Тема 4. АЛГЕБРАЇЧНІ СТРУКТУРИ

Лекція 4.1. Множини з однією операцією

План лекції

1. Групоїди.
2. Приклади розв'язання задач.
3. Приклади груп, що часто використовуються.

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.

4.1. Групоїди

Групоїд – це множина з замкненою операцією, тобто. результат операції не виходить за межі цієї множини:

$$G = (M, \circ) \text{ – групоїд} \quad \Leftrightarrow \quad a \circ b \in M \ \ \forall\, a, b \in M.$$

Властивість – замкненість.

Приклади. 1. Цілі числа з відніманням – групоїд.

2. Натуральні числа з відніманням – не групоїд.

3. Раціональні числа з операцією поділу – не групоїд, через нуль.

Півгрупа – групоїд з асоціативною операцією.

$$G = (M, \circ) \text{ – півгрупа} \quad \Leftrightarrow \quad (a \circ b) \circ c = a \circ (b \circ c) \quad \forall\, a, b, c \in M$$

Властивість – замкненість, асоціативність.

Приклади. 1. Цілі числа з відніманням – не півгрупа.

2. Множина слів в алфавіті A з операцією !! (конкатенація) – півгрупа.

3. Множина натуральних чисел з операцією складання (N, +) – півгрупа.

Циклічна півгрупа – півгрупа, яку можна побудувати лише за допомогою одного елемента та операції.

Приклад 2 – ні.

Приклад 3. Так, є такий елемент – 1 (називається утворюючим), позначається $N = [\{1\}]_{+}$.

Моноїд – півгрупа з нейтральним елементом e, для якого при $\forall a_i$

$$e \circ a_i = a_i; \quad a_i \circ e = a_i$$

Приклади. 1. Множина слів А*, складених з алфавіту А (операція !!) разом з порожнім словом Λ – моноїд, без порожнього слова – не моноїд.

2. Множина невід'ємних цілих чисел з операцією додавання, тобто $(\{N \cup 0\}, +)$ – моноїд.

Теорема. Моноїд має тільки один нейтральний елемент.

Доведення. Доводиться від протилежного:

Нехай $\exists e_2 \neq e_1 \quad \Rightarrow \quad \forall a\left(a \circ e_1 = e_1 \circ a = a\right) \& \left(a \circ e_2 = e_2 \circ a = a\right)$.

Підставимо в ці рівності замість a інші нейтральні елементи:

$\left(e_2 \circ e_1 = e_1 \circ e_2 = e_2\right) \& \left(e_1 \circ e_2 = e_2 \circ e_1 = e_1\right)$.

Виберемо дві однакові рівності:

$\left(e_1 \circ e_2 = e_2\right) \& \left(e_1 \circ e_2 = e_1\right)$

Маємо $e_1 = e_2$, отже протиріччя, тобто іншого нейтрального елемента не існує, що і потрібно було довести.

Група – моноїд G, в якому для кожного елемента існує обернений, тобто:

$$\forall a \in G \quad \exists \tilde{a} \big| \, a \circ \tilde{a} = \tilde{a} \circ a = e.$$

Приклади. 1. Множина невироджених квадратних матриць $n \times n$ (визначники яких не дорівнюють нулю) з операцією множення матриць.

2. Множина цілих чисел з операцією додавання.

Теорема. Кожний елемент групи має тільки один обернений елемент.

Доведення. Доводиться від протилежного:

Нехай $\exists \tilde{a}, b \quad \Rightarrow \quad \left(a \circ \tilde{a} = \tilde{a} \circ a = e\right) \& \left(a \circ b = b \circ a = e\right)$.

Тоды $\tilde{a} = \tilde{a} \circ e = \tilde{a} \circ \left(a \circ b\right) = \left(\tilde{a} \circ a\right) \circ b = e \circ b = b$

Отже, $\tilde{a} = b$, що і потрібно було довести.

Наслідок 1. У групі однозначно вирішується рівняння $a \circ x = b$. Його рішення $x = \tilde{a} \circ b$.

Наслідок 2. $c = a \circ b \quad \Rightarrow \quad \tilde{c} = \tilde{b} \circ \tilde{a}$.

Наслідок 3. $a \circ b = a \circ c \quad \Rightarrow \quad b = c$

Наслідок 4. $\tilde{\tilde{a}} = a$

Комутативна або абелева група – група G, операція якої є комутативною, тобто $\forall a, b \in G \quad \Rightarrow \quad a \circ b = b \circ a$.

Приклади. 1. $\langle Z,+\rangle$ – цілі числа з операцією додавання (адитивна нескінченна комутативна група).

2. M = {0, 1}, операція XOR (адитивна скінченна комутативна група).

3. $\langle Q\setminus\{0\},\times\rangle$ – раціональні числа без нуля з операцією множення (мультиплікативна нескінченна комутативна група).

4. Корені рівняння $x^n = 1$ (мультиплікативна скінченна комутативна група)

5. $\left\langle 2^M,\oplus\right\rangle$ – булеан базової множини з операцією «симетрична різниця»; при цьому порожня множина - нейтральний елемент, а обернений - доповнення до *M*.

6. Неабелева група – квадратні матриці 2×2 відносно множення.

4.2. Приклади груп, що часто використовуються

4.2.1. Група переставлень S_n або симетрична група порядку n!

$$S_n=\langle A,\circ\rangle,\ \text{card}\,M=n,\ A=\{a\in P_n(M)\}.$$

Порядок групи дорівнює потужності множини (кількості переставлень) групи. Припустимо n = 3, потужність множини n! = 3! = 6, Слово "переставлення" тут слід розуміти не як кортеж з трьох елементів у якому переставлено місцями елементи, а як алгоритм-вказівку про те, як саме здійснити одноразове переставлення. Такий алгоритм зображують двома рядками. Верхній рядок показує розташування елементів до переставлення, нижній – після переставлення, наприклад:

$$\begin{pmatrix}a\,b\,c\\ c\,a\,b\end{pmatrix}.$$

Тому загальний запис групи $S_n = (A, \circ)$ складається з множини переставлень

$$A=\left\{\begin{pmatrix}a\,b\,c\\ a\,b\,c\end{pmatrix},\begin{pmatrix}a\,b\,c\\ a\,c\,b\end{pmatrix}\begin{pmatrix}a\,b\,c\\ b\,a\,c\end{pmatrix}\begin{pmatrix}a\,b\,c\\ c\,b\,a\end{pmatrix}\begin{pmatrix}a\,b\,c\\ b\,c\,a\end{pmatrix}\begin{pmatrix}a\,b\,c\\ c\,a\,b\end{pmatrix}\right\}$$

та з операції композиції переставлень з позначкою "$\circ$". Операція з двох переставлень продукує третє, еквівалентне за дією послідовному виконанню двох, наприклад:

$$\begin{pmatrix}a\,b\,c\\ b\,c\,a\end{pmatrix}\circ\begin{pmatrix}a\,b\,c\\ a\,c\,b\end{pmatrix}=\begin{pmatrix}a\,b\,c\\ c\,b\,a\end{pmatrix}, \qquad (34)$$

Операція виконана за таким правилом. У першому стовпчику першого переставлення маємо перехід a $\to$ b. Стовпчик другого переставлення, що має верхній елемент b, має перехід b $\to$ c. З двох переходів маємо ланцюжок a $\to$ b $\to$ b $\to$c, у якому початковий та кінцевий елементи створюють стовпчик з переходом a $\to$ c, тобто, перший стовпчик переставлення результату операції. Аналогічно ланцюжок b $\to$ c $\to$ c $\to$ b дає другий стовпчик з переходом b $\to$ b і ланцюжок c $\to$ a $\to$ a $\to$ a дає третій стовпчик результату з переходом c $\to$ a.

Проаналізуємо, чи є система $S_3=(A,\circ)$ групою, тобто, чи відповідає вимогам.

1) вимога замкнености множини відносно операції виконана; це випливає з таких міркувань: результат операції над двома переставленнями є теж переставлення; множина A містить у собі всі можливі варіанти переставлень і тому містить у собі результат операції;

2) вимога асоціативності операції виконана, бо для будь-яких трьох елементів множини А можна довести можливість переставлення дужок так, як це показано у наступному прикладі:

$$\left(\begin{pmatrix} a\,b\,c \\ a\,c\,b \end{pmatrix}\circ\begin{pmatrix} a\,b\,c \\ b\,a\,c \end{pmatrix}\right)\circ\begin{pmatrix} a\,b\,c \\ c\,b\,a \end{pmatrix}=\begin{pmatrix} a\,b\,c \\ a\,c\,b \end{pmatrix}\circ\left(\begin{pmatrix} a\,b\,c \\ b\,a\,c \end{pmatrix}\circ\begin{pmatrix} a\,b\,c \\ c\,b\,a \end{pmatrix}\right)$$

після виконання операцій у дужках маємо:

$$\begin{pmatrix} a\,b\,c \\ b\,c\,a \end{pmatrix}\circ\begin{pmatrix} a\,b\,c \\ c\,b\,a \end{pmatrix}=\begin{pmatrix} a\,b\,c \\ a\,c\,b \end{pmatrix}\circ\begin{pmatrix} a\,b\,c \\ b\,c\,a \end{pmatrix} \text{ і далі } \begin{pmatrix} a\,b\,c \\ b\,a\,c \end{pmatrix}=\begin{pmatrix} a\,b\,c \\ b\,a\,c \end{pmatrix};$$

3) множині А належить елемент $\begin{pmatrix} a\,b\,c \\ a\,b\,c \end{pmatrix}$*, який є нейтральний, бо* $\begin{pmatrix} a\,b\,c \\ b\,a\,c \end{pmatrix}\circ\begin{pmatrix} a\,b\,c \\ a\,b\,c \end{pmatrix}=\begin{pmatrix} a\,b\,c \\ b\,a\,c \end{pmatrix}$ *або* $\begin{pmatrix} a\,b\,c \\ a\,b\,c \end{pmatrix}\circ\begin{pmatrix} a\,b\,c \\ b\,a\,c \end{pmatrix}=\begin{pmatrix} a\,b\,c \\ b\,a\,c \end{pmatrix}$*, тобто вимога наявності нейтрального елемента у множині – виконана;*

4) вимога наявності оберненого елемента для кожного у множині виконана бо можна запропонувати наступний спосіб одержання оберненого елемента для кожного елемента множини А: у елемента треба переставити місцями рядки, потім переставити місцями стовпчики, щоб верхній рядок мав вигляд a b c *; наприклад: .*

для елемента $\begin{pmatrix} a\,b\,c \\ c\,a\,b \end{pmatrix}$ *одержимо обернений* $\begin{pmatrix} a\,b\,c \\ c\,a\,b \end{pmatrix}\to\begin{pmatrix} c\,a\,b \\ a\,b\,c \end{pmatrix}\to\begin{pmatrix} a\,b\,c \\ b\,c\,a \end{pmatrix}$ *і доведемо, що це обернений елемент:*

$$\begin{pmatrix} a\,b\,c \\ c\,a\,b \end{pmatrix}\circ\begin{pmatrix} a\,b\,c \\ b\,c\,a \end{pmatrix}=\begin{pmatrix} a\,b\,c \\ a\,b\,c \end{pmatrix}$$

Таким чином, алгебраїчна система $S_3=(A,\circ)$ *є група.*

Але дана група не є абелевою, про це свідчить приклад:

$$\begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}\circ\begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}=\begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}, \text{ але}$$

$$\begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}\circ\begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}=\begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}.$$

Розгляд у якості прикладу саме такої групи пояснюється потребою підкреслити, що елементи групи не обов'язково числа і операції не обов'язково арифметичні.

4.2.2. Z_n – група остач за модулем n

Ця алгебраїчна система складається з множини остач від ділення цілих додатних чисел на n *та операції складання за модулем* n*, тобто;*

$$Z_n = \langle B,\oplus_n\rangle,\ B = (0,\ 1,\ 2,\ ...,\ n-1),\ b_i\oplus_n b_j = \left(b_i+b_j\right) mod\ n.$$

Операція mod n *залишає від числа у дужках залишок від його ділення на* n*. Доведемо, що* Z_n *є група.*

1)операція $\oplus_n$ *дає результат – остачу від ділення на* n*, а множина В містить всі варіанти залишків від ділення на* n*, тому результат операції завжди належить множині і замкненість гарантована;*

2)асоціативність операції випливає з того, що під час виконання операції спочатку виконують звичайне додавання, а воно асоціативне;

3) у складі множини є нейтральний елемент; це 0; складання з нулем дає у результаті другий операнд операції;

4) обернений елемент для кожного елемента множини групи можна обчислити за виразом

$$b_i^{-1} = n - b_i$$

бо

$$b_i \oplus_n (n - b_i) = (b_i + n - b_i) \bmod n = 0 .$$

5) Комутативність складання очевидна.

Таким чином Z_n є абелева група.

4.2.3. Група коренів рівняння $x^n = 1$

Рівняння $x^n = 1$ має один дійсний корінь $x = 1$, якщо n непарне, має ще один дійсний корінь $x = –1$, якщо n парне. Інші корені (всього їх має бути n) комплексні з модулем 1. Множина коренів з операцією множення створюють групу, тобто, система U_n = (A, ·),де A – множина коренів, є група. Підтвердимо це на прикладі для $n = 5$. Множина коренів рівняння $x^5 = 1$ $A = \left\{1, e^{j\frac{2\pi}{5}}, e^{j\frac{2\pi}{5}\cdot 2}, e^{j\frac{2\pi}{5}\cdot 3}, e^{j\frac{2\pi}{5}\cdot 4}\right\}$. *Впевнитись, що комплексні числа є корені рівняння, можна піднесенням кореня до степеня 5; результат дорівнюватиме 1. Наприклад*

$$\left(e^{j\frac{2\pi}{5}\cdot 3}\right)^5 = e^{j\frac{2\pi}{5}\cdot 3\cdot 5} = e^{j(6\pi) \bmod 2\pi} = e^{j0} = e^0 = 1 .$$

Перевіримо, що система U_n = (A, ·) відповідає вимогам до груп:

1) добуток, якщо співмножники є корені з множини A, теж належить множині A; це тому, що

$$A = \bigcup_{i=0}^{4} e^{j\frac{2\pi}{5}i} \qquad (35)$$

і під час множення маємо складати показники степеня, що зводиться після винесення за дужки $j2\pi/5$ *до складання за модулем 5 двох значень змінної i, а це дасть ціле число від 0 до 4 включно, тобто, один з коренів;*

2) асоціативність операції звичайного множення доведення не потребує;

3) для операції множення у складі множини A є нейтральний елемент, це 1;

4) для кожного кореня з певним значенням змінної i можна запропонувати корінь із значенням змінної 5-i, який є обернений елемент до нього та їх добуток дорівнюватиме нейтральному елементу, тобто 1.

5) множення – комутативна операція.

Таким чином, система U_n є абелева група.

4.2.4. Група n-розрядних двійкових чисел з операцією підсумування розрядами (XOR)

Алгебраїчна система G = ⟨C, XOR⟩ для $n = 3$ має множину C = {000, 001,011, 010, 100, 101, 110, 111). Операція XOR є у складі команд будь-якої ЕОМ і виконується складанням без перенесень у старший розряд. Покажемо виконання вимог групи:

1) підсумовування розрядами двох елементів множини C дасть трирозрядне двійкове число, а множина C містить всі варіанти таких чисел, тому результат операції обов'язково належить множині C і замкненість множини відносно операції гарантована;

2) під час виконання операції XOR кожен розряд обробляється окремо шляхом підсумовування за модулем 2, а ця операція була визнана асоціативною у прикладі груп залишків за модулем, тому операція XOR асоціативна;

3) у складі множини C є нейтральний елемент 000;

4) кожний елемент групи є обернений сам до себе, оскільки підсумовування розрядами двох однакових чисел дає нульовий результат, тобто, нейтральний елемент.

Таким чином, алгебраїчна система G = (C, XOR) є група.

4.2.5. Група багаточленів у двійковій системі числення

Багаточлени у двійковій системі числення мають складові з піднесеної до різного степеня (але не більше n) формальної змінної x з двійковими коефіцієнтами з поля Галуа характеристики 2. Операція – це додавання за модулем 2. Множина алгебраїчної системи складається з двох елементів {0, 1}. Це значить, що коефіцієнти складових або одиниці, або складові відсутні; під час додавання багаточленів коефіцієнти підсумовуються за модулем 2.

Розглянемо приклад для n = 3. Алгебраїчна система Mn = ⟨D, ⊕⟩ є група. Визначимо, що є множина і як виконується операція. Множина

$D = \{0, 1, x, x + 1, x^2 + 1, x^2 + x, x^2 + x + 1, x^3, x^3 + 1, x^3 + x, x^3 + x + 1,$
$x^3 + x^2, x^3 + x^2 + 1, x^3 + x^2 + x, x^3 + x^2 + x + 1\}$

Додавання:

$$(x^3 + x + 1) \oplus (x^3 + x^2 + x) = x^2 + 1.$$

Результат пояснюється тим, що

$$x^3 \oplus x^3 = x^3(1 \oplus 1) = x^3 \cdot 0 = 0 \quad x^2 \oplus x^2 = x^2(1 \oplus 1) = x^2 \cdot 0 = 0$$

Переглянемо виконання вимог до групи:

1) операція така, що поява у доданків показників степеня, відмінних від 0, 1, 2, 3 неможлива; всі варіанти багаточленів є у складі множини D, тому результат операції завжди буде належати множині D і замкненість гарантована;

2) під час обчислення коефіцієнтів багаточлена використовують операцію додавання за модулем, яка є асоціативною (розділ 6.2.2), тому операція додавання багаточленів теж є асоціативною;.

3) нейтральний елемент 0 належить множині D;

4) для кожного елемента множини D у складі множини B можна знайти обернений, бо кожний елемент є обернений сам собі.

Таким чином, алгебраїчна система Mn = ⟨D, ⊕⟩ є група.