

Розділ 7.

Алгебричні структури

У попередніх параграфах накопичилось доволі багато конкретного матеріалу, який необхідно осмислити із загальніших позицій. З цією метою ми введемо і вивчимо, поки що на елементарному рівні, фундаментальні для всієї алгебри поняття групи, кільця і поля.

7.1. Напівгрупи. Моноїди

Означення 7.1. Множина, на якій визначено бінарну асоціативну операцію, називається *напівгрупою*.

Означення 7.2. Напівгрупа, у якій існує одиничний (нейтральний) елемент, називається *моноїдом* (або *напівгрупою з одиницею*).

Як і довільну алгебричну структуру напівгрупи та моноїди X з визначеною на них операцією $*$ позначатимемо $(X, *)$. Інколи для наголосення того факту, який саме елемент є одиничним, в запис моноїда включають одиничний елемент e ; наприклад, $(X, *, e)$.

Означення 7.3. Моноїд $(X, +, 0)$ називають *адитивним*, а моноїд $(X, \cdot, 1)$ — *мультиплікативним*. Зауважимо, що в мультиплікативному моноїді в записі добутку елементів операцію « \cdot » часто опускають, записуючи ab замість $a \cdot b$.

Приклади 7.1. 1. $(2\mathbb{Z}, \cdot)$ — напівгрупа (не моноїд!), а $(2\mathbb{Z}, +)$ — моноїд.

2. Нехай $n\mathbb{Z} = \{ nk \mid k \in \mathbb{Z} \}$ — множина цілих чисел, що ділиться на натуральне число n (тобто кратні n). Зрозуміло, що $(n\mathbb{Z}, +, 0)$ — комутативний моноїд, а $(n\mathbb{Z}, \cdot)$ — комутативна напівгрупа (при $n \geq 2$).

3. Множини $\mathbb{Z}, \mathbb{R}, \mathbb{Q}$ є моноїдами стосовно як операції додавання, так і операції множення.

4. $(M_n(\mathbb{R}), +, O)$ — комутативний моноїд з нульовою матрицею O в ролі нейтрального елемента, $(M_n(\mathbb{R}), \cdot, E)$ — некомутативний моноїд з одиничною матрицею E в ролі нейтрального елемента.

Означення 7.4. Підмножина X' напівгрупи $(X, *)$ називається *піднапівгрупою*, якщо вона замкнена стосовно операції $*$, тобто якщо $a * b \in X'$ для усіх $a, b \in X'$. Якщо $(X, *, e)$ — моноїд і підмножина $X' \subset X$ не тільки замкнена стосовно операції $*$, але й містить одиничний елемент e , то X' називається *підмоноїдом* моноїда X .

Приклад 7.2. $(n\mathbb{Z}, \cdot)$ — піднапівгрупа в (\mathbb{Z}, \cdot) , а $(n\mathbb{Z}, +, 0)$ — підмоноїд в $(\mathbb{Z}, +, 0)$.

Твердження 7.1. Множина усіх оборотних елементів моноїда $(X, *)$ є підмоноїдом цього моноїда.

Доведення. По-перше, множина оборотних елементів моноїда X замкнена щодо операції $*$, тобто, якщо a, b — довільні оборотні елементи моноїда X , то $a * b$ також оборотний елемент. Дійсно,

$$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e,$$
$$(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b = b^{-1} * e * b = b^{-1} * b = e,$$

звідки випливає, що елемент $a * b$ оборотний (оберненим до нього є елемент $b^{-1} * a^{-1}$). По-друге, нейтральний елемент належить множині оборотних елементів, оскільки він обернений сам до себе. \square

Нехай a_1, \dots, a_k — впорядкована послідовність елементів множини X . Раніше ми вже користувались знаком сумування $\sum_{i=1}^k a_i$. Очевидно, що його можна використовувати і в будь-якому адитивному моноїді $(X, +)$. В мультиплікативному моноїді (X, \cdot) аналогом знаку сумування служить знак добутку

$$\prod_{i=1}^2 a_i = a_1 a_2, \quad \prod_{i=1}^3 a_i = (a_1 a_2) a_3, \quad \prod_{i=1}^k a_i = \left(\prod_{i=1}^{k-1} a_i \right) a_k.$$

Якщо $a_1 = a_2 = \dots = a_k = a$, то добуток $\underbrace{a \cdot a \cdot \dots \cdot a}_k$ позначають символом a^k , називаючи його *k-им натуральним степенем елемента a*.

Розглянемо більш загальний випадок, коли степінь елемента не натуральне, а довільне ціле число. Нехай a — будь-який оборотний елемент мультиплікативного моноїда X . Для довільного $k \in \mathbb{Z}$ позначимо

$$a^k = \begin{cases} \underbrace{a \cdot a \cdot \dots \cdot a}_{k \text{ множників}}, & \text{якщо } k > 0, \\ e, & \text{якщо } k = 0, \\ \underbrace{a^{-1} \cdot a^{-1} \cdot \dots \cdot a^{-1}}_{|k| \text{ множників}}, & \text{якщо } k < 0. \end{cases}$$

Елемент a^k назовемо *k-им степенем елемента a* моноїда X .

Твердження 7.2. Якщо a — довільний оборотний елемент моноїда (X, \cdot) , то для всіх $m, n \in \mathbb{Z}$ виконуються правила степенів

$$a^m a^n = a^{m+n}, \quad (a^m)^n = a^{mn}. \quad (7.1)$$

Доведення. Для $m, n \in \mathbb{N}$ це очевидно. Якщо ж, наприклад, $m > 0, n < 0$, то

$$a^m a^n = a^m (a^{-1})^{|n|} = \underbrace{a \cdot \dots \cdot a}_{m \text{ множників}} \cdot \underbrace{a^{-1} \cdot \dots \cdot a^{-1}}_{|n| \text{ множників}} = \begin{cases} a^{m-|n|}, & \text{якщо } m \geq |n|, \\ (a^{-1})^{|n|-m}, & \text{якщо } m < |n| \end{cases} = a^{m+n}.$$

Аналогічно доводяться решта випадків і друга рівність. \square

Якщо моноїд X адитивний, то замість степенів елементів розглядають їхні кратні: якщо $k \in \mathbb{Z}$, то під *k-им кратним елементом a* в X розуміють вираз

$$ka = \begin{cases} \underbrace{a + a + \dots + a}_{k \text{ доданків}}, & \text{якщо } k > 0, \\ 0, & \text{якщо } k = 0, \\ \underbrace{-a + (-a) + \dots + (-a)}_{|k| \text{ доданків}}, & \text{якщо } k < 0, \end{cases}$$

і правила степенів твердження 7.2 стають правилами кратних

$$ma + na = (m+n)a, \quad n(ma) = (nm)a, \quad \text{де } m, n \in \mathbb{Z}.$$

Зауважимо ще один корисний факт. Якщо у моноїді (X, \cdot) елементи a та b комутують, тобто $ab = ba$, то для довільного $m \in \mathbb{Z}$

$$(ab)^m = a^m b^m,$$

або, загальніше, якщо $a_i a_j = a_j a_i$ для всіх $a_i, a_j \in X$, $i, j = \overline{1, k}$, то

$$(a_1 \cdot \dots \cdot a_k)^m = a_1^m \cdot \dots \cdot a_k^m$$

(ці співвідношення легко доводяться індукцією за m , пропонуємо читачеві довести їх самостійно). Аналогічно в адитивному моноїді: якщо $a + b = b + a$, то $m(a + b) = ma + mb$, і якщо $a_i + a_j = a_j + a_i$ для усіх $i, j = \overline{1, k}$, то $m(a_1 + \dots + a_k) = ma_1 + \dots + ma_k$ для довільного $m \in \mathbb{Z}$.

7.2. Групи та підгрупи

Моноїд, в якому для кожного елемента існує обернений (тобто всі його елементи обернені), називається *групою*. Інакше кажучи,

Означення 7.5. Групою $(G, *)$ називається непорожня множина G , якщо виконуються такі аксіоми:

- [G0] на множині G визначена бінарна операція $*: G \times G \rightarrow G$;
- [G1] операція $*$ асоціативна, тобто $(a * b) * c = a * (b * c)$ для всіх $a, b, c \in G$;
- [G2] існує нейтральний елемент, тобто існує такий елемент $e \in G$, що для довільного $a \in G$ виконується $a * e = e * a = a$;
- [G3] для кожного елемента існує обернений, тобто для довільного елемента $a \in G$ існує такий елемент $a^{-1} \in G$, що $a * a^{-1} = a^{-1} * a = e$.

Означення 7.6. Якщо в групі $(G, *)$ операція $*$ комутативна, тобто для довільних елементів $a, b \in G$ виконується співвідношення $a * b = b * a$, то група G називається *комутативною* або, частіше, *абелевою*¹.

Приклади 7.3. 1. Числові множини $(\mathbb{Z}, +)$, $(2\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$ є абелевими групами, а множини $(\mathbb{N}, +)$, $(\mathbb{R}^+, +)$, (\mathbb{N}, \cdot) , (\mathbb{Z}, \cdot) , (\mathbb{Q}, \cdot) , (\mathbb{R}, \cdot) не є групами.

2. Двоелемента множина $\{-1, 1\}$ стосовно операції додавання не утворює групу, а от стосовно множення утворює абелеву групу. Цю групу $(\{-1, 1\}, \cdot)$ позначатимемо C_2 .

3. Множина $M_n(\mathbb{R})$ стосовно операції додавання матриць утворює абелеву групу, а стосовно операції множення — лише некомутативний моноїд.

4. Множина $GL_n(\mathbb{R})$ — всіх оборотних (невироджених) матриць порядку n з елементами із множини дійсних чисел — утворює некомутативну групу стосовно операції множення (ци групу називають *повною лінійною групою* порядку n над \mathbb{R}). Дійсно, якщо $A, B \in M_n(\mathbb{R})$ і $\det A \neq 0$, $\det B \neq 0$, то за теоремою 3.24 $\det AB \neq 0$, тобто операція множення замкнена на множині $GL_n(\mathbb{R})$. За твердженням 2.2 множення матриць асоціативне на всій множині $M_n(\mathbb{R})$, а отже й на множині $GL_n(\mathbb{R})$ зокрема. Очевидно, що одинична матриця E належить $GL_n(\mathbb{R})$. Далі, за теоремою 3.25 для довільної матриці з множини $GL_n(\mathbb{R})$ існує обернена матриця. І насамкінець, в силу зауваження 2.3 група $GL_n(\mathbb{R})$ є некомутативною.

Зауважимо, що *повну лінійну групу* $GL_n(\mathbb{R})$ коротко можна було б також означити, як підмоноїд всіх оборотних елементів моноїда $(M_n(\mathbb{R}), \cdot, E)$.

5. Будь-який арифметичний векторний простір \mathbb{R}^n є абелевою групою стосовно операції додавання векторів.

6. Нехай X — довільна множина. За результатами § 1.2, множина всіх бієктивних відображенень X в себе є групою стосовно операції добутку (композиції) відображень.

¹ В честь норвежського математика Абеля. Сам термін «група» належить французькому математику Галуа.

7. Нехай задано квадрат на площині (рис. 7.1), вершини якого занумеровані проти годинникової стрілки числами 1, 2, 3, 4 і нехай точка O — центр квадрата. Позначимо через e, a, b, c повороти квадрата навколо точки O , відповідно, на $0^\circ, 90^\circ, 180^\circ, 270^\circ$ проти годинникової стрілки.

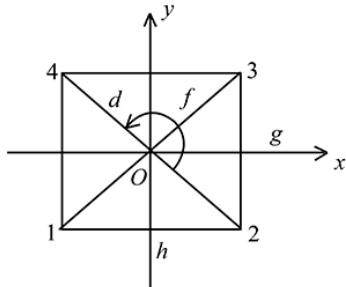


Рис. 7.1.

Якщо повернути квадрат навколо центру O на 90° , то вершина 1 перейде у вершину 2, 2 в 3, 3 в 4, 4 в 1. В результаті квадрат перейде сам в себе. Це перетворення квадрата можна задати як відображення множини вершин $\{1, 2, 3, 4\}$ в себе, яке, завичай, записують у вигляді таблиці з двох рядків $(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{smallmatrix})$, де у верхньому рядку вписані всі вершини, а в нижньому — їхні образи. Множина G всіх поворотів заданого квадрата складається з чотирьох елементів:

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},$$

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

Введемо на цій множині $G = \{e, a, b, c\}$ алгебраїчну операцію множення цих поворотів (позначимо її через \circ). Тоді множина (G, \circ) є моноїдом з одиничним елементом e , причому кожний елемент цього моноїда є оборотним: $e^{-1} = e, a^{-1} = c, b^{-1} = b, c^{-1} = a$. Рухи площин (тобто біективні відображення площини в себе, які зберігають відстань), які переводять задану геометричну фігуру в себе, називають *симетріями* цієї фігури. Так, e, a, b, c є симетріями квадрата. Крім цих симетрій, квадрат має й інші симетрії, а саме симетрії d і f стосовно діагоналей квадрата, а також симетрії h і g стосовно прямих, які проходять через центр квадрата паралельно сторонам. Легко переконатися, що множина $S = \{e, a, b, c, d, f, g, h\}$ також є прикладом групи, яку називають *групою симетрій квадрата*.

Якщо в групі G визначена операція додавання, то група $(G, +)$ називається *адитивною*. У цьому випадку нейтральний елемент називають *нулем* (позначають 0), а обернений до a елемент — *протилежним* (позначають $-a$). Якщо ж в групі G визначена операція множення, то група (G, \cdot) називається *мультипликативною*, а нейтральний елемент називають *одицією* (позначають 1 або e).

Без зменшення загальності, а тільки заради простоти викладу матеріалу, домовимося в подальшому використовувати мультиплікативну термінологію, тобто в ролі алгебричної операції $*$ розглядати операцію множення і замість виразу $x * y$ записувати просто xy .

Твердження 7.3 (наслідки з аксіом груп). В групі правильні такі твердження:

- 1) нейтральний елемент єдиний;
- 2) для кожного елемента існує єдиний обернений;
- 3) з кожної з рівностей $ab = ac$ і $ba = ca$ випливає рівність $b = c$ (закон скорочення);
- 4) кожне з двох рівнянь $ax = b$ і $ya = b$ має єдиний розв'язок.

Доведення. Перші дві властивості були доведені раніше для моноїдів (леми 1.15 та 1.16), а, отже, є правильними і для груп.

3) Домноживши обидві частини рівності $ab = ac$ зліва на a^{-1} , одержуємо

$$\begin{aligned} a^{-1}(ab) &= (a^{-1}a)b = eb = b, \\ a^{-1}(ac) &= (a^{-1}a)c = ec = c, \end{aligned}$$

звідки й випливає рівність $b = c$. Аналогічно доводиться правий закон скорочення.

4) Розв'язком рівняння $ax = b$ є елемент $x = a^{-1}b$, причому за законом скорочення цей розв'язок єдиний. \square

Означення 7.7. Кількість елементів в групі G називають *порядком* (або *потужністю*) цієї *групи*. Для позначення порядку групи G використовують рівносильні символи $|G|$, $\text{card } G$ або $(G : e)$. Групу, яка містить скінченну кількість n елементів, називають *групою порядку* n або, просто, *скінченною групою*; в протилежному випадку її називають *некінченою*.

Приклад 7.4. $(\mathbb{R}, +)$ — некінчена адитивна група, а $C_2 = (\{-1, 1\}, \cdot)$ — скінчена мультиплікативна група.

Означення 7.8. *Підгрупою* H групи G називається непорожня підмножина $H \subseteq G$, яка сама є групою стосовно тієї ж операції, що визначена в G .

Той факт, що H є підгрупою групи G , записуватимемо у вигляді $H < G$ або $H \leq G$. Довільна група G містить дві *тривіальні* підгрупи: підгрупу $\{e\}$, що складається лише з нейтрального елемента групи G , і всю групу G . Всі інші підгрупи (якщо такі існують) називають *власними*.

Приклади 7.5. 1. В уже відомій нам з прикладу 7.3 повній лінійній групі $(\text{GL}_n(\mathbb{R}), \cdot)$ розглянемо підмножину $\text{SL}_n(\mathbb{R})$ — усіх матриць n -го порядку з рівним одиниці визначником

$$\text{SL}_n(\mathbb{R}) = \{ A \in \text{GL}_n(\mathbb{R}) \mid \det A = 1 \}.$$

Очевидно, що одинична матриця E належить $\text{SL}_n(\mathbb{R})$. Крім цього, якщо $\det A = 1$, $\det B = 1$, то $\det(AB) = 1$ і $\det A^{-1} = (\det A)^{-1} = 1$. Тому $\text{SL}_n(\mathbb{R})$ — підгрупа $\text{GL}_n(\mathbb{R})$. Групу $(\text{SL}_n(\mathbb{R}), \cdot)$ називають *спеціальною лінійною групою* порядку n над \mathbb{R} (її ще називають *унімодулярною групою*, хоча до останньої часто відносять матриці з визначником, рівним ± 1).

Зауважимо, що група $\text{GL}_n(\mathbb{R})$ містить багато цікавих підгруп, а тому для різних поколінь математиків є джерелом нових ідей і ще нерозв'язаних задач.

2. Використовуючи в групі $\text{GL}_n(\mathbb{R})$ замість дійсних чисел раціональні, ми прийдемо до повної лінійної групи $\text{GL}_n(\mathbb{Q})$ порядку n над \mathbb{Q} і до її підгрупи $\text{SL}_n(\mathbb{Q})$. У свою чергу, $\text{SL}_n(\mathbb{Q})$ містить цікаву підгрупу $\text{SL}_n(\mathbb{Z})$ — ціличисельних матриць з визначником, рівним 1. Таким чином, правильні такі включення

$$\{E\} < \text{SL}_n(\mathbb{Z}) < \text{SL}_n(\mathbb{Q}) < \text{SL}_n(\mathbb{R}) < \text{GL}_n(\mathbb{R}),$$

$$\{E\} < \text{SL}_n(\mathbb{Z}) < \text{SL}_n(\mathbb{Q}) < \text{GL}_n(\mathbb{Q}) < \text{GL}_n(\mathbb{R}).$$

3. Поклавши у вищенаведених випадках 1 та 2 значення $n = 1$, ми отримаємо мультиплікативні групи $\mathbb{R}^* = \mathbb{R} \setminus \{0\} = \text{GL}_1(\mathbb{R})$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\} = \text{GL}_1(\mathbb{Q})$ дійсних та раціональних чисел. Ці групи, очевидно, некінченні. Оскільки в моноїді $(\mathbb{Z}, \cdot, 1)$ оборотними елементами є тільки 1 та -1 , то $\text{GL}_1(\mathbb{Z}) = \{\pm 1\}$. Далі, $\text{SL}_1(\mathbb{R}) = \text{SL}_1(\mathbb{Q}) = \text{SL}_1(\mathbb{Z}) = \{1\}$. Але уже при $n = 2$ група $\text{SL}_2(\mathbb{R})$ некінчена: її належать, наприклад, усі матриці вигляду

$$\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix}, \quad \begin{pmatrix} m & m-1 \\ 1 & 1 \end{pmatrix}, \quad m \in \mathbb{Z}.$$

4. У наведених нижче включеннях кожна попередня група є підгрупою кожної наступної, більшої групи:

$$(\{0\}, +) < (2\mathbb{Z}, +) < (\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +),$$

$$(\mathbb{Q}^+, \cdot) < (\mathbb{R}^+, \cdot),$$

$$(\{1\}, \cdot) < (\{1, -1\}, \cdot) < (\mathbb{Q}^*, \cdot) < (\mathbb{R}^*, \cdot).$$

5. Як було показано у прикладі 7.3, множина всіх біективних відображень множини X в себе є групою стосовно операції добутку (композиції) відображень. Ця група й особливо різні її підгрупи, які називаються *групами перетворень*, — стартова площа, з котрої розпочинаються всеможливі застосування теорії груп (достатньо згадати про знамениту «Ерлангенську програму» Ф. Клейна (1872р.), яка поклала поняття групи перетворень в основу класифікації різних типів геометрій).

Твердження 7.4 (критерій підгрупи). Непорожня підмножина $H \subseteq G$ є підгрупою групи G тоді і тільки тоді, коли виконуються дві умови:

- 1) для кожних двох елементів $a, b \in H$ добуток ab міститься в H ;
- 2) для кожного $a \in H$ обернений елемент a^{-1} теж міститься в H .

Доведення. Необхідність очевидна. Доведемо достатність. Оскільки алгебрична операція асоціативна на всій множині G , то вона асоціативна й на довільній її підмножині H . Нехай $a \in H$. Тоді за умовою твердження $a^{-1} \in H$ і $aa^{-1} = e \in H$. Отже, H утворює групу стосовно визначененої на G алгебричної операції, а тому $H \leq G$. \square

Твердження 7.5. Якщо H — підгрупа групи G , то

- 1) нейтральний елемент e_H підгрупи H співпадає з нейтральним елементом e_G групи G ;
- 2) для довільного $a \in H$ обернений до a в H співпадає з оберненим до a в G .

Доведення. 1) З рівностей $e_H e_H = e_H$ і $e_H e_G = e_H$ випливає, що $e_H e_H = e_H e_G$, звідки за законом скорочення отримуємо, що $e_H = e_G$.

2) Оскільки $e_H = e_G$, то $a^{-1} = a_H^{-1} e_G = a_H^{-1} (aa_G^{-1}) = (a_H^{-1} a)a_G^{-1} = e_H a_G^{-1} = e_G a_G^{-1} = a_G^{-1}$, що й треба було довести. \square

Твердження 7.6. Непорожня підмножина $H \subseteq G$ є підгрупою G тоді і тільки тоді, коли для довільних $a, b \in H$

$$a^{-1}b \in H. \quad (7.2)$$

Доведення. Необхідність очевидна, доведемо достатність. Нехай для довільних елементів $a, b \in H$ маємо $a^{-1}b \in H$. Оскільки $a \in H$, то $a^{-1}a = e \in H$. Тоді для довільного $a \in H$ маємо $a^{-1}e = a^{-1} \in H$. Насамкінець, якщо $a, b \in H$, то $a^{-1} \in H$, а тому $(a^{-1})^{-1}b = ab \in H$, і ми бачимо, що усі властивості підгрупи виконано. \square

Безпосередньо із означення підгрупи випливає, що якщо H_1 та H_2 підгрупи групи G , то $H_1 \cap H_2$ також буде підгрупою G . Більше того, правильним є таке твердження.

Твердження 7.7. Перетин довільної кількості підгруп H_i групи G є підгрупою G .

Доведення. Нехай $a, b \in \bigcap_{i \in I} H_i$. Тоді $a, b \in H_i$ для всіх i , а оскільки кожна H_i є підгрупою, то й $ab, a^{-1} \in H_i$ для всіх i . Це означає, що $ab, a^{-1} \in \bigcap_{i \in I} H_i$ і, отже, $\bigcap_{i \in I} H_i$ є підгрупою G за критерієм підгрупи. \square

7.3. Циклічні групи

Нехай G — мультиплікативна група і a — довільний фіксований елемент цієї групи. Розглянемо підмножину $H = \{a^k \mid k \in \mathbb{Z}\}$ — усіх цілих степенів елемента a . З рівностей $a^m a^n = a^{m+n}$ і $(a^m)^{-1} = a^{-m}$, де $m, n \in \mathbb{Z}$, випливає, що H є підгрупою групи G , тобто правильним є таке твердження.

Твердження 7.8. Множина усіх цілих степенів елемента a групи G є підгрупою групи G .

Підгрупа H всіх цілих степенів елемента a групи G називається *циклічною підгрупою*, породженою елементом a . Якщо циклічна підгрупа H співпадає з усією групою G , то група G називається *циклічною*.

Означення 7.9. Нехай G — мультиплікативна група, a — її фіксований елемент. Якщо довільний елемент $g \in G$ можна записати у вигляді $g = a^k$ для деякого $k \in \mathbb{Z}$, то кажуть, що G — *циклічна група з твірним елементом a* (або *породжена елементом a*) і позначають

$$G = \langle a \rangle = \{ a^k \mid k \in \mathbb{Z} \}.$$

В аддитивному випадку циклічна група визначається аналогічно: $\langle a \rangle = \{ ka \mid k \in \mathbb{Z} \}$.

Очевидно, що кожна циклічна група є абелевою.

Приклади 7.6. 1. Найпростішим прикладом циклічної групи є аддитивна група цілих чисел $(\mathbb{Z}, +)$, яка породжена звичайною одиницею 1 (або -1).

2. Легко перевірити, що матриця $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ породжує в $SL_2(\mathbb{Z})$ нескінченну циклічну підгрупу.

3. S_2 є циклічною групою порядку 2, породженою елементом -1 .

Твердження 7.9. Будь-яка підгрупа циклічної групи є циклічною.

Доведення. Нехай $G = \langle a \rangle$ і H — підгрупа G . Якщо $H = \{e\}$, то доводити нічого, бо $H = \langle e \rangle$. Тому нехай H — нетривіальна підгрупа G . Очевидно, що якщо $a^k \in H$, то й $a^{-k} \in H$, а тому серед степенів елемента a можна вибрати таке найменше із натуральних чисел k , для якого $a^k \in H$. Покажемо, що тоді $H = \langle a^k \rangle$. Дійсно, нехай a^m — довільний елемент підгрупи H . Поділивши з остаточою числа m та k , отримаємо, що $m = qk + r$, де $0 \leq r < k$. Звідси $r = m - qk$ і оскільки $a^m, a^k \in H$, то й

$$a^r = a^{m-qk} = a^m(a^k)^{-q} \in H.$$

Проте найменшим натуральним числом, у степені якого елемент a належить підгрупі H , є число k , а тому елемент a^r може належати H лише у випадку, коли $r = 0$. Отже, якщо a^m — довільний елемент H , то степінь m ділиться націло на k , і тому будь-який елемент із H є деяким степенем елемента a^k , тобто $H = \langle a^k \rangle$. \square

Приклад 7.7. Як нам уже відомо, група \mathbb{Z} є адитивною циклічною групою. Покажемо, що всі її підгрупи також циклічні (причому мають вигляд $a\mathbb{Z}$, де $a \in \mathbb{Z}$). Нехай H — нетривіальна підгрупа групи \mathbb{Z} . Очевидно, що якщо ненульовий елемент $h \in H$, то й $-h \in H$, причому один з елементів h чи $-h$ є додатним. Тому серед елементів підгрупи H можна вибрати найменший додатний елемент — позначимо його a — і нехай b — довільний інший елемент H . Якщо $b > 0$, то поділимо з остаточою b на a : $b = aq + r$, де $q, r \in \mathbb{Z}$, причому $0 \leq r < a$. Оскільки H підгрупа, то $r = b - aq \in H$. Звідси, в силу мінімальності елемента a , випливає, що $r = 0$ і, отже, $b = aq$. Якщо $b < 0$, то $-b > 0$ і знову прийдемо до рівності $b = -aq$. Це означає, що $H = \{ aq \mid q \in \mathbb{Z} \}$, тобто $(H, +)$ — циклічна група.

Нехай $G = \langle a \rangle$. Можливі два принципово різні випадки.

1. Всі степені елемента a різні, тобто $a^m \neq a^n$ для довільних $m \neq n$. У цьому випадку кажуть, що елемент a має *некінченний порядок* і група $\langle a \rangle$ некінчена.

2. Існують співпадіння $a^m = a^n$ при $m \neq n$. Нехай, для конкретності, $m > n$. Домножимо рівність $a^m = a^n$ на a^{-n} . Тоді $a^m a^{-n} = a^{m-n} = e$. Звідси випливає, що у цьому випадку в групі G існують додатні степени елемента a , які дорівнюють одиничному елементу.

Означення 7.10. Найменше із натуральних чисел n , для яких $a^n = e$, називають *порядком елемента a* і позначають $\text{ord}(a)$, тобто $\text{ord}(a) := \min\{ n \in \mathbb{N} \mid a^n = e \}$. Якщо такого натуральному числа n не існує, то $\text{ord}(a) := \infty$.

Твердження 7.10. Порядок елемента a групи G дорівнює порядку циклічної групи $\langle a \rangle$, породженої цим елементом, причому якщо a — елемент скінченного порядку k , то $\langle a \rangle = \{ e, a, a^2, \dots, a^{k-1} \}$.

Доведення. Якщо a — елемент нескінченного порядку, то доводити нічого. Нехай $\text{ord}(a) = k$. Тоді усі елементи $e = a^0, a, a^2, \dots, a^{k-1}$ попарно різні, бо якби $a^i = a^j$ для $0 \leq i < j \leq k-1$, то $a^{j-i} = e$ і $0 < j-i \leq k-1$, що суперечило б тому, що $\text{ord}(a) = k$. Покажемо, що будь-який інший цілий степінь a^m дорівнює одному з елементів e, a, \dots, a^{k-1} . Дійсно, якщо m додатне, то за алгоритмом ділення з остачею існують такі цілі числа q, r , що $m = kq + r$, причому $0 \leq r \leq k-1$. Тоді за правилами (7.1) отримаємо

$$a^m = a^{kq+r} = (a^k)^q a^r = ea^r = a^r,$$

що й треба було показати. Якщо ж m від'ємне, то $m = -n$, де $n > 0$, і $a^m = a^{-n} = (a^{-1})^n = (ea^{-1})^n = (a^k a^{-1})^n = (a^{k-1})^n = a^{(k-1)n}$, а це означає, що від'ємні степені зводяться до додатних. Отже, $\langle a \rangle = \{e, a, a^2, \dots, a^{k-1}\}$. \square

Наслідок 7.11. Всі елементи скінченної групи мають скінчений порядок.

Твердження 7.12. Нехай $a \in G$ і $\text{ord}(a) = k$. Тоді

- а) $a^{-1} = a^{k-1}$;
- б) $\forall m \in \mathbb{Z} \quad a^m = e \Leftrightarrow k|m$;
- в) $\forall m \in \mathbb{Z} \quad \text{ord}(a^m) = \frac{k}{(k,m)}$;
- г) якщо $b \in G$, $\text{ord}(b) = n$, $(k,n) = 1$ і $ab = ba$, то $\text{ord}(ab) = \text{ord}(a) \cdot \text{ord}(b) = kn$.

Доведення. а) Рівність $a^{-1} = a^{k-1}$ доводиться множенням рівності $e = a^k$ на a^{-1} .

б) Поділимо m на k з остачею: $m = qk + r$, $0 \leq r < k$. Тоді $a^m = (a^k)^q \cdot a^r$, і оскільки $r < k = \text{ord}(a)$, то

$$a^m = e \Leftrightarrow (a^k)^q \cdot a^r = e \Leftrightarrow a^r = e \Leftrightarrow r = 0 \Leftrightarrow k|m.$$

в) Нехай $b = a^m$ і $n \in \mathbb{N}$. Тоді, користуючись твердженням б) і властивістю подільності², отримаємо:

$$a^m = e \Leftrightarrow a^{mn} = e \Leftrightarrow (k|mn) \Leftrightarrow \left(\frac{k}{(k,m)} \mid \frac{mn}{(k,m)} \right) \Leftrightarrow \left(\frac{k}{(k,m)} \mid n \right).$$

Таким чином, $\text{ord}(b) < \infty$ і найменшим $n \in \mathbb{N}$ з властивістю $b^n = e$ є $n = \frac{k}{(k,m)}$.

г) Оскільки $(ab)^{kn} = (a^k)^n (b^n)^k$, то $\text{ord}(ab) < \infty$ і за властивістю б) $\text{ord}(ab) = m$, де $m|kn$. З іншого боку, оскільки $(ab)^m = a^m b^m = e$, то $a^m = b^{-m}$ і $\text{ord}(a^m) = \text{ord}(b^{-m})$. Звідси за твердженням в) отримаємо рівність $\frac{k}{(k,m)} = \frac{n}{(k,m)}$, а оскільки $(k,n) = 1$, то $\frac{k}{(k,m)} = \frac{n}{(k,m)} = 1$. Звідси випливає, що $k|m$ і $n|m$, а тому $kn|m$. Отже, $kn = m$. \square

Твердження 7.13. В циклічній групі порядку n порядок довільної підгрупи ділить n і для довільного дільника q числа n існує рівно одна підгрупа порядку q .

Доведення. Якщо $|G| = n$, то застосувавши попереднє міркування для $k = n$ (у цьому випадку $a^k = e \in H$), отримаємо, що $n = qm$. При цьому

$$H = \{e, a^m, a^{2m}, \dots, a^{(q-1)m}\} \tag{7.3}$$

і H є єдиною підгрупою порядку q в групі G . Навпаки, якщо q — довільний дільник числа n і $n = qm$, то підмножина H , яка визначається рівністю (7.3), є підгрупою порядку q . \square

Наслідок 7.14. Циклічна група простого порядку містить лише дві тривіальні підгрупи.

²Нехай a, b, c — довільні цілі числа. Якщо $a|bc$ і $(a,b) = 1$, то $a|c$.

7.4. Група підстановок S_n

Розвинемо тему § 1.2, яка стосується біективних відображень, на випадок скінчених множин. Нехай M — скінчена множина із n елементів. Оскільки природа елементів множини M для нас несуттєва, то можна вважати, що $M = \{1, 2, \dots, n\}$ — множина перших n натуральних чисел.

Означення 7.11. Взаємно однозначне відображення множини $M = \{1, 2, \dots, n\}$ на себе називають *підстановкою*. Множину всіх таких підстановок позначатимемо S_n , а самі підстановки — малими буквами грецького алфавіту.

В розгорнутий і наочній формі підстановку $\sigma \in S_n$ зображають дворядковим символом

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix} \quad \text{або} \quad \sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}, \quad (7.4)$$

повністю вказуючи усі образи

$$\sigma : \begin{matrix} 1 & 2 & \dots & n \\ \downarrow & \downarrow & & \downarrow \\ i_1 & i_2 & \dots & i_n \end{matrix},$$

де $i_k = \sigma(k)$, $k = \overline{1, n}$, — переставлені певним чином символи $1, 2, \dots, n$.

Оскільки, як уже було сказано, підстановки — це біективні відображення скінченої множини на себе, то, у відповідності із загальним правилом добутку (композиції) відображень, на множині S_n можна ввести алгебричну операцію множення.

Означення 7.12. Добутком підстановок $\sigma, \tau \in S_n$ називається підстановка $\sigma\tau \in S_n$, яка визначається рівністю

$$(\sigma\tau)(i) = \sigma(\tau(i))$$

для довільного $i = 1, 2, \dots, n$.

Приклад 7.8. Перемножимо дві підстановки $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$. Маємо

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{matrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 3 & 2 & 1 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 4 & 3 & 2 \end{matrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.$$

В той же самий час

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

тому, як бачимо, $\sigma\tau \neq \tau\sigma$.

Твердження 7.15. Множина S_n є групою стосовно операції множення підстановок, причому неабелевою при $n \geq 3$.

Доведення. За теоремою 1.1 добуток підстановок асоціативний. Роль нейтрального елемента у множині S_n відіграє тотожне відображення $\varepsilon = \varepsilon_M$, тобто *одинична* підстановка

$$\varepsilon = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix} \in S_n$$

(легко перевірити, що $\sigma\varepsilon = \varepsilon\sigma = \sigma$ для усіх $\sigma \in S_n$). Очевидно, що якщо у підстановці (7.4) довільним чином переставити місцями стовпчики, то ми одержимо запис тієї ж самої підстановки. Тому для довільної підстановки

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \in S_n,$$

існує така підстановка

$$\sigma^{-1} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ 1 & 2 & \dots & n \end{pmatrix} \in S_n,$$

що $\sigma\sigma^{-1} = \sigma^{-1}\sigma = \varepsilon$, тобто для довільної підстановки існує обернена. Отже, множина S_n стосовно операції множення підстановок утворює мультиплікативну групу. Її неабелевість при $n \geq 3$ показано у прикладі 7.8. При $n = 2$ множина S_n містить лише дві підстановки, які, очевидно, комутують. \square

Означення 7.13. Група S_n називається *симетричною групою степеня n* .

Твердження 7.16. $|S_n| = n!$.

Доведення. Достатньо зауважити, що нижній рядок у записі (7.4) підстановки є деякою перестановою із n елементів, а тому кількість підстановок у множині S_n дорівнює числу всеможливих перестановок із n елементів, тобто $n!$ за твердженням 3.1. \square

Нехай σ — довільна підстановка із S_n . Аналогічно, як у § 7.1, можна означити степінь σ^s підстановки і довести рівність $\sigma^s\sigma^t = \sigma^{s+t} = \sigma^t\sigma^s$ для довільних $s, t \in \mathbb{Z}$. Оскільки $|S_n| < \infty$, то для кожної підстановки $\sigma \in S_n$ знайдеться таке натуральне число k , що $\sigma^k = \varepsilon$.

Означення 7.14. Найменше з натуральних чисел k , при якому $\sigma^k = \varepsilon$, називають *порядком підстановки σ* .

Приклад 7.9. Підстановки σ і τ із прикладу 7.8 мають порядки 4 та 2 відповідно.

Існують підстановки, які деякі елементи переміщують, а деякі залишають на місці; причому переміщення відбувається, так би мовити, по колу (циклом). Наприклад, підстановка $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 6 & 5 & 1 \end{pmatrix}$ залишає на місці елементи 3 і 5, а решту переміщує так: $1 \rightarrow 2 \rightarrow 4 \rightarrow 6 \rightarrow 1$. Підстановки такого вигляду будемо називати циклами. Не всі підстановки є циклами. Наприклад, підстановка $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix}$ не є циклом.

Означення 7.15. Циклом $(i_1 i_2 \dots i_k)$, де i_1, \dots, i_k — деякі числа з множини $\{1, 2, \dots, n\}$, називається така підстановка $\sigma \in S_n$, яка ці числа циклічно переставляє

$$\sigma(i_1) = i_2, \quad \sigma(i_2) = i_3, \quad \dots, \quad \sigma(i_{k-1}) = i_k, \quad \sigma(i_k) = i_1,$$

а решта залишає на місці, тобто $\sigma(i) = i$ для довільного $i \notin \{i_1, i_2, \dots, i_k\}$.³ Множину елементів $\{i_1, i_2, \dots, i_k\}$ назовемо *орбітою* підстановки, яка відповідає циклу $(i_1 i_2 \dots i_k)$. Двоелементний цикл назовемо *транспозицією*.

Приклад 7.10. Підстановку $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ можна записати у вигляді циклу довжини 4

$$\sigma = (1 \ 2 \ 3 \ 4),$$

або, що те саме, у вигляді циклів $\sigma = (2 \ 3 \ 4 \ 1) = (3 \ 4 \ 1 \ 2) = (4 \ 1 \ 2 \ 3)$. Зауважимо також, що $\sigma^4 = \varepsilon$, звідки бачимо, що порядок підстановки σ дорівнює 4.

Означення 7.16. Два цикли з S_n назовемо *незалежними*, якщо орбіти, що їм відповідають, не мають спільних елементів.

Приклад 7.11. Розкладемо в добуток незалежних циклів підстановку $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$. Маємо

$$\sigma = (1 \ 4)(2 \ 3).$$

До речі, легко перевірити, що $\sigma^2 = \varepsilon$, а тому порядок цієї підстановки дорівнює 2.

³Звернемо увагу, що запис циклів у вигляді $(i_1 i_2 \dots i_k)$ або у вигляді (i_1, i_2, \dots, i_k) , тобто розділяючи елементи циклів комами, є питанням смаку читача. Залежно від ситуації ми використовуватимемо обидва записи.

Твердження 7.17. Якщо σ і τ незалежні цикли, то $\sigma\tau = \tau\sigma$.

Доведення. Позначимо через M_σ і M_τ орбіти, які відповідають циклам σ і τ . Якщо $i \in M_\sigma$, то $\sigma(i) \in M_\sigma$ та $i \notin M_\tau$. Якщо ж $i \in M_\tau$, то $\tau(i) \in M_\tau$ та $i \notin M_\sigma$. Тому для усіх $i \in \{1, 2, \dots, n\}$ маємо

$$(\tau\sigma)(i) = (\sigma\tau)(i) = \begin{cases} i, & \text{якщо } i \notin M_\sigma \cup M_\tau, \\ \sigma(i), & \text{якщо } i \in M_\sigma, \\ \tau(i), & \text{якщо } i \in M_\tau, \end{cases}$$

тобто $\sigma\tau = \tau\sigma$. □

Твердження 7.18. Кожна підстановка розкладається в добуток незалежних циклів.

Доведення. Для підстановки $\pi \in S_n$ через $k(\pi)$ позначимо кількість тих елементів i множини $M = \{1, 2, \dots, n\}$, для яких $\pi(i) \neq i$. Якщо $k(\pi) = 0$, то доведення очевидне. Нехай $k(\pi) = m > 0$. Припускаємо, що твердження доведене для всіх $\pi' \in S_n$ таких, що $k(\pi') < m$. Існує $i_1 \in M$ з властивістю $\pi(i_1) \neq i_1$. Нехай i_1 переходить в i_2, i_2 в i_3 і так далі. Нехай i_r перший елемент, який повторюється. Якщо $i_r = i_k$, де $2 \leq k \leq r - 1$, то отримаємо два різних елементи i_{r-1} та i_{k-1} , які підстановка π переводить в один і той же елемент i_k . Це неможливо, бо π біективне відображення. Тому $i_r = i_1$ і ми отримуємо цикл

$$\sigma_1 = (i_1 \ i_2 \ \dots \ i_{r-1}).$$

Розглянемо тепер підстановку π_1 , для якої

$$\pi_1(j) = \begin{cases} j, & \text{якщо } j \in \{i_1, \dots, i_{r-1}\}, \\ \pi(j), & \text{якщо } j \notin \{i_1, \dots, i_{r-1}\}. \end{cases}$$

Легко перевірити, що $\pi = \sigma_1\pi_1 = \pi_1\sigma_1$. Далі $k(\pi_1) = k(\pi) - r < k(\pi)$. Тому, за припущенням, підстановка π_1 розкладається в добуток незалежних циклів $\pi_1 = \sigma_2 \dots \sigma_t$. Отже, π теж розкладається в добуток незалежних циклів: $\pi = \sigma_1\pi_1 = \sigma_1\sigma_2 \dots \sigma_t$. □

Зауваження 7.1. Легко переконатися, що довільна підстановка розкладається в добуток незалежних циклів однозначно. В той же час, якщо не вимагати умови незалежності циклів, розклад не є єдиним. Наприклад, $(\frac{1}{2} \frac{2}{3} \frac{3}{1}) = (1 \ 2)(2 \ 3) = (1 \ 3)(1 \ 2)$.

Зауваження 7.2. Якщо підстановка τ розкладається в добуток незалежних циклів довжин k_1, k_2, \dots, k_t , то порядок підстановки τ дорівнює найменшому спільному кратному цих довжин

$$\text{ord}(\tau) = \text{НСК}\{k_1, k_2, \dots, k_t\}.$$

Приклад 7.12. Розглянемо підстановку $\tau = (\frac{1}{5} \frac{2}{6} \frac{3}{7} \frac{4}{8} \frac{5}{3} \frac{6}{2} \frac{7}{1}) \in S_8$. Оскільки $\tau = (2 \ 6 \ 3 \ 7)(1 \ 5 \ 8)$, то $\text{ord}(\tau) = \text{НСК}\{4, 3\} = 12$.

Твердження 7.19. Кожна підстановка розкладається в добуток транспозицій.

Доведення. Оскільки з рівності

$$(i_1 \ i_2 \ \dots \ i_k) = (i_1 \ i_k)(i_1 \ i_{k-1}) \dots (i_1 \ i_3)(i_1 \ i_2). \quad (7.5)$$

випливає, що будь-який цикл можна розкласти в добуток транспозицій, то розкладаємо спочатку підстановку в добуток незалежних циклів (тврдження 7.18), а тоді кожний цикл, в свою чергу, розкладаємо в добуток транспозицій за правилом (7.5). □

Як ми уже говорили вище, поняття підстановки та перестановки тісно пов'язані між собою: у довільній підстановці

$$\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \in S_n$$

обидва рядки $(1 \ 2 \ \dots \ n)$ та $(i_1 \ i_2 \ \dots \ i_n)$ є перестановками з n чисел. Цим зв'язок між підстановками і перестановками не обмежується.

Означення 7.17. Підстановка $\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ називається *парною* (*непарною*), якщо відповідна їй перестановка $(i_1 \ i_2 \ \dots \ i_n)$ парна (непарна).

Приклад 7.13. Підстановка $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 5 & 4 & 6 & 7 & 2 & 9 & 1 & 3 & 8 & 11 & 10 \end{pmatrix}$ парна, оскільки $\text{inv}(5, 4, 6, 7, 2, 9, 1, 3, 8, 11, 10) = 18$.

Теорема 7.20. Парна підстановка розкладається в добуток парного числа транспозицій, а непарна — в добуток непарного числа транспозицій.

Доведення. Спочатку доведемо, що множення підстановки справа на транспозицію змінює її парність. Дійсно,

$$\begin{pmatrix} \dots & r & \dots & s & \dots \\ \dots & i_r & \dots & i_s & \dots \end{pmatrix} (r \ s) = \begin{pmatrix} \dots & r & \dots & s & \dots \\ \dots & i_s & \dots & i_r & \dots \end{pmatrix},$$

тобто множення підстановки на цикл $(r \ s)$ дає транспозицію елементів i_r та i_s в нижньому рядку підстановки. Оскільки за твердженням 3.3 транспозиція змінює парність перестановки, то одержуємо, що початкова та отримана підстановки мають різну парність. Далі, за твердженням 7.19 кожна підстановка σ розкладається в добуток транспозицій

$$\sigma = \tau_1 \tau_2 \dots \tau_k.$$

Перепишемо цю рівність у вигляді

$$\sigma = \varepsilon \tau_1 \tau_2 \dots \tau_k,$$

де ε — одинична підстановка. Бачимо, що підстановка σ одержується з одиничної підстановки ε домноженням справа на транспозиції τ_1, \dots, τ_k . Оскільки множення підстановки на транспозицію змінює її парність, а ε — парна підстановка, то отримуємо, що σ — парна підстановка тоді і тільки тоді, коли k — парне число. \square

Легко бачити, що квадрат будь-якої транспозиції дорівнює одиничній підстановці, тобто $(r \ s)^2 = \varepsilon$. Звідси випливає, що якщо $\sigma = \tau_1 \tau_2 \dots \tau_k$, то $\sigma^{-1} = \tau_k \tau_{k-1} \dots \tau_1$. Це означає, що підстановки σ і σ^{-1} мають однакову парність. Тому підстановка, обернена до парної, є парною. Крім цього, добуток підстановок однакової парності є парною підстановкою. Це говорить про те, що множина всіх парних підстановок із S_n утворює підгрупу групи S_n (її називають *знакозмінною групою* і позначають A_n). Очевидно, що $|A_n| = \frac{1}{2}|S_n| = \frac{n!}{2}$.

Означення 7.18. Нехай $\sigma \in S_n$ і $\sigma = \tau_1 \tau_2 \dots \tau_k$ — довільний розклад підстановки σ у добуток k транспозицій. Число $\text{sgn } \sigma = (-1)^k$ називається *сигнатурою* (знаком) підстановки σ . Підстановка $\sigma \in S_n$ є *парною*, якщо $\text{sgn } \sigma = 1$ і *непарною*, якщо $\text{sgn } \sigma = -1$.

Означення 7.19. Якщо підстановка $\sigma \in S_n$ розкладена у добуток незалежних циклів довжин k_1, k_2, \dots, k_m , то сума d цих довжин, зменшених на 1, називається *декрементом* підстановки σ : $d = d(\sigma) = \sum_{t=1}^m (k_t - 1)$. Легко переконатись, що $\text{sgn } \sigma = (-1)^d$.

Приклад 7.14. Розглянемо підстановку $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 5 & 4 & 6 & 7 & 2 & 9 & 1 & 3 & 8 & 11 & 10 \end{pmatrix}$. Оскільки

$$\sigma = (1 \ 5 \ 2 \ 4 \ 7)(3 \ 6 \ 9 \ 8)(10 \ 11),$$

то $k_1 = 5$, $k_2 = 4$, $k_3 = 2$ і $\text{sgn}(\sigma) = (-1)^{4+3+1} = 1$.

7.5. Гомоморфізми та ізоморфізми груп

Нехай (G_1, \circ) і $(G_2, *)$ — дві довільні групи.

Означення 7.20. Відображення $\varphi: G_1 \rightarrow G_2$ називається *гомоморфізмом груп* (G_1, \circ) і $(G_2, *)$, якщо для довільних $a, b \in G_1$ виконується рівність

$$\varphi(a \circ b) = \varphi(a) * \varphi(b). \quad (7.6)$$

Очевидно, що якщо в групах G_1 і G_2 визначено операцію множення, то рівність (7.6) перешипиться так: $\varphi(ab) = \varphi(a)\varphi(b)$.

Ін'єктивний гомоморфізм називається *мономорфізмом*, сюр'єктивний гомоморфізм — *епіморфізмом*, а біективний гомоморфізм груп називається *ізоморфізмом* цих груп. Якщо існує ізоморфізм груп G_1 і G_2 , то кажуть, що ці групи *ізоморфні* і записують $G_1 \simeq G_2$.

Приклади 7.15. 1. Повна лінійна група $GL_n(\mathbb{R})$ гомоморфно відображається на мультиплікативну групу \mathbb{R}^* , якщо визначити відображення правилом $A \mapsto \det A$ для всіх $A \in GL_n(\mathbb{R})$.

2. Розглянемо відображення $\varphi: S_n \rightarrow C_2$, для якого

$$\varphi(\pi) = \begin{cases} 1, & \text{якщо підстановка } \pi \text{ парна,} \\ -1, & \text{якщо підстановка } \pi \text{ непарна.} \end{cases}$$

Тоді для довільних $\sigma, \tau \in S_n$ виконується співвідношення

$$\varphi(\sigma\tau) = \begin{cases} 1, & \text{якщо } \sigma \text{ і } \tau \text{ мають однакову парність,} \\ -1, & \text{в іншому випадку} \end{cases} = \varphi(\sigma)\varphi(\tau).$$

Отже, задане відображення φ є гомоморфізмом (але не ізоморфізмом!) груп S_n і C_2 .

3. Кожне додатне число $z \neq 1$ визначає гомоморфізм адитивної групи всіх дійсних чисел \mathbb{R} в мультиплікативну групу додатних дійсних чисел \mathbb{R}^+ за правилом $\varphi(a) = z^a$ для довільного $a \in \mathbb{R}$. Дійсно, $\varphi(a+b) = z^{a+b} = z^a z^b = \varphi(a)\varphi(b)$ для всіх $a, b \in \mathbb{R}$. Задане відображення $\varphi: \mathbb{R} \rightarrow \mathbb{R}^+$ має обернене відображення $\psi: \mathbb{R}^+ \rightarrow \mathbb{R}$, яке діє за правилом $\psi(a) = \log_z(a)$ для довільного $a \in \mathbb{R}^+$. Отже, за теоремою 1.5 відображення φ біективне і тому групи (\mathbb{R}^+, \cdot) і $(\mathbb{R}, +)$ ізоморфні.

Означення 7.21. Гомоморфізм групи G в себе називається *ендоморфізмом*. Множину всіх ендоморфізмів групи G позначають $\text{End } G$. Оскільки тотожне відображення ε_G є ендоморфізмом групи G , то $\text{End } G \neq \emptyset$.

Твердження 7.21. Якщо $\varphi: G_1 \rightarrow G_2$ — гомоморфізм груп (G_1, \circ) та $(G_2, *)$, то

- 1) образ нейтрального елемента групи G_1 є нейтральним елементом групи G_2 ;
- 2) множина $\varphi(G_1)$ є підгрупою групи G_2 .

Доведення. 1) Нехай e_1 та e_2 — нейтральні елементи груп G_1 та G_2 відповідно, a_1 — довільний елемент групи G_1 . Маємо

$$e_2 * \varphi(a_1) = \varphi(a_1) = \varphi(e_1 \circ a_1) = \varphi(e_1) * \varphi(a_1).$$

Застосувавши до рівності $e_2 * \varphi(a_1) = \varphi(e_1) * \varphi(a_1)$ закон скорочення (тврдження 7.3), одержимо $e_2 = \varphi(e_1)$, що й потрібно було довести.

2) Покажемо, що множина $\varphi(G_1)$ задовільняє умови критерію підгрупи. Нехай $a_2, b_2 \in \varphi(G_1)$. Тоді існують такі $a_1, b_1 \in G_1$, що $a_2 = \varphi(a_1)$, $b_2 = \varphi(b_1)$, причому

$$a_2 * b_2 = \varphi(a_1) * \varphi(b_1) = \varphi(a_1 \circ b_1).$$

Отже, $a_2 b_2 \in \varphi(G_1)$. Далі, за доведеним,

$$e_2 = \varphi(e_1) = \varphi(a_1 \circ a_1^{-1}) = \varphi(a_1) * \varphi(a_1^{-1}).$$

Звідси $a_2^{-1} = \varphi(a_1)^{-1} = \varphi(a_1^{-1}) \in \varphi(G_1)$. □

Твердження 7.22. Нехай (G_1, \circ) , $(G_2, *)$, (G_3, \bullet) — групи. Тоді

- 1) якщо φ — ізоморфізм груп G_1 і G_2 , то φ^{-1} — ізоморфізм груп G_2 і G_1 ;
- 2) якщо ψ — ізоморфізм груп G_2 і G_3 , то добуток $\psi\varphi$ є ізоморфізмом груп G_1 і G_3 .

Доведення. 1) Досить показати, що $\varphi^{-1}(a_2 * b_2) = \varphi^{-1}(a_2) \circ \varphi^{-1}(b_2)$ для всіх $a_2, b_2 \in G_2$. Оскільки відображення φ — біективне, то для елементів $a_2, b_2 \in G_2$ існують такі елементи $a_1, b_1 \in G_1$, що $\varphi(a_1) = a_2$, $\varphi(b_1) = b_2$. Тоді

$$\varphi^{-1}(a_2 * b_2) = \varphi^{-1}(\varphi(a_1) * \varphi(b_1)) = \varphi^{-1}(\varphi(a_1 \circ b_1)) = a_1 \circ b_1 = \varphi^{-1}(a_2) * \varphi^{-1}(b_2).$$

2) За теоремою 1.2 добуток $\psi\varphi$ є біективним відображенням групи G_1 у групу G_3 . Крім цього, для довільних $a, b \in G_1$ маємо

$$(\psi\varphi)(a \circ b) = \psi(\varphi(a \circ b)) = \psi(\varphi(a) * \varphi(b)) = (\psi\varphi)(a) \bullet (\psi\varphi)(b),$$

що й потрібно було довести. \square

Оскільки однічне відображення ε_G є ізоморфізмом групи G в себе, з твердження 7.22 випливає, що відношення ізоморфізму груп задовольняє умовам відношення еквівалентності (див. §1.5). Це дозволяє вивчати групи з точністю до ізоморфізму⁴, тобто не розрізняти ізоморфні групи.

Теорема 7.23. Всі циклічні групи одного і того ж порядку (зокрема, нескінченного) ізоморфні.

Доведення. Якщо $\langle a \rangle$ — нескінчена циклічна група, то усі цілі степені a^n різні. Задамо відображення $\varphi: \langle a \rangle \rightarrow (\mathbb{Z}, +)$ правилом $a^n \mapsto n$. Біективність такого відображення φ очевидна, а властивість

$$\varphi(a^m a^n) = \varphi(a^{m+n}) = m + n = \varphi(a^m) + \varphi(a^n), \quad \text{де } m, n \in \mathbb{Z},$$

випливає із твердження 7.2.

Нехай тепер $\langle a \rangle$ і $\langle b \rangle$ — дві скінченні циклічні групи порядку k (без зменшення загальності вважатимемо, що на цих групах визначена операція множення). Задамо біективне відображення $\varphi: \langle a \rangle \rightarrow \langle b \rangle$ правилом $a^s \mapsto b^s$ для усіх $s = 0, 1, \dots, k - 1$. За алгоритмом подільності для довільних степенів $n, m = 0, 1, \dots, k - 1$ існують такі цілі числа q, r , що $n + m = kq + r$ і $0 \leq r \leq k - 1$. Тоді $a^{m+n} = a^{kq+r} = (a^k)^q a^r = a^r$ і, аналогічно, $b^{m+n} = b^r$. Звідси отримаємо

$$\varphi(a^{m+n}) = \varphi(a^r) = b^r = b^{m+n} = b^m b^n = \varphi(a^m) \varphi(a^n),$$

що й потрібно було довести. \square

Приклад 7.16. Нескінчена група може бути ізоморфна своїй підгрупі. Дійсно, аддитивна група $(\mathbb{Z}, +)$ містить власну підгрупу $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$, де n — фіксоване неодиничне натуральне число. Легко перевірити, що відображення $\varphi_n: \mathbb{Z} \rightarrow n\mathbb{Z}$, задане правилом $\varphi_n(z) = nz$ для довільного $z \in \mathbb{Z}$, є ізоморфізмом. Крім цього, зауважимо, що \mathbb{Z} і $n\mathbb{Z}$ — нескінченні циклічні групи, у яких твірними є відповідно 1 (або -1) і n (або $-n$); тому φ_n і відображення $z \mapsto -nz$ вичерпують всі ізоморфізми $\mathbb{Z} \rightarrow n\mathbb{Z}$.

Теорема 7.24 (Келі). Довільна скінчена група порядку n ізоморфна деякій підгрупі симетричної групи S_n .

⁴Фраза «з точністю до ізоморфізму» відображає сутність не тільки теорії груп, яка прагне об'єднати в один клас усі ізоморфні групи, але й математики в цілому, яка без таких узагальнень не мала б змісту.

Доведення. Розглянемо групу G порядку n . Оскільки, як було сказано у §7.4, природа елементів, які переставляються підстановками із S_n , несуттєва, можна вважати, що S_n — група всіх біективних відображення групи G в себе. Для довільного елемента $a \in G$ розглянемо відображення $\sigma_a: G \rightarrow G$, яке визначимо формулою $\sigma_a(g) = ag$ для довільного $g \in G$. Якщо g_1, g_2, \dots, g_n — всі елементи групи G , то ag_1, ag_2, \dots, ag_n будуть тими ж самими елементами групи G , але розташованими в якомусь іншому порядку (чи в тому ж самому, якщо $a = e$ — одиничний елемент групи G). Дійсно, якщо $ag_i = ag_j$, то за законом скорочення $g_i = g_j$. Отже, σ_a — біективне відображення (тобто підстановка). Оберненим до відображення σ_a буде $\sigma_a^{-1} = \sigma_{a^{-1}}$. Одиничним відображенням є, природно, σ_e . Знову використавши асоціативність множення в G , отримаємо $\sigma_{ab}(g) = (ab)g = a(bg) = \sigma_a(\sigma_b(g))$, тобто $\sigma_{ab} = \sigma_a \sigma_b$. Отож, множина $\sigma_e, \sigma_{g_2}, \dots, \sigma_{g_n}$ утворює підгрупу (позначимо її H) в групі всіх біективних відображення групи G на себе, тобто в S_n . Ми маємо включення $H \subset S_n$ і маємо відповідність $a \mapsto \sigma_a \in H$, яка володіє усіма властивостями ізоморфізму. \square

Теорема Келі, незважаючи на свою простоту, має важливе застосування в теорії груп. Вона виділяє деякий універсальний об'єкт (множину $\{S_n \mid n = 1, 2, \dots\}$ симетричних груп) — вмістилище усіх скінчених груп, які розглядаються з точністю до ізоморфізму.

Зауваження 7.3. Ізоморфізм $\varphi: G \rightarrow G$ групи G в себе називається *автоморфізмом*. Множину всіх автоморфізмів групи G позначатимемо $\text{Aut } G$. Одиничне відображення e_G є автоморфізмом, а тому $\text{Aut } G \neq \emptyset$. Як правило, група G володіє й нетривіальними автоморфізмами. Перша властивість твердження 7.22 показує, що відображення, обернене до автоморфізму, також буде автоморфізмом. Крім того, якщо $\varphi, \psi \in \text{Aut } G$, то $(\varphi\psi)(ab) = \varphi(\psi(ab)) = \varphi(\psi(a)\psi(b)) = (\varphi\psi)(a) (\varphi\psi)(b)$ для довільних $a, b \in G$. Отже, множина $\text{Aut}(G)$ усіх автоморфізмів групи G утворює групу — підгрупу групи всіх біективних відображень $G \rightarrow G$.

Зауваження 7.4. В групі автоморфізмів $\text{Aut } G$ міститься одна особлива підгрупа. Вона позначається символом $\text{Int } G$ і називається *групою внутрішніх автоморфізмів*. Її елементами є відображення $i_a: g \mapsto aga^{-1}$ для довільних $g \in G$. Нескладні міркування показують, що i_a задовольняє всім властивостям, які вимагаються від автоморфізму. Крім цього, $i_a^{-1} = i_{a^{-1}}$, $i_e = \varepsilon_G$ — одиничний автоморфізм, $i_a i_b = i_{ab}$ (оскільки $(i_a i_b)(g) = i_a(i_b(g)) = i_a(bgb^{-1}) = abgb^{-1}a^{-1} = abg(ab)^{-1} = i_{ab}(g)$), а тому $\text{Int } G$ — група. Остання рівність показує, що відображення $\varphi: G \rightarrow \text{Int}(G)$ групи G на групу $\text{Int}(G)$ її внутрішніх автоморфізмів, яке визначається формулою $\varphi(a) = i_a$, $a \in G$, є гомоморфізмом. Проте властивість біективності при цьому не зобов'язана виконуватись. Якщо, наприклад, G — абелева група, то $aga^{-1} = g$ для всіх $a, g \in G$, тому $i_a = i_e$ і вся група $\text{Int}(G)$ складається лише з одного одиничного елемента i_e .

7.6. Суміжні класи. Теорема Лагранжа. Відношення еквівалентності

Означення 7.22. Нехай H — підгрупа групи G . Зафіксуємо елемент $a \in G$. Множину $aH = \{ah \mid h \in H\}$ називають *лівим суміжним класом* групи G за підгрупою H . Аналогічно, $Ha = \{ha \mid h \in H\}$ — *правий суміжний клас* групи G за підгрупою H .

Твердження 7.25. Якщо H — підгрупа групи G і $a, b \in G$, то

- 1) $aH = bH$ тоді і лише тоді, коли $a^{-1}b \in H$;
- 2) $|H| = |aH| = |bH|$;
- 3) якщо $b \in aH$, то $aH = bH$;
- 4) ліві (праві) суміжні класи групи G за підгрупою H або співпадають, або не перетинаються.

Доведення. 1) Дійсно, $b = ah$ тоді і лише тоді, коли $a^{-1}b = h \in H$.

2) Для доведення покажемо, що існують бієктивні відображення $H \rightarrow aH$ та $H \rightarrow Hb$. Дійсно, відображення $\varphi: H \rightarrow aH$, для якого $\varphi(h) = ah$, є бієктивним, оскільки для нього існує обернене $\varphi^{-1}: aH \rightarrow H$, $\varphi^{-1}(ah) = a^{-1}(ah) = h$. Аналогічно, відображення $\psi: H \rightarrow Hb$, $\psi(h) = hb$, є бієктивним.

3) Очевидно, що $bH \subseteq aH$. За умовою $b = ah$ для деякого $h \in H$. Як наслідок, для довільного $u \in H$ отримаємо $au = b(h^{-1}u)$, де $h^{-1}u \in H$. Звідси $aH \subseteq bH$, тобто $aH = bH$.

4) Очевидно, оскільки, якщо ліві (праві) суміжні класи мають хоча б один спільний елемент, то за властивістю 3) вони співпадають. \square

Теорема 7.26 (Лагранж). Порядок будь-якої підгрупи H скінченної групи G є дільником порядку групи G .

Доведення. Розглянемо ліві суміжні класи групи G за підгрупою H . Кожний елемент $a \in G$ лежить в деякому суміжному класі, а саме в aH . Оскільки ліві суміжні класи групи G за підгрупою H або співпадають, або не перетинаються і є рівнопотужними H (тврдження 7.25), то $|G| = |H| \cdot k$, де k — кількість лівих суміжних класів групи G за підгрупою H . \square

Аналогічно можна довести, що $|G| = |H| \cdot k$, де k — кількість правих суміжних класів групи G за підгрупою H . Звідси випливає правильність такого твердження.

Твердження 7.27. Множина лівих суміжних класів групи G за підгрупою H рівнопотужна множині правих суміжних класів.

Означення 7.23. Кількість лівих (правих) суміжних класів групи G за підгрупою H називається *індексом підгрупи H в групі G* і позначається $|G:H|$.

Наслідок 7.28. Порядок кожного елемента скінченної групи G ділить порядок групи G .

Доведення. За твердженням 7.10 порядок елемента дорівнює порядку циклічної підгрупи, породженої цим елементом. \square

Наслідок 7.29. Якщо порядок групи G є простим числом, то вона має лише тривіальні підгрупи і є циклічною.

Доведення. Нехай $|G| = p$, де p — просте число. Оскільки єдиними дільниками простого числа p є числа 1 і p , то за теоремою Лагранжа у ній не може існувати нетривіальних підгруп. Крім того, оскільки в цій групі порядки всіх елементів не можуть дорівнювати одиниці, то існує такий елемент $a \in G$, що $\text{ord}(a) = p$. А тому $\langle a \rangle = G$. \square

Приклади 7.17. 1. Нехай $G = S_n$, а $H = A_n$ — підгрупа парних підстановок (знакозмінна група).

Нехай $\sigma \in S_n$. Тоді множина σA_n складається з усіх парних підстановок, якщо підстановка σ — парна, і з усіх непарних підстановок в іншому випадку. З таких самих підстановок (всіх парних або всіх непарних) складається й правий суміжний клас $A_n\sigma$. Тому в цьому випадку

$$\sigma A_n = A_n\sigma = \begin{cases} A_n, & \text{якщо } \sigma \text{ — парна підстановка,} \\ S_n \setminus A_n, & \text{в іншому випадку.} \end{cases}$$

Бачимо, що тут ліві суміжні класи збігаються з правими. Наступний приклад показує, що так трапляється не завжди.

2. Нехай $G = S_3$, $H = \{e, (1 2)\}$. Тоді $(2 3)H = \{(2 3), (1 3 2)\}$, а $H(2 3) = \{(2 3), (1 2 3)\}$.

Ліві (праві) суміжні класи групи G за підгрупою H є класами еквівалентних стосовно відношення еквівалентності на множині елементів групи G , які визначаються за допомогою підгрупи H . А саме, задамо на групі G відношення еквівалентності \sim_H . Вважатимемо, що $a \sim_H b$, якщо $a^{-1}b \in H$. Переконаємося, що \sim_H — відношення еквівалентності.

1. Оскільки $a^{-1}a = e \in H$, то $a \sim_H a$.
2. Якщо $a \sim_H b$, то $a^{-1}b \in H$ і $(a^{-1}b)^{-1} = b^{-1}a \in H$, а тому $b \sim_H a$.
3. Нехай $a \sim_H b$ і $b \sim_H c$. Тоді $a^{-1}b \in H$ і $b^{-1}c \in H$. Звідси $a^{-1}bb^{-1}c = a^{-1}c \in H$, а тому $a \sim_H c$.

Таким чином, \sim_H — відношення еквівалентності на G . Тому група G розбивається на класи еквівалентних елементів, причому різні класи попарно не перетинаються. Кожний такий клас \bar{a} складається із таких елементів $g \in G$, що $a^{-1}g \in H$, тобто $a^{-1}g = h \in H$, $g = ah$. Отже, клас еквівалентності \bar{a} елемента a — це множина $aH = \{ah \mid h \in H\}$. Очевидно, що $G = \bigcup_{a \in G} aH$. Ми бачимо, що ліві суміжні класи є класами еквівалентних елементів стосовно відношення еквівалентності \sim_H . Аналогічно, праві суміжні класи одержуються з відношення еквівалентності ${}_H\sim$, для якого $a \sim_H b$ тоді і лише тоді, коли $ab^{-1} \in H$. Тому група G є об'єднанням як лівих, так і правих суміжних класів:

$$G = \bigcup_{a \in G} aH = \bigcup_{a \in G} Ha.$$

7.7. Розбиття групи, узгоджені з операцією. Факторгрупи

Серед відношень еквівалентності, заданих на групі G , особливу роль відіграють ті відношення еквівалентності, які узгоджені з груповою операцією.

Означення 7.24. Відношення еквівалентності \sim на групі G називається *узгодженим з операцією*, якщо для будь-яких елементів $a, b, a', b' \in G$ з $a \sim a'$ і $b \sim b'$ випливає $ab \sim a'b'$.

Приклад 7.18. Розглянемо підгрупу A_n парних підстановок в групі S_n . Ця підгрупа визначає розбиття $S_n = A_n \cup (S_n \setminus A_n)$ групи S_n (нагадаємо, що задання розбиття множини рівносильне заданню відношення еквівалентності на цій множині). Очевидно, добуток двох довільних парних підстановок є парною підстановкою, добуток двох непарних підстановок є парною, а добуток парної і непарної підстановок є непарною підстановкою. Тому ми маємо тут розбиття S_n (відношення еквівалентності на S_n), яке узгоджене з операцією.

Означення 7.25. Підгрупа H групи G називається *нормальною* (*нормальним дільником*), якщо для будь-якого $a \in G$ виконується рівність $aH = Ha$ (ліві суміжні класи збігаються з правими). Позначатимемо: $H \triangleleft G$.

- Приклади 7.19.**
1. В будь-якій групі G існують нормальні підгрупи, а саме $\{e\}$ та G (їх часто називають *тривіальними нормальними підгрупами*).
 2. Якщо група G абелева, то кожна підгрупа її підгрупа нормальна.
 3. Підгрупа A_n є нормальною підгрупою групи S_n (див. приклад 7.17).
 4. Будь-яка підгрупа H індексу 2 в групі G є нормальною. Дійсно, розглянемо в групі G ліві суміжні класи за підгрупою H . Оскільки H є підгрупою індексу 2, то цих суміжних класів буде два: eH та aH , де $a \notin H$. Правих суміжних класів також буде два: He та Ha . Зрозуміло, що $eH = H = He$ і, оскільки суміжні класи утворюють розбиття групи, то $aH = Ha$. Отже, $H \triangleleft G$.
 5. Група поворотів квадрата є нормальною підгрупою всіх симетрій квадрата.

Твердження 7.30. Підгрупа H групи G є нормальною в G тоді і тільки тоді, коли $aha^{-1} \in H$ для всіх $h \in H$, $a \in G$.

Доведення. Нехай $H \triangleleft G$, тобто $aH = Ha$ для довільного $a \in G$. Тоді для кожного $h \in H$ існує такий елемент $u \in H$, що $ah = ua$. Звідси $aha^{-1} = u \in H$.

Навпаки, якщо $aha^{-1} \in H$ для всіх $h \in H$, $a \in G$, то $aha^{-1} = u$ для деякого $u \in H$. Тоді $ah = ua$, звідки $aH \subset Ha$. З іншого боку, оскільки $a^{-1}h(a^{-1})^{-1} \in H$ для всіх $h \in H$, то $Ha \subset aH$. Отже, $aH = Ha$, тобто $H \triangleleft G$. \square

Теорема 7.31 (про розбиття групи). Розбиття групи G на класи еквівалентності узгоджене з груповою операцією тоді і тільки тоді, коли воно є розбиттям на суміжні класи за деякою нормальнюю підгрупою H групи G .

Доведення. Необхідність. Нехай $G = \bigcup_i G_i$ — розбиття на класи еквівалентності G_i , узгоджене з груповою операцією. Без зменшення загальності, припустимо, що нейтральний елемент e групи G належить до G_1 . Покажемо, що G_1 — підгрупа групи G . Нехай $g_1, g_2 \in G_1$. Тоді $g_1 \sim e, g_2 \sim e$, отже, $g_1 g_2 \sim e$, а тому $g_1 g_2 \in G_1$. Далі, якщо $g \sim e$ і, очевидно, $g^{-1} \sim g^{-1}$, то $g g^{-1} \sim e g^{-1}$, тобто $e \sim g^{-1}$ і тому $g^{-1} \in G_1$. Отже, за критерієм підгрупи, G_1 є підгрупою групи G . Позначимо підгрупу G_1 через H .

Тепер покажемо, що $H \triangleleft G$. Нехай $a \in G, h \in H$. Тоді $h \sim e$ і $aha^{-1} \sim aea^{-1} = e$, тобто $aha^{-1} \in H$ і, в за твердженням 7.30, H — нормальнна підгрупа групи G .

Насамкінець, переконаємося, що кожен клас еквівалентності G_i є суміжним класом за підгрупою H . Зафіксуємо елемент $g_i \in G_i$. Нехай g — довільний елемент множини G_i . Тоді з $g \sim g_i$ випливає $g_i^{-1}g \sim g_i^{-1}g_i = e$. Отже, елемент $u = g_i^{-1}g$ міститься в H , тому $g = g_i u \in g_i H$, тобто $G_i \subseteq g_i H$. Крім цього, якщо $u \in H$, то $u \sim e$ і тому $g_i u \sim g_i$. Це означає, що $g_i u \in G_i$, тобто $g_i H \subseteq G_i$ і, остаточно, $G_i = g_i H$.

Достатність. Нехай $H \triangleleft G$ і $G = \bigcup aH$ — розбиття G на суміжні класи за підгрупою H . Доведемо, що це розбиття узгоджене з операцією, тобто покажемо, що якщо $a \sim_H a', b \sim_H b'$, то $ab \sim_H a'b'$ для будь-яких елементів $a, b, a', b' \in G$. Дійсно, оскільки $a \sim_H a', b \sim_H b'$, то існують такі елементи $h_1, h_2 \in H$, що $a = a'h_1, b = b'h_2$. З нормальності підгрупи H випливає, що знайдеться такий елемент $h_3 \in H$, що $h_1 b' = b'h_3$. Звідси $ab = a'h_1 b'h_2 = a'b'h_3 h_2 = a'b'h_4$, де $h_4 = h_3 h_2 \in H$. Отже, $ab \sim_H a'b'$ і наше розбиття узгоджене з операцією. \square

Нехай $G = \bigcup_{i \in \mathcal{I}} G_i$ — розбиття групи G на суміжні класи G_i , узгоджене з груповою операцією. Нагадаємо, що коли задане розбиття (відношення еквівалентності) деякої множини, то множину, елементами якої є суміжні класи, називають *фактормножиною* (див. означення 1.20). На фактормножині $\{G_i \mid i \in \mathcal{I}\}$ означимо алгебричну операцію: *добутком класів еквівалентності* G_i та G_j назовемо такий клас G_k ($G_k = G_i \cdot G_j$), в якому лежать добутки $g_i g_j$ для всіх $g_i \in G_i, g_j \in G_j$. Оскільки розбиття узгоджене з операцією, то G_k не залежить від конкретного вибору елементів g_i та g_j , а залежить лише від вибору класів G_i та G_j , тобто так задана алгебраїчна операція на фактормножині $\{G_i \mid i \in \mathcal{I}\}$ означена коректно. Крім цього, оскільки за теоремою 7.31 розбиття групи G , узгоджене з операцією, є обов'язково розбиттям за деякою нормальнюю підгрупою H , то суміжні класи G_i є суміжними класами групи G за нормальнюю підгрупою H : $G_i = g_i H = Hg_i$.

Позначимо символом G/H фактормножину $\{G_i \mid i \in \mathcal{I}\} = \{aH \mid a \in G\}$. Означення алгебричної операції в G/H можна переформулювати у більш зручному вигляді.

Означення 7.26. Якщо $aH, bH \in G/H$, то

$$aH bH = abH. \quad (7.7)$$

Твердження 7.32. Множина G/H є групою стосовно алгебричної операції (7.7) над її елементами.

Доведення. Оскільки в множині G/H стосовно операції добутку суміжних класів нейтральним елементом є суміжний клас $eH = H$ і $(aH)^{-1} = a^{-1}H$ для довільного $a \in G$, то доведемо лише асоціативність заданої операції. Дійсно,

$$aH(bHcH) = aH(bcH) = a(bc)H = (ab)cH = abHcH = (aHbH)cH$$

для довільних $a, b, c \in G$. \square

Означення 7.27. Група G/H називається *факторгрупою* групи G за нормальною підгрупою H .

Приклади 7.20. 1. Як нам уже відомо з прикладу 7.19, $A_n \triangleleft S_n$. Легко бачити, що факторгрупа S_n/A_n складається з двох елементів A_n і $S_n \setminus A_n$.

2. Оскільки $\text{Int } G \triangleleft \text{Aut } G$ для довільної групи G (доведіть це самостійно), то $\text{Aut } G / \text{Int } G$ є факторгрупою. Цю факторгрупу позначають $\text{Out } G := \text{Aut } G / \text{Int } G$ і називають *групою зовнішніх автоморфізмів*.

Твердження 7.33. Якщо $H \triangleleft G$, то відображення $\pi: G \rightarrow G/H$, яке задане правилом $\pi(a) = aH$ для усіх $a \in G$, є гомоморфізмом груп G та G/H .

Доведення. Очевидно, оскільки $\pi(ab) = abH = aHbH = \pi(a)\pi(b)$ для усіх $a, b \in G$. \square

Означення 7.28. Якщо G — група і $H \triangleleft G$, то гомоморфізм $\pi: G \rightarrow G/H$, де $\pi(a) = aH$ для усіх $a \in G$, називають *канонічним*.

Приклади 7.21. 1. Розглянемо відображення $\varphi: S_n \rightarrow S_n/A_n$, яке діє за правилом

$$\varphi(\sigma) = \begin{cases} A_n, & \text{якщо підстановка } \sigma \text{ — парна,} \\ S_n \setminus A_n, & \text{в іншому випадку.} \end{cases}$$

Очевидно, що так задане відображення є канонічним гомоморфізмом груп S_n і S_n/A_n .

2. Побудуємо ще одне відображення групи S_n/A_n . Для цього розглянемо групу C_2 , яка, нагадаємо, складається з двох елементів 1 і -1 зі звичайним множенням, $C_2 = (\{-1, 1\}, \cdot)$. Відображення $\varphi: S_n/A_n \rightarrow C_2$, для якого $\varphi(A_n) = 1$, $\varphi(S_n \setminus A_n) = -1$, як легко бачити, ізоморфізмом груп S_n/A_n і C_2 .
3. Розглянемо підгрупу \mathbb{Z} адитивної групи \mathbb{Q} . Оскільки \mathbb{Q} — абелева група, то $\mathbb{Z} \triangleleft \mathbb{Q}$. Факторгрупа \mathbb{Q}/\mathbb{Z} складається з суміжних класів $\frac{m}{n} = \frac{m}{n} + \mathbb{Z}$, де $\frac{m}{n} \in \mathbb{Q}$. У кожному такому суміжному класі $\frac{m}{n}$ міститься єдине раціональне число $\frac{a}{b}$ з властивістю $0 \leq \frac{a}{b} < 1$ ($\frac{a}{b} = \frac{m}{n} - [\frac{m}{n}]$, де $[\frac{m}{n}]$ — ціла частина $\frac{m}{n}$). Це означає, що елементи групи \mathbb{Q}/\mathbb{Z} перебувають у біективній відповідності з раціональними числами $\frac{a}{b}$, $0 \leq \frac{a}{b} < 1$. Для прикладу, знайдемо суму елементів $\frac{3}{8}$ і $\frac{5}{7}$ групи \mathbb{Q}/\mathbb{Z} : $\frac{3}{4} + \frac{5}{7} = \frac{41}{28} = \frac{13}{28}$.

7.8. Теорема про гомоморфізми

Нехай $\varphi: G_1 \rightarrow G_2$ — гомоморфізм груп. Нам уже відомо (див. твердження 7.21), що множина $\varphi(G_1)$ гомоморфізму φ є підгрупою групи G_2 . Цю підгрупу називають *образом гомоморфізму* φ і позначають $\text{im } \varphi$. Введемо ще одне важливе поняття, пов'язане з гомоморфізмами.

Означення 7.29. Ядром гомоморфізму $\varphi: G_1 \rightarrow G_2$ називають множину $\ker \varphi := \{g_1 \in G_1 \mid \varphi(g_1) = e_2\}$, де e_2 — нейтральний елемент групи G_2 .

Як і образ гомоморфізму, ядро гомоморфізму $\varphi: G_1 \rightarrow G_2$ є підгрупою, але, на відміну від образу цього гомоморфізму, групи G_1 . Більше цього, правильним є таке твердження.

Твердження 7.34. Ядро гомоморфізму $\varphi: G_1 \rightarrow G_2$ є нормальною підгрупою групи G_1 .

Доведення. Якщо $a, b \in \ker \varphi$, то $\varphi(ab) = \varphi(a)\varphi(b) = e_2e_2 = e_2$ і $\varphi(a^{-1}) = \varphi(a)^{-1} = e_2^{-1} = e_2$, де e_2 — нейтральний елемент групи G_2 . Отже, за критерієм підгрупи, $\ker \varphi$ — підгрупа групи G_1 .

Нехай тепер $h \in \ker \varphi$, $a \in G$. Тоді за означенням гомоморфізму $\varphi(aha^{-1}) = \varphi(a)\varphi(h)\varphi(a^{-1}) = \varphi(a)e_2\varphi(a^{-1}) = e_2$. Тому $aha^{-1} \in \ker \varphi$ і, отже, $\ker \varphi \triangleleft G$ за твердженням 7.30. \square

Теорема 7.35. Якщо $\varphi: G_1 \rightarrow G_2$ — гомоморфізм груп, то існує ізоморфізм $\bar{\varphi}: G_1/\ker \varphi \xrightarrow{\sim} \text{im } \varphi$.

Доведення. Позначимо $H = \ker \varphi$ і нехай $aH \in G_1/H$. Означимо правило $\bar{\varphi}(aH) = \varphi(a)$ і перевіримо, що $\bar{\varphi}$ — біективний гомоморфізм.

Спочатку пересвідчимось, що правило $\bar{\varphi}$ є відображенням. Дійсно, якщо $aH = bH$, то $ab^{-1} \in \ker \varphi$, а тому $\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = e_2$, де e_2 — нейтральний елемент G_2 , і $\varphi(a) = \varphi(b)$.

Тепер покажемо, що відображення $\bar{\varphi}$ — біективне. Його сюр'ективність очевидна, а тому перевіримо лише його ін'ективність. Якщо $\bar{\varphi}(aH) = \bar{\varphi}(bH)$, то $\varphi(a) = \varphi(b)$, а, отже, $ab^{-1} \in \ker \varphi$ і тому $aH = bH$ за критерієм рівності суміжних класів.

Залишилося перевірити, що відображення $\bar{\varphi}$ зберігає операцію. Маємо

$$\bar{\varphi}(aH bH) = \bar{\varphi}(abH) = \varphi(ab) = \varphi(a)\varphi(b) = \bar{\varphi}(aH)\bar{\varphi}(bH).$$

Отже, $\bar{\varphi}$ — біективний гомоморфізм груп $G_1/\ker \varphi$ та $\text{im } \varphi$. \square

Приклади 7.22. 1. ???

2. ???

7.9. Кільця

Як ми уже раніше говорили, на множині може бути задано декілька бінарних алгебричних операцій, причому одна і та ж множина стосовно різних операцій може утворювати різні алгебричні структури. Наприклад, $(\mathbb{Z}, +)$ — аддитивна абелева група, а (\mathbb{Z}, \cdot) — мультиплікативний моноїд. Спробуємо об'єднати такі структури в одну. Для цього скористаємося дистрибутивним законом, який тільки на перший погляд виглядає тривіальним (наприклад, спробувавши об'єднати алгебричні структури $(\mathbb{Z}, +)$ та (\mathbb{Z}, \circ) , де $n \circ m = n + m + nm$, ми уже не побачимо настільки ж доброї узгодженості між алгебричними операціями). Без зменшення загальності, а лише для полегшення викладу матеріалу вважатимемо, що алгебричними операціями, які визначено на заданій множині, є операції додавання та множення.

Означення 7.30. Непорожня множина R з двома алгебричними операціями додавання і множення називається *кільцем* $(R, +, \cdot)$, якщо ці операції задовольняють таким умовам:

- [R1] $(R, +)$ — абелева група (яку називають *адитивною групою кільця*);
- [R2] множення асоціативне, тобто (R, \cdot) — напівгрупа (яку ще називають *мультиплікативною напівгрупою кільця*);
- [R3] множення дистрибутивне щодо додавання, тобто для будь-яких елементів $a, b, c \in R$

$$(a + b)c = ac + bc \quad \text{i} \quad c(a + b) = ca + cb.$$

Означення 7.31. Якщо в кільці R операція множення комутативна, то кільце R називають *комутативним*. Зауважимо, що на відміну від груп, комутативне кільце не прийнято називати абелевим.

Означення 7.32. Якщо в кільці R стосовно множення існує нейтральний елемент (тобто (R, \cdot) — моноїд), то кажуть, що $(R, +, \cdot)$ — *кільце з одиницею*. Одиничний елемент кільця прийнято позначати e або звичайною одиницею 1 і аналогічно, як у випадку мультиплікативної абелевої групи, можна довести, що якщо в кільці існує одиниця, то вона єдина.

Приклади 7.23. 1. Множини $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ зі звичайними операціями додавання і множення є кільцями з одиницею. Множина $2\mathbb{Z}$ — всіх парних цілих чисел — є кільцем без одиниці.

2. Нехай R — будь-яке кільце. Множина $M_n(R)$ є кільцем стосовно операцій додавання та множення матриць. Воно називається *повним матричним кільцем над R* . Це один із найважливіших

прикладів кілець. Кільце матриць $M_n(R)$ є некомутативним, навіть якщо кільце R комутативне (при $n > 1$). Зауважимо також, що можна розглядати кільця $M_n(M_m(R))$, тобто кільця матриць n -го порядку, елементами яких є матриці m -го порядку.

3. Множина дійсних функцій від дійсної змінної, визначених на проміжку (a, b) , є комутативним кільцем з одиницею стосовно звичайних операцій додавання та множення функцій.
4. Нехай R — довільне кільце. Розглянемо множину $R[[x]] = \{(a_0, a_1, \dots, a_n, \dots) \mid a_i \in R\}$ всіх нескінчених послідовностей елементів кільця R . Введемо позначення: $(a_0, a_1, \dots, a_n, \dots) = \sum_{n=0}^{\infty} a_n x^n$. Означимо на $R[[x]]$ операції

$$\begin{aligned} \sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n &= \sum_{n=0}^{\infty} (a_n + b_n) x^n \\ \left(\sum_{n=0}^{\infty} a_n x^n \right) \cdot \left(\sum_{n=0}^{\infty} b_n x^n \right) &= \sum_{n=0}^{\infty} \left(\sum_{i+j=n} a_i b_j \right) x^n. \end{aligned}$$

Легко перевірити, що $R[[x]]$ — кільце стосовно цих операцій. Воно називається *кільцем формальних степеневих рядів*.

5. Нехай X — непорожня множина, $M = 2^X$ — множина всіх підмножин множини X . Визначимо на 2^X операції Δ та \diamond : $X \Delta Y = (X \cup Y) \setminus (X \cap Y)$, $X \diamond Y = X \cap Y$. Очевидно, що M є кільцем стосовно цих операцій.
6. На довільній адитивній абелевій групі $(G, +)$ співвідношення $ab = 0$ для всіх $a, b \in G$ встановлює структуру *кільця з нульовим множенням*.

Зауваження 7.5. Нехай R — кільце з одиницею, і припустимо, що одиниця кільця співпадає з його нулем: $1 = 0$. Тоді за першою властивістю твердження 7.36 ми отримаємо, що $a = a \cdot 1 = a \cdot 0 = 0$ для усіх $a \in R$, тобто кільце R складається лише з одного нуля. Таким чином, в нетривіальному кільці R одиниця завжди відмінна від нуля.

В теорії кілець також розглядають алгебричні структури, в яких аксіома [R2] або зовсім забирається, або замінюється якоюсь іншою — залежно від конкретної задачі. У таких випадках говорять про *неасоціативні кільця*. Ми ж розглядатимемо лише *асоціативні* кільця, а тому можемо опиратися на твердження 1.14 і не перейматись розташуванням дужок у добутку $a_1 a_2 \dots a_k$ довільних елементів кільця.

Приклад 7.24. Множина векторів простору з операціями додавання і векторного множення є некомутативним і неасоціативним кільцем. Проте в ньому виконуються тотожності, які в певній мірі замінюють комутативність і асоціативність: $a \times b + b \times a = 0$ (антикомутативність), $(a \times b) \times c + (b \times c) \times a + (c \times a) \times b = 0$ (тотожність Якобі).

Велика кількість властивостей кілець можуть бути переформульовані з відповідних властивостей груп і, взагалі, множин з однією асоціативною операцією. Наприклад, $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$ для всіх натуральних m, n і усіх $a \in R$. Наведемо деякі інші властивості, які є більш специфічними для кілець і які випливають із аксіом кільця.

Твердження 7.36. Якщо a, b, c — довільні елементи кільця $(R, +, \cdot)$, то

- 1) $a \cdot 0 = 0 \cdot a = 0$;
- 2) $a(-b) = (-a)b = -ab$;
- 3) $(-a)(-b) = ab$;
- 4) $a(b - c) = ab - ac$ і $(a - b)c = ac - bc$.

Доведення. 1) З рівностей $0 \cdot a = (0+0)a = 0 \cdot a + 0 \cdot a = 0 \cdot a$ за законом скорочення випливає, що $0 \cdot a = 0$. Так само доводиться, що $a \cdot 0 = 0$.

2) $a(-b) + ab = a(-b+b) = a \cdot 0 = 0$ за щойно доведеним. Отже, $a(-b) = -ab$. Аналогічно доводиться, що $(-a)b = -ab$.

3) $(-a)(-b) + (-ab) = (-a)(-b) + (-a)b = (-a)(-b + b) = -a \cdot 0 = 0$. З іншого боку, $ab + (-ab) = 0$. За законом скорочення звідси випливає, що $(-a)(-b) = ab$
4) $a(b - c) + ac = a(b - c + c) = ab$ і, аналогічно, $(a - b)c + bc = ac$. \square

Зауважимо ще, що аксіома дистрибутивності має своїм наслідком *загальний закон дистрибутивності* $(a_1 + \dots + a_n)(b_1 + \dots + b_m) = \sum_{i=1}^n \sum_{j=1}^m a_i b_j$, в чому легко переконатись міркуванням за індукцією. Використовуючи вищеперелічені властивості, також отримаємо, що $n(ab) = (na)b = a(nb)$ для всіх $n \in \mathbb{Z}$ і $a, b \in R$. Насамкінець, відзначимо біноміальну формулу Ньютона $(a+b)^n = \sum_{i=0}^n \binom{n}{i} a^i b^{n-i}$, правильну для всіх $a, b \in R$, але тільки в комутативному кільці R (доведення пропонуємо провести самостійно).

7.10. Підкільця та ідеали

Означення 7.33. Непорожня підмножина L кільця R називається *підкільцем* кільця R , якщо L є кільцем стосовно тих же операцій, що і в R . Позначатимемо: $L \leq R$ або $L < R$.

Очевидно, що в будь-якому ненульовому кільці R існує, в крайньому випадку, два підкільця — нульове $\{0\}$ і саме кільце R . Ці підкільця називають *невласними*, а всі решта підкільця кільця R називають *власними*.

Приклади 7.25. 1. У ланцюжку $10\mathbb{Z} \subset 2\mathbb{Z} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ кожне попереднє кільце є підкільцем кожного наступного кільця (стосовно звичайних операцій додавання і множення).

2. Кільца $M_n(\mathbb{Q})$ і $M_n(\mathbb{Z})$ є підкільцями некомутативного кільця $M_n(\mathbb{R})$.

3. Кільце неперервних дійсних функцій, визначених на проміжку (a, b) , є підкільцем кільця всіх дійсних функцій, визначених на цьому ж проміжку.

Твердження 7.37. Непорожня підмножина $Q \subseteq R$ є підкільцем кільця R тоді і лише тоді, коли для довільних елементів $a, b \in Q$

- 1) $a - b \in Q$,
- 2) $ab \in Q$.

Доведення. Необхідність очевидна. Доведемо достатність. Нехай $a - b \in Q$ і $ab \in Q$ для довільних $a, b \in Q$. За твердженням 7.6 з першої із цих умов випливає, що Q — підгрупа групи $(R, +)$ і, зокрема, множина Q замкнена стосовно операції додавання. Друга умова означає замкненість Q стосовно операції множення, а тому множина Q — піднапівгрупа напівгрупи (R, \cdot) (див. означення 7.4). Залишилось зауважити, що дистрибутивність множення стосовно додавання виконується на множині Q , оскільки вона виконується на всьому кільці R . Отже, $(Q, +, \cdot)$ — кільце і тому $Q \leq R$. \square

З теорії підгруп (тврдження 7.5) випливає, що якщо Q — підкільце кільця R , то нульові елементи 0_Q і 0_R цих кілець збігаються. Питання ж про співпадіння одиничних елементів e_Q підкільця Q і e_R кільця R вирішується не так однозначно: Q може не мати одиниці, може мати одиницю $e_Q = e_R$ і може мати одиницю $e_Q \neq e_R$.

Приклад 7.26. Три вище зазначені ситуації виникають, наприклад, у кільці матриць $M_2(\mathbb{R})$ і його підкільцях Q_1, Q_2, Q_3 , де

$$Q_1 = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}, \quad Q_2 = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{R} \right\}, \quad Q_3 = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{R} \right\}.$$

Означення 7.34. Непорожня підмножина I кільця R називається *правим (лівим) ідеалом* в R , якщо

- 1) $a - b \in I$ для довільних $a, b \in I$;
- 2) $ar \in I$ для довільних $a \in I, r \in R$ (або $ra \in I$ у випадку лівих ідеалів).

У випадку комутативного кільця праві і ліві ідеали, очевидно, збігаються, тому в цьому випадку вживають термін *ідеал* кільця.

- Приклади 7.27.** 1. Множина $n\mathbb{Z}$ є ідеалом в кільці \mathbb{Z} , бо різниця двох цілих чисел, кратних n , є цілим числом, кратним n , і добуток цілого числа, кратного n , на довільне ціле число є цілим числом, кратним n .
 2. Нехай R — комутативне кільце з 1 і $a \in R$. Розглянемо множину $(a) = \{ar \mid r \in R\}$. Очевидно, що (a) є ідеалом (це узагальнення попереднього прикладу 1). Цей ідеал (a) називають *головним ідеалом*, породженим елементом a , і зазвичай позначають aR .

Твердження 7.38. Кожний ідеал I в кільці R є підкільцем кільця R .

Доведення. Якщо $a, b \in I$, то $0 = b - b \in I$, $-b = 0 - b \in I$ і $a + b = a - (-b) \in I$. Це означає, що множина I є підгрупою групи R стосовно додавання. Крім цього, з означення ідеалу випливає, що I замкнена стосовно множення. Залишилось зауважити, що для I правильні всі аксіоми з означення кільця (це випливає з того, що вони правильні всього кільця R). \square

Зауваження 7.6. Невірно, що підкільце зобов'язане бути ідеалом. Наприклад, підкільце \mathbb{Z} кільця \mathbb{Q} не є ідеалом в \mathbb{Q} .

7.11. Суміжні класи за ідеалом. Факторкільця

До кінця цього параграфа розглядаються лише комутативні кільця.

Нехай I — ідеал в комутативному кільці R . Тоді, очевидно, I — підгрупа адитивної групи R . Тому аналогічно, як і у випадку груп (див. § 7.6 та § 7.7), можна означити відношення еквівалентності: $a \sim_I b$ тоді і тільки тоді, коли $a - b \in I$ (в даному випадку ситуація навіть більш простіша, оскільки адитивна група R є комутативною). Отже, аналогічно, як у § 7.6, ми одержимо розбиття кільця R на суміжні класи $a + I$ за ідеалом I . Ми пишемо $a \sim a'$, якщо елементи a і a' належать до одного і того ж суміжного класу, тобто $a - a' \in I$.

Означення 7.35. Розбиття кільця R (відношення еквівалентності на R) називається *узгодженим з операціями*, якщо для будь-яких елементів $a, b, a', b' \in R$ з умови $a \sim a'$ і $b \sim b'$ випливає $a + b \sim a' + b'$ і $ab \sim a'b'$.

Теорема 7.39 (про розбиття кільця). Розбиття кільця узгоджене з кільцевими операціями тоді і тільки тоді, коли воно є розбиттям на суміжні класи за деяким ідеалом цього кільця.

Доведення. Якщо розбиття кільця R узгоджене з операціями, то з теореми 7.31 (про розбиття груп) випливає, що воно є розбиттям за деякою підгрупою I адитивної групи кільця R . Покажемо, що ця підгрупа I є ідеалом. Якщо $a, b \in I$, то $-b \in I$ і $a - b = a + (-b) \in I$ за критерієм підгрупи. Далі, для будь-яких $r \in R$ і $a \in I$ маємо $a \sim 0$, $r \sim r$, тому, осільки розбиття узгоджене з операцією множення, $a \cdot r \sim 0 \cdot r = 0$, тобто $ar \in I$. Отже, I є ідеалом кільця R .

Навпаки, якщо I — ідеал кільця R , то розбиття групи R на суміжні класи за підгрупою I узгоджене з операцією додавання за теоремою 7.31. Покажемо, що розбиття узгоджене й з операцією множення. Нехай $a \sim a'$, $b \sim b'$. Тоді $ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') \in I$, бо $a - a', b - b' \in I$. Це означає, що $ab \sim a'b'$, тобто задане розбиття узгоджене і з операцією множення. \square

Означення 7.36. Нехай $R/I = \{a + I \mid a \in R\}$ — множина всіх суміжних класів кільця R за ідеалом I . Позначимо (для скорочення) суміжний клас $a + I$ через \bar{a} . Означимо на множині R/I операції додавання і множення суміжних класів:

$$\bar{a} + \bar{b} = \overline{a + b}, \quad \bar{a} \cdot \bar{b} = \overline{ab}. \quad (7.8)$$

Зауваження 7.7. З теореми 7.39 випливає, що ці означення операцій додавання і множення суміжних класів є коректними: сума і добуток суміжних класів означаються за допомогою представників у цих класах, а теорема 7.39 гарантує, що ці операції залежать лише від суміжних класів, а не від конкретного вибору представників.

Твердження 7.40. Множина R/I є кільцем стосовно операцій (7.8) додавання і множення суміжних класів кільця R за ідеалом I .

Доведення. За твердженням 7.32 множина R/I є абелевою групою стосовно додавання, а асоціативність множення та дистрибутивність множення щодо додавання в R/I випливають з асоціативності множення та дистрибутивності в R . Дійсно, доведемо, наприклад, дистрибутивність:

$$(\bar{a} + \bar{b})\bar{c} = (\overline{a+b})\bar{c} = \overline{(a+b)c} = \overline{ac+bc} = \overline{ac} + \overline{bc} = \bar{a} \cdot \bar{c} + \bar{b} \cdot \bar{c}.$$

Зауважимо також, що якщо R — кільце з одиничним елементом 1, то й R/I є кільцем з одиничним елементом $\bar{1} = 1 + I$. \square

Означення 7.37. Кільце R/I , елементами якого є суміжні класи кільця R за ідеалом I , називається *факторкільцем* кільця R за ідеалом I .

Приклади 7.28. 1. ???

2. ???

7.12. Кільце класів лишків $\mathbb{Z}/n\mathbb{Z}$

Важливим прикладом факторкільця є так зване *кільце класів лишків* $\mathbb{Z}/n\mathbb{Z}$ — факторкільце кільця \mathbb{Z} за ідеалом $n\mathbb{Z}$, де $n > 1$. Поки що обмежимося лише найелементарнішими властивостями цього факторкільця і розглянемо його лише для того, щоб мати конкретний приклад факторкільця. Пізніше ми будемо вивчати факторкільця $\mathbb{Z}/n\mathbb{Z}$ більш детально, оскільки вони відіграють важливу роль у теорії чисел.

Отож, нехай n — фіксоване натуральне число, $n > 1$. Як нам уже відомо з прикладу 7.27, множина $n\mathbb{Z}$ є ідеалом кільця \mathbb{Z} , а тому ми можемо утворити факторкільце $\mathbb{Z}/n\mathbb{Z}$, елементами якого будуть суміжні класи $\bar{a} = a + n\mathbb{Z}$, де $a \in \mathbb{Z}$. Позначимо через $\bar{0}, \bar{1}, \bar{2}, \dots, \bar{n-1}$ суміжні класи з представниками $0, 1, 2, \dots, n-1$. Виявляється, що ці суміжні класи вичерпують всі елементи кільця $\mathbb{Z}/n\mathbb{Z}$. Дійсно, з означення суміжних класів випливає, що для $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$ рівність $\bar{a} = \bar{b}$ виконується тоді і тільки тоді, коли $a - b \in n\mathbb{Z}$, тобто до одного й того ж суміжного класу належать ті цілі числа, які при діленні на n дають однакову остачу. Отже, суміжні класи $\bar{0}, \bar{1}, \bar{2}, \dots, \bar{n-1}$ попарно різні. Далі, якщо \bar{a} — довільний суміжний клас факторкільця $\mathbb{Z}/n\mathbb{Z}$, то, розділивши a з остачею на n , одержимо $a = nq+r$ (тут $q = \left[\frac{a}{n}\right]$ — ціла частина дробу $\frac{a}{n}$, $r = a - nd$, $0 \leq r < n$) і $\bar{a} = \overline{nd+r} = \overline{nd} + \bar{r} = \bar{0} + \bar{r} = \bar{r} \in \{\bar{0}, \bar{1}, \dots, \bar{n-1}\}$.

Розглянемо таблички додавання і множення для деяких кілець класів лишків.

$\mathbb{Z}/2\mathbb{Z}$:	+		\cdot	
	$\bar{0}$	$\bar{1}$	$\bar{0}$	$\bar{1}$
	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
	$\bar{1}$	$\bar{1}$	$\bar{0}$	$\bar{1}$

$\mathbb{Z}/3\mathbb{Z}$:	+			\cdot		
	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
	$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
	$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
	$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{0}$

$\mathbb{Z}/4\mathbb{Z}$:	+				\cdot			
	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
	$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
	$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
	$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\bar{1}$
	$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$

		+					·				
		0	1	2	3	4	0	1	2	3	4
$\mathbb{Z}/5\mathbb{Z}$:	0	0	1	2	3	4	0	0	0	0	0
	1	1	2	3	4	0	1	0	1	2	3
	2	2	3	4	0	1	2	0	2	4	1
	3	3	4	0	1	2	3	0	3	1	4
	4	4	0	1	2	3	0	4	3	2	1
		+0	1	2	3	4	·	0	1	2	3
$\mathbb{Z}/6\mathbb{Z}$:	0	0	1	2	3	4	5	0	0	0	0
	1	1	2	3	4	5	0	1	2	3	4
	2	2	3	4	5	0	1	0	2	4	0
	3	3	4	5	0	1	2	0	3	0	3
	4	4	5	0	1	2	3	0	4	2	0
	5	5	0	1	2	3	4	0	5	4	3
							4	0	2	0	4
							5	0	5	4	3
								2	1		

Зауважимо, що, наприклад, в кільці $\mathbb{Z}/5\mathbb{Z}$ кожний ненульовий елемент має обернений стосовно множення ($\bar{1} \cdot \bar{1} = \bar{1}$, $\bar{2} \cdot \bar{3} = \bar{1}$, $\bar{4} \cdot \bar{4} = \bar{1}$), а у кільці $\mathbb{Z}/6\mathbb{Z}$ елементи $\bar{2}$, $\bar{3}$ і $\bar{4}$ не є обортними. Крім того, наприклад, в $\mathbb{Z}/6\mathbb{Z}$ добуток ненульових елементів може давати нульовий елемент ($\bar{2} \cdot \bar{3} = \bar{0}$); квадрат ненульового елемента, який не дорівнює $\bar{1}$, може давати цей самий елемент: $\bar{3}^2 = \bar{3}$. В кільцях класів лишків є й інші незвичні властивості множення. Той факт, що в $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$ кожний ненульовий елемент є обортним стосовно множення, допускає узагальнення.

Твердження 7.41. Нехай p — просте число, $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ і $\bar{a} \neq \bar{0}$. Тоді існує такий елемент $\bar{b} \in \mathbb{Z}/p\mathbb{Z}$, що $\bar{a} \cdot \bar{b} = \bar{1}$.

Доведення. Розглянемо головний ідеал $(\bar{a}) = \bar{a}\mathbb{Z}/p\mathbb{Z}$, породжений елементом \bar{a} (див. приклад 7.27). Оскільки $\bar{a} \in (\bar{a})$, то цей ідеал ненульовий і за твердженням 7.38 є підкільцем кільця $\mathbb{Z}/p\mathbb{Z}$, а томк є підгрупою адитивної групи $\mathbb{Z}/p\mathbb{Z}$. За наслідком 7.29 з теореми Лагранжа $(\bar{a}) = \mathbb{Z}/p\mathbb{Z}$. Звідси випливає, що знайдеться $\bar{b} \in \mathbb{Z}/p\mathbb{Z}$, для якого $\bar{a} \cdot \bar{b} = \bar{1}$. \square

7.13. Поля

Означення 7.38. Комутативне кільце F з одиничним елементом $1 \neq 0$ називається *полем*, якщо для кожного ненульового елемента з F існує обернений стосовно множення.

- Приклади 7.29.**
1. Множини раціональних і дійсних чисел є полями стосовно звичайних операцій додавання і множення.
 2. Множина $(\mathbb{Z}, +, \cdot)$ не утворює поле, оскільки серед цілих чисел обортними елементами є лише 1 та -1 .
 3. $\mathbb{Q}(\sqrt{2})$ — поле ??????????????????

Ще один приклад поля (причому скінченного) наведемо у вигляді твердження.

Твердження 7.42. $\mathbb{Z}/n\mathbb{Z}$ є полем тоді і тільки тоді, коли n — просте число.

Доведення. Якщо n — просте число, то за твердження 7.41 факторкільце $\mathbb{Z}/n\mathbb{Z}$ є полем. Якщо n не є простим числом, то $n = n_1 \cdot n_2$, де $1 < n_1, n_2 < n$. Тоді $\bar{n} = \bar{n}_1 \cdot \bar{n}_1 = \bar{0}$, причому $\bar{n}_1 \neq \bar{0}$, $\bar{n}_2 \neq \bar{0}$. Якби, наприклад, для елемента \bar{n}_1 існував обернений \bar{n}_1^{-1} , то виконувалась б рівність $\bar{n}_1^{-1} \cdot \bar{n}_1 \cdot \bar{n}_2 = \bar{n}_1^{-1} \cdot \bar{0} = \bar{0}$. Звідси $\bar{1} \cdot \bar{n}_2 = \bar{n}_2 = \bar{0}$. Суперечність. \square

Твердження 7.43. В полі існують лише тривіальні ідеали.

Доведення. Нехай F — поле, I — ідеал поля F . Якщо $a \in I$ і $a = 0$, то I — нульовий ідеал. Якщо ж $a \neq 0$ і $a \in I$, то $\bar{1} \in I$, оскільки $a^{-1}a \in I$ за другою аксіомою із означенням ідеалу. За цією ж аксіомою $1 \cdot r = r \in I$ для довільного $r \in F$, а тому в ідеалі містяться усі елементи поля F , що й потрібно було довести. \square

7.14. Гомоморфізми та ізоморфізми кілець і полів

Означення 7.39. Нехай R_1 і R_2 — кільця. Відображення $\varphi: R_1 \rightarrow R_2$ називається *гомоморфізмом* кілець, якщо

$$\varphi(a + b) = \varphi(a) + \varphi(b) \quad \text{i} \quad i\varphi(ab) = \varphi(a)\varphi(b)$$

для довільних $a, b \in R_1$.

З означення випливає, що $f(0_1) = 0_2$, де 0_1 і 0_2 — нульові елементи кілець R_1 і R_2 відповідно (див. твердження 7.21).

Означення 7.40. *Гомоморфізмом полів* F_1 і F_2 називають відображення $\varphi: F_1 \rightarrow F_2$, для якого

$$\varphi(a + b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b) \quad \text{i} \quad \varphi(1_1) = 1_2,$$

де 1_1 та 1_2 — одиничні елементи в F_1 та F_2 відповідно, a, b — довільні елементи поля F_1 .

Приклади 7.30. 1. Відображення кільця цілих чисел в поле раціональних чисел $\varphi: \mathbb{Z} \rightarrow \mathbb{Q}$ таке, що $\varphi(z) = z$ для довільного $z \in \mathbb{Z}$, є очевидно, гомоморфізмом.

2. Нехай R — кільце, I — ідеал в R . Розглянемо відображення $\pi: R \rightarrow {}^{R/I}$ кільця R у факторкільце ${}^{R/I}$, для якого $\pi(a) = \bar{a}$. Тоді $\pi(a + b) = \overline{a + b} = \bar{a} + \bar{b} = \pi(a) + \pi(b)$ і $\pi(ab) = \overline{ab} = \bar{a} \cdot \bar{b} = \pi(a)\pi(b)$. Отже, відображення π є гомоморфізмом кілець R і ${}^{R/I}$. Цей гомоморфізм називають *канонічним гомоморфізмом* кілець.

Означення 7.41. *Ізоморфізмом кілець (полів)* називають біективний гомоморфізм цих кілець (полів).

Приклади 7.31. 1. Одиничне відображення будь-якого кільця (поля) в себе є, очевидно, ізоморфізмом.

2. Відображення $\varphi: \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})$, для якого $\varphi(a + b\sqrt{2}) = a - b\sqrt{2}$, є ізоморфізмом поля $\mathbb{Q}(\sqrt{2})$ в себе. Справді, біективність тут очевидна. Крім цього, $\varphi((a + b\sqrt{2})(c + d\sqrt{2})) = \varphi(ac + 2bd + (ad + bc)\sqrt{2}) = ac + 2bd - (ad + bc)\sqrt{2} = (a - b\sqrt{2})(c - d\sqrt{2}) = \varphi(a - b\sqrt{2})\varphi(c - d\sqrt{2})$. Ще легше перевіряється, що $\varphi((a + b\sqrt{2}) + (c + d\sqrt{2})) = \varphi(a + b\sqrt{2}) + \varphi(c + d\sqrt{2})$.

Ідеали кілець тісно пов'язані з гомоморфізмами.

Означення 7.42. Нехай $\varphi: R_1 \rightarrow R_2$ — гомоморфізм кілець. Підмножина $\ker \varphi = \{a \in R_1 \mid \varphi(a) = 0\}$ кільця R_1 називається *ядром гомоморфізму* φ .

Твердження 7.44. Ядро гомоморфізму кілець $\varphi: R_1 \rightarrow R_2$ є ідеалом кільця R_1 .

Доведення. Якщо $a, b \in \ker \varphi$, то $\varphi(a - b) = \varphi(a) - \varphi(b) = 0 - 0 = 0$, тому $a - b \in \ker \varphi$. Якщо, крім цього, $c \in R_1$, то $\varphi(ca) = \varphi(c)\varphi(a) = \varphi(c) \cdot 0 = 0$, а тому $ca \in \ker \varphi$. \square

Твердження 7.45. Якщо I — ідеал кільця R , то I є ядром канонічного гомоморфізму $\pi: R \rightarrow {}^{R/I}$, де $\pi(a) = \bar{a}$ для довільного $a \in R$.

Доведення. Дійсно, $\ker \pi = \{a \in R \mid \bar{a} = \bar{0}\} = \{a \in R \mid a \in I\} = I$, що й треба було показати. \square

Твердження 7.46. Гомоморфізм полів завжди є ін'єктивним відображенням.

Доведення. За твердження 7.44 ядро гомоморфізму полів $\varphi: F_1 \rightarrow F_2$ є ідеалом в полі F_1 . Але за твердження 7.43 в полі F_1 є лише два ідеали (0) і F_1 . Оскільки $\varphi(1_{F_1}) = 1_{F_2}$, то $1_{F_1} \notin \ker \varphi$ і тому $\ker \varphi \neq F_1$. Отже, ядро гомоморфізму полів містить лише 0 . Тепер, якщо $\varphi(a_1) = \varphi(a_2)$ для $a_1, a_2 \in F_1$, то, оскільки φ — гомоморфізм, $\varphi(a_1 - a_2) = 0$. Тому $a_1 - a_2 \in \ker \varphi = (0)$, звідки $a_1 = a_2$. Отже, відображення φ — ін'єктивне. \square