Тема 4. АЛГЕБРАЇЧНІ СТРУКТУРИ

Лекція 4.3. Кільця і поля

План лекції

1. Подібність алгебраїчних систем.
2. Кільця та ідеали кілець.
3. Поля Галуа.

Література. *1. Конспект лекцій.*
2. Балога С.І. Дискретна математика. *Навчальний посібник. – Ужгород: ПП «АУТДОР-. ШАРК», 2021. – 124 с.*
3. Акимов О.Е. Дискретная математика. Логика. Группы. Графы. Фракталы. – М.: АКИМОВА, 2005. – 656 с.

1. Подібність алгебраїчних систем

Під час розгляду прикладів груп була помітна схожість групи залишків за модулем та групи коренів рівняння $x^n = 1$ або групи двійкових чисел з операцією XOR та групи багаточленів над GF(2).

Цілком доречне питання – за яких умов подібність є достатньою підставою для поширення результатів вивчення однієї алгебраїчної системи на іншу і коли таке можливі також у зворотному напрямку.

Якщо у двох алгебраїчних систем

$$K = (A, \varphi_1, \varphi_2, ..., \varphi_p) \quad та \quad M = (B, \psi_1, \psi_2, ..., \psi_p)$$

кількість операцій та арність для кожної пари φ_i та ψ_i однакова, існує відображення Г множини А на множину В (Г:А $\rightarrow$ В) таке, що

$$\Gamma(\varphi_n(a_1, a_2, \ldots, a_f)) = \psi_n(\Gamma(a_1, a_2, \ldots, a_f)),$$

тобто, результат операції на образами елементів першої системи у другій системі має збігатись з образі у другій системі результату операції над елементами в першій системі, то маємо ступінь подібності з назвою **гомоморфізм К** на М.

Цю тезу для бінарної операції, пояснює рис. 1.

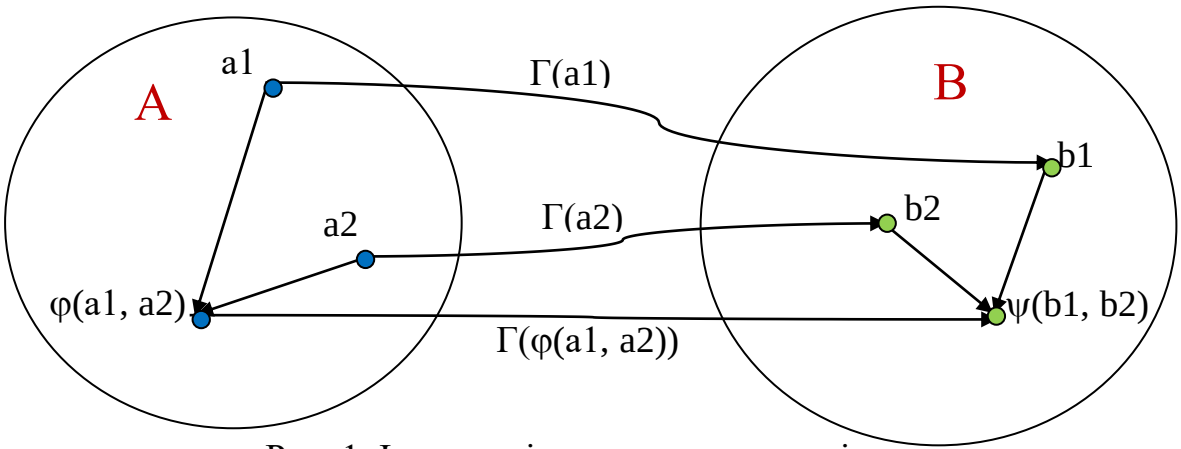

Рис. 1. Ілюстрація до умов наявності
гомоморфізма алгебраїчної системи К на систему М

Якщо водночас існує гомоморфізм К на М та гомоморфізм М на К, то такий ступінь подібності має назву **ізоморфізм.** Якщо використовується відображення множини на її підмножину то ступінь подібності має назву **автоморфізм.**

Приклади

Приклад **гомоморфізму** групи Z_6 та підгрупи групи коренів рівняння $x^6 = 1$. Маємо алгебраїчні системи:

$Z_6 = (A, \oplus_6)$ $A = \{0, 1, 2, 3, 4, 5)$ та $K = (B, \cdot)$, $B = \left\{1, e^{j\frac{2\pi}{6}3}\right\}$

відображення множини А на множину В подане, за допомогою двочасткового графа нижче (рис. 7-2).

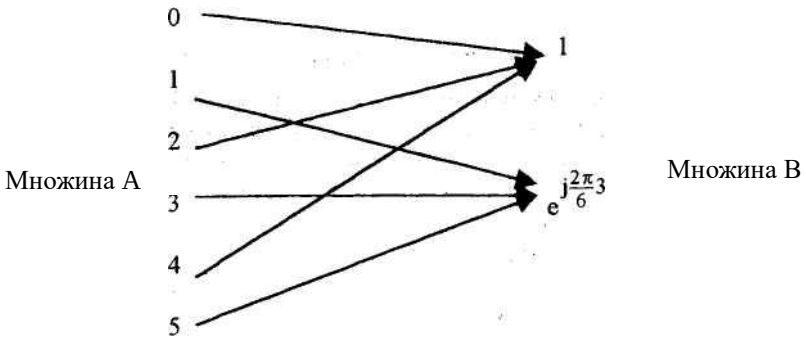

Рис. 2. Відображення А $\rightarrow$ В

Перевірка відповідності операндів та операцій полягає у наступному:

1) нейтральний елемент Z_6 відображено у нейтральний елемент К;

2) операція між будь-яким елементом та нейтральним у Z_6 дає у результаті вихідний елемент і це ж відбувається з їх образами у К, бо множення на 1 залишає результат $e^{j\frac{2\pi}{6}3}$;

3) операція між будь-якими двома елементами у Z_6 та її результат чітко відповідають операціям над образами елементів і образ результату, який одержано у Z_6, завжди дорівнює результату операції над образами операндів у системі К.

Приклад **ізоморфізму** між півгрупою додатних дійсних чисел та півгрупою дійсних чисел. Маємо системи:

A = (R+, ·) та B = (R,+)

R+ – множина додатних дійсних чисел

R – множина дійсних чисел

У цих систем кількість та арність операцій однакова.

Результати відображення:

множини R+ $\rightarrow$ R, якщо x $\in$ R+, дістають за виразом y = lgx;

множини R$\rightarrow$ R+ – за виразом $x = 10^y$.

Відповідність операндів та результатів відома, бо то є підстава для використання звичайних десяткових логарифмів, які добре полегшують виконання операцій множення та піднесення до степені.

Приклад **автоморфізму** групи трирозрядних двійкових чисел з операцією XOR G = (C, XOR), C = (000, 001,011, 010,100,101,110, 111) на підгрупу G1 = (D, XOR), D = {000, l 11}.

Зрозуміло, що кількість і арність операцій у групи та підгрупи не можуть бути різними. Відображення множини C на множину D можливе за таким правилом: якщо елемент у складі множини C має у молодшому розряді одиницю, то образ цього елемента у множині D1 є 111, інакше образ елемента є 000. Перевірки (невичерпні) не суперечать наявності автоморфізму:

011 → 111	011 → 111	101 → 111
XOR	XOR	XOR
100 → 000	010 → 000	111 → 111
– –	– –	– –
111 → 111	001 → 111	010 → 000

Взаємно-однозначна відповідність простору функцій на інтервалі аргументів та простору багатовимірних векторів була основою для побудови функціонального аналізу (розділ математики)

2. Кільця та ідеали кілець

Def. Кільце $\mathfrak{R} = (\mathbf{M}, +, \times)$ - це множина з двома бінарними операціями (+) и (×) **,** такими, що

1. **M** – абелева група відносно складання (+).

2. Операція (×) замкнута та асоціативна: для всіх $a, b, c \in \mathbf{M}$, $a \times (b \times c) = (a \times b) \times c$.

3. . Виконуються закони дистрибутивності: для всіх $a, b, c \in \mathbf{M}$, $a \times (b + c) = a \times b + a \times c$, $(b + c) \times a = b \times a + c \times a$.

Це алгебраїчні системи з двома визначальними операціями. Першу з цих операцій умовно звуть складанням або адитивною операцією, другу – мультиплікативною операцією або множенням.

Щоб алгебраїчна система була кільцем потрібно виконання таких вимог:

1) множина та операція складання мають створювати комутативну групу (операція має бути ще й комутативна);
2) замкненість множини відносно множення;
3) асоціативність множення
4) дистрибутивність множення відносно складання.

Якщо алгебраїчна система відповідає цим вимогам, то вона має назву – асоціативне кільце. Додатково

– якщо операція множення комутативна, то алгебраїчна система має назву комутативне кільце;

– якщо у множині є нейтральний елемент за множенням, то система має назву – кільце з одиницею;

– у кільці з одиницею є мультиплікативна група;

– якщо для елементів множини А можливо $a_i \cdot a_j = 0$, то система має назву – кільце з дільниками нуля, а ці елементи є дільники нуля.

Приклад: $R = (A, \oplus_6, \otimes_6)$, A = {0, 1, 2, 3, 4, 5), операція множення за модулем 6 виконується аналогічно додаванню за модулем, тобто, після звичайного множення знаходять залишок від ділення результату звичайного множення на 6. Перевіримо виконання вимог:

1) є комутативна група за складанням за модулем 6; операція комутативна;

2) результат операції множення за модулем обов'язково належить множині А, тобто замкненість множини відносно операції множення гарантована;

3) асоціативність множення можна стверджувати на підставі того, що під час виконання операції спочатку виконують звичайне множення, а воно асоціативне та комутативне;

4) дистрибутивність можна перевірити за виразом

$$a_i \otimes_6 (a_j \oplus_6 a_k) = a_i \otimes_6 a_j \oplus_6 a_i \otimes_6 a_k$$

для $a_i = 3$, $a_j = 4$, $a_k = 5$ маємо

$$3 \otimes_6 (4 \oplus_6 5) = 3 \otimes_6 4 \oplus_6 3 \otimes_6 5$$

$$3 \otimes_6 3 = 0 \oplus_6 3$$

$$3 = 3.$$

Таким чином, маємо комутативне кільце. До складу множини належить нейтральний елемент за множенням (це 1), а також $2 \otimes_6 3 = 0$. Це комутативне кільце з одиницею з дільниками нуля.

Ідеал кільця це підмножина кільця, яка є підгрупа за складанням, що містить в собі всі добутки елементів кільця (перший операнд) та підмножини кільця (другий операнд).

У попередньому прикладі група за додаванням має підгрупу з множиною I = {0, 2, 4}. Ця підмножина кільця має властивість: якщо її помножити за модулем 6 на будь–який елемент кільця, то результатом буде або повторення множини, або число, яке належить підмножині. Така підмножина і має назву – ідеал кільця. **Важлива властивість ідеал а – у ньому завжди є елемент, на який можна поділити без залишку всі елементи ідеалу**. У прикладі це 2.

Найпростішим прикладом кільця є кільце *Z* цілих чисел.

Оскільки ми в основному обмежуємося розглядом кінцевих алгебраїчних структур, то таким прикладом може служити кільце повної системи лишків за модулем n.

Наприклад, кільце парних цілих чисел не містить мультиплікативну одиницю і не є областю цілісності. Важливо, що ненульові елементи кільця необов'язково утворюють мультиплікативну групу, тобто. можуть мати зво-

ротних по множенню елементів. Однак у кільці з одиницею є мультиплікативна група оборотних елементів.

Наприклад, в кільці Z/9Z елементи {1, 2, 4, 5, 7, 8} утворюють мультиплікативну циклічну групу 6-го порядку. Усі її елементи взаємно прості з числом 9. Її генератором, наприклад, може бути елемент 2, оскільки 23 = - 1mod 9, 26 = 1mod 9.

Наприклад, кільце парних цілих чисел не містить мультиплікативну одиницю і не є областю цілісності. Важливо, що ненульові елементи кільця необов'язково утворюють мультиплікативну групу, тобто. можуть не мати обернених за множенням елементів. Однак у кільці з одиницею є мультиплікативна група обернених елементів. Наприклад, в кільці Z/9Z елементи {1, 2, 4, 5, 7, 8} утворюють мультиплікативну циклічну групу 6-го порядку. Усі її елементи взаємно прості з числом 9. Її генератором, наприклад, може бути елемент 2, оскільки $2^3 = -1 \mod 9$, $2^6 = 1 \mod 9$.

4.3. Поля Галуа

Def. Скінчене поле або поле Галуа **GF(q)** – це множина q елементів з бінарними операціями додавання (+) і множення (×), всі елементи якої утворюють адитивну абелеву групу, а всі ненульові елементи – мультиплікативну групу. Складання і множення у полі пов'язані законом дистрибутивності.

Число q елементів поля є його порядком (він збігається з порядком адитивної групи), при цьому порядок його мультиплікативної групи дорівнює q - 1.

Оскільки ненульові елементи поля становлять мультиплікативну групу, кожен елемент має зворотний, тоді множення на зворотний елемент можна розглядати як поділ: a/b = ab^{-1}

Розрізняють прості та розширені поля Галуа.

Просте поле Галуа **GF(p)** – це поле простого порядку q = p (p – просте число). Зокрема, кільце лишків за модулем n стає полем, якщо n = p – просте число. І тут будь-який ненульовий лишок є взаємно простим із числом p і, отже, має зворотний. Наприклад, при p = 5 таблиці Келі складання та множення елементів поля мають вигляд

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Неважко бачити, що всі умови для адитивної та мультиплікативної груп поля виконуються. Зокрема всі ненульові елементи мають єдині обернені елементи за множенням.

Мультиплікативна група простого поля позначається як F_p^* і має порядок p – 1. Вона є циклічною групою парного порядку (виключаючи групу F_2^*) і, отже, завжди має підгрупи порядків, які є дільниками числа p – 1.

Розширені поля Галуа **GF(p^n)** будуються як розширення простого поля. Вони мають порядок $q = p^n$, де p – просте число. Число називається характеристикою поля. Елементи розширених полів прийнято представляти за допомогою поліномів ступеня (n-1) над полем GF(p)

$$A(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1}, \quad a_i \in \mathbf{GF(p)},$$

або *n-вим*ірних векторів $\boldsymbol{A} = (a_0, a_1, a_2,,\ldots, a_{n-1})$ відповідного *n-вимір*ного векторного простору.

Додавання в розширеному полі здійснюється за правилами додавання поліномів (або покоординатним додаванням проекцій векторів за mod p), а множення зводиться до визначення остачі від ділення

$$C(x) = res\{A(x)B(x)/P(x)\} = A(x)B(x) \bmod P(x), \qquad (2)$$

де $P(x)$ – неприведений поліном.

Поліном P(x) називається неприведеним, якщо він не розкладається у добуток поліномів менших ненульових степенів над полем **GF(p)** (тобто з коефіцієнтами **GF(p)**). Це поняття споріднене з простим числом в теорії чисел. У табл. 4.1 наведені в двійковій формі всі неприведені поліноми ступенів n = 1, ..., 6 над полем **GF(2)**.

Таблиця 4.1. Неприведені поліноми ступеня n (двійкове представлення)

$n = 1$	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$
10	111	1011	10011	100101	1000011
11		1101	11001	101001	1001001
			11111	101111	1010111
				110111	1011011
				111011	1100001
				111101	1100111
					1101101
					1110011
					1110101

Оскільки всі операції з коефіцієнтами здійснюються за mod p, редукцію (2) називають редукцією за подвійним модулем modd (P(x), p).

Найбільш широко в теорії кодування використовуються розширення двійкового поля **GF(2^n)** або поля характеристики 2. Векторне пред-

ставлення відповідних поліномів у цьому разі записують зазвичай двійковою послідовністю з молодшим розрядом справа. Наприклад,

$$A(x) = x^4 + x^3 + x^2 + 1 = (11101).$$

Для простоти використовуємо знак рівності у правій частині виразу, хоча має місце еквівалентність між поліноміальною формою та векторним записом коефіцієнтів полінома.