

<sup>1</sup> канд. фізико-математичних наук, доцент, доцент каф. методики навчання математики та методики навчання інформатики, ДВНЗ «ДДПУ»

e-mail: kaydannv@gmail.com, ORCID 0000-0002-4184-8230

<sup>2</sup> студент 1 курсу магістратури фізико-математичного факультету, ДВНЗ «ДДПУ»

e-mail: Eldoeldo202@gmail.com, ORCID 0000-0001-9910-2020

## ЗВ'ЯЗОК МІЖ БУЛЕВИМИ АЛГЕБРАМИ, ЧАСТКОВО ВПОРЯДКОВАНИМИ МНОЖИНАМИ ТА КІЛЬЦЯМИ ПРИ ВИВЧЕННІ КУРСУ «ДИСКРЕТНА МАТЕМАТИКА»

У статті розглядається частково впорядковані множини та їх зв'язок з булевими алгебрами та кільцями. Представлено ряд тверджень, які доцільно вивчати при знайомстві з алгебраїчними структурами студентам фізико-математичного факультету спеціальності 014 Середня освіта (Інформатика) в курсі дискретної математики. Наведено ряд прикладів, які наочно пояснюють розглянуті структури.

**Ключові слова:** алгебраїчні структури, частково впорядковані множини, ґратки, кільця, булева алгебра, дискретна математика.

### Вступ

Серед технічних наук інформаційні технології та електроніка у значній мірі використовують математику. Дійсно, якщо поглянути на програми навчання студентів в університетах Євросоюзу, то легко виявити, що математичні дисципліни займають в них значне місце. Математика є теоретичним фундаментом комп'ютерних наук, і тому їй приділяється велика увага при підготовці фахівців у цій галузі. Дискретна математика займає тут центральне місце, оскільки саме з неї виростають три гілки програмної інженерії — алгоритми, програми, структури даних.

Однією з актуальних проблем сучасної алгебри є опис і класифікації скінченних кілець. Скінченні кільця є дуже важливою і цікавою алгебраїчною структурою [3]. Вивчення скінченних кілець має застосування в теорії кодування та в загальній теорії кілець. Скінченні кільця широко застосовуються в криптографії та криптографічних протоколах. Деякі сучасні криптосистеми, такі як сучасний стандарт шифрування даних (Advanced Encryption Standard) та криптосистема XTR, застосовують скінченні кільця, які мають більш загальний вигляд. Більш того, скінченні кільця лежать в основі еліптичних кривих, які в свою чергу утворюють фундамент цілого класу криптосистем [6].

Вивчення різних алгебраїчних структур пов'язано з іменами видатних алгебраїстів всього світу, таких як К. Асано, Т. Накаяма [5], Дж. Веддербарн, Е. Артін [1], Е. Нетер. Видатні українські вчені присвятили багато своїх праць вивченню цих структур, а саме Ю. Дрозд, В. Кириченко [4], Н. Губарені, Ю. Яременко [7] та інші.

Важливість алгебраїчних структур та значна практична значущість призводить до появи особливої уваги при вивченні цих тем. З урахуванням того, що знання мають стати фундаментальними, розгляд відповідних тем слід робити згідно чіткої, логічної та легкої для запам'ятовування структури. Спираючись на досвід викладання цих тем для студентів спеціальності 014 Середня освіта (Інформатика), нами було відтворено структуру, яка, на нашу думку, найбільш відповідає переліченим вимогам.

## Основна частина

Розглянемо частково впорядковані множини та їх зв'язок з булевими алгебрами та кільцями. Відомості, які розглядаються є в багатьох монографіях з теорії кілець та модулів. Наш виклад базуються на матеріалах глави 2 монографії [2].

Нагадаємо означення частково впорядкованої множини.

**Означення 1.** Множина  $S$  називається частково впорядкованою, якщо визначене відношення  $\leq$ , яке задовольняє наступним умовам:

1.  $a \leq a$  для довільного  $a \in S$  (рефлексивність);
2. з  $a \leq b$ ,  $b \leq c$  випливає  $a \leq c$  для довільних  $a, b, c \in S$  (транзитивність);
3. з  $a \leq b$ ,  $b \leq a$  випливає  $a = b$  для довільних  $a, b \in S$  (антисиметричність).

Відношення  $\leq$  називається частковим порядком.

**Приклад 1.** Відношення порядку  $\leq$  є частковим порядком для всіх додатних цілих чисел.

**Приклад 2.** Нехай  $S$  множина та  $\mathcal{P}(S)$  є множиною всіх підмножин множини  $S$ , включаючи порожню підмножину  $\emptyset$  та всю множину  $S$ . Тоді  $\mathcal{P}(S)$  є частково впорядкованою множиною відносно теоретико-множинного включення.

**Приклад 3.** Нехай  $A$  кільце і нехай  $S$  множина всіх його правих ідеалів. Очевидно,  $S$  частково впорядкована множина за включенням. Аналогічно можна розглядати частково впорядковані множини лівих та двосторонніх ідеалів.

Нехай  $T$  — підмножина частково впорядкованої множини  $S$ . Елемент  $a \in S$  називається верхньою гранню (відп. нижньою гранню)  $T$ , якщо  $t \leq a$  (відп.  $a \leq t$ ) для всіх  $t \in T$ . Звичайно в загальному випадку множина може мати декілька верхніх граней або не мати їх зовсім. Елемент  $a \in T$  є найбільшим (найменшим) елементом  $T$ , якщо  $t \leq a$  (відп.  $a \leq t$ ) для всіх  $t \in T$ . Не кожна підмножина  $T$  частково впорядкованої множини  $S$  має найбільший (найменший) елемент. Але якщо  $T$  має такий елемент, тоді він єдиний. Справді, нехай  $x$  та  $y$  найбільші елементи  $T$ . Тоді  $x \leq y$  та  $y \leq x$ , згідно умови антисиметричності  $x = y$ . Аналогічно доводиться єдиність мінімального елемента. Таким чином, найбільший (відп. найменший) елемент, якщо існує, то є єдиним і є верхньою (нижньою) гранню. Якщо множина верхніх граней  $T$  має найменший елемент, тоді він називається *найменшою верхньою гранню* (або супремумом)  $T$  і позначається  $\sup(\mathbf{T})$ . Якщо множина нижніх граней має найбільший елемент, то він називається *найбільшою нижньою гранню* (або інфімумом)  $T$  і позначається  $\inf(\mathbf{T})$ . Очевидно, що якщо підмножина  $T$  має супремум (відп. інфімум), тоді він є однозначно визначеним.

**Означення 2.** Частково впорядкована множина  $S$ , в якій кожна пара елементів з  $S$  має одночасно супремум та інфімум в  $S$  називається ґраткою.

**Приклад 4.** Якщо  $X$  та  $Y$  підмножини в  $S$ , тоді їх супремум в  $\mathcal{P}(S)$  дорівнює об'єднанню  $X \cup Y$ , а їх інфімумом в  $\mathcal{P}(S)$  є перетин  $X \cap Y$ . Отже  $\mathcal{P}(S)$  ґратка.

**Приклад 5.** Нехай  $A$  кільце та  $X$  — множина всіх ідеалів кільця  $A$ , впорядкованих за включенням. Нехай  $\mathcal{I}$  та  $\mathcal{J}$  — ідеали  $A$ . Тоді їх супремумом в  $X$  є сума  $\mathcal{I} + \mathcal{J}$ , а їх інфімумом в  $X$  є перетин  $\mathcal{I} \cap \mathcal{J}$ . Отже,  $X$  ґратка.

Операції  $\sup$  та  $\inf$  не є дійсно бінарними операціями для довільної частково впорядкованої множини. Характеристичною властивістю ґратки є те, що операції  $\sup$  та  $\inf$  можуть бути застосовані до будь-якої пари елементів.

Нехай  $S$  ґратка. Тоді кожна пара  $a, b \in S$  має одночасно супремум та інфімум. Позначимо  $a \vee b = \sup\{a, b\}$  та  $a \wedge b = \inf\{a, b\}$ . Тоді відображення  $\vee$  та  $\wedge$  з  $S \times S$  визначається через бінарні операції в  $S$ :  $(a, b) \rightarrow a \vee b$  та

$(a, b) \rightarrow a \wedge b$ . Наступне твердження представляє декілька цікавих властивостей цих операцій.

**Твердження 1.** (*[2], твердження 2.4.1*). Нехай  $a, b$  та  $c$  — елементи ґратки  $S$ . Тоді операції  $\vee$  та  $\wedge$  на  $S$  мають наступні властивості:

- 1) комутативні закони:  $a \vee b = b \vee a$ ;  $a \wedge b = b \wedge a$ ;
- 2) асоціативні закони:  $a \vee (b \vee c) = (a \vee b) \vee c$ ;  $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ ;
- 3) ідемпотентні закони:  $a \vee a = a$ ;  $a \wedge a = a$
- 4) закони поглинання:  $a \vee (a \wedge b) = a$ ,  $a \wedge (a \vee b) = a$ .

**Твердження 2.** (*[2], твердження 2.4.2*). Якщо ми маємо множину  $S$  з двома бінарними операціями  $\vee$  та  $\wedge$  такими, що для всіх елементів  $a, b$  та  $c$  множини  $S$  виконуються умови:

- (1)  $a \vee b = b \vee a$ ;  $a \wedge b = b \wedge a$ ;
- (2)  $a \vee (b \vee c) = (a \vee b) \vee c$ ;  $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ ;
- (3)  $a \vee a = a$ ;  $a \wedge a = a$
- (4)  $a \vee (a \wedge b) = a$ ,  $a \wedge (a \vee b) = a$ .

тоді єдине часткове впорядкування в  $S$ , яке перетворює  $S$  в ґратку, а задані операції  $\vee$  та  $\wedge$  є супремумом та інфімумом в цій ґратці.

**Означення 3.** Ґратка  $S$  є дистрибутивною, якщо виконується наступна властивість:

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

для всіх  $a, b, c \in S$ .

Справедливим є симетричне означення.

**Твердження 3.** (*[2], твердження 2.4.3*). Ґратка  $S$  є дистрибутивною тоді і тільки тоді, коли всі  $a, b, c \in S$  володіють наступною властивістю:

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

Ґратки з прикладу 4. та 5. є дистрибутивними. Частково впорядкована множина може мати, а може і не мати найбільший та найменший елементи. Це виконується і для ґраток. Дійсні числа із звичайним впорядкуванням утворюють ґратку без найбільшого і найменшого елемента; дійсні числа між нулем та одиницею включають ґратку з одночасно найбільшим і найменшим елементом. Якщо ґратка має найбільший і найменший елемент, то його позначають, відповідно, як 1 та 0.

Нехай ґратка  $S$  має найбільший елемент 1 та найменший елемент 0. *Доповненням* елемента  $a \in S$  називається елемент  $b \in S$  такий, що  $a \vee b = 1$  та  $a \wedge b = 0$ .

**Означення 4.** *Ґратка з найбільшим елементом 1 та найменшим елементом 0 називається доповнювальною ґраткою, якщо кожен її елемент має доповнення.*

Ґратка є особливим видом частково впорядкованої множини. Булева алгебра є особливим видом ґраток.

**Означення 5.** *Булевою алгеброю називається доповнювальна дистрибутивна ґратка.*

**Означення 6.** *Частково впорядкована множина  $S$ , в якій кожна підмножина одночасно має і супремум і інфімум в  $S$ , називається повною ґраткою.*

Ми будемо позначати через  $\bar{a}$  доповнення елемента  $a$  в булевій алгебрі.

**Приклад 6.** 1. *Частково впорядкована множина  $\mathcal{P}(S)$  є булевою алгеброю.*

2. *Розглянемо скінченний прямий добуток  $B^n = B \times \dots \times B$ , який є множиною  $n$ -ок  $(b_1, b_2, \dots, b_n)$ , де  $b_i \in B$ . Нехай  $(a_1, a_2, \dots, a_n)$  та  $(b_1, b_2, \dots, b_n)$  елементи в  $B^n$ . Введемо наступні операції в  $B^n$ :*

$$\begin{aligned}(a_1, a_2, \dots, a_n) \vee (b_1, b_2, \dots, b_n) &= (a_1 \vee b_1, a_2 \vee b_2, \dots, a_n \vee b_n) \\ (a_1, a_2, \dots, a_n) \wedge (b_1, b_2, \dots, b_n) &= (a_1 \wedge b_1, a_2 \wedge b_2, \dots, a_n \wedge b_n) \\ \overline{(a_1, a_2, \dots, a_n)} &= (\bar{a}_1, \bar{a}_2, \dots, \bar{a}_n).\end{aligned}$$

Тоді  $B^n$  булева алгебра з найбільшим елементом  $1 = (1, 1, \dots, 1)$  та найменшим елементом  $0 = (0, 0, \dots, 0)$ . Кількість елементів в  $B^n$  рівна  $2^n$ .

**Твердження 4.** ([2], твердження 2.4.4). В будь-якій булевій алгебрі операція доповнення задовільняє наступним умовам:

(a)  $\overline{\overline{a}} = a$

(b)  $\overline{a \vee b} = \overline{a} \wedge \overline{b}$

(c)  $\overline{a \wedge b} = \overline{a} \vee \overline{b}$

(d)  $a \vee b = \overline{\overline{a} \wedge \overline{b}}$

(e)  $a \wedge b = \overline{\overline{a} \vee \overline{b}}$

(f)  $\overline{1} = 0$

(g)  $\overline{0} = 1$

**Твердження 5.** ([2], твердження 2.4.5). Якщо ми маємо множину  $S$ , яка містить два спеціальні елементи  $1$  та  $0$  з двома бінарними операціями  $\vee$  та  $\wedge$  такими, що для всіх елементів  $a, b, c \in S$  виконуються умови:

(1)  $a \vee b = b \vee a$ ;  $a \wedge b = b \wedge a$ ;

(2)  $a \vee (b \vee c) = (a \vee b) \vee c$ ;  $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ ;

(3)  $a \vee a = a$ ;  $a \wedge a = a$

(4)  $a \vee (a \wedge b) = a$ ,  $a \wedge (a \vee b) = a$ .

(5)  $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ ;

(6) для кожного елемента  $a \in S$  існує елемент  $\overline{a} \in S$  такий, що  $a \vee \overline{a} = 1$  та  $a \wedge \overline{a} = 0$

тоді існує єдине відношення часткового порядку на  $S$ , яке перетворює  $S$  в булеву алгебру таку, що задані операції  $\vee$  та  $\wedge$ , відповідно є супремумом та інфімумом в булевій алгебрі. Більше того,  $1$  та  $0$  є найбільшим та найменшим елементом в  $S$ , елемент  $\overline{a}$  доповнення елемента  $a$ .

**Лема 1.** ([2], лема 2.4.7).

В довільній булевій алгебрі  $\mathcal{B}$  умова  $a \vee b = a$  виконується тоді і тільки тоді, якщо  $a \wedge b = b$ .

З цієї леми випливає, що в кожній булевій алгебрі  $a \leq b \Leftrightarrow a \vee b = b \Leftrightarrow a \wedge b = a$ .

**Лема 2.** ([2], лема 2.4.8). В довільній булевій алгебрі  $\mathcal{B}$  виконуються умови:

1.  $a \wedge b \leq a \leq a \vee b$ ;
2.  $0 \leq a \leq 1$

для довільних  $a, b \in \mathcal{B}$ .

**Означення 7.** Елемент  $a \neq 0$  булевої алгебри називається атомом, якщо він не виражається у вигляді  $a = b \vee c$  з  $a \neq b$  та  $a \neq c$ .

**Лема 3.** ([2], лема 2.4.9). Ненульовий елемент  $a$  булевої алгебри  $\mathcal{B}$  є атомом тоді і тільки тоді, коли нерівність  $x \leq a$  має рівно два розв'язки  $x = a$  та  $x = 0$ .

**Лема 4.** ([2], лема 2.4.10). Для будь-якого ненульового елемента  $b$  булевої алгебри існує принаймні один атом  $a \in \mathcal{B}$  такий, що  $a \leq b$ .

Нехай  $\mathcal{B}$  скінченна булева алгебра з множиною атомів  $A = \{a_1, \dots, a_n\}$ . Для будь-якого елемента  $x \in \mathcal{B}$  позначимо через  $T(x)$  множину всіх атомів  $a \in A$  таких, що  $a \leq x$ .

**Твердження 6.** Будь-який ненульовий елемент  $x \in \mathcal{B}$  може бути представлений у вигляді скінченної суми різних атомів:

$$x = a_{i_1} \vee a_{i_2} \vee \dots \vee a_{i_k}$$

де  $a_{i_j} \in T(x)$  для  $j = 1, \dots, k$ .

**Твердження 7.** ([2], твердження 2.4.12). Для будь-якої булевої алгебри  $\mathcal{B}$  і будь-яких елементів  $x, y \in \mathcal{B}$  виконуються умови:

- (1)  $T(x \vee y) = T(x) \cup T(y)$
- (2)  $T(x \wedge y) = T(x) \cap T(y)$
- (3)  $T(\bar{x}) = \overline{T(x)}$

**Лема 5.** ([2], лема 2.4.13). Для будь-якого елемента  $x \in \mathcal{B}$  виконується умова  $\sup T(x) = x$ .

**Означення 8.** Для двох булевих алгебр  $\mathcal{B}_1$  та  $\mathcal{B}_2$  бієктивне відображення  $\varphi$  з  $\mathcal{B}_1$  в  $\mathcal{B}_2$  називається ізоморфізмом булевих алгебр, якщо виконуються наступні умови:

$$(1) \quad \varphi(x \vee y) = \varphi(x) \vee \varphi(y)$$

$$(2) \quad \varphi(x \wedge y) = \varphi(x) \wedge \varphi(y)$$

$$(3) \quad \varphi(\bar{x}) = \overline{\varphi(x)}$$

для всіх  $x, y \in \mathcal{B}_1$ .

**Теорема 1.** *Будь-яка булева алгебра  $\mathcal{B}$  з множиною із  $n$  атомів  $A = \{a_1, a_2, \dots, a_n\}$  є ізоморфною булевій алгебрі  $\mathcal{P}(A)$  всіх підмножин заданих множиною  $A$ . Зокрема,  $\mathcal{B}$  має  $2^n$  елементів та  $1$  в  $\mathcal{B}$  однозначно розкладається в суму всіх різних атомів*

$$1 = a_1 \vee a_2 \vee \dots \vee a_n.$$

Дана теорема є частковим випадком відомої теореми Стоуна.

**Теорема 2.** *(теорема Стоуна) Будь-яка булева алгебра є ізоморфною булевій алгебрі деяких (не обов'язково усіх) підмножин заданої множини.*

Як наслідок теореми 1. отримується наступний результат, який стверджує, що скінченна булева алгебра повністю визначається числом її атомів.

**Теорема 3.** *( [2], теорема 2.4.18). Якщо  $\mathcal{B}_1$  та  $\mathcal{B}_2$  дві скінченні булеві алгебри з множинами атомів, рівними відповідно  $A_1 = \{a_1, a_2, \dots, a_n\}$  та  $A_2 = \{b_1, b_2, \dots, b_n\}$ , тоді існує ізоморфізм булевих алгебр  $\varphi: \mathcal{B}_1 \rightarrow \mathcal{B}_2$ , такий що  $\varphi(a_i) = b_i$  для  $i = 1, \dots, n$ .*

Розглянемо булеву алгебру  $\mathcal{B}^n$ . Вона має рівно  $n$  атомів і має  $2^n$  елементів. З іншої сторони,  $\mathcal{B}^n$  є скінченним прямим добутком  $n$  копій простої булевої алгебри  $\mathcal{B}$ .

**Наслідок 1.** *Будь-яка булева алгебра  $\mathcal{B}$ , яка має  $n$  атомів, ізоморфна булевій алгебрі  $\mathcal{B}^n$ , яка є скінченним добутком  $n$  копій простої булевої алгебри  $\mathcal{B}$ .*

**Означення 9.** *Асоціативне кільце  $\mathcal{R}$  (можна без одиниці) називається булевим кільцем, якщо кожен його елемент  $a \in \mathcal{R}$  є ідемпотентом, тобто  $a^2 = a$ .*

**Твердження 8.** *( [2], твердження 2.4.20)*

1. *Кожне булеве кільце  $\mathcal{R}$  є комутативним і  $a + \bar{a} = 0$  для кожного  $a \in \mathcal{R}$ ;*

2. Якщо  $\mathcal{R}$  — булеве кільце, тоді пряма сума  $\mathcal{T} = \bigoplus_{i \in I} \mathcal{R}$  є також булевим кільцем.

**Твердження 9.** ([2], твердження 2.4.21). Нехай  $\mathcal{B}$  — булева алгебра. Тоді  $\mathcal{B}$  перетворюється на булеве кільце з одиницею, якщо бінарні операції додавання та множення визначені в  $\mathcal{B}$  наступним чином

$$a + b = (a \wedge \bar{b}) \vee (\bar{a} \wedge b)$$

та

$$a \cdot b = a \wedge b.$$

**Твердження 10.** ([2], твердження 2.4.22). Нехай  $\mathcal{R}$  булеве кільце з одиницею. Тоді  $\mathcal{R}$  перетворюється на булеву алгебру, якщо покласти

$$a \vee b = a + b + ab$$

$$a \wedge b = ab$$

та відношення порядку  $\leq$  визначається в  $\mathcal{R}$  через

$$a \leq b \iff ab = a.$$

Оскільки булева алгебра  $\mathcal{B}$  є простим кільцем, з твердження 1. випливає наступне твердження.

**Теорема 4.** ([2], теорема 2.4.23). Будь-яке булеве кільце  $\mathcal{R}$  з одиницею ізоморфне прямій сумі простих булевих кілець.

**Означення 10.** Частково впорядкована множина  $S$  є лінійно впорядкованою (або ланцюгом), якщо для кожних двох елементів  $a, b \in S$  випливає, що або  $a \leq b$ , або  $b \leq a$ .

Елемент  $x_0$  називається верхньою гранню підмножини  $S \subset X$ , якщо  $x \leq x_0$  для всіх  $x \in S$ . Якщо верхня грань існує для  $S$ , то кажуть, що множина  $S$  обмежена зверху. Елемент  $x_0$  називається максимальним в  $X$ , якщо не існує елемента  $x \in X$ ,  $x \neq x_0$ , який задовольняє умові  $x_0 \leq x$ .

**Лема 6.** (лема Цорна, принцип максимуму) Якщо в частково впорядкованій множині  $X$  будь-яка лінійно впорядкована підмножина  $S$  обмежена зверху, то  $X$  містить максимальний елемент.

Лема Цорна еквівалентна добре відомій аксіомі вибору.

**Аксіома вибору.** Нехай  $S$  множина і  $\mathcal{P}(S)^*$  множина непорожніх підмножин  $S$ . Тоді існує відображення  $f$  з  $\mathcal{P}(S)^*$  в  $S$  таке, що  $f(A) \in A$  для кожного  $A \in \mathcal{P}(S)^*$ .

**Наслідок 2.** (*[2], наслідок 2.4.24*). Будь-який власний правий (лівий, двосторонній) ідеал  $I$  кільця  $A$  з одиницею міститься в максимальному власному правому (лівому, двосторонньому) ідеалі.

**Твердження 11.** (*[2], твердження 2.4.25*). Частково впорядкована множина  $S$  є повною ґраткою тоді і тільки тоді, якщо  $S$  має супремум та кожна непорожня підмножина множини  $S$  має інфімум в  $S$ .

**Означення 11.** ґратка  $S$  називається модулярною, якщо вона задовольняє наступній модулярній умові:

$$\text{якщо } b \leq a, \text{ то } a \wedge (b \vee c) = b \vee (a \wedge c)$$

для всіх  $a, b, c \in S$ .

**Твердження 12.** (*[2], твердження 2.4.26*). Всі ідеали кільця утворюють повну модулярну ґратку за відношенням включення.

Для ідеалів напівпростих кілець можна сказати дещо більше.

**Теорема 5.** (*[2], теорема 2.4.27*). Всі ідеали напівпростого кільця  $A$  утворюють скінченну булеву алгебру, яка містить  $2^s$  елементів.

## Висновки

Поняття алгебраїчної структури включає визначену множину об'єктів та операцій над цими об'єктами. Оскільки практично в будь-якій задачі обробки даних за допомогою комп'ютера виділяється множина самих даних і операцій, які застосовні до цих даних, очевидно, що при цьому формуються визначені алгебраїчні структури. З відношенням часткового порядку програмісти мають справу постійно, адже початкові дані для роботи програми та й ті дані, що поступають по ходу її роботи, потрібно весь час впорядковувати в структури так, щоб ці дані можна було швидко знаходити і використовувати для подальшої роботи.

Крім алгебраїчних структур на множині натуральних, цілих і дійсних чисел, на множинах та відношеннях доцільно вивчати і такі алгебраїчні структури, як підгрупи, моноїди і групи, що, зокрема, використовуються для перетворення рядків символів і беруть участь у формуванні більш складних структур – кілець і полів. Багато математичних конструкцій, які природно виникають у лінійній алгебрі, є кільцями або містять кільця як підструктури. Тобто ці поняття є базовими для загальної та лінійної алгебри, використовуються під час роботи з матрицями, при кодуванні інформації та обробці даних.

Добре закладений математичний фундамент освіти студентів фізико-математичного факультету, спеціальності 014 Середня освіта (Інформатика) дає можливість в подальшому навчити їх методам оцінки складності алгоритмів, підбору оптимальної структури даних і створенню ефективного та прозорого коду програми.

## Література

1. *Artin E.* Zur Theorie der hyperkomplexen Zahlen. 1927. № 5. P. 251-260.
2. *Gubareni N., Kirichenko V.* Rings and Modules. 2001. 306 p.
3. *Kaydan N.* Quivers of finite rings. 2009. С. 68-69.
4. *Кириченко В.* Semi-Perfect Semi-Distributive Rings. 2000. Vol. 3. P. 81-98.
5. *Nakayama T.* On Frobeniusean algebras I. 1939. P. 611-63.
6. *Кайдан Н., Остимчук Г.* Застосування циклічних кодів в теорії кодування. 2010. С. 76-78.
7. *Кириченко В., Яременко Ю.* Полусовершенные полудистрибутивные кольца. 2001. Т. 69. № 1. С. 153-156.

---

### **Nataliia V. Kaidan, Ruslan I. Kipchu**

Donbas State Pedagogical University, Sloviansk, Ukraine.

#### **Relationship between Boolean algebras, partially ordered sets and rings in the course of «Discrete mathematics»**

The paper describes partially ordered sets and their connection with Boolean algebras and rings. A number of statements are presented, which should be studied when getting acquainted with algebraic structures for students of the Faculty of Physics and Mathematics, specialty 014 of Secondary Education (Computer Science) in the course of discrete mathematics. A number of examples are given that clearly explain the considered structures.

**Keywords:** *algebraic structures, partially ordered sets, lattice, rings, Boolean algebras, discrete math.*

---