R nazywamy pierścieniem z rozkładem, gdy każdy niezerowy i nieodwracalny element tego pierścienia można przedstawić w postaci iloczynu elementów nierozkładalnych.
- Pierścień R nazywmy **pierścieniem z jednoznacznościa rozkładu** (lub *pierścieniem gaussowskim*, lub *UFD*), gdy każdy niezerowy i nieodwracalny element tego pierścienia można przedstawić w postaci iloczynu elementów nierozkładalnych w sposób jednoznaczny z dokładnością do stowarzyszenia.

Definicja

Niech p będzie elementem pierścienia R. element p nazywamy **pierwszym**, jeżeli zachodzi

$$p \mid ab \Rightarrow p \mid a \vee p \mid b.$$

Definicja

Niech p będzie elementem pierścienia R. element p nazywamy **pierwszym**, jeżeli zachodzi

$$p \mid ab \Rightarrow p \mid a \vee p \mid b.$$

Twierdzenie

Jeżeli p jest eleementem pierwszym pierścienia R to p jest elementem nierozkładalnym.

Elementy pierwsze

Pierścienie z jednoznacznością rozkładu

KOŁO NAUKOWE

Definicja

Niech p będzie elementem pierścienia R. element p nazywamy **pierwszym**, jeżeli zachodzi

$$p \mid ab \Rightarrow p \mid a \vee p \mid b.$$

Twierdzenie

Jeżeli p jest eleementem pierwszym pierścienia R to p jest elementem nierozkładalnym.

Uwaga

Twierdzenie odwrotne nie jest prawdziwe. Element nierozkładalny nie musi być pierwszy.

Twierdzenie

Niech R będzie pierścieniem z rozkładem. Następujące warunki są równoważne

- R jest pierścieniem z jednoznacznością rozkładu,
- Każdy element nierozkładalny w R jest pierwszy.

Twierdzenie

Niech R będzie pierścieniem z jednoznacznością rozkładu. Wtedy $R[x]$ jest pierścieniem z jednoznacznością rozkładu.

Twierdzenie

Niech R będzie pierścieniem z jednoznacznością rozkładu. Wtedy $R[x]$ jest pierścieniem z jednoznacznością rozkładu.

Wniosek

Niech R będzie pierścieniem z jednoznacznościa rozkładu. Wtedy $R[x_1, \dots x_n]$ jest pierścieniem z jednoznacznościa rozkładu.

Niech R będzie pierścieniem z jednoznacznościa rozkładu.

Obserwacja

Niech $\mathcal{P} \subseteq R$ będzie zbiorem reprezentantów klas abstrakcji względem relacji stowarzyszenia wyznaczonych przez elementy nierozkładalne to każdy element $a \in R$ ma jednoznaczne przedstawienie postaci

$$a = \varepsilon \prod_{p \in \mathcal{P}} p^{\alpha_p}$$

gdzie $\varepsilon \in U_R$ oraz $alpha_p \in \mathbb{N} \cup \{0\}$, z tym, że $\alpha_p = 0$ dla prawie wszystkich p. Takie przedstawienie nazywamy **rozkładem kanonicznym**.

Niech R będzie pierścieniem z jednoznacznościa rozkładu oraz $a, b \in R$ będą elementami pierścienia z rozkładami kanonicznymi odpowiednio $\varepsilon_1 \prod_{p\in\mathcal{P}} p^{\alpha_p}$ oraz $\varepsilon_2 \prod_{p\in\mathcal{P}} p^{\beta_p}$.

Twierdzenie

$b \mid a$ wtedy i tylko wtedy, gdy $\beta_p \leqslant \alpha_p$ dla każdego $p \in \mathcal{P}$.

NWD i NWW

Niech R będzie pierścieniem z jednoznacznością rozkładu oraz $a, b \in R$ będą elementami pierścienia z rozkładami kanonicznymi odpowiednio $\varepsilon_1 \prod_{p \in \mathcal{P}} p^{\alpha_p}$ oraz $\varepsilon_2 \prod_{p \in \mathcal{P}} p^{\beta_p}$.

Twierdzenie

$b \mid a$ wtedy i tylko wtedy, gdy $\beta_p \leqslant \alpha_p$ dla każdego $p \in \mathcal{P}$.

Definicja

- **Największym wspólnym dzielnikiem** a, b nazywamy $\mathrm{NWD(a, b)} = \prod_{\mathrm{p} \in \mathcal{P}} \mathrm{p}^{\min\{\alpha_\mathrm{p}, \beta_\mathrm{p}\}}$
- **Najmniejszą wspólną wielokrotnością** a, b nazywamy $\mathrm{NWW(a, b)} = \prod_{\mathrm{p} \in \mathcal{P}} \mathrm{p}^{\max\{\alpha_\mathrm{p}, \beta_\mathrm{p}\}}$

Rozszerzenie definicji

NWD i NWW

KOŁO NAUKOWE

Definicja

Niech *R* będzie pierścieniem z jednoznacznościa rozkładu i $a_1, \ldots a_m$ elementami tego pierścienia. Dla $m > 2$ pojęcie największego wspólnego dzielnika i najmniejszej wspólnej wielokrotności definiujemy rekurencyjnie jako

$$\mathrm{NWD}(a_1, \ldots, a_m) = \mathrm{NWD}(\mathrm{NWD}(a_1, \ldots, a_{m-1}), a_m)$$
$$\mathrm{NWW}(a_1, \ldots, a_m) = \mathrm{NWW}(\mathrm{NWW}(a_1, \ldots, a_{m-1}), a_m)$$

Obserwacja

Dla elementów $a_1, \ldots, a_m$, gdzie a_i ma rozkład kanoniczny $\varepsilon_i \prod_{p \in \mathcal{P}} p^{\alpha_{p_i}}$ zachodzi

$$\mathrm{NWD}(a_1, \ldots, a_m) = \prod_{p \in \mathcal{P}} p^{min\{\alpha_{p_1}, \ldots, \alpha_{p_m}\}}$$

$$\mathrm{NWW}(a_1, \ldots, a_m) = \prod_{p \in \mathcal{P}} p^{max\{\alpha_{p_1}, \ldots, \alpha_{p_m}\}}.$$

Obserwacja

Tak zdefiniowane NWD oraz NWW zależy od wyboru reprezentantów klas abstrakcji elementów nierozkładalnych. Rozważmy dwa różne zbiory tych reprezentantów $\mathcal{P}_1, \mathcal{P}_2 \subseteq R$ oraz elementy pierścienia $a_1, \ldots, a_m$. Zauważmy, że

$$\mathrm{NWD}_{\mathcal{P}_1}(\mathrm{a}_1, \ldots \mathrm{a}_\mathrm{m}) \sim \mathrm{NWD}_{\mathcal{P}_2}(\mathrm{a}_1, \ldots \mathrm{a}_\mathrm{m})$$
$$\mathrm{NWW}_{\mathcal{P}_1}(\mathrm{a}_1, \ldots \mathrm{a}_\mathrm{m}) \sim \mathrm{NWW}_{\mathcal{P}_2}(\mathrm{a}_1, \ldots \mathrm{a}_\mathrm{m}).$$

Z tego powodu można myśleć, że dla danych elementów NWD jest dokładnie jedno oraz NWW jest dokładnie jedno.

Twierdzenie

Niech R będzie pierścieniem z jednoznacznością rozkładu oraz niech $a_1, \ldots a_m$ będą elementami tego pierścienia.
$d = \mathrm{NWD}(\mathrm{a_1}, \ldots, \mathrm{a_m})$ wtedy i tylko wtedy, gdy

- $\forall i = 1, \ldots, m \quad d \mid a_i$,
- $\forall c \in R \quad [(\forall i = 1, \ldots, m \quad c \mid a_i) \Rightarrow c \mid d]$.

Twierdzenie

Niech R będzie pierścieniem z jednoznacznością rozkładu oraz niech $a_1, \ldots a_m$ będą elementami tego pierścienia.
$d = \mathrm{NWD}(a_1, \ldots, a_m)$ wtedy i tylko wtedy, gdy

- $\forall i = 1, \ldots, m \quad d \mid a_i$,
- $\forall c \in R \quad [(\forall i = 1, \ldots, m \quad c \mid a_i) \Rightarrow c \mid d]$.

Twierdzenie

Niech R będzie pierścieniem z jednoznacznością rozkładu oraz niech $a_1, \ldots a_m$ będą elementami tego pierścienia.
$d = \mathrm{NWW}(a_1, \ldots, a_m)$ wtedy i tylko wtedy, gdy

- $\forall i = 1, \ldots, m \quad a_i \mid d$,
- $\forall c \in R \quad [(\forall i = 1, \ldots, m \quad a_i \mid c) \Rightarrow d \mid c]$.

Definicja

Elementy a, b pierścienia z jednoznacznościa rozkładu R, nazywamy **względnie pierwszymi**, jeżeli $\mathrm{NWD}(a, b) = \mathbf{1}$

Twierdzenie

Niech R będzie pierścieniem z jednoznacznością rozkładu oraz $a_1, \ldots, a_m \in R$ elementami tego pierścienia. Zachodzi

- $\langle \mathrm{NWW}(a_1, \ldots, a_m) \rangle = \langle a_1 \rangle \cap \cdots \cap \langle a_m \rangle$
- $\mathrm{NWD}(a_1, a_2) = \dfrac{a_1 a_2}{\mathrm{NWW}(a_1, a_2)}$

Ideał główny

Niech R będzie pierścieniem.

Definicja

Ideał I pierścienia R nazywamy **głównym**, jeśli istnieje taki element $a \in R$, że $I = \langle a \rangle$.

Niech R będzie pierścieniem.

Definicja

Ideał I pierścienia R nazywamy **głównym**, jeśli istnieje taki element $a \in R$, że $I = \langle a \rangle$.

Definicja

R nazywamy **pierścieniem ideałów głównych** (lub *pierścieniem głównym*, lub *PID*), jeżeli każdy ideał tego pierścienia jest główny.

PID, a UFD

Twierdzenie

Niech R będzie pierścieniem ideałów głównych. Wtedy R jest pierścieniem z jednoznacznościa rozkładu.

PID, a UFD

Pierścienie ideałów głównych

Twierdzenie

Niech R będzie pierścieniem ideałów głównych. Wtedy R jest pierścieniem z jednoznacznościa rozkładu.

Twierdzenie

Niech R będzie pierścieniem ideałów głównych oraz $a_1, \ldots, a_m$ elementami tego pierścienia oraz $d = \mathrm{NWD(a_1, \ldots, a_m)}$. Zachodzi

$$\langle a_1, \ldots, a_m \rangle = \langle d \rangle$$

PID, a UFD

Pierścienie ideałów głównych

KOŁO NAUKOWE

Twierdzenie

Niech R będzie pierścieniem ideałów głównych. Wtedy R jest pierścieniem z jednoznacznościa rozkładu.

Twierdzenie

Niech R będzie pierścieniem ideałów głównych oraz $a_1, \ldots, a_m$ elementami tego pierścienia oraz $d = \mathrm{NWD}(\mathrm{a}_1, \ldots, \mathrm{a}_\mathrm{m})$. Zachodzi

$$\langle a_1, \ldots, a_m \rangle = \langle d \rangle$$

Wniosek

Niech $a_1, \ldots a_m$ będą elementami pierścienia ideałów głównych R oraz d największym wspólnym dzielnikiem tych elementów. Istnieją takie $r_1, \ldots r_m \in R$, że $r_1 a_1 + \ldots + r_m a_m = d$.

KOŁO NAUKOWE

Definicja

Pierścień R nazywamy **pierścieniem euklidesowym**, jeśli określona jest funkcja $N : R \setminus \{\mathbf{0}\} \to \mathbb{N} \cup \{0\}$ zwaną normą, gdzie zachodzi

$$\forall a, b \in R, b \neq \mathbf{0} \; \exists q, r \in R : [(a = bq + r) \wedge (N(r) < N(b) \vee r = \mathbf{0})].$$

element r w powyższym wzorze nazywamy *resztą*.

Twierdzenie

Niech R będzie pierścieniem euklidesowym. Wtedy R jest też pierścieniem ideałów głównych.

Uwaga

Twierdzenie odwrotne nie zachodzi. Np. $\mathbb{Z}[\frac{1}{2}(1+\sqrt{-19})]$ jest pierścieniem ideałów głównych, natomiast nie jest pierścieniem euklidesowym. Dowód można zobaczyć pod tym **linkiem**

Przykłady

Przykład

Pierścieniami euklidesowymi są np.

- $\mathbb{Z}$ z norma zadaną przez $N(a) = |a|$,
- $K[x]$, gdzie K jest ciałem, a norma jest zadana przez $N(f) = deg(f)$,
- $\mathbb{Z}[\sqrt{-1}]$ z normą zadaną przez $N(a + bi) = a^2 + b^2$.

Źródła

Paweł Gładki, Uniwersytet Śląski - Podstawowe pojęcia teorii podzielności. Pierścienie z jednoznacznym rozkładem

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

[2] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra 1*. Springer, 2000.

Pytania, wątpliwości, uwagi ?