Міністерство освіти і науки України
Кам’янець-Подільський національний університет імені Івана Огієнка
Фізико-математичний факультет
Кафедра математики

Дипломна робота
магістра

з теми: “ДОСЛІДЖЕННЯ МАТРИЦЬ ПОКАЗНИКІВ ТА ЛАТИНСЬКИХ КВАДРАТІВ”

Виконав: **Білий Олександр,**
студент 2 курсу ступеня вищої освіти магістр, групи М1-М22 спеціальності 014 Середня освіта (Математика)

Керівник: **Зеленський О. В.,**
кандидат фізико-математичних наук, доцент

Рецензент: **Кріль С. О.,**
кандидат фізико-математичних наук, доцент

Кам’янець-Подільський – 2023

ЗМІСТ

ВСТУП

Дипломна робота присвячена застосуванню матриць в теорії кілець. Один із важливих класів, що виникає в різних питаннях теорії кілець, – клас черепичних порядків. Кожний черепичний порядок повністю визначається своєю матрицею показників і дискретно нормованим кільцем [1]. Багато властивостей таких кілець повністю визначаються їх матрицями показників, зокрема, сагайдаки таких кілець [1]. Перші важливі результати в цьому напрямі належать українським алгебраїстам Ю.А. Дрозду та В.В. Кириченко. Порівняно недавно матриці показників стали окремим об'єктом вивчення. Для дослідження матриць показників та їх сагайдаків використовуються також комбінаторні та геометричні методи. Їхня прозора будова дає більше можливостей для обчислень та висновків. За допомогою матриць показників одержано інтерпретацію зображень частково впорядкованих множин.

В дипломній роботі розглянуті латинські квадрати які є горенштейновими матрицями та знайдено всі можливі підстановки Кириченка для таких матриць.

РОЗДІЛ І. ВІДОБРАЖЕНЯ ТА ГРАФИ

Функціональні відношення

Означення 1.1 Відношення $f \subset A \times B$ називається **функціональним** (або просто функцією), якщо виконується наступне:

$$\forall a\ (a,b) \in f \text{ та } (a,c) \in f \Rightarrow b=c.$$

Іншими словами, кожному $a \in A$: $(a,b) \in f$ відповідає один і тільки один елемент $b \in B$.

Іноді функціональне відношення f також позначають у префіксному записі: $b = f(a)$, де $a \in A$, $b \in B$.

Область (множина) визначення функції буде наступна множина:

$$\mathrm{Dom}\, f == \{a \in A \mid \exists\, b \in B,\ b = f(a)\}.$$

Область (множина) значень функції буде наступна множина:

$$\mathrm{Im}\, f == \{b \in B \mid \exists\, a \in A,\ b = f(a)\}.$$

Очевидно, для функціонального відношення f кожний переріз за будь-яким $a \in A$ містить не більше як один елемент. Якщо $a \notin \mathrm{Dom}\, f$, то переріз за a – порожній.

Якщо $\mathrm{Dom} f = A$, то функціональне відношення f називається **всюди визначеним**. Матриця функціонального відношення містить у кожному рядку не більше як один одиничний елемент, а його граф характеризується тим, що з кожної вершини може виходити тільки одна дуга (враховуючи й петлі).

Наприклад, розглянемо множини A = {1,2,3,4} та B = {1, 4, 9, 16, 25}, тоді відношення R = {(1,1), (2,4), (3,9), (4,16)} та Q = {(1,1), (2,4), (3,4), (4,16)} є функціональними. Відношення P = {(1,1), (1,4), (3,9)}, навпаки, не є функціональним.

Розглянемо інший приклад – українсько-англійський словник. Він установлює відповідність між множиною українських та англійських слів. Ця відповідність не є функціональною (оскільки одному українському слову, як правило, ставляться у відповідність декілька англійських слів); крім того, вона практично ніколи не є повністю визначеною: завжди можна знайти українське слово, що не міститься в цьому словнику.

Усяке функціональне відношення можна розглядати як функцію. При цьому перша координата a впорядкованої пари $(a,b) \in f$ є **прообразом** (аргументом, змінною), а друга b – **образом** (значенням). Потрібно розрізняти функцію f як множину впорядкованих пар (відношення) і значення функції $b = f(a)$ як другу координату однієї з таких пар.

Слід зазначити, що відношення, обернене до функціонального, загалом не є функціональним. У розглянутому вище прикладі відношення Q є функціональним, але обернене йому відношення $Q^{-1} = \{(1,1), (4,2), (4,3), (16,4)\}$ не є функціональним.

Якщо функціональне відношення $f \subset A \times B$ всюди визначене на A, то його називають **відображенням** множини A в B і записують $f : A \to B$. Очевидно, що різниця між відображенням та функцією зводиться до способу означення цих відношень на множині A, причому відображення потрібно розглядати як окремий випадок функції. Більшість математиків не розрізняють поняття відображення і функції.

Типи відображень

При відображенні A в B кожен елемент a з A має один і тільки один образ $(\forall a \in A\ \exists!\ b \in B\ (a = f(b)))$. Однак зовсім не обов'язково, щоб кожний елемент B був образом деякого елемента з A. Графічно ця ситуацію показана на рис. 1.1а. Для порівняння на рис. 1.1б наведено приклад функціонального відношення, яке не є відображенням.

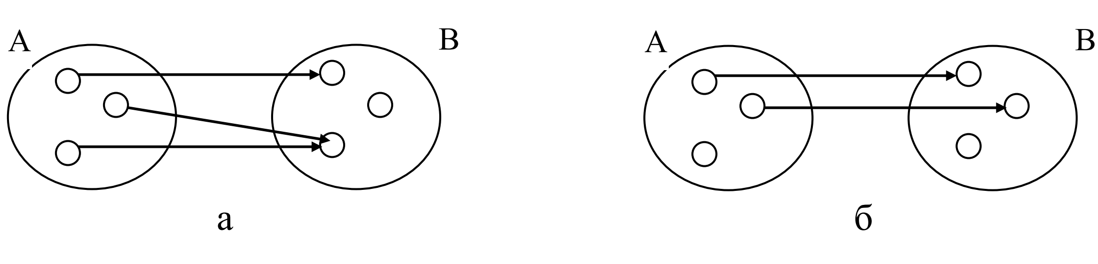

Рис. 1.1. Приклади відображення (а) та функціонального відношення (б).

Означення 1.2. Якщо для відображення f : A $\rightarrow$ B будь-який елемент b з B є образом принаймні одного елементу a з A, тобто:

$$\forall b \in B\ \exists a \in A : b = f(a),$$

то кажуть, що множина A накриває множину B, а відображення буде мати назву **сюр'єкції** (рис. 3.2).

Обернене відображення до сюр'єкції f^{-1} не буде порожнім.

Означення 1.3. Якщо для відображення f : A $\rightarrow$ B для будь-яких двох різних елементів a_1 та a_2 з A їх образи b_1 та b_2 також різні, то відображення f називається **ін'єкцією**, або взаємно однозначним відображенням (рис. 3.3). Іншим чином це можна записати як:

$$b = f(a_1) \text{ та } b = f(a_2) \Rightarrow a_1 = a_2.$$

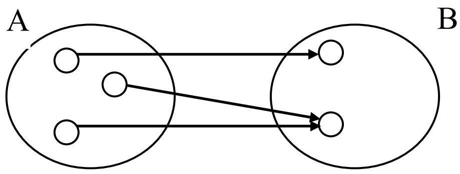

Рис. 1.2. Сюр'єкція

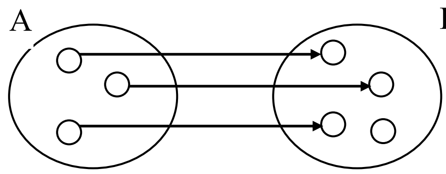

Рис 1.3. Ін'єкція

Означення 1.4. Відображення, яке одночасно є сюр'єктивним та ін'єктивним називається **бієкцією** (накладанням). У цьому випадку кажуть, що між елементами A та B існує взаємно однозначна відповідність (рис. 3.4).

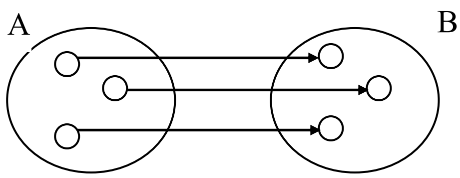

Рис 1.4. Бієкція

Якщо f – взаємно однозначне відображення, а A=B, то $f : A \to A$ називається відображенням множини A на себе. Елементи $(a,a) \in A \times A$ утворюють **тотожне відображення** E, причому $f \circ f^{-1} = f^{-1} \circ f = E$.

Означення 1.5. Відображення множини в її фактор-множину називається **канонічною сюр'єкцією.**

Наприклад, нехай A та B – множини дійсних чисел і $f : A \to B$ визначено таким чином: $f(a) = 3a + 5$. Функція f ін'єктивна, тому що якщо $f(a_1) = f(a_2)$, тоді $3a_1+5 = 3a_2+5$ і відповідно $a_1=a_2$. Функція f є також сюр'єкцією. Для будь-якого дійсного числа b треба знайти таке a, що $f(a) = b = 3a+5$. Розв'язуючи це рівняння відносно a, знаходимо, що якщо $a = (1/3)(b-5)$, тоді $f(a) = b$. Тому функція f представляє собою бієкцію або взаємно однозначне відповідність.

Розглянемо інший приклад. Нехай знову A та B – множини дійсних чисел а функція $f : A \to B$ визначена як $f(a) = a^2$. Функція f не є ін'єктивною, тому що $f(2) = f(-2)$, але $2 \neq -2$. Функція f не є також сюр'єкцією, тому що не існує такого дійсного числа a, для якого $f(a) = -1$. Відмітимо, що якщо A та B – множини невід'ємних дійсних чисел, то тоді f буде і сюр'єктивним, і ін'єктивним. У випадку коли A та B будуть множинами натуральних чисел, то f збереже ін'єктивність, але втратить сюр'єктивність.

Прикладом бієкційного, але не функціонального відображення є функція f : $\mathbf{R}^+ \to \mathbf{R}$, де $f(a) = \pm\sqrt{a}$.

Різні види кодування (подання чисел у різних системах числення, секретні шифри тощо) є відповідністю між об'єктами, що кодуються, і кодами, що присвоюються їм. Ця відповідність, як правило, має всі властивості взаємно однозначної відповідності, крім, може бути, однієї – сюр'єктивності. Єдність образу та прообразу в кодуванні гарантує однозначність шифрування і дешифрування. Відсутність сюр'єктивності означає, що не кожний код має значення, тобто відповідає якому-небудь об'єкту. Наприклад, кодування телефонів міста Києва семизначними номерами не є сюр'єктивним, оскільки деякі семизначні номери не відповідають жодним телефонам. У випадку коли мова йде про шифрування слів і не виконується умова ін'єкції, то це означає, що неможливо однозначно встановити початкове слово за його шифром або кодом.

Властивості відображень

Загалом при відображенні $f: A \to B$ елемент із B може бути образом не одного, а кількох елементів із A.

Означення 1.6. Сукупність усіх елементів, образом яких є заданий елемент b, називається **повним прообразом** елемента b і позначається f^{-1}(b). Сукупність елементів f(a), які є образами всіх елементів множини $C \subset A$, називається **образом множини** C та позначається f(C). Сукупність усіх елементів із A, образи яких належать якійсь множині $D \subset B$, називається **повним прообразом множини** D і позначається f^{-1}(D).

Наприклад, нехай A = {1,2,3,4} та B = {5, 6, 7, 8, 9}, а f = {(1,5), (2,6), (2,7), (3,8), (3,5)}. Тоді повним прообразом елемента "5" з множини B буде $f^{-1}(5)$ = {1,3}. Нехай також C = {1,2}. Тоді образ множини C буде f(C) = {5,6,7}. Нехай D = {6,7}. Тоді f^{-1}(D) = {2}.

Теорема 1.7. Нехай f є відображення $f: A \to B$. Тоді справедливі наступні властивості відображень:

а) Якщо $X \subset Y$, то $f(X) \subset f(Y)$, $f^{-1}(X) \subset f^{-1}(Y)$,

б) $f(X \cup Y) = f(X) \cup f(Y)$, $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$,

в) $f(X \setminus Y) = f(X) \setminus f(Y)$, $f^{-1}(X \setminus Y) = f^{-1}(X) \setminus f^{-1}(Y)$,

г) $f(X \cap Y) = f(X) \cap f(Y)$, $f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$,

д) $f^{-1}(X') = (f^{-1})'(X)$.

Доведення.

Розглянемо перше твердження пункту б) $f(X \cup Y) = f(X) \cup f(Y)$. Отримаємо наступне:

$f(a) \in f(X \cup Y) \Rightarrow a \in X \cup Y \Leftrightarrow a \in X$ або $a \in Y \Rightarrow f(a) \in f(X)$ або $f(a) \in f(Y) \Leftrightarrow f(a) \in f(X) \cup f(Y) \Rightarrow f(X \cup Y) \subseteq f(X) \cup f(Y)$.

$f(a) \in f(X) \cup f(Y) \Leftrightarrow f(a) \in f(X)$ або $f(a) \in f(Y) \Rightarrow a \in X$ або $a \in Y \Leftrightarrow a \in X \cup Y \Rightarrow f(a) \in f(X \cup Y) \Rightarrow f(X) \cup f(Y) \subseteq f(X \cup Y)$.

З цих двох результатів отримуємо, що $f(X \cup Y) = f(X) \cup f(Y)$.

Розглянемо друге твердження пункту б) $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$. Отримаємо наступне:

$a \in f^{-1}(X \cup Y) \Rightarrow f(a) \in X \cup Y \Leftrightarrow f(a) \in X$ або $f(a) \in Y \Rightarrow a \in f^{-1}(X)$ або $a \in f^{-1}(Y) \Leftrightarrow a \in f^{-1}(X) \cup f^{-1}(Y) \Rightarrow f^{-1}(X \cup Y) \subseteq f^{-1}(X) \cup f^{-1}(Y)$.

$a \in f^{-1}(X) \cup f^{-1}(Y) \Leftrightarrow a \in f^{-1}(X) \cup a \in f^{-1}(Y) \Rightarrow f(a) \in X$ або $f(a) \in Y \Leftrightarrow f(a) \in X \cup Y \Rightarrow$

$a \in f^{-1}(X \cup Y) \Rightarrow f^{-1}(X) \cup f^{-1}(Y) \subseteq f^{-1}(X \cup Y)$.

Тому отримуємо, що $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$.

Розглянемо перше твердження пункту в) $f(X \backslash Y) = f(X) \backslash f(Y)$. Отримаємо наступне доведення:

$f(a) \in f(X \backslash Y) \Rightarrow a \in X \backslash Y \Leftrightarrow a \in X$ та $a \notin Y \Rightarrow f(a) \in f(X)$ та $f(a) \notin f(X) \Leftrightarrow f(a) \in f(X) \backslash f(Y) \Rightarrow f(X \backslash Y) \subseteq f(X) \backslash f(Y)$,

Випадок зворотного включення $f(X) \backslash f(Y) \subseteq f(X \backslash Y)$ доводиться аналогічно і тому отримуємо, що $f(X \backslash Y) = f(X) \backslash f(Y)$.

Розглянемо друге твердження пункту г) $f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$. Отримаємо наступне доведення:

$a \in f^{-1}(X \cap Y) \Rightarrow f(a) \in X \cap Y \Leftrightarrow a \in X$ та $a \in Y \Rightarrow a \in f^{-1}(X)$ та $a \in f^{-1}(Y) \Leftrightarrow a \in f^{-1}(X) \cap f^{-1}(Y) \Rightarrow f^{-1}(X \cap Y) \subseteq f^{-1}(X) \cap f^{-1}(Y)$.

Випадок зворотного включення $f^{-1}(X) \cap f^{-1}(Y) \subseteq f^{-1}(X \cap Y)$ доводиться аналогічно і тому отримуємо, що $f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$.

Означення 3.7. Нехай функцію $f : A \to B$ задано на A, f_1 – на множині $C \subset A$, причому для кожного $a \in A$ виконується $f(a) = f_1(a)$. Тоді f_1 називається **обмеженням** (**звуженням**) функції f на C, а f – **продовженням** функції f_1 на A.

Наприклад, функція $f(a) = a^3$, яка задана на множині дійсних чисел, відображає цю множину на себе. Якщо ввести обмеження, щоб область визначення була лише множиною цілих чисел, то дістанемо звуження $f_1(a)$ функції $f(a)$ на цілих числах. Причому $f_1(a)$ відображає множину цілих чисел, але не на саму себе, оскільки не кожне ціле число є кубом самого себе.

Композиція відображень

Означення 1.8. Якщо $f : A \to B$, $g : B \to C$, то їх **композиція** $(g \circ f)$: $A \to C$, причому $(g \circ f)(a) = g(f(a))$. Іншими словами якщо існує множина пар $(a,b) \in f$ та $(b,c) \in g$, то множина пар $(a,c) \in f \circ g$ утворює композицію $(g \circ f)$.Запис $(g \circ f)$ проводиться в порядку, який є зворотнім до того, в якому виконується операції $f : A \to B$, $g : B \to C$. Таким чином, в математиці прийнято правило, згідно з яким композицію відображень $(g \circ f)$ треба починати з виконання операції f, яка розташована справа.

Наприклад, якщо $f = \sin$, $g = \ln$, то $(g \circ f)(a) = (\ln \circ \sin)(a) = \ln(\sin(a))$.

Легко показати, що композиція відображень асоціативна, тобто $(h \circ g) \circ f = h \circ (g \circ f)$ і записується у вигляді $h \circ g \circ f$. Так само легко з’ясувати, що композиція відображень не комутативне (це випливає з означення композиції відображень).

Теорема 1.9. Функція f є взаємно однозначним функціональним відношенням тоді і тільки тоді, коли f^{-1} – взаємно однозначне відношення.

Доведення. Доведемо, що f^{-1} – функція. Нехай $(b,a_1) \in f^{-1}$, $(b,a_2) \in f^{-1}$. за означенням оберненого відношення маємо $(a_1,b) \in f$, $(a_2,b) \in f$. Оскільки f за умовою є взаємно однозначною функцією, дістанемо $a_1 = a_2$, а це означає, що f^{-1} – функціональне відношення. Покажемо, що f^{-1} – взаємно однозначне функціональне відношення. Нехай $(b_1,a) \in f^{-1}$, $(b_2,a) \in f^{-1}$. Це означає, що $(a,b_1) \in f$, $(a,b_2) \in f$. Оскільки f – функція, маємо $b_1 = b_2$, а це означає, що f^{-1} є взаємно однозначним функціональним відношенням. Таким чином, необхідну умову теореми доведено.

Теорема 1.10. Композиція двох функціональних відношень є функціональним відношенням.

Доведення. Нехай $f : A \to B$, $g : B \to C$. За означенням композиції відношень $h = (g°f) = \{(a,c) \mid ((a,b) \in f$ та $(b,c) \in g\}$. Отже, це за означенням – підмножина декартового добутку A×C. Доведемо, що h – функціональне відношення. Нехай задано дві пари, які належать h:

$$\begin{cases} (a,c_1) \in h \Rightarrow \exists b_1 \in B \mid (a,b_1) \in f, (b_1,c_2) \in g; \\ (a,c_2) \in h \Rightarrow \exists b_2 \in B \mid (a,b_2) \in f, (b_2,c_2) \in g. \end{cases}$$

Оскільки f – функціональне відношення, маємо $b_1=b_2$, а оскільки g – функціональне відношення, дістаємо $c_1=c_2$. Отже h – функціональне відношення.

Означення 1.11. Функція, що утворюється з функцій $f_1, f_2,..., f_n$ деякою підстановкою їх одна в одну і перейменуванням аргументів, називається **суперпозицією** $f_1, f_2,..., f_n$.

Наприклад, у функції $f_1(a_1,a_2,a_3) = a_1+2a_2+7a_3$ перейменування a_3 в a_2 приводить до функції $f_1(a_1,a_2,a_2) = a_1+2a_2+7a_2 = f_2(a_1,a_2) = a_1+9a_2$. Перейменування a_1 та a_3 в a_2 приводить до одномісної функції $f_3(a_2) = 10a_2$.

На множині всіх перестановок (загальніше – на множині всіх кортежів довжиною n з елементами множини A'={1, 2, …, n}) означимо **лексикографічний порядок**: $a_1a_2…a_n < b_1b_2…b_n$, якщо для якогось k, $1 \le k \le n$, виконуються співвідношення $a_1=b_1$, $a_2=b_2$, ..., $a_{k-1}=b_{k-1}$, але $a_k<b_k$. У такому разі говорять, що перестановка $a_1a_2…a_n$ менша від перестановки $b_1b_2…b_n$, або перестановка $b_1b_2…b_n$ більша від перестановки $a_1a_2…a_n$. Якщо замість чисел 1, 2, …, n взяти літери a, b, …, z із природнім порядком a<b<…<z, то лексикографічний порядок – це стандартна послідовність, у якій слова довжиною n наведено в словнику.

Означення 1.12. Перестановку $b_1b_2…b_n$ називають **лексикографічно наступною** за $a_1a_2…a_n$, якщо не існує такої перестановки $c_1c_2…c_n$, що $a_1a_2…a_n < c_1c_2…c_n < b_1b_2…b_n$.

Наприклад, перестановка 23415 множини {1,2,3,4,5} менша від перестановки 23514.

Алгоритм генерування перестановок множини A'={1, 2, …, n} ґрунтується на процедурі, яка будує перестановку, лексикографічно наступну за даною перестановкою $a_1a_2\ldots a_n$. Покажемо, як це можна зробити. Спочатку припустимо, що $a_{n-1}<a_n$. Поміняємо місцями a_{n-1} та a_n і отримуємо більшу перестановку. Вона лексикографічно наступна, бо ніяка інша перестановка не більша за дану перестановку й не менша за отриману.

Наприклад, нехай 234156 – задана перестановка; тоді перестановка 234165 лексикографічно наступна.

Тепер розглянемо випадок $a_{n-1}>a_n$. Переглянемо останні три члени перестановки. Якщо $a_{n-2}<a_{n-1}$, то останні три члени можна переставити для отримання наступної перестановки. Поставимо менше з двох чисел a_{n-1} і a_n, яке, однак, більше, ніж a_{n-2}, на позиціюп n-2. Потім розмістимо число, яке залишилося, й a_{n-2} на останніх двох позиціях у висхідному порядку.

Наприклад, нехай 234165 – задана перестановка; тоді перестановка 234516 лексикографічно наступна.

Узагальнивши ці міркування, отримуємо такий алгоритм.

Алгоритм побудови лексикографічно наступної перестановки

1. Знайти такі числа a_j і a_{j+1}, що ($a_j<a_{j+1}$) та ($a_{j+1}>a_{j+2}>\ldots>a_n$). Для цього потрібно знайти в перестановці першу справа пару сусідніх чисел, у якій число, що ліворуч, менше від числа, що праворуч.
2. Записати в j-ту позицію таке найменше з чисел a_{j+1}, a_{j+2}, …, a_n, яке водночас більше, ніж a_j.
3. Записати у висхідному порядку число a_j і решту чисел a_{j+1}, a_{j+2},…, a_n у позиції j+1,…,n.

Обґрунтування алгоритму. Доведемо, що не існує перестановки, яка водночас більша від $a_1a_2\ldots a_n$, але менша від побудованої за цим алгоритмом. Це означає, що побудована перестановка дійсно лексикографічно наступна за даною перестановкою $a_1a_2\ldots a_n$. Справді, за наведеним алгоритмом нова перестановка збігається зі старою в позиціях 1, …, j-1. У j-й позиції нова перестановка містить a_k, а стара – a_j, причому $a_k>a_j$. Отже, нова перестановка лексикографічно більша від старої. Окрім того, вона перша в лексикографічному порядку з a_1, a_2, …, a_{j-1}, a_k у позиціях з 1 до j. Стара перестановка остання з a_1, a_2, …, a_{j-1} у цих самих позиціях. Згідно з алгоритмом a_k вибирають найменшим з a_{j+1}, a_{j+2}, …, a_n, але більшим, ніж a_j. Отже, не існує жодної перестановки між старою та новою.

Наприклад, побудуємо перестановку, наступну в лексикографічному порядку за 362541. Остання пара чисел, у якій перше число менше за друге, - 25. Отже, розглянемо послідовність чисел 541. Серед них найменше число, яке більше від 2, це – 4. Тепер 4 запишемо на місце 2, а решту чисел 251 розмістимо на останніх трьох позиціях у висхідному порядку: 364125.

Щоб побудувати всі n! перестановок множини A'={1, 2, …, n}, починаємо з лексикографічно найменшої перестановки 123…n і послідовно n!-1 разів виконуємо алгоритм побудови лексикографічно наступної перестановки.

Продемонструємо це на прикладі множини A' = {1, 2, 3, 4}. За наведеним алгоритмом буде побудована наступна послідовність перестановок: 1234, 1243, 1324, 1342, 1423, 1432, 2134, 2143, 2314, 2341, 2413, 2431, 3124, 3142, 3214, 3241, 3412, 3421, 4123, 4132, 4213, 4231, 4312, 4321. Як і очікувалось, кількість перестановок становить 4!=24.

Генерування сполучень

Розглянемо множину A'={1, 2, …, n}. Сполучення без повторень з n елементів по r – це r-елементна підмножина множини A'. Позаяк порядок запису елементів множини неістотний, то домовимося записувати елементи в кожному сполученні у висхідному порядку: наприклад, {3,5,1} будемо записувати як {1,3,5}. Отже, сполучення $\{a_1, a_2, \ldots, a_r\}$ розглядатимемо як рядок чисел $a_1a_2\ldots a_r$, причому $a_1<a_2<\ldots<a_r$.

Як і для перестановок, покажемо, як за даним сполученням знайти наступне відповідно до лексикографічного порядку. Припустимо, що n=5 та r=3. Якщо можна збільшити останню цифру перестановки, то так і будемо робити.

Тому, маючи рядок 123, його можна замінити на 124. Якщо ж маємо 125, останнє число збільшити не можна. Тому переходимо до наступного (справа) числа й дивимось, чи можна збільшити його. У даному разі це можна зробити: потрібно замінити 2 на 3. Проте ми прагнемо побудувати найменший рядок із тих, котрі більші 125. Тому збільшуємо останнє число (тобто 3) на 1 і записуємо результат у наступну позицію. Отже, перші два числа – 1 і 3, тому наступний рядок – 134. Припустимо, що є рядок 145. Останнє й передостаннє числа збільшити не можна. Проте перше число можна збільшити, тому замість 1 пишемо 2. Щоб зробити рядок мінімальним, як останні числа візьмемо 3 та 4, унаслідок чого отримаємо рядок 234.

Узагальнимо ці міркування. Значення останнього числа в рядку – найбільше можливе, якщо воно дорівнює $n = n - r + r$. Якщо останнє число – найбільше можливе, то передостаннє – найбільше можливо, якщо воно дорівнює $n - r + (r-1)$ або $n - r + i$, де $i = r-1$ – позиція числа. Загалом, значення кожного i-го числа найбільше можливе, якщо числа праворуч від нього – найбільші можливі, і це значення дорівнює $n - r + i$. Отже, переглядаємо рядок справа наліво й визначаємо, чи дорівнює значення i-го елемента $n - r + i$ (це максимальне значення, яке може бути в позиції i). Перше значення, яке не задовольняє цю умову, можна збільшити. Нехай, наприклад, це значення дорівнює m і займає j-ту позицію. Збільшуємо m на 1, а значення кожного елемента, який стоїть після j-го, дорівнює значенню попереднього елемента плюс 1. Тепер можемо сформулювати потрібний алгоритм.

Алгоритм побудови лексикографічно наступного сполучення

1. Знайти в рядку перший справа елемент a_i такий, що $a_i \neq n - r + i$.
2. Збільшити знайдений елемент a_i на 1.
3. Встановити значення елементів в позиціях $j = i+1, i+2, \ldots, r$ на $a_{j-1} + 1$.

Наприклад, нехай $A'=\{1,2,3,4,5,6\}$. Знайдемо сполучення, наступне за $\{1,2,5,6\}$ у лексикографічному порядку. Це сполучення подамо рядком 1256. Маємо $n=6$, $r=4$. Перший справа з таких елементів, що $a \neq 6 - 4 + i$, – це $a_2=2$.

Для обчислення наступного більшого сполучення збільшуємо a_2 на 1 й отримуємо $a_2=3$. Тепер нехай $a_3 = 3+1 = 4$ і $a_4 = 4+1 = 5$. Отже, наступне в лексикографічному порядку сполучення – те, що зображене рядком 1345.

Обґрунтування алгоритму. Доведемо, що наведений алгоритм дійсно будує наступне в лексикографічному порядку сполучення. Рядок чисел, яким подано лексикографічно наступне сполучення, відрізняється від рядка, що зображає дане сполучення, з позиції i, бо в даному сполученні в позиціях i+1, i+2, …, r є максимально можливі числа. Отже, a_i+1 – найменше можливе число, яке можна записати в позицію i, якщо хочемо отримати сполучення, більше від даного. Тоді $a_2 + 2$, … $a_i + r - i + 1$ – найменші можливі числа, які можна записати в позиціях від i+1 до r.

Продемонструємо наведений алгоритм на прикладі множини A’ = {1, 2, 3, 4, 5, 6}, коли потрібно знайти всі сполучення довжиною 4. За наведеним алгоритмом буде побудована наступна послідовність сполучень: 1234, 1235, 1236, 1245, 1246, 1256, 1345, 1346, 1356, 1456, 2345, 2346, 2356, 2456, 3456. Як і очікувалось, кількість сполучень становить $\frac{6!}{4!\cdot(6-4)!}=15$.

Коротко зупинимось на питанні генерування всіх розміщень з n елементів по r. Знову розглядатимемо цю задачу лише для множини A’={1,2,3,4,5,6}. Один із можливих способів її розв’язання такий. Використаємо алгоритм генерування лексикографічно наступного сполучення для побудови r-елементних сполучень n-елементної множини A’. Після кожної стадії, коли побудовано чергове r-сполучення, застосуємо r!-1 разів алгоритм побудови перестановки за умови n=r для побудови всіх перестановок елементів цього сполучення як r-елементної множини.

Генерування розбиттів множини

Опишемо алгоритм генерування всіх розбиттів множини. Ідею цього алгоритму найпростіше пояснити, сформулювавши його в рекурентній формі. Зазначимо спочатку, що кожне розбиття π множини {1, 2, …, n} однозначно задає розбиття π_{n-1} множини {1, 2, …, n-1}, яке одержане з π після вилучення елемента n із відповідного блока (і вилучення порожнього блока, якщо елемент n утворював одноелементний блок). Навпаки, якщо дано розбиття $\sigma = \{A_1,\ldots,A_k\}$ множини $\{1, 2, \ldots, n\text{-}1\}$, то легко знайти всі такі розбиття π_n множини $\{1, 2, \ldots, n\text{-}1, n\}$, що $\pi_{n-1} = \sigma$. Це розбиття:

$$
\begin{array}{lllll}
\{A_1, & A_2, & \ldots, & A_k, & \{n\}\} \\
\{A_1\cup\{n\}, & A_2, & \ldots, & A_k\} & \\
\{A_1, & A_2\cup\{n\}, & \ldots, & A_k\} & \\
\ldots & \ldots & \ldots & \ldots & \\
\{A_1, & A_2, & \ldots, & A_k\cup\{n\}\} &
\end{array}
$$

Наведені міркування підказують простий рекурентний спосіб генерування всіх розбиттів. Якщо дано список L_{n-1} усіх розбиттів множини $\{1, 2, \ldots, n\text{-}1\}$, то список L_n усіх розбиттів множини $\{1, 2, \ldots, n\text{-}1, n\}$ утворюють заміною кожного розбиття σ в списку L_{n-1} на відповідну йому послідовність з наведених вище.

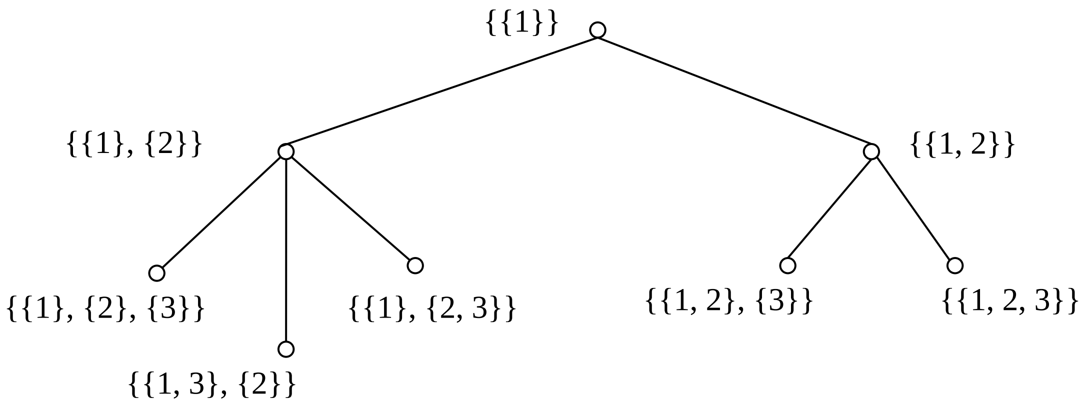

Рис. 1.2.

Наприклад, на рис. 1.2 показано формування списку всіх розбиттів множини $\{1, 2, 3\}$. Усього розбиттів $\Phi(3)=5$, де $\Phi(n)$ – число Белла.

Принцип включення-виключення

Цей принцип дає відповідь на запитання, як визначити кількість елементів у об’єднані множин. Для двох множин справджується формула

$$|A\cup B| = |A| + |B| – |A\cap B|.$$

Наприклад, знайдемо кількість додатних цілих чисел, що не перевищують 1000 та ділять на 7 або на 11. Позначимо як A множину чисел, які діляться на 7, B – множину чисел, які діляться на 11. Тоді

$$|A\cup B|=|A|+|B|-|A\cap B|=\left\lfloor\frac{1000}{7}\right\rfloor+\left\lfloor\frac{1000}{11}\right\rfloor-\left\lfloor\frac{1000}{7\cdot 11}\right\rfloor=142+90-12=220.$$

Для трьох множин формула для кількості елементів у їх об'єднанні ускладнюється:

$$|A\cup B\cup C| = |A| + |B| + |C| - |A\cap B| - |A\cap C| - |B\cap C| + |A\cap B\cap C|.$$

Теорема 1.13 (принцип включення-виключення). Нехай $A_1, A_2, \ldots, A_n$ – скінченні множини. Тоді

$$|A_1\cup A_2\cup\ldots\cup A_n|=\sum_{1\le i\le n}|A_i|-\sum_{1\le i<j\le n}|A_i\cap A_j|+$$
$$+\sum_{1\le i<j<k\le n}|A_i\cap A_j\cap A_k|-\ldots+(-1)^{n+1}|A_1\cap A_2\cap\ldots\cap A_n|.$$

Доведення. Достатньо довести, що кожний елемент в об'єднанні множин ураховано в правій частині рівності точно один раз. Припустимо, що елемент a належить рівно r множинам з $A_1, A_2, \ldots, A_n$, де $1\le r\le n$. Тоді цей елемент ураховано C_r^1 разів у $\sum_{1\le i\le n}|A_i|$, C_r^2 разів у $\sum_{1\le i\le j\le n}|A_i\cap A_j|$; загалом його враховано C_r^m разів під час сумування членів, які містять перетин m множин A_i. Отже, елемент a враховано точно $C_r^1-C_r^2+C_r^3-\ldots+(-1)^{r+1}C_r^r$ разів у виразі в правій частині рівності. За властивістю біноміальних коефіцієнтів $C_r^0-C_r^1+C_r^2-\ldots+(-1)^rC_r^r=0$. Отже, $C_r^0=C_r^1+C_r^2-\ldots+(-1)^{r+1}C_r^r$, але $C_r^0=1$ і тому $C_r^1+C_r^2-\ldots+(-1)^{r+1}C_r^r=1$. Це й означає, що кожний елемент об'єднання множин ураховано в правій частині рівності точно один раз.

Зазначимо, що формула включення-виключення містить 2^n-1 доданків, по одному для кожної непорожньої підмножини з $\{A_1, A_2, \ldots, A_n\}$.

Принцип включення-виключення можна розглянути в альтернативній формі. Ця форма є корисною, коли потрібно знайти кількість елементів заданої множини A, які не мають жодної з n властивостей $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Уведемо такі позначення:

- $A_i \subset A$ – підмножина елементів, які мають властивість α_i;
- $N(\alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{ik})$ – кількість елементів множини A, які водночас мають властивості $\alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{ik}$;
- $N(\overline{\alpha}_{i1}, \overline{\alpha}_{i2}, \ldots, \overline{\alpha}_{ik})$ – кількість елементів множини A, які не мають жодної з властивостей $\alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{ik}$;
- N – кількість елементів у заданій множин A.

Тоді очевидно,

$$N(\overline{\alpha}_1, \overline{\alpha}_2, \ldots, \overline{\alpha}_n) = N - |A_1 \cup A_2 \cup \ldots \cup A_n|.$$

За принципом включення-виключення можна записати

$$N(\overline{\alpha}_1, \overline{\alpha}_2, \ldots, \overline{\alpha}_n) = N - \sum_{1 \le i \le n} N(\alpha_i) + \sum_{1 \le i < j \le n} N(\alpha_i, \alpha_j) -$$
$$- \sum_{1 \le i < j < k \le n} N(\alpha_i, \alpha_j, \alpha_k) + \ldots + (-1)^n N(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Ця формула подає принцип включення-виключення в **альтернативній формі**.

Наприклад, знайдемо кількість розв’язків рівняння $x_1+x_2+x_3=11$ у невід’ємних цілих числах у разі обмежень $x_1 \le 3$, $x_2 \le 4$, $x_3 \le 6$.

Розглянемо альтернативі властивості.

- α_1: $x_1 \ge 4$;
- α_2: $x_2 \ge 5$;
- α_3: $x_3 \ge 7$.

Відома формула для знаходження кількості розв’язків, які водночас задовольняють нерівності $x_1 \le 3$, $x_2 \le 4$, $x_3 \le 6$:

$$N(\overline{\alpha}_1, \overline{\alpha}_2, \overline{\alpha}_3) = N - N(\alpha_1) - N(\alpha_2) - N(\alpha_3) +$$
$$+ N(\alpha_1, \alpha_2) + N(\alpha_1, \alpha_3) + N(\alpha_2, \alpha_3) - N(\alpha_1, \alpha_2, \alpha_3).$$

Далі маємо:

N = $\tilde{C}_3^{11} = C_{13}^{11} = 78$ (загальна кількість розв’язків);

N(α_1) = $\tilde{C}_3^{7} = C_9^{7} = 36$ (кількість розв’язків, які задовольняють умову $x_1 \geq 4$);

N(α_2) = $\tilde{C}_3^{6} = C_8^{6} = 28$ ($x_2 \geq 5$);

N(α_3) = $\tilde{C}_3^{4} = C_6^{4} = 15$ ($x_3 \geq 7$);

N(α_1, α_2) = $\tilde{C}_3^{2} = C_4^{2} = 6$ ($x_1 \geq 4$ та $x_2 \geq 5$);

N(α_1, α_3) = $\tilde{C}_3^{0} = 1$ ($x_1 \geq 4$ та $x_3 \geq 7$);

N(α_2, α_3) = 0 ($x_2 \geq 5$ та $x_3 \geq 7$);

N(α_1, α_2, α_3) = 0 ($x_1 \geq 4$ та $x_2 \geq 5$ та $x_3 \geq 7$).

Отже, кількість розв’язків із зазначеними обмеженнями дорівнює

$$N(\overline{\alpha}_1, \overline{\alpha}_2, \overline{\alpha}_3) = 78 - 36 - 28 - 15 + 6 + 1 + 0 - 0 = 6.$$

РОЗДІЛ ІІ. МАТРИЦІ ПОКАЗНИКІВ ТА ЛАТИНСЬКІ КВАДРАТИ

Нехай $M_n(\mathbb{Z})$ – це кільце з одиницею квадратних матриць розмірності n з натуральними абрнеульовими елементами.

Означення 2.1. [1]. Квадратна Матриця $\mathcal{E}=(\alpha_{ij})\in M_n(\mathbb{Z})$, для якої виконуються наступні умови:

1) $\alpha_{ij} + \alpha_{jk} \geq \alpha_{ik}$ для всіх $i, j, k =1, \dots , n,$

2) $\alpha_{ii} = 0$ для всіх $i=1, \dots , n,$називається *матрицею показників*.

Матриця показників, для якої виконується умова

3) $\alpha_{ij} + \alpha_{ji} \geq 1$ для всіх $i, j \in \{1,\dots , n\}$ $(i\neq j)$ називається *зведеною матрицею показників*.

Нехай $\mathcal{E}=(\alpha_{ij})$ – зведена матриця показників. Введемо матрицю $\mathcal{E}^{(1)}=(\beta_{ij})=\mathcal{E}+E_n \in M_n(\mathbb{Z}),$ де E_n – одинична матриця. Введемо матрицю $\mathcal{E}^{(2)}=(\gamma_{ij})\in M_n(\mathbb{Z})$: $\gamma_{ij}= \min\limits_k \{\beta_{ik}+\beta_{kj}\}$.

Означення 2.2. [1, c.357]. Сагайдаком зведеної матриці показників $Q=Q(\mathcal{E})$ називається сагайдак, матриця суміжності якого задається формулою $[Q]= \mathcal{E}^{(2)}- \mathcal{E}^{(1)}$.

Означення 2.3 Дві квадратні матриці показників $\mathcal{E}_1$ і $\mathcal{E}_2$ називається еквівалентними, якщо одну можна одержати з другої виконуючи послідовно елементарні перетворення двох типів:

1) Відняти натуральне число t від елементів $i^{го}$ рядка та добавити це число до елементів $i^{го}$ стовпчика,
2) Поміняти місцями два рядки і два стовпця з такими ж номерами.

чення **2.3.** [1].

Означення 2.4. [1, с.357]. Сагайдак Q називається *допустимим*, якщо існує зведена матриця показників $\mathcal{E}$, така що $Q(\mathcal{E})$ $=Q$. Сагайдак $Q=(VQ,\ AQ)$ називається зваженим, якщо визначена функція $\omega : AQ \to \square$. Функція ω називається ваговою, а її значення на стрілці називається вагою стрілки. Сума ваг всіх стрілок шляху називається вагою шляху.

Теорема 2.5. Сильно зв'язний сагайдак $Q = (VQ, AQ)$ є допустимим тоді і тільки тоді, коли існує вагова функція $\omega: AQ \to \mathbb{N} \cup \{0\}$, яка задовольняє наступним умовам:

1) вага стрілки з точки i у точку j менша за вагу шляху з точки i у точку j довжини $l \geq 2$;

2) вага петлі в точці i менше за вагу будь-якого циклу, що проходить через точку i, довжини $l \geq 2$;

3) вага будь-якого циклу більше або дорівнює 1;

4) вага петлі дорівнює 1,

5) через кожну точку без петлі проходить цикл довжини $l \geq 2$, вага якого дорівнює 1.

Зауваження 2.6. Легко бачити, що $[Q(\Gamma_\sigma)] = U_n - P_\sigma$.

Означення 2.7. Латинський квадрат порядку n– це квадратна матриця, у якої кожен ряжок і кожен стовпчик є перестановкою множини $S=\{s_1, \ldots, s_n\}$.

Далі будемо розглядати матриці з невід'ємними елементами. Якщо сагайдак одержується з матриці показників, яка є латинським квадратом, то будемо говорити, що сагайдак одержується з латинського квадрата.

Лема 2.8. Якщо матриця показників $\mathcal{E}=(\alpha_{ij})\in M_n(\mathbb{Z})$ є латинським квадратом то її сагайдак має петлю в кожній вершині.

Доведення. Припустимо протилежне, що у сагайдаку є вершина без петлі з номером "i". Тоді існує $k\in \{1, \ldots, n\}$, $k\neq i$ таке, що $\alpha_{ik}+\alpha_{ki}=1$. Звідси або $\alpha_{ik}=1$, або $\alpha_{ki}=1$. Оскільки $\alpha_{ii}=0$ (за означенням матриці показників), то у матриці $\mathcal{E}$

у рядку з номером k, або у стовпчику з номером k є два нулі. Що протирічить означенню латинського квадрата. Лема доведена.

Лема 2.9. Не для кожного допустимого сагайдака з петлею в кожній вершині існує матриця показників, яка є латинським квадратом з якої цей сагайдак одержується.

Доведення. Розглянемо матрицю показників $\mathcal{E}=\begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 1 \\ 2 & 1 & 0 \end{pmatrix}$. Матриця

суміжності сагайдака цієї матриці має вигляд : $[Q]=(q_{ij})=\begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$.

Доведемо, що цей сагайдак не може одержуватися з матриці показників, яка є латинським квадратом. Припустимо протилежне: нехай сагайдак

одержується з матриці показників $\mathcal{E}_L=\begin{pmatrix} 0 & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & 0 & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & 0 \end{pmatrix}$, яка є латинським

квадратом.

Оскільки $q_{13}=0$ то $\alpha_{13}=\alpha_{12+}\,\alpha_{23}$. Аналогічно з того, що $q_{31}=0$ випливає, що

$\alpha_{31}=\alpha_{32}+\alpha_{21}$. Отже, $\mathcal{E}_L=\begin{pmatrix} 0 & \alpha_{12} & \alpha_{12}+\alpha_{23} \\ \alpha_{21} & 0 & \alpha_{23} \\ \alpha_{32}+\alpha_{21} & \alpha_{32} & 0 \end{pmatrix}$.

Розглянемо два випадки:

Випадок 1. $\alpha_{12}\neq\alpha_{23}$. Тоді $0<\alpha_{12}$, $\alpha_{23}<\alpha_{12}+\alpha_{23}$. Латинський квадрат розмірності 3 не може містити 4 різних елемента. Одержали протиріччя.

Випадок 2. $\alpha_{12}=\alpha_{23}$. Тоді $\mathcal{E}_L=\begin{pmatrix} 0 & \alpha_{12} & 2\alpha_{12} \\ \alpha_{21} & 0 & \alpha_{12} \\ \alpha_{32}+\alpha_{21} & \alpha_{32} & 0 \end{pmatrix}$. Оскільки латинський квадрат розмірності 3 може складатися тільки з 3 різних елементів то ми одержуємо: $\alpha_{21}=2\alpha_{12}$, $\alpha_{32}=2\alpha_{12}$, $\mathcal{E}_L=\begin{pmatrix} 0 & \alpha_{12} & 2\alpha_{12} \\ 2\alpha_{12} & 0 & \alpha_{12} \\ 4\alpha_{12} & 2\alpha_{12} & 0 \end{pmatrix}$. Латинський квадрат складається з 4 різних елементів. Одержали протиріччя. Лема доведена**.**

Лема 2.10. Простий цикл із петлею в кожній вершині одержується з латинського квадрата.

Доведення. Розглянемо матрицю $\mathcal{E}_L=\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & ... & n-1 \\ n-1 & 0 & 1 & 2 & 3 & ... & n-2 \\ n-2 & n-1 & 0 & 1 & 2 & ... & n-3 \\ n-3 & n-2 & n-1 & 0 & 1 & ... & n-4 \\ n-4 & n-3 & n-2 & n-1 & 0 & ... & n-5 \\ ... & ... & ... & ... & ... & ... & ... \\ 1 & 2 & 3 & 4 & 5 & ... & 0 \end{pmatrix}$

тобто $\mathcal{E}_L=P_\sigma+2P_{\sigma^2}+...+(n-1)P_{\sigma^{n-1}}$, де P_σ – матриця підстановки σ=(1 2 3… n- -1). Легко переконатися, що $\mathcal{E}_L$ – латинський квадрат і матриця показників. Матриця суміжності сагайдака матриця показників має вигляд

$[Q(\mathcal{E}_L)]=\begin{pmatrix} 1 & 1 & 0 & ... & 0 & 0 \\ 0 & 1 & 1 & ... & 0 & 0 \\ 0 & 0 & 1 & ... & 0 & 0 \\ ... & ... & ... & ... & ... & ... \\ 0 & 0 & 0 & ... & 1 & 1 \\ 1 & 0 & 0 & ... & 0 & 1 \end{pmatrix}$. Отже, $Q(\mathcal{E}_L)$ – цикл із петлею в кожній вершині. Лема доведена.

Лема 2.11. Повний сагайдак з петлею в кожній вершині одержується з латинського квадрата.

Доведення. $L_n=nP_\sigma+(n+1)P_{\sigma^2}+(n+2)P_{\sigma^3}+...+(2n-2)P_{\sigma^{n-1}}$, де P_σ – матриця підстановки σ=(1 2 3… n-1).

Наприклад L_7= $\begin{pmatrix} 0 & 7 & 8 & 9 & 10 & 11 & 12 \\ 12 & 0 & 7 & 8 & 9 & 10 & 11 \\ 11 & 12 & 0 & 7 & 8 & 9 & 10 \\ 10 & 11 & 12 & 0 & 7 & 8 & 9 \\ 9 & 10 & 11 & 12 & 0 & 7 & 8 \\ 8 & 9 & 10 & 11 & 12 & 0 & 7 \\ 7 & 8 & 9 & 10 & 11 & 12 & 0 \end{pmatrix}$.

Кожен рядок та стовпчик матриці L_n складається з елементів множини $\{0, n, n+1, \ldots ,2n-2\}$. Тому L_n – латинський квадрат.

Доведемо, що $L_n =(\alpha_{ij})$ – матриця показників.

1) Очевидно, що α_{ii}=0 для всіх i та $\alpha_{ij}+ \alpha_{ji} \geq 2$ для всіх $i \neq j$.
2) Доведемо, що $\alpha_{ij} + \alpha_{jk} \geq \alpha_{ik}$ для всіх i, j, k =1, … , n. Якщо $i=j$, або $j=k$, або $i=k$, то нерівність очевидна. Якщо три індекси попарно різні, то $n \leq \alpha_{ij}$, α_{jk} , $\alpha_{ik} \leq 2n$-2, і тому $\alpha_{ij} + \alpha_{jk} \geq 2n > 2n-2 \geq \alpha_{ik}$. Отже, $\alpha_{ij} + \alpha_{jk} > \alpha_{ik}$.

З 1) та 2) випливає, що L_n – матриця показників. Крім того для довільних різних i, j, k виконується строга нерівність $\alpha_{ij} + \alpha_{jk} > \alpha_{ik}$. Тому $Q(L_n)$ – повний сагайдак**.** Лема доведена**.**

В попередньому розділі доведено, що існують сагайдаки, які одержуються тільки з горенштейнових матриць. Виникає питання: чи існує сагайдаки які одержуються тільки з латинських квадратів? Для відповіді на це питання дослідимо, як на латинський квадрат, який є матрицею показників, діють елементарні перетворення першого та другого типу.

Лема 2.12. Після виконанням над латинським квадратом, який є матрицею показників, елементарного не тотожного перетворення першого типу нова матриця показників не є латинським квадратом.

Доведення. Нехай елементи латинського квадрата є числа $0<\alpha_1< \alpha_2<\ldots< \alpha_{n-1}$. Виконаємо елементарне перетворення першого типу: від елементів першого рядка віднімемо число k та до елементів першого стовпчика додамо число k (для інших рядків та стовпчиків міркування аналогічні). Не зменшуючи загальності можна вважати, що $k>0$. Після перетворення рядок містить елементи 0, α_1-k, α_2-k , …, α_{n-1}-k. Якщо α_1-k=0, то матриця не є латинським квадратом бо в першому рядку два нуля. Якщо α_1-$k\neq 0$ то латинський квадрат містить стовпчик 0, α_1+k, α_2+k , …, $\alpha_{n-1}+k$ та елемент α_1-$k\neq 0$. При цьому α_1-k< α_1+k, α_2+k , …, $\alpha_{n-1}+k$, тобто елемент α_1-k не співпадає з жодним елементом стовпчика 0, α_1+k, α_2+k , …, $\alpha_{n-1}+k$. Тому латинський квадрат містить не менше (n+1)-го різного елемента. Отже, матриця не є латинським квадратом. Лема доведена.

Наслідок 2.13. Не існує допустимих сагайдаків, які одержуються тільки з латинських квадратів.

Доведення. Нехай Q – допустимий сагайдак, який одержується з латинського квадрата L. Тоді елементарне не тотожне перетворення першого типу перетворює латинський квадрат L у матрицю показників $\mathcal{E}$, яка за лемою 3.2 не є латинським квадратом. Але, $Q(L)= Q(\mathcal{E})$, де $\mathcal{E}$ – не є латинським квадратом. Наслідок доведений.

Лема 2.14. Елементарне перетворення другого типу залишає латинський квадрат латинським квадратом.

Доведення. Виконаємо елементарне перетворення другого типу матриці L. Поміняємо місцями два рядки. При цьому нова матриця $L^/$ буде складатися з тих же рядків, що й матриця L, але рядки записані у іншому порядку тому в кожному рядку матриці $L^/$ всі елементи різні. Кожен стовпчик матриці $L^/$ можна отримати з відповідного стовпчика матриці L помінявши в ньому два елемента місцями, тому кожен стовпчик матриці $L^/$ складається з різних елементів. Отже, $L^/$ – латинський квадрат. З аналогічних міркувань випливає, що після того, як в $L^/$ два стовпчика поміняти місцями знову одержується латинський квадрат. Лема доведена.

Лема 2.15. Нехай циклічна підстановка σ задана на множині $\{1, 2, \ldots, n\}$. Тоді матриця $L=\left(\alpha_{i\,j}\right)=\sum_{i=1}^{n-1}\rho_i P_{\sigma^i}$ є латинським квадратом для попарно різних ненульових ρ_i.

Доведення. Оскільки підстановка σ – циклічна підстановка, то її можна задати циклом $\left(i_1, i_2, \ldots, i_n\right)$, де $1 \le i_1, i_2, \ldots, i_n \le n$, та всі елементи $i_1, i_2, \ldots, i_n$ різні між собою. Не зменшуючи загальності можна вважати, що $i_1=1$ (випадок, коли одиниці дорівнює інший елемент циклу розглядається аналогічно). За умовою леми $L=\left(\alpha_{i\,j}\right)=\sum_{i=1}^{n-1}\rho_i P_{\sigma^i}$. Оскільки $P_{\sigma^j}=\sum_{k=1}^{n} e_{i_k \sigma^j(i_k)}$, то

$$a_{i_1\sigma^j(i_1)}=a_{i_2\sigma^j(i_2)}=\ldots=a_{i_n\sigma^j(i_n)}=p_j$$

Елементи $a_{i_1\sigma^j(i_1)}, a_{i_2\sigma^j(i_2)}, \ldots, a_{i_n\sigma^j(i_n)}$ рівні між собою, але стоять у різних рядках і у різних стовпчиках. Отже, кожне рядок і кожен стовпчик є перестановкою множини $\{0, p_1, p_2, \ldots, p_{n-1}\}$. Тому матриця L є латинським квадратом. Лема доведена.

З попередніх лем випливає, що існують допустимі сагайдаки, які одержуються з латинських квадратів, та допустимі сагайдаки, які не одержуються з латинських квадратів. Розглянемо клас допустимих сагайдаків, які одержуються з латинських квадратів.

Означення 2.16. Латинський квадрат порядку n– це квадратна матриця, у якої кожен ряжок і кожен стовпчик є перестановкою множини $S=\{s_1, \ldots, s_n\}$.

Далі будемо розглядати матриці з невід'ємними елементами. Якщо сагайдак одержується з матриці показників, яка є латинським квадратом, то будемо говорити, що сагайдак одержується з латинського квадрата.

Лема 2.17. [6]. Якщо матриця показників $\mathcal{E}=(\alpha_{ij})\in M_n(\mathbb{Z})$ є латинським квадратом то її сагайдак має петлю в кожній вершині.

Лема 2.18. [6]. Не для кожного допустимого сагайдака з петлею в кожній вершині існує матриця показників, яка є латинським квадратом з якої цей сагайдак одержується.

Лема 2.19. [6]. Простий цикл із петлею в кожній вершині одержується з латинського квадрата.

Лема 2.20. [6]. Повний сагайдак з петлею в кожній вершині одержується з латинського квадрата.

Лема 2.21. [6]. Після виконанням над латинським квадратом, який є матрицею показників, елементарного не тотожного перетворення першого типу нова матриця показників не є латинським квадратом.

Наслідок 2.22. [6]. Не існує допустимих сагайдаків, які одержуються тільки з латинських квадратів.

Доведення. Нехай Q – допустимий сагайдак, який одержується з латинського квадрата L. Тоді елементарне не тотожне перетворення першого типу перетворює латинський квадрат L у матрицю показників $\mathcal{E}$, яка за лемою 3.2 не є латинським квадратом. Але, $Q(L)= Q(\mathcal{E})$, де $\mathcal{E}$ – не є латинським квадратом. Наслідок доведений.

Лема 2.23. [6]. Елементарне перетворення другого типу залишає латинський квадрат латинським квадратом.

Лема 2.24. [6]. Нехай циклічна підстановка σ задана на множині $\{1, 2, \ldots, n\}$. Тоді матриця $L=\left(\alpha_{ij}\right)=\sum\limits_{i=1}^{n-1}\rho_i P_{\sigma^i}$ є латинським квадратом для попарно різних ненульових ρ_i.

Теорема 2.25. [6]. Нехай матриця суміжності $[Q]=(q_{ij})$ сагайдака Q має вигляд

$[Q]= E + P_\tau + q_{13}P_{\tau^2} + q_{14}P_{\tau^3} + \ldots + q_{1n}P_{\tau^{n-1}}$, де $q_{ij}\in\{0, 1\}$, P_τ – матриця циклічної підстановки $\tau = (1, 2, \ldots, n)$. Тоді існує матриця показників $\mathcal{E}=(\alpha_{ij})$ вигляду

$\mathcal{E}= \alpha_{12}P_{\tau}+\alpha_{13}P_{\tau^2}+\alpha_{14}P_{\tau^3}+\ldots+\alpha_{1n}P_{\tau^{n-1}}$ сагайдак якої $Q(\mathcal{E})$ співпадає з сагайдаком Q.

Навпаки, якщо зведена матриця показників має вигляд $\mathcal{E}= \alpha_{12}P_{\tau}+\alpha_{13}P_{\tau^2}+\alpha_{14}P_{\tau^3}+\ldots+\alpha_{1n}P_{\tau^{n-1}}$, де $\tau=(1, 2, \ldots, n)$, $1\le\alpha_{12}\le\alpha_{13}\le\ldots\le\alpha_{1n}$, то матриця суміжності $[Q(\mathcal{E})]$ сагайдака $Q(\mathcal{E})$ має вигляд

$[Q]= E+P_{\tau}+P_{\tau^{i_1-1}}+P_{\tau^{i_2-1}}+\ldots+P_{\tau^{i_p-1}}$..

Зауваження 2.26. [6]. Для довільного сагайдака Q з матрицею суміжності $[Q]=E+P_{\tau}+q_{13}P_{\tau^2}+\ldots+q_{1n}P_{\tau^{n-1}}$, *де* $q_{ij}\in\{0,1\}$, P_{τ} - матриця циклічної підстановки

Теорема 2.27. [6]. *Нехай матриця суміжності* $[Q]=(q_{ij})$ *сагайдака* Q *має вигляд* $[Q]=E+P_{\tau}+q_{13}P_{\tau^2}+\ldots+q_{1n}P_{\tau^{n-1}}$, *де* $q_{ij}\in\{0,1\}$, P_{τ} - *матриця циклічної підстановки* $\tau=(1\,2\ldots n)$. *Тоді існує зведена матриця показників* $\mathcal{E}$, *яка є латинським квадратом, і сагайдак якої* $Q(\varepsilon)$ *співпадає з сагайдаком* Q.

Лема 2.28. [6]. Для горенштейнового латинського квадрата $L=(\alpha_{ij})$ з підстановкою Кириченка σ існує таке число c, що $\alpha_{i\sigma(i)}=c$, для $i=1, \ldots, n$.

Лема 2.29. [6]. Нехай L горенштейновий латинський квадрат з циклічною підстановкою σ тоді $L=\left(\alpha_{ij}\right)=\sum_{i=1}^{n-1}\rho_i P_{\sigma^i}$.

Теорема 2.30. [6]. Підстановка Кириченка горенштейнового латинського квадрата $L=(\alpha_{ij})$ не може містити двох циклів взаємно простої довжини.

РОЗДІЛ III. КІЛЬЯЦЯ ТА МОДУЛІ

Модуль *M* називається *дистрибутивним*, якщо структура його підмодулів дистрибутивна, тобто для довільних підмодулів *K, L, N* виконується

$$K \bigcap (L+N) = K \bigcap L + K \bigcap N\,.$$

Очевидно, що довільний підмодуль чи фактор-модуль дистрибутивного модуля є дистрибутивними модулями. Напівдистрибутивний модуль – це пряма сума дистрибутивних модулів.

Кільце А називається *напівдистрибутивним справа (зліва*), якщо воно напівдистрибутивне як правий (лівий) модуль над самим собою. Кільце А є напівдистрибутивним, якщо воно напівдистрибутивне зліва та справа водночас.

Теорема 3.1. [2]. Модуль дистрибутивний тоді й тільки тоді, коли цоколь кожного фактормодуля містить не більше одного екземпляра кожного з простих модулів.

Теорема 3.2. [2]. Напівдосконале кільце *A* є правим (лівим) напівдистрибутивним тоді й тільки тоді, коли для кожних двох локальних ідемпотентів *e* та *f* кільця *A* множина *eAf* є ланцюговим правим *fAf*-модулем (лівим *eAe*-модулем).

Наслідок 3.3. Нехай *A* – напівдосконале кільце, $1=\varepsilon_1+...+\varepsilon_n$ – розклад одиниці кільця *A* у суму взаємно ортогональних локальних ідемпотентів. Кільце *A* напівдистрибутивне справа (зліва) тоді й тільки тоді, якщо для довільних ідемпотентів e_i та e_j *(i≠j)* вищезгаданого розкладу кільце $(e_i+e_j)A(e_i+e_j)$ є напівдистрибутивним справа (зліва).

Надалі ми вживатимемо позначення *SPSD*-кільця для напівдосконалих напівдистрибутивних кілець та *SPSDL*-кільця та *SPSDR*-кільця для напівдосконалих напівдистрибутивних зліва та справа кілець відповідно.

Теорема 3.4. [4]. Кожне напівмаксимальне кільце ізоморфне скінченному прямому добуткові первинних кілець наступного вигляду:

$$\Lambda = \begin{pmatrix} O & \pi^{a_{12}}O & \dots & \pi^{a_{1n}}O \\ \pi^{a_{21}}O & O & \dots & \pi^{a_{22n}}O \\ \pi^{a_{n1}}O & \pi^{a_{n2}}O & \dots & O \end{pmatrix}, \ (*)$$

де $n \geq 1$. O – дискретне нормоване кільце з простим елементом π; a_{ij} – цілі та такі, що для довільних i,j,k: $\alpha_{ij} + \alpha_{jk} \geq \alpha_{ik}$

Кільце O вкладене в классичне кільце часток D, а формула (*) вказує на те, що Λ - матриця з $M_n(D)$ така, що

$$\Lambda = (a_{ij}), \quad a_{ij} \in \pi^{\alpha_{ij}} O = e_{ii} \Lambda e_{jj}$$

де $e_{11},...e_{nn}$ – елементи матриці $M_n(D)$. Первинне напівмаксимальне кільце називається черепичним порядком. Очевидно, що черепичний порядок Λ над дискретним нормованим кільцем O є нетеровим зліва. Також ясно, що $M_n(D)$ - класичне кільце часток кільця Λ.

Теорема 3.5. Наступні умови для напівдосконалого напівпростого нетерового справа кільця A є еквівалентними:

1). Кільце A напівдистрибутивне;

2). Кільце A – прямий добуток напівпростих артінових кілець і напівмаксимальних кілець.

Звідси маємо, що черепичні порядки над дискретно нормованим кільцем співпадають з нетеровими (але не артиновими) первинними *SPSD*-кільцями.

Позначимо за $M_n(Z)$ кільце усіх квадратних матриць над кільцем цілих чисел $\boldsymbol{Z}$. Нехай $\varepsilon \in M_n(Z)$. Називатимемо матрицю $\varepsilon = (a_{ij})$ *матрицею показників*, якщо $a_{ij} + a_{jk} \geq a_{ik}$, для $i, j, k=1,..,n$, $a_{ii} = 0, \forall i = 1...n$

Матрицю ε називатимемо *зведеною матрицею показників*, якщо $a_{ij}+a_{ji}>0$, для $i,j=1,\ldots,n$.

Ми використовуватимемо надалі такий запис: Λ={*O*, ε(Λ)}, де ε(Λ)= (a_{ij}) – матриця показників кільця Λ, тобто $\Lambda=\sum_{i,j=1}^{n} e_{ij}\pi^{\alpha_{ij}}O$, де e_{ij} –матричні одиниці.

Якщо черепичний порядок зведений, то $a_{ij}+a_{ji}\geq 0$, для $i,j=1\ldots n$, тобто, ε(Λ) зведена.

Означення 3.6. Правий (лівий) Λ-модуль *M* (*N*) називається *правою* (*лівою*) Λ-*граткою*, якщо *M* (*N*) є скінченно породженим вільним *O*-модулем.

Наприклад, усі скінченно породжені проективні Λ-модулі є Λ-гратками.

Для даного черепичного порядку Λ ми позначимо $Lat_r(Z)$ (відповідно $Lat_l(Z)$) категорію правих (лівих) Λ-граток. Позначимо $S_r(\Lambda)$ (відповідно $S_l(\Lambda)$) частково впорядковану за включенням множину, утворену усіма Λ-гратками, що містяться у фіксованому простому $M_n(D)$-модулі ***W*** (відповідно для лівого фіксованого простого $M_n(D)$-модуля ***V***). Такі Λ-гратки називаються *незвідними*.

Нехай Λ= {*O*, ε(Λ)} черепичний порядок, ***W*** (***V***)– простий правий (лівий) $M_n(D)$–модуль з *D*-базисом $e_1\ldots e_n$, таким, що $e_i e_{jk}=\delta_{ij}e_k$.

Тоді довільну праву (ліву) незвідну Λ-гратку *M* (відповідно N), що лежить в ***W*** (відповідно в ***V***) можна розглядати як Λ-модуль з *O*-базисом $(\pi^{\alpha_1}e_1,\ldots,\pi^{\alpha_n}e_n)$, де

$$\begin{cases}\alpha_i+\alpha_{ij}\geq\alpha_j,\\ \alpha_{ij}+\alpha_j\geq\alpha_i,\end{cases}\qquad (**)$$

для правого та лівого випадків відповідно.

Тобто, незвідні Λ-структури *M* можна ототожнити з векторами, що задовільняють формулі (**).

Надалі писатимемо [*M*]=$(\alpha_1\ldots\alpha_n)$ або *M*=$(\alpha_1\ldots\alpha_n)$.

Відношення впорядкованості у множині таких векторів і операцій з ними відповідають сумі та перетину незвідних граток.

Зауваження 3.7. Очевидно, що незвідні Λ-гратки $M_1 = (\alpha_1 ... \alpha_n)$ та $M_2 = (\beta_1 ... \beta_n)$ ізоморфні тоді й тільки тоді, коли $\alpha_i = \beta_i + z, \forall z \in \mathrm{Z}$.

Твердження 3.8. [4]**.** Частково впорядковані множини $S_r(\Lambda)$ та $S_l(\Lambda)$ є анти-ізоморфними дистрибутивними гратками.

Доведення: оскільки Λ є напівдистрибутивним кільцем, то $S_r(\Lambda)$ (відповідно $S_l(\Lambda)$) – дистрибутивна структура відносно суми та перетину підмодулів.

Нехай $M = (\alpha_1 ... \alpha_n) \in S_r(\Lambda)$. Тоді $M^* = (-\alpha_1 ... -\alpha_n)^T \in S_l(\Lambda)$.

Якщо $N = (\beta_1 ... \beta_n)^T \in S_l(\Lambda)$, то $N^* = (-\beta_1 ... -\beta_n) \in S_r(\Lambda)$, отже, операція * задовольняє наступним умовам:

1). *M**=M.*

2). $(M_1 + M_2)^* = M_1^* \cap M_2^*$.

3). $(M_1 \cap M_2)^* = M_1^* + M_2^*$.

Умови виконуються для правого і, аналогічно, для лівого випадків.

Отже, відображення $*: Sr(\Lambda) \to Sl(\Lambda)$ - анти-ізоморфізм.

Означення 3.9. Пряму суму незвідних Λ-граток називатимемо *повністю розкладною Λ-граткою.*

Нехай $L = M_1 \oplus M_2 \oplus ... \oplus M_p$ буде правою повністю розкладеною Λ-граткою, а $K = N_1 \oplus N_2 \oplus ... \oplus N_q$ - лівою. Тоді L^* буде лівою, а K^* - правою повністю розкладною Λ-граткою.

Черепичний порядок $\Lambda = \sum_{i,j=1}^{n} e_{ij} \pi^{\alpha_{ij}} O$ є водночас лівою та правою повністю розкладною Λ-граткою та лежить в $\widetilde{\Lambda} = M_n(D)$.

Проективна Λ-гратка (тобто, скінченнопороджений проективний Λ-модуль) є повністю розкладною Λ-граткою.

Означення 3.10. Повністю розкладна Λ-гратка *M* називається *відносно ін'єктивною*, якщо *M=P*,* де *P* – проективна Λ-гратка.

Означення 3.11. Черепичний порядок Λ називається *горенштейновим черепичним порядком*, якщо Λ^*_Λ - проективна ліва Λ-гратка.

Зауваження 3.12. Очевидно, що Λ^*_Λ - проективна ліва Λ-гратка тоді й тільки тоді, коли $_\Lambda\Lambda^*$ - проективна права гратка. Надалі замість "горенштейнові черепичні порядки" вживатиметься "горенштейнові порядки".

Теорема 3.13. [4].Нехай $\Lambda = \{O, \varepsilon(\Lambda) = (\alpha_{pq})\}$ - зведений черепичний порядок. Тоді наступні твердження еквівалентні:

1). Λ - горенштейнів порядок.

2). Існує перестановка $\sigma = \{i \to \sigma(i)\}$, $\alpha_{ik} + \alpha_{k\sigma(i)} = \alpha_{i\sigma(i)}$ для $i, k = 1, \ldots, n$.

Зауважимо, що перестановка $\sigma(\Lambda)$ зведеного горенштейнового порядку не містить циклів довжиною 1.

Означення 3.14. Горенштейнів порядок Λ називається *циклічним*, якщо перестановка $\sigma(\Lambda)$ - цикл.

Позначимо за $M_r(\Lambda)$ (відповідно - $M_l(\Lambda)$) частково обмежену підмножину гратки $S_r(\Lambda)$ $(S_l(\Lambda))$, що утворена усіма проективними Λ-модулями, які містяться в $S_r(\Lambda)$ $(S_l(\Lambda))$.

Твердження 3.15. [2]. Незвідна Λ-гратка *M* з $S_r(\Lambda)$ (відповідно *N* з $(S_l(\Lambda))$) проективна тоді й тільки тоді, коли вона містить єдиного максимального підмодуля.

Покладемо $M \in S_r(\Lambda)$, $M^* \in S_l(\Lambda)$

Твердження 3.16. [2]. Черепичний порядок Λ є горенштейновим тоді й тільки тоді, якщо обмеження відображення $*: S_r(\Lambda) \to S_l(\Lambda)$ на $M_r(\Lambda)$ анти-ізоморфізм частково впорядкованих множин $M_r(\Lambda)$ та $M_l(\Lambda)$.

Звісно, в загальному випадку частково впорядковані множини $M_r(\Lambda)$ та $M_l(\Lambda)$ анти-ізоморфні, але не завжди цей анти-ізоморфізм може бути розширений до анти-ізоморфізму $S_r(\Lambda) \to S_l(\Lambda)$.

Нехай P - довільна частково впорядкована множина. Підмножина P називається *ланцюгом* (*лінійно впорядкованою множиною*), якщо її довільні два елементи порівнюються. Підмножина P називається *анти-ланцюгом,* якщо у ній не існує жодної пари елементів, між якими існує відношення порівняння.

Надалі використовуватимо для позначення ланцюга з n елементів CH_n, для анти-ланцюга з n елементів ACH_n.

Теорема 3.17. [2]. Для заданої множини P найменша кількість ланцюгів, що містять усі елементи P, дорівнює кількості елементів найбільшого анти-ланцюга, якщо вона скінченна.

Означення 3.18. Найбільшу кількість елементів анти-ланцюга частково впорядкованої множини P називають її *шириною* (*довжиною*). Позначимо надалі ширину P через $w(P)$.

Нехай P – довільна частково впорядкована множина. Тоді можна утворити непорожню множину $\widetilde{P}$, елементами якої є усі непорожні підмножини P, які містять попарно непорівнювані елементи. Якщо $A, B \in \widetilde{P}$, то $A \le B$ тоді й тільки тоді, коли для довільного елемента a з A існує такий b з B, що $a \le b$. Тоді P природньо вкладається в $\widetilde{P}$: довільний елемент $a \in P$ відображається у $\{a\}$.

Приклад. Якщо P – анти-ланцюг довжини n, то $\widetilde{P}$ - частково впорядкована множина усіх непорожніх підмножин P , частково впорядкована за включенням.

Твердження 3.19. [4]. Множина $\widetilde{M}_r(\Lambda)$ - гратка. Тоді існує природній ізоморфізм граток $\widetilde{M}_r(\Lambda)$ і $S_r(\Lambda)$, який тотожній $M_r(\Lambda)$ (для лівого випадку – аналогічно).

Позначимо $VQ=\{1,...,s\}$ множину усіх вершин *Q*, а за AQ – множину решти елементів *Q* (тобто, стрілок). Писатимемо, що $Q=\{VQ,AQ\}$. Позначимо за *1,…,s* вершини сагайдака *Q* , а за t_{ij} - кількість стрілок, що починаються у вершині *i*, а закінчуються у вершині *j*.

Матрицю

$$[Q]=\begin{pmatrix} t_{11} & t_{12} & \dots & t_{1s} \\ t_{21} & t_{22} & \dots & t_{2s} \\ \dots & \dots & \dots & \dots \\ t_{s1} & t_{s2} & \dots & t_{ss} \end{pmatrix}$$

називатимемо *матрицею суміжності* для сагайдака *Q*.

Нехай *Q* – сагайдак. Вершини *Q* позначатимемо за *1,…,s*. Стрілка σ з'єднує вершину *i* з *j*. Тоді *i* називаєтсья початковою вершиною, а *j* – кінцевою вершиною стрілки. Позначатимемо це так: $\sigma : i \to j$. *Шляхом* сагайдаку *Q* від *i* до *j* є обмежена множина *k* стрілок $\{\sigma_1,...,\sigma_k\}$, таких, що початкова точка кожної стрілки є кінцевою для попередньої, σ_1 починається у вершині *i*, а σ_k закінчується у вершині *j*. Кількість стрілок *k* називається *довжиною* шляху. Тоді вершина *i* називається початком шляху, а вершина *j* – його кінцем. Говоритимемо, що шлях з'єднує вершини *i* та *j* та позначатимемо $\sigma_1\sigma_2...\sigma_k : i \to j$.

Нехай *A* – напівдосконале нетерове справа кільце, *R* – радикал Джекобсона, $P_1,...P_n$ - попарно неізоморфні проективні нерозкладні модулі. Нехай проективним накриттям $P_{i1}R$ буде

$$P\left(P_iR\right)=\bigoplus_{j=1}^{s} P_j^{t_{ij}}, \quad i,j=1,...,s.$$

Поставимо у відповідність $P_1,...P_n$ вершинам *1,…,s*. Вершини *i* та *j* з'єднані за допомогою t_{ij} стрілок. Отриманий граф будемо називати *сагайдаком* нетерового справа напівдосконалого кільця *A* [7] та позначати як *Q(A)*.

Аналогічно можна визначити лівого сагайдака нетерового зліва напівдосконалого кільця $Q'(A)$.

З означення проективного накриття випливає, що $Q(A)=Q(A/R^2)$.

Зазначимо, що сагайдак напівдосконалого кільця інваріантний відносно Моріта-еквівалентності.

Твердження 3.20. [2]. Нехай *A*– напівдосконале кільце, таке, що фактор-кільце A/R^2 артінове справа та зліва водночас. Тоді

1). Якщо *Q(A)* (правий сагайдак) має стрілку з *i* в *j*, то лівий сагайдак $Q'(A)$ також має стрілку з *i* в *j*.

2). Якщо *Q(A)* має стрілку σ_{ij}, то існує ненульовий гомоморфізм з P_j в P_i та з Q_j в Q_i.

Доведення випливає з означення *Q(A)*.

За Q_u позначатимемо сагайдак, одержаний з *Q* заміною усіх стрілок, що йдуть з *i* в *j* на одиничну стрілку (*i*=*j*). Якщо не існує стрілок з *i* в *j*, то немає й Q_u.

Нехай $\overline{Q}$ - неорієнтований граф, одержаний з Q відкиданням його орієнтації.

Наслідок 3.21. Нехай А – кільце таке, що A/R^2 - артінове зліва та справа водночас. Тоді $\overline{Q_u}(A)=\overline{Q_u}'(A)$.

Доведення випливає з **твердження 3.19**.

Теорема 3.22. [7]. Якщо кільце А артінове справа та зліва з $R^2=0$, тоді наступні умови еквівалентні:

1). А – напівдистрибутивне;

2). Довільна вершина *Q(A)* з'єднана з іншою вершиною (можливо, що тією самою), щонайменше однією стрілкою та сагайдак $Q_u'(A)$ можна одержати з $Q_u(A)$ зміною напрямку всіх стрілок.

Кільце А називається *напівпервинним*, якщо *A/R* – артінове, а *R* – нільпотентне.

Теорема 3.23. [2]. Напівпервинне напівдистрибутивне кільце є артиновим справа та зліва водночас.

Означення 3.24. Напівдосконале кільце А називається *Q-симетричним*, якщо A/R^2 нетерове справа та зліва, а $Q'(A)$ одержане з $Q(A)$ реверсією усіх стрілок.

Твердження 3.25. Для *Q-симетричного* кільця А маємо

$$[Q(A)]^T = [Q'(A)].$$

Доведення випливає з **означення 2.5.**

Означення 3.26. Нехай *A* – напівдосконале кільце, таке, що A/R^2 - праве артінове. Тоді індексом *A* буде найбільше дійсне власне значення матриці суміжності [*Q(A)*]. Індекс A позначатимемо як *inA*.

Так само можна визначити лівий індекс напівдосконалого кільця A з артіновим зліва A/R^2. З твердження 3.20**.** маємо, що лівий та правий індекси *SPSD*-кільця співпадають. Зокрема, це вірно для черепичних порядків над дискретно нормованими кільцями.

Означення 3.27. Сагайдак *Q* називається *сильно зв'язним*, якщо існує шлях між будь-якими двома вершинами. За визначенням, одноточковий граф без стрілок приймається також за сильно зв'язного сагайдака.

Означення 3.28. Сагайдак *Q* без кратних стрілок та кратних петель називається *просто влаштованим*, тобто, *Q просто влаштований* тоді й лише тоді, коли матриця суміжності [*Q(A)*] є (0,1)-матрицею.

Теорема 3.29. [2]. Сагайдак *Q(A)* нетерового справа та зліва напівдосконалого кільця *A* є сильно зв'язним.

Нехай *I* – двосторонній ідеал черепичного порядку Λ. Очевидно, що $I = \sum_{i,j=1}^{n} e_{ij}\pi^{\mu_{ij}}O$, де e_{ij} - матричні одиниці. Позначимо за ε(I)= (μ_{ij}) матрицю показників ідеалу *I*.

Нехай *I* та *J* - двосторонні ідеали кільця Λ, ε(*I*)= (μ_{ij}), ε(*J*)= (ν_{ij}). Легко показати, що ε(*IJ*)= (δ_{ij}), де $\delta_{ij} = \min_k \{\mu_{ik} + \nu_{kj}\}$.

Лема 3.30.[1] Нехай $1 = f_1 + ... + f_s$ канонічне розкладення одиниці з *A*. Тоді для кожного простого правого *A*-модуля U_i та для кожного f_j маємо:

$U_i f_j = \delta_{ij} U_i$, i,j=1,…,s. Аналогічне твердження справедливе й для кожного простого лівого A-модуля.

Теорема 3.31. [8].Сагайдак $Q(\Lambda)$ черепичного порядку Λ над скінченно породженим кільцем O сильно зв'язний та просто влаштований. Якщо Λ - зведений, то $Q(\Lambda)$=ε(R^2)-ε(R).

Доведення. З того, що Λ - первинне нетерове напівдосконале кільце за теоремою 3.33 його сагайдак $Q(\Lambda)$ – сильно зв'язний. Нехай Λ - зведений порядок. Надалі використовуватимемо такі позначення :

ε(Λ)=(α_{ij}); ε(R)=(β_{ij}); $\beta_{ii} = 1$ для i=1,…,n та $\beta_{ij} = \alpha_{ij}$ для $i \neq j$; ε(R^2)=(γ_{ij}), де $\gamma_{ij} = \min\limits_{1\le k\le n}\{\beta_{ki} + \beta_{kj}\}$ для i,j=1,…, n. Оскільки ε(Λ) – зведена, то маємо нерівність $\alpha_{ij} + \alpha_{ji} \ge 1$ для $i,j=1,\ldots, n$ тобто,

$$\gamma_{ii} = \min_{1\le k\le n}\{\beta_{ik} + \beta_{ki}\} = \min_{\substack{1\le k\le n,\\ k\neq i}}\{\beta_{ik} + \beta_{ki}\}$$

З цього маємо, що γ_{ij} набуває значень 1 або 2. Якщо $i \neq j$, то $\beta_{ij} = \alpha_{ij}$ та

$\gamma_{ij} = \min\left\{\min\limits_{1\le k\le n, k\neq i}\{\alpha_{ik} + \alpha_{ki}\}, \alpha_{ij} + 1\right\}$, тобто, $\gamma_{ij} = \alpha_{ij}$ або $\gamma_{ij} = \alpha_{ij} + 1$.

Для довільної незвідної Λ-гратки M з O-базисом $\left(\pi^{\alpha_1} e_1, \ldots, \pi^{\alpha_n} e_n\right)$ ми задаємо n-ку $[M] = (\alpha_1, \ldots, \alpha_n)$.

Розгляньмо $[P_i] = (\alpha_{i1}, \ldots, 0, \ldots, \alpha_{in})$, $[P_i R] = (\alpha_{i1}, \ldots, 1, \ldots, \alpha_{in}) = (\beta_{i1}, \ldots, \beta_{in})$.

Зауважимо, що $[P_i R^2] = (\gamma_{i1}, \ldots, \gamma_{in})$. Тоді $\vec{q}_i = [P_i R^2] - [P_i R]$ - це (0,1)-вектор.

Нехай одиниці $\vec{q}_i$ розташовані на місцях $j_1, \ldots, j_m$. У світлі леми знищення це означає, що $P_i R / P_i R^2 = U_{j_1} \oplus \ldots \oplus U_{j_m}$. За значенням сагайдака ми маємо єдиний шлях від вершини i до кожної з вершин $j_1, \ldots, j_n$. Тобто, матриця суміжності $[Q(\Lambda)] = \mathcal{E}(R^2) - \mathcal{E}(R)$.

Теорема 3.32. Нехай $\mathcal{E}=(\alpha_{ij})$ - зведена матриця показників. Покладемо $\mathcal{E}^{(1)}=(\beta_{ij})$, де $\beta_{ij}=\alpha_{ij}, i\neq j; \beta_{ij}=1, i=j$, а $\mathcal{E}^{(2)}=(\gamma_{ij})$, де $\gamma_{ij}=\min\limits_{1\le k\le n}(\beta_{ik}+\beta_{kj})$.

Матриця $[Q]=\mathcal{E}^{(2)}-\mathcal{E}^{(1)}$ є матрицею суміжності для сильно зв'язаного просто влаштованого сагайдака *Q=Q(ε)*.

Доведення. $[Q]=\mathcal{E}^{(2)}-\mathcal{E}^{(1)}$ - це (0,1)-матриця. Отже, існує такий просто влаштований сагайдак, що $[Q]$ для нього – матриця суміжності. Покажемо, що цей сагайдак Q є сильно зв'язним.

Припустимо, що вірне протилежне твердження. Тобто, існують хоча б дві вершини, між якими шляху не існує. Позначимо їх через i та j. Позначимо *VQ(i)* множину всіх вершин сагайдака, які є кінцем шляхів, що починаються в вершині i. *VQ* – це множина вершин сагайдака *Q*. Очевидно, що *VQ*| *VQ(i)* - непорожня, оскільки хоча б j належить до неї. Очевидною є відсутність стрілок з *VQ(i) до VQ*| *VQ(i)*. Можна припустити, що *VQ(i)={1,…,m}*, *VQ*| *VQ(i)={m+1,…,s}*. Очевидною є можливість простих перетворень над рядками чи стовпчиками у матриці показників *ε*. Завдяки простим перетворенням стовпчиків ми можемо привести її до такого вигляду, коли усі елементи першого рядка дорівнюють нулю, тоді матриця $[Q]$ матиме вигляд:

$$[Q]=\begin{pmatrix} * & 0 \\ * & * \end{pmatrix}.$$

Матриця

$$\mathcal{E}=\begin{pmatrix} \mathcal{E}_1 & * \\ * & \mathcal{E}_2 \end{pmatrix}, \text{ де } \mathcal{E}_1\in M_m(\mathrm{Z}),\quad \mathcal{E}_2\in M_{s-m}(\mathrm{Z}).$$

З матрицею показників $\mathcal{E}_2 \in M_{s-m}(Z)$ ми пов'яжемо частково впорядковану множину $P_{\varepsilon_2} = \{m+1,...,s\}$ з відношенням впорядкованості $i \le j \Leftrightarrow \alpha_{ij} = 0$. Отже, m+1 – мінімальний елемент множини P_{ε_2}. Тоді $\alpha_{im+1} > 0$ для i>m+1. Тоді $q_{1m+1} = 0$ та існує таке k, $2 \le k \le m,$ таке, що виконується $\alpha_{1m+1} = \alpha_{1k} + \alpha_{km+1}$ Помінявши k-го та 2-го стовпчика та r-го та 2-го рядка матриці ε місцями, одержимо, що $\alpha_{2m+1} = 0$ та знову $q_{2m+1} = 0$ і $\alpha_{2m+1} = \alpha_{21k} + \alpha_{km+1}$ для деякого k, $3 \le k \le m$, отже бачимо, що $\alpha_{23} = 0$ та $\alpha_{3m+1} = 0$. Елементи матриці $\mathcal{E}^{(1)} = (\beta_{ij})$ $\beta_{31} = \alpha_{31} \ne 0$, $\beta_{32} = \alpha_{32} \ne 0$, $\beta_{33} = 1$ - ненульові. Отже, маємо $q_{3m+1} = 0$. Продовжуючи процес, маємо: $\alpha_{im+1} = 0$ для усіх i=1,…,m. Матриця $\mathcal{E}_1$ - нижньотрикутна, всі елементи β_{ij} - натуральні, а $q_{mm+1} = \min\{\beta_{mk} + \beta_{km+1}\} - \alpha_{mm+1} = 0$. Отримавши протиріччя, маємо невірність твердження про те, що сагайдак не є сильно зв'язним.

Означення 3.33. Черепичний порядок $\Lambda = \{O, \mathcal{E}(\Lambda)\}$ називається *(0,1)-порядком*, якщо ε(Λ) - (0,1)-матриця.

Тобто, під (0,1)-порядком ми завжди матимемо на увазі черепичний (0,1)-порядок над дискретно нормованим кільцем *O*.

З довільним зведеним (0,1)-порядком Λ ми пов'язуємо частково впорядковану множину (poset або ч.в.м.) $P_\Lambda = \{1,...,n\}$ з відношенням порядку ≤, що визначається за формулою $i \le j \Leftrightarrow \alpha_{ij} = 0$.

Очевидним є, що $(P, \le)$ – частково впорядкована множина (ч.в.м.).

Вірним є й обернене: для довільної ч.в.м. ми можемо поставити у відповідність (0,1)-матрицю $\mathcal{E}_P = (\lambda_{ij})$, яка задається таким чином: $\lambda_{ij} = 0 \Leftrightarrow i \le j, \lambda_{ij} = 1, \Leftrightarrow i > j$. Тоді $\Lambda(P) = \{O, \mathcal{E}_P\}$ - зведений (0,1)-порядок.

Твердження 3.34. [2]. Ширина зведеного (0,1)-порядку Λ w(Λ) співпадає з шириною частинно обмеженої множини P_Λ.

Доведення тривіальне.

Означення 3.35. Елемент a з P є *накриттям* b в P, якщо $a>x>b$ не виконується для жодного x з P.

Означення 3.36. Нехай $P=\{\alpha_1,...,\alpha_n\}$ - частково впорядкована множина з відношенням порядку $\le$. *Діаграма P* – це сагайдак $Q(P)$ з множиною вершин $VQ(P)=\{1,...,n\}$ та з множиною стрілок $AQ(P)=\left\{\sigma: i\to j,\quad \alpha_i \text{ накриває } \alpha_j\right\}$.

Означення 3.37. Сагайдак без орієнтованих циклів називаєтсья *ациклічним*.

Означення 3.38. Стрілка $\sigma: i\to j$ ациклічного сагайдака Q називаєтсья *надлишковою*, якщо якщо існує шлях від i до j довший за одиничний.

Теорема 3.39. Нехай Q – ациклічний просто влаштований сагайдак без надлишкових стрілок. Тоді Q – діаграма деякої частково впорядкованої множини P. І навпаки: діаграма частково впорядкованої множини є ациклічним просто влаштованим сагайдаком.

Означення 3.40. Частково впорядкована множина Р називається *зв'язною,* якщо її діаграма *Q(P)* – зв'язний сагайдак.

А тепер покажемо, яким шляхом можна для загаданої частково впорядкованої множини $P=\{p_1,...,p_n\}$ поставити у відповідність сильно зв'язний сагайдак без кратних петель та надлишкових стрілок.

Позначимо за $P_{\max}$ (відповідно $P_{\min}$) множину максимальних (мінімальних) елементів з Р, а за $P_{\max}\times P_{\min}$ їх декартів добуток.

Означення 3.41. Сагайдак $\widetilde{Q}(P)$, отриманий з діаграми *Q(P)* додаванням стрілок σ_{ij} для всіх $(p_i,p_j)\in P_{\max}\times P_{\min}$ називатиметься сагайдаком, асоційованим з частково впорядкованою множиною *P*.

Насправді, $\widetilde{Q}(P)$ - сильно зв'язний просто влаштований сагайдак.

Теорема 3.42. [2]. Сагайдак *Q(Λ(P))* співпадає з сагайдаком $\widetilde{Q}(P)$.

Доведення. Згадаймо з теореми 3.31, що $[Q(\Lambda(P))]=\mathcal{E}(R^2)-\mathcal{E}(R)$. Припустимо, що *Q(P)* містить стрілку з вершини s в t. Це означає, що $\alpha_{st}=0$ та немає такого натурального числа k, що $k \neq s,t$ та $\alpha_{sk} = 0$, $\alpha_{kt} = 0$. Елементи матриці показників $\mathcal{E}(R) = (\beta_{ij})$ β_{ss} та β_{tt} рівні 1. Тоді для $\mathcal{E}(R^2) = (\gamma_{ij})$ $\gamma_{ij} = \min\limits_{1 \le k \le n}(\beta_{sk} + \beta_{kt}) = 1$. Отже, у $[Q(\Lambda(P))]$ на (s,t)-ій позиції ми маємо $\gamma_{st} - \beta_{stt} = 1 - \alpha_{st} = 1 - 0 = 1$. Це означає, що $Q(\Lambda(P))$ має стрілку з s в t.

Припустимо, що $p \in P_{\max}$. Це означає, що $\alpha_{pk} = 1, k \neq p$. Тобто, усі елементи р-того рядка матриці $\mathcal{E}(R) = (\beta_{ij})$ - одиниці.

Аналогічно можна показати, що, якщо $q \in P_{\min}$, то елементи q-го стовпця $\mathcal{E}(R) = (\beta_{ij})$ усі є одиницями.

Отже, $\gamma_{pq} = 2, \beta_{pq} = 1$, а $Q(\Lambda(P))$ має стрілку з p *в* q. Ми довели, що $\widetilde{Q}(P)$ - підсагайдак сагайдака $Q(\Lambda(P))$.

Покажемо обернене включення. Припустимо, що $\gamma_{pq} = 2$. Звідси відразу отримуємо, що

$(\beta_{p1},..., \beta_{pn}) = (1,...,1)$ та $(\beta_{1q},..., \beta_{pqn})^T = (1,...,1)^T$. Тому $p \in P_{\max}, q \in P_{\min}$ та існує стрілка, що йде від вершини p в q.

Нехай $\gamma_{pq} = 1, \beta_{pq} = 0$. Очевидно, $p \neq q$, і тоді $p<q$.

Оскільки $\gamma_{pq} = \min\limits_{1 \le k \le n}(\beta_{pk} + \beta_{kp}) = 1$, то $(\beta_{pk} + \beta_{kq}) \ge 1$ для k=1,…,n. Для $p \neq k$ маємо: $\beta_{pk} + \beta_{kq} \ge 1$, звідки $\alpha_{pk} + \alpha_{kq} \ge 1$. Отже, не існує такого k, що $k \neq p,q$ і $\alpha_{pk} = \alpha_{kq} = 0$. Це означає, що якщо $Q(P)$ містить стрілку з p в q, то ми довели обернене включення.

Означення 3.43. Сагайдак Q називаєтсья жорстким, якщо з точністю до ізоморфізму існує такий черепичний порядок Λ, що $Q(\Lambda)=Q$.

Теорема 3.44. Зведений напівмаксимальний порядок $\Lambda=\{O,\varepsilon(\Lambda)\}$ ізоморфний трикутному горенштейновому порядку тоді й лише тоді, коли $Q(\Lambda)$ є простим циклом C_s або сагайдаком LC_s. В цьому випадку Λ ізоморфний порядку $T_{k,s}$.

Доведення. Нехай Λ – зведений напівмаксимальний порядок, ізоморфний горенштейновому трикутному порядку. Тоді Λ - також горенштейнів. Сагайдаки ізоморфних кілець також ізоморфні. Тому можна вважати, що Λ - трикутний. Оскільки $P_1 = e_{11}\Lambda = (0,...,0)$, то маємо $\alpha_{1k} + \alpha_{k\sigma(1)} = \alpha_{1\sigma(1)} = 0$. Тому $\alpha_{1\sigma(1)} = 0$ для усіх $k=1,...s$. Якщо $\sigma(1) < s$, то $\alpha_{s\sigma(1)} = 0$ та $\alpha_{\sigma(1)s} = 0$. Оскільки Λ - зведений напівмаксимальний порядок, то $\alpha_{s\sigma(1)} + \alpha_{\sigma(1)s} > 0$. Отже, $\sigma(1) = s$.

Нехай $\alpha_{21} = k$. Очевидно, що $\sigma(2) = 1$. З рівності $\alpha_{2k} + \alpha_{k1k} = \alpha_{21} = k$ маємо, що $\alpha_{31} = \alpha_{41} = ... = \alpha_{s1} = k$. Аналогічно $\sigma(3) = 2$ і $\alpha_{3k} + \alpha_{k2} = \alpha_{32}$. Звідси знаходимо $\alpha_{31} = \alpha_{32} = \alpha_{42} ... = \alpha_{s2} = k$. Якщо продовжити далі, то одержимо, що $\Lambda = T_{ks} = T_{ks}(O) = \{O, \mathcal{E}(T_{ks})\}$. В [9] обчислені матриці суміжності для сагайдака порядку $T_{k,s}$ при k>1 та k=1. В першому випадку сагайдак є сагайдаком LC_s, а в другому – простим циклом C_s.

І навпаки, нехай Λ - зведений напівмаксимальний порядок, $Q(\Lambda)=C_s$ або LC_s. Припустимо, що простий цикл C_s в $Q(\Lambda)$ має вигляд

$$C_s = \left\{ \begin{matrix} 1 & & 2 & & s-1 & & s & & 1 \\ \bullet & \to & \bullet & ... & \bullet & \to & \bullet & \to & \bullet \end{matrix} \right\}.$$

У випадку, коли $Q(\Lambda)=C_s$, можна розглядати елементи $\pi^{\alpha_{12}} e_{12}, ..., \pi^{\alpha_{s-1s}} e_{s-1s}, \pi^{\alpha_{s1}} e_{s1} \in R$ як мінімальну систему твірних радикала R. Якщо ж $Q(\Lambda)=LC_s$, то до наведеної вище множини твірних треба додати елементи $\pi^{r_{ii}} e_{ii} = \pi e_{ii}, \quad i = 1,...,s$.

Кожному елементу з $e_{ii} \mathrm{Re}_{jj}$ відповідає шлях у сагайдаку $Q(\Lambda)$, який починається в точці i та закінчується в точці j. Елементу $\pi^{r_{ij}} e_{ij}, \quad ((r_{ij}) = \mathcal{E}(R))$

відповідає найкоротший шлях (без циклів та петель). Тому

$$\pi^{r_{ij}}e_{ij}=\begin{cases}\pi^{\alpha_{ii+1}}e_{ii+1}\pi^{\alpha_{i+1i+2}}e_{i+1i+2}...\pi^{\alpha_{j-1j}}e_{j-1j}, & i<j,\\ \pi^{\alpha_{ii+1}}e_{ii+1}...\pi^{\alpha_{s-1s}}e_{s-1s}\pi^{\alpha_{s1}}e_{s1}\pi^{\alpha_{12}}e_{12}...\pi^{\alpha_{j-1j}}e_{j-1j}, & i>j.\end{cases}$$

Звідси при $i\neq j$ маємо:

$$\alpha_{ij}=\begin{cases}\alpha_{ii+1}+\alpha_{i+1i+2}+...+\alpha_{j-1j}, & i<j,\\ \alpha_{ii+1}+...+\alpha_{s-1s}+\alpha_{s1}+\alpha_{12}+...+\alpha_{j-1j}, & i>j.\end{cases}$$

будь-який напівмаксимальний порядок ізоморфний порядку, матриця показників якого має нульовий перший порядок. Причому сагайдак $Q(\Lambda)$ та підстановка Кириченка $\sigma=\begin{pmatrix}1 & 2 & 3 & ... & s-1 & s\\ s & 1 & 2 & ... & s-2 & s-1\end{pmatrix}$ при перетвореннях першого типу не змінюються. Тому можна вважати, що $\alpha_{1s}=0$.

Оскільки $\alpha_{12}+\alpha_{23}+...+\alpha_{s-1s}=\alpha_{1s}=0$, то $\alpha_{12}=\alpha_{23}=...=\alpha_{s-1s}=\alpha_{1s}=0$. Але тоді при *i*<*j* маємо $\alpha_{ij}=\alpha_{ii+13}+...+\alpha_{j-1j}=0$. Отже, порядок Λ - трикутний.

Нехай $Q(\Lambda)=C_s$. Тоді $r_{11}=\alpha_{12}+\alpha_{23}+...+\alpha_{s-1s}+\alpha_{s1}$. Оскільки $\alpha_{12}=\alpha_{23}=...=\alpha_{s-1s}=0$, то $\alpha_{s1}=1$, тому при i<j маємо: $\alpha_{ij}=\alpha_{ii+1}+...+\alpha_{s-1s}+\alpha_{s1}+\alpha_{12}+\alpha_{23}+...+\alpha_{j-1j}=\alpha_{s1}=1$.

Таким чином

$$\mathcal{E}(\Lambda)=\mathcal{E}(H_s)=\begin{pmatrix}0 & 0 & 0 & 0 & ... & 0 & 0\\ 1 & 0 & 0 & 0 & ... & 0 & 0\\ 1 & 1 & 0 & 0 & ... & 0 & 0\\ 1 & 1 & 1 & 0 & ... & 0 & 0\\ ... & ... & ... & ... & ... & ... & ...\\ 1 & 1 & 1 & ... & ... & 0 & 0\\ 1 & 1 & 1 & 1 & ... & 1 & 0\end{pmatrix}.$$

Нехай $Q(\Lambda)=LC_s$. Тоді елементи πe_{ii} входитимуть до мінімальної системи твірних радикала *R* і відповідатимуть петлям у вершинах сагайдака.

Оскільки петля – найкоротший шлях з довільної вершини до неї самої, то

$$\pi^{r_{ii}}e_{ii}=\pi e_{ii}\neq\pi^{\alpha_{ii+1}}e_{ii+1}\pi^{\alpha_{i+1i+2}}e_{i+1i+2}...\pi^{\alpha_{s-1s}}e_{s-1s}\pi^{\alpha_{s1}}e_{s1}\pi^{\alpha_{s12}}e_{12}...\pi^{\alpha_{i-1i}}e_{i-1i},\quad i=1,...,s.$$

Тому $\alpha_{s1} = k > 1$, $\alpha_{ij} = \alpha_{ii+1} + ... + \alpha_{s-1s} + \alpha_{s1} + \alpha_{12} + \alpha_{23} + ... + \alpha_{j-1j} = \alpha_{s1} = k$.

Отже

$$\mathcal{E}(\Lambda) = \mathcal{E}(T_{ks}) = \begin{pmatrix} 0 & 0 & 0 & 0 & ... & 0 & 0 \\ k & 0 & 0 & 0 & ... & 0 & 0 \\ k & k & 0 & 0 & ... & 0 & 0 \\ k & k & k & 0 & ... & 0 & 0 \\ ... & ... & ... & ... & ... & ... & ... \\ k & k & k & ... & ... & 0 & 0 \\ k & k & k & k & ... & k & 0 \end{pmatrix}$$

і теорему доведено.

РОЗДІЛ ІІІ. ПІДСТАНОВКА КИРИЧЕНКА ЛАТИНСЬКИХ КВАДРАТІВ

Теорема 4.1. (головна)

Горенштейнова матриця не може бути латинським квадратом у двох випадках

1) Розклад підстановки Кириченка горенштейнової матриці на незалежні цикли містить цикли різної довжини.

2) Розклад підстановки Кириченка горенштейнової матриці на незалежні цикли містить парну кількість циклів непарної довжини.

Для інших підстановок Кириченка існують горенштейнові латинські квадрати.

Доведення.

Лема 4.2. Розклад підстановки Кириченка горенштейнового латинського квадрату $L=(\alpha_{ij})$ на незалежні не містить двох циклів різної довжини.

Доведення. З леми 3.8 випливає, що $\alpha_{i\sigma(i)}=c$. Припустимо протилежне, що розклад підстановки σ на незалежні цикли містить цикли довжиною l_1, l_2 ($l_1\neq l_2$). За допомогою перетворення другого типу матрицю L можна перетворити так, що підстановка σ матиме вигляд $\sigma=\sigma_1\sigma_2\ldots\sigma_k$, де $\sigma_1=(1\ 2\ \ldots\ l_1)$, $\sigma_2=(l_1+1\ l_1+2\ \ldots\ l_1+l_2)$. За лемою 3.6 L також є горештейновим латинським квадратом. Розглянемо горенштейновий латинський квадрат $L^/=(\alpha_{ij})\in M_{l_1+l_2}(\mathbb{Z})$, де $L^/=\begin{pmatrix} L_1^/ & Y \\ X & L_2^/ \end{pmatrix}$ з підстановкой $\beta\cdot\psi.$, де $L_1^/\in M_{l_1}(\mathbb{Z})$, $L_2^/\in M_{l_2}(\mathbb{Z})$, $\beta=\sigma_1$, $\psi=\sigma_2$.

Розглянемо довільний елемент $\alpha_{ij}\in X$ ($i>l_1$, $j\leq l_1$). Оскільки $\alpha_{ij}+\alpha_{j\psi(i)}=\alpha_{i\psi(i)}=c$, то $\alpha_{j\psi(i)}=c-\alpha_{ij}$. Аналогічно $\alpha_{j\psi(i)}+\alpha_{\psi(i)\beta(j)}=\alpha_{\psi(i)\beta(j)}=c$, тому $c-\alpha_{ij}+\alpha_{\psi(i)\beta(j)}=c$. Звідси $\alpha_{ij}=\alpha_{\psi(i)\beta(j)}$. Отже, для довільного елемента $\alpha_{ij}\in X$ отримали рівність

$\alpha_{ij}=\alpha_{\psi(i)\beta(j)}$. Позначимо $\alpha^k(i,j)=\alpha_{\psi^k(i)\beta^k(i)}$. Оскільки у блоці X є $l_1\times l_2$ елементів, то в послідовності $\alpha^1(i,j)$, $\alpha^2(i,j)$, $\ldots,\alpha^{l_1\times l_2+1}(i,j)$ два елемента співпадають. Нехай елементи $\alpha^t(i, j)$ та $\alpha^z(i, j)$ співпадають ($1 \le t, z \le l_1 \times l_2+1$), а елементи $\alpha^t(i, j), \alpha^{t+1}(i, j), \ldots, \alpha^{z-1}(i, j)$ – різні. (Два елемента співпадають, коли в них однакове розташування в блоці X). Оскільки ψ – циклічна підстановка (цикл складається з l_2 елементів) та $\alpha_{\psi^t(i)\beta^t(i)} = \alpha_{\psi^z(i)\beta^z(i)}$, то $\psi^t(i) = \psi^z(i)$. З останньої рівності слідує, що $(z\text{-}t)$ ділиться на l_2. Аналогічно з рівності $\beta^t(i) = \beta^z(i)$ слідує, що $(z\text{-}t)$ ділиться на l_1. Отже, $(z\text{-}t)$ ділиться на l_1 та $(z\text{-}t)$ ділиться на l_2 а тому $(z\text{-}t)$ ділиться на НСК(l_1, l_2). Тоді $(z\text{-}t) \ge$ НСК(l_1, l_2). Тобто в блоці Х знаходиться не менше, ніж НСК(l_1, l_2) елементів, які мають однакове значення, але мають різне розташування. Нехай $l_1 < l_2$ (випадок $l_1 > l_2$ розглядається аналогічно). Тоді НСК(l_1, l_2)$> l_1$. Блок X складається з l_1 стовпчиків та містить не менше, ніж НСК(l_1, l_2) елементів рівних $\alpha_{\psi^t(i)\beta^t(i)}$. Оскільки НСК($l_1$, l_2)$> l_1$, то за принципом Діріхле хоча б в одному стовпчику блока X знаходиться два однакових елемента. Отже, L не є латинським квадратом, отримали протиріччя. Лема доведена.

Отже, розклад підстановки Кириченка σ горенштенйового латинського квадрату у добуток незалежних циклів не може містити двох циклів різної довжини. Розглянемо питання, коли цей розклад має цикли однакової довжини.

Лема 4.3. Для довільної циклічної підстановки Кириченка існує горенштейновий латинський квадрат з даною підстановкою.

Доведення. Якщо підстановка σ циклічна (складається з одного циклу) то, очевидно, що $L = \sum_{i=0}^{n-1} iP_{\sigma^i}$ є горенштейновим латинським квадратом з підстановкою Кириченка σ. Лема доведена.

За допомогою елементарного перетворення другого типу матрицю L можна перетворити так, що $\sigma = \sigma_1\sigma_2\ldots\sigma_k$, де

$\sigma_1=(1\ 2\ \ldots\ l)$, $\sigma_2=(l+1\ \ l+2\ \ldots\ 2l)$, …, $\sigma_t=((t-1)l+1\ \ (t-1)l+2\ \ldots\ tl)$. (1)

За лемою 3.6 після перетворення другого типу ми знову одержимо горештейновий латинський квадрат. Далі будемо вважати, що підстановка σ має вигляд (1).

Лема 4.4. Не існує горенштейнового латинського квадрата з підстановкою $\sigma=\sigma_1 \dots \sigma_{2k}$, де $\sigma_1, \dots , \sigma_{2k}$ – цикли непарної довжини.

Доведення. Враховуючи лему 3.16 досить довести лему для циклів однакової непарної довжини. Припустимо протилежне, що існує горенштейновий латинський квадрат $L=(\alpha_{ij})$ з підстановкою $\sigma=\sigma_1\ \sigma_2\dots\sigma_{2k}$, де $\sigma_1=(1\ 2\ \dots\ l)$, $\sigma_2=(\ l+1\ \ l+2\ \dots\ 2l)$, …, $\sigma_{2k}((2k-1)l+1\ (2k-1)l+2\ \dots\ 2k\, l)$.

$$L=\begin{pmatrix} L_1 & & \dots & \\ & L_2 & \dots & \\ \dots & \dots & \dots & \dots \\ & & \dots & L_{2k} \end{pmatrix},$$ де $L_i\in M_{2m+1}(\mathbb{Z})$, для всіх $i=1, \dots ,2k$.

Оскільки $L_1\in M_{2m+1}(\mathbb{Z})$–горенштенова матриця та $\alpha_{i\sigma(i)}=c$ для всіх

$i=1, \dots , 2m+1$, то $L_1=\left(\alpha_{ij}\right)=\sum\limits_{i=1}^{2m}\rho_i P_{\sigma^i}$.

Тобто $$L_1=\begin{pmatrix} 0 & s_1 & s_2 & \dots & s_{2m-2} & s_{2m-1} & s_{2m} \\ s_{2m} & 0 & s_1 & \dots & s_{2m-3} & s_{2m-2} & s_{2m-1} \\ s_{2m-1} & s_{2m} & 0 & \dots & s_{2m-4} & s_{2m-3} & s_{2m-2} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ s_3 & s_4 & s_5 & \dots & 0 & s_1 & s_2 \\ s_2 & s_3 & s_4 & \dots & s_{2m} & 0 & s_1 \\ s_1 & s_2 & s_3 & \dots & s_{2m-1} & s_{2m} & 0 \end{pmatrix}.$$

Оскільки L_1 – горенштейнова з підстановкою $\sigma_1=(1\ 2\ \dots\ 2m+1)$, то $s_1=s_2+s_{2m}=s_3+ s_{2m-1}=\dots=s_m+s_{m+2}=s_{m+1}+s_{m+1}$. Отже, $s_1=2s_{m+1}$.

Розглянемо детальніше перший рядок та другий стовпчик матриці L.

Оскільки L– горенштейнова матриця з підстановкою σ і $\sigma(1)=2$, то

$$\alpha_{1i}+\alpha_{i2}=\alpha_{12}=2s_{m+1}\text{ , звідки } \alpha_{i2}=2s_{m+1}-\alpha_{1i} \quad \text{для всіх} \quad i\in 1,...,n. \qquad (2)$$

За означенням латинського квадрату всі елементи першого рядка різні. Перший рядок містить $2k\times(2m+1)$ елементів, в тому числі елемент s_{m+1}. Тому перший рядок містить непарну кількість елементів, які відрізняються від s_{m+1}. Припустимо, що серед елементів першого рядка більше тих елементів, які перевищують s_{m+1} (випадок, коли більше елементів, які менше ніж s_{m+1} розглядається аналогічно). З рівності (2) одержуємо, що в другому стовпчику матриці рядку L більше тих елементів, які менші, ніж s_{m+1}. Одержали протиріччя (перший рядок та другий стовпчик латинського квадрата мають складатися з однакових елементів). Лема доведена.

Лема 4.5. Якщо розклад підстановки Кириченка σ у добуток незалежних циклів складається з непарної кількості циклів однакової довжини, то існує горенштейновий латинський квадрат з підстановкою σ.

Доведення. Нехай $\sigma=\sigma_1\sigma_2\ldots\sigma_{2k+1}$, де $\sigma_1=(1\ 2\ \ldots\ l)$, $\sigma_2=(l+1,\ l+2\ \ldots\ 2l)$, $\ldots,\sigma_{2k+1}=(2kl+1,\ \ldots\ ,(2k+1)l)$.

Розглянемо два випадка.

Випадок 1) l–парне.

Побудуємо латинський квадрат L.

$$L=\begin{pmatrix} L_0 & L_1 & L_2 & \cdots & L_{2k-2} & L_{2k-1} & L_{2k} \\ L'_{2k} & L_0 & L_1 & \cdots & L_{2k-3} & L_{2k-2} & L_{2k-1} \\ L'_{2k-1} & L'_{2k} & L_0 & \cdots & L_{2k-4} & L_{2k-3} & L_{2k-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ L'_3 & L'_4 & L'_5 & \cdots & L_0 & L_1 & L_2 \\ L'_2 & L'_3 & L'_4 & \cdots & L'_{2k} & L_0 & L_1 \\ L'_1 & L'_2 & L'_3 & \cdots & L'_{2k-1} & L'_{2k} & L_0 \end{pmatrix},$$

Спочатку побудуємо блок $L_0\in M_l(\mathbb{Z})$.

Нехай $r=\dfrac{l}{2}-2.$

$$L_0=\sum_{i=0}^{l-1}\rho_i P_{\sigma_1^i}\text{ , де } \rho_0=0,\ \rho_1=10n,\ \rho_2=4n-r,\ \rho_3=4n-r+1,...,\ \rho_{r+2}=4n,$$

$\rho_{r+3}=6n,\ \rho_{r+4}=6n+1,\ldots,\ \rho_{l-1}=6n+r.$

Наприклад для випадку n=18, l=6: $L\in M_{18}(\mathbb{Z})$, $L_0\in M_6(\mathbb{Z})$ (підстановка складається з трьох циклів довжини шість) l=6, r=1. $L_0=\sum_{i=0}^{5}\rho_i P_{\sigma_1^i}$, де

$\rho_0=0,\ \rho_1=180,\ \rho_2=71,\ \rho_3=72,\ \rho_4=108, \rho_5=109.$

$$L_0=\begin{pmatrix} 0 & 180 & 71 & 72 & 108 & 109\\ 109 & 0 & 180 & 71 & 72 & 108\\ 108 & 109 & 0 & 180 & 71 & 72\\ 72 & 108 & 109 & 0 & 180 & 71\\ 71 & 72 & 108 & 109 & 0 & 180\\ 180 & 71 & 72 & 108 & 109 & 0 \end{pmatrix}.$$

2) l – непарне. Нехай $r=\dfrac{l-5}{2}.$

$L_0=\sum_{i=0}^{l-1}\rho_i P_{\sigma_1^i}$, де $\rho_0=0,\ \rho_1=10n,\ \rho_2=4n-r,\ \rho_3=4n-r+1,\ldots,\ \rho_{r+2}=4n,$

$\rho_{r+3}=5n,\ \rho_{r+4}=6n,\ \rho_{r+5}=6n+1,\ldots,\ \rho_{l-1}=6n+r.$

Наприклад для випадку n=21, l=7: $L\in M_{21}(\mathbb{Z})$, $L_0\in M_7(\mathbb{Z})$ (підстановка складається з трьох циклів довжини сім) l=7, r=1. $L_0=\sum_{i=0}^{6}\rho_i P_{\sigma 1^i}$,

$$L_0=\begin{pmatrix} 0 & 210 & 83 & 84 & 105 & 126 & 127\\ 127 & 0 & 210 & 83 & 84 & 105 & 126\\ 126 & 127 & 0 & 210 & 83 & 84 & 105\\ 105 & 126 & 127 & 0 & 210 & 83 & 84\\ 84 & 105 & 126 & 127 & 0 & 210 & 83\\ 83 & 84 & 105 & 126 & 127 & 0 & 210\\ 210 & 83 & 84 & 105 & 126 & 127 & 0 \end{pmatrix}.$$

$\rho_0=0,\ \rho_1=210,\ \rho_2=83,\ \rho_3=84,\ \rho_4=105, \rho_5=126, \rho_6=127.$

$L=(\alpha_{ij})\in M_n(\mathbb{Z})$. Нехай $p=\dfrac{m+l}{2}$,

$$\alpha_{1i}=\begin{cases}5n+i-p-1, i\in[l+1,t]\\ 5n+i-p, i\in[t+1,n]\end{cases}.$$

Отже, ми задали блоки L_0, L_1, …, L_{2k}. Задамо блоки $L_1^{/}$, …, $L_{2k}^{/}$ наступним чином: нехай перший рядок блоку L_i складається з чисел s_1, s_2, …, s_l тоді перший рядок блоку $L_i^{/}$ складається з елементів s_{l-1}, s_l, s_1, s_2, …, s_{l-2}.

Наприклад, $L\in M_{12}(\mathbb{Z})$, $L_0 \in M_4(\mathbb{Z})$ (підстановка складається з трьох циклів довжини чотири)

$$L_{12}=\begin{pmatrix}
0 & 120 & 48 & 72 & 56 & 57 & 58 & 59 & 61 & 62 & 63 & 64\\
72 & 0 & 120 & 48 & 59 & 56 & 57 & 58 & 64 & 61 & 62 & 63\\
48 & 72 & 0 & 120 & 58 & 59 & 56 & 57 & 63 & 64 & 61 & 62\\
120 & 48 & 72 & 0 & 57 & 58 & 59 & 56 & 62 & 63 & 64 & 61\\
63 & 64 & 61 & 62 & 0 & 120 & 48 & 72 & 56 & 57 & 58 & 59\\
62 & 63 & 64 & 61 & 72 & 0 & 120 & 48 & 59 & 56 & 57 & 58\\
61 & 62 & 63 & 64 & 48 & 72 & 0 & 120 & 58 & 59 & 56 & 57\\
64 & 61 & 62 & 63 & 120 & 48 & 72 & 0 & 57 & 58 & 59 & 56\\
58 & 59 & 56 & 57 & 63 & 64 & 61 & 62 & 0 & 120 & 48 & 72\\
57 & 58 & 59 & 56 & 62 & 63 & 64 & 61 & 72 & 0 & 120 & 48\\
56 & 57 & 58 & 59 & 61 & 62 & 63 & 64 & 48 & 72 & 0 & 120\\
59 & 56 & 57 & 58 & 64 & 61 & 62 & 63 & 120 & 48 & 72 & 0
\end{pmatrix}$$

Лема 4.6. Якщо підстановка підстановка Кириченка σ складається з **парною** кількості циклів однакової парної довжини то існує Горенштейновий латинський квадрат з підстановкою σ.

Доведення

Нехай підстановка σ складається з $2k$ циклів довжини l, та нехай блок L_0 побудуємо так само, як і в лемі 2.11:

$$r=\frac{l}{2}-2,\ L_0=\sum_{i=0}^{l-1}\rho_i P_{\sigma_1^i}\text{ , де}$$

$$\rho_0=0, \rho_1=10n, \rho_2=4n-r, \rho_3=4n-r+1, ..., \rho_{r+2}=4n,$$

$$\rho_{r+3}=6n, \rho_{r+4}=6n+1, ..., \rho_{l-1}=6n+r. \qquad (3)$$

$$L = \left(\alpha_{ij}\right) = \begin{pmatrix} L_0 & L_1 & L_2 & \cdots & L_{2k-3} & L_{2k-2} & L_{2k-1} \\ L'_{2k} & L_0 & L_1 & \cdots & L_{2k-4} & L_{2k-3} & L_{2k-2} \\ L'_{2k-1} & L'_{2k} & L_0 & \cdots & L_{2k-5} & L_{2k-4} & L_{2k-3} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ L'_3 & L'_4 & L'_5 & \cdots & L_0 & L_1 & L_2 \\ L'_2 & L'_3 & L'_4 & \cdots & L'_{2k-1} & L_0 & L_1 \\ L'_1 & L'_2 & L'_3 & \cdots & L'_{2k-2} & L'_{2k-1} & L_0 \end{pmatrix} \tag{4}$$

В лемі 4.6 доведено, що для того щоб задати матрицю вигляду (4) досить задати її перший рядок $\alpha_{11}, \alpha_{12}, ..., \alpha_{1l}$ задається формулами (3) а інші елементи першого рядка:

$$p = \frac{m+l}{2}$$

$$\alpha_{1i} = \begin{cases} 5n + i - p - 1, i \in [l+1, t] \\ 5n + i - p, i \in [t+1, n] \end{cases}.$$

Наприклад n=8, l=4, p=6.

$$L_8 = \begin{pmatrix} 0 & 80 & 32 & 48 & 38 & 39 & 41 & 42 \\ 48 & 0 & 80 & 32 & 42 & 38 & 39 & 41 \\ 32 & 48 & 0 & 80 & 41 & 42 & 38 & 39 \\ 80 & 32 & 48 & 0 & 39 & 41 & 42 & 38 \\ 41 & 42 & 38 & 39 & 0 & 80 & 32 & 48 \\ 39 & 41 & 42 & 38 & 48 & 0 & 80 & 32 \\ 38 & 39 & 41 & 42 & 32 & 48 & 0 & 80 \\ 42 & 38 & 39 & 41 & 80 & 32 & 48 & 0 \end{pmatrix}$$

Отже, всі випадки розглянуті, Теорема 4.1 доведена.

ВИСНОВКИ

Горенштейнова матриця не може бути латинським квадратом у двох випадках:

1) підстановка Кириченка горенштейнової матриці містить цикли різної довжини

2) підстановка Кириченка складається з парної кількості циклів непарної довжини.

Для інших підстановок Кириченка існують горенштейнові матриці, які є латинськими квадратами.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Hazewinkel M. Algebras Rings and Modules, vol. 1/ M. Hazewinkel, N. Gubareni, V.V. Kirichenko – Kluwer Academic Publisheers, 2004.- 380 p.

2. Hazewinkel M. Algebras Rings and Modules, vol. 2/ M. Hazewinkel, N. Gubareni, V.V. Kirichenko – Kluwer Academic Publisheers, 2007.- 400 p.

3. Kirichenko V. V. Exponent Matrices and Tiled Order over Discrete Valuation Rings/ V. V. Kirichenko , O. V. Zelenskiy, V. N. Zhuravlev // International Journal of Algebra and Computation. – 2005. – Vol. 15, № 5 & 6. – p. 1-16.

4.Зеленський О. В. Жорсткі сагайдаки зведених матриць показників / О. В. Зеленський // Вісник Київського університету. Серія: фізико-математичні науки. – 2007. – №3. – С. 27-31.

5. Зеленський О.В., Дармосюк В.М., Касянюк М.В. Мінімальна матриця показникі/. О. В. Зеленський, В.М,Дармосюк, М.В, Касянюк//*Дослідження в математиці та механіці.* Одеський національний університет імені І. І. Мечникова, 2019. Том 24, №1(33). С. 15–24.

6. Kirichenko V. V. / Quivers and Latin square. // V. V. Kirichenko, M. A. Khibina, V. N Zhuravlev, O. V Zelenskiy Quivers and Latin square. São Paulo Journal of Mathematical Sciences P. 1-15.

7. Журавльов В. М. / Одиничні сагайдаки матриці показників/ В.М. Журавльов, О.В. Зеленський, В.М. Дармосюк // Вісник Київського університету. Серія: фізико-математичні науки. – 2012. – №4. – С. 27-31.

8. Зеленський О. В. Цикли допустимих сагайдаків / О. В. Зеленський// Математичні студії. Том 42, випуск 1.С. 3-8.