Київський національний університет імені Тараса Шевченка

О.Г.Ганюшкін, О.О.Безущак

ТЕОРІЯ ГРУП

Навчальний посібник
для студентів механіко – математичного факультету

Київ
Видавничо–поліграфічний центр
"Київський університет"
2005

О.Г.Ганюшкін, О.О.Безущак. Теорія груп: Навчальний посібник для студентів механіко – математичного факультету. – К.: Видавничо–поліграфічний центр “Київський університет”, 2005. – с.

Рецензенти: д-р фіз.-мат. наук, проф., А.П.Петравчук
канд. фіз.-мат. наук, доц., Ю.В.Боднарчук

Наведено .

Рекомендовано до друку вченою радою механіко – математичного факультету Київського національного університету імені Тараса Шевченка (протокол № від року)

Зміст

Позначення **5**

Передмова **8**

Вступ **9**

1 Множини з діями **12**

2 Ізоморфізм **16**

3 Напівгрупи **19**

4 Групи **22**

5 Підструктури **26**

6 Циклічні групи та порядок елемента **30**

7 Ізоморфізм груп **32**

8 Гомоморфізми **37**

9 Класи суміжності і нормальні підгрупи **39**

10 Факторструктури **46**

11 Спряженість **54**

12 Решітка підгруп і теореми про ізоморфізм **62**

13 Вільні групи **64**

14 Задання групи твірними і співвідношеннями **70**

15 p–групи **72**

16 Комутант **74**

17 Прості групи **76**

18 Дія групи на множині **79**

19 Теореми Силова **92**

20 Прямий добуток груп **96**

21 Періодичні групи **103**

22 Абелеві групи **105**

23 Розв'язні групи **114**

24 Мультиплікативна група поля, дискретний логарифм і криптографічні протоколи **118**

Література **122**

Позначення

$|a|$ — порядок елемента a; 31

$\langle a \rangle$ — циклічна група (скінченна або нескінченна) з твірним a; 31

$[a, b]$ — комутатор $a^{-1}b^{-1}ab$ елементів a і b; 74

$A * B = \{a * b \mid a \in A, b \in B\}$ — добуток непорожніх підмножин A та B напівгрупи (групи) $(S; *)$; 21

$A \subset B$ — множина A є власною підмножиною множини B; 56

$A \subseteq B$ — множина A є підмножиною множини B; 26

$\langle a, b, \ldots, c \rangle$ — група, породжена елементами $a, b, \ldots, c$; 28

A_n — знакозмінна група — група всіх парних підстановок степеня n; 23

арн ω — арність дії ω; 12

$\operatorname{Aut} G$ — група всіх автоморфізмів групи G; 36

$\mathbb{C}$ — множина (або адитивна група, або поле) комплексних чисел; 22

$\mathbb{C}^*$ — мультиплікативна група поля комплексних чисел; 22

C_∞ — нескінченна циклічна група; 34

$\mathbb{C}_\infty$ — група за множенням усіх комплексних коренів з 1 усіх можливих натуральних степенів; 22

$C_G(a)$ (або $C(a)$) — клас спряженості елемента a групи G; 55

C_n — циклічна група порядку n; 34

$\mathbb{C}_n$ — група за множенням усіх комплексних коренів степеня n з 1; 22

$\mathbb{C}_{p^\infty}$ — група за множенням усіх комплексних коренів з 1 степеня p^n, де просте число p — фіксоване, а натуральне число n — довільне; 22

D_n — діедральна група — група всіх рухів правильного n–кутника; 23

$D_n(P)$ — діагональна група — група за множенням усіх невироджених діагональних матриць порядку n з коефіцієнтами з поля P; 23

$\{e\}$ (або E) — одинична підгрупа групи G; 27

e_G (або просто e) — одиничний (нейтральний) елемент групи G; 22

$F(X)$ — вільна група з системою твірних X; 65

$F_n(X)$ (або F_n) — вільна група рангу n; 66

$|G|$ — порядок групи G; 22

$G' = [G, G]$ — комутант (похідна підгрупа) групи G; 75

G/H — факторгрупа групи G за нормальною підгрупою H; 52

$GL_n(P)$ — повна лінійна група порядку n з коефіцієнтами з поля P — група за множенням усіх невироджених матриць порядку n з коефіцієнтами з поля P; 22

$H < G$ — власна підгрупа H групи G; 27

$H \leq G$ — підгрупа H групи G; 27

$H \lhd G$ — нормальна підгрупа H групи G; 43

$\operatorname{Im}\varphi$ — образ гомоморфізму φ; 39

$\operatorname{Inn} G$ — група всіх внутрішніх автоморфізмів групи G; 61

K_4 — четверна група Кляйна — група підстановок $\{\varepsilon, (12)(34), (13)(24), (14)(23)\}$; 23

$\operatorname{Ker}\varphi$ — ядро гомоморфізму φ; 39

$(M;\circ) \simeq (N;*)$ (або $M \simeq N$) — алгебричні системи $(M;\circ)$ та $(N;*)$ ізоморфні; 16

$M_n(P)$ — множина матриць порядку n з коефіцієнтами з поля P; 14

$\mathbb{N}$ — множина (або адитивна напівгрупа) натуральних чисел; 21

$N_G(A)$ (або $N(A)$) — нормалізатор підмножини A групи G; 58

$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$; 35

O — група всіх поворотів куба; 80

O_n — ортогональна група — група за множенням усіх ортогональних матриць порядку n; 22

P^n — арифметичний векторний простір над полем P; 13

$P[x_1, \ldots, x_n]$ — кільце многочленів від змінних $x_1, \ldots, x_n$ з коефіцієнтами з поля P; **??**

$\mathbb{Q}$ — множина (або адитивна група, або поле) раціональних чисел;22

$\mathbb{Q}^+$ — множина (або мультиплікативна група) всіх додатних раціональних чисел; 17

$\mathbb{Q}^*$ — мультиплікативна група поля раціональних чисел; 22

Q_8 — група кватерніонів — група, породжена кватерніонними одиницями i, j, k, де $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$; 24

$\mathbb{R}$ — множина (або адитивна група, або поле) дійсних чисел; 17

$\mathbb{R}^+$ — множина (або мультиплікативна група) всіх додатних дійсних чисел; 17

$\mathbb{R}^*$ — мультиплікативна група поля дійсних чисел; 22

$SL_n(P)$ — спеціальна лінійна група порядку n з коефіцієнтами з поля P — підгрупа тих матриць із $GL_n(P)$, визначник яких дорівнює 1; 22

S_n — симетрична група степеня n — група всіх підстановок множини $\{1, \ldots, n\}$; 23

$St_G(m)$ (або $St(m)$) — стабілізатор в групі G точки $m \in M$; 83

T — мультиплікативна група комплексних чисел, модуль яких дорівнює 1; 22

$T_n(P)$ — трикутна група порядку n з коефіцієнтами з поля P — група за множенням усіх невироджених верхніх трикутних матриць порядку n з коефіцієнтами з поля P; 23

U_n — унітарна група порядку n — група за множенням усіх унітарних матриць порядку n; 22

$UT_n(P)$ — унітрикутна група порядку n з коефіцієнтами з поля P — група за множенням усіх верхніх трикутних матриць порядку n з коефіцієнтами з поля P і з одиницями на головній діагоналі; 23

$\mathbb{Z}$ — множина (або адитивна група, або кільце) цілих чисел; 22

$Z(G)$ — центр групи G; 57

$Z_G(A)$ (або $Z(A)$) — централізатор підмножини A групи G; 58

$\mathbb{Z}_n$— множина (або адитивна група, або кільце) класів лишків за модулем числа n; 23

$\mathbb{Z}_n^*$ — мультиплікативна група оборотних класів лишків за модулем числа n; 23

$\varphi|_H$ — обмеження гомоморфізму груп φ на підгрупу H; 62

$\varphi(n)$ — функція Ойлера; 31

$\varphi \circ \psi$ (тобто $(\varphi \circ \psi)(x) = \psi(\varphi(x))$) — композиція відображень φ і ψ; 17

ε — тотожна підстановка; 23

$\mathcal{C}_n$ — група всіх поворотів правильного n–кутника; 23

$\mathcal{O}(a)$ (або a^G) — орбіта точки $a \in M$ при дії групи G на множині M; 81

$\chi(g)$ — кількість нерухомих точок елемента $g \in G$ при дії групи G на множині M; 83

$\varnothing$ — порожня множина. 27

Передмова

Ряд понять і тверджень, які мають загальноалгебричний, а почасти і загальноматематичний, характер (як, наприклад, поняття ізоморфізму, підструктури, факторструктури чи основна теорема про гомоморфізми), формулюються спочатку не для груп, а для довільних алгебричних структур. Це дозволяє підкреслити важливість цих понять і уникнути в подальшому викладі непотрібного паралелелізму при вивченні конкретних типів алгебричних структур — груп, кілець і т.д. До того ж з'являється можливість апелювати до певного досвіду, набутого студентами при вивченні лінійної алгебри.

Вступ

Спочатку алгебра була наукою про розв'язування рівнянь. Із дослідження лінійних рівнянь та їх систем виросла уже відома нам лінійна алгебра — одна з основ сучасної математики. Дослідження рівнянь вищих степенів привело в першій половині XIX ст. до виникнення поняття групи. Паралельно з цим у XIX ст. відбувається активне розширення поняття числа (комплексні числа, класи лишків, кватерніони, ...) і формування понять поля і кільця. На поч. XX ст. це привело до появи загального поняття алгебричної структури і формування нового обличчя алгебри, коли вона з науки про розв'язування рівнянь перетворилася в науку про властивості операцій на множинах.

І сьогодні теорія рівнянь залишається вихідним пунктом і основним змістом деяких розділів сучасної алгебри. Однак тепер вона трактується зовсім інакше, а головне, перестала бути головним джерелом алгебричних проблем. Крім того, застосування до теорії рівнянь перестали бути мірилом важливості і успішності алгебричних досліджень.

У певному розумінні майже кожна математична теорія зводиться до вивчення об'єктів двох видів: множин і функцій на множинах. Якщо і аргументи і значення функції f належать одній і тій же множині M, то f називається *алгебричною операцією* на M. Предметом сучасної алгебри є вивчення вивчення *алгебричних структур*, тобто множин із визначеними в них алгебричними операціями.

Можна сказати, що в першому наближенні предметом математичного аналізу є вивчення визначених на $\mathbb{R}$ дійсних функцій, тобто алгебричних дій на $\mathbb{R}$. У чому ж тоді особливість алгебри?

1. Алгебру цікавлять властивості самих операцій, а не множин, на яких вони визначені. Зокрема, алгебрі байдужа природа елементів цих множин — одна й та ж алгебрична структура може з'являтися то у вигляді множини чисел, то у вигляді множини функцій або таблиць спеціального вигляду, то у вигляді множини перетворень якої–небудь геометричної фігури або музичного твору, і т.д. Зате в аналізі чи геометрії основна множина (множина $\mathbb{R}$ в аналізі, площина або простір в геометрії) і природа її елементів відіграють величезну роль.

2. Алгебра зазвичай вивчає властивості не усієї сукупності операцій на даній множині, а лише однієї (або дуже невеликого набору операцій), причому не довільної, а лише такої, яка з самого початку має деякі

“хороші” властивості. Список таких “хороших” властивостей пройшов жорстокий природний відбір і не дуже великий. Важливо, що операції з одними й тими ж властивостями з’являються при дослідженні дуже різних питань. Тому виникає потреба в “індустріальному” підході до їх вивчення, щоб не починати кожного разу спочатку при появі чергової множини з операцією, тим більше, що часто є важливими лише абстрактні властивості самої операції, а не специфічна природа чергової множини. Гарною ілюстрацією такого підходу є лінійна алгебра, яка розробила потужні методи дослідження векторних просторів незалежно від природи їх елементів. Більше того, виявлення факту, що дві різні операції на множинах влаштовані у певному сенсі однаково, може мати дуже важливі наслідки. Так, з’ясування аналогії між додаванням і множенням дійсних чисел привело до відкриття логарифмів.

Наявність у різних природних дій аналогічних і подібних властивостей наштовхує на думку зробити ці спільні властивості вихідним пунктом досліджень, тобто сформулювати їх як аксіоми і послідовно вивчати різноманітні логічні наслідки з них. Аксіоматичний метод є дуже характерним для алгебри. Одночасне вивчення цілих класів алгебричних структур, які виділяються тими чи іншими системами аксіом, корисне хоча б тим, що не обмежується початковими об’єктами, якими важливими вони не були б. Сфера застосувань алгебри надзвичайно зростає. Адже незалежно від того, як визначені дії в кожному конкретному випадку, якщо вони задовольняють аксіоми, то будь–яка теорема, одержана з аксіом логічним шляхом, буде для цих дій правильною.

Однак лише дуже небагато систем аксіом є справді цікавими. Неможливо видумати “з голови” систему аксіом, яка б привела до змістовної теорії. Ті системи аксіом, які вивчаються в сучасній алгебрі, пройшли дуже жорсткий історичний відбір і є результатом аналізу алгебричних структур, які природно виникли в математиці.

Зауваження про відмінність аксіоматичного підходу в геометрії та алгебрі.

Текст містить невелику кількість вправ (зазвичай вони дуже прості і даються для закріплення наведених перед ними понять), які є обов’язковими, і досить великої кількості задач, серед яких є важкі (останні виділені зірочками). Задачі розраховані на активну участь читача в оволодінні матеріалом, тому серед них мало чисто тренувальних. Крім того, задачі часто містять додаткову цікаву або важливу інформацію, тому бажаним є намагання читача спробувати розв’язати хоча б значну

частину з них, і обов'язковим — ознайомлення з їх формулюваннями.

При посиланні на задачу (вправу) використовується подвійна нумерація: перше число — номер параграфа, до якого ця задача (вправа) відноситься, а друге — номер задачі (вправи) в цьому параграфі. При посиланні на теорему чи твердження використовується наскрізна нумерація.

1 Множини з діями

Означення 1.1. *Бінарною дією (або просто дією)* $*$ *на непорожній множині* M *називається довільне відображення* $* : M \times M \longrightarrow M$. *Результат застосування дії* $*$ *до пари* (a, b) *позначається* $a * b$. *Синонімом до терміну "дія" є слово "операція".*

Бінарну дію $*$ на скінченній множині $\{a_1, \ldots, a_n\}$ можна задавати *таблицею множення* — на перетині m–го рядка і k–го стовпчика стоїть результат $a_m * a_k$ застосування дії $*$ до елементів a_m і a_k:

$*$	a_1	a_2	$\cdots$	a_k	$\cdots$	a_n
a_1	$a_1 * a_1$	$a_1 * a_2$	$\cdots$	$a_1 * a_k$	$\cdots$	$a_1 * a_n$
a_2	$a_2 * a_1$	$a_2 * a_2$	$\cdots$	$a_2 * a_k$	$\cdots$	$a_2 * a_n$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
a_m	$a_m * a_1$	$a_m * a_2$	$\cdots$	$a_m * a_k$	$\cdots$	$a_m * a_n$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
a_n	$a_n * a_1$	$a_n * a_2$	$\cdots$	$a_n * a_k$	$\cdots$	$a_n * a_n$

Цю таблицю ще називають *таблицею Келі*. З іншого боку, кожна така таблиця визначає на множині $\{a_1, \ldots, a_n\}$ бінарну дію.

Крім символу $*$ дія може позначається яким–небудь іншим спеціальним символом, наприклад, $+$, $-$, $\cdot$, $:$, $\times$, $\uparrow$, $\circ$. У залежності від вибору позначення дія може називатися *додаванням, відніманням, множенням*, ..., а результат її застосування до певної пари елементів — *сумою, різницею, добутком,* ... цих елементів.

Насправді назви і позначення дій в алгебричних структурах принципового значення не мають, за кількома винятками, коли за певними діями історично утвердилися персональні назви (найчастіше їх називають додаванням або множенням і позначають відповідним чином). Зокрема, це дозволяє використовувати розроблену термінологію і систему позначень.

Поняття алгебричної дії можна розширити.

Означення 1.2. *n–арною (або n–аргументовою) дією* ω *на непорожній множині* M *називається довільне відображення*

$$\omega : M^n = M \times \cdots \times M \longrightarrow M.$$

Число n *називається арністю дії* ω. *Надалі для арності дії використовуватимемо позначення* арн ω.

Зауваження. 0–арна дія — це просто виділення певного елемента, наприклад, 0 або 1 в полі. Дії арності 1 (їх ще називають *унарними*) зустрічаються досить часто, наприклад, взяття протилежного або оберненого елемента, взяття цілої або дробової частини числа, перехід до транспонованої матриці чи до спряженого числа. Дії арності ≥ 3 зустрічаються рідко.

Означення 1.3. *Множина M із заданим на ній певним набором алгебричних дій $(\omega_i)_{i\in I}$ (можливо, різної арності) називається алгебричною структурою (алгебричною системою або універсальною алгеброю), множина M — її носієм, а набір $\{\text{арн } \omega_i \mid i \in I\}$ — її типом. Зазвичай позначається $\big(M; (\omega_i)_{i\in I}\big)$.*

Якщо набір дій $(\omega_i)_{i\in I}$ відомий, то часто говорять просто про структуру M. Позначення алгебричної структури і її носія одним і тим же символом як правило не призводить до непорозумінь чи двозначності, хоча жодним чином не можна ототожнювати структуру із множиною її елементів.

Означення 1.4. *Кажуть, що дві алгебричні системи однотипні, якщо їх типи одинакові.*

Зауваження. Однотипність алгебричних систем $\big(M; (\omega_i)_{i\in I}\big)$ та $\big(N; (\vartheta_j)_{j\in J}\big)$ означає, що існує бієктивне відображення $f : I \to J$ таке, що арн $\omega_i =$ арн $\vartheta_{f(i)}$. Тому надалі, не обмежуючи загальності, будемо вважати, що в однотипних алгебричних системах $I = J$ і для всіх $i \in I$ арн $\omega_i =$ арн ϑ_i.

Наведемо тепер декілька прикладів алгебричних структур.

Приклади. 1. Множина $T(M)$ всіх перетворень множини M із дією композиції. У випадку $M = \{1, 2, \ldots, n\}$ для цієї множини використовуватимемо позначення T_n.

2. Множина P^n всіх n–вимірних векторів із коефіцієнтами з поля P з діями додавання і множення на скаляри з P утворює арифметичний векторний простір, який є також прикладом алгебричної структури (додавання є бінарною дією, а множення на скаляри можна розглядати як цілу родину унарних дій: для кожного скаляра — своя дія).

Зауваження. Множина P^n із скалярним множенням векторів структуру утворювати не буде, бо скалярний добуток не є алгебричною дією.

3. Множина всіх (неперервних) скрізь визначених дійсних функцій зі звичайними додаванням і множенням.

4. Множина $M_n(\mathbb{R})$ всіх квадратних дійсних матриць порядку n із бінарними діями додавання, множення, унарними — взяття протилежної матриці, транспонування і 0–арними — виділеними нульовою матрицею $\mathbf{0}$ та одиничною матрицею E.

Зауваження. Наведені приклади, як і більшість із тих, що будуть далі, є природними в тому сенсі, що вони з'явилися в результаті вивчення навколишнього світу і внутрішнього розвитку математики, а не були спеціально придумані. Взагалі кажучи можна розглядати довільні дії на довільних множинах. Це корисно з точки зору уніфікації термінології, понять і підходів, однак за широту підходу доводиться платити відсутністю глибоких результатів. Дій занадто багато (на n–елементній множині можна визначити n^{n^2} різних дій, що вже при $n = 10$ дає 10^{100}) і вони занадто різні. Тому для одержання змістовних результатів на алгебричні структури треба накладати якісь обмеження, бажано, природні. Як говорив на своїй лекції про найбільш раціональні способи крою тканини відомий російський математик татарського походження Чебишев: "Припустимо, для простоти, що людське тіло має форму кулі".

Ці обмеження бувають двох типів:
— обмеження на кількість дій;
— обмеження на властивості дій.

Але алгебриста цікавлять лише ті властивості алгебричних структур та їх елементів, які можна виразити в термінах заданих дій.

Серед **властивостей дій** відмітимо такі:

(a) дія $*$ на множині M називається *асоціативною*, якщо

$$\text{для довільних} \quad a, b, c \in M \quad (a * b) * c = a * (b * c);$$

(b) дія $*$ на множині M називається *комутативною*, якщо

$$\text{для довільних} \quad a, b \in M \quad a * b = b * a;$$

(c) дія $*$ на множині M називається *скоротною зліва* (*справа*), якщо для довільних $a, b, c \in M$ з рівності $c * a = c * b$ (відповідно $a * c = b * c$) випливає рівність $a = b$.

А серед **властивостей елементів** такі:

(a) елемент 0_l (відповідно 0_r) називається *лівим* (*правим*) *нулем* для дії $*$ на множині M, якщо для довільного $x \in M \quad 0_l * x = 0_l$ (відповідно $x * 0_r = 0_r$);

(b) елемент e_l (відповідно e_r) називається *лівим нейтральним* або *лівою одиницею* (*правим нейтральним* або *правою одиницею*) для дії

$*$ на множині M, якщо для довільного $x \in M$ $\quad e_l * x = x$ (відповідно $x * e_r = x$);

(c) якщо елемент одночасно є і лівим нулем, і правим, то він називається *двостороннім нулем* або просто *нулем* і позначається 0;

(d) якщо елемент одночасно є і лівим нейтральним, і правим, то він називається *двостороннім нейтральним* або просто *одиницею* і позначається e.

Зауваження. У випадку адитивного запису нейтральний елемент часто називають нулем дії, хоча насправді для додавання він нулем **не є**! Просто у випадку числових множин нейтральний елемент для додавання є одночасно нулем для іншої дії — множення, що й стало джерелом певної неузгодженості термінології.

Вправа 1.1. *Як за таблицею Келі з'ясувати:* a) *чи буде дія комутативною*; b) *чи існують для дії ліві або праві нулі*; c) *чи існує для дії нейтральний елемент*?

Твердження 1.1. *Якщо для бінарної дії $*$ існують права і ліва одиниці, то ці одиниці збігаються і їх спільне значення буде нейтральним елементом для $*$.*

Доведення. Позначимо символом M множину, на якій задана дія $*$, і нехай e_r, e_l — права і ліва одиниці для $*$. Тоді згідно означення правої (відповідно лівої) одиниці добуток $e_l * e_r$ з одного боку дорівнює e_l, а з іншого — e_r, тому $e_r = e_l$. Нехай $e = e_r = e_l$. Тоді для довільного елемента $a \in M$ матимемо $a * e = a * e_r = a = e_l * a = e * a$. Отже, e — нейтральний елемент для $*$. □

Вправа 1.2. *Наведіть приклад множини з бінарною дією, яка*: a) *має єдину ліву одиницю, а правих одиниць не має жодної*; b) *має нескінченно багато лівих одиниць, а правих — не має жодної.*

Твердження 1.2. *Для кожної бінарної дії $*$ існує не більше одного нейтрального елемента і не більше одного нуля.*

Доведення. Припустимо, що дія $*$ має два нейтральні елементи e_1 та e_2. Згідно означення $e_1 * e_2 = e_1$ з одного боку і $e_1 * e_2 = e_2$ з іншого. Звідки, $e_1 = e_2$.

Аналогічно, якщо дія $*$ має два нулі 0_1 та 0_2, то $0_1 * 0_2 = 0_1 = 0_1 * 0_2 = 0_2$ і $0_1 = 0_2$. □

За наявності нейтрального елемента e можна говорити про оборотність елементів. Елемент b називається *оберненим зліва* (*оберненим справа*) до a, якщо $b * a = e$ (відповідно $a * b = e$). Елемент b, який є оберненим і зліва, і справа до a називається просто *оберненим* до a. Якщо для a існує обернений елемент, то a називається *оборотним*. У випадку адитивної термінології замість "обернений" говорять "протилежний".

Більшість дій, які природним чином виникають у математиці, є асоціативними. Головним чином це викликано асоціативністю композиції перетворень множини, адже багато дій є безпосередньо або композицією відображень (як множення підстановок), або тісно з ними пов'язані (як множення матриць із композицією лінійних відображень), або вони можуть бути інтерпретовані як композиції певних відображень (додавання чисел — як композиція зсувів прямої, множення чисел — як композиція гомотетій).

Комутативні дії зустрічаються вже набагато рідше.

Асоціативність і комутативність є незалежними властивостями: (a) множення матриць є асоціативним, але не є комутативним; (b) дія $a*b = a^2 + b^2$ на $\mathbb{R}$ є комутативною, але не є асоціативною.

Задача 1.1. *Нехай M — деяка n–елементна множина. Для $2 \le n \le 5$ знайдіть кількість попарно неізоморфних алгебричних систем $(M; *)$ з одиницею, в яких кожний елемент є скоротним. Чи є серед цих систем неасоціативні?*

2 Ізоморфізм

Означення 2.1. *Алгебричні структури $(M; \circ)$ і $(N; *)$ з бінарними діями $\circ$ і $*$ відповідно називаються ізоморфними, якщо існує таке взаємно однозначне відображення $\varphi : M \to N$, що для всіх $x, y \in M$ виконується рівність*

$$\varphi(x \circ y) = \varphi(x) * \varphi(y).$$

Якщо структури $(M; \circ)$ і $(N; *)$ ізоморфні, то пишуть $(M; \circ) \simeq (N; *)$. Саме відображення φ називається ізоморфізмом структур $(M; \circ)$ і $(N; *)$.

Аналогічно визначається ізоморфізм для алгебричних структур з більшою кількістю дій та іншої арності.

Означення 2.2. *Однотипні алгебричні структури* $\big(M;(\omega_i)_{i\in I}\big)$ *і* $\big(N;(\vartheta_i)_{i\in I}\big)$ *з наборами дій* $(\omega_i)_{i\in I}$ *і* $(\vartheta_i)_{i\in I}$ *відповідно називаються ізоморфними, якщо існує таке взаємно однозначне відображення* $\varphi : M \to N$, *що для всіх* $i \in I$ *та* $x_1, \dots, x_{\text{арн }\omega_i} \in M$ *виконуються рівності:*

$$\varphi\big(\omega_i(x_1, \dots, x_{\text{арн }\omega_i})\big) = \vartheta_i\big(\varphi(x_1), \dots, \varphi(x_{\text{арн }\omega_i})\big).$$

Якщо структури $\big(M;(\omega_i)_{i\in I}\big)$ *і* $\big(N;(\vartheta_i)_{i\in I}\big)$ *ізоморфні, то пишуть* $\big(M;(\omega_i)_{i\in I}\big) \simeq \big(N;(\vartheta_i)_{i\in I}\big)$ *(або коротко* $M \simeq N$*). Саме відображення* φ *називається ізоморфізмом структур* $\big(M;(\omega_i)_{i\in I}\big)$ *і* $\big(N;(\vartheta_i)_{i\in I}\big)$.

Приклади. 1. Із властивостей логарифмічної функції випливає, що для кожного додатного $a \neq 1$ відображення $x \mapsto \log_a x$ є ізоморфізмом $(\mathbb{R}^+;\cdot)$ на $(\mathbb{R};+)$. Це, зокрема, означає, що між ізоморфними структурами може існувати багато різних ізоморфізмів.

Відкриття цього ізоморфізму чотири століття тому відіграло величезну роль у раціоналізації техніки обчислень, оскільки після появи таблиць логарифмів дозволяло замінити множення багатоцифрових чисел додаванням. На цьому ізоморфізмові ґрунтується і логарифмічна лінійка — протягом тривалого часу робочий інструмент кожного інженера.

2. Розглянемо множину поворотів на кути $0°$, $90°$, $180°$, $270°$ з дією композиції $\circ$ та множину $\{1, i, -1, -i\}$ із звичайною операцією множення комплексних чисел. Відображення $\varphi : 0° \mapsto 1$, $\varphi : 90° \mapsto i$, $\varphi : 180° \mapsto -1$, $\varphi : 270° \mapsto -i$ є ізоморфізмом цих алгебричних структур.

Твердження 2.1. a) *Композиція відображень ізоморфізму і відображення, обернене до ізоморфізму, також є ізоморфізмами.*
b) *На класі однотипних алгебричних систем відношення ізоморфності є відношенням еквівалентності.*

Доведення. Легко бачити, що доведення досить провести лише для множин з однією бінарною дією (доведення в загальному випадку повністю аналогічне). *a*) Нехай $\varphi : M_1 \to M_2$, $\psi : M_2 \to M_3$ — ізоморфізми алгебричних структур $(M_1;*_1)$, $(M_2;*_2)$ та $(M_2;*_2)$, $(M_3;*_3)$ відповідно. Оскільки відображення $(\varphi \circ \psi) : M_1 \to M_3$ задається так: $(\varphi\circ\psi)(m) = \psi(\varphi(m))$, то $\varphi\circ\psi$ є бієкцією і для довільних $x, y \in M_1$ матимемо: $(\varphi\circ\psi)(x*_1 y) = \psi\big(\varphi(x*_1 y)\big) = \psi\big(\varphi(x)*_2\varphi(y)\big) = \psi(\varphi(x))*_3\psi(\varphi(y)) = (\varphi \circ \psi)(x) *_3 (\varphi \circ \psi)(y)$. Тому $\varphi \circ \psi$ є також ізоморфізмом.

Покажемо тепер, що для ізоморфізму φ множин $(M_1; *_1)$ та $(M_2; *_2)$ оберенене відображення $\varphi^{-1} : M_2 \to M_1$ таке, що $\varphi^{-1}(y) = x$, де $\varphi(x) = y$, також буде ізоморфізмом. Справді, відображення φ^{-1} є бієктивним, бо таким же є відображення φ. Крім того, для довільних $y_1, y_2 \in M_2$ існують такі $x_1, x_2 \in M_1$, що $\varphi(x_1) = y_1$, $\varphi(x_2) = y_2$. Тому $\varphi^{-1}(y_1 *_2 y_2) = \varphi^{-1}\big(\varphi(x_1) *_2 \varphi(x_2)\big) = \varphi^{-1}\big(\varphi(x_1 *_1 x_2)\big) = x_1 *_1 x_2 = \varphi^{-1}(y_1) *_1 \varphi^{-1}(y_2)$ і відображення φ^{-1} також є ізоморфізмом.

b) Перевіримо, чи відношення ізоморфізму є рефлексивним, симетричним і транзитивним. Для довільної алгебричної структури $(M; *)$ тотожне відображення $\varepsilon : M \to M$, $\varepsilon(x) = x$, є ізоморфізмом M в себе, який називається *тотожним ізоморфізмом*. Якщо відображення φ задає ізоморфізм $(M_1; *_1)$ та $(M_2; *_2)$, то згідно п. a) відображення φ^{-1} задаватиме ізоморфізм $(M_2; *_2)$ та $(M_1; *_1)$. Якщо ж відображення φ_1 і φ_2 задають ізоморфізми $(M_1; *_1)$, $(M_2; *_2)$ і $(M_2; *_2)$, $(M_3; *_3)$ відповідно, то знову ж таки згідно п. a) відображення $\varphi_1 \circ \varphi_2$ задаватиме ізоморфізм $(M_1; *_1)$ та $(M_3; *_3)$. Отже, відношення $\simeq$ є відношенням еквівалентності. □

Задача 2.1. *Доведіть, що довільний ізоморфізм* $(\mathbb{R}^+; \cdot)$ *на* $(\mathbb{R}; +)$ *має вигляд* $x \to \log_a x$ *для деякого додатного* a.

Задача 2.2. *Побудуйте ізоморфізм між множиною всіх паралельних переносів прямої з дією композиції та* $(\mathbb{R}; +)$.

Зауваження. 1. Якщо дві алгебричні структури ізоморфні, то будь–яке твердження, яке можна сформулювати лише в термінах заданих дій, буде правильним для однієї з цих структур тоді й лише тоді, коли воно буде правильним і для іншої. Наприклад, якщо $(M; \circ) \simeq (N; *)$ і дія $\circ$ комутативна, то дія $*$ також комутативна. Таким чином, при вивченні алгебричних систем із точністю до ізоморфізму природа елементів цих систем ігнорується, а увага зосереджується на властивостях самих дій. Аналогічно читач, який цікавиться лише змістом твору, розглядає різні примірники одного й того ж роману, що віддруковані в різний час, різним шрифтом і на різному папері, як тотожні. Те, що властиве усім системам із певного класу ізоморфних систем, і є алгебричною системою у чистому, тобто *абстрактному*, вигляді.

Недоліками такого підходу є певне збіднення об'єктів дослідження і обмеження проблематики. Але це з головою перекривається загальністю підходу: одержані результати можна автоматично застосовувати

до конкретних систем найрізноманітнішого походження. Крім того, чистота такого підходу на практиці дуже часто порушується: вивчення конкретних систем продовжує відігравати в алгебрі величезну роль.

2. Для доведення ізоморфності двох алгебричних структур зазвичай вказують в явному вигляді відповідний ізоморфізм. Для доведення ж неізоморфності двох структур намагаються знайти твердження, яке формулюється лише в термінах заданих дій і яке є правильним тільки для однієї з цих структур.

Хоча в принципі байдуже, яку саме із ізоморфних одна одній алгебричних структур вивчати, вибір певної структури може виявитися важливим для розв'язування конкретної задачі, бо дозволить використати специфічні для цієї структури методи. Наприклад, якщо елементами структури є матриці, то можуть спрацювати методи лінійної алгебри.

Подібно тому, як у геометрії під геометричними властивостями фігур і тіл розуміють ті властивості, які зберігаються при відповідних геометричних перетвореннях (в евклідовій геометрії — при рухах), під *алгебричними властивостями* алгебричних структур розуміють ті властивості, які зберігаються при всіх ізоморфізмах. Зауважимо, що можна говорити про алгебричні властивості не тільки структур у цілому, а й їх підмножин, елементів, систем елементів і т.д. Наприклад, у теорії векторних просторів алгебричною є властивість системи векторів бути лінійно залежною. У теорії груп алгебричними є властивості (точні означення будуть далі): бути нейтральним, оборотним, мати скінченний порядок — для елементів, бути підгрупою чи системою твірних — для підмножини, бути комутативною чи розв'язною — для самої групи, і т.д.

3 Напівгрупи

Означення 3.1. *Алгебрична структура* $(M; *)$ *називається напівгрупою, якщо дія* $*$ *на множині* M *є асоціативною. Напівгрупа з нейтральним елементом називається напівгрупою з одиницею або моноїдом. Якщо дія ще й комутативна, то напівгрупа називається комутативною або абелевою.*

Зауважимо, що далеко не кожна напівгрупа має нейтральний елемент. Такими є, наприклад, напівгрупа натуральних чисел за додаванням і напівгрупа парних чисел за множенням.

Приклади. 1. Оскільки додавання і множення чисел асоціативне, то будь–яка замкнена відносно додавання або множення числова множина буде напівгрупою відносно відповідної дії.

2. Напівгрупою є і множина $T(M)$ всіх перетворень множини M з дією композиції (ця напівгрупа називається *симетричною напівгрупою*), і множина $\mathcal{B}(M)$ всіх бінарних відношень на множині M відносно де–морганівського добутку відношень.

3. Множина $\Omega(M)$ всіх підмножин множини M замкнена відносно кожної з операцій: об'єднання, перетин, різниця, симетрична різниця, але не з кожною з цих дій утворюватиме напівгрупу. Так, $(\Omega(M);\cup)$, $(\Omega(M);\cap)$ і $(\Omega(M);\triangle)$ є, принаймні, комутативними моноїдами, а $\Omega(M)$ з операцією різниця напівгрупу взагалі не утворюватиме.

Перевірка асоціативності деяких дій може бути досить складною процедурою. Зокрема, для n–елементної множини в загальному випадку треба перевірити виконання n^3 рівностей. І хоча розроблені певні процедури, які зменшують кількість перевірок, ці процедури не завжди ефективні. Зокрема, угорський математик Сас довів, що для $n > 3$ на n–елементній множині завжди можна визначити бінарну дію таким чином, щоб із n^3 рівностей асоціативності не виконувалася лише одна наперед вказана.

Твердження 3.1. *У напівгрупі добуток довільних n множників не залежить від способу розстановки дужок у виразі $x_1 * \cdots * x_n$.*

Доведення. Легко бачити, що для доведення цього твердження досить скористатися індукцією за кількістю множників n. □

Таким чином, у випадку асоціативної дії ми можемо дужки опускати і писати просто $x_1 * \cdots * x_n$.

Вправа 3.1. *Доведіть, що коли дія асоціативна і комутативна, то добуток довільних n множників не залежить і від порядку множників.*

Задача 3.1. *Скількома способами можна розставити дужки у виразі $x_1 * \cdots * x_n$?*

Задача 3.2. *Скільки різних раціональних виразів можна одержати за рахунок різної розстановки дужок у виразі $x_1 : x_2 : \cdots : x_n$?*

Елемент ϵ напівгрупи називається *ідемпотентом*, якщо $\epsilon \cdot \epsilon = \epsilon$. Ідемпотентами, зокрема, є всі ліві (праві) нулі і всі ліві (праві) одиниці. Кількість ідемпотентів у напівгрупі може змінюватися в дуже широких межах: у напівгрупі $(\mathbb{N}; +)$ ідемпотентів взагалі немає, у той час як у напівгрупі $(\Omega(M); \cup)$ кожен елемент є ідемпотентом.

Задача 3.3. *Доведіть, що лінійне перетворення скінченновимірного комплексного векторного простору буде ідемпотентом тоді й лише тоді, коли воно є проектуванням на підпростір.*

Задача 3.4. *Підрахуйте кількість ідемпотентів у напівгрупі T_n.*

Твердження 3.2. *Кожен елемент моноїда має не більше одного оберненого елемента.*

Доведення. Якщо b_1 і b_2 — два обернених до a елементи, то

$$b_1 = b_1 * e = b_1 * (a * b_2) = (b_1 * a) * b_2 = e * b_2 = b_2 \ .$$

□

Вправа 3.2. *Перевірте, що в довільному моноїді*: a) $(a^{-1})^{-1} = a$; b) $(ab)^{-1} = b^{-1}a^{-1}$.

Теорема 3.1 (Келі). *Кожна напівгрупа S ізоморфна деякій напівгрупі перетворень множини S.*

Доведення. Будемо вважати, що напівгрупа S містить одиницю e (у противному разі напівгрупу S можно перетворити в напівгрупу $S \cup \{e\}$ з одиницею, приєднавши до S елемент e). Зіставимо кожному $a \in S$ перетворення μ_a множини S, яке визначатиметься правилом: $\mu_a(x) = xa$. Нехай $\hat{T} = \{\mu_a \mid a \in S\}$. Тоді відображення $\varphi : S \to \hat{T}$, $a \mapsto \mu_a$, є бієкцією. Крім того, $\mu_{ab} = \mu_a \cdot \mu_b$. Тому $\hat{T}$ є замкненою відносно композиції перетворень (значить є напівгрупою), а відображення φ є ізоморфізмом. □

Для довільних непорожніх підмножин A, B напівгрупи $(S; *)$ можна визначити їх *добуток* $A * B = \{a * b \,|\, a \in A, b \in B\}$. Якщо одна з множин одноелементна, наприклад, $A = \{a\}$, то замість $\{a\} * B$ і $B * \{a\}$ вживають більш прості позначення $a * B$ і $B * a$. Це множення, як це випливає із наступної вправи, є асоціативним.

Вправа 3.3. *Доведіть, що для довільних непорожніх підмножин A, B, C напівгрупи $(S; *)$ має місце рівність:* $(A * B) * C = A * (B * C)$.

4 Групи

Означення 4.1. *Моноїд, в якому кожен елемент є оборотним, називається групою. Іншими словами, група* $(G;*)$ *— це непорожня множина* G *з бінарною дією* $*$*, яка задовольняє такі умови (аксіоми групи)* :
(a) *асоціативність*: *для довільних* $a,b,c \in G \quad (a*b)*c = a*(b*c)$;
(b) *існування нейтрального елемента*: *існує такий елемент* $e \in G$*, що для довільного* $a \in G \quad a*e = e*a = a$;
(c) *оборотність*: *для кожного* $a \in G$ *існує такий елемент* $a^{-1} \in G$*, що* $a*a^{-1} = a^{-1}*a = e$.

Якщо дія комутативна, тобто для всіх $a,b \in G \quad a*b = b*a$, то група називається *комутативною* або *абелевою*.

Найчастіше дія в групі називається множенням і використовується мультиплікативна термінологія (а саму групу інколи називають мультиплікативною). Якщо дія називається додаванням, то використовують адитивну термінологію. Причому абелевими групами частіше називають адитивні групи з комутативною дією на них, а комутативними групами — мультиплікативні з теж комутативною дією на них.

Потужність $|G|$ множини G називають *порядком* групи G. Якщо $|G| < \infty$, то кажуть, що група G є *скінченною*, у противному разі група G є *нескінченною*.

Зауваження. Введені поняття порядку групи, скінченної та нескінченної групи аналогічним чином переносяться на довільні універсальні алгебри.

Наведемо деякі приклади груп.

Приклади. 1. Множини $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ з дією додавання утворюють абелеві групи, які називають *числовими групами за додаванням.*

2. Множини $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{R}^+$, $\mathbb{C}^*$, множина $\mathbb{C}_n$ всіх коренів n–го степеня з 1, множина $\mathbb{C}_{p^\infty} = \bigcup\limits_{n\in\mathbb{N}} \mathbb{C}_{p^n}$, множина $T = \{z \in \mathbb{C} \mid |z| = 1\}$ з дією множення утворюють також абелеві групи, які називають *числовими групами за множенням.*

3. Так званими *матричними групами* за множенням є: *повна лінійна група* $GL_n(P)$ (група невироджених матриць порядку n над полем P, яка при $n \geq 2$ є неабелевою), *спеціальна лінійна група* $SL_n(P)$ (група матриць порядку n з визначником рівним 1 над полем P), *ортогональна група* O_n (група ортогональних матриць порядку n), *унітарна група* U_n

(група всіх унітарних матриць n–го порядку), *діагональна група* $D_n(P)$ (група всіх невироджених діагональних матриць порядку n над полем P), *трикутна група* $T_n(P)$ (група всіх невироджених матриць порядку n над полем P з нульовим кутом під головною діагоналлю), *унітрикутна група* $UT_n(P)$ (група всіх невироджених матриць порядку n над полем P з нульовим кутом під головною діагоналлю і з одиницями на діагоналі). Якщо в якості P береться скінченне поле із q елементів, то замість $GL_n(P)$ пишуть $GL_n(q)$ (аналогічно для інших матричних груп).

4. Розглянемо множину класів лишків $\mathbb{Z}_n = \{\bar{0}, \ldots, \overline{n-1}\}$ з дією додавання і множину класів лишків $\mathbb{Z}_n^* = \{\bar{i} \,|\, \text{НСД}(i,n) = 1\}$ з дією множення. Вони будуть утворювати відповідно *адитивну* і *мультиплікативну* групи. Ці групи є абелевими і називаються *групами класів лишків*.

5. Множина S_n всіх підстановок n–го степеня, тобто множина всіх взаємно однозначних відображень множини $\{1, \ldots, n\}$ відносно операції множення підстановок (суперпозиції відображень) утворює групу, яку прийнято називати *симетричною групою*. У свою чергу множина A_n всіх парних підстановок n–го степеня з дією множення підстановок утворює також групу, яка називається *знакозмінною групою*. Ці групи відносяться до класу так званих груп підстановок і S_n є неабелевою при $n \geq 3$, а A_n є неабелевою при $n \geq 4$.

6. Множина K_4 підстановок $\{\varepsilon, (12)(34), (13)(24), (14)(23)\}$ з дією множення утворює абелеву групу, яка називається *група ! четверна група Кляйна*.

7. Легко зрозуміти, що сукупність усіх перетворень площини (простору), які лишають незмінною певну фігуру (тіло), відносно композиції також утворює групу. Таким чином з'являються *групи поворотів* і *рухів правильних многогранників*, *групи рухів різних паркетів*, *кристалів* і т.д. Зокрема, *група* $\mathcal{C}_n$ *всіх поворотів правильного* n*–кутника* складається з поворотів на кути $0^\circ, 360^\circ/n, 2\cdot 360^\circ/n, \ldots, (n-1)\cdot 360^\circ/n$ відносно центра цього n–кутника. Група D_n всіх рухів правильного n–кутника (*діедральна група*) складається з n поворотів відносно його центра на кути 0°, $360^\circ/n$, $2\cdot 360^\circ/n$, $\ldots$, $(n-1)\cdot 360^\circ/n$ та n симетрій $l_1, \ldots, l_n$ відносно осей, що проходять при непарному n через вершини n–кутника та середини протилежних ребер, а при парному n — через дві протилежні

вершини або через середини двох протилежних ребер. *Група рухів ромба* складається із поворотів на кути 0° та 180° навколо точки перетину діагоналей ромба і двох симетрій l_1, l_2 відносно діагоналей ромба.

8. Кватерніонні одиниці i, j, k породжують так звану *групу кватерніонів* $Q_8 = \{1, -1, i, j, k, -i, -j, -k\}$ порядку 8, де $(-1)^2 = 1$, $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$.

Вправа 4.1. *Перевірте виконання аксіом групи у щойно наведених прикладах.*

Зауваження. 1. Остання серія прикладів груп пов'язана із загальнонауковим і навіть загальнокультурним поняттям *симетрії*, з яким обізнана кожна освічена людина. Однак не всі розуміють, що глибший аналіз поняття симетрії неминуче приводить нас до математичної структури — групи, бо симетрії (як рухи або перетворення) можна множити, виконуючи їх послідовно.

2. Поняття групи вперше ввів Ґалуа (1831 р.), хоча в неявному вигляді комутативні групи зустрічалися вже в Лагранжа і Ґауса. Після робіт Коші про підстановки (1847 р.) дослідження груп (головним чином — груп підстановок) починають наростати. У 1870 р. виходить знаменитий трактат Жордана про групи підстановок, але тут теорія груп розглядалась лише в обсязі, необхідному для дослідження розв'язності рівнянь у радикалах. Сучасна абстрактна теорія груп почалася з виходу книги Шмідта (1916 р.), яка так і називалася "Абстрактна теорія груп". Остання була перевидана в 1933 р. і протягом 25-30 років була основним підручником з теорії груп в університетах Росії, а згодом СРСР.

Вправа 4.2. *Покажіть, що в довільній групі* $(ab)^{-1} = b^{-1}a^{-1}$. *Більш того, для довільних елементів* $a_1, \ldots, a_n$ *групи має місце* $(a_1 a_2 \ldots a_{n-1} a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \ldots a_2^{-1} a_1^{-1}$.

Твердження 4.1. a) *У групі можна скорочувати, тобто з кожної з рівностей* $ac = bc$ *і* $ca = cb$ *випливає рівність* $a = b$.
b) *Для довільних* a *і* b *кожне з рівнянь* $ax = b$ *і* $ya = b$ *має в групі єдиний розв'язок.*

Доведення. a) Досить помножити рівності $ac = bc$ і $ca = cb$ відповідно справа і зліва на c^{-1}.
b) Легко перевірити, що $x = a^{-1}b$ і $y = ba^{-1}$ є розв'язками. Однозначність випливає з п. a). □

Наслідок 4.1. *У кожному рядку і в кожному стовпчику таблиці Келі групи кожний елемент групи зустрічається рівно один раз.*

Твердження 4.1 b) дозволяє визначити в групі *лівe* $a\backslash b = a^{-1}b$ і *правe* $b/a = ba^{-1}$ *ділення* b на a. Якщо група не є комутативною, то ці ділення — різні.

Задача 4.1. *Доведіть, що в означенні групи досить вимагати існування лише правосторонніх (або лише лівосторонніх) нейтрального і оберненого елементів.*

Задача 4.2. *Доведіть, що скінченна напівгрупа з лівостороннім і правостороннім скороченням є групою.*

Задача 4.3. *З'ясуйте, чи можна в попередній задачі відмовитися від скінченності.*

Із твердження 3.1 випливає, що для довільного елемента a групи і натурального числа n добуток n множників $a^n = a \cdot a \cdots a$ визначений однозначно. Цей добуток називається n–м *степенем* елемента a. Покладемо $a^0 = e$ і $a^{-n} = (a^{-1})^n$. Тоді поняття степеня елемента можна розглядати для довільного цілого показника. У випадку адитивного запису дії замість степенів говорять про *кратні* елемента і записують $na = a + a + \cdots + a$ (n раз).

Легко перевіряються наступні властивості степенів.

Твердження 4.2. *Для довільних елемента x групи G та цілих чисел n, m виконуються рівності*:

$$\text{a)}\ (x^n)^{-1} = x^{-n}\ ; \quad \text{b)}\ x^n x^m = x^{n+m}\ ; \quad \text{c)}\ (x^n)^m = x^{nm}\ .$$

Доведення. a) Оскільки $x^{-n} \cdot x^n = \underbrace{x^{-1} \cdots x^{-1}}_{n} \cdot \underbrace{x \cdots x}_{n} = e = \underbrace{x \cdots x}_{n} \cdot \underbrace{x^{-1} \cdots x^{-1}}_{n} = x^n \cdot x^{-n}$, то $(x^n)^{-1} = x^{-n}$.

b) Випадки, коли $n, m \geq 0$ або $n, m < 0$ — очевидні. Нехай тепер $n < 0$, $m \geq 0$ і $|n| \leq m$. Тоді

$$x^n \cdot x^m = x^{-|n|} \cdot x^m = (x^{-1})^{|n|} \cdot x^m = \underbrace{x^{-1} \cdots x^{-1}}_{|n|} \cdot \underbrace{x \cdots x}_{m} = x^{m-|n|} = x^{m+n}\ .$$

Якщо ж $n < 0$, $m \geq 0$ і $|n| > m$, то

$$x^n \cdot x^m = x^{-|n|} \cdot x^m = (x^{-1})^{|n|} \cdot x^m = \underbrace{x^{-1} \cdots x^{-1}}_{|n|} \cdot \underbrace{x \cdots x}_{m} =$$

$$= \underbrace{x^{-1} \cdots x^{-1}}_{|n|-m} = x^{-(|n|-m)} = x^{m-|n|} = x^{m+n}.$$

Випадок $n > 0$, $m \leq 0$ розглядається аналогічно.

c) Випадок $n, m \geq 0$ — очевидний. Якщо $n \geq 0$, $m < 0$, то

$$(x^n)^m = \big((x^n)^{-1}\big)^{|m|} = \big((x^{-1})^n\big)^{|m|} = (x^{-1})^{n\cdot|m|} = x^{-n\cdot|m|} = x^{nm} \ .$$

При $n < 0$, $m \geq 0$ матимемо

$$(x^n)^m = \big((x^{-1})^{|n|}\big)^m = (x^{-1})^{|n|\cdot m} = x^{-|n|\cdot m} = x^{nm} \ .$$

Якщо ж $n < 0$, $m < 0$, то

$$(x^n)^m = \big((x^n)^{-1}\big)^{|m|} = (x^{-n})^{|m|} = (x^{|n|})^{|m|} = x^{|n|\cdot|m|} = x^{nm} \ .$$

□

5 Підструктури

Нехай ω — n–арна дія на множині M. Підмножина $A \subseteq M$ називається *замкненою* (*інваріантною*, *стійкою*) відносно дії ω, якщо $\omega(A \times \cdots \times A) \subseteq A$. Іншими словами, якщо для довільного набору $(a_1, \ldots, a_n)$ елементів з A результат $\omega(a_1, \ldots, a_n)$ застосування дії ω до цього набору також належить A.

Якщо підмножина $A \subseteq M$ алгебричної структури $\big(M; (\omega_i)_{i\in I}\big)$ є замкненою відносно всіх визначених на цій структурі дій, то вона сама перетворюється в алгебричну структуру $\big(A; (\omega_i)_{i\in I}\big)$, яка називається *підструктурою* даної структури.

Які властивості дій успадковуються підструктурою? Якщо властивість має вигляд деякої тотожності (типу асоціативності чи комутативності), то напевне так (більш точно — властивості, які описуються т.зв. *універсальними* формулами). Але інші властивості можуть і не успадковуватися.

Означення 5.1. *Піднапівгрупою напівгрупи G називається така підмножина $H \subseteq G$, яка сама є напівгрупою відносно тієї ж дії. Якщо G — моноїд з одиницею e і піднапівгрупа $H \subseteq G$ містить e, то H називається підмоноїдом G.*

Означення 5.2. *Підгрупою групи G називається така її непорожня підмножина $H \subseteq G$, яка сама є групою відносно тієї ж дії. Факт, що H є підгрупою G, позначатимемо $H \leq G$.*

Твердження 5.1. *Непорожня підмножина H групи $(G; \cdot)$ буде підгрупою G тоді й лише тоді, коли H замкнена відносно множення та взяття оберненого елемента.*

Доведення. Оскільки H замкнена відносно дії $\cdot$, то треба перевірити виконання лише аксіом групи. Асоціативність дії очевидна. Крім того, для довільного елемента $a \in H$ елементи a^{-1} і $a \cdot a^{-1} = e$ також належать H. □

Вправа 5.1. *Наведіть приклад напівгрупи, кожна підмножина якої є піднапівгрупою.*

Зауваження. Порожню підмножину напівгрупи також зручно вважати піднапівгрупою. Але підмоноїд і підгрупа за означенням уже є непорожніми.

Піднапівгрупа (підмоноїд, підгрупа) H напівгрупи (моноїда, групи) G називається *власною*, якщо $H \neq G$. Той факт, що підгрупа H групи G є власною, записуємо як $H < G$.

G і $\varnothing$ називаються *тривіальними* піднапівгрупами напівгрупи G. Якщо G — моноїд (група) з одиницею e, то G і $\{e\}$ називаються *тривіальними* підмоноїдами (підгрупами) G, а довільний підмоноїд (підгрупа), відмінний від G і $\varnothing$ називається *нетривіальним*. Підгрупу $\{e\}$ ще називають *одиничною* підгрупою групи G і часто позначають E, а кожна підгрупа G, відмінна від $\{e\}$, називається *неодиничною*.

Нижче наведемо приклади деяких ланцюгів підгруп для груп, що розглядалися на стор. 22, 24.

Приклади. 1. $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$.

2. $\mathbb{Q}^* < \mathbb{R}^*, \quad \mathbb{R}^+ < \mathbb{R}^* < \mathbb{C}^*$.

3. $SL_n(\mathbb{Z}) < SL_n(\mathbb{Q}) < SL_n(\mathbb{R}) < SL_n(\mathbb{C}), \quad UT_n(\mathbb{Q}) < SL_n(\mathbb{Q}) < GL_n(\mathbb{Q}) < GL_n(\mathbb{R}) < GL_n(\mathbb{C}), \quad UT_n(\mathbb{R}) < T_n(\mathbb{R}) < GL_n(\mathbb{R}), \quad D_n(\mathbb{C}) < T_n(\mathbb{C}) < GL_n(\mathbb{C}), \quad U_n < GL_n(\mathbb{C}), \quad O_n < GL_n(\mathbb{R})$.

4. $A_n < S_n$.

Вправа 5.2. *Доведіть, що множина $SL_n(\mathbb{Z})$ є підгрупою групи $GL_n(\mathbb{Q})$.*

Твердження 5.2. *Перетин довільної родини піднапівгруп (підмоноїдів, підгруп) знову буде піднапівгрупою (підмоноїдом, підгрупою).*

Доведення легко випливає із означення. □

Зауваження. 1. Об'єднання довільної родини піднапівгруп (підмоноїдів, підгруп) піднапівгрупою (підмоноїдом, підгрупою), взагалі кажучи, не буде. Зокрема, об'єднання двох підгруп буде підгрупою тоді й лише тоді, коли одна з цих підгруп міститься в іншій (доведіть!).

2. Очевидно, що твердження 5.2 залишається правильним для перетину довільної родини підструктур довільної алгебричної структури.

Вправа 5.3. *Доведіть, що для скінченної групи поняття підгрупи і піднапівгрупи збігаються.*

Задача 5.1. *Доведіть, що коли H — підгрупа групи G, то $H \cdot H = H$. Чи правильне зворотне твердження?*

Задача 5.2. *Доведіть, що для скінченних підгруп A і B групи G виконується рівність* $|A \cdot B| = \dfrac{|A| \cdot |B|}{|A \cap B|}$.

Задача 5.3. *Наведіть приклад нескінченної групи, кожна власна підгрупа якої має скінченний порядок.*

Задача 5.4. *Знайдіть усі скінченні підгрупи групи ізометрій паркету з*: a) *правильних трикутників*; b) *квадратів.*

Нехай тепер A — довільна непорожня підмножина групи G. Можна розглядати ті підгрупи G, які містять цю множину (такою буде, зокрема, сама G). Природно поцікавитися найменшою за включенням серед таких підгруп. Одразу виникають два питання. (1) Чи існує серед таких підгруп найменша? (2) Якщо існує, то як її знайти?

Відповідь на перше питання дає

Твердження 5.3. *Перетин усіх підгруп групи G, що містять дану непорожню підмножину A, є найменшою підгрупою G, що містить A.*

Доведення. Безпосередньо випливає із твердження 5.2. □

Найменша підгрупа, що містять дану підмножину A, позначається $\langle A \rangle$. Відповідь на друге питання — про будову $\langle A \rangle$ — дає

Твердження 5.4. *Нехай A — деяка непорожня підмножина групи G. Позначимо $A^{-1} = \{a^{-1} \mid a \in A\}$. Тоді $\langle A\rangle = \{a_1 \cdots a_k \mid k \in \mathbb{N},\ \ a_i \in A \cup A^{-1}\}$.*

Доведення. Позначимо множину $\{a_1 \cdots a_k \mid k \in \mathbb{N},\ \ a_i \in A \cup A^{-1}\}$ символом B. Включення $A \subseteq B \subseteq \langle A\rangle$ є очевидними. Тому досить показати, що B є підгрупою групи G. А це випливає із твердження 5.1, бо B замкнена відносно множення та взяття оберненого елемента. □

Твердження 5.4 можна сформулювати у трохи іншій формі:

Твердження 5.4′. *Нехай A — деяка непорожня підмножина групи G. Тоді $\langle A\rangle = \{a_1^{\varepsilon_1} \cdots a_k^{\varepsilon_k} \mid k \in \mathbb{N},\ \ a_i \in A,\ \ \varepsilon_i = \pm 1\}$.*

Наслідок 5.1. *Нехай група G комутативна і $A = \{a_1, \ldots, a_n\}$. Тоді кожний елемент підгрупи $\langle A\rangle$ можна записати у вигляді $a_1^{m_1} \cdots a_n^{m_n}$, де $m_1, \ldots, m_n \in \mathbb{Z}$ (або у вигляді $m_1a_1 + \cdots + m_na_n$, якщо G — адитивна група).*

Якщо $\langle A\rangle = G$, то A називається *системою твірних* групи G. Система твірних називається *незвідною*, якщо жодна її власна підмножина не є системою твірних. У противному разі система твірних називається *звідною*. Якщо система твірних групи G складається з скінченної кількості елементів, то кажуть, що група G є *скінченно породженою*. Якщо ж група G не має скінченних систем твірних, то група G є *нескінченно породженою*.

Приклади. 1. Нескінченною, незвідною системою твірних групи $\mathbb{Q}^*$ є, наприклад, множина всіх простих чисел разом з -1.

2. Множина всіх транспозицій є звідною системою твірних групи S_n.

3. Множина всіх чисел вигляду $\frac{1}{n}$, $n \in \mathbb{N}$, є нескінченною, звідною системою твірних групи $\mathbb{Q}$.

4. Група $\mathbb{Z}$ і всі скінченні групи є скінченно породженими.

5. Кожна з груп $\mathbb{Q}$ і $\mathbb{Q}^*$ є нескінченно породженою.

Задача 5.5. *Доведіть, що* $S_n = \langle (12),\ (23),\ \ldots,\ (n-1, n)\rangle = \langle (12),\ (13),\ \ldots,\ (1n)\rangle$.

Задача 5.6. *Доведіть, що знакозмінна група A_n при $n \geq 3$ породжується циклами довжини 3.*

Задача 5.7. *Знайдіть необхідну й достатню умову того, щоб дана множина транспозицій була (незвідною) системою твірних групи S_n.*

Задача 5.8. *Нехай транспозиції $\pi_1, \ldots, \pi_k$ утворюють незвідну систему твірних групи S_n. Доведіть, що їх добуток у будь–якому порядку $\pi_{i_1} \cdots \pi_{i_k}$ буде циклом довжини n.*

Задача 5.9.** *Доведіть, що кількість різних незвідних систем твірних групи S_n, які складаються з транспозицій, дорівнює n^{n-2}.*

Задача 5.10. *Знайдіть в групі S_n двоелементну систему твірних.*

Задача 5.11. *Знайдіть в групі всіх поворотів куба двоелементну систему твірних.*

Задача 5.12. *Доведіть, що група $\mathbb{Q}$ не має незвідних систем твірних.*

Зауважимо, що системи твірних (навіть незвідні) для однієї й тієї ж групи можуть бути влаштовані дуже по різному. Наприклад, для довільного набору $p_1, p_2, \ldots, p_k$ різних простих чисел множина чисел $a_1 = p_2\ p_3 \cdots p_k$, $a_2 = p_1\ p_3 \cdots p_k$, $\ldots$, $a_{k-1} = p_1\ p_2 \cdots p_{k-2}\ p_k$, $a_k = p_1\ p_2 \cdots p_{k-2}\ p_{k-1}$ буде незвідною системою твірних адитивної групи $\mathbb{Z}$. Звідси випливає, що $\mathbb{Z}$ має незвідні системи твірних довільної скінченної потужності.

6 Циклічні групи та порядок елемента

Дуже важливими (і в певному сенсі найпростішими) прикладами груп є ті, які мають систему твірних з одного елемента. Такі групи називаються *циклічними*.

Із твердження 5.4 випливає, що $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$, тобто циклічна група складається з усіх степенів свого твірного елемента a. Зокрема, циклічна група є комутативною.

Приклади. 1. Група $\mathbb{Z}$ складається з усіх цілих кратних числа 1. Тому $\mathbb{Z} = \langle 1 \rangle$.

2. З першого курсу відомо, що група $\mathbb{C}_n$ породжується будь–яким первісним коренем степеня n з 1. Тому вона також циклічна.

3. Адитивна група $\mathbb{Z}_n$ класів лишків за модулем числа n породжується класом $\bar{1}$.

Задача 6.1* *Доведіть, що кожна скінченнопороджена підгрупа групи* $a)$ $\mathbb{Q}$, $b)$ $\mathbb{C}_{p^\infty}$ *є циклічною.*

Означення 6.1. *Порядком* $|a|$ *елемента* a *групи* G *називається порядок* $|\langle a\rangle|$ *циклічної підгрупи* $\langle a\rangle$, *породженої елементом* a.

Твердження 6.1. *Якщо елемент* a *має скінченний порядок* n, *то* $a^n = e$ *і* n *є найменшим натуральним числом із такою властивістю. У цьому випадку для довільного цілого числа* m $a^m = a^r$, *де* r *— остача від ділення* m *на* n, *причому якщо остачі* r_1 *і* r_2 *— різні, то* $a^{r_1} \neq a^{r_2}$. *Зокрема,* $a^m = e$ *тоді й лише тоді, коли* $n|m$. *Якщо ж елемент* a *має нескінченний порядок, то* $a^n \neq e$ *для будь–якого цілого числа* $n \neq 0$.

Доведення. Нехай група $\langle a\rangle$ — скінченна. Тоді серед елементів $a^n, n \in \mathbb{Z}$, є однакові. Нехай $a^k = a^l$ і $k > l$. Тоді $a^{k-l} = e$ і $k - l \in \mathbb{N}$. Нехай тепер n — найменше з таких натуральних чисел, що $a^n = e$. Тоді всі елементи $a^1 = a$, a^2, $\ldots$, $a^n = e$ — різні. З іншого боку, нехай m — довільне ціле число і r — його остача від ділення на n. Тоді $a^m = a^{nk+r} = (a^n)^k \cdot a^r = e^k \cdot a^r = a^r$. Отже, $\langle a\rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ і $n = |a|$.

Остання частина твердження доводиться аналогічно. □

Наслідок 6.1. *Якщо елемент* a *має скінченний порядок* n, *то* $a^k = a^m$ *тоді й лише тоді, коли* $n \,\big|\, (k - m)$.

Наслідок 6.2. *Якщо елемент* a *має скінченний порядок* n, *то* $\langle a\rangle = \{e, a, a^2, \ldots, a^{n-1}\}$. *Якщо ж елемент* a *має нескінченний порядок, то* $\langle a\rangle = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\}$.

Твердження 6.2. *Якщо елемент* a *має порядок* n, *то* a^k *має порядок* $n/\text{НСД}(n, k)$.

Доведення. Нехай $d = \text{НСД}(n, k)$. За наслідком 6.1 $(a^k)^m = a^{km} = e$ тоді й лише тоді, коли $n \,\big|\, km$, тобто коли $(n/d) \,\big|\, (k/d)m$. Оскільки n/d і k/d — взаємно прості, останнє означає, що $(n/d) \,\big|\, m$. Отже, a^k має порядок n/d. □

Нагадаємо, що *функція Ойлера* $\varphi(n)$ визначається як кількість натуральних чисел, які не більші за n і взаємно прості з n.

Наслідок 6.3. *Циклічна група порядку* n *має рівно* $\varphi(n)$ *елементів порядку* n.

Група, в якій порядок кожного елемента є скінченним, називається *періодичною*.

Приклади. 1. У кожній групі є єдиний елемент порядку 1 — це нейтральний.

2. Підстановка $\left(\begin{smallmatrix}1&2&3&4&5&6&7&8&9\\3&4&5&6&7&8&9&2&1\end{smallmatrix}\right) = (13579)(2468)$ із групи S_9 має порядок 20.

3. У групі $\mathbb{R}^*$ число -1 порядку 2, а всі інші неодиничні елементи мають нескінченний порядок.

4. У групі $\mathbb{C}^*$ число z має скінченний порядок n тоді й лише тоді, коли z є первісним коренем степеня n з 1. Зокрема, в групі $\mathbb{C}^*$ є рівно $\varphi(n)$ елементів порядку n.

Задача 6.2. *Доведіть, що кожна група парного порядку містить елемент порядку* 2.

Задача 6.3. *Наведіть приклад нескінченної періодичної групи.*

Задача 6.4***.** *Доведіть, що коли елементи a і b комутують і $|a| = m$, $|b| = n$, то в групі існує елемент порядку* $\mathrm{НСК}(m, n)$.

Теорема 6.1. *Кожна підгрупа циклічної групи G є циклічною.*

Доведення. Очевидно, що одинична підгрупа E є циклічною. Нехай тепер $G = \langle a\rangle$ і $H \le G$ — неодинична підгрупа. Виберемо найменше натуральне n, для якого $a^n \in H$. Нехай тепер a^m — довільний елемент з H. Розділимо m на n з остачею: $m = nk+r$. Тоді $a^r = a^{m-nk} = a^m\cdot(a^n)^{-k} \in H$. Оскільки $r < n$, то $r = 0$. Таким чином, $a^m = a^{nk} = (a^n)^k$, тобто кожний елемент з H є степенем елемента a^n. □

7 Ізоморфізм груп

Нагадаємо, що групи $(G;*)$ і $(H;\circ)$ називаються *ізоморфними*, якщо існує така бієкція $\varphi : G \longrightarrow H$, що $\varphi(x * y) = \varphi(x) \circ \varphi(y)$ для довільних $x, y \in G$.

Приклади. 1. Якщо позначити неодиничні елементи кожної з груп: $G_1 = \{\varepsilon, (12), (34), (12)(34)\}$; $G_2 = \{\varepsilon, (13), (24), (13)(24)\}$; $G_3 = \{\varepsilon, (14), (23), (14)(23)\}$; $G_4 = \{0°, 180°, l_1, l_2\}$ — групи рухів ромба; G_5 — групи

поворотів простору навколо трьох взаємно перпендикулярних осей та групи K_4, через a, b, c, то в усіх випадках таблиця Келі кожної з груп буде мати вигляд

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Отже, множення в усіх цих групах влаштоване однаково, і вони є ізоморфними.

2. Із тотожності $\ln xy = \ln x + \ln y$ для додатних x і y випливає, що відображення $x \mapsto \ln x$ є ізоморфізмом групи $(\mathbb{R}^+;\cdot)$ на групу $(\mathbb{R};+)$.

3. Відображення $z = \cos\varphi + i\sin\varphi \mapsto \varphi$ є ізоморфізмом групи $\mathbb{C}_n$ на групу $\mathcal{C}_n$.

Твердження 7.1. *Якщо $\varphi : G \to H$ — ізоморфізм груп G та H, то:*
a) $\varphi(e_G) = e_H$, *де e_G, e_H — нейтральні елементи груп G та H відповідно;*
b) *для кожного $a \in G$ матимемо $\varphi(a^{-1}) = \varphi(a)^{-1}$, $|\varphi(a)| = |a|$.*

Доведення. Рівність $\varphi(a^{-1}) = \varphi(a)^{-1}$ випливає з того, що $\varphi(a)\cdot\varphi(a^{-1}) = \varphi(a\cdot a^{-1}) = \varphi(e_G) = e_H$. Інші співвідношення пропонуємо довести самостійно. □

Задача 7.1. *Доведіть, що група матриць* $\left\{ \pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \pm\left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right), \pm\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right), \pm\left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right) \right\}$ *($i = \sqrt{-1}$) з дією множення і група кватерніонів Q_8 — ізоморфні.*

Задача 7.2. *Доведіть, що групи поворотів куба і правильного октаедра та група S_4 — ізоморфні.*

Задача 7.3. *Доведіть, що групи $(\mathbb{Q}^+;\cdot)$ і $(\mathbb{Q};+)$ — не ізоморфні.*

В ідеалі метою теорії груп можна вважати опис усіх груп із точністю до ізоморфізму. І хоча вимога оборотності кожного елемента є дуже сильною і з ростом n кількість неізоморфних груп порядку n зростає набагато повільніше, ніж кількість неізоморфних напівгруп порядку n (див. таблицю),

n	1	2	3	4	5	6	7	8
кількість напівгруп	1	5	24	188	1915	28634	$> 1{,}5 \cdot 10^6$	$> 3{,}5 \cdot 10^9$
кількість груп	1	1	1	2	1	2	1	5

все одно груп виявляється настільки багато і вони настільки різні, що ідеал видається принципово недосяжним навіть для груп скінченного порядку.

Задача 7.4. *Обґрунтуйте якомога більше чисел цієї таблиці.*

Теорема 7.1 (Келі). *Кожна група ізоморфна деякій групі підстановок.*

Доведення. У порівнянні з доведенням теореми Келі для напівгруп (див. теорему 3.1) треба лише додатково показати, що кожне μ_a є підстановкою, тобто взаємно однозначним перетворенням множини S. Але це випливає з твердження 4.1 (b). □

Теорема 7.2. a) *Кожна циклічна група порядку n ізоморфна групі $\mathbb{Z}_n$.* b) *Кожна нескінченна циклічна група ізоморфна групі $\mathbb{Z}$.*

Доведення. a) Нехай $G = \langle a \rangle$ і $|a| = n$. Розглянемо відображення $\varphi : a^k \mapsto \overline{k} = k \bmod n$. Згідно твердження 6.1 це відображення взаємно однозначно відображає групу G на $\mathbb{Z}_n$. Позаяк

$$\varphi(a^k \cdot a^m) = \varphi(a^{k+m}) = \overline{k+m} = \overline{k} + \overline{m} = \varphi(a^k) + \varphi(a^m) \,,$$

то φ є ізоморфізмом.

b) Нехай тепер $|a| = \infty$. Знову ж таки згідно твердження 6.1 відображення $\varphi : a^k \mapsto k$ взаємно однозначно відображає групу G на $\mathbb{Z}$. Але

$$\varphi(a^k \cdot a^m) = \varphi(a^{k+m}) = k + m = \varphi(a^k) + \varphi(a^m) \,,$$

тому φ — ізоморфізм. □

Наслідок 7.1. *Циклічні групи ізоморфні тоді й лише тоді, коли вони мають однаковий порядок.*

У тих випадках, коли природа елементів циклічної групи нам байдужа, будемо говорити про циклічну групу $C_n = \{e, a, a^2, \ldots, a^{n-1}\}$ порядку n і нескінченну циклічну групу $C_\infty = \{\ldots, a^{-1}, e, a, \ldots\}$.

Теорема 6.1 стверджувала, що кожна підгрупа циклічної групи є циклічною. Тепер ми можемо розібратися з будовою підгруп циклічної групи докладніше. Із теореми 7.2 випливає, що для цього досить розглянути будову підгруп у групах $\mathbb{Z}$ і $\mathbb{Z}_n$.

Теорема 7.3 (про будову підгруп циклічної групи). a) *Кожна підгрупа групи* $\mathbb{Z}$ *має вигляд* $\langle n\rangle = n\mathbb{Z}$. *Якщо* $n \neq 0$, *то підгрупа* $n\mathbb{Z}$ *нескінченна, а тому ізоморфна самій групі* $\mathbb{Z}$. *Відповідність* $n\mathbb{Z} \leftrightarrow n$ *є бієкцією між множиною підгруп групи* $\mathbb{Z}$ *і множиною* $\mathbb{N}_0$ *невід'ємних цілих чисел. Підгрупа* $n\mathbb{Z}$ *міститься в підгрупі* $m\mathbb{Z}$ *тоді й лише тоді, коли* $m\big|n$.

b) *Кожна підгрупа групи* $\mathbb{Z}_n$ *має вигляд* $\langle\overline{d}\rangle$, *де* d *є дільником числа* n. *Підгрупа* $\langle\overline{d}\rangle$ *має порядок* n/d *і ізоморфна групі* $\mathbb{Z}_{n/d}$. *Відповідність* $\langle\overline{d}\rangle \leftrightarrow d$ *є бієкцією між множиною підгруп групи* $\mathbb{Z}_n$ *і множиною дільників числа* n. *Підгрупа* $\langle\overline{d_1}\rangle$ *міститься в підгрупі* $\langle\overline{d_2}\rangle$ *тоді й лише тоді, коли* $d_2\big|d_1$.

Доведення. a) Розглянемо довільну підгрупу $H \leq \mathbb{Z}$. Якщо $H = \{0\}$, то $H = \langle 0\rangle = 0 \cdot \mathbb{Z}$. Нехай тепер $H \neq \{0\}$. Тоді серед елементів H є натуральні числа, бо разом із числом x підгрупа H містить і $-x$, а одне з чисел $x, -x$ є натуральним. Позначимо через n найменше з них. Очевидно, що $H \geq n\mathbb{Z}$. З іншого боку, довільне число $m \in H$ можна поділити на n з остачею: $m = kn + r$. Тоді $kn \in H$, $r = m - kn \in H$ і з вибору n випливає, що $r = 0$. Отже, $m = kn$ і $H \leq n\mathbb{Z}$. Разом із попереднім включенням це дає $H = n\mathbb{Z}$.

Таким чином, кожна підгрупа $H \leq \mathbb{Z}$ має вигляд $H = n\mathbb{Z}$, де $n \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$. З іншого боку легко перевіряється, що для довільного $n \in \mathbb{N}_0$ множина $n\mathbb{Z}$ є підгрупою групи $\mathbb{Z}$. Оскільки при цьому n є найменшим елементом із $n\mathbb{Z} \cap \mathbb{N}_0$, то нерівність $n \neq m$ тягне за собою $n\mathbb{Z} \neq m\mathbb{Z}$.

Нарешті, якщо $n\mathbb{Z} \leq m\mathbb{Z}$, то $n \in m\mathbb{Z}$ і для деякого $k \quad n = mk$, тобто $m|n$. Навпаки, якщо $n = mk$, то $n \in m\mathbb{Z}$ і $n\mathbb{Z} \leq m\mathbb{Z}$.

b) Міркуючи аналогічно попередньому, вибираємо в ненульовій підгрупі $H \leq \mathbb{Z}_n$ найменший ненульовий клас лишків $\bar{d}$ і показуємо, що $H = \langle\bar{d}\rangle$. Справді, виберемо довільний елемент $\bar{m} \in H$ і поділимо m на d з остачею: $m = kd + r$, де $0 \leq r < d$. Тоді $r = 0$, бо $\bar{d}$ — найменший ненульовий клас із H. Тому $H =< \bar{d} >$. Крім того, оскільки $\bar{n} = \bar{0} \in H$, то звідси випливає, що $n = dl$ і $d|n$. З іншого боку, очевидно, що для кожного власного дільника $d|n$ множина $H = \langle\bar{d}\rangle$ є підгрупою із $\mathbb{Z}_n$, причому $\bar{d}$ є найменшим ненульовим класом лишків із цієї підгрупи. Разом із зауваженням, що $\{\bar{0}\} = \langle\bar{n}\rangle$, це дає бієкцію між множиною підгруп групи $\mathbb{Z}_n$ і множиною дільників числа n. Оскільки $\langle\bar{d}\rangle$ — циклічна група і має порядок n/d, то $\langle\bar{d}\rangle \simeq \mathbb{Z}_{n/d}$.

Нарешті, останнє твердження випливає з того, що $\langle\overline{d_1}\rangle \leq \langle\overline{d_2}\rangle$ тоді

й лише тоді, коли $\overline{d_1} \in \langle \overline{d_2} \rangle$, тобто тоді й лише тоді, коли d_1 є кратним d_2. □

Зауваження. **1.** Із теореми 7.3 зовсім не випливає, що твірними елементами підгруп циклічної групи $\mathbb{Z}_n$ повинні бути лише дільники числа n. Наприклад, у групі $\mathbb{Z}_{10}$ маємо: $\langle \overline{2} \rangle = \langle \overline{4} \rangle = \langle \overline{6} \rangle = \langle \overline{8} \rangle$.

2. Із теореми 7.3 а) випливає, що група може бути ізоморфною своїй власній підгрупі.

Наслідок 7.2. *Якщо канонічний розклад числа n має вигляд $n = p_1^{k_1} \cdots p_m^{k_m}$, то циклічна група C_n має $(k_1+1)\cdots(k_m+1)$ різних підгруп.*

Доведення випливає з теореми 7.3 а) і того, що число $n = p_1^{k_1} \cdots p_m^{k_m}$ має $(k_1 + 1)\cdots(k_m + 1)$ різних дільників. □

Наслідок 7.3. *У скінченній циклічній групі порядок підгрупи ділить порядок групи, причому для кожного дільника d порядку групи G існує єдина підгрупа $H \leq G$ порядку d.*

Доведення випливає з того, що відображення $d \mapsto n/d$ є бієкцією множини дільників числа n на себе. □

Зауваження. Теореми 7.2 і 7.3 повністю описують будову циклічних груп та їх підгруп. Після цього природно спробувати описати будову тих груп, які мають 2–елементну систему твірних. Однак, як випливає з теореми Келі і наступної задачі, це нереально навіть для скінченних груп.

Задача 7.5. *Доведіть, що $S_n = \langle (12), (123\ldots n) \rangle$.*

Ізоморфізм групи на себе називається *автоморфізмом*. Множину всіх автоморфізмів групи G позначають $\mathrm{Aut}\, G$.

Приклади. 1. Відображення $n \mapsto -n$ є автоморфізмом групи $\mathbb{Z}$.

2. Для кожної абелевої групи відображення $a \mapsto a^{-1}$ є автоморфізмом.

3. Для кожної з груп $(\mathbb{C}; +)$ і $(\mathbb{C}^*; \cdot)$ відображення $z \mapsto \overline{z}$ є автоморфізмом.

4. Відображення $A \mapsto (A^\top)^{-1}$ є автоморфізмом групи $GL_n(\mathbb{R})$.

Твердження 7.2. *Множина* $\mathrm{Aut}\, G$ *утворює групу відносно композиції перетворень.*

Доведення. Розглянемо симетричну групу $\operatorname{Sym} G$ всіх взаємно однозначних перетворень множини G. Оскільки $\operatorname{Aut} G \subseteq \operatorname{Sym} G$, то досить показати лише замкненість $\operatorname{Aut} G$ відносно композиції і взяття оберненого перетворення. Але це випливає з твердження 2.1 а). □

Зауваження. Поняття автоморфізму як ізоморфізму на себе має сенс для довільної алгебричної системи A, причому множина $\operatorname{Aut} A$ також буде утворювати групу.

Задача 7.6. *Доведіть, що кожна група порядку більшого, ніж 2 має нетривіальний автоморфізм.*

Задача 7.7. *Доведіть, що група* $\operatorname{Aut}(\mathbb{Q}^+;\cdot)$ *має потужність континуум.*

Задача 7.8. *Доведіть, що* $\operatorname{Aut} D_3 \simeq D_3$ *і* $\operatorname{Aut} D_4 \simeq D_4$. *Чи правильне аналогічне твердження для довільного* n?

Задача 7.9. *Доведіть, що для некомутативної групи* G *група* $\operatorname{Aut} G$ *є нециклічною.*

Задача 7.10. *Доведіть, що відображення* $g \mapsto g^{-1}$ *буде автоморфізмом групи* G *тоді й лише тоді, коли група* G *— комутативна.*

8 Гомоморфізми

Якщо в означенні ізоморфізму двох однотипних алгебричних систем відмовитися від вимоги бієктивності відображення φ, то приходимо до поняття гомоморфізму однієї системи $\big(M;(\omega_i)_{i\in I}\big)$ в іншу $\big(N;(\vartheta_i)_{i\in I}\big)$. Таким чином,

Означення 8.1. *Гомоморфізм системи* $\big(M;(\omega_i)_{i\in I}\big)$ *в однотипну їй систему* $\big(N;(\vartheta_i)_{i\in I}\big)$ *— це довільне відображення* $\varphi : M \to N$, *узгоджене з усіма визначеними в цих системах діями. Зокрема, гомоморфізм групи* $(G;*)$ *в групу* $(H;\circ)$ *— це таке відображення* $\varphi : G \to H$, *що*

$$\varphi(x * y) = \varphi(x) \circ \varphi(y) \quad \text{для довільних} \quad x, y \in G\,.$$

Приклади. 1. У випадку векторних просторів над одним і тим же полем гомоморфізми це не що інше як лінійні відображення.

2. Для кожної групи G є тривіальний гомоморфізм $x \mapsto e$ групи G на одиничну групу E.

3. Відображення $k \mapsto k \bmod n$ є гомоморфізмом групи $\mathbb{Z}$ на групу $\mathbb{Z}_n$ класів лишків за модулем n.

4. Відображення $A \mapsto \det A$ є гомоморфізмом мультиплікативної напівгрупи $(M_n(\mathbb{R}); \cdot)$ на напівгрупу $(\mathbb{R}; \cdot)$, а також гомоморфізмом групи $GL_n(\mathbb{R})$ на групу $\mathbb{R}^*$. Однак це відображення не є гомоморфізмом алгебричної системи $(M_n(\mathbb{R}); \cdot, +)$ на систему $(\mathbb{R}; \cdot, +)$.

5. Відображення $x \mapsto |x|$ є гомоморфізмом групи $\mathbb{R}^*$ (групи $\mathbb{C}^*$) на групу $\mathbb{R}^+$.

6. Відображення $z = r(\cos\psi + i\sin\psi) \mapsto \arg z = \psi$ є гомоморфізмом групи $\mathbb{C}^*$ у групу всіх поворотів площини навколо фіксованої точки.

Твердження 8.1. *Якщо $\varphi : G \to H$ — гомоморфізм груп, то:*
a) *$\varphi(e_G) = e_H$, де e_G, e_H — нейтральні елементи груп G та H відповідно;*
b) *для кожного $a \in G$ матимемо $\varphi(a^{-1}) = \varphi(a)^{-1}$, а якщо до того ж a — елемент скінченного порядку, то $|\varphi(a)| \,\big|\, |a|$.*

Доведення. Доведемо лише другу частину п. b), а решту пропонуємо довести самостійно. Нехай $|a| = n$. Тоді $a^n = e_G$, звідки $\varphi(a)^n = \varphi(a^n) = \varphi(e_G) = e_H$. Із твердження 6.1 тепер випливає, що $|\varphi(a)| \,\big|\, n$. □

Твердження 8.2. *Якщо $\varphi : G \to H$ — гомоморфізм груп, то:*
a) *образ $\varphi(A)$ довільної підгрупи $A \leq G$ буде підгрупою групи H;*
b) *повний прообраз $\varphi^{-1}(B)$ довільної підгрупи $B \leq H$ буде підгрупою групи G.*

Доведення. Замкненість відповідних множин відносно множення і взяття оберненого елемента випливає з рівностей $\varphi(a)\varphi(b) = \varphi(ab)$ і $\varphi(a)^{-1} = \varphi(a^{-1})$ та замкненості відносно цих дій підгруп A і B. □

Окремі класи гомоморфізмів одержали спеціальні назви. Зокрема, ін'єктивні гомоморфізми називаються *мономорфізмами*, а сюр'єктивні — *епіморфізмами*. Гомоморфізм $\varphi : G \to G$ групи G в себе називається *ендоморфізмом*.

Вправа 8.1. *Доведіть, що відображення $n \mapsto 2n$ є ін'єктивним ендоморфізмом групи $\mathbb{Z}$, а відображення $z \mapsto z^2$ — сюр'єктивним ендоморфізмом групи $\mathbb{C}^*$, але жодне з цих відображень не є автоморфізмом.*

Задача 8.1. *Чи існують епіморфізми*: a) $\mathbb{Z} \to \mathbb{Q}$; b) $\mathbb{Q} \to \mathbb{Z}$; c) $\mathbb{Q} \to \mathbb{Q}^*$; d) $\mathbb{Q}^* \to \mathbb{Z}$; e) $\mathbb{Q}^* \to \mathbb{Q}$?

Якщо $\varphi : G \to H$ — гомоморфізм груп, то його *ядром* називається множина $\operatorname{Ker}\varphi = \{g \in G \mid \varphi(g) = e_H\}$, де e_H — нейтральний елемент групи H, а його *образом* називається множина $\operatorname{Im}\varphi = \{h \in H \mid h = \varphi(g)$ для деякого $g \in G\}$, Із твердження 8.2 одразу випливає

Наслідок 8.1. *Якщо $\varphi : G \to H$ — гомоморфізм груп G та H, то його ядро $\operatorname{Ker}\varphi$ є підгрупою G, а образ $\operatorname{Im}\varphi$ — підгрупою H.*

Твердження 8.3. *Якщо $\varphi : G \to H$ — гомоморфізм груп і $\varphi(a) = b$, то $\varphi^{-1}(b) = a \cdot \operatorname{Ker}\varphi = \operatorname{Ker}\varphi \cdot a$.*

Доведення. Якщо $x \in \operatorname{Ker}\varphi$, то $\varphi(ax) = \varphi(a)\varphi(x) = be_H = b$. Отже, $a \cdot \operatorname{Ker}\varphi \subseteq \varphi^{-1}(b)$. З іншого боку, якщо $\varphi(y) = b$, то $y = a \cdot a^{-1}y$ і $\varphi(a^{-1}y) = \varphi(a^{-1})\varphi(y) = b^{-1}b = e_H$. Тому $y \in a \cdot \operatorname{Ker}\varphi$. Таким чином, $\varphi^{-1}(b) = a \cdot \operatorname{Ker}\varphi$. Рівність $\varphi^{-1}(b) = \operatorname{Ker}\varphi \cdot a$ доводиться аналогічно. □

Наслідок 8.2. a) *Якщо $\varphi : G \to H$ — гомоморфізм груп, то $|G| = |\operatorname{Ker}\varphi| \cdot |\varphi(G)|$.*
b) *Гомоморфізм $\varphi : G \to H$ є ін'єктивним відображенням тоді й лише тоді, коли $\operatorname{Ker}\varphi = E$.*

Твердження 8.4. *Гомоморфний образ циклічної групи є циклічною групою.*

Доведення. Якщо a — твірний елемент групи G і $\varphi : G \to H$ — гомоморфізм, то з рівності $\varphi(a^k) = \varphi(a)^k$ випливає, що $\varphi(a)$ є твірним елементом образу $\varphi(G)$. □

Вправа 8.2. *Доведіть, що гомоморфний образ скінченної (відповідно абелевої, періодичної) групи є скінченною (відповідно абелевою, періодичною) групою.*

9 Класи суміжності і нормальні підгрупи

Твердження 8.3 є підставою для наступного означення.

Означення 9.1. *Нехай H — підгрупа групи G. Для довільного $g \in G$ множина $gH = \{gh \mid h \in H\}$ називається лівим класом суміжності*

групи G за підгрупою H. Елемент g називається представником класу суміжності gH. Аналогічно визначаються праві класи суміжності $Hg = \{hg \mid h \in H\}$ групи G за підгрупою H.

Оскільки $e \in H$ і $ge = eg = g$, то кожен із класів суміжності gH і Hg містить свого представника g. Крім того, серед лівих (правих) класів суміжності за підгрупою H зустрічається і сама H. Справді, $H = eH = He$.

Твердження 9.1. *Довільні два ліві (праві) класи суміжності групи G за підгрупою H або збігаються, або не мають спільних елементів.*

Доведення. Нехай g_1H і g_2H — два ліві класи суміжності. Припустимо, що перетин $g_1H \cap g_2H$ не є порожнім, і нехай $a = g_1h_1 = g_2h_2$ — якийсь елемент із цього перетину. Тоді для довільного елемента g_2h із класу суміжності g_2H маємо: $g_2h = g_1h_1h_2^{-1} \cdot h = g_1 \cdot h_1h_2^{-1}h$. Оскільки $h_1h_2^{-1}h \in H$, то $g_2h \in H$ і $g_2H \subseteq g_1H$. Включення $g_1H \subseteq g_2H$ доводиться аналогічно, а тому $g_1H = g_2H$.

Для правих класів суміжності доведення аналогічне. □

Із твердження 9.1 випливає, що ліві класи суміжності групи G за підгрупою H утворюють розбиття групи G, тобто G розпадається в *диз'юнктне об'єднання* (тобто об'єднання множин, що не перетинаються) лівих класів суміжності за підгрупою H:

$$G = H \cup g_2H \cup g_3H \cup \cdots = \bigcup_i g_iH$$

(вважається, що $g_1 = e$, і замість eH пишемо просто H). Інколи, як відгомін тих часів, коли об'єднання множин називали їх сумою і позначали знаком $+$, використовується запис

$$G = H + g_2H + g_3H + \cdots .$$

Аналогічні розклади можна написати і для правих класів суміжності.

Приклади. 1. Класами суміжності групи $\mathbb{Z}$ за підгрупою $n\mathbb{Z}$ є класи лишків за модулем n.

2. Група S_n має 2 класи суміжності за підгрупою A_n, які одночасно є і лівими, і правими: сама A_n і множина всіх непарних підстановок.

3. Класами суміжності (одночасно лівими і правими) групи $GL_n(\mathbb{R})$ за підгрупою $SL_n(\mathbb{R})$ є множини матриць з одним і тим же визначником.

4. Ліві класи суміжності групи S_3 за підгрупою $H = \{\varepsilon, (12)\}$ мають вигляд $\varepsilon H = H$, $(13)H = \{(13), (132)\}$, $(23)H = \{(23), (123)\}$, а праві — $H\varepsilon = H$, $H(13) = \{(13), (123)\}$, $H(23) = \{(23), (132)\}$. Таким чином, ліві і праві класи суміжності за однією і тією ж підгрупою можуть не збігатися.

Якщо в класі суміжності gH вибрати довільний елемент g_1, то класи gH і g_1H будуть мати спільний елемент g_1 і, згідно твердження 9.1, будуть збігатися. Отже, довільний елемент лівого класу суміжності можна вибирати представником цього класу.

Аналогічне зауваження стосується і правих класів суміжності.

Твердження 9.2. *Нехай H — підгрупа групи G. Тоді*: a) $aH = bH \Leftrightarrow a^{-1}b \in H \Leftrightarrow b^{-1}a \in H$;
b) $Ha = Hb \Leftrightarrow ba^{-1} \in H \Leftrightarrow ab^{-1} \in H$.

Доведення. Якщо $aH = bH$, то існує такий елемент $h \in H$, що $b = ah$. Але тоді $a^{-1}b = h \in H$.

Навпаки, якщо $a^{-1}b = h \in H$, то $b = ah$ і перетин $aH \cap bH$ не пустий, бо містить елемент b. Із твердження 9.1 тоді випливає, що $aH = bH$.

Інші рівносильності доводяться аналогічно. □

Твердження 9.3. *Усі класи суміжності (ліві та праві) групи G за підгрупою H рівнопотужні.*

Доведення. Із того, що в групі можна скорочувати (твердження 4.1), випливає, що відображення $H \to gH$, $h \mapsto gh$, є бієкцією підгрупи H на клас суміжності gH, а тому кожен із лівих класів суміжності за підгрупою H рівнопотужний цій підгрупі. Аналогічно для правих класів. □

Нехай тепер група G має скінченний порядок n, а її підгрупа H — порядок k. Позначимо кількість лівих класів суміжності за підгрупою H через m_l, а кількість правих — через m_r. Тоді з тверджень 9.1 і 9.3 випливає, що

$$n = m_l k = m_r k \ . \tag{1}$$

З цієї рівності випливає кілька важливих наслідків.

Наслідок 9.1 (теорема Лагранжа). *У скінченній групі порядок кожної підгрупи ділить порядок групи.*

Наслідок 9.2. *У скінченній групі порядок кожного елемента ділить порядок групи.*

Доведення. Це випливає з означення порядку елемента і теореми Лагранжа. □

Наслідок 9.3. *Якщо порядок групи є простим числом, то вона не містить нетривіальних підгруп. Зокрема, кожна група простого порядку є циклічною.*

Доведення. Оскільки просте число p має лише два дільники — 1 і p то з теореми Лагранжа випливає, що підгрупа може мати або порядок 1 (і тоді вона збігається з одиничною), або p (і тоді вона збігається з усією групою). Крім того, для довільного $a \neq e$ підгрупа $\langle a \rangle$ не є одиничною, а тому збігається з усією групою. □

Зауваження. 1. З останнього доведення випливає, що в циклічній групі простого порядку кожний неодиничний елемент є твірним.

2. Теорема Лагранжа і наслідки 9.3 та 9.2 — це початок дуже великої і важливої серії теорем, які щось стверджують про властивості групи, виходячи з арифметичних властивостей її порядку.

Задача 9.1. *Доведіть, що коли в групі G порядку n для кожного дільника k числа n рівняння $x^k = e$ має не більше k розв'язків, то група G — циклічна.*

Вказівка. Група G містить не більше однієї циклічної підгрупи порядку n, тому, за наслідком 6.3, вона містить не більше $\varphi(n)$ елементів порядку n. Далі скористайтесь рівністю $n = \sum_{k|n} \varphi(k)$ і наслідком 9.2.

Задача 9.2. *Доведіть, що для довільних підгруп H_1 і H_2 групи G з рівності $g_1H_1 = g_2H_2$ випливає рівність $H_1 = H_2$.*

Задача 9.3. a) *Доведіть, що для кожного дільника k числа* 24 *група S_4 містить підгрупу порядку k.*
b) *Доведіть, що група A_4 не містить підгруп порядку* 6.

Таким чином, у деяких групах порядок підгрупи може бути довільним дільником порядку групи, як, наприклад, у групі S_4 або в циклічних групах (останнє випливає з теореми 7.3 b). Однак приклад групи A_4 показує, що в загальному випадку теорема Лагранжа дає лише необхідну умову для існування підгрупи даного порядку.

Твердження 9.4. *Відображення $gH \mapsto Hg^{-1}$ є бієкцією множини лівих класів суміжності групи G за підгрупою H на множину правих класів суміжності за цією підгрупою.*

Доведення. Треба довести коректність, ін'єктивність і сюр'єктивність даного відображення.

Коректність випливає з твердження 9.2. Справді, якщо $g_1H = g_2H$, то $g_1^{-1}g_2 = g_1^{-1}(g_2^{-1})^{-1} \in H$ і $Hg_1^{-1} = Hg_2^{-1}$.

Ін'єктивність доводиться аналогічно: якщо $g_1H \neq g_2H$, то $g_1^{-1}g_2 = g_1^{-1}(g_2^{-1})^{-1} \notin H$ і $Hg_1^{-1} \neq Hg_2^{-1}$.

Сюр'єктивність випливає з того, що довільний правий клас суміжності Hg є образом лівого класу $g^{-1}H$. □

Таким чином, для довільних групи G та її підгрупи H кількість лівих класів суміжності за підгрупою H завжди дорівнює кількості правих класів за цією підгрупою (зауважимо, що для скінченних груп це випливає і з рівності (1)). Ця кількість називається *індексом* підгрупи H у групі G і позначається $|G : H|$.

Із твердження 9.4 і зауваження, що ліві (праві) класи суміжності за підгрупою утворюють розбиття групи, одразу випливає

Наслідок 9.4. $|G| = |G : H| \cdot |H|$. *Зокрема, в скінченній групі індекс кожної підгрупи ділить порядок групи.*

Приклади. a) $|D_n : \mathcal{C}_n| = 2$; b) $|S_n : A_n| = 2$; c) $|S_4 : K_4| = 6$; d) $|\mathbb{Q}^* : \mathbb{Q}^+| = 2$; e) $|\mathbb{Q}^* : \{\pm 1\}| = \infty$.

Задача 9.4. *Доведіть, що*: a) *всі нетривіальні підгрупи групи* $\mathbb{Z}$ *мають скінченні індекси*; b) *всі нетривіальні підгрупи групи* $\mathbb{Q}$ *мають нескінченні індекси.*

Задача 9.5. *Доведіть, що коли* $A < B < G$, *то* $|G : A| = |G : B| \cdot |B : A|$.

Задача 9.6. *Доведіть, що з рівності* $|G : A| = |B : A \cap B|$ *випливає рівність* $G = A \cdot B = B \cdot A$.

Задача 9.7*. *Доведіть, що перетин двох підгруп скінченного індексу також буде підгрупою скінченного індексу.*

Задача 9.8. *Нехай* p *і* q *— прості числа і* $p < q$. *Доведіть, що кожна група порядку* pq *містить*: a) *підгрупу порядку* p; b)* *підгрупу порядку* q.

Підгрупу $H \leq G$ називають *нормальною* (або *інваріантною*) підгрупою групи G (і позначають $H \lhd G$), якщо ліві і праві класи суміжності за цією підгрупою збігаються, тобто якщо $gH = Hg$ для всіх $g \in G$.

У випадку нормальної підгрупи можна говорити просто про класи суміжності за підгрупою.

Приклади. 1. Тривіальні підгрупи E і G групи G є нормальними, бо $g \cdot \{e\} = \{e\} \cdot g = \{g\}$ і $gG = Gg = G$ для для довільного $g \in G$.

2. Усі підгрупи абелевої групи є нормальними.

3. Із твердження 8.3 випливає, що ядро $\operatorname{Ker} \varphi$ довільного гомоморфізму $\varphi : G \to H$ буде нормальною підгрупою групи G.

Твердження 9.5. *Кожна підгрупа $H \leq G$ індексу 2 є нормальною в G.*

Доведення. Сама підгрупа H завжди є і лівим, і правим класом суміжності: $eH = He = H$. Оскільки класи суміжності утворюють розбиття групи, то множина $G \setminus H$ елементів, що лишились, також має бути і лівим, і правим класом суміжності. □

Приклад. Із цього твердження випливає, що $\mathcal{C}_n \lhd D_n$ і $A_n \lhd S_n$ як підгрупи індексу 2.

Теорема 9.1 (критерій нормальності підгрупи). *Підгрупа $H \leq G$ буде нормальною в G тоді й лише тоді, коли для довільних елементів $g \in G$ і $h \in H$ елемент $g^{-1}hg$ також належить H.*

Доведення. Необхідність. Нехай $H \lhd G$ і $g \in G$, $h \in H$ — довільні елементи. Із рівності $Hg = gH$ випливає, що існує такий елемент $h_1 \in H$, що $hg = gh_1$. Але тоді $g^{-1}hg = h_1 \in H$.

Достатність. Нехай $g \in G$ і $x \in gH$ — довільні елементи. Тоді існує такий $h \in H$, що $x = gh$. Із рівності $x = ghg^{-1} \cdot g = (g^{-1})^{-1}hg^{-1} \cdot g$ і того, що $(g^{-1})^{-1}hg^{-1} \in H$, випливає, що $x \in Hg$. Тому $gH \subseteq Hg$. Аналогічно доводиться включення $Hg \subseteq gH$. Отже, $Hg = gH$. □

Приклади. 1. Із властивості визначника добутку матриць випливає, що для довільних матриць $A \in GL_n(P)$ і $B \in SL_n(P)$ добуток $A^{-1}BA$ належить підгрупі $SL_n(P)$, бо $\det(A^{-1}BA) = \det(A^{-1}) \det B \det A = (\det A)^{-1} \cdot 1 \cdot \det A = 1$. Тому $SL_n(P) \lhd GL_n(P)$.

2. Зафіксувавши на площині який–небудь трикутник і вказавши порядок обходу його вершин, можна двома різними способами визначити орієнтацію площини. Кожен рух площини або зберігає її орієнтацію, або

змінює цю орієнтацію на протилежну. Очевидно, що множина H тих рухів площини, які зберігають орієнтацію, утворює підгрупу в групі G всіх рухів площини. Якщо $\varphi \in H$, то для довільного руху $\psi \in G$ композиція $\psi^{-1} \circ \varphi \circ \psi$ двічі міняє орієнтацію на протилежну, а тому в результаті зберігає початкову орієнтацію. Отже, $\psi^{-1} \circ \varphi \circ \psi \in H$ для довільних $\varphi \in H$ і $\psi \in G$. Це означає, що $H \lhd G$.

Із критерію нормальності випливає, що нормальна підгрупа $H \lhd G$ буде нормальною і в кожній проміжній підгрупі $H \leq F \leq G$.

Твердження 9.6. *Якщо $\varphi : G \to H$ — гомоморфізм груп, то*: а) *образ $\varphi(A)$ нормальної підгрупи $A \lhd G$ буде нормальною підгрупою групи $\varphi(G)$*; b) *повний прообраз $\varphi^{-1}(B)$ нормальної підгрупи $B \lhd H$ буде нормальною підгрупою групи G.*

Доведення. а) Нехай $u \in \varphi(G)$ і $v \in \varphi(A)$ — довільні. Виберемо такі $g \in G$ і $a \in A$, що $u = \varphi(g)$, $v = \varphi(a)$. Із $A \lhd G$ випливає, що $g^{-1}ag \in A$. Тому $\varphi(g^{-1}ag) = \varphi(g)^{-1}\varphi(a)\varphi(g) = u^{-1}vu \in \varphi(A)$ і $\varphi(A) \lhd \varphi(G)$.

Твердження b) доводиться аналогічно. □

Вправа 9.1. *Наведіть приклад таких груп G і H, нормальної підгрупи $N \lhd G$ і гомоморфізму $\varphi : G \to H$, що $\varphi(N) \not\lhd H$.*

Твердження 9.7. *Якщо H_1 і H_2 — нормальні підгрупи групи G, то їх перетин $H_1 \cap H_2$ і добуток $H_1 \cdot H_2 = \{h_1h_2 \mid h_1 \in H_1, h_2 \in H_2\}$ також є нормальними підгрупами.*

Доведення. Перше твердження випливає з того, що для довільних $g \in G$ і $h \in H_1 \cap H_2$ добуток $g^{-1}hg$ належить кожній з підгруп H_1 і H_2, а друге — з рівності $g^{-1}h_1h_2g = g^{-1}h_1g \cdot g^{-1}h_2g$. □

Задача 9.9. *Доведіть, що коли A — нормальна підгрупа групи G, то для довільної підгрупи $B \leq G$ перетин $A \cap B$ є нормальною підгрупою групи B.*

Зауважимо однак, що відношення "бути нормальною підгрупою" не є транзитивним. Справді, K_4 є нормальною підгрупою в A_4 (перевірте!). Оскільки K_4 — абелева, то кожна з трьох її підгруп порядку 2 буде нормальною в K_4. Однак жодна з них не буде нормальною в A_4 (перевірте!).

Вправа 9.2. *Покажіть, що жодна із підгруп* $G_1 = \{\varepsilon, (12), (34), (12)(34)\}$, $G_2 = \{\varepsilon, (13), (24), (13)(24)\}$, $G_3 = \{\varepsilon, (14), (23), (14)(23)\}$ *не є нормальною підгрупою групи* S_4.

Задача 9.10 (теорема Пуанкаре).* *Доведіть, що коли група* G *має власну підгрупу скінченного індексу, то* G *має і власну нормальну підгрупу скінченного індексу.*

Вказівка. Використайте зад. 9.7.

10 Факторструктури

Перехід до факторструктури — це спосіб побудови за відомою алгебричною структурою нових структур, який ґрунтується на важливій для багатьох розділів математики конструкції "склеювання" — утворення фактормножини за відношенням еквівалентності.

Нагадаємо, що бінарне відношення $\sim$ на множині M називається *відношенням еквівалентності,* якщо воно
a) *рефлексивне* (тобто $a \sim a$ для кожного $a \in M$),
b) *симетричне* (тобто $a \sim b$ тягне за собою $b \sim a$), і
c) *транзитивне* (тобто для довільних $a, b, c \in M$ із $a \sim b$ і $b \sim c$ випливає $a \sim c$).

Серед усіх відношень еквівалентності на множині M є найменше, коли кожний елемент еквівалентний лише собі (це відношення збігається зі звичайною рівністю), і найбільше, коли будь–які два елементи оголошуються еквівалентними (останнє відношення інколи називають *тотальним*).

Якщо на множині M задано відношення еквівалентності $\sim$, то для $a \in M$ через $[a]$ або $\bar{a}$ позначають *клас еквівалентності* елемента a, тобто множину $\{b \in M \,|\, a \sim b\}$. Класи еквівалентності завжди утворюють розбиття множини M. Для відношення рівності всі класи еквівалентності одноелементні, а тотальне відношення має лише один клас еквівалентності, який збігається з множиною M.

Множина $\{[a] \,\big|\, a \in M\}$ усіх класів еквівалентності називається *фактормножиною* множини M за відношенням еквівалентності $\sim$. Інколи її позначають $M/\!\sim$. Відображення $M \to M/\!\sim$, $a \mapsto [a]$, є, очевидно, сюр'єктивним. Його називають *відображенням факторизації* або *канонічним відображенням* множини M на фактормножину $M/\!\sim$.

Приклади. 1. Відношення "вчитися в одній групі", "спеціалізуватися по одній кафедрі", "вчитися на одному курсі" і т.п. є відношеннями еквівалентності на множині студентів механіко–математичного факультету Київського національного університету (що буде класами еквівалентності?).

2. Відношення "мати однакову площу" є відношенням еквівалентності на множині всіх опуклих многокутників площини.

3. Відношення "давати однакову остачу при діленні на 5" є відношенням еквівалентності на множині $\mathbb{Z}$. Класами еквівалентності будуть класи лишків за модулем числа 5.

4. Важливим для теорії груп прикладом відношення еквівалентності на групі є відношення "належати до одного лівого (правого) класу суміжності за даною підгрупою H". У випадку нормальної підгрупи ці два відношення збігаються, а класами еквівалентності будуть класи суміжності за підгрупою H.

В алгебрі для побудови факторструктур використовуються не будь–які відношення еквівалентності, а лише ті, які узгоджені з діями на відповідних множинах.

Означення 10.1. *Відношення еквівалентності $\sim$ на множині M називається узгодженим з бінарною дією $*$ на M, якщо з умов $a_1 \sim a_2$ і $b_1 \sim b_2$ завжди випливає, що $a_1 * b_1 \sim a_2 * b_2$.*

Узгодженість відношення еквівалентності з діями інших арностей визначається аналогічно.

Означення 10.2. *Відношення еквівалентності, узгоджене з усіма діями алгебричної системи $\big(M; (\omega_i)_{i\in I}\big)$, називається конгруенцією на цій системі.*

На кожній алгебричній системі є дві *тривіальні конгруенції* — відношення рівності і тотальне відношення. Питання про існування та будову інших конгруенцій є одним з найважливіших при дослідженні будь–якої алгебричної системи.

Приклади. 1. Відношення $\equiv (\mathrm{mod}\ n)$ є конгруенцією на $(\mathbb{Z}; +, \cdot)$.

2. Розбиття $\mathbb{N} = \{1\} \cup \ \{2\} \cup \{2k+1 \,|\, k \geq 1\} \cup \{2k \,|\, k > 1\}$ визначає конгруенцію алгебричної системи $(\mathbb{N}; +, \cdot)$.

Задача 10.1. *Доведіть, що кожна конгруенція на* $(\mathbb{Z}; +, \cdot)$ *має вигляд* $\equiv (\mathrm{mod}\ n)$ *для деякого* n.

Задача 10.2. *Опишіть усі конгруенції на алгебричній системі* $(\mathbb{N}; +, \cdot)$.

Якщо відношення еквівалентності $\sim$ на множині M узгоджене з дією $*$ на M, то аналогічну дію можна природним чином визначити і на фактормножині $M/\sim$ (за новою дією звичайно зберігається те ж саме позначення):

$$\overline{a} * \overline{b} := \overline{a * b}\,. \tag{2}$$

Таким чином, щоб застосувати дію $*$ до двох класів еквівалентності, треба взяти по довільному представнику в кожному з цих класів і застосувати дію $*$ до цих представників. Клас, у який попаде одержаний результат, і є результатом застосування дії $*$ до початкових класів. Коректність означення, тобто незалежність результату від вибору представників, гарантується узгодженістю відношення еквівалентності з дією. Дійсно, якщо $a_1 \sim a$, $b_1 \sim b$, то $a_1 * b_1 \sim a * b$ і $\bar{a} * \bar{b} = \overline{a * b} = \overline{a_1 * b_1} = \bar{a}_1 * \bar{b}_1$.

Аналогічно на фактормножину $M/\sim$ переносяться й узгоджені з цією еквівалентністю дії інших арностей.

Таким чином, у випадку конгруенції $\sim$ на алгебричній структурі $\big(M; (\omega_i)_{i\in I}\big)$ всі визначені в цій структурі дії можна перенести на фактормножину $M/\sim$. У результаті одержуємо нову алгебричну структуру $\big(M/\sim; (\omega_i)_{i\in I}\big)$, яка називається *факторструктурою* структури M за конгруенцією $\sim$.

Приклади. 1. Якщо конгруенція $\sim$ збігається з відношенням рівності, то всі класи еквівалентності одноелементні і факторструктура $M/\sim$ природно ототожнюється з початковою структурою M.

2. У випадку кільця $(\mathbb{Z}; +, \cdot)$ і конгруенції $\equiv\ (\mathrm{mod}\ n)$ факторструктурою є кільце $\mathbb{Z}_n$ класів лишків за модулем числа n.

3. Для конгруенції на алгебричній системі $(\mathbb{N}; +, \cdot)$, яка описана в прикладі 2 на стор. 47, таблички додавання і множення факторсистеми $(\mathbb{N}/\sim; +, \cdot)$ виглядають наступним чином (для зручності класи $\{2k+1 \,|\, k \geq 1\}$ і $\{2k \,|\, k > 1\}$ позначені відповідно a і b):

$+$	1	2	a	b
1	2	a	b	a
2	a	b	a	b
a	b	a	b	a
b	a	b	a	b

,

$\times$	1	2	a	b
1	1	2	a	b
2	2	b	b	b
a	a	b	a	b
b	b	b	b	b

.

Твердження 10.1. *Нехай відношення $\sim$ є конгруенцією на алгебричній структурі $\big(M;(\omega_i)_{i\in I}\big)$. Тоді відображення $\pi : a \mapsto \overline{a}$ є епіморфізмом структури M на факторструктуру $\big(M/\sim;(\omega_i)_{i\in I}\big)$.*

Доведення. Сюр'єктивність відображення π очевидна, а гомоморфність випливає з означення дій на факторструктурі. □

Епіморфізм π з твердження 10.1 називається *канонічним* (або *природним*).

Важливим є питання про те, які властивості дій початкової структури успадковуються факторструктурою. До таких належать у першу чергу ті, які мають вигляд тотожностей (наприклад, асоціативність чи комутативність). Успадковується і наявність нейтрального елемента та оберненого (протилежного) елемента. Але певні властивості, наприклад, скоротність, можуть і не успадковуватися (згадайте, що вам відомо про скоротність у кільці класів лишків $\mathbb{Z}_n$).

Твердження 10.2. *Нехай $\varphi : M \to N$ — гомоморфізм однотипних алгебричних систем $\big(M;(\omega_i)_{i\in I}\big)$ і $\big(N;(\tau_i)_{i\in I}\big)$. Покладемо*

$$a \sim_\varphi b :\Leftrightarrow \varphi(a) = \varphi(b)\ . \tag{3}$$

Тоді відношення $\sim_\varphi$ є конгруенцією на алгебричній системі M.

Доведення. Доведемо, наприклад, узгодженість відношення $\sim_\varphi$ з визначеною на M дією ω_i арності n. Справді, якщо $a_1 \sim_\varphi b_1, \ldots, a_n \sim_\varphi b_n$ для $a_1, \ldots, a_n, b_1, \ldots, b_n \in M$, то

$$\varphi(\omega_i(a_1,\ldots,a_n)) = \vartheta_i(\varphi(a_1),\ldots,\varphi(a_n)) =$$

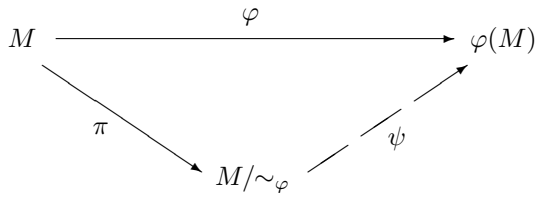
$$= \vartheta_i(\varphi(b_1),\ldots,\varphi(b_n)) = \varphi(\omega_i(b_1,\ldots,b_n)),$$

тобто відношення $\sim_\varphi$ узгоджене з дією ω_i. □

Приклади. 1. Відображення $\varphi : \mathbb{Z} \to \mathbb{C}^*$, визначене правилом $k \mapsto \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$, є гомоморфізмом груп. У цьому випадку $\sim_\varphi$ збігається з відношенням $\equiv (\mathrm{mod}\ n)$.

2. Відображення $\varphi : \mathbb{C}^* \to \mathbb{R}^*$, визначене правилом $x \mapsto |x|$, є гомоморфізмом груп. При зображенні комплексних чисел точками площини класами еквівалентності конгруенції $\sim_\varphi$ будуть усі можливі кола з центром у початку координат.

Теорема 10.1 (основна теорема про гомоморфізми алгебричних систем). *Нехай $\varphi : M \to N$ — гомоморфізм однотипних алгебричних систем $\big(M; (\omega_i)_{i\in I}\big)$ та $\big(N; (\tau_i)_{i\in I}\big)$, а $\sim_\varphi$ — відповідна конгруенція на M. Тоді відображення $\psi : M/\!\sim_\varphi \longrightarrow \varphi(M)$, $\overline{a} \mapsto \varphi(a)$, є ізоморфізмом факторсистеми $M/\!\sim_\varphi$ на образ $\varphi(M)$ системи M при гомоморфізмі φ, а діаграма*



де $\pi : M \to M/\!\sim_\varphi$ — канонічний епіморфізм, є комутативною.

Доведення. а) *Коректність* визначення ψ. Виберемо довільного представника $b \in \overline{a}$. Тоді $b \sim_\varphi a$ і $\varphi(b) = \varphi(a)$. А тому $\psi(\overline{b}) = \varphi(b) = \varphi(a) = \psi(\overline{a})$.

b) *Ін'єктивність* ψ:

$$\psi(\overline{a}) = \psi(\overline{b}) \Rightarrow \varphi(a) = \varphi(b) \Rightarrow a \sim_\varphi b \Rightarrow \overline{a} = \overline{b}\,.$$

c) *Сюр'єктивність* ψ. Якщо $b \in \varphi(M)$, то існує таке $a \in M$, що $\varphi(a) = b$. Але тоді $\psi(\overline{a}) = \varphi(a) = b$.

d) *Гомоморфність* ψ. Якщо ω_i — якась дія на M арності n, то для довільних $a_1, \ldots, a_n \in M$ маємо:

$$\psi(\omega_i(\overline{a}_1, \ldots, \overline{a}_n)) = \psi(\overline{\omega_i(a_1, \ldots, a_n)}) = \varphi(\omega_i(a_1, \ldots, a_n)) =$$

$$= \vartheta_i(\varphi(a_1), \ldots, \varphi(a_n)) = \vartheta_i(\psi(\overline{a}_1), \ldots, \psi(\overline{a}_n)),$$

тобто відображення ψ узгоджене з діями на M.

e) *Комутативність* діаграми. Для довільного $a \in M$ маємо: $\varphi(a) = \psi(\overline{a}) = \psi(\pi(a))$, тому $\varphi = \pi\psi$. □

Про задовільний опис усіх конгруенцій для довільних алгебричних систем можна лише мріяти. Але конгруенції на групах влаштовані відносно просто.

Теорема 10.2. *Відношення еквівалентності на групі G буде конгруенцією тоді й лише тоді, коли класи еквівалентності цього відношення є класами суміжності за деякою нормальною підгрупою.*

Доведення. Необхідність. Нехай $\sim$ — конгруенція на групі G. Позначимо символом $\cdot$ дію на G і розглянемо той клас еквівалентності H, який містить одиницю e. Тоді для довільних $a, b \in H$ маємо: $a \sim e$, $b \sim e$, звідки $a \cdot b \sim e \cdot e = e$, тобто $ab \in H$. Крім того, з $a^{-1} \sim a^{-1}$ випливає, що $a \cdot a^{-1} \sim e \cdot a^{-1}$, тобто $e \sim a^{-1}$. Отже, H є підгрупою.

Далі, для довільних $g_1, g_2 \in G$ із $g_2^{-1} \sim g_2^{-1}$ випливає, що

$$g_1 \sim g_2 \quad \Leftrightarrow \quad g_1 \cdot g_2^{-1} \sim g_2 \cdot g_2^{-1} = e \,,$$

Отже, $g_1 \sim g_2$ тоді й тільки тоді, коли $g_1 \cdot g_2^{-1} \in H$, тобто коли g_1 і g_2 належать одному правому класові суміжності за підгрупою H.

Аналогічно доводиться, що $g_1 \sim g_2$ тоді й тільки тоді, коли $g_2^{-1} \cdot g_1 \in H$, тобто коли g_1 і g_2 належать одному лівому класові суміжності за підгрупою H.

Таким чином, класи еквівалентності конгруенції $\sim$ є класами суміжності за підгрупою H, причому ліві і праві класи збігаються, тобто підгрупа H є нормальною.

Достатність. Навпаки, нехай H є нормальною підгрупою групи G. Розглянемо відношення еквівалентності $\sim$, класами еквівалентності якого є класи суміжності за підгрупою H. Нехай $a \sim a_1$ і $b \sim b_1$. Тоді існують такі $h_1 \in H$ і $h_2 \in H$, що $a_1 = ah_1$ і $b_1 = bh_2$. Тому $a_1 b_1 = ah_1 \cdot bh_2 = ab \cdot b^{-1} h_1 b h_2$. Із нормальності H випливає, що $b^{-1} h_1 b h_2 \in H$. Але тоді $a_1 b_1 \in abH$ і $a_1 b_1 \sim ab$. Отже, відношення $\sim$ узгоджене з діями на G, а тому є конгруенцією. □

Задача 10.3. *Доведіть, що конгруенція на групі однозначно визначається будь–яким своїм класом еквівалентності.*

Наслідок 10.1. *Якщо $\varphi : G \to H$ — гомоморфізм груп, то класи еквівалентності конгруенції $\sim_\varphi$ є класами суміжності за ядром $Ker\,\varphi$.*

Доведення. Це випливає з теореми 10.2, твердження 8.3 і означення (3) конгруенції $\sim_\varphi$. □

Зауваження. Оскільки моноїд містить одиницю, то для довільного гомоморфізму φ моноїдів також можна визначити ядро $\mathrm{Ker}\ \varphi$ як повний прообраз одиниці. Однак на відміну від груп, де, як випливає з

теорем 10.1 і 10.2, образ гомоморфізму повністю (точніше — з точністю до ізоморфізму) визначається його ядром, у випадку моноїдів ядро гомоморфізму не визначає навіть потужності образу.

Приклад. Розглянемо моноїд $(M;\circ)$, де $M = \{a \in \mathbb{R} \mid a \geq 0\}$ і $a \circ b = \max(a,b)$, та два його ендоморфізми: $\varepsilon : M \to M$, $a \mapsto a$, та $\varphi : M \to M$, де $\varphi(0) = 0$ і $\varphi(a) = 1$, якщо $a \neq 0$. Тоді оскільки нейтральним елементом $(M;\circ)$ є 0, то $\operatorname{Ker}\varepsilon = \operatorname{Ker}\varphi = \{0\}$, хоча $\varepsilon(M) = M$, а $\varphi(M) = \{0,1\}$.

Якщо класи еквівалентності конгруенції $\sim$ на групі G є класами суміжності за нормальною підгрупою H, то відповідну факторструктуру звичайно позначають G/H і називають *факторгрупою* групи G за *нормальною підгрупою* H. Оскільки клас еквівалентності елемента a в цьому випадку має вигляд $\overline{a} = aH$, то елементами факторгрупи G/H є класи суміжності за нормальною підгрупою H, рівність (2) набуває вигляду

$$aH \cdot bH = abH, \tag{4}$$

а порядок факторгрупи G/H збігається з індексом $|G:H|$ підгрупи H. Із наслідку 9.4 одержуємо, що $|G| = \big|G/H\big| \cdot |H|$. Зокрема, в скінченній групі порядок факторгрупи завжди ділить порядок групи.

Зауважимо, що канонічний епіморфізм π переводить елемент a у клас суміжності $\overline{a} = aH$, тому ядром $\operatorname{Ker}\pi$ канонічного епіморфізму буде клас $\overline{e} = eH$, тобто сама підгрупа H. Таким чином, кожна нормальна підгрупа є ядром певного гомоморфізму. Разом із твердженням 8.3 це дає

Наслідок 10.2. *Множина нормальних підгруп групи G збігається з множиною ядер визначених на групі G гомоморфізмів. Іншими словами, підгрупа $H \leq G$ є нормальною тоді й лише тоді, коли вона є ядром деякого гомоморфізму.*

Таким чином, теорему 10.1 — основну теорему про гомоморфізми алгебричних систем — для випадку груп можна сформулювати у трохи іншій формі:

Теорема 10.1′(основна теорема про гомоморфізми груп). *Нехай $\varphi : G \to H$ — гомоморфізм груп G та H. Тоді ядро $\operatorname{Ker}\varphi$ цього гомоморфізму — нормальна підгрупа в G і $G/\operatorname{Ker}\varphi \simeq \operatorname{Im}\varphi$. Навпаки, якщо K — нормальна підгрупа групи G, то існує група H (а саме G/H) та епіморфізм $\psi : G \to H$, ядро якого збігається з K.*

Приклади. 1. Очевидно, що $G/G \simeq E$ і $G/E \simeq G$.

2. Факторгрупа S_n/A_n є циклічною групою порядку 2 (див. приклад 2 на стор. 40).

3. Із опису класів суміжності групи $GL_n(P)$ за підгрупою $SL_n(P)$ (див. приклад 3 на стор. 40) і рівності (4) випливає, що $GL_n(P)/SL_n(P) \simeq P^*$ для довільного натурального числа n.

Задача 10.4. *Доведіть, що факторгрупа $\mathbb{Q}/\mathbb{Z}$ періодична і для кожного натурального n містить єдину підгрупу порядку n, до того ж циклічну.*

Зауваження. Виникає природне питання, чи не можна використати рівність (4) для визначення дії на лівих класах суміжності за довільною, не обов'язково нормальною, підгрупою. Виявляється, що ні.

Вправа 10.1. *Клас суміжності abH не залежить від вибору представників a і b класів aH і bH тоді й лише тоді, коли підгрупа H — нормальна.*

Основна теорема про гомоморфізми є дуже корисною при вивченні будови факторгруп. Адже для того, щоб довести ізоморфність факторгрупи G/H і групи A, досить побудувати епіморфізм групи G на A, ядром якого є підгрупа H.

Приклади. 1. Нехай $\mathbb{C}_\infty$ — група всіх комплексних коренів всіх натуральних степенів з 1. Тоді для довільного n факторгрупа $\mathbb{C}_\infty/\mathbb{C}_n$ ізоморфна самій групі $\mathbb{C}_\infty$. Це випливає з того, що відображення $\varphi : \mathbb{C}_\infty \to \mathbb{C}_\infty$, $z \mapsto z^n$, є епіморфізмом, ядром якого є підгрупа $\mathbb{C}_n$.

2. Аналогічно доводиться, що $\mathbb{C}^*/\mathbb{C}_n \simeq \mathbb{C}^*$.

3. $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^*$. Це випливає з того, що відображення $\varphi : GL_n(\mathbb{R}) \to \mathbb{R}^*$, $A \mapsto \det A$, є епіморфізмом, ядром якого є підгрупа $SL_n(\mathbb{R})$.

Задача 10.5. *Доведіть, що факторгрупа групи $(\mathbb{Q}^+;\cdot)$ за підгрупою $H = \{\frac{m}{n} \mid m, n$ — непарні натуральні числа$\}$ ізоморфна групі $\mathbb{Z}$.*

Задача 10.6. *Доведіть, що*: а) $\mathbb{C}^*/\mathbb{R}^+ \simeq \mathbb{R}/\mathbb{Z} \simeq T$; b) $\mathbb{C}^*/T \simeq \mathbb{R}^+$.

Твердження 10.3. *Кожна факторгрупа абелевої групи є абелевою.*

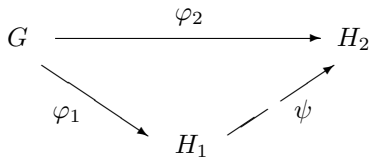
Доведення безпосередньо випливає з рівності (4). □

Твердження 10.4. *Кожна факторгрупа циклічної групи є циклічною.*

Доведення. Нехай a — твірний елемент циклічної групи G. Тоді з рівності (4) випливає, що кожний елемент a^kH факторгрупи G/H можна записати у вигляді $a^kH = (aH)^k$, тобто він є степенем елемента aH. □

Якщо $\varphi : G \to H$ — гомоморфізм груп, то для канонічного епіморфізму $\pi : G \to G/\operatorname{Ker}\varphi$ маємо: $\operatorname{Ker}\pi = \operatorname{Ker}\varphi$. Тому наступну задачу можна розглядати як певне узагальнення основної теореми про гомоморфізми груп.

Задача 10.7. *Нехай $\varphi_1 : G \to H_1$ і $\varphi_2 : G \to H_2$ — такі два гомоморфізми, що $\varphi_1(G) = H_1$ і $\operatorname{Ker}\varphi_1 \leq \operatorname{Ker}\varphi_2$. Доведіть, що тоді існує такий гомоморфізм $\psi : H_1 \to H_2$, що діаграма*



комутативна, причому $\psi(H_1) = \varphi_2(G)$ і $\operatorname{Ker}\psi = \varphi_1(\operatorname{Ker}\varphi_2)$.

Задача 10.8. *Доведіть, що коли H — нормальна підгрупа групи G і* НСД$(|g|, |G : H|) = 1$, *то елемент g належить H.*

Вказівка. Розгляньте образ елемента g при канонічному епіморфізмі $\pi : G \to G/H$.

Задача 10.9. *Нехай H_1 і H_2 — нормальні підгрупи груп G_1 і G_2 відповідно. Наведіть приклади, які показують, що жоден із ізоморфізмів $G_1 \simeq G_2$, $H_1 \simeq H_2$, $G_1/H_1 \simeq G_2/H_2$ не випливає з двох інших.*

11 Спряженість

Означення 11.1. *Елементи a і b групи G називаються спряженими, якщо існує такий елемент $c \in G$, що $a = c^{-1}bc$. Говорять також, що a спряжений з b за допомогою c, або що c спрягає a з b.*

Рівність $a = c^{-1}bc$ часто зручно записувати в показниковій формі: $a = b^c$.

Вправа 11.1. *Доведіть, що*: а) $(a^b)^c = a^{bc}$; b) $(ab)^c = a^c b^c$.

Твердження 11.1. *Відношення спряженості є відношенням еквівалентності.*

Доведення. Якщо $a = b^x$, $b = c^y$, то $b = a^{x^{-1}}$, $a = (c^y)^x = c^{yx}$. Крім того, $a = a^e$. Тому відношення спряженості є симетричним, транзитивним і рефлексивним. □

Класи еквівалентності відношення спряженості називаються *класами спряжених елементів* або просто *класами спряженості.* Клас спряженості, що містить елемент g, позначається через $C(g)$. Якщо треба вказати явно, в якій саме групі G розглядається відношення спряженості, то використовують позначення $C_G(g)$.

Приклади. 1. У будь–якій групі $C(e) = \{e\}$.

2. В абелевій групі $c^{-1}bc = b$, тому всі класи спряженості одноелементні.

3. Як випливає з теореми Жордана про нормальну форму матриць, у групі $GL_n(\mathbb{C})$ матриці A і B попадають в один і той же клас спряженості тоді й лише тоді, коли ці матриці мають однакові жорданові нормальні форми.

Твердження 11.2. *У симетричній групі S_n дві підстановки є спряженими тоді й лише тоді, коли вони мають однаковий цикловий тип.*

Доведення. Безпосередньо перевіряється, що результатом спряження підстановки $\pi = (a_1 \dots a_k) \cdots (c_1 \dots c_m)$ за допомогою підстановки

$$\tau = \begin{pmatrix} a_1 & \dots & a_k & \dots & c_1 & \dots & c_m \\ a'_1 & \dots & a'_k & \dots & c'_1 & \dots & c'_m \end{pmatrix}$$

буде підстановка $\pi_1 = \tau^{-1}\pi\tau = (a'_1 \dots a'_k) \cdots (c'_1 \dots c'_m)$ того ж циклового типу. Навпаки, будь–які дві підстановки $\pi = (a_1 \dots a_k) \dots (c_1 \dots c_m)$ і $\pi_1 = (a'_1 \dots a'_k) \dots (c'_1 \dots c'_m)$ однакового циклового типу будуть спряжені за допомогою підстановки

$$\tau = \begin{pmatrix} a_1 & \dots & a_k & \dots & c_1 & \dots & c_m \\ a'_1 & \dots & a'_k & \dots & c'_1 & \dots & c'_m \end{pmatrix}. \qquad \square$$

Зауваження. Якщо елементи a і b підгрупи H групи G спряжені в підгрупі H, то вони, очевидно, будуть спряженими і в групі G. Однак обернене твердження хибне, адже той елемент групи G, за допомогою якого a спрягається з b, може і не належати підгрупі H. Тому в довільній групі підстановок рівність циклових типів двох елементів є лише необхідною умовою їх спряженості.

Задача 11.1. *Вкажіть у групі A_4 дві підстановки, які мають однаковий цикловий тип, але не спряжені в A_4.*

Поняття спряженості легко переноситься на довільні підмножини групи G: *підмножини A і B спряжені*, якщо існує такий елемент $c \in G$, що $A = B^c = \{b^c \mid b \in B\}$. Використовуючи поняття спряженості, критерію нормальності підгрупи (теорема 9.1) можна надати іншого вигляду:

Теорема 11.1. *Наступні твердження рівносильні:*
a) *підгрупа H групи G є нормальною;*
b) *підгрупа H групи G є об'єднанням класів спряженості G;*
c) *для довільного елемента $g \in G$ виконується рівність $g^{-1}Hg = H$, тобто підгрупа H є спряженою в групі G тільки з собою.*

Доведення. a) $\Rightarrow$ b). Із теореми 9.1 випливає, що нормальна підгрупа H разом з елементом h містить і всі елементи вигляду $g^{-1}hg$, тобто всі елементи, спряжені з h. Тому кожний клас спряженості, який має непорожній перетин з H, повністю міститься в H.

b) $\Rightarrow$ c). Оскільки H є об'єднанням класів спряженості, то $g^{-1}Hg \subseteq H$. Припустимо, що $g^{-1}Hg \neq H$. Тоді маємо строге включення $g^{-1}Hg \subset H$, і із твердження 9.2:

$$Hg = g \cdot g^{-1}Hg \subset gH, \quad H = Hg \cdot g^{-1} \subset gH \cdot g^{-1} = (g^{-1})^{-1}Hg^{-1} \ .$$

Останнє строге включення означає, що знайдеться такий елемент $h \in H$, що $(g^{-1})^{-1}hg^{-1} \notin H$. Але це суперечить тому, що H є об'єднанням класів спряженості. Отже, $g^{-1}Hg = H$.

c) $\Rightarrow$ a). Із рівності $g^{-1}Hg = H$ випливає, що для довільного $h \in H$ елемент $g^{-1}gh$ також належить підгрупі H. Оскільки елемент $g \in G$ — довільний, то за критерієм нормальності (теорема 9.1) підгрупа H є нормальною. □

Задача 11.2. a) *Доведіть, що коли H є власною підгрупою скінченної групи G, то $G \neq \bigcup_{a \in G} H^a$.*

b) *Доведіть, що для нескінченних груп попереднє твердження може бути хибним.*

Рівність $C(a) = \{a\}$ рівносильна тому, що $g^{-1}ag = a$ для довільного g з групи G. Але $g^{-1}ag = a$ тоді й лише тоді, коли $ag = ga$. Тому клас спряженості $C(a)$ буде одноелементним тоді й лише тоді, коли a комутує з усіма елементами групи. Звідси одразу випливає

Твердження 11.3. *Всі класи спряженості групи G одноелементні тоді й тільки тоді, коли група G — абелева.*

Об'єднання $Z(G)$ всіх одноелементних класів спряженості називається *центром* групи G. Іншими словами, $Z(G) = \{g \in G \mid gx = xg \text{ для всіх } x \in G\}$.

Центр $Z(G)$ може служити певною "мірою комутативності" групи G: чим він більший, тим група "комутативніша". Зокрема, центр збігається з усією групою тоді й лише тоді, коли група абелева.

Твердження 11.4. *Центр $Z(G)$ є абелевою нормальною підгрупою групи G.*

Доведення. Якщо $a \in Z(G)$ і $b \in Z(G)$, то для всіх $x \in G$ буде $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$, тому $ab \in Z(G)$. Крім того, з рівності $ax = xa$ випливає рівність $xa^{-1} = a^{-1}x$. Тому згідно твердження 5.1 $Z(G)$ є підгрупою G. Комутативність $Z(G)$ очевидна. Нормальність $Z(G)$ одразу випливає з теореми 11.1. □

Вправа 11.2. *Доведіть, що кожна підгрупа центру $Z(G)$ групи G є нормальною в G.*

Задача 11.3. *Доведіть, що для довільного епіморфізму груп $\varphi : G \to H$ виконується включення $Z(G) \leq \varphi^{-1}(Z(H))$.*

Задача 11.4. *Доведіть, що центр $Z(H)$ нормальної підгрупи $H \lhd G$ також є нормальною підгрупою групи G.*

Твердження 11.5. *Якщо група G — не комутативна, то факторгрупа $G/Z(G)$ — не циклічна.*

Доведення. Припустимо, що факторгрупа $G/Z(G)$ є циклічною. Виберемо у факторгрупі твірний елемент $\overline{g} = gZ(G)$. Позаяк кожний елемент факторгрупи можна записати у вигляді $\overline{g}^k = g^k Z(G)$, то кожний

елемент групи можна записати у вигляді $g^k h$, де $h \in Z(G)$. Але тоді для довільних елементів $a = g^{k_1} h_1$ і $b = g^{k_2} h_2$ із G маємо:

$$ab = g^{k_1} h_1 g^{k_2} h_2 = g^{k_1} g^{k_2} h_1 h_2 = g^{k_2} g^{k_1} h_2 h_1 = g^{k_2} h_2 g^{k_1} h_1 = ba\ .$$

Отже, група G — комутативна, що суперечить умові. □

Наступні два поняття є певним узагальненням поняття центру. Нехай A — довільна підмножина групи G. *Централізатором* $Z(A)$ підмножини A називається множина всіх елементів групи G, переставних з усіма елементами множини A, тобто $Z(A) = \{g \in G \mid gx = xg \text{ для всіх } x \in A\}$. Зокрема, централізатором самої групи G є її центр. *Нормалізатором* підмножини A називається множина $N(A) = \{g \in G \mid g^{-1}Ag = A\}$. У разі потреби явного вказання групи використовують позначення $Z_G(A)$ і $N_G(A)$. Очевидно, що для одноелементної підмножини $\{a\}$ централізатор $Z_G(A)$ і нормалізатор $N_G(a)$ збігаються.

Вправа 11.3. *Доведіть, що*: а) *для довільної підмножини $A \subseteq G$ централізатор $Z(A)$ і нормалізатор $N(A)$ є підгрупами групи G, причому $Z(A) \lhd N(A)$*; b) *кожна підгрупа $H \leq G$ є нормальною підгрупою свого нормалізатора $N_G(H)$.*

Задача 11.5.** *Доведіть, що нормалізатор $N_G(A)$ підмножини A групи G, взагалі кажучи, не збігається з множиною $\{g \in G \mid g^{-1}Ag \subseteq A\}$.*

Вказівка. Доведіть, що в групі $G = \left\{\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \mid a, b \in \mathbb{Q}, a \neq 0\right\}$ підгрупа $H = \left\{\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) \mid n \in \mathbb{Z}\right\}$ при спряженні за допомогою діагональної матриці може перейти у свою власну підгрупу.

Задача 11.6. *Доведіть, що централізатор класу спряжених елементів $C_G(a)$ є нормальною підгрупою групи G.*

Задача 11.7. *Доведіть, що коли елементи a і b — спряжені, то їх нормалізатори $N(a)$ і $N(b)$ — також спряжені. З'ясуйте, чи буде правильним зворотне твердження.*

Вказівка. Нехай $b = g^{-1}ag$. Тоді $x \in N(a) \Leftrightarrow x^{-1}ax = a \Leftrightarrow g^{-1}x^{-1}axg = g^{-1}ag \Leftrightarrow g^{-1}x^{-1}gbg^{-1}xg = b \Leftrightarrow g^{-1}xg \in N(b)$.

Теорема 11.2. *Потужність класу спряженості $C_G(x)$ елемента x групи G дорівнює індексові його нормалізатора $N_G(x)$, тобто*

$$|C_G(x)| = |G : N_G(x)|\ .$$

Доведення. Із ланцюжка рівносильних тверджень

$$g^{-1}xg = h^{-1}xh \iff hg^{-1}xgh^{-1} = x \iff gh^{-1} \in N_G(x) \iff g \in N_G(x) \cdot h$$

випливає, що спряження елемента x за допомогою g і h дає однаковий результат тоді й лише тоді, коли g і h належать до одного й того ж правого класу суміжності групи G за нормалізатором $N_G(x)$. Тому елементи класу спряженості $C_G(x)$ знаходяться у взаємно однозначній відповідності з правими класами суміжності за нормалізатором $N_G(x)$, а їх кількість дорівнює індексові $|G : N_G(x)|$. □

Наслідок 11.1. *Потужність класу спряженості $C_G(x)$ елемента x скінченної групи G є дільником порядку групи G.*

Нагадаємо, що коли розклад підстановки $\pi \in S_n$ у добуток незалежних циклів має l_1 цикл довжини 1, l_2 цикли довжини 2, …, l_n циклів довжини n, то набір $(l_1, l_2, \ldots, l_n)$ називається її *цикловим типом.*

Наслідок 11.2. *Якщо підстановка $\pi \in S_n$ має цикловий тип $(l_1, l_2, \ldots, l_n)$, то*

$$|C(\pi)| = \frac{n!}{1^{l_1}l_1! \cdot 2^{l_2}l_2! \cdot \ldots \cdot n^{l_n}l_n!} \;\; i \;\; |N(\pi)| = 1^{l_1}l_1! \cdot 2^{l_2}l_2! \cdot \ldots \cdot n^{l_n}l_n!.$$

Доведення. Формула для $|C(\pi)|$ випливає з твердження 11.2 і того, що кількість підстановок циклового типу $(l_1, l_2, \ldots, l_n)$ дорівнює

$$\frac{n!}{1^{l_1}l_1! \cdot 2^{l_2}l_2! \cdot \ldots \cdot n^{l_n}l_n!}\,.$$

Після цього формула для $|N(\pi)|$ випливає з теореми 11.2 і того, що $|S_n| = n!$. □

Задача 11.8*. *Знайдіть із точністю до ізоморфізму всі групи, які мають рівно 4 класи спряжених елементів.*

Теорема 11.3 (формула класів). *Виберемо в кожному неодноелементному класі спряженості C_i, $1 \le i \le k$, скінченної групи G представника a_i. Тоді*

$$|G| = |Z(G)| + \sum_{i=1}^{k} |G : N(a_i)|\,. \tag{5}$$

Доведення. Оскільки класи спряженості утворюють розбиття групи G, а центр $Z(G)$ є об'єднанням усіх одноелементних класів спряженості, то

$$G = Z(G) \bigcup (\bigcup_{i=1}^{k} C(a_i)) \ ,$$

причому це об'єднання є диз'юнктним. Тому $|G| = |Z(G)| + \sum_{i=1}^{k} |C(a_i)|$. Застосовуючи до доданків з останньої суми теорему 11.2, одержуємо рівність (5). □

Наслідок 11.3 (лема Коші). *Якщо порядок скінченної групи G ділиться на просте число p, то G містить елемент порядку p.*

Доведення. Для циклічних груп це випливає з теореми 7.3 b). Нехай тепер група G — абелева і $A_1, \ldots, A_k$ — список усіх її циклічних підгруп. Очевидно, що $G = A_1 \cup \ldots \cup A_k$. Крім того, $G \supseteq A_1 \cdots A_k \supseteq A_1 \cup \ldots \cup A_k$. Тоді $G = A_1 \cdots A_k$. Якби порядок жодної циклічної підгрупи A_i не ділився на p, то із зад. 5.2 випливало б, що і порядок групи G не ділиться на p. Тому порядок якоїсь циклічної підгрупи A_i ділиться на p і знову ж згідно теореми 7.3 b) вона містить елемент порядку p. Для неабелевих груп лема Коші тепер легко доводиться індукцією за порядком групи G. Справді, для груп порядку p лема Коші випливає з наслідку 9.3 із теореми Лагранжа. Якщо ж порядок групи G більший за p, то досить показати, що якась із власних підгруп групи G містить елемент порядку p. Для цього розглянемо нормалізатори $N(a_i)$ з правої частини рівності (5). Якщо порядок $|N(a_i)|$ ділиться на p, то, за припущенням індукції, $N(a_i)$ містить елемент порядку p. Якщо ж жодне з чисел $|N(a_i)|$ не ділиться на p, то на p будуть ділитися всі індекси $|G : N(a_i)|$. Із формули класів випливає, що тоді на p буде ділитися і порядок абелевої підгрупи $Z(G)$. Далі можна зіслатися або на першу частину доведення, або на припущення індукції, бо для неабелевих груп $|Z(G)| < |G|$. □

Задача 11.9. *Доведіть, що кожна група порядку* 6 *ізоморфна або циклічній групі C_6, або групі S_3.*

Для фіксованого елемента $a \in G$ відображення

$$\varphi_a : G \to G \, , \quad x \mapsto a^{-1} x a \, , \tag{6}$$

називається *спряженням* групи G за допомогою елемента a.

Твердження 11.6. *Для кожного елемента a групи G відображення φ_a є автоморфізмом G.*

Доведення. Спочатку зауважимо, що φ_e є тотожним перетворенням групи G, бо $\varphi_e(x) = e^{-1}xe = x$. Оскільки для довільних $x, y \in G$

$$\varphi_a(xy) = a^{-1}xya = a^{-1}xa \cdot a^{-1}ya = \varphi_a(x)\varphi_a(y)\,,$$

то φ_a є ендоморфізмом G. Із рівностей

$$(\varphi_a \circ \varphi_b)(x) = \varphi_b(\varphi_a(x)) = b^{-1}a^{-1}xab = \varphi_{ab}(x) \tag{7}$$

випливає, що $\varphi_a \circ \varphi_{a^{-1}} = \varphi_{a^{-1}} \circ \varphi_a = \varphi_e$. Значить, для відображення φ_a існує обернене, а тому воно є бієктивним. Отже, φ_a є автоморфізмом групи G. □

Автоморфізми спряження φ_a називаються *внутрішніми автоморфізмами* групи G і для них має місце наступна

Теорема 11.4. 1. *Множина* $\operatorname{Inn} G$ *всіх внутрішніх автоморфізмів групи G відносно композиції перетворень утворює групу.*

2. *Група* $\operatorname{Inn} G$ *ізоморфна факторгрупі $G/Z(G)$.*

3. $\operatorname{Inn} G$ *є нормальною підгрупою групи* $\operatorname{Aut} G$.

Доведення. З рівностей (7) випливає, що відображення $\psi : a \mapsto \varphi_a$ є гомоморфізмом групи G в групу $\operatorname{Aut} G$. І оскільки $\operatorname{Inn} G = \psi(G)$, то згідно твердження 8.1 множина $\operatorname{Inn} G$ є підгрупою групи $\operatorname{Aut} G$.

Крім того, φ_a буде тотожним автоморфізмом тоді й лише тоді, коли $a^{-1}xa = x$ для всіх $x \in G$, тобто, коли $a \in Z(G)$. Тому $\operatorname{Ker}\psi = Z(G)$ і згідно теореми $10.1'$ — основної теореми про гомоморфізми груп, $\operatorname{Inn} G \simeq G/Z(G)$.

Нарешті, для довільних $\phi \in \operatorname{Aut} G$ і $\varphi_a \in \operatorname{Inn} G$ виконується рівність $\phi^{-1} \cdot \varphi_a \cdot \phi = \varphi_{\phi(a)}$, бо $(\phi^{-1} \cdot \varphi_a \cdot \phi)(x) = \phi(\varphi_a(\phi^{-1}(x))) = \phi(a^{-1}\phi^{-1}(x)a) = \phi(a^{-1})\phi(\phi^{-1}(x))\phi(a) = \phi(a^{-1})x\phi(a) = \phi(a)^{-1}x\phi(a) = \varphi_{\phi(a)}(x)$ (тут x — довільний елемент із G). Тому $\operatorname{Inn} G$ є нормальною підгрупою групи $\operatorname{Aut} G$. □

Наслідок 11.4. a) *Спряжені елементи групи G мають однаковий порядок.*
b) *Множина, спряжена до підгрупи групи G, також буде підгрупою в G, причому ізоморфною початковій підгрупі.*
c) *Спряжені підгрупи групи G мають однакові індекси.*

Факторгрупа $\operatorname{Aut} G/\operatorname{Inn} G$ називається *групою зовнішніх автоморфізмів* групи G і позначається $\operatorname{Out} G$.

Задача 11.10. *Доведіть, що кожний автоморфізм групи S_3 є внутрішнім.*

Вказівка. Із теореми 11.4 і того, що $Z(S_3) = \{\varepsilon\}$, випливає, що група S_3 має 6 внутрішніх автоморфізмів. З іншого боку, кожен автоморфізм групи S_3 індукує перестановку множини транспозицій з S_3 і цією перестановкою повністю визначається.

Задача 11.11. *Доведіть, що коли група G має тільки одну підгрупу H даного порядку n, то H є нормальною підгрупою групи G.*

Задача 11.12.* *Доведіть, що коли центр групи G є одиничною підгрупою, то центр її групи автоморфізмів $\operatorname{Aut} G$ також є одиничною підгрупою.*

12 Решітка підгруп і теореми про ізоморфізм

Теорема 12.1 (про ізоморфізм факторгруп). *Нехай $H \leq G$ і $K \lhd G$. Тоді*: a) $KH \leq G$; b) $K \lhd KH$; c) $K \cap H \lhd H$; d) $(KH)/K \simeq H/(K \cap H)$.

Доведення. a) Для довільних k, k_1, $k_2 \in K$ та h, h_1, $h_2 \in H$ маємо:

$$(kh)^{-1} = h^{-1}k^{-1} = h^{-1}k^{-1}h \cdot h^{-1} \in KH \text{ і}$$

$$k_1h_1 \cdot k_2h_2 = k_1h_1k_2h_1^{-1} \cdot h_1h_2 \in KH,$$

бо згідно нормальності підгрупи K добутки $h^{-1}k^{-1}h$ і $h_1k_2h_1^{-1}$ належать K. Із твердження 5.1 тоді випливає, що KH є підгрупою.

b) одержуємо з того, що $K \lhd G$ і $K \leq KH \leq G$.

c) Якщо $h_1 \in K \cap H$ і $h \in H$, то $h^{-1}h_1h \in K$ (бо K — нормальна підгрупа групи G) і $h^{-1}h_1h \in H$. Тому $h^{-1}h_1h \in K \cap H$ і, за критерієм нормальності, $K \cap H \lhd H$.

d) Розглянемо канонічний епіморфізм $\pi : x \mapsto xK$ групи G на факторгрупу G/K. Тоді $\pi(KH) = \pi(H)$, а тому образи гомоморфізмів $\pi\big|_{KH} : KH \to G/K$ і $\pi\big|_{H} : H \to G/K$ збігаються. Але ядром першого гомоморфізму є K, а ядром другого — $K \cap H$. Далі лишається лише скористатися основною теоремою про гомоморфізми. □

Зауваження. Твердження d) теореми 12.1 ще називають теоремою Нетер про ізоморфізм або теоремою про паралелограм.

Для довільної підгрупи $K \leq G$ через $L(G,K)$ позначимо множину всіх проміжних підгруп групи G, тобто таких підгруп $H \leq G$, які містять K. Множину всіх нормальних підгруп групи G, які містяться в $L(G,K)$, позначимо через $LN(G,K)$. Якщо $K = E$, то замість $L(G,E)$ і $LN(G,E)$ пишемо просто $L(G)$ і $LN(G)$.

Теорема 12.2 (про відповідність підгруп). *Нехай K — нормальна підгрупа групи G. Тоді визначене на множині $L(G,K)$ відображення $\tau : H \mapsto \overline{H} = H/K$ є бієкцією множини $L(G,K)$ на множину $L(G/K)$ і одночасно бієкцією множини $LN(G,K)$ на множину $LN(G/K)$, причому для довільної нормальної підгрупи N групи G, яка містить K, будемо мати*

$$G/N \simeq \big(G/K\big)\Big/\big(N/K\big) \, .$$

Доведення розіб'ємо на кілька кроків.

a) Оскільки кожна підгрупа $H \in L(G,K)$ є об'єднанням класів суміжності за підгрупою K, то $\tau(H)$ одержується обмеженням на підгрупу H канонічного епіморфізму $\pi : G \to G/K$. Зокрема, $\tau(H) = \pi(H)$ є підгрупою групи G/K.

b) Відображення τ — ін'єктивне. Справді, якщо $H_1 \neq H_2$, то без обмеження загальності можна припустити, що існує такий елемент $a \in H_1$, що $a \notin H_2$. Але тоді $aK \in \overline{H_1}$ і $aK \notin \overline{H_2}$, тому $\overline{H_1} \neq \overline{H_2}$.

c) Сюр'єктивність відображення τ випливає з твердження 8.2 b).

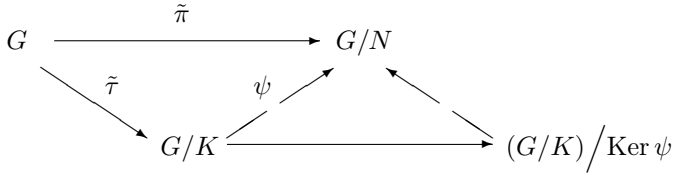
d) Якщо підгрупа $H \in L(G,K)$ є нормальною, то для довільних $hK \in \overline{H}$ і $gK \in \overline{G}$ маємо

$$(gK)^{-1} \cdot hK \cdot gK = g^{-1}hg \cdot K \in \overline{H} \, . \tag{8}$$

Отже, $\overline{H} \lhd \overline{G}$.

e) Навпаки, якщо $\overline{H} \lhd \overline{G}$, то для довільних $h \in H$ і $g \in G$ із рівності (8) випливає, що $g^{-1}hg \in H$. Тому $H \lhd G$.

f) Нарешті, розглянемо діаграму



,

де $\tilde{\pi}$ і $\tilde{\tau}$ — канонічні епіморфізми на факторгрупи, а відображення $\psi : G/K \to G/N$ визначається правилом $\psi(gK) = gN$ (тоді лівий трикутник діаграми буде комутативним). Легко перевіряється, що ψ є епіморфізмом. Тому на підставі основної теореми про гомоморфізми маємо:

$$\psi(G/K) = G/N \simeq (G/K)\Big/\operatorname{Ker}\psi\,.$$

Але

$$gK \in \operatorname{Ker}\psi \Leftrightarrow gN = N \Leftrightarrow g \in N \Leftrightarrow gK \in N/K\,.$$

Отже, $\operatorname{Ker}\psi = N/K$, що й доводить теорему. □

Приклад. Для довільних натуральних k, m і $n = km$ виконується $n\mathbb{Z} \lhd k\mathbb{Z} \lhd \mathbb{Z}$. Тому

$$\mathbb{Z}_k = \mathbb{Z}/k\mathbb{Z} \simeq (\mathbb{Z}/n\mathbb{Z})\big/(k\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}_n/\mathbb{Z}_m\,.$$

Таким чином, $\mathbb{Z}_k \simeq \mathbb{Z}_{mk}/\mathbb{Z}_m$.

13 Вільні групи

Нехай $X = \{x_i \mid i \in I\}$ — деяка сукупність символів, що не повторюються, проіндексова елементами множини I. Називатимемо множину X *алфавітом*, а її елементи — *буквами*. Також розглядатимемо множину $\{x_i^{-1} \mid i \in I\}$, яку природно позначити символом X^{-1}.

Груповим словом w в алфавіті X називається або порожня (позначається символом Λ), або скінченна послідовність букв із $X \cup X^{-1}$. Кількість букв в такій послідовності є *довжиною* цього слова, яку позначатимемо $l(w)$.

Якщо $u = y_1 \dots y_r$, $v = z_1 \dots z_s$ — два слова в алфавіті X (тобто y_1, $\dots$, y_r, z_1, $\dots$, $z_s \in X \cup X^{-1}$), то uv означає слово $y_1 \dots y_r z_1 \dots z_s$.

Слово вважається *нескоротним*, якщо воно або пусте, або у ньому поряд не зустрічаються символи виду x_i^k та x_i^{-k}, де $k = \pm 1$. Інакше,

слово буде *скоротним*. Наприклад, слово $x_3x_1^{-1}x_1^{-1}x_1x_4$ є скоротним, а слово $x_2^{-1}x_2^{-1}x_3x_2$ — нескоротним.

Будемо казати також, що два слова u та v є *сусідніми*, якщо одне з них має вигляд $w_1x_i^kx_i^{-k}w_2$, а інше — w_1w_2, де $k = \pm 1$.

Означення 13.1. *Два слова u та v називаються еквівалентними (позначаємо $u \sim v$), якщо одне можна одержати з іншого за допомогою скінченної кількості вставок чи скорочень виду $x_i^kx_i^{-k}$, де $k = \pm 1$. Іншими словами, $u \sim v$, якщо існує скінченна послідовність слів $w_1, \ldots, w_r$ така, що $u = w_1$, $v = w_r$, а w_i та w_{i+1} є сусідніми словами при $i = 1, \ldots, r-1$.*

Зокрема, два сусідні слова є, очевидно, еквівалентними.

Задача 13.1. *Доведіть, що відношення $\sim$ є відношенням еквівалентності.*

Позначимо символом $[u]$ сукупність усіх слів, еквівалентних слову u. Ця множина утворює клас еквівалентності відношення $\sim$.

Задача 13.2. *Доведіть, що кожний клас еквівалентності $[u]$ містить єдине нескоротне слово.*

Із цієї задачі, зокрема, випливає, що хоча процедура скорочення слова не є однозначною, результатом завжди буде одне й те ж нескоротне слово.

Позначимо символом $F(X)$ множину класів еквівалентних слів в алфавіті X

$$F(X) = \{[u] \mid u \text{ — слово в алфавіті } X\}$$

і визначимо на цій множині операцію приписування за правилом:

$$[u][v] = [uv]\ . \tag{9}$$

Твердження 13.1. *Множина $F(X)$ із заданою на ній операцією (9) є групою.*

Доведення. Перш за все перевіримо, що операція (9) задана коректно. Для цього досить показати, що якщо $u_1 \sim u_2$, $v_1 \sim v_2$, то $u_1v_1 \sim u_2v_2$. Згідно означення 13.1 $u_1 \sim u_2$, а $v_1 \sim v_2$, якщо існують скінченні послідовності слів $w_1, \ldots, w_r$ та $t_1, \ldots, t_s$, такі що $u_1 = w_1$, $u_2 = w_r$, $v_1 = t_1$, $v_2 = t_s$, а w_i та w_{i+1}, t_j та t_{j+1} є сусідніми словами при $i = 1, \ldots, r-1$

і $j = 1, \ldots, s-1$. Тоді, легко бачити, $u_1v_1 = u_1t_1 \sim u_1t_2 \sim \ldots \sim u_1t_s = u_1v_2 = w_1v_2 \sim w_2v_2 \sim \ldots \sim w_rv_2 = u_2v_2$. Тому $[u_1v_1] = [u_2v_2]$.

Перевіримо, що операція приписування є асоціативною, тобто для довільних u, v, $w \in F(X)$ виконується

$$([u][v])[w] = [u]([v][w]) \ . \tag{10}$$

Для цього застосуємо індукцію за довжиною $l(v)$. Не порушуючи загальності можна вважати, що слова u, v, w є нескоротними. Якщо $l(v) = 0$, тобто $v = \Lambda$, то, очевидно, рівність (10) має місце. Нехай $l(v) = 1$, тобто $v = x$, де $x \in X \cup X^{-1}$. Якщо слово ux нескоротне і нескоротним є слово xw, то (10) виконується. Нехай ux є скоротним словом. Це означає, що $u = u'x^{-1}$, і тоді $([u][v])[w] = [uv][w] = [u'][w]$. Якщо, у свою чергу, слово xw є скоротним, то $w = x^{-1}w'$, а, отже,

$$[u]([v][w]) = [u][vw] = [u][w'] = [u'x^{-1}][w'] = [u'x^{-1}w'] = [u'][w].$$

Інші випадки розглядаються аналогічним чином, тому ми їх опускаємо. Припустимо тепер, що співвідношення (10) має місце для всіх v таких, що $l(v) < n$, і нехай v — слово довжини n. Тоді $v = v_1v_2$, де слова v_1, v_2 меншої за n довжини: $l(v_1) < n$, $l(v_2) < n$. А тому із індукційного припущення одержуємо ланцюг рівностей:

$$([u][v])[w] = ([u][v_1v_2])[w] = ([u]([v_1][v_2]))[w] = (([u][v_1])[v_2])[w] =$$

$$= ([u][v_1])([v_2][w]) = [u]([v_1]([v_2][w])) = [u](([v_1][v_2])[w]) = [u]([v][w]),$$

і тим самим асоціативність доведена.

Нейтральним елементом операції приписування є, очевидно, клас $[\Lambda]$, а оберненим до класу $[u]$, де $u = y_1 \ldots y_r$, $y_1, \ldots, y_r \in X \cup X^{-1}$, є клас $[u]^{-1} = [y_r^{-1} \ldots y_1^{-1}]$, бо $[u][u]^{-1} = [y_1 \ldots y_r y_r^{-1} \ldots y_1^{-1}] = [\Lambda] = [u]^{-1}[u] = [y_r^{-1} \ldots y_1^{-1} y_1 \ldots y_r]$. □

Означення 13.2. *Множина $F(X)$ із операцією* (9) *називається вільною групою з системою твірних X, а потужність множини X називається рангом вільної групи.*

Якщо $F(X)$ — вільна група рангу n, то поряд із позначенням $F(X)$ також використовують позначення $F_n(X)$ або коротко F_n.

Вправа 13.1. *Доведіть, що коли $|X| = 1$, то $F(X) \simeq \mathbb{Z}$, а коли $|X| > 1$, то група $F(X)$ є неабелевою.*

Вправа 13.2. *Доведіть, що у вільній групі немає відмінних від* Λ *елементів скінченного порядку.*

Задача 13.3. *Доведіть, що вільні групи скінченного рангу є зліченими, а вільні групи нескінченного рангу мають потужність, яка збігається з цим рангом.*

Теорема 13.1. *Дві вільні групи ізоморфні тоді і тільки тоді, коли їх ранги однакові.*

Доведення. Достатність. Нехай $F(X)$ та $F(Y)$ — вільні групи одинакового рангу. Оскільки множини X та Y рівнопотужні, то існує бієктивне відображення $\varphi : X \to Y$, яке продовжується до взаємно однозначного відображення $\bar{\varphi} : F(X) \to F(Y)$ природним чином: якщо $[w] = [x_{i_1}^{k_1} \dots x_{i_s}^{k_s}] \in F(X)$, де $i_1, \dots, i_s \in I$, а $k_1, \dots, k_s \in \{\pm 1\}$, то $\bar{\varphi}([w]) = [\varphi(x_{i_1})^{k_1} \dots \varphi(x_{i_s})^{k_s}]$. Відображення $\bar{\varphi}$ є, крім того, гомоморфізмом, бо для довільних $[u] = [x_{i_1}^{k_1} \dots x_{i_s}^{k_s}]$, $[v] = [x_{j_1}^{l_1} \dots x_{j_r}^{l_r}] \in F(X)$, де $i_1, \dots, i_s$, $j_1, \dots, j_r \in I$, а $k_1, \dots, k_s$, $l_1, \dots, l_r \in \{\pm 1\}$, матимемо

$$\bar{\varphi}([u][v]) = \bar{\varphi}([uv]) = [\varphi(x_{i_1})^{k_1} \dots \varphi(x_{i_s})^{k_s} \varphi(x_{j_1})^{l_1} \dots \varphi(x_{j_r})^{l_r}] =$$

$$= [\varphi(x_{i_1})^{k_1} \dots \varphi(x_{i_s})^{k_s}][\varphi(x_{j_1})^{l_1} \dots \varphi(x_{j_r})^{l_r}] = \bar{\varphi}([u])\bar{\varphi}([v]).$$

Отже, $\bar{\varphi}$ — ізоморфізм $F(X)$ та $F(Y)$.

Необхідність. Доведемо, що коли групи $F(X)$ та $F(Y)$ мають різні ранги, то вони неізоморфні. Розглянемо підгрупу $\langle F(X)^2 \rangle = \langle a^2 \mid a \in F(X) \rangle$ вільної групи $F(X)$, породжену всіма квадратами елементів з $F(X)$ і покажемо, що вона є нормальною підгрупою групи $F(X)$. Справді, якщо $f \in \langle F(X)^2 \rangle$ має вигляд $f = a^2$, $a \in F(X)$, то для довільного $b \in F(X)$ матимемо: $b^{-1}a^2b = (b^{-1}a^2)^2(a^{-1})^2b^2 \in \langle F(X)^2 \rangle$. А тому для довільних елементів $b \in F(X)$ та $a_1^2 \dots a_k^2 \in \langle F(X)^2 \rangle$

$$b^{-1}(a_1^2 \dots a_k^2)b = (b^{-1}a_1^2b)(b^{-1}a_2^2b) \dots (b^{-1}a_k^2b) =$$

$$= ((b^{-1}a_1^2)^2(a_1^{-1})^2b^2) \dots ((b^{-1}a_k^2)^2(a_k^{-1})^2b^2) \in \langle F(X)^2 \rangle.$$

Отже, $\langle F(X)^2 \rangle \lhd F(X)$. Крім того, елементи факторгрупи $F(X)/\langle F(X)^2 \rangle$ комутують: якщо $a_1\langle F(X)^2 \rangle, a_2\langle F(X)^2 \rangle \in F(X)/\langle F(X)^2 \rangle$, то

$$a_1\langle F(X)^2 \rangle \cdot a_2\langle F(X)^2 \rangle = a_1a_2\langle F(X)^2 \rangle = a_2a_1(a_1^{-2}(a_1a_2^{-1})^2a_2^2)\langle F(X)^2 \rangle =$$

$$a_2a_1\langle F(X)^2 \rangle = a_2\langle F(X)^2 \rangle a_1\langle F(X)^2 \rangle,$$

причому $(a\langle F(X)^2\rangle)^2 = a^2\langle F(X)^2\rangle = \langle F(X)^2\rangle$. Тому $F(X)/\langle F(X)^2\rangle$ є абелевою групою, в якій усі неодиничні елементи мають порядок 2.

Визначимо дію множення елемента $v = a\langle F(X)^2\rangle$ із $F(X)/\langle F(X)^2\rangle$ на елементи поля $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ наступним чином:

$$\bar{0} \cdot v = \langle F(X)^2\rangle,\ \bar{1} \cdot v = v.$$

Тоді факторгрупа $F(X)/\langle F(X)^2\rangle$ з визначеним таким чином множенням на елементи із $\mathbb{Z}_2$ утворює векторний простір над полем $\mathbb{Z}_2$, причому базою цього векторного простору є множина $\{x\langle F(X)^2\rangle | x \in X\}$, а його розмірність дорівнює $|X|$, тобто збігається з рангом групи $F(X)$ (перевірку цього факту ми залишаємо читачеві у якості нескладної домашньої вправи). Аналогічно, факторгрупа $F(Y)/\langle F(Y)^2\rangle$ утворюватиме векторний простір над тим же полем $\mathbb{Z}_2$ але розмірності $|Y|$. І оскільки векторні простори різних розмірностей неізоморфні, тому неізоморфними будуть також вільні групи $F(X)$ та $F(Y)$. □

Приклади. 1. Вільна група F_1 рангу 1 ізоморфна нескінченній циклічній групі $(\mathbb{Z}, +)$.

2. Розглянемо підгрупу H спеціальної лінійної групи $SL_2(\mathbb{Z})$, яка породжена матрицями $a = \left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right)$ і $b = \left(\begin{smallmatrix} 1 & 0 \\ m & 1 \end{smallmatrix}\right)$, де $m \geq 2$ — деяке фіксоване ціле число. Покажемо, що H ізоморфна вільній групі $F(x, y)$ рангу 2. Для цього розглянемо відображення $\varphi : F(x, y) \to H$, $x \mapsto a$, $y \mapsto b$. Це відображення є, очевидно, епіморфізмом. Покажемо, що $\operatorname{Ker}\varphi = \{\Lambda\}$. Для цього спочатку зауважимо, що оскільки $H =< a, b >$, то довільний елемент h із H зображується у вигляді слова $h = a^{i_1}b^{j_1}\dots a^{i_k}b^{j_k}$, де при $k \geq 2$ числа i_1, j_k — цілі, а числа $i_2, \dots, i_k$, $j_1, \dots, j_{k-1}$ є цілими, відмінними від нуля, а при $k = 1$ цілі числа i_1 та j_1 одночасно не рівні 0 (окремо, для одиничної матриці E матимемо: $E = a^0b^0$). Покажемо, що тоді $h \neq E$. Справді, оскільки $a^{i_r} = \left(\begin{smallmatrix} 1 & i_r m \\ 0 & 1 \end{smallmatrix}\right)$, а $b^{j_r} = \left(\begin{smallmatrix} 1 & 0 \\ j_r m & 1 \end{smallmatrix}\right)$, тому якщо (u_r, u_{r+1}) — перший рядок матриці $d = a^{i_1}b^{j_1}\dots a^{i_t}b^{j_t}$, де $t < k$, то перший рядок матриці $da^{i_{t+1}}$ матиме вигляд $(u_r, u_r i_{t+1} m + u_{r+1})$, а матриці $db^{j_{t+1}}$ — матиме вигляд $(u_r + u_{r+1}j_{t+1}m, u_{r+1})$. Виходячи з індукційного припущення, що $|u_{l+1}| > |u_l|$ для $l \leq r$, одержимо $|u_{r+1}| = |u_{r-1} + u_r s_{t+2} m| \geq |u_r||s_{t+2}|m - |u_{r-1}| \geq 2|u_r| - |u_{r-1}| \geq 2|u_r| - (|u_r| - 1) = |u_r| + 1$, де s_{t+2} дорівнює або i_{t+2}, або j_{t+2}. Тому матриця h ніколи не дорівнюватиме E. Звідси, оскільки $\operatorname{Ker}\varphi = \{w \in F(x, y) \mid \varphi(w) = E\}$, то $\operatorname{Ker}\varphi = \{\Lambda\}$ і відображення φ є ізоморфізмом.

Значення вільних груп у теорії груп стає зрозумілим з наступного твердження, яке можна вважати основною властивістю вільних груп.

Теорема 13.2. *Нехай група G породжується множиною елементів $S = \{s_1, \dots, s_n\}$. Тоді для вільної групи $F(X)$ із системою твірних $X = \{x_1, \dots, x_n\}$ існує єдиний гомоморфізм $\varphi : F(X) \to G$, при якому $\varphi : x_i \mapsto s_i$ для всіх $i = 1, \dots, n$.*

Доведення. Нехай $\varphi : F(X) \to G$ — гомоморфізм, такий що $\varphi : x_j \mapsto s_j$ для всіх $j = 1, \dots, n$, і нехай $[w]$ — довільний елемент із $F(X)$, де слово $w = x_{i_1}^{k_1} \dots x_{i_r}^{k_r}$, $i_1, \dots, i_r \in I$, $k_1, \dots, k_r \in \{\pm 1\}$, є єдиним нескоротним словом із класу $[w]$. Оскільки φ є гомоморфізмом, то мають місце наступні рівності:

$$\varphi([x_{i_1}^{k_1} \dots x_{i_r}^{k_r}]) = \varphi([x_{i_1}^{k_1} \dots x_{i_{r-1}}^{k_{r-1}}][x_{i_r}^{k_r}]) = \varphi([x_{i_1}^{k_1} \dots x_{i_{r-1}}^{k_{r-1}}])\varphi([x_{i_r}^{k_r}]) =$$

$$= \varphi([x_{i_1}^{k_1} \dots x_{i_{r-1}}^{k_{r-1}}])\varphi([x_{i_r}])^{k_r} = \varphi([x_{i_1}^{k_1} \dots x_{i_{r-1}}^{k_{r-1}}])s_{i_r}^{k_r} = \dots =$$

$$= \varphi([x_{i_1}^{k_1}])s_{i_2}^{k_2} \dots s_{i_r}^{k_r} = s_{i_1}^{k_1} \dots s_{i_r}^{k_r}.$$

Тим самим матимемо, що коли існує гомоморфізм φ, який задовольняє умові теореми, то він єдиний.

З іншого боку, відображення $\varphi : F(X) \to G$, $\varphi([x_{i_1}^{k_1} \dots x_{i_r}^{k_r}]) = s_{i_1}^{k_1} \dots s_{i_r}^{k_r}$, де $w = x_{i_1}^{k_1} \dots x_{i_r}^{k_r}$ $(i_1, \dots, i_r \in I, k_1, \dots, k_r \in \{\pm 1\})$ — нескоротне слово із класу $[w]$, задано коректно, бо кожен клас $[w]$ містить єдине нескоротне слово. Крім того, φ є гомоморфізмом, бо $\varphi([u][v])$ означає, що ми спочатку виконали скорочення в слові uv, а потім кожну букву x_i в цьому слові замінили буквою s_i, а $\varphi([u])\varphi([v])$ означає, що ми спочатку в словах $[u]$ та $[v]$ кожну букву x_i замінили буквою s_i, а вже потім виконали скорочення в одержаному слові.

Отже, існує єдиний гомоморфізм $\varphi : F(X) \to G$, при якому $\varphi : x_i \mapsto s_i$ для всіх $i = 1, \dots, n$. □

Таким чином, довільна група є гомоморфним образом вільної групи певного рангу.

Наслідок 13.1. *Кожна скінченнопороджена група G ізоморфна факторгрупі деякої вільної групи скінченного рангу.*

Доведення. Нехай $G =< S >$, де $S = \{s_1, \dots, s_n\}$. Розглянемо вільну групу $F(X)$ з системою твірних $X = \{x_1, \dots, x_n\}$. Згідно теореми 13.2

відображення $\varphi : F(X) \to G$, при якому $\varphi : x_i \mapsto s_i$ для всіх $i = 1, \ldots, n$, є гомоморфізмом. Крім того, легко видно, що φ є сюр'єктивним відображенням. Тому за основною теоремою про гомоморфізми груп матимемо $F(X)/\operatorname{Ker}\varphi \simeq G$. □

Зауваження. Одним із важливих моментів при дослідженні будови будь-якої групи є вивчення її підгруп. У 20-х роках минулого століття Нільсен і Шрейер довели, що кожна підгрупа вільної групи також є вільною. Доведення цього факту ми опустимо.

14 Задання групи твірними і співвідношеннями

Згідно теореми 13.2 довільна група G з системою твірних $S = \{s_1, \ldots, s_n\}$ є гомоморфним образом вільної групи $F(X)$, де $X = \{x_1, \ldots, x_n\}$. Іншими словами, відображення $\varphi : x_i \mapsto s_i$ продовжується до гомоморфізму $\varphi : F(X) \to G$. Позначимо символом H ядро цього гомоморфізму, і нехай R — така множина елементів підгрупи H, що H є найменшою нормальною підгрупою, яка містить R, тобто R така, що $< w^{-1}w_i w, w_i \in R, w \in F(X) >= H$. Згідно наслідку 13.1 група G ізоморфна факторгрупі $F(X)/H$. Тому група G повністю визначається заданням алфавіту X та множини R із ядра H. Пара $\langle X|R\rangle$ називається *зображенням Діка* групи G, множина X — *множиною твірних елементів*, а множина R — *множиною визначальних співвідношень*. Одна й та ж група може мати різні зображення Діка, і дуже часто визначити, чи дані зображення твірними елементами і визначальними співвідношеннями є зображеннями Діка однієї і тієї ж групи, важко. Найбільш суттєвим є те, що не існує алгоритмів, які би розв'язували наступні *проблеми Дена*:

- *проблему рівності* двох слів групи, яка задана твірними елементами і визначальними співвідношеннями;
- *проблему спряженості* двох слів групи, яка задана твірними елементами і визначальними співвідношеннями;
- *проблему ізоморфності* двох груп, які задані твірними елементами і визначальними співвідношеннями.

Приклади. 1. Очевидно, що $F(X) \simeq \langle X \,|\, \emptyset \rangle$, тобто вільна група немає співвідношень. Тому $F(X)$ ще називають групою, вільною від співвідношень.

2. $C_n \simeq \langle a \,|\, a^n \rangle$.

3. Четверна група Кляйна K_4 допускає наступне зображення твірними елементами і визначальними співвідношеннями:

$$K_4 \simeq \langle x, y \,|\, x^2, y^2, x^{-1}y^{-1}xy \rangle.$$

4. Покажемо, що зображенням Діка симетричної групи S_3 є $\langle x, y \,|\, x^2, y^2, (xy)^3 \rangle$. Справді, група $G = \langle x, y \,|\, x^2, y^2, (xy)^3 \rangle$ має порядок ≤ 6, бо $x^2 = 1$, $y^2 = 1$, $(xy)^3 = 1$, тому $yx = (xy)^2$, $xy = (yx)^2$, $xyxyx = y$, $yxyxy = x$ і група G містить лише елементи 1, x, y, xy, xyx, $xyxy$. Розглянемо відображення $\varphi : G \to S_3$, задане наступним чином: $\varphi : x \mapsto (12)$, $\varphi : y \mapsto (13)$. Неважко переконатися у тому, що φ є ізоморфізмом, тому $G \simeq S_3$.

Задача 14.1. *Покажіть, що* $S_3 \simeq \langle x, y \,|\, x^2, y^3, (xy)^2 \rangle$.

5. Зображення Діка знакозмінної групи A_4 :

$$A_4 \simeq \langle x, y \,|\, x^3, y^3, (xy)^2 \rangle \simeq \langle x, y \,|\, x^3, y^2, (xy)^3 \rangle.$$

6. Вільна абелева група G рангу n має наступне зображення твірними елементами і визначальними співвідношеннями:

$$G \simeq \langle x_1, \ldots, x_n \,|\, x_i^{-1}x_j^{-1}x_ix_j, i, j \in \{1, \ldots, n\}, i < j \rangle$$

(про цю групу див. також на стор. 107).

Задача 14.2. *Доведіть зображення груп твірними елементами і визначальними співвідношеннями із прикладів* 2, 3, 5, 6.

7. Розглянемо зображення Діка діедральної групи D_n. Нагадаємо (див. приклад 7 на стор. 23), що D_n — це група рухів правильного n–кутника, елементами якої є n поворотів відносно його центра на кути $0°$, $360°/n$, $2{\cdot}360°/n$, $\ldots$, $(n{-}1){\cdot}360°/n$ та n симетрій $l_1, \ldots, l_n$ відносно осей, що проходять при непарному n через вершини n–кутника та середини протилежних ребер, а при парному n — через дві протилежні вершини

або через середини двох протилежних ребер. Покажемо, що $D_4 \simeq G$, де $G = \langle a, b \,|\, a^2, b^n, baba^{-1} \rangle$. Справді, із визначальних співвідношень матимемо, що $ba = ab^{-1}$. Тому кожен елемент групи G зображується словом вигляду $a^{\varepsilon} b^k$, де $\varepsilon \in \{0, 1\}$, $k \in \{0, 1, \ldots, n-1\}$. Отже, порядок G не перевищує $2n$.

З іншого боку, згідно теореми 13.2 існують епіморфізми $\varphi : F(x, y) \to G$ та $\psi : F(x, y) \to D_n$ вільної групи $F(x, y)$ на групи G та D_n відповідно. Тоді відображення $\mu : G \to D_n$, $\mu(g) = \psi(\varphi^{-1}(g))$ також буде гомоморфізмом, а тому $|G| \geq |D_n|$.

Отже, $|G| = |D_n|$, і, легко бачити, що бієктивне відображення $\nu : D_n \to G$, $\nu : 360^\circ/n \mapsto b$, $\nu : l_1 \mapsto a$, буде ізоморфізмом цих груп.

Діедральна група допускає інше задання твірними елементами і визначальними співвідношеннями:

Вправа 14.1. *Доведіть, що* $D_4 \simeq \langle x, y \,|\, x^2, y^2, (xy)^n \rangle$.

8. Покажемо, що групу кватерніонів $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ можна задати твірними елементами і визначальними співвідношеннями наступним чином:

$$Q_8 \simeq \langle x, y \,|\, x^4, x^2 y^{-2}, yxy^{-1}x \rangle.$$

Справді, нехай $G = \langle x, y \,|\, x^4, x^2 y^{-2}, yxy^{-1}x \rangle$. Тоді оскільки $ba = a^{-1}b = a^3 b$, $a^2 = b^2$, то кожне слово групи G зводитиметься до вигляду $a^k b^l$, де $0 \leq k \leq 3$, $0 \leq l \leq 1$, а тому порядок G не перевищує 8. З іншого боку, елементи групи Q_8 задовольняють співвідношенням: $i^4 = 1$, $i^2 = j^2$, $jij^{-1} = i^{-1}$. Розглянемо відображення $\varphi : G \to Q_8$, $\varphi : x \mapsto i$, $\varphi : y \mapsto j$. Легко перевірити, що φ є ізоморфізмом (покажіть це!). Тому $Q_8 \simeq G$.

Задача 14.3. *Покажіть, що* $Q_8 \simeq \langle x, y \,|\, x^{-1}yxy, y^{-1}xyx \rangle$.

15 p–групи

Нехай p — фіксоване просте число.

Означення 15.1. *Група G називається p–групою, якщо порядок кожного її елемента є степенем числа p.*

Очевидно, що підгрупа і факторгрупа p–групи також є p–групами.

Приклади. 1. Група Q_8 є 2–групою.

2. В адитивній групі векторного простору над полем $\mathbb{Z}_p$ усі ненульові вектори мають порядок p, тому вона є p–групою.

3. Група $\mathbb{C}_{p^\infty}$ є нескінченною p–групою.

Задача (жарт). *Дайте загальне означення α–групи, яке б мало зміст для кожного дійсного числа α і яке б при $\alpha = 1$ переходило в означення групи, при $\alpha = 1/2$ — в означення напівгрупи, при $\alpha = 0$ — в означення неструктурованої множини, а для кожного простого p — в означення p–групи.*

Твердження 15.1. *Скінченна група G буде p–групою тоді й лише тоді, коли її порядок $|G|$ є числом вигляду p^n, де $n \in \mathbb{N}_0$.*

Доведення. Достатність умови випливає з теореми Лагранжа, а необхідність — з леми Коші (якщо порядок групи G не є числом вигляду p^n, то він ділиться на якесь просте число $q \neq p$, а тому група G містить елемент порядку q). □

Теорема 15.1. *Кожна скінченна неодинична p–група G має неодиничний центр.*

Доведення. За попереднім твердженням $|G| = p^n$, де $n \geq 1$. Нехай $C_1, \ldots, C_k$ — усі неодноелементні класи спряженості групи G. Тоді

$$G = Z(G) \bigcup \Big(\bigcup_{i=1}^{k} C_i \Big) \quad \text{і} \quad |G| = |Z(G)| + \sum_{i=1}^{k} |C_i| \,.$$

Кожне з чисел $|C_i|$ є дільником порядку групи, тому воно ділиться на p. Але тоді в правій частині рівності $|Z(G)| = |G| - \sum_{i=1}^{k} |C_i|$ всі доданки діляться на p. Отже, число $|Z(G)|$ ділиться на p, а тому $Z(G) \neq E$. □

Наслідок 15.1. *Кожна група G порядку p^2 є абелевою.*

Доведення. Із теореми 15.1 випливає, що або $Z(G) = G$, і тоді група G є абелевою, або $|Z(G)| = p$. У другому випадку факторгрупа $G/Z(G)$ має порядок p і є циклічною, що суперечить твердженню 11.5. Отже, другий випадок неможливий. □

Теорема 15.2. *Якщо $|G| = p^n$, то група G містить ланцюг підгруп*

$$E = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_n = G,$$

кожна з яких є нормальною в G, причому кожна факторгрупа G_i/G_{i-1}, $i = 1, \ldots, n$, є циклічною порядку p.

Доведення. Застосуємо індукцію за порядком групи. Для $n = 1$ твердження очевидне. Нехай тепер $n > 1$. За теоремою 15.1 центр $Z(G)$ має порядок $\geq p$, тому згідно леми Коші центр містить елемент a порядку p. Оскільки кожна підгрупа центру, як об'єднання одноелементних класів спряженості, є нормальною в G, то нормальною буде і підгрупа $R = \langle a \rangle$. За припущенням індукції у факторгрупі G/R існує ланцюг підгруп

$$E = H_0 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_{n-1} = G/R$$

такий, що кожна H_i є нормальною в G/R, а кожна факторгруупа H_i/H_{i-1} є циклічною порядку p. Нехай тепер $\pi : G \to G/R$ — канонічний епіморфізм. Покладемо $G_i = \pi^{-1}(H_{i-1})$, $i = 1, 2, \ldots, n$. Тоді, за теоремою 12.2, ланцюг підгруп

$$E = G_0 < G_1 < G_2 < \cdots < G_n = G$$

задовольняє умови теореми. □

Задача 15.1. *Доведіть, що коли підгрупа H нескінченної p–групи G має скінченний індекс, то цей індекс є степенем числа p.*

Вказівка. Доведіть, що перетин $\bigcap_{a \in G} H^a$ усіх спряжених із H підгруп є нормальною підгрупою скінченного індексу, і скористайтеся тим, що факторгрупа p–групи також є p–групою.

Задача 15.2. *Доведіть, що в довільній p–групі G кожна нормальна підгрупа $H \lhd G$ порядку p лежить у центрі $Z(G)$.*

Вказівка. Із задачі 15.1 і теореми 11.2 випливає, що потужності скінченних класів спряжених елементів групи G є степенями p.

16 Комутант

Означення 16.1. *Комутатором елементів a і b групи G називається елемент $[a, b] = a^{-1}b^{-1}ab$.*

Очевидно, що комутатор двох елементів дорівнює e тоді й лише тоді, коли ці елементи переставні. Безпосередньою перевіркою легко довести наступні властивості комутатора.

Твердження 16.1. *Для довільних a, b, с елементів групи G виконуються рівності*: a) $[a,b]^{-1} = [b,a]$; b) $ab = ba \cdot [a,b]$; c) $[a,b]^x = [a^x, b^x]$.

Вправа 16.1. *Доведіть твердження* 16.1.

Означення 16.2. *Комутантом (або похідною підгрупою) групи G називають підгрупу G' $(= [G,G])$, яка породжена всіма комутаторами, тобто $G' = \langle [a,b] \mid a,b \in G \rangle$.*

Зауваження. Хоча $[a,b]^{-1} = [b,a]$ є комутатором, добуток двох комутаторів взагалі кажучи комутатором може і не бути. Тому комутант $[G,G]$ групи G складається із всіх можливих добутків виду

$$[a_1,b_1] \cdot \dots \cdot [a_k,b_k], \quad \text{де} \quad a_i,\ b_i \in G.$$

Із твердження 16.1 п. b) легко випливатиме, що чим більше в групі комутаторів (тобто чим більший комутант групи G), то тим група "некомутативніша". Тому, поруч із центром групи, комутант є "мірою комутативності" групи.

Твердження 16.2. *Комутант $[G,G]$ групи G є її нормальною підгрупою.*

Доведення. Нехай $g \in G$ і $h \in [G,G]$ — довільні. Тоді $g^{-1}hg = h \cdot [h,g] \in [G,G]$. □

Проілюструємо це поняття на прикладах.

Приклади. 1. $[G,G] = E$ тоді й лише тоді, коли група G — абелева.

2. Комутант довільної неабелевої групи G, яка не містить неодиничних нормальних підгруп, збігається з всією групою, бо згідно твердження 16.2 комутант є нормальною підгрупою, а тому є тривіальною підгрупою. Але до того ж G — неабелева. Отже, $[G,G] = G$.

3. Комутатори діедральної групи D_4 і групи кватерніонів Q_8 збігаються з своїми центрами: $[D_4,D_4] = \{0^\circ, 180^\circ\} = Z(D_4)$, $[Q_8,Q_8] = \{1,-1\} = Z(Q_8)$.

Теорема 16.1 (основна властивість комутанта). *Довільна підгрупа H групи G, яка містить комутант, є нормальною в G. Факторгрупа групи G по нормальній підгрупі H буде абелевою тоді й лише тоді, коли H містить комутант $[G,G]$ групи G.*

Доведення. Нормальність кожної надгрупи $H \geq [G,G]$ доводиться так, як і твердження 16.2. Нехай тепер $H \lhd G$. Тоді для довільних елементів aH, bH факторгрупи G/H

$$aH \cdot bH = bH \cdot aH \iff abH = baH \iff [a,b]H = H \iff [a,b] \in H \ .$$

□

Приклад. $[S_n, S_n] = A_n$ для довільного натурального n. Справді, комутатор довільних двох підстановок очевидно є парною підстановкою, тому $[S_n, S_n] \subseteq A_n$. З іншого боку, $(ijk) = [(ik),(ij)] = [(ikl),(ijm)]$, де i, j, k, l, m — попарно різні елементи. А далі залишилося скористатися лише тим, що A_n породжується циклами довжини 3 (задача 5.6).

Задача 16.1. *Доведіть, що комутант $[H,H]$ нормальної підгрупи H групи G є нормальною підгрупою G.*

Задача 16.2. *Доведіть, що комутант скінченної p–групи є її власною підгрупою.*

Задача 16.3. *Доведіть, що центр і комутант довільної некомутативної групи порядку p^3 збігаються.*

17 Прості групи

Означення 17.1. *Група G називається простою, якщо G не має нетривіальних нормальних підгруп.*

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.

Твердження 17.1. *Кожна скінченна p–група G порядку $|G| > p$ не є простою.*

Доведення. Згідно теореми 15.1 група G має неодиничний центр $Z(G)$, а за лемою Коші центр містить елемент порядку p. Тоді підгрупа $\langle a \rangle$ є нетривіальною підгрупою групи G, яка згідно вправи 11.2 є нормальною. Тому G не є простою. □

Задача 17.1*. *Доведіть, що кожна неабелева група порядку, меншого за* 60*, не є простою.*

Вправа 17.1. *Доведіть, що коли підгрупа H групи S_n містить непарні підстановки, то рівно половина її елементів буде парними підстановками, а половина — непарними.*

Розглянемо один із прикладів простих груп, а саме:

Теорема 17.1. *Група A_5 — проста.*

Доведення. Очевидно, що підстановка $b \in S_n$ належить нормалізатору $N_{A_n}(a)$ елемента $a \in A_n$ тоді й лише тоді, коли b належить нормалізатору $N_{S_n}(a)$ і є парною підстановкою. Отже, $N_{A_n}(a) = N_{S_n}(a)$, якщо $N_{S_n}(a)$ містить лише парні підстановки, і $|N_{A_n}(a)| = \frac{1}{2}|N_{S_n}(a)|$, якщо $N_{S_n}(a)$ містить також непарні підстановки (останнє випливає з вправи 17.1). За теоремою 11.2 у першому випадку потужність $|C_{A_n}(a)| = |A_n : N_{A_n}(a)|$ класу $C_{A_n}(a)$ спряжених з a у групі A_n елементів вдвічі менша за потужність $|C_{S_n}(a)| = |S_n : N_{S_n}(a)|$ відповідного класу в групі S_n, а в другому випадку ці потужності рівні:

$$|A_n : N_{A_n}(a)| = \frac{|A_n|}{|N_{A_n}(a)|} = \frac{\frac{1}{2}|S_n|}{\frac{1}{2}|N_{S_n}(a)|} = \frac{|S_n|}{|N_{S_n}(a)|} = |S_n : N_{S_n}(a)| \,.$$

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 $C\big((123)\big)$ потужності 20, клас $C\big((12)(34)\big)$ потужності 15 і клас $C\big((12345)\big)$ 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. □

Зауваження. 1. Ґалуа довів, що простими є всі групи A_n, $n \geq 5$. Тому існує нескінченно багато простих некомутативних скінченних груп.

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.

Задача 17.2. *Доведіть, що кожна група порядку pq, де p і q — не обов'язково різні прості числа, не є простою.*

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

Задача 17.3.* *Доведіть, що група $GL_3(\mathbb{Z}_2)$ є простою.*

Зауваження. 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. Вважаєтья, 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 кла-

сифікація скінченних простих груп великим міфом XX сторіччя, чи — реальністю, все ще відповісти важко.

18 Дія групи на множині

Означення 18.1. *Нехай G — деяка група, M — множина. Кажуть, що група G діє на множині M, якщо для довільних елементів $m \in M$ та $g \in G$ визначений елемент $m^g \in M$, причому:*

1) $m^e = m$ *для всіх* $m \in M$;

2) $\big(m^{g_1}\big)^{g_2} = m^{g_1 g_2}$ *для всіх* $m \in M$, $g_1, g_2 \in G$.

Той факт, що група G діє на множині M, позначатимемо (G, M), а елементи множини M називатимемо точками.

Поруч із показниковим записом m^g образу точки m під дією елемента g вживається і позначення $g(m)$. Показниковий запис є коротшим, а часто і зручнішим.

Якщо задана дія групи G на множині M, то кожному елементу $g \in G$ відповідає перетворення $\varphi(g)$ множини M, яке точку $m \in M$ переводить у точку m^g.

Твердження 18.1. *Нехай задана дія групи G на множині M. Тоді*

a) *для довільного елемента $g \in G$ перетворення $\varphi(g)$ буде бієкцією множини M;*

b) *відображення $g \mapsto \varphi(g)$ буде гомоморфіізмом групи G в симетричну групу $\mathrm{Sym}(M)$ всіх взаємно однозначних перетворень множини M.*

Доведення. a) Із рівностей

$$\varphi(g)\big(\varphi(g^{-1})(m)\big) = (m^{g^{-1}})^g = m^{g^{-1}g} = m^e = m =$$

$$= m^{gg^{-1}} = (m^g)^{g^{-1}} = \varphi(g^{-1})\big(\varphi(g)(m)\big)$$

випливає, що перетворення $\varphi(g)$ і $\varphi(g^{-1})$ є взаємно оберненими. А тому кожне з них є бієктивним.

b) Нам треба довести, що $\varphi(gh) = \varphi(g) \cdot \varphi(h)$. Але це випливає з того, що для довільної точки $m \in M$

$$\varphi(gh)(m) = m^{gh} = (m^g)^h = \big(\varphi(g)(m)\big)^h =$$

$$= \varphi(h)\big(\varphi(g)(m)\big) = \big(\varphi(g) \cdot \varphi(h)\big)(m).$$

□

Гомоморфізм $\varphi : G \to \mathrm{Sym}(M)$, який пов'язаний із дією групи G на множині M, будемо називати *зображенням групи G взаємно однозначними перетвореннями* множини M.

Оскільки взаємно однозначні перетворення скінченної множини звичайно називають підстановками, то у випадку, коли множина M скінченна, будемо говорити також про *зображення групи G підстановками множини M*.

Множина $K = \{g \in G \mid \text{ для всіх } m \in M\ m^g = m\}$ називається *ядром дії* (G, M) групи G на множині M і збігається з ядром $Ker\,\varphi$ гомоморфізма φ при зображенні G в $\mathrm{Sym}(M)$.

Твердження 18.2. *Нехай K — ядро дії (G, M) групи G на множині M. Елементи g_1 і g_2 групи G діють на множині M однаково тоді й лише тоді, коли вони належать до одного класу суміжності за підгрупою K.*

Доведення. Якщо для всіх $m \in M\ \ m^{g_1} = m^{g_2}$, то $m = m^{g_2 g_1^{-1}}$. Тоді за означенням ядра K дії (G, M) матимемо $g_2 g_1^{-1} \in K$ і $g_2 \in K g_1$. З іншого боку, якщо $g_1, g_2 \in Kg$ для деякого $g \in G$, тобто існують такі $h_1, h_2 \in K$, що $g_1 = h_1 g$, $g_1 = h_2 g$, то для всіх $m \in M\ \ m^{g_1} = m^{h_1 g} = \left(m^{h_1}\right)^g = m^g$, $m^{g_2} = m^{h_2 g} = \left(m^{h_2}\right)^g = m^g$, тобто $m^{g_1} = m^{g_2}$. □

Дія (G, M) називається *точною* або *ефективною*, якщо ядро цієї дії тривіальне (тобто $K = E$) або якщо гомоморфізм φ є ін'єктивним. Оскільки згідно твердження 18.2 усі елементи з класу суміжності за ядром K діють на множині M однаково, то це дозволяє визначити природну дію на множині M факторгрупи G/K, яка, очевидно, буде вже точною. У випадку точної дії групи G на скінченній множині M говорять також про *групу підстановок* (G, M) або про *точне зображення групи G підстановками*.

Нехай групи G, G' точно діють відповідно на множинах M, M'. Природно називати їх *ізоморфними як групи підстановок*, якщо існують взаємно однозначна відповідність ψ між множинами M та M' і ізоморфізм φ групи G на групу G' такі, що

$$\psi(m^g) = \psi(m)^{\varphi(g)} \quad \text{для всіх} \quad m \in M,\ g \in G.$$

Ізоморфні групи підстановок називаються також *подібними*.

Приклади. 1. Групу O всіх поворотів куба можна примусити природно діяти на множині: a) прямих, що проходять через центри протилежних граней куба; b) діагоналей куба; c) граней куба; d) вершин

куба; е) ребер куба. Після нумерації елементів відповідної множини натуральними числами одержуємо гомоморфізм групи O в групу: а) S_3; b) S_4; c) S_6; d) S_8; e) S_{12}. Усі ці дії групи O, крім першої, є точними. Ядром першої дії є підгрупа порядку 4, що складається з тотожного перетворення і поворотів на 180° навколо осей, що проходять через центри протилежних граней.

2. Можна кількома природними способами визначити дію довільної групи G на множині $\dot{G}$ своїх же елементів. Найважливішими з них є:
а) *дія правими зсувами*: $x^g = xg$ (т. зв. *регулярне зображення* групи, воно вже зустрічалося при доведенні теореми Келі); і
b) *дія спряженнями*: $x^g = g^{-1}xg$.
Перша дія є точною, а ядром другої дії є центр $Z(G)$ групи G.

3. Узагальненням регулярного зображення є дія групи правими зсувами на правих класах суміжності за довільною підгрупою H: $(Hx)^g = Hxg$.

4. Із кожною дією групи G на множині M природно пов'язується цілий ряд т. зв. *індукованих* дій цієї групи, зокрема, на множині $M^{(k)} = \{A \subseteq M \,|\, |A| = k\}$ k–елементних підмножин множини M за правилом $A^g = \{a^g \,|\, a \in A\}$ і на множині $M^k = \{(m_1, \ldots, m_k) \,|\, m_1, \ldots, m_k \in M\}$ наборів довжини k за правилом $(m_1, \ldots, m_k)^g = (m_1^g, \ldots, m_k^g)$.

Кожна дія групи G на множині M визначає певне відношення еквівалентності $\sim$ на множині M:

$$a \sim b \;\Leftrightarrow\; \text{існує такий елемент } \; g \in G, \text{ що } \; a^g = b.$$

Вправа 18.1. *Перевірте, що це справді відношення еквівалентності.*

Класи еквівалентності $\mathcal{O}$ цього відношення називаються *орбітами* групи G. Легко бачити, що довільні дві орбіти або збігаються, або не перетинаються, а тому множина M розбивається в диз'юнктне об'єднання орбіт $M = \sqcup_{i \in I} \mathcal{O}_i$. Також позначимо символом $\mathcal{O}(a)$ або a^G множину $\{a^g \,|\, g \in G\}$, яку природно назвати *орбітою точки* $a \in M$.

Твердження 18.3. *Нехай задана дія (G, M) групи G на множині M. Тоді для довільного елемента a орбіти $\mathcal{O}$ матимемо $\mathcal{O} = \mathcal{O}(a)$.*

Доведення. Нехай $b \in \mathcal{O}$, $b \neq a$. Тоді існує $g \in G$ такий, що $a^g = b$. Звідки включення $\mathcal{O} \subseteq \mathcal{O}(a)$ легко випливає. І навпаки, якщо $b \in \mathcal{O}(a)$, то знайдеться такий елемент $g \in G$, що $b = a^g$, а тому $a \sim b$ і $b \in \mathcal{O}$. $\square$

Наслідок 18.1. *Якщо група G діє на множині M, то для довільних* $a, b \in M \quad a \sim b \;\Leftrightarrow\; \mathcal{O}(a) = \mathcal{O}(b)$.

Таким чином, орбіта точки $a \in M$ — це клас еквівалентності, що містить точку a.

Приклади. 1. Для природної дії групи G всіх поворотів площини навколо фіксованої точки O на множині точок площини орбітами будуть кола з центром у точці O.

2. При природній дії групи ортогональних перетворень на множині векторів арифметичного векторного простору орбітами будуть множини векторів однакової довжини.

3. Для дії групи G на собі спряженнями орбітами будуть класи спряжених елементів групи G. Зокрема, у випадку групи $GL_n(\mathbb{C})$ це будуть класи невироджених матриць з однією і тією ж нормальною жордановою формою.

4. Група може діяти по–різному навіть на одній і тій же множині. Наприклад, дію нециклічної групи $G = \{e, a, b, c\}$ порядку 4 на множині $M = \{1, 2, 3, 4\}$ можна визначити так, щоб її елементам відповідали підстановки $\varphi(e) = \varepsilon$, $\varphi(a) = (12)(34)$, $\varphi(b) = (13)(24)$, $\varphi(c) = (14)(23)$, а можна елементам групи G зіставити підстановки $\varphi(e) = \varepsilon$, $\varphi(a) = (12)$, $\varphi(b) = (34)$, $\varphi(c) = (12)(34)$. Тоді у першому випадку матимемо лише одну орбіту M, а в другому — дві орбіти $\mathcal{O}_1 = \{1, 2\}$ і $\mathcal{O}_2 = \{3, 4\}$.

Вправа 18.2. *Нехай H — підгрупа групи G. Доведіть, що кожне з правил $g^h = gh$ і $g^h = h^{-1}g$ визначає дію підгрупи H на множині $\dot{G}$ елементів групи G. Знайдіть орбіти цих дій.*

Група підстановок (G, M) називається *транзитивною*, якщо вона має лише одну орбіту (тобто для довільних $x, y \in M$ знайдеться такий елемент $g \in G$, що $x^g = y$), та *інтранзитивною*, якщо орбіт більше однієї.

Зауваження. 1. Раніше (див. приклад 3 на стор. 81) з кожною підгрупою $H < G$ ми зв'язали зображення групи G взаємно однозначними перетвореннями множини правих класів суміжності G за підгрупою H. Таке зображення є транзитивним, бо якщо Hg_1, Hg_2 — два праві класи суміжності, то $(Hg_1)g_1^{-1}g_2 = Hg_2$. Насправді, має місце і зворотне: кожне транзитивне зображення даної групи взаємно однозначними пе-

ретвореннями подібне зображенню цієї групи правими зсувами на множині правих класів суміжності за деякою підгрупою.

2. Транзитивні дії у певному сенсі можна вважати найпростішими діями групи, а інтранзитивні — як узгодження кількох транзитивних дій групи на різних орбітах.

Дія (G, M) називається *k–транзитивною*, якщо індукована дія групи G на множині $M^{[k]}$ усіх тих наборів $(m_1, \ldots, m_k)$ довжини k, компоненти $m_1, \ldots, m_k$ яких є попарно різними, є транзитивною. Іншими словами, дія (G, M) є k–транзитивною, якщо для довільних двох наборів $m_1, \ldots, m_k$ та $\tilde{m}_1, \ldots, \tilde{m}_k$ із множини M, елементи кожного з яких є попарно різними, існує такий $g \in G$, що $m_1^g = \tilde{m}_1, \ldots, m_k^g = \tilde{m}_k$.

Задача 18.1. *Нехай $\chi(g)$ — кількість нерухомих точок елемента $g \in G$ при дії групи G на множині M. Доведіть, що*: а) *для 2–транзитивної групи G*

$$\sum_{g \in G} \chi^2(g) = 2 \cdot |G|;$$

b) *для 3–транзитивної групи G*

$$\sum_{g \in G} \chi^3(g) = 5 \cdot |G|.$$

Вказівка. а) Якщо $\chi(g)$ і $\chi'(g)$ — кількість нерухомих точок елемента g при дії G на M і $M^{[2]}$ відповідно, то $\sum_{g \in G} \chi(g) = |G|$ і $\sum_{g \in G} \chi'(g) = |G|$. Додайте ці рівності і врахуйте, що $\chi'(g) = \chi(g)(\chi(g) - 1)$.

Задача 18.2. *Доведіть, що*: а) *група S_n є $n-$транзитивною*; b) *група A_n є $(n-2)-$транзитивною і не є $(n-1)-$транзитивною.*

Підмножина $N \subseteq M$ називається *інваріантною відносно дії групи* G, якщо $m^g \in N$ для всіх $m \in N$ і $g \in G$. Очевидно, що підмножина є інваріантною тоді й лише тоді, коли вона є об'єднанням орбіт групи G. Тому для кожної інваріантної підмножини N можна розглядати обмеження (G, N) дії групи G на цю підмножину.

Точка $m \in M$ називається *нерухомою* відносно елемента $g \in G$, якщо $m^g = m$. Точки, нерухомі відносно усіх елементів групи G — це просто 1–елементні орбіти групи G. Множина $\{g \in G \,|\, m^g = m\}$ називається *стабілізатором* точки m і позначається $St_G(m)$ або коротко $St(m)$. Очевидно, що для кожної точки $m \in M$ її стабілізатор $St_G(m)$ є підгрупою групи G.

Теорема 18.1. *Нехай група G діє на множині M. Тоді існує природна взаємно однозначна відповідність між елементами орбіти $\mathcal{O}(m)$ і правими класами суміжності групи G за підгрупою $St_G(m)$. Зокрема, $|\mathcal{O}(m)| = |G : St_G(m)|$, тобто довжина орбіти точки дорівнює індексові її стабілізатора.*

Доведення. Нехай $a \in \mathcal{O}(m)$. Виберемо такий елемент $g \in G$, що $a = m^g$. Тоді

$$m^h = a \iff (m^h)^{g^{-1}} = m \iff hg^{-1} \in St_G(m) \iff h \in St_G(m) \cdot g.$$

Таким чином, кожній точці $a \in \mathcal{O}(m)$ природно зіставляється правий клас суміжності $St_G(m) \cdot g$ тих елементів групи G, які точку m переводять в a. □

Наслідок 18.2. a) *Потужність $|\mathcal{O}(m)|$ орбіти точки m ділить порядок $|G|$ групи G.*
b) *Стабілізатори точок, що належать одній орбіті, мають однаковий порядок.*

Приклад. Знайдемо $\binom{n}{k}$ кількість k–елементних підмножин множини M, яка складається з n елементів. Для цього розглянемо природну дію симетричної групи S_n на множині $M^{\{k\}}$ k–елементних підмножин множини $M = \{1, \ldots, n\}$. Така дія є транзитивною. Нехай $A = \{i_1, \ldots, i_k\}$ — довільна підмножина із $M^{\{k\}}$. Тоді стабілізатор $St_{S_n}(A)$ складається із усіх тих підстановок множини M, які переставляють тільки точки всередині кожної з множин A та $M \backslash A$. А таких підстановок, як легко бачити, буде $|A|! \cdot |M \backslash A|! = k! \cdot (n-k)!$. Крім того,

$$|M^{\{k\}}| = |\mathcal{O}(A)| = |S_n : St_{S_n}(A)| = \frac{n!}{|St_{S_n}(A)|}.$$

Тому $|M^{\{k\}}| = \frac{n!}{k!(n-k)!}$ і $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Наслідок 18.2 b) можна трохи посилити:

Твердження 18.4. *Стабілізатори точок, що належать до однієї орбіти, є спряженими підгрупами.*

Доведення. Оскільки згідно твердження 18.3 орбіта $\mathcal{O}$ збігається з орбітою довільного елемента m, що їй належить, то досить показати, що для довільнних $m \in M$ та $g \in G$ $St(m^g) = g^{-1}St(m)g$. Нехай

$\tilde{g} \in St(m)$. Тоді $(m^g)^{g^{-1}\tilde{g}g} = m^{gg^{-1}\tilde{g}g} = (m^{\tilde{g}})^g = m^g$ і $g^{-1}\tilde{g}g \in St(m^g)$. Тому $St(m^g) \supseteq g^{-1}St(m)g$. З іншого боку, для $h \in St(m^g)$ матимемо: $(m^g)^h = m^g$, звідки $m^{ghg^{-1}} = m$ і $ghg^{-1} \in St(m)$. Тобто $h \in g^{-1}St(m)g$ і $St(m^g) \subseteq g^{-1}St(m)g$. Отже, $St(m^g) = g^{-1}St(m)g$. □

Задача 18.3. *Доведіть, що у скінченній p–групі число тих підгруп, які не є нормальними, ділиться на p.*

Вказівка. Розгляньте дію групи спряженнями на множині своїх підгруп.

Дія групи на різних множинах є дуже ефективним методом дослідження груп. Фактично ми вже ним користувалися. Так, при доведенні теореми Келі (теорема 7.1) використовувалося регулярне зображення групи, а при доведенні леми Коші (наслідок 11.3) і неодиничності центра скінченної неодиничної p–групи (теорема 15.1) — формула класів (теорема 11.3), в якій йдеться про потужності класів спряженості, тобто про довжини орбіт при дії групи на собі спряженнями. Використовуючи іншу дію, можна дати значно коротше доведення леми Коші.

Нове доведення леми Коші. Нехай порядок $|G|$ групи G ділиться на просте число p. Розглянемо множину

$$M = \{(g_1, g_2, \ldots, g_p) \,|\, g_1, g_2, \ldots, g_p \in G,\ g_1 g_2 \cdots g_p = e\}$$

і визначимо дію на M групи $\mathbb{Z}_p$ таким правилом:

$$(g_1, g_2, \ldots, g_p)^{\bar{k}} = (g_{p-k+1}, g_{p-k+2}, \ldots, g_p, g_1, g_2, \ldots, g_{p-k})\ .$$

Множина M містить $|G|^{p-1}$ наборів, тому її потужність $|M|$ ділиться на p. За теоремою 18.1 орбіти групи $\mathbb{Z}_p$ мають порядок 1 або p. Оскільки одна 1–елементна орбіта напевно є — це $\{(e, e, \ldots, e)\}$, то мусять бути й інші 1–елементні орбіти. Кожна така орбіта має вигляд $\{(g, g, \ldots, g)\}$. Але тоді g — елемент порядку p. □

У багатьох задачах належність чи неналежність елементів множини M до однієї орбіти дії певної групи G на M є основою класифікації цих елементів. Наприклад, в геометрії рівність двох плоских фігур визначається саме як їх належність до однієї орбіти при природній дії групи рухів площини на множині фігур. У теорії графів можна розглянути природну дію симетричної групи S_n на множині всіх n–вершинних графів із множиною вершин $V = \{1, 2, \ldots, n\}$: підстановка $\pi \in S_n$ задає

перенумерацію вершин графа, коли вершина зі старим номером i одержує новий номер $\pi(i)$. Тоді належність двох n–вершинних графів до однієї орбіти групи S_n означає їх ізоморфність. У таких випадках дуже корисно вміти знаходити кількість орбіт групи G.

Лема 18.1 (Коші–Фробеніуса–Бернсайда). *Нехай скінченна група G діє на скінченній множині M. Тоді*

$$\textit{кількість орбіт групи } G \textit{ дорівнює } \frac{1}{|G|}\sum_{g\in G}\chi(g),$$

де $\chi(g)$ — кількість нерухомих точок елемента g.

Доведення. Підрахуємо двома способами кількість таких пар (g, m), в яких $g \in G$, $m \in M$ і $m^g = m$. З одного боку, вона дорівнює $\sum_{g\in G}\chi(g)$. З іншого боку, кількість таких пар дорівнює $\sum_{m\in M}|St(m)|$. Щоб перетворити останню суму, розглянемо всі орбіти M_1, M_2, …, M_N групи G і в кожній орбіті M_i виберемо представника m_i. Враховуючи теорему 18.1 і наслідок 18.2 b), маємо:

$$\sum_{m\in M}|St(m)| = \sum_{i=1}^{N}\sum_{m\in M_i}|St(m)| = \sum_{i=1}^{N}\sum_{m\in M_i}|St(m_i)| =$$

$$= \sum_{i=1}^{N}|M_i|\cdot|St(m_i)| = \sum_{i=1}^{N}|G| = N\cdot|G|\,.$$

Таким чином, $\sum_{g\in G}\chi(g) = N\cdot|G|$, що й доводить твердження. □

Зауваження. Функція $\chi : G \to \mathbb{N}_0$, $g \mapsto \chi(g)$, називається *підстановочним характером* групи G. Якщо група транзитивна, то з леми Коші–Фробеніуса–Бернсайда випливає, що $\sum_{g\in G}\chi(g) = |G|$, тобто в цьому випадку кожен елемент групи G має в середньому рівно 1 нерухому точку.

Задача 18.4. *Доведіть, що кожна підстановка з симетричної групи S_n має в середньому рівно $1/k$ циклів довжини k $(k = 1, 2, \ldots, n)$.*

Лема Коші–Фробеніуса–Бернсайда має численні застосування в комбінаторному аналізі, де вона використовується для підрахунку різних комбінаторних об'єктів.

Приклади. 1. Кожна грань куба фарбується в один із даних k кольорів. При фіксованому розміщенні куба в просторі маємо, очевидно, k^6 різних розфарбувань. На множині M цих розфарбувань природно діє група O поворотів куба. Назвемо два розфарбування геометрично різними, якщо одне з них не можна перевести в інше жодним поворотом куба. Підрахуємо кількість геометрично різних розфарбувань.

Група O містить такі елементи: a) 1 тотожне перетворення; b) 6 поворотів навколо осей, що проходять через центри протилежних граней, на кути $\pm 90°$; c) 3 повороти навколо осей, що проходять через центри протилежних граней, на кут $180°$; d) 8 поворотів навколо осей, що проходять через протилежні вершини, на кути $\pm 120°$; e) 6 поворотів навколо осей, що проходять через середини протилежних ребер, на кут $180°$. Для кожного з таких поворотів кількість нерухомих точок — кількість тих розфарбувань куба, які при цьому повороті переходять у себе, дорівнює: a) k^6; b) k^3; c) k^4; d) k^2; e) k^3. Тому згідно леми Коші–Фробеніуса–Бернсайда кількість геометрично різних розфарбувань дорівнює

$$\frac{1}{|O|}(1 \cdot k^6 + 6 \cdot k^3 + 3 \cdot k^4 + 8 \cdot k^2 + 6 \cdot k^3) = \frac{k^6 + 3 \cdot k^4 + 12 \cdot k^3 + 8 \cdot k^2}{24} .$$

Зауважимо, що звідси випливає не зовсім очевидний факт, що для довільного натурального k число $k^6 + 3 \cdot k^4 + 12 \cdot k^3 + 8 \cdot k^2$ ділиться на 24.

2. Знайдемо кількість попарно неізоморфних 5–вершинних простих графів (тобто графів без кратних ребер). Позначимо символом M множину усіх 5–вершинних простих графів і підрахуємо, для початку, потужність цієї множини. Оскільки дві вершини графа можуть або з'єднуватися ребром, або ні, то для визначення графа нам потрібно знати, чи з'єднані ребром наступні вершини: перша та друга, перша та третя, перша та четверта, перша та п'ята, друга та третя, друга та четверта, друга та п'ята, третя та четверта, третя та п'ята і четверта та п'ята (10 пар). Тому всього 5–вершинних простих графів буде 2^{10}. На множині M природним чином діє симетрична група S_5: нехай $\Gamma = (V, E)$ — довільний 5–вершинний простий граф, де $V = \{1, 2, 3, 4, 5\}$ — множина його вершин, а E — множина його ребер, $\pi \in S_5$, тоді $\Gamma^\pi = (V, E^\pi) \in M$, де вершини $\pi(i)$ та $\pi(j)$ з'єднані ребром, тобто $(\pi(i), \pi(j)) \in E^\pi$, якщо ребром з'єднані вершини i та j, тобто $(i, j) \in E$. Два графи Γ_1 і Γ_2 будуть ізоморфними, якщо знайдеться така підстановка $\pi \in S_5$, що $\Gamma_1^\pi = \Gamma_2$. Таким чином, кількість попарно неізоморфних 5–вершинних простих

графів дорівнює кількості орбіт групи (S_5, M).

Знайдемо тепер кількість нерухомих точок елементів із S_5. Порядок групи S_5 дорівнює $5! = 120$. Ця група містить один елемент циклового типу $(a)(b)(c)(d)(f)$ (це тотожна підстановка ε). Кожен граф $\Gamma \in M$ при дії на нього ε залишається на місці, тому $\chi(\varepsilon) = |M| = 2^{10}$.

Група S_5 містить 10 елементів циклового типу (ab). Нехай $\{a, b, c, d, f\}$ — множина вершин графа, який є нерухомою точкою для такого типу підстановки. Тоді якщо в такому графі вершини a та i (i — одна із вершин $\{c, d, f\}$) з'єднані ребром, то ребром з'єднані і вершини b та i. А тому для визначення цього графа нам потрібно знати з'єднані ребром, чи ні тільки наступні вершини: a та b, a та c, a та d, a та f, c та d, c та f, d та f. Отже, $\chi((ab)) = 2^7$.

Аналогічно, група S_5 містить 15 елементів циклового типу $(ab)(cd)$. І для визначення графа, який є нерухомою точкою для такого типу підстановки, нам потрібно знати з'єднані ребром, чи ні тільки наступні вершини: a та b, a та c, a та d, a та f, c та d, c та f. Отже, $\chi((ab)(cd)) = 2^6$.

Група S_5 містить 20 елементів циклового типу (abc). Для визначення нерухомої точки для такого типу підстановки, нам потрібно знати з'єднані ребром, чи ні тільки вершини: a та b, a та c, a та d, a та f. Отже, $\chi((ab)(cd)) = 2^4$.

Стільки ж, а саме 20, містить S_5 елементів циклового типу $(abc)(df)$. Для визначення графа, який є нерухомої точкою у цьому випадку, нам потрібно знати з'єднані ребром, чи ні тільки вершини: a та b, a та c, a та d. Отже, $\chi((abc)(df)) = 2^3$.

І, нарешті, S_5 містить 24 елементи циклового типу $(abcdf)$. Для визначення нерухомої точки нам досить знати з'єднані ребром, чи ні вершини: a та b (тобто в такому графі або одночасно всі вершини попарно з'єднані ребрами, або ж жодні дві вершини не з'єднані ребром). Тому, $\chi((abcdf)) = 2^2$.

І згідно леми Коші–Фробеніуса–Бернсайда кількість попарно неізоморфних 5–вершинних простих графів дорівнює

$$\frac{2^{10} + 10 \cdot 2^7 + 15 \cdot 2^6 + 20 \cdot 2^4 + 20 \cdot 2^3 + 30 \cdot 2^3 + 24 \cdot 2^2}{120} = 34 \ .$$

Прикладом ще однієї дії є дія симетричної групи S_n на множині $P[x_1, \ldots, x_n]$ многочленів від змінних $x_1, \ldots, x_n$ з коефіцієнтами з поля P.

Нехай

$$f(x_1, \ldots, x_n) = \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} x_1^{i_1} \ldots\ x_n^{i_n} \tag{11}$$

— деякий многочлен від змінних x_1, …, x_n.

Степенем одночлена $a_{i_1,\ldots,i_n} x_1^{i_1} \ldots\ x_n^{i_n}$ називається число $i_1 + \cdots + i_n$. Найбільший із степенів одночленів $a_{i_1,\ldots,i_n} x_1^{i_1} \ldots\ x_n^{i_n}$ у зображенні (11) називається *степенем многочлена* f.

Вправа 18.3. *Покажіть, що кількість різних одночленів n змінних степеня m дорівнює* $\binom{m+n-1}{m}$.

Вказівка. Скористайтеся тим, що $\binom{m+(n-1)-1}{m} + \binom{(m-1)+n-1}{m-1} = \binom{m+n-1}{m}$.

Для однозначного впорядкування членів многочлена багатьох змінних використовується так званий *лексикографічний порядок* (аналогічний впорядкуванню слів у словнику): спочатку порівнюють показники при x_1, якщо вони рівні, то при x_2 і т.д. Наприклад, у многочлені f його члени розміщенні у лексикографічному порядку від вищого до нижчого: $f(x_1, x_2, x_3) = x_1^5 x_3 + 2x_1^4 x_3^2 + x_2^5$.

Старшим членом многочлена називатимемо найвищий член у лексикографічному порядку.

Розглянемо дію симетричної групи S_n на $P[x_1, \ldots, x_n]$: елемент π симетричної групи S_n діє на многочлен $f(x_1, \ldots, x_n)$ за правилом:

$$f^\pi(x_1, \ldots, x_n) = f(x_{\pi(1)}, \ldots, x_{\pi(n)}).$$

Така дія є точною. Якщо орбіта многочлена f при такій дії одноелементна, то кажуть, що f є *симетричним многочленом*. Іншими словами

Означення 18.2. *Многочлен $f \in P[x_1, \ldots, x_n]$ називається симетричним, якщо $f^\pi(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$ для всіх $\pi \in S_n$.*

Позначимо символом $SP[x_1, \ldots, x_n]$ множину симетричних многочленів.

Вправа 18.4. *Доведіть, що множина всіх симетричних многочленів $SP[x_1, \ldots, x_n]$ утворює кільце, яке є підкільцем кільця $P[x_1, \ldots, x_n]$.*

Вказівка. Скористайтеся тим, що відображення $\varphi_\pi : f \mapsto f^\pi$ є автоморфізмом кільця $P[x_1, \ldots, x_n]$.

Прикладом симетричних многочленів є, так звані, *елементарні симетричні многочлени* σ_k :

$$\sigma_1(x_1,\dots,x_n) = x_1 + \dots + x_n, \quad \dots,$$

$$\sigma_k(x_1,\dots,x_n) = \sum_{1\le i_1<\dots<i_k\le n} x_{i_1}\dots x_{i_k}, \quad \dots,$$

$$\sigma_n(x_1,\dots,x_n) = x_1\dots x_n.$$

Елементи кільця $SP[x_1,\dots,x_n]$ симетричних многочленів влаштовані досить прозоро, про що говорить наступна

Теорема 18.2 (основна теорема про симетричні многочлени). *Для кожного симетричного многочлена $f \in SP[x_1,\dots,x_n]$ змінних x_1, $\dots$, x_n над полем P існує, причому тільки один, такий многочлен $F \in P[x_1,\dots,x_n]$, що*

$$f(x_1,\dots,x_n) = F(\sigma_1(x_1,\dots,x_n),\dots,\sigma_n(x_1,\dots,x_n)). \qquad (12)$$

Для доведення основної теореми про симетричні многочлени нам знадобляться наступні дві леми.

Лема 18.2. *Нехай $u = ax_1^{k_1}\dots x_n^{k_n}$ — старший член симетричного многочлена $f(x_1,\dots,x_n)$. Тоді $k_1 \ge \dots \ge k_n$.*

Доведення. Припустимо, від супротивного, що $k_i < k_{i+1}$. Тоді f крім члена u має містити також $\breve{u}$, який одержаний із u перестановкою змінних x_i та x_{i+1}. А, отже, u не є старшим членом. Одержали протиріччя. □

Лема 18.3. *Для довільного одночлена $u = ax_1^{k_1}\dots x_n^{k_n}$ такого, що $k_1 \ge \dots \ge k_n$, існують єдиним чином визначені невід'ємні цілі числа l_1, $\dots$, l_n, такі що старший член могочлена $\sigma_1^{l_1}\dots\sigma_n^{l_n}$ збігається з u.*

Доведення. Старший член многочлена σ_k дорівнює $x_1\dots x_k$. Тоді старшим членом многочлена $\sigma_1^{l_1}\dots\sigma_n^{l_n}$ буде

$$x_1^{l_1}(x_1x_2)^{l_2}\dots(x_1\dots x_n)^{l_n} = x_1^{l_1+\dots+l_n}x_2^{l_2+\dots+l_n}\dots x_n^{l_n}.$$

Порівнюючи цей старший член із одночленом u одержимо систему

$$\begin{cases} l_1+\dots+l_n = k_1\ , \\ l_2+\dots+l_n = k_2\ , \\ \qquad\dots\ , \\ l_n = k_n\ , \end{cases}$$

яка, очевидно, має єдиний розв'язок $l_i = k_i - k_{i+1}$, $i = 1, \ldots, n-1$, $l_n = k_n$. Легко бачити, що всі l_i — невід'ємні. □

Доведемо тепер основну теорему про симетричні многочлени

Доведення. Нехай $f \in SP[x_1, \ldots, x_n]$ — довільний симетричний многочлен. Нам потрібно знайти такий многочлен $F \in P[x_1, \ldots, x_n]$, що має місце (12).

Якщо $f = 0$, то $F = 0$. Нехай $f \neq 0$ і $u_1 = ax_1^{k_1} \ldots x_n^{k_n}$ — старший член многочлена f. Тоді згідно леми 18.2 $k_1 \geq \ldots \geq k_n$, а згідно леми 18.3 існує такий одночлен $F_1 \in P[x_1, \ldots, x_n]$, що старший член многочлена $F_1(\sigma_1, \ldots, \sigma_n)$ дорівнює u_1. Розглянемо симетричний многочлен $f_1 = f - F_1(\sigma_1, \ldots, \sigma_n)$. Якщо $f_1 = 0$, то $F = F_1$. Нехай $f_1 \neq 0$ і u_2 — його старший член. Тоді у лексикографічному порядку u_1 вищий за u_2. А тому існуватиме $F_2 \in P[x_1, \ldots, x_n]$, такий що старший член $F_2(\sigma_1, \ldots, \sigma_n)$ дорівнює u_2. Далі розглянемо симетричний многочлен $f_2 = f_1 - F_2(\sigma_1, \ldots, \sigma_n)$. При $f_2 = 0$ матимемо $F = F_1 + F_2$. Якщо це не так, то продовжуємо і т.д. Згідно леми 18.2 для показників одночленів u_1, u_2, ... є лише скінченне число можливостей, так що описаний процес обірветься. Отже, $f_m = 0$ для деякого m. Тоді $F = F_1 + \ldots + F_m$.

Доведемо тепер єдиність зображення (12). Припустимо, що для многочлена f існує два різні зображення у вигляді многочлена від σ_1, ..., σ_n, а саме $f(x_1, \ldots, x_n) = F(\sigma_1, \ldots, \sigma_n) = G(\sigma_1, \ldots, \sigma_n)$, де $H := F - G \neq 0$, а $H(\sigma_1, \ldots, \sigma_n) = 0$. Позначимо символами H_1, ..., H_s всі ненульові члени H, а символом w_i $(i = 1, \ldots, s)$ — старший член $H_i(\sigma_1, \ldots, \sigma_n) \in K[x_1, \ldots, x_n]$. Згідно леми 18.3 серед $w_1, \ldots, w_s$ немає пропорційних. Тому виберемо серед них старший. Не обмежуючи загальності, можна вважати, що ним буде w_1. Тоді w_1 у лексикографічному порядку буде старшим за інші члени самого многочлена $H_1(\sigma_1, \ldots, \sigma_n)$ і всіх членів многочленів $H_i(\sigma_1, \ldots, \sigma_n)$ $(i = 2, \ldots, s)$. А тому після зведення подібних членів у сумі $H_1(\sigma_1, \ldots, \sigma_n) + \ldots + H_s(\sigma_1, \ldots, \sigma_n)$ член w_1 збережеться, так що ця сума не дорівнюватиме нулю. Тому $H(\sigma_1, \ldots, \sigma_n) \neq 0$. Одержали протиріччя. Отже, зображення многочлена f у вигляді (12) єдине. □

Задача 18.5. *Виразіть симетричний многочлен* $f = (x_1 + x_2)(x_1 + x_3)(x_1 + x_4)(x_2 + x_3)(x_2 + x_4)(x_3 + x_4)$ *через елементарні симетричні многочлени.*

19 Теореми Силова

Теорема Лагранжа накладає на порядки підгруп скінченної групи необхідні умови. Але, як показує вже приклад групи A_4, що не містить підгрупи порядку 6 (див. зад. 9.3 b)), ці умові не є достатніми.

Задача 19.1. *Доведіть, що група A_5 не містить підгруп порядків* 15, 20 *і* 30.

Вказівка. Скористайтеся 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.

Надалі вважатимемо, що p є фіксованим простим числом.

Теорема 19.1 (1-ша теорема Силова). *Нехай G — скінченна група.*
a) *Якщо $p^k \Big| |G|$, то G містить підгрупу порядку p^k.*
b) *Якщо до того ж $p^{k+1} \Big| |G|$, то кожна підгрупа порядку p^k нормальна принаймні в одній підгрупі порядку p^{k+1}.*

Доведення. Досить довести тільки пункт b). Застосуємо індукцію по k. Базою індукції — для $k = 0$ — є лема Коші.

Нехай тепер P — підгрупа із G порядку p^k і $p^{k+1} \Big| |G|$. Розглянемо дію P правими зсувами на правих класах суміжності групи G за підгрупою P: $(Px)^g = Pxg$. Оскільки індекс $|G : P|$ ділиться на p, тому і кількість класів суміжності кратна p. Крім того, потужності орбіт є степенями p. І позаяк серед орбіт принаймні одна — а саме $\{Pe\}$ — є 1–елементною, то кількість 1–елементних орбіт також кратна p.

Покажемо, що об'єднання H тих класів суміжності, які утворюють 1–елементні орбіти цієї дії, є підгрупою групи G, причому P є нормальною підгрупою в H. Справді, нехай $\{Px\}$ і $\{Py\}$ 1–елементні орбіти і $h_1x \in Px$, $h_2y \in Py$. Оскільки $(Px)^{h_2} = Px$, то $h_1xh_2 = h_3x$ для деякого $h_3 \in P$. Тоді $h_1x \cdot h_2y = h_3xy$. Крім того, для довільного $h \in P$ $(Py)^h = Py$, тому $yh = h_4y$ для деякого $h_4 \in P$. Отже, $(Pxy)^h = Pxy \cdot h = Px \cdot h_4y = Pxy$, тобто орбіта $\{Pxy\}$ також 1–елементна. Таким чином,

H є підгрупою. Нехай тепер $h \in P$ і $g = h_1 x \in Px$ — довільні. Тоді $g^{-1}hg = x^{-1}h_1^{-1}hh_1x = x^{-1}h^{'}x = h^{''}x^{-1}x = h^{''} \in P$. Тому P є нормальною підгрупою в H.

Порядок факторгрупи H/P ділиться на p, а значить, за лемою Коші, H/P містить підгрупу Q порядку p. Тоді, згідно теореми 12.2 про відповідність підгруп, її прообраз $P_1 = \pi^{-1}(Q)$ при канонічному епіморфізмі $\pi : H \to H/P$ є підгрупою порядку p^{k+1}, причому $P \lhd P_1$. □

Наслідок 19.1. *У p–групі G порядку p^n кожна власна підгрупа міститься в деякій підгрупі порядку p^{n-1}, причому всі підгрупи порядку p^{n-1} є нормальними підгрупами в G.*

Очевидно, що перетин довільної родини p–підгруп групи G також буде p–підгрупою. Тому сукупність усіх p–підгруп групи G утворює нижню напіврешітку відносно включення. Максимальними елементами цієї напіврешітки є так звані *силовські p–підгрупи.*

Означення 19.1. *Ті p–підгрупи групи G, які не містяться в жодній більшій p–підгрупі цієї групи, називаються силовськими p–підгрупами групи G.*

Зразу ж хотілося б зауважити, що у нескінченній групі силовські p–підгруп можуть і не існувати.

Наслідок 19.2. *Якщо порядок $|G|$ скінченної групи G ділиться на p^k, але не ділиться на p^{k+1}, то всі силовські p–підгрупи групи G мають порядок p^k.*

Теорема 19.2 (2-га теорема Силова). *Усі силовські p–підгрупи скінченної групи G є спряженими.*

Доведення. Нехай P — силовська p–підгрупа групи G, порядок $|P|$ якої дорівнює p^k (тобто $p^k \big| |G|$, а $p^{k+1} \nmid |G|$). Позначимо символом A множину $\{P, P_1, \ldots, P_{m-1}\}$ всіх підгруп, спряжених з підгрупою P елементами із G. Якщо розглянути дію групи G на множині підгруп порядку p^k, то відносно цієї дії A утворюватиме орбіту групи G, причому згідно теореми 18.1 $m = |A| = |G : St_G(P)|$. З іншого боку, за наслідком 19.2 індекс $|G : P|$ підгрупи P не ділиться на p, а тому на p не ділиться і індекс $|G : St_G(P)|$ її стабілізатора $St_G(P)$, бо $P \leq St_G(P)$. Отже, $p \nmid m$.

Нехай тепер Q — довільна силовська p–підгрупа групи G. Розглянемо дію Q спряженням на множині A. Оскільки довжина кожної орбіти

групи Q є степенем p, а число m не ділиться на p, то існує принаймні одна 1–елементна орбіта $\{P_i\}$, тобто для довільного $a \in Q$ виконується $P_i^a = a^{-1}P_i a = P_i$. Тоді для довільних елементів a_1b_1 і a_2b_2 з QP_i їх добуток $a_1b_1 \cdot a_2b_2 = a_1a_2 \cdot a_2^{-1}b_1a_2b_2 = a_1a_2b_3b_2$ також належить QP_i. Тому QP_i є підгрупою групи G. Згідно задачі 5.2 її порядок $|QP_i| = \frac{|Q|\cdot|P_i|}{|Q\cap P_i|}$, тому є степенем числа p, причому $|QP_i| \geq \max(|Q|, |P_i|)$. Але Q і P_i — силовські, тобто максимальні p–підгрупи групи G. Отже, $QP_i = Q = P_i$. □

Наслідок 19.3. a) *Силовська p–підгрупа P скінченної групи G буде нормальною в G тоді й лише тоді, коли вона єдина.*
b) *Якщо p–підгрупа H скінченної групи G є нормальною в G, то H міститься в кожній силовській p–підгрупі групи G.*

Задача 19.2. *Доведіть, що нормальна силовська p–підгрупа P скінченної групи G є інваріантною (або ще кажуть характеристичною) відносно дії довільного автоморфізму $\varphi \in \operatorname{Aut} G$ групи G, тобто для кожного $\varphi \in \operatorname{Aut} G$ матимемо $\varphi(P) = P$.*

Задача 19.3. *Доведіть, що силовські p–підгрупи нескінченної групи не завжди спряжені в самій групі, тобто припущення про скінченність групи в 2-й теоремі Силова є суттєвим.*

Теорема 19.3 (3-тя теорема Силова). *Нехай $|G| = p^k l$, де числа p і l — взаємно прості. Позначимо через t_p число силовських p–підгруп групи G. Тоді:* a) $t_p \mid l$; b) $t_p \equiv 1 \pmod p$.

Доведення. Нехай A — множина всіх підгруп групи G, які спряжені з силовською p–підгрупою $P \leq G$. Із 2-ї теореми Силова (теореми 19.2) випливає, що усі силовські p–підгрупи є спряженими. Тому число t_p збігається з числом $m = |A|$ і із рівностей $m = |G : St_G(P)|$ і $l = |G : P| = |G : St_G(P)| \cdot |St_G(P) : P|$ одразу випливає, що $t_p \mid l$. Нехай Q — довільна силовська p–підгрупа групи G. Тоді при дії Q спряженням на множині A є лише одна 1–елементна орбіта, а саме $\{Q\}$, бо якщо існує ще одна 1–елементна орбіта (нехай $\{Q'\}$) то, як це було показано при доведенні теореми 19.2, QQ' є p–групою, яка містить Q та Q', а тому збігається з ними. І оскільки довжини інших орбіт групи Q є степенями p, то $t_p = m \equiv 1 \pmod p$. □

Зауваження. Часто першу теорему Силова називають ще теоремою Силова про *існування та вкладення*, другу — теоремою Силова про *спряженість* і, нарешті, третю — теоремою Силова про *кількість*.

Приклади. 1. Порядок групи $|S_4|$ дорівнює $24 = 2^3 3$. Тому вона містить силовські 3–підгрупи порядку 3 і силовські 2–підгрупи порядку 8. Неважко переконатися в тому, що силовських 3–підгруп буде 4, а силовських 2–підгруп — 3.

2. Покажемо, що кожна група G порядку 196 не є простою. Справді, $196 = 2^2 7^2$. За теоремою 19.3 кількість t_7 силовських 7–підгруп групи G є дільником числа 2^2 і конгруентна 1 за модулем числа 7. Отже, $t_7 = 1$. За наслідком 19.3 а) єдина силовська 7–підгрупа групи G є нормальною.

3. Знайдемо порядок силовської p–підгрупи симетричної групи S_n. Для цього визначимо, який найвищий степінь числа p ділить порядок $n!$ групи S_n. Множниками числа $n!$, що діляться на p, є числа p, $2p$, $\ldots$, kp, де $k = [n/p]$ — найбільше ціле число, яке не перевищує n/p. Тому $n!$ ділиться на p^k і ще на ту максимальну степінь числа p, яка ділить $k!$. Але оскільки $[k/p] = [n/p^2]$, то, продовжуючи аналогічним чином міркування, одержимо, що найвищий степінь числа p, який ділить $n!$, дорівнює p^r, де

$$r = \Big[\frac{n}{p}\Big] + \Big[\frac{n}{p^2}\Big] + \Big[\frac{n}{p^3}\Big] + \ldots \ .$$

Зокрема, якщо $n = p^s$, то порядок силовської p–підгрупи дорівнює p^r, де $r = p^{s-1} + \ldots + p + 1$.

4. Покажемо, що силовською p–підгрупою групи $GL_n(\mathbb{Z}_p)$ усіх невироджених матриць порядку n над скінченним полем лишків $\mathbb{Z}_p$ є підгрупа $UT_n(\mathbb{Z}_p)$ верхніх трикутних матриць з одиницями по діагоналі. Для цього підрахуємо, для початку, порядки цих груп. Оскільки квадратна матриця A є невиродженою тоді й лише тоді, коли її вектор–рядки (вектор–стовпчики) лінійно незалежні, то в якості першого рядка $A \in GL_n(\mathbb{Z}_p)$ можуть бути довільні вектори із $\mathbb{Z}_p^n$, за винятком нульового. Тому всього різних таких рядків буде $p^n - 1$. Другим рядком матриці A можуть бути тільки ті вектори із $\mathbb{Z}_p^n$, які не пропорційні першому рядку. Різних коефіцієнтів пропорційності буде $|\mathbb{Z}_p| = p$. Отже, другий рядок можна вибрати $p^n - p$ способами. Тоді в якості третього рядка можна взяти рядок, який не є лінійною комбінацією перших двох. І різних таких рядків, очевидно, буде $p^n - p^2$. Продовжуючи і т.д., одержимо: $|GL_n(\mathbb{Z}_p)| = (p^n - 1) \cdot (p^n - p) \cdot \ldots \cdot (p^n - p^{n-1})$, і, легко бачити, що порядок силовської p–підгрупи цієї групи дорівнюватиме $p^{1+\ldots+(n-1)} = p^{n(n-1)/2}$.

У свою чергу, порядок підгрупи $UT_n(\mathbb{Z}_p)$ дорівнює також $p^{n(n-1)/2}$,

оскільки всі елементи матриці, які розміщуються над головною діагоналлю, пробігають незалежно один від одного все поле $\mathbb{Z}_p$. Тому підгрупа $UT_n(\mathbb{Z}_p)$ є силовською p–підгрупою групи $GL_n(\mathbb{Z}_p)$.

Задача 19.4. *Доведіть, що довільна група G порядку pq, де p та q — різні прості числа і $p < q$, є або*
1) *циклічною, або*
2) *неабелевою з нормальною силовською q–підгрупою, причому p і q такі, що p ділить $q - 1$.*

Задача 19.5. *Доведіть, що довільна група G порядку ≤ 30 не є простою.*

Теорема 19.4 (теорема Вільсона). *Число p буде простим тоді й лише тоді, коли $(p-1)! \equiv -1 \pmod{p}$.*

Доведення. Достатність. Нехай число p — складене. Якщо $p = mk$, де $1 < m < k < p$, або $p = q^2$, де $q > 2$, то $(p-1)! \equiv 0 \pmod{p}$. Якщо ж $p = 2^2 = 4$, то $(4-1)! = 6 \not\equiv -1 \pmod{4}$.

Необхідність. Нехай тепер число p — просте. Оскільки $p!$ ділиться на p, але не ділиться на p^2, то всі силовські p–підгрупи групи S_p є циклічними порядку p. А кожен елемент порядку p з S_p є циклом довжини p, тому S_p містить $(p-1)!$ елементів порядку p і $(p-1)!/(p-1) = (p-2)!$ підгруп порядку p. За теоремою 19.3 $(p-2)! \equiv 1 \pmod{p}$. Перемноживши цю конгруенцію почленно на $p - 1 \equiv -1 \pmod{p}$, одержуємо $(p-1)! \equiv -1 \pmod{p}$. □

20 Прямий добуток груп

Для теорії груп є дуже важливими різні конструкції, які дозволяють з одних груп будувати інші. Такі конструкції, з одного боку, дають можливість будувати нові приклади груп, у тому числі з наперед заданими властивостями, а з іншого, якщо вдається встановити, що дана група побудована певним чином із менших або простіших груп, то це значно полегшує дослідження її будови. Чи не найважливішою з таких конструкцій є прямий добуток груп.

Означення 20.1. *Зовнішнім прямим добутком груп $(A; *)$ і $(B; \circ)$ називається множина $A \times B = \{(a, b) \mid a \in A, b \in B\}$ із множенням, визначеним правилом:*

$$(a_1, b_1)(a_2, b_2) = (a_1 * a_2, b_1 \circ b_2).$$

Зазвичай зовнішній прямий добуток груп A і B також позначають символом $A \times B$.

Очевидно, що для визначеного таким чином множення

$$\big((a_1, b_1)(a_2, b_2)\big)(a_3, b_3) = \big((a_1 * a_2) * a_3, (b_1 \circ b_2) \circ b_3\big) =$$

$$= \big(a_1 * (a_2 * a_3), b_1 \circ (b_2 \circ b_3)\big) = (a_1, b_1)\big((a_2, b_2)(a_3, b_3)\big),$$

тобто множення асоціативне. Крім того, нейтральним елементом буде пара (e_A, e_B), а оберненою до пари (a, b) — пара (a^{-1}, b^{-1}). Отже, зовнішній прямий добуток груп A і B справді є групою, причому $|A \times B| = |A| \cdot |B|$.

Якщо групи A і B є адитивними, то замість прямого добутку часто говорять про *пряму суму* і використовують позначення $A \oplus B$. Якщо групи A та B є скінченними, то $|A \times B| = |A| \cdot |B|$.

Вправа 20.1. *Доведіть, що коли елементи $a \in A$ і $b \in B$ мають скінченні порядки, то $|(a, b)| = \text{НСК}(|a|, |b|)$.*

Відображення $\mu_A : A \to A \times B$, $a \mapsto (a, e_B)$, є мономорфізмом груп, бо воно ін'єктивне і $\mu_A(a_1 * a_2) = \mu_A(a_1)\mu_A(a_2)$. Аналогічно мономорфізмом є і відображення $\mu_B : B \to A \times B$, $b \mapsto (e_A, b)$. Подібно тому, як дійсні числа ототожнюються з комплексними числами вигляду $a + 0 \cdot i$, групи A і B можна ототожнити з їх образами $\widetilde{A} = \mu_A(A)$ і $\widetilde{B} = \mu_B(B)$ при цих мономорфізмах. При цьому елемент $(a, b) \in A \times B$ природно ототожнюється з добутком $\tilde{a}\tilde{b} = (a, e_B)(e_A, b)$.

Твердження 20.1. *Нехай $A \times B$ — зовнішній прямий добуток груп $(A; *)$ та $(B; \circ)$. Тоді:*
a) *$\widetilde{A}$ і $\widetilde{B}$ є нормальними підгрупами групи $A \times B$;*
b) *$\widetilde{A} \cap \widetilde{B} = \{(e_A, e_B)\}$;*
c) *$\widetilde{A} \cdot \widetilde{B} = A \times B$;*
d) *розклад довільного елемента $g \in A \times B$ в добуток $g = \tilde{a}\tilde{b}$, де $\tilde{a} \in \widetilde{A}$ і $\tilde{b} \in \widetilde{B}$, — однозначний;*
e) *кожний елемент $\tilde{a} \in \widetilde{A}$ комутує з кожним елементом $\tilde{b} \in \widetilde{B}$.*

Доведення. a) Нормальність підгрупи $\widetilde{A}$ випливає з того, що для довільних елементів $(a_1, e_B) \in \widetilde{A}$ і $(a, b) \in A \times B$ маємо:

$$(a, b)^{-1}(a_1, e_B)(a, b) = (a^{-1} * a_1 * a, b^{-1} \circ e_B \circ b) = (a^{-1} * a_1 * a, e_B) \in \widetilde{A}\,.$$

Нормальність $\widetilde{B}$ доводиться аналогічно.
b) Очевидно.
c) $\widetilde{A}\cdot\widetilde{B}=\{(a,e_B)(e_A,b)\,|\,a\in A,b\in B\}=\{(a,b)\,|\,a\in A,b\in B\}=A\times B$.
d) Якщо $\tilde{a}\tilde{b}=\tilde{a}_1\tilde{b}_1$, то $\tilde{a}_1^{-1}\tilde{a}=\tilde{b}_1\tilde{b}^{-1}$. Із пункту b) тепер випливає, що $\tilde{a}_1^{-1}\tilde{a}=\tilde{b}_1\tilde{b}^{-1}=(e_A,e_B)$, звідки $\tilde{a}=\tilde{a}_1$ і $\tilde{b}=\tilde{b}_1$.
e) Також очевидно. □

Кажуть, що група G є *внутрішнім прямим добутком* своїх підгруп A і B, якщо виконуються такі дві умови: 1) кожний елемент $a\in A$ комутує з кожним елементом $b\in B$, і 2) кожний елемент g групи G однозначно записується у вигляді $g=ab$, де $a\in A$ і $b\in B$.

Задача 20.1.

Із твердження 20.1 випливає, що зовнішній прямий добуток $A\times B$ груп A і B одночасно є внутрішнім прямим добутком своїх підгруп $\widetilde{A}$ і $\widetilde{B}$. Якщо множники A і B ототожнювати з підгрупами $\widetilde{A}$ і $\widetilde{B}$, то зовнішній і внутрішній прямі добутки не розрізняються і говорять просто про *прямий добуток* підгруп A і B. Далі з контексту завжди буде зрозуміло, який саме прямий добуток мається на увазі.

Розклад $G=A\times B$ групи G у прямий добуток називатимемо *нетривіальним*, якщо обидва множники A і B є неодиничними групами. Очевидно, що розклад $G=A\times B$ є нетривіальним тоді й лише тоді, коли обидва множники A і B є власними підгрупами групи G.

Теорема 20.1 (критерій розкладності групи в прямий добуток двох своїх підгруп). *Група G розкладається в прямий добуток своїх підгруп A і B тоді й лише тоді, коли ці підгрупи задовольняють такі три умови*:

$$\text{a) } A,B\lhd G\,;\qquad \text{b) } A\cap B=E\,;\qquad \text{c) } \langle A,B\rangle=G\,.$$

Доведення. Необхідність випливає з пунктів a) — c) твердження 20.1.

Достатність. Із нормальності підгруп A і B випливає, що комутатор $[a,b]=a^{-1}b^{-1}ab=a^{-1}(b^{-1}ab)=(a^{-1}b^{-1}a)b$ елементів $a\in A$ і $b\in B$ належить обом цим підгрупам, бо $b^{-1}ab\in A$, $a^{-1}b^{-1}a\in B$. Тому $[a,b]=e$ і $ab=ba$.

З умови c) випливає, що кожний елемент $g\in G$ можна записати у вигляді $g=a_1b_1\cdots a_kb_k$, де $a_1,\dots,a_k\in A$, $b_1,\dots,b_k\in B$. Але елементи з A та B комутують, тому $g=ab$, де $a=a_1\cdots a_k\in A$, $b=b_1\cdots b_k\in B$.

Нарешті, якщо $ab = a_1b_1$, то $a_1^{-1}a = b_1b^{-1}$, і з умови b) випливає, що $a_1^{-1}a = b_1b^{-1} = e$. Тому $a = a_1$, $b = b_1$, і зображення g у вигляді $g = ab$ — однозначне. Таким чином, обидві умови з означення розкладності групи G в прямий добуток підгруп A і B виконуються. □

Приклади груп, які розкладаються в прямий добуток.

1. Із правила додавання комплексних чисел, записаних в алгебричній формі, випливає, що $\mathbb{C} \simeq \mathbb{R} \oplus \mathbb{R}$.

2. Із правила множення комплексних чисел, записаних у тригонометричній формі, випливає, що $\mathbb{C}^* \simeq T \times \mathbb{R}^+$.

3. Очевидно, що $\mathbb{R}^* = \{1, -1\} \times \mathbb{R}^+$.

Приклади груп, які не розкладаються в прямий добуток.

1. Кожна власна підгрупа групи S_3 має порядок ≤ 3, а тому є абелевою. Очевидно, що прямий добуток абелевих груп знову є абелевою групою. А оскільки група S_3 — не абелева, то вона в нетривіальний прямий добуток не розкладається.

Аналогічно доводиться нерозкладність у прямий добуток груп D_4 і Q_8.

2. Для довільних двох ненульових підгруп $m\mathbb{Z}$ і $n\mathbb{Z}$ групи $\mathbb{Z}$ не виконується умова b) критерію розкладності в прямий добуток. Справді, перетин $m\mathbb{Z} \cap n\mathbb{Z}$ містить підгрупу $mn\mathbb{Z}$, отже, є ненульовим. Тому $\mathbb{Z}$ у прямий добуток власних підгруп не розкладається.

Вправа 20.2. *Доведіть, що*: a) $A \times B \simeq B \times A$; b) $(A \times B) \times C \simeq A \times (B \times C)$; c) $Z(A \times B) = Z(A) \times Z(B)$.

Твердження 20.2. *Якщо* $A \lhd G$ *і* $B \lhd H$, *то* $(A \times B) \lhd (G \times H)$ *і*

$$(G \times H)/(A \times B) \simeq \big(G/A\big) \times \big(H/B\big)\ .$$

Доведення. Нормальність підгрупи $A \times B$ перевіряється легко за означенням. Друга частина твердження випливає з того, що відображення

$$(g, h)(A \times B) \mapsto (gA, hB), \text{ де } g \in G,\ h \in H,$$

є ізоморфізмом факторгрупи $(G \times H)/(A \times B)$ на прямий добуток факторгруп G/A і H/B. □

Операція зовнішнього прямого добутку легко узагальнюється на довільну скінченну кількість груп: *прямим добутком* груп $G_1, \dots, G_n$ називається множина $G_1 \times \dots \times G_n = \{(g_1, \dots, g_n) \mid g_1 \in G_1, \dots, g_n \in G_n\}$ із покомпонентним множенням: $(g_1', \dots, g_n')(g_1'', \dots, g_n'') = (g_1'g_1'', \dots, g_n'g_n'')$. У випадку довільної родини $G_i, i \in I$, множників є два варіанти конструкції.

Означення 20.2. *Декартовим добутком родини груп $G_i, i \in I$, називається множина $\prod\limits_{i\in I}^{D} G_i = \{(g_i)_{i\in I} \mid g_i \in G_i$ для всіх $i \in I\}$ із покомпонентним множенням наборів*: $(g_i)_{i\in I} \cdot (h_i)_{i\in I} = (g_ih_i)_{i\in I}$.

Означення 20.3. *Прямим добутком родини груп $G_i, i \in I$, (позначається $\prod\limits_{i\in I} G_i$) називається підмножина всіх тих наборів із $\prod\limits_{i\in I}^{D} G_i$, в яких всі, за винятком щонайбільше скінченної кількості, компонент є одиничними.*

Очевидно, що у випадку скінченної множини індексів I декартовий і прямий добутки груп збігаються. Для нескінченних множин індексів це вже не так.

Задача 20.2. *Доведіть, що коли всі групи $G_n, n \in \mathbb{N}$, є скінченними, то прямий добуток $\prod\limits_{n\in\mathbb{N}} G_n$ є зліченним, а декартовий добуток $\prod\limits_{n\in\mathbb{N}}^{D} G_n$ має потужність континуум.*

Задача 20.3. *Доведіть, що $\prod\limits_{i\in I} G_i \lhd \prod\limits_{i\in I}^{D} G_i$ для довільної родини груп $G_i, i \in I$.*

Внутрішній прямий добуток також природно узагальнюється на довільну кількість підгруп: група G є *внутрішнім прямим добутком* родини $A_i, i \in I$, своїх підгруп, якщо 1) для довільних $i \neq j$ кожний елемент $a_i \in A_i$ комутує з кожним елементом $a_j \in A_j$, і 2) кожний елемент g групи G можна подати у вигляді добутку $g = a_{i_1} \cdots a_{i_k}$, де елементи $a_{i_1} \in A_1, \dots, a_{i_k} \in A_k$ — не одиничні і індекси $i_1, \dots, i_k$ — попарно різні, причому з точністю до порядку множників існує тільки одне таке зображення елемента g.

Зрозуміло, що при природному зануренні $\mu_k : A_k \to \prod\limits_{i\in I} A_i$, коли елемент $a \in A_k$ переходить у набір, в якому k–та компонента дорівнює a,

а всі інші компоненти — одиничні, зовнішній прямий добуток $\prod\limits_{i\in I} A_i$ груп $A_i, i \in I$, переходить у внутрішній прямий добуток своїх підгруп $\widetilde{A}_i = \mu_i(A_i)$. Тому, як і у випадку двох множників, зовнішній і внутрішній прямі добутки родини груп зазвичай не розрізняють.

У випадку більше ніж двох підгруп критерій розкладності в прямий добуток (теорема 20.1) набуває такого вигляду:

Теорема 20.1′ (критерій розкладності групи в прямий добуток родини своїх підгруп). *Група G розкладається в прямий добуток родини $A_i, i \in I$, своїх підгруп тоді й лише тоді, коли ці підгрупи задовольняють такі три умови:*
a) $A_i \lhd G$ *для довільного* $i \in I$;
b) $A_i \bigcap \big\langle \bigcup\limits_{j\neq i} A_j \big\rangle = E$ *для довільного* $i \in I$;
c) $\big\langle \bigcup\limits_{i} A_i \big\rangle = G$.

Вправа 20.3. *Доведіть теорему* 20.1′ *(її доведення не дуже відрізняється від доведення теореми* 20.1*).*

Розберемося докладніше з розкладністю в прямий добуток циклічних груп.

Твердження 20.3. *Циклічна група C_{p^k} порядку p^k не розкладається в прямий добуток власних підгруп.*

Доведення. Із теореми про будову підгруп циклічної групи (теорема 7.3) випливає, що підгрупи групи $C_{p^k} = \langle a\rangle$ утворюють ланцюг

$$E < \langle a^{p^{k-1}}\rangle < \cdots < \langle a^p\rangle < \langle a\rangle = C_{p^k}\ .$$

Тому для довільних двох підгруп $A, B \leq C_{p^k}$ або $A \leq B$, або $B \leq A$, зокрема, перетин $A\cap B$ збігається з меншою з цих підгруп. Таким чином, умова b) критерію розкладності в прямий добуток порушується і група C_{p^k} в нетривіальний прямий добуток не розкладається. □

Твердження 20.4. *Якщо $n = mk$, де числа m і k — взаємно прості, то циклічна група C_n розкладається в нетривіальний прямий добуток: $C_{mk} \simeq C_m \times C_k$.*

Доведення. Нехай $C_n = \langle a \rangle$. Доведемо, що для підгруп $A = \langle a^m \rangle$ і $B = \langle a^k \rangle$ порядків k і m відповідно виконуються умови критерію розкладності в прямий добуток. Справді, з комутативності C_n випливає, що $A, B \lhd C_n$. Оскільки m і k — взаємно прості, то існують такі цілі числа p і q, що $pm + qk = 1$. Але тоді для довільного r $a^r = a^{pmr+qkr} = (a^m)^{pr} \cdot (a^k)^{qr}$, причому $(a^m)^{pr} \in A$, $(a^k)^{qr} \in B$. Отже, $C_n = \langle A, B \rangle$.

Довільний елемент $c \in A \cap B$ можна записати у вигляді $c = a^{mu} = a^{kv}$, де $0 \leq u < k$ і $0 \leq v < m$. Із твердження 6.1 випливає, що $mu - kv \equiv 0 \pmod{mk}$, тому $m|kv$, $k|mu$. Позаяк m і k — взаємно прості, то $m|v$ і $k|u$. Із обмежень на u і v випливає, що $u = v = 0$. Але тоді $c = e$. Отже, $A \cap B = E$. □

Наслідок 20.1. *Якщо $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ — канонічний розклад числа n, то*

$$C_n \simeq C_{p_1^{k_1}} \times C_{p_2^{k_2}} \times \cdots \times C_{p_m^{k_m}} .$$

Твердження 20.5. *Скінченна група G порядку $n = p_1^{k_1} \cdots p_m^{k_m}$ розкладається в прямий добуток $G = P_1 \times \cdots \times P_m$ своїх силовських p–підгруп $P_1, \ldots, P_m$ тоді й лише тоді, коли всі вони нормальні в G, тобто тоді й лише тоді, коли для кожного простого дільника p порядку $|G|$ група G містить лише одну силовську p–підгрупу.*

Доведення. Оскільки кожен множник P_i прямого добутку $G = P_1 \times \cdots \times P_m$ є нормальною підгрупою в G, то необхідність умови очевидна.

Для доведення достатності покажемо, що за даного припущення всі три умови критерію розкладності в прямий добуток (теорема 20.1′) виконані.

Для умови а) це очевидно.

Згідно твердження 9.7 добуток $AB = \{ab \,|\, a \in A, b \in B\}$ нормальних підгруп A і B є нормальною підгрупою. Очевидно, що $|AB| \leq |A| \cdot |B|$. З іншого боку, з включення $A, B \leq AB$ і теореми Лагранжа випливає, що порядок $|AB|$ ділиться на кожне з чисел $|A|$ і $|B|$. Тому коли числа $|A|$ і $|B|$ взаємно прості, то $|AB| = |A| \cdot |B|$.

Із наведених міркувань випливає, що для довільного i групи P_i та

$$\Big\langle \bigcup_{j \neq i} P_j \Big\rangle = P_1 \cdots P_{i-1} P_{i+1} \cdots P_m$$

мають взаємно прості порядки $p_i^{k_i}$ та $p_1^{k_1} \cdots p_{i-1}^{k_{i-1}} p_{i+1}^{k_{i+1}} \cdots p_m^{k_m}$, а тому

$P_i \bigcap \langle \bigcup\limits_{j\neq i} P_j \rangle = E$. Крім того,

$$|\langle \bigcup_i P_i \rangle| = |P_1 \cdots P_m| = p_1^{k_1} \cdots p_m^{k_m} = |G|.$$

Звідси випливає, що $\langle \bigcup\limits_i P_i \rangle = G$. Отже, умови b) і c) також виконуються. □

Задача 20.4. *Нехай $N_i, i \in I$, — родина нормальних підгруп групи G і $H = \prod\limits_{i\in I}(G/N_i)$ — прямий добуток факторгруп G/N_i. Доведіть, що:*
a) *відображення $\varphi : G \to H, g \mapsto (gN_i)_{i\in I}$, є гомоморфізмом груп;*
b) *для кожного $k \in I$ канонічна проекція $(gN_i)_{i\in I} \mapsto gN_k$ підгрупи $\varphi(G)$ на k–й множник G/N_k збігається з G/N_k;*
c) $\operatorname{Ker}\varphi = \bigcap\limits_{i\in I} N_i$.

Задача 20.5. *Доведіть, що в скінченній групі жодна власна підгрупа не збігається зі своїм нормалізатором тоді й лише тоді, коли група є прямим добутком своїх силовських підгруп.*

21 Періодичні групи

Нагадаємо ще раз, що

Означення 21.1. *Група називається періодичною, якщо кожний елемент групи має скінченний порядок.*

А також

Означення 21.2. *Група називається групою без скруту, якщо кожний неодиничний елемент групи має нескінченний порядок.*

Твердження 21.1. *Довільні підгрупа і факторгрупа періодичної групи також є періодичними групами.*

Вправа 21.1. *Доведіть твердження* 21.1.

Приклади періодичних груп:
a) довільна скінченна група;
b) група $\mathbb{C}_{p^\infty}$;

c) група всіх комплексних коренів з одиниці всіх можливих натуральних степенів;

d) адитивна група векторного простору над полем $\mathbb{Z}_p$, бо кожен ненульовий елемент має порядок p.

Приклади груп без скруту:

a) числові групи за додаванням $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$;

b) група $(\mathbb{Q}^+;\cdot)$;

c) адитивна група довільного дійсного або комплексного векторного простору.

Приклади груп, які містять як елементи скінченних порядків, так і нескінченних:

a) числові групи за множенням $\mathbb{R}^*$, $\mathbb{C}^*$, T;

b) група рухів площини містить як осьові і центральні симетрії (елементи порядку 2), так і паралельні переноси (елементи нескінченного порядку).

Задача 21.1. a) *Доведіть, що прямий добуток довільної родини періодичних груп є періодичною групою.*
b) *Наведіть приклад декартового добутку періодичних груп, який не є періодичною групою.*

Задача 21.2. *Доведіть, що факторгрупа $\mathbb{Q}/\mathbb{Z}$ є періодичною і для кожного натурального числа n містить рівно одну, причому циклічну, підгрупу порядку n.*

Задача 21.3. *Доведіть, що факторгрупи $\mathbb{R}/\mathbb{Z}$ і $\mathbb{R}/\mathbb{Q}$ — не періодичні.*

22 Абелеві групи

Множина T всіх елементів скінченного порядку абелевої групи A називається її *періодичною частиною.*

Теорема 22.1. *Періодична частина T абелевої групи A є нормальною підгрупою, а факторгрупа A/T є групою без скруту.*

Доведення. В абелевій групі $(ab)^n = a^n b^n$, тому $|ab| \le |a| \cdot |b|$. Крім того, $|a^{-1}| = |a|$. Отже, множина T замкнена відносно множення і взяття оберненого елемента, а тому згідно твердження 5.1 є підгрупою. Вона нормальна, бо в абелевій групі кожна підгрупа є нормальною.

Припустимо тепер, що елемент aT факторгрупи A/T має скінченний порядок n. Тоді $(aT)^n = a^nT = T$, звідки $a^n \in T$. Отже, елемент a^n має якийсь скінченний порядок k. Але тоді $a^{nk} = e$ і $|a| < \infty$, тобто $a \in T$ і $aT = T$. Таким чином, єдиним елементом скінченного порядку у факторгрупі A/T є її одиниця T. Тому A/T є групою без скруту. $\square$

Зауваження. 1. У неабелевій групі елементи скінченного порядку підгрупи, взагалі кажучи, не утворюють. Наприклад, у групі всіх рухів площини композиція двох різних центральних симетрій — елементів порядку 2 — є паралельним переносом, тобто елементом нескінченного порядку.

2. Якщо абелева група містить як елементи скінченного, так і нескінченного порядків, то елементи нескінченного порядку, навіть разом із одиничним, підгрупи, взагалі кажучи, не утворюють (наведіть відповідний приклад!).

Із теореми 22.1 випливає, що проблема опису всі абелевих груп зводиться до трьох основних задач:
1) описати всі періодичні абелеві групи;
2) описати всі абелеві групи без скруту;
3) описати всі абелеві групи, періодична частина яких ізоморфна даній періодичній групі A, а факторгрупа за періодичною частиною — даній групі без скруту B.

На жаль, кожна з цих задач поки що безнадійно далека від остаточного розв'язання.

Група G називається *примарною*, якщо вона є p–групою для деякого простого числа p.

Множина всіх p–елементів абелевої групи G, тобто тих елементів, порядки яких є степенями фіксованого простого числа p, називається її p–*компонентою*. Аналогічно доведенню першої частини теореми 22.1 можна показати, що p–компонента абелевої групи є її підгрупою.

Під *примарною компонентою* абелевої групи G будемо розуміти її p–компоненту для довільного простого числа p.

Приклад. Примарними компонентами групи $\mathbb{C}_\infty$ всіх комплексних коренів натуральних степенів з одиниці є групи $\mathbb{C}_{p^\infty}$.

Лема 22.1. *В абелевій групі для кожного елемента g скінченного порядку існує розклад $g = a_{p_1} \cdots a_{p_k}$, де $p_1, \ldots, p_k$ — попарно різні прості числа, а множники $a_{p_1}, \ldots, a_{p_k}$ є, відповідно, p_1–, $\ldots$, p_k–елементами,*

причому з точністю до порядку множників такий розклад однозначний.

Доведення. Існування розкладу випливає з наслідку 20.1.

Єдиність розкладу. Якщо для якогось простого числа p відповідні p–множники в розкладах $g = a_{p_1} \cdots a_{p_k}$ і $g = b_{q_1} \cdots b_{q_m}$ є різними, то рівність $a_{p_1} \cdots a_{p_k} = b_{q_1} \cdots b_{q_m}$ можна звести до рівності $c_p = c_{r_1} \cdots c_{r_l}$, де $c_p, c_{r_1}, \ldots, c_{r_l}$ є, відповідно, p–, r_1–, $\ldots$, r_l–елементами, причому $c_p \neq e$ і $p \notin \{r_1, \ldots, r_l\}$. Але підгрупа $\langle c_{r_1}, \ldots, c_{r_l} \rangle$ — скінченна і її порядок не ділиться на p, що суперечить включенню $c_p \in \langle c_{r_1}, \ldots, c_{r_l} \rangle$. □

Теорема 22.2. *Кожна періодична абелева група розкладається в прямий добуток своїх примарних компонент.*

Доведення. Безпосередньо випливає з леми 22.1. □

Приклад. Оскільки примарними компонентами групи $\mathbb{C}_\infty$ є підгрупи $\mathbb{C}_{p^\infty}$, то $G = \prod\limits_p \mathbb{C}_{p^\infty}$.

Очевидно, що для кожного простого дільника p свого порядку скінченна абелева група містить єдину силовську p–підгрупу. Позаяк кожен p–елемент входить в якусь силовську p–підгрупу, то в скінченній абелевій групі силовська p–підгрупа збігається з p–компонентою. Тому з теореми 22.2 одразу випливає

Наслідок 22.1. *Кожна скінченна абелева група розкладається в прямий добуток своїх силовських підгруп.*

Вправа 22.1. *Доведіть, що періодична скінченно породжена абелева група є скінченною.*

Систему $a_1, \ldots, a_m$ елементів групи $\mathbb{Z}^n$ назвемо *лінійно незалежною*, якщо для довільних цілих чисел $k_1, \ldots, k_m$ з рівності $k_1 a_1 + \cdots + k_m a_m = 0$ випливає, що $k_1 = \cdots = k_m = 0$.

Серед систем твірних групи $\mathbb{Z}^n$ є і лінійно незалежні. Такою буде, зокрема, система $e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, 0, \ldots, 0)$, $\ldots$, $e_n = (0, \ldots, 0, 1)$.

Вільною абелевою групою рангу n називається прямий добуток n нескінченних циклічних груп. Оскільки кожна нескінченна циклічна група ізоморфна групі $\mathbb{Z}$, то вільна абелева група рангу n ізоморфна групі $\mathbb{Z}^n = \bigoplus\limits_{i=1}^{n} \mathbb{Z}$.

Твердження 22.1. *Система твірних групи $\mathbb{Z}^n$ буде лінійно незалежною тоді й лише тоді, коли вона містить n елементів. Якщо a_1, $\ldots$, a_n — лінійно незалежна система твірних групи $\mathbb{Z}^n$, то кожний елемент $a \in \mathbb{Z}^n$ однозначно записується у вигляді $a = k_1a_1 + \cdots + k_na_n$.*

Доведення. Очевидно, що елементи групи $\mathbb{Z}^n$ можна розглядати і як вектори з арифметичного векторного простору $\mathbb{Q}^n$. При цьому $a_1, \ldots, a_m$ будуть лінійно незалежні як елементи групи $\mathbb{Z}^n$ тоді й лише тоді, коли вони будуть лінійно незалежні як вектори простору $\mathbb{Q}^n$. Зауважимо також, що кожна система твірних групи $\mathbb{Z}^n$ буде і системою твірних простору $\mathbb{Q}^n$. Тому лінійно незалежні системи твірних групи $\mathbb{Z}^n$ можна ототожнити з тими базами простору $\mathbb{Q}^n$, які складаються з векторів із цілими координатами. Тепер наше твердження випливає з того, що система твірних простору $\mathbb{Q}^n$ буде лінійно незалежною, тобто базою, тоді й лише тоді, коли вона містить n векторів, і що розклад за векторами бази є однозначним. □

Теорема 22.3. *Групи $\mathbb{Z}^n$ і $\mathbb{Z}^m$ ізоморфні тоді й лише тоді, коли $n = m$.*

Доведення. Досить довести, що коли $n \neq m$, то $\mathbb{Z}^n \not\cong \mathbb{Z}^m$. Але це випливає з твердження 22.1 і того, що при ізоморфізмі лінійно незалежна система елементів перходить у лінійно незалежну систему. □

Твердження 22.2. *Якщо a_1, $\ldots$, a_n — система твірних абелевої групи A, то відображення $\varphi : \mathbb{Z}^n \to A$, $(k_1, \ldots, k_n) \mapsto a_1^{k_1} \cdots a_n^{k_n}$, є епіморфізмом груп.*

Доведення. Оскільки $a_1, \ldots, a_n$ утворюють систему твірних групи A і, як елементи абелевої групи, попарно переставні, то кожний елемент $a \in A$ можна записати у вигляді $a = a_1^{k_1} \cdots a_n^{k_n}$, а тому відображення φ є сюр'єктивним. Гомоморфність відображення φ випливає з рівностей

$$\varphi\big((k_1, \ldots, k_n) + (l_1, \ldots, l_n)\big) = \varphi\big((k_1 + l_1, \ldots, k_n + l_n)\big) = a_1^{k_1+l_1} \cdots a_n^{k_n+l_n} =$$

$$a_1^{k_1} \cdots a_n^{k_n} \cdot a_1^{l_1} \cdots a_n^{l_n} = \varphi\big((k_1, \ldots, k_n)\big) \cdot \varphi\big((l_1, \ldots, l_n)\big).$$

□

Із цього твердження і основної теореми про гомоморфізми алгебричних систем (теореми 10.1) одразу випливає

Наслідок 22.2. *Кожна скінченно породжена абелева група ізоморфна факторгрупі деякої вільної абелевої групи.*

Таким чином, щоб з'ясувати будову скінченно породжених абелевих груп, досить розібратися з будовою факторгруп вільних абелевих груп.

Лема 22.2. *Якщо в системі твірних $a_1, \ldots, a_n$ адитивної абелевої групи A*

a) *переставити місцями два елементи,*

b) *замінити один із елементів на протилежний,*

c) *до одного з елементів додати довільне кратне іншого елемента, то знову одержимо систему твірних групи A.*

Доведення випливає з рівностей

$$\begin{gathered} k_1a_1 + \cdots + k_ia_i + \cdots + k_ja_j + \cdots + k_na_n = \\ = k_1a_1 + \cdots + k_ja_j + \cdots + k_ia_i + \cdots + k_na_n = \\ = k_1a_1 + \cdots + (-k_i)(-a_i) + \cdots + k_ja_j + \cdots + k_na_n = \\ = k_1a_1 + \cdots + k_i(a_i + ma_j) + \cdots + (k_j - mk_i)a_j + \cdots + k_na_n. \quad \square \end{gathered}$$

Описані в лемі 22.2 перетворення системи твірних адитивної абелевої групи будемо називати *елементарними.*

Зауваження. Звернемо увагу, що при елементарних перетвореннях системи твірних коефіцієнти $k_1, \ldots, k_n$ в зображенні $a = k_1a_1 + \cdots + k_na_n$ елемента $a \in A$ через твірні $a_1, \ldots, a_n$ змінюється за простими правилами:

— якщо два елементи системи твірних переставляються, то й відповідні коефіцієнти переставляються;

— якщо один з твірних елементів міняємо на протилежний, то й відповідний коефіцієнт міняється на протилежний;

— якщо до одного з твірних елементів додати кратне іншого, то від коефіцієнта при другому твірному елементі треба відняти відповідне кратне коефіцієнта при першому елементі.

Лема 22.3. *Кожна підгрупа групи $\mathbb{Z}^n$ має систему твірних, що містить не більше ніж n елементів.*

Доведення. Застосуємо індукцію за числом n. При $n = 1$ твердження леми випливає з того, що будь–яка підгрупа циклічної $\mathbb{Z}^1 = \mathbb{Z}$ групи є циклічною.

Нехай тепер $n > 1$ і $H \leq \mathbb{Z}^n$. Множина H_0 усіх тих елементів з H, в яких остання координата дорівнює 0, є підгрупою в H, бо замкнена відносно додавання і взяття протилежного елемента. Очевидно, що H_0

можна розглядати і як підгрупу із $\mathbb{Z}^{n-1}$. Тому за припущенням індукції H_0 має систему твірних $b, \ldots, c$ не більше ніж з $n-1$ елементів.

Якщо $H_0 = H$, то лему доведено. У противному разі серед елементів множини $H \setminus H_0$ виберемо той, в якого остання координата є найменшою за модулем. Нехай це $a = (a_1, \ldots, a_n)$. Тоді в довільного елемента $x = (x_1, \ldots, x_n)$ із підгрупи H остання координата x_n ділиться на a_n. Справді, в противному разі x_n можна було б розділити на a_n з остачею: $x_n = ka_n + r$, де $0 < r < |a_n|$, і тоді елемент $x - ka = (x_1 - ka_1, \ldots, x_{n-1} - ka_{n-1}, r)$ належав би множині $H \setminus H_0$ і мав би останню координату r меншу за $|a_n|$. А це суперечить вибору елемента a.

Отже, для для довільного елемента $x = (x_1, \ldots, x_n) \in H$ знайдеться таке ціле число k, що $x_n = ka_n$. Але тоді елемент $x - ka = (x_1 - ka_1, \ldots, x_{n-1} - ka_{n-1}, 0)$ належить підгрупі H_0 і може бути записаний у вигляді $x - ka = mb + \cdots + lc$. Звідси випливає, що набір $a, b, \ldots, c$, який містить не більше ніж n елементів, є системою твірних підгрупи H. $\square$

Лема 22.4. *Якщо H є підгрупою групи $\mathbb{Z}^n$, то можна вибрати такі системи твірних $a_1, \ldots, a_n$ групи $\mathbb{Z}^n$ і $b_1, \ldots, b_n$ підгрупи H, що $b_1 = k_1 a_1, \ldots, b_n = k_n a_n$ для деяких невід'ємних цілих чисел $k_1, \ldots, k_n$.*

Доведення. За лемою 22.3 підгрупа $H \leq \mathbb{Z}^n$ має систему твірних, що містить не більше ніж n елементів. Узявши в разі потреби необхідну кількість разів нульовий елемент, можна вважати, що система твірних підгрупи H складається рівно з n елементів $v_1, \ldots, v_n$. Виберемо також якусь лінійно незалежну систему твірних $u_1, \ldots, u_n$ групи $\mathbb{Z}^n$. Розглянемо розклади

$$v_1 = k_{11}u_1 + \cdots + k_{1n}u_n\ , \quad \ldots, \quad v_n = k_{n1}u_1 + \cdots + k_{nn}u_n$$

і матрицю

$$A_{(u,v)} = \begin{pmatrix} k_{11} & \cdots & k_{1n} \\ \ldots & \ldots & \ldots \\ k_{n1} & \cdots & k_{nn} \end{pmatrix}.$$

Елементарними перетвореннями матриці $A_{(u,v)}$ назвемо перестановку двох довільних рядків (стовпчиків), множення рядка (стовпчика) на число -1 і додавання до одного рядка (стовпчика) цілого кратного іншого рядка (стовпчика). Очевидно, що кожному елементарному перетворенню системи твірних $v_1, \ldots, v_n$ підгрупи H відповідає таке ж елементарне перетворення рядків матриці $A_{(u,v)}$, і навпаки. Із зауваження після

доведення леми 22.2 випливає також, що є взаємно однозначна відповідність між елементарними перетвореннями системи твірних $u_1, \dots, u_n$ групи $\mathbb{Z}^n$ та елементарними перетвореннями стовпчиків матриці $A_{(u,v)}$.

Доведемо індукцією за порядком матриці $A_{(u,v)}$, що елементарними перетвореннями рядків і стовпчиків її можна звести до діагонального вигляду. Це очевидно, якщо матриця $A_{(u,v)}$ має порядок 1 або є нульовою. Припустимо тепер, що $A_{(u,v)}$ ненульова і має порядок більший за 1.

Виберемо серед ненульових елементів матриці $A_{(u,v)}$ найменший за модулем. Застосувавши в разі потреби перестановку рядків і/або стовпчиків і множення на -1, можемо вважати, що найменшим за модулем елементом є k_{11}, причому $k_{11} > 0$. Після цього розділимо з остачею елементи першого рядка на k_{11}:

$$k_{12} = q_2 k_{11} + r_2 \ , \quad \dots, \quad k_{1n} = q_n k_{11} + r_n,$$

а потім від кожного стовпчика, починаючи з другого, віднімемо перший стовпчик, помножений на $q_2, \dots, q_n$ відповідно. У результаті цих перетворень перший рядок набуде вигляду $(k_{11}, r_2, \dots, r_n)$.

Потім аналогічно розділимо з остачею на k_{11} елементи першого стовпчика і від кожного рядка, починаючи з другого, віднімемо відповідне кратне першого рядка.

Внаслідок цих перетворень відмінні від k_{11} елементи першого рядка і першого стовпчика стануть за модулем меншими за k_{11}. Якщо серед них будуть ненульові, то повторюємо описаний цикл перетворень: знову вибираємо найменший за модулем ненульовий елемент матриці (позначимо його k'_{11}) і ставимо його на верхнє ліве місце, потім ділимо з остачею на k'_{11} елементи першого рядка і першого стовпчика і т.д.

Оскільки числа k_{11}, k'_{11}, ... є цілими невід'ємними і $k_{11} > k'_{11} > \cdots$, то щонайбільше через k_{11} циклів перетворень одержимо матрицю вигляду

$$\left(\begin{array}{c|ccc} k_1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \cdots & & A_1 & \\ 0 & & & \end{array}\right). \tag{13}$$

Тепер для матриці (13) елементарні перетворення, які зачіпають тільки рядки і стовпчики з 2–го по n–й, фактично будуть лише елементарними перетвореннями рядків і стовпчиків матриці A_1, бо першого рядка і першого стовпчика матриці (13) вони не мінятимуть. Але матриця A_1 має

порядок $n-1$, тому за припущенням індукції її можна звести елементарними перетвореннями рядків і стовпчиків до діагонального вигляду $\mathrm{diag}(k_2,\dots,k_n)$. Тоді початкова матриця $A_{(u,v)}$ зведеться до діагонального вигляду

$$\begin{pmatrix} k_1 & 0 & \cdots & 0 \\ 0 & k_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & k_n \end{pmatrix}, \tag{14}$$

причому $k_1,\dots,k_n \geq 0$.

Оскільки елементарним перетворенням рядків (стовпчиків) матриці $A_{(u,v)}$ відповідають елементарні перетворення системи твірних підгрупи H групи $\mathbb{Z}^n$, то з леми 22.2 випливає, що матриця (14) є матрицею вигляду $A_{(a,b)}$ для певних систем твірних $a_1,\dots,a_n$ групи $\mathbb{Z}^n$ і $b_1,\dots,b_n$ підгрупи H. Але тоді для цих систем твірних маємо: $b_1 = k_1a_1,\dots,b_n = k_na_n$. □

Теорема 22.4. *Нехай H — довільна підгрупа групи $\mathbb{Z}^n$. Якщо системи твірних $a_1,\dots,a_n$ групи $\mathbb{Z}^n$ і $b_1,\dots,b_n$ її підгрупи H вибрані так, як у лемі* 22.4, *то*

$$\mathbb{Z}^n/H \simeq \mathbb{Z}_{k_1} \oplus \cdots \oplus \mathbb{Z}_{k_n}.$$

Доведення. Оскільки при елементарних перетвореннях системи твірних кількість елементів у ній не змінюється, то з твердження 22.1 випливає, що при елементарних перетвореннях лінійно незалежної системи твірних групи $\mathbb{Z}^n$ знову одержуємо лінійно незалежну систему твірних. Зокрема, зображення $a = r_1a_1 + \cdots + r_na_n$ для довільного елемента $a \in \mathbb{Z}^n$ є однозначним.

Далі, з рівності $m_1b_1+\cdots+m_nb_n = m_1k_1\cdot a_1+\cdots+m_nk_n\cdot a_n$ випливає, що елемент $a = r_1a_1+\cdots+r_na_n$ належить підгрупі H тоді й лише тоді, коли $k_1|r_1,\dots,k_n|r_n$.

Нехай тепер $a = r_1a_1 + \cdots + r_na_n$. За твердженням 9.2 елемент $b = l_1a_1+\cdots+l_na_n$ належить класу суміжності $a+H$ тоді й лише тоді, коли різниця $b-a = (l_1-r_1)a_1+\cdots+(l_n-r_n)a_n$ належить підгрупі H, тобто тоді й лише тоді, коли $k_1|(l_1-r_1),\dots,k_n|(l_n-r_n)$, або, що те саме, $l_1 \equiv r_1 \pmod{k_1}$,…, $l_n \equiv r_n \pmod{k_n}$. Тому клас суміжності $a+H$ можна ототожнити з набором $(a_1 \bmod k_1,\dots,a_n \bmod k_n) \in \mathbb{Z}_{k_1} \oplus \cdots \oplus \mathbb{Z}_{k_n}$.

Таким чином, ми побудували ін'єктивне відображення $\varphi : \mathbb{Z}^n/H \to \mathbb{Z}_{k_1}\oplus\cdots\oplus\mathbb{Z}_{k_n}$, $a+H \mapsto (a_1 \bmod k_1,\dots,a_n \bmod k_n)$. Сюр'єктивність цього

відображення очевидна. Оскільки

$$\varphi(a)+\varphi(b)=(a_1 \bmod k_1,\dots,a_n \bmod k_n)+(b_1 \bmod k_1,\dots,b_n \bmod k_n)=$$
$$=((a_1+b_1) \bmod k_1,\dots,(a_n+b_n) \bmod k_n)=\varphi(a+b),$$

то φ є ізоморфізмом, що й доводить теорему. □

Оскільки при $k>0$ група $\mathbb{Z}_k$ є циклічною порядку k, а $\mathbb{Z}_0\simeq\mathbb{Z}$, то з теореми 22.4 і наслідку 22.2 одразу випливає

Наслідок 22.3. *Кожна скінченно породжена абелева група розкладається в пряму суму своїх циклічних підгруп.*

Теорема 22.5 (основна теорема про скінченно породжені абелеві групи). *Кожна скінченно породжена абелева група розкладається в пряму суму своїх нескінченних циклічних і примарних циклічних підгруп, причому такий розклад однозначний із точністю до порядку доданків.*

Доведення. Існування такого розкладу випливає з наслідків 22.3 і 20.1.

Із ізоморфності циклічних груп однакових порядків випливає, що єдиність такого розкладу досить довести для групи

$$G=\underbrace{\mathbb{Z}\oplus\dots\oplus\mathbb{Z}}_{m}\oplus\mathbb{Z}_{p_1^{k_1}}\oplus\dots\oplus\mathbb{Z}_{p_1^{k_n}}\oplus\dots\oplus\mathbb{Z}_{p_r^{s_1}}\oplus\dots\oplus\mathbb{Z}_{p_r^{s_t}},$$

де $p_1,\dots,p_r$ — попарно різні прості числа. Легко бачити, що елемент $g=(g_1,\dots,g_m,g_{m+1},\dots)$ групи G матиме скінченний порядок тоді й лише тоді, коли його перші m компонент $g_1,\dots,g_m$ будуть нульовими. Тому періодична частина T групи G збігається з

$$\mathbb{Z}_{p_1^{k_1}}\oplus\dots\oplus\mathbb{Z}_{p_1^{k_n}}\oplus\dots\oplus\mathbb{Z}_{p_r^{s_1}}\oplus\dots\oplus\mathbb{Z}_{p_r^{s_t}}$$

і є скінченною. Крім того, для факторгрупи G/T групи G за своєю періодичною частиною T маємо:

$$G/T\simeq\underbrace{\mathbb{Z}\oplus\dots\oplus\mathbb{Z}}_{m}=\mathbb{Z}^m.$$

Із теореми 22.3 тепер випливає, що число m визначене однозначно.

Прямі суми

$$\mathbb{Z}_{p_1^{k_1}}\oplus\dots\oplus\mathbb{Z}_{p_1^{k_n}},\ \dots,\ \mathbb{Z}_{p_r^{s_1}}\oplus\dots\oplus\mathbb{Z}_{p_r^{s_t}}$$

є, відповідно, p_1–, …, p_r–силовськими підгрупами періодичної частини T. Оскільки для кожного простого числа p, що ділить її порядок, скінченна абелева група містить єдину силовську p–підгрупу, то лишилося довести, що з точністю до порядку доданків група вигляду

$$A = \mathbb{Z}_{p^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_n}} \tag{15}$$

розкладається в пряму суму циклічних підгруп лише одним способом.

Легко зрозуміти, що кількість елементів порядку $\leq p^k$ у групі $\mathbb{Z}_{p^r}$ дорівнює p^k, якщо $k \leq r$, і p^r, якщо $k > r$. Крім того, елемент $g = (g_1, \ldots, g_n)$ групи $A = \mathbb{Z}_{p^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_n}}$ має порядок $\leq p^k$ тоді й лише тоді, коли кожна його компонента $g_i, 1 \leq i \leq n$, має порядок $\leq p^k$. Тому кількість t_k тих тих елементів групи A, порядок яких не перевищує p^k, дорівнює

$$t_k = \prod_{\substack{i \\ k_i \geq k}} p^k \cdot \prod_{\substack{j \\ k_j < k}} p^{k_j}.$$

Звідси одержуємо, що $t_1 = p^n$ і для всіх $k \geq 0$

$$\frac{t_{k+1}}{t_k} = p^{u_k}, \quad \text{де} \quad u_k = |\{i : k_i > k\}|.$$

Таким чином, для всіх $k \geq 1$ маємо: $u_k - u_{k-1} = |\{i : k_i = k\}|$. Оскільки числа t_k, а тим самим і числа u_k, визначаються самою групою A, а не її розкладом (15) у пряму суму, то кількість доданків порядку p^k у розкладі (15) визначається однозначно. Це й доводить однозначність із точністю до порядку доданків розкладу (15). □

Зрозуміло, що в розкладі у пряму суму скінченної абелевої групи нескінченні доданки відсутні. Тому з теореми 22.5 одразу випливає

Теорема 22.6 (основна теорема про скінченні абелеві групи). *Кожна скінченна абелева група розкладається в пряму суму своїх примарних циклічних підгруп, причому такий розклад однозначний із точністю до порядку доданків.*

Позначимо через $t(n)$ кількість розбиттів $n = n_1 + \cdots + n_k$ числа n в суму натуральних доданків $n_1, \ldots, n_k$ за умови, що порядок доданків не є істотним. Для малих n число $t(n)$ легко обчислюється безпосередньо: $t(1) = 1$, $t(2) = 2$, $t(3) = 3$, $t(4) = 5$, $t(5) = 7$.

Лема 22.5. *Для кожного простого числа p кількість попарно неізоморфних абелевих груп порядку p^n дорівнює $t(n)$.*

Доведення. Для кожного розкладу $n = n_1 + \cdots + n_k$ існує абелева група $\mathbb{Z}_{p^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_n}}$. Із теореми 22.6 випливає, що різним розкладам числа n будуть при цьому відповідати неізоморфні групи, і що таким чином ми одержимо з точністю до ізоморфізму усі абелеві групи порядку n. □

Теорема 22.7. *Якщо $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ — канонічний розклад числа n, то з точністю до ізоморфізму існує рівно $t(k_1) \cdots t(k_m)$ абелевих груп порядку n.*

Доведення. За наслідком 22.1 кожна скінченна абелева група розкладається в прямий добуток своїх своїх силовських підгруп. Звідси випливає, що дві групи порядку n будуть ізоморфними тоді й лише тоді, коли для кожного простого дільника p числа n їх силовські p–підгрупи будуть ізоморфними. Твердження теореми тепер випливає з леми 22.5 і того, що для різних простих p відповідні множники у розкладі групи в добуток своїх силовських підгруп можна вибирати незалежно. □

23 Розв'язні групи

Скінченний ряд підгруп

$$E = G_0 \leq G_1 \leq \cdots \leq G_n = G$$

групи G називається *субнормальним рядом* групи G, якщо для кожного i, $0 \leq i < n$, підгрупа G_i є нормальною в підгрупі G_{i+1}, і *нормальним рядом*, якщо кожна підгрупа G_i є нормальною в усій групі G. Факторгрупи G_{i+1}/G_i, $0 \leq i < n$, називаються *факторами* субнормального (нормального) ряду.

Очевидно, що кожний нормальний ряд є субнормальним, але зворотне твердження, взагалі кажучи, хибне. Наприклад, ряд

$$\{\varepsilon\} < \langle (12)(34) \rangle < K_4 < A_4 < S_4$$

є субнормальним рядом групи S_4, але не є нормальним, бо підгрупа $\langle (12)(34) \rangle$ не є нормальною в S_4.

Означення 23.1. *Група G називається розв'язною, якщо для неї існує нормальний ряд, усі фактори якого є абелевими групами.*

Приклади. 1. Кожна абелева група G є розв'язною. У цьому випадку потрібним рядом є $E < G$.

2. Якщо в субнормальному ряді $\{\varepsilon\} < \langle(12)(34)\rangle < K_4 < A_4 < S_4$ викинути підгрупу $\langle(12)(34)\rangle$, то одержимо нормальний ряд $\{\varepsilon\} < K_4 < A_4 < S_4$, усі фактори $K_4/\{\varepsilon\} \cong K_4$, $A_4/K_4 \cong C_3$, $S_4/A_4 \cong C_2$ якого є абелевими. Тому група S_4 є розв'язною.

Розв'язні групи вперше з'явилися у видатного французького математика Евариста Ґалуа (1811 — 1832) при дослідженні проблеми розв'язності алгебричних рівнянь у радикалах (походження терміну "розв'язні групи" також пов'язане з цією проблемою). Детальніше про зв'язок між розв'язністю рівнянь у радикалах і розв'язністю відповідних груп йтиметься в наступному семестрі. Крім того, що розв'язні групи виникають у багатьох розділах алгебри, вони й самі є дуже цікавим об'єктом для досліджень.

Теорема 23.1. a) *Кожна підгрупа розв'язної групи також є розв'язною*;
b) *кожна факторгрупа розв'язної групи також є розв'язною*;
c) *коли в групі G нормальна підгрупа N і факторгрупа G/N є розв'язними, то група G також є розв'язною.*

Доведення. Нехай $\{e\}E = G_0 \le G_1 \le \cdots \le G_n = G$ — нормальний ряд із абелевими факторами для групи G.

a) Доведемо, що для підгрупи H ряд

$$\{e\} = G_0 \cap H \le G_1 \cap H \le \cdots \le G_n \cap H = G \cap H = H$$

буде нормальним рядом із абелевими факторами. Справді, за теоремою про ізоморфізм факторгруп (теорема 12.1) для довільного i підгрупа $G_i \cap H$ буде нормальною в H. Крім того, із включення $G_{i-1} \le G_i$ випливають рівність $G_{i-1} \cap H = G_{i-1} \cap (G_i \cap H)$ і включення $G_{i-1} \cdot (G_i \cap H) \le G_i$. Тому за тією ж теоремою 12.1

$$(G_i \cap H)\big/(G_{i-1} \cap H) = (G_i \cap H)\big/(G_{i-1} \cap (G_i \cap H)) \simeq$$
$$\simeq (G_{i-1} \cdot (G_i \cap H))\big/G_{i-1} \le G_i/G_{i-1}.$$

Отже, факторгрупа $(G_i \cap H)\big/(G_{i-1} \cap H)$ ізоморфна підгрупі абелевої групи G_i/G_{i-1}, а тому і сама є абелевою.

b) Доведемо тепер, що ряд

$$E = NG_0/N \le NG_1/N \le \cdots \le NG_n/N = G/N$$

буде нормальним рядом із абелевими факторами для факторгрупи G/N. Справді, оскільки підгрупи N, G_{i-1}, G_i нормальні і $G_{i-1} \leq G_i$, то $G_i = G_{i-1} \cdot G_i$ і $NG_i = NG_{i-1} \cdot G_i$. А тому з теореми 12.1 про ізоморфізм факторгруп і теореми 12.2 про відповідність підгруп випливає, що

$$NG_i/NG_{i-1} = (NG_{i-1} \cdot G_i)/NG_{i-1} \simeq G_i/(NG_{i-1} \cap G_i) \simeq$$
$$\simeq \big(G_i/G_{i-1}\big)\Big/\Big((NG_{i-1} \cap G_i)/G_{i-1}\Big).$$

Таким чином, факторгрупа NG_i/NG_{i-1} ізоморфна факторгрупі абелевої групи G_i/G_{i-1}, а тому і сама є абелевою.

c) Легко перевіряється, що коли $\{e\} = N_0 \leq N_1 \leq \cdots \leq N_n = N$ і $E = N/N \leq G_1/N \leq \cdots \leq G_m/N = G/N$ — нормальні ряди з абелевими факторами для підгрупи N і факторгрупи G/N відповідно, то ряд

$$\{e\} = N_0 \leq N_1 \leq \cdots \leq N_n = N \leq G_1 \leq \cdots \leq G_m = G$$

буде нормальним рядом із абелевими факторами для групи G. □

Вправа 23.1. *Доведіть, що кожна з груп* a) Q_8, b) A_4, c) D_n *є розв'язною.*

Задача 23.1. *Доведіть, що коли групи G і H розв'язні, то група $G \times H$ також є розв'язною.*

Теорема 23.2. *Кожна скінченна p–група є розв'язною.*

Доведення. Це випливає з теореми 15.2. □

Але не кожна група є розв'язною. Зокрема, не є розв'язною група A_5. Справді, ця група є простою, а тому вона має єдиний нормальний ряд $\{\varepsilon\} < A_5$ із неабелевим фактором $A_5/\{\varepsilon\} \simeq A_5$. Із теореми 23.1 одразу випливає, що довільна група, яка місить підгрупу, ізоморфну групі A_5, також не є розв'язною. Зокрема, звідси випливає, що при $n > 4$ групи A_n і S_n не є розв'язними.

Важливим прикладом розв'язної групи є група $T_n(P)$ верхніх трикутних матриць порядку n з коефіцієнтами з поля P. Доведення цього факту розпадається на ряд нескладних кроків, які пропонуємо провести самостійно.

Задача 23.2. *Позначимо через $UT_n^k(P)$ множину верхніх трикутних матриць порядку n з коефіцієнтами з поля P, в яких на головній діагоналі стоять одиниці і які містять k нульових похилих рядків над*

діагоналлю. Доведіть, що:
a) *для довільного* $k = 0, 1, \ldots, n-1$ *множина* $UT_n^k(P)$ *буде нормальною підгрупою групи* $T_n(P)$;
b) $T_n(P)/UT_n^0(P) \cong P^* \times \cdots \times P^*$ (n *множників*);
c) *для довільного* $k = 0, 1, \ldots, n-2 \quad UT_n^k(P)/UT_n^{k+1}(P) \cong P \oplus \cdots \oplus P$ ($n-k-1$ *доданків*);
d) *ряд підгруп* $\{E\} < UT_n^{n-2}(P) < \cdots < UT_n^0(P) < T_n(P)$ *є нормальним рядом з абелевими факторами.*

Задача 23.3. *Нехай* p *і* q *— різні прості числа. Доведіть, що кожна група порядку* a) pq, b) $2pq$, c) p^2q *є розв'язною.*

Задача 23.4. *Використовуючи факт, що не існує неабелевих простих груп порядку* < 60, *доведіть, що кожна група порядку* < 60 *є розв'язною.*

Вказівка. Скористайтеся теоремою 23.1.

Уже із задачі 23.3 видно, що порядок скінченної нерозв'язної групи повинен мати досить складну арифметичну структуру. Зокрема, із відомої теореми Бернсайда про розв'язність кожної групи порядку $p^n q^m$ випливає, що порядок нерозв'язної групи повинен ділитися принаймні на 3 простих числа. Тому серед груп невеликих порядків нерозв'язні зустрічаються порівняно рідко. Наприклад, ще в кінці XIX ст. Гьольдер довів, що серед груп порядку < 480 з точністю до ізоморфізму є рівно 25 нерозв'язних. Наведемо таблицю порядків таких груп і їх кількостей:

Порядок	60	120	168	180	240	300	336	360	420
Кількість груп	1	3	1	1	8	1	3	6	1

24 Мультиплікативна група поля, дискретний логарифм і криптографічні протоколи

У класичних криптографічних системах спосіб шифрування тримається в глибокій таємниці, бо інакше секретне повідомлення зможуть розшифрувати й ті, від кого воно засекречується. У сучасних же системах (так званих системах з відкритим ключем), винахід яких став у криптографії справжнім переворотом, тримати в таємниці спосіб шифрування (чи так званий ключ шифру) немає жодної потреби. Він є доступним для всіх, відкритим, що й пояснює таку їх назву. Все одно знання ключа

жодним чином не допомагає в розшифруванні секретних повідомлень. Ідея таких систем була запропонована американськими математиками У.Діффі та М.Геллманом у 1976 р.

Прикладом успішного застосування ідеології відкритого ключа до розв'язування різноманітних задач, пов'язаних із захистом інформації при взаємодії віддалених абонентів, є криптографічні протоколи. Це відносно молода галузь математичної криптографії (перші протоколи з'явилися біля 30 років тому). Але за цей час вона бурхливо розвивалася і на даний момент перетворилася в основний об'єкт дослідження в теоретичній криптографії.

Під *криптографічним протоколом* слід розуміти послідовність узгоджених приписів, згідно з якими відбувається обмін повідомленнями між сторонами – учасниками протоколу задля досягнення певної мети. Іншими словами: віддалені абоненти, взаємодіючи через відкриті канали зв'язку, розв'язують певну задачу. При цьому є супротивник (ним може виявитися навіть один або декілька абонентів, що вступили в зговір), який тим чи іншим чином може втручатися у процес обміну інформацією між абонентами.

Надійність чималої кількості криптосистем грунтується на складності задачі дискретного логарифмування.

Означення 24.1. *Нехай g — первісний корінь за простим модулем p і число x не ділиться на p. Якщо $g^y \equiv x \pmod p$, то y називається дискретним логарифмом або індексом числа x за основою g і модулем p. Позначатимемо $y = ind(x, g, p)$ і для однозначності вважатимемо, що $0 \le ind(x, g, p) < p - 1$.*

Вправа 24.1. *Знайдіть такі дискретні логарифми*: $ind(1, 5, 19)$, $ind(2, 5, 19)$, $ind(3, 5, 19)$, $ind(4, 5, 19)$, $ind(5, 5, 19)$, $ind(6, 5, 19)$.

Вправа 24.2. *Нехай g_1, g_2 — первісні корені за простим модулем p і число x не ділиться на p. Доведіть, що*

$$ind(x, g_1, p) = ind(g_2\, ind(x, g_2, p), g_1, p).$$

Сама ж *задача дискретного логарифмування* полягає в наступному. Нехай відомо такі натуральні числа x, g, p, що p — просте число, $p \nmid x$, а g — первісний корінь за модулем p. Потрібно знайти таке число y, що $g^y \equiv x \pmod p$.

Час виконання задачі дискретного логарифмування такого ж порядку, як і *задачі факторизації* (розкладу числа на прості множники), хоча про звідність однієї задачі до іншої поки нічого не відомо. Найбільш

швидкі із нині діючих алгоритмів розв'язання задачі дискретного логарифмування базуються на так званому методі решета числового поля і вимагають $\exp(c(\ln p)^{1/3}(\ln \ln p)^{2/3})$ арифметичних операцій (тут $c > 0$ — деяка константа). Ці алгоритми уже не є експоненційними, але все ще не є поліноміальними, і практично не реалізуються вже для значень $p \approx 10^{150}$. Тому з обчислювальної точки зору задача дискретного логарифмування вважається складною математичною задачею.

На прикладах двох протоколів продемонструємо, як задача дискретного логарифмування використовується в криптографії.

Протокол відкритого розподілу ключів (протокол вироблення спільного ключа).

Протокол відкритого розподілу ключів розв'язує наступну задачу: абоненти A та B, які спочатку не володіють жодною секретною інформацією, зрештою таку інформацію (спільний ключ K для використання традиційної криптосистеми) виробляють, а супротивник, який перехоплює усі повідомлення і знає, що хочуть одержати A та B, однак не в змозі відновити ключ K. Протокол виглядає так:

1. Абонент A вибирає велике просте число p та деяке менше за p натуральне число g і відкритими каналами зв'язку посилає p і g абоненту B.

2. A і B вибирають випадковим чином у межах від 1 до $p-1$ числа a і b відповідно.

3. A обчислює $g^a \bmod p$ і посилає отримане значення B, а B обчислює $g^b \bmod p$ і теж посилає A.

4. A і B обчислюють одне і теж число $K = (g^b)^a \bmod p = (g^a)^b \bmod p = g^{ab} \bmod p$, яке і буде спільним ключем.

Що ж може зробити суперник? Перехопивши числа $g^a \bmod p$ і $g^b \bmod p$, він прагне отримати ключ $g^{ab} \bmod p$. Але для цього йому необхідно розв'язати таку задачу: знаючи p, g, r, $s \in \mathbb{N}$, де p – просте число, $1 < g < p-1$, і те, що $r \equiv g^a (\bmod\ p)$, $s \equiv g^b (\bmod\ p)$ для деяких a і b, потрібно знайти $t \equiv g^{ab} (\bmod\ p)$. На даний момент немає більш ефективного алгоритму для розв'язання цієї задачі, ніж алгоритм дискретного логарифмування.

Задача 24.1. *Розробіть протокол вироблення спільного ключа для* а) *трьох*, b) *чотирьох*, c) *n абонентів.*

Протокол цифрового підпису.

Нехай клієнту A банку B треба терміново, повздовж години, оплати вартість цінних паперів, що виставлені для продажу на одній з бірж. Якщо клієнт і банк знаходяться на значній відстані один від одного, то здійснити таку фінансову операцію за короткий час звичайними засобами зв'язку неможливо. Такі операції потрібно проводити електронними засобами. Але тоді не можна використати звичні нам способи засвідчення платіжних документів, такі як підпис особи, яка здійснює операцію, та гербову печатку, яка засвідчує достовірність підпису. Тому при використанні електронних каналів зв'язку банку треба вміти оберігатися від зловмисника, який може від імені його клієнта підписати платіжне доручення. Таку задачу розв'язує протокол цифрового підпису.

Для загального користування вибирають велике просте число p і число g у межах від 1 до $p-1$, яке в мультиплікативній групі Z_p^* має великий порядок. Крім того, кожен клієнт банку вибирає випадковим чином деяке своє натуральне число a, що не перевищує $p-1$, і обчислює $h \equiv g^a (\mathrm{mod}\ p)$. Числа p, g, h становлять відкритий ключ, а число a – таємний. Сам же протокол виглядає таким чином:

1. Кожен клієнт виробляє свій власний підпис x на повідомленні M. Для цього він
   (a) вибирає випадкове число $r \in Z_{p-1}^*$,
   (b) обчислює $x_1 = g^r \bmod p$,
   (c) обчислює $t = r^{-1} \bmod (p-1)$,
   (d) обчислює $x_2 = (M - ax_1)t \bmod (p-1)$ і приймає в якості свого підпису $x = (x_1, x_2)$.
2. Банк B підтверджує підпис клієнта A, перевіряючи, чи $g^M \equiv h^{x_1} x_1^{x_2} (\mathrm{mod}\ p)$.

Перевіримо коректність роботи цього протоколу. Із (c) та (d) матимемо, що $M \equiv ax_1 + rx_2 (\mathrm{mod}\ p-1)$, тобто $M = ax_1 + rx_2 + l(p-1)$ для деякого l. Окрім того, згідно теореми Ойлера $g^{p-1} \equiv 1 (\mathrm{mod}\ p)$. Отже,

$$g^M = g^{ax_1 + rx_2 + l(p-1)} \equiv (g^a)^{x_1} (g^r)^{x_2} = h^{x_1} x_1^{x_2} \ (\mathrm{mod}\ p),$$

і легко бачити, що надійність цього протоколу знову ж таки базується на складності задачі дискретного логарифмування.

Протоколи типу "підкидання монети по телефону".

Припустимо, що два віддалені один від одного абоненти A та B хочуть кинути жереб за допомогою монети (тобто вибрати випадкові числа із множини $\{0,1\}$) так, щоб абонент, який підкидає монету, не зміг змінити результат підкидання після отримання здогаду від абонента, який намагається вгадати цей результат. Відповідна реалізація такого протоколу на базі задачі дискретного логарифмування виглядає так: A і B заздалегідь вибирають велике просте число p і натуральне число g в межах від 1 до $p-1$.

1. Абонент A вибирає випадкове число x у межах від 1 до $p-1$, обчислює $y = g^x \bmod p$ і відправляє y абоненту B.

2. B вибирає випадкові числа $b \in \{0,1\}$ і k у межах від 1 до $p-1$, обчислює $r = y^b g^k \bmod p$ і відправляє r абоненту A.

3. A вибирає випадкове число $c \in \{0,1\}$ і відправляє його B.

4. B надсилає A b та k.

5. A перевіряє, чи виконується конгруенція $r \equiv y^b g^k (\bmod p)$. Якщо так, то результатом виконання протоколу буде число $d = b + c \bmod 2$.

Чи може абонент B, одержавши здогад c від абонента A, відкривати значення b і як 0, і як 1 (за власним бажанням), але так, щоб $y^b g^k \equiv r \pmod p$? B може обманювати, але лише в тому випадку, коли він уміє знаходити $xb + k$, знаючи r, g та те, що $y^b g^k = g^{xb+k} \equiv r (\bmod p)$. Для цього він повинен розв'язати задачу дискретного логарифмування.

Література

[1] Вербіцький О.В. *Вступ до криптології.* — Львів: Вид–во наук.-тех. л-ри, 1998.

[2] Завало С.Т. *Курс алгебри.* — К.: Вища школа, 1985.

[3] Каргаполов М.И., Мерзляков Ю.И. *Основы теории групп.* — М.: Наука, 1982.

[4] Кострикин А.И. *Введение в алгебру. Ч.III.* — М.: Физматлит, 2000.

[5] Сущанський В.І., Сікора В.С. *Операції на групах підстановок. Теорія та застосування.* — Чернівці: Рута, 2003.

[6] Холл М. *Теория групп.* — М.: ИЛ, 1962.

[7] *Введение в криптографию.* Под общей редакцией Ященко В.В. — М.: МЦНМО – ЧеРо, 1999.

Покажчик

група