

**ALGEBRA IR – WYKŁADY IV, V, VI, VII I VIII (24. I 31. PAŹDZIERNIKA
ORAZ 7., 14. I 21. LISTOPADA 2012 R.)**

RAFAL R. SUSZEK (KMMF)

4. GRUPY – STRUKTURY OGÓLNE

Po szczegółowym omówieniu dwóch struktur pierścieniopodobnych, tj. ciała (na przykładzie ciała liczb zespolonych) oraz pierścienia (na przykładzie pierścienia wielomianów o współczynnikach z ciała), przechodzimy do dyskusji grup. Fundamentalne znaczenie tych struktur w rygorystycznym opisie przyrody – począwszy od krystalografii, 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 fizyczne – pozostaje poza wszelką wątpliwością. Szczególną rolę odgrywa przy tym teoria reprezentacji grup, czy ogólniej – teoria działania grup na zbiorach, o której więcej powiemy w dziale 4.

Zacznijmy od rozpisania i rozszerzenia definicji grupy.

Definicja 19. Grupa to czwórka $(G, \phi_2, \phi_1, \phi_0)$, w której

- G jest zbiorem;
- $\phi_2 : G^{\times 2} \rightarrow G$ jest operacją 2-argumentową zwaną **działaniem grupowym**;
- $\phi_1 : G \hookrightarrow G$ 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)

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

(G2) (istnienie elementu neutralnego względem działania grupowego)

$$\begin{array}{ccc} G \times \{\bullet\} & \xrightarrow{\text{id}_G \times \phi_0} & G \times G \\ \text{pr}_1 \searrow & & \downarrow \phi_2 \\ & & G \end{array} \quad , \quad \begin{array}{ccc} \{\bullet\} \times G & \xrightarrow{\phi_0 \times \text{id}_G} & G \times G \\ \text{pr}_2 \searrow & & \downarrow \phi_2 \\ & & G \end{array} \quad \equiv \quad \forall_{g \in G} : \phi_2(g,e) = g = \phi_2(e,g) ;$$

(G3) (fundamentalna własność ϕ_1)

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

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

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

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

Grupa przemienna (zwana też **abelową**) to taka, w której działanie grupowe jest przemienne, co wyraża diagram przemienny

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

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

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

Przykład(y) 12.

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

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

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

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

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

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

- (5) 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. ciągłe odwzorowania¹

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

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**

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

¹Pojęcie ciągłości jest dyskutowane na kursie analizy matematycznej, patrz, np., [Mau91, Rozdz. II § 7] i [Die65, Rozdz. II.11].

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

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 intuicją geometryczną – 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

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

Twierdzącą (i konstruktywną) odpowiedź 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

$$H : I^2 \rightarrow X$$

o własnościach

$$\forall s, t \in I : (H(s, 0) = \gamma_1(s) \quad \wedge \quad H(s, 1) = \gamma_2(s) \quad \wedge \quad H(0, t) = x_* = H(1, t)) .$$

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

$$\star : \Omega(X; x_*)/\sim \times \Omega(X; x_*)/\sim \rightarrow \Omega(X; x_*)/\sim : ([\gamma_1]_\sim, [\gamma_2]_\sim) \mapsto [\gamma_1 \circ \gamma_2]_\sim$$

oraz branie odwrotności

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

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

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

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 fizykalnym znaczeniu tej ostatniej przekonuje nas, m.in., mechanika kwantowa cząstek naładowanych (patrz i pytaj o efekt Aharonowa–Bohma).

(6) Grupa warkoczy o n pasmach.

Notacja 3. O ile nie będzie to prowadziło do nieporozumień, będziemy czasem używać pojęcia „grupa” w odniesieniu do zbioru będącego nośnikiem tej struktury.

Dwa najbardziej popularne zapisy dla grup to

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

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

o oczywistych własnościach:

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

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

$$\forall n \in \mathbb{N} \setminus \{0\} \quad \forall g \in G : ng := \underbrace{g + g + \dots + g}_{n \text{ razy}} \quad \wedge \quad -ng := \underbrace{(-g) + (-g) + \dots + (-g)}_{n \text{ razy}}, \quad \forall g \in G : 0g := \mathbf{0}, \quad (4.1)$$

o oczywistych własnościach:

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

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

✓

Stwierdzenie 13. W dowolnej grupie element neutralny oraz element odwrotny do danego są określone jednoznacznie.

Stwierdzenie 14. Niechaj $(G, \phi_2 = \cdot)$ będzie półgrupą jak w Def. 4 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 15. W notacji (mnożeniowej) Def. 19 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. 14), co w świetle Stw. 13 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. 13.

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

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

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

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

Przykład(y) 13.

- (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 udowodnimy w dziale 5.

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

Definicja 21. W notacji Def. 19 **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:

(PG1) $\phi_2 : H^{\times 2} \longrightarrow H \subset G$;

(PG2) $\phi_1 : H \longrightarrow H \subset G$.

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

Przykład(y) 14.

(1) Grupa $(\sqrt[n]{1}, \cdot, \bar{\cdot}, (1, 0))$ pierwiastków stopnia $n \in \mathbb{N} \setminus \{0\}$ jest podgrupą grupy $(U(1), \cdot, \bar{\cdot}, (1, 0))$.

(2) **Grupa ortogonalna stopnia 2 nad $\mathbb{R}$** o nośniku

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

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, jest podgrupą tejże.

(3) Podgrupy grupy homografii 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 generuje grupę homografii uzwarconej płaszczyzny zespolonej.

(4) 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 $(\mathbb{R}_{>0}, \cdot)$.

(5) 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 **pochoďnej**) grupy G . Jasnym jest, że grupa G jest przemienna, gdy jej komutant jest trywialny. Przykładem komutanta jest **grupa alternująca** na zbiorze X ,

$$\mathfrak{A}_X := [\mathfrak{S}_X, \mathfrak{S}_X].$$

W dziale 5 zapoznamy się z alternatywną definicją tej podgrupy, wysłowioną w terminach znaku tworzących ją permutacji.

Stwierdzenie 16. *Każda podgrupa grupy danej jest grupą.*

Użyteczne własności podgrup zbiera

Stwierdzenie 17. *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) $(A \cap B = A \cap C \quad \wedge \quad A \cdot B = A \cdot C) \implies B = C$.

Dowód: Na ćwiczeniach. □

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

Definicja 22. Niechaj $(G^{(\alpha)}, \phi_2^{(\alpha)}, \phi_1^{(\alpha)}, \phi_0^{(\alpha)})$, $\alpha \in \{1, 2\}$ będą grupami. **Homomorfizm** $G^{(1)}$ w $G^{(2)}$ to odwzorowanie $\chi : G^{(1)} \rightarrow G^{(2)}$ o własności wyrażonej przez diagram przemienny

$$\begin{array}{ccc} G^{(1)} \times G^{(1)} & \xrightarrow{\phi_2^{(1)}} & G^{(1)} \\ \chi \times \chi \downarrow & & \downarrow \chi \\ G^{(2)} \times G^{(2)} & \xrightarrow{\phi_2^{(2)}} & G^{(2)} \end{array} . \quad (\text{HM})$$

Jak poprzednio w oczywisty sposób wyróżniamy

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

Przykład(y) 15.

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

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

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 18. W notacji Def. 22 poniższe diagramy są przemiennie:

(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

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

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. 13 daje tezę.

□

Szczególny typ homomorfizmów grup opisuje

Stwierdzenie 19. 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

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

jest epimorfizmem grup.

Mamy oczywiste

Stwierdzenie 20. Grupa automorfizmów wewnętrznych grupy przemiennej jest trywialna.

Przykład(y) 16.

(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 23. W notacji Def. 22 **jądro homomorfizmu** to podzbiór

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

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 21. W notacji Def. 22 i 23 $\text{Ker } \chi$ jest podgrupą $G^{(1)}$.

Dowód:

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

□

Stwierdzenie 22. W notacji Def. 22 i 23 $\text{Im } \chi$ 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) $g \in \text{Im } \chi \iff \exists_{a \in G^{(1)}} : g = \chi(a) \implies \text{Inv}^{(2)}(g) = \text{Inv}^{(2)}(\chi(a)) = \chi(\text{Inv}^{(1)}(a)) \in \text{Im } \chi.$

□

Przykład(y) 17.

- (1) Jądrem epimorfizmu z przykładu 15 (2) jest **grupa specjalna ortogonalna stopnia 2 nad $\mathbb{R}$** , o nośniku dopuszczającym 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 15 (6) jest podgrupa $\text{U}(1) \subset \mathbb{C}^\times$.
- (3) Jądrem epimorfizmu $e^{i\lambda \cdot}$, $\lambda \in \mathbb{R}^\times$ jest podgrupa $\frac{2\pi}{\lambda} \mathbb{Z} \subset \mathbb{R}$.
- (4) Jądrem epimorfizmu Ad ze Stw. 19 jest podgrupa $\mathcal{Z}(G) \subset G$.

Przyjrzymy się bliżej jądro homomorfizmu.

Stwierdzenie 23. W notacji Def. 22 i 23 χ jest monomorfizmem $\iff \text{Ker } \chi = \{e^{(1)}\}$.

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 $\text{Ker } \chi$ to implikuje $g \cdot_{(1)} \text{Inv}^{(1)}(h) = e^{(1)}$, czyli $g = h$.

□

Przypomnijmy następujące pojęcie znane z kursu analizy matematycznej.

Definicja 24. Niechaj X, Y będą zbiorami i niech będzie dane odwzorowanie $f : X \longrightarrow Y$. **Pozio-**
mica (albo **przeciwobraz**) **podzbioru** $Z \subset f(X)$ **względem** f to podzbiór

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

Stwierdzenie 24. W notacji Def. 22, 23 i 24

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

Odpowiedzi na pytanie o postać pozostałych poziomów dostarcza

Stwierdzenie 25. W notacji Def. 22, 23 oraz 24 i dla dowolnego $g \in G^{(1)}$ słuszną jest formuła

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

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

Powyższa analiza dopuszcza następujące uogólnienie.

Definicja 25. W notacji Def. 21 **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 26. W notacji Def. 21 i 25 zachodzi

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

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

Dowód: Pożądana bijekcja to

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

$\square$

Definicja 26. W notacji Def. 25 **indeksem (lewostronnym) podgrupy H w grupie G** nazywamy moc zbioru warstw (lewostronnych) względem H w G ,

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

Stwierdzenie 27. W notacji Def. 21 i 25 relacja na G zadana, jak następuje:

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

jest relacją równoważności.

Dowód:

- (1) Na mocy Stw. 16 $e \in H$, 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. 16 $h \in H \implies h^{-1} \in H$, co w sumie oznacza, że $b \in aH$, czyli $b \sim_H a$.
- (3) $a \sim_H b \wedge b \sim_H c \iff \exists_{h_1, h_2 \in H} : (a = b \cdot h_1 \wedge b = c \cdot h_2) \implies a = c \cdot (h_1 \cdot h_2) \in cH \iff a \sim_H c.$

$\square$

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

Przykład(y) 18.

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

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

- (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) (nietożsamy) elementów X jest wybrana dowolnie.

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

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

- (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 $(+\mathbb{C}, -(\cdot), \bullet \mapsto (0, 0))$. 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

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

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

Corollarium 2. (Twierdzenie Lagrange’a) *Przyjmijmy notację Def. 19 i 21. 26. Wówczas zachodzi tożsamość*

$$|G| = |H| \cdot (G : H) . \quad (4.2)$$

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

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

Stwierdzenie 28. *W notacji Def. 21, 22, 23 i 25 zachodzi*

$$\forall_{g \in G(1)} : g \text{Ker } \chi = \text{Ker } \chi g ,$$

albo – równoważnie –

$$\forall_{g \in G(1)} : g \text{Ker } \chi g^{-1} = \text{Ker } \chi .$$

Definicja 27. W notacji Def. 21 i 25 **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}) –

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

Przykład(y) 19.

- (1) Dla dowolnej liczby $n \in \mathbb{N}$ 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 $\text{Inn}(G) \subset \text{Aut}(G)$ automorfizmów wewnętrznych dowolnej grupy G . Wynika to z oczywistej tożsamości

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

Prawdziwe jest ogólne

Stwierdzenie 29. *Każda podgrupa grupy przemiennej jest normalna.*

Dyskusja istnienia dzielników normalnych grupy danej prowadzi do naturalnej

Definicja 28. **Grupa prosta** to taka, która nie posiada podgrup normalnych właściwych i nietrywialnych, tj. różnych od całej grupy i od podgrupy trywialnej.

Przykład(y) 20. Grupa alternująca na zbiorze X o mocy $|X| \neq 4$. (Dowód na ćwiczeniach.)

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

Stwierdzenie 30. W notacji Def. 21, 25 i 27 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)

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

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

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

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 $\odot$ 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 29. W notacji Def. 21 i 25 oraz Stw. 30 **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

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

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

Przykład(y) 21.

- (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 adekwatnie² – **grupą klas automorfizmów**)

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

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

$$\text{Ker } \pi_{G/H} = \text{Im } j_H.$$

Wyraża ona, w połączeniu ze Stw. 28, zapowiedziane wcześniej utożsamienie pomiędzy dzielnikami normalnymi a jądrami homomorfizmów. Jej abstrakcję opisuje

Definicja 30. 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

$$\text{Ker } \chi_{(2)} = \text{Im } \chi_{(1)}.$$

²Należy zauważyć, że elementami $\text{Out}(G)$ nie są automorfizmy zewnętrzne G , lecz ich warstwy w $\text{Aut}(G)$.

Ogólniej, rodzina grup i stowarzyszonych homomorfizmów opisana diagramem

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

nosi miano ciągu dokładnego, jeśli

$$\forall_{k \in \overline{1, n-2}} : \text{Ker } \chi_{(k+1)} = \text{Im } \chi_{(k)} .$$

Krótki ciąg dokładny to ciąg dokładny szczególnej postaci

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

w którym spełniona jest koniunkcja warunków:

- (1) $\chi(1)$ jest mono;
- (2) $\chi(2)$ jest epi;
- (3) $\text{Ker } \chi(2) = \text{Im } \chi(1)$.

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

Przykład(y) 22. Niechaj $(G, \phi_2, \phi_1, \phi_0)$ będzie dowolną grupą, $H \subset G$ zaś – jej dzielnikiem normalnym. Wówczas diagram

$$1 \longrightarrow H \xrightarrow{j_H} G \xrightarrow{\pi_{G/H}} G/H \longrightarrow 1 \quad (4.3)$$

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

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

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

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

wypisanej dla epimorfizmu grup z Przykł. 15 (6), dostajemy – na mocy Tw. 3 –

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

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

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

Ciągi dokładne odegrają istotną rolę w dyskusji wybranych zagadnień algebry homologicznej w dziale 11.

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, względnie
- opisują transport struktury dzielnika normalnego za pośrednictwem homomorfizmu grup.

Zacniemy od twierdzenia podsumowującego dyskusję struktury jądra homomorfizmu.

Twierdzenie 3. (Pierwsze twierdzenie o izomorfizmie) *W notacji Def. 22, 23 i 29 oraz Stw. 30 $\text{Ker } \chi$ jest dzielnikiem normalnym $G^{(1)}$, a nadto istnieje kanoniczny izomorfizm grup*

$$G^{(1)}/\text{Ker } \chi \cong \text{Im } \chi .$$

³Rozszerzenia centralne grup odgrywają istotną rolę w opisie symetrii kwantowej teorii pola.

Dowód: Pierwsza część twierdzenia wynika wprost ze Stw. 28, zajmijmy się przeto częścią drugą. Zdefiniujmy odwzorowanie

$$\lambda_\chi : G^{(1)}/\text{Ker } \chi \longrightarrow \text{Im } \chi : g \text{ Ker } \chi \longmapsto \chi(g).$$

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

$$\chi(h) = \chi(g \cdot_{(1)} k) = \chi(g) \cdot_{(2)} \chi(k) = \chi(g) \cdot_{(2)} e^{(2)} = \chi(g). \quad (4.4)$$

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

Jest ono także injektywne, co wynika z następującego rozumowania (wykorzystującego Stw. 28):

$$\begin{aligned} \lambda_\chi(g_1 \text{ Ker } \chi) = \lambda_\chi(g_2 \text{ Ker } \chi) &\iff \chi(g_1) = \chi(g_2) \iff \chi(g_1 \cdot_{(1)} g_2^{-1}) = e^{(2)} \iff g_1 \cdot_{(1)} g_2^{-1} \in \text{Ker } \chi \\ &\iff g_1 \in \text{Ker } \chi g_2 = g_2 \text{ Ker } \chi \iff g_1 \text{ Ker } \chi = g_2 \text{ Ker } \chi. \end{aligned}$$

Na koniec przekonujemy się, że λ_χ jest homomorfizmem grup,

$$\lambda_\chi(g_1 \text{ Ker } \chi \odot g_2 \text{ Ker } \chi) = \lambda_\chi(g_1 \cdot_{(1)} g_2 \text{ Ker } \chi) = \chi(g_1 \cdot_{(1)} g_2) = \chi(g_1) \cdot_{(2)} \chi(g_2) = \lambda_\chi(g_1 \text{ Ker } \chi) \cdot_{(2)} \lambda_\chi(g_2 \text{ Ker } \chi).$$

□

Prostą konsekwencją powyższego twierdzenia jest

Corollarium 3. Niechaj $(G, \phi_2, \phi_1, \phi_0)$ będzie grupą i przyjmijmy notację Przykł. 5 (2), Stw. 19 i 30 oraz Def. 29. Istnieje kanoniczny izomorfizm grup

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

Dowód: Na mocy Stw. 19 oraz Przykł. 17 (4) zachodzi

$$\text{Im Ad.} = \text{Inn}(G) \quad \wedge \quad \text{Ker Ad.} = \mathcal{Z}(G).$$

□

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

Twierdzenie 4. (O uniwersalności rzutu kanonicznego) W notacji Def. 22, 23 i 29 oraz Stw. 30 (dla $H = \text{Ker } \chi$) istnieje dokładnie jeden **monomorfizm indukowany**

$$\tilde{\chi} : G^{(1)}/\text{Ker } \chi \rightarrow G^{(2)}$$

o własności

$$\chi = \tilde{\chi} \circ \pi_{G^{(1)}/\text{Ker } \chi}. \quad (4.5)$$

Indukuje on – wedle Tw. 3 – izomorfizm

$$\lambda_\chi : G^{(1)}/\text{Ker } \chi \xrightarrow{\cong} \text{Im } \chi,$$

co pozwala rozłożyć χ w postaci

$$\chi = j_{\text{Im } \chi} \circ \lambda_\chi \circ \pi_{G^{(1)}/\text{Ker } \chi},$$

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

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

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

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

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

por. (4.4). Ponadto, jak łatwo widać, $\tilde{\chi}$ jest homomorfizmem. Pozostaje upewnić się, że jest to odwzorowanie injektywne, pamiętając, że $\mathbf{1}_{G^{(1)}/\text{Ker } \chi} = \text{Ker } \chi$. Zachodzi

$$\tilde{\chi}(g \text{Ker } \chi) = e^{(2)} \iff \chi(g) = e^{(2)} \iff g \in \text{Ker } \chi \iff g \text{Ker } \chi = \text{Ker } \chi \iff \text{Ker } \tilde{\chi} = \{\text{Ker } \chi\}.$$

□

Kolejnym ważnym wynikiem jest

Twierdzenie 5. (Drugie twierdzenie o izomorfizmie) *Niechaj $(G, \phi_2, \phi_1, \phi_0)$ będzie grupą i niech $H, K \subset G$ niosą 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: Sprawdzimy 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 w takim razie – 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

$$\text{Ker } \varphi = K \cap H,$$

co zarazem pokazuje, że $K \cap H$ jest podgrupą (na mocy Stw. 21). Tw. 3 odniesione do φ przesądza o istnieniu pożądanego izomorfizmu kanonicznego,

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

□

Powyższe twierdzenie, pozornie dość abstrakcyjne, opisuje szeroką klasę fizykalnie istotnych struktur określaną 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 dla 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 rachunek⁴:

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

Jest zatem

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

Zapiszmy

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

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 31. Niechaj $(G, \phi_2, \phi_1, \phi_0)$ będzie grupą. Podzbiory $H, K \subset G$ noszące 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 $G = H \bullet K$.

O naturalności pojęcia dopełnienia w kontekście naszych rozważań przekonuje

Stwierdzenie 31. Każde dopełnienie podgrupy normalnej grupy danej jest kanonicznie izomorficzne z grupą ilorazową warstw względem tejże podgrupy (w grupie).

Dowód: W świetle Tw. 5 zachodzi, dla dopełnienia K podgrupy normalnej $H \subset G$ grupy G ,

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

□

Znaczenie warunku istotnej rozłączności eksponuje

Stwierdzenie 32. Przyjmijmy notację Def. 31. 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:

⁴W istocie przemycamy tutaj strukturę modułu grupy ruchów euklidesowych na zbiorze $\mathbb{R}^2$. O strukturach takich powiemy więcej już wkrótce.

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 32. Przyjmijmy notację Def. 31. Grupa G jest (**wewnętrznym**) **iloczynem półprostym podgrupy 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

$$G = H \ltimes K.$$

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

Zajmiemy się w pierwszej kolejności szczególnym przypadkiem iloczynu półprostego, jakim jest iloczyn prosty.

Stwierdzenie 33. W notacji Def. 31 i 32 istnieje kanoniczny izomorfizm

$$H \ltimes K \cong H \times K,$$

przy czym po prawej stronie mamy tu do czynienia z **zewnątrznym iloczynem prostym grup H i K** ze strukturą grupy (dziedziczoną z G) zadawaną przez działanie

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

o elemencie neutralnym (e_H, e_K) (czyli tutaj (e_G, e_G)) oraz przez odwrotność

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

Dowód: Rzeczony izomorfizm przyjmuje postać

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

Jednoznaczność rozkładu w $H \ltimes K$ 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,

$$\varepsilon(h_1 \cdot k_1 \cdot h_2 \cdot k_2) = \varepsilon(h_1 \cdot h_2 \cdot k_1 \cdot k_2) = (h_1 \cdot h_2, k_1 \cdot k_2) = \phi_2^x((h_1, k_1), (h_2, k_2)) = \phi_2^x(\varepsilon(h_1 \cdot k_1), \varepsilon(h_2 \cdot k_2)).$$

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

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

□

Struktura iloczynu prostego grup stanowi zatem banalne rozszerzenie struktury grupy na iloczyny

kartezjańskie zbiorów. O wiele ciekawszą (także z fizykalnego punktu widzenia) jest ogólniejsza struktura iloczynu półprostego, do której przejdziemy obecnie.

Przykład(y) 23.

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

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

śłuszną 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 $\mathbb{R}^2 \cong \mathbb{C}$, 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 $\mathfrak{I}(z) = 0$,

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

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, wespół z grupą cykliczną, podstawową rolę w klasyfikacji siatek kryształograficznych 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 fizykalne i chemiczne.

- (4) Prosty, lecz zarazem pobudzających wyobrażeń przykładów iloczynów półprostych grup dostarcza niskowymiarowa topologia, z którą zetknęliśmy się w Przykł.12(5) 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 $\sim_B$),

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

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 $([a]_{\sim}, [b]_{\sim})$, 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 $(0,1) \sim_X (0,0)$, $X \in \{\mathbb{T}^2, \mathbb{KB}\}$. Otrzymujemy w ten sposób następującą relację

$$\begin{aligned} [a \circ b \circ \bar{a}]_{\sim} &= [b]_{\sim} & \iff & [a]_{\sim} \star [b]_{\sim} \star \text{Inv}([a]_{\sim}) = [b]_{\sim} \\ & & \iff & [a]_{\sim} \star [b]_{\sim} = [b]_{\sim} \star [a]_{\sim} \end{aligned} \quad (4.6)$$

dla torusa i analogiczną relację

$$\begin{aligned} [a \circ \bar{b} \circ \bar{a}]_{\sim} &= [b]_{\sim} & \iff & [a]_{\sim} \star \text{Inv}([b]_{\sim}) \star \text{Inv}([a]_{\sim}) = [b]_{\sim} \\ & & \iff & \text{Inv}([a]_{\sim}) \star [b]_{\sim} \star [a]_{\sim} = \text{Inv}([b]_{\sim}) \end{aligned} \quad (4.7)$$

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

$$\prod_{k=1}^N ([a]_{\sim}^{m_k} \cdot [b]_{\sim}^{n_k}) = [\varepsilon_{x^*}]_{\sim} \quad (4.8)$$

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 (4.6),

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

oraz – odpowiednio – 4.7

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

bez trudu przepisujemy relację (4.8) 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 wypadkowy wykładnik $\tilde{n}(m_k, n_k) \in \mathbb{Z}$ daje się prosto wyznaczyć w zależności od m_k i n_k . 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,

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

Naturalnej motywacji algebraicznej dla wprowadzenia pojęcia iloczynu półprostego dostarcza dyskusja rozszerzeń homomorfizmów oraz zagadnienia ich jednostronnej odwracalności. W tym pierwszym przypadku ustalimy dla uproszczenia obraz homomorfizmu (wyjściowego i jego rozszerzenia), czyli w praktyce ograniczymy się do epimorfizmów.

Definicja 33. Niechaj $(G^{(\alpha)}, \phi_2^{(\alpha)}, \phi_1^{(\alpha)}, \phi_0^{(\alpha)})$, $\alpha \in \{1, 2\}$ będą grupami i niech $H^{(1)}$ będzie podgrupą $G^{(1)}$, na której zadany jest homomorfizm $\chi : H^{(1)} \longrightarrow G^{(2)}$. **Rozszerzeniem homomorfizmu χ do grupy $G^{(1)}$** nazywamy dowolny homomorfizm $\tilde{\chi} : G^{(1)} \longrightarrow G^{(2)}$ o własności

$$\tilde{\chi}|_{H^{(1)}} = \chi,$$

tj.

$$\forall_{h \in H^{(1)}} : \tilde{\chi}(h) = \chi(h).$$

Punktem wyjścia do naszych dalszych rozważań będzie następująca obserwacja.

Stwierdzenie 34. Przyjmijmy notację Def. 30. Niechaj $(G, \phi_2, \phi_1, \phi_0)$ będzie grupą i niech $H, K \subset G$ będą jej dwiema podgrupami, co do których zakładamy, że zawierają podgrupę normalną $N \subset G$, tj.

$$N \subset H \cap K.$$

Podgrupa H/N jest dopełnieniem podgrupy K/N w grupie ilorazowej G/N wtedy i tylko wtedy, gdy

$$H \cap K = N \quad \wedge \quad G = H \cdot K.$$

Dowód:

$\Leftarrow$ Każda z warstw leżących w przecięciu $H/N \cap K/N$ zawiera się w $H \cap K$. Jeśli zatem $H \cap K = N$, to wszystkie one leżą w N , ale podgrupa N sama jest pojedynczą warstwą, zatem koniecznie $H/N \cap K/N \subset \{N\}$. Z drugiej strony zawsze dzielnik normalny jest zawarty w odnośnej grupie ilorazowej jako warstwa elementu neutralnego, więc też $\{N\} \subset H/N \cap K/N$, co ostatecznie daje pożądaną równość $H/N \cap K/N = \{N\}$.

Jeśli ponadto $G = H \cdot K$, to $\forall_{g \in G} \exists_{(h,k) \in H \times K} : g = h \cdot k$, a zatem również $gN = (h \cdot k)N \equiv hN \odot kN$. Jest przy tym jasne, że możemy w ten sposób otrzymać dowolny element $H/N \odot K/N$, przeto $G/N = H/N \odot K/N$.

$\Rightarrow$ Tym razem zakładamy, że $H/N \cap K/N = \{N\}$. Skoro zaś wprost z definicji $N \subset H \cap K$, to wystarczy pokazać, że zachodzi zawieranie odwrotne. Załóżmy, przeciwnie, że istnieje $g \in H \cap K \setminus N$, a wtedy

$$gN = gN \cap gN \in H/N \cap K/N \implies gN = N \iff g \in N,$$

co doprowadza nas do sprzeczności.

Założmy dodatkowo, że $G/N = H/N \odot K/N$. Wobec oczywistego zawierania $H \cdot K \subset G$ musimy jedynie udowodnić zawieranie odwrotne. I tym razem załóżmy, przeciwnie, że istnieje $g \in G \setminus H \cdot K$, a wtedy dla $gN = hN \odot kN$ otrzymujemy

$$gN = (h \cdot k)N \iff \exists_{n \in N} : g = h \cdot k \cdot n,$$

ale $N \subset K$, przeto $\tilde{k} := k \cdot n \in K$, czyli $g = h \cdot \tilde{k} \in H \cdot K$, a zatem sprzeczność. □

Z sytuacji opisanej w powyższym stwierdzeniu możemy wyabstrahować

Definicja 34. Niechaj $(G, \phi_2, \phi_1, \phi_0)$ będzie grupą i niech $H, K, N \subset G$ będą jej podgrupami, przy czym N jest dzielnikiem normalnym. Podgrupa H jest **dopełnieniem podgrupy K modulo N** (i *vice versa*), gdy

$$H \cap K = N \quad \wedge \quad G = H \cdot K.$$

Ilekoć H jest dzielnikiem normalnym, podgrupę tę nazywamy **dopełnieniem normalnym podgrupy K modulo N** i piszemy

$$G = H \rtimes K \pmod{N}.$$

Związek między iloczynami półprostymi a rozszerzeniami epimorfizmów ustala

Twierdzenie 6. (O rozszerzeniu epimorfizmu) Niechaj $(G^{(\alpha)}, \phi_2^{(\alpha)}, \phi_1^{(\alpha)}, \phi_0^{(\alpha)})$, $\alpha \in \{1, 2\}$ będą grupami i niech $H^{(1)}$ będzie podgrupą $G^{(1)}$, na której zadany jest epimorfizm $\chi : H^{(1)} \twoheadrightarrow G^{(2)}$. Wówczas

(i) Dla dowolnego rozszerzenia $\tilde{\chi}$ homomorfizmu χ do grupy $G^{(1)}$ zachodzi

$$G^{(1)} = \text{Ker } \tilde{\chi} \rtimes H^{(1)} \pmod{\text{Ker } \chi},$$

tj. rozszerzenie jest określone jednoznacznie przez swoje jądro jako odwzorowanie **pomiń-Ker $\tilde{\chi}$** dane wzorem

$$\tilde{\chi} : G^{(1)} = \text{Ker } \tilde{\chi} \cdot_{(1)} H^{(1)} \longrightarrow G^{(2)} : k \cdot_{(1)} h \longmapsto \chi(h).$$

(ii) Jeśli N jest dopełnieniem normalnym $H^{(1)}$ modulo $\text{Ker } \chi$,

$$G^{(1)} = N \rtimes H^{(1)} \pmod{\text{Ker } \chi},$$

to wówczas odwzorowanie **pomiń- N**

$$\tilde{\chi}_N : G^{(1)} \longrightarrow G^{(2)} : n \cdot_{(1)} h \longmapsto \chi(h)$$

jest jedynym rozszerzeniem χ o jądrze N .

Dowód:

Ad (i) Wprost z definicji rozszerzenia wynika równość

$$\text{Ker } \tilde{\chi} \cap H^{(1)} = \text{Ker } \chi,$$

pozostaje zatem udowodnić, że $G^{(1)}$ rozkłada się, jak następuje:

$$G^{(1)} = \text{Ker } \tilde{\chi} \cdot_{(1)} H^{(1)}. \quad (4.9)$$

Biorąc pod uwagę surjektywność χ , dostajemy

$$\begin{aligned} g \in G^{(1)} &\implies \exists_{h \in H^{(1)}} : \tilde{\chi}(g) = \chi(h) \equiv \tilde{\chi}(h) \implies \tilde{\chi}(g \cdot_{(1)} h^{-1}) = e^{(2)} \iff g \cdot_{(1)} h^{-1} \in \text{Ker } \tilde{\chi} \\ &\implies g = (g \cdot_{(1)} h^{-1}) \cdot_{(1)} h \in \text{Ker } \tilde{\chi} \cdot_{(1)} H^{(1)}, \end{aligned}$$

co wobec oczywistej relacji

$$\text{Ker } \tilde{\chi} \cdot_{(1)} H^{(1)} \subset G^{(1)}$$

daje pożądaną równość (4.9). Zachodzi przy tym oczywista tożsamość dla $g = k \cdot_{(1)} h$, $(k, h) \in \text{Ker } \tilde{\chi} \times H^{(1)}$,

$$\tilde{\chi}(g) = \tilde{\chi}(k) \cdot_{(2)} \tilde{\chi}(h) = e^{(2)} \cdot_{(2)} \tilde{\chi}(h) = \tilde{\chi}(h) \equiv \chi(h),$$

zatem $\tilde{\chi}$ jest odwzorowaniem pomiń-Ker $\tilde{\chi}$.

Ad (ii) Odwzorowanie pomiń- N zdefiniowane wzorem

$$\tilde{\chi}(n \cdot_{(1)} h) := \chi(h)$$

dla dowolnej pary $(n, h) \in N \times H^{(1)}$ jest dobrze określone. Istotnie, ilekroć pary $(n_1, h_1), (n_2, h_2) \in N \times H^{(1)}$ spełniają równość $n_1 \cdot_{(1)} h_1 = n_2 \cdot_{(1)} h_2$, zachodzi $n_2^{-1} \cdot_{(1)} n_1 = h_2^{-1} \cdot_{(1)} h_1 \in N \cap H^{(1)} =$

$$\text{Ker } \chi \implies \chi(h_2^{-1} \cdot_{(1)} h_1) = e^{(2)} \iff \chi(h_2) = \chi(h_1).$$

Łatwo widać, że $\tilde{\chi}$ jest homomorfizmem, oto bowiem wobec normalności N dostajemy

$$\begin{aligned} \tilde{\chi}((n_1 \cdot_{(1)} h_1) \cdot_{(1)} (n_2 \cdot_{(1)} h_2)) &= \tilde{\chi}((n_1 \cdot_{(1)} h_1 \cdot_{(1)} n_2 \cdot_{(1)} h_1^{-1}) \cdot_{(1)} (h_1 \cdot_{(1)} h_2)) = \chi(h_1 \cdot_{(1)} h_2) \\ &= \chi(h_1) \cdot_{(2)} \chi(h_2) = \tilde{\chi}(n_1 \cdot_{(1)} h_1) \cdot_{(2)} \tilde{\chi}(n_2 \cdot_{(1)} h_2). \end{aligned}$$

Jest też

$$\text{Ker } \tilde{\chi} \equiv \{ n \cdot_{(1)} h \mid \chi(h) = \tilde{\chi}(n \cdot_{(1)} h) = e^{(2)} \} = N \cdot_{(1)} \text{Ker } \chi,$$

ale $\text{Ker } \chi \subset N$, przeto ostatecznie

$$\text{Ker } \tilde{\chi} = N.$$

Na koniec pokazujemy, że $\tilde{\chi}$ jest rozszerzeniem jedynym. Niech $\tilde{\chi}'$ będzie dowolnym takim rozszerzeniem, a wtedy dla każdego $g = n \cdot_{(1)} h$ obliczamy

$$\tilde{\chi}'(g) \equiv \tilde{\chi}'(n \cdot_{(1)} h) = \tilde{\chi}'(n) \cdot_{(2)} \tilde{\chi}'(h) = \chi(h) = \tilde{\chi}(n \cdot_{(1)} h) \equiv \tilde{\chi}(g),$$

co kończy dowód. □

Z ostatniego twierdzenia możemy wysnuć prosty wniosek:

Stwierdzenie 35. Przyjmijmy notację Tw. 6 i niech

$$G^{(1)} = N \rtimes H^{(1)}.$$

Wówczas homomorfizm χ ma jednoznacznie określone rozszerzenie do grupy $G^{(1)}$, dla którego

$$\text{Ker } \tilde{\chi} = N \cdot_{(1)} \text{Ker } \chi.$$

Dowód: Skoro $G^{(1)} = N \cdot_{(1)} H^{(1)}$ to wobec relacji $\text{Ker } \chi \subset H^{(1)}$ możemy także zapisać

$$G^{(1)} = (N \cdot_{(1)} \text{Ker } \chi) \cdot_{(1)} H^{(1)}.$$

Jest też, na mocy Stw. 17 (ii),

$$(N \cdot_{(1)} \text{Ker } \chi) \cap H^{(1)} = (N \cap H^{(1)}) \cdot_{(1)} \text{Ker } \chi = \{e^{(1)}\} \cdot_{(1)} \text{Ker } \chi = \text{Ker } \chi,$$

zatem $N \cdot_{(1)} \text{Ker } \chi$ jest dopełnieniem normalnym $H^{(1)}$ modulo $\text{Ker } \chi$. To w sumie oznacza, że

$$G^{(1)} = (N \cdot_{(1)} \text{Ker } \chi) \rtimes H^{(1)} \pmod{\text{Ker } \chi},$$

a zatem teza stwierdzenia wynika z Tw. 6 (ii). $\square$

Dotychczasowe wyniki dotyczące rozszerzeń epimorfizmów pełnią kluczową rolę w dyskusji zagadnienia jednostronnej odwracalności homomorfizmów, która z kolei pokazuje dowodnie naturalność (i powszechność) struktury iloczynu półprostego grup.

Definicja 35. W notacji Def. 22 **lewostronna odwrotność** χ to homomorfizm $\chi_L^{-1} : G^{(2)} \rightarrow G^{(1)}$ spełniający warunek

$$\chi_L^{-1} \circ \chi = \text{id}_{G^{(1)}}.$$

Analogicznie, **prawostronna odwrotność** χ to homomorfizm $\chi_R^{-1} : G^{(2)} \rightarrow G^{(1)}$ spełniający warunek

$$\chi \circ \chi_R^{-1} = \text{id}_{G^{(2)}}.$$

Homomorfizm lewostronnie (wzgl. **prawostronnie**) **odwracalny** to taki, który ma lewostronną (wzgl. prawostronną) odwrotność.

Związek pomiędzy jednostronną odwracalnością a injektywnością tudzież surjektywnością homomorfizmu precyzuje

Stwierdzenie 36. *Każdy homomorfizm lewostronnie odwracalny jest injektywny. Każdy homomorfizm prawostronnie odwracalny jest surjektywny.*

Dowód: Niech χ_L^{-1} będzie lewostronną odwrotnością homomorfizmu $\chi : G^{(1)} \rightarrow G^{(2)}$. Wówczas dla dowolnych $g_1, g_2 \in G^{(1)}$ zachodzi

$$\chi(g_1) = \chi(g_2) \implies g_1 = \chi_L^{-1} \circ \chi(g_1) = \chi_L^{-1} \circ \chi(g_2) = g_2.$$

Niech teraz χ_R^{-1} będzie prawostronną odwrotnością homomorfizmu $\chi : G^{(1)} \rightarrow G^{(2)}$. Wówczas dowolny element $g \in G^{(2)}$ możemy zapisać w postaci

$$g = \chi \circ \chi_R^{-1}(g) \in \text{Im } \chi.$$

$\square$

Jednostronna odwrotność, jeśli istnieje, nie jest w ogólności zadana jednoznacznie. Kwantyfikacji tego stwierdzenia dostarcza

Twierdzenie 7. (O jednostronnej odwracalności homomorfizmu) *W notacji Def. 22 niechaj $\mathcal{N}(\text{Im } \chi)$ oznacza zbiór dopełnień normalnych $\text{Im } \chi$ w $G^{(2)}$, natomiast $\mathcal{D}(\text{Ker } \chi)$ – zbiór dopełnień $\text{Ker } \chi$ w $G^{(1)}$. Ponadto oznaczmy przez $\text{Inv}_L(\chi)$ (wzgl. $\text{Inv}_R(\chi)$) zbiór odwrotności lewostronnych (wzgl. prawostronnych) χ .*

(i) *Jeśli χ jest injektywny, to istnieje bijekcja*

$$\mathcal{N}(\text{Im } \chi) \xrightarrow{\sim} \text{Inv}_L(\chi) : N \longmapsto \chi_L^{-1}(N),$$

przy czym $\text{Ker } \chi_L^{-1}(N) = N$;

(ii) *Jeśli χ jest surjektywny, to istnieje bijekcja*

$$\mathcal{D}(\text{Ker } \chi) \xrightarrow{\sim} \text{Inv}_R(\chi) : H \longmapsto \chi_R^{-1}(H),$$

przy czym $\text{Im } \chi_R^{-1}(H) = H$.

Dowód:

Ad (i) Na mocy Stw. 1 monomorfizm χ indukuje izomorfizm $\lambda_\chi : G^{(1)} \xrightarrow{\cong} \text{Im } \chi \subset G^{(2)}$, por. Tw. 3. Jest przy tym oczywiste, że każda lewostronna odwrotność χ jest rozszerzeniem λ_χ^{-1} do $G^{(2)}$ i *vice versa*. W świetle Tw. 6 rozszerzenie takie istnieje (i jest określone jednoznacznie) wtedy i tylko wtedy, gdy istnieje w $G^{(2)}$ dopełnienie normalne K obrazu χ modulo $\text{Ker } \lambda_\chi^{-1} = \{e^{(2)}\}$. Oznaczmy to rozszerzenie przez $\chi_L^{-1}(K)$. Zachodzi równość $\text{Ker } \chi_L^{-1}(K) = K \cdot_{(2)} \text{Ker } \lambda_\chi^{-1} = K$.

Ad (ii) Niechaj H będzie dopełnieniem $\text{Ker } \chi$ w $G^{(1)}$, tak że

$$G^{(1)} = \text{Ker } \chi \rtimes H. \quad (4.10)$$

Wówczas χ indukuje kanoniczny izomorfizm $\chi_H \equiv \chi|_H : H \xrightarrow{\cong} G^{(2)} : h \mapsto \chi(h)$. Istotnie, χ_H jest surjekcją, bo z racji surjektywności χ i wobec istnienia rozkładu (4.10)

$$\forall_{g \in G^{(2)}} \exists_{(k,h) \in \text{Ker } \chi \times H} : g = \chi(k \cdot_{(1)} h) = \chi(k) \cdot_{(2)} \chi(h) = \chi_H(h),$$

a ponadto χ_H jest injekcją, gdyż – wobec $\text{Ker } \chi \cap H = \{e^{(1)}\}$ i dla dowolnego $h \in H$ –

$$\chi_H(h) = e^{(2)} \iff h \in \text{Ker } \chi \cap H \iff h = e^{(1)}.$$

W tej sytuacji jedynym odwzorowaniem spełniającym warunek $\chi \circ \chi_R^{-1} = \text{id}_{G^{(2)}}$ jest χ_H^{-1} (odwzorowanie któregośkolwiek z punktów $G^{(2)}$ w $\text{Ker } \chi \setminus \{e^{(1)}\}$ prowadziłoby do utraty injektywności złożenia $\chi \circ \chi_R^{-1}$). Widzimy zatem, że każdemu dopełnieniu H jądra χ w $G^{(1)}$ odpowiada jednoznacznie określona prawostronna odwrotność $\chi_R^{-1} = \chi_H^{-1}$.

I odwrotnie, jeśli teraz $\chi_R^{-1} : G^{(2)} \rightarrow G^{(1)}$ jest prawostronną odwrotnością χ , to koniecznie

$$G^{(1)} = \text{Ker } \chi \rtimes \text{Im } \chi_R^{-1},$$

gdź

$$\begin{aligned} g \in \text{Ker } \chi \cap \text{Im } \chi_R^{-1} &\iff \exists_{h \in G^{(2)}} : (g = \chi_R^{-1}(h) \wedge \chi(g) = e^{(2)}) \implies h = \chi \circ \chi_R^{-1}(h) = \chi(g) = e^{(2)} \\ &\implies g = \chi_R^{-1}(e^{(2)}) = e^{(1)}, \end{aligned}$$

a ponadto dowolny element $g \in G^{(1)}$ ma rozkład

$$g = [g \cdot_{(1)} \text{Inv}_{(1)}(\chi_R^{-1} \circ \chi(g))] \cdot_{(1)} \chi_R^{-1} \circ \chi(g) \in \text{Ker } \chi \cdot_{(1)} \text{Im } \chi_R^{-1}.$$

Wnosimy stąd, że każda prawostronna odwrotność zadaje dopełnienie $\text{Ker } \chi$ w $G^{(1)}$. □

W następnym kroku zbadamy relacje pomiędzy grupami ilorazowymi wynikające z relacji zawierania pomiędzy odnośnymi dzielnikami normalnymi grupy danej.

Twierdzenie 8. (Trzecie twierdzenie o izomorfizmie) *Niechaj $(G, \phi_2, \phi_1, \phi_0)$ będzie grupą i niech $H_1 \supset H_2$ będą jej dzielnikami normalnymi. Istnieje kanoniczny izomorfizm*

$$(G/H_2)/(H_1/H_2) \cong G/H_1.$$

Dowód: Zauważmy, że H_2 jest w oczywisty sposób dzielnikiem normalnym H_1 . Istotnie, $gH_2g^{-1} = H_2$ dla dowolnego $g \in G$, w szczególności więc dla każdego $g \in H_1 \subset G$. Można zatem zdefiniować H_1/H_2 jako grupę (ilorazową). Określmy odwzorowanie

$$\chi : G/H_2 \rightarrow G/H_1 : gH_2 \mapsto gH_1.$$

Powyższa definicja ma sens, bo dla dowolnego reprezentanta $g_1 \in gH_2$ zachodzi $g_1 = g \cdot h$ dla pewnego $h \in H_2$, zatem wobec $H_2 \subset H_1$ jest $g_1H_1 = (g \cdot h)H_1 = gH_1$. Łatwo widać, że jest to homomorfizm grup, o jądrze

$$\text{Ker } \chi = \{gH_2 \mid g \in H_1\} \equiv H_1/H_2,$$

gdź

$$\chi(gH_2) = H_1 \iff gH_1 = H_1 \iff g \in H_1.$$

Wobec surjektywności χ teza przyjmuje teraz oczywistą postać

$$(G/H_2)/\text{Ker } \chi \cong \text{Im } \chi,$$

por. Tw. 3. □

Niniejszy dział, poświęcony abstrakcyjnym własnościom kategorii grup, zamkniemy opisem transportu ciągów dokładnych typu (4.3) względem homomorfizmów grup.

Twierdzenie 9. (O homomorficznym przeciwobrazie normalnego ciągu dokładnego) W notacji Def. 22, 29 oraz 30 i dla dowolnego dzielnika normalnego $H^{(2)} \subset G^{(2)}$ istnieje **kanoniczny monomorfizm indukowany**

$$\bar{\chi} : G^{(1)}/\chi^{-1}(H^{(2)}) \rightarrow G^{(2)}/H^{(2)},$$

który czyni przemiennym diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & \chi^{-1}(H^{(2)}) & \xrightarrow{J_{\chi^{-1}(H^{(2)})}} & G^{(1)} & \xrightarrow{\pi_{G^{(1)}/\chi^{-1}(H^{(2)})}} & G^{(1)}/\chi^{-1}(H^{(2)}) \longrightarrow 1 \\ & & \downarrow \chi & & \downarrow \chi & & \downarrow \bar{\chi} \\ 1 & \longrightarrow & H^{(2)} & \xrightarrow{J_{H^{(2)}}} & G^{(2)} & \xrightarrow{\pi_{G^{(2)}/H^{(2)}}} & G^{(2)}/H^{(2)} \longrightarrow 1 \end{array}.$$

W szczególności jeśli χ jest epimorfizmem, to wówczas $\bar{\chi}$ jest izomorfizmem.

Dowód: Zauważmy najpierw, że $\chi^{-1}(H^{(2)})$ jest podgrupą $G^{(1)}$. Istotnie, $h_1, h_2 \in \chi^{-1}(H^{(2)}) \iff \chi(h_1), \chi(h_2) \in H^{(2)}$, ale $H^{(2)}$ jest grupą, zatem wtedy także $\chi(h_1 \cdot_{(1)} h_2) = \chi(h_1) \cdot_{(2)} \chi(h_2) \in H^{(2)} \implies h_1 \cdot_{(1)} h_2 \in \chi^{-1}(H^{(2)})$. Ponadto $h \in \chi^{-1}(H^{(2)}) \iff \chi(h) \in H^{(2)} \implies \chi(\text{Inv}_{(1)}(h)) = \text{Inv}_{(2)}(\chi(h)) \in H^{(2)} \implies \text{Inv}_{(1)}(h) \in \chi^{-1}(H^{(2)})$.

Bez trudu przekonujemy się, że rozważana podgrupa jest normalna, bowiem

$$g \in G \implies \chi(g \cdot_{(1)} \chi^{-1}(H^{(2)}) \cdot_{(1)} \text{Inv}_{(1)}(g)) = \chi(g) \cdot_{(2)} H^{(2)} \cdot \text{Inv}_{(2)}(\chi(g)) = H^{(2)},$$

przy czym ostatnia równość wynika stąd, że $H^{(2)}$ jest dzielnikiem normalnym, i implikuje inkluzję $g \cdot_{(1)} \chi^{-1}(H^{(2)}) \cdot_{(1)} \text{Inv}_{(1)}(g) \subset \chi^{-1}(H^{(2)})$, co wobec dowolności g potwierdza wypowiedzianą tezę.

Jako że podgrupa $H^{(2)}$ jest normalna, możemy zdefiniować grupę ilorazową $G^{(2)}/H^{(2)}$ i rozważyć złożenie homomorfizmów

$$G^{(1)} \xrightarrow{\chi} G^{(2)} \xrightarrow{\pi_{G^{(2)}/H^{(2)}}} G^{(2)}/H^{(2)}.$$

Jądrem tego ostatniego jest

$$\text{Ker}(\pi_{G^{(2)}/H^{(2)}} \circ \chi) = \chi^{-1}(H^{(2)}),$$

a to dlatego że wobec równości $\text{Ker} \pi_{G^{(2)}/H^{(2)}} = \text{Im } J_{H^{(2)}}$ zachodzi (dla dowolnego $g \in G^{(1)}$)

$$\pi_{G^{(2)}/H^{(2)}} \circ \chi(g) = H^{(2)} \iff \chi(g) \in H^{(2)} \iff g \in \chi^{-1}(H^{(2)}).$$

Stąd wynika – na mocy Tw. 4 – istnienie kanonicznego monomorfizmu (indukowanego)

$$G^{(1)}/\chi^{-1}(H^{(2)}) \cong G^{(1)}/\text{Ker}(\pi_{G^{(2)}/H^{(2)}} \circ \chi) \rightarrow G^{(2)}/H^{(2)},$$

który oznaczamy jako $\bar{\chi}$. Przemienność diagramu jest teraz treścią definicji $\bar{\chi}$ – istotnie, $\bar{\chi}$ to w świetle Tw. 4 (jedyne) monomorfizm spełniający warunek

$$\bar{\chi} \circ \pi_{G^{(1)}/\chi^{-1}(H^{(2)})} = \pi_{G^{(2)}/H^{(2)}} \circ \chi,$$

por. (4.5).

Dla dowodu ostatniej części twierdzenia wystarczy policzyć, dla χ surjektywnego i dla dowolnego $g \in G^{(1)}$,

$$\bar{\chi}(g\chi^{-1}(H^{(2)})) = \pi_{G^{(2)}/H^{(2)}} \circ \chi(g) = \chi(g)H^{(2)},$$

oto bowiem z racji założonej surjektywności χ , $\text{Im } \chi = G^{(2)}$, jest $\chi(G^{(1)})H^{(2)} = G^{(2)}/H^{(2)}$, czyli $\text{Im } \bar{\chi} = G^{(2)}/H^{(2)}$, co wobec injektywności $\bar{\chi}$ daje tezę. $\square$

Przykład(y) 24. Niechaj $G^{(1)} = \mathbb{Z}$ (z dodawaniem) i $G^{(2)} = \mathbb{Z}/6\mathbb{Z}$ (z dodawaniem *modulo* 6), a ponadto niech $\chi = \pi_{\mathbb{Z}/6\mathbb{Z}}$ będzie rzutem kanonicznym. Wybierzmy podgrupę (normalną) $\{[0]_6, [2]_6, [4]_6\} \subset \mathbb{Z}/6\mathbb{Z}$, w oczywisty sposób izomorficzną z $\mathbb{Z}/3\mathbb{Z}$. Zachodzi

$$\pi_{\mathbb{Z}/6\mathbb{Z}}^{-1}(\{[0]_6, [2]_6, [4]_6\}) = 2\mathbb{Z}.$$

Diagram przemienny, o którym mowa w twierdzeniu, przyjmuje teraz postać (po rozszerzeniu o krótki ciąg dokładny definiujący χ)

$$\begin{array}{ccccccc}
 & & 1 & & & & \\
 & & \downarrow & & & & \\
 & & 6\mathbb{Z} & & & & \\
 & & \downarrow & & & & \\
 1 & \longrightarrow & 2\mathbb{Z} & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \cong \\
 1 & \longrightarrow & \{[0]_6, [2]_6, [4]_6\} & \longrightarrow & \mathbb{Z}/6\mathbb{Z} & \longrightarrow & (\mathbb{Z}/6\mathbb{Z})/\{[0]_6, [2]_6, [4]_6\} \longrightarrow 1 \\
 & & & & \downarrow & & \\
 & & & & 1 & &
 \end{array}$$

i daje nam kanoniczny izomorfizm

$$(\mathbb{Z}/6\mathbb{Z})/(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}.$$

Ten ostatni odpowiada rozkładowi półprostemu $\mathbb{Z}/6\mathbb{Z} = \{[0]_6, [2]_6, [4]_6\} \rtimes \{[0]_6, [3]_6\} \cong \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

* * *

Literatura uzupełniająca: Obok wymienionych wcześniej klasycznych pozycji Bourbakiego i Cohna, warto zajrzeć także do książki Romana [Rom12].

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.
- [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.
- [Rom12] S. Roman, *Fundamentals of Group Theory: An Advanced Approach*, Birkhäuser, 2012.

Address: KATEDRA METOD MATEMATYCZNYCH FIZYKI, WYDZIAŁ FIZYKI UNIwersYTETU WARSZAWSKIEGO, UL. HOŻA 74, PL-00-682 WARSZAWA, POLAND
E-mail address: suszek@fuw.edu.pl