Навчальна дисципліна:
Дискретна математика

Лектор:

професор Кучук Георгій Анатолійович

E-mail: kuchuk56@ukr.net

3 семестр навчання на бакалавраті

Наприкінці семестру - іспит

Тема 4. Алгебраїчні структури

Лекція 4.3. Кільця і поля

Питання лекції

1. Подібність алгебраїчних систем.
2. Кільця та ідеали кілець.
3. Поля Галуа.
4. Приклад аналізу алгебраїчної системи.

Рекомендована література

1. *Конспект лекцій.URL: https://drive.google.com/drive/folders/1ZyA3u4y8ZqiAVgu_YeL2XdTk9vp4y9VS?usp=drive_link*

2. *Балога С.І.* Дискретна математика*. Навчальний посібник. – Ужгород: ПП «АУТДОР-. ШАРК», 2021. – 124 с.* *https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/3415/1/%D0%BD%D0%B0%D0%B2%D1%87%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE-%D0%BC%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D1%87%D0%BD%D0%B8%D0%B9%20%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA.pdf*

1. Подібність алгебраїчних систем

Def. Якщо у двох алгебраїчних систем

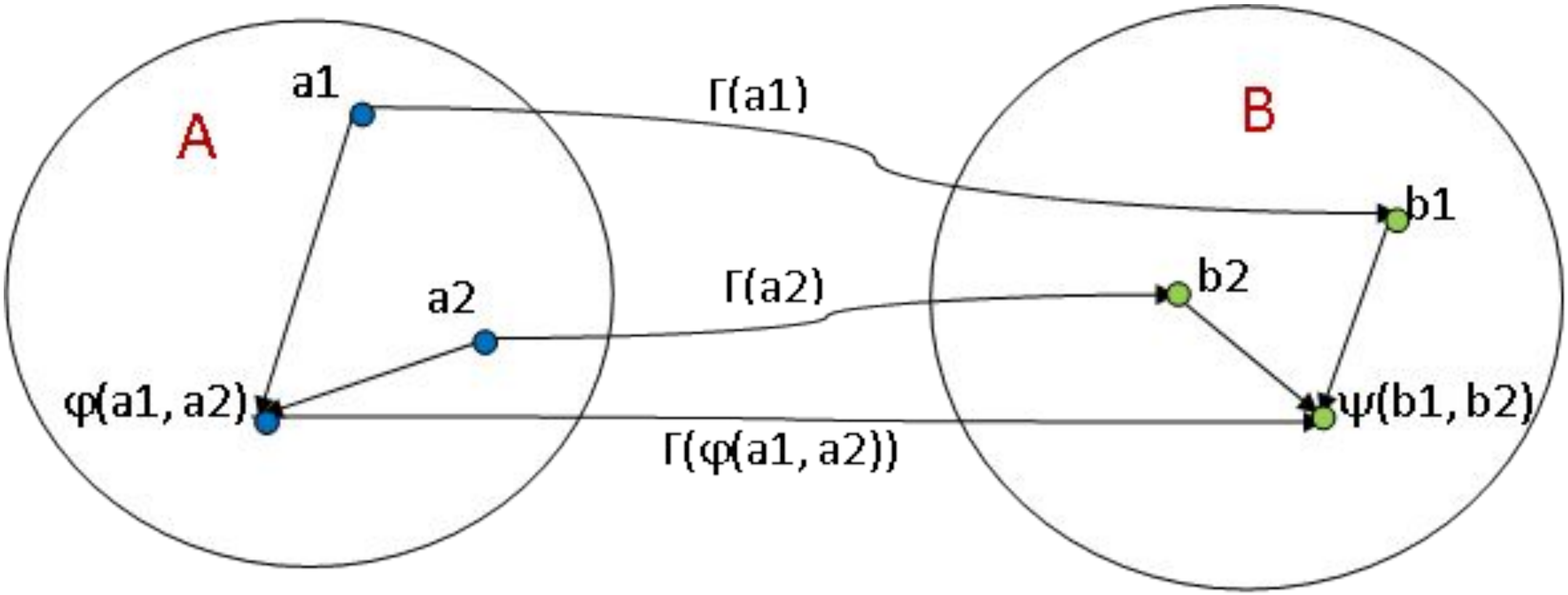
$$К = (A, \phi_1, \phi_2, ..., \phi_p) \quad \text{та} \quad M = (B, \psi_1, \psi_2, ..., \psi_p)$$

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

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

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

Пояснення гомоморфізму алгебраїчної системи К на систему М



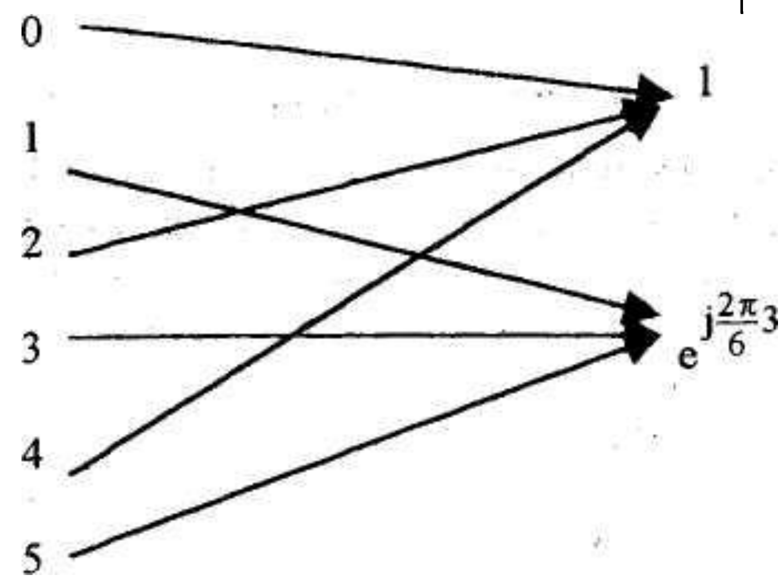
Def. Якщо водночас існує гомоморфізм К на М та гомоморфізм М на К, то такий ступінь подібності має назву **ізоморфізм.**

Def. Якщо використовується відображення множини на її підмножину то ступінь подібності має назву **автоморфізм.**

Приклад гомоморфизму. Група Z_6 та підгрупа 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 Г:



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,
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 ізоморфизму. Група додатних дійсних чисел та група дійсних чисел.

$$A = (R+, \cdot) \text{ та } B = (R, +);$$

R+ – множина додатних дійсних чисел; R – множина дійсних чисел.

У цих систем кількість та арність операцій однакова.
Результати відображення множини R+ → R, якщо $x \in R+$ – за виразом $y = \lg x$; відображення множини R→ R+ – за виразом $x = 10^y$.
Відповідність операндів та результатів доводиться за відомими правилами логарифмування та піднесення до степеня.

Приклад **автоморфізму** Група трирозрядних двійкових чисел з операцією XOR G = (C, XOR), C = (000, 001,011, 010,100,101,110, 111) та підгрупа G1 = (D, XOR), D = {000, 111}.
Є автоморфізм G на G1.
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.

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 додавання (+).

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 $a, b, c \in \mathbf{M}$,

$$a \times (b + c) = a \times b + a \times c, \qquad (b + c) \times a = b \times a + c \times a.$$

Першу з цих операцій (+) умовно звуть додаванням або адитивною операцією, другу (×) – мультиплікативною операцією або множенням.

Щоб алгебраїчна система була кільцем потрібно виконання таких вимог:

1) множина та операція додавання мають створювати комутативну групу (операція має бути ще й комутативна);

2) замкненість множини відносно множення;

3) асоціативність множення

4) дистрибутивність множення відносно додавання.

Кільце – три операції (вводимо операцію віднімання).

Def. Кільце з одиницею – кільце, у якого у множині є нейтральний елемент за множенням.
Властивість: у кільці з одиницею завжди є мультиплікативна група.

Def. Кільце з дільниками нуля – кільце, у якого для елементів множини A можливо $a_i \cdot a_j = 0$, ці елементи є дільники нуля.

Def. Комутативне кільце – кільце, у якого операція множення комутативна.

Ідеал кільця – це підмножина кільця, яка є підгрупа за додаванням, що містить в собі всі добутки елементів кільця (перший операнд) та підмножини кільця (другий операнд).
Важлива властивість ідеалу – у ньому завжди є елемент, на який можна поділити без залишку всі елементи ідеалу.

Ідеал - чотири операції (ще додаємо ділення).

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. Додавання і множення у полі пов'язані законом дистрибутивності.

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

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

Def. Просте поле Галуа **GF(p)** – це поле простого порядку q = p (p – просте число).

Приклад простого поля Галуа.

GF (5) = $\langle$ A, $\oplus_5$, $\otimes_5$ $\rangle$, де A = {0, 1, 2, 3, 4}.

Побудуємо таблиці Келі:

+	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

Def. Розширені поля Галуа GF(p^n) будуються як розширення простого поля. Вони мають порядок $q = p^n$, де p – просте число.

Def. Число p називаються характеристикою поля.

Елементи розширених полів прийнято представляти за допомогою поліномів ступеня (n-1) над полем GF(p):

$$A(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1}, \quad a_i \in \mathbf{GF(p)},$$

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

Def. 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.

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:

$$C(x) = res\{A(x)B(x)/P(x)\} = A(x)B(x) \bmod P(x).$$

4. Приклад аналізу алгебраїчної системи

$$G = GF(5) = \langle A, \oplus_5, \otimes_5 \rangle, \text{ де } A = \{0, 1, 2, 3, 4\}.$$

1. Перевірка наявності адитивної абелевої групи:
   1) Замкненість (+)
   2) Асоціативність (+)
   3) Нейтральний елемент (+)
   4) Обернені елементи (+)
   5) Комутативність (+)
2. Перевірка властивостей мультиплікативної складової (чи є півгрупа)?
   1) Замкненість (+)
   2) Асоціативність (+)
3. Перевірка властивості дистрибутивності (+) ⇒ **G - кільце**
4. Наявність мультиплікативної одиниці (є, це число 1) ⇒ **G - кільце з одиницею**
5. . Перевірка властивостей мультиплікативної складової без адитивного 0:
   4) Обернені елементи (+)
   5) Комутативність (+) ⇒ **G – просте поле Галуа.**