# Розділ 3. Алгебраїчні структури

# 3.1. Алгебраїчні операції та їх властивості

- *унарна операція, бінарна операція*
- *записи infix, prefix, postfix*
- *таблиця Келі*
- *комутативність, асоціативність, дистрибутивність*
- *одиниця, обернений елемент*
- *операції додавання та множення за модулем*

- ***Операцією*** на множині $S$ називається функція $f$, яка є відображенням виду $S^n \to S$, $n \in N$, де $S^n$ — декартів добуток $S \times S \times \ldots \times S$, в який $S$ входить $n$ разів.

Важливо: 1) оскільки операція є функцією, то результат застосування операції визначено однозначно;
2) операція замкнена на $S$.

- 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 звичайно позначають символами, що називають ***операторами***.

# Способи запису операцій

- ***infix* - *оператор між операндами***

  $a + b$

- ***prefix* - *оператор перед операндами***

  $+\ a\ b$

- ***postfix* - *оператор після операндів***

  $a\ b\ +$

## Алгоритм обчислення значень виразу, що записаний у формі *postfix*:

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. Якщо у виразі ще є знаки операцій, то повертаємося до кроку 1, якщо немає – отримано результат.

**Приклад**.

Вираз у *infix*-формі:

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

Результат переведення його до *postfix* буде таким:

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

Обчислення значення виразу:

$1\ \underline{2\ 3*} + 4\ 5\ 6\ 7 + * + + = \underline{1\ 6 +}\ 4\ 5\ 6\ 7 + * + + =$

$= 7\ 4\ 5\ \underline{6\ 7 +} * + + = 7\ 4\ \underline{5\ 13\ *} + + = 7\ \underline{4\ 65 +} + =$

$= \underline{7\ 69 +} = 76.$

# Таблиця Келлі

Символи $\otimes$ і $\oplus$ використовуються як змінні для позначення будь-яких операцій.

- 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 $a_k = a_i \otimes a_j$.

| **⊗** | ***a*** | ***b*** | ***c*** | ***d*** |
|---|---|---|---|---|
| ***a*** | *a* | *b* | *c* | *d* |
| ***b*** | *b* | *a* | *d* | *c* |
| ***c*** | *c* | *d* | *a* | *b* |
| ***d*** | *d* | *c* | *b* | *a* |

$a \otimes b = b$,

$b \otimes b = a$,

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

# Властивості операцій

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 $A$ ***комутативна***.
- 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 $A$ ***асоціативна***.
- 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 $\otimes$ ***дистрибутивна*** відносно операції $\oplus$.

**Приклад.**

На множині дійсних чисел $R$ :

додавання $1+2=2+1$; $(1+2)+3=1+(2+3)$

комутативне, асоціативне

віднімання $1-2\neq 2-1$; $(3-2)-1\neq 3-(2-1)$

не комутативне, не асоціативне

додавання відносно множення не дистрибутивне

$2+(2*3) \neq (2+2)*(2+3)$

множення відносно додавання дистрибутивне

$2*(2+3) = (2*2)+(2*3)$

множення відносно віднімання дистрибутивне

$2*(3-2) = (2*3)-(2*2)$

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 $a \in A$: $e \otimes a = a \otimes e = a$,
тоді $e$ називається ***одиницею*** відносно 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 елементом*** до $x$ відносно операції $\otimes$.

Іноді розрізняють ліві та праві одиниці ($e_{лів} \otimes a = a$ або $a \otimes e_{прав} = a$ для будь-якого $a \in A$) і ліві та праві обернені елементи, однак у більшості випадків одиниці є двосторонніми.

**Приклад.**

На множині дійсних чисел $R$ :

0 для додавання — двостороння одиниця

$x + 0 = x = 0 + x$

0 для віднімання — права одиниця

$x - 0 = x,\ 0 - x \neq x$

В алгебрі множин одиниця для:

операції об'єднання $\cup$ — порожня множина $\varnothing$

операції перетину $\cap$ — універсальна множина $U$

# Додавання за модулем

Нехай *n* — довільне натурально число.

- ***Додавання за модулем n*** цілих чисел *a* і *b* називається алгебраїчна операція $\oplus_n$, результатом якої є решта від ділення суми $a + b$ на $n$.

$a \oplus_n b = c$, так, що $a+b = k*n+c$, $0 \le c < n$; $a, b, k \in Z+$

Областю значень операції є множина цілих невід'ємних чисел, менших за *n*.

**Приклад**.

$2 \oplus_3 2$ =Зал.(4/3)= 1 $\quad$ $7 \oplus_{10} 8$ =Зал.(15/10)= 5

$2 \oplus_4 2$ =Зал.(4/4)= 0 $\quad$ $7 \oplus_{12} 8$ = Зал.(15/12)= 3

# Множення за модулем

Нехай $n$ — довільне натурально число.

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

$a \otimes_n b = d$, так, що $a*b = f*n+d$, $0 \le d < n$; $a, b, f \in Z+$

Областю значень операції є множина цілих невід'ємних чисел, менших за $n$.

**Приклад**.

$2 \otimes_3 2$ =Зал.(4/3)= 1 $2 \otimes_4 2$ =Зал.(4/4)= 0

$7 \otimes_{10} 8$ =Зал.(56/10)= 6 $7 \otimes_{12} 8$ =Зал.(56/12)= 8

# 3.2. Поняття алгебраїчної структури

- *алгебраїчна структура*
- *підструктура*
- *гомоморфізм*
- *ізоморфізм*

- ***Алгебраїчною структурою*** 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. $A' \in A$
  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.

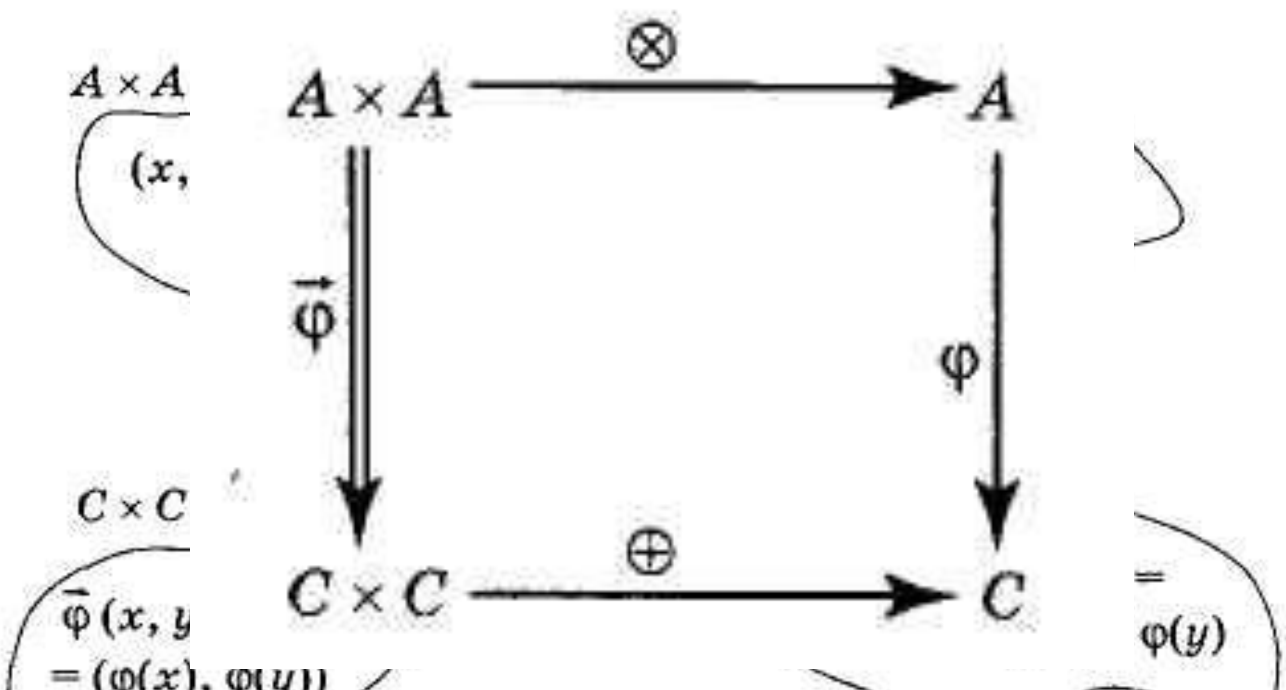
**Приклад**. Нехай $E$ — множина парних натуральних чисел, тоді $(E, +)$ буде підструктурою структури $(N, +)$, де $N$ — множина натуральних чисел.

# Гомоморфізм

Нехай задано дві структури $(A, \otimes)$, $(C, \oplus)$ з операціями $\otimes$, $\oplus$ одного порядку $n$.

- Відображення $\phi: A \to C$ називається ***гомоморфізмом*** із структури $(A, \otimes)$ у структуру $(C, \oplus)$, якщо воно переставлене з операціями у такому розумінні: $\phi \cdot \otimes = \oplus \cdot \square\phi$ ,
  де відображення $\square\phi : A^n \to C^n$ діє за правилом
  $\square\phi\,(a_1, a_2,\ldots,a_n) = (\phi\,(a_1),\phi\,(a_2),\ldots,\phi(a_n)),\ \ \forall\ a_i \in A$
  Для бінарних операцій ($n = 2$), зокрема,
  $\phi\,(x \otimes y) = \phi\,(x) \oplus \phi\,(y)$ , для будь-яких $x, y \in A$.

# Графічне визначення гомоморфізму для випадку бінарних операцій.




Комутативна діаграма, що зображує гомоморфізм $\phi$

**Приклад.**

Нехай задано відображення $\theta$: $Z_+ \to Z_{10}$, що переводить будь-яке ціле невід'ємне число у решту від ділення цього числа на 10.

Тоді $\theta(20) = 0$, $\theta(17) = 7$,...

Якщо $(Z_+, +)$ і $(Z_{10}, \oplus_{10})$ структури з операцією звичайного додавання +, що визначена на $Z_+$ і додаванням за модулем 10 на $Z_{10}$, то $\theta$ є гомоморфізмом з першої структури у другу.

$$\begin{tikzcd}
(24, 38) \arrow[r] \arrow[d, Rightarrow, "\vec{\theta}"'] & 62 \arrow[d, "\theta"] \\
(4, 8) \arrow[r, "\oplus_{10}"] & 2
\end{tikzcd}$$

Комутативна діаграма гомоморфізму $\theta$ з $(Z_+, +)$ в $(Z_{10}, \oplus_{10})$

$\theta(24 + 38) = \theta(62) = 2$

$\theta(24) \oplus_{10} \theta(38) = 4 \oplus_{10} 8 = 2$

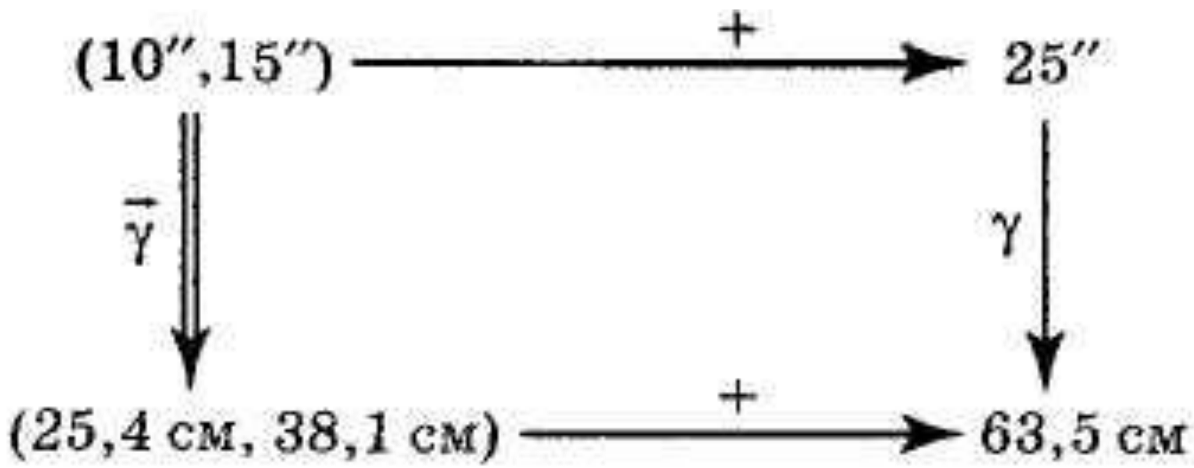
# Ізоморфізм

- Гомоморфізм, який є бієкцією, називають ***ізоморфізмом***. Якщо існує ізоморфізм між двома структурами, то говорять, що вони ***ізоморфні одна одній***.

  Відношення ізоморфізму — це відношення еквівалентності на множині алгебраїчних структур, тому ізоморфізм розбиває множину всіх алгебраїчних структур на класи еквівалентності. Використовуючи ізоморфізм, можна здійснювати еквівалентні перетворення алгебраїчних структур. Будь-яке співвідношення у структурі $S$ зберігається у будь-якій ізоморфній їй структурі $Q$. Це дозволяє, одержавши певні співвідношення у структурі $S$, автоматично поширити їх на всі структури, що ізоморфні $S$.

**Приклад.**

Розглянемо спосіб вимірювання довжини у дюймах та сантиметрах. Якщо додати бінарну операцію додавання, то одержимо дві структури: (inch, +), (см, +). Визначимо ізоморфізм $\gamma$: $x$ (см) = 2,54 * $x$ (inch).




$\gamma$

(см, +)

$d$ = 10" + 15" = 25", 2,54 * 25" = 63,5 см;

$d$ = 10" * 2,54 + 15" * 2,54 = 25,4 см + 38,1 см = 63,5 см.

# 3.3. Найпростіші алгебраїчні структури

- *півгрупа*
- *моноїд*
- *група*
- *абелева група*
- *кільце*
- *поле*

# Структури з однією операцією

- ***Півгрупою*** називається алгебраїчна структура з множиною-носієм $A$ і бінарною операцією $\otimes$: $A^2 \rightarrow A$, 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: $x \otimes (y \otimes z) = (x \otimes y) \otimes z$, для всіх $x, y, z \in M$.
2. Існує $e \in M$ — одиниця відносно $\otimes$: $e \otimes x = x = x \otimes e$ для всіх $x \in M$.

Таким чином, моноїд — це півгрупа з одиницею.

**Приклад**.

Якщо позначимо через $A^*$ множину всіляких рядків, що складаються з букв українського алфавіту і порожнього рядку $\varepsilon$=«», то одержимо структуру ($A^*$, •), яка є моноїдом з одиничним елементом $\varepsilon$.

«паровоз» • «» = «» • «паровоз» = «паровоз»

- ***Групою*** називають множину $G$ з бінарною операцією $\otimes$, що замкнена в $G$, такою, що

1. $\otimes$ асоціативна:
   $x \otimes (y \otimes z) = (x \otimes y) \otimes z$, для всіх $x, y, z \in M$.
2. Існує $e \in M$ — одиниця відносно $\otimes$:
   $e \otimes x = x = x \otimes e$ для всіх $x \in M$.
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***.

# Структури з двома операціями

- ***Кільцем*** $(R, \oplus, \otimes)$ називається множина $R$ з визначеними на неї бінарними операціями $\oplus$ і $\otimes$ :

1. $\otimes$ асоціативна:
   $x \otimes (y \otimes z) = (x \otimes y) \otimes z$, для всіх $x, y, z \in M$.
2. $\oplus$ комутативна:
   $x \oplus y = y \oplus x$ для всіх $x, y \in R$.
3. $\oplus$ має одиницю, яка називається нулем і позначається 0:
   $0 \oplus x = x$ для всіх $x \in R$.
4. Існує обернений елемент відносно $\oplus$ для кожного $x \in R$:
   $(-x) \oplus x = x \oplus (-x) = 0$ для всіх $x \in R$.
5. $\otimes$ асоціативна:
   $x \otimes (y \otimes z) = (x \otimes y) \otimes z$ для всіх $x, y, z \in R$.
6. $\otimes$ дистрибутивна відносно $\oplus$ зліва і справа:
   $x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$,
   $(x \oplus y) \otimes z = (x \otimes z) \oplus (y \otimes z)$ 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***.

***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***.