Міністерство освіти та науки України
Ужгородський національний університет

Тилищак О. А.

ЕЛЕМЕНТИ ТЕОРІЇ ГРУП

Ужгород
Видавництво УжНУ «Говерла»
2009

УДК 512.54

Тилищак О. А.

Елементи теорії груп. – Видавництво УжНУ «Говерла», 2009. – 40 с.

Наведено теоретичний матеріал без доведень з курсу за вибором «Теорія груп» в обсязі передбаченому навчальним планом математичного факультету. Методична розробка містить вправи для самостійного розв'язування з кожної розглянутої теми.

Рецензент: кандидат фізико-математичних наук, доцент *О. А. Кирилюк*

Рекомендовано до друку вченою радою математичного факультету, протокол №4 від 24 грудня 2008 р.

© О. А. Тилищак, 2009

© Видавництво УжНУ «Говерла», 2009

Зміст

Передмова 4
§1. Означення групи. Підгрупи 5
§2. Нормальні підгрупи 10
§3. Гомоморфізми 12
§4. Вільні групи. Визначальні співвідношення 17
§5. Прямі добутки та нормальні ряди 21
§6. Скінченні групи 23
§7. Групи підстановок 27
§8. Нільпотентні групи 31
§9. Розв'язні групи 33
Література 35
Предметний показчик 36
Позначення 39

Передмова

Ця розробка написана на базі лекцій та практичних занять з курсу за вибором «Теорія груп», які проводились автором студентам 3-го курсу спеціалізації алгебра і теорія чисел математичного факультету УжНУ. Мета даної розробки — допомогти студентам в засвоєнні першого розділу абстрактної алгебри — теорії груп, без якого неможливим є вивчення теорії Галуа, теорії зображень скінченних груп, групових алгебр, теорії лінійних груп.

В діючій програмі курсу «Теорія груп» розглядаються основні поняття теорії груп (група, підгрупа, гомоморфізми та ізоморфізми, нормальні підгрупи, фактор-групи, суміжні класи, класи спряжених елементів), автоморфізми груп, вільні групи, нормальні ряди груп, теореми Силова для скінченних груп, групи підстановок, нільпотентні та розв'язні групи. В розробці наведено теоретичний матеріал, що висвітлює весь обсяг курсу «Теорія груп» на рівні означень та формулювань тверджень. Кожний параграф містить вправи для самостійного розв'язування. В кінці розробки приводиться список рекомендованої літератури.

§1. Означення групи. Підгрупи

Нехай M і N — непорожні множини. Множина всіх впорядкованих пар (x, y) $(x \in M,\ y \in N)$ називається *декартовим добутком* множин M і N. Позначається цей добуток символом $M \times N$.

Бінарною алгебраїчною операцією на множині M називається відображення f множини $M \times M$ в множину M. Отже, бінарна алгебраїчна операція f на множині M — це деяке правило, за яким кожній впорядкованій парі (a, b) $(a, b \in M)$ ставиться у відповідність певний елемент $f(a, b)$ з множини M. Будемо $f(a, b)$ позначати так:

$$f(a, b) = a \cdot b = ab.$$

Такий запис операції називають *мультиплікативним*, f — *множенням*, а ab — *добутком* елементів a і b.

Непорожня множина G, на якій задана бінарна алгебраїчна операція множення, називається *групою відносно операції множення*, якщо виконуються умови:

1) алгебраїчна операція асоціативна, тобто для довільних елементів a, b, $c \in G$ справедлива рівність $(ab)c = a(bc)$;
2) існує *одиничний елемент*, тобто існує такий елемент e множини G, що для довільного елемента $a \in G$ справедливі рівності $ae = ea = a$;
3) для всякого елемента $a \in G$ існує *обернений елемент* a^{-1} із множини G, тобто такий елемент, що $aa^{-1} = a^{-1}a = e$.

Ця система аксіом надлишкова. Можна послабити вимоги аксіом 2 та 3 замінивши їх на такі:

$2'$) існує *лівий одиничний елемент*, тобто існує такий елемент e множини G, що для довільного елемента $a \in G$ справедлива рівність $ea = a$;

$3'$) для всякого елемента $a \in G$ існує *лівий обернений елемент* a^{-1} із множини G, тобто такий елемент, що $a^{-1}a = e$.

Нехай задано дві групи, між елементами яких можна встановити взаємно однозначну відповідність. Якщо при цій відповідності результат алгебраїчної операції від любих двох елементів одної групи відповідає результату алгебраїчної операції від відповідних двох елементів іншої групи, то групи називають *ізоморфними*. Ізоморфні групи однаково влаштовані в смислі операції, тому в алгебрі їх не розрізняють або вважають точними копіями одна одної. Таким чином, взаємно однозначне відображення φ групи G на групу G^* називається *ізоморфізмом*, якщо

$$\varphi(ab) = \varphi(a)\varphi(b)\ (a, b \in G).$$

Отже, дві групи G та G^* є ізоморфними, якщо існує ізоморфізм

$$\varphi : \ G \to G^*.$$

Для будь-якої групи G мають місце властивості:

1) G володіє єдиним одиничним елементом;
2) для всякого елемента групи G існує єдиний обернений елемент в цій групі;
3) $(ab)^{-1} = b^{-1}a^{-1}$ для будь-яких елементів a, b групи G;
4) $\left(a^{-1}\right)^{-1} = a$ для будь-якого елемента a групи G.

Нехай G — група, a — деякий елемент групи G. Елемент

$$a^n = \underbrace{a \cdot a \cdots a}_{n \text{ раз}} \qquad (n \in \mathbb{N})$$

називається n-ю *степеню* елемента a. За означенням $a^0 = e$, $a^{-n} = (a^n)^{-1}$ $(n \in \mathbb{N})$. Якщо для довільного натурального числа n $a^n \neq e$, то a називається *елементом нескінченного порядку*. Нехай a — елемент скінченого порядку, n — найменше з натуральних чисел m таких, що $a^m = e$. Тоді число n називають *порядком елемента* a.

Для довільного елемента a та b групи G і цілих чисел m, n мають місце властивості:

1) $a^m a^n = a^{m+n}$;
2) $(a^m)^n = a^{mn}$;
3) $a^n = e$ тоді і тільки тоді, коли n ділиться на порядок елемента a;
4) якщо елементи a та b комутують, тобто $ab = ba$, і їх порядки взаємно прості, то порядок елемента ab рівний добутку порядків елементів a та b.

Група, всі елементи якої, окрім одиничного, є нескінченного порядку, називається *групою без скруту*. Група G називається *періодичною*, якщо кожен її елемент є елементом скінченного порядку. Якщо порядки елементів групи обмежені в сукупності, то їх найменше спільне кратне називають *показником групи*. Нехай p — просте число. Періодична група, порядок будь-якого елемента якої є степеню числа p, називається *p-групою*. Потужність множини G називається *порядком* групи G і позначається $|G|$. Якщо це число скінченне, то група G називається *скінченною*, в іншому випадку група G називається *нескінченною*. Група, яка складається з одного одиничного елемента, називається *тривіальною*. Якщо операція в групі G *комутативна*, тобто $ab = ba$ для довільних елементів a, b групи G, то група G називається *комутативною* або *абелевою*.

Часто комутативну операцію записують *адитивно* і тоді змінюються термінологія та позначення.

$\cdot$	$+$
множення	додавання
добуток	сума
одиниця	нуль
обернений	протилежний
степінь	кратне
e або 1	0
a^{-1}	$-a$
a^n	na

Множина елементів довільного кільця K розглядувана відносно операції додавання є групою, яку називають *адитивною групою кільця* K і позначається K^+. Множина оборотних елементів кільця K з одиницею розглядувана відносно операції множення утворює *мультиплікативну групою кільця* K і позначається K^*.

Часто операцію в скінченній групі задаємо за допомогою *таблиці Келі*. Для цього, якщо група G має скінченний порядок n, нумеруємо її елементи, починаючи з одиниці: $e,\ a_2,\ a_3,\ \ldots,\ a_n$. Утворюємо квадратну таблицю, в якій визначаємо добутки a_ia_j довільних двох елементів a_i та a_j групи G.

	e	a_2	$\ldots$	a_j	$\ldots$	a_n
e	e	a_2	$\ldots$	a_j	$\ldots$	a_n
a_2	a_2	a_2a_2	$\ldots$	a_2a_j	$\ldots$	a_2a_n
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
a_i	a_i	a_ia_2	$\ldots$	a_ia_j	$\ldots$	a_ia_n
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
a_n	a_n	a_na_2	$\ldots$	a_na_j	$\ldots$	a_na_n

Нехай G — група. Підмножина H групи G називається *підгрупою* групи G, якщо відносно алгебраїчної операції, заданої на G, H є групою. Очевидно, $\{e\}$, G є підгрупами групи G. Підгрупу групи G, відмінну від групи G, називають *власною* підгрупою групи G.

Для довільної групи G виконуються властивості.

1) Непорожня підмножина H групи G є підгрупою групи G тоді і тільки тоді, коли для довільних елементів a і b із H виконуються умови:
$$ab \in H, \qquad a^{-1} \in H. \tag{1.1}$$
2) Добуток $A \cdot B = \{ab | a \in A,\ b \in B\}$ підгруп A та B групи G тоді і тільки тоді буде підгрупою групи G, коли $A \cdot B = B \cdot A$.

Легко бачити, що перетин будь-якої не порожньої множини підгруп групи G — підгрупа групи G. Якщо M — довільна непорожня підмножина групи G, то перетин $\langle M\rangle$ всіх підгруп групи G, що містять M, називається підгрупою, *породженою* множиною M, а сама M — *системою твірних елементів* підгрупи $\langle M\rangle$. Підмножина N множини M називається *власною*, якщо $N \neq M$. Система твірних елементів деякої групи називається *незвідною*, якщо жодна її власна підмножина, не є системою твірних елементів цієї групи.

Теорема 1.1. *Якщо M — непорожня підмножина групи G, то*

$\langle M\rangle = \{a_1^{\varepsilon_1}a_2^{\varepsilon_2}\dots a_m^{\varepsilon_m} | a_i \in M;\ \varepsilon_i = \pm 1;\ i = 1, 2, \dots, m;\ m = 0, 1, 2, \dots\}$.

Якщо $m = 0$, то вважаємо, що $a_1^{\varepsilon_1}a_2^{\varepsilon_2}\dots a_m^{\varepsilon_m} = e$. При заданні підгрупи через твірні елементи ми пишемо $\langle M\rangle = \langle \dots | \dots\rangle$, якщо M задано у вигляді $M = \{\dots | \dots\}$.

Підгрупа, породжена скінченною множиною, називається *скінченно породженою*.

Теорема 1.2. *Всяка система твірних елементів скінченно породженої групи містить підмножину, яка є скінченною системою твірних елементів цієї ж групи.*

Підгрупа $\langle a\rangle$, породжена одним елементом a, називається *циклічною*.

За теоремою 1.1 вона складається з степенів твірного елемента:

$$\langle a\rangle = \{a^n | n \in \mathbb{Z}\}.$$

Всяка циклічна група, очевидно, абелева. Група $\langle a\rangle$ скінченна тоді і тільки тоді, коли елемент a є елементом скінченного порядку. В цьому випадку $|\langle a\rangle|$ рівний порядку елемента a.

Циклічна група має такі властивості.

1) Всяка нескінченна циклічна група G ізоморфна адитивній групі цілих чисел $\mathbb{Z}^+$.
2) Всяка циклічна група порядку n ізоморфна мультиплікативній групі U_n комплексних коренів n-го степеня з 1.
3) Всяка підгрупа циклічної групи — циклічна.
4) Всяка підгрупа H скінченної циклічної групи $G = \langle a\rangle$ порядку n породжується елементом a^s, де s — дільник числа n, і є циклічною групою порядку t, причому $n = st$.
5) У циклічної групи скінченного порядку n є стільки підгруп, скільки є дільників у числа n.

Нехай H — підгрупа групи G, a — фіксований елемент групи G. Позначимо через $aH = \{ah \mid h \in H\}$. Множина $aH \subset G$ назива-

ється *лівим суміжним класом* групи G за підгрупою H. Аналогічно множина $Ha = \{ha \mid h \in H\}$ називається *правим суміжним класом* групи G за підгрупою H. Кожен елемент суміжного класу називається *представником* цього класу. Легко перевірити, що для довільної групи G та її підгрупи H

1) два одноймненні (ліві або праві) суміжні класи групи G за підгрупою H або суміщаються або не перетинаються;
2) $aH = bH$ $(a, b \in G)$ тоді і тільки тоді, коли $a^{-1}b \in H$;
3) $Ha = Hb$ $(a, b \in G)$ тоді і тільки тоді, коли $ab^{-1} \in H$;
4) кожен клас aH, Ha $(a \in G)$ рівнопотужний з підгрупою H.

Можна показати, що для довільної групи G та її підгрупи H відповідність $aH \to Ha^{-1}$ $(a \in G)$ є взаємно однозначним відображенням множини лівих суміжних класів групи G за її підгрупою H у множину її правих суміжних класів. Тобто множини лівих та правих суміжних класів групи G за її підгрупою H рівнопотужні. Потужність множини лівих суміжних класів групи G за її підгрупою H називають *індексом* підгрупи H в групі G і позначають $[G : H]$. Якщо це число скінченне, то підгрупа H називається *підгрупою скінченного індекса* в групі G.

Теорема 1.3 (Теорема Лагранжа)**.** *Нехай G — скінченна група, H — підгрупа групи G. Тоді $|G| = [G : H] \cdot |H|$.*

З теореми випливає, що порядок та індекс підгрупи скінченної групи є дільниками порядку групи. Оскільки для довільного елемента a скінченної групи $|\langle a \rangle|$ скінченний і рівний порядку елемента a, то порядок кожного елемента скінченної групи є скінченним і є дільником порядку групи.

Вправи

1. Показати, що множина S_n підстановок n-го степеня утворює групу. Цю групу називають *симетричною групою степеня n*. Задати операцію в симетричній групі S_3 степеня 3 таблицею Келі.
2. Показати, що множина A_n парних підстановок n-го степеня утворює групу. Цю групу називають *знакозмінною групою степеня n*. Вказати одну незвідну систему твірних елементів знакозмінної групи A_4 степеня 4.
3. Вказати по одній системі твірних елементів для груп: $\mathbb{Z}^+$, $\mathbb{Z}^*$, $\mathbb{Q}^+$, $\mathbb{Q}^*$.
4. Довести, що група $\mathbb{Q}^+$ не має незвідних систем твірних.
5. Підстановка n-го степеня називається *транспозицією*, якщо вона не змінює жодного натурального числа $i \leqslant n$, крім k та l $(k \neq l)$, причому

l є образом k а k — образом l. Показати, що симетрична група S_n степеня $n > 1$ породжується всіма транспозиціями.

§2. Нормальні підгрупи

Підгрупа H групи G називається *нормальною підгрупою* (позначають $H \triangleleft G$), якщо для довільного елемента $a \in G$ виконується рівність $aH = Ha$. Ця умова еквівалентна умові: $a^{-1}Ha = H$ $(a \in G)$, де $a^{-1}Ha = \{a^{-1}ha \mid h \in H\}$. Крім того, підгрупа H групи G є її нормальною підгрупою тоді і тільки тоді, коли

$$a^{-1}Ha \subset H \qquad (a \in G). \tag{2.1}$$

Говорять, що в групі G елемент a *спряжений* з елементом b за допомогою елемента x, якщо $a = x^{-1}bx$. Часто використовують степеневі позначення: $x^{-1}bx = b^x$. Легко перевірити, що для довільного цілого числа n та довільних елементів a, b, x, y групи G

1) $(a^x)^y = a^{xy}$;
2) $(ab)^x = a^x b^x$;
3) $e^x = e$;
4) $(a^n)^x = (a^x)^n$;
5) $a^e = a$.

Якщо A, B — дві підмножини групи G, то позначимо

$$A^B = \{a^b | a \in A,\ b \in B\}.$$

Таким чином, підгрупа H групи G тоді і тільки тоді є нормальна в групі G, якщо разом з кожним своїм елементом H містить і всі елементи, які спряжені з ним за допомогою елементів з групи G, або, коротше, якщо $H^G \subset H$. Перетин всіх нормальних підгруп довільної групи, що містять деяку непорожню підмножину N цієї групи, є нормальною підгрупою даної групи, яку називатимемо підгрупою *нормально породженою* множиною N. Зрозуміло, що всякий елемент з підгрупи нормально породженою множиною N може бути записаний у вигляді добутку степенів елементів з N і степенів елементів, які спряжені з елементами множини N.

Нехай $x \in G$. Підмножина $M^x = M^{\{x\}}$ називається *спряженою* з підмножиною M в групі G. Тепер ми можемо казати, що підгрупа тоді і лише тоді нормальна, коли вона суміщається з усіма своїми спряженими. Групи, що не містять власних нетривіальних нормальних підгруп, називаються *простими*.

Нехай G — довільна група. Введемо на ній відношеня $\sim$, покладаючи $a \sim b$, якщо елементи a і b спряжені в групі G. Легко перевіряється, що

$\sim$ — відношення еквівалентності, тобто воно рефлексивне ($a \sim a$), симетричне ($a \sim b \Rightarrow b \sim a$) і транзитивне ($a \sim b$, $b \sim c \Rightarrow a \sim b$). Тому G розбивається на *класи спряжених елементів* $a^G = \{a\}^G$ ($a \in G$), які не перетинаються. Зокрема, нормальними підгрупами групи G будуть такі її підгрупи, які складаються з декількох повних класів спряжених елементів. Нехай M — підмножина, H — підгрупа групи G. *Нормалізатором* множини M в підгрупі H називається множина

$$N_H(M) = \{h | h \in H,\ M^h = M\},$$

яка, як легко перевірити, є підгрупою в H. Нехай $m \in G$, $N_H(\{m\})$ будемо позначати $N_H(m)$. Якщо не вказано, в якій підгрупі H береться нормалізатор, то це означає, що він береться у всій групі G. Очевидно, підгрупа групи G тоді і тільки тоді нормальна в групі G, коли її нормалізатор суміщається зі всією групою G.

Теорема 2.1. *Якщо M — підмножина, H — підгрупа групи G, то потужність класу підмножин, які спряжені з M елементами з H, рівна індексу $[H : N_H(M)]$. Зокрема, потужність класу спряжених елементів a^G ($a \in G$) рівна індексу $[G : N_G(a)]$.*

Нехай G — довільна група. *Добутком* підмножин A і B групи G називається підмножина $A \cdot B = \{xy \mid x \in A, y \in B\}$. Очевидно, для довільних підмножин A, B і C групи G $(A \cdot B) \cdot C = A \cdot (B \cdot C)$. Розглянемо множину всіх суміжних класів групи G за нормальною підгрупою H. Очевидно, добутком двох суміжних класів aH і bH є суміжний клас $(ab)H$:

$$aH \cdot bH = (ab)H. \tag{2.2}$$

Легко перевірити, що множина $\{aH \mid a \in G\}$ з введеною операцією множення (2.2) є групою. Одиничним елементом цієї групи є суміжний клас $eH = H$. Оберненим елементом до суміжного класу aH є суміжний клас $a^{-1}H$. Так визначена група називається *фактор-групою* групи G за підгрупою H і позначається G/H.

Нехай M — підмножина, H — підгрупа групи G. *Централізатором* множини M в підгрупі H називається множина

$$\mathfrak{Z}_H(M) = \{x | x \in H,\ m^x = m \text{ для всіх } m \in M\}.$$

Легко перевірити, що $\mathfrak{Z}_H(M)$ є нормальною підгрупою нормалізатора $N_H(M)$. Якщо M складається з одного елементу a, то, звичайно, його нормалізатор $N_H(a)$ і централізатор $\mathfrak{Z}_H(a) = \mathfrak{Z}_H(\{a\})$ в H суміщаються. Якщо не вказано, в якій підгрупі H береться централізатор, то це означає, що він береться у всій групі G.

Централізатор $\mathfrak{Z}(G)$ всієї групи G називається її *центром*. Очевидно,

група тоді і тільки тоді абелева, коли вона суміщається з своїм центром. Зауважимо, що будь-яка підгрупа центру нормальна в групі. Нехай a — довільний елемент групи G. Очевидно, $a \in \mathfrak{Z}(G)$ тоді і тільки тоді, коли $a^G = \{a\}$, а це виконується тоді і тільки тоді, коли $\mathfrak{Z}(a) = G$.

Теорема 2.2. *Нехай G — група. Якщо фактор-група $G/\mathfrak{Z}(G)$ циклічна, то група G абелева.*

Очевидно, елементи a, b групи G тоді і тільки тоді комутують, коли $a^{-1}b^{-1}ab = e$. Ліва частина цього співвідношення називається *комутатором* елементів a, b — у вказаному порядку — і позначається $[a, b]$. Підгрупа $G' = \langle [a, b] |\, a, b \in G \rangle$, породжена в G всілякими комутаторами, називається *комутантом* групи G. Ясно, що група тоді і тільки тоді абелева, коли її комутант тривіальний. Легко перевірити, що для довільної групи G та її елементів a, b, c

1) $ab = ba[a, b]$;
2) $[a, b]^{-1} = [b, a]$;
3) $[ab, c] = [a, c]^b[b, c]$;
4) $[a^{-1}, b] = [b, a]^{a^{-1}}$.

Нехай G — група, G' — комутант групи G, H — підгупа групи G.

1) Якщо $G' \subset H$, то $H \lhd G$ і G/H абелева.
2) Якщо $H \lhd G$, G/H абелева, то $G' \subset H$.

Вправи

1. Показати, що множина підстановок $K_4 = \{e,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$ є нормальною підгрупою знакозмінної групи A_4 4-го степеня. Цю підгрупу називають *четверною групою Кляйна*.

2. Вияснити, які підгрупи нормально породжуються в симетричній групі S_4 4-го степеня кожною з множин $M_1 = \{(1\ 2),\ (1\ 3\ 2\ 4)\}$, $M_2 = \{e,\ (1\ 2\ 3),\ (1\ 3\ 2)\}$.

3. Нехай H — підгрупа групи G індексу $[G : H] = 2$. Показати, що H нормальна підгрупа групи G.

4. Знайти центр та класи спряжених елементів знакозмінної групи A_4 4-го степеня.

5. Знайти комутант симетричної групи S_n n-го степеня.

§3. Гомоморфізми

Відображення f групи G в групу G^* називається *гомоморфізмом*,

якщо для довільних елементів a і b групи G справедлива рівність $f(ab) = f(a)f(b)$. *Ядром* гомоморфізма $f : G \to G^*$ називається множина

$$\operatorname{Ker} f = \{g \in G | f(g) = e^*\},$$

де e^* — одиничний елемент групи G^*. *Образом* гомоморфізма $f : G \to G^*$ називається множина

$$f(G) = \{f(g) | g \in G\}.$$

При гомоморфізмі $f : G \to G^*$

1) $f(e) = e^*$;
2) $f(a^{-1}) = f(a)^{-1}$ $(a \in G)$;
3) $\operatorname{Ker} f \lhd G$;
4) $f(a) = f(b)$ тоді і тільки тоді, коли $a \operatorname{Ker} f = b \operatorname{Ker} f$ $(a,\ b \in G)$;
5) f — інєктивний тоді і тільки тоді, коли $\operatorname{Ker} f = \{e\}$;
6) для всякої підгрупи H групи G її образ $f(H) = \{f(h) | h \in H\}$ є підгрупою групи G^*.

Гомоморфізм f групи G в групу G^* називається гомоморфізмом G *на* групу G^* або *епіморфізмом*, якщо $f(G) = G^*$, тобто для довільного елемент b групи G^* існує елемент $a \in G$ такий, що $f(a) = b$. Гомоморфізм f групи G в групу G^* називається *мономорфізмом*, якщо для довільних різних елементів a і b групи G $(a \neq b)$ їх образи різні, тобто $f(a) \neq f(b)$. Очевидно, гомоморфізм є ізоморфізмом, якщо він одночасно є епіморфізмом та мономорфізмом. В разі існування ізоморфізму групи G на групу G^* ці групи є ізоморфними, що позначають $G \cong G^*$. Легко перевіряється, що $\cong$ — відношення еквівалентності, тобто воно рефлексивне $(A \cong A)$, симетричне $(A \cong B \Rightarrow B \cong A)$ і транзитивне $(A \cong B,\ B \cong C \Rightarrow A \cong C)$.

Із означення ізоморфізму випливає, що ізоморфні групи рівнопотужні, зокрема, якщо групи скінченні, то складаються з однакового числа елементів. Ізоморфні групи можуть відрізнятися одна від другої тільки природою своїх елементів, можливо, назвою своєї операції і символікою для її позначення. Вони, проте, не розрізняються з точки зору властивостей операцій — все, що може бути доведено для деякої групи на основі властивостей введеної на ній операції, але без використання конкретної природи елементів групи, автоматично переноситься на всі групи ізоморфні з нею. Так, наприклад, група ізоморфна абелевій групі сама абелева.

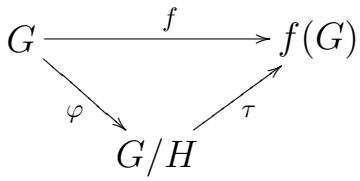
Крім гомоморфізмів, іноді розглядають *антигомоморфізм*, тобто такі відображення f групи G в групу G^*, що для довільних елементів a і b групи G справедлива рівність $f(ab) = f(b)f(a)$. Аналогічно до ізоморфізму

вводиться поняття *антиізоморфізму*. При будь-якому антигомоморфізмі $f : G \to G^*$ виконуються аналогічні умови, що й при гомоморфізмі, зокрема, $f(e) = e^*$, $f(a^{-1}) = f(a)^{-1}$ $(a \in G)$.

Відображення $f : G \to G^*$ визначене за правилом $f(a) = e^*$ є одночасно і гомоморфізмом і антигомоморфізмом групи G в групу G^*, який називають *тривіальним*. Гомоморфізм групи G в групу G називається *ендоморфізмом* групи G, ізоморфізм — *автоморфізмом*.

Виявляється, ядрами гомоморфізмів вичерпуються всі нормальні підгрупи в групі. Дійсно, нехай G — група, H — її нормальна підгрупа, G/H — фактор-група групи G за підгрупою H. Безпосередньо перевіряється, що відображення $\varphi : G \to G/H$, яке задане за правилом $\varphi(g) = gH$, є епіморфізм. Такий епіморфізм називають *природним епіморфізмом*. Очевидно, ядром природного епіморфізму $G \to G/H$ є якраз H.

Теорема 3.1 (Перша теорема про ізоморфізм)**.** *Якщо f — гомоморфізм групи G з ядром H, то $f(G) \cong G/H$. Більш того, гомоморфізм f рівносильний послідовному виконанню природного епіморфізму $\varphi : G \to G/H$, а потім деякого ізоморфізму τ: $G/H \to f(G)$.*



Теорема 3.2 (Друга теорема про ізоморфізм)**.** *Якщо A і B — підгрупи групи G, $A \lhd \langle A, B\rangle$, то $\langle A, B\rangle = A \cdot B$, $A \cap B \lhd B$ і*

$$\langle A, B\rangle / A \cong B / A \cap B.$$

Теорема 3.3 (Третя теорема про ізоморфізм)**.** *Якщо $H \lhd G$, $A \lhd G$ і H — підгрупа групи A, то $A/H \lhd G/H$ і*

$$(G/H)/(A/H) \cong G/A.$$

Якщо G — група, H — її нормальна підгрупа, то позначимо через $L(G, H)$ сукупність всіх підгруп групи G, що містять H. Зокрема, $L(G, \{e\})$ — сукупність всіх підгруп групи G. Справедлива теорема про відповідність підгруп при гомоморфізмі.

Теорема 3.4 (Теорема про відповідність підгруп при гомоморфізмі)**.** *Якщо заданий природний епіморфізм $\varphi : G \to G/H$, то виникає відображення $\psi : L(G, H) \to L(G/H, \{H\})$, яке зіставляє підгрупам з $L(G, H)$ їх образи відносно φ. Відображення ψ є взаємно однозначним відображенням. Якщо A, B — підгрупи з $L(G, H)$, то вони спряжені в G тоді і тільки тоді, коли їх образи $\overline{A}$, $\overline{B}$ спряжені в G/H. Зокрема,*

A нормальна в G тоді і тільки тоді, коли $\overline{A}$ нормальна в G/H.

Теорема 3.5 (Теорема Келі)**.** *Нехай G — скінченна група порядку n. Тоді група G ізоморфна деякій підгрупі симетричної групи S_n n-го степеня.*

Добутком $\varphi\psi$ відображень φ та ψ групи G в себе називається відображення, що полягає в послідовному виконанні спочатку ψ а потім φ. Тобто, $\varphi\psi(g) = \varphi(\psi(g))$ для будь-якого елемента g групи G. Позначимо множину всіх автоморфізмів групи G через $\operatorname{Aut} G$. Множина $\operatorname{Aut} G$ перетворюється в групу відносно множення відображень, яку називають *групою автоморфізмів* групи G.

Для будь-якого елемента a групи G відображення $I_a : G \to G$, яке задане за правилом $I_a(g) = g^a$, є автоморфізмом групи G, який називають *внутрішнім автоморфізмом* групи G, породженим елементом a. Легко перевірити, що для довільних $a,\ b \in G$, $\varphi \in \operatorname{Aut} G$

1) $I_a I_b = I_{ba}$;
2) $I_{a^{-1}} = {I_a}^{-1}$;
3) $\varphi^{-1} I_a \varphi = I_{\varphi^{-1}(a)}$.

Звідси випливає, що множина $\operatorname{Inn} G$ всіх внутрішніх автоморфізмів групи G є нормальною підгрупою групи $\operatorname{Aut} G$, яку називають *групою внутрішніх автоморфізмів* групи G: $\operatorname{Inn} G \lhd \operatorname{Aut} G$. Автоморфізм групи G, який не є внутрішнім, називають *зовнішнім*, а групу

$$\operatorname{Out} = \operatorname{Aut} G / \operatorname{Inn} G$$

називають *групою зовнішніх автоморфізмів*. Очевидно, для абелевої групи G група $\operatorname{Out} G$ та $\operatorname{Aut} G$ суміщаються.

Властивість 1) показує, що відображення $G \to \operatorname{Inn} G$, що ставить кожному елементу g групи G внутрішній автоморфізм I_g групи G, є антигомоморфізмом. Ядро цього антигомоморфізму складається з тих елементів g групи G, для яких $x^g = x,\ x \in G$, тобто суміщається з центром $\mathfrak{Z}(G)$ групи G. Звідси одержимо, що групи $\operatorname{Inn} G$ та $G/\mathfrak{Z}(G)$ антиізоморфні.

Нехай α — відображення множини M у множину L, N — деяка підмножина множини M. Розглянувши дію відображення α тільки на елементах множини N, одержимо відображення $\alpha|_N$ множини N у множину L, яке називають *звуженням* відображення α на множину N.

Множина $S(G)$ всіх взаємно однозначних відображень групи G на себе відносно множення відображень буде, очевидно, групою. Ми одержимо також мономорфне відображення групи G в групу $S(G)$, якщо кожно-

му елементу a цієї групи поставимо у відповідність відображення $\overline{a}$, що переводить всякий елемент x групи G в елемент ax. Підгрупа $\overline{G}$ групи $S(G)$, на яку група G цим шляхом ізоморфно відобразиться, може вважатися тотожною з самою групою G. Нормалізатор $\operatorname{Hol} G$ підгрупи G в групі $S(G)$ називається *голоморфом* групи G.

З визначення нормалізатора випливає, що група $\operatorname{Hol} G$ містить G як нормальну підгрупу. Можна показати, що всі автоморфізми групи G є звуженнями внутрішніх автоморфізмів групи $\operatorname{Hol} G$.

Група називається *досконалою*, якщо вона без центру і всякий її автоморфізм є внутрішнім. Досконала група антиізоморфна, отже, з групою всіх своїх автоморфізмів.

Теорема 3.6 (Теорема Гельдера)**.** *Симетрична група S_n степеня $n > 3$ і $n \neq 6$ є досконалою.*

Нехай дано групи A і B і кожному елементу $a \in A$ відповідає автоморфізм φ_a групи B, так, що відповідність $a \to \varphi_a$ є антигомоморфізмом групи A в групу $\operatorname{Aut} B$. Множина

$$A \ltimes B = \{(a, b) \mid a \in A, b \in B\}$$

відносно операції

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, \varphi_{a_2}(b_1) b_2)$$

утворює групу, яку називають *напівпрямим добутком* групи A на групу B.

Теорема 3.7. *Група G ізоморфна напівпрямому добутку своєї підгрупи A на свою підгрупу B, якщо виконуються такі умови:*

1) $B \lhd G$;
2) $G = A \cdot B$;
3) $A \cap B = \{e\}$.

Вправи

1. Нехай C_n — абстрактна циклічна група порядку n. Зобразити групу $C_5 = \langle a \rangle$ як групу підстановок.
2. Довести, що $\operatorname{Aut}(K_4) \cong S_3$.
3. Описати групу $\operatorname{Aut}(C_{10})$.
4. Довести, що $\operatorname{Hol} G \cong \operatorname{Aut} G \ltimes G$.
5. Довести, що

$$\operatorname{Hol} \mathbb{Z}^+ \cong \left\{ \begin{pmatrix} 1 & \beta \\ 0 & \alpha \end{pmatrix} \middle| \, \alpha \in \mathbb{Z}^*, \ \beta \in \mathbb{Z} \right\}.$$

§4. Вільні групи. Визначальні співвідношення

Нехай дана деяка непорожня множина $\mathfrak{M}$ символів x_α, x_β, x_γ, ... Домовимося позначати ці символи також через x_α^{+1}, x_β^{+1}, x_γ^{+1}, ... і вважатимемо, що цим символам взаємно однозначно відповідають деякі нові символи x_α^{-1}, x_β^{-1}, x_γ^{-1}, ... Вираз

$$w = x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \dots x_{\alpha_n}^{\varepsilon_n} \ (\varepsilon_i = \pm 1,\ i = 1, 2, \dots, n), \tag{4.1}$$

тобто впорядкована система з скінченного числа символів вигляду x_α^{+1} і x_β^{-1} (кожний з символів, що входять у вираз (4.1), може зустрічатися в ньому кілька разів), називатиметься *словом*, якщо ніде в (4.1) не зустрічаються поряд який-небудь символ x_α^{+1} і відповідний йому символ x_α^{-1}. Число n називається *довжиною* слова w і позначається через $l(w)$. При будь-якій непорожній множині $\mathfrak{M}$ можна утворити, очевидно, слова будь-якої довжини. Словами довжини 1 будуть самі символи x_α і x_α^{-1}, і лише вони. До числа слів ми приєднуємо також *порожнє слово* w_0, що не містить жодного символу; $l(w_0) = 0$. Множина всіх слів, які можуть бути записані за допомогою нашого запасу символів, стає групою, якщо так визначити операцію: якщо дані слова

$$w_1 = x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \dots x_{\alpha_n}^{\varepsilon_n} \ (\varepsilon_i = \pm 1,\ i = 1, 2, \dots, n), \tag{4.2}$$

$$w_2 = x_{\beta_1}^{\delta_1} x_{\beta_2}^{\delta_2} \dots x_{\beta_m}^{\delta_m} \ (\delta_j = \pm 1,\ j = 1, 2, \dots, m)$$

і рівності

$$\alpha_{n-i+1} = \beta_i \text{ і } \varepsilon_{n-i+1} + \delta_i = 0,$$

які виконуються для всіх i, $1 \leqslant i \leqslant k$, де k задовольняє умові $0 \leqslant k \leqslant \min(n, m)$, але при $k < \min(n, m)$ або $\alpha_{n-k} \neq \beta_{k+1}$, або ж, при $\alpha_{n-k} = \beta_{k+1}$ має місце рівність $\varepsilon_{n-k} = \delta_{k+1}$, то покладемо

$$w_1 w_2 = x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \dots x_{\alpha_{n-k}}^{\varepsilon_n - k} x_{\beta_{k+1}}^{\delta_{k+1}} x_{\beta_{k+2}}^{\delta_{k+2}} \dots x_{\beta_m}^{\delta_m}.$$

іншими словами, для отримання добутку $w_1 w_2$ потрібно слово w_2 написати безпосередньо за словом w_1; якщо одержаний таким шляхом вираз

$$w_1 w_2 = x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \dots x_{\alpha_n}^{\varepsilon_n} x_{\beta_1}^{\delta_1} x_{\beta_2}^{\delta_2} \dots x_{\beta_m}^{\delta_m}. \tag{4.3}$$

буде словом, тобто якщо символи x_{α_n} і x_{β_1} або різні, або ж однакові, але володіють в цьому випадку однаковими показниками, то добуток $w_1 w_2$ одержаний. Інакше необхідно виконати у виразі (4.3) декілька *скорочень*, тобто послідовно видалити пари, що стоять поруч, однакових символів з протилежними показниками. Зрозуміло, що при виконанні цих скорочень символи, що становлять один з множників w_1, w_2 або навіть обидва, можуть випадково виявитися повністю знищеними.

Роль одиниці при такому визначенні множення слів грає, очевидно,

порожнє слово w_0. Оберненим для слова (4.2) буде слово

$$w_1^{-1} = x_{\alpha_n}^{-\varepsilon_n} \dots x_{\alpha_2}^{-\varepsilon_2} x_{\alpha_1}^{-\varepsilon_1}.$$

Зокрема, оберненим до символа x_α буде символ x_α^{-1}.

Група слів, складених з символів, що входять в множину $\mathfrak{M}$, і символів, до них обернених називається *вільною групою*, яка вільно породжена множиною $\mathfrak{M}$. Вона цілком визначається, очевидно, заданням потужності множини $\mathfrak{M}$ і не залежить ні від яких індивідуальних властивостей елементів цієї множини. Назвемо *рангом* вільної групи, побудованої за допомогою множини $\mathfrak{M}$, потужність цієї множини (тобто число його елементів, якщо це число скінченне).

Легко перевірити, що для довільної вільної групи мають місце властивості.

1) Вільна група рангу 1 буде нескінченною циклічною групою.
2) Всяка вільна група, ранг якої більше одиниці, некомутативна.
3) Всі елементи вільної групи, окрім одиниці, мають нескінченний порядок.

Нехай дана довільна група G і M є деяка система твірних для цієї групи; елементи з M позначатимемо через a_α, a_β, a_γ, ... Розглянемо вільну групу W, система вільних твірних $\mathfrak{M}$ якої має таку ж потужність, як множина M. Між елементами з M і узятими нами вільними твірними групи W встановлюємо взаємно однозначну відповідність, причому твірний елемент групи W, що відповідає елементу a_α з M, домовимося позначати через x_α. Відображення, що переводить елемент x_α, з W у відповідний йому елемент a_α з G і взагалі елемент

$$w = x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \dots x_{\alpha_n}^{\varepsilon_n} \ (\varepsilon_i = \pm 1,\ i = 1, 2, \dots, n) \tag{4.4}$$

у елемент групи G, що рівний добутку

$$\overline{w} = a_{\alpha_1}^{\varepsilon_1} a_{\alpha_2}^{\varepsilon_2} \dots a_{\alpha_n}^{\varepsilon_n}, \tag{4.5}$$

буде гомоморфним відображенням групи W на всю групу G. Звідси, за теоремою про гомоморфізми, випливає, що $G \cong W/H$ для деякої нормальної підгрупи H групи W. Отже, має місце теорема.

Теорема 4.1. *Всяка група ізоморфна фактор-групі деякої вільної групи.*

Зауважимо, що нормальна підгрупа H групи W складений з тих і лише тих слів вигляду (4.4), відповідні яким добутки (4.5) рівні в групі G одиниці. Отже, всяка група з скінченним числом твірних є фактор-групою вільної групи скінченного рангу. Точніше, всяка група з n твірними є фактор-група вільної групи рангу n. Нехай дана довільна група

G, яка подана у вигляді фактор-групи деякої вільної групи W за нормальною підгрупою H. Знову, якщо x_α, x_β, x_γ, ... — вільні твірні групи W, то відповідні їм при природному гомоморфізмі елементи з G позначатимемо через a_α, a_β, a_γ, ... а множина всіх цих елементів (серед яких можуть виявитися, звичайно, і рівні) — через M. Нехай слово

$$x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \dots x_{\alpha_n}^{\varepsilon_n},\ (\varepsilon_i = \pm 1,\ i = 1, 2, \dots, n),$$

є довільний елемент з H. Йому відповідає в групі G рівність

$$a_{\alpha_1}^{\varepsilon_1} a_{\alpha_2}^{\varepsilon_2} \dots a_{\alpha_n}^{\varepsilon_n} = 1,$$

яку називатимемо *співвідношенням*, що зв'язує в групі G елементи множини M.

Вибираємо в H таку підмножину $\mathfrak{N}$, що підгрупа нормально породжена в групі W цією підмножиною, суміщається з H. Система співвідношень, що відповідають словам, що входять в $\mathfrak{N}$, називається *системою визначальних співвідношень* групи G. Всі співвідношення, що зв'язують в групі G елементи з M, можуть вважатися наслідками визначальних співвідношень, оскільки всякий елемент з H може бути записаний у вигляді добутку степенів елементів з $\mathfrak{N}$ і степенів елементів, які спряжені з елементами множини $\mathfrak{N}$.

Рівність

$$G = \langle M | \{\overline{w} = e | w \in \mathfrak{N}\}\rangle$$

називають *визначенням групи через твірні елементи та визначальні співвідношення*. При такому визначені часто співвідношення записують у вигляді $a = b$, яке замінює співвідношення $ab^{-1} = e$ чи співвідношення $b^{-1}a = e$. Зауважимо, що для довільних елементів a та b групи G існують спряжені в групі W прообрази елементів ab^{-1} та $b^{-1}a$ при гомоморфізмі $w \to \overline{w}$, отже, вони одночасно лежать в нормальній підгрупі $\mathfrak{N}$ або одночасно не лежать в ній.

Теорема 4.2 (Теорема Діка)**.** *Якщо група G задається деякою системою визначальних співвідношень, а група G^* задається щодо тих же символів крім цих співвідношень ще деякими іншими, то група G^* ізоморфна фактор-групі групи G.*

Нехай H — підгрупа довільної групи G. Зафіксуємо в кожному правому суміжному класі групи G за підгрупою H по представнику. Для підгрупи H вибираємо представником e. Відображення групи G у групу G, яке будь-якому елементу правого суміжного класу uH ставить у відповідність один і той же фіксований представник цього класу $\overline{u}$ і, крім того, $\overline{e} = e$, називається *правою вибираючою функцією* групи G за під-

групою H. Безпосередньо перевіряються властивості цієї функції:

1) $\overline{\overline{u}} = \overline{u}$ $(u \in G)$;
2) $\overline{u\overline{v}} = \overline{uv}$ $(u,\ v \in G)$.

Теорема 4.3. *Нехай групи G породжується множиною M, H — підгрупа групи G і $u \to \overline{u}$ — функція, що вибирає праві представники групи G за підгрупою H, S — множина вибраних представників. Тоді* $H = \langle sx\overline{sx}^{-1} | s \in S, x \in M \rangle$.

Наслідок 4.1. *Підгрупа скінченного індексу в скінченно породженій групі сама скінченно породжена.*

Нехай вільна група породжена непорожньою множиною $\mathfrak{M}$. Слово

$$w = x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \dots x_{\alpha_k}^{\varepsilon_k}$$

називають *початковим відрізком* слова

$$w = x_{\alpha_1}^{\varepsilon_1} x_{\alpha_2}^{\varepsilon_2} \dots x_{\alpha_k}^{\varepsilon_k} \dots x_{\alpha_n}^{\varepsilon_n},$$

де $\alpha_i \in \mathfrak{M}$, $\varepsilon_i = \pm 1$ $(i = 1, 2, \dots, n)$, $0 \leq k < n$. Множина слів вільної групи називається *шраєрівською системою*, якщо з кожним словом вона містить всі його початкові відрізки.

Теорема 4.4 (Теорема Нільсена — Шраєра)**.** *Нехай $\mathfrak{M}$ — довільна непорожня множина символів, H — довільна нетривіальна підгрупа вільної групи F вільно породженої множиною $\mathfrak{M}$. Існує принаймні одна шраєрівська система представників групи F за підгрупою H. Якщо $u \to \overline{u}$ — відповідна їй вибираюча функція, то H вільно породжується неодиничними елементами $sx\overline{sx}^{-1}$, де s пробігає множину вибраних представників, а x пробігає $\mathfrak{M}$.*

Вправи

1. Задати знакозмінну групу A_4 степеня 4 через твірні елементи і визначальні співвідношення.

2. Переконатися, що множина ортогональних перетворень площини, які дану плоску фігуру F переводять у себе утворює групу, яку називають *групою самосуміщень фігури F*. Задати групу самосуміщень ромба, що не є квадратом, через твірні елементи і визначальні співвідношення.

3. Переконатися, що множина Q_8 квадратних матриць: $\pm E$, $\pm I$, $\pm J$, $\pm K$ порядку 2 з комплексними елементами, де

$$I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

$K = IJ$, E — одинична матриця другого порядку, утворює групу відносно множення матриць. Її називають *групою кватерніонів*. Задати Q_8 через твірні елементи і визначальні співвідношення.

4. Нехай натуральне число $n > 2$. Довести, що *група діедра* $D_{2n} = \langle a,\ b \mid a^n = b^2 = e,\ b^{-1}ab = a^{-1}\rangle$ має порядок $2n$ і ізоморфна групі самосуміщень правильного n-кутника.

5. Знайти центр та класи спряжених елементів групи діедра $D_8 = \langle a,\ b \mid a^4 = b^2 = e,\ b^{-1}ab = a^{-1}\rangle$ 8-го порядку.

§5. Прямі добутки та нормальні ряди

Теорія груп має на озброєнні різноманітні конструкції, що генерує із заданих груп нові групи. Одна з найпростіших, але важливих конструкцій полягає в такому. Нехай $G_1, G_2, \ldots, G_m$ — групи. Легко перевірити, що множина $G = G_1 \times G_2 \times \cdots \times G_m$ всіх послідовностей $(g_1, g_2, \ldots, g_m)$, $g_\alpha \in G_\alpha$, з покомпонентним множенням

$$(g_1, g_2, \ldots, g_m) \cdot (g_1', g_2', \ldots, g_m') = (g_1 g_1', g_2 g_2', \ldots, g_m g_m')$$

є групою. Її називають *декартовим добутком груп* G_α, а самі G_α — його *множниками*. Це поняття легке поширюється на випадок довільної сукупності множників G_α, $\alpha \in I$. А саме, позначимо через

$$G = \overline{\prod_{\alpha \in I}} G_\alpha$$

множину функцій

$$f : I \to \bigcup_{\alpha \in I} G_\alpha$$

при умові, що $f(\alpha) \in G_\alpha$ для будь-якого $\alpha \in I$. Легко перевірити, що множина G з множенням за правилом $(fg)(\alpha) = f(\alpha)g(\alpha)$ є групою; вона і називається *декартовим добутком* груп G_α. Значення функції f у точці α називається *проекцією* або *компонентою* елемента f в множнику G_α. Множина

$$\operatorname{supp}(f) = \{\alpha | \alpha \in I,\ f(\alpha) \neq e\}$$

називається *носієм* або *супортом* функції f.

Ясно, що множина функцій з скінченними носіями з декартового добутку груп G_α сама є групою відносно множення функцій. Ця група називається *прямим добутком* груп G_α і позначається через

$$\prod_{\alpha \in I} G_\alpha.$$

Очевидно, для скінченного числа множників прямий і декартовий добуток суміщаються.

Якщо антигомоморфізм групи A в групу автоморфізмів групи B, який визначає напівпрямий добуток $A \ltimes B$ групи A на групу B, є тривіальним, то напівпрямий добуток групи $A \ltimes B$ є прямим.

Теорема 5.1. *Група G ізоморфна прямому добутку своїх підгруп A та B, якщо виконуються такі умови:*

1) $A,\ B \lhd G$;
2) $G = A \cdot B$;
3) $A \cap B = \{e\}$.

При адитивному записі групової операції замість добутків говорять про суми, замість множників — про доданки і пишуть:

$$G = G_1 \oplus G_2 \oplus \cdots \oplus G_m,\ G = \overline{\sum_{\alpha \in I}} G_\alpha,\ G = \sum_{\alpha \in I} G_\alpha.$$

Ланцюжок

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \ldots \subset G_n = G \tag{5.1}$$

вкладених один в одного нормальних підгруп групи G називають *нормальним* рядом групи G. Наприклад, будь-який ланцюжок вкладених один в одного підгруп абелевої групи буде в ній нормальним рядом. Ряд (5.1) називається *субнормальним*, якщо виконується слабкіша умова: кожен його член крім останнього є нормальна підгрупа наступного члена, тобто $G_{i-1} \lhd G_i$ для $i = 1, 2, \ldots, n$. Члени субнормальних рядів називаються *субнормальними підгрупами* (якщо підгрупа H субнормальна в G, то пишуть $H \lhd\lhd G$). Фактор-групи G_i/G_{i-1} називаються *факторами*, а число n — *довжиною* ряду (5.1). Очевидно, тільки тривіальна група володіє нормальним (субнормальним) рядом довжини 0.

Говорять, що група G є *розширенням* групи A за допомогою групи B, якщо в G існує така нормальна підгрупа H, що $H \cong A$, $G/H \cong B$. У цьому значенні фактори субнормального ряду — це ті будівельні блоки, з яких шляхом послідовних розширень можна зібрати всю групу. Якщо група $G = A \ltimes B$, то $G/B = A \cdot B/B \cong B/A \cap B = A/\{e\} \cong A$. Отже, група $A \ltimes B$ є розширенням групи B за допомогою групи A.

Субнормальний ряд з циклічними факторами називається *поліциклічним*, а група з таким рядом — *поліциклічною* групою. Підгрупи і фактор-групи поліциклічної групи — поліциклічні.

Встановити зв'язки між факторами субнормальних рядів дозволяє лема Цасенхауза:

Теорема 5.2 (Лема Цасенхауза)**.** *Якщо в групі G дані підгрупи A, A^*, B і B^* і $A^* \lhd A$, $B^* \lhd B$, то $A^*(A \cap B^*) \lhd A^*(A \cap B)$, $B^*(B \cap A^*) \lhd B^*(B \cap A)$,*

а відповідні фактор-групи ізоморфні:

$$A^*(A \cap B)/A^*(A \cap B^*) \cong B^*(B \cap A)/B^*(B \cap A^*).$$

Два субнормальні (нормальні) ряди групи називаються *ізоморфними*, якщо вони мають однакову довжину і між їх факторами існує взаємно однозначна відповідність, при якій відповідні фактори ізоморфні. Якщо один з субнормальних (нормальних) рядів містить всі члени іншого враховуючи число входжень одного і того ж члена, то перший ряд називається *ущільненням* другого.

Теорема 5.3 (Теорема Шрайера про ряди)**.** *Будь-які два субнормальні (нормальні) ряди групи володіють ізоморфними субнормальними (нормальними) ущільненнями.*

Субнормальний (нормальний) ряд групи без повторення членів називається *композиційним* (*головним*), якщо його не можна ущільнити без повторення членів.

Теорема 5.4. *Субнормальний ряд групи є композиційним тоді і тільки тоді, коли його фактори є нетривіальними простими групами.*

Теорема 5.5 (Теорема Жордана — Гельдера)**.** *Будь-які два композиційні (головні) ряди ізоморфні.*

Вправи

1. Нехай A, B — групи. Показати, що $(A \times B)' = A' \times B'$, $\mathfrak{Z}(A \times B) = \mathfrak{Z}(A) \times \mathfrak{Z}(B)$.

2. Показати, що група G ізоморфна прямому добутку своїх підгруп G_1, G_2, ..., G_n , якщо виконуються такі умови:

1) $G_i \lhd G$ $(i = 1, 2, \ldots, n)$;
2) $G = G_1 \cdot G_2 \ldots G_n$;
3) $(G_1 \cdot G_2 \ldots G_i) \cap G_{i+1} = \{e\}$ $(i = 1, 2, \ldots, n-1)$.

3. Доведіть, що кожна група G порядку p^2, де p — просте число, або циклічна, або ізоморфна прямому добутку $C_p \times C_p$ двох циклічних груп порядку p.

4. Нехай H підгрупа симетричної групи S_4 4-го степеня, $H = \langle (1\,2)(3\,4) \rangle$. Показати, що $H \lhd\lhd S_4$.

5. Показати, що група група діедра $D_{2n} = \langle a,\ b \mid a^n = b^2 = e,\ b^{-1}ab = a^{-1} \rangle$ порядку $2n$ $(n > 2)$ поліциклічна.

§6. Скінченні групи

Кажуть, що група G діє на множині M, якщо для довільного елемента

$g \in G$ визначене відображення $g: M \to M$ таке, що

1) $e(m) = m$ $(m \in M)$;
2) $g_1 g_2(m) = g_1(g_2(m))$ $(g_1, g_2 \in G,\ m \in M)$
   або
2′) $g_1 g_2(m) = g_2(g_1(m))$ $(g_1, g_2 \in G,\ m \in M)$.

Множина $G(m) = \{g(m) | g \in G\}$ називається *G-орбітою* елементу m. Множина $\mathrm{St}(m) = \{g \in G | g(m) = m\}$ називається *стабілізатором* елемента m в групі G. Легко перевірити такі властивості цих множин.

1) G-орбіти будь-яких двох елементів з M або суміщаються, або не перетинаються.
2) Стабілізатор довільного елемента з M є підгрупою групи G.
3) Потужність G-орбіти будь-якого елемента m множини M рівна індексу $[G : \mathrm{St}(m)]$ стабілізатора цього елемента в групі G.

Таким чином, множину M можна подати у вигляді

$$M = \bigcup_{i \in I} G(m_i) \quad (G(m_i) \text{ попарно не перетинаються}),$$

де I — деяка множина символів і m_i — елементи різних орбіт. Для числа n елементів скінченної множини M одержимо *формулу орбіт*:

$$n = \sum_{i \in I} [G : \mathrm{St}(m_i)].$$

Теорема 6.1 (Теорема Силова про існування)**.** *Нехай G — скінченна група, p — просте число. Для кожного числа p^α, що ділить порядок групи G, в G існує підгрупа порядку p^α.*

Наслідок 6.1. *Нехай p — просте число. Скінченна група G є p-групою тоді і тільки тоді, коли $|G| = p^r$ для деякого цілого r.*

Нехай τ — деяка властивість підгруп групи G. Підгрупа H група G називається *максимальною підгрупою* з властивістю τ, якщо H не міститься в жодній іншій підгрупі з властивістю τ. Зауважимо, що група взагалі кажучи може володіти не одною максимальною підгрупою з властивістю τ або не володіти жодною, навіть при існуванні підгрупою з властивістю τ.

Теорема 6.2 (Теорема Силова про вкладення)**.** *Нехай G — скінченна група, p — просте число. Якщо $p^{\alpha+1}$ ділить порядок групи G, то кожна підгрупа порядку p^α групи G є нормальною підгрупою деякої підгрупи порядку $p^{\alpha+1}$ групи G. Зокрема, максимальні p-підгрупи групи G — підгрупи порядку p^r, де p^r — максимальний степінь p, що ділить порядок групи G.*

Максимальна p-підгрупа групи G називається *силовською p-підгрупою* групи G.

Теорема 6.3 (Теорема Силова про спряженість)**.** *Нехай G — скінченна група, p — просте число. Всі силовські p-підгрупи групи G спряжені в G.*

Наслідок 6.2. *Нехай G — скінченна група, p — просте число, P — силовська p-підгрупа групи G. P — єдина силовська p-підгрупа свого нормалізатора $N(P)$.*

$$N(N(P)) = N(P).$$

Теорема 6.4 (Теорема Силова про кількість)**.** *Нехай G — скінченна група, p — просте число. Кількість силовських p-підгрупа групи G конгруентна 1 за модулем p і ділить порядок групи G.*

Нехай p, q — прості числа, $p < q$, G — скінченна група порядку pq. Силовські p- і q-підгрупи в групі G, будучи підгрупами простого порядку, є циклічними. Нехай $\langle a\rangle$, $\langle b\rangle$ — відповідно силовські p- і q-підгрупи. За теоремою Силова число силовських q-підгруп в G має вигляд $1 + kq$ і ділить p, тому силовська q-підгрупа $\langle b\rangle$ єдина. Зокрема, вона нормальна в G. Число силовських p-підгруп має вигляд $1+lp$ і ділить q, тому можливі два випадки.

a) Силовська p-підгрупа $\langle a\rangle$ єдина. Тоді вона нормальна і, отже, $[a, b] \in \in \langle a\rangle \cap \langle b\rangle = e$. Таким чином, в цьому випадку $G = \langle a\rangle \times \langle b\rangle = \langle ab\rangle$ — циклічна група.

b) Є q максимальних p-підгруп. Звичайно, це можливо лише за умови $q \equiv 1 \pmod p$. Нехай $b^a = b^r$. Якщо $r = 1$, то знову $G = \langle ab\rangle$ — циклічна група. Нехай $r \neq 1$. Індукцією за x одержуємо $b^{a^x} = b^{r^x}$, звідки

$$b^{ya^x} = b^{r^x y}$$

для всіх цілих x, y. При $x = p$, $y = 1$ це дає $r^p \equiv 1 \pmod q$, крім того, одержуємо формулу множення

$$a^x b^y \cdot a^z b^t = a^{x+z} b^{yr^z+t}, \tag{6.1}$$

де x, y, z, t — довільні цілі числа. Навпаки, легко перевірити, що якщо $q \equiv 1 \pmod p$, $r^p \equiv 1 \pmod q$, $r \not\equiv 1 \pmod q$, то формула (6.1) множення визначає неабелеву групу порядку pq, яка породжена елементами a, b. Нарешті, роз'вязки конгруенції $r^p \equiv 1 \pmod q$ складають циклічну групу порядку p, тому ті з них, які відмінні від $1 + q\mathbb{Z}$, мають вигляд $r + q\mathbb{Z}$, $r^2 + q\mathbb{Z}$, $\ldots$, $r^{p-1} + q\mathbb{Z}$, де $r + q\mathbb{Z}$ — один з таких розв'язків. Всі ці розв'язки визначають одну і ту ж групу,

оскільки заміна твірного a на a^j $(j = 1, 2, \ldots, p-1)$ веде до заміни r на r^j.

Таким чином, за допомогою теорем Силова ми описали всі можливі типи груп порядку pq; їх виявилося дві – абелева:

$$G = \langle a,\ b \mid a^p = b^q = e,\ ab = ba \rangle$$

і неабелева:

$$G = \langle a,\ b \mid a^p = b^q = e,\ a^{-1}ba = b^r \rangle,$$

де $r \in \mathbb{Z}$, $r^p \equiv 1 \pmod{q}$, $r \not\equiv 1 \pmod{q}$, при цім друга існує тільки за умови $q \equiv 1 \pmod{p}$.

Теорема 6.5. *Всяка скінченна нетривіальна p-група містить нетривіальний центр.*

Наслідок 6.3. *Всяка скінченна p-група порядку p^2 абелева.*

Нехай G — неабелева група порядку 8. Група G не містить елемент порядку 8, оскільки, інакше, вона була б циклічною. Якщо всі її елементи порядку 2, то $ba = a^2bab^2 = a(ab)^2b = ab$, і група G абелева. Тому група G володіє елементом порядку 4. Нехай, наприклад, a — елемент 4-го порядку. Якщо $b \notin \langle a \rangle = A$, тоді $G = A \cup bA$ і $b^2 \in A$. Якщо $b^2 = a$ або $b^2 = a^3$, то b — елемент порядку 8 і G — циклічна група. Отже, $b^2 = e$ або $b^2 = a^2$. Оскільки $A \lhd G$, то $a^b \in A$ а оскільки a^b — елемент порядку 4, то $a^b = a$ або $a^b = a^3$. Але при $a^b = a$, G — абелева група. Тому $a^b = a^3$. Отже, ми знайшли дві неабелеві групи: групу діедра:

$$D_8 = \langle a,\ b \mid a^4 = b^2 = e,\ b^{-1}ab = a^3 \rangle$$

і групу кватерніонів:

$$Q_8 = \langle a,\ b \mid a^4 = e,\ b^2 = a^2,\ b^{-1}ab = a^3 \rangle.$$

Легко перевірити, що обидві системи твірних елементів та визначальних співвідношень дійсно визначають дві групи порядка 8, неізоморфні одна одній.

Вправи

1. Знайти центр групи кватерніонів Q_8.
2. Знайти силовські підгрупи симетричної групи S_3 3-го степеня.
3. Знайти силовські підгрупи знакозмінної групи A_4 4-го степеня.
4. Описати всі, з точністю до ізоморфізму, скінченні групи G порядку $|G| \leq 10$.
5. Показати, що в знакозмінній групі A_4 степеня 4 не має підгруп порядку 6.

§7. Групи підстановок

За теоремою 3.5 всяка скінченна група порядку n ізоморфна підгрупі групи S_n всіх підстановок n-го степеня. Розглянемо більш загальний підхід.

Нехай дано деяку множину X. Назвемо всяке взаємно однозначне відображення множини X *підстановкою* множини X, а всяку підгрупу групи $S(X)$ всіх взаємно однозначних відображень X на себе — *групою підстановок* над множиною X. Потужність множини X називають *степеню підстановок* множини X. Якщо множина X скінченна і складається з n елементів, то група всіх підстановок над X ізоморфна S_n. Якщо P є група підстановок над множиною X, то можна розглянути природну дію групи P на множині X. X таким чином розпадається на P-орбіти

$$X = \bigcup_{\alpha \in I} X_\alpha, \tag{7.1}$$

які не перетинаються. Елементи a і $b \in X$ тоді і тільки тоді будуть віднесені в одну P-орбіту, якщо в групі P міститься хоча б одна підстановка, що переводить a в b. Кожен елемент множини X, що залишається на місці при всіх підстановках з групи P, складає, очевидно, окрему P-орбіту. Група підстановок P над множиною X називається *транзитивною* над X, якщо P володіє однією-єдиною P-орбітою, що суміщається, очевидно, з X, тобто якщо всякий елемент множини X може бути переведений деякою підстановкою з групи P в будь-який інший елемент цієї множини. Група, що володіє більш ніж однією P-орбітою, називається *інтранзитивною*.

Нехай група P транзитивна над X. X є P-орбітою довільного свого елемента a. Якщо множина X скінченна, то її порядок рівний індексу стабілізатора $P_a = \mathrm{St}\, a = \{\delta \in P | \delta(a) = a\}$ в групі P. Звідси отримаємо теорему.

Теорема 7.1. *Порядок транзитивної групи підстановок скінченного степеня ділиться на цей степінь.*

Нехай група P транзитивна над X. $P_a = \mathrm{St}\, a$. Якщо підстановка σ з P переводить елемент a в елемент b, то має місце рівність $P_a = \sigma^{-1} P_b \sigma$. Тобто, зважаючи на транзитивність групи P, підгрупи P_a для всіх a з X будуть між собою спряжені. Вони складатимуть навіть повний клас спряжених підгруп в групі P. Група підстановок P над множиною X називається *k раз транзитивною* (k — деяке натуральне число), якщо всяку впорядковану систему з k різних елементів множини X можна деякою підстановкою з P перевести в любу іншу впорядковану систему

з k різних елементів цієї множини. Так, симетрична група S_n степеня n є n раз транзитивною. Зрозуміло, що k раз транзитивна група є і l разів транзитивної для всіх $l < k$.

Говоритимемо, що дві групи G_1 і G_2 підстановок множини X мають один і той же *орбітальний тип*, якщо існує таке взаємно однозначне відображення φ: $X \to X$, яка переводить всяку орбіту групи G_1 в орбіту групи G_2. Нехай s, t — підстановки множини X, $x_1 \in X$. Якщо $t(x_1) = x_2$, то

$$s^{-1}ts(s^{-1}(x_1)) = s^{-1}(x_2).$$

Звідси слідує, зокрема, що якщо (7.1) — розклад множини X на Q-орбіти, які не перетинаються, для деякої групи Q підстановок множини X, то

$$X = \bigcup_{\alpha \in I} s^{-1}(X_\alpha).$$

— розклад множини X на Q^s-орбіти, які не перетинаються. Отже, спряжені підгрупи групи $S(X)$ мають один і той же орбітальний тип.

Нехай $a \in S(X)$, N_a — підмножина множини X, яка складається з усіх таких елементів $x \in X$, що $a(x) \neq x$. Очевидно звуження $a|_{N_a} \in \in S(N_a)$. Підстановка a називається *циклічно* підстановкою або *циклом*, якщо група $\langle a|_{N_a} \rangle$ транзитивна, тобто а N_a утворює одну орбіту групи $\langle a \rangle$. Потужність множини N_a називається *довжиною циклу* a.

Ясно, що будь-яка орбіта групи $\langle a \rangle$ для довільної підстановки $a \in \in S(X)$ є множиною всіх елементів множини X вигляду $x_k = a^k(x_0)$, де $k \in \mathbb{Z}$. Отже, довжина будь-якого циклу скінченна або зліченна. У останньому випадку $x_k \neq x_l$, якщо $k \neq l$. Зрозуміло, що циклічної підстановки довжини 1 не існує. Циклічні підстановки довжини 2 називають *транспозиціями*.

Цикли $a, b \in S(X)$ називають *незалежними*, якщо $N_a \cap N_b = \emptyset$.

Теорема 7.2. *Будь-яка підстановка скінченного степеня однозначно з точністю до порядку множників представляється у вигляді добутку незалежних циклів.*

Кажуть, що підстановки a і b з $S(X)$ мають один і той же *циклічний тип*, якщо циклічні групи $\langle a \rangle$ і $\langle b \rangle$ мають один і той же орбітальний тип.

Теорема 7.3. *Дві підстановки групи $S(X)$ тоді і тільки тоді спряжені в $S(X)$, коли вони мають один і той же циклічний тип.*

Наслідок 7.1. *Дві підстановки групи скінченного степеня тоді і тільки тоді спряжені в $S(X)$, коли між циклами їх розкладів у вигляді добутку незалежних циклів існує взаємно однозначна відповідність така, що відповідні цикли мають однакову довжину.*

Транзитивна група підстановок P над множиною X буде називатися *імпримітивною*, якщо множину X можна розкласти

$$X = \bigcup_{\alpha \in I} X_\alpha$$

на підмножини X_α, які не перетинаються, так, що

1) хоча б одна з підмножини X_α власна;
2) хоча б одна з підмножини X_α містить не менше двох елементів;
3) для будь-якої підстановки $\sigma \in P$ і довільної підмножини X_α існує така підмножини X_β, що

$$\sigma(X_\alpha) = \{\sigma(a) | a \in X_\alpha\} \subset X_\beta. \tag{7.2}$$

Підмножини X_α називаються *системами імпримітивності* групи P. Якщо такий розклад множини X неможливий, то група P називається *примітивною*.

З (7.2) одержимо $\sigma(X_\alpha) = X_\beta$, тобто всі системи імпримітивності X_α мають однакову потужність і в скінченному випадку складаються з однакового числа елементів. Ми бачимо, що всяка підстановка з групи P лише переставляє системи імпримітивності X_a, тобто породжує деяку підстановку множини цих систем. Всі ці підстановки множини систем X_a складають, очевидно, групу, ізоморфну фактор-групі групи P за нормальною підгрупою, що складається зі всіх тих підстановок з P, які залишають кожен елемент множини X усередині тієї системи X_α, в якій він міститься.

Всі розклади множини M в системи імпримітивності транзитивної групи P можна одержати таким чином. Нехай P_a, буде підгрупа групи P, складена з підстановок, що залишають незмінним елемент a з X. Якщо Q є деяка власна підгрупа групи P, що містить P_a як власну підгрупу, $P_a \subset Q \subset P$, то розкладаємо групу P на праві суміжні класи за підгрупі Q і збираємо разом елементи множини X, в які елемент a переводиться підстановками, що входять в один правий суміжний клас групи P за підгрупою Q. Це дає розкладання множини X на власні підмножини, що не перетинаються і кожна з яких містить не менше двох елементів. Легко перевірити, що це є розкладом множини X в системи імпримітивності групи P: два праві суміжні класи групи P за P_a, лежачі в одному правому класі P за Q, залишаються при множенні справа на деякий елемент з P знову в одному правому класі за Q. Таким чином, всяка підгрупа, між P і P_a, породжує деякий розклад множини X на системи імпримітивності групи P.

Цим шляхом можуть бути одержані всі такі розклади: якщо дано де-

який розклад множини X в системи імпримітивності групи P і якщо елемент a лежить в системі X_α та множину Q всіх підстановок з P, що залишають елемент a усередині системи X_α буде підгрупою групи P, такою, що $P_a \subset Q \subset P$ і відмінної від P_a та P. Розклад множини X, що відповідає підгрупі Q, дає задані систем імпримітивності.

Теорема 7.4. *Транзитивна група P підстановок над множиною X буде примітивною тоді і тільки тоді, коли підгрупа $P_a = \{\delta \in P | \delta(a) = a\}$ $(a \in P)$ є її власною підгрупою, яка не міститься в жодній іншій власній підгрупі групи P.*

Відмітимо, що k раз транзитивна група при $k > 1$ примітивна.

Теорема 7.5. *Власна підмножина X_0 множини X тоді і тільки тоді буде системою імпримітивності для транзитивної групи P підстановок над множиною X, якщо X_0 містить не менше двох елементів і якщо всяка підстановка σ з P, що залишає один елемент з X_0 в цій підмножині, відображає всю підмножину X_0 на себе або в себе.*

Теорема 7.6. *Всяка відмінна від $\{e\}$ нормальна підгрупа примітивної групи P підстановок над множиною X транзитивна над множиною X.*

Нормальною підгрупою всякої групи є вона сама і її тривіальна підгрупа. Наведемо приклади простих груп, тобто груп, в яких не має інших нормальних підгруп, окрім цих двох. Абелева група буде простою тоді і тільки тоді, коли вона циклічна і якщо всякий її елемент, відмінний від 1, є для неї твірним. Отже, абелева група буде простою тоді і тільки тоді, коли вона циклічна і порядок її є просте число. Існують, проте, і некомутативні прості групи, як скінченні, так і нескінченні.

Лема 7.1. *Якщо нормальна підгрупа H знакозмінної групи A_n степеня $n \geqslant 5$ містить циклічну підстановку довжини 3, то вона суміщається зі всією групою A_n.*

На основі леми можна довести справедливість теореми, яка відіграє важливу роль в теорії Галуа.

Теорема 7.7 (Теорема Галуа)**.** *Знакозмінна група A_n степеня n при $n \geqslant 5$ проста.*

Вправи

1. Показати, що транзитивна група підстановок степені n містить не менше ніж $n - 1$ підстановку, кожна з яких δ не має нерухомих точок i $(\delta(i) = i)$.

2. Показати, що знакозмінна група A_n степеня $n > 2$ буде $n-2$ рази транзитивною.

3. Показати, що симетрична група S_n та знакозмінна група A_n степеня n примітивні.

4. Показати, що знакозмінна група A_5 степеня 5 не має підгруп порядку 15.

5. Показати, що група з 12 елементів не є простою.

§8. Нільпотентні групи

Нехай A, B — підгрупи групи G. Підгрупа $[A,B] = \langle [a,b] | a \in A,\ b \in B \rangle$ називається *взаємним комутантом* підгруп A та B.

Для будь-яких підгруп A, B групи G мають місце властивості.

1) $[A,B] = [B,A]$.
2) $A \lhd \langle A,B \rangle$ тоді і тільки тоді, коли $[A,B] \subset A$.
3) $[A,B] \lhd \langle A,B \rangle$.
4) Нехай A, $B \lhd G$, $A \subset B$. $[B,G] \subset A$ тоді і тільки тоді, коли $B/A \subset \subset \mathfrak{Z}(G/A)$.

Нехай G — група. Нормальний ряд

$$\{e\} = G_0 \subset G_1 \subset \ldots \subset G_s = G \tag{8.1}$$

групи G називається *центральним*, якщо

$$G_i/G_{i-1} \subset \mathfrak{Z}(G/G_{i-1}) \text{ для всіх } i = 1,2,\ldots,s \tag{8.2}$$

або, що рівносильне,

$$[G_i, G] \subset G_{i-1} \text{ для всіх } i = 1,2,\ldots,s. \tag{8.3}$$

Група, що володіє центральними рядами, називається *нільпотентною*, а мінімальна довжина таких рядів — її *степенем нільпотентності*. Очевидно фактори центрального ряду абелеві. Безпосередньо з визначення видно, що всі абелеві групи вичерпують всі нільпотентні групи степеня 1.

Нехай G — довільна група. Ми можемо спробувати побудувати в ній центральний ряд, керуючись або формулою (8.2), або формулою (8.3). Саме, нехай

$$\zeta_0 G = \{e\},\ \zeta_i G \text{ — повний прообраз } \mathfrak{Z}(G/\zeta_{i-1}G)$$

при природному епіморфізмі $G \to G/\zeta_{i-1}G$ $(i = 1,\ 2,\ \ldots)$;

$$\gamma_0 G = G,\ \gamma_j G = [\gamma_{j-1}G, G]$$

$(j = 1,\ 2,\ \ldots)$. Якщо для деякого s $\zeta_s G = G$ і s — найменший індекс з такою властивістю, то ряд

$$\{e\} = \zeta_0 G \subset \zeta_1 G \subset \ldots \subset \zeta_s G = G \tag{8.4}$$

є центральним рядом групи G, який називається *верхнім центральним* рядом групи G. Якщо для деякого t $\gamma_t G = \{e\}$ і t — найменший індекс з такою властивістю, то ряд

$$\{e\} = \gamma_t G \subset \gamma_{t-1} G \subset \ldots \subset \gamma_0 G = G \tag{8.5}$$

є центральним рядом групи G, який називається *нижнім центральним* рядом групи G.

Підгрупи $\zeta_i G$ називаються *гіперцентрами* групи G, а підгрупи $\gamma_j G$ — *централами* групи G. Ясно, що якщо деякий гіперцентр суміщається з всією групою G або деякий централ суміщається з одиницею $\{e\}$, то група G нільпотентна.

Навпаки, нехай група G нільпотентна і (8.1) — довільний центральний ряд в ній. Визначення і легка індукція дають включення.

$$\begin{array}{ccccccccccccc}
\{e\} = \zeta_0 G & \subset & \zeta_1 G & \subset \ldots \subset & \zeta_{i-1} G & \subset & \zeta_i G & \subset \ldots, & & & & & \\
\cup & & \cup & & \cup & & \cup & & & & & & \\
\{e\} = G_0 & \subset & G_1 & \subset \ldots \subset & G_{i-1} & \subset & G_i & \subset \ldots \subset & G_s & = G, & & & \\
 & & & & \cup & & \cup & & \cup & & & & \\
 & & & \ldots \subset & \gamma_{s-i+1} G & \subset & \gamma_{s-i} G & \subset \ldots \subset & \gamma_0 G & = G. & & &
\end{array} \tag{8.6}$$

Звідси видно, що в нільпотентної групі ряди гіперцентрів і централів обриваються. Отже, група G володіє верхнім та нижнім центральним рядом.

Теорема 8.1. *Якщо група G нільпотентна, то G володіє верхнім та нижнім центральним рядом, довжини яких рівні степені нільпотентності групи.*

Хоча верхній і нижній центральні ряди нільпотентної групи мають однакову довжину, вони самі не зобов'язані бути ізоморфними.

Теорема 8.2. *Всяка скінченна p-груп нільпотентна.*

Теорема 8.3. *Всяка підгрупа нільпотентної групи степеня s є нільпотентною групою степеня $r \leqslant s$.*

Теорема 8.4. *Всяка фактор-група нільпотентної групи степеня s є нільпотентною групою степеня $t \leqslant s$.*

Теорема 8.5. *Прямий добуток скінченної кількості нільпотентних груп є нільпотентною групою.*

Лема 8.1. *Нормалізатор довільної власної підгрупи H нільпотентної групи G відмінний від H.*

Теорема 8.6 (Теорема Бернсайда — Віланда)**.** *Скінченна група є нільпотентною групою тоді і тільки тоді, коли вона є прямим до-*

бутком своїх силовських підгруп.

Вправи

1. Побудувати верхній та нижній центральний ряд для групи кватерніонів Q_8. Який степінь нільпотентності групи Q_8?

2. Нехай комутант неабелевої групи G лежить в її центрі. Довести, що G нільпотентна група. Який степінь нільпотентності групи G?

3. Довести, що всяке субнормальне ущільнення центрального ряду групи є також її центральним рядом.

4. Довести, що всяка нільпотентна група має нормальний ряд з циклічними факторами.

5. Нехай p_1, p_2, p_3 — різні прості числа, G — нільпотентна група порядку $p_1p_2p_3$. Довести, що G абелева група.

§9. Розв'язні групи

Група G називається *розв'язною*, якщо ланцюг

$$G \supset G' \supset G'' \supset \ldots \supset G^{(i-1)} \supset G^{(i)} \supset \ldots,$$

де кожна підгрупа $G^{(i)}$ є комутантом попередньої групи $G^{(i-1)}$, обривається після скінченної кількості кроків на одиничній підгрупі (наприклад $G^{(l)} = \{e\}$). Найменше невід'ємне ціле число l таке, що $G^{(l)} = \{e\}$ називається *степеню розв'язності* групи.

Теорема 9.1. *Всяка підгрупа розв'язної групи степеня s є розв'язною групою степеня $r \leqslant s$.*

Теорема 9.2. *Всяка фактор-група розв'язної групи степеня s є розв'язною групою степеня $t \leqslant s$.*

Теорема 9.3. *Подані дві властивості групи G еквівалентні властивості розв'язності:*

1) *група G володіє нормальним рядом*

$$\{e\} = G_0 \subset G_1 \subset \ldots \subset G_{i-1} \subset G_i \subset \ldots \subset G_s = G,$$

у якому всі фактори G_i/G_{i-1} $(i = 1, 2, \ldots, s)$ абелеві;

2) *група G володіє субнормальним рядом*

$$\{e\} = H_0 \subset H_1 \subset \ldots \subset H_{j-1} \subset H_j \subset \ldots \subset H_t = G,$$

у якому всі фактори H_j/H_{j-1} $(j = 1, 2, \ldots, t)$ абелеві.

Наслідок 9.1. *Група G розв'язна, якщо вона володіє такою нормальною підгрупою H, що H і G/H — розв'язні групи.*

Теорема 9.4. *Група G скінченного порядку розв'язна тоді і тільки тоді, коли фактори H_i/H_{i-1} композиційного ряду*

$$\{e\} = H_0 \subset H_1 \subset \ldots \subset H_{i-1} \subset H_i \subset \ldots \subset H_n = G$$

є циклічними групами простого порядку.

Очевидно всяка поліциклічна група розв'язна. Важливий підклас поліциклічних груп складають *надрозв'язні* групи — це групи, які володіють нормальним (а не просто субнормальним) рядом з циклічними факторами. Зрозуміло, що всяка нільпотентна група буде надрозв'язна.

Теорема 9.5. *Всяка підгрупа та фактор-група надрозв'язної групи є надрозв'язними групами.*

Відзначимо одну властивість скінченних надрозв'язних груп. Нехай G — скінченна група порядку $|G| = p_1^{s_1} p_2^{s_2} \ldots p_n^{s_n}$, де p_i — прості числа, $p_1 < p_2 < \ldots < p_n$. Нормальний ряд

$$\{e\} = G_0 \subset G_1 \subset \ldots \subset G_{i-1} \subset G_i \subset \ldots \subset G_n = G \qquad (9.1)$$

називають *силовським* рядом групи G, якщо його фактори G_i/G_{i-1} є силовськими p_i-підгрупами групи G/G_{i-1} $(i = 1, 2, \ldots, n)$. Очевидно, нормальний ряд (9.1) групи G буде силовськими тоді і тільки тоді, коли $|G_i/G_{i-1}| = p_i^{s_i}$ $(i = 1, 2, \ldots, n)$.

Теорема 9.6. *Скінченна надрозв'язна група володіє силовським рядом.*

Вправи

1. Показати, що напівпрямий добуток розв'язних груп є розв'язною групою.

2. Довести, що всяка скінченна група порядку 100 розв'язна.

3. Побудувати один композиційний ряд симетричної групи S_4 4-го степеня. Чи є вона розв'язною?

4. Довести, що симетричної групи S_n при $n > 4$ не є розв'язною.

5. Нехай порядок групи G рівний p^2q, де p, q — різні прості числа. Довести, що в цьому випадку одна з силовських підгруп групи G нормальна, а група G розв'язна.

Література

1. *Ван дер Варден Б. Л.* Алгебра. – М.: Наука, 1979.
2. *Ганюшкін О. Г., Безущак О. О.* Завдвння до практичних занять з алгебри і теорії чисел (теорія груп): навчальний посібник. – К.: ВПЦ Київський університет, 2005.
3. *Ганюшкін О. Г., Безущак О. О.* Теорія груп. – К.: ВПЦ Київський університет, 2005.
4. *Дрозд Ю. А., Кириченко В. В.* Конечномерные алгебры. – К.: Вища школа, 1980.
5. *Завало С. Т.* Курс алгебри. – К.: Вища школа, 1985.
6. *Калужнин Л. А.* Введение в общую алгебру. – М.: Наука, 1973.
7. *Каргаполов М. И., Мерзляков Ю. И.* Основы теории групп. – М.: Наука, 1982.
8. *Кострикин А. И.* Введение в алгебру. – М.: Наука, 1977.
9. *Курош А. Г.* Курс высшей алгебры. – М.: Наука, 1971.
10. *Курош А. Г.* Теория групп. – М.: Наука, 1967.
11. *Ляпин Е. С., Айзенштат А. Я., Лесохин М. М.* Упражнения по теории групп. – М.: Наука, 1967.
12. Сборник задач по алгебре / Под редакцией Кострикина А. И. – М.: Наука, 1987.
13. *Фаддеев Д. К.* Лекции по алгебре. – М.: Наука, 1984.
14. *Холл М.* Теория групп. – М.: Иностранная литература, 1962.

Предметний показчик

Автоморфізм 14
— внутрішній автоморфізм 15
— зовнішній 15
Антигомоморфізм 13
Антиізоморфізм 14

Бінарна алгебраїчна операція 5

Визначення групи через твірні елементи та визначальні співвідношення 19

Голоморф 16
Гомоморфізм 12
— тривіальний 14
Група 5
— абелева 6
— автоморфізмів 15
— адитивна кільця 7
— без скруту 6
— вільна 18
— внутрішніх автоморфізмів 15
— діедра 21
— досконала 16
— знакозмінна 9
— зовнішніх автоморфізмів 15
— кватерніонів 21
— комутативна 6
— мультиплікативна кільця 7
— надрозв'язна 34
— нескінченна 6
— нільпотентна 31
— періодична 6
— підстановок 27
— — імпримітивна 29
— — примітивна 29
— — інтранзитивна 27
— — k раз транзитивна 27
— — транзитивна 27
— поліциклічна 22
— проста 10, 30
— розв'язна 33
— самосуміщень фігури 20
— симетрична 9
— скінченна 6
— тривіальна 6
— циклічна 8
— четверна Кляйна 12
гіперцентр 32

Добуток 5
— відображень 15
— декартовий 5, 21
— напівпрямий 16
— підмножин 11
— прямий 21
Довжина ряду 22
— слова 17
— циклу 28
Додавання 7
Доданок 22

Елемент нескінченного порядку 6
— обернений 5
— одиничний елемент 5
— лівий обернений 5
— лівий одиничний 5
— протилежний 7
Ендоморфізм 14
— природними 14
Епіморфізм 13

Звуження відображення 15

Ізоморфізм 5
Ізоморфні групи 5, 13

Ізоморфні ряди 23
Індекс підгрупи 9

Клас спряжених елементів 11
Компонента 21
Комутант 12
— взаємний 31
Комутатор 12
Кратне елемента 7

Лема Цасенхауза 22
Лівий суміжний клас 9

Множення 5
Множник 21
Мономорфізм 13

Нормалізатор 11
Носій 21
Нуль 7

Образ гомоморфізму 13
Операція адитивна 7
— бінарна алгебраїчна 5
— комутативна 6
— мультиплікативна 5
— G-орбіта 24
Орбітальний тип 28

Підстановка 27
Підгрупа 7
— власна 7
— максимальна підгрупа 24
— нормальна 10
— нормально породжена множиною 10
— породжена множиною 8
— скінченно породжена 8
— скінченного індекса 9
— субнормальна 22
Підмножина власна 8
Підстановка 27
— циклічна 28
Показник групи 6
Порядок групи 6
Порядок елемента 6
Початковий відрізок слова 20
Правою вибираюча функція 19
Правий суміжний клас 9
Представник 9
Протилежний елемент 7
Проекція 21
p-група 6
p-підгрупа силовська 25

Ранг вільної групи 18
Розширення групи 22
Ряд верхній центральний 32
— головний 23
— композиційний 23
— нормальний 22
— нижній центральний 32
— поліциклічний 22
— силовський 34
— субнормальний 22
— центральний 31

Слово 17
— порожнє 17
Співвідношення 19
Спряженність 10
Стабілізатор 24
Степінь елемента 6
— нільпотентності групи 31
— підстановки 27
— розв'язності групи 33
Система визначальних співвідношень 19
— імпримітивності 29

— твірних елементів 8
— шраєрівська 20
Скорочення 17
Сума 7
— пряма 22
Супорт 21

Таблиця Келі 7
Теорема Бернсайда — Віланда 32
— Галуа 30
— Гельдера 16
— Діка 19
— Жордана — Гельдера 23
— Келі 15
— Лагранжа 9
— про відповідність підгруп при гомоморфізмі 14
— про ізоморфізм друга 14
— про ізоморфізм перша 14
— про ізоморфізм третя 14
— Нільсена — Шраєра 20
— Силова про вкладення 24
— Силова про існування 24
— Силова про кількість 25
— Силова про спряженість 25
— Шрайера про ряди 23
Транспозиція 9, 28

Ущільнення ряду 23

Фактор ряду 22
Фактор-група 11
Формула орбіт 24

Центр 11
Централ 32
Централізатор 11
Цикл 28
Циклічний тип 28

Ядро гомоморфізму 13

Позначення

$\mathbb{N}$ — множина всіх натуральних чисел,
$\mathbb{Z}$ — множина всіх цілих чисел,
$\mathbb{Q}$ — множина всіх раціональних чисел,
$A \cup B$ — об'єднання множин A і B,
$A \cap B$ — переріз множин A і B,
$\emptyset$ — порожня множина,
$f : M_1 \to M_2$ — відображення f множини M_1 в множину M_2,
S_n — симетрична група степеня n,
A_n — знакозмінна група степеня n,
C_n — абстрактна циклічна група порядку n,
D_n — група діедра порядку n,
K_4 — четверна група Кляйна,
Q_8 — група кватерніонів,
$|G|$ — порядок групи G,
$[G : H]$ — індекс підгрупи H в групі G,
$[a, b]$ — комутатор $a^{-1}b^{-1}ab$ елементів a, b групи G,
$[A, B]$ — взаємним комутантом підгруп A та B деякої групи,
G' — комутант групи G,
$G_1 \times G_2 \times \cdots \times G_n$ — прямий добуток груп G_1, G_2, …, G_n,
$G_1 \oplus G_2 \oplus \cdots \oplus G_n$ — пряма сума груп G_1, G_2, …, G_n,
$\langle M \rangle$ — підгрупа породжена підмножиною M групи G,
$H \lhd G$ — H нормальна підгрупа групи G,
$H \lhd\lhd G$ — H субнормальна підгрупа групи G,
$\operatorname{Aut} G$ — група всіх автоморфізмів групи G,
$\operatorname{Inn} G$ — група внутрішніх автоморфізмів групи G,
$\operatorname{Out} G$ — група зовнішніх автоморфізмів групи G,
$\operatorname{Hol} G$ — голоморф групи G,
a^G — клас спряженості елемента a в групі G,
M^x — спряжена підмножина з множиною M групі,
G/H — фактор-група групи G за підгрупою H,
e — одиниця групи,
$(x_1\, x_2\, \ldots\, x_n)$ — цикл підстановки,
$\operatorname{Ker} f$ — ядро гомоморфізма f,
$f(G)$ — образ гомоморфізма $f : G \to G^*$,
$N_H(M)$ — нормалізатор множини M в підгрупі H,
$\mathfrak{Z}_H(M)$ — централізатор множини M в підгрупі H,
$\operatorname{St}(m)$ — стабілізатор елемента m,
$G(m)$ — G-орбіта елемента m.

О. А. Тилищак

ЕЛЕМЕНТИ ТЕОРІЇ ГРУП

Відповідальний за випуск:
доктор фізико-математичних наук, професор *П. М. Гудивок*

Формат 60 × 84/16. Умов. друк. арк. . Замовлення № . Наклад екз.
Видавництво УжНУ «Говерла»м. Ужгород, вул. Капітульна, 18. Тел.: (0312) 233248.
Свідоцтво про внесення до державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції — Серія Зт №32