

Лекція 17. Кільця та поля.

Визначення кілець та полів

Нехай K – непорожня множина, на якій задані дві бінарні алгебраїчні операції $+$ (додавання) і \cdot (множення), які задовольняють наступним умовам:

(K1) $(K, +)$ – абелева група;

(K2) (K, \cdot) – півгрупа;

(K3) операція множення дистрибутивна зліва та справа відносно операції додавання, тобто

$$(x + y) \cdot z = x \cdot z + y \cdot z$$

та

$$z \cdot (x + y) = z \cdot x + z \cdot y$$

для всіх $x, y, z \in K$.

Тоді $(K, +, \cdot)$ називається кільцем.

Алгебраїчна структура $(K, +)$ називається адитивною групою кільця, а (K, \cdot) – його мультиплікативною півгрупою.

Якщо (K, \cdot) – півгрупа з одиницею, то кажуть, що $(K, +)$ – кільце з одиницею. Кільце називається комутативним, якщо (K, \cdot) – абелева півгрупа (на відміну від груп, комутативне кільце не прийнято називати абелевим). Нейтральний елемент 0 – відносно додавання і 1 – відносно множення (якщо він існує) називають відповідно нулем і одиницею кільця.

Далі наведено приклади кілець:

1) множина $(\mathbf{Z}, +, \cdot)$ цілих чисел відносно звичайних операцій додавання й множення;

2) множина $(\mathbf{Q}, +, \cdot)$ раціональних чисел відносно звичайних операцій додавання й множення;

3) множина $(\mathbf{R}, +, \cdot)$ дійсних чисел відносно звичайних операцій додавання й множення;

4) множина $(\mathbf{C}, +, \cdot)$ комплексних чисел відносно звичайних операцій додавання й множення;

5) множина дійснозначних матриць $M_n(\mathbf{R})$ розміру $n \times n$ відносно додавання та множення матриць є кільцем з одиницею. Роль двостороннього нейтрального елемента відносно множення тут відіграє одинична матриця. Таке кільце називається повним матричним кільцем над \mathbf{R} або кільцем

квадратних матриць порядку n над R . Це один з найважливіших прикладів кілець. Оскільки при $n > 1$, множення матриць є не комутативною операцією, то $M_n(\mathbf{R})$ – некомутативне кільце.

Підмножина L кільця K називається підкілцем, якщо для будь-яких елементів $x, y \in L$ виконуються умови $x + y \in L$, $-y \in L$ та $x \cdot y \in L$.

Підкілце L кільця K з одиницею називається ідеалом, коли для будь-яких елементів $x \in L$ та $a \in K$ виконується $a \cdot x \in L$ і $x \cdot a \in L$.

Нехай K – кільце з одиницею, а L – ідеал у цьому кільці. Фактор-групу K/L адитивної групи $(K, +)$ кільця за ідеалом L (який є нормальною підгрупою у вказаній адитивній групі) можна перетворити в кільце, наступним чином задаючи операцію множення суміжних класів: $(x + L) \cdot (y + L) = x \cdot y + L$. Це кільце називається фактор-кілцем кільця K за ідеалом L і його прийнято позначати K/L .

Нижче наведено приклад фактор-кілця, який широко зустрічається. Множина $n\mathbf{Z}$ цілих чисел, кратних деякому фіксованому натуральному числу n , є ідеалом в кільці цілих чисел \mathbf{Z} . Розглянуту раніше фактор-групу $\mathbf{Z}/n\mathbf{Z} = \mathbf{Z}_n$ можна перетворити в кільце, задаючи операцію множення \otimes класів за модулем числа n . Щоб перемножити два класи \bar{r} і \bar{s} потрібно спочатку перемножити цілі числа r і s , а потім знайти остачу від ділення знайденого добутку на число n . Клас знайденої остачі й буде результатом множення класів \bar{r} і \bar{s} . Множина \mathbf{Z}_n разом із заданими на ній операціями додавання \oplus та множення \otimes є комутативним кілцем з одиницею, яке має n елементів.

У табл. 19 наведено таблицю Келі для операції множення \otimes кільця \mathbf{Z}_5 .

Табл. 19. Таблиця Келі для операції множення кільця \mathbf{Z}_5 .

\otimes	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Відображення $f: K_1 \rightarrow K_2$ кільця $(K_1, +, \cdot)$ в кільце (K_2, \oplus, \otimes) називається гомоморфізмом, якщо воно узгоджує обидві операції, тобто коли для будь-яких елементів $x, y \in K_1$

$$f(x + y) = f(x) \oplus f(y),$$

$$f(x \cdot y) = f(x) \otimes f(y).$$

Якщо гомоморфізм кілець є ін'єктивним відображенням, то його називають мономорфізмом кілець. Якщо гомоморфізм кілець є сюр'єктивним відображенням, то його називають епіморфізмом кілець. Якщо гомоморфізм кілець є бієктивним відображенням, то його називають ізоморфізмом кілець. Два кільця K_1 і K_2 називаються ізоморфними, якщо існує ізоморфізм кільця K_1 в кільце K_2 ; факт ізоморфізму кілець прийнято коротко записувати у вигляді $K_1 \cong K_2$.

Поле P – це комутативне кільце з одиницею, в якому кожен відмінний від нуля елемент має обернений відносно операції множення. Іншими словами, комутативне кільце з одиницею P є полем, коли сукупність його відмінних від нуля елементів утворює абелеву групу відносно операції множення.

Два поля P_1 і P_2 називаються ізоморфними, якщо вони ізоморфні як кільця.

Далі наведено приклади полів:

1) множина $(\mathbf{Q}, +, \cdot)$ раціональних чисел відносно звичайних операцій додавання й множення;

2) множина $(\mathbf{R}, +, \cdot)$ дійсних чисел відносно звичайних операцій додавання й множення;

3) множина $(\mathbf{C}, +, \cdot)$ комплексних чисел відносно звичайних операцій додавання й множення.

Слід зауважити, що множина $(\mathbf{Z}, +, \cdot)$ цілих чисел відносно звичайних операцій додавання й множення не є полем. Дійсно, всі цілі числа, крім 1 та -1, не мають обернених відносно операції множення.