

Підстановки
Лекції для студентів ММФ ХНУ.

Курінний Г.Ч. Невмержицька О.М. Шугайло О.М.

Травень — 2015

Зміст

1	Перетворення, підстановки, перестановки	1
1.1	Відповідності та відношення	2
1.2	Підстановки	3
1.2.1	Означення та задання	3
1.2.2	Перестановки, інверсії перестановок, парність перестановок та підстановок	4
1.3	Множення підстановок	7
1.4	Цикли і транспозиції	8
1.5	Застосування підстановок для обчислення визначників . . .	12
1.6	Числа Стірлінга 1-го роду	15
2	Симетрична та знакозмінна група	20
2.1	Напівгрупа. Група. Підгрупа	20
2.2	Властивості спряження	30
2.3	Простота групи A_n при $n \geq 5$	31
2.4	Гомоморізми та ізоморфізми груп	34

1 Перетворення, підстановки, перестановки

.

1.1 Відповідності та відношення

Означення 1.1 Беремо непорожні множини M, N , утворюємо прямий добуток цих множини $M \times N$. Підмножини цього прямого добутку називають відповідностями між елементами M та N . Відповідність між елементами однієї і тієї ж множини, тобто підмножину декартового квадрату $M \times M = M^2 = \{(a, b) | a, b \in M\}$., називають бінарним відношенням, або просто відношенням на множині M .

Серед відношень найважливішими є перетворення (функції, функціональні відношення ...), еквівалентність та відношення порядку. Зараз нас цікавлять перетворення, які ще називають відображеннями із множини в себе (або функціями, або частковими відображеннями, частковими функціями. — в залежності від мовного оточення та традицій)

Означення 1.2 Відображенням із множини M у множину N називають таку відповідність f між елементами множин M, N , (тобто $f \subseteq M \times N$,) що для кожного $x \in M$ існує і до того ж єдиний елемент $y \in N$ такий, що $(x, y) \in f$.

Таке складне означення і позначення потрібне для максимально строгого розвою математики. До звичних (шкільних) означень та позначень переходимо таким чином. Якщо f — відображення із множини M у множину N , і $(x, y) \in f$, то використовуємо позначення

$$f : M \rightarrow N, \quad x \xrightarrow{f} y, \quad y = f(x).$$

Якщо $y = f(x)$, то y називається образом елемента x , а x називається прообразом елемента y .

Означення 1.3 Відображення $f : M \rightarrow N$ називається ін'єктивним, якщо для будь-яких $x_1, x_2 \in M, x_1 \neq x_2$ виконується нерівність $f(x_1) \neq f(x_2)$. Згадане відображення називається сюр'єктивним, якщо для будь-якого $y \in N$ знайдеться хоч один елемент $x \in M$ такий, що $y = f(x)$. Коли відображення є і ін'єктивним і сюр'єктивним, то воно бієктивне.

1.2 Підстановки

1.2.1 Означення та задання

Означення 1.4 *Бієктивні відображення непорожніх скінченних множин у себе називають підстановками.*

Оскільки елементи скінченної множини можна перенумерувати числами починаючи з одиниці, то можна вважати із самого початку, що скінченна множина — це $\{1, 2, 3, \dots, n\}$ для деякого натурального $n \geq 1$.

Підстановки на n -елементній множині (або n -елементної множини) звичайно задають таблично, у два рядки: у верхньому рядку виписують образи, а в нижньому прообрази. Отже, для

$$\sigma : \{1, 2, \dots, n\} \longrightarrow \{1, 2, \dots, n\}$$

ми пишемо

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix} \quad (1)$$

або

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix} \quad (2)$$

замість $\sigma(1) = i_1, \sigma(2) = i_2, \sigma(3) = i_3, \dots, \sigma(n) = i_n$.

Прикладами підстановок є

$$\sigma_1 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & 2n-1 & 2n \\ 2 & 1 & 4 & 3 & \dots & 2n & 2n-1 \end{pmatrix} \quad (3)$$

Теорема 1.1 (про порядок групи підстановок) *На n -елементній множині існує $n!$ підстановок.*

Доведення. Нехай σ — підстановка на множині $1, 2, \dots, n$. Для образу $\sigma(1)$ першого елемента $1 \in n$ можливостей, для образу $\sigma(2)$ другого елемента 2 коли образ першого вибраний, є $n-1$ можливість, для образу $\sigma(3)$ третього елемента 3 , коли образи $\sigma(1), \sigma(2)$ уже вибрані, маємо є $n-2$ можливості, і т.д. Для образу останнього елемента лишається єдина можливість. За комбінаторним правилом добутку для вибору підстановки σ є $n!$ можливостей.



1.2.2 Перестановки, інверсії перестановок, парність перестановок та підстановок

Верхній рядок при заданні підстановки таблично, двома рядками, стає зайвим, якщо домовитися про стандарт, звичайне розтшування чисел у зростаючому порядку,

$$(1, 2, 3, \dots, n),$$

то цей верхній рядок стає зайвим і підстановку (1) задають одним нижнім рядком:

$$(\sigma(1), \sigma(2), \sigma(3), \dots, \sigma(n))$$

За такою домовленістю підстановки $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ в прикладах (3) можна задати послідовностями:

$$\sigma_1 = (2, 1), \quad \sigma_2 = (1), \quad \sigma_3 = (3, 1, 5, 2, 4), \quad \sigma_4 = (2, 1, 4, 3, \dots, 2n, 2n - 1). \quad (4)$$

Означення 1.5 *Запис елементів скінченної множини у певному лінійному порядку (один за другим) називають перестановкою.*

В записі перестановки використовують круглі дужки, щоб підкреслити важливість порядку елементів у послідовності, на відміну від фігурних дужок, в які береться перелік елементів множини, де порядок запису елементів не має значення. Таким чином

$$(1, 2), \quad (3, 2, 1), \quad (5, 3, 2, 1, 4)$$

є перестановками — перша на множині $\{1, 2\}$; друга на множині $\{1, 2, 3\}$, третя на множині $\{1, 2, 3, 4, 5\}$.

Означення 1.6 *У перестановці $(i_1, i_2, \dots, i_n)$ чисел $1, 2, \dots, n$ два елементи i_p, i_q утворюють інверсію (зворотний порядок) коли $p < q, i_p > i_q$, тобто коли більше число стоїть раніше, ніж менше.*

Так у перестановці 2,1,5,4,3 елементи 1,2 утворюють інверсію, а елементи 1,4 інверсії не утворюють.

Означення 1.7 *Перестановка назвається парною, якщо вона має парну кількість інверсій. Підстановка називається парною, якщо вона задана парною перестановкою.*

В наведеній вище перестановці 4 інверсії — $\{1, 2\}, \{3, 4\}, \{3, 5\}, \{4, 5\}$, отже підстановка $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$ парною.

Лема 1.1 (про зміну парності кількості інверсій у перестановці) *Якщо у перестановці поміняти місцями два елементи, то парність кількості інверсій зміниться на протилежну (якщо кількість інверсій була парною, то стане непарною, а якщо була непарною, то стане парною).*

Доведення.

Нехай перестановка

$$\beta = (x_1, x_2, \dots, x_u, q, y_1, y_2, \dots, y_v, p, z_1, z_2, \dots, z_w), \quad 0 \leq u, v, w < n$$

на множині $\{1, 2, \dots, n\}$ одержан із перестановки

$$\alpha = (x_1, x_2, \dots, x_u, p, y_1, y_2, \dots, y_v, q, z_1, z_2, \dots, z_w)$$

переставлянням двох елементів $1 \leq p, q \leq n$. Позначимо

$$X = \{x_1, x_2, \dots, x_u\}, \quad Y = \{y_1, y_2, \dots, y_v\}, \quad Z = \{z_1, z_2, \dots, z_w\}.$$

Всі інверсій підстановок α розіб'ємо на кілька типів — до першого віднесмо ті інверсії, що не містять жодного із елементів p, q (позначимо їх кількість в перестановці α через a); до другого віднесемо ті інверсії, що містять один із елементів p, q , а другий із множини $X \cup Z$ (позначимо їх кількість в перестановці α через b); до третього віднесемо ті інверсії, що містять p і елемент із множини Y (позначимо їх кількість в перестановці α через c); до четвертого віднесемо ті інверсії, що містять q і елемент із множини Y (позначимо їх кількість в перестановці α через d). Також позначимо

$$\delta_1 = \begin{cases} 1, & \text{якщо } \{p, q\} \text{ утворюють інверсію в перестановці } \alpha \\ 0, & \text{якщо } \{p, q\} \text{ не утворюють інверсію в перестановці } \alpha. \end{cases}$$

В цих позначеннях перестановка α має

$$m_1 = a + b + c + d + \delta_1$$

інверсій.

Підрахуємо кількість інверсій в підстановці β . Позначимо

$$\delta_2 = \begin{cases} 1, & \text{якщо } \{p, q\} \text{ утворюють інверсію в перестановці } \beta \\ 0, & \text{якщо } \{p, q\} \text{ не утворюють інверсію в перестановці } \beta. \end{cases}$$

Підстановка β ожержана із α переставлянням елементів p, q . Тому $\{p, q\}$ утворюють інверсію в α тоді і тільки тоді, коли $\{p, q\}$ не є інверсією в перестановці β , тобто $\delta_1 = 1 \leftrightarrow \delta_2 = 0$ і в будь-якому випадку

$$\delta_1 + \delta_2 = 1$$

Оскільки елемент p стояв в перестановці α після всіх елементів із Y , елемент q стояв в перестановці α після всіма елементами із Y , а в підстановці β навпаки, то інверсій в β , що містять p і елемент із множини Y буде $v - c$, а тих, що містять q і елемент із множини Y буде $v - d$. Інверсії перестановки β , що не містять жодного із елементів $\{p, q\}$ збігаються з відповідними інверсіями перестановки α . Також збігаються ті інверсії перестановок α, β , в яких один елемент належить $\{p, q\}$, а другий належить $X \cup Z$. Тому всього інверсій в перестановці β буде

$$m_2 = a + b + v - c + v - d + \delta_2.$$

Остання формула дозволяє записати

$$m_1 + m_2 = 2a + 2b + 2v + (\delta_1 + \delta_2) = 2(a + b + v) + 1,$$

$m_1 + m_2$ є непарним числом і, відповідно, числа m_1, m_2 мають протилежну парність.

Теорема доведена

■

Теорема 1.2 *Коли підстановка задана таблично, двома рядками, і в верхньому рядку числа стоять в довільному (не обов'язково в зростаючому) порядку, то парність цієї підстановки збігається з парністю суми кількості інверсій у верхньому і в нижньому рядках.*

Доведення. Твердження теореми впливає з того, що коли переставити два стовпчики табличного задання підстановки, то одночасно зміниться парність кількості інверсій і в верхньому і в нижньому рядках, а парність суми залишиться незмінною.

■

1.3 Множення підстановок

Підстановки (як і будь-які відображення із множини в себе) можна перемножати. Так якщо f, g — дві підстановки, то підстановка $h = fg$ визначається правилом: для будь-яких x $h(x) = f(g(x))$. Звернемо увагу на те, що ім'я елемента, на який діє відображення, ми записуємо справа від імені відображення. Де писати це ім'я — справа чи зліва є питанням домовленості. Наслідком прийнятої домовленості є те, що в добутку двох відображення першим відображенням в добутку, яке діє на елемент множини, є те, яке записане справа. На рис. 1 графічно зображено дві підстановки

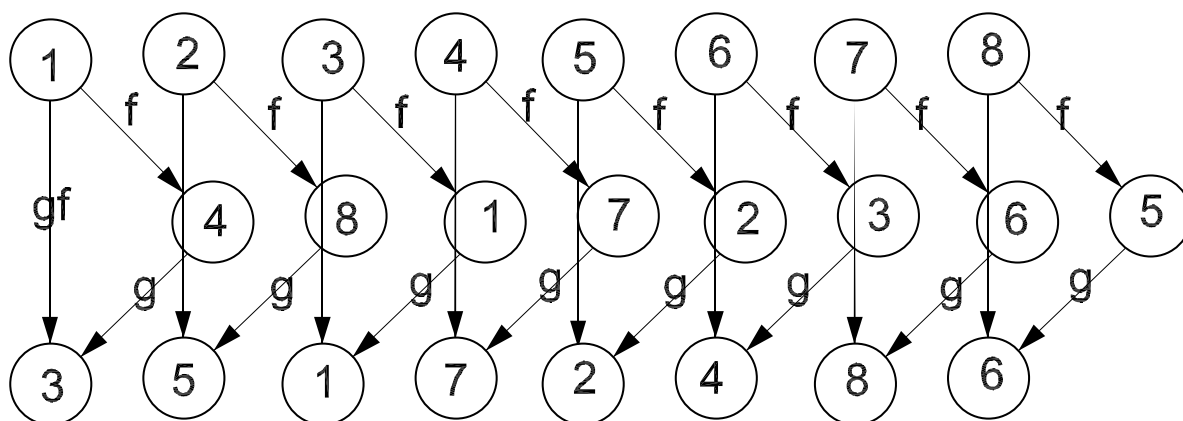


Рис. 1: Добуток двох підстановок. Першою діє на елементи та підстановка, яка в добутку стоїть справа — така домовленість

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 8 & 1 & 7 & 2 & 3 & 6 & 5 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 4 & 3 & 6 & 8 & 7 & 5 \end{pmatrix}, \quad (5)$$

та їх композицію (добуток) gf

$$gf = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 1 & 7 & 2 & 4 & 8 & 6 \end{pmatrix}.$$

В прикладі (5) підстановка f може бути задана перестановкою $(4,8,1,7,2,3,6,5)$. В ній з числом 1 є 2 інверсії $\{4,1\} \{8,1\}$, з числом 2 є 3 інверсії $\{4,2\} \{8,2\} \{7,2\}$, з числом 3 є також 3 інверсії $\{4,3\} \{8,3\} \{7,3\}$, з числом 5 є 3 інверсії $\{8,5\} \{7,5\} \{6,5\}$ і з числом 6 є 2 інверсії $\{7,6\} \{8,6\}$, число 7 утворює одну інверсію $\{8,7\}$. Всього в перестановці $(4,8,1,7,2,3,6,5)$ є $2+3+3+3+2+1=14$ інверсій, отже підстановка f парна.

1.4 Цикли і транспозиції

Означення 1.8 *Одинична підстановка id_M на множині $M = \{1, 2, \dots, n\}$ визначається за допомогою рівності $id(x) = x$, $x = 1, 2, \dots, n$. Елементи $x, f(x), f^2(x) = f(f(x)), f^3(x) = f(f^2(x)), \dots$ утворюють орбіту елемента x . Якщо підстановка має єдину неодноріччелюментну орбіту, то це цикл. Довжина циклу це кількість елементів у його неодноріччелюментній орбіті. Цикли довжини 2 називають транспозиціями. Два цикли називаються незалежними, якщо їх неодноріччелюментні орбіти мають порожній перетин — не мають спільних елементів.*

Запис $a = (a_1, a_2, a_3, \dots, a_{k-1}, a_k)$ означає цикл, який переводить a_1 в a_2 , a_2 в a_3 , і так далі, a_{k-1} в a_k , і a_k в a_1 . Транспозиції мають вигляд (a, b) .

Теорема 1.3 (про розкладання підстановки в добуток незалежних циклів)
Кожна неодноріччелюментна підстановка є добутком незалежних циклів.

Доведення. Нехай $M = \{1, 2, \dots, n\}$ $n \geq 2$ — множина і $f : M \rightarrow M$ неодноріччелюментна підстановка. Розглянемо множину $C_1, C_2, \dots$ різних орбіт. Оскільки кожен елемент належить своїй орбіті, то

$$C_1 \cup C_2 \cup \dots = M.$$

Кожна орбіта є орбітою кожного свого елемента, — це впливає із бієктивності підстановки і із того, що множина M скінченна. Із цього впливає, що

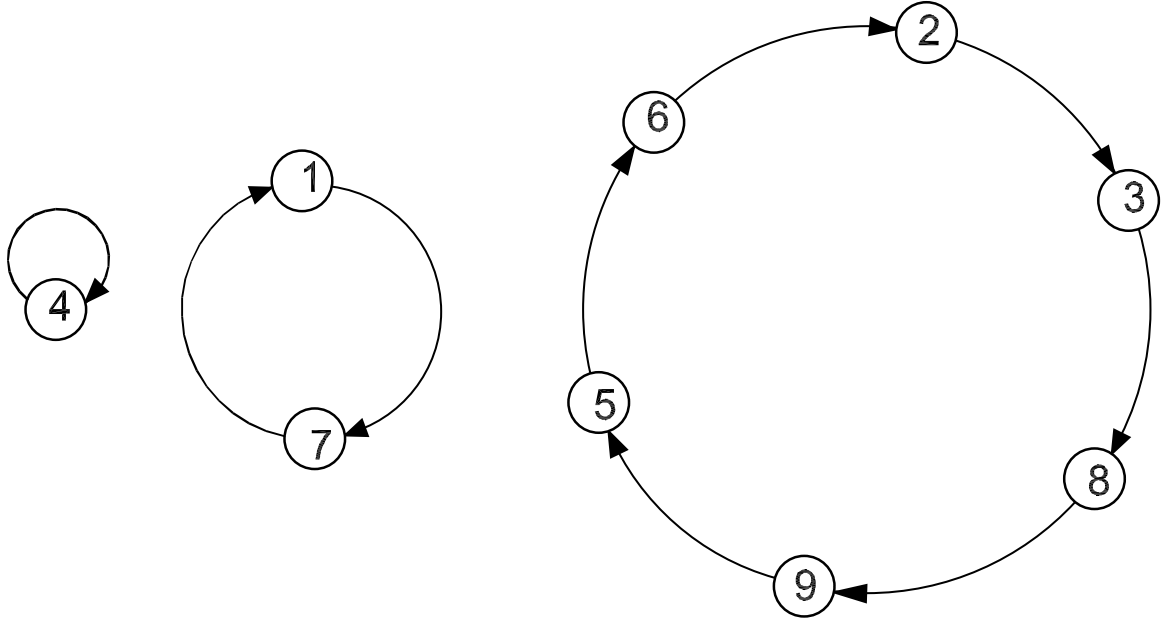


Рис. 2: Підстановка розкладена в добуток 2 незалежних (неодноеlementних) циклів і має три орбіти

різні орбіти мають порожній перетин, тобто

$$C_i \neq C_j \Rightarrow C_i \cap C_j = \emptyset.$$

Далі, за кожною неодноеlementною орбітою $C = \{x, f(x), f^2(x), f^3(x), \dots, f^{k-1}(x)\}$ для деякого $x \in M$ визначаємо цикл $f_C : M \rightarrow M$ правилом: для $y \in M$

$$f_C(y) = \begin{cases} f(y), & \text{якщо } y \in C; \\ y, & \text{якщо } y \notin C. \end{cases}$$

Тепер підстановка f є добутком побудованих незалежних циклів.

■

На рисунку 2 графічно зображено підстановку, яка розкладається у добуток двох незалежних циклів — транспозиції та циклу довжини 6, і має три орбіти.

Підстановка f в прикладі (5) розкладається в добуток двох незалежних циклів $f = (1, 4, 7, 6, 3)(2, 8, 5)$ довжини 5 та 3.

Коли потрібно вказати нерухомі елементи підстановки, тобто ті, орбіти яких одоеlementні, то до запису незалежних циклів додають одоеlementні

орбіти — один елемент в круглих дужках. Наведемо приклад. Підстановка

$$\sigma = (2, 1, 5, 8)(6, 3, 4)$$

є добутком двох циклів. Але коли потрібно вказати, що ця підстановка діє на 10-елементній множині і нерухомими є елементи 7,9,10, то потрібно писати

$$\sigma = (2, 1, 5, 8)(6, 3, 4)(7)(10)$$

Теорема 1.4 *Кожну підстановку на множині $M = \{1, 2, \dots, n\}$ $n \geq 2$ можна записати у вигляді добутку транспозицій.*

Доведення. Справді, одиничну підстановку можна записати у вигляді квадрата транспозиції $(1, 2)$. Неодінчну підстановку можна розкласти в добуток циклів, а кожен цикл можна розкласти в добуток транспозицій, кількість яких на одиницю менша ніж довжина цикла

$$(i_1, i_2, \dots, i_{k-1}, i_k) = (i_1, i_2) \cdot (i_2, i_3) \cdot (i_3, i_4) \cdot \dots \cdot (i_{k-1}, i_k) \quad k > 1. \quad (6)$$

■

Так, можна записати

$$(1, 4, 7, 6, 3) = (1, 4)(4, 7)(7, 6)(6, 3), \quad (2, 8, 5) = (2, 8)(8, 5).$$

Тепер підстановку

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 8 & 1 & 7 & 2 & 3 & 6 & 5 \end{pmatrix}$$

можна записати як добуток 6 транспозицій (циклів довжини 2):

$$f = (1, 4, 7, 6, 3)(2, 8, 5) = (1, 4)(4, 7)(7, 6)(6, 3)(2, 8)(8, 5).$$

Підстановка

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 4 & 3 & 6 & 8 & 7 & 5 \end{pmatrix}$$

може бути задана перестановкою $(1, 2, 4, 3, 6, 8, 7, 5)$. Її можна задати як добуток двох незалежних циклів $g = (3, 4)(5, 6, 8)$ і у вигляді добутку 3 транспозицій $g = (3, 4)(5, 6)(6, 8)$, або, якщо потрібно відмітити нерухомі елементи, у вигляді $g = (1)(2)(3, 4)(5, 6)(6, 8)(7)$. Порядок запису циклів не має значення.

Теорема 1.5 (про парність підстановки) . Підстановка є парною в тому і тільки тому випадку, коли вона є добутком парної кількості транспозицій.

Доведення. Для доведення теореми досить показати, що множення підстановки на транспозицію змінює парність кількості інверсій.

Нехай $\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & p & \dots & q & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_p & \dots & i_q & \dots & i_n \end{pmatrix}$. Тоді $(i_p, i_q)\sigma = \sigma(p, q)$ одержується із σ переставлянням $2(q - p) - 1$ сусідніх елементів у нижній перестановці, кожне з яких змінює парність.

■

Означення 1.9 Якщо від кількості елементів відняти кількість незалежних циклів, на які розкладається підстановка, то одержне число називають декрементом підстановки. Декремент одиначної підстановки дорівнює нулю.

Лекремент підстановки $g = (3, 4)(5, 6, 8)$, дорівнює $5-2=3$, де 6 це число рухомих елементів, 3 кількість неоднорелементних циклів. Декремент цієї ж підстановки, записаної у вигляді $g = (1)(2)(3, 4)(5, 6, 8)(7)$, дорівнює $8-5$, де 8 це кількість елементів множини, на якій діє підстановка, а 6 це кількість незалежних циклів, включаючи однорелементні.

Теорема 1.6 Підстановка є парною тоді і тільки тоді, коли її декремент є парним числом.

Доведення. Доведення полягає в тому, що кожен цикл є добутком транспозицій, кількість яких на одиницю менша ніж довжина циклу.

■

Згідно з наведеною теоремою підстановка $g = (3, 4)(5, 6, 8)$ непарна.

1.5 Застосування підстановок для обчислення визначників

Означення 1.10 Визначником (або детермінантом) $\det A$ квадратної матриці

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix}$$

називається число

$$\det A = \begin{vmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{vmatrix}$$

яке обчислюється за формулою

$$\det A = \sum_{\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \in S_n} \text{sign}(\sigma) a_{1i_1} a_{2i_2} a_{3i_3} \dots a_{ni_n}, \quad (7)$$

де S_n сукупність всіх підстановок на множині $\{1, 2, \dots, n\}$, $n \geq 1$, а

$$\text{sign } \sigma = \begin{cases} 1, & \text{підстановка } \sigma \text{ парна,} \\ -1, & \text{підстановка } \sigma \text{ непарна,} \end{cases}$$

Із означення парності підстановки видно, що sign можна обчислювати за формулою

$$\text{sign } \sigma = (-1)^{N(\sigma(1), \sigma(2), \sigma(3), \dots, \sigma(n))},$$

де $N(\sigma(1), \sigma(2), \sigma(3), \dots, \sigma(n))$ — кількість інверсій у перестановці $(\sigma(1), \sigma(2), \sigma(3), \dots, \sigma(n))$.

Теорема 1.7 (про розкладення визначника за елементами першого рядка)

Для кожної матриці A розміру $n \times n$ $n \geq 2$ правильною є формула

$$\det A = \sum_{i=1}^n (-1)^{i-1} a_{1,i} M_i^1 \quad (8)$$

де M_i^1 — мінор, тобто визначник матриці розміру $(n-1) \times (n-1)$ $n \geq 2$, яка одержується із матриці A викреслюванням першого рядка та i -го стовпчика.

Доведення. За означенням

$$\begin{aligned} \det A &= \sum_{\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \in S_n} \text{sign}(\sigma) a_{1i_1} a_{2i_2} a_{3i_3} \dots a_{ni_n} = \\ &= \sum_{i=1}^n \sum_{\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i & \sigma(2) & \dots & \sigma(n) \end{pmatrix} \in S_n} (-1)^{N(i, \sigma(2), \sigma(3), \dots, \sigma(n))} a_{1,i} a_{2, \sigma(2)} a_{3, \sigma(3)} \dots a_{n, \sigma(n)}. \end{aligned} \quad (9)$$

j -й рядок ($j > 1$) після викреслювання 1-го рядка в матриці A матиме номер $j-1$, а j -й стовпчик після викреслювання i -го стовпчика матиме той же номер j , якщо $j < i$, і буде мати номер $j-1$, якщо $j > i$. Тому

$$\begin{aligned} M_i^1 &= \begin{vmatrix} a_{21} & \dots & a_{2,i-1} & a_{2,i+1} & \dots & a_{2n} \\ a_{31} & \dots & a_{3,i-1} & a_{3,i+1} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{n,i-1} & a_{n,i+1} & \dots & a_{nn} \end{vmatrix} = \begin{vmatrix} m_{1,1} & m_{1,2} & \dots & m_{1,n-1} \\ m_{2,1} & m_{2,2} & \dots & m_{2,n-1} \\ \dots & \dots & \dots & \dots \\ m_{n-1,1} & m_{n-1,2} & \dots & m_{n-1,n-1} \end{vmatrix} = \\ &= \sum_{\tau \in S_{n-1}} (-1)^{N(\tau(1), \tau(2), \dots, \tau(n-1))} m_{1, \tau(1)} m_{2, \tau(2)} \dots m_{n-1, \tau(n-1)} \end{aligned} \quad (10)$$

де

$$m_{p,q} = \begin{cases} a_{p+1,q}, & \text{якщо } q < i, \\ a_{p+1,q+1}, & \text{якщо } q > i, \end{cases}$$

і при заданому фіксованому $1 \leq i \leq n$ між доданками (9) і (10) встановлюється взаємно однозначна відповідність, де відповідні доданки рівні, а саме, ми можемо вважати, що

$$\tau(j) = \begin{cases} \sigma(j), & \text{якщо } \sigma(j) < i, \\ \sigma(j) - 1, & \text{якщо } \sigma(j) > i. \end{cases}$$

Оскільки для будь-якої підстановки $\sigma \in S_n$ $\sigma(1) = i$ утворює інверсію з числами $1, 2, \dots, \sigma(1) - 1$, то $\sigma(1)$ утворює рівно $i - 1$ інверсій і

$$(-1)^{N(i, \sigma(2), \sigma(3), \dots, \sigma(n))} = (-1)^{i-1} (-1)^{N(\sigma(2), \sigma(3), \dots, \sigma(n))} = (-1)^{N(\tau(1), \tau(2), \dots, \tau(n-1))} = (-1)^{i-1} \text{sign } \tau \quad (11)$$

Формула (11) дозволяє переписати формулу (9) у вигляді

$$\det A = \sum_{i=1}^n (-1)^{i-1} a_{1,i} \sum_{\tau \in S_{n-1}} \text{sign } \tau \cdot m_{1, \tau(1)} m_{2, \tau(2)} \dots m_{n-1, \tau(n-1)} = \sum_{i=1}^n a_{1,i} (-1)^{i-1} M_i^1. \quad (12)$$

Теорема доведена.

Теорема (1.7) дозволяє записати

$$\begin{vmatrix} a & b & c \\ -1 & 2 & 0 \\ 3 & 5 & -7 \end{vmatrix} = a \cdot \begin{vmatrix} 2 & 0 \\ 5 & -7 \end{vmatrix} - b \cdot \begin{vmatrix} -1 & 0 \\ 3 & -7 \end{vmatrix} + c \cdot \begin{vmatrix} -1 & 2 \\ 3 & 5 \end{vmatrix}.$$

■

Теорема 1.8 (про визначник транспонованої матриці) *Визначник транспонованої матриці збігається із визначником самої матриці.*

Доведення. Нехай маємо матрицю A розміру $n \times n$ і матриця $B = A^T$, що транспонована до A :

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}, \quad A^T = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{n1} \\ a_{12} & a_{22} & \dots & a_{n2} \\ \dots & \dots & \dots & \dots \\ a_{1n} & a_{2n} & \dots & a_{nn} \end{pmatrix} = B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \dots & \dots & \dots & \dots \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{pmatrix}.$$

Відповідно $b_{i,j} = a_{j,i}$, $i, j = 1, 2, \dots, n$. В цих позначеннях враховуючи, що для $\sigma \in S_n$

$$\text{sign } (\sigma) = (-1)^{N(\sigma(1), \sigma(2), \sigma(3), \dots, \sigma(n))} = \text{sign } \begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ 1 & 2 & \dots & n \end{pmatrix}$$

маємо

$$\det A = \sum_{\sigma \in S_n} (-1)^{N(\sigma(1), \sigma(2), \sigma(3), \dots, \sigma(n))} a_{1, \sigma(1)} a_{2, \sigma(2)} \dots a_{n, \sigma(n)} =$$

$$= \sum_{\sigma \in S_n} (-1)^{N(\sigma(1), \sigma(2), \sigma(3), \dots, \sigma(n))} b_{1, \sigma(1)} b_{2, \sigma(2)} \dots b_{n, \sigma(n)} = \det B.$$

Теорема доведена.

■

Розглянемо матриці розміру $n \times n$, що утворені рядками

$$e_1 = (1, 0, 0, \dots, 0), e_2 = (0, 1, 0, \dots, 0), e_3 = (0, 0, 1, \dots, 0), \dots e_n = (0, 0, 0, \dots, 1),$$

тобто рядок e_i має довжину n і всі його елементи, крім i -го, дорівнюють нулю, а i -й, дорівнює одиниці. Якщо $\sigma \in S_n$, то ми можемо розглянути матрицю A_σ , першим рядком якої є $e_{\sigma(1)}$, другим рядком є $e_{\sigma(2)}$ і т.д., а n -м рядком є $e_{\sigma(n)}$. Таку матрицю можна назвати матрицею-підстановкою. За формулою (7)

$$\det A_\sigma = \text{sign}(\sigma).$$

Для прикладу, якщо $n = 4$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \in S_4,$$

,то

$$A_\sigma = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

і

$$\det A_\sigma = (-1)^{N(2,4,1,3)} = (-1)^3 = -1.$$

1.6 Числа Стірлінга 1-го роду

Підстановки є давнім і важливим і інструментом досліджень і об'єктом досліджень. Зокрема, підстановок стосується і ряд комбінаторних задач. Числа, що є спільною відповіддю до кількох різних комінаторних задач, які часто використовуються, називаються комбінаторними числами. А задачі, відповіді до яких є комбінаторними числами, називають модельними задачами. Прикладом комбінаторного числа є число Стірлінга першого роду, і

модельна задача, відповіддю до якої слугує це число, стосується підстановок.

Означення 1.11 *Кількість підстановок n -го степеня, $n \geq 1$, які мають k різних орбіт, $k \geq 1$, називається числом Стірлінга першого роду із n по k і позначається $\left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right]$. Зручно вважати, що $\left[\begin{smallmatrix} n \\ 0 \end{smallmatrix} \right] = 0$ для всіх $n = 1, 2, \dots$, і $\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix} \right] = 1$.*

Існує єдина підстановка в S_n , яка має n орбіт - це одинична підстановка. Тому $\left[\begin{smallmatrix} n \\ n \end{smallmatrix} \right] = 1$.

Щоб підстановка мала одну орбіту, потрібно, щоб ця підстановка була циклом довжини n . Циклів довжини n в S_n $(n-1)!$, тому що образів одиниці $n-1$, образів двійки, коли образ одиниці вибраний, $n-2$ і так далі. Образ останнього елемента визначається однозначно. Отже $\left[\begin{smallmatrix} n \\ 1 \end{smallmatrix} \right] = (n-1)!$.

Оскільки підстановка із S_n не може мати більше n орбіт, то при $k > n$ $\left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right] = 0$.

При малих значеннях n всі ненульові числа Стірлінга легко підраховуються

$$\begin{aligned} \left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix} \right] &= 1; \\ \left[\begin{smallmatrix} 2 \\ 1 \end{smallmatrix} \right] &= \left[\begin{smallmatrix} 2 \\ 2 \end{smallmatrix} \right] = 1; \\ \left[\begin{smallmatrix} 3 \\ 1 \end{smallmatrix} \right] &= 2, \left[\begin{smallmatrix} 3 \\ 2 \end{smallmatrix} \right] = 3, \left[\begin{smallmatrix} 3 \\ 3 \end{smallmatrix} \right] = 1. \end{aligned}$$

Таким чином одержується своєрідний трикутник, що нагадує трикутник Паскаля для біномних коефіцієнтів.

Одержимо рекурентне співвідношення для чисел Стірлінга першого роду, яке дозволить обчислити елементи наступних рядків в трикутнику, коли

відомі попередні, тобто дозволяє обчислити $\begin{bmatrix} n \\ k \end{bmatrix}$ для всіх k , коли при всіх k відомі всі коефіцієнти $\begin{bmatrix} n-1 \\ k \end{bmatrix}$, $n \geq 2$.

Теорема 1.9 (рекурентне співвідношення для чисел Стірлінга першого роду)
Для $n \geq 2$ числа Стірлінга першого роду підкоряються умові

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + (n-1) \begin{bmatrix} n-1 \\ k \end{bmatrix}, n = 2, 3, \dots; k = 1, 2, \dots \quad (13)$$

Доведення.

Нехай U множина підстановок на n -елементній множині A , які мають рівно k орбіт, $n = 2, 3, 4, \dots; k = 0, 1, 2, \dots$. За комбінаторним визначенням чисел Стірлінга першого роду кількість елементів у множині U дорівнює $\begin{bmatrix} n \\ k \end{bmatrix}$. Виділимо в A один елемент $a \in A$ і позначимо $B = A \setminus \{a\}$.

Всі підстановки із U розбиваємо на два типи. До першого типу відносимо ті підстановки, для яких a утворює одноелементну орбіту (або є одноелементним циклом). До другого типу віднесемо ті підстановки, для яких a знаходиться у неодноелементній орбіті. Множину підстановок першого типу позначимо через U_1 , а множину підстановок другого типу позначимо через U_2 . Таким чином $U = U_1 \cup U_2$, $U_1 \cap U_2 = \emptyset$, і за правилом суми $|U| = |U_1| + |U_2|$.

Зрозуміло, що між підстановками із U_1 і тими підстановками на множині B , які мають $k-1$ орбіту, існує взаємно однозначна відповідність. Тому $|U_1| = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}$.

Якщо взяти підстановку f на множині B , яка має k орбіт, і довільний елемент $b \in B$, то за ними можна побудувати підстановку $g \in U$ наступним чином: вважаємо для $g(a) = b$, $g(c) = a$, якщо $f(c) = b$, і $g(x) = f(x)$, якщо $x \neq a$, $f(x) \neq b$. У запропонований спосіб кожна підстановка на множині B , яка має k орбіт, породжує $n-1$ підстановку із U_2 і всі підстановки із U_2 у такий спосіб одержаться по одному разу. Оскільки ми маємо $\begin{bmatrix} n-1 \\ k \end{bmatrix}$

дорівнює кількості підстановок на множині B , які мають рівно k орбіт, то за правилом добутку маємо $|U_2| = (n-1) \cdot \begin{bmatrix} n-1 \\ k \end{bmatrix}$. Звідси одержуємо рекурентне співвідношення (13)

Неспер ми можемо обчислити всі ненульові числа $\begin{bmatrix} 4 \\ k \end{bmatrix}$: ■

$$\begin{bmatrix} 4 \\ 1 \end{bmatrix} = \begin{bmatrix} 3 \\ 0 \end{bmatrix} + 3 \begin{bmatrix} 3 \\ 1 \end{bmatrix} = 6, \quad \begin{bmatrix} 4 \\ 2 \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \end{bmatrix} + 3 \begin{bmatrix} 3 \\ 2 \end{bmatrix} = 11,$$

$$\begin{bmatrix} 4 \\ 3 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \end{bmatrix} + 3 \begin{bmatrix} 3 \\ 3 \end{bmatrix} = 6, \quad \begin{bmatrix} 4 \\ 4 \end{bmatrix} = \begin{bmatrix} 3 \\ 3 \end{bmatrix} + 3 \begin{bmatrix} 3 \\ 4 \end{bmatrix} = 1.$$

Означення 1.12 Для змінної x і $n = 0, 1, 2, \dots$ многочлен $x^{\bar{n}}$, що визначається умовами

$$x^{\bar{0}} = 1, \quad x^{\bar{1}} = x, \quad x^{\bar{n}} = x \cdot (x+1) \cdot (x+2) \cdot \dots \cdot (x+n-1) \text{ коли } n > 1,$$

називається зростаючим факторіальним степенем.

Теорема 1.10 (аналітичне введення чисел Стірлінга першого роду)

Числа Стірлінга першого роду є коефіцієнтами зростаючого факторіального степеня, точніше, при $n = 0, 1, 2, \dots$

$$x^{\bar{n}} = \begin{bmatrix} n \\ 0 \end{bmatrix} + \begin{bmatrix} n \\ 1 \end{bmatrix} x + \begin{bmatrix} n \\ 2 \end{bmatrix} x^2 + \dots + \begin{bmatrix} n \\ n \end{bmatrix} x^n.$$

Доведення. Доведення поводимо методом математичної індукції.

База індукції — превряємо теорему при малих значеннях n . При $n = 0$

$$x^{\bar{0}} = 1 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

і теорема справджується.

При $n = 1$

$$x^{\bar{1}} = x = \begin{bmatrix} 1 \\ 1 \end{bmatrix} x$$

і також теорема справджується.

При $n = 2$

$$x^{\bar{1}} = x = \begin{bmatrix} 1 \\ 1 \end{bmatrix} x$$

і також теорема справджується.

При $n = 2$

$$x^{\bar{1}} = x(x + 1) = 0 + x + x^2 = \begin{bmatrix} 2 \\ 2 \end{bmatrix} x + \begin{bmatrix} 2 \\ 1 \end{bmatrix} x^2.$$

і теорема знову справджується.

Зауважимо також, що для будь-якого $n \geq 1$ вільний член зростаючого факторіального степеня $x^{\bar{n}}$ дорівнює 0, тобто $\begin{bmatrix} n \\ 0 \end{bmatrix}$.

Індуктивне припущення: Припустимо, що теорема правильна для деякого $n \geq 2$.

Індуктивний перехід. Доведемо теорему для зростаючого степеня $x^{\overline{n+1}}$.

Нехай зростаючі факторіальні степені $x^{\bar{m}}, m \geq 2$ мають коефіцієнти $\alpha(m, i), i = 0, 1, 2, \dots$, тобто

$$x^{\bar{n}} = \alpha(m, 0) + \alpha(m, 1)x + \alpha(m, 2)x^2 + \dots + \alpha(m, m)x^m.$$

Лема 1.2 Коефіцієнти зростаючого факторіального степеня підкоряються рекурентному співвідношенню

$$\alpha(m, k) = \alpha(m - 1, k - 1) + (m - 1)\alpha(m - 1, k), \quad m \geq 2, k \geq 1 \quad (14)$$

Доведення.

$$\begin{aligned} \sum_{k=0}^{\infty} \alpha(m, k)x^k &= x^{\bar{m}} = x^{\overline{m-1}} \cdot (x+m-1) = \left(\sum_{k=0}^{\infty} \alpha(m-1, k)x^k \right) \cdot (x+m-1) = \\ &= \sum_{k=0}^{\infty} (\alpha(m-1, k-1) + (m-1) \cdot \alpha(m-1, k)) x^k. \end{aligned}$$

Звідси, для будь-яких натуральних $m \geq 2, k > 1$ одержуємо формулу (14)

Лема доведена.

■

Продовжимо доведення теореми. Оскільки за індуктивним припущенням

$$\alpha(n, k) = \begin{bmatrix} n \\ k \end{bmatrix}, \quad k = 0, 1, 2, \dots,$$

то згідно з формулами (13),(14)

$$\alpha(n+1, k) = \begin{bmatrix} n+1 \\ k \end{bmatrix}, \quad k = 0, 1, 2, \dots$$

■

2 Симетрична та знаковмінна група

2.1 Напівгрупа. Група. Підгрупа

Означення 2.1 Множина S з однією асоціативною бінарною (двомісною) операцією $f : S \times S \rightarrow S$, тобто

$$f(f(a, b), c) = f(a, f(b, c))$$

для будь-яких $a, b, c \in S$, називається напівгрупою. Якщо операція названа додаванням, то напівгрупа адитивна, а якщо операція названа множенням, то напівгрупа буде мультиплікативною. Елемент $e \in S$ називається нейтральним елементом відносно операції f , якщо $f(e, a) = f(a, e) = a$ для будь-якого елемента $a \in S$. В адитивній напівгрупі нейтральний елемент звичайно називається нулем, і позначається 0 , а в мультиплікативній напівгрупі нейтральний елемент називається одиницею і позначається 1 . Якщо в напівгрупі є нейтральний елемент і застосування бінарної операції до двох елементів дає нейтральний елемент, то ці два елементи називають оберненими один до другого. В адитивній напівгрупі обернений до $a \in S$ позначається a^{-1} . В адитивній напівгрупі обернений до $a \in S$ елемент позначається $-a$ і називається протилежним.

Отже, адитивна напівгрупа S підкоряється одній аксіомі

$$\forall a, b, c \in S \quad (s + (b + c)) = ((a + b) + c) \text{ — асоціативність додавання;}$$

мультиплікативна напівгрупа S підкоряється одній аксіомі

$$\forall a, b, c \in S \quad (s \cdot (b \cdot c)) = ((a \cdot b) \cdot c) \text{ — асоціативність множення;}$$

нуль адитивної напівгрупи визначається умовою

$$\forall a \in S \quad (s + 0 = 0 + a = a;$$

нуль мультиплікативної напівгрупи визначається умовою

$$\forall a \in S \quad (s \cdot 0 = 0 \cdot a = 0;$$

одиниця мультиплікативної напівгрупи визначається умовою

$$\forall a \in S \quad (s \cdot 0 = 0 \cdot a = 0;$$

протилежний до елемента $a \in S$ напівгрупи S визначається умовою

$$s + (-a) = -a + aa = 0;$$

обернений до елемента $a \in S$ напівгрупи S визначається умовою

$$s \cdot a^{-1} = a^{-1} \cdot a = 1.$$

Зауважимо, що напівгрупа може бути порожньою.

Прикладами півгруп будуть:

Напівгрупа всіх відображень із множини в себе з операцією множення (або композицією) відображень. Тотожне відображення, що переводить кожен елемент в себе є нейтральним елементом.

Адитивна напівгрупа натуральних чисел. В шкільному курсі математики вважається, що нуль не є натуральним числом. В цьому випадку адитивна напівгрупа натуральних чисел не має нуля. Оскільки нуль є кількістю елементів порожньої множини, то можна вважати, що нуль є натуральним числом, в такому разі адитивна напівгрупа натуральних чисел має нуль.

Мультиплікативна напівгрупа натуральних чисел має одиницю, але обернений елемент існує лише для одиниці (одиниця сама до себе обернена).

Адитивна напівгрупа прямокутних матриць заданого розміру над заданим полем має нуль — всі елементи нульової матриці нулі.

Мультіплікативна напівгрупа квадратних матриць заданого розміру над заданим полем має одиницю — в одиничній матриці по головній діагоналі стоять одиниці, а решта елементів нулі.

Всі підмножини заданої множини і з операцією перетину і операцією об'єднання і з операцією симетричної різниці утворюють напівгрупу з нейтральним елементом. Якщо операція перетин, то нейтральним елементом є вся множина, якщо операція симетрична різниця або об'єднання, то нейтральним елементом є порожня множина.

Множина S з операцією

$$\forall a, b \in S \ a \cdot b = a$$

утворює так звану напівгрупу лівих нулів. А множина S з операцією

$$\forall a, b \in S \ a \cdot b = b.$$

утворює так звану напівгрупу правих нулів. Ряди, многочлени з операціями множення.

Мультіплікативні і адитивні напівгрупи формальних степеневих рядів та многочленів мають нейтральні елементи 0 та 1.

Означення 2.2 *Напівгрупа називається групою, якщо вона має нейтральний елемент і кожен елемент має обернений.*

Із умови "В групі існує нейтральний елемент" випливає, що група обов'язково не порожня.

Оборотні квадратні матриці заданого розміру утворюють мультіплікативну групу: цілі числа утворюють адитивну групу; ненульові дійсні числа утворюють мультіплікативну групу; симетрії кола утворюють мультіплікативну групу; рухи площини утворюють мультіплікативну групу.

Означення 2.3 *Нехай маємо дві напівгрупи — S_1 з операцією $a \cdot b$ для $a, b \in S_1$ і S_2 з операцією $c \star d$ для $c, d \in S_2$, і виконуються умови*

$$S_2 \subseteq S_1;$$

$$\forall, x, y \in S_2 \quad x \cdot y = x \star y,$$

то кажуть, що множина S_2 замкнена відносно операції $\cdot$; операція $\star$ є обмеженням операції $\cdot$ на множину S_2 ; напівгрупа S_2 з операцією $\star$ є піднапівгрупою напівгрупи S_1 з операцією $\cdot$.

Означення 2.4 Нехай маємо дві групи — S_1 з операцією $a \cdot b$ для $a, b \in S_1$ та S_2 з операцією $c \star d$ для $c, d \in S_2$, і операція $\star$ є обмеженням операції $\cdot$ на S_2 , то S_2 називають підгрупою групи S_1 .

Так адитивна група цілих чисел є підгрупою адитивної групи дійсних чисел, а $\{0, 1\}$ — двоелементна мультиплікативна підгрупа мультиплікативної групи ненульових дійсних чисел.

Кожна група має дві так звані "тривіальні" підгрупи — одна збігається з усією групою, а друга одноелементна, вона складається із одного нейтрального елемента.

Означення 2.5 Степінь g^k елемента $g \in G$ мультиплікативної групи G визначається індуктивно. Для $g \in G$ нульовий степінь збігається із нейтральним елементом, і

$$g^{n+1} = g^n \cdot g, \quad g^{-n} = (g^{-1})^n \quad n = 0, 1, 2, \dots$$

Якщо група G адитивна, то для $g \in G$ і $k = 0, 1, 2, \dots$ використовують термін " k —кратний" елемент $k \cdot g$, який визначається умовами

$$0 \cdot g = 0, \quad (n+1) \cdot g = n \cdot g + g, \quad (-n) \cdot g = n \cdot (-g), \quad n = 0, 1, 2, \dots$$

Можна переконатися, що множення степенів заданого елемента $g \in G$ групи підкоряється правилам

$$g^0 = 1, \quad g^1 = g, \quad g^{-n} = (g^n)^{-1}, \quad g^n \cdot g^m = g^{n+m}, \quad g^n \cdot (g^m)^{-1} = g^{n-m}. \quad (15)$$

Теорема 2.1 (про степені елемента групи) Всі степені заданого елемента заданої групи утворюють підгрупу цієї групи.

Доведення. Нехай G група, $g \in G$ її елемент і

$$H = \{g^n | n \in \mathbb{Z}\} \subseteq G.$$

Щоб довести, що H є підгрупою групи G потрібно довести, що H не порожня множина і переконатися в тому що

$$x, y \in H \Rightarrow x \cdot y^{-1} \in H. \quad (16)$$

Множина H не порожня, тому що в ній містяться $g = g^1$ і нейтральний елемент g^0 .

Для перевірки (16) вибираємо $x = g^i, y = g^j, \quad i, j \in \mathbb{Z}$, і записуємо

$$x \cdot y^{-1} = g^i \cdot g^{-j} = g^{i-j}$$

■

Означення 2.6 Група називається циклічною, якщо вона збігається із множиною степенів якогось свого елемента.

Оскільки всі степені елемента утворюють підгрупу заданої групи, то ця підгрупа буде циклічною.

Означення 2.7 Група називається комутативною, якщо результат застосування операції до двох елементів не залежить від порядку цих двох елементів. Відповідно, мультиплікативна група G комутативна, якщо

$$\forall a, b \in G \quad a \cdot b = b \cdot a,$$

адитивна група G комутативна, якщо

$$\forall a, b \in G \quad a + b = b + a.$$

Адитивна група цілих чисел комутативна, кожна циклічна група комутативна, адитивна група прямокутних матриць заданого розміру комутативна, група обертань кола комутативна.

Комутативна група квадратних оборотних матриць некомутативна.

Традиційно, операцію в групі називають додаванням лише для комутативних груп.

Означення 2.8 Кількість елементів групи називають порядком групи. Якщо група нескінченна, то кажуть, що вона "нескінченного порядку". Кількість елементів циклічної підгрупи, що утворена степенями заданого елемента, називається порядком цього елемента. Можна сказати, що порядок елемента, це найменший ненульовий степінь, о якого потрібно піднести заданий елемент, що одержати нейтральний елемент. Порядок групи G позначається $|G|$.

Означення 2.9 Якщо G — група, H — її підгрупа, і $g \in G$ елемент групи, то множина

$$g \cdot H = \{g \cdot h | h \in H\} \subseteq G$$

називається правим суміжним класом елемента $g \in G$ за підгрупою H , а множина

$$H \cdot g = \{h \cdot g | h \in H\} \subseteq G$$

називається лівим суміжним класом елемента $g \in G$ за підгрупою H .

Теорема 2.2 (Лагранжа про порядок підгрупи) В скінченній групі порядок підгрупи є дільником порядку групи і дорівнює добутку порядку підгрупи на кількість різних правих (або лівих) суміжних класів.

Доведення. Нехай G — група і $H \subseteq G$ її підгрупа. Оскільки $g \in H \cdot g$ для будь-якого $g \in G$, то

$$\bigcup_{g \in G} g \cdot H = G.$$

Переконаємося, що різні суміжні класи мають порожній перетин, тобто коли суміжні класи мають спільний елемент, то вони збігаються. Справді, нехай $g_1, g_2 \in G$ і $u \in g_1 H \cap g_2 H$. Тоді для деяких h_1, h_2

$$g_1 h_1 = u = g_2 h_2,$$

і для будь-якого $h \in H$

$$g_1 h = g_2 (h_2 h_1 h); \tag{17}$$

$$g_2 h = g_1 (h_1 h_2 h). \tag{18}$$

Із рівності (18) випливає, що

$$g_1 H \subseteq g_2 H,$$

а із рівності (??) випливає, що

$$g_2 H \subseteq g_1 H.$$

Отже, $g_1 H = g_2 H$, і група є об'єднанням різних суміжних класів, що мають порожній перетин.

Для доведення теореми лишилося переконатись, що всі суміжні класи мають одну і ту ж кількість елементів, а саме, вона дорівнює кількості елементів в підгрупі H , тобто

$$|g \cdot H| = |H|, \quad g \in G. \quad (19)$$

За комбінаторним правилом рівності дві множини мають одну і ту ж кількість елементів тоді і тільки тоді, коли існує взаємно однозначна відповідність між елементами цих множин, або існує оборотне відображення із однієї множини в другу. Ми можемо вказати взаємно обернені відображення

$$\hat{g} : H \rightarrow gH, \quad \hat{g}(h) = gh, \quad (20)$$

$$\hat{g}^{-1} : gH \rightarrow H, \quad \hat{g}^{-1}(u) = g^{-1}u, \quad (21)$$

тому (19) справджується. Теорема доведена. ■

В загальному випадку ліві суміжні класи не збігаються із правими суміжними класами, але в деяких випадках (зокрема, в комутативних групах) це так.

Означення 2.10 Підгрупа, для якої ліві суміжні класи збігаються із правими суміжними класами називається інваріантною або нормальним дільником.

Теорема 2.3 (умова інваріантності підгрупи) Підгрупа H групи G інваріантна тоді і тільки тоді, коли для будь-яких $g \in G$, $h \in H$ буде $ghg^{-1} \in H$.

Доведення. Нехай підгрупа H групи G нваріантна і, відповідно, для $g \in G$ суміжні класи $gH = Hg$. Тоді для будь-якого $h \in H$ снує $h_1 \in H$ такий, що $gh = h_1g$, $ghg^{-1} = h_1 \in H$. Ми довели, що

$$gH = Hg \Rightarrow \forall h \in H \exists h_1 \in H (ghg^{-1} = h_1).$$

Припустимо тепер, що для деякого $h \in H$ $ghg^{-1} = g_1 \notin H$. Тоді припущення $gh = g_1g = h_1g \in Hg$ приводить до суперечності $g_1 = h_1$.

Теорема доведена. ■

Означення 2.11 Унарна (одномісна) операція в групі G

$$x \rightarrow g \cdot x \cdot g^{-1},$$

яка визначається елементом $g \in G$, називається спряженням.

Використовуючи цей термін умову інваріантності підгрупи можна переформулювати наступним чином.

Теорема 2.4 Підгрупа інваріантна тоді і тільки тоді, коли вона замкнена відносно всіх спряжень, що визначаються елементами групи.

Класи сужності групи G по підгрупі H можна множити — в заданих класах K_1, K_2 вибираємо по представнику $x \in K_1, y \in K_2$, знаходимо добуток цих представників, застосовуючи операцію в групі, і знаходимо той клас K , якому належить знайдений добуток.

Теорема 2.5 (коректність визначення операції на класах суміжності)

Якщо підгрупа є нормальним ділянком, то результат множення класів не залежить від вибору представників в цих класах.

Доведення.

Нехай G — група, H — підгрупа, два класи суміжності

$$K_1 = g_1H, \quad K_2 = g_2H, \quad g_1, g_2 \in G, x \in K_1, y \in K_2.$$

Представники вибрані так, що $x = g_1h_1, y = g_2h_2$ для деяких h_1, h_2 . Тоді

$$xy = g_1h_1g_2h_2 = g_1g_2g_2^{-1}h_1g_2h_3.$$

Оскільки підгрупа H інваріантна, то спряжений до $h_1 \in H$ знову лежить в H , тобто для деякого $f \in H$

$$g_2^{-1}h_1g_2 = f_1 \in H, \quad x_1y_1 = g_1g_2fh_2 \in g_1g_2H. \quad (22)$$

Із (22) бачимо, що клас, якому належить добуток, не залежить від вибору представників.

Теорема доведена. ■

Означення 2.12 Класи суміжності групи G за нормальним дільником H із введеною операцією множення класів утворюють групу — в ній нейтральним елементом буде $H = 1 \cdot H$, оберненим до класа gH слугує $g^{-1}H$. Нейтральним елементом слугує клас нейтрального елемента. Побудована група називається факторгрупою групи G по нормальному дільнику $H \subseteq G$ і позначається G/H . Кількість елементів факторгрупи, тобто кількість різних суміжних класів групи за підгрупою, називається індексом підгрупи відносно групи і позначається $[G : H]$.

Означення 2.13 Множина S_n всіх підстановок на $(1, 2, \dots, n)$ разом з операцією множення утворює групу, що називається групою підстановок або симетричною групою і позначається S_n . Її підгрупа, що складається із парних підстановок називається знакозмінною групою і позначається A_n .

Однакове позначення і множини підстановок і групи підстановок не призводить до непорозумінь — що мається на увазі в конкретному випадку, видно із мовного оточення.

Означення коректне в тому розумінні, що S_n є групою, і що A_n є її підгрупою. Справді, асоціативність множення підстановок гарантується асоціативністю множення будь-яких відображень. Нафвність оберненої підстановки гарантується бієктивністю підстановки і тим, що добуток бієктивних відображень знову є бієктивним відображенням.

Прні підстановки це ті, що розкладається в добуток парної кількості транспозицій. Обернена підстановка розкладається в добуток тих же транспозицій, що і сама підстановка, але в зворотному порядку. Щоб знайти

розкладення добутку двох підстановок у добуток транспозицій, достаньмо розкласти обидві підстановки окремо, а потім записати одне розкладення за другим. Так, коли

$$\sigma = (1, 5)(5, 7)(1, 3), \quad \tau = (2, 7)(5, 3)(2, 7)(1, 4),$$

то

$$\sigma\tau = (1, 5)(5, 7)(1, 3)(2, 7)(5, 3)(2, 7)(1, 4).$$

Тому добуток парних підстановок знову є парною підстановкою, обернена до парної підстановки також є парною підстановкою, і одинична підстановка за означенням також є парною підстановкою. Як наслідок — A_n є підгрупою групи S_n .

Теорема 2.6 (про порядок підстановки) *Порядок підстановки дорівнює найменшому спільному кратному довжин незалежних циклів, на які розкладається ця підстановка.*

Для прикладу візьмемо підстановку σ , що розкладається у добуток двох незалежних циклів — (i_1, i_2) та (j_1, j_2, j_3) , тобто

$$\sigma = (i_1, i_2) \cdot (j_1, j_2, j_3).$$

Підносимо підстановку σ до степенів, враховуючи, що цикли переставні, порядок їх перемноження не має значення. Отже,

$$\sigma^2 = (j_1, j_3, j_2), \quad \sigma^3 = (i_1, i_2), \quad \sigma^4 = (j_1, j_2, j_3), \quad \sigma^5 = (i_1, i_2)(j_1, j_3, j_2) = \sigma^{-1}, \quad \sigma^6 = \text{id}.$$

Доведення. Якщо $\sigma = (i_1, i_2, \dots, i_k)$ — цикл довжини $k \geq 2$, то $\sigma^r(i_1) = i_{r+1}$ для $r = 1, 2, \dots, k-1$ і найменший степінь, в якому цикл дорівнює одиничній підстановці, дорівнює довжині цикла. Далі твердження теореми випливає з того, що цикли незалежні і щоб знайти степінь підстановки потрібно піднести до цього степеня цикли і результати перемножити.

■

Згідно з введеною теоремою підстановка, що розкладається в добуток незалежних циклів довжини 6 та 8, має порядок 24.

Теорема 2.7 (про індекс знакозмінної групи) *Якщо $n \geq 2$, то індекс знакозмінної групи A_n в симетричній групі S_n дорівнює 2.*

Доведення. Для доведення потрібно переконатися, що множина непарних підстановок $S_n \setminus A_n$ збігається із одним суміжним класом підгрупи A_n в S_n .

Дійсно, беремо транспозицію $\tau = (1, 2) \in S_n$ і будуємо суміжний клас τA_n . Цей суміжний клас збігається із множиною всіх непарних підстановок. Щоб переконатися в цьому, вибираємо довільну непарну підстановку $\sigma \in S_n \setminus A_n$, парну підстановку $(1, 2)\sigma = \sigma_1 \in A_n$ і бачимо, що $\sigma = (1, 2)\sigma_1 \in (1, 2)A_n$.

Теорема доведена. ■

2.2 Властивості спряження

Спряження $g \rightarrow tgt^{-1}$ елемента g групи G за допомогою $t \in G$ будемо позначати через g^t , тобто для $g, t \in G$

$$g^t = tgt^{-1}.$$

Очевидні властивості спряження в групі G з нейтральним елементом 1 об'єднаємо в наступну теорему

Теорема 2.8 (про властивості спряження в групі) *Спряження в групі G з нейтральним елементом 1 має наступні властивості. Для $g, g_1, g_2, t, t_1, t_2 \in G$*

1. $1^t = 1$;
2. $g^1 = g$;
3. $(g_1 g_2)^t = g_1^t g_2^t$;
4. $g^{t_1 t_2} = (g^{t_1})^{t_2}$;
5. $g_1 = g^{t_1}, g_2 = g_1^{t_2} \Rightarrow g_2 = g^{t_1 t_2}$;
6. $t_2 = t_1^{-1}, g_2 = g_1^{t_1} \Rightarrow g_1 = g_2^{t_2}$.

Теорема 2.9 (про спряженість циклів довжини 3) *Всі цикли довжини 3 спряжені в S_n , коли $n \geq 3$, і всі цикли довжини 3 спряжені в групі A_n , коли $n \geq 5$.*

Доведення. Властивості (5),(6) спряження дозволяють доводити лише те, що всі цикли довжини 3 спряжені до цикла $(1,2,3)$ в S_n , коли $n \geq 3$, а також всі цикли довжини 3 спряжені до цикла $(1,2,3)$ в A_n , коли $n \geq 5$.

В S_3 є всього два цикли довжини три — $\sigma_1 = (1, 2, 3)$ і $\sigma_2 = (1, 3, 2)$. Ці цикли спряжені:

$$\sigma_2 = (2, 3)\sigma_1(2, 3), \quad (2, 3) \in S_3.$$

В A_5 цикли σ_1, σ_2 спряжені, тому, що

$$\sigma_2 = (2, 3)(5, 2)(4, 5)(2, 4)\sigma_1(2, 4)(4, 5)(5, 2)(2, 3), \quad (2, 3)(5, 2)(4, 5)(2, 4) \in A_5.$$

В S_n $n \geq 3$ можна міняти один елемент циклу на інший, що не водить у цикл, за допомогою спряження однією транспозицією. Так

$$(1, 2, i) = (3, i)(1, 2, 3)(3, i);$$

$$(1, i, 3) = (2, i)(1, 2, 3)(2, i);$$

Щоб здійснити подібний перехід в A_n , тобто за допомогою парної кількості транспозицій, застосовують послідовність, подібну до наступної

$$(1, 2, 3) \rightarrow (1, 2, j) \rightarrow (1, 2, i)$$

Отже

$$(1, 2, i) = (i, j)(3, j)(1, 2, 3)(3, j)(i, j) \quad i, j \geq 4, \quad i \neq j.$$

Заміна двох елементів в циклі здійснюється добутком двох транспозицій, тобто

$$(1, i, j) = (2, i)(3, j)(1, 2, 3)(3, j)(2, i) \quad i, j \geq 4, \quad i \neq j.$$

Оскільки міняючи елементи в циклі і переставляючи їх за допомогою спряження в A_n , $n \geq 5$ ми можемо перейти до будь-якого триелементного цикла, то теорема доведена

■

2.3 Простота групи A_n при $n \geq 5$.

Теорема 2.10 (про те, що цикли довжини 3 породжують знакозмінну групу)

Кожен елемент знакозмінної групи A_n , $n \geq 3$ є добутком триелементних циклів.

Доведення. Твердження теореми випливає з того, що кожен елемент (підстановка) знакозмінної групи є добутком парної кількості транспозицій, а добуток двох різних транспозицій можна виразити через цикли довжини три: Коли a, b, c, d — чотири різні елементи, то

$$(a, b)(c, d) = (a, b)(b, c)(b, c)(c, d) = (a, b, c)(b, c, d),$$

а коли a, b, c — три різні елементи, то

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

■

Означення 2.14 Групу, яка не має нетривіальних інваріантних підгруп, називають *просою*.

Теорема 2.11 (про простоту групи A_n , $n \geq 5$) Група A_n , $n \geq 5$ проста, тобто не має нетривіальних інваріантних підгруп.

Доведення. Будемо доводити, що підгрупа $G \subseteq A_n$ ($n \geq 5$), $|G| > 1$ обов'язково збігається із A_n .

Випадок 1 — група G містить цикл довжини 3. Тоді за теоремою (2.9) ця група містить всі цикли, а за теоремою (2.10) вона збігається із всією групою.

Випадок 2 — група G містить підстановку, яка має в своєму розкладенні в добуток незалежних циклів цикл довжини більше ніж 3. Нехай

$$\sigma = \tau_1 \tau_2 \tau_3 \dots$$

розкладення підстановки $\sigma \in G$ в добуток незалежних циклів і

$$\tau_1 = (c_1, c_2, \dots, c_{s-3} c_{s-2}, c_{s-1}, c_s)$$

цикл довжини $s \geq 4$. Позначимо $t = (c_{s-2}, c_{s-1}, c_s)$

Тоді

$$t^{-1} \sigma t = (t^{-1} \tau_1 t) \tau_2 \tau_3 \dots$$

і

$$(t^{-1} \tau_1 t) = (c_1, c_2, \dots, c_{s-3} c_{s-1}, c_s, c_{s-2}).$$

Оскільки G піжгрупа групи A_n і до того ж інваріантна, то $\sigma^{-1}, t^{-1}\sigma^{-1}t \in G$
і

$$\sigma t^{-1}\sigma^{-1}t = (c_{s-3}, c_s, c_{s-2}) \in G.$$

і ми звели випадок 2 до випадку 1.

Випадок 3 — група G містить підстановку σ , яка має в своєму розкладенні в добуток незалежних циклів два цикли довжини 3:

$$\sigma = \tau_1\tau_2\tau_3 \dots$$

і

$$\tau_1 = (a_1, a_2, a_3), \quad \tau_2 = (b_1, b_2, b_3)$$

цикли довжини 3.

Для елемента $t = (a_3, b_1, b_2) \in A_n$

$$h = t^{-1}\sigma t = (a_1, a_2, b_1)(b_2, a_3, b_3)\tau_3 \dots \in G$$

і

$$\sigma h^{-1} = (a_2, b_2, a_3, b_1, b_3) \in G.$$

Отже випадок 3 звівся до випадку 2.

Випадок 4 — група G містить підстановку σ , яка має в своєму розкладенні в добуток незалежних циклів один чи декілька циклів довжини 3, а решта циклів є транспозиціями:

$$\sigma = \tau_1\tau_2\tau_3 \dots \quad \tau_1 = (a, b, c), \quad \tau_2 = (d, e, f).$$

Тоді $\sigma^2 = \tau_1^2\tau_2^2 \dots = (a, c, b)(d, f, e) \dots$, і в цьому розкладенні немає транспозицій. Отже випадок 4 звівся до випадку 3 або до випадку 1.

Випадок 5 — група G містить підстановку σ , яка розкладається в добуток незалежних транспозицій, причому їх кількість не менше 4:

$$\sigma = (x, y)(z, u) \dots (a, b)(c, d).$$

Позначимо $t = (y, a)(b, c)$. Тоді

$$h = t^{-1}\sigma t = (x, a)(z, u) \dots (y, c)(b, d) \in G$$

і

$$gh = (x, c, b)(y, a, d) \in G.$$

Випадок 5 звівся до випадку 3.

Випадок 6 — в групі G є елемент, який є добутком рівно двох незалежних транспозицій

$$\sigma = (a, b)(c, d) \in G.$$

Оскільки за припущенням $n \geq 5$, то ми можемо вибрати цикл $t = (a, b, e) \in A_n$, $e \notin \{a, b, c, d\}$. Для так вибраного цикла буде

$$h = t^{-1}\sigma t = (b, e)(c, d) \in G, \quad \sigma h = (a, e, b) \in G$$

І ми знову прийшли до уже розклянутого випадку 1. ■

Знкозмінна група A_4 не проста, вона має нормальний дільник H , що складається із 4 підстановок

$$H = \{\text{id}, \sigma_1 = (1, 2)(3, 4), \sigma_2 = (1, 3)(2, 4), \sigma_3 = (1, 4)(2, 3)\}.$$

2.4 Гомоморізми та ізоморфізми груп

Означення 2.15 Гомоморфізмами $f : G_1 \rightarrow G_2$ із групи G_1 в групу G_2 називають такі відображення, що узгоджені з операціями в групах, тобто, для $a, b \in G_1$

$$f(a \cdot b) = f(a) \cdot f(b), \quad f(1) = 1, \quad f(a^{-1}) = (f(a))^{-1}.$$

Сюр'єктивний гомоморфізм називають епіморфізмом, ін'єктивний гомоморфізм називають мономорфізмом, гомоморфізм із групи в себе називають ендоморфізмом, а ізоморфізм із групи в себе називають автоморфізмом. Автоморфізм із групи в себе, який кожному елементу ставить у відповідність спряжений елемент, називається внутрішнім автоморфізмом.

Теорема 2.12 (про універсальність групи підстановок) Кожна скінченна група ізоморфна підгрупі деякої групи підстановок.

Доведення. Множину елементів групи можна перенумерувати, і тоді множення всіх елементів групи на заданий елемент можна розглядати як підстановку. Всі такі підстановки і утворюють необхідну підгрупу. ■

Література

- [1] Л.А.Калужнін, В.І.Сущанський Преобразования и перестановки.: М.:Наука, 1976
- [2] М.Холл — Теория групп, — М:Издательство иностранной литературы, 1962
- [3] Завало С.Т — Курс алгебри. — Київ:Головне видавничого видавничого об'єднання “Вища школа“, 1985
- [4] В.І.Андрійчук , Б.В. Забавський “Алгебра і теорія чисел“ — Львів. — 2005.
- [5] В.І. Андрійчук , Б.В. Забавський “Лінійна алгебра“ — Львів. — 2008.
- [6] В.І. Андрійчук, Б.В. Забавський “Загальна алгебра“ — Львів. — 2009.
- [7] Гудименко Ф.С., Борисенко Д.М., Волкова В.О., Зражевська Г.М., Ющенко О.А. “Збірник задач з вищої математики“ — К., Видавництво Київського університету, 1967 р. 352 с.
- [8] И.В. Проскуряков “Сборник задач по линейной алгебре“. — М:Наука, 1967

Показчик

- асоціативність
 - додавання, 20
 - множення, 21
- автоморфізм, 34
 - внутрішній, 34
- цикл, 8
- цикли, 10
 - незалежні, 8, 10
- числа
 - Стірлінга 1-го роду, 15
- число
 - комбінаторне, 15
- декремент, 11
- детермінант, 12
- добуток
 - циклів, 10
 - незалежних циклів, 8
 - підстановок, 7
 - прямий, 2
 - транспозицій, 10
 - відображень, 7
- елемент
 - кратний, 23
 - нейтральний, 20
 - нейтральний відносно операції, 20
 - нерухомий, 9
 - обернений, 20
 - протилежний, 20
- ендоморфізм, 34
- епіморфізм, 34
- факторгрупа, 28
- функція, 2
 - часткова, 2
- гомоморфізм, 34
- група
 - адитивна, 22
 - циклічна, 23
 - комутативна, 24
 - мультиплікативна, 22
 - некомутативна, 24
 - проста, 32
 - симетрична, 28
 - знакозмінна, 28
- індекс, 28
- інверсія, 4, 8
- композиція
 - підстановок, 7
 - відображень, 7
- матриця
 - транспонована, 14
- матриця-підстановка, 15
- мінор, 13
- множення
 - підстановок, 7
 - відображень, 7
- множина
 - замкнена відносно операції, 22
- моморфізм, 34
- напівгрупа, 20
 - адитивна, 20
 - прямокутних матриць, 22
 - натуральних чисел, 22

мультиплікативна, 20
 підмножин множини, 22
 нуль, 20
 обмеження операції, 22
 образ елемента, 2
 одиниця, 20
 операція, 20
 асоціативна, 20
 одномісна, 27
 спряження, 27
 унарна, 27
 орбіта, 8
 одноеlementна, 9
 парність
 перестановки, 6
 підстановки, 6
 перестановка, 4
 непарна, 5
 парна, 5
 перетворення, 2
 підгрупа, 22, 23
 циклічна, 23
 інваріантна, 26
 нормальний дільник, 26
 тривіальна, 23
 піднапівгрупа, 22
 підстановка, 3
 непарна, 5
 одинична, 8
 парна, 5
 порядок
 елемента, 25
 групи, 25
 групи підстановок, 3
 зворотний, 4
 правило
 рівності, 26
 представник
 класа суміжності, 27
 прообраз елемента, 2
 співвідношення
 рекурентне, 16
 спряження, 27
 степінь
 елемента, 23
 зростаючий факторіальний, 18
 суміжний клас
 лівий, 25
 правий, 25
 транспозиції, 10
 транспозиція, 8
 триктник
 Паскаля, 16
 визначник, 12
 транспонованої матриці, 14
 відношення, 2
 бінарне, 2
 функціональне, 2
 відображення
 бієктивне, 2
 часткове, 2
 ін'єктивне, 2
 сюр'єктивне, 2
 відображення
 оборотне, 26
 відповідність, 2

задача
модельна, 15