Гомоморфізми та факторкільця

Євгенія Кочубінська

Київський національний університет імені Тараса Шевченка

1 березня 2023

Факторкільце

Нехай R — кільце, I — ідеал кільця R.

На факторгрупі

$$R/I = \{a + I \mid a \in R\}$$

можна визначити операцію множення

$$(a + I)(b + I) = ab + I.$$

Оскільки в R множення асоціативне, то в R/I також.

Ця операція дистрибутивна відносно додавання.

Отже, $\langle R/I, +, \cdot \rangle$ — кільце, яке називається *факторкільцем* кільця R за ідеалом I.

Позначається R/I.

Факторкільце: резюме

Нехай R — кільце, I — ідеал кільця R.

Множина: $R/I = \{a + I \mid a \in R\}$.

Дії:

- Додавання: $(a + I) + (b + I) = a + b + I$.
- Множення: $(a + I)(b + I) = ab + I$.

Нулем є $0 + I$.

Якщо R — кільце з одиницею, то R/I — теж кільце з одиницею, одиницею є $1 + I$.

Факторкільце: приклад 1

$$R = \mathbb{Z}, \quad I = 6\mathbb{Z}$$

$$\mathbb{Z}/6\mathbb{Z} = \{6\mathbb{Z}, 1 + 6\mathbb{Z}, 2 + 6\mathbb{Z}, 3 + 6\mathbb{Z}, 4 + 6\mathbb{Z}, 5 + 6\mathbb{Z}\}$$

$$(2 + 6\mathbb{Z}) + (3 + 6\mathbb{Z}) = 5 + 6\mathbb{Z}$$

$$(2 + 6\mathbb{Z})(3 + 6\mathbb{Z}) = 6 + 6\mathbb{Z} = 6\mathbb{Z}$$

Факторкільце: приклад 2

$$R = \mathbb{R}[x], \quad I = (x^2+1) = \{(x^2+1)g(x) \mid g(x) \in \mathbb{R}[x]\}$$

Елементи цього факторкільця мають вигляд $h(x) + I$.

Які елементи є різними?

$h_1(x) + I, h_2(x) + I \in R/I$:

$$h_1(x) + I = h_2(x) + I \Leftrightarrow h_1(x) - h_2(x) \in I \Leftrightarrow (x^2+1) \mid \big(h_1(x) - h_2(x)\big).$$

Розділимо з остачею на (x^2+1):

$$h_1(x) = (x^2+1)q_1(x) + r_1(x), \quad h_2(x) = (x^2+1)q_2(x) + r_2(x).$$

Тому

$$(x^2+1) \mid \big(h_1(x) - h_2(x)\big) \Leftrightarrow r_1(x) = r_2(x).$$

Отже,

$$h_1(x) + I = h_2(x) + I \Leftrightarrow h_1(x) = h_2(x) \pmod{x^2+1}.$$

$$\mathbb{R}[x]/(x^2+1) = \{ax + b + (x^2+1) \mid a, b \in \mathbb{R}\}.$$

Факторкільце: приклад 2

$$\mathbb{R}[x]/(x^2+1) = \left\{ax + b + (x^2+1) \,|\, a, b \in \mathbb{R}\right\}.$$

$$2x + 1 + (x^2+1),\, 3x + 2 + (x^2+1) \in \mathbb{R}[x]/(x^2+1):$$

$$\big(2x + 1 + (x^2+1)\big) + \big(3x + 2 + (x^2+1)\big) = 5x + 3 + (x^2+1);$$

$$\big(2x + 1 + (x^2+1)\big) \cdot \big(3x + 2 + (x^2+1)\big) = 6x^2 + 7x + 2 + (x^2+1) = x + 2 + (x^2+1).$$

Гомоморфізм кілець

Означення

Нехай R_1, R_2 — кільця.
Відображення $f : R_1 \to R_2$ називається гомоморфізмом кілець, якщо

1. $f(x+y) = f(x) + f(y)$ для всіх $x, y \in R_1$;
2. $f(xy) = f(x)f(y)$ для всіх $x, y \in R_1$.

Приклади

1. $f : \mathbb{R}[x] \to \mathbb{C}: \quad g(x) \mapsto g(i)$.
2. $f : \mathbb{Z} \to \mathbb{Z}_n: \quad z \mapsto z \pmod n$.

Ядро та образ

Означення

Нехай $f : R_1 \to R_2$ — гомоморфізм кілець R_1 та R_2.
Множина

$$\operatorname{Ker} f = \{x \in R_1 \,|\, f(x) = 0_{R_2}\}$$

називається *ядром гомоморфізму* f.

Ядро та образ

Твердження

Нехай $f : R_1 \to R_2$ — гомоморфізм кілець R_1 та R_2.
Тоді $\operatorname{Ker} f$ є ідеалом кільця R_1.

Доведення.

Очевидно $\operatorname{Ker} f \lhd R_1$.
Нехай $x \in \operatorname{Ker} f$, $y \in R_1$.
Тоді

$$f(xy) = f(x)f(y) = 0, \quad f(yx) = f(y)f(x) = 0$$

$\Rightarrow xy \in \operatorname{Ker} f$ та $yx \in \operatorname{Ker} f$
$\Rightarrow \operatorname{Ker} f$ — ідеал. $\square$

Ядро та образ

Означення

Нехай $f : R_1 \to R_2$ — гомоморфізм кілець R_1 та R_2.
Множина
$$\operatorname{Im} f = \{f(x) \,|\, x \in R_1\}$$
називається *образом гомоморфізму* f.

Ядро та образ

Твердження

Нехай $f : R_1 \to R_2$ — гомоморфізм кілець R_1 та R_2.
Тоді $\operatorname{Im} f$ є підкільцем кільця R_2.

Доведення.

Нехай $x', y' \in \operatorname{Im} f \Rightarrow \exists\, x, y \in R_1 : f(x) = x', f(y) = y'$.
Тоді $x'y' = f(x)f(y) = f(xy) \Rightarrow x'y' \in \operatorname{Im} f$.
Решта аксіом очевидні. $\square$

Теореми про гомоморфізм для кілець

Нехай I — ідеал кільця R.

З теорії груп відомо, що відображення

$$\pi : R \to R/I : \quad a \mapsto a + I$$

є епіморфізмом адитивних груп.

Покажемо, що π зберігає множення:

$$\pi(ab) = ab + I = (a + I)(b + I) = \pi(a)\pi(b).$$

Отже, π є епіморфізмом кілець, який називається *канонічним* епіморфізмом кільця R на факторкільце R/I, або *канонічною проекцією* R на R/I.

Очевидно, що $\operatorname{Ker} \pi = I$.

Основна теорема про гомоморфізм для кілець

Теорема

Нехай $f : R_1 \to R_2$ — гомоморфізм кілець. Тоді

$$R_1/\operatorname{Ker} f \simeq \operatorname{Im} f.$$

Більш точно, існує ізоморфізм

$$\varphi : \operatorname{Im} f \to R_1/\operatorname{Ker} f : \quad b = f(a) \mapsto \pi(a) = a + \operatorname{Ker} f.$$

Доведення.

За теоремою (про гомоморфізм для груп) відображення φ є ізоморфізмом адитивних груп.
Перевіримо, що воно зберігає множення.
Нехай $f(x) = u$, $f(y) = v$.
Тоді $f(xy) = uv$ та

$$\varphi(uv) = \pi(xy) = \pi(x)\pi(y) = \varphi(u)\varphi(v). \quad \square$$

Приклади

1. Нехай P — поле, $c \in P$ — фіксований елемент. Відображення
$$f : P[x] \to P : \quad g(x) \mapsto g(c)$$
є гомоморфізмом кілець.
За теоремою Безу його ядром є всі многочлени, які діляться на $x - c$. Отже,
$$P[x]/(x-c)P[x] \simeq P.$$

2. Нехай $t^2 + pt + q \in \mathbb{R}[t]$, $p^2 - 4q < 0$, $c \in \mathbb{C}$ — один з його уявних коренів. Відображення
$$f : \mathbb{R}[t] \to \mathbb{C} : \quad g \mapsto g(c)$$
є гомоморфізмом кілець.
Для нього $\operatorname{Im} f = \mathbb{C}$, $\operatorname{Ker} f = \left\{ \underbrace{(t-c)(t-\overline{c})}_{=t^2+pt+q} g(t) \mid g(t) \in \mathbb{R}[t] \right\}$.
Отже,
$$\mathbb{R}[t]/(t^2 + pt + q)\mathbb{R}[t] \simeq \mathbb{C}.$$

Друга теорема про гомоморфізм

Теорема

Нехай A — підкільце і I — ідеал кільця R. Тоді $A+I$ є підкільцем R, $A\cap I$ є ідеалом A і

$$(A+I)/I \simeq A/(A\cap I).$$

Третя теорема про гомоморфізм

Теорема

Нехай I та J — ідеали кільця R і $J \subseteq I$. Тоді I/J є ідеалом кільця R/J і

$$(R/J)/(I/J) \simeq R/I.$$

Теорема про відповідність для кілець

Теорема

Нехай I — ідеал R. Відображення

$$A \longleftrightarrow A/I$$

встановлює взаємно однозначну відповідність між множиною підкілець A з R, які містять I, і множиною підкілець в R/I.
Причому, A є ідеалом кільця R тоді і тільки тоді, коли A/I є ідеалом факторкільця R/I.