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 4.1. Множини з однією операцією

Питання лекції

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

Рекомендована література

1. *Конспект лекцій.URL:* [*https://drive.google.com/drive/folders/1OMJU17COF9O5E11HEhS_Ou6B9VEyltOu?usp=share_link*](https://drive.google.com/drive/folders/1OMJU17COF9O5E11HEhS_Ou6B9VEyltOu?usp=share_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*

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. Групоїди

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

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

Властивість – замкненість.

Приклади.

1. Цілі числа з відніманням – групоїд.
2. Натуральні числа з відніманням – не групоїд.
3. Раціональні числа з операцією ділення – не групоїд, через нуль.

Півгрупа – групоїд з асоціативною операцією:

$G = \langle M, \circ \rangle$ – півгрупа $\Leftrightarrow$ $(a \circ b) \circ c = a \circ (b \circ c)$ $\forall\ a, b, c \in M$

Властивість – замкненість, асоціативність.
Приклади. 1. Цілі числа з відніманням – не півгрупа:
$(5-3)-1 \neq 5-(3-1)$
2. Множина слів в алфавіті A з операцією !! (конкатенація) – півгрупа: (a!!b)!!c = a!!(b!!c) = abc aaa!!b = aaab
3. Множина натуральних чисел з операцією додавання (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 якої при $\forall a_i$

$$e \cdot a_i = a_i; \quad a_i \cdot e = a_i$$

Властивість – наявність нейтрального елемента.

Приклади. 1. Множина слів A*, складених з алфавіту A (операція !!) разом з порожнім словом Λ – моноїд, без порожнього слова – не моноїд.
2. Множина невід'ємних цілих чисел з операцією додавання, тобто $\langle\{N \cup 0\}, +\rangle$ – моноїд.

Теорема. Моноїд має тільки один нейтральний елемент.

Група – Моноїд $G = \langle M, \circ \rangle$, в якому для кожного елемента існує обернений, тобто:

$$\forall a \in M \quad \exists \tilde{a} \,\middle|\, a \circ \tilde{a} = \tilde{a} \circ a = e$$

Приклади. 1. Множина невироджених квадратних матриць 2×2 (визначники яких не дорівнюють нулю) з операцією множення матриць.

2. Множина цілих чисел з адитивною операцією.

Теорема. Кожний елемент групи має тільки один обернений елемент.

Наслідки:

1. У групі однозначно вирішується рівняння $a \circ x = b$.
2. $c = a \circ b \quad \Rightarrow \quad \tilde{c} = \tilde{b} \circ \tilde{a}$
3. $a \circ b = a \circ c \quad \Rightarrow \quad b = c$
4. $\tilde{\tilde{a}} = a$

Комутативна або абелева група – група $G = \langle M, \circ \rangle$, операція якої комутативна, тобто:

$$\forall a, b \in M \quad \Rightarrow \quad a \circ b = b \circ a$$

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

2. M = {0, 1}, операція XOR (адитивна скінченна комут. 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. $\langle 2^M, \oplus \rangle$ – 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

2. Приклади розв’язання задач

1. Яку алгебраїчну систему утворюють парні цілі числа з адитивною операцією?

- Не входить до класифікації
- 1) Замкненість (4+2=6) Групоїд
- 2) Асоціативність (+) Півгрупа
- 3) Нейтральний елемент (e = 0) Моноїд
- 4) Обернений елемент (-6 + 6 = 0) Група
- 5) Комутативність (+) ***Абелева група***

2. Яку алгебраїчну систему утворюють парні цілі числа з мультиплікативною операцією?

- Не входить до класифікації
- 1) Замкненість($4 \times 2 = 8$) Групоїд
- 2) Асоціативність($\times$) ***Півгрупа***
- 3) Нейтральний елемент(e = 1 ???) Моноїд
- 4) Обернений елемент Група
- 5) Комутативність Абелева група

3. Яку алгебраїчну систему утворюють парні цілі числа з операцією віднімання?

- Не входить до класифікації
- 1) Замкненість(-4-2=-6) ***Групоїд***
- 2) Асоціативність (6-3-1≠6-(3-1)) Півгрупа
- 3) Нейтральний елемент Моноїд
- 4) Обернений елемент Група
- 5) Комутативність Абелева група

4. Яку алгебраїчну систему утворюють невід'ємні цілі числа (додатні та 0) з операцією віднімання?

- ***Не входить до класифікації***
- 1) Замкненість (4-6=-2???) Групоїд
- 2) Асоціативність Півгрупа
- 3) Нейтральний елемент Моноїд
- 4) Обернений елемент Група
- 5) Комутативність Абелева група

5. Яку алгебраїчну систему утворюють невід'ємні числа (додатні та 0) з адитивною операцією?

- Не входить до класифікації
- 1) Замкненість(4+6=10) Групоїд
- 2) Асоціативність(+) Півгрупа
- 3) Нейтральний елемент(e = 0) ***Моноїд***
- 4) Обернений елемент (5 + (-5) = 0) Група
- 5) Комутативність Абелева гр.

3. Приклади груп, які часто використовуються

3.1. Група переставлень S_n або симетрична група порядку n!

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

Запис елемента множини *A. Верхній рядок показує розташування елементів до переставлення, нижній – після переставлення, наприклад:*

(n = 3, M = {a, b, c}) $\begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$

Приклад множини A для $\boldsymbol{S_3}$: $A = \left\{ \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} \right\}$

Операція композиції*:* $\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} \circ \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}$

Це скінчена група з нейтральним елементом $\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}$ *, але не є абелевою.*

3.2. 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:

$$Z_n =_j \langle B, \oplus_n \rangle,\ B = (0,\ l,\ 2,\ \ldots,\ n-l),\ b_i \oplus_n b_j = (b + b)\, mod\ n.$$

***Особливість**: обернений елемент знаходиться за таким правилом:* $b_i^{-1} = n - b_i,$

тому що $b_i \oplus_n (n - b_i) = (b_i + n - b_i) \operatorname{mod} n = 0.$

Z_n є скінченою абелевою групою.

.

3.3. Група коренів рівняння $x^n = 1$

***Операція** – множення чисел (дійсних або комплексних).*

1) $n = 1$, *базова множина* $\{1\}$;
2) $n = 2$, *базова множина* $\{1, -1\}$;
3) $n = 5$, *базова множина* $\left\{1, e^{j\frac{2\pi}{5}}, e^{j\frac{2\pi}{5}\cdot 2}, e^{j\frac{2\pi}{5}\cdot 3}, e^{j\frac{2\pi}{5}\cdot 4}\right\}$.

Це скінчена абелева група.

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

Особливість *- кожний елемент групи є обернений сам до себе.*

Це скінчена абелева група.

3.5. Група багаточленів у двійковій системі числення

Операція *– додавання багаточленів за модулем 2.*

Розглянемо приклад для n = 3.

Базова множина $\{0, 1, x, x + 1, x^2 + 1, x^2 + x, x^2 + x + 1, x^3, x^3 + 1, x^3 + x, x^3 + x + 1, x^3 + x^2, x^3 + x^2 + 1, x^3 + x^2 + x, x^3 + x^2 + x + 1\}$;

Приклад операції додавання:

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

Особливість *- кожний елемент групи є обернений сам до себе.*

Це скінчена (або є варіант нескінченої) абелева група.