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 $S' = <A', \oplus'>$ є ***підструктурою*** алгебраїчної структури $S = <A, \oplus>$, якщо:

1. $A' \subseteq A$
2. $\oplus'$ і $\oplus$ операції одного порядку і звуження операції $\oplus$ на підмножині A' співпадає з операцією $\oplus'$ (наприклад, для бінарних операцій $a \oplus b = a \oplus' b$ 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».

Очевидно, що 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 $\otimes$:

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

Таким чином, 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 $\langle A^*, \bullet\rangle$, 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:

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

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

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

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

Часто до слів «група» і «моноїд» приписують термін «комутативний». Це означає, що операція у розглянутій структурі задовольняє властивість комутативності, тобто $y \otimes x = x \otimes y$ для всіх $x, y \in M$ або G.

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

Приклади. 1. Групою є множина дійсних чисел разом з операцією додавання: $\langle R, +\rangle$, підгрупою цієї групи є $\langle Z, +\rangle$, де Z — множина цілих чисел.

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

2. Структура $\langle N, +\rangle$, де N – множина натуральних чисел, не є групою, оскільки не існує обернених елементів і одиниці. Насправді, $\langle N, +\rangle$ – півгрупа.

3. Структури $\langle R, *\rangle$ і $\langle N, *\rangle$ 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 $\langle R\setminus\{0\}, *\rangle$.

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

Множення комутативне, отже, ці групи є абелевими.

4. 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.

5. Структура $<Z_n, \otimes_n>$ – група з одиницею 0 і оберненим елементом $x' = n - x$; $<Z_n, \otimes_n>$ — 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

Розглянемо алгебраїчні структури з двома бінарними операціями $\otimes$ і $\oplus$. 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 $-x$. Зрозуміло, що для різних структур ці операції визначаються по-різному, хоча часто називаються однаково.

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

1. $\oplus$ асоціативна:
$$x \oplus (y \oplus z) = (x \oplus y) \oplus z, \quad \text{для всіх } x, y, z \in R.$$
2. $\oplus$ комутативна:
$$x \oplus y = y \oplus x \quad \text{для всіх } x, y \in R.$$
3. $\oplus$ має одиницю, яка називається нулем і позначається 0:
$$0 \oplus x = x \quad \text{для всіх } x \in R.$$
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:
$$x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z),$$
$$(x \oplus y) \otimes z = (x \otimes z) \oplus (y \otimes z) \quad \text{для всіх } x, y, z \in R.$$

Будемо вважати, що ***кільце комутативне***, якщо множення $\otimes$ комутативне і є ***кільцем з одиницею***, якщо існує одиниця відносно множення. Кільце з одиницею називається ***алгеброю***. Зазвичай її позначають символом 1.

Легко показати, що 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 $(a \oplus b) \,\Theta\, b = a$. Дійсно,

$$(a \oplus b) \,\Theta\, b = (a \oplus b) \oplus (-b) = a \oplus b \oplus (-b) = a \oplus 0 = a.$$

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***.