

GRUPY – STRUKTURY I KONSTRUKCJE ELEMENTARNE
(TG '24/25 1.I, 1.II, 1.III & 1.IV [RRS])

SPIS TREŚCI

1. Struktura grupy i jej transport	1
2. Warstwy i grupy ilorazowe	13
3. Ciągi dokładne i rozszerzenia grup	17
4. Iloczyn półprosty grup w algebrze i geometrii	21
Literatura	27
Zadania domowe i na ćwiczenia	28

Grupy to proste struktury algebraiczne o niezwykle szerokim spektrum zastosowań w modelowaniu matematycznym rzeczywistości. Ich struktura i aksjomatyka w możliwie zwięzły sposób formalizuje intuicyjne pojęcie symetrii obiektów geometrycznych i teorii fizycznych, ale też objawia się w studium ewolucji układów dynamicznych. Fundamentalne znaczenie grup w rygorystycznym opisie przyrody – począwszy od krytalografii, poprzez teorię grawitacji i (inne) teorie pola z cechowaniem, a skończywszy na kwantowej teorii pola, teorii strun oraz grawitacji kwantowej, by wymienić te najbardziej oczywiste konteksty fizykalne – pozostaje zatem poza wszelką wątpliwością. Aksjomatyka grup dopuszcza też nader ciekawe uogólnienia, które odnajdujemy w bardziej egzotycznych zakamarkach fizyki matematycznej, a wśród nich: grupy i algebry pętlowe (oraz ich centralne rozszerzenia) obecne w analizie prądowych realizacji symetrii w klasycznej i kwantowej teorii pola w dwóch wymiarach, supergrupy (Liego) istotne w modelowaniu tzw. supersymetrii, czy wreszcie grupy kwantowe opisujące symetrie kwantowej teorii pola z ładunkiem topologicznym w dwóch wymiarach (np. w tzw. modelach Wessa–Zumino–Wittena konformnej teorii pola o przestrzeni zanurzenia danej przez zwartą grupę Liego) i wpisujące się w szerszy kadr geometrii nieprzemiennej (np. w rozumieniu Connesa).

1. STRUKTURA GRUPY I JEJ TRANSPORT

Zacniemy od najbardziej elementarnej

Definicja 1. **Magma** to para (S, ϕ_2) złożona ze zbioru S oraz operacji 2-argumentowej $\phi_2 : S \times S \rightarrow S$.

Przykłady 1. Para $(\mathbb{N} \setminus \{0\} =: \mathbb{N}_{>0}, \wedge)$ złożona ze zbioru $\mathbb{N}_{>0}$ dodatnich liczb całkowitych i operacji 2-argumentowej (nieprzemiennej i niełącznej)

$$\wedge : \mathbb{N}_{>0}^2 \rightarrow \mathbb{N}_{>0} : (m, n) \mapsto m^n.$$

a dalej wprowadzimy

Definicja 2. **Półgrupa** to magma (S, ϕ_2) , w której operacja ϕ_2 jest łączna, co wyraża diagram przemienności

$$\begin{array}{ccc} S \times S \times S & \xrightarrow{\phi_2 \times \text{id}_S} & S \times S \\ \text{id}_S \times \phi_2 \downarrow & & \downarrow \phi_2 \\ S \times S & \xrightarrow{\phi_2} & S \end{array} .$$

Przykłady 2. Para (\mathfrak{T}, Γ) złożona z

- zbioru \mathfrak{T} **osadzonych drzew binarych**, tj. niezorientowanych grafów acyklicznych i spójnych (czyli takich, których krawędzie są odcinkami bez wyróżnionej orientacji, tj. bez wyróżnionego porządku na zbiorze końców, i w których od każdego wierzchołka do każdego innego wierzchołka można dotrzeć wzdłuż grafu dokładnie jedną ścieżką), o wierzchołkach, z których każdy leży na końcu nie więcej niż trzech krawędzi (czyli ma **walencję** $w \leq 3$), i z wyróżnionym wierzchołkiem – zwanym **korzeniem** – o walencji 1, a także z wyróżnionym uporządkowaniem (tj. przypisaniem cech „prawy/lewy”) dwójki krawędzi wychodzących z każdego z wierzchołków o walencji 3 przy przemierzaniu grafu w kierunku od korzenia do tegoż wierzchołka;
- łącznej (i nieprzemiennej) operacji 2-argumentowej Γ , zwanej **szczepieniem**, która polega na przyłączeniu korzenia drugiego argumentu do wyróżnionego wierzchołka pierwszego argumentu, który leży na końcu ścieżki prowadzącej od korzenia i skracającej w prawo w każdym wierzchołku łączącym ze sobą trzy krawędzie.

Za powyższymi kroczy zasadnicza

Definicja 3. Grupa to czwórka $(G, \phi_2, \phi_1, \phi_0)$, w której

- G jest zbiorem;
- $\phi_2 : G \times G \rightarrow G$ jest operacją 2-argumentową zwaną **działaniem grupowym**;
- $\phi_1 : G \circlearrowleft$ jest operacją 1-argumentową;
- $\phi_0 : \{\bullet\} \rightarrow G : \bullet \mapsto e$ jest operacją 0-argumentową.

Elementy struktury spełniają następujące aksjomaty (wyrażone przez diagramy przemienne i równoważne zdania logiczne):

(G1) (łączność działania grupowego)

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{\phi_2 \times \text{id}_G} & G \times G \\ \text{id}_G \times \phi_2 \downarrow & & \downarrow \phi_2 \\ G \times G & \xrightarrow{\phi_2} & G \end{array} \equiv \forall_{g,h,k \in G} : \phi_2(\phi_2(g,h),k) = \phi_2(g,\phi_2(h,k));$$

(G2) (istnienie elementu neutralnego względem działania grupowego)

$$\begin{array}{ccc} G \times \{\bullet\} & \xrightarrow{\text{id}_G \times \phi_0} & G \times G \\ & \searrow \text{pr}_1 & \downarrow \phi_2 \\ & & G \end{array}, \quad \begin{array}{ccc} \{\bullet\} \times G & \xrightarrow{\phi_0 \times \text{id}_G} & G \times G \\ & \searrow \text{pr}_2 & \downarrow \phi_2 \\ & & G \end{array}$$

$$\equiv \forall_{g \in G} : \phi_2(g, e) = g = \phi_2(e, g);$$

(G3) (fundamentalna własność ϕ_1)

$$\begin{array}{ccc} G \times \{\bullet\} & \xrightarrow{(\text{id}_G, \phi_1) \circ \text{pr}_1} & G \times G \\ & \searrow \phi_0 \circ \text{pr}_2 & \downarrow \phi_2 \\ & & G \end{array}, \quad \begin{array}{ccc} G \times \{\bullet\} & \xrightarrow{(\phi_1, \text{id}_G) \circ \text{pr}_1} & G \times G \\ & \searrow \phi_0 \circ \text{pr}_2 & \downarrow \phi_2 \\ & & G \end{array}$$

$$\equiv \forall_{g \in G} : \phi_2(g, \phi_1(g)) = e = \phi_2(\phi_1(g), g).$$

Grupa przeciwna do $(G, \phi_2, \phi_1, \phi_0)$ to grupa $(G, \phi_2^{\text{opp}}, \phi_1, \phi_0)$ z działaniem danym wzorem

$$\phi_2^{\text{opp}} := \phi_2 \circ \tau_G,$$

gdzie

$$\tau_G : G \times G \circlearrowleft : (g_1, g_2) \mapsto (g_2, g_1)$$

jest standardową transpozycją składowych pary.

Grupa przemienna (zwana też **abelową**) to taka, w której działanie grupowe jest przemienne, co wyraża diagram przemienny (wypisany wraz z równoważnym zdaniem logicznym)

$$\begin{array}{ccc} G \times G & \xrightarrow{\tau_G} & G \times G \\ & \searrow \phi_2 & \downarrow \phi_2 \\ & & G \end{array} \equiv \forall_{g,h \in G} : \phi_2(g,h) = \phi_2(h,g),$$

a zatem taka, która jest kanonicznie izomorficzna z grupą do niej przeciwną,

$$(G, \phi_2, \phi_1, \phi_0) \stackrel{\text{id}_G}{\cong} (G, \phi_2^{\text{opp}}, \phi_1, \phi_0).$$

Przykłady 3.

- (1) **Grupa trywialna:** $(\{e\}, (e, e) \mapsto e, e \mapsto e, \{\bullet\} \mapsto e)$.
- (2) Grupa liczb zespolonych o module jednostkowym: $(U(1), \cdot_{\mathbb{C}}, \bar{\cdot}, \bullet \mapsto (1, 0))$.
- (3) Przykłady arytmetyczne (w których opuszczamy oczywiste elementy struktury):
 $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +_{\mathbb{C}}), (\mathbb{Q}^{\times}, \cdot), (\mathbb{R}^{\times}, \cdot), (\mathbb{C}^{\times}, \cdot_{\mathbb{C}}), (\mathbb{Q}_{>0}, \cdot), (\mathbb{R}_{>0}, \cdot)$.
- (4) Grupa

$$\left(\text{GL}(2, \mathbb{C}), \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right) \mapsto \begin{pmatrix} a \cdot e + b \cdot g & a \cdot f + b \cdot h \\ c \cdot e + d \cdot g & c \cdot f + d \cdot h \end{pmatrix}, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \frac{1}{a \cdot d - b \cdot c} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}, \bullet \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right)$$

odwracalnych macierzy wymiaru 2×2 o wyrazach zespolonych, zwana **pełną grupą liniową stopnia 2 nad \mathbb{C}** .

- (5) Dla dowolnej grupy przemiennej $(G, \phi_2, \phi_1, \phi_0)$ i dowolnego zbioru niepustego S określamy grupę przemienną $(\mathbf{Map}(S, G), \tilde{\phi}_2, \tilde{\phi}_1, \tilde{\phi}_0)$, której nośnikiem jest zbiór odwzorowań z S w G z działaniem 2-argumentowym $\tilde{\phi}_2$ indukowanym przez ϕ_2 wedle formuły:

$$\tilde{\phi}_2(f_1, f_2) : S \longrightarrow G : s \mapsto \phi_2(f_1(s), f_2(s)),$$

zapisanej dla dowolnych $f_1, f_2 \in \mathbf{Map}(S, G)$, z działaniem 1-argumentowym $\tilde{\phi}_1$ indukowanym przez ϕ_1 wedle formuły:

$$\tilde{\phi}_1(f) : S \longrightarrow G : s \mapsto \phi_1(f(s)),$$

zapisanej dla dowolnego $f \in \mathbf{Map}(S, G)$, oraz z działaniem 0-argumentowym $\tilde{\phi}_0$ indukowanym przez ϕ_0 wedle formuły:

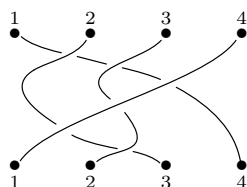
$$\tilde{\phi}_0(\bullet) : S \longrightarrow G : s \mapsto \phi_0(\bullet).$$

- (6) Interesującym uogólnieniem konstrukcji grupy symetrycznej, znajdującym zastosowanie w mechanice płynów (w kontekście teorii mieszania chaotycznego), topologicznej kwantowej teorii pola, topologicznej teorii informacji kwantowej (zajmującej się, m.in., rozwijaniem koncepcji topologicznego komputera kwantowego) i niskowymiarowej topologii, jest grupa warkoczy. Wykorzystując jej prostą geometryczną realizację, podamy poniżej jej definicję opisową, która pozwala uniknąć przeciążenia pojęciowego. Czytelnik zainteresowany rygorystycznym opisem grupy warkoczy i jej zastosowaniami w nowoczesnej fizyce i matematyce może sięgnąć do opracowań specjalistycznych takich jak, np., [Tur94, PS97, KT08].

Rozważmy dwa n -elementowe zbiory, Σ_+ i Σ_- , punktów współliniowych leżących na dowolnej płaszczyźnie $\Pi \subset \mathbb{R}^3$, zakładając przy tym, że proste Λ_+ i Λ_- wyznaczone przez zbiory Σ_+ i Σ_- , odpowiednio, są do siebie równoległe. Punktom ze zbioru Σ_{\pm} przypiszemy indeksy naturalne od 1 do n , w kolejności ich ułożenia na prostej Λ_{\pm} , przy czym kierunek wzrostu indeksu przyjmujemy wspólny dla obu prostych. **Warkocz o n pasmach** to układ w utworzony przez n nieprzecinających się ścieżek (czyli odcinków krzywych) łączących punkty zbioru Σ_+ z punktami zbioru Σ_- w taki sposób, że każdy punkt zbioru Σ_+ jest połączony z dokładnie jednym punktem zbioru Σ_- (tj. warkocz zadaje permutację zbioru $1, n$, która liczbie $k \in 1, n$ indeksującej punkt na prostej Λ_+ , z której wychodzi ścieżka, przyporządkowuje liczbę będącą indeksem punktu na prostej Λ_- , w którym ścieżka ta się

kończy¹), a ponadto na ścieżkach nie występują pętle i przecięcie każdej prostej $\Lambda \subset \Pi$ równoległej do Λ_+ ze zbiorem ścieżek jest albo puste (gdy Λ biegnie na zewnątrz obszaru (paska) Ξ rozdzialającego Λ_+ i Λ_-), albo zawiera dokładnie n punktów (gdy $\Lambda \subset \Xi$). Umawiamy się przy tym, że będziemy utożsamiać układy ścieżek, które można nałożyć na siebie poprzez *ciągłą* deformację ścieżek w \mathbb{R}^3 zachowującą punkty ich zaczepienia. Taką deformację określimy mianem **izotopii warkocza**. Zbiór wszystkich klas $[w]$ izotopii warkoczy w o n pasmach będziemy oznaczać symbolem \mathfrak{B}_n .

Warkocze przedstawiamy w postaci **diagramów warkoczowych** stanowiących rzut warkocza na płaszczyznę Π , na którym zaznaczamy sposób krzyżowania się ścieżek (ścieżka biegnąca z lewa na prawo może przechodzić powyżej lub poniżej ścieżek na prawo od niej). Przykładem diagramu warkoczowego (dla warkocza o 4 pasmach) jest



Odpowiada mu permutacja $(14)(23)$. Nie jest natomiast diagramem warkoczowym (żaden diagram zawierający jako poddiagram)



Jak jasno wynika z opisu ogólnego i powyższej ilustracji, różnica między warkoczami a indukowanymi przez nie permutacjami z \mathfrak{S}_n polega na tym, że w w procesie indukcji tracona jest informacja o tym, czy ścieżka wychodząca z punktu odpowiadającego elementowi nośnika permutacji opisywanej przez dany układ ścieżek biegnie powyżej czy poniżej ścieżek pozostałych na swej drodze ku obrazowi tegoż punktu względem rzeczony permutacji. Różnica ta, z pozoru drobna, ma kolosalne konsekwencje dla struktury grupy zbudowanej na bazie warkoczy, którą opiszemy w następnej kolejności.

Grupa (Artina) warkoczy o n pasmach to czwórka

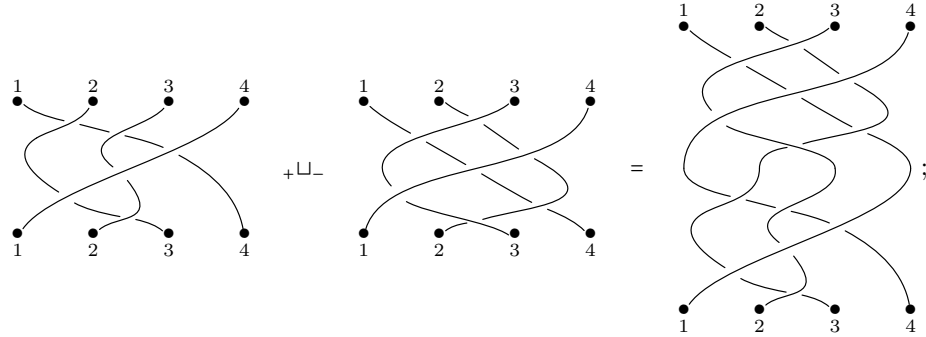
$$(\mathfrak{B}_n, *, \text{Inv}, \bullet \mapsto \mathbf{1})$$

złożona z następujących elementów:

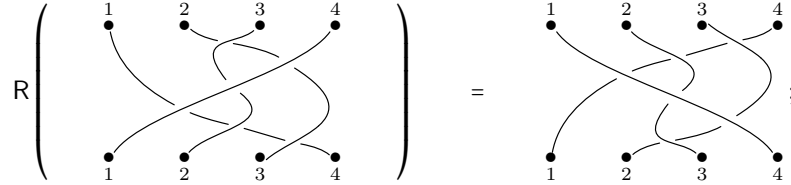
- \mathfrak{B}_n to wprowadzony wcześniej zbiór klas izotopii warkoczy o n pasmach;
- operacja 2-argumentowa $*$: $\mathfrak{B}_n^{\times 2} \rightarrow \mathfrak{B}_n$: $([w_2], [w_1]) \mapsto [w_2 \updownarrow w_1]$ przyporządkowuje klasom izotopii warkoczy w_2 i w_1 (traktowanych jako podzbiory w *niezależnych* kopiach \mathbb{R}^3) klasę izotopii warkocza $w_2 \updownarrow w_1$ otrzymanego przez utożsamienie, zaznaczone symbolem \updownarrow , prostej Λ_- warkocza w_1 z prostą Λ_+ warkocza w_2 w taki sposób, że punkty o tych samych indeksach przechodzą na siebie,

¹Przyjmujemy konwencję naturalistyczną, wedle której „włosy rosną w dół”.

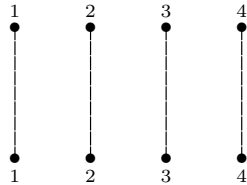
np.



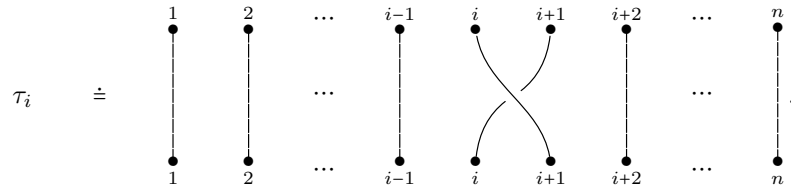
- operacja 1-argumentowa $\text{Inv} : \mathfrak{B}_n \hookrightarrow [\mathfrak{B}_n]$ przyporządkowuje klasie izotopii warkocza w klasę izotopii warkocza $\text{R}(w)$ otrzymanego przez odbicie w w prostej $\Lambda_0 \subset \Pi$ równoległej do Λ_+ i leżącej w połowie odległości między Λ_+ i Λ_- , np.



- element neutralny $\mathbf{1}$ względem \star będący klasą izotopii warkocza trywialnego złożonego z n odcinków (prostych) wzajem równoległych, z których k -ty biegnie od punktu o indeksie k na prostej Λ_+ do punktu o tym samym indeksie na prostej Λ_- , np.



Grupę warkoczy można także zdefiniować w nieco bardziej abstrakcyjny, tj. czysto algebraiczny sposób, a mianowicie przez wypisanie pełnego układu relacji² spełnianych przez zbiór generatorów grupy. Wychodząc od powyższej reprezentacji geometrycznej, jako generatory wybieramy klasy izotopii warkoczy o pasmach wychodzących z punktów o indeksach $i \in \overline{1, n-1}$ oraz $i+1$ jednokrotnie skrzyżowanych ze sobą w taki sposób, że pasmo wychodzące z punktu o indeksie niższym przechodzi na odnośnym diagramie warkoczowym ponad pasmem o indeksie wyższym, i o pozostałych pasmach niesplecionych,



Generatory te spełniają następujące relacje, wypisane dla dowolnych indeksów $i \in \overline{1, n-2}$ oraz $j, k \in \overline{1, n-1}$,

$$[\tau_i] \star [\tau_{i+1}] \star [\tau_i] = [\tau_{i+1}] \star [\tau_i] \star [\tau_{i+1}],$$

$$|j - k| \geq 2 \implies [\tau_j] \star [\tau_k] = [\tau_k] \star [\tau_j].$$

²Zupełność układu oznacza, że dowolna relacja między generatorami jest konsekwencją relacji z układu.

Można wykazać, że dowolna grupa o n generatorach spełniających powyższe relacje jest kanonicznie izomorficzna z geometryczną grupą \mathfrak{B}_n , patrz: [KT08, Rozdz. 1].

- (7) Przykładem grupy odgrywającej istotną rolę w opisie topologii zbiorów, a więc także w geometrii, jest **grupa podstawowa** $\pi_1(X; x_*)$ **przestrzeni topologicznej** X **o bazie** $x_* \in X$ (przestrzenie topologiczne są omawiane na kursie analizy matematycznej, por., np., [Mau91, Rozdz. II] oraz [Die68, Rozdz. XII] w połączeniu z [Die65, Rozdz. II]), której konstrukcję pokrótce tu opiszemy, odsyłając zainteresowanych dalszymi szczegółami do literatury źródłowej, np., [Lee11, Rozdz. 7]. Podstawowymi obiektami są tutaj **ścieżki** w X , tj. ciągle odwzorowania³

$$\gamma : I := [0, 1] \longrightarrow X,$$

na które nakładamy dodatkowy warunek zamkniętości,

$$\gamma(0) = \gamma(1),$$

co ogranicza nasze rozważania do **pętli** w X . **Pętle o bazie** $x_* \in X$ to takie, dla których zachodzi

$$\gamma(0) = x_*.$$

Wyróżniamy pośród nich **pętle stałe** (o bazie $x_* \in X$) postaci

$$\varepsilon_{x_*} : I \longrightarrow X : t \longmapsto x_*.$$

Na zbiorze $\Omega(X; x_*)$ pętli o bazie $x_* \in X$ określamy operację \circ zwaną **mnożeniem** (lub **składaniem**) **pętli**, daną wzorem

$$\circ : \Omega(X; x_*)^{\times 2} \longrightarrow \Omega(X; x_*) : (\gamma_1, \gamma_2) \longmapsto \gamma_1 \circ \gamma_2,$$

$$\gamma_1 \circ \gamma_2(t) := \begin{cases} \gamma_1(2t) & \text{dla } t \in [0, \frac{1}{2}] \\ \gamma_2(2t - 1) & \text{dla } t \in [\frac{1}{2}, 1] \end{cases},$$

jak również operację 1-argumentową zwaną **braniem odwrotności** (lub **odwracaniem**) **pętli**

$$\bar{\cdot} : \Omega(X; x_*) \longrightarrow \Omega(X; x_*) : \gamma \longmapsto \bar{\gamma},$$

$$\bar{\gamma}(t) = \gamma(1 - t).$$

Na tym etapie konstrukcji pojawiają się dwa naturalne pytania: Czy możemy – kierując się intuicją algebraiczną – zdefiniować na $\Omega(X; x_*)$ (lub na zbiorze prosto z nim związanym) strukturę grupy indukowaną przez powyższe operacje? Czy możemy – kierując się tą samą intuicją – utożsamić w jakiś naturalny sposób pętle γ_1 i γ_2 różniące się jedynie reparametryzacją, tj. spełniające tożsamość

$$\gamma_2 = \gamma_1 \circ \varrho$$

dla pewnego odwzorowania ciągłego

$$\varrho : I \curvearrowright, \quad \varrho(0) = 0 \quad \wedge \quad \varrho(1) = 1?$$

Twierdzącej (i konstruktywnej) odpowiedzi na oba pytania dostarcza koncepcja przejścia od zbioru $\Omega(X; x_*)$ do zbioru $\Omega(X; x_*) / \sim$ klas abstrakcji względem relacji **homotopijnej równoważności** (albo inaczej **homotopijności**), przy czym pętle $\gamma_1, \gamma_2 \in \Omega(X; x_*)$ uznajemy za równoważne, gdy istnieje **homotopia** przeprowadzająca γ_1 na γ_2 , tj. odwzorowanie ciągłe

$$H : I^{\times 2} \longrightarrow X$$

³Pojęcie ciągłości jest dyskutowane na kursie analizy matematycznej, patrz, np., [Mau91, Rozdz. II § 7] i [Die65, Rozdz. II.11].

o własnościach

$$\forall_{s,t \in I} : \begin{cases} H(s, 0) = \gamma_1(s) \\ H(s, 1) = \gamma_2(s) \\ H(0, t) = x_* = H(1, t) \end{cases} .$$

Jak nietrudno pokazać, pętle różniące się reparametryzacją są homotopijnie równoważne. Ponadto definiując operacje: mnożenie

$$\star : \Omega(X; x_*) / \sim \times \Omega(X; x_*) / \sim \longrightarrow \Omega(X; x_*) / \sim : ([\gamma_1]_{\sim}, [\gamma_2]_{\sim}) \longmapsto [\gamma_1 \circ \gamma_2]_{\sim}$$

oraz branie odwrotności

$$\text{Inv} : \Omega(X; x_*) / \sim \longrightarrow \Omega(X; x_*) / \sim : [\gamma]_{\sim} \longmapsto [\bar{\gamma}]_{\sim} ,$$

otrzymujemy strukturę grupy na zbiorze klas homotopii pętli o bazie x_* ,

$$\pi_1(X; x_*) := (\Omega(X; x_*) / \sim, \star, \text{Inv}, \bullet \longmapsto [\varepsilon_{x_*}]_{\sim}) .$$

Jest to zapowiedziana wcześniej grupa podstawowa X o bazie $x_* \in X$. W oczywisty sposób pozwala nam ona skwantyfikować elementarną cechę przestrzeni topologicznej X , jaką jest jej jednospójność. O fizycznym znaczeniu tej ostatniej przekonuje nas, m.in., mechanika kwantowa cząstek naładowanych (patrz na i pytaj o efekt Aharonowa–Bohma).

Uwaga 1. Dwa najbardziej rozpowszechnione zapisy dla grup to

- zapis mnożeniowy $(\phi_2, \phi_1, e) \equiv (\cdot \equiv M, \text{Inv} \equiv (\cdot)^{-1}, \mathbf{1})$ =(mnożenie, odwrotność, jedynka), w którym wprowadzamy pojęcie **potęgi**

$$\forall_{n \in \mathbb{N} \setminus \{0\}} \forall_{g \in G} : g^n := \underbrace{g \cdot g \cdots g}_{n \text{ razy}} \quad \wedge \quad g^{-n} := \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{n \text{ razy}}, \quad \forall_{g \in G} : g^0 := e ,$$

o oczywistych własnościach:

$$\forall_{m, n \in \mathbb{N} \setminus \{0\}} \forall_{g \in G} : g^m \cdot g^n = g^{m+n} \quad \wedge \quad \text{Inv}(g^n) = g^{-n} .$$

- zapis addytywny $(\phi_2, \phi_1, e) \equiv (+ \equiv A, \text{P} \equiv -(\cdot), \mathbf{0})$ =(przeciwność, dodawanie, zero), w którym wprowadzamy pojęcie **krotności**

$$\forall_{n \in \mathbb{N} \setminus \{0\}} \forall_{g \in G} : ng := \underbrace{g + g + \cdots + g}_{n \text{ razy}} \quad \wedge \quad -ng := \underbrace{(-g) + (-g) + \cdots + (-g)}_{n \text{ razy}},$$

$$(1) \quad \forall_{g \in G} : 0g := \mathbf{0} ,$$

o oczywistych własnościach:

$$\forall_{m, n \in \mathbb{N} \setminus \{0\}} \forall_{g \in G} : mg + ng = (m + n)g \quad \wedge \quad \text{P}(ng) = -ng .$$

Ten ostatni najczęściej stosuje się w odniesieniu do grup przemiennych. Poniżej będziemy (niemal) konsekwentnie używać zapisu mnożeniowego.

Stwierdzenie 1. W dowolnej grupie element neutralny oraz element odwrotny do danego są określone jednoznacznie.

Stwierdzenie 2. Niechaj $(G, \phi_2 = \cdot)$ będzie półgrupą jak w Def. 1 i niech e_L będzie lewostronnym elementem neutralnym względem ϕ_2 , tj.

$$\forall_{g \in G} : e_L \cdot g = g ,$$

a ponadto niech

$$\forall_{g \in G} \exists_{g^\vee \in G} : g^\vee \cdot g = e_L .$$

Wówczas

- (i) $\forall_{g \in G} : g \cdot g^\vee = e_L$.
- (ii) e_L jest elementem neutralnym względem ϕ_2 (obustronnym).

Dowód:

Ad (i) Zachodzi $g^\vee \cdot (g \cdot g^\vee) = (g^\vee \cdot g) \cdot g^\vee = e_L \cdot g^\vee = g^\vee$, zatem $g \cdot g^\vee = e_L \cdot (g \cdot g^\vee) = ((g^\vee)^\vee \cdot g^\vee) \cdot (g \cdot g^\vee) = (g^\vee)^\vee \cdot g^\vee = e_L$.

Ad (ii) Na mocy powyższego $g \cdot e_L = g \cdot (g^\vee \cdot g) = (g \cdot g^\vee) \cdot g = e_L \cdot g = g$.

□

Podstawowe własności operacji $\phi_1 = \text{Inv}$ zbiera

Stwierdzenie 3. W notacji (multyplikatywnej) Def. 3 zachodzi

- (i) $\text{Inv} \circ \text{Inv} = \text{id}_G$;
- (ii) $\text{Inv} \circ M = M \circ (\text{Inv} \times \text{Inv}) \circ \tau_G$;
- (iii) $\forall_{g,h,k \in G} : g \cdot h = k \iff g = k \cdot h^{-1} \iff h = g^{-1} \cdot k$.

Dowód:

Ad (i) Aksjomat (G2) możemy przepisać w postaci

$$\forall_{g \in G} : g \cdot g^{-1} = e,$$

a stąd wynika, że g jest odwrotnością g^{-1} (por. Stw. 2), co w świetle Stw. 1 daje tezę.

Ad (ii) Sprawdzamy, dla dowolnych $g, h \in G$, że $h^{-1} \cdot g^{-1}$ jest – w istocie – odwrotnością $g \cdot h$,

$$(g \cdot h) \cdot (h^{-1} \cdot g^{-1}) = g \cdot (h \cdot h^{-1}) \cdot g^{-1} = g \cdot e \cdot g^{-1} = g \cdot g^{-1} = e,$$

co daje tezę na mocy Stw. 1.

Ad (iii) $g \cdot h = k \iff g = g \cdot e = g \cdot (h \cdot h^{-1}) = (g \cdot h) \cdot h^{-1} = k \cdot h^{-1}$. Drugiej równoważności dowodzimy analogicznie.

□

Definicja 4. Niechaj $(G, \phi_2 \equiv \cdot, \phi_1, \phi_0)$ będzie grupą i niech $S \subset G$ będzie podzbiorem jej nośnika o własności

$$\forall_{g \in G} \exists_{\substack{n \in \mathbb{N} \setminus \{0\} \\ k_1, k_2, \dots, k_n \in \mathbb{Z} \\ x_1, x_2, \dots, x_n \in S}} : g = x_1^{k_1} \cdot x_2^{k_2} \cdot \dots \cdot x_n^{k_n},$$

przy czym dla dowolnych $g \in G$ i $k \in \mathbb{Z}$ mamy

$$g^k = \begin{cases} \underbrace{g \cdot g \cdot \dots \cdot g}_{k \text{ razy}} & \text{gdym } k > 0 \\ \underbrace{g^{-1} \cdot g^{-1} \cdot \dots \cdot g^{-1}}_{|k| \text{ razy}} & \text{gdym } k < 0 \\ e & \text{gdym } k = 0 \end{cases} .$$

Wówczas S nazywamy **zbiorem generatorów** grupy G , o samej zaś grupie mówimy, że **jest generowana** przez zbiór S , co zapisujemy jako

$$G = \langle S \rangle .$$

Definiowanie grupy w terminach generatorów i spełnianych przez nie relacji jest szczególnie wygodne w okolicznościach analizy homomorfizmów grup, oto bowiem w takiej analizie wystarczy zbadać obraz zbioru generatorów dziedziny w przeciwdziedzinie (zamiast pełnej tabelki odwzorowania), upewniając się w szczególności, że w obrazie tym spełnione są te same relacje, którym podlegają generatory dziedziny, co zapewnia istnienie i jednoznaczność rozszerzenia takiego przyporządkowania do homomorfizmu grup. To ogólnoteoriogrupowy odpowiednik faktu z algebry liniowej: odwzorowanie liniowe jest w pełni określone przez wartości przyjmowane przez nie na

bazie jego dziedziny i każde przyporządkowanie wektorów pewnej przestrzeni liniowej wektorom bazowym danej przestrzeni liniowej daje się rozszerzyć do odwzorowania liniowego z tej drugiej w tę pierwszą, przy czym rozszerzenie to jest dane jednoznacznie.

Przykłady 4.

- (1) Grupa symetryczna na zbiorze X jest generowana przez zbiór wszystkich **transpozycji**, tj. permutacji postaci

$$\tau_{x_0, y_0} : X \curvearrowright : x \mapsto \begin{cases} x, & \text{gdy } x \notin \{x_0, y_0\} \\ y_0, & \text{gdy } x = x_0 \\ x_0, & \text{gdy } x = y_0 \end{cases} .$$

Stwierdzenie to było dowodzone na pierwszorocznym wykładzie z Algebry.

- (2) Grupa reszt *modulo* $n \in \mathbb{N} \setminus \{0\}$ (z dodawaniem *modulo* n) jest generowana przez element $[1]_n$.

Definicja 5. W notacji Def.3 **podgrupa** grupy $(G, \phi_2, \phi_1, \phi_0)$ to czwórka $(H, \phi_2, \phi_1, \phi_0)$, w której H jest podzbiorem G o następujących własnościach:

- (SG1) $\phi_2 : H^{\times 2} \rightarrow H \subset G$;
 (SG2) $\phi_1 : H \rightarrow H \subset G$.

Mówimy, że operacje grupowe ograniczone do H domykają się w H .

Przykłady 5.

- (1) Podgrupa

$$\mathcal{Z}(G) = \{ z \in G \mid \forall_{g \in G} : g \cdot z = z \cdot g \}$$

określana jest mianem **centrum grupy** G . W szczególności dla G przemiennej zachodzi $\mathcal{Z}(G) \equiv G$.

- (2) Grupa $(\sqrt[n]{1}, \cdot_{\mathbb{C}}, \bar{\cdot}, (1, 0))$ pierwiastków stopnia $n \in \mathbb{N} \setminus \{0\}$ jest podgrupą grupy $(U(1), \cdot_{\mathbb{C}}, \bar{\cdot}, (1, 0))$.
 (3) **Grupa ortogonalna stopnia 2 nad \mathbb{R}** o nośniku

$$O(2, \mathbb{R}) := \{ M \in GL(2, \mathbb{R}) \mid M^T \cdot M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = M \cdot M^T \},$$

zdefiniowanym w terminach operacji **transpozycji macierzy**

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^T := \begin{pmatrix} a & c \\ b & d \end{pmatrix},$$

który wyposażamy w operacje indukowane z pełnej grupy liniowej nad \mathbb{R} (zdefiniowanej analogicznie do pełnej grupy liniowej nad \mathbb{C} z Przykł. 3(4)), jest podgrupą tejże.

- (4) Podgrupy **grupy homografii** $\text{Hom}(\overline{\mathbb{C}})$ uzwarconej płaszczyzny zespolonej $\overline{\mathbb{C}} := \mathbb{C} \cup \{\infty\}$, tj. odwzorowań postaci

$$h : \overline{\mathbb{C}} \curvearrowright : z \mapsto \frac{a \cdot z + b}{c \cdot z + d}, \quad a, b, c, d \in \mathbb{C}, \quad a \cdot d - b \cdot c \neq 0,$$

to, m.in., grupa jednokładności płaszczyzny o środku $(0, 0)$ (czyli skalowań), tj. odwzorowań postaci

$$J_{(0,0)}^\lambda : \overline{\mathbb{C}} \curvearrowright : z \mapsto \lambda \cdot z, \quad \lambda \in \mathbb{R}^\times,$$

grupa przesunięć na płaszczyźnie, tj. odwzorowań postaci

$$T_{(v_1, v_2)} : \overline{\mathbb{C}} \curvearrowright : z \mapsto z + (v_1, v_2),$$

oraz grupa obrotów płaszczyzny o środku $(0, 0)$, tj. odwzorowań postaci

$$R_{(0,0)}^\theta : \overline{\mathbb{C}} \curvearrowright : z \mapsto e^{i\theta} \cdot z, \quad \theta \in \mathbb{R}.$$

Łatwo można pokazać, że zbiór wszystkich opisanych wyżej jednokładności, przesunięć i obrotów, uzupełniony o inwersję

$$I : \overline{\mathbb{C}} \curvearrowright : z \mapsto z^{-1},$$

generuje grupę $\text{Hom}(\overline{\mathbb{C}})$.

- (5) Przykłady arytmetyczne: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ i $(\mathbb{R}, +)$ to podgrupy $(\mathbb{C}, +_{\mathbb{C}})$; $(\mathbb{Q}^{\times}, \cdot)$ i $(\mathbb{R}^{\times}, \cdot)$ to podgrupy $(\mathbb{C}^{\times}, \cdot_{\mathbb{C}})$; $(\mathbb{Q}_{>0}, \cdot)$ to podgrupa $(\mathbb{R}_{>0}, \cdot)$.
- (6) Niechaj $(G, \phi_2 \equiv \cdot, \phi_1 \equiv (\cdot)^{-1}, \phi_0)$ będzie grupą i niech $A, B \subset G$ będą podgrupami G . **Komutant podgrup** A i B to podgrupa $[A, B] \subset G$ generowana przez wszystkie elementy G postaci

$$[g, h] := g \cdot h \cdot g^{-1} \cdot h^{-1}, \quad g, h \in G,$$

zwane **komutatorami**. W szczególności, grupa $[G, G] \equiv G'$ nosi miano **komutanta** (lub inaczej **pochodnej**) grupy G . Jasnym jest, że grupa G jest przemienna, gdy jej komutant jest trywialny. Przykładem komutanta jest **grupa alternująca** na zbiorze X ,

$$(2) \quad \mathfrak{A}_X := [\mathfrak{S}_X, \mathfrak{S}_X].$$

Wkrótce zapoznamy się z alternatywną definicją tej podgrupy, wysłowioną w terminach znaku tworzących ją permutacji.

Stwierdzenie 4. Każda podgrupa grupy danej jest grupą.

Użyteczne własności podgrup zbiera

Stwierdzenie 5. Niechaj $(G, \phi_2, \phi_1, \phi_0)$ będzie grupą i niech $A, B, C \subset G$ będą podgrupami G , przy czym $C \subset B$. Wówczas

- (i) $A \cap B$ jest podgrupą G .
- (ii) $(A \cap B) \cdot C = (A \cdot C) \cap B$ (Prawo Dedekinda).
- (iii) $(A \cap B = A \cap C \wedge A \cdot B = A \cdot C) \implies B = C$.

Przejdziemy teraz do dyskusji odwzorowań między grupami, które zachowują strukturę grupy.

Definicja 6. W notacji Def. 3 **homomorfizm grupy** $(G^{(1)}, \phi_2^{(1)}, \phi_1^{(1)}, \phi_0^{(1)})$ **w grupę** $(G^{(2)}, \phi_2^{(2)}, \phi_1^{(2)}, \phi_0^{(2)})$ to odwzorowanie

$$\chi : G^{(1)} \longrightarrow G^{(2)}$$

o własności wyrażonej przez diagram przemienny (wypisany wraz z równoważnym zdaniem logicznym):

$$(GH) \quad \begin{array}{ccc} G^{(1)} \times G^{(1)} & \xrightarrow{\phi_2^{(1)}} & G^{(1)} \\ \chi \times \chi \downarrow & & \downarrow \chi \\ G^{(2)} \times G^{(2)} & \xrightarrow{\phi_2^{(2)}} & G^{(2)} \end{array} \quad \equiv \quad \forall_{g, h \in G} : \begin{array}{l} \chi \circ \phi_2^{(1)}(g, h) \\ = \phi_2^{(2)}(\chi(g), \chi(h)) \end{array} .$$

Jak poprzednio w oczywisty sposób wyróżniamy

- **monomorfizmy** (homomorfizmy iniektywne, $G^{(1)} \hookrightarrow G^{(2)}$);
- **epimorfizmy** (homomorfizmy surjektywne, $G^{(1)} \twoheadrightarrow G^{(2)}$);
- **izomorfizmy** (homomorfizmy bijektywne, $G^{(1)} \xrightarrow{\cong} G^{(2)}$);
- **endomorfizmy** (homomorfizmy wewnętrzne, $G^{(2)} \equiv G^{(1)} \circlearrowright$);
- **automorfizmy** (bijektywne homomorfizmy wewnętrzne).

Przykłady 6.

- (1) Odwzorowanie $\mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} : [k]_2 \mapsto [2k]_4$ jest monomorfizmem.
- (2) Odwzorowanie $O(2, \mathbb{R}) \longrightarrow \sqrt[2]{1} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a \cdot d - b \cdot c$ jest epimorfizmem.
- (3) Odwzorowanie $\sqrt[n]{1} \longrightarrow \mathbb{Z}/n\mathbb{Z} : e^{i\frac{2\pi k}{n}} \mapsto [k]_n, n \in \mathbb{N} \setminus \{0, 1\}$ jest izomorfizmem.
- (4) Odwzorowanie

$$\mathfrak{S}_{\{x, y, z\}} \circlearrowright : \sigma \mapsto \begin{cases} \text{id}_{\{x, y, z\}}, & \text{gdy } \sigma \in \mathfrak{A}_{\{x, y, z\}} \\ \tau_{x, y} & \text{w przeciwnym przypadku} \end{cases}$$

jest endomorfizmem $\mathfrak{S}_{\{x, y, z\}}$.

- (5) Odwzorowanie $\mathbb{Z}/(2n+1)\mathbb{Z} \curvearrowright : [k]_{2n+1} \mapsto 2[k]_{2n+1}$ jest automorfizmem.
 (6) Przykłady arytmetyczne (opuszczamy oczywiste elementy struktury):

$(G^{(1)}, \phi_2^{(1)})$	$(G^{(2)}, \phi_2^{(2)})$	χ	typ
$(\mathbb{R}_{>0}, \cdot)$	$(\mathbb{R}_{>0}, \cdot)$	$x \mapsto x^{\frac{p}{q}}, \frac{p}{q} \in \mathbb{Q}$	iniektywny endomorfizm
$(\mathbb{R}_{>0}, \cdot)$	$(\mathbb{R}, +)$	$x \mapsto \log x$	izomorfizm
$(\mathbb{R}, +)$	$(\mathbb{R}_{>0}, \cdot)$	$x \mapsto e^{\lambda x}, \lambda \in \mathbb{R}^\times$	izomorfizm
$(\mathbb{C}^\times, \cdot_{\mathbb{C}})$	$(\mathbb{C}^\times, \cdot_{\mathbb{C}})$	$z \mapsto \bar{z}$	automorfizm
$(\mathbb{C}, +_{\mathbb{C}})$	$(\mathbb{C}, +_{\mathbb{C}})$	$z \mapsto \bar{z}$	j/w
$(\mathbb{C}^\times, \cdot_{\mathbb{C}})$	$(\mathbb{R}_{>0}, \cdot)$	$z \mapsto z $	epimorfizm
$(\mathbb{R}, +)$	$(U(1), \cdot_{\mathbb{C}})$	$x \mapsto e^{i\lambda x}, \lambda \in \mathbb{R}^\times$	epimorfizm

- (7) Każda podgrupa $H \subset G$ zadaje kanoniczny monomorfizm $j_H : H \hookrightarrow G$, zwany **standardowym włożeniem**, który utożsamia elementy H traktowanego jako niezależny zbiór z tymi samymi elementami H traktowanego jako podzbiór G .
 (8) Operacja 1-argumentowa $\phi_1 : G \curvearrowright$ zadaje izomorfizm między grupą G a przeciwną do niej.

Proste własności homomorfizmu w odniesieniu do pozostałych elementów struktury grupy zbiera

Stwierdzenie 6. W notacji Def. 6 poniższe diagramy są przemienne:

- (i) (transport elementu neutralnego)

$$\begin{array}{ccc} \{\bullet\} & \xrightarrow{\phi_0^{(1)}} & G^{(1)} \\ & \searrow \phi_0^{(2)} & \downarrow \chi \\ & & G^{(2)} \end{array} ;$$

- (ii) (zgodność z braniem odwrotności)

$$\begin{array}{ccc} G^{(1)} & \xrightarrow{\phi_1^{(1)}} & G^{(1)} \\ \chi \downarrow & & \downarrow \chi \\ G^{(2)} & \xrightarrow{\phi_1^{(2)}} & G^{(2)} \end{array} .$$

Dowód:

Ad (i) $\chi(e^{(1)}) \cdot_{(2)} \chi(e^{(1)}) = \chi(e^{(1)} \cdot_{(1)} e^{(1)}) = \chi(e^{(1)})$, ale $G^{(2)}$ jest grupą, więc istnieje $\chi(e^{(1)})^{-1} \in G^{(2)}$, a zatem

$$\begin{aligned} \chi(e^{(1)}) &= e^{(2)} \cdot_{(2)} \chi(e^{(1)}) = \chi(e^{(1)})^{-1} \cdot_{(2)} \chi(e^{(1)}) \cdot_{(2)} \chi(e^{(1)}) \\ &= \chi(e^{(1)})^{-1} \cdot_{(2)} \chi(e^{(1)}) = e^{(2)} . \end{aligned}$$

Ad (ii) Sprawdzamy, dla dowolnego $g \in G^{(1)}$, że $\chi(g^{-1})$ jest – wobec powyższego – odwrotnością $\chi(g)$,

$$\chi(g^{-1}) \cdot_{(2)} \chi(g) = \chi(g^{-1} \cdot_{(1)} g) = \chi(e^{(1)}) = e^{(2)},$$

co na mocy Stw.1 daje tezę. □

Mamy też oczywiste acz ważne

Stwierdzenie 7. Każdy monomorfizm jest izomorfizmem dziedziny na jej obraz względem tego monomorfizmu.

Szczególny typ homomorfizmów grup opisuje

Stwierdzenie 8. Niechaj $(G, \phi_2, \phi_1, \phi_0)$ będzie grupą, $\text{Aut}(G)$ zaś – zbiorem jej automorfizmów. Wówczas czwórka

$$(\text{Aut}(G), \circ, (\cdot)^{-1}, \{\bullet\} \mapsto \text{id}_G)$$

jest grupą, określaną mianem **grupy automorfizmów** G .

Odwzorowania postaci

$$\text{Ad}_h : G \curvearrowright : g \mapsto h \cdot g \cdot h^{-1}, \quad h \in G,$$

są automorfizmami G , zwanymi **automorfizmami wewnętrznymi**. Tworzą one podgrupę $\text{Inn}(G) \subset \text{Aut}(G)$ określaną jako **grupa automorfizmów wewnętrznych** G . Każdy automorfizm z $\text{Aut}(G) \setminus \text{Inn}(G)$ określamy mianem **automorfizmu zewnętrznego**.

Odwzorowanie

$$(3) \quad \text{Ad} : G \longrightarrow \text{Inn}(G) : g \mapsto \text{Ad}_g$$

jest epimorfizmem grup.

Mamy oczywiste

Stwierdzenie 9. Grupa automorfizmów wewnętrznych grupy przemiennej jest trywialna.

Przykłady 7.

- (1) Grupa $\mathbb{Z}/5\mathbb{Z}$, jako grupa przemienna, nie posiada nietrywialnych automorfizmów wewnętrznych. Jej grupa automorfizmów to – jak łatwo stwierdzić na podstawie analizy możliwych obrazów generatora $[1]_5$ względem endomorfizmu –

$$\text{Aut}(\mathbb{Z}/5\mathbb{Z}) = \{ \zeta_n : \mathbb{Z}/5\mathbb{Z} \curvearrowright : [k]_5 \mapsto n[k]_5 \mid n \in \overline{1,4} \} \cong \mathbb{Z}/4\mathbb{Z}.$$

- (2) $\forall_{n \in \mathbb{N}_{>2}} : \text{Inn}(\mathfrak{S}_n) \cong \mathfrak{S}_n$ oraz $\forall_{n \in \mathbb{N}_{>2} \setminus \{6\}} : \text{Aut}(\mathfrak{S}_n) \cong \text{Inn}(\mathfrak{S}_n)$.

W dalszej części wykładu dokonamy bardziej wnikliwej analizy struktury homomorfizmu grup.

Definicja 7. W notacji Def.6 **jądro homomorfizmu** to podzbiór

$$\ker \chi := \{ g \in G^{(1)} \mid \chi(g) = e^{(2)} \},$$

natomiast **obraz homomorfizmu** to podzbiór

$$\text{im } \chi := \{ g \in G^{(2)} \mid \exists_{h \in G^{(1)}} : g = \chi(h) \} \equiv \chi(G^{(1)}).$$

Stwierdzenie 10. W notacji Def.6 i 7 $\ker \chi$ jest podgrupą $G^{(1)}$.

Dowód:

- (1) $g, h \in \ker \chi \implies \chi(g \cdot_{(1)} h) = \chi(g) \cdot_{(2)} \chi(h) = e^{(2)} \cdot_{(2)} e^{(2)} = e^{(2)} \implies g \cdot_{(1)} h \in \ker \chi$.
 (2) $g \in \ker \chi \implies \chi(\text{Inv}^{(1)}(g)) = \text{Inv}^{(2)}(\chi(g)) = \text{Inv}^{(2)}(e^{(2)}) = e^{(2)} \implies \text{Inv}^{(1)}(g) \in \ker \chi$. □

Stwierdzenie 11. W notacji Def. 6 i 7 $\text{im } \chi$ jest podgrupą $G^{(2)}$.

Dowód:

- (1) $g, h \in \text{im } \chi \iff \exists_{a, b \in G^{(1)}} : (g = \chi(a) \wedge h = \chi(b)) \implies g \cdot_{(2)} h = \chi(a) \cdot_{(2)} \chi(b) = \chi(a \cdot_{(1)} b) \in \text{im } \chi$.
- (2) $g \in \text{im } \chi \iff \exists_{a \in G^{(1)}} : g = \chi(a) \implies \text{Inv}^{(2)}(g) = \text{Inv}^{(2)}(\chi(a)) = \chi(\text{Inv}^{(1)}(a)) \in \text{im } \chi$. □

Przykłady 8.

- (1) Jądrem epimorfizmu z przykładu 6(2) jest **grupa specjalna ortogonalna stopnia 2 nad \mathbb{R}** , o nośniku dopuszczającą naturalną parametryzację:

$$\text{SO}(2, \mathbb{R}) := \left\{ \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} \mid \theta \in \mathbb{R} \right\}.$$

- (2) Jądrem epimorfizmu $|\cdot|$ z przykładu 6(6) jest podgrupa $U(1) \subset \mathbb{C}^\times$.
- (3) Jądrem epimorfizmu $e^{i\lambda}$, $\lambda \in \mathbb{R}^\times$ jest podgrupa $\frac{2\pi}{\lambda} \mathbb{Z} \subset \mathbb{R}$.
- (4) Jądrem epimorfizmu Ad . ze Stw. 8 jest podgrupa $\mathcal{Z}(G) \subset G$.

Przyjrzymy się bliżej jądru homomorfizmu.

Stwierdzenie 12. W notacji Def. 6 i 7 χ jest monomorfizmem $\iff \ker \chi = \{e^{(1)}\}$.

Dowód:

- $\implies \chi(e^{(1)}) = e^{(2)}$, zatem $\chi(g) = e^{(2)}$ implikuje $g = e^{(1)}$ wobec iniektywności χ .
- $\impliedby \chi(g) = \chi(h) \iff \chi(g \cdot_{(1)} \text{Inv}^{(1)}(h)) = e^{(2)}$, ale wobec trywialności $\ker \chi$ to implikuje $g \cdot_{(1)} \text{Inv}^{(1)}(h) = e^{(1)}$, czyli $g = h$. □

2. WARSTWY I GRUPY ILORAZOWE

Przypomnijmy następujące pojęcie znane z kursu analizy matematycznej.

Definicja 8. Niechaj X, Y będą zbiorami i niech będzie dane odwzorowanie $f : X \rightarrow Y$. **Poziomica** (albo **przeciwobraz**) **podzbioru** $Z \subset f(X)$ **względem** f to podzbiór

$$f^{-1}(Z) := \{ x \in X \mid f(x) \in Z \}.$$

Stwierdzenie 13. W notacji Def. 6, 7 i 8

$$\ker \chi = \chi^{-1}(\{e^{(2)}\}).$$

Odpowiedzi na pytanie o postać pozostałych poziomic dostarcza

Stwierdzenie 14. W notacji Def. 6, 7 oraz 8 i dla dowolnego $g \in G^{(1)}$ słuszną jest formuła

$$\chi^{-1}(\{\chi(g)\}) = \{ g \cdot_{(1)} h \mid h \in \ker \chi \} =: g \ker \chi.$$

Dowód: $x \in \chi^{-1}(\{\chi(g)\}) \iff \chi(x) = \chi(g) \iff \chi(\text{Inv}^{(1)}(g) \cdot_{(1)} x) = e^{(2)} \iff \text{Inv}^{(1)}(g) \cdot_{(1)} x \in \ker \chi \iff \exists_{h \in \ker \chi} : x = g \cdot_{(1)} h$. □

Powyższa analiza dopuszcza następujące uogólnienie.

Definicja 9. W notacji Def. 5 **warstwa lewostronna względem podgrupy H w grupie G** to zbiór

$$gH := \{ g \cdot h \mid h \in H \}$$

dla pewnego $g \in G$. Analogicznie definiujemy **warstwę prawostronną względem podgrupy H w grupie G** ,

$$Hg := \{ h \cdot g \mid h \in H \}.$$

Stwierdzenie 15. W notacji Def. 5 i 9 zachodzi

$$\forall_{g \in G} : |gH| = |H|,$$

przy czym $|X|$ oznacza moc zbioru X .

Dowód: Pożądana bijekcja to

$$H \longrightarrow gH : h \longmapsto g \cdot h.$$

□

Definicja 10. W notacji Def. 9 **indeksem (lewostronnym) podgrupy H w grupie G** nazywamy moc zbioru warstw (lewostronnych) względem H w G ,

$$(G : H) := |\{ gH \mid g \in G \}|.$$

Stwierdzenie 16. W notacji Def. 5 i 9 relacja na G zadana, jak następuje:

$$a \sim_H b \iff a \in bH,$$

jest relacją równoważności.

Dowód:

- (1) Na mocy Stw. 4 $e \in H$, ale w takim razie $a = a \cdot e \in aH$, zatem $a \sim_H a$.
- (2) $a \sim_H b \iff \exists_{h \in H} : a = b \cdot h \implies b = a \cdot h^{-1}$, ale na mocy Stw. 4 $h \in H \implies h^{-1} \in H$, co w sumie oznacza, że $b \in aH$, czyli $b \sim_H a$.
- (3) $a \sim_H b \wedge b \sim_H c \iff \exists_{h_1, h_2 \in H} : (a = b \cdot h_1 \wedge b = c \cdot h_2) \implies a = c \cdot (h_1 \cdot h_2) \in cH \iff a \sim_H c$.

□

Corollarium 1. Dowolna podgrupa grupy danej zadaje rozkład tej ostatniej na sumę rozłączną równolicznych warstw (względem tejże podgrupy).

Przykłady 9.

- (1) Rozkład grupy $\mathbb{Z}/6\mathbb{Z}$ na warstwy względem podgrupy $\{[0]_6, [3]_6\} \cong \mathbb{Z}/2\mathbb{Z}$ to

$$\mathbb{Z}/6\mathbb{Z} = ([0]_6 +_6 \mathbb{Z}/2\mathbb{Z}) \cup ([1]_6 +_6 \mathbb{Z}/2\mathbb{Z}) \cup ([2]_6 +_6 \mathbb{Z}/2\mathbb{Z}).$$

- (2) Rozkład grupy \mathfrak{S}_X na (lewostronne) warstwy względem podgrupy \mathfrak{A}_X to

$$\mathfrak{S}_X = \text{id}_X \mathfrak{A}_X \cup \tau_{x_0, y_0} \mathfrak{A}_X,$$

przy czym para (x_0, y_0) (niezośmarnych) elementów X jest wybrana dowolnie.

- (3) Rozkład grupy $O(2, \mathbb{R})$ na (lewostronne) warstwy względem podgrupy $SO(2, \mathbb{R})$ to

$$O(2, \mathbb{R}) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} SO(2, \mathbb{R}) \cup \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} SO(2, \mathbb{R}).$$

- (4) Prostej ilustracji geometrycznej pojęcia warstwy dostarcza teoria liczb zespolonych. Ustalmy $(x_0, y_0) \in \mathbb{C}^\times$, a wtedy zbiór

$$\mathbb{R} \cdot (x_0, y_0) := \{ \lambda \cdot (x_0, y_0) \in \mathbb{C} \mid \lambda \in \mathbb{R} \}$$

jest wyposażony w naturalną strukturę grupy (przemiennej) względem operacji $(+_{\mathbb{C}}, -(\cdot))$, $\bullet \longmapsto (0, 0)$. Grupa ta jest izomorficzna z \mathbb{R} , a jej geometrycznym przedstawieniem jest prosta na płaszczyźnie \mathbb{R}^2 przechodząca przez punkty o współrzędnych $(0, 0)$ i (x_0, y_0) . Warstwy względem tej podgrupy reprezentują proste równoległe do tej ostatniej.

W szczególności, dla $(x_0, y_0) := (1, 0)$ otrzymujemy rozkład (rozwarstwienie) płaszczyzny zespolonej na rodzinę prostych

$$\mathbb{C} = \bigcup_{y \in \mathbb{R}} ((0, y) +_{\mathbb{C}} \mathbb{R} \cdot (1, 0)) .$$

Warto również przytoczyć w formie prostego wniosku z dwóch ostatnich stwierdzeń dość nieoczekiwaną własność grup skończonych.

Corollarium 2. (Twierdzenie Lagrange'a) Przyjmijmy notację Def. 3 i 5. 10. Wówczas zachodzi tożsamość

$$(4) \quad |G| = |H| \cdot (G : H) .$$

W szczególności więc moc dowolnej podgrupy grupy skończonej jest dzielnikiem mocy grupy.

Tytułem ilustracji nietrywialnych konsekwencji Tw. Lagrange'a, rozważymy obecnie

Corollarium 3. Niechaj G będzie grupą, g zaś – jej dowolnym elementem. Zdefiniujmy **rząd elementu g** jako

$$\text{ord}(g) := \min \{ N \in \mathbb{N}^{\times} \mid g^N = e \} .$$

Zachodzi

$$\text{ord}(g) \mid |G| ,$$

tj. rząd dowolnego elementu grupy skończonej jest dzielnikiem rzędu grupy.

Dowód: Liczba $\text{ord}(g)$ jest rzędem podgrupy generowanej przez g ,

$$\text{ord}(g) \equiv \langle g \rangle .$$

□

Następnie dowodzimy

Corollarium 4. Niechaj G będzie grupą rzędu $|G| = p$, gdzie $p \in \mathbb{N}^{\times}$ jest liczbą pierwszą. Wówczas G jest **cykliczna**, tj. generowana przez swój dowolny element $g \neq e$,

$$(5) \quad G \equiv \langle g \rangle .$$

Dowód: Rozważmy dowolny element $g \neq e$ grupy G . Skoro $\langle g \rangle \ni g, e$, to $|\langle g \rangle| > 1$, ale też – w świetle Cor. 3 – $|\langle g \rangle| \mid p$, co wobec pierwszości p implikuje $|\langle g \rangle| = p$, czyli też tożsamość (5). □

Na koniec – wynik z innej beczki, zaczerpnięty z niej przy użyciu Tw. Lagrange'a właśnie:

Corollarium 5 (Tw. Fermata). Niechaj $p \in \mathbb{N}^{\times}$ będzie liczbą pierwszą, n zaś – dowolną liczbą całkowitą. Wówczas zachodzi kongruencja

$$n^p \equiv n \pmod{p} .$$

Dowód: Rozważmy ciało \mathbb{Z}_p reszt modulo p . Po usunięciu zeń reszty zerowej $[0]_p$ otrzymujemy grupę o nośniku \mathbb{Z}_p^{\times} z mnożeniem mod p jako operacją binarną (patrz: Zad. dom. 6). Jest to grupa rzędu $|\mathbb{Z}_p^{\times}| = |\mathbb{Z}_p| - |\{[0]_p\}| = p - 1$.

Jeśli $[n]_p = [0]_p$, to jest też $[n^p]_p \equiv [n]_p^p = [0]_p^p \equiv [0^p]_p = [0]_p \equiv [n]_p$, czyli $n^p \equiv n \pmod{p}$, pozostaje zatem rozpatrzyć przypadek $[n]_p \neq [0]_p$. Wówczas $[n]_p \in \mathbb{Z}_p^{\times}$, przeto na mocy Cor. 3 jest $p - 1 = k \cdot \text{ord}([n]_p)$ dla pewnego $k \in \mathbb{N}^{\times}$. Wobec tego zachodzi równość $[n]_p^{p-1} = ([n]_p^{\text{ord}([n]_p)})^k = [1]_p^k \equiv [1^k]_p = [1]_p$, która implikuje pożądaną równość $[n]_p^p = [n]_p^{p-1} \cdot_p [n]_p = [1]_p \cdot_p [n]_p \equiv [1 \cdot n]_p = [n]_p$. □

W dalszej części wykładu dokonamy abstrakcji pewnej oczywistej cechy podgrupy $\ker \chi$ (zadanej przez dowolny homomorfizm grup χ), która pozwoli precyzyjniej scharakteryzować każdą taką podgrupę.

Stwierdzenie 17. W notacji Def. 5, 6, 7 i 9 zachodzi

$$\forall_{g \in G^{(1)}} : g \cdot_{(1)} \ker \chi = \ker \chi \cdot_{(1)} g,$$

albo – równoważnie –

$$\forall_{g \in G^{(1)}} : g \cdot_{(1)} \ker \chi \cdot_{(1)} \text{Inv}_{(1)}(g) = \ker \chi.$$

Dowód: Niech $g \in G^{(1)}$, a wtedy $h \in \ker \chi \implies \chi(g \cdot_{(1)} h \cdot_{(1)} \text{Inv}_{(1)}(g)) = \chi(g) \cdot_{(2)} \chi(h) \cdot_{(2)} \chi(\text{Inv}_{(1)}(g)) = \chi(g) \cdot_{(2)} e_{(2)} \cdot_{(2)} \chi(\text{Inv}_{(1)}(g)) = \chi(g) \cdot_{(2)} \chi(\text{Inv}_{(1)}(g)) = \chi(g \cdot_{(1)} \text{Inv}_{(1)}(g)) = \chi(e_{(1)}) = e_{(2)}$, zatem $g \cdot_{(1)} \ker \chi \cdot_{(1)} \text{Inv}_{(1)}(g) \subset \ker \chi$. I odwrotnie, niech $h \in \ker \chi$, a wtedy zachodzi – w konsekwencji poprzednio udowodnionego zawierania – $h = g \cdot_{(1)} (\text{Inv}_{(1)}(g) \cdot_{(1)} h \cdot_{(1)} g) \cdot_{(1)} \text{Inv}_{(1)}(g) \in g \cdot_{(1)} \ker \chi \cdot_{(1)} \text{Inv}_{(1)}(g)$. \square

Definicja 11. W notacji Def. 5 i 9 **dzielnik normalny** (albo inaczej **podgrupa normalna**) grupy $(G, \phi_2, \phi_1, \phi_0)$ to jej podgrupa (o nośniku) $H \subset G$ o własności

$$\forall_{g \in G} : gH \subset Hg.$$

Równoważna definicja to

$$\forall_{g \in G} : gHg^{-1} \subset H,$$

czyli też – wobec dowolności g (obok którego możemy rozważać g^{-1}) –

$$\forall_{g \in G} : gHg^{-1} = H.$$

Przykłady 10.

- (1) Dla dowolnego $n \in \mathbb{N}$ podgrupa $n\mathbb{Z}$ (wielokrotności n) jest dzielnikiem normalnym \mathbb{Z} .
- (2) Podgrupa $[G, G]$ dowolnej grupy G . Istotnie, dla dowolnych elementów $x, g, h \in G$ zachodzi tożsamość

$$\text{Ad}_x[g, h] = [x \cdot g, h] \cdot [h, x] \in [G, G].$$

W szczególności zatem grupa alternująca na zbiorze X jest dzielnikiem normalnym grupy symetrycznej na X .

- (3) Podgrupa $\mathcal{I}nn(G) \subset \text{Aut}(G)$ automorfizmów wewnętrznych dowolnej grupy G . Wynika to z oczywistej tożsamości

$$\forall_{\substack{\chi \in \text{Aut}(G) \\ g \in G}} : \chi \circ \text{Ad}_g \circ \chi^{-1} = \text{Ad}_{\chi(g)} \in \mathcal{I}nn(G).$$

Prawdziwe jest ogólne

Stwierdzenie 18. Każda podgrupa grupy przemiennej jest normalna.

Dyskusja istnienia dzielników normalnych grupy danej prowadzi do naturalnej

Definicja 12. **Grupa prosta** to taka, która nie posiada podgrup normalnych właściwych i nie-trywialnych, tj. różnych od całej grupy i od podgrupy trywialnej.

Przykłady 11. Grupa alternująca na zbiorze X o mocy $|X| \neq 4$.

W przypadku ogólnym pokażemy, że każdy dzielnik normalny jest jądrem pewnego homomorfizmu, co doprowadzi nas do pojęcia grupy ilorazowej.

Stwierdzenie 19. W notacji Def. 5, 9 i 11 struktura grupy na grupie G i jej dzielniku normalnym $H \subset G$ indukuje naturalną strukturę grupy na zbiorze warstw (lewostronnych, a więc też – w tym przypadku – prawostronnych)

$$G/H := \{ gH \mid g \in G \}$$

określona, jak następuje (poniżej $g, g_1, g_2 \in G$ są dowolne)

- mnożenie: $g_1H \odot g_2H := g_1H \cdot g_2H$;
- odwrotność: $\text{Inv}_{G/H}(gH) := g^{-1}H$;
- jedyńka: $\mathbf{1}_{G/H} := H$.

Dowód: Pokażemy najpierw, że $g_1H, g_2H \in G/H \implies g_1H \odot g_2H \in G/H$. Istotnie,

$$\begin{aligned} g_1H \odot g_2H &= \{ g_1 \cdot h_1 \cdot g_2 \cdot h_2 \mid h_1, h_2 \in H \} = \{ g_1 \cdot g_2 \cdot (g_2^{-1} \cdot h_1 \cdot g_2) \cdot h_2 \mid h_1, h_2 \in H \} \\ &= \{ g_1 \cdot g_2 \cdot \tilde{h}_1 \cdot h_2 \mid \tilde{h}_1, h_2 \in H \} = \{ g_1 \cdot g_2 \cdot \tilde{h} \mid \tilde{h} \in H \} = (g_1 \cdot g_2)H \in G/H, \end{aligned}$$

przy czym przedostatnia równość wynika z tożsamości $H \cdot H = H$. Łączność działania grupowego \cdot implikuje natychmiast łączność \odot .

Wobec powyższego jest też $g^{-1}H \odot gH = H$, a ponadto $gH \odot H = gH$, czyli – istotnie – H jest elementem neutralnym \odot i $g^{-1}H$ jest odwrotnością gH . \square

Definicja 13. W notacji Def. 5 i 9 oraz Stw. 19 **grupa ilorazowa** grupy $(G, \phi_2, \phi_1, \phi_0)$ względem dzielnika normalnego H to grupa

$$(G/H, \odot, \text{Inv}_{G/H}, \{\bullet\} \mapsto H).$$

Homomorfizm kanoniczny grupy G w jej grupę ilorazową G/H to odwzorowanie

$$\pi_{G/H} : G \rightarrow G/H : g \mapsto gH.$$

Bywa ono też nazywane **rzutem kanonicznym modulo H** .

Przykłady 12.

- (1) Opisana wcześniej struktura grupy (przemiennej) na zbiorze $\mathbb{Z}/n\mathbb{Z}$ reszt *modulo* $n \in \mathbb{N} \setminus \{0\}$ (z dodawaniem *modulo* n) to struktura grupy ilorazowej na zbiorze warstw w \mathbb{Z} względem dzielnika normalnego $n\mathbb{Z}$.
- (2) **Grupa automorfizmów zewnętrznych** (zwana także – bardziej adekwatnie⁴ – **grupą klas automorfizmów**)

$$\text{Out}(G) := \text{Aut}(G)/\text{Inn}(G).$$

Dotychczasowe nasze rozważania ustanawiają jedno-jednoznaczność odpowiedniość pomiędzy jądrami homomorfizmów grup i podgrupami normalnymi.

3. CIĄGI DOKŁADNE I ROZSZERZENIA GRUP

Para homomorfizmów $(j_H, \pi_{G/H})$, którą zapiszemy w postaci

$$H \xrightarrow{j_H} G \xrightarrow{\pi_{G/H}} G/H$$

spełnia oczywistą relację

$$\ker \pi_{G/H} = \text{im } j_H.$$

Wyraża ona, w połączeniu ze Stw. 17, zapowiedziane wcześniej utożsamienie pomiędzy dzielnikami normalnymi a jądrami homomorfizmów. Jej abstrakcję opisuje

Definicja 14. Niechaj $(G^{(\alpha)}, \phi_2^{(\alpha)}, \phi_1^{(\alpha)}, \phi_0^{(\alpha)})$, $\alpha \in \{1, 2, 3\}$ będzie trójką grup i niech $\chi_{(\beta)} : G^{(\beta)} \rightarrow G^{(\beta+1)}$, $\beta \in \{1, 2\}$ będzie parą homomorfizmów grup. Piątkę

$$G^{(1)} \xrightarrow{\chi_{(1)}} G^{(2)} \xrightarrow{\chi_{(2)}} G^{(3)}$$

nazywamy **ciągami dokładnymi (grup)**, jeżeli

$$\ker \chi_{(2)} = \text{im } \chi_{(1)}.$$

⁴Należy zauważyć, że elementami $\text{Out}(G)$ *nie* są automorfizmy zewnętrzne G , lecz ich warstwy w $\text{Aut}(G)$.

Ogólniej, przeliczalna rodzina grup $\{G_n\}_{n \in \mathbb{Z}}$ i stowarzyszonych homomorfizmów opisana diagramem

$$\dots \xrightarrow{\chi^{(0)}} G^{(1)} \xrightarrow{\chi^{(1)}} G^{(2)} \xrightarrow{\chi^{(2)}} \dots \xrightarrow{\chi^{(n-1)}} G^{(n)} \xrightarrow{\chi^{(n)}} \dots$$

nosi miano **ciągu dokładnego**, jeśli

$$\forall_{k \in \overline{1, n-2}} : \ker \chi_{(k+1)} = \operatorname{im} \chi_{(k)}.$$

Krótki ciąg dokładny to ciąg dokładny szczególnej postaci

$$\mathbf{1} \longrightarrow G^{(1)} \xrightarrow{\chi^{(1)}} G^{(2)} \xrightarrow{\chi^{(2)}} G^{(3)} \longrightarrow \mathbf{1},$$

w którym spełniona jest koniunkcja warunków:

- (1) $\chi_{(1)}$ jest mono;
- (2) $\chi_{(2)}$ jest epi;
- (3) $\ker \chi_{(2)} = \operatorname{im} \chi_{(1)}$.

Trójkę $(G^{(2)}, \chi_{(1)}, \chi_{(2)})$ nazywamy wtedy **rozszerzeniem grupy $G^{(3)}$ przez grupę $G^{(1)}$** . Przy tym ilekroć $\operatorname{im} \chi^{(1)} \subset \mathcal{Z}(G^{(2)})$, mówimy o **rozszerzeniu centralnym**⁵ (możliwym wtedy tylko, gdy $G^{(1)}$ jest przemienna).

Przykłady 13. Niechaj $(G, \phi_2, \phi_1, \phi_0)$ będzie dowolną grupą, $H \subset G$ zaś – jej dzielnikiem normalnym. Wówczas diagram

$$(6) \quad \mathbf{1} \longrightarrow H \xrightarrow{J_H} G \xrightarrow{\pi_{G/H}} G/H \longrightarrow \mathbf{1}$$

zadaje krótki ciąg dokładny. Każdy ciąg dokładny tej postaci będziemy odtąd nazywać **normalnym ciągiem dokładnym**. Ważnym przykładem takiego ciągu jest

$$\mathbf{1} \longrightarrow 2\pi\mathbb{Z} \xrightarrow{J_{2\pi\mathbb{Z}}} \mathbb{R} \xrightarrow{\pi_{\mathbb{R}/2\pi\mathbb{Z}}} \mathbb{R}/2\pi\mathbb{Z} \longrightarrow \mathbf{1},$$

w którym $2\pi\mathbb{Z}$ i \mathbb{R} należy rozumieć jako nośniki struktury grupy zadawanej przez dodawanie liczb (rzeczywistych). Wobec oczywistej relacji

$$\ker e^i = 2\pi\mathbb{Z}$$

wypisanej dla epimorfizmu grup z Przykł. 6 (6), dostajemy – na mocy Tw. 1 –

$$\mathbb{R}/2\pi\mathbb{Z} \cong \operatorname{U}(1),$$

co pozwala przepisać powyższy normalny ciąg dokładny w postaci powszechnie spotykanej w literaturze, tj.

$$\mathbf{1} \longrightarrow 2\pi\mathbb{Z} \longrightarrow \mathbb{R} \longrightarrow \operatorname{U}(1) \longrightarrow \mathbf{1}.$$

Ciągi dokładne odgrywają istotną rolę w analizie niektórych zagadnień algebry homologicznej oraz (nie bez związku z poprzednim) w dyskusji rozszerzeń algebr i grup Liego, spotykanych w fizyce.

Na koniec tej części wykładu omówimy ważne przykłady **homomorfizmów indukowanych i kanonicznych**, które

- pozwalają nam lepiej zrozumieć kanoniczną strukturę dowolnego homomorfizmu grup, względnie
- wytyczają prostą drogę ku fizykalnie nader istotnej konstrukcji iloczynu półprostego grup, względnie
- ustalają naturalną hierarchię w zbiorze grup ilorazowych względem dzielników normalnych grupy danej.

Zacniemy od twierdzenia podsumowującego dyskusję struktury jądra homomorfizmu.

Twierdzenie 1 (Pierwsze twierdzenie o izomorfizmie). W notacji Def. 6, 7 i 13 oraz Stw. 19 $\ker \chi$ jest dzielnikiem normalnym $G^{(1)}$, a nadto istnieje **kanoniczny izomorfizm** grup

$$G^{(1)}/\ker \chi \cong \operatorname{im} \chi.$$

⁵Rozszerzenia centralne grup odgrywają istotną rolę w opisie symetrii kwantowej teorii pola.

Dowód: Pierwsza część twierdzenia wynika wprost ze Stw. 17, zajmiemy się przeto częścią drugą. Zdefiniujmy odwzorowanie

$$\lambda_\chi : G^{(1)}/\ker \chi \longrightarrow \operatorname{im} \chi : g \ker \chi \longmapsto \chi(g).$$

Łatwo widać, że definicja ta ma sens (tj. nie zależy od wyboru reprezentanta warstwy), bowiem dla dowolnego $h \in g \ker \chi$ zachodzi – wobec $\exists_{k \in \ker \chi} : h = g \cdot_{(1)} k$ – tożsamość

$$(7) \quad \chi(h) = \chi(g \cdot_{(1)} k) = \chi(g) \cdot_{(2)} \chi(k) = \chi(g) \cdot_{(2)} e^{(2)} = \chi(g).$$

Odwzorowanie to jest jawnie surjektywne, gdyż $h \in \operatorname{im} \chi \implies \exists_{g \in G^{(1)}} : h = \chi(g) = \lambda_\chi(g \ker \chi)$, czyli $\operatorname{im} \lambda_\chi = \operatorname{im} \chi$.

Jest ono także injektywne, co wynika z następującego rozumowania (wykorzystującego Stw. 12):

$$\lambda_\chi(g \ker \chi) = e^{(2)} \iff \chi(g) = e^{(2)} \iff g \in \ker \chi \iff g \ker \chi = \ker \chi,$$

czyli $\ker \lambda_\chi = \{\ker \chi\}$, a $\ker \chi$ jest elementem neutralnym w grupie $G^{(1)}/\ker \chi$.

Na koniec przekonujemy się, że λ_χ jest homomorfizmem grup,

$$\begin{aligned} \lambda_\chi(g_1 \ker \chi \odot g_2 \ker \chi) &= \lambda_\chi(g_1 \cdot_{(1)} g_2 \ker \chi) = \chi(g_1 \cdot_{(1)} g_2) = \chi(g_1) \cdot_{(2)} \chi(g_2) \\ &= \lambda_\chi(g_1 \ker \chi) \cdot_{(2)} \lambda_\chi(g_2 \ker \chi). \end{aligned}$$

□

Prostą konsekwencją powyższego twierdzenia jest

Corollarium 6. Niechaj $(G, \phi_2, \phi_1, \phi_0)$ będzie grupą i przyjmijmy notację Przykł. 5 (1), Stw. 8 i 19 oraz Def. 13. Istnieje kanoniczny izomorfizm grup

$$\operatorname{Inn}(G) \cong G/\mathcal{Z}(G).$$

Dowód: Na mocy Stw. 8 oraz Przykł. 8 (4) zachodzi

$$\operatorname{im} \operatorname{Ad} = \operatorname{Inn}(G) \quad \wedge \quad \ker \operatorname{Ad} = \mathcal{Z}(G).$$

□

Pierwsze twierdzenie o izomorfizmie pozwala również dokonać kanonicznego rozkładu dowolnego homomorfizmu.

Twierdzenie 2 (O uniwersalności rzutu kanonicznego). W notacji Def. 6, 7 i 13 oraz Stw. 19 (dla $H = \ker \chi$) istnieje dokładnie jeden **monomorfizm indukowany**

$$\tilde{\chi} : G^{(1)}/\ker \chi \twoheadrightarrow G^{(2)}$$

o własności

$$(8) \quad \chi = \tilde{\chi} \circ \pi_{G^{(1)}/\ker \chi}.$$

Indukuje on – wedle Tw. 1 – izomorfizm

$$\lambda_\chi : G^{(1)}/\ker \chi \xrightarrow{\cong} \operatorname{im} \chi,$$

co pozwala rozłożyć χ w postaci

$$\chi = j_{\operatorname{im} \chi} \circ \lambda_\chi \circ \pi_{G^{(1)}/\ker \chi},$$

gdzie $j_{\operatorname{im} \chi} : \operatorname{im} \chi \hookrightarrow G^{(2)}$ jest standardowym włożeniem.

Dowód: Istnienie λ_χ jest oczywistą konsekwencją injektywności $\tilde{\chi}$ – patrz: Stw. 7. Również jednoznaczność określenia $\tilde{\chi}$ jest poza wszelką wątpliwością wobec surjektywności $\pi_{G^{(1)}/\ker \chi}$. Pozostaje zatem wykazać istnienie $\tilde{\chi}$. Postulujemy

$$\tilde{\chi} : G^{(1)}/\ker \chi \longrightarrow G^{(2)} : g \ker \chi \longmapsto \chi(g).$$

Powyższa definicja ma sens, albowiem dla innego wyboru reprezentanta $h = g \cdot_{(1)} k \in g \ker \chi$ dostajemy

$$\chi(h) = \chi(g),$$

por. (7). Ponadto, jak łatwo widać, $\tilde{\chi}$ jest homomorfizmem. Pozostaje upewnić się, że jest to odwzorowanie iniektywne, pamiętając, że $\mathbf{1}_{G^{(1)}/\ker \chi} = \ker \chi$. Zachodzi

$$\begin{aligned} \tilde{\chi}(g \ker \chi) = e^{(2)} &\iff \chi(g) = e^{(2)} \iff g \in \ker \chi \iff g \ker \chi = \ker \chi \\ &\iff \ker \tilde{\chi} = \{\ker \chi\}. \end{aligned}$$

□

Kolejnym ważnym wynikiem jest

Twierdzenie 3 (Drugie twierdzenie o izomorfizmie). Niechaj $(G, \phi_2, \phi_1, \phi_0)$ będzie grupą i niech $H, K \subset G$ noszą strukturę podgrupy G , przy czym zakładamy, że H jest normalna. Wówczas $K \cdot H \subset G$ jest podgrupą, $K \cap H \subset G$ jest podgrupą normalną, a ponadto istnieje **kanoniczny izomorfizm** grup ilorazowych

$$K \cdot H / H \cong K / (K \cap H).$$

Dowód: Sprawdźmy najpierw, że $K \cdot H$ jest podgrupą.

- (1) Niechaj $(k_1, h_1), (k_2, h_2) \in K \times H$, a wtedy – wobec $\forall_{g \in G} : gHg^{-1} = H$ – zachodzi $k_1 \cdot h_1 \cdot k_2 \cdot h_2 = (k_1 \cdot k_2) \cdot (k_2^{-1} \cdot h_1 \cdot k_2 \cdot h_2) \in K \cdot H$.
- (2) Niech teraz $(k, h) \in K \times H$. Skoro K i H są podgrupami, to także $(k^{-1}, h^{-1}) \in K \times H$, a zatem – wobec normalności H – znajdujemy $(k \cdot h)^{-1} = h^{-1} \cdot k^{-1} = k^{-1} \cdot (k \cdot h^{-1} \cdot k^{-1}) \in K \cdot H$.

W następnym kroku rozpatrujemy odwzorowanie

$$\varphi : K \longrightarrow (K \cdot H) / H : k \longmapsto (k \cdot e)H \equiv kH,$$

które jest dobrze określone, gdyż $H \equiv eH \subset K \cdot H$ jako podgrupa normalna. Łatwo widać, że φ jest homomorfizmem,

$$\varphi(k_1 \cdot k_2) = (k_1 \cdot k_2)H = k_1H \odot k_2H = \varphi(k_1) \odot \varphi(k_2),$$

a przy tym jest surjektywne, bowiem

$$g = k \cdot h \in K \cdot H \implies \varphi(k) = kH = (k \cdot h)H = gH.$$

Jądro epimorfizmu φ wyznaczamy w rachunku

$$\varphi(k) = H \iff kH = H \iff k \in H,$$

ale też $k \in K$, zatem

$$\ker \varphi = K \cap H,$$

co zarazem pokazuje, że $K \cap H$ jest podgrupą (na mocy Stw. 10). Tw. 1 odniesione do φ przesądza o istnieniu pożądanego izomorfizmu kanonicznego,

$$K / (K \cap H) \equiv K / \ker \varphi \cong \text{im } \varphi = (K \cdot H) / H.$$

□

4. ILOCZYN PÓLPROSTY GRUP W ALGEBRZE I GEOMETRII

Powyższe twierdzenie, pozornie dość abstrakcyjne, opisuje szeroką klasę fizykalnie istotnych struktur określanych mianem iloczynów (pół)prostych grup. Dla ich omówienia konieczne będzie wprowadzenie dodatkowych pojęć, które poprzedzimy uwagą o charakterze ogólnym. Będą nas otóż interesować grupy o strukturze iloczynowej

$$G = H \cdot K$$

z jednoznacznym rozkładem na czynniki (z H i K) oraz prostym prawem rozkładu dla wyniku operacji grupowej ϕ_2 . Motywacji do tego typu rozważań dostarcza intuicyjny przykład geometryczny. Oto można pokazać, że dowolny ruch euklidesowy na płaszczyźnie \mathbb{R}^2 (tj. przekształcenie płaszczyzny na siebie zachowujące odległości pitagorejskie) jest złożeniem przesunięcia T_V o pewien wektor V i obrotu R_θ o pewien kąt θ (czasem uwzględniamy jeszcze odbicia) względem wyróżnionego punktu płaszczyzny (np. tego o współrzędnych $(0,0)$),

$$\mathbb{R}^2 \longrightarrow \mathbb{R}^2 : x \longmapsto R_\theta x + V =: (T_V, R_\theta) \triangleright x.$$

Powstaje naturalne pytanie o strukturę grupy na zbiorze par (T_V, R_θ) , na które odpowiedź daje prosty rachunek⁶:

$$\begin{aligned} (T_{V_2}, R_{\theta_2}) \circ (T_{V_1}, R_{\theta_1}) \triangleright x &= (T_{V_2}, R_{\theta_2}) \triangleright (R_{\theta_1} x + V_1) = R_{\theta_2} (R_{\theta_1} x + V_1) + V_2 \\ &= R_{\theta_2} \circ R_{\theta_1} x + (R_{\theta_2} V_1 + V_2) \\ &= (T_{R_{\theta_2} V_1 + V_2}, R_{\theta_2} \circ R_{\theta_1}) \triangleright x. \end{aligned}$$

Jest zatem

$$(T_{V_2}, R_{\theta_2}) \circ (T_{V_1}, R_{\theta_1}) = (T_{R_{\theta_2} V_1 + V_2}, R_{\theta_2} \circ R_{\theta_1}).$$

Wprowadźmy oznaczenia

$$\widehat{T}_V := (T_V, R_0), \quad \widehat{R}_\theta := (T_0, R_\theta),$$

a wtedy ogólny element grupy ruchów euklidesowych zapiszemy jako iloczyn przesunięcia i obrotu,

$$g := (T_V, R_\theta) \equiv \widehat{T}_V \circ \widehat{R}_\theta.$$

Przy mnożeniu elementów grupy rozłożonych jak wyżej dostajemy

$$g_1 \circ g_2 = \widehat{T}_{V_1} \circ \widehat{R}_{\theta_1} \circ \widehat{T}_{V_2} \circ \widehat{R}_{\theta_2} = (\widehat{T}_{V_1} \circ \widehat{R}_{\theta_1} \circ \widehat{T}_{V_2} \circ \widehat{R}_{\theta_1}^{-1}) \circ (\widehat{R}_{\theta_1} \circ \widehat{R}_{\theta_2}),$$

ale też

$$\widehat{R}_\theta \circ \widehat{T}_V \circ \widehat{R}_\theta^{-1} \equiv \widehat{R}_\theta \circ \widehat{T}_V \circ \widehat{R}_{-\theta} = \widehat{T}_{R_\theta V},$$

czyli translacje tworzą podgrupę normalną grupy ruchów euklidesowych, a stąd ostatecznie

$$g_1 \circ g_2 = \widehat{T}_{V_1 + R_{\theta_1} V_2} \circ \widehat{R}_{\theta_1 + \theta_2}.$$

Tego typu struktury (tutaj: iloczyn półprosty grupy obrotów i grupy przesunięć płaszczyzny, ale też grupa Poincarégo, którą spotykamy w teorii względności!) omówimy w sposób ogólny poniżej.

Definicja 15. Niechaj $(G, \phi_2, \phi_1, \phi_0)$ będzie grupą. Podzbiory $H, K \subset G$ niosące strukturę podgrupy G określamy mianem **istotnie rozłącznych**, gdy

$$H \cap K = \{e\}.$$

Iloczyn algebraiczny (nośników) podgrup istotnie rozłącznych zapisujemy jako

$$H \bullet K$$

i określamy mianem **istotnie rozłącznego iloczynu grup** H i K . Przy tym grupa H jest nazywana **dopełnieniem** K w $H \bullet K$ i *vice versa*.

Niechaj $H \subset G$. Wówczas H jest **podgrupą z dopełnieniem**, jeśli (jest podgrupą G oraz) istnieje podgrupa $K \subset G$ spełniająca warunek $G = H \bullet K$.

⁶W istocie przemycamy tutaj strukturę modułu grupy ruchów euklidesowych na zbiorze \mathbb{R}^2 . O strukturach takich powiemy więcej już wkrótce.

O naturalności pojęcia dopełnienia w kontekście naszych rozważań przekonuje

Stwierdzenie 20. Każde dopełnienie podgrupy normalnej grupy danej jest kanonicznie izomorficzne z grupą ilorazową warstw względem tejże podgrupy (w grupie).

Dowód: W świetle Tw.3 zachodzi, dla dopełnienia K podgrupy normalnej $H \subset G$ grupy G ,

$$G/H \cong (H \bullet K)/H \cong K/(H \cap K) = K/\{e\} \cong K.$$

□

Znaczenie warunku istotnej rozłączności eksponuje

Stwierdzenie 21. Przyjmijmy notację Def.15. Wówczas

- (i) $(\forall_{g \in G} \exists!_{(h,k) \in H \times K} : g = h \cdot k) \iff G = H \bullet K.$
- (ii) $(\forall_{g \in H \cdot K} \exists!_{(h,k) \in H \times K} : g = h \cdot k) \iff H \cap K = \{e\}.$

Dowód:

Ad (i) Na to, iżby $\forall_{g \in G} \exists_{(h,k) \in H \times K} : g = h \cdot k$, potrzeba $G \subset H \cdot K$, ale $H, K \subset G$, przeto $H \cdot K \subset G$, więc ostatecznie istnienie rozkładu dla dowolnego elementu grupy G jest równoważne równości

$$G = H \cdot K.$$

Jego jednoznaczność jest treścią punktu (ii), którego dowodzimy w następnej kolejności.

Ad (ii) Niech $H \cap K = \{e\}$, a wtedy równości $h_1 \cdot k_1 = g = h_2 \cdot k_2$ zachodzące dla $(h_1, k_1), (h_2, k_2) \in H \times K$ implikują $h_2^{-1} \cdot h_1 = e = k_2 \cdot k_1^{-1}$, czyli $(h_1, k_1) = (h_2, k_2)$.

Wynikanie odwrotne udowodnimy przez sprowadzenie do niedorzeczności. Niechaj $g \in H \cap K \setminus \{e\}$. Wówczas $g \cdot e = g = e \cdot g$ ma rozkład jawnie niejednoznaczny, co jest sprzeczne z założeniem.

□

Istnienie jednoznacznego rozkładu na elementy podgrup nie określa jeszcze względnej relacji między H i K , koniecznej do zdefiniowania działania grupowego na $H \bullet K = G$. Najprostsza taka relacja to

$$\forall_{(h,k) \in H \times K} : h \cdot k = k \cdot h.$$

Pozwala ona utożsamić $G \cong H \times K$ (jako grupy). Poniżej omówimy nieco mniej restryktywną strukturę.

Definicja 16. Przyjmijmy notację Def.15. Grupa G jest (**wewnętrznym**) **iloczynem półprostym podgrup H z podgrupą K** , oznaczanym symbolem

$$G = H \rtimes K,$$

gdy jest ona istotnie rozłącznym iloczynem H i K , przy czym H jest dzielnikiem normalnym G . Wówczas H jest **dopełnieniem normalnym** K w G .

Jeśli także K jest dzielnikiem normalnym, to G nazywamy (**wewnętrznym**) **iloczynem prostym podgrup H i K** , pisząc przy tym

$$G = H \rtimes K.$$

H jest wtedy **dopełnieniem prostym** K w G (i *vice versa*).

Poszukamy obecnie naturalnych i wygodnych modeli obu zdefiniowanych powyżej struktur, przy czym będziemy abstrahować od relacji pomiędzy podgrupami H i K zapośredniczonymi przez nad-grupę G . W pierwszej kolejności zajmiemy się szczególnym przypadkiem iloczynu półprostego, jakim jest iloczyn prosty.

Stwierdzenie 22. W notacji Def. 15 i 16 istnieje kanoniczny izomorfizm

$$H \rtimes K \cong H \times K,$$

przy czym po prawej stronie mamy tu do czynienia z **zewnątrznym iloczynem prostym** grup H i K ze strukturą grupy na nośniku $H \times K$ (produkt kartezjański *zbiorów* H i K) zadaną przez operację binarną

$$\phi_2^\times : (H \times K) \times (H \times K) \longrightarrow H \times K : ((h_1, k_1), (h_2, k_2)) \longmapsto (h_1 \cdot h_2, k_1 \cdot k_2)$$

o elemencie neutralnym (e_H, e_K) oraz odwrotności

$$\phi_1^\times : H \times K \circlearrowleft : (h, k) \longmapsto (h^{-1}, k^{-1}).$$

Dowód: Rzeczony izomorfizm przyjmuje postać

$$\varepsilon : H \rtimes K \longrightarrow H \times K : h \cdot k \mapsto (h, k).$$

Jednoznaczność rozkładu w $H \rtimes K$ gwarantuje, że jest on dobrze określony, a nadto, wobec równości

$$H \cdot K \ni h \cdot (h^{-1} \cdot k \cdot h) = k \cdot h = (k \cdot h \cdot k^{-1}) \cdot k \in H \cdot K,$$

implikuje

$$\forall_{(h,k) \in H \times K} : h \cdot k = k \cdot h,$$

co oznacza, że ε jest homomorfizmem grup,

$$\begin{aligned} \varepsilon(h_1 \cdot k_1 \cdot h_2 \cdot k_2) &= \varepsilon(h_1 \cdot h_2 \cdot k_1 \cdot k_2) = (h_1 \cdot h_2, k_1 \cdot k_2) = \phi_2^\times((h_1, k_1), (h_2, k_2)) \\ &= \phi_2^\times(\varepsilon(h_1 \cdot k_1), \varepsilon(h_2 \cdot k_2)). \end{aligned}$$

Jest on jawnie surjektywny, a przy tym ma trywialne jądro,

$$\varepsilon(h \cdot k) = (e, e) \iff h = e = k \implies h \cdot k = e.$$

□

Bez trudu dowodzimy

Stwierdzenie 23. Przyjmijmy zapis jak w Stw. 22. Podzbiory $\underline{H} := H \times \{e_K\} \subset H \times K$ i $\underline{K} := \{e_H\} \times K \subset H \times K$ noszą strukturę podgrup normalnych w $H \times K$ i zachodzi

$$H \times K \cong \underline{H} \rtimes \underline{K}.$$

Struktura iloczynu prostego grup stanowi zatem banalne rozszerzenie struktury grupy na iloczyny kartezjańskie zbiorów, a każdy iloczyn prosty jest – w istocie – wewnętrzny (lub zewnętrzny – wedle gustu). O wiele ciekawszą (także z fizykalnego punktu widzenia) jest ogólniejsza struktura iloczynu półprostego, do której przejdziemy obecnie.

Stwierdzenie 24. W notacji Def. 15 i 16 oraz Stw. 8 istnieje kanoniczny izomorfizm

$$H \rtimes K \cong H \rtimes_{\widetilde{\text{Ad}}} K,$$

przy czym po prawej stronie mamy tu do czynienia z **zewnątrznym iloczynem półprostim** grup H i K stowarzyszonym z homomorfizmem grup

$$\widetilde{\text{Ad}} : K \longrightarrow \text{Aut}(H)$$

indukowanym – w świetle Stw. 8 – poprzez ograniczenie odwzorowania (3) do podgrupy $K \subset G$ w dziedzinie (w której zanurza się kanonicznie $j_K : K \longrightarrow G$) i do podgrupy *normalnej* $H \subset G$ (w której zanurza się kanonicznie $j_H : H \longrightarrow G$) jako dziedziny elementów obrazu $\mathcal{I}nn(G)$, tj. danym – dla dowolnych $(k, h) \in K \times H$ – w postaci

$$\widetilde{\text{Ad}}(k)(h) = j_H^{-1}(\text{Ad}_{j_K(k)} \circ j_H(h)),$$

ze strukturą grupy na nośniku $H \rtimes_{\widetilde{\text{Ad}}} K \equiv H \times K$ (produkt kartezjański zbiorów H i K) zadaną przez operację binarną

$$\phi_2^{\widetilde{\text{Ad}}} : (H \times K) \times (H \times K) \longrightarrow H \times K : ((h_1, k_1), (h_2, k_2)) \longmapsto (h_1 \cdot \widetilde{\text{Ad}}(k_1)(h_2), k_1 \cdot k_2)$$

o elemencie neutralnym (e_H, e_K) oraz odwrotności

$$\phi_1^{\widetilde{\text{Ad}}} : H \times K \circlearrowleft : (h, k) \longmapsto (\widetilde{\text{Ad}}(k^{-1})(h^{-1}), k^{-1}).$$

Dowód: W pierwszej kolejności należy upewnić się, że wskazane operacje określają na zbiorze $H \times K$ strukturę grupy. W tym celu porównujemy wynik

$$\begin{aligned} & \phi_2^{\widetilde{\text{Ad}}}(\phi_2^{\widetilde{\text{Ad}}}((h_1, k_1), (h_2, k_2)), (h_3, k_3)) = \phi_2^{\widetilde{\text{Ad}}}((h_1 \cdot \widetilde{\text{Ad}}(k_1)(h_2), k_1 \cdot k_2), (h_3, k_3)) \\ & = ((h_1 \cdot \widetilde{\text{Ad}}(k_1)(h_2)) \cdot \widetilde{\text{Ad}}(k_1 \cdot k_2)(h_3), (k_1 \cdot k_2) \cdot k_3) \end{aligned}$$

z wynikiem

$$\begin{aligned} & \phi_2^{\widetilde{\text{Ad}}}((h_1, k_1), \phi_2^{\widetilde{\text{Ad}}}((h_2, k_2), (h_3, k_3))) = \phi_2^{\widetilde{\text{Ad}}}((h_1, k_1), (h_2 \cdot \widetilde{\text{Ad}}(k_2)(h_3), k_2 \cdot k_3)) \\ & = (h_1 \cdot \widetilde{\text{Ad}}(k_1)(h_2 \cdot \widetilde{\text{Ad}}(k_2)(h_3)), k_1 \cdot (k_2 \cdot k_3)), \end{aligned}$$

wnioskując o ich tożsamości na podstawie założenia o łączności operacji binarnych w H i K , a nadto – na gruncie automorficzności $\widetilde{\text{Ad}}(k_1)$,

$$\widetilde{\text{Ad}}(k_1)(h_2 \cdot \widetilde{\text{Ad}}(k_2)(h_3)) = \widetilde{\text{Ad}}(k_1)(h_2) \cdot (\widetilde{\text{Ad}}(k_1) \circ \widetilde{\text{Ad}}(k_2))(h_3),$$

i homomorficzności $\widetilde{\text{Ad}}$,

$$\widetilde{\text{Ad}}(k_1 \cdot k_2) = \widetilde{\text{Ad}}(k_1) \circ \widetilde{\text{Ad}}(k_2).$$

Powyższe porównanie przesądza o łączności operacji binarnej $\phi_2^{\widetilde{\text{Ad}}}$. Ponadto mamy

$$\phi_2^{\widetilde{\text{Ad}}}((e_H, e_K), (h, k)) = (e_H \cdot \widetilde{\text{Ad}}(e_K)(h), e_K \cdot k) = (\widetilde{\text{Ad}}(e_K)(h), k) = (\text{id}_H(h), k) = (h, k),$$

znów z racji homomorficzności $\widetilde{\text{Ad}}$, a do tego

$$\phi_2^{\widetilde{\text{Ad}}}((h, k), (e_H, e_K)) = (h \cdot \widetilde{\text{Ad}}(k)(e_H), k \cdot e_K) = (h \cdot \widetilde{\text{Ad}}(k)(e_H), k) = (h \cdot e_H, k) = (h, k)$$

w konsekwencji automorficzności $\widetilde{\text{Ad}}(k)$. Istotnie przeto element (e_H, e_K) jest elementem neutralnym działania $\phi_2^{\widetilde{\text{Ad}}}$. Wreszcie też – z przyczyn j/w –

$$\begin{aligned} & \phi_2^{\widetilde{\text{Ad}}}((h, k), (\widetilde{\text{Ad}}(k^{-1})(h^{-1}), k^{-1})) = (h \cdot (\widetilde{\text{Ad}}(k) \circ \widetilde{\text{Ad}}(k^{-1}))(h^{-1}), k \cdot k^{-1}) \\ & = (h \cdot \widetilde{\text{Ad}}(k \cdot k^{-1})(h^{-1}), e_K) = (h \cdot \widetilde{\text{Ad}}(e_K)(h^{-1}), e_K) = (h \cdot h^{-1}, e_K) = (e_H, e_K) \end{aligned}$$

i analogicznie

$$\begin{aligned} & \phi_2^{\widetilde{\text{Ad}}}((\widetilde{\text{Ad}}(k^{-1})(h^{-1}), k^{-1}), (h, k)) = (\widetilde{\text{Ad}}(k^{-1})(h^{-1}) \cdot \widetilde{\text{Ad}}(k^{-1})(h), k^{-1} \cdot k) \\ & = (\widetilde{\text{Ad}}(k^{-1})(h^{-1} \cdot h), e_K) = (\widetilde{\text{Ad}}(k^{-1})(e_H), e_K) = (e_H, e_K), \end{aligned}$$

co oznacza – koniec końców, więc po wykorzystaniu wszystkich poczynionych założeń – że w istocie mamy do czynienia z grupą $(H \times K, \phi_2^{\widetilde{\text{Ad}}}, \phi_1^{\widetilde{\text{Ad}}}, \bullet \longmapsto (e_H, e_K))$.

Istotna rozłączność H i K w $H \rtimes K$ pozwala zdefiniować jawnie bijektywne odwzorowanie

$$\iota : H \rtimes K \longrightarrow H \times K : h \cdot k \longmapsto (h, k).$$

To spełnia

$$\begin{aligned} \iota((h_1 \cdot k_1) \cdot (h_2 \cdot k_2)) & \equiv \iota((h_1 \cdot (k_1 \cdot h_2 \cdot k_1^{-1})) \cdot (k_1 \cdot k_2)) \equiv (h_1 \cdot (k_1 \cdot h_2 \cdot k_1^{-1}), k_1 \cdot k_2) \\ & \equiv (h_1 \cdot \widetilde{\text{Ad}}(k_1)(h_2), k_1 \cdot k_2) \equiv \phi_2^{\widetilde{\text{Ad}}}((h_1, k_1), (h_2, k_2)) \\ & \equiv \phi_2^{\widetilde{\text{Ad}}} \circ (\iota \times \iota)(h_1 \cdot k_1, h_2 \cdot k_2), \end{aligned}$$

czyli jest homomorfizmem grup. □

Wiedzeni intuicją wyprowadzoną w przypadku iloczynu prostego grup łatwo dowodzimy

Stwierdzenie 25. Przyjmijmy zapis Def. 15 i 16 oraz Stw. 8 i . Niechaj H i K będą grupami i niech

$$\alpha : K \longrightarrow \text{Aut}(H)$$

będzie *dowolnym* homomorfizmem grup. Zbiór $H \times K$ wraz z operacjami: binarną

$$\phi_2^\alpha : (H \times K) \times (H \times K) \longrightarrow H \times K : ((h_1, k_1), (h_2, k_2)) \longmapsto (h_1 \cdot \alpha(k_1)(h_2), k_1 \cdot k_2),$$

unarną

$$\phi_1^\alpha : H \times K \circlearrowleft : (h, k) \longmapsto (\alpha(k^{-1})(h^{-1}), k^{-1})$$

oraz nularną

$$\phi_0^\alpha : \{\bullet\} \longrightarrow H \times K : \bullet \longmapsto (e_H, e_K)$$

jest grupą, określaną mianem **zewnętrznego iloczynu półprostego grup H i K stowarzyszonego z α** . Podzbiory $\underline{H} := H \times \{e_K\} \subset H \times K$ i $\underline{K} := \{e_H\} \times K \subset H \times K$ niosą strukturę podgrup w $H \rtimes_\alpha K$, przy czym pierwsza z nich jest podgrupą normalną, i zachodzi

$$H \rtimes_\alpha K \equiv \underline{H} \rtimes \underline{K}.$$

W konsekwencji powyższych rozważań możemy poddać tezę Stw. 20 sugestywnej interpretacji: Oto każda grupa zawierająca podgrupę z dopełnieniem normalnym jest kanonicznie modelowana na iloczynie półprostym (zewnętrznym) podgrupy normalnej i grupy ilorazowej przez nią wyznaczonej.

Nieoczywisty pomost pomiędzy powyższymi rozważaniami i tymi z Rozdz. 3 przerzuca

Twierdzenie 4. Niechaj H, K i G będą grupami. Grupa G jest izomorficzna z zewnętrznym iloczynem półprostym $H \rtimes_\alpha K$ stowarzyszonego z pewnym homomorfizmem $\alpha : K \longrightarrow \text{Aut}(H)$ wtedy i tylko wtedy, gdy grupy H, K i G są w relacji opisywanej przez krótki ciąg dokładny grup

$$\mathbf{1} \longrightarrow H \xrightarrow{j} G \xrightarrow{\pi} K \longrightarrow \mathbf{1},$$

w którym epimorfizm π **rozszczenia się**, tj. istnieje homomorfizm grup

$$\sigma : K \longrightarrow G$$

o własności

$$\pi \circ \sigma = \text{id}_K.$$

Homomorfizm o tej własności nazywamy **cięciem** π .

Przy tym $\alpha = \text{id}_H$ (homomorfizm stały, określający na $H \times K$ strukturę iloczynu prostego) zachodzi wtedy i tylko wtedy, gdy

$$[j(H), \sigma(K)] = \{e_G\}.$$

Przykłady 14.

- (1) $O(2, \mathbb{R}) = \text{SO}(2, \mathbb{R}) \rtimes \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\} \cong \text{SO}(2, \mathbb{R}) \rtimes \mathbb{Z}/2\mathbb{Z}$.
- (2) Dla dowolnego zbioru $X \ni \{x_0, y_0\}$, $x_0 \neq y_0$ mamy równość

$$\mathfrak{S}_X = \mathfrak{A}_X \rtimes \{\text{id}_X, \tau_{x_0, y_0}\},$$

słuszną dla dowolnego wyboru elementów x_0 i $y_0 \neq x_0$. Przykład ten ilustruje następującą tezę: Dopełnienie podgrupy – o ile istnieje – nie jest w ogólności dane jednoznacznie.

- (3) **Grupa dwuścienna** (albo **diedralna**) rzędu $2n$, czyli grupa symetrii n -kąta foremnego na płaszczyźnie $\mathbb{R}^2 \equiv \mathbb{C}$, o środku symetrii w punkcie o współrzędnych $(0, 0)$ i wierzchołkach w punktach o współrzędnych $(x_k, y_k) \in \sqrt[n]{1}$, $k \in \overline{0, n-1}$. Grupa ta jest generowana przez obrót R_{θ_n} o kąt $\theta_n := \frac{2\pi}{n}$ wokół punktu o współrzędnych $(0, 0)$, pod wpływem którego współrzędne punktu wielokąta $z = (x, y)$ transformują się wedle przepisu

$$R_{\theta_n} \triangleright (x, y) = e^{i\theta_n} \cdot (x, y),$$

oraz przez odbicie P_{OX} względem prostej $\text{Im}(z) = 0$,

$$P_{OX} \triangleright (x, y) = \overline{(x, y)} = (x, -y).$$

Oczywiście odbicie to nie jest obrotem, mamy zatem rozkład

$$D_{2n} = \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} = \left\langle R_{\frac{2\pi}{n}} \right\rangle \rtimes \langle P_{OX} \rangle,$$

z prawem komutacji dla generatorów

$$P_{OX} \circ R_{\frac{2\pi}{n}} \circ P_{OX}^{-1} = R_{-\frac{2\pi}{n}} \equiv R_{\frac{2\pi}{n}}^{-1}.$$

Opisana grupa odgrywa, wspólnie z grupą cykliczną, podstawową rolę w klasyfikacji siatek krystalograficznych w dwóch wymiarach (w większej liczbie wymiarów pojawiają się jako grupy symetrii dodatkowe grupy skończone), patrz: [DNF79, Rozdz. 3 § 20]. Symetrie kryształów rzeczywistych współokreślają ich własności fizyczne i chemiczne.

- (4) Prostych, lecz zarazem pobudzających wyobraźnię przykładów iloczynów półprostych grup dostarcza niskowymiarowa topologia, z którą zetknęliśmy się w Przykł. 5 (7) pod postacią grupy podstawowej przestrzeni topologicznej. Przyjrzymy się strukturze tej grupy w przypadku dwóch powierzchni 2-wymiarowych: 2-torusa i butelki Kleina, por. [DNF84, Rozdz. 1 § 3]. Pierwszą z nich możemy przedstawić jako wynik utożsamienia punktów (oznaczane symbolem \sim_T) na brzegu kwadratu $I \times I \equiv [0, 1] \times [0, 1]$ według przepisu

$$\mathbb{T}^2 := I^{\times 2} / \sim_T \quad \forall_{s,t \in I} : ((s, 0) \sim_T (s, 1) \quad \wedge \quad (0, t) \sim_T (1, t)).$$

Łatwo się przekonać (używając w tym celu kartki papieru), że ten przepis w istocie zadaje znany kształt torusa zanurzonego w \mathbb{R}^3 . W przypadku butelki Kleina ogólna zasada jest ta sama, jednak konkretny przepis na utożsamienie punktów na brzegu kwadratu (oznaczane symbolem \sim_B),

$$\mathbb{K}\mathbb{B} := I^{\times 2} / \sim_B \quad \forall_{s,t \in I} : ((s, 0) \sim_B (s, 1) \quad \wedge \quad (0, t) \sim_B (1, 1-t)),$$

jest jakościowo na tyle złożony, że nie dopuszcza realizacji (przez tzw. zanurzenie – patrz: kurs analizy matematycznej na 3. semestrze) w postaci powierzchni w \mathbb{R}^3 bez samoprzecięć. Bez trudu identyfikujemy generatory grupy podstawowej o bazie np. w punkcie o współrzędnych $x_* := (0, 0)$ – w obu przypadkach są to klasy homotopii pętli biegnących wzdłuż krawędzi kwadratu, które łączą się w tym wierzchołku. Oznaczmy je, odpowiednio, jako

$$a : I \longrightarrow I^{\times 2} : t \longmapsto (t, 0),$$

$$b : I \longrightarrow I^{\times 2} : t \longmapsto (0, t).$$

Zachodzą oczywiste tożsamości:

$$\langle [a]_{\sim} \rangle \cong \mathbb{Z} \cong \langle [b]_{\sim} \rangle$$

(każdą z „dziur” w powierzchni trzeba obejść całkowitą liczbę razy, aby powrócić do punktu wyjścia). Pozostaje określić strukturę algebraiczną na zbiorze par $([a^m]_{\sim}, [b^n]_{\sim})$, które koduje relacja przemienności spełniana przez parę generatorów $([a]_{\sim}, [b]_{\sim})$. Jej wyprowadzenie w przyjętym modelu obu powierzchni jest banalne, oto bowiem wystarczy homotopijnie ściągnąć na okrąg $b(I)$ (poprzez pozbawione „dziur”, czyli jednospójne wnętrza $I^{\times 2}$) pętlę biegnącą od $(0, 0)$ wzdłuż $a(I)$ (w kierunku wzrostu wartości parametru t) do $(1, 0)$, a dalej wzdłuż $b(I)$ (w kierunku zgodnym z kierunkiem wzrostu wartości parametru t na torusie i przeciwnym do tego kierunku na butelce Kleina) do $(1, 1)$ i na koniec wzdłuż $a(I)$ (w kierunku przeciwnym do kierunku wzrostu wartości parametru t) do $(0, 1) \sim_X (0, 0)$, $X \in \{\mathbb{T}^2, \mathbb{K}\mathbb{B}\}$. Otrzymujemy w ten sposób następującą relację

$$[a \circ b \circ \bar{a}]_{\sim} = [b]_{\sim} \quad \iff \quad [a]_{\sim} * [b]_{\sim} * \text{Inv}([a]_{\sim}) = [b]_{\sim}$$

$$(9) \quad \iff \quad [a]_{\sim} * [b]_{\sim} = [b]_{\sim} * [a]_{\sim}$$

dla torusa i analogiczną relację

$$(10) \quad \begin{aligned} [a \circ \bar{b} \circ \bar{a}]_{\sim} = [b]_{\sim} &\iff [a]_{\sim} \star \text{Inv}([b]_{\sim}) \star \text{Inv}([a]_{\sim}) = [b]_{\sim} \\ &\iff \text{Inv}([a]_{\sim}) \star [b]_{\sim} \star [a]_{\sim} = \text{Inv}([b]_{\sim}) \end{aligned}$$

dla butelki Kleina. *A priori* nie można wykluczyć pojawienia się dalszych relacji między generatorami a i b , łatwo jednak przekonujemy się, że żadne dodatkowe nietrywialne relacje pojawić się nie mogą. Istotnie, każdą taką relację można sprowadzić do postaci

$$(11) \quad \prod_{k=1}^N ([a]_{\sim}^{m_k} \cdot [b]_{\sim}^{n_k}) = [\varepsilon_{x^*}]_{\sim}$$

dla pewnych $m_k, n_k \in \mathbb{Z}$. Uwzględniając relacje przemienności dla elementów $a^m \in \langle a \rangle$, $m \in \mathbb{Z}$ i $b^n \in \langle b \rangle$, $n \in \mathbb{Z}$ implikowane przez (9),

$$a^m \cdot b^n = b^n \cdot a^m,$$

oraz – odpowiednio – 10

$$a^m \cdot b^n = b^{(-1)^{m-1}n} \cdot a^m,$$

bez trudu przepisujemy relację (11) w postaci

$$[a]_{\sim}^{\sum_{k=1}^N m_k} \cdot [b]_{\sim}^{\tilde{n}(m_k, n_k)} = [\varepsilon_{x^*}]_{\sim} \iff [a]_{\sim}^{\sum_{k=1}^N m_k} = [b]_{\sim}^{-\tilde{n}(m_k, n_k)},$$

przy czym zależność wypadkowego wykładnika $\tilde{n}(m_k, n_k) \in \mathbb{Z}$ od m_k i n_k daje się prosto wyznaczyć. Rzut oka na obie geometrie przekonuje, że powyższa relacja może być spełniona (tożsamościowo) przy

$$\sum_{k=1}^N m_k = 0 = \tilde{n}(m_k, n_k).$$

Z naszej analizy wynika jasno, że o ile w przypadku torusa mamy do czynienia z iloczynem prostym podgrup generowanych przez obie klasy homotopii pętli,

$$\pi_1(\mathbb{T}^2, x_*) = \langle [b]_{\sim} \rangle \rtimes \langle [a]_{\sim} \rangle \cong \mathbb{Z} \rtimes \mathbb{Z},$$

o tyle w przypadku butelki Kleina grupa podstawowa ma strukturę nietrywialnego iloczynu półprostego,

$$\pi_1(\mathbb{KB}, x_*) = \langle [b]_{\sim} \rangle \rtimes \langle [a]_{\sim} \rangle \cong \mathbb{Z} \rtimes \mathbb{Z}.$$

LITERATURA

- [Die65] J. Dieudonné, *Éléments d'analyse*, vol. 1, Gauthier–Villars, 1965.
- [Die68] ———, *Éléments d'analyse*, vol. 2, Gauthier–Villars, 1968.
- [DNF79] B.A. Dubrovin, S.P. Novikov, and A.T. Fomenko, *Sovremennaja geometrija: Metody i priloženija. Tom 1: Geometrija poverkhnostej, grup preobrazowanij i polej*, Nauka, 1979.
- [DNF84] ———, *Sovremennaja geometrija: Metody i priloženija. Tom 3: Teorija gomologij*, Nauka, 1984.
- [KT08] C. Kassel and V.G. Turaev, *Braid Groups*, Graduate Texts in Mathematics, vol. 247, Springer, 2008.
- [Lee11] J.M. Lee, *Introduction to Topological Manifolds*, Graduate Texts in Mathematics, vol. 202, Springer, 2011.
- [Mau91] K. Maurin, *Analiza. Część I. Elementy*, Biblioteka Matematyczna, vol. 69, Państwowe Wydawnictwo Naukowe, 1991.
- [PS97] V.V. Prasolov and A.B. Sossinsky, *Knots, Links, Braids and 3-Manifolds: An Introduction to the New Invariants in Low-Dimensional Topology*, Translations of Mathematical Monographs, vol. 154, American Mathematical Society, 1997.
- [Tur94] V.G. Turaev, *Quantum Invariants of Knots and 3-Manifolds*, de Gruyter Studies in Mathematics, vol. 18, Walter de Gruyter, 1994.

ZADANIA DOMOWE I NA ĆWICZENIA

Zadanie domowe 1. Udowodnij Stw. 1.

Zadanie domowe 2. Przekonaj się o prawdziwości stwierdzeń dot. grupy homografii wypisanych w Przykł. 5 (4) (ustal jawną postać operacji binarnej, unarnej i nularnej na $\text{Hom}(\overline{\mathbb{C}})$; sprawdź, że wskazane szczególne homografie tworzą układ generujący – czy rozkład homografii na ich superpozycję jest jednoznaczny?). Przeanalizuj własności teoriogrupowe przyporządkowania $h \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{C}(2)$ (jądro, obraz *etc.*), patrz: Przykł. 3 (4).

Zadanie domowe 3. Udowodnij Stw. 5.

Zadanie domowe 4. Udowodnij Stw. 8.

Zadanie domowe 5. Używając odwrotnego algorytmu Euklidesa pokaż, że zbiór $\mathbb{Z}_p = \{[k]_p \mid k \in \overline{0, p-1}\}$ reszt modulo tworzy ciało, ilekroć $p \in \mathbb{N}^\times$ jest pierwsza.

Zadanie domowe 6. Niechaj $(\mathbb{K}, +, \cdot, -(\cdot), (\cdot)^{-1}, \bullet \mapsto 0, \bullet \mapsto 1)$ będzie ciałem. Rozważmy zbiory: $\mathbb{K}^\times := \mathbb{K} \setminus \{0\}$ i $\mathbb{K}^* := \mathbb{K} \setminus \{1\}$. Udowodnij, że pierwszy z nich z (ograniczeniem) mnożenia \cdot na \mathbb{K} jest grupą przemienną, drugi zaś staje się taką grupą, gdy wyposażyć go w operację binarną $\mu : \mathbb{K}^* \times \mathbb{K}^* \rightarrow \mathbb{K}^* : (k, l) \mapsto k + l - k \cdot l$ (w szczególności należy sprawdzić, że operacja ta jest dobrze określona). Wskaż izomorfizm pomiędzy tymi dwiema grupami.

Zadanie domowe 7. Dowiedz prostoty grupy z Przykł. 11.

Zadanie domowe 8. Udowodnij Stw. 23.

Zadanie domowe 9. Udowodnij Stw. 25.

Zadanie domowe 10. Udowodnij Tw. 4.

Zadanie domowe 11. Udowodnij

Twierdzenie 5 (Grupa symetryczna w terminach generatorów i relacji). Przyjmijmy notację Def. 3 i 6 oraz Przykł. 4 (1). Ustalmy $n \in \mathbb{N} \setminus \{0\}$ i niechaj $(G_n, \cdot, (\cdot)^{-1}, \bullet \mapsto e)$ będzie grupą generowaną przez rodzinę $\{g_i\}_{i \in \overline{1, n-1}}$ swoich elementów,

$$G_n = \langle g_1, g_2, \dots, g_{n-1} \rangle,$$

spełniających następujący zupełny układ relacji, wypisanych dla dowolnych indeksów $i, j \in \overline{1, n-1}$,

$$g_i^2 = e,$$

$$|i - j| = 1 \implies (g_i \cdot g_j)^3 = e,$$

$$|i - j| \geq 2 \implies (g_i \cdot g_j)^2 = e.$$

Wówczas istnieje jedyny homomorfizm grup

$$\chi : G_n \longrightarrow \mathfrak{S}_n$$

o własności

$$\forall_{i \in \overline{1, n-1}} : \chi(g_i) = \tau_i,$$

gdzie $\tau_i \equiv (i, i + 1)$ jest transpozycją o nośniku $\{i, i + 1\}$. Homomorfizm ten jest izomorfizmem.

Zadanie domowe 12. (dodatkowe) Udowodnij

Stwierdzenie 26 (Lemat o Pięciu (Morfizmach)). Niechaj

$$\dots \longrightarrow G_1 \xrightarrow{\gamma_1} G_2 \xrightarrow{\gamma_2} G_3 \xrightarrow{\gamma_3} G_4 \xrightarrow{\gamma_4} G_5 \longrightarrow \dots$$

i

$$\dots \longrightarrow H_1 \xrightarrow{\eta_1} H_2 \xrightarrow{\eta_2} H_3 \xrightarrow{\eta_3} H_4 \xrightarrow{\eta_4} H_5 \longrightarrow \dots$$

będą dwoma ciągami dokładnymi grup przemiennych. Dla dowolnego diagramu *przemiennego*

$$\begin{array}{ccccccccccc}
 \dots & \longrightarrow & G_1 & \xrightarrow{\gamma_1} & G_2 & \xrightarrow{\gamma_2} & G_3 & \xrightarrow{\gamma_3} & G_4 & \xrightarrow{\gamma_4} & G_5 & \longrightarrow & \dots \\
 & & \downarrow \chi_1 & & \downarrow \chi_2 & & \downarrow \chi_3 & & \downarrow \chi_4 & & \downarrow \chi_5 & & \\
 \dots & \longrightarrow & H_1 & \xrightarrow{\eta_1} & H_2 & \xrightarrow{\eta_2} & H_3 & \xrightarrow{\eta_3} & H_4 & \xrightarrow{\eta_4} & H_5 & \longrightarrow & \dots
 \end{array} ,$$

w którym $\gamma_i, i \in \{1, 2, 3, 4, 5\}$ są homomorfizmami grup przemiennych, zachodzą implikacje:

- (i) χ_1 jest epimorfizmem i χ_2 oraz χ_4 są monomorfizmami $\implies \chi_3$ jest monomorfizmem;
- (ii) χ_5 jest monomorfizmem i χ_2 oraz χ_4 są epimorfizmami $\implies \chi_3$ jest epimorfizmem;
- (iii) $\chi_j, j \in \{1, 2, 4, 5\}$ są izomorfizmami $\implies \chi_3$ jest izomorfizmem.

Zadanie domowe 13. (dodatkowe) Przeliczalną rodzinę grup przemiennych $C_\bullet \equiv \{C_n\}_{n \in \mathbb{Z}}$ wraz z homomorfizmami grup przemiennych opisanymi diagramem

$$\dots \longrightarrow C_1 \xrightarrow{d_1} C_2 \xrightarrow{d_2} C_3 \xrightarrow{d_3} C_4 \xrightarrow{d_4} C_5 \longrightarrow \dots$$

o własności

$$\ker d_{n+1} \supset \operatorname{im} d_n, \quad n \in \mathbb{Z}$$

określamy mianem **kompleksu kółanuchów** o **operatorach kobrzegu** $d_\bullet \equiv \{d_n\}_{n \in \mathbb{Z}}$. **Kohomologia** kompleksu (C_\bullet, d_\bullet) to suma prosta grup przemiennych

$$H^\bullet(C_\bullet, d_\bullet) := \bigoplus_{n \in \mathbb{Z}} H^n(C_\bullet, d_\bullet)$$

o składowych

$$H^n(C_\bullet, d_\bullet) = \ker d_n / \operatorname{im} d_{n-1}.$$

Składowa $H^n(C_\bullet, d_\bullet)$ jest przy tym określana mianem *n-tej grupy kohomologii kompleksu* (C_\bullet, d_\bullet) . Jej elementy zwyczajowo zapisujemy w postaci

$$[c] \equiv c + \operatorname{im} d_{n-1}.$$

Udowodnij (w szczególności określoność wszystkich wskazanych w treści odwzorowań i ich homomorficzny charakter, a także – dokładność ciągu w kohomologii w każdym z jego wierzchołków)

Twierdzenie 6 (O homomorfizmie łączącym). Niechaj $(C_\bullet^i, d_\bullet^i), i \in \{1, 2, 3\}$ będą trzema kompleksami kółanuchów, dla których dany jest krótki ciąg dokładny

$$\{1\}_{n \in \mathbb{Z}} \longrightarrow C_\bullet^1 \xrightarrow{x_\bullet^1} C_\bullet^2 \xrightarrow{x_\bullet^2} C_\bullet^3 \longrightarrow \{1\}_{n \in \mathbb{Z}},$$

o składowych

$$\mathbf{1} \longrightarrow C_n^1 \xrightarrow{x_n^1} C_n^2 \xrightarrow{x_n^2} C_n^3 \longrightarrow \mathbf{1},$$

które czynią przemianym każdy z (pod)diagramów

$$\begin{array}{ccccccc}
 \mathbf{1} & \longrightarrow & \vdots & & \vdots & & \vdots \longrightarrow \mathbf{1} \\
 & & \downarrow d_{n-1}^1 & & \downarrow d_{n-1}^2 & & \downarrow d_{n-1}^3 \\
 \mathbf{1} & \longrightarrow & C_n^1 & \xrightarrow{\chi_n^1} & C_n^2 & \xrightarrow{\chi_n^2} & C_n^3 \longrightarrow \mathbf{1} \\
 & & \downarrow d_n^1 & & \downarrow d_n^2 & & \downarrow d_n^3 \\
 \mathbf{1} & \longrightarrow & C_{n+1}^1 & \xrightarrow{\chi_{n+1}^1} & C_{n+1}^2 & \xrightarrow{\chi_{n+1}^2} & C_{n+1}^3 \longrightarrow \mathbf{1} \\
 & & \downarrow d_{n+1}^1 & & \downarrow d_{n+1}^2 & & \downarrow d_{n+1}^3 \\
 \mathbf{1} & \longrightarrow & \vdots & & \vdots & & \vdots \longrightarrow \mathbf{1}
 \end{array}$$

Powyższy krótki ciąg dokładny kanonicznie indukuje (**długi**) **ciąg dokładny w kohomologii**

$$\dots \xrightarrow{\chi_{n-1}^2} H^n(C_\bullet^3, d_\bullet^3) \xrightarrow{\beta_{n-1}} H^n(C_\bullet^1, d_\bullet^1) \xrightarrow{\chi_{n*}^1} H^n(C_\bullet^2, d_\bullet^2) \xrightarrow{\chi_{n*}^2} H^n(C_\bullet^3, d_\bullet^3) \xrightarrow{\beta_n} H^{n+1}(C_\bullet^1, d_\bullet^1) \xrightarrow{\chi_{n+1*}^1} H^{n+1}(C_\bullet^2, d_\bullet^2) \xrightarrow{\chi_{n+1*}^2} \dots,$$

w którego zapisie

$$\chi_{n*}^A : H^n(C_\bullet^A, d_\bullet^A) \longrightarrow H^n(C_\bullet^{A+1}, d_\bullet^{A+1}) : [c] \longmapsto [\chi_n^A(c)], \quad A \in \{1, 2\},$$

a

$$\beta_n : H^n(C_\bullet^3, d_\bullet^3) \longrightarrow H^{n+1}(C_\bullet^1, d_\bullet^1)$$

są tzw. **homomorfizmami łączącymi** określonymi, jak następuje: Niechaj $c \in C_n^3$ będzie kołańcuchem **zamkniętym**, tj. $d_n^3 c = 0$. Wówczas **kobrzeg** $d_n^2 b$ jego przeciwobrazu $b \in C_n^2$ względem χ_n^2 należy do jądra χ_{n+1}^2 , zatem wyznacza kołańcuch $a \in C_{n+1}^1$ spełniający równość $\chi_{n+1}^1(a) = d_n^2 b$. Kołańcuch ten jest zamknięty, $d_{n+1}^1 a = 0$, zatem można zdefiniować

$$\beta_n([c]) := [a].$$