2 Алгебраїчні структури

Поняття алгебраїчної структури включає визначену множину об'єктів та операцій над цими об'єктами. Оскільки практично в будь-якій задачі обробки даних за допомогою комп'ютера виділяється множина самих даних і операції, які застосовні до цих даних, очевидно, що при цьому формуються визначені алгебраїчні структури. Ми вже знайомі з алгебраїчними структурами на множині натуральних, цілих і дійсних чисел, на множинах та відношеннях. Розглянемо такі алгебраїчні структури, як півгрупи, моноїди і групи, що, зокрема, використовуються для перетворення рядків символів і беруть участь у формуванні більш складних структур – кілець і полів. Ці поняття є базовими для загальної та лінійної алгебри, використовуються під час роботи з матрицями, при кодуванні інформації та обробці даних.

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 $S \times S \times ... \times S$.

У цьому визначенні є два важливих моменти. По-перше, оскільки операція є функцією, то результат застосування операції визначено однозначно. Тому даний упорядкований набір з n елементів множини S функція f переводить тільки в один елемент із S. По-друге, операція замкнена на S у тому розумінні, що область визначення та область значень операції лежать у S^n і S відповідно.

Стверджують, що операція $S^n \to S$ має ***порядок n*** або є ***n-арною операцією***. Частіше зустрічається ситуація, коли порядок дорівнює 1 або 2. 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***. Операції зазвичай позначають символами, що називають ***операторами***. У випадку унарних операцій символ оператора ставлять перед або над операндом.

Приклад. Операція нульового степеня – це константа. Прикладами унарних операцій є операція зміни знаку (-) на множині дійсних чисел R(-2,678; -56), операція піднесення до степеня (наприклад, до квадрату) на множині R: 56^2, 7^2. В алгебрі множин прикладом унарної операції є операція доповнення множин. 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 (\).

Операції записують одним з трьох способів. У першому випадку оператор ставиться між операндами (***infix***), у другому — перед операндами (***prefix***) і у третьому — після операндів (***postfix***). Отже, існують три форми запису виразів — ***інфіксна, префіксна*** та ***постфіксна***.

Загальноприйнятий запис арифметичних виразів являє приклад інфіксного запису. Запис математичних функцій і функцій у мовах програмування є префіксним (інші приклади префіксного запису – команди ассемблера, тріади і тетради). Постфіксний запис у повсякденному житті зустрічається рідко. З ним зіштовхуються тільки користувачі стекових калькуляторів і програмісти мовою Forth.

Префіксна нотація також відома як ***польська нотація***. Польську нотацію запропонував у 1924 році польський логік Ян Лукашевич з метою спрощення логіки висловлень. Постфіксну нотацію називають ще ***зворотний польський запис*** (зворотний бездужковий запис, польський інверсний запис (ПОЛІЗ).

Розглянемо три варіанти запису бінарної операції арифметичного виразу $a + b$.

infix: $a + b$,
prefix: $+ab$,
postfix: $ab+$.

Відповідно до більшості математичних текстів ми будемо використовувати позначення *infix*. Форми запису *postfix* і *prefix* мають ту перевагу, що не потребують дужок при визначенні порядку обчислень складних виразів, і це робить їх особливо зручними для автоматичної обробки. Вони часто використовуються для представлення виразів у пам'яті комп'ютера. Розглянемо їх докладніше на прикладі *postfix*.

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

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, який у стандартній звичній для нас *infix*-формі виглядає так:

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

Результат переведення його до *postfix* буде таким:

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

Обчислимо тепер значення виразу, використовуючи наведений алгоритм:

$$1\ \underline{2\ 3*}\ +\ 4\ 5\ 6\ 7\ +\ *\ +\ +\ =\ \underline{1\ 6\ +}\ 4\ 5\ 6\ 7\ +\ *\ +\ +\ =$$
$$=\ 7\ 4\ 5\ \underline{6\ 7\ +}\ *\ +\ +\ =\ 7\ 4\ \underline{5\ 13\ *}\ +\ +\ =\ 7\ \underline{4\ 65\ +}\ +\ =$$
$$=\ \underline{7\ 69\ +}\ =\ 76.$$

Крім стандартних відомих нам операцій (наприклад, +, -, *), існує багато інших. Будемо використовувати символи $\otimes$ і $\oplus$ для позначення абстрактних

бінарних операцій. Інакше кажучи, символи $\otimes$ і $\oplus$ використовуються як змінні для позначення будь-яких операцій.

Бінарні операції, визначені на скінченних множинах, зручніше задавати за допомогою таблиць. Таблиця, що задає деяку бінарну операцію $\otimes$ на деякій множині A, називається ***таблицею Келі***, її рядки та стовпці нумеруються елементами множини A, а елементом таблиці, що стоїть на перетині рядку a_i і стовпця a_j є елемент $a_k = a_i \otimes a_j$.

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

Очевидно, що використання таблиць має велике значення, оскільки деякі операції, з якими доводиться мати справу в комп'ютерній математиці, не придатні для словесного завдання.

Наведемо важливі властивості, які можуть мати операції.

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 $\oplus$.

Зауважимо, що у визначенні асоціативності порядок операндів a, b і c збережено (операція може бути некомутативною) і використано круглі дужки, щоб вказати порядок виконання операцій. Таким чином, вираз $(a \otimes b) \otimes c$ потребує, щоб спочатку обчислювалося $a \otimes b$ і потім результат цього (скажімо, x) брав участь в операції $x \otimes c$ як перший операнд. Якщо операція асоціативна, то порядок обчислень несуттєвий і, отже, дужки не потребуються.

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 $(a - b) - c \neq a - (b - c)$.

Крім того, 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 $a + (b * c) \neq (a + b) * (a + c)$.

Для розв'язання рівнянь відносно кожної операції у множині-носії алгебраїчної структури виділяється особливий елемент, що називається одиничним елементом.

Якщо для бінарної операції $\otimes$ на множині A існує елемент $e \in A$ такий, що для всіх $a \in A$ $\quad e \otimes a = a \otimes e = a$, 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, як у нашому визначені.

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'.

Приклади одиниць і обернених елементів. 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.

Для подальшого необхідно визначити операції додавання та множення за модулем n на множині цілих чисел.

Нехай n — довільне натуральне число.

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

Множенням за модулем n чисел a і b називається алгебраїчна операція, результатом якої є залишок від ділення добутку $a * b$ на n.

Ці операції (позначимо їх $\otimes_n$ і $\oplus_n$) 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, позначимо її Z_n, $Z_n = \{0, 1, ..., n - 1\}$. Часто використовується позначення

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

для додавання та множення за модулем n.

Приклад. Наведемо приклади додавання та множення за модулем n.

$2 \oplus_3 2 =$ Зал. $(4/3) = 1$, $2 \otimes_3 2 =$ Зал. $(4/3) = 1$,

$2 \oplus_4 2 =$ Зал. $(4/4) = 0$, $2 \otimes_4 2 =$ Зал. $(4/4) = 0$,

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

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