МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХЕРСОНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Факультет комп'ютерних наук, фізики та математики
Кафедра алгебри, геометрії та математичного аналізу

ТЕОРЕМИ СИЛОВА ТА ЇХ ЗАСТОСУВАННЯ

Кваліфікаційна робота (проєкт)
на здобуття ступеня вищої освіти «бакалавр»

Виконала: студетка 4 курсу, групи 421
Спеціальності 014.04
Середня освіта (математика)
Освітньо-професійної програми
Матійків Світлана Володимирівна

Керівник: кандидат фізико-
математичних наук, доцент Котова О.В.
Рецензент: кандидат педагогічних наук,
професор Шерман М.І.

Херсон - 2020

ЗМІСТ

ВСТУП

Одним з основних розділів сучасної алгебри є теорія груп. Групи - це один з основних типів алгебраїчних структур.

Знадобилася близько ста років роботи кількох поколінь математиків, перш ніж ідея групи кристалізувалася з її сьогоденною ясністю.

Теорія груп почала оформлюватися в якості самостійного розділу математики в кінці XVIII століття. Протягом перших десятиліть XIX століття вона розвивалася повільно і практично не привертала до себе уваги. Але потім, близько 1830 року, завдяки роботам Галуа і Абеля про можливості розв'язання алгебраїчних рівнянь всього за кілька років вона зробила гігантський стрибок, який вплинув на розвиток усієї математики. З тих пір основні поняття теорії груп стали детально досліджуватися.

В теперішній час теорія груп є однією з найбільш розвинених областей алгебри, має численні застосування як в самій математиці, так і за її межами - в теорії функцій, квантової механіки, топології, кристалографії і інших областях математики і природознавства.

Поняття групи тісно пов'язане з поняттям підгрупи. Слово підгрупа означає - група всередині групи.

Поняття підгрупи є основним в теорії груп. Весь зміст теорії пов'язано в більшій чи меншій мірі з питаннями про наявність в групі підгруп з тими чи іншими спеціальними властивостями, про групи, які можуть бути вкладені в дану групу, про ті чи інші властивості, що характеризують взаємне розташування підгруп в групі, про способи побудови групи по її підгрупах. Крім того, за допомогою підгруп можна описати внутрішню структуру деяких груп. Виділення тих чи інших

спеціальних типів груп також пов'язано переважно з поняттям підгрупи. Тому підгрупи грають особливу роль в розвитку і застосуванні теорії групи.

Найстаршою і гілкою теорії груп, що інтенсивно розвивається, є теорія скінчених груп. Теорема Силова є наріжним каменем в теорії скінчених груп.

Келі розв’язав задачу, яка полягає в тому, щоб дати повну класифікацію всіх груп, порядки яких дорівнюють заданим натуральним числом n. Він здійснив фіксування порядку і вивчення неабелевих груп, виходячи або з розмірів центру, або нормальності підгрупи чи інших характеристик групи. Для вирішення цього завдання було застосовано різні математичні методи. Другий напрямок, який здійснив вчений, - це розгляд цілого класу груп порядку n з певним канонічним розкладом цього порядку. Так, наприклад, відомо, що якщо n - просте число, то існує єдина група такого порядку. Класичний приклад опису груп порядку $n = pq$, де p і q - різні прості числа, реалізований за допомогою теорем Людвіга Силова. Ф. Холл узагальнив результати Силова.

Метою даної дипломної роботи є вивчення силовських p-підгруп скінченої групи і їх властивостей.

Мета зумовила постановку і вирішення наступних завдань.

1. Вивчити основні поняття теорії груп.

2. Розглянути теорему Силова і проаналізувати різні способи її доведення.

3. Навести приклади застосування теорем Силова.

Об’єкт дослідження – теорія груп та її застосування.

Предмет дослідження – теорема Силова та її застосування.

Поставлені завдання визначили структуру дипломної роботи, яка складається зі вступу, трьох розділів, висновків та списку використаних джерел.

У першому розділі зібрані допоміжні поняття і теореми, які використовуються в роботі, що дозволило зробити виклад більш доступним і замкнутим.

У другому розділі дається визначення p-підгрупи, доводяться теореми Силова, дається опис груп порядку pq і, крім того, наводяться приклади силовських p-підгруп.

У третьому розділі застосування теорем Силова.

РОЗДІЛ 1
ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

1.1. Основні алгебраїчні структури

Теорія груп – це розділ загальної алгебри, що вивчає алгебраїчні структури, які називаються групами, і їх властивості. Група являється центральним поняттям в загальній алгебрі, так як багато важливих алгебраїчні структури, такі як кільця, поля, векторні простори, являють собою групи з розширеним набором операцій і аксіом. Групи виникають у всіх областях математики, і методи теорії груп роблять сильний вплив на багато розділів алгебри [36].

В процесі розвитку теорії груп побудований потужний інструментарій, багато в чому визначив специфіку загальної алгебри в цілому, сформований власний глосарій, елементи якого активно запозичуються суміжними розділами математики і додатками. Найбільш розвинені галузі теорії груп - лінійні алгебраїчні групи і групи Лі - стали самостійними областями математики [36].

Різні фізичні системи, такі як кристали або атом водню, мають симетрії, які можна змоделювати групами симетрії, таким чином знаходячи важливі застосування теорії груп і тісно пов'язаної з нею теорії зображень у фізиці і хімії [36].

Одним з найбільш значних математичних проривів XX століття [1] стала повна класифікація простих скінчених груп – результат спільних зусиль багатьох математиків, що займає більше 10 тисяч друкованих сторінок, основний обсяг яких опубліковано з 1960 по 1980 роки [36].

У теорії груп три історичних кореня: теорія алгебраїчних рівнянь, теорія чисел і геометрія. Математики, які стоять біля витоків теорії груп, - це Леонард Ейлер, Карл Фрідріх Гаус, Жозеф Луї Лагранж, Нільс

Хенрік Абель і Еваріст Галуа. Галуа був першим математиком, хто зв'язав теорію груп з іншою гілкою абстрактної алгебри - теорією полів, розробивши теорію, нині звану теорією Галуа [36].

Однією з перших завдань, що призвели до виникнення теорії груп, була задача отримання рівняння ступеня m, яке мало б корінням m коренів даного рівняння ступеня n (m <n). Це завдання в простих випадках розглянув Худде (1659 г.). У 1740 р Сондерсон зауважив, що перебування квадратичних множників біквадратних виразів зводиться до вирішення рівняння 6 ступеня, а Ле Сер (1748 г.) і Вейрінг (з 1762 по 1782 рр.) Розвинули цю ідею [36].

Загальну основу для теорії рівнянь, що будується на теорії перестановок, в 1770-1771 рр. знайшов Лагранж, і на цьому грунті в подальшому виросла теорія підстановок. Він виявив, що коріння всіх резольвент, з якими він стикався, є раціональними функціями від коренів відповідних рівнянь. Щоб вивчити властивості цих функцій, він розробив «обчислення поєднань» (Calcul des Combinaisons). Сучасна йому робота Вандермонда (1770 г.) також передбачала розвиток теорії груп [36].

Паоло Руффини в 1799 році запропонував доказ нерозв'язності рівнянь п'ятого і вищих ступенів в радикалах. Для доказу він використовував поняття теорії груп, хоч і називав їх іншими іменами. Руффини також опублікував лист, написаний йому абат, лейтмотивом якого була теорія груп. Галуа виявив, що якщо у алгебраїчного рівняння кілька коренів, то завжди існує група перестановок цих коренів така, що

1. всяка функція, інваріантна щодо підстановок групи, раціональна і, навпаки,

2. всяка раціональна функція від коренів інваріантна щодо перестановок групи. Свої перші праці з теорії груп він опублікував в

1829 р, у віці 18 років, але вони залишилися практично непоміченими, поки в 1846 р не було видано зібрання його творів [36].

Артур Келі і Огюстен Луї Коші стали одними з перших математиків, оцінили важливість теорії груп. Ці вчені також довели деякі важливі теореми теорії. Досліджуваний ними предмет був популяризував Серре, який присвятив теорії секцію зі своєї книги з алгебри, Жорданом, чия праця «Дії над підстановками» (Traité des Substitutions) став класикою, і Ойген Нетто (1882 рік). Великий внесок у розвиток теорії груп внесли також багато інших математики XIX століття: Бертран, Ерміт, Фробениус, Кронекер і Матьє [36].

Сучасне визначення поняття «група» було дано тільки в 1882 р Вальтером фон Дюком.

У 1884 р Софус Лі поклав початок вивченню як груп перетворень того, що ми зараз називаємо групами Лі і їх дискретними підгрупами; за його працями пішли роботи Кіллінг, штудії, Шура, Маурера і Елі Картана. Теорія дискретних груп була розроблена Клейном, Лі, Пуанкаре і Пікаром в зв'язку з вивченням модулярних форм та інших об'єктів [36].

В середині XX століття (в основному, між 1955 і 1983 рр.) Була проведена величезна робота по класифікації всіх скінчених простих груп, що включає десятки тисяч сторінок статей [36].

Відчутний внесок в теорію груп внесли і багато інших математики, такі як Артін, Еммі Нетер, Людвіг Сілов і інші.

Означення 1.1.1. Безліч А, разом з однією або декількома операціями алгебри, визначеними на цій множині називають структурою алгебри [35].

Позначення: (А, *) - алгебраїчна структура з однієї алгебраїчній операцією; (А,*,) - алгебраїчна структура з двома алгебраїчними операціями [35].

Розглянемо спочатку алгебраїчну структуру з однією алгебраїчній операцією (А, *).

Означення 1.1.2. Елемент $e \in A$ називається нейтральним елементом щодо алгебраїчної операції *, якщо $\forall x \in A$ виконують рівність*: x*e=e*x=x.* Нейтральний елемент щодо складання називається нульовим елементом або просто нулем і позначається відповідною цифрою 0:

$$\forall x \in A \quad , \quad x+0=0+x=x \quad [35].$$

Означення 1.1.3. Нейтральний елемент щодо множення називається одиничним елементом або просто одиницею і позначається або цифрою 1, або буквою е:

$$\forall x \in A \quad , \quad x \cdot 1 = 1 \cdot x = x \quad \text{або} \quad x \cdot e = e \cdot x = x \quad .$$

Теорема1.1.1. Нехай (А, *) - алгебраїчна структура. Тоді, якщо в множині A існує нейтральний елемент, то він єдиний [35].

Доведення.

Припустимо, що в багатьох A є два нейтральних елемента: $e \in A$ і $e' \in A$. Тоді $\forall x \in A$ виконується рівність: $x*e=x$ і $e'*x=x$.

Це означає, що ці рівності виконуються і при $x=e$ і при $x=e'$: $e'*e=e'$ і $e'*e=e$. Звідси випливає, що $e=e'$, ч.т.д. [35].

Означення 1.1.4. Нехай (А, *) - алгебраїчна структура з нейтральним елементом е. Елемент$x' \in A$ називається симетричним елементу$x \in A$ щодо алгебраїчної операції *, якщо $x*x'=x'*x=e$ *[35].*

Означення 1.1.5. Нехай (А, *) - алгебраїчна структура з нейтральним елементом е. Якщо кожен елемент $x \in A$ має симетричний йому $x' \in A$ і хтось скаже, що безліч A симетрично щодо операції * [35].

Теорема 1.1.2. Нехай (А, *) - алгебраїчна структура з нейтральним елементом е і асоціативної алгебри операцією *. якщо елемент $x \in A$ має симетричний йому елемент$x' \in A$, то такий елемент єдиний [35].

Доведення.

Припустимо, що елемент $x \in A$ має два симетричних йому: $x' \in A$ і $x'' \in A$. Тоді з визначення симетричного елемента слід, що виконуються дві рівності:

$$x * x' = x' * x = e \quad \text{і} \quad x * x'' = x'' * x = e \quad [35].$$

Отже тоді $x' = x' * e = x' * (x * x'') = (x' * x) * x'' = e * x'' = x''$

, ч.т.д.

Зауваження. В алгебраїчній структурі з адитивною формою записи елемент симетричний елементу х називається протилежним і позначається (-х):

$$x + (-x) = (-x) + x = 0 \quad .$$

Означення 1.1.6. В алгебраїчній структурі з мультиплікативною формою запису елемент симетричний елементу *x* називається зворотним і позначається x^{-1} :

$$x \cdot x^{-1} = x^{-1} \cdot x = e \quad \text{або} \quad x \cdot x^{-1} = x^{-1} \cdot x = 1 \quad [35].$$

Теорема 1.1.3. (Загальна властивість будь-яка а.о.) Нехай (А,*) – алгебраїчна структура і $a,b,c,d \in A$. Якщо $a=b$ і $c=d$, то $a*c=b*d$ і $c*a=d*b$ [35].

Доведення.

З визначення рівності упорядкованих пар слід, що $(a;c)=(b;d)$. Тепер з визначення алгебраїчної операції слід, що $(a;c) \to a*c$ і $(b;d) \to b*d$.

Так як кожній парі елементів безлічі *A* ставиться у відповідність єдиний елемент множини *A* (результат алгебраїчної операції), то з рівності $(a;c)=(b;d)$ відразу ж слід рівність $a*c=b*d$. Аналогічно доводиться друга рівність. Теорема доведена [35].

Слідство. Якщо на безлічі A визначена операція додавання (множення), то будь-які два рівності можна почленно складати (множити), тобто якщо $a=b$ і $c=d$, то $a+c=b+d$ і $c+a=d+d$ ($ac=bd$ і $ca=db$) [35].

Означення 1.1.7. Нехай (A,*) – алгебраїчна структура і $a,b,c \in A$. Кажуть, що алгебраїчна операція підкоряється закону скорочення зліва, якщо з рівності $a*b=a*c$ виконується рівність $b=c$ і кажуть, що алгебраїчна операція підкоряється закону скорочення справа, якщо з рівності $a*b=c*b$ виконується рівність $a=c$ [35].

Означення 1.1.8. Кажуть, що алгебраїчна операція підкоряється закону скорочення, якщо вона підкоряється закону скорочення як зліва, так і справа.

На множині A може бути задано багато різних алгебраїчних операцій. Якщо бажають виділити одну з них, наприклад *, то записують $(A, *)$ і вважають, що операція * визначає на множині M алгебраїчну структуру або що $(A, *)$ є алгебраїчною структурою [32].

Означення 1.1.9. Множина A, на якій задано одну або кілька алгебраїчних операцій, називається алгебраїчною структурою.

В математиці виділилося невелика кількість основних типів алгебраїчних структур, які докладно вивчаються: група, кільце, поле, лінійний простір. Вивчення цих структур і зв'язків між ними є одним з найважливіших завдань алгебри на сучасному етапі її розвитку [32].

Означення 1.1.10. Непорожня множина із визначеною в ній бінарною операцією, називається групоїдом. Групоїд, визначена в якому операція є асоціативною, називається півгрупою. Півгрупа, в якій існує одиничний (нейтральний) елемент, називається моноїдом. Одиничний елемент позначають e: для будь-якого $g \in G$ $[g * e = e * g = g]$. Моноїд, кожен елемент якого є оборотним, називається групою. Оборотним називається такий елемент множини, для якого в цій множині існує

обернений. Оберненим до елемента $g \in G$ називається такий елемент g^{-1} цієї ж множини, для якого

$$g * g^{-1} = g^{-1} * g = e \quad [11].$$

Означення 1.1.11. Повне означення групи: непорожня множина *G,* на якій визначено бінарну операцію , називається групою, якщо виконуються наступні умови:

1. операція асоціативна;

2. в множині *G* існує одиничний елемент;

3. кожний елемент множини *G* є оборотним.

Означення 1.1.12. Якщо операція, визначена в групі, є комутативною, то група *G* називається комутативною або абелевою [11].

Означення 1.1.13. Група *G* називається скінченною, якщо кількість її елементів (порядок групи) скінченна [32].

Приклади 1.1.1.

1. Множини цілих, раціональних та дійсних чисел відносно додавання: (Z,+), (Q,+), (R,+).

2. Множини додатніх раціональних, додатніх дійсних чисел відносно множення: (Q+,•), (R+,•).

3. Множини чисел 1 та -1 утворює групу відносно множення: ({1;-1},•).

4. Множини всіх підстановок *n*-го степеня відносно множення (симетрична група, позначають S_n та всіх парних підстановок *n*-го степеня відносно множення (знакозмінна група, позначають A_n [32].

Означення 1.1.14. Групу за додаванням називають адитивною, за множенням – мультиплікативною [32].

Означення 1.1.15. Непорожню підмножину *H* групи *G* називають підгрупою цієї групи, якщо *H* є групою відносно бінарної операції, визначеної в групі *G* [32].

Щоб встановити, чи непорожня підмножина H групи G є підгрупою групи G, потрібно перевірити:

1. чи містить підмножина H разом із будь-якими своїми елементами g_1 та g_2 і результат операції між ними, тобто елемент $g_1 * g_2$;

2. чи містить підмножина H разом із будь-яким своїм елементом g і обернений йому елемент g^{-1} [11].

Теорема 1.1.4. (про перетин підгруп). Якщо H_1 і H_2 – підгрупи групи G, то їх перетин $H_1 \cap H_2$ теж є підгрупою групи G [32].

Доведення.

Якщо елементи a та b належать перетину $H_1 \cap H_2$, то вони містяться в кожній з підгруп H_1 та H_2 , тому елементи ab та a^{-1} теж містяться в кожній з підгруп, а значить, і в їх перетині. Отже, $H_1 \cap H_2$ – теж підгрупа групи G [32].

Означення 1.1.16. Підгрупа, що складається з усіх степенів елемента $g \in G$, називається циклічною підгрупою групи G, породженою елементом g (позначається $<g>$) [32].

Означення 1.1.17. Група G називається циклічною, якщо вона складається тільки зі степенів одного із своїх елементів g, тобто збігається з однією із своїх циклічних підгруп $<g>$. Елемент g називають твірним елементом циклічної групи $<g>$. Кожна циклічна група є абелевою (оскільки множення її елементів зводиться до додавання показників степеня, яке є комутативним) [11].

Приклади 1.1. 2.

1. Адитивна група цілих чисел (Z,+) є нескінченою циклічною групою з твірним елементом 1 (можна -1).

2. Мультиплікативна група ({1;-1},•) є циклічною групою 2-го порядку з твірним елементом -1 [32].

Означення 1.1.18. Групи G і G_1 називаються ізоморфними, якщо між їх елементами можна встановити таку взаємно однозначну

відповідність, що якщо будь-яким елементам a, $b \in G$ відповідають деякі елементи a_1, $b_1 \in G_1$, то результату операції $a * b$ між елементами групи G відповідає результат операції $a_1 \circ b_1$ між відповідними елементами групи G_1 [32].

Тут $*$ – $\circ$ – позначення операції в групі G, $\circ$ – в групі G_1 [32].

Приклади 1.1.3.

1. Адитивна група Z цілих чисел ізоморфна адитивній групі G цілих чисел, кратних 5 (відображення $k \to 5k$, $k \in Z$). $(Z,+) \to (\{5k, k \in Z\},+)$.

2. Мультиплікативна група R+ додатних дійсних чисел ізоморфна адитивній групі R всіх дійсних чисел $(R_+,\bullet) \to (R,+)$ [32].

При ізоморфному відображенні груп G та G_1:

1. одиничний елемент групи G відображається в одиничний елемент групи G_1;

2. кожна пара взаємнообернених елементів g та g^{-1} групи G відображається у відповідну пару взаємнообернених елементів групи G_1 [32].

Означення 1.1.19. Непорожня множина K, на якій визначено операції додавання і множення, називається кільцем, якщо виконуються наступні умови:

1. множина K є адитивною абелевою групою;

2. множина K є мультиплікативною півгрупою;

3. операція множення є дистрибутивною відносно додавання, тобто

$\forall a,b,c \in K$ $[(a+b)c = ac+bc;\ c(a+b) = ca+cb]$ [32].

Позначається (К,+, •).

Означення 1.1.20. Кільце називають комутативним, якщо операція множення в кільці комутативна.

Приклади 1.1.4:

1. 1. Z,+, •), (Q,+, •), (R,+, •).

2. $(\{5k, k \in Z\},+,\bullet)$.

Означення 1.1.21. Ненульове кільце, яке містить одиничний елемент e, називають кільцем з одиницею [32].

Означення 1.1.22. Елементи a, b кільця K називаються дільниками нуля, якщо якщо $a \neq \theta$, $b \neq \theta$, але $ab = \theta$, де θ – нульовий елемент кільця [32].

Означення 1.1.23. Комутативне кільце з одиницею, в якому немає дільників нуля, називається цілісним кільцем (областю цілісності) [32].

Означення 1.1.24. Підмножина K_1 кільця K називається підкільцем кільця K, якщо K_1 є кільцем відносно операцій додавання і множення, визначених в кільці K. Кільце K при цьому називають розширенням кільця K_1 [32].

Щоб встановити, чи непорожня підмножина K_1 кільця K є його підкільцем, потрібно перевірити, чи різниця й добуток довільних двох елементів підмножини K_1 належить до K_1 [32].

Приклади 1.1.5.

1. Кільце парних чисел, кільце $(\{5k, k \in Z\},+,\bullet)$ – підкільця кільця (Z, +, •) цілих чисел.

2. Кільце (Z,+, •) цілих чисел – підкільце кільця (Q,+, •) раціональних чисел.

3. Кільце (Q,+, •) раціональних чисел – підкільце кільця (R,+, •) дійсних чисел [32].

Означення 1.1.25. Кільця K і K' називаються ізоморфними, якщо між їх елементами можна встановити таку взаємно однозначну відповідність, що для будь-яких елементів $a,b \in K$ і відповідних їм елементів $a',b' \in K'$ сумі $a+b$ відповідає сума $a'+b'$, добутку ab відповідає добуток $a'b'$ [11].

Означення 1.1.26. Комутативне кільце з одиницею, в якому кожен ненульовий елемент є оборотним, називається полем. Позначають (P, +, •).

Поле (P,+, •) являє собою поєднання в тій самій множині P двох абелевих груп – адитивної (P,+) та мультиплікативної (P\{0},•) [32].

Приклади 1.1.6.

1. Поле раціональних чисел (Q,+, •).

2. Поле дійсних чисел (R,+, •).

Очевидно, що жодне поле не має дільників нуля [32].

Означення 1.1.27. Характеристикою поля P називають:

- число нуль, якщо $ne=\theta$ лише при $n=0$;
- натуральне число p, якщо $pe = \theta$ і немає такого $k \in N$ меншого ніж p, що $ke = \theta$ [32].

Ясно, що ненульова характеристика p поля P є числом простим.

Означення 1.1.28. Підмножину P_1 поля P називають підполем цього поля, якщо вона сама є полем відносно бінарних операцій, визначених у полі P. Поле P при цьому називають розширенням поля P_1 [32].

Означення 1.1.29. Нехай A і K - довільні непусті безлічі. $K \times A$ – декартовій твір цих множин. Відображення $K \times A \to A$ називають зовнішньою бінарною алгебраїчною операцією, визначеної на множині A над безліччю K [35].

Іншими словами, кожній парі елементів $(\alpha; a)$ з декартова твори ставиться у відповідність єдиний для цієї пари елемент $\alpha * a \in A$. (Зазвичай при написанні результату алгебраїчної операції елемент $\alpha \in K$ пишеться зліва від елемента $a \in A$).

Приклад 1.1.7. Нехай R[x] - безліч многочленів від однієї змінної x з дійсними коефіцієнтами, R - поле дійсних чисел. Тоді операція множення многочлена на число є зовнішньої алгебраїчній операцією на

безлічі многочленів: $\mathrm{R}\times R[x]\to R[x]$, тобто в результаті знову виходить багаточлен з дійсними коефіцієнтами [35].

Приклад 1.1.8. Нехай - множина всіх векторів як спрямованих відрізків. Тоді множення вектора на число є зовнішня алгебраїчна операція на безлічі V: $\mathrm{R}\times V\to V$, так як в результаті виходить вектор (спрямований відрізок) [35].

Означення 1.1.30. Нехай - довільна множина, елементи якого ми будемо називати векторами, K - поле, елементи якого ми будемо називати скалярами. Нехай на безлічі v визначена внутрішня бінарна алгебраїчна операція, яку ми будемо позначати знаком + і називати складанням векторів. Нехай також на безлічі визначена зовнішня бінарна алгебраїчна операція над полем К, яку ми будемо називати множенням вектора на скаляр і позначати знаком множення. Іншими словами визначені два відображення:

$$V\times V\to V,\ \forall x,y\in V:\ (x,y)\to x+y\in V\ ;$$
$$K\times V\to V,\ \forall \lambda\in K,\ \forall x\in V:\ (\lambda,x)\to \lambda\cdot x\in V\ .$$
(1.1)

Означення 1.1.31. Безліч v разом з цими двома алгебраїчними операціями називають векторним простором над полем K, якщо ці операції алгебри підкоряються наступним законам (аксіоми векторного простору) [35].

1. Закон асоціативності додавання:

$$\forall x,y,z\in V:\ (x+y)+z=x+(y+z)\ .$$ (1.2)

2. Існування нульового вектора:

$$\exists' 0\in V':\ \forall x\in V\ \ x+0=0+x=x\ .$$

(1.3)

3. Існування протилежного вектора:

$$\forall x \in V, \exists (-x) \in V : x + (-x) = (-x) + x = 0 .$$

(1.4)

4. Закон комутативності складання:

$$\forall x, y \in V : x + y = y + x .$$

(1.5)

5. Закон асоціативності множення вектора на скаляр:

$$\forall \alpha, \beta \in K, \forall x \in V : (\alpha\beta)x = \alpha(\beta x) .$$

(1.6)

6. Закон дистрибутивності множення вектора на скаляр щодо додавання векторів:

$$\forall \lambda \in K, \forall x, y \in V : \lambda(x + y) = \lambda x + \lambda y .$$

(1.7)

7. Закон дистрибутивності множення вектора на скаляр щодо складання скалярів:

$$\forall \lambda, \mu \in K, \forall x \in V : (\lambda + \mu)x = \lambda x + \mu x .$$

(1.8)

8. $\forall x \in V : 1 \cdot x = x$, де 1 - це одиниця поля *K*.

Означення 1.1.32. Векторний простір v над полем дійсних чисел називається речовим векторних простором.

Теорема 1.1.5. (Прості властивості векторних просторів.)

1. У векторному просторі існує єдиний нульовий вектор.

2. У векторному просторі будь-який вектор має єдиний протилежний йому.

3. $\forall \lambda \in K, \forall x \in V : \lambda x = 0 \Leftrightarrow \lambda = 0$ або x = 0.

4. $\forall x \in V : (-1) \cdot x = -x$.

Доведення.

Векторний простір щодо складання утворює абелевих груп (аксіоми 1 - 4) звідки і слідують відразу ж перші два твердження теореми [35].

3) а) Спочатку ми доведемо, що твір нульового скаляра на будь-який вектор дорівнює нульовому вектору. Нехай $\lambda=0$. Тоді, застосовуючи аксіоми векторного простору, отримуємо:

$$0\cdot x+x=0\cdot x+1\cdot x=(0+1)\cdot x=1\cdot x=x=0+x \quad .$$

Застосовуючи закон скорочення, отримуємо $0\cdot x=0$.

б) Тепер доведемо твердження 4):

Нехай $x\in$ V - довільний вектор. Тоді

$$x+(-1)x=1\cdot x+(-1)x=(1+(-1))x=0\cdot x=0 \quad .$$

Звідси відразу ж випливає, що вектор (-1)x є протилежним вектору x.

в) Нехай тепер x=0. Тоді, застосовуючи аксіоми векторного простору,

$\forall\ y\in V$ отримуємо:

$$\lambda\cdot 0=\lambda\cdot(y+(-y))=\lambda\cdot y+\lambda\cdot(-y)=\lambda y+\lambda(-1)y=$$
$$=(\lambda+(-\lambda))y=0\cdot y=0 \quad .$$

(1.9)

г) Нехай $\lambda x=0$ і допустимо, що $\lambda\neq 0$. Так як $\lambda\in K$, де K – поле, то існує $\lambda^{-1}\in K$. Помножимо рівність $\lambda x=0$ зліва на λ^{-1}:

$\lambda^{-1}(\lambda x)=\lambda^{-1}\cdot 0=0$ звідки випливає $(\lambda^{-1}\lambda)x=0$, $1\cdot x=0$ і остаточно $x=0$. Теорема доведена.

Приклад 1.1.9. Позначимо через v безліч всіх векторів як спрямованих відрізків. Ми вже знаємо, що щодо додавання векторів безліч v є абелевою групою. Зі шкільного курсу геометрії нам відома ще одна операція з векторами - множення вектора на число, в результаті

якої виходить теж вектор. Значить ця операція є зовнішньої бінарної алгебраїчної операцією на безлічі v над полем дійсних чисел: $R \times V \to V$. Таким чином, безліч всіх векторів як спрямованих відрізків утворює речовий векторний простір.

1.2. Група A_n та її властивості

Означення 1.2.1. Група G називається простою, якщо G не має нетривіальних нормальних підгруп [4].

Очевидно, що простою буде кожна група простого порядку. Як випливає з леми Коші, серед абелевих груп інших простих немає. Неабелеві прості групи також існують, але вони влаштовані значно складніше [4].

Твердження 1.2.1. Кожна скінченна p–група G порядку $|G| > p$ не є простою [4].

Доведення.

Згідно теореми (Кожна скінченна неодинична p–група G має неодиничний центр) група G має неодиничний центр $Z(G)$, а за лемою Коші центр містить елемент порядку p. Тоді підгрупа ha і є нетривіальною підгрупою групи G, яка є нормальною. Тому G не є простою [4].

Задача 1.2.1. Доведіть, що кожна неабелева група порядку, меншого за 60, не є простою [4].

Вправа 1.2.1. Доведіть, що коли підгрупа H групи S_n містить непарні підстановки, то рівно половина її елементів буде парними підстановками, а половина — непарними [4].

Розглянемо один із прикладів простих груп, а саме:

Теорема 1.2.1. Група A_5 — проста.

Доведення.

Очевидно, що підстановка $b \in S_n$ належить нормалізатору $N_{An}(a)$ елемента $a \in A_n$ тоді й лише тоді, коли b належить нормалізатору $N_{Sn}(a)$ і є парною підстановкою. Отже, $N_{An}(a) = N_{Sn}(a)$, якщо $N_{Sn}(a)$ містить лише парні підстановки, і $|N_{A_n}(a)| = \frac{1}{2}|N_{S_n}(a)|$, якщо $N_{Sn}(a)$ містить також непарні підстановки (останнє випливає з вправи 1.2.1). За теоремою (Потужність класу спряженості $C_G(x)$ елемента x групи G дорівнює індексові його нормалізатора $N_G(x)$, тобто $|C_G(x)| = |G : N_G(x)|$)у першому випадку потужність $|C_{An}(a)| = |A_n : N_{An}(a)|$ класу $C_{An}(a)$ спряжених з a у групі A_n елементів вдвічі менша за потужність $|C_{Sn}(a)| = |S_n : N_{Sn}(a)|$ відповідного класу в групі S_n, а в другому випадку ці потужності рівні:

$$\left|A_n : N_{A_n}(a)\right| = \frac{\left|A_n\right|}{\left|N_{A_n}(a)\right|} = \frac{\frac{1}{2}\left|A_n\right|}{\frac{1}{2}\left|N_{A_n}(a)\right|} =$$

$$= \frac{\left|S_n\right|}{\left|N_{S_n}(a)\right|} = \left|S_n : N_{S_n}(a)\right| \qquad (1.10)$$

Група A_5, як нормальна підгрупа групи S_5, є об'єднанням класів спряженості групи S_5. Із доведеного вище випливає, що кожний клас спряжених елементів групи S_5, який міститься в A_5, або залишається класом спряжених елементів групи A_5, або розпадається в A_5 на два рівнопотужні класи. Група S_5 містить такі класи спряженості, що складаються з парних підстановок: клас $C(\varepsilon)$ потужності 1, клас $C((123))$ потужності 20, клас C((12)(34)) потужності 15 і клас C((12345)) потужності 24. Тому A_5 має один одноелементний клас спряженості, два класи по 10 елементів (або замість них один 20–елементний), один 15–елементний і два класи по 12 елементів (24–елементний клас спряженості група A_5 мати не може, бо її порядок не ділиться на 24). Якщо H — нормальна підгрупа A_5, то H є об'єднанням класів спряженості групи A_5 і містить $C(\varepsilon)$. Крім того, за теоремою Лагранжа, порядок підгрупи H повинен ділити число $|A_5| = 60$. Але сума

потужностей будь–якого нетривіального набору класів спряженості групи A_5, який містить клас $C(\varepsilon)$, не є дільником числа 60. Тому підгрупа H є тривіальною, а група A_5 — простою [4].

Зауваження. 1.2.1. Ґалуа довів, що простими є всі групи A_n, $n \geq 5$. Тому існує нескінченно багато простих некомутативних скінченних груп [4].

Але такі групи далеко не вичерпуються знакозмінними, хоча фактом, відомим ще Ґалуа, є той, що група A_5 серед таких груп має найменший порядок.

2. Той факт, що група A_n є простою для всіх $n \geq 5$ є дуже важливим, бо, як показав той же Ґалуа, з нього випливає не тільки неіснування загальної алгебричної формули для знаходження коренів многочлена степеня $n \geq 5$, а й нерозв'язність у радикалах багатьох конкретних рівнянь [4].

Задача 1.2.2. Доведіть, що кожна група порядку pq, де p і q — не обов'язково різні прості числа, не є простою [4].

Зауваження 1.2.2. Іншими важливими прикладами простих груп є $SO(3)$ і серія проективних спеціальних лінійних груп $PSL_n(F)$ над полем F. Група $SO(3)$ — це група всіх дійсних матриць порядку 3 з визначником рівним 1, обернена до кожної з яких збігається з її транспонованою, тобто

$$SO(3) = \{A \in M_3(\mathrm{R}) | A^T \cdot A = A \cdot A^T = E, \det A = 1\}.$$

Означення 1.2.1. А проективна спеціальна лінійна група $PSL_n(F)$ — це факторгрупа спеціальної лінійної групи $SL_n(F)$ за її центром — підгрупою скалярних матриць (тобто матриць виду λE). Групи $PSL_n(F)$ були введені Жорданом (1870 р.). Він же і встановив, що, за вийнятком $PSL_2(2)$ і $PSL_2(3)$, ці групи є простими (недоліки доведення Жордана були пізніше виправлені Діксоном) [4].

Задача 1.2.3. Доведіть, що група $GL_3(\mathrm{Z}2)$ є простою.

Зауваження 1.2.3. Свою назву прості групи отримали завдяки тому, що вивчення групи G з нетривіальною нормальною підгрупою H у певному сенсі можна звести до вивчення “менших” чи “простіших” груп H і $G_1 = G/H$ (говорять, що група G одержується розширенням групи H за допомогою групи G_1). Принаймні у скінченному випадку групи H і G_1 справді простіші, бо мають менший порядок. Тому прості групи — це ті найменші “цеглинки”, з яких за допомогою розширень можна будувати інші групи. Довгий час задача класифікації простих груп була актуальною. Вважається, що у певному сенсі класифікація простих скінченних груп була завершена в лютому 1981 року. Існуюче доведення, об’єм якого займає від 5000 до 10000 журнальних сторінок, об’єднав результати декількох сотень математиків усього світу за 30 років із 300-500 індивідуальних робіт. Хоча вважається, що всі скінченні прості групи вже відомі, проте повного доведення досі немає. Тому чи є класифікація скінченних простих груп великим міфом XX сторіччя, чи — реальністю, все ще відповісти важко [4].

РОЗДІЛ 2
ТЕОРЕМИ СИЛОВА

2.1. Перша теорема

Теорема Лагранжа накладає на порядки підгруп скінченної групи необхідні умови. Але, як показує вже приклад групи A_4, (Доведіть, що для кожного дільника k числа 24 група S_4 містить підгрупу порядку k.

Доведіть, що група A_4 не містить підгруп порядку 6*)*, що не містить підгрупи порядку 6, ці умові не є достатніми.

Задача 2.1.1. Доведіть, що група A_5 не містить підгруп порядків 15*,* 20 *і* 30.

Вказівка. Скористаймося тим, що дія групи A_5 правими зсувами на правих класах суміжності за підгрупою одного із вказаних порядків матиме нетривіальне ядро.

З іншого боку, лема Коші дає достатні умови існування підгрупи простого порядку. У 1872 р. норвезький математик Силов значно посилив результат Коші, довівши, що коли дільник d порядку групи є степенем простого числа, то підгрупа порядку d існує. Крім того, Силов описав багато цікавих властивостей таких груп [33].

Надалі вважатимемо, що p є фіксованим простим числом.

Одним з яскравих результатів теорії кінцевих груп в напрямку часткового звернення теореми Лагранжа є наступні три теореми Силова (1872) [33].

Теорема 2.1.1. (перша теорема Силова про існування сіловских підгруп).

Сіловські p-підгрупи існують.

Доведемо теорему індукцією один по одному G. При | G | = P теорема вірна. Нехай тепер | G | > P. Нехай Z (G) - центр групи G. Можливі два випадки:

Нехай G-скінчена група, $|G| = n = p^k m$, $k \geq 1$, p —прості числа, (p,m) = 1. Тоді група G містить підгрупу H таку, що $|H| = p^k$ (така підгрупа називається сіловською підгрупою групи G) [33].

Доведення.

1) Якщо G - абелева група, $|G| = p^k m$, $(p,m) = 1$,то в якості H можна взяти примарну компоненту G_p групи G (тобто пряму суму всіх p-примарний циклічних груп канонічного розкладання), і тоді $G_p = p^k$ [33].

2) Якщо |G| = pk (тобто m = 1), то G = H.

3) Проведемо доказ индуктивно.

Випадок 2.1.1. p ділить число$|\mathbf{Z}(G)|$ елементів центру $\mathbf{Z}(G)$ групи G. Зі звернення теореми Лагранжа для абелевих груп знайдеться підгрупа A в центрі $\mathbf{Z}(G)$, $|A| = p$. Зрозуміло, що $A \subset G$, $|G/A| = n/p = p^{k-1}m < n$. В силу індуктивного припущення в $\bar{G} = G/A$ знайдеться підгрупа $\bar{B}$, $|\bar{B}| = p^{k-1}$. Але $\bar{B} = B/A \subset G/A$, де $A \subseteq B \subseteq G$, тому $|B| = |A||B/A| = pp^{k-1} = p^k$, тобто B — силовська підгрупа групи G [33].

Випадок 2.1.2. p поділяє порядок |Z(G)| центру Z(G) групи G.

Розглянемо розкладання групи на класи пов'язаних елементів $G = \sum^{S} C_i$. Нехай $C_1,\ldots,C_r$ — одноелементні класи пов'язаних елементів (тобто всі елементи центру $\mathbf{Z}(G)$, $r = |\mathbf{Z}(G)|$). Так як | G | ділиться на p, а число r не ділиться на p, знайдеться орбіта $C_i = \mathrm{Orb}(x_i)$, $r + 1 \leq i \leq l$, така, що $|G|/|C(x_i)| = |C_i|$ не ділиться на p. Тоді $|C(x_i)| < n$, але по індуктивному припущенню в C(xi) знайдеться підгрупа H така, що |H| = pk, тобто H — силовська підгрупа групи G (H ⊆ C(xi) ⊆ G) [33].

2.2. Друга теорема

Означення 2.2.1. Максимальна по вкладенню *p*-підгрупа скінченої групи *G* називається силовською *p*-підгрупою групи *G*. З доведеної теореми випливає зокрема, що силовскі *p*-підгрупи кінцевої групи, це в точності підгрупи порядку p^t де p^t - максимальний ступінь *p* ділить порядок групи [34].

Теорема 2.2.1. (Друга теорема Силова)

(Спряженість) Всі силовскі *p* - підгрупи групи *G* пов'язані.

Доведення.

Нехай *P* - Силовська підгрупа, якщо $|G| = p^t m$, де НОД*(p,m)*=1, то $|P| = p^t$. Нехай, Δ як і раніше клас підгруп, пов'язаних з *P* елементами з *G*. Покажемо, що якщо *Q* симетрична *p* - підгрупа, то *QÎ*Δ. З теореми (Якщо *M* - підмножина, *H* - підгрупа групи *G,* то потужність класу підмножин, пов'язаних з *M* елементами з *H,* дорівнює індексу $|H : N_H(M)|$. Зокрема $|a^G| = |G : N_G(a)|$.) маємо

$$\Delta | = |G : N_G(P)| \text{ [34]}. \qquad (2.1)$$

По теоремі Лагранжа, отримуємо:

$$|G| = |N_G(P)| \cdot |G : N_G(p)| = |N_G(P)| \cdot |\Delta|$$

$$= (P \subset N_G(P) = |P| \cdot |P \div N_G(P)| \cdot |\Delta| = |P| \cdot |\Delta| \cdot |N_G(p)/P|, \quad \text{НСД}(|\Delta|, p),$$

звідки $p^t m = p^t \cdot |\Delta| \cdot |N_G(P)/P|$ і, отже, розіб'ємо Δ на підкласи підгруп пов'язаних між собою елементами з *Q*: $\Delta = \Delta_1 È \Delta_2 \ldots È \Delta_k$

Якщо підгрупа $S Î \Delta_i$, то $|\Delta| = |Q : N_Q(S)| = p^{\alpha_i}$, $\alpha_i \geq 0$ [34].

Отже, $|\Delta| = p^{\alpha_1} + p^{\alpha_2} + \ldots p^{\alpha_k}$.

(2.2)

Звідси так як НСД(Δ $|,p)=1$, то існує *i* таке що $\alpha^i=0$ і $\Delta_i=\{S\}$. Таким чином, $S^q=S$ и, значить, $Q\subset N_G(S)$. Тоді за пропозицією (*H и K* підгрупи групи *G* і $K\subset N_G(H)$, тоді HK являється підгрупой групи G, $HK=KH$ і $H\lhd HK$) $QS=SQ$ підгрупа групи *G*, $S\lhd QS$. Застосовуя теорему (об изоморфизме) отримуємо: $QS/S\cong Q/Q\cap S$. Звідки отримуєм $|QS|=|S|\cdot|QS/S|=|S|\cdot|Q/Q\cap S|=p^t\cdot p^\alpha=p^{t+\alpha}$. Отже, за теоремою Лагранжа порядок *G* ділитися $p^{t+\alpha}$, але *t* - максимальна ступінь числа *p,* тому $\alpha=0$ і $Q\cap S=Q$. Звідси випливає: $Q\subset S$ і значить $Q=S$ (так як $|Q|=|S|=p^t$). І так $Q=S\subset\Delta$, що і требовалось довести [34].

2.3. Третя теорема

Теорема 2.3.1. (третя теорема Силова про кількість силовських підгруп). Нехай G-кінцева $n=|G|=p^km$, $k\geq 1$, $(p,m)=1$.

Через *n (p)* позначимо число силовськіи *p*-підгруп. тоді:

$n(p)$ — дільник числа $n=|G|$;

$n(p)=1+pq$ (тобто залишок при діленні числа *n (p)* на просте число *p* дорівнює 1) [34].

Доведення.

1) Розглянемо ліве дію групою *G*

$$M_G=L(G)=\{H\mid H\subseteq G\},$$
$$(H,g)\to gHg^{-1},\quad g\in G$$

(тобто група *G* діє на множині всіх підгруп *H* групи *G* сполученням). В силу другий теореми Силова всі силовські *p*-підгрупи утворюють одну з орбіт Orb(*S*) в M_G, де *S* - одна з силовських підгруп групи *G*, $n(p)=|$

Orb(S)|. Так як $|G| = |\mathrm{St}(S)| \cdot |\mathrm{Orb}(S)|$, то ясно, що $n(p) = |\mathrm{Orb}(S)|$ — дільник числа

$n = |G|$ [34].

2) Розглянемо тепер безліч всіх силовських p-підгруп $\Sigma_{S1} = \{S_1,\ldots,S_{n(p)}\}_{S1}$ як лівий S_1-полігон(тут $S = S_1$) зі сполученням:

$$(a,S_i) \to aS_ia^{-1}, \qquad S_i \in \Sigma, a \in S_1$$

(ясно, що $|aS_ia^{-1}| = |S_i| = p^k$, тобто $aS_ia^{-1} \in \Sigma$).

а) Ясно, що $aS_1a^{-1} = S_1$ для $a \in S_1$, тобто S_1 — нерухома точка в Σ при дії групи S_1 ((т. е. одноелементна орбіта в Σ_{S1}). Покажемо, що S_1 - єдина нерухома точка [34].

Дійсно, припустимо противне, тобто що $|\mathrm{Orb}(S_i)| = 1$ для i 6= 1, т.обто $aS_ia^{-1} = S_i$ для всіх $a \in S_1$. Отже, $S_1S_i = S_iS_1$, і тому підмножина $H = S_iS_1 = S_1S_i$ являється підгрупою [34].

По теоремі Лагранжа для підгрупи H маємо: $|G| = |H| \cdot [G : H]$, таким чином, S_1 і S_i також є силовську p-підгрупами і в групі H; застосовуючи до них в групі H другу теорему Силова, отримуємо, що $S_1 = hS_ih^{-1}$ для $h = ab \in H = S_1S_i$, $a \in S_1$, $b \in S_i$ [34].

Але тоді $S_I = hSih{-}1 = (ba)Si(ba){-}1 = b(aSia{-}1)b{-}1 = bSib{-}1 = Si$ (тут ми використовували рівність $aS_ia^{-1} = S_i$, оскільки Si - орбіта, що складається з одного елемента), але це суперечить тому, що $i > 1$, тобто S_i 6= S_1 [34].

б) Завершення докази третьої теореми Силова. Отже, розглядаючи для полігону $\Sigma_{S1} = \{S_1,\ldots,S_{n(p)}\}$ розбиття на орбіти, маємо єдину одноелементна орбіту $\mathrm{Orb}(S_1) = \{S_1\}$, при цьому при i> 1 для інших орбіт (що містять більше одного елемента) $p^k = |S_1| = |\mathrm{St}(S_i)||\mathrm{Orb}(S_i)|$, тобто число елементів в цих орбітах ділиться на p (як дільник числа p^k) [34].

Таким чином,

$$n(p) = 1 + pq. \tag{2.3}$$

2.4. Наслідки з теореми Силова

Слідство 2.4.1. У кінцевій групі Силовська *p*-група єдина (тобто N (p) = 1) тоді і тільки тоді, коли ця Силовська підгрупа є нормальною підгрупою [34].

Слідство 2.4.2. (звернення теореми Лагранжа для кінцевих *p*-груп). Нехай G-кінцева *p*-група, | G | = p^k. Тоді для будь-якого дільника p^l, $l \le k$ числа p^k існує підгрупа *H* групи *G* така, що $|H| = p$. *[34].*

Доведення (індукцією по *k*). Випадок *k = 0* ясний. Нехай

$$|G| = p^k > 1.$$

В силу теореми про центр *Z (G) p*-групи *G*: $|\mathbf{Z}(G)| > 1$. В силу слідства з структурної теореми для кінцевої абелевих групи *Z (G)* має місце звернення теореми Лагранжа. Зокрема, для дільника *p* числа $p^l = |H|$ знайдеться циклічна підгрупа (c) з *p* елементів в групі *Z (G).* Зрозуміло, що(*c*) C *G.* Тоді для фактор-групи $\bar{G} = G/(c)$ має:

$$|\bar{G}| = |G|/p = p^{k-1} \text{ [34].} \qquad (2.4)$$

В силу індуктивного припущення (так як $p^{k-1} < p^k$) в $\bar{G}$ знайдеться підгрупа $\bar{H}$ така, що $|\bar{H}| = p^{l-1}$, при цьому $\bar{H} = H/(c)$, де *H* — підгрупа групи *G* така, що $(c) \subseteq H \subset G$. Так як $|H| = |\bar{H}||(c)| = p^{l-1} \cdot p = p^l$, то підгрупа *H* є шуканою [34].

Слідство 2.4.3. Якщо *M C G* і P -силовська *p*-підгрупа групи *M,* $\mathbf{N}_G(P)$ — нормалізатор підгрупи *P в G,* то $M \cdot \mathbf{N}_G(P) = G$ [34].

Доведення.

Нехай g ∈ G. Тоді $gPg^{-1} \subseteq gMg^{-1} = M$, тому *P* і gPg^{-1} — дві силовські *p*-підгрупи групи *M*. За другою теоремою Силова підгрупи *P* і gPg^{-1} пов'язані з допомогою елемента $h \in M$, $hPh^{-1} = gPg^{-1}$, тому $g{-}1hP(g{-}1h){-}1 = P$. Таким чином, $g^{-1}h \in \mathbf{N}_G(P)$, і тому $g = hh^{-1}g = h(g^{-1}h) \in M \cdot \mathbf{N}_G(P)$. Отже,

$$M \cdot \mathbf{N}_G(P) = G \quad [34]. \qquad (2.5)$$

РОЗДІЛ 3
ЗАСТОСУВАННЯ ТЕОРЕМ СИЛОВА

Лемма 3.1. Не існує неабелевих простих груп G порядку$|G| = p^l m$, де p - просте число, p поділяє m, p^l поділяє$(m - 1)!$ [35].

Доведення.

Припустимо противне, нехай G - така група. Тоді G містить сіловську p-підгрупу S, $|S| = p^l$, $(G : S) = m$. Так як кінцеві неабелева p-групи не є простими (центр є нетривіальною нормальної підгрупою), то можна вважати, що $m > 1$. Зрозуміло (дія на безлічі суміжних класів G по S), що існує гомоморфізм ϕ: $G \to \mathbf{S}m$ такої, що $ker\phi \subseteq S$. Так як G — проста група, то $ker\phi = \{e\}$, тобто ϕ — ін'єкція. Тому $G \cong \phi(G) \subseteq \mathbf{S}m$. За теоремоу Лагранжа $plm \mid m!$, отже, $pl \mid (m - 1)!$, що суперечить нашим припущенням [35].

Лемма 3.2. Якщо p -просте число, G - скінчена p-група і $| G | > P$, то група G не є простою [35].

Доведення.

Центр $Z(G)$ нетривіальний, при цьому $Z(G) \subset G$.

Якщо $Z(G) \neq G$, то група G не є простою.

Якщо $Z(G) = G$, то G - абелева група. Якщо вона проста, то $| G | = P$, що суперечить нашим припущенням [35].

Теорема 3.1. Серед скінчених груп G, порядок яких менше ніж 60, $| G | <60$, немає неабелевих простих груп [35].

Доведення.

В силу двох попередніх лем з чисел 2,3, ..., 59 треба розглянути лише випадки $n = | G | = 30,40,56$.

а) Нехай є проста група G, $n = | G | = 30 = 2 \cdot 3 \cdot 5$. Нехай S – силовська 5-підгрупа простої групи G, | S | = 5. Число r_5 пов'язаних силовських 5-підгруп (як дільник 30 і $r_5 \equiv 1 \pmod 5$) дорівнює 1 або 6.

Але якщо $r_5 = 1$, то *SCG,* що суперечить простоті групи *G*. Отже, $r_5 = 6$, при цьому перетин будь-яких двох різних силовських 5-підгруп з п'яти елементів кожна дорівнює {e}. Отже, їх об'єднання містить 24 непоодиноких елемента [35].

Аналогічно число r_3 силовських 3-підгруп дорівнює 10 (r_3 6 = 1, r_3 - дільник 30, r_3 3 ≡ 1 (mod 3)), в їх об'єднанні 20 непоодиноких елементів [35].

Так як 24 + 20 = 44> 30, то отримуємо протиріччя. Отже, група *G* 〖 | *G* | = 30 не може бути простою [35].

б) Нехай є проста група *G, n* = | *G* | = 40 = $2^3 \cdot 5$. Нехай *S* - силовська 5-підгрупа групи *G*. Оскільки r_5= 1 (r | 40, r ≡ 1 (mod 5)), то *P C G,* і тому група *G* не може бути простою [35].

в) Нехай є проста група *G, n* = | *G* | = 56 = $2^3 \cdot 7$. Нехай *S* - силовська 7-підгрупа групи *G*. Оскільки r_7 = 8 (r_7 | 56, r_7 ≡ 1 (mod 7)) і перетин будь-яких двох різних підгруп з семи елементів дорівнює {e}, то їх об'єднання містить 48 непоодиноких елементів [35].

Силовська 2-підгрупа містить вісім елементів, тому 48 + 8 = 56 = | G |, але $r_8 > 1$ (якщо $r_8 = 1$, то ця силовська підгрупа з восьми елементів нормальна, що суперечить простоті нашої групи *G*), однак для непоодиноких елементів другий силовської 2-підгрупи в нашому балансі підрахунку елементів вже немає місця. Отримали протиріччя [35].

ВИСНОВКИ

У роботі Супруненко [37], присвяченій дослідженню р-груп повної лінійної групи над алгебраїчно замкненим полем нульової характеристики, було доведено, що для кожного простого р р-іодичні групи Силова повної лінійної групи спряжні в ній; при цьому в роботі було наведено їх повний опис.

В процесі виконання даної дипломної роботи були виконані всі поставлені завдання, а саме у першому розділі були зібрані допоміжні поняття і теореми, які використовуються в дипломній роботі.

У другому розділі доводяться теореми Силова, що в теорії скінчених груп максимальні *p*- підгрупи також грають істотну роль. В роботі були доведені теоремі Силова про скінчені групи: для кожного ступеня, що ділить порядок групи, то будь-яка підгрупа порядку, причому якщо ділить порядок групи, то будь-яка підгрупа порядку, всі максимальні *p* - підргупи попарно сполучені в групі, а їх число порівняло з 1 по модулю *p*. Ця теорема була доведена норвезьким математиком Л. Силовим в 1972 році. У зв'язку з цією теоремою і в честь її автора максимальні *p* - підгрупи скінчених (а частоі нескінчених) груп називаються силовськими *p* – підгрупами.

З теоремі Силова випливає, в часності, що силовські *p* - підгрупи скінченої підгрупи - це в точності підгрупи порядку, де максимальна ступінь *p*, що ділить порядок групи. Відзначимо, що якщо число *m* ділить порядок кінцевої групи *G*, але не є ступінь простого числа, то в *G* може і не бути підгруп прядка *m* - наприклад, в знакозмінної групі А4 близько 12 немає підгруп порядку 6. У теорії груп теореми Силова є неповний варіант зворотної теореми до теореми Лагранжа і для деяких дільників порядку групи *G* гарантують існування підгруп такого порядку.

В третьому розділі наведені приклади застосування теорем Силова тим самим мета роботи досягнута.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Акимов О.Е. Дискретная математика: логика, группы, графы. М.: Лаборатория базовых знаний, 2001 – 352 с.: ил.

2. Бахтурин Ю. А. Основные структуры современной алгебры. М.: Наука, 1990. 320 с.; Калуж-нинЛ. А. Введение в общую алгебру. М.: Наука, 1973. 448 с.; Курош А. Г. Лекции по общей алгебре. М.: Наука, 1970. Мальцев А. И. Алгебраические системы. М.: Наука, 1970. 392 с.; Общая алгебра / под общ. ред. Л. А. Скорнякова. М.: Наука, 1990. Т. 1; 1991. 592 с., Т. 2. 480 с.; Скорняков Л. А. Элементы алгебры. М.: Наука, 1986. 240 с.; Он же. Элементы общей алгебры. М.: Наука, 1983. 272 с.; Фрид Э. Элементарное введение в абстрактную алгебру. М.: Мир, 1979. 262 с.

3. БелоусовА.И., Ткачев С.Б.. Дискретная математика: Учеб. для вузов / Под ред. В.С. Зарубина, А.П. Крищенко. – 3-е изд., стереотип. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2004. – 744 с.

4. Беклемишев Д. В. Курс аналитической геометрии и линейной алгебры: Учебник для вузов. М.: Физматлит, 2008.

5. Биркгоф Г., Барти Т. Современная прикладная алгебра - Издательство «Мир», Москва, 1976 – 400 с.

6. Бурбаки Н., Алгебра, Многочлены и поля. Упорядоченные группы, пер. с франц., М., 1965.

7. Варпаховский Ф.Л. и др. Алгебра. Группы, кольца, поля. Векторные и евклидовы пространства. Линейные отображения. - Учебное пособие. - М.: Просвещение, 1978 .

8. Ван дер Варден Б.Л. Алгебра / Ван дер Варден Б.Л. – М.: Наука, Главная редакция физико-математической литературы, 1979. - 623 с.

9. Ван дер Варден Б., Алгебра, пер. с нем., М., 1976.

10. Винберг Э.Б. Курс алгебры. - М.: Факториал, 1999. – 528 с.

11. Волошина Т.В. Основні алгебраїчні структури: курс лекцій / Волошина Т.В. // Луцьк: Вежа-Друк, 2015.– 58 с. – Режим доступа: https://fisfm.education/content/files/bd/fa/bdfafnfp5iejwqnkfhee5bq5k36r3gp4.pdf.

12. Ганюшкін О.Г. Теорія груп: навчальний посібник / О.Г. Ганюшкін, О.О. Безущак. — К.: Видавничо-поліграфічний центр «Київський університет», 2005. — 127 с.

13. Ганюшкін О.Г. Завдання до практичних занять з алгебри і теорії чисел / О.Г.

14. Галуа Э., Сочинения, пер. с франц., М.-Л., 1936.

15. Группы, кольца, поля: Методические указания по дисциплине «Геометрия и алгебра» / Сост. И. Г. Зельвенский; ГЭТУ «ЛЭТИ». СПб., 1997.

16. Каргаполов М. И. Основы теории групп / М. И. Каргаполов, Ю.И. Мерзляков. – М.: Наука, 1977. — 240 с. 10. Кострикин А.И. Введение в алгебру / Кострикин А.И. – М.: Наука, 1977. — 400 с. 11. Курош А.Г. Теория групп / Курош А.Г. – М.: Наука, 1967. —648 с.

17. Каргополов М.И, Мерзляков Ю.И. Основы теории групп. - М.: Наука, 1982.

18. Кострикин А.И. Сборник задач по алгебре. – Учебник для вузов. – М.: ФИЗМАЛИТ, 2001.

19. Кон П. Универсальная алгебра. М.: Мир, 1968. 352 с.; Цаленко М. Ш., Шульгейфер Е. Г. Основы теории категорий. М.: Наука, 1974. 256 с.

20. Кострикин А.И. Введение в алгебру. Часть III. Основные структуры алгебры. - Учебник для вузов. - М.: Физико-математичекая литература, 2001.

21. Кох Г., Теория Галуа p-расширений, пер. с нем., М., 1973.

22. Кострикин А. И. Введение в алгебру: Учебник для ун-тов. М.: Наука, 1977.

23. Курош А.Г. Курс высшей алгебры. - М.: Наука, 1965.

24. Курош А.Г. Теория групп. - М.: Гостехиздат, 1953.

25. Ларин С.В. Лекции по теории групп. - Красноярск, 1994.

26. Ленг С. Алгебра. – М.: Мир, 1968.

27. Ляпин Е.С. и др. Упражнения по теории групп. – М.: Наука, 1967.

28. Оре О. Графы и их применения - Издательство "Мир", Москва, 1965 – 172 с.

29. Фадеев Д.К. Лекции по алгебре. – Учебное пособие для вузов. – М.: Наука, 1984.

30. Холл М. Теория групп. – М.: ИЛ, 1962.

31. Чеботарев Н. Г., Основы теории Галуа, ч. 1 -2, М.-Л., 1934-37.

32. https://studfile.net/preview/5258839/page:4/.

33. https://halgebra.math.msu.su › wiki › lib › exe › fetch.php › lecture10.

34. http://halgebra.math.msu.su/wiki/lib/exe/fetch.php/staff:bunina:lecture9.pdf.

35. https://studfile.net/preview/3814070/.

36.https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BE%D1%80%D0%B8%D1%8F_%D0%B3%D1%80%D1%83%D0%BF%D0%BF.

37. Супрун е н к о Д. А., Линейные р-группы, Доклады АН БССР, т. 4, № 6 (1960), 233—235.