

# Групи

Костянтин Крутой  
krutoy@imj-prg.fr

## 1 Групи

Одна із мотиваційних ідей теорії груп полягає в тому, що в математиці дуже часто виникають бінарні операції на певних об'єктах (наприклад, множинах), які задовольняють певні властивості. Нагадаємо, що бінарна операція на множині  $X$  є просто відображенням  $\circ: X \times X \rightarrow X$ . В цих нотатках, для елементів  $a, b \in X$  ми будемо позначати значення відображення  $\circ$  на парі  $(a, b)$  наступними еквівалентними способами

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

Наступні два приклади є джерелом нашої мотивації.

**Приклад 1.1.** Розглянемо множину цілих чисел  $\mathbb{Z}$  із заданою на ній бінарною операцією додавання  $+$ :  $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ . Маємо наступні властивості:

1. *Асоціативність*: для будь-яких чисел  $a, b, c \in \mathbb{Z}$  виконується рівність:  $(a+b)+c = a+(b+c)$ .
2. *Існування нейтрального елемента*: у множині  $\mathbb{Z}$  існує елемент  $0$ , такий, що для будь-якого  $a \in \mathbb{Z}$  маємо:  $a + 0 = 0 + a = a$ .
3. *Існування оберненого елемента*: для кожного елемента  $a \in \mathbb{Z}$  існує протилежне йому число  $-a \in \mathbb{Z}$ , таке, що виконується рівність:  $a + (-a) = (-a) + a = 0$ .

**Приклад 1.2.** Розглянемо множину  $\text{Aut}(X)$  усіх бієктивних відображень множини  $X$  на себе із операцією композиції відображень  $\circ: \text{Aut}(X) \times \text{Aut}(X) \rightarrow \text{Aut}(X)$ . Маємо наступні властивості:

1. *Асоціативність*: для довільних бієктивних відображень  $f, g, h: X \rightarrow X$  виконується наступна рівність:  $(f \cdot g) \cdot h = f \cdot (g \cdot h)$ .
2. *Існування нейтрального елемента*: у множині  $\text{Aut}(X)$  існує тотожне відображення  $\text{id}_X$ , таке, що для будь-якого відображення  $f \in \text{Aut}(X)$  маємо:  $f \cdot \text{id}_X = \text{id}_X \cdot f = f$ .
3. *Існування оберненого елемента*: для кожного бієктивного відображення  $f \in \text{Aut}(X)$  існує обернене відображення  $f^{-1} \in \text{Aut}(X)$ , яке задовольняє:  $f \cdot f^{-1} = f^{-1} \cdot f = \text{id}_X$ .

Як ми бачимо, ці два, апріорі різних, об'єкти мають схожі властивості, а саме: обидві операції є асоціативними, мають нейтральний елемент і мають обернені елементи. Ми покажемо, що такі об'єкти можна вивчати схожим чином — під егідою теорії груп.

### 1.1 Напівгрупи, моноїди, групи, та їх приклади

Замість того, щоб одразу дати означення групи, яке має бути відносно громіздким з огляду на згадані властивості прикладів 1.1 та 1.2, ми будемо поступово досліджувати властивості асоціативності, існування нейтрального елемента та обернених елементів.

**Означення 1.1.** *Напівгрупою* називається множина  $S$  разом із заданою на ній бінарною операцією  $\circ: S \times S \rightarrow S$ , яка задовольняє умову асоціативності. Тобто, для будь-яких  $a, b, c \in S$  виконується рівність:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

Очевидно, що цілі числа із операцією додавання і множина всіх бієкцій множини  $X$  із операцією композиції є прикладами напівгруп. Проте ці об'єкти також задовольняють додаткові умови (а саме: існування нейтрального елемента і існування обернених елементів). Легко побудувати приклад напівгрупи, яка не має ані нейтрального елемента ані обернених елементів.

**Приклад 1.3.** Множина натуральних<sup>1</sup> чисел  $\mathbb{N}$  із операцією додавання є класичним прикладом *напівгрупи*. Дійсно для будь-яких  $a, b, c \in \mathbb{N}$  маємо рівність:

$$(a + b) + c = a + (b + c).$$

Також легко навести приклад бінарної операції, яка не є асоціативною. Наприклад, визначимо функцію  $f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  як  $f(n, m) = n^m$ . Іншим прикладом слугуватиме вільна напівгрупа на двох елементах.

**Приклад 1.4.** Нехай  $S$  є множиною всіх слів над абеткою із двох елементів  $\{a, b\}$ . Визначимо бінарну операцію *конкатенації*

$$\circ: S \times S \rightarrow S, \quad (w_1, w_2) \mapsto w_1 w_2.$$

Тобто, операція конкатенації склеює два слова в одне, наприклад:  $aba \cdot bbb = ababbb$ . Безпосередньо перевіряється, що конкатенація є асоціативною операцією, отже, наділяє множину  $S$  структурою напівгрупи. Аналогічно можна визначити напівгрупу на довільній абетці

Насправді, вищевизначена напівгрупа  $S$  має нейтральний елемент. Дійсно, нехай  $\emptyset$  є порожнім словом, тоді очевидно, що  $\emptyset \cdot w = w \cdot \emptyset = w$  для довільного слова  $w \in S$ . З огляду на наступне означення, напівгрупа  $S$  називається *вільним моноїдом на двох елементах*.

**Означення 1.2.** *Моноїдом* називається множина  $M$  разом із заданою на ній бінарною операцією  $\circ: M \times M \rightarrow M$ , яка задовольняє такі дві умови:

1. *Асоціативність*: для будь-яких  $a, b, c \in M$  виконується рівність:  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ .
2. *Існування нейтрального елемента*: існує такий елемент  $e \in M$ , що для будь-якого  $a \in M$  виконується рівність:  $a \cdot e = e \cdot a = a$ .

Іншими словами, моноїдом є напівгрупа із нейтральним елементом. Із означення випливає, що будь-який моноїд є напівгрупою. Помітимо, що множина натуральних чисел із додаванням не є моноїдом. Дійсно, для довільного  $a \in \mathbb{N}$  елементи  $a + 1$  і  $1$  різні. Проте якщо розглянути аналогічно визначену напівгрупу  $(\mathbb{N} \cup \{0\}, +)$ , то  $0$  є нейтральним елементом. Отже,  $(\mathbb{N} \cup \{0\}, +)$  є моноїдом. Вільний моноїд, як свідчить назва, є моноїдом.

**Приклад 1.5.** Розглянемо двоелементну множину  $M = \{1, \infty\}$ . Задамо на цій множині бінарну операцію множення  $\circ: M \times M \rightarrow M$ , яка діє за правилами звичайного множення для одиниці (тобто  $1 \cdot 1 = 1$ ), а також за правилом:

$$1 \cdot \infty = \infty \cdot 1 = \infty \cdot \infty = \infty.$$

Ця структура утворює *моноїд*. Дійсно, легко переконатися, що ця операція є асоціативною і  $1 \in M$  є нейтральним елементом.

В усіх попередніх прикладах можна переконатися, що нейтральний елемент єдиний. Для  $\mathbb{N} \cup \{0\}$  доведення цього написано перед прикладом 1.5, а у випадку вільного моноїда на двох елементах можна розглянути функцію, яка слову ставить у відповідність кількість літер у ньому. В такому випадку нейтральний елемент має бути словом без літер, а єдиним таким є  $\emptyset$ .

**Лема 1.1.** Нехай  $M$  — моноїд; тоді нейтральний елемент єдиний. Тобто для довільних двох елементів  $e, e'$  які задовольняють

$$ae = ea = a, \quad ae' = e'a = a$$

виконується  $e = e'$ .

*Доведення.* Дійсно,  $e = ee' = e'$ . □

Введемо домовленість: для *комутативних* моноїдів (тобто тих, які задовольняють  $ab = ba$  для всіх  $a, b \in M$ ), якщо не оголошено інакше, бінарна операція позначатиметься  $+$ , а нейтральний елемент позначатиметься  $0$ . Для необов'язково комутативних моноїдів бінарна операція позначатиметься згідно із початковими домовленостями (див. початок розділу), а одиничний елемент позначатиметься  $1$ .

Щоб додати приклади 1.1 та 1.2 до того, що охоплюють наші означення, залишається єдина умова — існування обернених елементів. Як показують приклади 1.4 та 1.5, моноїди не мають містити обернених елементів, проте, як показує наступна лема, якщо елемент  $a \in M$  має обернений, то він єдиний.

<sup>1</sup>В цих нотатках множина натуральних чисел **не** містить нуля.

**Лема 1.2.** Нехай  $M$  — моноїд,  $a \in M$  — його елемент; тоді обернений елемент до  $a$  (якщо він існує) є єдиним. Тобто для довільних двох елементів  $b, b'$  які задовольняють

$$ab = ba = 1, \quad ab' = b'a = 1$$

виконується  $b = b'$ .

*Доведення.* Дійсно,  $b = b1 = bab' = 1b' = b'$ . □

**Означення 1.3.** Групою називається множина  $G$  разом із заданою на ній бінарною операцією  $\circ: M \times M \rightarrow M$ , яка задовольняє наступні умови:

1. *Асоціативність:* для будь-яких  $a, b, c \in M$  виконується рівність:  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ .
2. *Існування нейтрального елемента:* існує такий елемент  $e \in M$ , що для будь-якого  $a \in M$  виконується рівність:  $a \cdot e = e \cdot a = a$ .
3. *Існування оберненого елемента:* для кожного елемента  $x \in G$  існує елемент  $y \in G$ , який задовольняє:  $x \cdot y = e$ , де  $e$  — нейтральний елемент групи  $G$ .

Ми кажемо, що група  $G$  є абелевою (або комутативною), якщо для довільних  $a, b \in G$  виконується  $a \cdot b = b \cdot a$ .

Очевидно, що будь-яка група є моноїдом, а отже, напівгрупою, але не будь-який моноїд є групою (як показує приклад із  $(\mathbb{N} \cup \{0\}, +)$ ). Також зрозуміло, що перші приклади  $(\mathbb{Z}, +)$  та  $(\text{Aut}(X), \circ)$  є групами. Група  $(\mathbb{Z}, +)$  є абелевою, проте  $(\text{Aut}(X), \circ)$  не має бути абелевою.

**Вправа 1.** Покажіть, що  $(\text{Aut}(X), \circ)$  є абелевою тоді і лише тоді, коли  $|X| \leq 2$ .

Оскільки кожна група є моноїдом, то з лем 1.1 та 1.2 випливає єдиність нейтрального елемента та обернених. Нотаційні домовленості про позначення операцій, сформульовані після леми 1.1, мають місце. Більш при аддитивному записі (випадок комутативних груп) обернений до елемента  $a \in G$  позначатиметься  $-a$ . В загальному випадку (випадку необов'язково комутативних груп) обернений до елемента  $a \in G$  позначатиметься  $a^{-1}$ . Ми підсумовуємо цю секцію прикладами груп.

**Приклад 1.6** (Векторні простори). Нехай  $\mathbb{K}$  є полем (наприклад,  $\mathbb{K} = \mathbb{R}$  або  $\mathbb{K} = \mathbb{C}$ ) і  $V$  є  $\mathbb{K}$ -векторним простором. За визначенням векторного простору,  $V$  наділено асоціативною операцією додавання

$$+: V \times V \longrightarrow V.$$

Очевидно, що  $0 \in V$  є нейтральним елементом, і для довільного  $v \in V$  знайдеться обернений елемент  $-v \in V$  такий, що  $v + (-v) = 0$ .

**Приклад 1.7** (Обертонні матриці). Нехай  $\mathbb{K}$  є полем і  $V$  є  $\mathbb{K}$ -векторним простором. Розглянемо множину  $\text{GL}(V)$  всіх обертонних  $\mathbb{K}$ -лінійних відображень  $A: V \longrightarrow V$ . Бінарна операція композиції лінійних відображень наділяє множину  $\text{GL}(V)$  структурою групи. Наприклад, якщо  $V = \mathbb{R}^n$ , то  $\text{GL}(V)$  співпадає із множиною всіх оборотних дійсних  $n \times n$ -матриць, а операція композиції співпадає зі звичайним множенням матриць.

**Приклад 1.8** (Залишки по модулю  $n$ ). Нехай  $n \in \mathbb{N}$ . Розглянемо групу  $(\mathbb{Z}, +)$  і введемо відношення еквівалентності  $\sim$  визначене наступним чином: для  $a, b \in \mathbb{Z}$  маємо

$$a \sim b \iff a - b \text{ ділиться на } n.$$

Позначимо множину класів суміжності  $\mathbb{Z}/\sim$  через  $\mathbb{Z}/n\mathbb{Z}$  і визначимо бінарну операцію  $+$  на  $\mathbb{Z}/n\mathbb{Z}$  наступним чином:

$$+: \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, \quad [a] + [b] = [a + b].$$

Нам треба перевірити, що визначення коректне, адже елемент  $[a + b]$  має залежати лише від  $[a]$  та  $[b]$ , а не від представників цих класів. Помітимо, що якщо  $a, a'$  задовольняють  $[a] = [a']$  і  $b, b'$  задовольняють  $[b] = [b']$ , то

$$(a + b) - (a' + b') = (a - a') + (b - b') \text{ ділиться на } n,$$

оскільки  $a - a'$  і  $b - b'$  діляться на  $n$ . Отже, клас  $[a + b]$  не залежить від вибору представників для  $a$  та  $b$ . Перевіримо асоціативність:

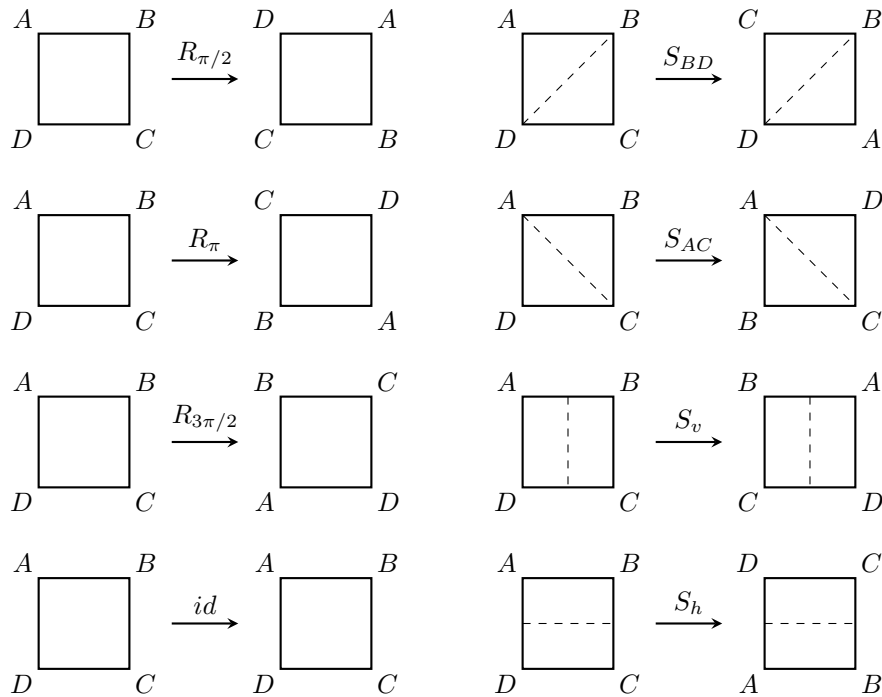
$$[a] + ([b] + [c]) = [a] + [b + c] = [a + (b + c)] = [(a + b) + c] = [a + b] + [c] = ([a] + [b]) + [c].$$

Легко бачити, що клас  $[0]$  є нейтральним елементом для  $\mathbb{Z}/n\mathbb{Z}$  і для  $a \in \mathbb{Z}$  оберненим елементом до  $[a]$  є елемент  $[-a]$ .

**Приклад 1.9** (Симетрії квадрата). Розглянемо квадрат  $ABCD$ , і множину  $D_4$  яка складається із наступних бієкцій квадрату  $ABCD$ :

1. Тотожного відображення  $\text{id}$ ;
2. Поворотів  $R_{\pi/2}$ ,  $R_\pi$ ,  $R_{3\pi/2}$  на кути  $\pi/2$ ,  $\pi$ , та  $3\pi/2$ , відповідно;
3. Симетрій  $S_{BD}$ ,  $S_{AC}$  відносно головних діагоналей;
4. Симетрій відносно сторін  $S_h$ ,  $S_v$ .

Візуально ці симетрії можна зобразити наступними малюнками:



Як тільки ми покажемо, що композиція двох вищезазначених перетворень є одним із вищезазначених перетворень — стане очевидним, що операція композиції є асоціативною, адже це просто композиція бієкцій квадрата. Помітимо, що

$$R_{\pi/2}^k = R_{k\pi/2}, \quad S^2 = 1, \quad R_{\pi/2}S_{BD} = S_h, \quad R_{\pi/2}S_h = S_{AC}, \quad R_{\pi/2}S_{AC} = S_v, \quad R_{\pi/2}S_v = S_{BD},$$

де  $S$  є будь-яким перетворенням, зазначеним справа. Одиничним елементом є  $\text{id}$ , а обернені зрозумілі із наведених співвідношень.

**Приклад 1.10.** Нехай  $K_4$  є множиною  $\{1, a, b, ab\}$  із бінарною операцією  $\cdot : K_4 \times K_4 \rightarrow K_4$  визначеною як

$$\begin{aligned} 1 \cdot 1 &= 1, & 1 \cdot a &= a, & 1 \cdot b &= b, & 1 \cdot ab &= ab, \\ a \cdot 1 &= a, & a \cdot a &= 1, & a \cdot b &= ab, & a \cdot ab &= b, \\ b \cdot 1 &= b, & b \cdot a &= ab, & b \cdot b &= 1, & b \cdot ab &= a, \\ ab \cdot 1 &= ab, & ab \cdot a &= b, & ab \cdot b &= a, & ab \cdot ab &= 1. \end{aligned}$$

Легко перевірити, що  $K_4$  є комутативною групою, в якій для кожного  $x \in K_4$  виконується  $x^2 = 1$ .

Групу  $K_4$  можна легко побудувати як добуток  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . Для двох груп  $(G_1, \circ_1), (G_2, \circ_2)$  визначимо нову групу  $(G_1 \times G_2, \circ)$ , де для  $a, c \in G_1$  та  $b, d \in G_2$  операція  $\circ$  задана як покомпонентне множення, тобто

$$(a, b)(c, d) = \circ((a, b), (c, d)) = (\circ_1(a, c), \circ_2(b, d)) = (ac, bd).$$

Очевидно, що елемент  $(1_{G_1}, 1_{G_2})$  є нейтральним елементом для  $G_1 \times G_2$ , та елемент  $(a^{-1}, b^{-1}) \in G_1 \times G_2$  є оберненим до  $(a, b) \in G_1 \times G_2$ . Єдине, що залишається перевірити, — це асоціативність операції. Для  $(a, b), (c, d), (x, y) \in G_1 \times G_2$  маємо

$$(a, b)[(c, d)(x, y)] = (a, b)(cx, dy) = (a(cx), b(dy)) = ((ac)x, (bd)y) = (ac, bd)(x, y) = [(a, b)(c, d)](x, y).$$

Отже,  $G_1 \times G_2$  дійсно є групою. Розглянемо  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ , яка складається із елементів  $(0, 0), (1, 0), (0, 1), (1, 1)$ . Помітимо, що зробити наступні перепозначення:

$$1 := (0, 0), \quad a := (1, 0), \quad b := (0, 1), \quad ab := (1, 1), \quad \cdot := +,$$

то елементи  $1, a, b, ab$  задовольняють співвідношення групи  $K_4$ . Отже, з точністю до перейменування елементів,  $K_4$  співпадає із  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

## 1.2 Підгрупи, гомоморфізми та фактор групи

Як і в будь-якій частині математики, визначивши об'єкти, наступним кроком стає розробка методів, які описують взаємодію між ними. Наприклад, у вправі 1.9, якщо замість групи  $D_4$  розглянути лише групу поворотів квадрата (яка складається із бієкцій  $\text{id}, R_{\pi/2}, R_{\pi}, R_{3\pi/2}$ ), то ми помітимо, що, перейменувавши елементи  $\text{id}, R_{\pi/2}, R_{\pi}, R_{3\pi/2}$  на  $[0], [1], [2], [3]$ , ми отримаємо групу  $\mathbb{Z}/4\mathbb{Z}$ . Отже, в певному сенсі  $D_4$  "містить"  $\mathbb{Z}/4\mathbb{Z}$ . Щоб формалізувати слово «містить», нам потрібні деякі означення.

**Означення 1.4.** Нехай  $(G, \circ)$  — група. Підмножина  $H \subset G$  називається підгрупою, якщо виконуються наступні умови:

1. Для довільних  $a, b \in H$  маємо  $a \cdot b \in H$ ;
2. Для довільного  $a \in H$  маємо  $a^{-1} \in H$ .

Помітимо, що підмножина  $H = \{\text{id}, R_{\pi/2}, R_{\pi}, R_{3\pi/4}\} \subset D_4$  є підгрупою. Дійсно, композиція двох поворотів є поворотом, отже,  $H$  задовольняє перший пункт означення. Помітимо також що

$$\text{id}^{-1} = \text{id}, \quad R_{\pi/2}^{-1} = R_{3\pi/2}, \quad R_{\pi}^{-1} = R_{\pi}, \quad R_{3\pi/2}^{-1} = R_{\pi/2}.$$

Отже, довільний обернений до елемента з  $H$  міститься в  $H$ . Маємо, що  $H$  задовольняє другий пункт і є підгрупою.

**Лема 1.3.** Нехай  $(G, \circ)$  є групою і  $H \subset G$  є підгрупою. Визначимо бінарну операцію

$$\circ: H \times H \longrightarrow H,$$

як звуження бінарної операції із  $G$  на  $H$ . Тоді  $(H, \circ)$  є групою.

*Доведення.* Асоціативність операції  $\circ: H \times H \longrightarrow H$  очевидна, адже це звуження асоціативної операції із  $G$ . Для кожного елемента  $h \in H$  існує обернений  $h^{-1} \in G$ , але за другою умовою означення підгрупи маємо  $h^{-1} \in H$ ; отже,  $H$  містить обернені для всіх своїх елементів. Наявність нейтрального елемента випливає із першого пункту означення підгрупи та тотожності  $hh^{-1} = h^{-1}h = e$ .  $\square$

Ми довели, що підгрупа групи є сама по собі групою, отже, ми можемо розглядати множину  $H = \{\text{id}, R_{\pi/2}, R_{\pi}, R_{3\pi/4}\} \subset D_4$  як групу, повністю забувши про те, що вона міститься в  $D_4$ . Проте щоб ототожнити  $H$  із  $\mathbb{Z}/4\mathbb{Z}$ , нам також потрібно зробити співставлення елементів групи  $\mathbb{Z}/4\mathbb{Z}$  із елементами групи  $H$ , тобто побудувати відображення  $f: \mathbb{Z}/4\mathbb{Z} \longrightarrow H$ . Очевидно, що довільне відображення не переконає нас, що ці дві групи ідентичні, тому маємо знайти визначення відображень, які поважають структуру групи. Ця задача є простішою для напівгруп, адже напівгрупа є менш вибагливою структурою. Єдине, що наші відображення мають поважати, — це операції напівгруп.

**Означення 1.5.** Нехай  $(G, \circ)$  та  $(H, \bullet)$  — дві напівгрупи. Відображення  $f: G \rightarrow H$  називається гомоморфізмом, якщо, для довільних  $g, h \in G$  виконується рівність:

$$f(g \circ h) = f(g) \bullet f(h).$$

Іншими словами, гомоморфізм між двома напівгрупами — це відображення, яке зберігає операції напівгруп. Очевидно, що композиція двох гомоморфізмів є гомоморфізмом, адже для двох гомоморфізмів  $f: G \rightarrow H$  та  $g: H \rightarrow K$  між напівгрупами  $G, H$  та  $K$  виконується

$$g \circ f(ab) = g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b)) = (g \circ f)(a)(g \circ f)(b).$$

Виявляється, що нам не треба докладати додаткових зусиль, щоб визначити резонні відображення між групами, як показує наступна лема.

**Лема 1.4.** Нехай  $(G, \circ)$  та  $(H, \bullet)$  — дві групи і  $f: G \rightarrow H$  — гомоморфізм напівгруп. Виконуються наступні твердження:

1. Відображення  $f$  заберігає нейтральні елементи, тобто якщо  $1_G$  та  $1_H$  є нейтральними елементами груп  $G$  та  $H$  відповідно, то  $f(1_G) = 1_H$ ;
2. Відображення  $f$  зберігає обернені елементи, тобто для елемента  $a \in G$  виконується рівність  $f(a)^{-1} = f(a^{-1})$ .

*Доведення.* Для першої умови помітимо, що для довільного  $a \in G$  маємо  $f(a) = f(1_G \circ a) = f(1_G) \bullet f(a)$ . Помноживши на обернений до  $f(a)$  в групі  $H$  маємо рівність

$$1_H = f(a) \bullet f(a)^{-1} = f(1_G) \bullet f(a) \bullet f(a)^{-1} = f(1_G) \bullet 1_H = f(1_G).$$

Для другого пункту помітимо, що  $1_H = f(1_G) = f(a \circ a^{-1}) = f(a) \bullet f(a^{-1})$ . Аналогічно показується, що  $1_H = f(a^{-1}) \bullet f(a)$ . З єдиності оберненого елемента випливає, що  $f(a^{-1}) = f(a)^{-1}$ .  $\square$

Ми довели, що гомоморфізм між двома групами автоматично зберігає всю структуру групи (тобто одиничний елемент і обернені), отже, є резонним визначенням відображення між групами. Легко переконатися, що включення підгрупи в групу є гомоморфізмом. У вищезгаданому порівнянні  $\mathbb{Z}/4\mathbb{Z}$  та  $D_4$  маємо, що відображення

$$f: \mathbb{Z}/4\mathbb{Z} \rightarrow D_4, \quad [k] \mapsto R_{k\pi/2}$$

є гомоморфізмом, який ототожнює  $\mathbb{Z}/4\mathbb{Z}$  із підгрупою  $D_4$ , яка складається із поворотів. Наведемо більше прикладів підгруп та гомоморфізмів.

**Приклад 1.11** (Унітарні матриці). Нехай  $H$  є дійсним або комплексним Гільбертовим простором із скалярним добутком  $\langle \cdot, \cdot \rangle$ . Пригадаємо, що обмежений лінійний оператор  $U \in \mathcal{B}(H)$  називається унітарним, якщо  $UU^* = U^*U = 1$ . Безпосередньо випливає, що  $U$  — обертовний оператор, отже, множина унітарних операторів є підмножиною групи обертовних операторів із операцією композиції. Ми позначимо множину унітарних операторів через  $\mathcal{U}(H)$ . Очевидно, що для унітарних операторів  $U, V \in \mathcal{U}(H)$  виконується

$$U^{-1} = U^* \in \mathcal{U}(H), \quad UV \in \mathcal{U}(H).$$

Отже,  $\mathcal{U}(H)$  є підгрупою групи обертовних операторів, і включення  $i: \mathcal{U}(H) \rightarrow \text{GL}(H)$  є ін'єктивним гомоморфізмом.

**Приклад 1.12.** Для натурального числа  $n \in \mathbb{N}$  розглянемо відображення  $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ , задане як  $\pi(n) = [n]$ . Із побудови групи  $\mathbb{Z}/n\mathbb{Z}$  випливає, що  $\pi$  є сюр'єктивним гомоморфізмом.

Приклади 1.8 і 1.12 узагальнюються до конструкції, яка називається фактор-групою. Щоб зробити це узагальнення майже безпосереднім, ми поставимо приклади 1.8 і 1.12 в трішки інакший контекст. Помітимо, що множина чисел  $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$  є підгрупою групи  $\mathbb{Z}$ . Відношення еквівалентності із означення групи  $\mathbb{Z}/n\mathbb{Z}$  можна переформулювати як

$$[a] = [b] \iff a - b \in n\mathbb{Z}.$$

В такому разі очевидно, що якщо  $a, a', b, b' \in \mathbb{Z}$  такі що  $[a] = [a']$  і  $[b] = [b']$ , то  $[a + b] = [a' + b']$ , адже

$$[a + b] = [a' + b'] \iff a + b - a' - b' = (a - a') + (b - b') \in n\mathbb{Z}.$$

Як наслідок, ми визначили бінарну операцію на множині класів еквівалентності, яка задовольняє означенню групи. Більше того, відображення  $a \mapsto [a]$  є гомоморфізмом груп. Проте для некомутативних груп ми маємо перешкоду. Припустимо, що ми хочемо повторити процес для довільної групи  $G$  і її підгрупи  $H$ . В загальному випадку група  $G$  не має бути комутативною, одже, нам доведеться розрізняти право та ліво. Визначимо два відношення еквівалентності на  $G$  наступним чином:

$$a \sim_l b \iff a^{-1}b \in H, \quad a \sim_r b \iff ba^{-1} \in H.$$

Легко переконатися, що визначені відношення є відношеннями еквівалентності. Дійсно, якщо  $a \sim_l b$ , то  $b^{-1}a = (a^{-1}b)^{-1} \in H$ , отже,  $b \sim_l a$  і відношення  $\sim_l$  є симетричним. Для рефлексивності помітимо, що  $a^{-1}a = 1 \in H$ , отже  $a \sim_l a$ . Нарешті, якщо  $a \sim_l b$  та  $b \sim_l c$ , то  $a^{-1}b$  та  $b^{-1}c$  належать групі  $H$ , але тоді їхній добуток  $a^{-1}c$  теж належить  $H$ , отже, відношення  $\sim_l$  є транзитивним. Клас елементу  $a$  по відношенню  $\sim_l$  позначимо через  $aH$  і називатимемо *лівим класом суміжності елемента  $a$  за підгрупою  $H$* . Можна мислити  $aH$  як множину елементів  $b \in G$ , таких, що  $a \sim_l b$ . Позначення  $aH$  аргументоване наступними рівностями

$$aH = \{b \in G \mid a \sim_l b\} = \{b \in G \mid a^{-1}b = h \in H\} = \{b \in G \mid b = ah, h \in H\} = \{ah \mid h \in H\}.$$

Аналогічно можна визначити *правий клас суміжності елемента  $a$  за підгрупою  $H$* , який позначатиметься  $Ha$  як клас елемента  $a$  по відношенню  $\sim_r$ . Аналогічно доводиться рівність

$$Ha = \{b \in G \mid a \sim_r b\} = \{b \in G \mid ba^{-1} = h \in H\} = \{b \in G \mid b = ha, h \in H\} = \{ha \mid h \in H\}.$$

Множину всіх лівих класів суміжності позначимо через  $G/H$ .

**Лема 1.5.** Нехай  $G$  група і  $H \leq G$  підгрупа, тоді мають місце декомпозиції

$$G = \bigsqcup_{[a] \in G/\sim_l} aH = \bigsqcup_{[a] \in G/\sim_r} Ha.$$

Два ліві (праві) класи суміжності або непертинні, або співпадають.

*Доведення.* Доведення для правих класів суміжності аналогічне до випадку лівих класів суміжності. Для довільного елемента  $a$  очевидно, що  $a \in aH$ , адже  $1 \in H$ , отже, об'єднання всіх класів суміжностей покриває групу  $G$ . Нехай  $a, b \in G$  і припустимо, що  $c \in aH \cap bH$ . Тоді для довільного  $x \in aH$  маємо  $x \sim a \sim c \sim b$ , отже  $x \in bH$ . Ми показали, що  $aH \subset bH$ . Симетричний аргумент показує, що  $bH \subset aH$ , отже,  $aH = bH$ . Ми довели, що якщо перетин двох класів суміжності нетривіальний, то вони співпадають. Декомпозиції із умови леми випливають автоматично.  $\square$

**Наслідок 1.1.** Нехай  $G$  — група і  $H$  — її підгрупа; довільні два ліві (праві) класи суміжності по  $H$  є рівнопотужними. Якщо  $G$  скінченна група, то  $|G| = |H||G/\sim_r| = |H||G/\sim_l|$ , де  $|\cdot|$  позначає кількість елементів множини. Отже, кількість елементів скінченної групи ділиться на кількість елементів підгрупи.

*Доведення.* Достатньо показати, що класи  $aH$  та  $bH$  рівнопотужні для довільних  $a, b \in G$ . Дійсно, визначимо бієкції

$$\begin{aligned} f: aH &\longrightarrow bH, & x &\longmapsto ba^{-1}x; \\ g: bH &\longrightarrow aH, & x &\longmapsto ab^{-1}x; \end{aligned}$$

Легко перевірити, що  $f$  та  $g$  є взаємно оберненими відображеннями, отже, бієкціями. Якщо група  $G$  скінченна, то множини  $G/\sim_r$ ,  $G/\sim_l$ , та  $H$  є скінченними, отже

$$|G| = \sum_{a \in G/\sim_l} |aH| = \sum_{a \in G/\sim_l} |H| = |G/\sim_l| |H|.$$

Доведення для правих класів суміжності аналогічне.  $\square$

Помітимо, що для комутативних груп (як, наприклад,  $\mathbb{Z}$ ) відношення еквівалентності  $\sim_l$  та  $\sim_r$  співпадають, в той час як в загальному ці відношення є різними. Це створює певні проблеми із визначенням добутку на множині класів еквівалентності, а саме, добуток, заданий як  $[ab] =$

$[a][b]$ , може залежати від вибору представників для  $[a]$  та  $[b]$  (порівняйте із прикладом 1.8). Дійсно, припустимо, що  $a \sim a'$  та  $b \sim b'$ , маємо

$$[ab] = [a'b'] \iff (ab)^{-1}(a'b') = b^{-1}a^{-1}a'b' \in H. \quad (1)$$

Елемент  $a^{-1}a'$  дійсно належить підгрупі  $H$ , більш того, оскільки  $b \sim b'$ , то  $b' \in Hb$ , отже

$$b^{-1}a^{-1}a'b' \in b^{-1}Hb' = b^{-1}Hb = \{b^{-1}hb \mid h \in H\}.$$

Але немає жодних гарантій, що цей елемент належить підгрупі  $H$ . Наступний приклад показує, що це, більш того, неправда.

**Приклад 1.13.** Нехай  $X = \{1, 2, 3\}$  — множина із трьох елементів, і  $S_3 = \text{Aut}(X)$  є групою її бієкцій. Нехай  $H$  є підгрупою в  $S_3$  тих бієкцій  $f: X \rightarrow X$ , які задовольняють  $f(3) = 3$ . Розглянемо бієкції

$$\begin{aligned} f_1: X &\longrightarrow X, & 1 &\mapsto 1, & 2 &\mapsto 3, & 3 &\mapsto 2; \\ f_2: X &\longrightarrow X, & 1 &\mapsto 3, & 2 &\mapsto 1, & 3 &\mapsto 2; \\ g: X &\longrightarrow X, & 1 &\mapsto 2, & 2 &\mapsto 3, & 3 &\mapsto 1; \end{aligned}$$

Таким чином, маємо  $f_2^{-1}f_1(3) = f_2^{-1}(2) = 3$ , отже,  $f_2^{-1}f_1 \in H$ , проте  $g^{-1}f_2^{-1}f_1g(3) = 1$ . Отже, навіть якщо  $f_1 \sim f_2$  та  $g \sim g$ , еквівалентність  $f_1g \sim f_2g$  не виконується.

Зважаючи на приклад 1.13, замість того, щоб розглядати довільні підгрупи, ми обмежимося підгрупами, для яких відношення  $\sim_l$  та  $\sim_r$  співпадають. Наступне твердження характеризує такі підгрупи.

**Означення-Твердження 1.1.** Підгрупа  $H$  групи  $G$  називається *нормальною* (позначатиметься  $H \triangleleft G$ ), якщо виконується одна (всі) із наступних еквівалентних умов:

1.  $gHg^{-1} = H$  для довільного  $g \in G$ ;
2.  $gH = Hg$  для довільного  $g \in G$ ;
3. Відношення еквівалентності  $\sim_r$  та  $\sim_l$  співпадають.

*Доведення.* Припустимо, що виконується перша умова. Тоді маємо рівності:

$$Hg = \{hg \mid h \in H\} = \{hg \mid h = gh'g^{-1} \in gHg^{-1}\} = \{gh' \mid h' \in H\} = gH.$$

Отже, виконується друга умова. Припустимо, що виконується друга умова, тоді  $a \sim_l b$  еквівалентно  $a \in bH = Hb$ , отже,  $a \in Hb$ , що еквівалентно  $a \sim_r b$ . Симетричним аргументом доводиться, що із  $a \sim_r b$  випливає  $a \sim_l b$ , отже, два відношення еквівалентності рівні і пункт три виконується. Нарешті, якщо виконується третій пункт, то для  $x \in gHg^{-1}$  маємо  $g^{-1}x \in Hg^{-1}$ , отже  $g^{-1}x \sim_r g^{-1}$ , але тоді  $g^{-1}x \sim_l g^{-1}$ , отже  $x = gg^{-1}x \in H$ . Маємо  $gHg^{-1} \subset H$ . Навпаки, якщо  $x \in H = gg^{-1}H$ , то  $g^{-1}x \in g^{-1}H$ , отже  $g^{-1}x \sim_l g^{-1}$ , але тоді  $g^{-1}x \sim_r g^{-1}$ , отже  $g^{-1}x \in Hg^{-1}$ . Маємо  $x \in gHg^{-1}$ .  $\square$

Очевидно, що будь-яка підгрупа комутативної групи є нормальною, бо відношення  $\sim_l$  та  $\sim_r$  співпадають. Як показує приклад 1.13, підгрупа групи  $S_3$ , яка складається із бієкцій, фіксуючих точку 3, не є нормальною. Ми побачимо більше прикладів нормальних підгруп в некомутативних групах згодом. Повертаючись до узагальнення конструкції 1.8, нехай  $N \triangleleft G$  є нормальною підгрупою, тоді в (1) маємо

$$b^{-1}a^{-1}a'b' \in b^{-1}Hb' = b^{-1}Hb = H,$$

отже, клас  $[ab] = [a'b']$  не залежить від вибору представників класів  $[a]$  та  $[b]$ .

**Означення-Твердження 1.2.** Нехай  $G$  — група і  $N \triangleleft G$  — нормальна підгрупа. Множина класів еквівалентності  $G/\sim$ , де  $\sim$  визначено як  $a \sim b \iff a^{-1}b \in N$ , із операцією  $[ab] = [a][b]$ , є групою, яка називається фактор-групою  $G$  по  $N$  і позначається  $G/N$ . Відображення

$$\pi: G \longrightarrow G/N, \quad g \longmapsto [g]$$

є гомоморфізмом груп, який називатимемо *канонічною проекцією*  $G$  на  $G/N$ .



*Доведення.* Доведення безпосередньо випливає із вищеописаної побудови.  $\square$

**Приклад 1.14.** Нехай  $V$  є скінченно-вимірним векторним простором і  $SO(V) \subset GL(V)$  позначає підмножину всіх обертовних матриць із визначником 1. Оскільки визначник є мультіплікативною функцією (тобто,  $\det(AB) = \det(A)\det(B)$ , для довільних  $A, B \in GL(V)$ ), то можна переконатись, що для  $A, B \in SO(V)$  виконується

$$\det(AB) = \det(A)\det(B) = 1, \quad \det(A^{-1}) = \det(A) = 1.$$

Отже,  $SO(V)$  є підгрупою групи  $GL(V)$ . Більше того, помітимо, що  $\det(A^{-1}BA) = \det(B)$  для довільних  $A, B \in GL(V)$ , отже, для довільного  $A \in SO(V)$  маємо  $BAB^{-1} \in SO(V)$ . Виявляється, що  $SO(V)$  є нормальною підгрупою в  $GL(V)$ . Як ми переконаємось пізніше, якщо  $V$  є векторним простором над полем  $\mathbb{K}$ , фактор-групою  $GL(V)$  по  $SO(V)$  є

$$GL(V)/SO(V) \cong \mathbb{K}^\times = \mathbb{K} \setminus \{0\}.$$

### 1.3 Ядро, образ і деякі класи морфізмів

В минулій секції ми визначили головні приклади гомоморфізмів, а саме — включення підгрупи в групу та канонічна проекція з групи на фактор-групу по нормальній підгрупі. Очевидно, що перше є ін'єктивним, а друге сюр'єктивним. В цій секції ми покажемо, що будь-який гомоморфізм є композицією проекції, ототожнення та включення підгрупи.

**Означення 1.6.** Нехай  $G$  та  $H$  — групи і  $f: G \rightarrow H$  — гомоморфізм груп.

1.  $f$  називається *ізоморфізмом*, якщо знайдеться гомоморфізм груп  $g: H \rightarrow G$  такий, що

$$g \circ f = \text{id}_G, \quad f \circ g = \text{id}_H. \quad (2)$$

Гомоморфізм  $g$  називається *оберненням до  $f$* . Дві групи, між якими існує ізоморфізм, називаються *ізоморфними*. В такому випадку ми використовуємо позначення  $G \cong H$ .

2.  $f$  називається *моно(морфізмом)*, якщо  $f$  є ін'єктивним відображенням;
3.  $f$  називається *епі(морфізмом)*, якщо  $f$  є сюр'єктивним відображенням

Легко переконатися, що відношення  $\cong$  на множині всіх груп є відношенням еквівалентності. Дійсно, для довільної групи  $G$  тотожне відображення показує, що  $G \cong G$ . Якщо  $G \cong H$  і  $f: G \rightarrow H$  — це ізоморфізм, то за означенням існує гомоморфізм  $g: H \rightarrow G$ , який також є ізоморфізмом, отже  $H \cong G$ . Нарешті, якщо  $f: G \rightarrow H$  і  $h: H \rightarrow K$  є ізоморфізмами, із оберненими  $g: H \rightarrow G$  та  $t: K \rightarrow H$ , то  $g \circ t$  є оберненням до  $h \circ f$ .

**Лема 1.6.** Гомоморфізм груп є ізоморфізмом тоді і тільки тоді, коли він є бієктивним.

*Доведення.* Очевидно, що ізоморфізм груп завжди є бієкцією. Навпаки, нехай  $f: G \rightarrow H$  є бієктивним гомоморфізмом груп. Оскільки  $f$  є бієкцією, то знайдеться відображення множин  $g: H \rightarrow G$  таке, що (2) виконується. Залишається переконатися, що  $g$  є гомоморфізмом. Дійсно, для  $a, b \in H$  нехай  $a', b' \in G$  — такі елементи, що  $f(a') = a$  і  $f(b') = b$ . Маємо

$$g(ab) = g(f(a')f(b')) = g(f(a'b')) = a'b' = (g \circ f)(a')(g \circ f)(b') = g(a)g(b).$$

Отже,  $g: H \rightarrow G$  є гомоморфізмом груп і  $f$  є ізоморфізмом.  $\square$

Апріорі кожен ізоморфізм є просто переназиванням елементів групи, сумісним із операціями цих груп, отже, ізоморфні групи мають мислитись як тотожні об'єкти.

**Наслідок 1.2.** Якщо гомоморфізм груп є і моно, і епі одночасно, то він є ізоморфізмом.

Очевидно, не будь-який гомоморфізм є ізоморфізмом, мономорфізмом чи епіморфізмом. Наприклад, вкладіть  $2\mathbb{Z}$  в  $\mathbb{Z}$  і профакторте по  $4\mathbb{Z}$ . Виходить гомоморфізм груп

$$f: 2\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z}, \quad 2n \mapsto [2n].$$

Це відображення не є ін'єктивним, адже  $f(4) = [0]$ . Воно не є сюр'єктивним, адже жодне число, яке дає остачу 3 при діленні на 4, не ділиться на 2. Виникає питання, чи можна визначити «міру» ін'єктивності чи сюр'єктивності гомоморфізму.

**Означення 1.7.** Нехай  $f: G \rightarrow H$  — гомоморфізм груп. Ядром гомоморфізму  $f$  називається множина  $\ker(f) = \{g \in G \mid f(g) = 1_H\} \subset G$ . Образом гомоморфізму називається множина  $\operatorname{im}(f) = \{f(g) \mid g \in G\} \subset H$ .

**Лема 1.7.** Нехай  $f: G \rightarrow H$  — гомоморфізм груп. Тоді його ядро є нормальною підгрупою в  $G$ ; його образ є підгрупою в  $H$ . Більш того наступні речі еквівалентні:

1.  $f$  є моно тоді і лише тоді, коли  $\ker(f) = \{1\}$ ;
2.  $f$  є епі тоді і лише тоді, коли  $\operatorname{im}(f) = H$ .

*Доведення.* Зрозуміло, що  $\ker(f)$  та  $\operatorname{im}(f)$  є підгрупами, адже  $f(xy) = f(x)f(y)$ . Помітимо, що  $f(g^{-1}xg) = f(g)^{-1}f(x)f(g) = f(g)^{-1}f(g) = 1_H$ , для довільного  $g \in G$ , а отже

$$g^{-1}\ker(f)g = \{gxg^{-1} \mid f(x) = 0\} = \{x \mid f(x) = 0\} = \ker(f).$$

Маємо, що  $\ker(f)$  є нормальною підгрупою. Той факт, що  $f$  є епіморфізмом, тоді і тільки тоді, коли  $\operatorname{im}(f) = H$ , є просто переформулюванням означення. Щодо ядра, очевидно, що із ін'єктивності  $f$  випливає  $\ker(f) = \{1\}$ . Навпаки, припустимо, що  $f$  не є ін'єкцією, тоді є елементи  $g \neq h$  в  $G$ , такі, що  $f(g) = f(h)$ . Але тоді  $g^{-1}h \neq 1_G$  і задовольняє  $f(g^{-1}h) = 1_H$ , отже, є нетривіальним елементом ядра.  $\square$

Ми довели, що групи  $\ker(f)$  та  $\operatorname{im}(f)$  дійсно є “мірами” того, що гомоморфізм є мономорфізмом або епіморфізмом відповідно.

**Лема 1.8.** Нехай  $f: G \rightarrow H$  — гомоморфізм груп і  $K \triangleleft G$  є нормальною підгрупою, такою, що  $K \subset \ker(f)$ . Тоді знайдеться єдиний гомоморфізм груп  $g: G/K \rightarrow H$ , для якого наступна діаграма комутує:

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \downarrow \pi & \nearrow g & \\ G/K & & \end{array}$$

Іншими словами,  $g \circ \pi = f$ , де  $\pi: G \rightarrow G/K$  — канонічна проекція.

*Доведення.* Нехай  $a \in G/K$  і  $a' \in G$  такий, що  $\pi(a') = a$ . Визначимо відображення

$$g: G/K \rightarrow H, \quad a \mapsto f(a').$$

Варто перевірити, що  $g$  не залежить від вибору представника для аргументу. Нехай  $a', a'' \in G$  двома елементами групи  $G$ , які задовольняють  $\pi(a') = \pi(a'')$ . В такому разі елемент  $(a')^{-1}a''$  належить  $\ker(\pi) = N$ . Оскільки  $N \subset \ker(f)$ , маємо  $f((a')^{-1}a'') = 1$ , а отже  $f(a') = f(a'')$ . Як наслідок, відображення  $g$  не залежить від вибору представника для аргументу. Перевіримо, що  $g$  є гомоморфізмом. Для  $a, b \in G/K$  нехай  $a', b' \in G$  такі, що  $\pi(a') = a$  та  $\pi(b') = b$ . Оскільки  $\pi$  є гомоморфізмом, то  $\pi(a'b') = ab$ , отже маємо:

$$g(ab) = f(a'b') = f(a')f(b') = g(a)g(b).$$

Коммутативність діаграми тепер очевидна. Дійсно, для елементів  $a, b$  групи  $G$  маємо рівності  $g \circ \pi(a) = g(\pi(a)) = f(a)$ . Залишається довести єдиність. Припустимо, що  $g': G/K \rightarrow H$  — інший гомоморфізм, який задовольняє  $g' \circ \pi = f$ . Але тоді для довільного  $a \in G/K$  і  $a' \in G$ , який задовольняє  $\pi(a') = a$ , маємо  $g'(a) = g' \circ \pi(a') = f(a') = g(a)$ .  $\square$

Минула лема дає певну декомпозицію гомоморфізмів у композицію епіморфізму  $\pi$  та нового гомоморфізму  $g$ . З іншого боку, існує тривіальна декомпозиція гомоморфізмів у композицію мономорфізму та іншого відображення. Дійсно, нехай  $f: G \rightarrow H$  — гомоморфізм, а  $i: \operatorname{im}(f) \rightarrow H$  — гомоморфізм включення підгрупи. Визначимо гомоморфізм

$$h: G \rightarrow \operatorname{im}(f), \quad g \mapsto f(g).$$

Очевидно бачити, що  $f = i \circ h$  і гомоморфізм  $i$  є ін'єктивним, а отже, моно, а гомоморфізм  $h$  є сюр'єктивним, отже, епі. Також легко помітити, що відображення  $h$  є єдиним таким, що задовольняє  $f = i \circ h$ . Скомбінувавши попередню лему із цим зауваженням, можна отримати теорему.

**Теорема 1.1.** Нехай  $f: G \rightarrow H$  — гомоморфізм груп. Існує єдиний ізоморфізм

$$\tilde{f}: G/\ker(f) \rightarrow \operatorname{im}(f),$$

такий, що  $f = i \circ \tilde{f} \circ \pi$ , де  $\pi: G \rightarrow G/\ker(f)$  є канонічною проекцією, а  $i: \operatorname{im}(f) \rightarrow H$  є канонічним включенням.

*Доведення.* Застосовуючи лему 1.8 до  $f$  та підгрупи  $N = \ker(f)$  (яка є нормальною за лемою 1.7) отримаємо гомоморфізм груп  $g: G/\ker(f) \rightarrow H$ . За побудовою  $g$  очевидно, що групи  $\operatorname{im}(g)$  та  $\operatorname{im}(f)$  співпадають. Застосовуючи вищезгадане зауваження до гомоморфізму  $g$ , отримуємо гомоморфізм  $\tilde{f}: G/\ker(f) \rightarrow \operatorname{im}(f)$ . Єдиність впливає із єдиності відображення  $g$ . Відображення  $\tilde{f}$  сюр'єктивне за побудовою. Щоб побачити ін'єктивність, припустимо, що  $a \in G/\ker(f)$  задовольняє  $\tilde{f}(a) = 1$ . В такому разі, для довільного  $a' \in G$ , який задовольняє  $\pi(a') = a$ , маємо  $f(a') = 1$ , отже  $a' \in \ker(f)$ , але тоді  $\pi(a') = 1 = a$ . Отже,  $\ker(\tilde{f}) = \{1\}$  і  $\tilde{f}$  є ін'єктивним за лемою 1.7. Як наслідок,  $\tilde{f}$  є ізоморфізмом.  $\square$

Ця теорема і дає бажану декомпозицію, анонсовану на початку секції.

**Приклад 1.15.** Пригадаємо з прикладу 1.14, що  $\operatorname{SO}(V)$  є нормальною підгрупою в  $\operatorname{GL}(V)$  обертових матриць із визначником 1. Легко помітити, що відображення

$$\det: \operatorname{GL}(V) \rightarrow \mathbb{K}^\times = \mathbb{K} \setminus \{0\}$$

є гомоморфізмом груп, ядро якого (за визначенням) є  $\operatorname{SO}(V)$ . Легко помітити також, що  $\det$  є сюр'єктивним. Отже за Теоремою 1.1 маємо

$$\operatorname{GL}(V)/\operatorname{SO}(V) \cong \operatorname{im}(\det) = \mathbb{K}^\times.$$

**Приклад 1.16.** Група  $G$  називається *циклічною*, якщо знайдеться  $g \in G$  такий, що кожне  $h \in G$  задовольняє  $h = g^n$  для деякого  $n \in \mathbb{Z}$ . Легко бачити, що циклічні групи комутативні, адже для  $h, k \in G$  знайдуться  $n, m \in \mathbb{Z}$  такі, що  $h = g^n$  та  $k = g^m$ , але тоді

$$hk = g^n g^m = g^{n+m} = g^m g^n = kh.$$

Очевидно, що групи  $\mathbb{Z}$  та  $\mathbb{Z}/n\mathbb{Z}$  є циклічними, і роль елемента  $g$  виконують елементи  $1 \in \mathbb{Z}$ ,  $[1] \in \mathbb{Z}/n\mathbb{Z}$ . Насправді, інших циклічних груп не існує. Дійсно, нехай  $G$  — циклічна група і  $g \in G$  є таким елементом, що для довільного  $h \in G$  виконується  $h = g^n$  для деякого  $n \in \mathbb{Z}$ . Побудуємо відображення

$$f: \mathbb{Z} \rightarrow G, \quad k \mapsto g^k.$$

Легко перевірити, що  $f$  є гомоморфізмом, адже  $f(k)f(l) = g^k g^l = g^{k+l} = f(k+l)$ . Більше того, оскільки  $G$  циклічна, то  $f$  є сюр'єктивним. Отже, за теоремою 1.1 маємо ізоморфізм

$$G \cong \mathbb{Z}/\ker(f),$$

де  $\ker(f)$  є підгрупою (автоматично нормальною через комутативність  $\mathbb{Z}$ ) в  $\mathbb{Z}$ . Але всі підгрупи  $\mathbb{Z}$  мають вигляд  $n\mathbb{Z}$ , де  $n \in \mathbb{N}$ . Дійсно, якщо  $H$  є підгрупою в  $\mathbb{Z}$  і  $a, b \in H$  є додатніми числами, то за теоремою Безу маємо

$$\gcd(a, b) = ca + bd$$

для деяких  $c, d \in \mathbb{Z}$ , отже  $\gcd(a, b)$  належить  $H$ . Виберемо  $a \in H$  — найменше додатне число в  $H$ . Якщо  $\gcd(a, b) \neq a$  для всіх  $b \in H$ , то  $a$  не є найменшим, отже, маємо протиріччя. Інакше маємо  $H = a\mathbb{Z}$ .

## 1.4 Порядки елементів та класифікація скінчених комутативних груп

Попередні викладки дають нам змогу відносно легко будувати гомоморфізми і доводити, що дві групи ізоморфні. Постає питання, чи можна виписати повний список скінчених груп. У загальному випадку це відкрите питання, яке навряд чи коли-небудь буде вирішене, проте для комутативних груп в цій секції ми дамо повне рішення цієї проблеми. Почнемо з того, що ми досі не знаємо, чи групи  $K_4$  та  $\mathbb{Z}/4\mathbb{Z}$  є різними. Доволі простим і корисним в цій ситуації інваріантом стає поняття порядку елемента.

**Означення 1.8.** Для  $g \in G$  його порядком називається найменше натуральне число  $n \in \mathbb{N}$ , яке задовольняє  $g^n = 1_G$ ; якщо такого числа не знайдеться, то  $n = \infty$ . Порядок елемента  $g \in G$  позначатиметься як  $\operatorname{ord}(g)$ . Для скінченної групи її порядком називається кількість її елементів.

Очевидно, що скінченна група не може мати елементів нескінченного порядку. Дійсно, якщо  $G$  скінченна група, то множина  $\{g^n \mid n \in \mathbb{N}\} \subset G$  має бути скінченною, отже, для деяких  $n < m$  виконується  $g^n = g^m$ . Помноживши на  $g^{-n}$ , маємо  $g^{m-n} = 1_G$ , отже  $\text{ord}(g) \leq m - n$ .

**Лема 1.9.** Якщо  $f: H \rightarrow G$  — гомоморфізм груп, то для довільного  $g \in G$  порядок  $f(g)$  ділить порядок  $g$ . Якщо  $f$  є мономорфізмом, то виконується рівність

$$\text{ord}(g) = \text{ord}(f(g)).$$

*Доведення.* Нехай  $H_0 \leq H$  є підгрупою в  $H$  яка породжена елементом  $g$ , тобто

$$H_0 = \{1, g, g^2, \dots, g^{\text{ord}(g)-1}\}.$$

Нехай  $i: H_0 \rightarrow H$  є гомоморфізмом включення  $H_0$  в  $H$ . Помітимо, що образ  $f \circ i: H_0 \rightarrow G$  складається із степенів  $f(g)$  і має порядок  $\text{ord}(f)$ . За теоремою 1.1 маємо

$$\text{ord}(g) = |H_0| = |\ker(f \circ i)| |\text{im}(f \circ i)| = |\ker(f \circ i)| \text{ord}(f(g)).$$

Отже,  $\text{ord}(f(g))$  ділить  $\text{ord}(g)$ , і якщо  $f$  є мономорфізмом, то  $f \circ i$  є мономорфізмом, отже, ядро гомоморфізму  $f \circ i$  складається лише із нейтрального елемента і  $\text{ord}(g) = \text{ord}(f(g))$ .  $\square$

**Наслідок 1.3.** Нехай  $g \in G$ , тоді порядок елемента ділить порядок групи  $\text{ord}(g) \mid |G|$ .

*Доведення.* Достатньо розглянути підгрупу  $H = \{1, g, g^2, \dots, g^{\text{ord}(g)-1}\} \leq G$ .  $\square$

Тепер ми можемо легко довести, що  $K_4$  не ізоморфна до  $\mathbb{Z}/4\mathbb{Z}$ . Більше того, це єдині групи на множині із чотирьох елементів. Дійсно,  $\mathbb{Z}/4\mathbb{Z}$  має елемент порядку 4, проте всі елементи  $K_4$  окрім нейтрального мають порядок 2. Якщо  $H$  — це група із чотирьох елементів, то якщо вона має елемент  $x$  порядку 4, вона є ізоморфною до  $\mathbb{Z}/4\mathbb{Z}$ , через відображення  $[k] \mapsto x^k$ . Інакше, кожен її елемент має порядок 2, отже  $H = \{1, a, b, ab\}$ , де елементи  $a, b$  задовольняють співвідношення  $a^2 = b^2 = 1$ ,  $ab = ba$ .

Ми можемо спробувати почати класифікувати скінченні групи. Нехай  $G$  є скінченною групою. Якщо  $G$  має нетривіальну власну нормальну підгрупу  $H_1$  (тобто  $H_1 \neq \{1\}$  та  $H_1 \neq G$ ), то  $H_1$  є новою скінченною групою, порядок якої строго менший за порядок  $G$ . Повторюючи цю процедуру для  $H_1$  і для її нормальних підгруп ми отримуємо ланцюжок нормальних підгруп

$$H_n \triangleleft H_{n-1} \triangleleft \dots \triangleleft H_1 \triangleleft G.$$

Оскільки група  $G$  скінченна, то ланцюжок нормальних підгруп не може бути нескінченним, отже, остання із підгруп  $H_n$  є групою, яка не містить нетривіальних власних нормальних підгруп (еквівалентно, якщо  $K \triangleleft H_n$  є нормальною підгрупою, то або  $K = H_n$ , або  $K = \{1\}$ ). Група  $H$  називається *простою*, якщо вона не містить нетривіальних власних нормальних підгруп. Класифікація простих груп завершена, і ми маємо повний (нескінченний) список простих груп, проте доведення, як і повний список простих груп, є копіляцією декількох сотень робіт різних авторів і точно не є матеріалом для літніх шкіл. Натомість ми сфокусуємося на класифікації комутативних груп. У комутативному випадку кожна підгрупа є нормальною, отже, простою комутативною групою є група, єдині підгрупи якої — це вона сама та  $\{1\}$ .

**Лема 1.10.** Для кожного простого числа  $p \in \mathbb{N}$  існує єдина група порядку  $p$ . Більше того, кожна проста комутативна група має простий порядок.

*Доведення.* Дійсно, нехай  $p \in \mathbb{N}$  є простим числом і  $G$  є групою із  $p$  елементів. Елемент  $x \in G \setminus \{1_G\}$  має скінченний порядок, нерівний одиниці, отже  $\text{ord}(x)$  ділить  $p$ , але тоді  $\text{ord}(x) = p$ . Побудуємо

$$f: \mathbb{Z} \rightarrow G, \quad [k] \mapsto x^k.$$

Помітимо, що  $f(a) = 1$  тоді і тільки тоді, коли  $a$  ділиться на  $p$ , отже,  $\ker(f) = p\mathbb{Z}$ . Більше того, оскільки  $G$  має  $p$  елементів і  $x$  має порядок  $p$ , то підмножина  $\{1, x, x^2, \dots, x^{p-1}\}$  групи  $G$  має  $p$  елементів і збігається із  $G$ . Отже,  $f$  є сюр'єктивним. За теоремою 1.1 маємо ізоморфізми:

$$\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/\ker(f) \cong \text{im}(f) = G.$$

Для другої частини нехай  $G$  — проста комутативна група. Для  $x \in G \setminus \{1_G\}$  підмножина  $\{1, x, x^2, \dots\}$  групи  $G$  є підгрупою, відмінною від тривіальної, отже, вона рівна  $G$  і  $G$  є скінченною циклічною групою (отже, має вигляд  $\mathbb{Z}/n\mathbb{Z}$ ). Припустимо, що  $n$  не є простим числом, і нехай  $k \in \mathbb{N}$  — нетривіальний дільник  $n$ . Тоді елемент  $[n/k] \in \mathbb{Z}/n\mathbb{Z}$  має порядок  $k \neq n$ , отже, породжує нетривіальну підгрупу. Маємо протиріччя, отже  $G \cong \mathbb{Z}/p\mathbb{Z}$  для деякого простого числа  $p$ .  $\square$

**Означення 1.9.** Нехай  $p \in \mathbb{N}$  є простим числом. Скінченна група  $G$  називається  $p$ -групою, якщо порядок кожного її елемента є степінню  $p$ .

Наприклад, для простого числа  $p$  довільний добуток груп вигляду  $\mathbb{Z}/p^k\mathbb{Z}$  є  $p$ -групою. Прикладом некомутативної 2-групи є  $D_4$  (порядок  $D_4$  дорівнює 8, отже, порядок кожного з її елементів є степінню двійки).

**Лема 1.11.** Нехай  $G$  скінченна комутативна група і  $p \in \mathbb{N}$  — просте число, яке ділить порядок  $G$ . Тоді  $G$  містить підгрупу порядку  $p$ .

*Доведення.* Ми доведемо це твердження індукцією за порядком групи  $G$ . Оскільки достатньо розглядати порядки, які діляться на  $p$ , то нехай  $G$  є групою, порядок якої рівний  $p$ . Як вже було зазначено, єдиною такою групою є  $\mathbb{Z}/p\mathbb{Z}$ , а вона містить елемент порядку  $p$ .

Припустимо, що твердження доведено для всіх груп, порядок яких менший за  $pk$ , і нехай  $G$  є групою порядку  $p(k+1)$ . Оскільки єдиними простими комутативними групами є групи вигляду  $\mathbb{Z}/p\mathbb{Z}$ , порядком яких є  $p$ , то  $G$  має нетривіальну власну підгрупу  $H$ . Оскільки всі підгрупи комутативної групи нормальні, то  $G/H$  є групою та  $|G| = |H||G/H|$ . Отже,  $p$  ділить  $|H|$  або  $|G/H|$ . Але порядки цих підгруп є строго меншими за порядок  $|G|$ , отже, за припущенням індукції твердження справджується для  $H$  та  $G/H$ . В першому випадку (якщо  $p$  ділить порядок  $H$ ), за припущенням маємо, що  $H$  містить елемент порядку  $p$ , але тоді і  $G$  містить елемент порядку  $p$ . В другому випадку (якщо  $p$  ділить порядок  $G/H$ ), за припущенням  $G/H$  має елемент порядку  $p$ , і нехай  $g \in G$  його прообраз. Оскільки канонічна проекція  $\pi: G \rightarrow G/H$  є гомоморфізмом, то  $p = \text{ord}(\pi(g))$  ділить  $\text{ord}(g)$ . Отже,  $\text{ord}(g) = pk$ , але тоді  $g^k \in G$  має порядок  $p$ . Отже,  $G$  містить елемент порядку  $p$ .  $\square$

Із попередньої леми легко випливає, що кожна  $p$ -група має порядок  $p^k$ , для якогось  $k \in \mathbb{N}$ . Дійсно, нехай  $G$  є  $p$ -групою, і припустимо, що просте число  $q \neq p$  ділить порядок  $G$ . Але тоді  $G$  має підгрупу порядку  $q$ , а отже, елемент порядку  $q$ , що суперечить означенню  $p$ -групи.

**Приклад 1.17.** Розглянемо циклічну  $p$ -групу  $\mathbb{Z}/p^k\mathbb{Z}$ . Оскільки елемент  $[1] \in \mathbb{Z}/p^k\mathbb{Z}$  є породжуючим, то його порядок рівний  $p^k$ . Для елемента  $g = [p^{k-1}] \in \mathbb{Z}/p^k\mathbb{Z}$  маємо

$$p[p^{k-1}] = p \sum_{i=1}^{p^{k-1}} [1] = \sum_{i=1}^{p^k} [1] = 0,$$

отже  $\text{ord}(g) \leq p$ . Порядок елемента  $g$  не може бути строго меншим за  $p$ , адже тоді він не ділитиме порядок групи  $\mathbb{Z}/p^k\mathbb{Z}$ . Більше того, припустимо, що  $h \in \mathbb{Z}/p^k\mathbb{Z}$  є елементом порядку  $p$ . Оскільки  $\mathbb{Z}/p^k\mathbb{Z}$  є циклічною, то знайдеться ціле число  $n$  таке, що  $h = [n]$ . Маємо, що  $0 = ph = p[n] = [pn]$ , отже,  $pn$  ділиться на  $p^k$ , а тоді  $n = ap^{k-1}$ , для якогось  $a \in \mathbb{Z}$ . Але кожен такий клас  $[n]$  належить підгрупі, породженій  $[p^{k-1}]$  в  $\mathbb{Z}/p^k\mathbb{Z}$ . Отже, циклічна  $p$ -група має єдину підгрупу порядку  $p$ .

**Лема 1.12.** Нехай  $p$  — просте число, а  $G$  — скінченна комутативна  $p$ -група, яка містить єдину підгрупу порядку  $p$ . Тоді  $G$  є циклічною.

*Доведення.* Ми знову застосуємо індукцію за кількістю елементів у  $G$ . Якщо  $|G| = p$ , то  $G \cong \mathbb{Z}/p\mathbb{Z}$  за попередньо доведеним і є циклічною. Припустимо, що твердження доведено для всіх комутативних груп, порядок яких менший або рівний  $p^k$ , і нехай  $G$  має порядок  $p^{k+1}$ . Визначимо відображення

$$\phi: G \rightarrow G, \quad g \mapsto g^p.$$

Легко перевірити, що  $\phi$  є гомоморфізмом. Помітимо, що ядром гомоморфізму  $\phi$  є в точності елементи, порядки яких рівні  $p$ . Оскільки  $G$  має єдину підгрупу  $H$ , порядок якої рівний  $p$ , то  $H \subset \ker(\phi)$ . Більше того, якщо  $H \neq \ker(\phi)$ , то знайдеться елемент порядку  $p$  в  $G$ , який не належить  $H$ , але тоді він породить іншу підгрупу порядку  $p$ , відмінну від  $H$ , що суперечить припущенню. Отже,  $\ker(\phi) = H$ . Якщо  $H = G$ , то  $G$  має порядок  $p$ , а отже  $G \cong \mathbb{Z}/p\mathbb{Z}$  і твердження очевидне. Інакше  $\phi(G)$  є нетривіальною власною підгрупою в  $G$ , ізоморфною  $G/H$ . Оскільки  $G$  є  $p$ -групою, то порядок  $\text{im}(\phi) \cong G/H$  має ділитись на  $p$ . За попередньою лемою  $\text{im}(\phi)$  має підгрупу порядку  $p$ . Оскільки  $\text{im}(\phi)$  є підгрупою в  $G$ , то така підгрупа є єдиною (і рівною  $H = \ker(\phi)$ ) в  $\text{im}(\phi)$ . Застосовуючи припущення індукції,  $\text{im}(\phi)$  є циклічною групою.

Залишається показати, що  $G$  сама є циклічною. Нехай  $g_0 \in \text{im}(\phi)$  є породжуючим цієї групи і  $g \in G$  є довільним прообразом  $g_0$  під дією гомоморфізму  $\phi$ . Нехай  $G_0$  є підгрупою  $G$ , яка породжена елементом  $g$ . Оскільки  $G$  є  $p$ -групою, група  $G_0$  теж є  $p$ -групою, а отже, за попередньою

лемою містить підгрупу порядку  $p$ . Оскільки така підгрупа в  $G$  єдина, то  $G_0$  містить  $H$ . Нехай  $h \in G$ , тоді для певного  $k \in \mathbb{N}$  маємо  $\phi(h) = \phi(g^k)$ , отже  $hg^{-k} \in H \subset G_0$ , але тоді  $h \in G_0$ . Отже,  $G_0 = G$  є циклічною групою, яка породжена  $g$ .  $\square$

Перед тим, як продовжити шлях до повної класифікації скінченних комутативних груп, нам треба охарактеризувати, коли група  $G$  ізоморфна добутку своїх підгруп. Наприклад, якщо  $H$  та  $K$  є групами та  $G \cong H \times K$ , то  $G$  містить підгрупи  $H \times \{1\}$  та  $\{1\} \times K$ , які ізоморфні до  $H$  та  $K$  відповідно. Помітимо, що  $H \times \{1\} \cap \{1\} \times K = \{1 \times 1\}$ , де  $1 \times 1$  є нейтральним елементом добутку  $H \times K \cong G$ . Отже, дві підгрупи мають тривіальний перетин. Виявляється, що це і є характеристикою.

**Лема 1.13.** Нехай  $G$  є групою,  $H, K$  є нормальними підгрупами в  $G$ . Тоді відображення

$$i: H \times K \longrightarrow G, \quad (h, k) \longmapsto hk$$

є ізоморфізмом тоді і лише тоді, коли виконуються наступні умови:

1.  $H \cap K = \{1_G\}$ ;
2.  $HK = \{hk \mid h \in H, k \in K\} = G$ .

*Доведення.* Помітимо, що дві нормальні підгрупи, перетин яких тривіальний, комутують (тобто для довільних  $h \in H$  та  $k \in K$  виконується  $hk = kh$ ). Дійсно, якщо  $h \in H$  та  $k \in K$ , то  $hkh^{-1} \in K$  за нормальністю підгрупи  $K$ , отже,  $hkh^{-1}k \in K$ . З іншого боку,  $kh^{-1}k^{-1} \in H$  за нормальністю  $H$ , отже,  $hkh^{-1}k \in H$ . Оскільки перетин тривіальний, маємо  $hkh^{-1}k^{-1} = 1_G$ , отже  $hk = kh$ . Нарешті, через те, що  $H$  та  $K$  комутують, відображення  $i$  є гомоморфізмом, образом якого є добуток  $HK$ . Із другої умови випливає, що  $i$  є епіморфізмом. Ядром  $i$  є пари  $(h, k)$ , такі, що  $hk^{-1} = 1_G$ . Оскільки  $H$  є підгрупою, то пара  $(h, k)$ , яка задовольняє  $hk^{-1} = 1_G$ , складається із елементів  $H$ , отже  $k \in H \cap K$ . Із першої умови випливає, що  $h = k = 1_G$  та  $i$  є мономорфізмом. Отже,  $i$  є ізоморфізмом.  $\square$

**Лема 1.14.** Якщо  $G$  є скінченною комутативною  $p$ -групою і  $C$  є циклічною підгрупою  $G$  максимального порядку, то  $G = C \times H$  для деякої підгрупи  $H$  групи  $G$ .

*Доведення.* Знов-таки, застосовуємо індукцію за порядком групи. Якщо  $|G| = p$ , то  $G$  сама по собі є циклічною (адже вона ізоморфна  $\mathbb{Z}/p\mathbb{Z}$ ) і маємо  $C := G$  та  $H = \{1_G\}$ . Припустимо, що ми довели твердження для всіх груп, порядок яких не перевищує  $p^k$ , і  $G$  має порядок  $p^{k+1}$ . За лемою 1.11 група  $G$  містить підгрупу порядку  $p$ . Якщо така група є єдиною, то за лемою 1.12 група  $G$  є циклічною, і ми знов покладемо  $C := G$  та  $H = \{1_G\}$ . Інакше група  $G$  містить принаймні дві різні підгрупи порядку  $p$ . Нехай  $C$  є циклічною підгрупою  $G$  максимального порядку. Оскільки  $C$  циклічна, вона не може містити більше однієї підгрупи порядку  $p$ , то нехай  $K$  є підгрупою порядку  $p$  в  $G$ , яка не міститься в  $C$ . Маємо  $C \cap K = \{1_G\}$ , адже інакше їхній спільний елемент породить  $K$  всередині  $C$ , що суперечить припущенню. Розглянемо групу  $G/K$ , яка є комутативною групою порядку  $p^k$ . Оскільки  $C \cap K = \{1_G\}$ , то композиція вкладення  $i: C \longrightarrow G$  та проєкції  $\pi: G \longrightarrow G/K$  є ін'єктивною, отже  $C$  є циклічною підгрупою факторгрупи  $G/K$ . Якщо  $C$  не є циклічною групою максимального порядку в  $G/K$ , то знайдеться елемент  $g \in G$  такий, що порядок  $[g] \in G/K$  більший за порядок  $C$ , але тоді порядок  $g \in G$  є більшим за порядок  $C$ , що суперечить максимальності порядку  $C$  в  $G$ . Отже,  $C$  є циклічною групою максимального порядку в  $G/K$  і за припущенням індукції маємо  $G/K \cong C \times H'$ , для якоїсь підгрупи  $H' \leq G/K$ . Розглянемо підгрупу  $H = \pi^{-1}(H')$  в групі  $G$ . Очевидно, що  $C$  та  $H$  є нормальними підгрупами в  $G$  (як і будь-які підгрупи), добуток яких дорівнює  $G$ . Залишається показати, що  $C \cap H = \{1_G\}$ . Дійсно, якщо  $x \in C \cap H$ , то  $\pi(x) \in C \times \{1\} \cap \{1\} \times H'$ , отже,  $\pi(x) = 1$ , з чого випливає, що  $x \in K$ . Оскільки  $C$  та  $K$  перетинаються тривіально, маємо  $x = 1_G$ . Із леми 1.13 випливає, що  $G \cong C \times H$ .  $\square$

**Теорема 1.2.** Довільна скінченна комутативна група є добутком циклічних  $p$ -груп.

*Доведення.* Нехай  $G$  комутативна група. Побачимо, що для  $a, b \in G$  порядок елемента  $ab$  ділить  $\text{ord}(a) \text{ord}(b)$ . Дійсно, виконується рівність

$$(ab)^{\text{ord}(a) \text{ord}(b)} = (a^{\text{ord}(a)})^{\text{ord}(b)} (b^{\text{ord}(b)})^{\text{ord}(a)} = 1,$$

Отже, гомоморфізм  $\phi: \mathbb{Z} \longrightarrow G$ , який відправляє  $k$  в  $(ab)^k$ , містить  $\text{ord}(a) \text{ord}(b)$  в своєму ядрі, яке складається із чисел, які діляться на  $\text{ord}(ab)$ .

Нехай  $G$  скінченна комутативна група і  $G_p = \{g \in G \mid \text{ord}(g) = p^k, k \in \mathbb{N}\}$  є підгрупою всіх елементів, порядок яких є степінню  $p$ . Нехай також  $G^p = \{g \in G \mid p \text{ не ділить } \text{ord}(g)\}$ . Те, що  $G_p$  та  $G^p$  є підгрупами, випливає із вищедоведеної властивості порядку добутку елементів. Із побудови випливає, що  $G_p \cap G^p = \{1_G\}$ . Помітимо також, що якщо для  $g \in G$  маємо  $\text{ord}(g) = p^k t$ , де  $t$  не ділиться на  $p$ , то  $p^k$  та  $t$  є взаємно простими, отже за теоремою Безу маємо

$$1 = at + bp^k,$$

для деяких  $a, b \in \mathbb{Z}$ . Отже,  $g = g^{at} g^{bp^k}$ , де порядок елемента  $g^{at}$  є степінню  $p$ , а порядок елемента  $g^{bp^k}$  не ділиться на  $p$ . Як наслідок,  $G = G_p G^p$ . Із леми 1.13 випливає, що група  $G$  ізоморфна добутку  $G_p \times G^p$ , де  $G_p$  є  $p$ -групою, а порядок  $G^p$  не ділиться на  $p$ . Повторюючи цю процедуру для  $G^p$  і простих чисел, які фігурують в розкладі  $|G^p|$ , отримуємо, що  $G$  ізоморфна добутку груп, кожна з яких є  $p$ -групою, для якогось простого числа  $p$ . Залишається довести, що кожна комутативна  $p$ -група є добутком циклічних груп.

Нехай  $G$  є комутативною  $p$ -групою. Якщо  $G$  має порядок  $p$ , то твердження доведене. Припустимо, що ми довели ствердження для довільної комутативної  $p$ -групи, порядок якої не перевищує  $p^k$ . Для комутативної  $p$ -групи  $G$  порядку  $p^k$  нехай  $C \leq G$  є циклічною підгрупою максимального порядку. Із леми 1.14 випливає, що  $G \cong C \times H$ , де  $H \leq G$  — деяка підгрупа в  $G$ . Оскільки  $H$  є підгрупою меншого порядку, то  $H$  є добутком циклічних  $p$ -груп, отже,  $G$  також.  $\square$