2 Алгебраїчні структури

2.1 Алгебраїчні операції та їх властивості

Операцією на множині S називається функція f, яка є відображенням виду $S^n \to S$, $n \in N$, де S^n — декартів добуток $S \times S \times ... \times S$.

Операція $S^n \to S$ має ***порядок n*** або є ***n-арною операцією***.

Операції виду $S \to S$ називають ***унарними***, а операції $S^2 \to S$ називають ***бінарними***.

Елементи упорядкованого набору з n елементів в області визначення S^n називають ***операндами***.

Приклад.

Операція нульового степеня – це константа.

Унарні операції: операція зміни знаку (-) на множині дійсних чисел R(-2,678; -56); операція піднесення до степеня на множині R: 56^2, 7^2.

Унарна операція в алгебрі множин: операція доповнення множин.

Приклад.

Бінарними операціями на множині дійсних чисел R є арифметичні операції — додавання, віднімання, множення, ділення (+, -, *, /).

В алгебрі множин бінарними є операції — об'єднання ($\cup$), перетин ($\cap$), різниця (\).

Існують три форми запису виразів — ***префіксна, інфіксна*** та ***постфіксна***.

У першому випадку оператор ставиться між операндами (***infix***), у другому — перед операндами (***prefix***) і у третьому — після операндів (***postfix***).

Префіксна нотація також відома як ***польська нотація***.

Постфіксну нотацію називають ще ***зворотний польський запис*** (зворотний бездужковий запис, польський інверсний запис (ПОЛІЗ).

Приклад. Три варіанти запису бінарної операції арифметичного виразу $a + b$.

infix: $a + b$,

prefix: $+ab$,

postfix: $ab+$.

Алгоритм обчислення значень виразу, що записаний у формі *postfix*:

1) при перегляді запису зліва направо виконується перша знайдена операція, якій безпосередньо передує достатня для неї кількість операндів;

2) на місці виконаної операції і використаних для цього операндів у рядок записується результат виконання операції;

3) повертаємося до кроку 1.

Приклад. Нехай є вираз у *infix*-формі:

$$1 + 2*3 +(4 + 5* (6 + 7)).$$

Результат переведення даного виразу до *postfix*:

$$1\ 2\ 3\ *\ +\ 4\ 5\ 6\ 7\ +\ *\ +\ +.$$

Обчислимо тепер значення виразу, використовуючи наведений алгоритм:

$$1\ \underline{2\ 3*}\ +\ 4\ 5\ 6\ 7\ +\ *\ +\ +\ =\ \underline{1\ 6\ +}\ 4\ 5\ 6\ 7\ +\ *\ +\ +\ =$$

$$=\ 7\ 4\ 5\ \underline{6\ 7\ +}\ *\ +\ +\ =\ 7\ 4\ \underline{5\ 13\ *}\ +\ +\ =\ 7\ \underline{4\ 65\ +}\ +\ =$$

$$=\ \underline{7\ 69\ +}\ =\ 76.$$

Символи $\otimes$ і $\oplus$ використовуються для позначення абстрактних бінарних операцій.

Таблиця, що задає деяку бінарну операцію $\otimes$ на деякій множині A, називається ***таблицею Келі***.

Приклад. Нехай операція $\otimes$ визначена на множині $\{a, b, c\}$ за допомогою таблиці

$\otimes$	a	b	c
a	a	a	b
b	b	a	c
c	a	b	b

Отже, $a \otimes b = a$, $b \otimes b = a$, $c \otimes b = b$, ...

Нехай дано множину A, на якій визначено деяку бінарну операцію $\otimes$.

Якщо $a \otimes b = b \otimes a$ для всіх a, $b \in A$, то стверджують, що бінарна операція $\otimes$ на множині A має властивість — ***комутативність***.

Якщо $(a \otimes b) \otimes c = a \otimes (b \otimes c)$ для всіх $a, b, c \in A$, то стверджують, що бінарна операція $\otimes$ на множині A має властивість — ***асоціативність***.

Нехай на множині A визначено дві бінарні операції $\otimes$ і $\oplus$.

Якщо для всіх $a, b, c \in A$ виконується $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$, то стверджують, що операція $\otimes$ має властивість — ***дистрибутивність*** відносно операції $\oplus$.

Приклад. Звичайна бінарна операція додавання (+) на множині дійсних чисел R комутативна і асоціативна, а операція віднімання (-) — некомутативна і неасоціативна, тобто

$a + b = b + a$, але $a - b \neq b - a$;

$(a + b) + c = a + (b + c)$, але $(a - b) - c \neq a - (b - c)$.

Приклад. На множині дійсних чисел R множення дистрибутивне відносно додавання, а додавання не дистрибутивне відносно множення, тобто

$a*(b + c) = a*b + a*c,\ \ (a + b)*c = a*c + b*c,$

але $a + (b * c) \neq (a + b) * (a + c)$.

Якщо для бінарної операції $\otimes$ на множині A існує елемент $e \in A$ такий, що для всіх $a \in A$

$$e \otimes a = a \otimes e = a,$$

тоді e називається ***одиницею*** (***нейтральним елементом***) відносно до операції $\otimes$.

Нехай $\otimes$ — операція на A з одиницею e і елементи $x, y \in A$ задовольняють рівності

$$x \otimes y = e = y \otimes x.$$

Тоді y називається ***оберненим*** (***симетричним***) ***елементом*** до x відносно операції $\otimes$, і x називається ***оберненим елементом*** до y відносно операції $\otimes$.

Іноді розрізняють ліві та праві одиниці ($e_{\text{лів.}} \otimes a = a$ або $a \otimes e_{\text{прав.}} = a$ для будь-якого $a \in A$) і ліві та праві обернені елементи, однак, у більшості випадків одиниці є двосторонніми.

У випадках, коли бінарна операція вважається аналогічною множенню (*), одиничний елемент позначається 1, а обернений до елемента x елемент записується у вигляді x^{-1}.

Коли бінарна операція вважається аналогічною додаванню (+), одиничний елемент позначається 0, а обернений до елемента x елемент записується у вигляді $-x$. Будемо також позначати обернений елемент до x як x'.

Приклад. На множині дійсних чисел R правою одиницею відносно віднімання та одиницею відносно додавання є 0, оскільки

$a - 0 = a$, але $0 - a \neq a$, якщо $a \neq 0$;

$a + 0 = a$ і $0 + a = a$ для всіх a.

В алгебрі множин для операції об'єднання $\cup$ одиничним елементом є порожня множина $\varnothing$, для операції перетину $\cap$ одиницею є універсальна множина U.

Нехай n — довільне натуральне число.

Додаванням за модулем n цілих чисел a і b (позначення: $\oplus_n$) називається алгебраїчна операція, результатом якої є залишок від ділення суми $a + b$ на n.

Множенням за модулем n чисел a і b (позначення: $\otimes_n$) називається алгебраїчна операція, результатом якої є залишок від ділення добутку $a * b$ на n.

Операції додавання та множення за модулем n визначені на множині цілих невід'ємних чисел $\mathbb{Z}^+$:

$a \oplus_n b = c$, так, що $a + b = k * n + c$, $0 \le c < n$; $a, b, k \in \mathbb{Z}^+$

$a \otimes_n b = d$, так, що $a * b = f * n + d$, $0 \le d < n$; $a, b, f \in \mathbb{Z}^+$

Областю значень цих операцій є множина цілих невід'ємних чисел, менших за n:

$$Z_n = \{0, 1, ..., n - 1\}.$$

Часто використовується позначення

$$a + b \equiv c \pmod{n}, \qquad a \times b \equiv d \pmod{n}$$

для додавання та множення за модулем n.

Приклади додавання та множення за модулем n:

$2 \oplus_3 2 = \text{Зал.}\ (4/3) = 1,$ $\qquad$ $2 \otimes_3 2 = \text{Зал.}\ (4/3) = 1,$

$2 \oplus_4 2 = \text{Зал.}\ (4/4) = 0,$ $\qquad$ $2 \otimes_4 2 = \text{Зал.}\ (4/4) = 0,$

$7 \oplus_{10} 8 = \text{Зал.}\ (15/10) = 5,$ $\qquad$ $7 \otimes_{10} 8 = \text{Зал.}\ (56/10) = 6,$

$7 \oplus_{12} 8 = \text{Зал.}\ (15/12) = 3,$ $\qquad$ $7 \otimes_{12} 8 = \text{Зал.}\ (56/12) = 8.$

2.2 Поняття алгебраїчної структури. Найпростіші алгебраїчні структури

2.2.1 Поняття алгебраїчної структури

Алгебраїчною структурою $< S, O >$ називається множина разом із заданими операціями, визначеними і замкненими на цій множині.

Ця множина називається ***носієм алгебраїчної структури***.

Приклад. Алгебраїчна структура з операцією додавання на множині N натуральних чисел позначається $<N, +>$.

Приклад. Множина $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$ разом із звичайною операцією додавання (+) не буде алгебраїчною структурою, оскільки результат виконання операції може не належати множині Z_7, наприклад, $6 + 3 = 9$, $9 \notin Z_7$. Але $<Z_7, \oplus_7>$ є алгебраїчною структурою, оскільки область значень операції $\oplus_7$ лежить у Z_7.

Відношення між алгебраїчними структурами

Структура $S' = \langle A', \oplus' \rangle$ є ***підструктурою*** алгебраїчної структури $S = \langle A, \oplus \rangle$, якщо:

1. $A' \subseteq A$

2. $\oplus'$ і $\oplus$ операції одного порядку і звуження операції $\oplus$ на підмножині A' співпадає з операцією $\oplus'$ (наприклад, $a \oplus b = a \oplus' b$ для всіх $a, b \in A'$).

Найбільшою підструктурою структури S є сама структура S. У деяких випадках інших підструктур може не бути.

Приклад. Нехай E — множина парних натуральних чисел, тоді $<E, +>$ буде підструктурою структури $<N, +>$, де N — множина натуральних чисел.

2.2.2 Найпростіші алгебраїчні структури

Структури з однією операцією

Півгрупою називається алгебраїчна структура з множиною-носієм A і бінарною операцією $\otimes$: $A^2 \to A$, яка задовольняє властивості асоціативності:

$$x \otimes (y \otimes z) = (x \otimes y) \otimes z; \qquad x, y, z \in A.$$

Приклад. При обробці рядків символів використовується операція конкатенації $\alpha \bullet \beta = \alpha\beta$. Візьмемо рядки: «пар», «о», «воз». Застосувавши операції конкатенації, одержуємо такі рядки:

«пар»•«о» = «паро»; «паро»•«воз» = «паровоз».

Ця операція асоціативна, оскільки

(«пар»•«о»)•«воз» = «пар»•(«о»•«воз») = «паровоз».

Отже, $<A^+, \bullet>$ є півгрупою, де A^+ — множина різних рядків, що складаються з букв українського алфавіту.

Моноїдом називають алгебраїчну структуру з множиною-носієм M і бінарною операцією $\otimes$: $M^2 \to M$ такою, що

1. $\otimes$ асоціативна:

$$x \otimes (y \otimes z) = (x \otimes y) \otimes z, \quad \text{для всіх } x, y, z \in M.$$

2. Існує $e \in M$ — одиниця відносно $\otimes$:

$$e \otimes x = x = x \otimes e \quad \text{для всіх } x \in M.$$

Моноїд — це півгрупа з одиницею.

Приклад. Якщо позначимо через A^* множину довільних рядків, що складаються з букв українського алфавіту і порожнього рядку ε=«», то одержимо структуру $<A^*, \bullet>$, яка є моноїдом з одиничним елементом ε.

«паровоз» • «» = «» • «паровоз» = «паровоз»

Групою називають множину G з бінарною операцією $\otimes$, що замкнена в G, такою, що

1. $\otimes$ асоціативна:

$x \otimes (y \otimes z) = (x \otimes y) \otimes z$, для всіх $x, y, z \in G$.

2. Існує $e \in G$ — одиниця відносно $\otimes$:

$e \otimes x = x = x \otimes e$ для всіх $x \in G$.

3. Кожному елементу $x \in G$ відповідає обернений елемент $x' \in G$ відносно $\otimes$: $x' \otimes x = x \otimes x' = e$ для всіх $x \in G$.

Комутативна група називається ***абелевою групою***.

Приклад. Групою є множина дійсних чисел разом з операцією додавання: $<R, +>$, підгрупою цієї групи є $<Z, +>$, де Z — множина цілих чисел.

Структура $<K, +>$, де K — множина цілих чисел, що кратні k, $k \in N$, є підгрупою групи $<Z, +>$. Для цих груп одиницею є 0, обернений елемент утворюється за допомогою застосування унарної операції зміни знака «-». Наведені групи є абелевими групами, оскільки додавання комутативне.

Приклад. Структура $<N, +>$, де N – множина натуральних чисел, не є групою, оскільки не існує обернених елементів і одиниці.

$<N, +>$ – півгрупа.

Приклад. Структури $<R, *>$ і $<N, *>$ не є групами, а є моноїдами. Одиничним елементом для операції множення є 1. Обернені елементи існують на множині дійсних чисел R для всіх елементів, крім 0: не існує 0^{-1}, такого, що

$$0 * 0^{-1} = 1.$$

Таким чином, операція множення задає групу на множині дійсних чисел, крім нуля $<R\backslash\{0\}, *>$.

Додатна підмножина множини дійсних чисел з операцією множення $<R_+, *>$ теж є групою – підгрупою групи $<R\backslash\{0\}, *>$.

Приклад. Позначимо $M_n(R)$ множину всіх квадратних матриць порядку n з елементами з множини дійсних чисел.

Структура $<M_n(R), +>$ – комутативний моноїд з одиницею — нульовою матрицею.

Структура $<M_n(R), *>$ – некомутативний моноїд з одиницею — одиничною матрицею.

Приклад. Структура $\langle Z_n, \otimes_n \rangle$ – група з одиницею 0 і оберненим елементом $x' = n - x$;

$\langle Z_n, \otimes_n \rangle$ — моноїд з одиницею 1.

Твердження 1. Нехай $\otimes$ — операція на множині A й існує одиниця e відносно $\otimes$, тоді ***одиничний елемент єдиний***.

Твердження 2. Нехай $\otimes$ — асоціативна операція на множині A і e — одиниця відносно $\otimes$. Тоді, якщо $x \in A$ і x має обернений елемент, то ***обернений елемент єдиний*** відносно $\otimes$.

Структури з двома операціями

Операцію $\otimes$ називають множенням, а операцію $\oplus$ — додаванням.

Для $\otimes$ одиничний елемент позначається 1, а обернений до елемента x відносно $\otimes$ записується у вигляді x^{-1}.

Для $\oplus$ одиничний елемент позначається 0, а обернений до елемента x відносно $\oplus$ записується у вигляді $-x$.

Кільцем $<R, \{\otimes, \oplus\}>$ називається множина R з визначеними на ній бінарними операціями $\otimes$ і $\oplus$:

1. $\oplus$ асоціативна:

$x \oplus (y \oplus z) = (x \oplus y) \oplus z$, для всіх $x, y, z \in R$.

2. $\oplus$ комутативна:

$$x \oplus y = y \oplus x \quad \text{для всіх} \quad x, y \in R.$$

3. $\oplus$ має одиницю, яка називається нулем і позначається 0:

$$0 \oplus x = x \quad \text{для всіх} \quad x \in R.$$

4. Існує обернений елемент відносно $\oplus$ для кожного $x \in R$:

$$(-x) \oplus x = x \oplus (-x) = 0 \quad \text{для всіх } x \in R.$$

5. $\otimes$ асоціативна:

$$x \otimes (y \otimes z) = (x \otimes y) \otimes z \quad \text{для всіх } x, y, z \in R.$$

6. $\otimes$ дистрибутивна відносно $\oplus$ зліва і справа:

$$x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z),$$

$$(x \oplus y) \otimes z = (x \otimes z) \oplus (y \otimes z) \quad \text{для всіх } x, y, z \in R.$$

Кільце комутативне, якщо множення $\otimes$ комутативне і є ***кільцем з одиницею***, якщо існує одиниця відносно множення.

Кільце з одиницею називається ***алгеброю***.

В кільці $<R, \oplus, \otimes>$ для будь-яких $a, b \in R$ виконуються співвідношення

$$0 \otimes a = a \otimes 0 = 0,$$

$$a \otimes (-b) = (-a) \otimes b = -(a \otimes b),$$

$$(-a) \otimes (-b) = a \otimes b.$$

В кільці $<R, \oplus, \otimes>$ фактично присутня некомутативна бінарна операція віднімання Θ, визначена за правилом $a \Theta b = a \oplus (-b)$. Вона є правою оберненою відносно додавання в тому розумінні, що $(a \oplus b) \Theta b = a$.

Поле $<R, \oplus, \otimes>$ — це комутативне кільце з одиницею 1 (що відрізняється від 0), в якому кожний елемент a (що відрізняється від 0) обернений за множенням.

Структуру $<R, *, +>$ називають ***полем дійсних чисел***.

2.3 Ґратки

2.3.1 Основні означення

Ґратками називається частково впорядкована множина, в якій два елемента x та y мають точну нижню межу, яка називається **перетином** (позначається $x \wedge y$), та точну верхню межу, яка називається **об'єднанням** (позначається $x \vee y$).

Ґратки називаються **повними**, якщо будь-яка їх підмножина має точні верхні та нижні межі.

Лема 1. Будь-який ланцюг є ґратками, в яких $x \wedge y$ співпадає з найменшим, а $x \vee y$ – з найбільшим із елементів x та y.

Приклад. Будь-яку абсолютно впорядковану множину можна перетворити на ґратки, означивши для будь-яких елементів x та y

$$x \wedge y = min(x, y), \quad x \vee y = max(x, y).$$

Приклад. Система підмножин будь-якої множини A (булеан A) – частково впорядкована множина за включенням множин. Ця система є ґратками, елементами яких є множини, а операціями – звичайні теоретико-множинні операції об’єднання та перерізу.

Приклад. Впорядкована множина раціональних чисел не є повними ґратками, тому що в ній немає універсальних меж 0 та 1.

У впорядкованій множині дійсних чисел умова повноти буде виконуватись, якщо додати до неї в якості універсальних меж $-\infty$ та $+\infty$.

Підґратками ґраток L називається підмножина $X \subset L$ така, що якщо $a \in X$, $b \in X$, то $a \wedge b \in X$ та $a \vee b \in X$.

Порожня підмножина та будь-яка одноелементна підмножина є підґратками.

Приклад. Підмножина $Y = \{\varnothing, \{b\}, \{c\}, \{b,c\}\}$ є підґратками.

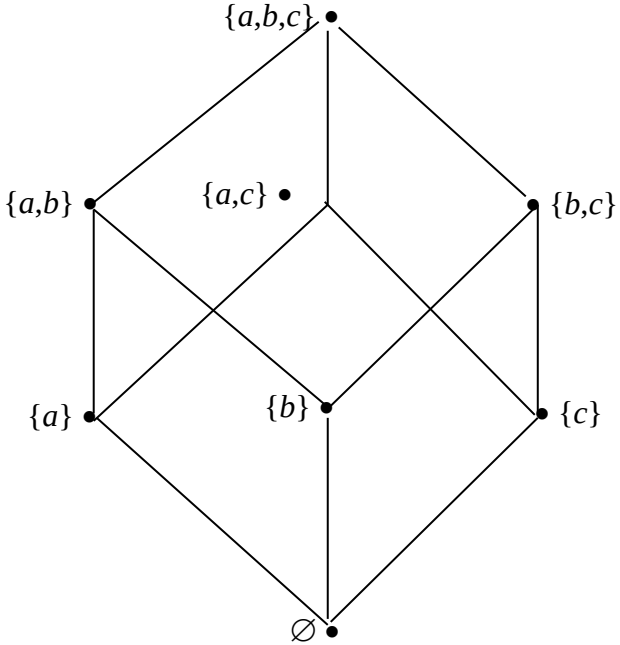
Підмножина $Z = \{\varnothing, \{a\}, \{a,b\}, \{a,c\}, \{c\}\}$ не є підґратками, тому що $\{a,b\} \vee \{a,c\} = \{a,b,c\} \notin Z$. Ця підмножина також не є інтервалом.

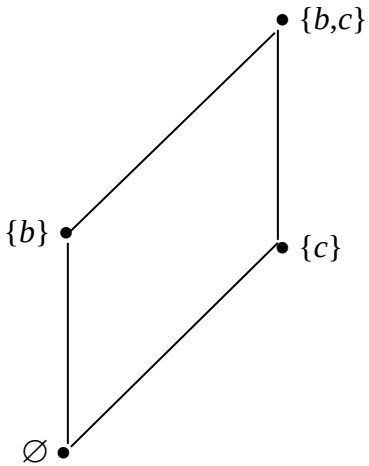
Підґратками будуть також підмножини:

$\{\varnothing, \{a\}\}, \{\{c\}, \{a,c\}\}, \{\{a\}, \{a,b\}\}$ і т.д.,

всі ланцюги, наприклад, $\{\varnothing, \{b\}\}, \{\varnothing, \{b\}, \{b,c\}\}$,

а також всі елементи ґраток.


{a,b,c}
{a,b}
{a,c}
{b,c}
{a}
{b}
{c}
∅


{b,c}
{b}
{c}
∅

2.3.2 Булеві ґратки

У повних ґратках елемент a' називається **доповненням** елемента a, якщо $a \wedge a' = 0$ та $a \vee a' = 1$.

Якщо кожний елемент ґраток має доповнення, то ґратки називаються ґратками із доповненням.

Дистрибутивні ґратки з доповненням називаються **булевими**.

Теорема 1. У булевих ґратках довільний елемент x має одне й тільки одне доповнення x'. При цьому виконується:

1) інволюція: $(x')' = x$,

2) межі доповнюють одна одну: $1' = 0$, $0' = 1$,

3) виконуються закони де Моргана:

$$(x \wedge y)' = x' \vee y', \; (x \vee y)' = x' \wedge y'.$$

Булевою алгеброю $B = \langle L, \vee, \wedge, ', 0, 1 \rangle$ називається алгебра з двома булевими операціями $\vee$ та $\wedge$, однією унарною операцією $'$ та двома нульарними операціями (константами) 0 та 1, для яких виконуються:

1. $a \vee a = a$, $a \wedge a = a$;	самопоглинання
2. $a \vee b = b \vee a$, $a \wedge b = b \wedge a$	комутативність
3. $a \vee (b \vee c) = (a \vee b) \vee c$, $a \wedge (b \wedge c) = (a \wedge b) \wedge c$	асоціативність

4. $(a \wedge b) \vee a = a$, $(a \vee b) \wedge a = a$	поглинання
5. $a \vee (b \wedge c) = (a \wedge b) \vee (a \wedge c)$	дистрибутивність
$a \wedge (b \vee c) = (a \vee b) \wedge (a \vee c)$	
6. $a \vee 1 = 1$, $a \wedge 0 = 0$	властивості 0 та 1
$a \vee 0 = a$, $a \wedge 1 = a$	
7. $(a')' = a$	властивості доповнення
8. $(a \wedge b)' = a' \vee b'$, $(a \vee b)' = a' \wedge b'$	закони де Моргана
9. $a \vee a' = 1$, $a \wedge a' = 0$	існування доповнення

Приклад. $\langle P(M); \cup, \cap, ' \rangle$ – булева алгебра, причому M – верхня межа, $\varnothing$ – нижня межа, "$\subset$" – природній частковий порядок.

Приклад. $\langle \{0, 1\}; \wedge, \vee, \neg \rangle$ – булева алгебра, причому 1 – верхня межа, 0 – нижня межа.

Приклад. Будь-яке поле множин і, зокрема, множина всіх підмножин деякої множини є булевою алгеброю. Довільна підалгебра булевої алгебри сама також є булевою алгеброю. Прямий (декартовий) добуток булевих алгебр є булевою алгеброю.