Тема 4. АЛГЕБРАЇЧНІ СТРУКТУРИ

Лекція 4.2. Скінчені групи. Підгрупи

План лекції

1. Скінчені групи та таблиці Келі.
2. Циклічні групи та підгрупи.
3. Приклади розв'язання завдань.

Литература.

1. *Конспект лекцій.*
2. *Балога С.І.* Дискретна математика. *Навчальний посібник. – Ужгород: ПП «АУТДОР-. ШАРК», 2021. – 124 с.*
3. Слєсарєв В. В., Новицький І. В., Ус С. А. Дискретна математика: навч. посібник. Дніпро : НТУ «ДП», 2023. 183 с. URL : https://ir.nmu.org.ua/bitstream/handle/123456789/164331/DyskretnaMatematyka%28Slesarev_Novytskyi_Us%29.pdf?sequence=1&isAllowed=y.

1. Скінчені групи та таблиці Келі

У цікавих для нас застосунках велике значення мають скінчені групи, тобто групи, що базуються на скінчених множинах.

Розглянемо декілька прикладів.

Приклад. В прикладних завданнях часто використовується множина **Z** цілих чисел, рівних між собою за модулем натурального числа n.

МИ знаємо, що a и b є рівними за модулем n ($a \equiv b \pmod n$), якщо різниця $a - b$ ділиться на n, тобто, $a = b + kn$ для деякого цілого k.

Відношенням рівності за модулем n множина **Z** розбивається на класи *лишків* за модулем n:

$$[0] = \{\ldots, -2n, -n, 0, n, 2n, 3n, \ldots\},$$
$$[1] = \{\ldots, -2n + 1, -n + 1, 1, n + 1, 2n + 1, 3n + 1, \ldots\},$$
$$[2] = \{\ldots, -2n + 2, -n + 2, 2, n + 2, 2n + 2, 3n + 2, \ldots\},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$[n-1] = \{\ldots, -n - 1, -1, n - 1, 2n - 1, 3n - 1, \ldots\}.$$

Такі класи лишків з операцією додавання елементів утворюють адитивну групу, що позначається як $\mathbf{Z}_n$. Елемент, що стоїть у квадратних дужках і позначає клас, можна розглядати як невід'ємну остачу від ділення чисел цього класу на n (найменший невід'ємний лишок). Всі ці елементи утворюють повну систему лишків за *mod* n: $\mathbf{Z}_n = \{0, 1, 2, 3, \ldots, n - 1\}$. Оскільки операції з найменшими лишками можна порівняти за модулем n з операціями над класами n з операціями над класами лишків, повна система лишків зі складанням елементів також утворює скінчену адитивну групу.

Для опису операцій скінчених груп на практиці доволі часто використовуються таблиці Келі.

Таблиці Келі вперше з'явилися в статті Келі "On The Theory of Groups, as depending on the symbolic equation θ n = 1" в 1854 році. В цій статті це були просто таблиці, які використовувалися з ілюстративною метою. Називати таблицями Келі їх почали пізніше, в честь їх творця.

Таблиця Келі — таблиця, яка описує структуру скінченних алгебраїчних систем шляхом розміщення результатів операції в таблиці, яка нагадує таблицю множення. Таблиця має важливе значення в дискретній математиці, зокрема, в теорії груп. Таблиця дозволяє визначити деякі властивості групи, наприклад, чи є група абелевою, знайти центр групи і обернені (симетричні) елементи для елементів групи.

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

×	1	−1
1	1	−1
−1	−1	1

Оскільки чимало таблиць Келі описують групи, які не є абелевими, добуток *ab* не обов'язково рівний добутку *ba* для всіх *a* і *b* в групі. Щоб уникнути плутанини, приймається, що множник, який відповідає рядкам, йде першим, а множник, який відповідає стовпцям — другим. Наприклад, перетин рядка *a* і стовпця *b* — це *ab*, а не *ba*, що показано в наступному прикладі:

*	*a*	*b*	*c*
a	a^2	*ab*	*ac*
b	*ba*	b^2	*bc*
c	*ca*	*cb*	c^2

Таблиця Келі показує нам, чи є група абелевою. Оскільки групова операція в абелевій групі комутативна, група є абелевою в тому і тільки в тому випадку, коли її таблиця Келі є симетричною (відносно діагоналі). Циклічна група {1, −1} по звичайному множенню є прикладами абелевої групи, і симетрія її таблиці Келі це доводить.

Ніякий рядок або стовпець таблиці Келі не може містити один елемент двічі. Таким чином, кожний рядок і стовпець таблиці є перестановкою елементів групи.

Щоб побачити, чому рядки і стовпці не можуть містити однакових елементів, припустимо, що *a*, *x* та *y* — елементи групи, причому *x* та *y* відрізняються, а групову операцію зіставимо із операцією добутку. Тепер в рядку, який відповідає елементу *a*, і стовпці, який відповідає елементу *x*, буде знаходитися добуток *ax*. Аналогічно в стовпці, який відпо-

відає y, буде знаходитись ay. Нехай два добутки рівні, тобто є рядок a, який містить два однакові елементи. За правилом скорочення з $ax = ay$ можемо зробити висновок, що $x = y$, що суперечить вибору x і y. Для стовпців ці міркуванням також істинні. Оскільки група скінченна, за принципом Діріхле кожен елемент групи міститиметься в кожному рядку і в кожному стовпці тільки по одному разу.

Приклад. Розглянемо повну систему лишків за модулем 6 з лишками $\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ та операцією складання. Складання всіх можливих пар елементів системи за модулем 6 зручно подати за допомогою таблиці Келі

+	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

Звідси легко бачити, що всі 5 умов групи виконуються, тобто. множина Z_6 з операцією додавання утворює групу Z_6, яка є адитивною абелевою групою. Єдиним елементом адитивної групи є 0**,** , і для кожного елемента a існує зворотний $(-a)$, такий, що $a + (-a) = 0$.

Якщо спробувати побудувати на елементах множини Z_6 мультиплікативну групу, замінивши операцію додавання операцією множення за модулем 6, це виявиться неможливим з двох причин. По-перше, для елемента 0 немає зворотного (за множенням) елемента (на 0 ділити не можна, як у звичайній арифметиці). По-друге, зворотних елементів немає і у таких лишків, як 2, 3 і 4. У цьому можна переконатися, побудувавши таблицю Келі для множення. Зауважимо, що всі вони взаємно прості з числом $n = 6$. Лише 1 і 5 мають обернені елементи, що збігаються із самими собою.

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

Пример 4.3. Побудуємо таблицю Келі для лишків 1, 2, 3, 4 множенням елементів за модулем $p = 5$.

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

Тут кожен рядок (кожен стовпець) містить одну одиницю 1, тобто. для кожного елемента існує єдиний обернений елемент, добуток якого з вихідним елементом дає 1. Наприклад, $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$. Виконання інших умов групи видно з таблиці Келі . Таким чином, лишки 1, 2, 3, 4 з операцією множення за модулем 5 утворюють мультиплікативну групу $\mathbf{Z}_5^*$ порядку 4 (в загальному випадку мультиплікативна група $\mathbf{Z}_p^*$ зменшується в порівнянні з адитивною групою $\mathbf{Z}_p$ на один елемент и має порядок $p - 1$).

У наведених прикладах додавання та множення за модулем *n* здійснюється майже як звичайні додавання та множення, з тією відмінністю, що результат визначається як остача від ділення суми (добутку) на *n*. Існує безліч прикладів груп, для котрих терміни “складання” чи “множення” досить умовні і може бути замінений чимось іншим. Наприклад, деякі функціонально зв'язані точки (*x*, *y*) на площині можуть утворити групу, при цьому можна ввести операцію суми або добутку пари точок для отримання третьої точки. Тому нерідко поняття адитивної чи мультиплікативної груп умовні і прив'язуються до найзручнішої системи позначень. Поділ цих понять стає суттєвим у алгебраїчних системах з двома операціями.

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.

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

Приклад. У групі лишків за модулем $Z_6 = (A, \oplus_6)$, де $A = \{0, 1, 2, 3, 4, 5\}$, виділимо підмножину D. $D \subset A$, $D = \{0, 3\}$. Перевіримо виконання вимог до групи у алгебраїчній системі $(D, \oplus_6)$:

1) множина має всього 2 елементи, тому неважко виконати всі можливі операції в системі і впевнитись, що результат операції завжди належить множині D: $0 \oplus_6 3 = 3$, $0 \oplus_6 0 = 0$, $3 \oplus_6 3 = 0$; наявна замкненість множини відносно операції;

2) асоціативність у операції є, бо операцію не змінювали;

3) нейтральний елемент у групі та підгрупі той же самий – 0;

4) кожний з елементів підгрупи є сам собі обернений – ця вимога теж виконана. Таким чином, система $(D, \oplus_6)$ є підгрупа у групі.

Розглянемо спосіб виділити підгрупу у групі. Нехай маємо деяку групу з множиною Q та абстрактною операцією $\circ$, тобто, систему $(Q,\circ)$. Візьмемо елемент множини $q \in Q$ і будемо виконувати багаторазово групову операцію, щоб одержати q q o q (умовно позначимо, як q^2), q ° q ° q. (позначимо, як q^3) і так доти, поки не отримаємо $q^m = e$ (нейтральний елемент). Тоді з множиною $F = \{q, q, q, ... q^m\}$ система (F,°) є циклічна підгрупа. Доведемо, що вимоги групи тут виконані. Якщо перемножити два елементи з множини F,

$$q^i \circ q^j = q^{(i+j)\mathrm{mod}m}$$

можна стверджувати, що у показниках степеню відбуваються такі ж дії, як у групі Z_m. Для доведення виконання вимог групи цього достатньо з посиланням на ізоморфізм груп (подібність алгебраїчних систем розглянемо нижче).

Приклад. Задача. Знайти циклічну підгрупу у групі Z_{12}, беручи q = 4.

Розв'язок: $q = 4$, $q \oplus_{12} q = 8$, $q \oplus_{12} q \oplus_{12} q = 12\mathrm{mod}12 = 0$. Звідси $G = (B, \oplus_{12})$, де $B = \{4, 8, 0\}$, є підгрупа порядку 3 у множині Z_{12}.

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 встановлює зв’язок між порядком групи та можливими варіантами порядку підгруп у цій групі. Формулювання її таке:

Теорема. 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. У цьому випадку (коли порядок групи є просте число) намагання виділити циклічну підгрупу призведе до виділення всієї групи. Це іноді використовують для пошуку розв’язку рівнянь, відносно яких відомо, що розв'язки створюють групу. Маючи один з розв’язків, виділенням циклічної підгрупи знаходять інші розв'язки.

Наприклад, знаємо, що корені алгебраїчного рівняння $x^7 = 1$ створюють групу відносно множення. Коренів всього 7. Один корінь x = 1 – дійсне число, інші – комплексні числа, достатньо знайти хоча б один комплексний ко-

рінь – багаторазовим множенням можна знайти всі інші комплексні корені. Нехай знаємо один комплексний корінь

$$x = e^{j\frac{2\pi}{7}}, \text{ тоді інші } xx = e^{j\frac{2\pi}{7}2},\ xxx = e^{j\frac{2\pi}{7}3},\ xxxx = e^{j\frac{2\pi}{7}4},\ xxxxx = e^{j\frac{2\pi}{7}5},$$
$$xxxxxx = e^{j\frac{2\pi}{7}6}.$$

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

Якщо виконати групову операцію між елементом групи, який не належить підгрупі, та всіма елементами підгрупи, то одержимо підмножину групи з такою властивістю, виконання групової операції між будь-яким елементом цієї підмножини і множиною підгрупи виділить знову цю ж підмножину групи (суміжний клас). Для виділення наступного суміжного класу треба виконати групову операцію між елементом групи, що не належить ні підгрупі, ні вже виділеній підмножині групи (суміжному класу), та множиною підгрупи.

Тобто, маємо групу G = (A,°) , маємо також підгрупу у цій групі B = (H, °), де $H \subset A$, A = {a_1, a_2, a_3, ..., a_m}; якщо $a_i \notin H$, операція a_i°H виділить суміжний клас $H_1 = a_i$°H, якщо $a_j \notin H$ та $a_j \notin H_1$, то операція a_j°H виділить наступний суміжний клас $H_2 = a_j$°H і так далі, поки не будуть виявлені всі n суміжних класів (n = |A| / |H|).

Приклад: Розбиття групи Z_{12} = (A $\oplus_{12}$) на суміжні класи за підгрупою B = (H, $\oplus_{12}$), де A = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11}, H = {4, 8, 0). Суміжний клас, якщо виберемо елемент 3 $\notin$ H, H_1 = 3 $\oplus_{12}$H = 3 $\oplus_{12}$ {4,8, 0} = {4, 8, 0} = {7, 11, 3}; наступний суміжний клас з елементом 5 $\notin$ H, H_2 = 5 $\oplus_{12}$H = 5 $\oplus_{12}${4, 8, 0} = {9, l, 5}; і нарешті з елементом 2, який не належить ні підмножині, ні жодному з виділених суміжних класів, маємо H_3 = 2$\oplus_{12}$H = 2 $\oplus_{12}${4, 8, 0} = {6, 10, 2}. Таким чином, маємо розбиття A = H $\cup$ H_1 $\cup$ H_2 $\cup$ H_3, 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 = $\varnothing$.