ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
МІНІСТЕРСТВА ОСВІТИ І НАУКИ УКРАЇНИ

Є.В.Стєганцев

ТЕОРІЯ ГРУП

Методичні вказівки
для студентів напряму підготовки «Математика»
спеціалізації «Алгебра і теорія чисел»

Затверджено
вченою радою ЗНУ
Протокол № 2 від 24.09 2013 р.

Запоріжжя
2013

УДК 512.55
ББК 22.144

Стєганцев Є.В. Теорія груп: методичні вказівки для студентів напряму підготовки «Математика» спеціалізації «Алгебра і теорія чисел».– Запоріжжя: ЗНУ, 2013. – 45 с.

Методичні вказівки розроблено відповідно до галузевих стандартів а також до навчальної та робочої програм спецкурсу за вибором студентів «Теорія груп». Методичні вказівки містять достатньо задач з детальними обґрунтованими розв'язаннями, що дозволяє студентам навчитися застосовувати означення та теореми курсу, а також повторити матеріал курсу «Алгебра і теорія чисел». Для самостійної роботи студентів до методичних вказівок включено питання для самоконтролю та задачі для самостійного розв'язання.

Методичні вказівки призначені для студентів напряму підготовки «Математика», які навчаються за спеціалізацією «Алгебра і теорія чисел». Вони можуть зацікавити студентів інших напрямів підготовки, оскільки групи широко використовуються в топології, теорії функцій, квантовій механіці, кристалографії та інших галузях знань.

Рецензент А.К. Приварников

Відповідальний за випуск А.К. Приварников

ЗМІСТ

Вступ

Поняття групи виникло у 18 столітті із потреб розв'язання алгебраїчних рівнянь в радикалах а також дослідження можливості побудов геометричних фігур циркулем та лінійкою та ін. Сучасне абстрактне поняття групи склалось у 19 столітті і майже одразу знайшло численні застосування. Ф. Клейн у 1872 р. запропонував покласти в основу класифікації неевклідових геометрій поняття групи перетворень. Теорія чисел теж успішно користується теоретико-груповими конструкціями. Теорія груп знаходиться на одному із самих високих рівнів абстракції, це один із розділів сучасної математики, що є найбільш розвинутим і продовжує інтенсивно розвиватись.

При вивченні теорії груп поняття множини, елемента множини, відношення належності а також відображення є базовими. Важливим поняттям теорії груп є поняття ізоморфізму. Основною задачею теорії груп є вивчення груп з точністю до ізоморфізму.

В вищих навчальних закладах основні положення теорії груп входять до курсу алгебри та теорії чисел, дискретної математики. Більш детальне вивчення цього розділу математики, ознайомлення з основними теоретико-груповими конструкціями та питання класифікації груп а також демонстрація різноманітних застосувань понять та теорем теорії груп відбувається в рамках дисциплін спеціалізації.

Метою навчальної дисципліни «Теорія груп» є ознайомлення студентів з базовими поняттями та теоремами, основними конструкціями теорії груп та напрямами їх застосування в різних галузях знань.

Основні завдання:

- ознайомити з основними фактами аксіоматичної теорії структури групи;
- забезпечити засвоєння основних теоретичних відомостей і набуття практичних вмінь і навичок розв'язування основних типів задач;
- ознайомити з історією розвитку теорії груп та сучасним станом досліджень в ній.

У результаті вивчення навчальної дисципліни студент повинен

знати:

- означення основних понять;
- основні моделі структур груп;
- означення різних морфізмів груп;
- формулювання основних теорем курсу;

вміти:

- перевіряти виконання аксіом групи;
- розв'язувати основні типи задач;

- застосовувати означення та властивості гомоморфізмів та ізоморфізмів груп для розв’язання задач.

Дані методичні вказівки будуть сприяти формуванню вмінь та навичок застосування означень та теорем теорії груп до розв’язання основних типів задач, ознайомлять студентів із найважливішими конструкціями теорії груп.

ПРАКТИЧНЕ ЗАНЯТТЯ 1
Означення групи. Наслідки з аксіом групи. Порядок групи. Порядок елемента групи

План

1. Означення групи. Приклади груп.
2. Доведення наслідків з аксіом групи.
3. Означення порядку групи та порядку елемента групи.

Ключові поняття: алгебраїчна операція, група, групові аксіоми, порядок групи, порядок елемента групи, нейтральний елемент, симетричний елемент

В означенні групи використовується поняття алгебраїчної операції [7]. Саме перевірка алгебраїчності операції є першим завданням при перевірці існування на множині структури групи. Зверніть увагу на часто вживану щодо цієї властивості термінології: якщо задана на множині операція є алгебраїчною, то говорять, що ця множина є замкненою відносно операції. Означення групи містить три аксіоми, що є властивостями операції, яку будемо позначати символом $*$: 1) асоціативність операції, тобто для будь-яких трьох елементів a,b,c множини G $a*(b*c)=(a*b)*c$, 2) існування нейтрального елемента, тобто $\exists e\in G:\forall a\in G\ \ a*e=a$, 3) існування симетричного елемента, тобто $\forall a\in G\,\exists a'\in G\quad a*a'=e$.

☝ Зверніть увагу на те, що порядок перевірки аксіом можна змінювати, особливо цим фактом доцільно користуватись у разі не існування структури групи на заданій множині. Для позначення групи доцільно користуватись символом $(G,*)$, де G – множина, на якій задана бінарна операція.

Для скінчених груп користуються поняттям порядку групи, яке означає кількість елементів у групі, але і у випадку нескінчених груп говорять про групу нескінченого порядку. Зверніть увагу на те, що в будь-якій групі для кожного елемента, який не є нейтральним, можна знайти порядок [7]. В скінченій групі порядок кожного елемента є натуральним числом, в нескінченій групі можуть існувати елементи як скінченого так і нескінченого порядків.

☝ Зверніть увагу на найпростіші наслідки з аксіом групи:

- Нейтральний елемент єдиний,
- До кожного елемента групи існує єдиний обернений (протилежний) елемент.

Приклади розв'язування задач

Задача 1. Чи є групами відносно вказаних операцій наступні числові множини: Z,Q,R,C (відносно операції додавання) та $Q\setminus\{0\}$, $R\setminus\{0\}$, $C\setminus\{0\}$ (відносно операції множення)?

Розв'язання. Розглянемо множину Q і операцію додавання на ній. Оскільки сумою будь-яких двох раціональних чисел є раціональне число, то множина Q є замкнутою відносно операції додавання.

Аксіома асоціативності в множині Q виконується. Раціональне число 0 має властивість: для будь-якого раціонального числа a виконується рівність $a+0=a$, тобто існування нульового елемента доведено. Далі, для кожного раціонального числа a існує число $(-a)$ таке, що $a+(-a)=0$, тобто для кожного раціонального числа існує протилежне.

Можна зробити висновок, що $(Q,+)$ є адитивною групою. Очевидно, вона є нескінченою, абелевою (оскільки операція + є комутативною).

Аналогічно всі інші множини теж є групами .

Задача 2. Чи є групою множина всіх невироджених матриць n - го порядку з дійсними елементами відносно операції множення матриць?

Розв'язання. Для множини всіх невироджених матриць n - го порядку з дійсними елементами використовують позначення $GL(n,R)=\left\{A=\left(a_{ij}\right)_{i,j=1}^{n} : \det A\neq 0\right\}$. З курсу алгебри відомо, що ця множина є замкнутою відносно операції множення, тобто добутком будь-яких двох невироджених матриць n - го порядку є невироджена матриця того ж порядку. Цей факт випливає із властивості $\det(AB)=\det A\cdot\det B$. Асоціативність операції множення матриць також доводиться в курсі алгебри. Одинична матриця E порядку n є невиродженою і для будь-якої матриці $A\in GL(n,R)$ виконується рівність $AE=A$. І, нарешті, для будь-якої матриці $A\in GL(n,R)$ існує обернена матриця, тобто така матриця A^{-1}, що $AA^{-1}=E$. Легко довести, що $A^{-1}\in GL(n,R)$. Дійсно, $\det A^{-1}=\dfrac{1}{\det A}\neq 0$.

Робимо висновок, що $GL(n,R)$ – мультиплікативна неабелева група. Вона є нескінченою. Для цієї групи використовують термін загальна лінійна група.

Задача 3. Дано групу парного порядку. Довести, що в ній обов'язково знайдеться елемент порядку 2.

Доведення. Нехай порядок групи дорівнює $2n$. Виберемо n різних елементів цієї групи, які не є нейтральними, і припустимо, що порядок кожного з них не дорівнює 2. Тоді кожний з цих елементів і обернений до нього є різними елементами цієї групи. Якщо прийняти до уваги, що в групі є ще нейтральний елемент, то отримаємо, що загальна кількість елементів в групі дорівнює $2n+1$, що суперечить умові. Тобто, зроблене припущення не є вірним.

Задача 4. Довести, що з аксіом групи випливає теорема: Якщо $a*a'=e$, то $a'*a=e$, де e - нейтральний елемент групи.

Доведення. Позначимо через x елемент, обернений до елемента a', тоді $a'*x=e$. Далі $a=a*e=a*(a'*x)=(a*a')*x=e*x$. Отже, $a'*a=a'*(e*x)=(a'*e)*x=a'*x=e$.

Задача 5. Довести, що в будь-якій групі рівняння $a * x = b$ і $x * a = b$ завжди можуть бути розв'язані.

Доведення. Перевіримо безпосередньо, що елемент $x = a^{-1} * b$ задовольняє перше рівняння, а елемент $x = b * a^{-1}$ - друге:

$a * x = a * \left(a^{-1} * b\right) = \left(a * a^{-1}\right) * b = e * b = b$,

$x * a = \left(b * a^{-1}\right) * a = b * \left(a^{-1} * a\right) = b * e = b$.

Такий вигляд розв'язку першого рівняння можна отримати, помножаючи його зліва на елемент a^{-1} і застосовуючи аксіоми групи і раніше доведені теореми. Аналогічно доводиться і для другого рівняння.

Задача 6. Довести, що коли $(a * b)^k = e$, то $(b * a)^k = e$, де $(a*b)^k = \underbrace{(a*b)*(a*b)*...*(a*b)}_{k}$.

Доведення. Згідно з домовленістю задану рівність можна записати у вигляді $\underbrace{(a*b)*(a*b)*...*(a*b)}_{k} = e$. Помножимо обидві частини цієї рівності зліва на елемент b, а справа – на b^{-1} - обернений до b. Застосуємо зліва властивість асоціативності, а справа – послідовно аксіоми 1, 2 і 3 групи, отримаємо $b*\underbrace{(a*b)*(a*b)*...*(a*b)}_{k}*b^{-1} = b*e*b^{-1}$, звідки і випливає рівність, яку треба було довести.

Задача 7. Нехай група G має непарний порядок. Довести, що для всякого $x \in G$ існує $y \in G$ такий, що $x = y^2$.

Доведення. Відомо, що в скінченій групі порядку n для будь-якого елемента $g \in G$ має місце рівність $g^n = e$, де e - нейтральний елемент. За умовою задачі n - непарне число, тобто $n = 2m+1, m \in N$. Отже, для $x \in G$ маємо $x^{2m+1} = e$. Перепишемо цю рівність у вигляді $\left(x^m\right)^2 x = e$. Помножимо обидві частини останньої рівності на $\left(x^{-m}\right)^2$, отримаємо $x = \left(x^{-m}\right)^2$, тобто елемент $y = x^{-m}$ шуканий.

Питання для самоконтролю

1. Означення алгебраїчної операції.
2. Означення групи, адитивної групи, мультиплікативної групи.
3. Означення абелевої групи.
4. Нейтральні та симетричні елементи адитивної та мультиплікативної груп.
5. Основні властивості груп.
6. Поняття порядку групи, порядку елемента групи.

7. Загальна лінійна група.

8. Множина класів лишків за модулем, додавання та множення класів лишків.

Задачі для самостійного розв'язання

1. Довести, що наступні множини є групами:

А) векторний простір V відносно операції додавання векторів,

Б) множина невироджених квадратних матриць однакового порядку з раціональними елементами відносно операції множення матриць,

В) $M = \{z \in C : |z| = 1\}$ відносно операції множення комплексних чисел,

Г) $M = \{\varepsilon_0, \varepsilon_1, ..., \varepsilon_{n-1}\}$, де $\varepsilon_k = \cos\frac{2\pi k}{n} + \sin\frac{2\pi k}{n}$, $k = \overline{0, n-1}$ - корені n-го степеня із одиниці, відносно операції множення ($\varepsilon_k \varepsilon_l = \varepsilon_p$, $p \equiv (k+l) (\mathrm{mod}\, n)$).

Д) $Z_2 = \{\overline{0}, \overline{1}\}$ - множина класів лишків за модулем 2 відносно операції додавання.

2. Довести, що в будь-якій групі $(a')' = a$, де a' - елемент групи, обернений до елементу a.

3. Довести, що в будь-якій групі $(a * b)' = b' * a'$.

4. Знайти порядок елемента ε_2 в групі коренів четвертого степеня із одиниці.

5. Знайти симетричний (протилежний) елемент до елемента $a = \frac{1}{2} - \frac{\sqrt{3}}{2} i$ в групах $(C, +)$ і $(C \setminus \{0\}, \cdot)$.

6. Довести наступні теореми:

А) Якщо $a * e = a$, то $e * a = a$.

Б) Нейтральний елемент єдиний.

В) Обернений елемент для кожного елемента в групі єдиний.

7. Перевірте, що в будь-якій мультиплікативній групі для порядків наступних елементів виконуються рівності:
$|x| = |yxy^{-1}|$, $|ab| = |ba|$, $|abc| = |bca| = |cab|$.

8. Нехай N - множина натуральних чисел. Чи є операція $x * y = НСД(\mathrm{x}, \mathrm{y})$ асоціативною на множині N ?

ПРАКТИЧНЕ ЗАНЯТТЯ 2
Підгрупи. Теорема Лагранжа. Центр групи

План

1. Означення підгрупи. Приклади підгруп.
2. Поняття невласної та власної підгруп.
3. Теорема Лагранжа та її застосування.
4. Означення центру групи.

Ключові поняття: підгрупа, власна і невласна підгрупи, теорема Лагранжа, центр групи, абелева група, критерій підгрупи, комутатор елементів групи, комутант групи

Означення підгрупи дуже схоже на означення підпростору векторного простору, яке вивчалось у лінійній алгебрі. Тобто для доведення, що дана підмножина групи є її підгрупою, слід довести, що вона є групою відносно тієї ж алгебраїчної операції. Якщо підмножина H групи G є її підгрупою, то пишуть $H < G$. Іноді зручніше користуватись критерієм підгрупи.

Зверніть увагу на те, що кожна група має принаймні дві підгрупи: $\{e\} < G$ і $G < G$. Їх називають невласними або тривіальними, всі інші підгрупи називають власними. Одним із завдань цієї теми є доведення факту, що центр [3] будь-якої групи є її підгрупою. Надалі, буде потрібна теорема Лагранжа: порядок скінченої групи ділиться на порядок будь-якої її підгрупи. Зверніть увагу на те, що вона не гарантує існування в групі порядку n підгрупи порядку k, де k є дільником числа n.

Слід поміркувати і про зв'язок між порядком групи і порядком будь-якого елементу групи. Висновок про цей зв'язок теж є наслідком теореми Лагранжа і полягає в наступному: порядок будь-якого елементу групи є дільником порядку групи.

Зверніть увагу на поняття центру групи. Так називають множину всіх тих елементів групи, які є переставними з усіма елементами групи. Ця властивість елементів центру групи впливає на її будову. Так групи, в яких будь-які два елементи є переставними, називаються комутативними або абелевими. Мірою відхилення групи від абелевої є її комутант [3].

Приклади розв'язування задач

Задача 1. Довести, що множина M невироджених матриць виду $A=\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, де $a,b\in R,\ a^2+b^2=1,$ є підгрупою загальної лінійної групи $GL(2,R)$.

Розв'язання. Скористаємось критерієм підгрупи. Розглянемо два елементи $A=\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ і $C=\begin{pmatrix} c & d \\ -d & c \end{pmatrix}$ з множини M. Знайдемо елемент C^{-1} - обернений до елемента C. Отримаємо $C^{-1}=\dfrac{1}{c^2+d^2}\begin{pmatrix} c & -d \\ d & c \end{pmatrix}=\begin{pmatrix} c & -d \\ d & c \end{pmatrix}$, оскільки $c^2+d^2=1$. На головній діагоналі цієї матриці однакові дійсні числа, а на побічній діагоналі – дійсні числа, що відрізняються знаком. Крім того, $\det\left(C^{-1}\right)=1$, тобто $C^{-1}\in M$. Знайдемо далі добуток AC^{-1}, отримаємо $AC^{-1}=\begin{pmatrix} ac+bd & -ad+bc \\ -bc+ad & bd+ac \end{pmatrix}$. Вид матриці-добутку такий же, як і у матриць з множини M. Її визначник дорівнює 1, в чому можна переконатись або безпосереднім підрахунком, або за допомогою властивості $\det(AB)=\det A\cdot\det B$.

Розглядувана множина матриць є підгрупою групи $GL(2,R)$ (це є критерій підгрупи), що і треба було довести.

Задача 2. Довести, що $S=\{\overline{0},\overline{2},\overline{4}\}$ з операцією додавання є підгрупою групи $(Z_6,+)$.

Розв'язання. Легко безпосередньо переконатись в замкненості цієї множини відносно операції додавання, що і доводить властивість множини S бути підгрупою групи $(Z_6,+)$ у відповідності до критерію підгрупи для скінчених груп.

Задача 3. Довести, що центр C групи є підгрупою в G.

Розв'язання. Якщо $x\in C(G)$, то $\forall g\in G\ \ xg=gx$. Аналогічно, якщо $y\in C(G)$, то $\forall g\in G\ \ yg=gy$. Доведемо, що елемент $y'\in G$, обернений до y, належить $C(G)$ Дійсно, якщо обидві частини вірної рівності $yg=gy$ помножити зліва і справа на y', то отримаємо вірну для будь-якого $g\in G$ рівність $gy'=y'g$, з якої випливає $y'\in C(G)$. Далі, $(xy')g=x(y'g)=x(gy')=(xg)y'=(gx)y'=g(xy')$. Отже, $xy'\in C(G)$. За критерієм, $C(G)<G$, що і треба було довести.

Задача 4. При яких n множина $\left\{\begin{pmatrix} x & y \\ ny & x \end{pmatrix} : x, y \in R\right\}$, де n - фіксоване ціле число, є підгрупою групи $GL(2, R)$ відносно множення матриць?

Розв'язання. Знайдемо умову, при якій елемент, обернений до елемента з даної множини, належить цій множині.

Нехай $A = \begin{pmatrix} x & y \\ ny & x \end{pmatrix}$. Визначник цієї матриці дорівнює $x^2 - ny^2$. При $n \geq 0$ обов'язково знайдеться пара дійсних чисел x, y, які одночасно не рівні нулю і задовольняють рівняння $x^2 - ny^2 = 0$, тобто матриця A не матиме оберненої. Якщо ж $n < 0$, то рівняння $x^2 - ny^2 = 0$ не має ненульових розв'язків, а значить визначник матриці A відмінний від нуля, тобто матриця має обернену: $A^{-1} = \frac{1}{\det A}\begin{pmatrix} x & -y \\ -ny & x \end{pmatrix}$, яка належить даній множині. Далі, для $B = \begin{pmatrix} a & b \\ nb & a \end{pmatrix}$ і $A = \begin{pmatrix} x & y \\ ny & x \end{pmatrix}$ з даної множини елемент $BA^{-1} = \begin{pmatrix} a & b \\ nb & a \end{pmatrix}\frac{1}{\det A}\begin{pmatrix} x & -y \\ -ny & x \end{pmatrix} = \frac{1}{\det A}\begin{pmatrix} ax - nby & -ay + bx \\ n(bx - ay) & -nby + ax \end{pmatrix}$ при $n < 0$ також їй належить.

Отже, згідно з критерієм підгрупи, при умові $n < 0$ множина вказаних матриць є підгрупою групи $GL(2, R)$.

Задача 5. Знайти центр загальної лінійної групи $GL(n, R)$.

Вказівка. Розглянути матриці E_{ij} порядку n, в яких елементи E_{ii} дорівнюють 1, а елементи E_{ij} дорівнюють 0 при $i \neq j$ (матричні одиниці). Будь-яка матриця загальної лінійної групи є, очевидно, лінійною комбінацією матриць E_{ij}. Множення матричних одиниць дає наступний результат: $E_{ij}E_{kl} = \begin{cases} E_{il}, \textit{ якщо } \text{j} = \text{k}, \\ 0, \text{ в противному випадку.} \end{cases}$

Питання для самоконтролю

1. Формулювання критерію підгрупи.
2. Поняття власної підгрупи.
3. Означення центру групи.
4. Поняття комутатора двох елементів групи.
5. Комутант групи. Приклади комутантів.

Задачі для самостійного розв'язання

1. Множина діагональних матриць з ненульовими діагональними елементами є підгрупою загальної лінійної групи. Довести.

2. Знайти комутатор невироджених матриць $A=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ і $B=\begin{pmatrix}a & 0\\ 0 & 1\end{pmatrix}$.

3. Довести, що перетин будь-якої множини підгруп групи G знову є підгрупою цієї групи.

4. Множина $T_n(R)$ верхньотрикутних матриць з ненульовими діагональними елементами є підгрупою загальної лінійної групи, а множина діагональних матриць з ненульовими діагональними елементами є підгрупою групи $T_n(R)$. Довести.

5. Довести, що комутант групи є її підгрупою.

6. Довести, що для елементів a і b довільної групи $[a,b]^{-1}=[b,a]$.

7. Довести, що в будь-якій нескінченій групі нескінченно багато підгруп.

8. Знайти деякі підгрупи в адитивній групі цілих чисел.

9. Знайти всі підгрупи в мультиплікативній групі U_n коренів n-го степеня з одиниці при різних значеннях n (розглянути випадки простого і складеного n).

ПРАКТИЧНЕ ЗАНЯТТЯ 3
Група підстановок. Група симетрій многокутника. Таблиця Келі та її властивості

План

1. Означення підстановки. Парні та непарні підстановки.
2. Симетрична та знакозмінна групи.
3. Поняття симетрії фігури. Означення групи діедра.
4. Таблиця Келі. Доведення асоціативності алгебраїчної операції за допомогою таблиці Келі.

Ключові поняття: підстановка, симетрична група, знакозмінна група, таблиця Келі, група діедра, група симетрій фігури

 Поняття підстановки n - го степеня відоме з курсу алгебри та теорії чисел [2, додаткова 4]. Повторення цього матеріалу полегшить доведення факту, що множина всіх підстановок n - го степеня відносно операції композиції утворює групу (цю групу називають симетричною групою n - го степеня), а її підмножина парних підстановок відносно тієї ж операції є підгрупою симетричної групи і називається знакозмінною групою n - го степеня.

 Для вивчення групи симетрій даної фігури та її частинного випадку – групи діедра – треба повторити основні відображення площини та простору в курсі аналітичної геометрії: повороти площини та простору (позначають R_O^α), осьові та центральні симетрії (позначають відповідно S_l та Z_O), та ін. [9].

 Зверніть увагу на те, що таблиця є одним із способів завдання групи, для цього необхідно, щоб вона мала 5 властивостей. В цьому разі вона називається таблицею Келі групи.

Приклади розв'язування задач

Задача 1. Чому дорівнює порядок групи рухів, які суміщають із самим собою правильний n - кутник?

Розв'язання. В групі симетрій правильного n - кутника є рівно $2n$ елементів: n поворотів за годинниковою стрілкою на кути $\frac{2\pi k}{n}\,(k=1,2,...,n-1)$ навколо центру і n осьових симетрій відносно прямих, що проходять через центр і одну з вершин многокутника або через середини протилежних сторін. Всі повороти в групі симетрій правильного n - кутника утворюють підгрупу, яка називається підгрупою поворотів даного n - кутника.

Задача 2. Знайти порядки всіх елементів в групі симетрій квадрата.

Розв'язання. У відповідності до задачі 1 в цій групі 8 елементів, а саме $D_4 = \left\{e, R_O^{90^0}, R_O^{180^0}, R_O^{270^0}, S_{AC}, S_{BD}, S_{MN}, S_{KL}\right\}$, де AC, BD - діагоналі квадрата, M, N та K, L середини пар протилежних сторін квадрата. Очевидно всі симетрії мають порядок 2, а для поворотів легко отримати, що $\left|R_O^{90^0}\right| = 4, \left|R_O^{180^0}\right| = 2, \left|R_O^{270^0}\right| = 4$.

Задача 3. Довести, що кожний рядок (стовпець) таблиці Келі скінченої групи є перестановкою першого рядка (стовпця).

Розв'язання. Нехай $G = \{a_1, a_2, ..., a_n\}$ - мультиплікативна група порядку n. Оберемо будь-який елемент цієї групи і позначимо його символом b. Розглянемо добутки $ba_1, ba_2, ..., ba_n$. Припустимо, що при $i \neq j$ виконується рівність $ba_i = ba_j$. Але тоді $b^{-1}ba_i = b^{-1}ba_j$ або $a_i = a_j$, що суперечить умові. Отже, всі добутки різні. Вони є тими ж елементами групи, але можливо записаними в іншому порядку, тобто утворюють перестановку елементів першого рядка. Так само і для стовпців.

Задача 4. Знайти порядок групи симетрій ромба.

Розв'язання. Ромб не являється правильним n - кутником. Група R симетрій ромба складається з чотирьох елементів – нейтрального елемента, центральної симетрії та двох осьових симетрій відносно діагоналей. Позначимо їх наступним чином: $R = \{e, Z_O, m, n\}$. Тобто група складається з чотирьох елементів і тому має порядок чотири.

Задача 5. Описати всі підгрупи групи S_3.

Розв'язання. Порядок групи S_3 дорівнює 6. З теореми Лагранжа випливає, що власні підгрупи (див. практичне заняття 2) цієї групи можуть складатись лише із 2 або із 3 підстановок.

Нехай H - двоелементна підгрупа групи S_3. Тоді $H = \{e, a\}$. Елемент, обернений до a, не може співпадати з e, тому $a^{-1} = a$, звідки $a^{-1}a = a^2 = e$. Таким чином, елемент a має порядок 2, тобто є транспозицією. Це єдина можливість для нетривіального елемента в групі S_3. В цій групі є лише три транспозиції, кожна з яких визначить двоелементну підгрупу. Отже, $H' = \{e, (12)\}$, $H'' = \{e, (13)\}$, $H''' = \{e, (23)\}$ всі можливі підгрупи порядку 2.

Нехай тепер F - підгрупа порядку 3 групи S_3. Введемо позначення $F = \{e, a, b\}$. Очевидно, що порядок кожного ненульового елемента не перевищує 3. Припустимо, що хоча б один з елементів має порядок 2. Наприклад, $a^2 = e$. Тоді $a^{-1} = a$. Якщо $b^{-1} \neq b$, то $b^{-1} = a$ і $b^{-1} = a^{-1}$, звідки випливає $b = a$, що суперечить умові. Отже, $b^{-1} = b$. Але тоді в підгрупі F більше 3 елементів. Дійсно, повинно бути $ab \in F$, але $ab \neq a$, $ab \neq b$ і $ab \neq e$, бо якщо $ab = e$, то $a = b^{-1} = b$.

Отже, наше припущення невірне і кожен з елементів a,b має порядок 3. Відомо, що цикл довжини 3 має порядок 3. Розглянемо цикл $\alpha=(123)$. Тоді $\alpha^2=(132)$, $\alpha^3=e$. Отримали $F=\{e,(123),(132)\}$. Оскільки інших циклів довжини 3 в цій групі не існує, то й інших триелементних підгруп, крім F не існує.

Повний список підгруп групи S_3 складається з шести підгруп: $E=\{e\}$, $H'=\{e,(12)\}$, $H''=\{e,(13)\}$, $H'''=\{e,(23)\}$, $F=\{e,(123),(132)\}$, S_3. Перша і остання є невласними, всі інші – власні.

Задача 6. Знайти всі підгрупи в групах симетрій правильного трикутника і квадрата.

Розв'язання. Для D_4 існує 8 власних підгруп: 3 порядку 4 (підгрупа поворотів; 2 підгрупи містять нейтральний, центральну симетрію і осьову симетрію відносно однієї із пар перпендикулярних осей), 5 підгруп порядку 2 (одна містить центральну симетрію, кожна з інших – одну з осьових симетрій).

Питання для самоконтролю

1. Означення циклу, довжини циклу.
2. Поняття транспозиції.
3. Означення парної та непарної підстановок.
4. Поняття знакозмінної групи степеня n.
5. Властивості таблиці Келі.
6. Поняття інволюції.

Задачі для самостійного розв'язання

1. Довести, що множина $F=(f_1,f_2,f_3,f_4)$ таких функцій від однієї змінної $f_1(x)=x$, $f_2(x)=-x$, $f_3(x)=\frac{1}{x}$, $f_1(x)=-\frac{1}{x}$ відносно операції композиції: $f_i * f_k = f_i(f_k(x))$ є групою. Скласти таблицю Келі.

2. Чи утворюють групу відносно операції композиції (див. задачу 6) наступні множини:

$\{e,(13),(24),(12)(34),(13)(24),(14)(23)\}$,

$\{e,(13),(24),(12)(34),(13)(24),(14)(23),(1234),(1432)\}$?

3. Довести, що множина поворотів площини, які переводять правильний n- кутник в себе, утворює підгрупу групи його симетрій (її називають групою поворотів правильного многокутника).

4. Нехай $\sigma \in S_n$, де S_n - група підстановок n - го порядку і $\sigma = \sigma_1\sigma_2...\sigma_m$ де $\sigma_1, \sigma_2, ...\sigma_m$ - незалежні цикли. Довести, що $|\sigma| = НСК(|\sigma_1|, |\sigma_2|, ..., |\sigma_m|)$.

5. Знайти порядки всіх елементів в групах симетрій правильного трикутника.

6. Довести, що добуток парної (непарної) підстановки на будь-який цикл довжини 2 є непарною (парною) підстановкою.

7. Знайти комутатор транспозицій: а) $(ij),(kl)$, б) $(ij),(il)$, в) $(ij),(ij)$.

8. Знайти центр групи D_n (див задачу 2).

ПРАКТИЧНЕ ЗАНЯТТЯ 4
Ізоморфізм груп

План

1. Означення ізоморфізму груп.
2. Приклади ізоморфних груп.
3. Властивості ізоморфізмів.
4. Теорема Келі.

Ключові поняття: відображення груп, образ елемента, прообраз елемента, ізоморфізм груп, ізоморфні групи, теорема Келі

При вивченні ізоморфізмів груп слід звернути увагу на основну вимогу ізоморфізму – існування взаємно однозначного відображення між множинами елементів груп. Якщо для двох заданих груп існує хоча б один ізоморфізм, то групи називають ізоморфними і позначають $G \cong H$. При цьому значно легше перевіряти, чи буде задане відображення ізоморфізмом груп, ніж знайти таке відображення. В цій темі пропонується також цікавий клас задач на доведення неізоморфності двох груп, особливо у випадку, коли взаємно однозначна відповідність між множинами елементів цих груп існує.

Головною метою вивчення ізоморфізмів є той факт, що ізоморфні групи мають одні і ті ж самі властивості. Таким чином, ізоморфні групи ми не будемо розрізняти, хоча вони можуть бути різними. Зрозуміло, що коли б вдалося скласти повний перелік попарно неізоморфних груп, то всі дослідження в теорії груп було б завершено.

Слід звернути увагу на дуже важливу теорему, яка носить ім'я Келі:

будь-яка скінчена група порядку n ізоморфна деякій підгрупі симетричної групи n - го порядку.

З цієї теореми випливає, що всі скінчені групи вичерпуються підгрупами симетричних груп і цей факт пояснює, чому в теорії груп так багато уваги приділяється вивченню груп підстановок.

Обов'язковими для вивчення є наступні властивості ізоморфізмів:

1) Ізоморфізм зберігає нейтральний елемент, тобто $f(e) = e'$,
2) Образом оберненого елементу є обернений до образу, тобто $f(a^{-1}) = (f(a))^{-1}$,
3) Відображення, обернене до ізоморфізму, знову є ізоморфізмом.

В теорії та в практичній частині курсу приділяється увага особливому виду ізоморфізмів – автоморфізмам. Цей термін використовують для ізоморфізмів групи на себе.

Приклади розв'язування задач

Задача 1. Довести, що групи $(R,+)$ і $(R_+,*)$ ізоморфні.

Розв'язання. Для доведення ізоморфності груп достатньо вказати ізоморфне відображення однієї з них на іншу. Розглянемо відображення множини R_+ додатних дійсних чисел x у множину R всіх дійсних чисел y, яке задається формулою $y = \ln x$. Воно є бієктивним і, оскільки $(\forall a, b \in R_+)\ \ln(ab) = \ln a + \ln b$, то це відображення є ізоморфізмом.

Задача 2. Нехай $(G,*)$ і $(H,\circ)$ - ізоморфні групи одного порядку і $f : G \to H$. Довести, що образом нейтрального елемента групи G є нейтральний елемент групи H, тобто $f(e) = e'$.

Розв'язання. Запишемо властивість ізоморфізму для елементів a і e, отримаємо $f(a * e) = f(a) \circ f(e)$. З іншого боку, $f(a) = f(a * e)$. Тому $f(a) = f(a) \circ f(e)$. Остання рівність означає, що $f(e) = e'$, що і треба було довести.

Задача 3. В мультиплікативній групі $(G,\cdot)$ зафіксовано елемент a і задано нову операцію за правилом $x \circ y = x \cdot a \cdot y$**.** Довести, що відносно цієї операції G є групою, ізоморфною заданій.

Розв'язання. Замкнутість G відносно нової операції очевидна. Перевіримо аксіоми.

1) асоціативність.

$$(x \circ y) \circ z = (x \cdot a \cdot y) \circ z = (x \cdot a \cdot y) \cdot a \cdot z = (x \cdot a) \cdot y \cdot a \cdot z = x \cdot a \cdot (y \cdot a \cdot z) =$$
$$= x \cdot a \cdot (y \circ z) = x \circ (y \circ z)$$

Тут використана асоціативність операції в групі G.

2) існування нейтрального елемента.

Якщо E - нейтральний відносно операції $\circ$, то $x \circ E = x$ для будь-якого x або $x \cdot a \cdot E = x$. Помножимо обидві частини зліва на x^{-1} - обернений до x. Він існує, оскільки G - група. отримаємо $a \cdot E = e$, де e - нейтральний елемент в групі G. З останньої рівності отримаємо, що $E = a^{-1}$. Такий елемент в групі G очевидно існує.

3) існування симетричного елемента для будь-якого x.

Якщо x' - симетричний до x, то $x \circ x' = E = a^{-1}$ або $x \cdot a \cdot x' = a^{-1}$ або $(x \cdot a) \cdot x' = a^{-1}$. Помножимо обидві частини зліва на $(x \cdot a)^{-1} = a^{-1} \cdot x^{-1}$, тоді $e \cdot x' = x' = a^{-1} \cdot x^{-1} \cdot a^{-1}$. Це і є симетричний до x.

Всі аксіоми виконуються, значить G є групою і відносно нової операції.

Існування бієкції $f : G \to G$ очевидне. Розглянемо, наприклад, бієкцію f таку, що $f(x) = a \cdot x$. Перевіримо виконання вимоги $f(x \circ y) = f(x) \cdot f(y)$.

$$f(x \circ y) = a \cdot (x \circ y) = a \cdot (x \cdot a \cdot y),$$
$$f(x) \cdot f(y) = (a \cdot x) \cdot (a \cdot y) = a \cdot (x \cdot a \cdot y) = f(x \circ y),$$

що і треба було довести.

Задача 4. Побудувати ізоморфізм групи $G=([0,1),\oplus)$, де $\alpha\oplus\beta$ - дробова частина числа $\alpha+\beta$ і групи G' комплексних чисел з модулем $r=1$ відносно множення.

Вказівка. Розглянути відображення $f:G\to G'$ за правилом: $\forall\alpha\in G\quad f(\alpha)=\cos 2\pi\alpha+i\sin 2\pi\alpha$.

Задача 5. Нехай G - нескінчена циклічна група. Довести, що $Aut(G)\cong Z_2$.

Вказівка. Довести спочатку, що $Aut(Z)\cong Z_2$. Для цього врахувати, що автоморфізм є інволюцією [7]. Розглянути відображення $\varphi:Z\to Z$ за правилом $\varphi:a\to\lambda a$ і довести, що $\lambda=\pm 1$. Це означає що група $Aut(Z)$ складається з двох елементів.

Питання для самоконтролю

1. Означення ізоморфних груп і ізоморфізму двох груп.
2. Властивості ізоморфізму.
3. Приклади ізоморфних груп.
4. Означення автоморфізму групи.
5. Побудова автоморфізмів в адитивній групі цілих чисел.
6. Формулювання теореми Келі.
7. Група автоморфізмів даної групи.

Задачі для самостійного розв'язання

1. Довести, що відображення $g:(R,+)\to(R_+,\cdot)$ таке, що $g(a)=2^a$ є ізоморфізмом.

2. Мультиплікативна група коренів n - го степеня із одиниці ізоморфна адитивній групі Z_n. Довести.

3. Довести, що група симетрій правильного трикутника ізоморфна групі S_3 (див. попереднє практичне заняття).

4. Довести, що група поворотів правильного n - кутника ізоморфна групі Z_n класів лишків по модулю n .

5. Які з наступних груп ізоморфні: 1) група поворотів квадрата, 2) група симетрій ромба, 3) група симетрій прямокутника, 4) група лишків з операцією додавання по модулю 4?

6. Довести, що множина всіх елементів a групи S_n, які мають властивість $a(k)=k$, утворює підгрупу, ізоморфну групі S_{n-1}.

7. Довести, що група поворотів правильного n - кутника ізоморфна мультиплікативній групі коренів n - го степеня із одиниці.

8. Довести ізоморфність груп $(R,+)$ і $(UT_2(R),\cdot)$, де $UT_2(R)=\left\{\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}: a\in R\right\}$ - група з операцією множення матриць.

ПРАКТИЧНЕ ЗАНЯТТЯ 5
Твірні елементи групи. Циклічна група. Системи твірних елементів симетричної та знакозмінної груп

План

1. Означення системи твірних.
2. Незалежна система твірних. Циклічні групи (скінченні та нескінченні).
3. Властивості циклічних груп.
4. Групи з більш ніж однією твірною.
5. Системи твірних елементів симетричної та знакозмінної груп.

Ключові поняття: система твірних, циклічна група, скінчено породжена група

Зауважимо, що таблиця Келі, з якою ми вже познайомились, є зручною формою завдання групи, але для груп з великою кількістю елементів, очевидно, таблиця Келі непридатна. Для таких груп істотне значення набуває поняття твірної множини або системи твірних групи.

Існують різні означення системи твірних групи. Частіше за все ми будемо користуватись наступним означенням:

Для даної групи G її підмножина T така, що будь-який елемент групи можна отримати як результат алгебраїчної операції над скінченою кількістю елементів із множини T, називається множиною (системою) твірних групи G. Саму групу називають породженою множиною T і позначають $G =< T >$ [3,7].

Зверніть увагу на те, що згідно з цим означенням в представленні елемента групи елементи із множини T можуть повторюватись.

Наступним важливим поняттям є поняття незалежної або мінімальної системи твірних. Особлива увага в цій темі приділяється вивченню циклічних груп, тобто таких груп, для яких мінімальна система твірних складається лише із одного елемента. Значення поняття циклічної групи в теорії груп розкриває наступна

Теорема. Будь-яка нескінчена циклічна група, тобто група, для якої існує система твірних, що складається з одного елементу, ізоморфна групі Z, а будь-яка скінчена циклічна група ізоморфна групі Z_n.

Важливі приклади систем твірних з'являються при вивченні симетричної та знакозмінної груп. При розв'язанні задач будемо користуватись наступними системами твірних:

для симетричної групи n – го степеня

1) $\{(12),(23),...,(n-1,n)\}$,
2) $\{(12),(13),...,(1\,n)\}$,
3) $\{(12),(12...n)\}$,

для знакозмінної групи n – го степеня

1) множина триелементних циклів (abc),

2) $\{(123),(124),...,(12n)\}$ [4 додаткова].

Приклади розв'язування задач

Задача 1. Довести, що будь-яка група, порядок якої менше 6, є абелевою.

Розв'язання. Очевидно, група другого порядку є абелевою, групи простих порядків 3 і 5 є циклічними, а значить теж є абелевими. Залишилось довести, що група порядку 4 абелева. Очевидно, достатньо довести для випадку нециклічної групи четвертого порядку. Оскільки порядок групи є парним числом, то в ній обов'язково є елемент порядку 2. Позначимо елементи цієї групи символами e,a,b,c і припустимо, що $a^2 \neq e, b^2 \neq e$. Тоді $c^2 = e$ і з іншого боку $c = ab$. Але тоді $ab = ba$, що і треба було довести.

Задача 2. Знайти всі підгрупи циклічної групи порядку p^n, де p - просте число.

Розв'язання. За теоремою Лагранжа порядок будь-якої підгрупи є дільником порядку групи. Крім того, підгрупа циклічної групи сама є циклічною.

Нехай дана група G породжується елементом a, тобто $G = \langle a \rangle = \left\{e, a, a^2, ..., a^p, ..., a^{p^2}, ..., a^{p^n-1}\right\}$. Її нетривіальні підгрупи породжуються елементами $a^p, a^{p^2}, ..., a^{p^{n-1}}$. До них слід додати тривіальні підгрупи $G_0 = \{e\}$ і G. Наприклад, для циклічної групи порядку 2^3, тобто для $G = \left\{e, a, a^2, ..., a^7\right\}$ підгрупами є $G_1 = \left\langle a^2 \right\rangle = \left\{e, a^2, a^4\right\}$, $G_2 = \left\langle a^{2^2} \right\rangle = \left\{e, a^4\right\}$, $G_0 = \{e\}$, G.

Задача 3. В циклічній групі $\langle a \rangle$ порядку n знайти всі елементи g, які задовольняють умову $g^k = e$, а також всі елементи порядку k, якщо $n = 360, k = 30$.

Розв'язання. Нехай g - шуканий елемент, тоді $g^{30} = \left(a^l\right)^{30} = a^{30l} = e$. З іншого боку, $a^{360} = e$. Значить, якщо $30l$ ділиться на 360, то $a^{30l} = e$, а значить і $g^{30} = e$. Це має місце при $l = 12p, p \in N$. Таким чином, $g = a^{12}, g = a^{24}, ..., g = a^{348}$ - шукані елементи групи. З них порядок 30 має тільки елемент $g = a^{12}$.

Задача 4. Довести, що: 1) коли в групі порядок кожного не нейтрального елемента дорівнює 2, то група абелева; 2) коли при цьому група скінчена, то її порядок є степенем числа 2.

Розв'язання. 1) Нехай $g \neq e$ - довільний елемент даної групи. Тоді за умовою $g^2 = e$ або $g = g^{-1}$. Розглянемо ще один елемент $h \neq e$ цієї групи. Тоді елементи gh і hg теж належать цій групі і за умовою теж мають порядок 2. Розглянемо рівність $(gh)^2 = e$. Запишемо її у вигляді $(gh)(gh) = e$, або за аксіомою асоціативності $g(hg)h = e$. Помножимо ліву і праву частини останньої рівності зліва на елемент g^{-1}, а справа на елемент h^{-1}, отримаємо $hg = g^{-1}eh^{-1} = gh$, що і треба було довести.

2) Якщо в скінченій групі кожен елемент співпадає зі своїм оберненим, то в ній можна виділити систему твірних $M = \{a_1, a_2, ..., a_n\}$. Повний набір елементів цієї групи містить всі можливі добутки по 2, по 3,…, по n елементів із множини M, причому порядок елементів в кожному добутку несуттєвий. Отже, загальна кількість елементів в такій групі дорівнює кількості всіх підмножин множини , що складається із n елементів, тобто дорівнює 2^n, що і треба було довести.

Задача 5. Довести, що будь-яка група простого порядку є циклічною.

Розв'язання. Нехай $|G| = p$, p - просте число, $\beta \in G, \beta \neq e$ і β має порядок n, $n > 1$. Множина $H = \{e, \beta, \beta^2, ..., \beta^{n-1}\}$ є циклічною підгрупою групи G. За теоремою Лагранжа число n є дільником числа p. Оскільки $n \neq 1$, то $n = p$, тобто H співпадає з усією групою, і отже група G - циклічна.

Задача 6. Довести, що при $n \geq 3$ група S_n некомутативна і знайти $[S_n, S_n]$.

Вказівка. Для будь-яких $\alpha, \beta \in S_n$ комутатор $[\alpha, \beta] = \alpha\beta\alpha^{-1}\beta^{-1}$ є парною підстановкою. Значить, $[S_n, S_n] \subseteq A_n$. Оскільки $(ij)(ik)(ij)^{-1}(ik)^{-1} = (ijk)$ і цими циклами породжується вся A_n, то $[S_n, S_n] = A_n$.

Задача 7. Довести, що при $n \geq 3$ група S_n некомутативна і знайти $[S_n, S_n]$.

Вказівка. Для будь-яких $\alpha, \beta \in S_n$ комутатор $[\alpha, \beta] = \alpha\beta\alpha^{-1}\beta^{-1}$ є парною підстановкою. Значить, $[S_n, S_n] \subseteq A_n$. Оскільки $(ij)(ik)(ij)^{-1}(ik)^{-1} = (ijk)$ і цими циклами породжується вся A_n, то $[S_n, S_n] = A_n$.

Питання для самоконтролю

1. Поняття системи твірних групи.
2. Означення циклічної групи.
3. Приклади систем твірних.
4. Приклади циклічних груп.

Задачі для самостійного розв'язання

1. Довести теорему: будь-яка підгрупа циклічної групи є циклічною.

2. Навести приклад двох груп з однаковим числом елементів і не ізоморфних.

3. Знайти мінімальні системи твірних в групах: 1) симетрій правильного трикутника, 2) симетрій квадрата, 3) поворотів правильного 12-кутника, 4) коренів 6 – го степеня із 1.

4. В групі $SL(2,Z)$ знайти підгрупу, породжену елементом $A=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$. Яким є порядок цієї підгрупи?

5. Знайти підгрупу групи S_5, породжену підстановкою $\alpha=(13)(245)$.

6. Довести, що адитивна група Z є циклічною. Знайти всі її одноелементні системи твірних.

7. Яким може бути найбільший порядок циклічної підгрупи групи S_9?

8. Довести, що в циклічній групі порядку n порядок будь-якої підгрупи, ділить n і що для кожного дільника d числа n існує рівно одна підгрупа порядку d.

ПРАКТИЧНЕ ЗАНЯТТЯ 6
Нормальна підгрупа і фактор-група

План

1. Означення нормальної підгрупи.
2. Побудова прикладів нормальних підгруп.
3. Суміжні класи по підгрупі та їх властивості.
4. Означення фактор-групи.

Ключові поняття: нормальна підгрупа, лівий суміжний клас по підгрупі, правий суміжний клас по підгрупі, розклад групи по підгрупі, фактор-група

Для розуміння означення нормальної підгрупи необхідно ознайомитись з поняттям добутку (у випадку мультиплікативної групи) підмножин. Так називають множину $AB = \{a * b \mid a \in A, b \in B\}$, де A, B підмножини групи $(G,*)$. Зокрема, підмножина aH (Ha), де $a \in G, H < G$ називається лівим (правим) суміжним класом по підгрупі H, породженим елементом a, а сам елемент a називають представником суміжного класу [3,7].

Слід ознайомитись з поняттям індексу підгрупи і новим формулюванням теореми Лагранжа з використанням поняття індексу: Якщо H - підгрупа скінченої групи G, то $|G| = [G:H] \cdot |H|$, де $[G:H]$ - індекс підгрупи.

 Зверніть увагу на еквівалентні умови, які виділяють нормальну підгрупу. Ми будемо користуватись такими двома умовами:

1) Підгрупа $N < G$ є нормальною, якщо для всіх $a \in G$ виконується $a^{-1}Na = N$.

2) Підгрупа $N < G$ є нормальною, якщо для всіх $a \in G$ виконується $Na = aN$.

Якщо N - нормальна підгрупа групи G, то будемо писати $N \lhd G$.

Треба уважно вивчати означення фактор-групи, оскільки часто в ньому забувають про те, що треба розглядати нормальну підгрупу. Нетривіальною є також доведення існування структури групи на множини суміжних класів групи по її нормальній підгрупі [4]. Для подолання цих труднощів слід потренуватись виконувати дії над суміжними класам для конкретних груп, наприклад, групи підстановок або адитивної групи цілих чисел.

 Запам’ятайте значення в теорії груп понять нормальної підгрупи і фактор-групи – вони дозволяють частково зводити вивчення груп до груп меншого порядку (частково, тому що по заданим нормальній підгрупі N і фактор-групі G/N група G визначається неоднозначно).

Приклади розв'язування задач

Задача 1. Дано групу симетрій квадрата. Довести, що її підгрупа, яка складається з симетрій відносно центра квадрата, є нормальною та знайти фактор-групу групи симетрій квадрата по цій підгрупі.

Розв'язання. Нагадаємо, що сама група симетрій квадрату має вигляд $D_4 = \left\{ e, R_O^{90^0}, R_O^{180^0}, R_O^{270^0}, S_{AC}, S_{BD}, S_{MN}, S_{KL} \right\}$ (задача 2 практичного заняття 3) або $D_4 = \{E, A, B, C, a, b, c, d\}$. Підгрупа симетрій квадрата відносно його центру складається з двох елементів: $M = \{E, B\}$. Легко переконатись, що ліве і праве розкладання групи по цій підгрупі співпадають. Тому вона є нормальною підгрупою, а фактор-група групи D_4 по підгрупі M центральних симетрій має вигляд $D_4 / M = \{\{E, B\}, \{A, C\}, \{a, b\}, \{c, d\}\}$.

Задача 2. Нехай $H < G$, $g \in H$. Доведіть, що $gHg^{-1} < G$.

Розв'язання. Застосуємо критерій підгрупи. За умовою $H < G$, тому $\forall a, b \in H \quad ab^{-1} \in H$. Позначимо $N = gHg^{-1}$, тобто $N = \left\{ ghg^{-1} : h \in H \right\}$. Якщо елементи h_1, h_2 належать H, то елементи $a = gh_1g^{-1}, b = gh_2g^{-1}$ належать N. Далі, $b^{-1} = \left(gh_2g^{-1}\right)^{-1} = \left(g^{-1}\right)^{-1} h_2^{-1} g^{-1} = gh_2^{-1}g^{-1} \in N$ тому, що $h_2^{-1} \in H$. Для добутку ab^{-1} отримаємо $ab^{-1} = \left(gh_1g^{-1}\right)\left(gh_2^{-1}g^{-1}\right) = gh_1\left(g^{-1}g\right)h_2^{-1}g^{-1} = g\left(h_1h_2^{-1}\right)g^{-1} \in N$ тому, що $h_1h_2^{-1} \in H$. Отже, $N = gHg^{-1} < G$, що і треба було довести.

Задача 3. Нехай n - порядок групи G, m - порядок її підгрупи H і $n = 2m$. Довести, що H є нормальною підгрупою.

Нехай G - група, і H - її підгрупа індексу 2 (індекс підгрупи $[G : H]$ - це кількість суміжних класів по цій підгрупі). Уся група розбивається на два суміжних класи по H. Оскільки один із них – це сама підгрупа H, то в інший суміжний клас входять усі елементи групи G, що залишились. Позначимо цей клас H'. Згідно означенню суміжного класу $H' = g'H$, де $g' \notin H$. Аналогічно для правих суміжних класів: один із класів - це знову H, а другий клас - це $H'' = Hg''$, де $g'' \notin H$. Зрозуміло, що $H' = H'' = G \setminus H$, оскільки і в один і в інший клас входять в точності ті елементи групи, які не належать H.

Тому, будь-яка підгрупа індексу 2 буде нормальною. Звідси отримаємо нетривіальний приклад нормальної підгрупи.

Задача 4. Довести, що група A_4 не має підгруп порядку 6.

Розв'язання. Зауважимо спочатку, що з теореми Лагранжа випливає лише те, що коли в групі є підгрупа, то її порядок ділить порядок групи. Але не для кожного дільника порядку групи існує підгрупа, порядок якої дорівнює

цьому дільнику, тобто обернена теорема не має місця. Сформульована задача є контрприкладом, який доводить цей факт.

Припустимо, що така підгрупа існує. Тоді із задачі 3 випливає, що вона повинна бути нормальною, оскільки її порядок дорівнює половині порядку групи. Але будь-яка нормальна підгрупа групи A_4 містить тільки елементи порядку 2, тобто максимальний можливий порядок підгрупи групи A_4 дорівнює 2. Отримали протиріччя.

Питання для самоконтролю

1. Властивості лівих (правих) суміжних класів.
2. Поняття індексу підгрупи.
3. Формулювання теореми Лагранжа з використанням поняття індексу підгрупи.
4. Означення нормальної підгрупи.
5. Критерій нормальної підгрупи.
6. Означення фактор-групи.

Задачі для самостійного розв'язання

1. Довести, що в комутативній групі будь-яка підгрупа є нормальною підгрупою.

2. Довести наслідки з теореми Лагранжа:

А) Порядок елемента скінченої групи ділить порядок цієї групи,

Б) Будь-яка група простого порядку p ізоморфна групі Z_p.

3. Нехай ліві суміжні класи по підгрупі H, породжені елементами x і y мають спільний елемент. Довести, що вони співпадають.

4. Знайти суміжні класи а) Z по nZ, в) R по Z, с) C по R, д) S_n по S_{n-1}.

а) $k + nZ$, де, наприклад, $k = 0,1,...,n-1$;

в) $x + Z$, де, наприклад, $x \in [0,1)$;

с) $z + R$, де, наприклад, $z \in iR$;

5. Знайти всі ліві і всі праві суміжні класи групи S_3 по підгрупі $H = \{e,(12)\}$.

6. Знайти порядок фактор-групи: а) групи S_3 по її комутанту A_3; б) групи A_4 по її комутанту V_4; в) групи V_4 по її комутанту $\{e\}$.

7. Довести, що центр будь-якої групи є її нормальною підгрупою.

8. Доведіть, що Z / Z_n є циклічною групою порядку n. Довести, що фактор-група циклічної групи є циклічною.

9. Чи вірно, що скалярні ненульові матриці утворюють нормальну підгрупу в групі $GL(n, R)$?

10. Довести, що підгрупа $K = \{e, (12)(34), (13)(24), (14)(23)\}$ в S_4 є нормальною і довести, що $S_4 / K \cong S_3$.

ПРАКТИЧНЕ ЗАНЯТТЯ 7
Гомоморфізми груп

План

1. Означення гомоморфізму груп.
2. Означення ядра та образу гомоморфізму груп.
3. Властивості гомоморфізмів.
4. Поняття природного гомоморфізму.
5. Основна теорема про гомоморфізми та її застосування.

Ключові поняття: гомоморфізм груп, ядро гомоморфізму, образ гомоморфізму, природний гомоморфізм, основна теорема про гомоморфізми

Порівняйте означення ізоморфізму та гомоморфізму груп, зверніть увагу на те, що в означенні гомоморфізму не вимагається, щоб відображення було взаємно однозначним [4].

Зверніть увагу на доведення наступних властивостей гомоморфізмів:

1) Гомоморфізм зберігає нейтральний елемент, тобто $f(e)=e'$,

2) Образом оберненого елементу є обернений до образу, тобто $f(a^{-1})=(f(a))^{-1}$,

3) Композиція двох гомоморфізмів є гомоморфізмом.

При вивченні понять ядра та образу гомоморфізму $f: G \to H$ бажано довести, що ядро $Kerf = \{a \in G \mid f(a)=e\} \subset G$ та образ $\operatorname{Im} f = \{b \in H \mid \exists a \in G\ f(a)=b\} \subset H$ гомоморфізму є підгрупами, а $Kerf$ є нормальною підгрупою.

З означень випливає, що поняття гомоморфізму більш загальне в порівнянні з поняттям ізоморфізму. Умови, при яких гомоморфізм буде ізоморфізмом, можна сформулювати у термінах ядра та образу наступним чином:

Якщо $f: G \to H$ - гомоморфізм і $Kerf = \{e\}$, $\operatorname{Im} f = H$, то f є ізоморфізмом груп G і H.

Приклади розв'язування задач

Задача 1. Чи є відображення $f: C \setminus \{0\} \to R \setminus \{0\}$ за правилом $f(z)=2|z|$ гомоморфізмом?

Розв'язання. треба перевірити виконання рівності $f(u \cdot v)=f(u)\cdot f(v)$ для будь-яких $u, v \in C^* = C \setminus \{0\}$. В обох групах операцією є звичайне множення.

Так як $f(u \cdot v)=2|u \cdot v|$, $f(u)\cdot f(v)=2|u|\cdot 2|v|$, то рівність не виконується, відображення не є гомоморфізмом.

Задача 2. Довести, що фактор-група групи симетрій квадрата по нормальній підгрупі симетрій відносно центру ізоморфна групі симетрій ромба.

Доведення. Раніше будо знайдено фактор-групу групи $D_4 = \left\{ e, R_O^{90^0}, R_O^{180^0}, R_O^{270^0}, S_{AC}, S_{BD}, S_{MN}, S_{KL} \right\}$ по її підгрупі $M = \left\{ e, R_O^{180^0} \right\}$. Ми використовували позначення $D_4 = \{E, A, B, C, a, b, c, d\}$ і $M = \{E, B\}$, в яких фактор-група мала вигляд $D_4 / M = \{\{E, B\}, \{A, C\}, \{a, b\}, \{c, d\}\}$. Користуючись означенням добутку множин в групі, знайдемо $\{E, B\}\{E, B\} = \{E, B\}$, $\{A, C\}\{A, C\} = \{E, B\}$, $\{a, b\}\{a, b\} = \{E, B\}$, $\{c, d\}\{c, d\} = \{E, B\}$. В групі $R = \{e, Z, m, n\}$ симетрій ромба кожний елемент теж має порядок 2, а отже існування ізоморфізму між цими групами є очевидним.

Теорема (про гомоморфізми груп) Нехай дано гомоморфізм φ групи G на групу G' і N ядро цього гомоморфізму. Тоді група G' ізоморфна фактор-групі G/N, причому гомоморфізм φ дорівнює послідовному виконанню природного гомоморфізму $\varepsilon : G \to G/N$ та ізоморфізму $\tau : G/N \to G'$.

Доведення. Задамо відображення τ фактор-групи G/N на групу G' за правилом: $\tau(xN) = \varphi(x), x \in G$. Покажемо, що τ - ізоморфізм. По-перше, якщо $xN = yN$, то $\varphi(x) = \varphi(y)$ і $\tau(xN) = \tau(yN)$. По-друге, образи різних елементів різні, оскільки з $\varphi(x) = \varphi(y)$ випливає $x^{-1}y \in N = Ker\varphi$. Отже, і для прообразів матимемо $xN = yN$. Протиріччя. По-третє, відображення τ зберігає операцію: $\tau(xN \cdot yN) = \tau(xyN) = \varphi(xy) = \varphi(x)\varphi(y) = \tau(xN)\tau(yN)$. Отже, відображення τ є ізоморфізмом.

Гомоморфізм φ є композицією $\varepsilon\tau$. Дійсно, φ діє за правилом $\varphi : x \to \varphi(x)$. З іншого боку, $x \xrightarrow{\varepsilon} xN \xrightarrow{\tau} \varphi(x)$. Теорему доведено.

Питання для самоконтролю

1. Види гомоморфізмів.
2. Означення ядра та образу гомоморфізму.
3. Який гомоморфізм має тривіальне ядро?
4. Порівняння понять гомоморфізму та ізоморфізму груп.
5. Поняття природного гомоморфізму.
6. Основна теорема про гомоморфізми та її значення.

Задачі для самостійного розв'язання

1. Довести, що наступні відображення є гомоморфізмами, знайти їх ядра та образи:

А) $f:(R,+)\to(R\setminus\{0\},\cdot)\quad f(x)=e^x$,

Б) $f:(R,+)\to(C\setminus\{0\},\cdot)\quad f(x)=e^{2\pi ix}$,

В) $f:S_n\to\{1,-1\}\quad f(\sigma)=\operatorname{sgn}\sigma$.

2. . Довести, що не існує гомоморфізму груп $G=(R,+)$ і $G'=(Z,+)$.

3. Опишіть гомоморфізми із Z_6 в Z_{18}, із Z_{18} в Z_6, із Z_{12} в Z_{15}, із Z_m в Z_n.

4. Побудувати природній гомоморфізм групи $(Z,+)$ в групу $Z/3Z$.

ПРАКТИЧНЕ ЗАНЯТТЯ 8
Теореми Силова

План

1. Поняття силовської підгрупи. Поняття *p*-групи.
2. Зв'язок довільної *p*-підгрупи з силовською *p*-підгрупою групи G.
3. Теореми Силова.

Ключові поняття: *p*-група, *p*-підгрупа, силовська *p*-підгрупа, теореми Силова, порівняння за модулем

Згадайте, що теорема Лагранжа у загальному випадку не гарантує існування в групі порядку n підгрупи порядку k, де k є дільником числа n. Теореми Силова для деяких дільників порядку групи гарантують існування підгруп такого порядку. Доведені норвезьким математиком Силовим у 1872 році [7].

Для розуміння теорем Силова слід ознайомитись з означенням понять *p* – підгрупи і силовської *p* – підгрупи. Ці поняття вводяться для скінчених груп.

У більшості підручників формулюються три теореми Силова. Всі вони мають одну і ту саму умову. Тому зручніше буде об'єднати їх у вигляді одного твердження з трьома пунктами висновків.

Тобто бажано запам'ятати теорему Силова у наступному формулюванні:

Нехай $|G| = p^k m$, де p просте число, НСД$(p, m) = 1$. Тоді

1) в групі G існує силовська *p* – підгрупа,
2) будь-яка *p* – підгрупа групи G міститься в деякій силовській *p* – підгрупі,
3) число силовських *p* – підгруп ділить m і є порівняним з 1 по модулю *p*.

Приклади розв'язування задач

Задача 1. Описати силовські підгрупи в групах S_3, A_4, D_5, D_6.

Розв'язання. Оскільки $|S_3| = 2 \cdot 3$, то в S_3 існують три силовські 2-підгрупи (кожна породжена транспозицією) і одна силовська 3-підгрупа (A_3).

Для другої групи $|A_4| = 2^2 \cdot 3$. В A_4 одна силовська 2-підгрупа $\{e, (12)(34), (13)(24), (14)(23)\}$ і чотири силовські 3-підгрупи (кожна породжена циклом довжини 3).

Враховуючи розклад $|D_5| = 2 \cdot 5$ отримаємо наступний висновок: в групі D_5 п'ять силовських 2-підгруп (кожна породжена симетрією) і одна силовська 5-підгрупа (підгрупа поворотів).

Нарешті $|D_6| = 2^2 \cdot 3$. В D_6 три силовські 2-підгрупи і одна силовська 3-підгрупа.

Задача 2. Довести, що коли $|G| = 56$, то G містить нормальну силовську підгрупу (в частинному випадку, не є простою).

Розв'язання. Маємо $|G| = 56 = 2^3 \cdot 7$. Достатньо довести, що силовська 2-підгрупа або силовська 7-підгрупа єдина. За теоремою Силова число силовських 2-підгруп дорівнює 1 або 7, число силовських 7-підгруп дорівнює 1 або 8. Нехай G містить 8 силовських 7-підгруп. Оскільки всі вони мають простий порядок 7, то їх об'єднання містить $1 + 6 \cdot 8 = 49$ елементів. Звідси випливає, що силовська 2-підгрупа єдина.

Задача 3. Довести, що коли $|G| = p^2 q$, де p і q - різні прості числа, то G містить нормальну силовську підгрупу (в частинному випадку, не є простою).

Розв'язання. Достатньо довести, що силовська p – підгрупа або силовська q - підгрупа єдина. Припустимо, що силовська p – підгрупа неєдина. Тоді, за теоремою Силова, їх число дорівнює q, причому $q \equiv 1 (\mathrm{mod}\, p)$. В частинному випадку, $q > p$. Але тоді p не порівняне з 1 по модулю q, тобто число силовських q - підгруп не може дорівнювати p. Якщо і силовська q - підгрупа неєдина, то число силовських q - підгруп дорівнює p^2. Це значить, що $p^2 \equiv 1 (\mathrm{mod}\, q)$, звідки $p \equiv 1 (\mathrm{mod}\, q)$, тобто $p = q - 1$. Отже, $p = 2, q = 3$. Далі, такі ж міркування, як і в попередній задачі.

Задача 4. Довести, що серед скінчених груп, порядок яких менший за 60, немає неабелевих простих груп.

Доведення. Згідно з лемами з чисел 2, 3, …, 59 треба розглянути лише випадки $n = |G| = 30, 40, 56$.

а) Нехай існує проста група G порядку $|G| = 30 = 2 \cdot 3 \cdot 5$. Нехай S - силовська 5-підгрупа простої групи G, $|S| = 5$. Число $n(5)$ силовських 5 - підгруп є дільником числа 30 і порівняне з 1 по модулю 5. Це або 1, або 6. Перший варіант не підходить, бо тоді $S \lhd G$. Отже, $n(5) = 6$. При цьому перетин будь-яких двох силовських 5-підгруп дорівнює $\{e\}$, а значить їх об'єднання містить 24 ненейтральних елементи.

Аналогічно, $n(3) = 10$ ($n(3) \neq 1$, $n(3)$) ділить число 30, $n(3) \equiv 1 (\mathrm{mod}\, 3)$, об'єднання силовських 3-підгруп містить 20 ненейтральних елементів.

Отже, група G має більше 30 елементів (24+20), що суперечить умові. Таким чином, група G не може бути простою.

б) Нехай існує проста група G така, що $|G| = 40 = 2^3 \cdot 5$ і S - силовська 5-підгрупа групи G. Оскільки $n(5) = 1$ ($n(5)$) ділить число 40, $n(5) \equiv 1 (\mathrm{mod}\, 5)$, то $S \lhd G$ і тому група G не може бути простою.

в) Нехай існує проста група G така, що $|G| = 56 = 2^3 \cdot 7$ і S - силовська 7-підгрупа групи G. Оскільки $n(5) = 8$ ($n(7)$) ділить число 56, $n(7) \equiv 1 (\mathrm{mod}\, 7)$ і перетин будь-яких двох різних підгруп із 7 елементів дорівнює $\{e\}$, то їх об'єднання містить 48 ненейтральних елементів.

Силовська 2-підгрупа містить вісім елементів, тому 48+8=56=$|G|$, але $n(8) > 1$, бо у випадку $n(8) = 1$ матимемо нормальну силовську 2-підгрупу. Умова $n(8) > 1$ показує, що в групі G більше, ніж 56 елементів. Цей випадок теж відповідає непростій групі.

Питання для самоконтролю

1. Поняття порівнянності цілих чисел.
2. Поняття силовської p – підгрупи.
3. Критерій існування в групі єдиної силовської p – підгрупи.

Задачі для самостійного розв'язання

1. Описати силовські підгрупи в групі S_4.

2. Довести, що коли $|G|$ дорівнює 80,196,200, то G містить нормальну силовську підгрупу (в частинному випадку, не є простою).

3. Описати всі групи з 12 елементів.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Батурин Ю.А. Основные структуры современной алгебры [Текст] / Ю.А. Батурин. - М.: Наука, 1990. – 237 с.
2. Ван дер Варден Б.Л. Алгебра [Текст] / Б.Л. Ван дер Варден. - М.: Наука, 1979. – 624 с.
3. Каргополов М.И. Основы теории групп [Текст] / М.И. Каргополов, Ю.И. Мерзляков. - М.: Наука, 1982. – 288 с.
4. Курош А.Г. Теория групп [Текст] / А.Г Курош. - М.: Наука, 1967. – 648 с.
5. Мельников О.В. Общая алгебра. Т.1 [Текст] / О.В. Мельников, В.Н. Ремесленников, В.А. Романьков и др.- М.: Наука, 1990. – 592 с.
6. Кострикин А.И. Сборник задач по алгебре [Текст]/ А.И Кострикин. - М.: Физ-мат. л-ра, 2001.- 463 с.
7. Кострикин А. И. Введение в алгебру. III часть [Текст]/ А. И. Кострикин. - М.: Физматлит, 2001.- 271 с.
8. Каролинский Е.А. Сборник задач по теории групп [Текст] / Е.А. Каролинский, Б.В. Новиков. – Луганск, 2002. - 68 с.
9. Федорчук В.В. Курс аналитической геометрии и линейной алгебры / В.В. Федорчук – М.: Изд-во МГУ, 1990. – 328 с.

Додаткова

1. Белоногов В. А. Задачник по теории групп [Текст] / В.А. Белоногов. - М.: Наука, 2000. – 239 с.
2. Богопольский О.В. Введение в теорию групп [Текст] / О.В. Богопольский. – Москва – Ижевск, 2002. -148 с.
3. Винберг Э.Б. Курс алгебры [Текст] / Э.Б. Винберг. – М.: Факториал Пресс, 2002. – 544 с.
4. Калужнин Л.А. Преобразования и перестановки [Текст] / Л.А Калужнин, В.И. Сущанский. – М.: Наука, 1979. – 112 с.
5. Куликов Л.Я. Сборник задач по алгебре и теории чисел: Учебное пособие для студентов физ.-мат. специальностей пед. институтов [Текст] / Л.Я. Куликов. – М.: Просвещение, 1993. - 288 с.
6. Марков С.Н. Историческое введение в теорию Галуа [Текст] / С.Н. Марков.- Иркутск: ИГУ, 1997. – 20 с.
7. Холл Ю.А. Теория групп [Текст] / Ю.А.Холл. М.: Издательсьво иностранной литературы, 1962. – 468 с.

ТЕРМІНОЛОГІЧНИЙ СЛОВНИК

Абелева група – група, в якій алгебраїчна операція комутативна.

Автоморфізм групи – ізоморфізм групи на себе.

Адитивна група – група, в якій алгебраїчна операція є додаванням.

Алгебраїчна операція на множині – відображення, при якому кожній впорядкованій парі елементів даної множини однозначно ставиться у відповідність єдиний елемент цієї ж множини.

Асоціативність – властивість алгебраїчної операції, яка виражається рівністю $a*(b*c)=(a*b)*c$, для будь-яких трьох елементів множини.

Бієкція – див. взаємно однозначне відображення.

Взаємно однозначне відображення – одночасно ін'єктивне та сюр'єктивне відображення.

Власна підгрупа – будь-яка підгрупа даної групи, відмінна від одиничної підгрупи і самої групи.

Гомоморфізм груп – відображення із однієї групи в іншу, яке зберігає операцію.

Група – будь-яка непорожня множина разом із заданою на ній алгебраїчною операцією, яка має наступні властивості: 1) асоціативна, 2) існує нейтральний елемент, 3) для кожного елемента множини існує симетричний.

Група автоморфізмів – множина всіх автоморфізмів даної групи відносно операції композиції автоморфізмів.

Група діедра – див. діедральна група.

Група лишків за модулем n **-** множина класів лишків за модулем n відносно операції додавання класів.

Група поворотів правильного многокутника – множина всіх поворотів площини, кожен з яких відображає правильний многокутник на себе.

Група симетрій фігури – множина всіх відображень площини або простору, які переводять дану фігуру саму в себе, відносно операції композиції відображень.

Діедральна група – група відображень площини, які не змінюють правильний многокутник.

Добуток підстановок – підстановка, отримана послідовним виконанням двох даних підстановок (множенням підстановок).

Довжина циклу – кількість елементів в ньому.

Загальна лінійна група – множина всіх невироджених матриць *n*- го порядку з дійсними елементами відносно операції множення матриць.

Знакозмінна група *n* – го степеня – множина всіх парних підстановок *n* – го степеня відносно операції множення підстановок.

Ізоморфізм груп – взаємно однозначне відображення із однієї групи в іншу, яке зберігає операцію.

Ізоморфні групи – групи, для яких існує хоча б один ізоморфізм.

Інверсія двох чисел – впорядкований набір двох чисел, в якому перше число більше за друге.

Інволюція – відображення, яке співпадає зі своїм оберненим.

Індекс підгрупи – кількість лівих (правих) суміжних класів групи по цій підгрупі.

Клас лишків за модулем m - множина цілих чисел, які дають при діленні на m однакові остачі.

Композиція автоморфізмів – див. композиція відображень.

Композиція двох відображень – послідовне виконання заданих відображень.

Комутант групи – множина всіх можливих добутків скінченого числа комутаторів групи.

Комутативна група – див. абелева група.

Комутативність – властивість алгебраїчної операції, яка виражається рівністю $a*b=b*a$, для будь-яких двох елементів множини.

Комутатор двох елементів a **і** b **групи** є елемент групи: $a*b*a^{-1}*b^{-1}$, тобто є результатом операції першого з даних елементів, другого, оберненого до першого, оберненого до другого елементів.

Лівий суміжний клас групи по її підгрупі – множина елементів виду ah, де a - фіксований елемент групи, а h належить підгрупі.

Незвідна система твірних– система твірних, з якої не можна вилучити жодної твірної без втрати властивості бути системою твірних.

Нейтральний елемент групи – елемент e групи такий, що для будь-якого елемента a цієї групи виконується рівність $a * e = a$.

Непарна підстановка – підстановка, в якій число інверсій непарне.

Мінімальна система твірних – див. незвідна система твірних.

Мультиплікативна група – група, в якій алгебраїчна операція є множенням.

Невласна підгрупа даної групи – одинична підгрупа, сама група.

Незалежні цикли – цикли, в яких відсутні однакові елементи.

Нормальна підгрупа групи – підгрупа, по якій множини всіх лівих суміжних класів і всіх правих суміжних класів співпадають.

НСД двох чисел – найбільший спільний дільник двох чисел, тобто найбільше з чисел, на які одночасно ділиться кожне з даних чисел.

НСК двох чисел – найменше спільне кратне двох чисел, тобто найменше з чисел, які одночасно діляться на кожне з даних чисел.

Нульовий елемент – нейтральний елемент адитивної групи.

Образ гомоморфізму – множина елементів другої групи, які є образами при гомоморфізмі елементів першої групи.

Одиничний елемент – нейтральний елемент мультиплікативної групи.

Парна підстановка - підстановка, в якій число інверсій парне.

Переставні елементи групи – два елементи групи, результат алгебраїчної операції над якими не залежить від їх порядку.

Підгрупа – підмножина елементів групи, яка сама є групою відносно тієї ж операції, що і в групі.

Підстановка *n*-го степеня – взаємно однозначне відображення множини перших n натуральних чисел на себе.

Порівняні за модулем *p* числа – два числа, різниця яких ділиться на p.

Порядок групи – кількість елементів в скінченій групі, або нескінченість (для нескінчених груп).

Порядок елемента групи – найменший натуральний степінь цього елемента, який дорівнює нейтральному елементу (для не нейтрального елемента).

Правий суміжний клас групи по її підгрупі – множина елементів виду ha, де a - фіксований елемент групи, а h належить підгрупі.

Природний гомоморфізм – гомоморфізм із групи в групу суміжних класів даної групи по її нормальній підгрупі.

Проста група – група, в якій немає власних нормальних підгруп.

Протилежний елемент – симетричний елемент адитивної групи.

Розклад групи по підгрупі – представлення групи у вигляді об'єднання лівих (або правих) суміжних класів по цій підгрупі.

Силовська *p* – підгрупа - підгрупа H групи G, $|G| = p^k m$, для якої $|H| = p^k$, де p просте число, НСД$(p, m) = 1$.

Симетричний елемент – елемент a' групи такий, що для будь-якого елемента a цієї групи виконується рівність $a * a' = e$.

Симетрична група *n* – го степеня – множина всіх підстановок n-го степеня відносно операції множення підстановок.

Система твірних – множина елементів групи така, що кожен елемент групи можна отримати як результат операції над скінченою кількістю елементів цієї множини або обернених до них елементів.

Скінченопороджена група – група, для якої існує система твірних, що складається зі скінченого числа елементів.

Спеціальна лінійна група – множина всіх матриць n-го порядку з дійсними елементами, визначник яких дорівнює одиниці.

Суміжний клас групи по її підгрупі – лівий або правий суміжний клас.

Таблиця Келі – квадратна таблиця, елементами якої є результати групової операції для всіх впорядкованих пар елементів скінченої групи.

Транспозиція – цикл довжини 2.

Фактор-група – множина суміжних класів групи по її нормальній підгрупі відносно операції множення суміжних класів.

Центр групи – множина елементів групи, яки є переставними з кожним елементом цієї групи.

Цикл – перестановка.

Циклічна група – група, для якої існує система твірних, що складається з одного елементу.

Ядро гомоморфізму – множина елементів першої групи, образами яких при гомоморфізми є нейтральний елемент другої групи.

***p* – група –** скінчена група, порядок якої є натуральним степенем простого числа p.

***p* – підгрупа –** підгрупа порядку p^k скінченої групи G, де p – просте число, яке ділить порядок групи.

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ

$\exists$ – квантор існування,
$\forall$ – квантор загальності,
$\wedge$ – логічна операція, кон'юнкція,
$\vee$ – логічна операція, диз'юнкція,
$\left.\begin{matrix}\Rightarrow,\\ \Leftarrow\end{matrix}\right\}$ – логічна імплікація,
$\Leftrightarrow$ – логічна еквівалентність (рівносильність),
$\bigcup$ – множинна операція, об'єднання,
$\bigcap$ – множинна операція, перетин,
$\in$ – символ належності елемента деякій множині,
$\varnothing$ - порожня множина,
Z - множина цілих чисел,
Q - множина раціональних чисел,
R - множина дійсних чисел,
C - множина комплексних чисел,
Z_n - множина класів лишків за модулем n,
nZ - множина цілих чисел, кратних заданому числу $n \neq 0$,
U_n - група коренів n-го степеня з одиниці,
D_n - група діедра,
S_n - симетрична група степеня n,
A_n - знакозмінна група степеня n,
$GL(n,R)$ - загальна лінійна група,
$SL(n,R)$ - спеціальна лінійна група,
$(G,*)$ - група на множині G відносно операції *,
$Aut(G)$ - група автоморфізмі групи G,
$H < G$ - множина H є підгрупою групи G,
$|G|$ - порядок групи G,
$\cong$ - відношення ізоморфізму груп,
G/H - фактор –група групи G по підгрупі H,
$[G:H]$ - індекс підгрупи H групи G,
$Kerf$ - ядро гомоморфізму f,
$\mathrm{Im}\, f$ - образ ізоморфізму f,
$\det A$ - детермінант матриці A,
A^{-1} - матриця, обернена до матриці A,
E - одинична матриця,
НСД(a,b) - найбільший спільний дільник чисел a і b,
НСК(a,b) - найменше спільне кратне чисел a і b,
$M \times N$ - декартовий добуток множин M і N,

$\operatorname{Re} z$ - дійсна частина комплексного числа z,
$\operatorname{Im} z$ - уявна частина комплексного числа z,
$|z|$ - модуль комплексного числа z,
$\arg z$ - аргумент комплексного числа z,

Навчально - методичне видання
(українською мовою)

СТЄГАНЦЕВ ЄВГЕНІЙ ВІКТОРОВИЧ

ТЕОРІЯ ГРУП

Методичні вказівки
для студентів напряму підготовки «Математика»
спеціалізації «Алгебра і теорія чисел»

Рецензент А.К. Приварников
Відповідальний за випуск А.К. Приварников
Коректор Є.В. Стєганцев