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 4.2. Скінчені групи. Підгрупи

Питання лекції

1. Скінчені групи та таблиці Келі.
2. Циклічні групи та підгрупи.
3. Приклади розв’язання задач.

Рекомендована література

1. *Конспект лекцій.URL: https://drive.google.com/drive/folders/12QYRD4L8kQr0g48DJVN386FrlSDuyPwQ?usp=sharing*

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. Скінчені групи та таблиці Келі

Скінчені групи – це групи, що базуються на скінчених множинах.

Таблиця Келі — таблиця, яка описує структуру скінченних алгебраїчних систем шляхом розміщення результатів операції в таблиці.

Приклад таблиці Келі для скінченої групи {1, −1} з звичайним множенням:

×	1	−1
1	1	−1
−1	−1	1

Приклад 1. Побудова таблиці Келі для класу лишків за модулем 4 (складання та множення за модулем 4):

$\oplus_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\otimes_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Приклад 2. Побудова таблиці Келі для класу лишків за модулем 3 (складання та множення за модулем 3):

$\oplus_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\otimes_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\otimes_3$	1	2
1	1	2
2	2	1

Приклад 3:

$Z_6 = \langle A, \oplus_6 \rangle$, *де* $A = \{0, 1, 2, 3, 4, 5\}$.

$\oplus_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

На елементах множини Z_6 мультиплікативну групу, замінивши операцію додавання операцією множення за модулем 6, побудувати неможливо.

Т е о р е м а. *Елемент a из множини* Z_n *має обернений за множенням елемент* a^{-1} *тоді і тільки тоді, якщо* НЗД(*a, n*) = 1, *тобто. a и n є взаємно простими*.

Умови абелевої групи для мультиплікативної групи системи лишків виконуються, якщо з неї виключити 0, а операцію множення робити за модулем простого числа *p*. Оскільки всі лишки взаємно прості з числом *p*, кожен із них має обернений за множенням елемент.

2. Циклічні групи та підгрупи

Група називається ***циклічною***, якщо в ній є такий елемент *a*, всі степені якого пробігають усі елементи групи (у термінах мультиплікативної групи).

Такий елемент називають ***утворюючим*** (***примітивним***) елементом групи чи генератором.

Для адитивної групи замість *k*-го степеню говорять про *k*-ту кратність.

Приклади: $Z_6 = (A, \oplus_6\rangle$, *де* $A = \{0, 1, 2, 3, 4, 5\}$.
Примітивні елементи: 1, 5.

$Y_3 = (A, \otimes_3\rangle$, *де* $A = \{1, 2\}$.
Примітивний елемент: 2.

Підгрупа – це підмножина групи, яка відповідає всім вимогам групи.

Приклад 4: *$G = (Z, +\rangle$, де Z – цілі числа.*

$G_2 = (ZP, +\rangle$, де ZP – парні числа

$G_5 = (Z5, +\rangle$, де $Z5$ – цілі числа, що кратні 5

$G_{1000} = (Z1000, +\rangle$, де $Z1000$ – цілі числа, що кратні 1000

Приклад 5. У групі лишків за модулем $Z_6 = \langle A, \oplus_6 \rangle$, де A = {0, 1, 2, 3, 4, 5}, виділимо підмножину D = {0, 3}.

$Z^* = \langle D, \oplus_6 \rangle$ - підгрупа.

Порядок підгрупи (або групи) є потужність множини підгрупи (або групи).

Порядок елемента групи є порядок циклічної підгрупи, яку виділено за допомогою цього елемента.

Теорема Лагранжа. Порядок елемента групи (порядок підгрупи) є дільником порядки групи.

Це означає, що, коли, наприклад, у групі 12 елементів, то можливі підгрупи з 1, 2, 3, 4, 6, 12 елементів. А якщо у групі 7 елементів, то можуть бути лише тривіальні підгрупи (вони є завжди) з одного та з семи елементів.

Приклад 6. Розглянемо групу лишків за модулем $Z_6 = \langle A, \oplus_6 \rangle$, де A = {0, 1, 2, 3, 4, 5}.

$Z^* = \langle D, \oplus_6 \rangle$ - підгрупа.

Порядок групи – 6.
Можливі порядки підгруп: 1, 2, 3, 6.

{0, 1, 2, 3, 4, 5}

Порядки елементів відповідно: {1, 6, 3, 2, 3, 6}

Суміжні класи – це специфічні підмножини групи, які не мають взаємних перетинів і мають однакові потужності з підгрупою, використаною для розбиття.

За кожною підгрупою існує єдине розбиття на суміжні класи.

3. Приклади розв'язання задач

Приклад 7.

Знайти циклічну підгрупу у групі $Z_{12} = \langle A, \oplus_{12} \rangle$,
$A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$, беручи $q = 4$.

Розв'язання:

$q = 4$,

$q \oplus_{12} q = 8$,

$q \oplus_{12} q \oplus_{12} q = 12 \bmod 12 = 0$.

Звідси $G = \langle H, \oplus_{12} \rangle$, де $H = \{4, 8, 0\}$, є підгрупа порядку 3 у множині Z_{12}.

Приклад 8.

Розбиття групи $Z_{12} = \langle A, \oplus_{12} \rangle$ на суміжні класи за підгрупою $H = \langle H, \oplus_{12} \rangle$, де

$A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$, $H = \{4, 8, 0\}$.

Розв'язання:

Викреслимо з множини A елементи підмножини H:

$A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$.

Беремо найменший серед невикреслених (1) та додаємо до H:

$1 \oplus H = 1 \oplus \{4, 8, 0\} = \{5, 9, 1\} = H_1$

Далі викреслюємо з множини A елементи підмножини H_1

$A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$.

Беремо найменший серед невикреслених (2) та додаємо до H:

$2 \oplus H = 2 \oplus \{4, 8, 0\} = \{6, 10, 2\} = H_2$

Далі викреслюємо з множини A елементи підмножини H_2

$A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$.

Беремо найменший серед невикреслених (3) та додаємо до H:

$3 \oplus H = 3 \oplus \{4, 8, 0\} = \{7, 11, 3\} = H_3$

Далі викреслюємо з множини A елементи підмножини H_3

$A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$.

Все, множина A – порожня, тобто розбиття є таким:

$$A = H \cup H_1 \cup H_2 \cup H_3, \text{ бо}$$

$H \cap H_1 = \varnothing$, $H \cap H_3 = \varnothing$, $H_1 \cap H_2 = \varnothing$, $H_1 \cap H_3 = \varnothing$, $H_2 \cap H_3 = \varnothing$.