Тема 7. Типи алгебр

7.1. Початкові означення

Означення 7.1. Нехай $\langle S; \perp\rangle$ - алгебра. Елемент $a\in S$ називається **регулярним**, якщо з того, що $a\perp x = a\perp y$ та $x\perp a = y\perp a$ випливає $x = y$.

Таким чином, будь-яке число – регулярне відносно “+”, а для добутку регулярним є всяке число, крім нуля.

Означення 7.2. **Нейтральним елементом** або **одиницею** називається такий елемент $e\in S$, коли для всіх елементів $x\in S$ справджується рівність $e\perp x = x\perp e = x$.

Лема 7.1. Якщо нейтральний елемент існує, то він – єдиний і регулярний.

Доведення. Доведемо єдність від супротивного: припустимо, що нейтральний елемент не єдиний. Нехай існують два нейтральних елементи $e_1\in S$ та $e_2\in S$, $e_1\neq e_2$. Оскільки e_1 – нейтральний елемент, $e_1\perp e_2 = e_2\perp e_1 = e_2$, а оскільки e_2 – теж нейтральний елемент, $e_2\perp e_1 = e_1\perp e_2 = e_1$. Одержана суперечність доводить твердження.

Доведемо регулярність від супротивного: припустимо, що нейтральний елемент – не регулярний, тобто нехай $e\perp x = e\perp y$ та $x\perp e = y\perp e$, але $x \neq y$. Оскільки e – нейтральний елемент, $e\perp x = x\perp e = x$, але $e\perp x = e\perp y$ за умовою, а $e\perp y = y\perp e = y$. Одержана суперечність доводить твердження. ►

Наприклад, на множині дійсних чисел 0 – нейтральний елемент відносно “+”, а 1 – нейтральний елемент відносно добутку. У $P(U)$ $\varnothing$ - нейтральний елемент відносно об’єднання, а U – нейтральний елемент відносно перерізу множин. Для множини всіх квадратних матриць n-го порядку з числовими елементами, нульова матриця є нейтральним елементом відносно додавання матриць, а одинична матриця – нейтральним елементом відносно добутку матриць.

Означення 7.3. Якщо множина містить нейтральний елемент e відносно операції $\perp$, то елемент b називається **симетричним** (**оберненим**, **протилежним**) елементу a, коли $a\perp b = b\perp a = e$. При цьому a називається **симетрованим елементом** і b позначається через $\bar{a}$, тобто $b = \bar{a}$. Множина, в якій всякий елемент має симетричний, називається також симетрованою.

Лема 7.2. Якщо елемент $\bar{a}$, симетричний елементу a, існує, то він – єдиний та регулярний.

Пропонуємо читачеві довести це твердження самостійно.

Наприклад, на множині дійсних чисел для операції додавання “+” будь-якому елементу x симетричним є елемент $-x$, а для операції добутку – елемент x^{-1}. Симетричними елементами на множині квадратних матриць n-го порядку відносно операції добутку матриць є взаємно обернені матриці.

7.2. Алгебри з однією операцією

Означення 7.4. **Півгрупою** називається алгебра з однією асоціативною бінарною операцією.

Наприклад, множина функцій, яка замкнена відносно суперпозиції, є півгрупою.

Якщо у півгрупі існує система твірних, яка містить тільки один елемент, то така півгрупа називається **циклічною**. Наприклад, $\langle N; +\rangle$ є циклічною півгрупою, тому що $\{1\}$ є системою твірних.

Означення 7.5. Якщо операція півгрупи комутативна, то півгрупа називається комутативною або **абелевою**. Якщо півгрупа має нейтральний елемент (одиницю), то така півгрупа називається **моноїдом**.

Одиниця у моноїді завжди єдина.

Нехай $A = \langle S; *\rangle$ - півгрупа зі скінченою системою твірних $T = \{t_1, \ldots, t_n\}$. Тоді $\forall x\in S\ \exists y_1, \ldots, y_k\in T : x = y_1 * \ldots * y_k$. Якщо відкинути позначення операції $*$, то кожний елемент $x\in S$ можна представити як слово α в алфавіті T. Деякі слова можуть виявитися однаковими як елементи, тобто елемент a, який відповідає слову α, буде дорівнювати елементу b, який відповідає слову β: $a = b$. Такі рівності називаються **визначальними співвідношеннями**. Якщо ж в півгрупі їх немає, тобто будь-які два різних слова є різними елементами півгрупи, то така півгрупа називається **вільною**.

Будь-яку півгрупу можна утворити з вільної півгрупи введенням деяких визначальних співвідношень. Два слова в алфавіті T вважаються рівними, якщо одне із іншого утворюється за допомогою визначальних співвідношень. Відношення рівності слів у півгрупі із визначальними відношеннями є відношенням еквівалентності. З будь-якого слова, використовуючи визначальні співвідношення, легко утворити різні еквівалентні йому слова. Набагато складнішою є проблема: для двох заданих слів з'ясувати, чи можна здобути одне з іншого, застосовуючи визначальні співвідношення. Класи еквівалентності по цьому відношенню відповідають елементам півгрупи.

Наприклад, у півгрупі $\langle \boldsymbol{N}; +\rangle$ є скінчена система твірних $\{1\}$. Іншими словами, кожне натуральне число можна представити як послідовність символів "1". Очевидно, що різні слова в алфавіті $\{1\}$ суть різні елементи носія, тобто ця півгрупа вільна.

Означення 7.6. **Групою** називається півгрупа з одиницею, в якій для кожного елемента a існує елемент $\overline{a}$, який називається оберненим до a і який задовольняє умову $a\perp\overline{a} = \overline{a}\perp a = e$. Число елементів носія групи називається її порядком.

В загальному випадку операція групи не є комутативною, тобто властивості $\overline{a}\perp a = e$ та $a\perp\overline{a} = e$ не рівнозначні. Але коли комутативність виконується, то група називається **комутативною** або **абелевою**. Група, всі елементи якої є степенями одного елемента a, називається **циклічною**.

Циклічна група – завжди абелева. Для таких груп часто застосовується адитивний запис: операція позначається як додавання – "+", а одиниця як – "0".

Наприклад, множина раціональних чисел, що не містить нуля, з операцією множення є абелевою групою. Оберненим до елемента a буде елемент $1/a$.

Множина цілих чисел $\boldsymbol{Z}$ з операцією додавання є абелевою циклічною групою. Роль одиниці тут відіграє 0, оберненим до елемента a буде елемент $-a$.

Множина невироджених квадратних матриць порядку n з операцією добутку є некомутативною групою. Одиниця групи – одинична матриця. Обернений елемент – обернена матриця.

Множина $\{0, 1, 2, 3, 4\}$ з операцією "додавання за mod 5" – скінченна абелева циклічна група. Її одиницею є 0. У цій групі $\overline{3} = 2$, $\overline{1} = 4$.

Теорема 7.1. В групі виконуються наступні співвідношення:

1. $\overline{a+b} = \overline{b} + \overline{a}$.
2. $a+b = a+c \Rightarrow b=c$.
3. $b+a = c+a \Rightarrow b=c$.
4. $\overline{\overline{a}} = a$.

Доведення. Доведемо перше та друге співвідношення. Решту залишаємо читачеві на самостійну роботу.

1. $(a+b)+(\overline{b}+\overline{a}) = a+(b+\overline{b})+\overline{a} = a+e+\overline{a} = a+\overline{a} = e$.
2. $a+b = a+c \Rightarrow \overline{a}+(a+b) = \overline{a}+(a+c) \Rightarrow (\overline{a}+a)+b = (\overline{a}+a)+c \Rightarrow e+b = e+c \Rightarrow b = c$ ►

Теорема 7.2. В групі можна однозначно розв'язати рівняння $a + x = b$, (розв'язок: $x = \overline{a} + b$.

Доведення.

$a+x = b \Rightarrow \overline{a}+(a+x) = \overline{a}+b \Rightarrow (\overline{a}+a)+x = \overline{a}+b \Rightarrow e+x = \overline{a}+b \Rightarrow x = \overline{a}+b$ ►

7.3. Група підстановок

Взаємне однозначне відображення множини X на себе (f: $X \to X$) називається **підстановкою** множини X. Звичайно прийнято записувати підстановку двома рядками, взятими в дужки. Перший рядок – аргументи (перші координати), другий рядок – образи (другі координати). Наприклад:

$$f=\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix},\ g=\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}.$$

Оскільки байдуже, в якому порядку записано впорядковані пари відображення, одна й та сама підстановка допускає різні подання, наприклад:

$$\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}=\begin{pmatrix}4&3&2&1\\1&3&4&2\end{pmatrix}=\begin{pmatrix}4&2&3&1\\1&4&3&2\end{pmatrix}...$$

Це означає, що асоціативність виконується.

Тотожна підстановка $e=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$ відіграє роль нейтрального елемента, тобто одиниці.

Якщо в підстановці f поміняти місцями її рядки, то дістанемо підстановку, симетричну f:

$$f=\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix},\ \bar{f}=\begin{pmatrix}2&4&3&1\\1&2&3&4\end{pmatrix}.$$

Композицією або добутком підстановок f та g є їх суперпозиція:

$$fg=\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix}.$$

Покажемо, що підстановки утворюють групу з операцією “композиція підстановок”. Композиція підстановок f та g – це композиція двох взаємно однозначних відображень множини об’єктів X на себе, тобто $X\xrightarrow{f}X\xrightarrow{g}X$, завдяки чому дістаємо деяку підстановку fg.

Нейтральним елементом у групі підстановок є тотожна підстановка e, а симетричним елементом для будь-якої підстановки f – симетрична підстановка $\bar{f}$. Оскільки композиція підстановок не підпорядковується комутативному закону ($fg\neq gf$), група підстановок не є комутативною.

У будь-якій скінченій групі її операція може бути задана таблицею Келі. Для груп ця таблиця має важливу особливість: будь-який її стовпець містить усі елементи групи. Справді, якщо стовпець a_i не містить якого-небудь елемента, то деякий інший елемент a_j в ньому має зустрітися двічі, скажімо, в m-му та n-му рядках. Однак тоді $a_m a_i = a_j$, $a_n a_i = a_j$ і, отже, $a_m a_i = a_n a_i$. Якщо помножимо обидві частини цієї рівності на $\bar{a}_i$, дістанемо $a_m = a_n$, що неправильно. Таким чином, i-й стовпець таблиці Келі містить усі елементи групи, тобто добуток на a_i є підстановкою на множині елементів групи. Перевіривши, що ця відповідність є ізоморфізмом, маємо таку теорему Келі:

<u>Теорема 7.3</u> (Келі, без доведення). Будь-яка скінченна група є ізоморфною групі підстановок на множині її елементів.

7.4. Алгебри з двома операціями

В цьому розділі ми звернемо увагу на об’єкти, що знайомі читачеві зі школи. Серед алгебр з двома операціями найбільш важливими є кільця та поля, а основними прикладами кілець та полей є множини цілих, раціональних та дійсних чисел з операціями добутку та додавання.

<u>Означення 7.7.</u> **Кільце** – це множина M із двома бінарними операціями + та × (вони називаються додаванням та добутком відповідно), в якій:

1. $(a+b)+c = a+(b+c)$ додавання асоціативне
2. $\exists 0\in M\ \forall a$: $a+0 = 0+a = a$ існує нуль – нейтральний елемент відносно додавання;
3. $\forall a\ \exists -a$: $a+(-a) = 0$ існує обернений елемент для операції додавання;
4. $a+b = b+a$ додавання комутативне, тобто кільце – абелева група за додаванням;

5. $a \times (b \times c) = (a \times b) \times c$ — добуток асоціативний, тобто кільце – півгрупа за добутком;
6. $a \times (b+c) = (a \times b) + (a \times c)$, $(a+b) \times c = (a \times c) + (b \times c)$ — добуток дистрибутивний відносно додавання зліва та справа;

Кільце називається комутативним, якщо

7. $a \times b = b \times a$ — добуток комутативний;

Комутативне кільце називається кільцем з одиницею, якщо

8. $\exists 1 \in M$: $1 \times a = a \times 1 = a$ — існує одиниця – нейтральний елемент відносно добутку, тобто кільце з одиницею – моноїд за добутком.

<u>Теорема 7.4.</u> В кільці виконуються наступні співвідношення:

1. $0 \times a = a \times 0 = 0$
2. $a \times (-b) = (-a) \times b = -(a \times b)$
3. $(-a) \times (-b) = a \times b$

Доведення.

1. $0 \times a = (0+0) \times a = (0 \times a) + (0 \times a) \Rightarrow$
   $-(0 \times a) + (0 \times a) = -(0 \times a) + ((0 \times a) + (0 \times a)) = (-(0 \times a) + (0 \times a)) + (0 \times a) \Rightarrow$
   $0 = 0 + (0 \times a) = (0 \times a)$.
2. $(a \times (-b)) + (a \times b) = a \times (-b+b) = a \times 0 = 0 \Rightarrow a \times (-b) = -(a \times b)$,
   $(a \times b) + ((-a) \times b) = (a+(-a)) \times b = 0 \times b = 0 \Rightarrow (-a) \times b = -(a \times b)$.
3. $(-a) \times (-b) = -(a \times (-b)) = -(-(a \times b)) = a \times b$. ►

Наприклад, $\langle \mathbf{Z}; +, \times \rangle$ – комутативне кільце з одиницею. Непорожня система S множин утворює кільце множин, якщо для будь-яких множина A і B цієї системи $A \oplus B \in S$ та $A \cap B \in S$. Тут означено два внутрішніх закони композиції: диз'юнктивну суму та переріз множин. Перший закон – асоціативний. Нейтральним елементом відносно $\oplus$ слугує $\varnothing$, тому що $\forall A$: $A \oplus \varnothing = A$. Також він є симетричним, тому що $\forall A\ \exists A'$: $A \oplus A' = \varnothing$. Другий закон – також асоціативний, тому що $A \cap (B \cap C) = (A \cap B) \cap C$, і дистрибутивний відносно першого, тобто $A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$. Нейтральний елемент (одиниця) U відносно другого закону означається співвідношенням $A \cap U = A$. Отже, наведена система є комутативним кільцем з одиницею.

<u>Означення 7.8.</u> Якщо в кільці існують елементи $x \neq 0$ та $y \neq 0$ такі, що $x \times y = 0$, то x називається лівим, а y – правим **дільником нуля**.

В групі $a \times b = a \times c \Rightarrow b = c$, але в довільному кільці це не так.

<u>Теорема 7.5.</u> Нехай $a \neq 0$. Тоді

$$\left.\begin{array}{l}(a \times b = a \times c \Rightarrow b = c)\\(b \times a = c \times a \Rightarrow b = c)\end{array}\right\} \Leftrightarrow (x \neq 0,\ y \neq 0 \Rightarrow x \times y \neq 0)\,.$$

Доведення. Необхідність доведемо від супротивного. Нехай $x \times y = 0$. Тоді $x \neq 0$ та $x \times 0 = 0$, звідки маємо, що $y = 0$. Нехай $y \neq 0$, але з $x \times y = 0$ та $0 \times y = 0$ маємо $x = 0$. Прийшли до протиріччя.

Доведемо достатність. $0 = (a \times b) + (-(a \times b)) = (a \times b) + (-(a \times c)) = (a \times b) + (a \times (-c)) = a \times (b + (-c))$, $a \times (b+(-c)) = 0$ та $a \neq 0$. Звідси маємо: $b + (-c) = 0$, тобто $b = c$. ►

<u>Означення 7.9.</u> Комутативне кільце з одиницею, яке не має дільників нуля, називається **областю цільності**.

Цілі числа $\langle \mathbf{Z}; +, \times \rangle$ є областю цільності.

<u>Означення 7.10.</u> **Поле** – це множина M із двома бінарними операціями + та $\times$, в якій:

1. $(a+b) + c = a + (b+c)$ — додавання асоціативне;
2. $\exists 0 \in M\ \forall a$: $a+0 = 0+a = a$ — існує нуль – нейтральний елемент відносно додавання;
3. $\forall a\ \exists -a$: $a + (-a) = 0$ — існує обернений елемент для операції додавання;
4. $a+b = b+a$ — додавання комутативне, тобто поле - абелева група за додаванням;

5. $a\times(b\times c) = (a\times b)\times c$ добуток асоціативний;
6. $a\times(b+c) = (a\times b) + (a\times c)$, $(a+b)\times c = (a\times c) + (b\times c)$ добуток дистрибутивний відносно додавання зліва та справа;
7. $a\times b = b\times a$ добуток комутативний;
8. $\exists 1\in M$: $1\times a = a\times 1 = a$ існує одиниця – нейтральний елемент відносно добутку;
9. $\forall a\neq 0\ \exists\ a^{-1}$: $a\times a^{-1} = 1$ існує обернений елемент для операції добутку.

Наприклад, $\langle \boldsymbol{R}; +, \times\rangle$ - поле дійсних чисел, $\langle \boldsymbol{Q}; +, \times\rangle$ - поле раціональних чисел.

Нехай $E = \{0, 1\}$. Визначимо операції +, ×: $E\times E\rightarrow E$ наступним чином: $0\times 0 = 0$, $0\times 1 = 0$, $1\times 0 = 0$, $1\times 1 = 1$, $0+0 = 0$, $0+1 = 1$, $1+0 = 1$, $1+1=0$. Тоді $\langle E; +, \times\rangle$ є полем і називається двійковою арифметикою. Тут 0 – це нуль, 1 – це одиниця, $-1 = 1$, $-0 = 0$, $1^{-1} = 1$, а 0^{-1} – не визначено.

<u>Теорема 7.6.</u> В полі виконуються наступні властивості:

1. $(-a) = a\times(-1)$
2. $-(a+b) = (-a) + (-b)$
3. $a\neq 0 \Rightarrow (a^{-1})^{-1} = a$
4. $a\times b = 0 \Rightarrow a=0$ або $b=0$.

Доведення.

1. $(a\times(-1)) + a = (a\times(-1)) + (a\times 1) = a\times(-1 + 1) = a\times 0 = 0$.
2. $(a + b) + ((-a) + (-b)) = (a + b) + ((-b) + (-a)) = a + (b + (-b)) + (-a) = a + 0 + (-a) =$ $= a + (-a) = 0$.
3. $a^{-1}\times a = 1$.
4. Нехай $a\times b = 0$ і $a\neq 0$, тоді $b = 1\times b = (a^{-1}\times a)\times b = a^{-1}\times(a\times b) = a^{-1}\times 0 = 0$.

Нехай $a\times b = 0$ і $b\neq 0$, тоді $a = 1\times a = (b^{-1}\times b)\times a = b^{-1}\times(b\times a) = b^{-1}\times 0 = 0$. ►

<u>Теорема 7.7.</u> Якщо $a\neq 0$, то в полі єдиним чином розв'язується рівняння $a\times x + b = 0$, (розв'язок: $x = -(a^{-1})\times b$).

Доведення. $a\times x + b = 0 \Rightarrow a\times x + b + (-b) = 0 + (-b) \Rightarrow a\times x + 0 = (-b) \Rightarrow a\times x = -b \Rightarrow$ $a^{-1}\times(a\times x) = a^{-1}\times(-b) \Rightarrow (a^{-1}\times a)\times x = -(a^{-1}\times b) \Rightarrow 1\times x = -(a^{-1}\times b) \Rightarrow x = -(a^{-1}\times b)$. ►

Можна навести таблицю, яка містить всі наведені вище типи алгебр і деякі додаткові:

Тип алгебри	Перший закон (адитивний)				Другий закон (мультиплікативний)			
	Властивості		Елементи		Властивості		Елементи	
	Асоціативність	Комутативність	Нейтральний	Симетричний	Асоціативність	Комутативність	Нейтральний	Симетричний
Півгрупа	X							
Абелева півгрупа	X	X						
Моноїд	X		X					
Абелева півгрупа з нулем	X	X	X					
Група	X		X	X				
Абелева група	X	X	X	X				
Кільце	X	X	X	X	X			
Абелеве кільце	X	X	X	X	X	X		
Кільце з одиницею (унітарне кільце)	X	X	X	X	X		X	
Абелеве кільце з одиницею	X	X	X	X	X	X	X	
Тіло	X	X	X	X	X		X	X
Поле	X	X	X	X	X	X	X	X