Поняття кільця та підкільця

Євгенія Кочубінська

Київський національний університет імені Тараса Шевченка

15 лютого 2023

Кільце

Означення

Кільцем називається непорожня множина R, на якій задано дві бінарні операції,

$$+, \cdot : R \times R \to R,$$

які називаються *додаванням* та *множенням* відповідно, і які задовольняють умови:

1. $(R, +)$ є абелевою групою (яка називається *адитивною групою* кільця);
2. множення є асоціативним;
3. додавання та множенням пов'язані *дистрибутивними законами*:
   - $a \cdot (b + c) = a \cdot b + a \cdot c$ для довільних $a, b, c \in R$;
   - $(a + b) \cdot c = a \cdot c + b \cdot c$ для довільних $a, b, c \in R$.

Нейтральний елемент для додавання називається *нулем* і позначається 0.

Кільця

Кільце R називається

- *комутативним*, якщо множення є комутативним;
- *кільцем з одиницею*, якщо існує нейтральний елемент для множення, який називається *одиницею* і позначається 1, тобто елемент $1 \in R$ з властивістю $1 \cdot a = a \cdot 1 = a$ для всіх $a \in R$;
- *кільцем з діленням*, або *тілом*, якщо $1 \neq 0$ і $(R \setminus \{0\}, \cdot)$ — група;
- *полем*, якщо $(R \setminus \{0\}, \cdot)$ — комутативна група.

Приклади кілець

1. Множина $\mathbb{Z}$ цілих чисел є комутативним кільцем з одиницею відносно звичайних операцій додавання і множення.
2. Множина $2\mathbb{Z}$ парних цілих чисел є комутативним кільцем (без одиниці) відносно звичайних операцій додавання і множення.
3. Довільне поле є кільцем: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
4. Множина $\mathbb{Z}_n$ лишків за модулем n є комутативним кільцем з одиницею відносно додавання і множення за модулем натурального числа n. Це кільце називається *кільцем лишків*.

Приклади кілець

5. Множина комплексних чисел вигляду

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

є комутативним кільцем з одиницею, яке називається *кільцем цілих гаусових чисел*. Очевидно, $\mathbb{Z}[i]$ є підкільцем $\mathbb{C}$.

6. Нехай $d \in \mathbb{Z}$ — вільне від квадратів число. Множина

$$\mathbb{Z}[\sqrt{d}] = \left\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\right\}$$

є комутативним кільцем з одиницею відносно звичайних операцій додавання і множення. Кільця такого вигляду називаються *квадратичними кільцями*.

Приклади кілець

7. *Матричні кільця.* Множина $M_n(R)$ квадратних матриць порядку n над кільцем R є некомутативним кільцем з одиницею відносно операцій матричних додавання і множення.
8. *Кільце функцій.* Нехай $A \subset \mathbb{R}$. Множина $\mathbb{R}^A$ всіх функцій $f : A \to \mathbb{R}$ є кільцем відносно операцій $f + g$ та fg, визначених рівностями

$$(f + g)(x) = f(x) + g(x)$$

та

$$(fg)(x) = f(x)g(x)$$

для всіх $x \in A$.

Приклади кілець

9. *Кільце многочленів.* Нехай $R[x]$ — множина многочленів від змінної x з коефіцієнтами з поля R.
Сума і добуток многочленів $f(x) = \sum_{i=0}^{n} a_i x^i$ і $g(x) = \sum_{i=0}^{m} b_i x^i$ ($n \geq m$) визначається як

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i,$$

$$f(x)g(x) = \sum_{i=0}^{n+m} \left(\sum_{i+j=k} a_i b_j \right) x^k.$$

Відносно так введених операцій множина $R[x]$ є кільцем.

Прямий добуток кілець

Прямим добутком кілець R та S називається множина

$$R \times S = \{(r, s) \mid r \in R,\ s \in S\}$$

з покомпонентними операціями додавання і множення:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2),$$

$$(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2),$$

де $r_1, r_2 \in R$, $s_1, s_2 \in S$. Легко перевірити, що прямий добуток кілець є кільцем .

Найпростіші властивості кілець

R — кільце.

1. Для довільного $a \in R$
$$a \cdot 0 = 0 \cdot a = 0.$$

♣ $a \cdot 0 = b \Rightarrow$

$$b + b = a \cdot 0 + a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 = b \ \Rightarrow \ b = b + (-b) = 0.$$

Аналогічно доводиться, що $0 \cdot a = 0$. ♠

2. Для довільних $a, b \in R$
$$(-a) \cdot b = a \cdot (-b) = -ab.$$

♣ $ab + a(-b) = a(b + (-b)) = a(b - b) = a \cdot 0 = 0 \Rightarrow a(-b) = -ab$. ♠

3. Для довільних $a, b \in R$
$$(-a) \cdot (-b) = ab.$$

Найпростіші властивості кілець

4. Якщо R — кільце з одиницею, то вона єдина та

$$(-1)\,a = a\,(-1) = -a.$$

♣ Якщо 1 та $1'$ — дві одиниці кільця R, то $1 = 1 \cdot 1' = 1'$. ♠

5. Кільце R з одиницею — тривіальне, тоді і лише тоді, коли $1 = 0$.
♣ ($\Rightarrow$) R — тривіальне $\Rightarrow 1 = 0$.
($\Leftarrow$) Нехай $1 = 0$. Візьмемо довільний $a \in R$. Тоді $a = a \cdot 1 = a \cdot 0 = 0$. ♠

Отже, якщо кільце містить більше одного елемента, то в ньому $1 \neq 0$.

Найпростіші властивості кілець

Зауваження

В кожному кільці R завжди визначена і операція віднімання: $a - b = a + (-b)$.

6. Для довільних $a, b, c \in R$:
   - $a(b - c) = ab - ac$,
   - $(a - b)c = ac - bc$.

   ♣ $a(b - c) + ac = a(b - c + c) = ab$. ♠

Підкільце

Означення

Непорожня підмножина S кільця R називається *підкільцем* кільця R, якщо S є кільцем відносно тих самих бінарних операцій, що задані на кільці R.

Твердження (Критерій підкільця)

Нехай S — непорожня підмножина кільця R. Наступні умови рівносильні:

1. S є підкільцем R;
2. $(S, +)$ є підгрупою $(R, +)$ і S замкнена відносно множення;
3. $a - b, ab \in S$ для всіх $a, b \in S$.