Розділ II. Алгебри

Тема 6. Алгебри

Словом “алгебра” позначають, взагалі, не тільки розділ математики, але й один із конкретних об’єктів, які вивчаються в цьому розділі.

Алгебраїчні методи опису моделей знаходять широке застосування при формалізації різних предметних галузей. Інакше кажучи, при побудові предметної галузі все починається із введення позначень для операцій і відношень із наступним вивченням їх властивостей. Володіння алгебраїчною термінологією, таким чином, входить у арсенал засобів, необхідних для абстрактного моделювання, яке передує будь-яким практичним впровадженням у конкретній предметній галузі.

6.1. Композиція об’єктів

У математиці та її застосуваннях велике значення мають відношення, що ставлять у відповідність парі яких-небудь об’єктів (a, b) третій об’єкт c, тобто тернарні відношення, наприклад, дії над числами. Загалом тернарні відношення можуть бути не тільки між числами, а й між об’єктами різної природи. При цьому запис $a\perp b = c$ означає, що a в композиції з b дає c, де $\perp$ - **операція**; a, b – **операнди**; c – результат операції або композиції об’єктів a і b.

Позначимо множини операндів A та B ($a\in A$, $b\in B$) і множину результатів операції C ($c\in C$); тоді операцію (композицію) можна означити як відображення $A\times B \to C$. Її часто називають **законом композиції**.

Будь-який закон композиції $A\times B \to C$ над скінченними множинами можна задавати прямокутною матрицею (таблицею Келі):

	b_1	b_2	b_3	…
a_1	c_{11}	c_{12}	c_{13}	…
a_2	c_{21}	c_{22}	c_{23}	…
a_3	c_{31}	c_{32}	c_{33}	…
…	…	…	…	…

Тут рядки – це елементи множини A, стовпці – елементи множини B. На перетині рядка та стовпця, що відповідають (a_i, b_j), розташовується елемент $c_{ij} = a_i\perp b_j$.

Множини A, B, C, які беруть участь в операції $A\times B \to C$, не обов’язково мають бути різними. Якщо $A = B = C = S$, то кажуть, що закон композиції означений на множині S. Розрізняють внутрішній закон композиції $S\times S \to S$ і зовнішній $Q\times S \to S$, де Q й S – різні множини ($Q \neq S$).

У разі внутрішнього закону композиції кажуть, що множина утворює **групоїд** відносно операції $\perp$. У разі зовнішнього закону композиції операнди $a\in Q$ називаються **операторами**, а Q – множиною операторів на множині S. Наприклад, множина дійсних чисел утворює групоїд відносно операції “+” та “×”, множина всіх векторів на площині – групоїд відносно операції геометричного підсумовування.

Прикладами зовнішнього закону композиції можуть бути добуток вектора на скаляр на множині векторів, причому операторами є скаляри – елементи з R.

Скінченний групоїд S відносно закону $\perp$ визначається таблицею Келі, тобто квадратною матрицею n-го порядку, де n – число елементів групоїда.

Наприклад, таблиця Келі для групоїда $S = \{a, b, c, d\}$ відносно деякої операції $\perp$ може мати такий вигляд:

	a	b	c	d
a	a	b	a	b
b	a	b	c	a
c	b	a	d	d
d	d	b	d	b

6.2. Означення алгебри. Замкнення

Означення 6.1. Якщо справджується внутрішній закон композиції $S^n \to S$, то функцію типу φ: $S^n \to S$ будемо називати ***n*-арною операцією** на множині S; n – **арність** операції φ. Множина S разом із заданою на ній сукупністю операції $\Sigma = \{\varphi_1, \ldots, \varphi_m\}$, тобто система $A = \{S; \Sigma\}$ (або $A = \{S; \varphi_1, \ldots, \varphi_m\}$), називається **алгеброю**; S – **основою** або **носієм** алгебри A. Вектор арностей операцій алгебри є її **типом**, сукупність операції Σ - **сигнатурою**.

Алгебра, таким чином, записується як $\langle S; \Sigma\rangle$ або $\langle S; \varphi_1, \ldots, \varphi_m\rangle$. Операції φ_i скінченномісні, сигнатура Σ скінченна. Носій не обов'язково скінченний, але не порожній.

Часто використовується наступне узагальнене означення алгебри. Нехай $S = \{S_1, \ldots, S_n\}$ – множина носіїв, $\Sigma = \{\varphi_1, \ldots, \varphi_m\}$ – сигнатура, де φ_i: $S_{i1} \times \ldots \times S_{in} \to S_j$. Тоді $\langle S; \Sigma\rangle$ називається **багатоосновною** алгеброю. Іншими словами, багатоосновна алгебра має декілька носіїв, а операції сигнатури діють із прямого добутку деяких носіїв на деякий носій.

Означення 6.2. Підмножина $X \subset S$ називається **замкненою** відносно операції φ, якщо

$$\forall x_1, \ldots, x_n \in X \mid \varphi(x_1, \ldots, x_n) \in X.$$

Якщо X замкнена відносно всіх $\varphi \in \Sigma$, то $\langle X; \Sigma_X\rangle$ називається **підалгеброю** $\langle S; \Sigma\rangle$, де Σ_X – множина операцій $\varphi_1, \ldots, \varphi_m$, які розглядаються як операції над X.

Наприклад, множина дійсних чисел з операціями додавання і добутку $\langle R; +, \times\rangle$ – алгебра. Обидві операції є бінарними, тому тип цієї алгебри (2, 2). Усі скінченні підмножини R, крім $\{0\}$, - не замкнені відносно обох операції. Підалгеброю цієї алгебри є, наприклад, множина раціональних чисел із тими самим операціями $\langle Q; +, \times\rangle$.

Алгебра $B = \langle P(U); \cup, \cap, \bar{\ }\rangle$ називається булевою алгеброю множин над U. Її тип (2, 2, 1). Елементами основи цієї алгебри є множини (підмножини U). Для будь-якого $X \subset U$ $C = \langle P(X); \cup, \cap, \bar{\ }\rangle$ є підалгеброю B. Наприклад, якщо $U = \{a, b, c, d\}$, то основа алгебри B містить 16 елементів; алгебра $\langle P(\{a, c\}); \cup, \cap, \bar{\ }\rangle$ - підалгебра B, її основа містить чотири елементи.

Алгебра гладких функцій $\langle\{ f \mid f\colon R \to R\}; \frac{d}{dx}\rangle$, де $\frac{d}{dx}$ - операція диференціювання. Множина елементарних функцій є замкненою відносно диференціювання, оскільки похідні елементарних функції – елементарні й, отже, утворює підалгебру цієї алгебри.

Розглянемо квадрат із вершинами в точках a_1, a_2, a_3, a_4, занумерованих проти руху стрілки годинника, і повороти квадрата навколо центра в тому самому напрямку, що переводять вершини у вершини. Таких поворотів є нескінченна множина: на кути 0, $\pi/2$, π, $3\pi/2$, 2π, $5\pi/2, \ldots$, однак вони задають усього чотири різних відображення множини вершин у себе, які відповідають першим чотирьом поворотам. Таким чином, маємо алгебру з основою $\{a_1, a_2, a_3, a_4\}$ та чотирма унарними операціями $\alpha, \beta, \gamma, \delta$. Їх можна задати у вигляді таблиці:

	α	β	γ	δ
a_1	a_1	a_2	a_3	a_4
a_2	a_2	a_3	a_4	a_1
a_3	a_3	a_4	a_1	a_2
a_4	a_4	a_1	a_2	a_3

Операція α, що відображає будь-який елемент у себе, називається тотожною. Вона відповідає нульовому повороту. Підалгебр у цій алгебрі немає.

Теорема 6.1. Непорожній переріз підалгебр утворює підалгебру.

Доведення. Нехай $\langle X_i; \Sigma_{Xi}\rangle$ - підалгебра $\langle S; \Sigma\rangle$. Тоді

$$\forall i, j\ \varphi_j^{X_i}(x_1,\ldots,x_{n_j}) \in X_i \Rightarrow \forall j\ \varphi_j^{X_i}(x_1,\ldots,x_{n_j}) \in \bigcap X_i\ .\blacktriangleright$$

Означення 6.3. **Замкнення множини** $X \subset S$ відносно сигнатури Σ (позначається $[X]_\Sigma$) називається множина всіх елементів (включаючи самі елементи X), які можна отримати з X, застосовуючи операції з Σ. Якщо сигнатура зрозуміла, то її можна не вказувати.

Наприклад, в алгебрі цілих чисел $\langle Z; +, \times\rangle$ замиканням числа 2 є парні числа, тобто $[\{2\}] = \{n \in Z \mid n = 2k, k \in Z\}$.

Властивості замкнення:

1. $X \subset Y \Rightarrow [X] \subset [Y]$
2. $X \subset [X]$
3. $[[X]] = [X]$
4. $[X] \cup [Y] \subset [X \cup Y]$

Нехай $A = \langle S; \Sigma\rangle$ - деяка алгебра і $X_1,\ldots,X_n \subset S$ – деякі підмножини носія, а $\varphi \in \Sigma$ – одна з операцій алгебри. Тоді використовується наступна угода про позначення:

$$\varphi(X_1, \ldots, X_n) \equiv \{\varphi(x_1, \ldots, x_n) \mid x_1 \in X_1, \ldots, x_n \in X_n\},$$

тобто алгебраїчні операції можна використовувати не тільки до окремих елементів, але й до множин (підмножин носія), отримуючи, відповідно, не окремі елементи, а множини (підмножини носія).

Означення 6.4. Множина $X \subset S$ називається **системою твірних** алгебри $\langle S; \Sigma\rangle$, якщо $[X]_\Sigma = S$. Якщо алгебра має скінченну систему твірних, то вона називається **скінченно-породженою**. Нескінченні алгебри можуть мати скінченні системи твірних.

Наприклад, алгебра натуральних чисел $\langle N; +\rangle$ має скінченну систему твірних $1 \in N$.

6.3. Властивості операцій

Деякі властивості операцій мають спеціальні назви. Нехай задана алгебра $\langle S; \Sigma\rangle$ і $a, b, c \in S$; $\lozenge, \perp \in \Sigma$; $\lozenge, \perp: S \times S \to S$. Тоді

1. Асоціативність: $(a \perp b) \perp c = a \perp (b \perp c)$.
2. Комутативність: $a \perp b = b \perp a$
3. Дистрибутивність зліва: $a \lozenge (b \perp c) = (a \lozenge b) \perp (a \lozenge c)$.
4. Дистрибутивність справа: $(a \perp b) \lozenge c = (a \lozenge c) \perp (b \lozenge c)$.
5. Поглинання: $(a \perp b) \lozenge a = a$.
6. Ідемпотентність (самопоглинання): $a \perp a = a$.

Прикладами асоціативних операції є операція добутку та додавання чисел, об'єднання та переріз множин, композиція відношень. Неасоціативні операції: піднесення у степінь, віднімання множин.

Комутативні операції: добуток та додавання чисел, об'єднання та переріз множин. Не комутативні операції: добуток матриць, композиція відношень, піднесення у степінь.

Дистрибутивні операції: добуток відносно додавання чисел. Не дистрибутивні операції: піднесення у степінь дистрибутивно справа, але не зліва: $(\{ab\}^c = a^c b^c$, $a^{bc} \neq a^b a^c)$.

Переріз поглинає об'єднання, об'єднання поглинає переріз. Добуток та додавання не поглинають один одного.

Ідемпотентні операції: об'єднання та переріз множин. Не ідемпонентні операції: добуток та додавання чисел.

6.4. Гомоморфізм та ізоморфізм алгебр

Алгебри з різними типами, очевидно, мають істотно різну будову. Якщо ж алгебри мають однаковий тип, то наявність у них подібності характеризується за допомогою понять гомоморфізму й ізоморфізму.

Означення 6.5. Нехай є дві алгебри $A = \langle S; \varphi_1,\ldots,\varphi_m\rangle$ та $B = \langle T; \psi_1,\ldots, \psi_m\rangle$ однакового типу. Якщо існує функція $f: S \to T$, така що

$$\forall i \in 1..m \;\; f(\varphi_i(a_1,...,a_n)) = \psi_i(f(a_1),.., f(a_n)),$$

то кажуть, що f – **гомоморфізм** із A в B.

Зміст цієї умови в тому, що, незалежно від того, чи здійснено спочатку операцію φ_i в A, а потім виконано відображення f, або спочатку зроблено відображення f, а потім в B здійснено відповідну операцію ψ_i, результат буде однаковим.

Наприклад, нехай $A = \langle N; +\rangle$, $B = \langle N_{10}; +_{10}\rangle$, де $N_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, а $+_{10}$ – додавання по модулю 10. Тоді $f \equiv a \bmod 10$ – гомоморфізм із A у B.

Гомоморфізми, які мають додаткові властивості, мають спеціальні назви:

- гомоморфізм, який є ін'єкцією, називається **мономорфізмом**;
- гомоморфізм, який є сюр'єкцією, називається **епіморфізмом**;
- гомоморфізм, який є бієкцією, називається **ізоморфізмом**;
- Якщо $A = B$, то гомоморфізм називається **ендоморфізмом**, а ізоморфізм називається **автоморфізмом**.

Теорема 6.2. Якщо існує ізоморфізм A на B, то є ізоморфізм B на A.

Доведення. Розглянемо довільну операцію φ із сигнатури A і відповідну їй операцію ψ із сигнатури B. Маємо:

$$f(\varphi(a_1,...,a_n)) = \psi(f(a_1),.., f(a_n),$$

крім того, f – бієкція. Позначимо $b_1 = f(a_1),\dots, b_n = f(a_n)$, при цьому $a_1 = f^{-1}(b_1),\dots, a_n = f^{-1}(b_n)$. Тоді

$$f^{-1}(\psi(b_1,...,b_n)) = f^{-1}(\psi(f(a_1),.., f(a_n))) = f^{-1}(f(\varphi(a_1,...,a_n))) =$$
$$= \varphi(a_1,...,a_n) = \varphi(f^{-1}(b_1),..., f^{-1}(b_n)) . \blacktriangleright$$

Якщо f: $S \to T$ – ізоморфізм, то алгебри A та B називається ізоморфними і позначають так: $A \overset{f}{\sim} B$. Якщо f зрозуміло з контексту, то пишуть $A \sim B$.

Наприклад, нехай Z - множина всіх цілих чисел, Z_2 – множина всіх парних чисел. Алгебри $\langle Z; +\rangle$ і $\langle Z_2; +\rangle$ – ізоморфні; ізоморфним є відображення f: $n \to 2n$, причому $2(a+b) = 2a + 2b$. Оскільки $Z_2 \subset Z$, f – ізоморфізм $\langle Z; +\rangle$ у себе. Відображення g: $n \to (-n)$ для алгебри $\langle Z; +\rangle$ є автоморфізмом. Для алгебри $\langle Z; \times\rangle$ відображення g не є автоморфізмом, оскільки $(-a)\times(-b) \neq -(ab)$. Ізоморфізмом між алгебрами $\langle R_+; \times\rangle$ і $\langle R; +\rangle$, де R_+ – додатна підмножина R, є відображення $a \to \log a$.

Розглянемо алгебри $\langle S; \varphi\rangle$ та $\langle T; \psi\rangle$, де $S = \{a, b, c, d\}$, $T = \{\alpha, \beta, \gamma, \delta\}$, а бінарні операції φ та ψ задано відповідними таблицями.

	a	b	c	d
a	c	b	b	a
b	a	d	d	b
c	d	b	b	a
d	a	a	c	c

	α	β	γ	δ
α	δ	δ	γ	α
β	α	α	δ	γ
γ	α	α	β	γ
δ	γ	β	γ	β

Відображення f: $a \to \gamma$, $b \to \alpha$, $c \to \beta$, $d \to \delta$ є ізоморфізмом.

Перевірка умови означення 6.5 полягає ось у чому. В комірках (внутрішньої частини) першої таблиці замінюємо елементи множини S на елементи множини T відповідно до f і дістаємо ліву частину умови означення 6.5, тобто таблицю функції $f_\varphi(x, y)$; в зовнішній частині другої таблиці виконуємо заміну й одержуємо праву частину умови означення 6.5; порівнянням утворених двох таблиць переконуємося, що вони задають одну й ту саму функцію. Справді, досить у першій таблиці перейменувати всі елементи множини S на елементи множини T і порівняти утворену із другою таблицею.

	a	b	c	d
a	β	α	α	γ
b	γ	δ	δ	α
c	δ	α	α	γ
d	γ	γ	β	β

	b	c	a	d
b	δ	δ	γ	α
c	α	α	δ	γ
a	α	α	β	γ
d	γ	β	γ	β

<u>Теорема 6.3.</u> Відношення ізоморфізму на множині однотипних алгебр є відношенням еквівалентності.

Доведення.

Рефлективність. $A \overset{f}{\sim} A$, де f – тотожне відображення.

Симетричність. $A \overset{f}{\sim} B \Rightarrow B \overset{f^{-1}}{\sim} A$.

Транзитивність. $A \overset{f}{\sim} B$, $B \overset{g}{\sim} C \Rightarrow A \overset{g\circ f}{\sim} C$. ►

Класами еквівалентності в розбитті за відношенням ізоморфізму є класи ізоморфних між собою алгебр.

Поняття ізоморфізму є одним із центральних понять, що надає змогу застосовувати алгебраїчні методи у різних галузях. Його сутність можна виразити наступним чином: якщо алгебри A та B – ізоморфні, то елементи й операції B можна перейменувати так, що B збігатиметься з A. З умови означення 6.5 випливає, що будь-яке еквівалентне співвідношення в алгебрі A зберігається в будь-якій ізоморфній їй алгебрі A'. Це дає змогу, одержавши такі співвідношення в алгебрі A, автоматично поширити їх на всі алгебри, ізоморфні A. Відомий у математиці вираз "розглядати об'єкти з точністю до ізоморфізму" означає, що розглядаються тільки ті властивості об'єктів, які зберігаються при ізоморфізмі, тобто є загальними для всіх ізоморфних об'єктів. Зокрема, ізоморфізм зберігає такі властивості: асоціативність, комутативність і дистрибутивність операцій.