Тема 4.
Алгебраїчні структури

§1 Алгебраїчні операції

Алгебра вивчаємножини, для елементівяких введено відношення, якіназиваютьсяалгебраїчнимиопераціями.

Підn-арноюалгебраїчноюоперацією (внутрішнім законом композиції) на множиніMрозуміють відображення множини $\underbrace{M \times M \times \cdots \times M}_{n}$в M.

Поняттяn-арноїалгебраїчноїоперації є рівносильнедо поняттявідношення R: $(a1, a2, \ldots, an, b) \in R$, якщо

$(a1, a2, \ldots, an) \to b$.

Під бінарною операцією на множиніM розумітимемо закон, за якимкожнимдвомелементамa та b множиниM ставиться у відповідністьпевнийелементd цієїмножини: $(a, b) \to d$.

Для запису композиції елементів a та b їх позначають спеціальним знаком.

Закон композиції, який позначається знаком «+», переважно називають додаванням і стверджують, що для нього прийнято адитивне позначення.

Закон композиції, який позначається знаком «•», переважно називають множенням і стверджують, що для нього прийнято мультиплікативне позначення.

При вивчанні загальних властивостей бінарних операцій використовують символ «*».

Прикладом бінарної операції є операція векторного множення векторів.

Операція скалярного добутку векторів не є бінарною алгебраїчною операцією, оскільки скалярний добуток є число, а не вектор.

Для задання бінарної алгебраїчної операції складають таблицю операції (**таблицю Келлі**), рядки і стовпці якої позначають елементами множини *M*, а на перетинанні рядка і стовпця ставиться відповідний результат операції.

$*$	a_1	a_2	…	a_n
a_1	$a_1 * a_1$	$a_1 * a_2$	…	$a_1 * a_n$
…	…	…	…	…
a_n	$a_n * a_1$	…	…	$a_n * a_n$

Кількістьбінарнихопераційна множині з *n* елементівможнавизначитив такийспосіб: маючи n^2 клітиноктаблиці, до кожної з них слідзаписатибудь-який з *n* елементів множини *M*.

Звідси випливає, що кількість бінарнихопераційна множині з *n* елементівдорівнюєn^{n^2}.

Якщомножинаскладається з елементівa та b, то існує$2^{2^2} = 16$ операцій.

*	**a**	**b**
a	b	a
b	a	b

Використання таблиць має велике значення, оскільки деякі операції в комп'ютерній математиці не придатні для словесного завдання.

Множина, в якій введено бінарну алгебраїчну операцію, називається ***групоїдом.***

§2 Властивості алгебраїчних операцій

Бінарна операція називається ***асоціативною***, якщо для будь-яких елементів a, b, c множини M

$$(a * b) * c = a * (b * c).$$

Прикладом асоціативної операції є операція множення матриць.

Прикладом неасоціативної операції є операція векторного добутку векторів, тому що, наприклад,

$$(i \times j) \times j \neq i \times (j \times j).$$

Множина, для якої введена асоціативна операція, називається ***півгрупою.***

Бінарна операція називається ***комутативною***, якщо для будь-яких елементів множини M

$$a * b = b * a.$$

Прикладом комутативної операції є операція додавання матриць, а прикладом некомутативної операції є операція множення матриць.

Векторний добуток векторів є антикомутативною операцією:

$$a \times b = -b \times a \ .$$

Бінарна операція * називається ***дистрибутивною зліва*** відносно операції °, якщо для будь-яких елементів a, b, c

$$a * (b \circ c) = (a * b) \circ (a * c).$$

Операція називається **дистрибутивною справа**, якщо

$$(a \circ b) * c = (a * c) \circ (b * c).$$

Операція множення чисел є дистрибутивною відносно додавання чисел:

$$(a + b)\cdot c = a\cdot c + b\cdot c.$$

Але операція додавання не є дистрибутивною відносно множення:

$$a + (b\cdot c) \neq (a + b)\cdot(a + c).$$

Операції перерізу й об’єднання множин є дистрибутивною відносно одна одної і зліва, і справа.

Елемент e називається ***нейтральним елементом*** відносно операції $\circ$, якщо для кожного елемента a

$$a \circ e = a \text{ і } e \circ a = a.$$

Нейтральний елемент є єдиний, оскільки, якщо e' − інший нейтральний елемент, то

$$e = e \circ e' = e' .$$

Нейтральний елемент відносно операції додавання називається ***нульовим*** елементом і позначається символом 0.

Нейтральний елемент відносно операції множення називається ***одиничним*** елементом і позначається символом 1.

Елементa' називається***симетричним***елементуa у групоїдіз нейтральнимелементомe, якщо

$$a \circ a' = a' \circ a = e.$$

Елементa' , симетричний до a відносноопераціїдодавання, називаєтьсяпротилежнимдо a і позначається символом $-a$.

Елементa' , симетричний до a відносноопераціїмноження, називаєтьсяоберненим до елементаa і позначається символом a^{-1}.

§3 Алгебраїчні структури

Алгебраїчною структурою називається множина M разом із заданими Q операціями, визначеними і замкненими на цій множині. M – носій алгебраїчної структури.

3.1 Група

Групою називається множина з визначеною на ній бінарною асоціативною операцією, для якої існує обернена операція.

Група називається **скінченною**, якщо вона містить скінчену множину елементів.

Число елементів скінченної групи називається ***порядком*** групи.

У теорії груп зазвичай використовується мультиплікативна термінологія (тобто групова операція називається множенням, нейтральний елемент – одиничним, симетричний елемент – оберненим).

З визначеннявипливає, що в кожнійгрупііснуєодиничний (нейтральний) елемент і для кожного елементагрупиіснуєоберненийелемент.
З іншого боку, можнапоказати, щоякщоасоціативнаопераціягарантуєіснування нейтрального та оберненогоелементів, то множина з такою операцією є групою.

У зв'язку з цим часто користуютьсяіншимвизначеннямгрупи, рівносильним до першого.

НепорожнямножинаG, на якійвизначенабінарнаоперація, називається***групою***, якщовиконуютьсятакіумови:
1) операція є асоціативна;
2) в G існуєнейтральнийелемент;
3) для кожного елементаa існуєоберненийелементa^{-1}.

Група називається ***комутативною***, або ***абелевою***, якщо вона має наступні властивості:

1. **Замкнутість**. Якщо a і b — елементи G, то c = a * b — також елемент G.
2. **Асоціативність**. Якщо a і b — елементи G, то

$$(a* b) * c = a* (b *c)$$

3. **Комутативність**. Для всіх a і b в G маємо

$$a * b = b * a.$$

4. **Існування нейтрального елемента**. Для всіх елементів в G існує елемент *e*, такий, що

$$e * a = a * e = a.$$

5. **Існування інверсії**. Для кожного a в G існує елемент a', такий, що

$$a * a' = a' * a = e.$$

П р и к л а д.

Множина цілих чисел є абелевою групою відносно операції додавання.

1. Результатом додавання двох цілих чисел є ціле число.
2. Асоціативність: 4+(5+6)=(4+5)+6.
3. Комутативність: 4+5=5+4.
4. Нейтральним елементом групи є число 0.
5. Симетричним елементом для числа *n* є число *–n (4, -4)*.

Дана група називається адитивною групою цілих чисел і позначається $G = \langle Z_n, + \rangle$.

Розглянемо групу $(Z_5;\oplus_5)$. Побудуємо для операції таблицю Келі.

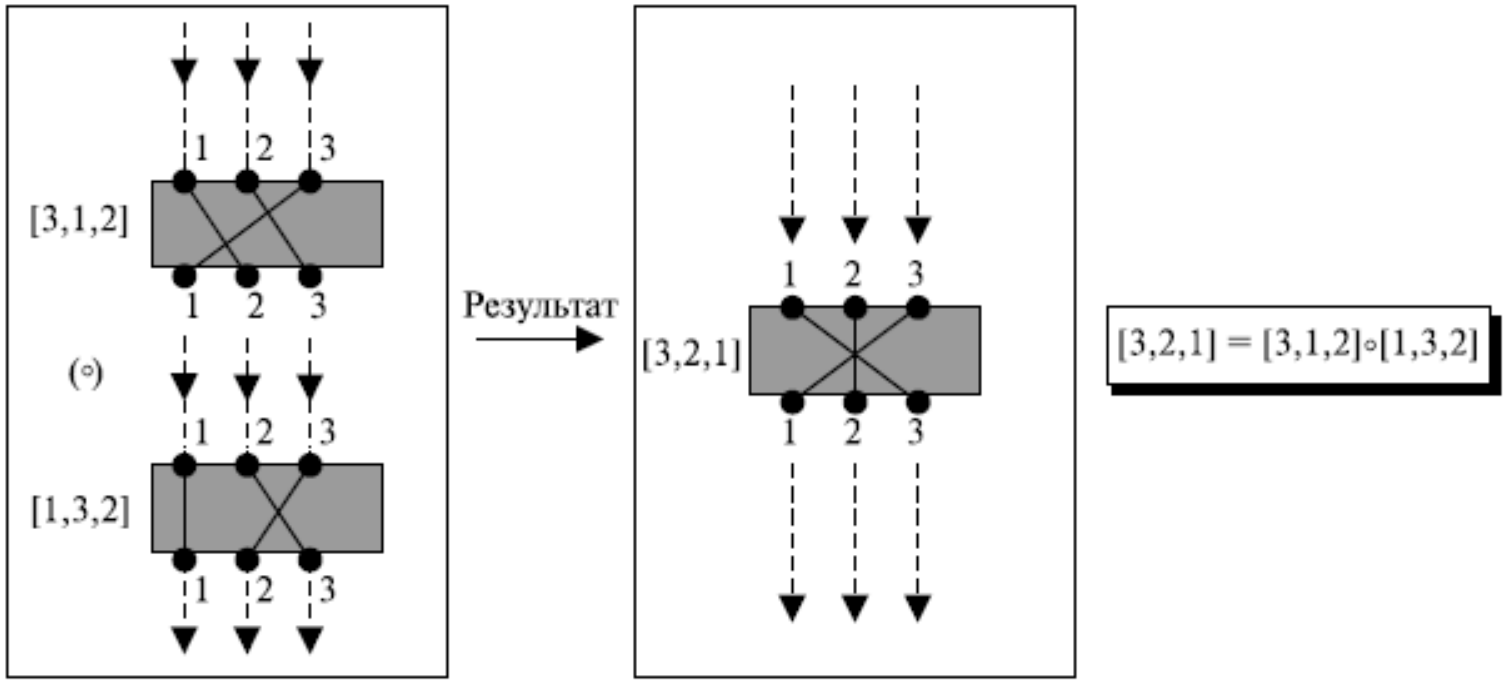
$\oplus_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Нейтральним елементом відносно операції $\oplus_5$ e=0, таблиця симетрична відносно діагоналі - операція комутативна, існують обернені елементи x=1 , x'=4; y=2, y'=3; x=3, x'=2…

В групі елементами множини можуть бути не лише числа та об’єкти, а й правила, відображення, функції, дії.

Розглянемо групу підстановок. Множина всіх перестановок і оператор є композицією.

Приклад композиції двох перестановок, які переміщують три вхідні сигнали, щоб утворити три вихідні сигнали.

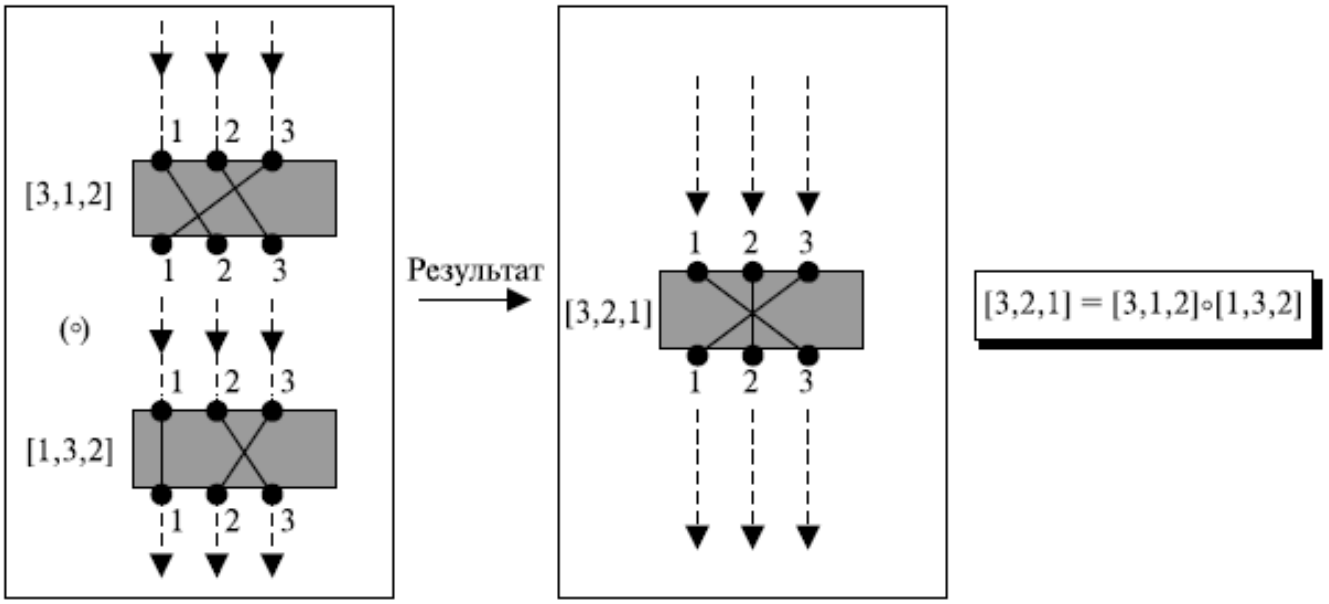


	[1 2 3]	[1 3 2]	[2 1 3]	[2 3 1]	[3 1 2]	[3 2 1]
[1 2 3]	**[1 2 3]**	[1 3 2]	[2 1 3]	[2 3 1]	[3 1 2]	[3 2 1]
[1 3 2]	[1 3 2]	**[1 2 3]**	[2 3 1]	[2 1 3]	[3 2 1]	[3 1 2]
[2 1 3]	[2 1 3]	[3 1 2]	**[1 2 3]**	[3 2 1]	[1 3 2]	[2 3 1]
[2 3 1]	[2 3 1]	[3 2 1]	[1 3 2]	[3 1 2]	**[1 2 3]**	[2 1 3]
[3 1 2]	[3 1 2]	[2 1 3]	[3 2 1]	**[1 2 3]**	[2 3 1]	[1 3 2]
[3 2 1]	[3 2 1]	[2 3 1]	[3 1 2]	[1 3 2]	[2 1 3]	**[1 2 3]**

Властивості:

1. Замкнутість – так
2. Асоціативність – так
3. Комутативність – ні
4. Нейтральний елемент – так (1 2 3)
5. Інверсія – так

Група не є абелевою.



3.2 Кільце

Кільцем **(R,+,×)** називається множина R, на якій визначені дві бінарні алгебраїчні операції (додавання та множення), при цьому відносно однієї з цих операцій множина є абелевою групою, а друга операція є дистрибутивна відносно першої.

Кільце називається ***комутативним***, якщо друга операція є комутативна, і ***асоціативним***, якщо вона є асоціативна.

3.3 Поле

Ненульові елементи кільця можуть утворювати групу відносно операції множення.

Таке кільце називається ***кільцем з діленням***, або ***тілом***. Комутативне тіло називається ***полем***.

Поле являє собою єдність двох абелевих груп – адитивної та мультиплікативної.

В криптографії використовують тільки снінчені поля.

Скінчене поле — це поле зі скінченою кількістю елементів.

Галуа показав що скенчені поля повинні мати кількість елементів p^n, де p — просте, а n — додатнє ціле число. Скінчені поля називають **полями Галуа** і позначають $GF(p^n)$.

Розглянемо алгебраїчну структуру $(Z_n; \otimes_n; \oplus_n)$, n=8. Побудуємо таблиці Келі.

$\oplus_8$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

$\otimes_8$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Існують випадки, коли добуток ненульових членів дорівнює 0, а саме (2;4), (4;6), (4;4)…, отже $(Z_8; \otimes_8; \oplus_8)$ не є полем, а є комутативним кільцем з нейтральним елементом 0.

Алгебраїчна структура	**Операції**	**Набори цілих чисел**
Група	(+ -) або (× /)	Z_n або$Z^*{}_n$
Кільце	(+ -) та (×)	Z
Поле	(+ -) та (× /)	Z_p