Matematyczne Metody Fizyki II

Mariusz Przybycień

Wydział Fizyki i Informatyki Stosowanej
Akademia Górniczo-Hutnicza

Wykład 13

Pojęcie grupy

Definicja: **Grupą** nazywamy zbiór G wraz z określonym iloczynem elementów tego zbioru, który każdej uporządkowanej parze $(g_1, g_2) \in G$ przyporządkowuje inny element tego zbioru, oznaczany przez $g_1 g_2 \in G$, przy czym spełnione są następujące warunki:

a) iloczyn jest łączny, tzn. $(g_1 g_2) g_3 = g_1 (g_2 g_3)$ dla dowolnych $g_1, g_2, g_3 \in G$,

b) istnieje element jednostkowy $e \in G$ taki, że $eg = ge = g$ dla każdego $g \in G$,

c) dla każdego $g \in G$ istnieje element odwrotny $g^{-1} \in G$: $\quad g^{-1} g = g g^{-1} = e$.

Uwaga: W warunkach (b) i (c) druga równość wynika z pierwszej:

$$g^{-1}(gg^{-1}) \overset{(a)}{=} (g^{-1}g)g^{-1} \overset{(c)}{=} eg^{-1} \overset{(b)}{=} g^{-1} \in G \quad \Rightarrow \quad \exists g_1 \in G:\ g_1 g^{-1} = e \quad (*)$$

$$\left.\begin{aligned} g_1(g^{-1}(gg^{-1})) &\overset{(a)}{=} (g_1 g^{-1})(gg^{-1}) \overset{(*)}{=} e(gg^{-1}) \overset{(b)}{=} gg^{-1} \\ &= g_1 g^{-1} \overset{(*)}{=} e \end{aligned}\right\} \quad \Rightarrow \quad gg^{-1} = e \qquad (\mathrm{c}')$$

$$ge \overset{(c)}{=} g(g^{-1}g) \overset{(a)}{=} (gg^{-1})g \overset{(c')}{=} eg \overset{(b)}{=} g$$

Lemat: Dla każdego elementu grupy $g \in G$ zachodzi $(g^{-1})^{-1} = g$

D: $\quad g = ge = g(g^{-1}(g^{-1})^{-1}) = (gg^{-1})(g^{-1})^{-1} = e(g^{-1})^{-1} = (g^{-1})^{-1}$

Definicja: Grupę która zawiera skończoną liczbę elementów nazywamy grupą skończoną. W przeciwnym razie grupę nazywamy nieskończoną. Rzędem grupy (skończonej) nazywamy liczbę n jej elementów.

Własności grup

Lemat: Elementy neutralny i odwrotny są wyznaczone jednoznacznie.

D: Niech e oraz e' będą elementami neutralnymi, wówczas:

$$\left.\begin{array}{l} e'g = ge' = g \quad \Rightarrow \quad e'e = e \\ eg = ge = g \quad \Rightarrow \quad ee' = e' \end{array}\right\} \quad \Rightarrow \quad e = e'$$

Niech g_1 i g_2 będą elementami odwrotnymi elementu g, wówczas:

$$g_1(gg_2) = (g_1g)g_2 \quad \Rightarrow \quad g_1e = eg_2 \quad \Rightarrow \quad g_1 = g_2$$

Z jednoznaczności elementu odwrotnego wynika, że

$$(g_1g_2\cdots g_n)(g_n^{-1}\cdots g_2^{-1}g_1^{-1}) = (g_1g_2\cdots g_{n-1})(g_ng_n^{-1})(g_{n-1}^{-1}\cdots g_2^{-1}g_1^{-1}) = e$$

co oznacza, że: $\quad (g_1g_2\cdots g_n)^{-1} = g_n^{-1}\cdots g_2^{-1}g_1^{-1}$

Lemat: Jeśli G jest grupą rzędu n o elementach $\{e, g_2, g_3, ..., g_n\}$ to dla dowolnego i w ciągu $eg_i, g_2g_i, g_3g_i, ..., g_ng_i$, każdy element grupy G pojawia się tylko raz (analogicznie dla $g_ie, g_ig_2, ..., g_ig_n$).

D: Niech $g_k \neq g_l$ oraz $g_kg_i = g_lg_i \quad \Rightarrow \quad (g_kg_i)g_i^{-1} = (g_lg_i)g_i^{-1} \quad \Rightarrow \quad \underbrace{g_k = g_l}_{\text{sprzeczność}}$

Wniosek: W tabelach mnożenia grupowego w każdym rzędzie i w każdej kolumnie dany element może wystąpić tylko jeden raz.

Wniosek: Dla dowolnych elementów $g_1, g_2 \in G$ istnieją jednoznaczne elementy $h_1, h_2 \in G$ takie, że $g_1h_1 = g_2$ oraz $h_2g_1 = g_2$.

Przykłady grup

- Najprostsza grupa składa się z jednego elementu (C_1): elementu neutralnego e ($ee = e$; $e^{-1} = e$). Np. "1" i zwykłe mnożenie.
- Grupa złożona z dwóch elementów $C_2 = \{e, a\}$: ($ee = e$, $aa = e$, $ea = ae = a$). Np. grupa złożona z liczb $+1\,(e)$ i $-1\,(a)$ i zwykłego mnożenia.
- Zbiór liczb całkowitych wraz ze zwykłym dodawaniem $(\mathbb{Z}, +)$: $e = 0,\ g = n \ \Rightarrow\ g^{-1} = -n$.
- $(\mathbb{R}^+, \cdot)$ oraz $(\mathbb{Q}^+, \cdot):\ \ e = 1,\ \ g = x \ \Rightarrow\ g^{-1} = 1/x$.
- Zbiór $\{-1, +1, -i, +i\}$ wraz z operacją mnożenia.
- $(\mathbb{C}, +)$ oraz $(\mathbb{C} - \{0\}, \cdot)$.
- Zbiór wszystkich wektorów w przestrzeni wektorowej $\mathcal{V}$ ze względu na ich dodawanie.
- Zbiory złożone ze wszystkich transfromacji fizycznych danego typu, np.:
  - (obroty i odbicia) zbiór transformacji zachowujących odległość od początku układu w przestrzeni n-wymiarowej,
  - (translacje) zbiór wszystkich transformacji zachowujących różnicę $\vec{x} - \vec{y}$ pomiędzy współrzędnymi dwóch punktów w przestrzeni n-wymiarowej,
  - (grupa Lorentza) zbiór transformacji liniowych zachowujących kwadrat długości 4-wektora, $x_0^2 - x_1^2 - x_2^2 - x_3^2$, w przestrzeni Minkowskiego,
  - (grupa Poincarego) zbiór wszystkich transformacji liniowych zachowujących odległość pomiędzy dwoma 4-wektorami w przestrzeni Minkowskiego (tr. Lorentza + translacje).

Grupa cykliczna

Definicja: Grupa cykliczna rzędu n to grupa której elementy można zapisać w postaci $C_n = \{e, a, a^2, ..., a^{n-1}\}$.

Przykład: Modelem grupy cyklicznej rzędu n jest zbiór n pierwiastków n-tego stopnia z 1 wraz z operacją iloczynu liczb zespolonych $(z_k = \exp(i\, 2\pi k/n),\ k = 0, ..., n-1)$

Uwaga: Wszystkie grupy 1-, 2- lub 3-elementowe są wyłącznie cykliczne.

Definicja: Najmniejszą całkowitą liczbę dla której zachodzi $g^n = e$ nazywamy rzędem elementu g. Gdy n jest nieskończone wówczas element g jest rzędu nieskończonego.

Lemat: Jeśli g jest elementem rzędu n w grupie cyklicznej rzędu n, wówczas wszystkie elementy grupy $e = g^0, g^1, ..., g^{n-1}$ są różne.

D: Niech $g^i = g^j$ dla $0 \leqslant i < j \leqslant n-1 \quad \Rightarrow \quad g^i (g^i)^{-1} = g^j (g^i)^{-1}$

tzn. że $e = g^{j-i}$ dla $0 < j - i < n$ co jest sprzeczne z założeniem, że n jest najmniejszą liczbą całkowitą dla której zachodzi $g^n = e$.

Definicja: Grupę G nazywamy abelową (przemienną) jeśli dla dowolnych $g_1, g_2 \in G$ zachodzi $g_1 g_2 = g_2 g_1$.

Przykład: Grupa trójelementowa $C_2 = \{e, a, b\}$ (eliminacja sprzecznych relacji):

$$\left.\begin{array}{lll} ab = a & \Rightarrow & b = e \\ ab = b & \Rightarrow & a = e \end{array}\right\} \text{ a więc } ab = e \ \text{ (podobnie } ba = e)$$

$$\left.\begin{array}{lll} aa = a & \Rightarrow & a = e \\ aa = e & \Rightarrow & a = b \end{array}\right\} \text{ a więc } aa = b \ \text{ (podobnie } bb = a)$$

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Przykłady grup

Przykład: Grupa czteroelementowa $G = \{e, a, b, c\}$:

$$a^2 = a \quad \Rightarrow \quad a = e$$

$$a^2 = b \quad \Rightarrow \quad \begin{cases} \left.\begin{array}{l} ac = e \\ ac = b = a^2 \quad \Rightarrow \quad a = c \end{array}\right\} \text{ a więc } ac = e \text{ (podobnie } ca = e) \\ ab = e \quad \Rightarrow \quad a^3 = ac \quad \Rightarrow \quad a^2 = c \\ ab = a \quad \Rightarrow \quad a^2 = e \\ ab = b \quad \Rightarrow \quad a = e \\ \text{a więc } ab = c \ \ \text{(podobnie } ba = c) \end{cases}$$

$$a^2 = c \quad \Rightarrow \quad \text{jak wyżej, tylko tym razem } ac = a^3 = b$$

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

W obu przypadkach otrzymujemy grupę cykliczną $C_4 = \{e, a, a^2, a^3\}$.

Inne możliwości:

$$a^2 = e \quad \Rightarrow \quad \begin{cases} \left.\begin{array}{l} ab = c \\ ab = e \quad \Rightarrow \quad b = a \end{array}\right\} \text{ a więc } ab = c \quad \text{(podobnie } ba = c) \\ ac = e \qquad \Rightarrow \quad a^2 c = a \quad \Rightarrow \quad c = a \\ ac = a \qquad \Rightarrow \quad c = e \\ ac = c \qquad \Rightarrow \quad a = e \\ \text{a więc } ac = b \quad \text{(podobnie } ca = b) \\ (ba) \cdot (ab) = c^2 \quad \Rightarrow \quad b^2 = c^2 \ \text{ a więc } \ c^2 = a \text{ lub } c^2 = e \\ \text{niech } c^2 = a \quad \Rightarrow \quad ac^2 = a^2 = e \quad \overset{ac=b}{\Rightarrow} \quad bc = e \ \ (cb = e) \\ \text{niech } c^2 = e \quad \Rightarrow \quad ac^2 = a \quad \overset{ac=b}{\Rightarrow} \quad bc = a \ \ (cb = a) \end{cases}$$

Przykłady grup

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

$\Leftarrow \quad c^2 = a$, grupa izomorficzna z C_4

$b^4 = e \rightarrow e'$
$b^2 = a \rightarrow b'$
$b \rightarrow a'$
$b^3 = c \rightarrow c'$

$c^2 = e \quad \Rightarrow$
ta grupa nie jest izomorficzna z C_4 (tzw. czterogrupa)

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

- Zbiór wszystkich odwracalnych macierzy $n \times n$ względem operacji mnożenia macierzy:

$$GL(n) = \{A_{n\times n} : a_{ij} \in \mathbb{C},\ \det(A) \neq 0\}$$

$$A^{-1} = \frac{C_A^T}{\det(A)} \qquad (C_A)_{ij} = (-1)^{i+j} M_{ij} \qquad \det(AB) = \det(A)\det(B)$$

- (grupy ortogonalne) Zbiór wszystkich macierzy rzeczywistych $n \times n$ zachowujących formę $x_1^2 + x_2^2 + ... + x_n^2$ - grupa $O(n)$.
  Jeśli dodatkowo wyznacznik jest równy 1 - grupa $SO(n)$.
  $SO(3)$ to grupa obrotów.
- (grupy unitarne) Zbiór wszystkich macierzy zespolonych $n \times n$, które zachowują formę kwadratową $x_1^\star x_1 + x_2^\star x_2 + ... + n_n^\star x_n$ - grupa $U(n)$.
  Jeśli dodatkowo wyznacznik jest równy 1 - grupa $SU(n)$.
- $SU(3)$ to grupa symetrii oddziaływań silnych (Quantum Chromodynamics, QCD) - więcej na ten temat na przedmiocie obieralnym Wstęp do oddziaływań hadronów.

Grupa symetryczna

Definicja: Grupą symetryczną (grupą permutacji) nazywamy grupę utworzoną przez zbiór odwracalnych odwzorowań $f\colon S_n \to S_n$, gdzie S_n jest zbiorem złożonym z $n!$ elementów.

$$p = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ p_1 & p_2 & p_3 & \dots & p_n \end{pmatrix}, \qquad e = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}, \qquad p^{-1} = \begin{pmatrix} p_1 & p_2 & p_3 & \dots & p_n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}$$

Przykład: Składanie permutacji: $\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$

$$\pi_2 \circ \pi_1(i) \equiv \pi_2(\pi_1(i)) \qquad \pi_2 \circ \pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \qquad \pi_1 \circ \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

Przykład: Grupa S_3:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\pi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad \pi_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

e	π_2	π_3	π_4	π_5	π_6
π_2	e	π_5	π_6	π_3	π_4
π_3	π_6	e	π_5	π_4	π_2
π_4	π_5	π_6	e	π_2	π_3
π_5	π_4	π_2	π_3	π_6	e
π_6	π_3	π_4	π_2	e	π_5

Definicja: Niech $\pi \in S_n,\ i \in \{1, 2, ..., n\}$ oraz niech r będzie najmniejszą liczbą naturalną taką, że $\pi^r(i) = i$. Cyklem permutacji π o długości r generowanym przez i nazywamy zbiór r różnych elementów $\{\pi^k(i)\},\ k = 0, ..., r-1$.

Lemat: Każda permutacja może być jednoznacznie rozłożona na rozłączne cykle.

Grupa symetryczna - cykle

Przykład: Rozkład na cykle permutacji π_1, $\pi_2 \in S_8$:

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 7 & 1 & 2 & 8 & 4 & 6 \end{pmatrix} = (1374)(25)(68)$$

$$\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 6 & 8 & 1 & 7 & 4 & 3 \end{pmatrix} = (125)(36748)$$

$$\pi_1 \circ \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 8 & 6 & 3 & 4 & 1 & 7 \end{pmatrix} = (1374)(25)(68)$$

Definicja: Jeśli $\pi \in S_n$ ma cykl o długości r, a wszystkie pozostałe cykle π mają tylko po jednym elemencie, to π nazywamy permutacją cykliczną o długości r.

Definicja: Permutację cykliczną o długości 2 nazywamy transpozycją.

Przykład: Znajdowanie permutacji danej w postaci cykli (niekoniecznie rozłącznych)

$$\pi_1 \in S_6 \qquad \pi_1 = (143)(24)(456) \qquad \pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 5 & 6 & 2 \end{pmatrix} = (145623)$$

$$\pi_2 \in S_5 \qquad \pi_2 = (13)(15)(12)(14) \qquad \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix} = (14253)$$

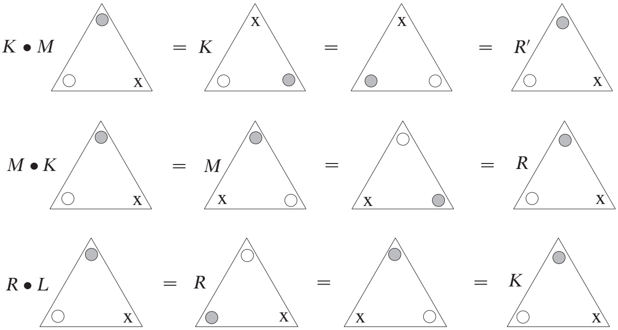
Lemat: Dowolny r-cykl $(i_1, i_2, ..., i_r)$ może być rozłożony na iloczyn $r-1$ transpozycji: $(i_1, i_2, ..., i_r) = (i_1, i_r)(i_1, i_{r-1})...(i_1, i_3)(i_1, i_2)$.

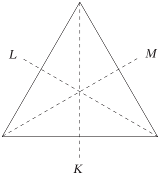
Definicja: Permutację nazywamy parzystą (nieparzystą) jeśli może być przedstawiona jako iloczyn parzystej (nieparzystej) liczby transpozycji.

Przykład: Rozważmy grupę utworzoną przez operacje symetrii (obroty i odbicia) które przeprowadzają w płaszczyźnie trójkąt równoboczny w siebie. Grupa ta jest określana jako $3m$ lub C_{3v}.

Operacje symetrii:

e - operacja zerowa; R, R' - obroty o $2\pi/3$ i $4\pi/3$; K, L, M - odbicia.





e	L	M	K	R'	R
L	e	R'	R	M	K
M	R	e	R'	K	L
K	R'	R	e	L	M
R'	K	L	M	R	e
R	M	K	L	e	R'

$$R \leftrightarrow \pi_6, \quad R' \leftrightarrow \pi_5, \quad K \leftrightarrow \pi_4, \quad L \leftrightarrow \pi_2, \quad M \leftrightarrow \pi_3$$

Izomorfizm i homomorfizm grup

Definicja: Mówimy, że dwie grupy G i G' są izomorficzne jeśli istnieje bijekcja pomiędzy ich elementami, która zachowuje działanie grupowe, tzn. jeśli $g_i \in G \leftrightarrow g'_i \in G'$ oraz jeśli $g_1 g_2 = g_3$ w G, to $g'_1 g'_2 = g'_3$ w G' i na odwrót.

Definicja: Odwzorowanie $f : G \to G'$ nazywamy homomorfizmem, jeśli każdej parze elementów $g_1, g_2 \in G$ przyporządkowany zostaje element grupy G', przy czym zachodzi $f(g_1 g_2) = f(g_1) f(g_2)$,

Własności homomorfizmu:

- $eg = g \quad \Rightarrow \quad g' = (eg)' = e'g' \quad \Rightarrow \quad f(e) = e'$
- $e' = (gg^{-1})' = g'(g^{-1})' \quad \Rightarrow \quad (g')^{-1} = (g^{-1})'$
- $e = g^m \quad \Rightarrow \quad e' = (g^m)' = (gg...g)' = g'g'...g' = (g')^m$

Własności izomorfizmu:

- $g'_1 = g'_2 \quad \Rightarrow \quad g_1 = g_2$ ("1:1" - monomorfizm)
  (grupy izomorficzne mają tą samą liczbę elementów danego rzędu).
- każdy element G' jest obrazem jakiegoś elementu G („na" - epimorfizm).

Definicja: Jądrem homomorfizmu $f : G \to G'$ nazywamy zbiór:

$$Ker(f) = \{g \in G \,|\, f(g) = e'\}$$

Przykład: Odwzorowanie $f : x \to e^{ix}$ grupy $(\mathbb{R}, +)$ na grupę $U(1)$ liczb zespolonych o jednostkowym module jest homomorfizmem, ponieważ:

$$(x+y)' \to e^{i(x+y)} = e^{ix} e^{iy} = x'y'$$

ale nie jest izomorfizmem, ponieważ np. $f((2k+1)\pi) = -1$, $f(2k\pi) = +1$, itp.

Podgrupy

Definicja: Podgrupą grupy G nazywamy niepusty podzbiór H zbioru G, który tworzy grupę z tym samym działaniem co G.

Uwaga: Każda grupa zawiera dwie podgrupy trywialne

$$H = G \quad \text{oraz} \quad H = \{e\}$$

Wszystkie inne podgrupy nazywamy właściwymi.

Przykład: Grupy cykliczne nie mają podgrup właściwych.

Przykład: Element rzędu m ($g^m = e$) poprzez mnożenie przez siebie utworzy podgrupę $\{e, g, g^2, ..., g^{m-1}\}$ rzędu m. Jest to podgrupa abelowa.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Własności podgrup:

- Element jednostkowy e grupy G należy do każdej jej podgrupy H.
- Jeśli element $g \in H$, to również $g^{-1} \in H$.
- Zbiór elementów $g \in G$, które należą do wszystkich podgrup również tworzy podgrupę (może to być tylko $\{e\}$).

Twierdzenie: Niech będzie dany homomorfizm $f\colon G \to G'$.

(a) Zbiór $H' \subset G'$ obrazów elementów grupy G tworzy pogrupę w G'.

(b) Zbiór $K \subset G$ elementów które są odwzorowane w $e' \in G'$, tworzy podgrupę w G.

D: (a) $e' \in H'; \quad g'_1, g'_2 \in H' \quad \Rightarrow \quad g'_1 g'_2 = (g_1 g_2)' \in H'; \; (g')^{-1} = (g^{-1})' \in H'$

(b) $e \in K; \quad g_1, g_2 \in K \quad \Rightarrow \quad (g_1 g_2)' = g'_1 g'_2 = e'e' = e' \quad \Rightarrow \quad g_1 g_2 \in K$

$$g \in K \quad \Rightarrow \quad e' = (gg^{-1})' = g'(g^{-1})' = e'(g^{-1})' = (g^{-1})' \quad \Rightarrow \quad g^{-1} \in K$$

Podgrupy

Przykład: $f\colon \mathbb{R} \to U(1) \quad \Rightarrow \quad Ker(f) = \{2k\pi, k \in \mathbb{Z}\}$ - podgrupa w $\mathbb{R}$

Definicja: Podgrupę H grupy G nazywamy normalną, jeśli dla każdego $g \in G$ i każdego $h \in H$, również $ghg^{-1} \in H$.

Przykład: Jądro homomorfizmu, $Ker(f)$, jest podgrupą normalną:

$$g \in G,\ h \in Ker(f) \quad \Rightarrow \quad (ghg^{-1})' = g'h'(g^{-1})' = g'e'(g^{-1})' = g'(g^{-1})' = e'$$