Дільники нуля та одиниці

Євгенія Кочубінська

Київський національний університет імені Тараса Шевченка

15 лютого 2023

FACULTY OF MECHANICS AND MATHEMATICS

Дільники нуля

Нехай R — нетривіальне кільце з одиницею.

Означення

Ненульовий елемент $a \in R$ називається *правим дільником нуля*, якщо для нього існує такий ненульовий елемент $b \in R$, що $ba = 0$.

Означення

Ненульовий елемент $a \in R$ називається *лівим дільником нуля* , якщо для нього існує такий ненульовий елемент $b \in R$, що $ab = 0$.

Дільники одиниці

Означення

Ненульовий елемент $a \in R$ називається *правим дільником одиниці*, якщо для нього існує такий ненульовий елемент $b \in R$, що $ba = 1$.

Означення

Ненульовий елемент $a \in R$ називається *лівим дільником одиниці*, якщо для нього існує такий ненульовий елемент $b \in R$, що $ab = 1$.

Означення

Елемент називається *дільником одиниці*, або *оборотним*, якщо він є і лівим, і правим дільником одиниці.

Приклади: дільники нуля та одиниці в $\mathbb{Z}$ та $\mathbb{Z}_n$

Приклад

1. В $\mathbb{Z}_{12}$ дільниками нуля є $\overline{2}, \overline{3}, \overline{4}, \overline{6}, \overline{8}, \overline{9}, \overline{10}$; дільниками одиниці є $\overline{1}, \overline{5}, \overline{7}, \overline{11}$.
2. В $\mathbb{Z}$ дільників нуля немає, дільники одиниці ± 1.

Приклади: дільники нуля та одиниці в $\mathbb{Z}_n$

Твердження

У кільці $\mathbb{Z}_n$ ненульовий елемент a є дільником нуля $\Leftrightarrow (a, n) \neq 1$.

Доведення.

$(\Rightarrow)$ a — дільник нуля $\Rightarrow \exists b \in \mathbb{Z}_n, b \neq 0 : ab = 0 \Rightarrow n \,|\, ab$.
Позначимо $d_1 = (a, n)$, $d_2 = (b, n)$: $a = a_1 d_1$, $b = b_1 d_2$, $(a_1, n) = 1$, $(b_1, n) = 1$
$\Rightarrow ab = a_1 d_1 b_1 d_2$ та $(a_1 b_1, n) = 1 \Rightarrow n \,|\, d_1 d_2$. Оскільки $d_2 \leq b < n$, то $d_1 > 1$.
$(\Leftarrow)$ $(a, n) = d > 1$. Покладемо $b = \frac{n}{d} \neq 0$: $ab = 0$. □

Приклади: дільники нуля та одиниці в $\mathbb{Z}_n$

Твердження

У кільці $\mathbb{Z}_n$ ненульовий елемент a є дільником одиниці $\Leftrightarrow (a, n) = 1$.

Доведення.

1. $(\Rightarrow)$ a — дільник одиниці $\Rightarrow \exists b \in \mathbb{Z}_n, b \neq 0 : ab = 1$.
   Якщо $d = (a, n)$, то $d \,|\, (ab - 1)$, а тому $d = 1$.
   $(\Leftarrow)$ $(a, n) = 1 \Rightarrow \exists x, y \in \mathbb{Z} : ax + ny = 1 \Rightarrow ax = 1$ в $\mathbb{Z}_n$.

$\square$

Приклади: дільники нуля та одиниці в $\mathbb{Z}_n$

Твердження

Кожний ненульовий елемент кільця $\mathbb{Z}_n$ є або дільником нуля, або дільником одиниці.

Приклади: дільники нуля та одиниці в $M_n(R)$

Приклад

Матриці $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ та $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ є дільниками нуля, бо $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Матриця $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ є дільником одиниці.

Твердження

В кільці $M_n(R)$ дільниками нуля є вироджені матриці, дільниками одиниці невироджені матриці.

Мультиплікативна група кільця

Твердження

Позначимо через R^* множину всіх оборотних елементів кільця з одиницею R. Множина R^* є групою відносно множення.

Доведення.

$R \neq \varnothing$, бо $1 \in R^*$.
Нехай $a, b \in R^*$:

$$abb^{-1}a^{-1} = 1 \Rightarrow (ab)^{-1} = b^{-1}a^{-1} \quad \Rightarrow \quad ab \in R^*$$

$$\Rightarrow R^* \text{— група.}$$

$$aa^{-1} = a^{-1}a = 1 \quad \Rightarrow \quad a^{-1} \in R^*$$

□

Мультиплікативна група кільця

Означення

Група R^* називається *мультиплікативною* групою кільця R.

Приклади

Приклад

1. $\mathbb{Z}^* = \{1, -1\} \simeq C_2$.
2. $\mathbb{Z}_n^* = \{\overline{a} \in \mathbb{Z}_n \,|\, (a, n) = 1\}$, $\left|\mathbb{Z}_n^*\right| = \varphi(n)$.
3. Нехай $\Bbbk$ — поле. $\left(M_n(\Bbbk)\right)^* = GL_n(\Bbbk)$.

Твердження

1. Правий (лівий) дільник одиниці не може бути лівим (правим) дільником нуля.
2. Правий (лівий) дільник нуля не може бути лівим (правим) дільником одиниці.

Доведення.

1. Нехай a — правий дільник одиниці $\Rightarrow \exists b \in R,\ b \neq 0\colon ba = 1$.
   Припустимо, що $ac = 0$ ($a \neq 0$, $c \neq 0$). Тоді

$$bac = \begin{cases} = (ba)c = c \\ = b(ac) = 0 \end{cases} \Rightarrow c = 0 \quad ↯↯↯$$

2. Нехай a — правий дільник нуля $\Rightarrow \exists b \in R\colon ba = 0$.
   Припустимо, що $ac = 1$. Тоді

$$bac = \begin{cases} = (ba)c = 0 \\ = b(ac) = b \end{cases} \Rightarrow b = 0 \quad ↯↯↯$$

Нільпотентні елементи

Означення

Елемент $a \in R$ називається *нільпотентним*, якщо $a^m = 0$ для деякого $m \in \mathbb{N}$.
Найменше таке m називається *класом нільпотентності*.

Приклад

1. Нільпотентні елементи кільця $\mathbb{Z}_{12}$: $\overline{0}$ та $\overline{6}$.
2. Нільпотентні елементи в кільці $M_n(k)$: матриці, всі власні числа яких дорівнюють нулю.

Нільпотентні елементи в $\mathbb{Z}_n$

Твердження

Елемент $a \in \mathbb{Z}_n$ є нільпотентним $\Leftrightarrow$ a ділиться на кожний простий дільник числа n.

Доведення.

Нехай $n = p_1^{k_1} \dots p_s^{k_s}$ — канонічний розклад числа n.

($\Rightarrow$) $a \in \mathbb{Z}_n$ — нільпотентний $\Rightarrow$ $\exists k \in \mathbb{N}$: $n \mid a^k$.

Тоді

$$n \mid a^k \Rightarrow p_i \mid a^k \ (i = 1, \dots, s) \Rightarrow p_i \mid a \ (i = 1, \dots, s) \Rightarrow p_1 \dots p_s \mid a.$$

($\Leftarrow$) Нехай $p_i \mid a$, $i = 1, \dots, s$. Покладемо $k = \max\{k_1, \dots, k_s\}$.

Тоді $n \mid a^k \Rightarrow a$ — нільпотентний. □