

Algebra. Podstawy

Rafał R. Suszek

KATEDRA METOD MATEMATYCZNYCH FIZYKI

WYDZIAŁ FIZYKI

UNIwersytet Warszawski

Warszawa, 1 lipca 2013 r.

STRESZCZENIE. Niniejszy skrypt stanowi poszerzoną wersję zapisu wykładów algebry przeznaczonych dla słuchaczy pierwszego roku studiów indywidualnych na Wydziale Fizyki Uniwersytetu Warszawskiego i wygłoszonych w roku akademickim 2012/2013.

Spis treści

Przedmowa	5
Podziękowania	6
Część 1. Prolegomena: Struktury algebraiczne i ich transport	7
Rozdział 1. Struktury algebraiczne	9
Rozdział 2. Transport struktur algebraicznych	17
Część 2. Struktury proste	20
Rozdział 3. Liczby zespolone	22
3.1. Struktura ciała i jej transport	22
3.2. Algebra i geometria liczb zespolonych	26
Rozdział 4. Wielomiany	35
4.1. Struktura pierścienia i jej transport	35
4.2. Wielomiany	41
4.3. Podzielność i algebraiczna domkniętość	45
4.4. Dodatkowe własności dziedzin ideałów głównych	49
Rozdział 5. Grupy	51
5.1. Struktura grupy i jej transport	51
5.2. Warstwy i grupy ilorazowe	63
5.3. Ciągi dokładne i rozszerzenia grup	68
5.4. Iloczyn półprosty grup w algebrze i geometrii	72
5.5. Rozszerzenia homomorfizmów a ich jednostronna odwracalność	78
5.6. Grupy ilorazowe i ciągi dokładne w obrazie homomorfizmu	83
Rozdział 6. Działanie grupy na zbiorze	87
6.1. Struktura zbioru z działaniem grupy i jej transport	87
6.2. Stratyfikacja grupy i G -zbioru indukowana przez działanie	93
6.3. Modele struktury zbioru z działaniem grupy	98
Rozdział 7. Grupa symetryczna jako model grupy ogólnej	101
7.1. Permutacje i orbity – szczegóły anatomii	101
7.2. Grupa symetryczna w terminach generatorów i relacji	108
7.3. Parzystość permutacji	112
Część 3. Struktury złożone	115

Rozdział 8. Elementy teorii modułów	117
8.1. Struktury elementarne i ich transport	117
8.2. Proste własności odwzorowań R -liniowych	124
8.3. Liniowa niezależność, baza i pojęcia pochodne	128
8.4. Produkt i suma prosta modułów jako struktury uniwersalne	142
8.5. Suma prosta – związek z sumą algebraiczną i rodzinami rzutów, warunki rozszczepialności modułu	154
8.6. Macierzowy opis modułów rozszczepionych i ich homomorfizmów	169
8.7. Równania liniowe	183
8.8. Elementy teorii form wieloliniowych i wyznaczników	186
8.9. Moduły sprzężone, formy dwuliniowe oraz pary dwoiste	204
8.10. Ciągi dokładne grup odwzorowań R -liniowych i ciągi dualne	222
8.11. Moduł i odwzorowanie dwukrotnie sprzężone	233
8.12. Formy współrzędniowe i bazy (wzajem) dualne	234
8.13. Ślad endomorfizmu	240
Rozdział 9. Dis legomenon: Przestrzenie wektorowe	244
9.1. Przestrzenie ϵ -hermitowskie – struktura i jej transport	244
9.2. Przestrzenie hermitowskie	254
9.3. Przestrzenie symetryczne i formy kwadratowe	265
9.4. Formy skośnie symetryczne i przestrzenie symplektyczne	277
9.5. Zagadnienie własne endomorfizmu	280
9.6. Rozkład dziedziny endomorfizmu na przestrzenie pierwiastkowe	291
9.7. Jordanova postać normalna endomorfizmu	299
9.8. Kompleksyfikacja i rzeczywiste bazy jordanowskie	305
9.9. Endomorfizmy nilpotentne i diagonalizujące	310
9.10. Przestrzenie unitarne	317
9.11. Struktury afiniczne i kwadryki	333
Część 4. Epilegomena	334
Rozdział 10. Iloczyn tensorowy	335
Rozdział 11. Algebry Liego	336
Rozdział 12. Algebry Clifforda	337
Rozdział 13. Teoria kategorii	338
Rozdział 14. Elementy algebry homologicznej	339
Część 5. Konwencje	340
Bibliografia	345
Indeks	346

Przedmowa

Skrypt, który oddajemy w ręce Czytelnika, traktuje o algebrze. Inspirującego przykładu nietrywialnej algebry dostarcza poniższy cytat:

If you have an apple and I have an apple and we exchange these apples then you and I will still each have one apple. But if you have an idea and I have an idea and we exchange these ideas, then each of us will have two ideas.

[G.B. Shaw]

W kursie algebry padnie wiele słów – due words in due course. Tych słów wystarczy za przedmowę. Kurs ma służyć zabawie, zatem dobrej zabawy!

Rafał R. Suszek

Podziękowania

Autor wyraża serdeczną wdzięczność Przemkowi Majewskiemu za czas, wysiłek i serce włożone w pracę edytorsko-programistyczną nad ostatecznym kształtem niniejszego skryptu.

Część 1

Prolegomena:
Struktury algebraiczne i ich transport

Jedną z najbardziej fundamentalnych składowych formalnego opisu rzeczywistości poznawalnej, motywowanego potrzebą komunikacji wyników jej obserwacji dla zobiektywizowania wyciąganych na ich podstawie wniosków poznawczych, jest pojęcie **zbioru**, określanego choćby poprzez wskazanie cechy u wspólnianej przez wszystkie jego elementy. Kategorifikacja bytów i zjawisk fizycznych prowadzi dalej do określenia klas obiektów fizycznych ze strukturą i wskazania relacji pomiędzy nimi zachowujących ową strukturę (np. klasy obserwatorów inercjalnych i transformacji Lorentza jako relacji pomiędzy nimi). Ta prosta konstatacja stanowi elementarne uzasadnienie konieczności wnikliwej i abstrakcyjnej dyskusji **zbiorów ze strukturą**. Część tej dyskusji ma charakter analityczny i jest przedmiotem wykładu z analizy matematycznej, część zaś, o charakterze algebraicznym i geometrycznym, stanowi treść niniejszego wykładu z algebry. Naturalnie istnieje silne sprzężenie strukturalne obu kursów.

Struktury algebraiczne

Dla sprecyzowania przedmiotu dociekań zaczniemy od kilku podstawowych definicji.

DEFINICJA 1. Niechaj S będzie zbiorem i wprowadźmy oznaczenie

$$S^{\times n} := \bigtimes_{i=1}^n S.$$

Dla dowolnej liczby $n \in \mathbb{N} \setminus \{0\}$ **operacja n -argumentowa** na S to odwzorowanie

$$\phi_n : S^{\times n} \longrightarrow S.$$

Pojęcie to rozszerzamy na przypadek $n = 0$ przyjmując konwencję $S^{\times 0} := \{\bullet\}$ (zbiór jednoelementowy, czyli singleton) i określając **operację 0-argumentową**

$$\phi_0 : S^{\times 0} \longrightarrow S,$$

którą w dalszej części wykładu będziemy najczęściej utożsamiać z obrazem elementu $\bullet$ w S względem ϕ_0 ,

$$\phi_0(\bullet) \equiv e_0 \in S,$$

zwanym **stałą**.

▲

Powyższa definicja pozwala wprowadzić pojęcie centralne dla całej naszej dalszej dyskusji.

DEFINICJA 2. W notacji Def. 1 **struktura algebraiczna o nośniku S** to kolekcja

$$\mathcal{S} := (S, \phi_{k_1}, \phi_{k_2}, \dots, \phi_{k_N})$$

złożona ze zbioru S oraz – dla pewnych ustalonych liczb naturalnych $k_1 \geq k_2 \geq \dots \geq k_N \geq 0$, $N \in \mathbb{N} \setminus \{0\}$ – z operacji k_i -argumentowych ϕ_{k_i} , $i \in \overline{1, N}$.

Podstruktura algebraiczna na podzbiórze $P \subset S$ to analogiczna do poprzedniej kolekcja

$$(P, \phi_{k_1}, \phi_{k_2}, \dots, \phi_{k_N})$$

spełniająca **warunki domkniętości**

$$\forall_{i \in \overline{1, N}} : \phi_{k_i}(P^{\times k_i}) \subset P.$$

▲

O ile nie będzie to prowadziło do nieporozumień, będziemy czasem używać nazwy konkretnej struktury algebraicznej w odniesieniu do zbioru będącego jej nośnikiem.

W dalszej części wykładu dokonamy abstrakcji prostych struktur algebraicznych ze znanych konstrukcji arytmetycznych.

PRZYKŁAD(Y) 1.

(1) Liczby naturalne:

- zbiór $\mathbb{N} = \{0, 1, 2, \dots\}$;
- operacja 2-argumentowa

$$+ : \mathbb{N}^{\times 2} \longrightarrow \mathbb{N} : (m, n) \longmapsto m + n$$

o własnościach:

$$\forall_{m, n \in \mathbb{N}} : m + n = n + m \quad (\text{przemienność});$$

$$\forall_{k, l, m \in \mathbb{N}} : (k + l) + m = k + (l + m) \quad (\text{łączność});$$

- element 0 neutralny względem +, który spełnia

$$\forall_{n \in \mathbb{N}} : n + 0 = n = 0 + n.$$

(2) Liczby całkowite:

- zbiór $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$;
- operacja 2-argumentowa

$$+ : \mathbb{Z}^{\times 2} \longrightarrow \mathbb{Z} : (m, n) \longmapsto m + n$$

o własnościach j/w;

- element 0 neutralny względem + j/w;
- operacja 1-argumentowa

$$P : \mathbb{Z} \longrightarrow \mathbb{Z} : n \longmapsto -n$$

o własności

$$\forall_{n \in \mathbb{Z}} : n + P(n) = 0.$$

Stosujemy tu skrócony zapis: $m + (-n) \equiv m - n$.

(3) Liczby wymierne:

- zbiór $\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} \times \{0\})) / \sim$, przy czym $(p, q) \sim (r, s) \xLeftrightarrow{\text{ex def}} p \cdot s = q \cdot r$ – łatwo pokazać, że jest to relacja równoważności¹ na $\mathbb{Z} \times (\mathbb{Z} \times \{0\})$, zadająca rozkład zbioru na klasy abstrakcji $[(p, q)] \equiv \frac{p}{q}$;
- operacje 2-argumentowe

$$+_{\mathbb{Q}} : \mathbb{Q}^{\times 2} \longrightarrow \mathbb{Q} : [(p, q)], [(r, s)] \longmapsto [(p \cdot s + q \cdot r, q \cdot s)],$$

$$\cdot_{\mathbb{Q}} : \mathbb{Q}^{\times 2} \longrightarrow \mathbb{Q} : [(p, q)], [(r, s)] \longmapsto [(p \cdot r, q \cdot s)]$$

o własnościach:

- $+_{\mathbb{Q}}$ i $\cdot_{\mathbb{Q}}$ przemienne i łączne j/w;
- $\forall_{a, b, c \in \mathbb{Q}} : a \cdot_{\mathbb{Q}} (b +_{\mathbb{Q}} c) = (a \cdot_{\mathbb{Q}} b) +_{\mathbb{Q}} (a \cdot_{\mathbb{Q}} c)$ (rozdzielność $\cdot_{\mathbb{Q}}$ względem $+_{\mathbb{Q}}$);

¹O relacjach równoważności traktuje kurs analizy matematycznej, por., np., [Mau91, Rozdz. I § 4] i [Die65, Rozdz. I.8].

- elementy neutralne: $[(0,1)]$ względem $+_{\mathbb{Q}}$ o własności j/w oraz $[(1,1)]$ względem $\cdot_{\mathbb{Q}}$ o własności

$$\forall_{q \in \mathbb{Q}} : [(1,1)] \cdot_{\mathbb{Q}} q = q;$$

- operacja 1-argumentowa $P_{\mathbb{Q}} : \mathbb{Q} \rightarrow \mathbb{Q} : [(p,q)] \mapsto [(-p,q)]$ o własności j/w;
- operacja 1-argumentowa (o ograniczonym nośniku) $\text{Inv}_{\mathbb{Q}} : \mathbb{Q} \setminus \{[(0,1)]\} \rightarrow \mathbb{Q} : [(p,q)] \mapsto [(q,p)]$ o własności

$$\forall_{q \in \mathbb{Q} \setminus \{[(0,1)]\}} : q \cdot_{\mathbb{Q}} \text{Inv}_{\mathbb{Q}}(q) = [(1,1)].$$

✓

Wymienione przykłady prowadzą do następujących definicji.

I Struktury grupopodobne.

DEFINICJA 3. **Magma** to para (S, ϕ_2) złożona ze zbioru S oraz operacji 2-argumentowej $\phi_2 : S^{\times 2} \rightarrow S$.

▲

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

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

✓

DEFINICJA 4. **Półgrupa** to magma (S, ϕ_2) , w której operacja ϕ_2 jest łączna, co wyraża diagram przemienności

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

▲

PRZYKŁAD(Y) 3. Para $(\mathfrak{T}, \Gamma)$ złożona z następujących elementów:

- $\mathfrak{T}$ jest zbiorem **osadzonych drzew binarnych**, 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;

- Γ jest łączną (i nieprzemienne) operacją 2-argumentową, zwaną **szczępieniem**, która polega na przyłączeniu korzenia drugiego argumentu do wyróżnionego wierzchołka pierwszego argumentu, który leży na końcu ścieżki prowadzącej od korzenia i skręcającej w prawo w każdym wierzchołku łączącym ze sobą trzy krawędzie.

✓

DEFINICJA 5. **Monoid** to trójka (S, ϕ_2, ϕ_0) , w której para (S, ϕ_2) jest półgrupą, natomiast ϕ_0 jest operacją 0-argumentową zadającą stałą $\phi_0(\bullet) = e \in S$, która jest elementem neutralnym względem operacji ϕ_2 , przy czym tę ostatnią własność wyrażają diagramy przemienne

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

▲

PRZYKŁAD(Y) 4.

- (1) Trójka $(\mathbb{N}, +, \mathbf{0})$ złożona ze zbioru $\mathbb{N}$ liczb naturalnych, dodawania $+$ oraz operacji 0-argumentowej $\mathbf{0}$, której obrazem jest stała $0 \in \mathbb{N}$.
- (2) Trójka $(\mathcal{A}_X, \mathbf{c}, \emptyset)$ złożona ze **słownika** $\mathcal{A}_X$ będącego zbiorem skończonych ciągów elementów zbioru skończonego $X = \{x_1, x_2, \dots, x_n\}$, $n \in \mathbb{N}$, zwanego **alfabetem**, z operacji 2-argumentowej $\mathbf{c}$ zwanej **konkatenacją** i polegającej na dostawianiu wyrazów drugiego argumentu do wyrazów pierwszego argumentu na jego końcu, tj., np.

$$\mathbf{c}((x_{i_1}, x_{i_2}, \dots, x_{i_M}), (x_{j_1}, x_{j_2}, \dots, x_{j_N})) = (x_{i_1}, x_{i_2}, \dots, x_{i_M}, x_{j_1}, x_{j_2}, \dots, x_{j_N}),$$

oraz z operacji 0-argumentowej $\emptyset$, której obrazem jest ciąg pusty. Elementy słownika (tj. **wyrazy**) są zwykle zapisywane z opuszczeniem nawiasów i przecinków, np.

$$(x_{i_1}, x_{i_2}, \dots, x_{i_M}) \equiv x_{i_1} x_{i_2} \dots x_{i_M}.$$

Opisany monoid nosi miano **monoidu swobodnego nad X** .

✓

DEFINICJA 6. **Grupa** to czwórka $(S, \phi_2, \phi_1, \phi_0)$, w której trójka (S, ϕ_2, ϕ_0) jest monoidem, natomiast $\phi_1 : S \rightarrow S$ jest operacją 1-argumentową o własności wyrażonej przez diagramy przemienne

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

W szczególności **grupa przemienna** (zwana także **abelową**) to taka, w której operacja ϕ_2 jest przemienna, co wyraża diagram przemienny

$$\begin{array}{ccc} S \times S & \xrightarrow{\tau_S} & S \times S \\ & \searrow \phi_2 & \downarrow \phi_2 \\ & & S \end{array}$$

▲

PRZYKŁAD(Y) 5.

- (1) Czwórka $(\mathfrak{S}_X, \circ, (\cdot)^{-1}, \bullet \mapsto \text{id}_X)$ złożona ze zbioru $\mathfrak{S}_X$ permutacji elementów pewnego zbioru X (tj. bijektywnych odwzorowań $\sigma : X \rightarrow X$), (nieprzemiennej) operacji 2-argumentowej $\circ$ będącej złożeniem (czyli superpozycją) odwzorowań, operacji 1-argumentowej $\sigma \mapsto \sigma^{-1}$ brania odwrotności odwzorowania i operacji 0-argumentowej $\bullet \mapsto \text{id}_X$, której obrazem jest odwzorowanie identycznościowe. Opisana grupa nosi miano **grupy symetrycznej na X** .

indexgrupa!symetryczna W przypadku zbioru $X = \overline{1, n}$ stosuje się oznaczenie $\mathfrak{S}_X \equiv \mathfrak{S}_n$.

- (2) Czwórka $(\mathcal{Z}(G), \phi_2, \phi_1, \phi_0)$ będąca podgrupą (dowolnej) grupy $(G, \phi_2, \phi_1, \phi_0)$ o nośniku

$$\mathcal{Z}(G) := \{ z \in G \mid \forall_{g \in G} : \phi_2(z, g) = \phi_2(g, z) \}$$

zwanym **centrum grupy G** .

- (3) 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 odwzorowania²

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

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

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

²Pojęcie ciągłości jest dyskutowane na kursie analizy matematycznej, patrz, np., [Mau91, Rozdz. II § 7] i [Die65, Rozdz. II.11].

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

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

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 ciągle

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

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

✓

II Struktury pierścieniopodobne.

DEFINICJA 7. **Półpierścień** to piątka $(S, \phi_2^{(1)}, \phi_2^{(2)}, \phi_0^{(1)}, \phi_0^{(2)})$, w której obie trójki $(S, \phi_2^{(\alpha)}, \phi_0^{(\alpha)})$, $\alpha \in \{1, 2\}$ są monoidami, a przy tym

(PP1) operacja $\phi_2^{(1)}$ jest przemienne;

(PP2) operacja $\phi_2^{(2)}$ jest rozdzielna względem operacji $\phi_2^{(1)}$, co wyrażają diagramy przemienne

$$\begin{array}{ccc} S \times S \times S & \xrightarrow{\text{id}_S \times \phi_2^{(1)}} & S \times S \\ \downarrow (\phi_2^{(2)} \circ \text{pr}_{1,2}, \phi_2^{(2)} \circ \text{pr}_{1,3}) & & \downarrow \phi_2^{(2)} \\ S \times S & \xrightarrow{\phi_2^{(1)}} & S \end{array}, \quad \begin{array}{ccc} S \times S \times S & \xrightarrow{\phi_2^{(1)} \times \text{id}_S} & S \times S \\ \downarrow (\phi_2^{(2)} \circ \text{pr}_{1,3}, \phi_2^{(2)} \circ \text{pr}_{2,3}) & & \downarrow \phi_2^{(2)} \\ S \times S & \xrightarrow{\phi_2^{(1)}} & S \end{array};$$

(PP3) operacja 0-argumentowa $\phi_0^{(1)}$ spełnia tożsamości wyrażone przez diagramy przemienne

$$\begin{array}{ccc} \{\bullet\} \times S & \xrightarrow{\phi_0^{(1)} \times \text{id}_S} & S \times S \\ \searrow \phi_0^{(1)} \circ \text{pr}_1 & & \downarrow \phi_2^{(2)} \\ & & S \end{array}, \quad \begin{array}{ccc} S \times \{\bullet\} & \xrightarrow{\text{id}_S \times \phi_0^{(1)}} & S \times S \\ \searrow \phi_0^{(1)} \circ \text{pr}_2 & & \downarrow \phi_2^{(2)} \\ & & S \end{array}.$$

▲

PRZYKŁAD(Y) 6. Piątka $(\mathbb{R} \cup \{\infty\}, (x, y) \mapsto \min(x, y), (x, y) \mapsto x + y, \bullet \mapsto \infty, \bullet \mapsto 0)$. Z racji związku z tzw. geometrią tropikalną, opisana struktura nosi miano **półpierścienia tropikalnego**.

✓

DEFINICJA 8. **Pierścień** to szóstka $(S, \phi_2^{(1)}, \phi_2^{(2)}, \phi_1, \phi_0^{(1)}, \phi_0^{(2)})$, w której piątka $(S, \phi_2^{(1)}, \phi_2^{(2)}, \phi_0^{(1)}, \phi_0^{(2)})$ jest półpierścieniem (przy czym aksjomat (PP3) jest tu konsekwencją pozostałych aksjomatów), a ponadto czwórka $(S, \phi_2^{(1)}, \phi_1, \phi_0^{(1)})$ jest grupą przemienne. W szczególności **pierścień przemienny** to taki, w którym operacja $\phi_2^{(2)}$ jest przemienne.

▲

PRZYKŁAD(Y) 7. Szóstka $(\mathbb{Z}, +, \cdot, n \mapsto -n, \bullet \mapsto 0, \bullet \mapsto 1)$. Jest to pierścień przemienny.

✓

DEFINICJA 9. **Ciało** to siódemka $(S, \phi_2^{(1)}, \phi_2^{(2)}, \phi_1^{(1)}, \phi_1^{(2)}, \phi_0^{(1)}, \phi_0^{(2)})$, w której szóstka $(S, \phi_2^{(1)}, \phi_2^{(2)}, \phi_1^{(1)}, \phi_0^{(1)}, \phi_0^{(2)})$ jest pierścieniem przemiennym, natomiast $\phi_1^{(2)} : S \setminus \{\phi_0^{(1)}(\bullet)\} \rightarrow S^\times$ jest operacją 1-argumentową (o ograniczonym nośniku) o własności wyrażonej przez diagram przemienny

$$\begin{array}{ccc} S^\times \times \{\bullet\} & \xrightarrow{(\text{id}_S, \phi_1^{(2)}) \circ \text{pr}_1} & S^\times \times S^\times \\ & \searrow \phi_0^{(2)} \circ \text{pr}_2 & \downarrow \phi_2^{(2)} \\ & & S^\times \end{array} \quad (\text{F})$$

▲

PRZYKŁAD(Y) 8. Siódemka $(\mathbb{Z}/p\mathbb{Z}, ([k]_p, [l]_p) \mapsto [k+l]_p, ([k]_p, [l]_p) \mapsto [k \cdot l]_p, [k]_p \mapsto [p-k]_p, [k]_p \mapsto [\tilde{k}]_p, \bullet \mapsto [0]_p, \bullet \mapsto [1]_p)$, określona dla dowolnej liczby pierwszej p , o nośniku

$$\mathbb{Z}/p\mathbb{Z} = \{[0]_p, [1]_p, [2]_p, \dots, [p-1]_p\}$$

będącym zbiorem reszt *modulo* p ($[x]_p$ jest resztą z dzielenia liczby x przez p), w którym każdej reszcie $[k]_p$ odpowiada (dokładnie jedna) reszta $[\tilde{k}]_p$ o własności $[k \cdot \tilde{k}]_p = [0]_p$. Struktura ta nosi miano **ciała reszt modulo** p .

✓

Oprócz powyższych rozpatruje się struktury bardziej złożone, jak choćby struktury modulo- i algebropodobne, w których skład wchodzi dwa zbiory i kilka operacji 2-argumentowych, także mieszanych. W dalszej części kursu zajmiemy się tymi spośród nich, które pełnią szczególnie istotną rolę w matematycznym modelowaniu przyrody, a mianowicie modułami nad pierścieniem danym i – jeśli czas na to pozwoli – algebrami Liego. Ponadto wspomnimy o strukturach noszących miano algebr Clifforda, wyposażonych w co najmniej 4 działania 2-argumentowe (zwane iloczynem zewnętrznym i iloczynami wewnętrznymi). Pojawia się też przestrzenie Hilberta o dodatkowej strukturze (analitycznej) przestrzeni Banacha.

Transport struktur algebraicznych

Zanim przejdziemy do dyskusji ważnych – z matematycznego i przede wszystkim fizykalnego punktu widzenia – przykładów struktur wymienionych wyżej, wprowadzimy ważne pojęcie odwzorowania transportującego strukturę algebraiczną z dziedziny na przeciwdziedzinę.

DEFINICJA 10. Przyjmijmy notację Def. 1 i 2. **Homomorfizm¹ struktury algebraicznej** $(S^{(1)}, \phi_{k_1}^{(1)}, \phi_{k_2}^{(1)}, \dots, \phi_{k_N}^{(1)})$ **w strukturę algebraiczną** (tego samego typu) $(S^{(2)}, \phi_{k_1}^{(2)}, \phi_{k_2}^{(2)}, \dots, \phi_{k_N}^{(2)})$ to odwzorowanie pomiędzy ich nośnikami,

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

zgodne z obecną na nich strukturą algebraiczną w sensie wyrażanym przez rodzinę diagramów przemiennych:

$$\forall_{i \in \overline{1, N}} : \quad \begin{array}{ccc} (S^{(1)})^{\times k_i} & \xrightarrow{\phi_{k_i}^{(1)}} & S^{(1)} \\ \downarrow \times_{i=1}^{k_i} \chi & & \downarrow \chi \\ (S^{(2)})^{\times k_i} & \xrightarrow{\phi_{k_i}^{(2)}} & S^{(2)} \end{array} .$$

Wyróżniamy następujące typy homomorfizmów:

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

▲

Należy w tym momencie przypomnieć, że odwzorowanie $f : X \longrightarrow Y$ ze zbioru X w zbiór Y jest

- **iniektywne**, gdy dla dowolnych $x, y \in X$ zachodzi implikacja

$$f(x) = f(y) \implies x = y;$$

- **surjektywne**, gdy prawdziwe jest zdanie

$$\forall_{y \in Y} \exists_{x \in X} : y = f(x);$$

¹Homomorfizm to algebraiczna specjalizacja fundamentalnego w teorii kategorii [ML71] pojęcia morfizmu. Oto więc w naszych rozważaniach miejsce ogólnej klasy obiektów zajmuje klasa zbiorów z ustaloną strukturą algebraiczną, w roli zaś morfizmów, tj. odwzorowań pomiędzy obiektami zachowujących definiujące własności kategorii, występują homomorfizmy.

- bijektywne, gdy jest injektywne i surjektywne zarazem.

PRZYKŁAD (Y) 9.

- (1) Monomorfizmem ciała $(\mathbb{Q}, +_{\mathbb{Q}}, \cdot_{\mathbb{Q}}, P_{\mathbb{Q}}, \text{Inv}_{\mathbb{Q}}, \frac{0}{1}, \frac{1}{1})$ liczb wymiernych (opisanego wcześniej) w ciało $(\mathbb{R}, +_{\mathbb{R}}, \cdot_{\mathbb{R}}, P_{\mathbb{R}}, \text{Inv}_{\mathbb{R}}, \bullet \mapsto [(\frac{0}{1})_{n \in \mathbb{N}}]_{\sim}, \bullet \mapsto [(\frac{1}{1})_{n \in \mathbb{N}}]_{\sim})$ liczb rzeczywistych (o nośniku rozumianym – w duchu konstrukcji Cantora–Méraya – jako zbiór klas abstrakcji ciągów Cauchy’ego liczb wymiernych względem relacji „dowolnej bliskości wyrazów o dostatecznie dużych indeksach”, co opisuje, np., K. Maurin w [Mau91, §6 i §7]) jest odwzorowanie

$$\mathbb{Q} \rightarrow \mathbb{R} : \frac{p}{q} \mapsto [(\frac{p}{q})_{n \in \mathbb{N}}]_{\sim},$$

przypisujące liczbie $\frac{p}{q}$ klasę ciągu stałego $(\frac{p}{q})_{n \in \mathbb{N}}$.

- (2) Epimorfizmem grupy

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

odwracalnych macierzy wymiaru 2×2 o wyrazach rzeczywistych (zwanej **pełną grupą liniową stopnia 2 nad $\mathbb{R}$**) na grupę $(\mathfrak{H}_{\overline{\mathbb{R}}}, \circ, h \mapsto h^{-1}, \text{id}_{\overline{\mathbb{R}}})$ homografii uzwarconej osi rzeczywistej $\overline{\mathbb{R}} := \mathbb{R} \cup \{\infty\}$, tj. odwzorowań postaci

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

jest odwzorowanie

$$\text{GL}(2, \mathbb{R}) \rightarrow \mathfrak{H}_{\overline{\mathbb{R}}} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \left(x \mapsto \frac{a \cdot x + b}{c \cdot x + d} \right).$$

- (3) Izomorfizmem monoidu $(\mathbb{N}, +, \mathbf{0})$ liczb naturalnych w monoid $(2\mathbb{N}, +, \mathbf{0})$ parzystych liczb naturalnych jest odwzorowanie

$$\mathbb{N} \xrightarrow{\cong} 2\mathbb{N} : n \mapsto 2n.$$

- (4) Endomorfizmem dowolnego półpierścienia $(S, \phi_2^{(1)}, \phi_2^{(2)} \equiv \cdot, \phi_0^{(1)}, \phi_0^{(2)})$ jest odwzorowanie

$$S \curvearrowright : s \mapsto x \cdot s \cdot x,$$

określone dla dowolnego takiego jego elementu $x \in S$, który spełnia tożsamość

$$x \cdot x = \phi_0^{(2)}(\bullet).$$

- (5) Automorfizmem dowolnej grupy $(G, \phi_2 \equiv \cdot, \phi_1 \equiv \text{Inv}, \phi_0)$ jest odwzorowanie, określone dla dowolnego jej elementu $h \in G$,

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

✓

Nierzadko narzucenie warunku zachowania niektórych elementów rozważanej struktury algebraicznej pociąga za sobą zachowanie tejże w całości. Przykładowo dostarcza tutaj teoria homomorfizmów grup, którą omówimy w Rozdz. 5.1.

Warto na tym etapie wysłowić oczywistą acz ważną obserwację.

STWIERDZENIE 1. *Każdy monomorfizm jest izomorfizmem dziedziny na jej obraz względem tego monomorfizmu.*

■

*

*

*

Literatura uzupełniająca: Szczegółowe omówienie wprowadzonych tu (i wielu innych) struktur algebraicznych można znaleźć w opracowaniu Bourbakiego [Bou07b] oraz w klasycznym kursie Langa [Lan02] i doskonałej trzytomowej monografii Cohna [Coh82, Coh89, Coh91].

Część 2

Struktury proste

Celem pierwszej części niniejszego kursu, a zarazem oczywistym punktem wyjścia do dyskusji zastosowań algebry w fizyce i geometrii, jest dokładne zbadanie wybranych elementarnych struktur algebraicznych, których związek z nowoczesnym opisem zjawisk – ledwie wzmiankowany w poświęconych im rozdziałach – dowodnie wykażą przyszłe kursy specjalistyczne z rozmaitych dziedzin fizyki teoretycznej i matematycznej. Konsekwentnie realizowany schemat opisu, wedle którego po aksjomatyzacji struktury podstawowej następuje szczegółowa analiza morfizmów tejże struktury oraz relacji indukowanych w jej nośniku, ma w zamyśle posłużyć wykształceniu narzędzi precyzyjnego, efektywnego i (choćby już z tych tylko względów) naturalnego opisu obiektów o charakterze algebraicznym, także tych bardziej złożonych, jak również strukturalnych relacji pomiędzy nimi. W opisanym schemacie dociekliwy Czytelnik dostrzeże bez trudu odzwierciedlenie logicznego porządku, jaki w opisie struktur algebraicznych (i nie tylko) wprowadza teoria kategorii [ML71].

Liczby zespolone

Dyskusję konkretnych struktur algebraicznych o znaczeniu fizykalnym zaczniemy od szczegółowego omówienia rozszerzenia algebraicznego dobrze znanego (choćby z wykładu analizy matematycznej) ciała liczb rzeczywistych. Rozszerzenie to stanowi ważny przykład ciała algebraicznie domkniętego, a w przyszłości znajdzie szereg zastosowań – zarówno technicznych jak i strukturalnych – w mechanice fal, klasycznej teorii elektromagnetyzmu, mechanice kwantowej, kwantowej teorii pola i teorii strun.

3.1. Struktura ciała i jej transport

Zacznijmy od wypisania w jawnej postaci aksjomatów ciała.

DEFINICJA 11. **Ciało** to siódemka $(\mathbb{K}, A, M, P, \text{Inv}, \mathbf{0}, \mathbf{1})$, w której

- $\mathbb{K}$ jest zbiorem;
- $A : \mathbb{K}^{\times 2} \longrightarrow \mathbb{K} : (x, y) \longmapsto A(x, y) \equiv x +_{\mathbb{K}} y$ jest operacją 2-argumentową zwaną **dodawaniem**;
- $M : \mathbb{K}^{\times 2} \longrightarrow \mathbb{K} : (x, y) \longmapsto M(x, y) \equiv x \cdot_{\mathbb{K}} y$ jest operacją 2-argumentową zwaną **mnożeniem**;
- $P : \mathbb{K} \longrightarrow \mathbb{K} : x \longmapsto P(x) \equiv -x$ jest operacją 1-argumentową zwaną **braniem przeciwności**;
- $\text{Inv} : \mathbb{K} \setminus \{\mathbf{0}(\bullet)\} \longrightarrow \mathbb{K} : x \longmapsto \text{Inv}(x) \equiv x^{-1}$ jest operacją 1-argumentową (o ograniczonym nośniku) zwaną **braniem odwrotności**;
- $\mathbf{0} : \{\bullet\} \longrightarrow \mathbb{K} : \bullet \longmapsto \mathbf{0}$ jest operacją 0-argumentową zwaną **zerem**;
- $\mathbf{1} : \{\bullet\} \longrightarrow \mathbb{K} : \bullet \longmapsto \mathbf{1}$ jest operacją 0-argumentową zwaną **jedynką**,

przy czym składowe struktury spełniają następujące aksjomaty (wyrażone przez diagramy przemienne i równoważne zdania logiczne):

(F1) (łączność działań)

$$\begin{array}{ccc}
 \mathbb{K} \times \mathbb{K} \times \mathbb{K} & \xrightarrow{A \times \text{id}_{\mathbb{K}}} & \mathbb{K} \times \mathbb{K} \\
 \text{id}_{\mathbb{K}} \times A \downarrow & & \downarrow A \\
 \mathbb{K} \times \mathbb{K} & \xrightarrow{A} & \mathbb{K}
 \end{array} \quad \equiv \quad \forall_{x,y,z \in \mathbb{K}} : (x +_{\mathbb{K}} y) +_{\mathbb{K}} z = x +_{\mathbb{K}} (y +_{\mathbb{K}} z);$$

$$\begin{array}{ccc}
 \mathbb{K} \times \mathbb{K} \times \mathbb{K} & \xrightarrow{M \times \text{id}_{\mathbb{K}}} & \mathbb{K} \times \mathbb{K} \\
 \text{id}_{\mathbb{K}} \times M \downarrow & & \downarrow M \\
 \mathbb{K} \times \mathbb{K} & \xrightarrow{M} & \mathbb{K}
 \end{array} \quad \equiv \quad \forall_{x,y,z \in \mathbb{K}} : (x \cdot_{\mathbb{K}} y) \cdot_{\mathbb{K}} z = x \cdot_{\mathbb{K}} (y \cdot_{\mathbb{K}} z);$$

(F2) (przemienność działań)

$$\begin{array}{ccc}
\mathbb{K} \times \mathbb{K} & \xrightarrow{\tau_{\mathbb{K}}} & \mathbb{K} \times \mathbb{K} \\
& \searrow A & \downarrow A \\
& & \mathbb{K}
\end{array} \equiv \forall_{x,y \in \mathbb{K}} : x +_{\mathbb{K}} y = y +_{\mathbb{K}} x ;$$

$$\begin{array}{ccc}
\mathbb{K} \times \mathbb{K} & \xrightarrow{\tau_{\mathbb{K}}} & \mathbb{K} \times \mathbb{K} \\
& \searrow M & \downarrow M \\
& & \mathbb{K}
\end{array} \equiv \forall_{x,y \in \mathbb{K}} : x \cdot_{\mathbb{K}} y = y \cdot_{\mathbb{K}} x ;$$

(F3) (rozdzielność mnożenia względem dodawania)

$$\begin{array}{ccc}
\mathbb{K} \times \mathbb{K} \times \mathbb{K} & \xrightarrow{\text{id}_{\mathbb{K}} \times A} & \mathbb{K} \times \mathbb{K} \\
(M \circ \text{pr}_{1,2}, M \circ \text{pr}_{1,3}) \downarrow & & \downarrow M \\
\mathbb{K} \times \mathbb{K} & \xrightarrow{A} & \mathbb{K}
\end{array} \equiv \forall_{x,y,z \in \mathbb{K}} : \begin{array}{l} x \cdot_{\mathbb{K}} (y +_{\mathbb{K}} z) \\ = (x \cdot_{\mathbb{K}} y) +_{\mathbb{K}} (x \cdot_{\mathbb{K}} z) \end{array} ;$$

(F4) (istnienie elementów neutralnych względem działań)

$$\begin{array}{ccc}
\mathbb{K} \times \{\bullet\} & \xrightarrow{\text{id}_{\mathbb{K}} \times \mathbf{0}} & \mathbb{K} \times \mathbb{K} \\
& \searrow \text{pr}_1 & \downarrow A \\
& & \mathbb{K}
\end{array} \equiv \forall_{x \in \mathbb{K}} : x +_{\mathbb{K}} \mathbf{0} = x ;$$

$$\begin{array}{ccc}
\mathbb{K} \times \{\bullet\} & \xrightarrow{\text{id}_{\mathbb{K}} \times \mathbf{1}} & \mathbb{K} \times \mathbb{K} \\
& \searrow \text{pr}_1 & \downarrow M \\
& & \mathbb{K}
\end{array} \equiv \forall_{x \in \mathbb{K}} : x \cdot_{\mathbb{K}} \mathbf{1} = x ;$$

(F5) (istnienie elementów przeciwnych i odwrotnych do niezerowych)

$$\begin{array}{ccc}
\mathbb{K} \times \{\bullet\} & \xrightarrow{(\text{id}_{\mathbb{K}}, \text{P}) \circ \text{pr}_1} & \mathbb{K} \times \mathbb{K} \\
& \searrow \mathbf{0} \circ \text{pr}_2 & \downarrow A \\
& & \mathbb{K}
\end{array} \equiv \forall_{x \in \mathbb{K}} : x +_{\mathbb{K}} (-x) = \mathbf{0} ;$$

$$\begin{array}{ccc}
\mathbb{K}^{\times} \times \{\bullet\} & \xrightarrow{(\text{id}_{\mathbb{K}}, \text{Inv}) \circ \text{pr}_1} & \mathbb{K}^{\times} \times \mathbb{K}^{\times} \\
& \searrow \mathbf{1} \circ \text{pr}_2 & \downarrow M \\
& & \mathbb{K}^{\times}
\end{array} \equiv \forall_{x \in \mathbb{K}^{\times}} : x \cdot_{\mathbb{K}} x^{-1} = \mathbf{1} ;$$

(F6) (nietrywialność) $\mathbf{0} \neq \mathbf{1}$.



PRZYKŁAD(Y) 10.

- (1) Liczby wymierne z podaną wcześniej strukturą.
- (2) Liczby rzeczywiste ze strukturą indukowaną przez powyższą w konstrukcji Cantora–Méraya.
- (3) Ciało Galois rzędu 2 (najmniejsze ciało nietrywialne) o nośniku $\text{GF}_2 = \{0, 1\}$ i tabelkach działań:

$+_{\text{GF}_2}$	0	1
0	0	1
1	1	0

 oraz

$\cdot_{\text{GF}_2}$	0	1
0	0	0
1	0	1

 .
- (4) Ciało rzeczywistych funkcji wymiernych o nośniku¹ $\mathbb{R}(\cdot) := \left\{ \frac{f(\cdot)}{g(\cdot)} \mid f, g \in \mathbb{R}[t] \wedge g \neq 0 \right\}$ ($\mathbb{R}[t]$ to zbiór wielomianów o współczynnikach rzeczywistych) z dodawaniem i mnożeniem punktowym funkcji.



Mamy oczywistą

DEFINICJA 12. W notacji Def. 11 **podciało** ciała $(\mathbb{K}, A, M, P, \text{Inv}, \mathbf{0}, \mathbf{1})$ to siódemka $(\mathbb{L}, A, M, P, \text{Inv}, \mathbf{0}, \mathbf{1})$, w której $\mathbb{L}$ jest podzbiorem $\mathbb{K}$ o następujących własnościach:

- (SF1) $A : \mathbb{L}^{\times 2} \longrightarrow \mathbb{L} \subset \mathbb{K}$;
- (SF2) $M : \mathbb{L}^{\times 2} \longrightarrow \mathbb{L} \subset \mathbb{K}$;
- (SF3) $P : \mathbb{L} \longrightarrow \mathbb{L} \subset \mathbb{K}$;
- (SF4) $\text{Inv} : \mathbb{L} \setminus \{0\} \longrightarrow \mathbb{L} \subset \mathbb{K}$;
- (SF5) $\mathbb{L} \ni 1$.



Przykroiwszy treść ogólnej Definicji 10 do wprowadzonej powyżej struktury algebraicznej, otrzymujemy

DEFINICJA 13. W notacji Def. 11 **homomorfizm ciała** $(\mathbb{K}^{(1)}, A^{(1)}, M^{(1)}, P^{(1)}, \text{Inv}^{(1)}, \mathbf{0}^{(1)}, \mathbf{1}^{(1)})$ w ciało $(\mathbb{K}^{(2)}, A^{(2)}, M^{(2)}, P^{(2)}, \text{Inv}^{(2)}, \mathbf{0}^{(2)}, \mathbf{1}^{(2)})$ to odwzorowanie

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

o własnościach

$$\begin{array}{ccc}
 \mathbb{K}^{(1)} \times \mathbb{K}^{(1)} & \xrightarrow{A^{(1)}} & \mathbb{K}^{(1)} \\
 \downarrow \chi \times \chi & & \downarrow \chi \\
 \mathbb{K}^{(2)} \times \mathbb{K}^{(2)} & \xrightarrow{A^{(2)}} & \mathbb{K}^{(2)}
 \end{array}
 \quad \equiv \quad
 \forall_{x, y \in \mathbb{K}^{(1)}} : \quad \chi(x +_{(1)} y) = \chi(x) +_{(2)} \chi(y) ;$$

(FH1)

¹Ściśle rzecz biorąc, w definicji $\mathbb{R}(\cdot)$ używamy *funkcji wielomianowych*, patrz: Def. 25.

$$(FH2) \quad \begin{array}{ccc} \mathbb{K}^{(1)} \times \mathbb{K}^{(1)} & \xrightarrow{M^{(1)}} & \mathbb{K}^{(1)} \\ \chi \times \chi \downarrow & & \downarrow \chi \\ \mathbb{K}^{(2)} \times \mathbb{K}^{(2)} & \xrightarrow{M^{(2)}} & \mathbb{K}^{(2)} \end{array} \quad \equiv \quad \forall_{x,y \in \mathbb{K}^{(1)}} : \chi(x \cdot_{(1)} y) = \chi(x) \cdot_{(2)} \chi(y).$$

Dowolny inwolutywny (anty)automorfizm²

$$J : \mathbb{K} \curvearrowright : \lambda \mapsto \bar{\lambda},$$

$$J(\lambda +_{\mathbb{K}} \mu) = J(\lambda) +_{\mathbb{K}} J(\mu), \quad J(\lambda \cdot_{\mathbb{K}} \mu) = J(\mu) \cdot_{\mathbb{K}} J(\lambda), \quad J \circ J = \text{id}_{\mathbb{K}}$$

określamy mianem **sprzężenia**.

Jądro homomorfizmu to zbiór

$$\text{Ker } \chi := \{ x \in \mathbb{K}^{(1)} \mid \chi(x) = 0^{(2)} \},$$

natomiast **obraz homomorfizmu** to zbiór

$$\text{Im } \chi := \{ x \in \mathbb{K}^{(2)} \mid \exists_{y \in \mathbb{K}^{(1)}} : x = \chi(y) \} \equiv \chi(\mathbb{K}^{(1)}).$$

▲

PRZYKŁAD(Y) 11. Niechaj $(\mathbb{K}, A \equiv +, M \equiv \cdot, P, \text{Inv}, \bullet \mapsto 0, \bullet \mapsto 1)$ będzie ciałem o **charakterystyce** $\text{char}(\mathbb{K}) = p$ danej przez liczbę pierwszą p , przy czym przez charakterystykę ciała rozumiemy najmniejszą z liczb $n \in \mathbb{N} \setminus \{0\}$, dla których jest spełniona równość

$$\underbrace{1 + 1 + \dots + 1}_{n \text{ razy}} = 0,$$

np. $\text{char}(\mathbb{Z}/p\mathbb{Z}) = p$. Odwzorowanie

$$\mathbb{K} \curvearrowright : x \mapsto x^p \equiv \underbrace{x \cdot x \cdot \dots \cdot x}_{p \text{ razy}}$$

jest injektywnym endomorfizmem ciała $\mathbb{K}$. Prawdziwość tego stwierdzenia jest prostą konsekwencją twierdzenia o współczynniku dwumianowym dla liczby pierwszej p , które stwierdza, co następuje:

$$\forall_{k \in \overline{1, p-1}} : \left[\binom{p}{k} \right]_p = 0$$

(dowód stanowi proste zastosowanie Tw. 4.2).

✓

²Według konwencji przyjętej w tym wykładzie każde ciało jest pierścieniem przemiennym, co usuwa podstawę do rozróżnienia pomiędzy izomorfizmami moltiplikatywnymi i antymoltiplikatywnymi (tj. takimi, które odwracają porządek czynników). Ponieważ jednak niektóre z konstrukcji opisywanych w dalszej części kursu dopuszczają uogólnienia na szerszą klasę pierścieni, zdecydowaliśmy się zachować – tam gdzie jest to możliwe – bardziej ogólny zapis.

3.2. Algebra i geometria liczb zespolonych

Przejdziemy obecnie do omówienia zasadniczej konstrukcji, której poświęcony jest niniejszy rozdział.

DEFINICJA 14. Ciało liczb zespolonych to siódemka $(\mathbb{C}, A_{\mathbb{C}} \equiv +_{\mathbb{C}}, M_{\mathbb{C}} \equiv \cdot_{\mathbb{C}}, P_{\mathbb{C}}, \text{Inv}_{\mathbb{C}}, \mathbf{0}_{\mathbb{C}}, \mathbf{1}_{\mathbb{C}})$, w której

- $\mathbb{C} := \mathbb{R}^{\times 2}$;
- $A_{\mathbb{C}} : \mathbb{C}^{\times 2} \rightarrow \mathbb{C} : ((x_1, y_1), (x_2, y_2)) \mapsto (x_1 + y_1, x_2 + y_2)$;
- $M_{\mathbb{C}} : \mathbb{C}^{\times 2} \rightarrow \mathbb{C} : ((x_1, y_1), (x_2, y_2)) \mapsto (x_1 \cdot x_2 - y_1 \cdot y_2, x_1 \cdot y_2 + x_2 \cdot y_1)$;
- $P_{\mathbb{C}} : \mathbb{C} \rightarrow \mathbb{C} : (x, y) \mapsto (-x, -y)$;
- $\text{Inv}_{\mathbb{C}} : \mathbb{C} \setminus \{(0, 0)\} =: \mathbb{C}^{\times} \rightarrow \mathbb{C} : (x, y) \mapsto \left(\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2}\right)$;
- $\mathbf{0}_{\mathbb{C}} : \bullet \mapsto (0, 0)$;
- $\mathbf{1}_{\mathbb{C}} : \bullet \mapsto (1, 0)$.

▲

TWIERDZENIE 3.1. *Ciało liczb zespolonych jest ciałem nietrywialnym.*

■

Relację pomiędzy opisaną powyżej strukturą ciała na zbiorze par liczb rzeczywistych a także strukturą na zbiorze liczb rzeczywistych ustala

STWIERDZENIE 2. *W notacji Def. 14 odwzorowanie*

$$(3.1) \quad \iota : \mathbb{R} \rightarrow \mathbb{C} : x \mapsto (x, 0)$$

jest monomorfizmem ciał³.

■

Ostatnia obserwacja pozwala – w świetle Stw. 1, które implikuje $\iota(\mathbb{R}) \cong \mathbb{R}$ – utożsamić $\mathbb{R}$ z obrazem tegoż ciała względem włożenia ι i tym samym traktować $\mathbb{R}$ jako podciało $\mathbb{C}$. Możemy też zdefiniować strukturę $\mathbb{R}$ -modułu⁴ (czyli działanie $\mathbb{R}$) na $\mathbb{C}$.

DEFINICJA 15. W notacji Def. 14 i Stw. 2 **struktura modułu nad pierścieniem** $(\mathbb{R}, +_{\mathbb{R}}, \cdot_{\mathbb{R}}, P_{\mathbb{R}}, \bullet \mapsto [(\frac{0}{1})_{n \in \mathbb{N}}]_{\sim}, \bullet \mapsto [(\frac{1}{1})_{n \in \mathbb{N}}]_{\sim})$ **na grupie** $(\mathbb{C}, +_{\mathbb{C}}, P_{\mathbb{C}}, \bullet \mapsto 0)$ to odwzorowanie

$$(3.2) \quad \mathbb{R} \times \mathbb{C} \rightarrow \mathbb{C} : (x, (y, z)) \mapsto \iota(x) \cdot_{\mathbb{C}} (y, z) =: x \cdot (y, z)$$

o własnościach

$$x \cdot (y \cdot (a, b)) = (x \cdot y) \cdot (a, b), \quad 1 \cdot (a, b) = (a, b),$$

$$(x +_{\mathbb{R}} y) \cdot (a, b) = x \cdot (a, b) +_{\mathbb{C}} y \cdot (a, b), \quad x \cdot ((a, b) +_{\mathbb{C}} (c, d)) = x \cdot (a, b) +_{\mathbb{C}} x \cdot (c, d),$$

wypisanych dla dowolnych $x, y, a, b, c, d \in \mathbb{R}$.

▲

³Godzi się w tym miejscu zauważyć, że wszystkie homomorfizmy ciał są monomorfizmami.

⁴Nasza uwaga ma na obecnym etapie charakter wyłącznie pomocniczy. Istotne elementy teorii modułów nad pierścieniem zostaną omówione w dziale 8.

Dotychczasowa dyskusja prowadzi wprost do wygodnej realizacji struktury algebraicznej na $\mathbb{C}$ w terminach dobrze znanego jej odpowiednika na $\mathbb{R}$, przy czym ostatnim brakującym elementem jest tutaj analiza własności wyróżnionej liczby zespolonej $(0, 1)$.

STWIERDZENIE 3. W notacji Def. 14 i 3.2 oraz Stw. 2 i dla jednostki urojonej

$$i := (0, 1) \in \mathbb{C}$$

zachodzi

$$i \cdot_{\mathbb{C}} i = \iota(-1),$$

a ponadto

$$\forall_{(x,y) \in \mathbb{C}} : (x, y) = x \cdot_{\mathbb{C}} \iota(1) +_{\mathbb{C}} y \cdot i.$$

■

Powyższy zapis uzasadnia

DEFINICJA 16. W notacji Def. 14 część rzeczywista liczby zespolonej $(x, y) \in \mathbb{C}$ to

$$\Re(x, y) := x,$$

natomiast jej część urojona to

$$\Im(x, y) := y.$$

▲

NOTACJA 1. W dalszej części wykładu przyjmiemy wygodną (i powszechnie stosowaną) umowę dotyczącą zapisu liczb zespolonych zwanego **zapisem kartezjańskim**. Jej podstawą jest opuszczenie oznaczenia monomorfizmu (3.1), pozwalające zapisać

$$\forall_{x \in \mathbb{R}} : \iota(x) \equiv x,$$

jak również indeksów $\mathbb{C}$ na symbolach operacji na $\mathbb{C}$ oraz znaku działania $\mathbb{R}$ na $\mathbb{C}$. Zapiszemy zatem dowolną liczbę zespoloną $z \in \mathbb{C}$ w postaci

$$z = \Re(z) + i \Im(z).$$

Oczywista korzyść ze stosowania takiego zapisu to możliwość wykonywania wszelkich operacji algebraicznych na liczbach zespolonych według reguł obowiązujących w ciele $\mathbb{R}$, wzbogaconych o jedną dodatkową regułę:

$$i^2 = -1.$$

* * *

Prostej ilustracji przydatności przyjętej konwencji zapisu liczb zespolonych dostarczają poniższe proste rachunki (prowadzone dla dowolnych $(x, y), (x_1, y_1), (x_2, y_2) \in \mathbb{C}$):

$$(x_1 + i y_1) + (x_2 + i y_2) = (x_1 + x_2) + i(y_1 + y_2),$$

$$(x_1 + i y_1) \cdot (x_2 + i y_2) = x_1 \cdot x_2 + i(x_1 \cdot y_2 + y_1 \cdot x_2) + i^2 y_1 \cdot y_2 = (x_1 \cdot x_2 - y_1 \cdot y_2)$$

$$\begin{aligned}
& +i(x_1 \cdot y_2 + y_1 \cdot x_2), \\
(x+i y)^{-1} &= \frac{1}{x+i y} \cdot \frac{1}{x-i y} \cdot (x-i y) = \frac{1}{(x+i y) \cdot (x-i y)} \cdot (x-i y) \\
&= \frac{1}{x^2+y^2} \cdot (x-i y) \equiv \frac{x}{x^2+y^2} + i \frac{(-y)}{x^2+y^2}.
\end{aligned}$$

Możemy już teraz przejść do opisu dodatkowej struktury obecnej w ciele liczb zespolonych.

DEFINICJA 17. W notacji Def. 14 **moduł (liczby zespolonej)** to odwzorowanie

$$|\cdot| : \mathbb{C} \longrightarrow \mathbb{R} : z \longmapsto \sqrt{\Re(z)^2 + \Im(z)^2}.$$

▲

DEFINICJA 18. W notacji Def. 14 **sprzężenie (zespolone)** to odwzorowanie

$$\bar{\cdot} : \mathbb{C} \longrightarrow \mathbb{C} : z \longmapsto \Re(z) - i \Im(z) =: \bar{z},$$

spełniające oczywiste tożsamości:

$$\Re(z) = \frac{z + \bar{z}}{2}, \quad \Im(z) = \frac{z - \bar{z}}{2i}.$$

▲

Proste własności modułu są zebrane poniżej.

STWIERDZENIE 4. W notacji Def. 14 oraz 17 i dla dowolnych $z, z_1, z_2 \in \mathbb{C}$ zachodzą następujące relacje:

- (i) $|z| = 0 \iff z = 0$;
- (ii) $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$;
- (iii) $|z|^2 = z \cdot \bar{z}$;
- (iv) $|z_1 + z_2| = \sqrt{|z_1|^2 + |z_2|^2 + 2\Re(z_1 \cdot \bar{z}_2)} \leq |z_1| + |z_2|$ (nierówność trójkąta);
- (v) $|z_1 - z_2| \geq ||z_1| - |z_2||$.

■

Dowód: (Na ćwiczeniach lub w domu.)

□

Własności sprzężenia zespolonego opisuje

STWIERDZENIE 5. Sprzężenie zespolone jest inwolutywnym automorfizmem ciała liczb zespolonych, tj. w notacji Def. 14 oraz 18 i dla dowolnych $z, z_1, z_2 \in \mathbb{C}$ zachodzi, co następuje:

- (i) $\bar{\cdot} : \mathbb{C} \rightarrow \mathbb{C}$;
- (ii) $\text{Ker } \bar{\cdot} = \{0\} \quad \wedge \quad \text{Im } \bar{\cdot} = \mathbb{C}$;
- (iii) $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$;
- (iv) $\overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2$;
- (v) $\bar{\bar{z}} = z$.

Ponadto, w notacji Stw. 2,

$$\bar{z} = z \iff z \in \iota(\mathbb{R}) \equiv \mathbb{R},$$

$$\bar{z} = -z \iff z \in i \cdot \iota(\mathbb{R}) \equiv i\mathbb{R}.$$

■

Zgromadzona dotąd wiedza na temat ciała liczb zespolonych daje podstawy do naturalnej interpretacji geometrycznej części struktury algebraicznej na $\mathbb{C}$, a mianowicie $(\mathbb{C}, +_{\mathbb{C}}, \mathbf{P})$, w terminach elementarnego rachunku wektorowego na $\mathbb{R}^2$, znanego ze szkoły średniej⁵. W rachunku tym przedmiotem zainteresowania jest zbiór wektorów zaczepionych w wyróżnionym punkcie o współrzędnych $(0,0)$ na płaszczyźnie $\mathbb{R}^2$,

$$\text{Vect}_0(\mathbb{R}^2) := \{ \overrightarrow{[(0,0);(x,y)]} \mid (x,y) \in \mathbb{R}^2 \}.$$

Jego elementy możemy dodawać według dobrze znanej „reguły równoległoboku”, a ponadto każdemu z nich przypisujemy liczbę nieujemną zwaną długością wektora i równą – z definicji – długości wyznaczanego przezeń odcinka, obliczanej na podstawie twierdzenia Pitagorasa. Sumę wektorową wektorów $\vec{v}_1$ i $\vec{v}_2$ oznaczmy symbolem $\vec{v}_1 + \vec{v}_2$, długość zaś wektora $\vec{v}$ zapiszemy jako $\|\vec{v}\|$. Punktem wyjścia dla zapowiedzianej interpretacji geometrycznej jest określenie bijekcji

$$\vec{\cdot} : \mathbb{C} \longrightarrow \text{Vect}_0(\mathbb{R}^2) : z \longmapsto \overrightarrow{[(0,0);(\Re(z), \Im(z))]} =: \vec{z}.$$

Łatwo stwierdzamy prawdziwość tożsamości (zapisanej dla dowolnych $z_1, z_2 \in \mathbb{C}$)

$$\overrightarrow{z_1 +_{\mathbb{C}} z_2} = \vec{z}_1 + \vec{z}_2,$$

a ponadto dowodzimy, dla dowolnej liczby $z \in \mathbb{C}$, równość

$$|z| = \|\vec{z}\|.$$

Na koniec wreszcie możemy w prosty sposób zrealizować sprzężenie zespolone

$$\vec{\bar{z}} = P_{OX}(\vec{z})$$

jako odbicie wektora przyporządkowanego liczbie zespolonej z w prostej w $\mathbb{R}^2$ o wektorze kierunkowym $\overrightarrow{[(0,0);(1,0)]}$.

W celu rozszerzenia interpretacji geometrycznej na pozostałą część struktury algebraicznej na $\mathbb{C}$ wygodnie jest przejść do odmiennej (od kartezjańskiej) prezentacji liczb zespolonych, przy czym przejście to w języku geometrii płaszczyzny kartezjańskiej odpowiada zmianie układu współrzędnych używanego w opisie punktów i wektorów z kartezjańskiego na biegunowy. Tym razem zaczynamy od konstatacji, słusznej dla dowolnej pary $(x,y) \in \mathbb{R}^2 \setminus \{(0,0)\}$ wobec przebiegu funkcji $\sin$, że oto oczywista równość

$$\left(\frac{x}{\sqrt{x^2 + y^2}} \right)^2 + \left(\frac{y}{\sqrt{x^2 + y^2}} \right)^2 = 1$$

⁵W istocie pełną strukturę ciała na $\mathbb{C}$ wraz ze strukturą modułu nad ciałem $\mathbb{R}$ można bez trudu zinterpretować w terminach standardowej struktury przestrzeni $\mathbb{R}$ -liniowej z normą (euklidesową) na $\mathbb{R}^2$, wzbogaconej o strukturę modułu nad grupą dylatacji (przeskalowań) i translacji. Taka interpretacja wyprzedza jednak bieg niniejszego kursu i dlatego zostanie (chwilowo) przemilczana.

w połączeniu z układem nierówności

$$-1 \leq \frac{x}{\sqrt{x^2 + y^2}} \leq 1$$

prowadzi do wniosku

$$(3.3) \quad \exists_{\varphi(x,y) \in \mathbb{R}} : \frac{x}{\sqrt{x^2 + y^2}} = \cos \varphi(x, y),$$

przy czym liczba $\varphi(x, y)$ jest określona wysoce niejednoznacznie. Istotnie, jeśli ustalić liczbę $\varphi_0(x, y) \in [0, 2\pi[$ spełniającą warunek definiujący (3.3) (co zawsze jest możliwe), to wówczas wszystkie liczby postaci

$$\epsilon \varphi_0(x, y) + 2k\pi, \quad (\epsilon, k) \in \{+1, -1\} \times \mathbb{Z}$$

także będą go spełniać. Otrzymujemy zatem dwie rodziny rozwiązań warunku definiującego, z których każdą tworzą liczby różniące się o całkowitą wielokrotność liczby 2π . Ustalenie rodziny, do której należy $\varphi(x, y)$, odpowiada wyborowi znaku $\epsilon' \in \{+1, -1\}$ w równości

$$\frac{y}{\sqrt{x^2 + y^2}} = \epsilon' \cdot \sin \varphi(x, y)$$

będącej konsekwencją warunku definiującego i „jedynki trygonometrycznej”. Dalsze sprecyzowanie wartości $\varphi(x, y)$ nie jest możliwe. Poniżej sformalizujemy nasze wnioski, najpierw jednak wprowadzimy pomocne oznaczenia.

NOTACJA 2. Definiujemy **symbol Eulera**⁶ dla dowolnej liczby $\varphi \in \mathbb{R}$

$$e^{i\varphi} := \cos \varphi + i \sin \varphi \in \mathbb{C}, .$$

Ponadto **zbiór liczb zespolonych o module jednostkowym** będziemy oznaczać symbolem

$$U(1) := \{ u \in \mathbb{C} \mid |u| = 1 \}.$$

Istotne własności symbolu Eulera są opisane w

STWIERDZENIE 6. Dla dowolnych $\varphi, \varphi_1, \varphi_2 \in \mathbb{R}$ prawdziwe są zdania:

- (i) $e^{i\varphi} \in U(1)$;
- (ii) $(e^{i\varphi})^{-1} = \overline{e^{i\varphi}} = e^{-i\varphi}$;
- (iii) $e^{i\varphi_1} \cdot e^{i\varphi_2} = e^{i(\varphi_1 + \varphi_2)}$ (wzór de Moivre'a);
- (iv) $e^{i\varphi_1} = e^{i\varphi_2} \iff \varphi_2 - \varphi_1 \in 2\pi\mathbb{Z}$.

■

Zauważmy też, że

STWIERDZENIE 7. Przyjmijmy notację Def. 14 oraz 18. Zbiór $U(1)$ jest nośnikiem naturalnej struktury grupy przemiennej względem operacji 2-argumentowej (indukowanej z $\mathbb{C}$)

$$U(1) \times U(1) \longrightarrow U(1) : (u_1, u_2) \longmapsto u_1 \cdot u_2$$

⁶Drugoroczny kurs analizy matematycznej pozwoli zrozumieć symbol Eulera jako wartość przyjmowaną przez funkcję wykładniczą zmiennej zespolonej w wyróżnionym punkcie $i\varphi$ jej dziedziny, przez co podana tu definicja zyska status twierdzenia.

oraz operacji 1-argumentowej

$$\text{Inv} : \mathbf{U}(1) \ni u \mapsto \bar{u},$$

z których pierwsza ma element neutralny $e = 1 \in \mathbf{U}(1)$.

■

W interpretacji geometrycznej zbiór $\mathbf{U}(1)$ jest okręgiem jednostkowym $\mathbb{S}^1 = \mathcal{O}((0,0);1)$ na płaszczyźnie kartezjańskiej o środku w punkcie o współrzędnych $(0,0)$ (i promieniu $r = 1$), co pokazuje parametryzacja

$$\mathbf{U}(1) = \{ e^{i\varphi} \mid \varphi \in \mathbb{R} \}.$$

Możemy teraz sformułować przydatne

TWIERDZENIE 3.2 (O rozkładzie biegunowym i prezentacji trygonometrycznej liczby zespolonej). *W notacji Def. 14*

$$\forall z \in \mathbb{C}^\times \exists!_{(r,u) \in \mathbb{R}_{>0} \times \mathbf{U}(1)} : z = r \cdot u,$$

przy czym

$$\forall u \in \mathbf{U}(1) \exists \varphi \in \mathbb{R} : u = e^{i\varphi}.$$

■

Dowód: Rzeczony rozkład istnieje, bo dowolne $z \in \mathbb{C}^\times$ możemy zapisać w postaci $z = |z| \cdot \frac{z}{|z|}$, przy czym $r = |z| \in \mathbb{R}_{>0}$ i $u = \frac{z}{|z|} \in \mathbf{U}(1)$. Zarazem rozkład ten jest jedyny, gdyż dla dowolnego takiego rozkładu $z = r \cdot u$ zachodzi – na mocy Stw. 4 (ii) – $|z| \equiv |r \cdot u| = |r| \cdot |u| = r \cdot 1 = r$, czyli też $z = |z| \cdot u$, a stąd $u = \frac{z}{|z|}$. □

Zaobserwowaną wcześniej nieusuwalną niejednoznaczność określenia liczby $\varphi(\Re(z), \Im(z))$ przypisanej danej liczbie zespolonej $z \in \mathbb{C}^\times$ zgrabnie kwantyfikuje

DEFINICJA 19. W notacji Def. 14 **argument liczby zespolonej** (niezerowej) to odwzorowanie

$$\text{Arg} : \mathbb{C}^\times \longrightarrow \mathbb{R}/2\pi\mathbb{Z} : z \mapsto \{ \varphi \in \mathbb{R} \mid z = |z| \cdot e^{i\varphi} \},$$

przy czym $\mathbb{R}/2\pi\mathbb{Z}$ oznacza tu zbiór klas abstrakcji w $\mathbb{R}$ względem relacji równoważności – zapisanej dla dowolnych $x, y \in \mathbb{R}$ –

$$x \sim y \iff x - y \in 2\pi\mathbb{Z}.$$

Argument główny liczby $z \in \mathbb{C}^\times$ to reprezentant

$$\arg(z) \in \text{Arg}(z) \cap [0, 2\pi[.$$

▲

Elementarne własności argumentu zbiera

STWIERDZENIE 8. W notacji Def. 14 oraz 19 i dla dowolnych $z, z_1, z_2 \in \mathbb{C}^\times$ zachodzi, co następuje:

- (i) $\text{Arg}(z_1 \cdot z_2) = \text{Arg}(z_1) + \text{Arg}(z_2)$, przy czym prawa strona wypisanej równości jest sumą algebraiczną podzbiorów grupy przemiennej $(\mathbb{R}, +, x \mapsto -x, \bullet \mapsto 0)$ (rozumianą w sensie Konw. 4).

- (ii) $\text{Arg}(z^{-1}) = \text{Arg}(\bar{z}) = -\text{Arg}(z)$, przy czym prawa strona wypisanego ciągu równości jest przeciwnością algebraiczną podzbioru wspomnianej grupy przemiennej.
- (iii) $z_1 = z_2 \iff (|z_1| = |z_2| \wedge \text{Arg}(z_1) = \text{Arg}(z_2))$.

■

Dowód: Jedynym nietrywialnym punktem powyższego stwierdzenia jest punkt (i), którego prawdziwości dowiedzimy.

Niech $\varphi \in \text{Arg}(z_1 \cdot z_2)$ i wybierzmy dowolne $\varphi_1 \in \text{Arg}(z_1)$, a wtedy na mocy Stw. 4 (ii) i 6 (iii) zachodzi $|z_2| \cdot e^{i(\varphi - \varphi_1)} = \frac{|z_1 \cdot z_2| \cdot e^{i\varphi}}{|z_1| \cdot e^{i\varphi_1}} = \frac{z_1 \cdot z_2}{z_1} = z_2$, zatem wprost z definicji $\varphi - \varphi_1 \in \text{Arg}(z_2)$, co oznacza, że $\text{Arg}(z_1 \cdot z_2) \subset \text{Arg}(z_1) + \text{Arg}(z_2)$.

I odwrotnie,

$$\begin{aligned} \varphi_\alpha \in \text{Arg}(z_\alpha), \alpha \in \{1, 2\} &\implies |z_1 \cdot z_2| \cdot e^{i(\varphi_1 + \varphi_2)} = |z_1| \cdot e^{i\varphi_1} \cdot |z_2| \cdot e^{i\varphi_2} = z_1 \cdot z_2 \\ &\implies \varphi_1 + \varphi_2 \in \text{Arg}(z_1 \cdot z_2) \\ &\implies \text{Arg}(z_1) + \text{Arg}(z_2) \subset \text{Arg}(z_1 \cdot z_2). \end{aligned}$$

□

Należy podkreślić, że własność (i) ze Stw. 8 nie jest dziedziczona przez żadnego reprezentanta klasy funkcji $\Phi : \mathbb{C}^\times \longrightarrow \mathbb{R}$ o własności $\Phi(z) \in \text{Arg}(z)$.

STWIERDZENIE 9. W notacji Def. 14 i 19 nie istnieje funkcja $\Phi : \mathbb{C}^\times \longrightarrow \mathbb{R}$ o własnościach

$$\forall_{z, z_1, z_2 \in \mathbb{C}^\times} : (\Phi(z) \in \text{Arg}(z) \wedge \Phi(z_1 \cdot z_2) = \Phi(z_1) + \Phi(z_2)).$$

■

Dowód: (A.a.) Niechaj Φ będzie taką funkcją. Wówczas $\Phi(1) + \Phi(1) = \Phi(1 \cdot 1) = \Phi(1) = \Phi((-1) \cdot (-1)) = \Phi(-1) + \Phi(-1)$, zatem $\Phi(1) = 0$, skąd też $\Phi(-1) = 0$, ale w takim razie $-1 = |-1| \cdot e^{i\Phi(-1)} = e^{i0} = 1$, czyli sprzeczność. □

Możemy już teraz bez trudu zinterpretować geometrycznie operację mnożenia liczb zespolonych: oto wymnożenie danej liczby z przez liczbę o rozkładzie biegunowym $\zeta = r \cdot e^{i\varphi}$ sprowadza się do przeskalowania wektora $\vec{z}$ o czynnik r , a następnie obrócenia go o kąt φ wokół punktu zaczepienia. Również operacja brania odwrotności niezerowej liczby zespolonej z nabiera prostego sensu geometrycznego złożenia odwzorowania końca wektora $\vec{z}$ w punkt doń sprzężony względem okręgu jednostkowego z odbiciem w prostej o wektorze kierunkowym $\overrightarrow{[(0, 0); (1, 0)]}$.

Rozkład biegunowy liczby zespolonej okazuje się szczególnie wygodny w analizie potęgowania (wzór de Moivre'a) i pierwiastkowania. Zajmiemy się teraz szczególnie tą drugą, mniej trywialną operacją.

DEFINICJA 20. W notacji Def. 14 i dla dowolnych $z \in \mathbb{C}$ oraz $n \in \mathbb{N} \setminus \{0\}$ **pierwiastek stopnia n z z** to zbiór

$$\sqrt[n]{z} := \{ w \in \mathbb{C} \mid w^n = z \}.$$



Łatwo się przekonać, że dla $n > 1$ zbiór ten *nie* jest singletonem.

STWIERDZENIE 10. W notacji Def. 20 i dla dowolnych $(r, \varphi) \in \mathbb{R}_{\geq 0} \times \mathbb{R}$ jest

$$\sqrt[n]{r \cdot e^{i\varphi}} = \left\{ r^{\frac{1}{n}} \cdot e^{i\frac{\varphi+2\pi k}{n}} \mid k \in \overline{0, n-1} \right\}.$$



Dowód: Zauważmy, że na mocy Stw. 6 i 8 zachodzi

$$\begin{aligned} \rho \cdot e^{i\psi} \in \sqrt[n]{r \cdot e^{i\varphi}} &\iff \rho^n \cdot e^{in\psi} = r \cdot e^{i\varphi} \iff \left(\rho^n = r \wedge e^{in\psi} = e^{i\varphi} \right) \\ &\iff \left(\rho = r^{\frac{1}{n}} \wedge \exists_{k \in \mathbb{Z}} : n\psi - \varphi = 2\pi k \right) \\ &\iff \left(\rho = r^{\frac{1}{n}} \wedge \exists_{k \in \mathbb{Z}} : \psi = \frac{\varphi + 2\pi k}{n} \right), \end{aligned}$$

przy czym $\psi' = \psi + 2\pi l$, $l \in \mathbb{Z}$ spełnia równość $\rho \cdot e^{i\psi'} = \rho \cdot e^{i\psi}$, skąd teza wobec implikacji

$$k \mapsto k + n \implies \frac{\varphi + 2\pi k}{n} \mapsto \frac{\varphi + 2\pi k}{n} + 2\pi.$$



Proste intuicje dotyczące zachowania pierwiastka (rozumianego jako liczba) w dziedzinie rzeczywistej pozostają w mocy po przeniesieniu ich na poziom odnośnych zbiorów.

STWIERDZENIE 11. W notacji Def. 14 i 20 jest

$$\forall_{n \in \mathbb{N} \setminus \{0\}} \forall_{z_1, z_2 \in \mathbb{C}} : \sqrt[n]{z_1 \cdot z_2} = \sqrt[n]{z_1} \cdot \sqrt[n]{z_2}.$$



Dowód: Zaczniemy od tego, że ilekroć $z_1 = 0$, teza przyjmuje trywialną postać $\{0\} = \{0\}$, możemy zatem ograniczyć się do przypadku $z_1 \neq 0$.

Niechaj $w \in \sqrt[n]{z_1 \cdot z_2}$ i wybierzmy dowolne $w_1 \in \sqrt[n]{z_1}$, a wtedy $w_2 := \frac{w}{w_1}$ spełnia $w_2^n \equiv \left(\frac{w}{w_1}\right)^n = \frac{w^n}{w_1^n} = \frac{z_1 \cdot z_2}{z_1} = z_2$, czyli $w_2 \in \sqrt[n]{z_2}$, skąd też $w = w_1 \cdot w_2 \in \sqrt[n]{z_1} \cdot \sqrt[n]{z_2}$. Jest więc

$$\sqrt[n]{z_1 \cdot z_2} \subset \sqrt[n]{z_1} \cdot \sqrt[n]{z_2}.$$

I odwrotnie, gdy $w_\alpha \in \sqrt[n]{z_\alpha}$, $\alpha \in \{1, 2\}$, to zachodzi $(w_1 \cdot w_2)^n = w_1^n \cdot w_2^n = z_1 \cdot z_2$, czyli $w_1 \cdot w_2 \in \sqrt[n]{z_1 \cdot z_2}$. Jest przeto

$$\sqrt[n]{z_1} \cdot \sqrt[n]{z_2} \subset \sqrt[n]{z_1 \cdot z_2}.$$

Ostatecznie więc

$$\sqrt[n]{z_1 \cdot z_2} = \sqrt[n]{z_1} \cdot \sqrt[n]{z_2}.$$

□

Wieloznaczność (w sensie liczbowym) odwzorowania Arg pociąga za sobą tę samą własność pierwiastka.

STWIERDZENIE 12. *W notacji Def. 14 i 20 nie istnieje funkcja $p_n : \mathbb{C} \rightarrow \mathbb{C}$ o własnościach*

$$\forall_{z, z_1, z_2 \in \mathbb{C}} : \left(p_n(z) \in \sqrt[n]{z} \quad \wedge \quad p_n(z_1 \cdot z_2) = p_n(z_1) \cdot p_n(z_2) \right).$$

■

Dowód: (A.a.) Niechaj p_n będzie taką funkcją, wobec czego

$$\forall_{z \in \mathbb{C}} : p_n(z^n) = (p_n(z))^n = z.$$

Wówczas dla $e^{\frac{2\pi i}{n}}$, $n \in \mathbb{N} \setminus \{0, 1\}$ zachodzi $1 = p_n(1^n) = p_n(1) = p_n\left(\left(e^{\frac{2\pi i}{n}}\right)^n\right) = e^{\frac{2\pi i}{n}}$, czyli sprzeczność. □

* * *

Literatura uzupełniająca: Więcej o liczbach zespolonych, w ujęciu algebraicznym i geometrycznym, można znaleźć w książce Andreescu i Andriki [AA06].

Wielomiany

Drugą modelową strukturą algebraiczną, którą omówimy na niniejszym wykładzie, jest struktura pierścienia. Pierścienie odegrają istotną rolę na późniejszych etapach kursu – tym poświęconym teorii modułów nad pierścieniami (i przestrzeni wektorowych) oraz tym wprowadzającym nas w dziedzinę algebry homologicznej. Tymczasem jednak skupimy się na dość technicznych aspektach struktury pierścienia, niezbędnych do zrozumienia kluczowej cechy ciała liczb zespolonych odróżniającej je od ciała liczb rzeczywistych, jaką jest jego algebraiczna domkniętość. Wybór celu tej części wykładu wytycza zarazem jasno najkrótszą ścieżkę dojścia do niego, którą będziemy podążać. Wiedzie ona przez zwięzłą analizę podstawowych własności pierścienia wielomianów o współczynnikach z ciała. O powszechności i praktycznym znaczeniu tych ostatnich w algebrze i analizie matematycznej nie potrzebujemy Czytelnika przekonywać, wystarczy wspomnieć o wielomianie Taylora oraz wielomianach interpolujących, o wielomianowych funkcjach specjalnych, jak również o wielomianach charakterystycznych endomorfizmów przestrzeni wektorowych. Godzi się także zaznaczyć w tym miejscu, że nieco bardziej abstrakcyjne podejście do teorii ciał pozwala zrozumieć strukturę ciała liczb zespolonych jako „minimalne” rozszerzenie struktury ciała liczb rzeczywistych o pierwiastek wielomianu nierozkładalnego (nad $\mathbb{R}$) $t^2 + 1$. Jak się okazuje, konstrukcję tę można prosto uogólnić, dochodząc w ten sposób do teorii rozszerzeń algebraicznych, czego jednak nie będziemy tutaj czynić¹.

4.1. Struktura pierścienia i jej transport

Tytułem przygotowania do dyskusji właściwej wypiszmy

DEFINICJA 21. **Pierścień** to szóstka $(R, A, M, P, \mathbf{0}, \mathbf{1})$, w której

- R jest zbiorem;
- $A : R^{\times 2} \longrightarrow R : (x, y) \mapsto A(x, y) \equiv x +_R y$ jest operacją 2-argumentową zwaną **dodawaniem**;
- $M : R^{\times 2} \longrightarrow R : (x, y) \mapsto M(x, y) \equiv x \cdot_R y$ jest operacją 2-argumentową zwaną **mnożeniem**;
- $P : R \longrightarrow R : x \mapsto P(x) \equiv -x$ jest operacją 1-argumentową zwaną **braniem przeciwności**;
- $\mathbf{0} : \{\bullet\} \longrightarrow R : \bullet \mapsto 0$ jest operacją 0-argumentową zwaną **zerem**;
- $\mathbf{1} : \{\bullet\} \longrightarrow R : \bullet \mapsto 1$ jest operacją 0-argumentową zwaną **jedynką**,

przy czym składowe struktury spełniają następujące aksjomaty (wyrażone przez diagramy przemienne i równoważne zdania logiczne):

¹Zainteresowanego Czytelnika odsyłamy choćby do wykładów Langa [Lan02, Rozdz. V] i Cohna [Coh89, Rozdz. 3].

(R1) (łączność działań)

$$\begin{array}{ccc}
R \times R \times R & \xrightarrow{A \times \text{id}_R} & R \times R \\
\text{id}_R \times A \downarrow & & \downarrow A \\
R \times R & \xrightarrow{A} & R
\end{array} \quad \equiv \quad \forall_{x,y,z \in R} : (x +_R y) +_R z = x +_R (y +_R z);$$

$$\begin{array}{ccc}
R \times R \times R & \xrightarrow{M \times \text{id}_R} & R \times R \\
\text{id}_R \times M \downarrow & & \downarrow M \\
R \times R & \xrightarrow{M} & R
\end{array} \quad \equiv \quad \forall_{x,y,z \in R} : (x \cdot_R y) \cdot_R z = x \cdot_R (y \cdot_R z);$$

(R2) (przemienność dodawania)

$$\begin{array}{ccc}
R \times R & \xrightarrow{\tau_R} & R \times R \\
& \searrow A & \downarrow A \\
& & R
\end{array} \quad \equiv \quad \forall_{x,y \in R} : x +_R y = y +_R x;$$

(R3) (rozdzielność mnożenia względem dodawania)

$$\begin{array}{ccc}
R \times R \times R & \xrightarrow{\text{id}_R \times A} & R \times R \\
(M \circ \text{pr}_{1,2}, M \circ \text{pr}_{1,3}) \downarrow & & \downarrow M \\
R \times R & \xrightarrow{A} & R
\end{array} \quad \equiv \quad \forall_{x,y,z \in R} : \begin{array}{l} x \cdot_R (y +_R z) \\ = (x \cdot_R y) +_R (x \cdot_R z) \end{array};$$

$$\begin{array}{ccc}
R \times R \times R & \xrightarrow{A \times \text{id}_R} & R \times R \\
(M \circ \text{pr}_{1,3}, M \circ \text{pr}_{2,3}) \downarrow & & \downarrow M \\
R \times R & \xrightarrow{A} & R
\end{array} \quad \equiv \quad \forall_{x,y,z \in R} : \begin{array}{l} (x +_R y) \cdot_R z \\ = (x \cdot_R z) +_R (y \cdot_R z) \end{array};$$

(R4) (istnienie elementów neutralnych względem działań)

$$\begin{array}{ccc}
R \times \{\bullet\} & \xrightarrow{\text{id}_R \times \mathbf{0}} & R \times R \\
& \searrow \text{pr}_1 & \downarrow A \\
& & R
\end{array} \quad \equiv \quad \forall_{x \in R} : x +_R \mathbf{0} = x;$$

$$\begin{array}{ccc}
R \times \{\bullet\} & \xrightarrow{\text{id}_R \times \mathbf{1}} & R \times R \\
& \searrow \text{pr}_1 & \downarrow M \\
& & R
\end{array}, \quad \begin{array}{ccc}
\{\bullet\} \times R & \xrightarrow{\mathbf{1} \times \text{id}_R} & R \times R \\
& \searrow \text{pr}_2 & \downarrow M \\
& & R
\end{array}$$

$$\equiv \quad \forall_{x \in R} : x \cdot_R \mathbf{1} = x = \mathbf{1} \cdot_R x;$$

(R5) (istnienie elementów przeciwnych)

$$\begin{array}{ccc}
 \mathbb{K} \times \{\bullet\} & \xrightarrow{(\text{id}_R, P) \circ \text{pr}_1} & R \times R \\
 & \searrow \text{0} \circ \text{pr}_2 & \downarrow A \\
 & & R
 \end{array} \quad \equiv \quad \forall_{x \in R} : x +_R (-x) = 0.$$

Pierścień przeciwny do $(R, A, M, P, \mathbf{0}, \mathbf{1})$ to pierścień $(R, A, M^{\text{opp}}, P, \mathbf{0}, \mathbf{1})$ z mnożeniem danym wzorem

$$M^{\text{opp}} := M \circ \tau_R.$$

Pierścień przemienny to taki, w którym mnożenie jest operacją przemenną, co wyraża następujący diagram przemienności (wypisany wraz z równoważnym zdaniem logicznym):

$$\begin{array}{ccc}
 R \times R & \xrightarrow{\tau_R} & R \times R \\
 & \searrow M & \downarrow M \\
 & & R
 \end{array} \quad \equiv \quad \forall_{x, y \in R} : x \cdot_R y = y \cdot_R x.$$

Dziedzina całkowitości to pierścień przemienności o własności

$$(\text{ID}) \quad \forall_{x, y \in R} : (x \cdot_R y = 0 \implies (x = 0 \vee y = 0)),$$

która wyraża brak nietrywialnych dzielników zera.

Dziedzina euklidesowa (zwana też **pierścieniem euklidesowym**) to para $((R, A, M, P, \mathbf{0}, \mathbf{1}), \delta)$, w której $(R, A, M, P, \mathbf{0}, \mathbf{1})$ jest dziedziną całkowitości, δ zaś jest odwzorowaniem

$$\delta : R \setminus \{0\} \longrightarrow \mathbb{N},$$

zwanym **normą euklidesową**, o własnościach

$$(\text{ED1}) \quad \forall_{\substack{a \in R \\ b \in R \setminus \{0\}}} \exists_{q, r \in R} : (a = q \cdot_R b +_R r \quad \wedge \quad (r = 0 \vee \delta(r) < \delta(b)));$$

$$(\text{ED2}) \quad \forall_{a, b \in R \setminus \{0\}} : \delta(a) \leq \delta(a \cdot_R b).$$

▲

PRZYKŁAD(Y) 12.

(1) **Pierścień trywialny**: $(\{0 = 1\}, (0, 0) \mapsto 0, (0, 0) \mapsto 0, 0 \mapsto 0, 0 \mapsto 0, \bullet \mapsto 0, \bullet \mapsto 0)$.

(2) Szóstka $(\mathbb{Z}/(p \cdot q)\mathbb{Z}, ([k]_{p \cdot q}, [l]_{p \cdot q}) \mapsto [k + l]_{p \cdot q}, ([k]_{p \cdot q}, [l]_{p \cdot q}) \mapsto [k \cdot l]_{p \cdot q}, [k]_{p \cdot q} \mapsto [p \cdot q - k]_{p \cdot q}, \bullet \mapsto [0]_{p \cdot q}, \bullet \mapsto [1]_{p \cdot q})$, określona dla dowolnych liczb $p, q \in \mathbb{N} \setminus \{0, 1\}$ (patrz: Przykł. 8), jest pierścieniem przemiennym nie będącym dziedziną całkowitości (bo np. iloczyn niezerowych liczb $[p]_{p \cdot q}$ i $[q]_{p \cdot q}$ jest równy $[0]_{p \cdot q}$).

(3) Zbiór $C([0, 1], \mathbb{R})$ funkcji ciągłych na odcinku $[0, 1] \subset \mathbb{R}$ o wartościach rzeczywistych z dodawaniem, mnożeniem i braniem przeciwności zdefiniowanymi punktowo,

$$(f + g)(x) := f(x) + g(x), \quad (f \cdot g)(x) := f(x) \cdot g(x), \quad (-f)(x) := -f(x),$$

dla dowolnych $f, g \in C([0, 1], \mathbb{C})$ i $x \in [0, 1]$, oraz z funkcją zerową

$$0 : [0, 1] \longrightarrow \{0\} : x \longmapsto 0$$

jako elementem neutralnym dodawania, a także funkcją stałą

$$1 : [0, 1] \longrightarrow \{1\} : x \longmapsto 1$$

jako elementem neutralnym mnożenia jest pierścieniem przemennym nie będącym dziedziną całkowitości (wystarczy rozważyć funkcje $f_1 : x \longmapsto \max(\frac{1}{4} - |x - \frac{1}{4}|, 0)$ oraz $f_2 : x \longmapsto \max(\frac{1}{4} - |x - \frac{3}{4}|, 0)$).

- (4) Dla dowolnego zbioru X szóstka $(2^X, \Delta, \cap, \text{id}_X, \bullet \longmapsto \emptyset, \bullet \longmapsto X)$, w której 2^X jest zbiorem potęgowym zbioru X (czyli zbiorem wszystkich jego podzbiorów), Δ zaś jest różnicą symetryczną zbiorów,

$$A \Delta B := (A \setminus B) \cup (B \setminus A), \quad A, B \in 2^X,$$

jest pierścieniem przemennym nie będącym dziedziną całkowitości, o ile tylko $|X| > 1$. Jest to przykład tzw. **pierścień Boole'a**, którego dowolny element $A \in 2^X$ jest idempotentem, tj. spełnia tożsamość $A \cap A = A$.

- (5) Dla dowolnego pierścienia R zbiór $\text{Mat}(2 \times 2; R)$ *wszystkich* macierzy wymiaru 2×2 o wyrazach z R z mnożeniem i elementem neutralnym dla mnożenia jak w Przykł. 9 (2), a ponadto z dodawaniem

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right) \longmapsto \begin{pmatrix} a+Re & b+Rf \\ c+Rg & d+Rh \end{pmatrix},$$

elementem neutralnym dla dodawania

$$\bullet \longmapsto \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

oraz operacją brania przeciwności

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$$

jest pierścieniem nieprzemennym.

- (6) Szóstka $(\mathbb{Z}[\frac{1+i\sqrt{19}}{2}], +_{\mathbb{C}}, \cdot_{\mathbb{C}}, \text{P}_{\mathbb{C}}, \bullet \longmapsto 0, \bullet \longmapsto 1)$, w której

$$\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right] := \left\{ m +_{\mathbb{C}} n \cdot \frac{1+i\sqrt{19}}{2} \mid m, n \in \mathbb{Z} \right\} \subset \mathbb{C},$$

jest dziedziną całkowitości. Można też pokazać, że nie jest to pierścień euklidesowy.

- (7) Zbiór $\mathbb{Z}^{\times 2} \ni (m, n), (m_1, n_1), (m_2, n_2)$ z dodawaniem

$$((m_1, n_1), (m_2, n_2)) \longmapsto (m_1 + m_2, n_1 + n_2)$$

o elemencie neutralnym $(0, 0)$, z mnożeniem

$$((m_1, n_1), (m_2, n_2)) \longmapsto (m_1 \cdot m_2 - n_1 \cdot n_2, m_1 \cdot n_2 + n_1 \cdot m_2 - n_1 \cdot n_2)$$

o elemencie neutralnym $(1, 0)$, oraz z braniem przeciwności

$$(m, n) \longmapsto (-m, -n)$$

jest pierścieniem euklidesowym z normą

$$\delta(m, n) := m^2 + n^2 - m \cdot n.$$

Można go zrealizować jako **zbiór liczb całkowitych Eisensteina**

$$\mathbb{Z}[\omega] := \{ m +_{\mathbb{C}} n \cdot \omega \mid m, n \in \mathbb{Z} \},$$

określony dla dowolnego elementu $\omega \in \sqrt[3]{1} \setminus \{1\}$, z operacjami indukowanymi z $\mathbb{C}$.

✓

Mamy też

DEFINICJA 22. W notacji Def. 21 **podpierścień** pierścienia $(R, A, M, P, \mathbf{0}, \mathbf{1})$ to szóstka $(Q, A, M, P, \mathbf{0}, \mathbf{1})$, w której Q jest podzbiorem R o następujących własnościach:

- (SR1) $A : Q^{\times 2} \longrightarrow Q \subset R$;
- (SR2) $M : Q^{\times 2} \longrightarrow Q \subset R$;
- (SR3) $P : Q \longrightarrow Q \subset R$;
- (SR4) $Q \ni 1$.

Podpierścień o własności

$$(I) \quad M : R \times Q \longrightarrow Q \subset R \quad (\text{wzgl. } M : Q \times R \longrightarrow Q \subset R)$$

nazywamy **ideałem lewostronnym** (wzgl. **prawostronnym**) pierścienia R . **Ideał obustronny** to taki, który jest zarówno lewo- jak i prawostronny. **Ideał główny** to ideał spełniający warunek

$$(PI) \quad \exists_{q_* \in R} \forall_{q \in Q} \exists_{r \in R} : q = r \cdot_R q_* \quad (\text{wzgl. } \exists_{q_* \in R} \forall_{q \in Q} \exists_{r \in R} : q = q_* \cdot_R r),$$

co zapisujemy jako

$$Q = \langle q_* \rangle_R.$$

Pierścień przemienny, w którym każdy ideał jest główny, nosi miano **pierścienia ideałów głównych**. Jeśli pierścień ten jest dodatkowo dziedziną całkowitości, to mówimy o **dziedzinie ideałów głównych**.

▲

W późniejszych zastosowaniach teorii pierścieni przydatnym okaże się następujące

STWIERDZENIE 13. *Każdy pierścień euklidesowy jest dziedziną ideałów głównych.*

■

Dowód: Niechaj $J \subset R$ będzie ideałem w pierścieniu R . W przypadku $J = \{0_R\}$ teza jest trywialnie spełniona, przyjmijmy zatem, że $J \neq \{0_R\}$. Określmy

$$n := \min_{q \in J \setminus \{0_R\}} \{\delta(q)\}$$

i niech $q_* \in J$ będzie dowolnym elementem ideału o własności $\delta(q_*) = n$. Na mocy (ED1) każdy $q \in J$ można przedstawić w postaci

$$q = q_* \cdot_R r +_R s,$$

gdzie $r, s \in R$, przy czym albo $s = 0_R$, albo też $\delta(s) < \delta(q_*) = n$. W tym drugim przypadku stwierdzamy, że $s = q +_R P_R(q_* \cdot_R r) \in J +_R J \cdot_R R \subset J$ jest elementem ideału J o własności $\delta(s) < \min_{q' \in J \setminus \{0_R\}} \{\delta(q')\}$, co jest absurdem, a zatem koniecznie $q = q_* \cdot_R r$. To jednak oznacza, że $J \subset q_* \cdot_R R$, z drugiej jednak strony $q_* \cdot_R R \subset J \cdot_R R \subset J$, więc ostatecznie $J = q_* \cdot_R R$, czyli

$$J = \langle q_* \rangle_R.$$

□

Dla utrzymania narzuconego wcześniej porządku logicznego wykładu podajemy jeszcze

DEFINICJA 23. W notacji Def. 21 **homomorfizm pierścienia** $(R^{(1)}, A^{(1)}, M^{(1)}, \mathbf{p}^{(1)}, \mathbf{0}^{(1)}, \mathbf{1}^{(1)})$ w pierścień $(R^{(2)}, A^{(2)}, M^{(2)}, \mathbf{p}^{(2)}, \mathbf{0}^{(2)}, \mathbf{1}^{(2)})$ to odwzorowanie

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

o własnościach wyrażonych przez diagramy przemienne (wypisane wraz z równoważnymi zdaniami logicznymi):

$$(RH1) \quad \begin{array}{ccc} R^{(1)} \times R^{(1)} & \xrightarrow{A^{(1)}} & R^{(1)} \\ \chi \times \chi \downarrow & & \downarrow \chi \\ R^{(2)} \times R^{(2)} & \xrightarrow{A^{(2)}} & R^{(2)} \end{array} \quad \equiv \quad \forall_{x,y \in R^{(1)}} : \quad \begin{array}{l} \chi(x +_{(1)} y) \\ = \chi(x) +_{(2)} \chi(y) \end{array} ;$$

$$(RH2) \quad \begin{array}{ccc} R^{(1)} \times R^{(1)} & \xrightarrow{M^{(1)}} & R^{(1)} \\ \chi \times \chi \downarrow & & \downarrow \chi \\ R^{(2)} \times R^{(2)} & \xrightarrow{M^{(2)}} & R^{(2)} \end{array} \quad \equiv \quad \forall_{x,y \in R^{(1)}} : \quad \begin{array}{l} \chi(x \cdot_{(1)} y) \\ = \chi(x) \cdot_{(2)} \chi(y) \end{array} ;$$

$$(RH3) \quad \begin{array}{ccc} \{\bullet\} & \xrightarrow{\mathbf{1}^{(1)}} & R^{(1)} \\ & \searrow \mathbf{1}^{(2)} & \downarrow \chi \\ & & R^{(2)} \end{array} \quad \equiv \quad \chi(\mathbf{1}^{(1)}) = \mathbf{1}^{(2)} .$$

▲

PRZYKŁAD(Y) 13.

- (1) Dla dowolnego pierścienia R odwzorowanie $\mathbb{Z} \longrightarrow R : n \mapsto \underbrace{1 +_R 1 +_R \cdots +_R 1}_{n \text{ razy}}$ jest homomorfizmem.
- (2) Odwzorowanie ewaluacji $\text{ev}_{\frac{1}{2}} : C([0, 1], \mathbb{R}) \longrightarrow \mathbb{R} : f \mapsto f(\frac{1}{2})$ jest epimorfizmem pierścienia z Przykł. 12 (3) na pierścień $(\mathbb{R}, +_{\mathbb{R}}, \cdot_{\mathbb{R}}, P_{\mathbb{R}}, \bullet \mapsto [(\frac{0}{1})_{n \in \mathbb{N}}]_{\sim}, \bullet \mapsto [(\frac{1}{1})_{n \in \mathbb{N}}]_{\sim})$.
- (3) Odwzorowanie $\mathbb{C} \longrightarrow \text{Mat}(2 \times 2; \mathbb{R}) : x + iy \mapsto \begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ jest monomorfizmem pierścienia $(\mathbb{C}, +_{\mathbb{C}}, \cdot_{\mathbb{C}}, P_{\mathbb{C}}, \mathbf{0}_{\mathbb{C}}, \mathbf{1}_{\mathbb{C}})$ w pierścień z Przykł. 12 (5).

✓

4.2. Wielomiany

Możemy już teraz określić przedmiot naszego bezpośredniego zainteresowania

DEFINICJA 24. Przyjmijmy notację Def. 6, 67 oraz 14. Niechaj $(T := \{t^n\}_{n \in \mathbb{Z}}, \phi_2, \phi_1, \phi_0)$ będzie grupą przemenną z operacją 2-argumentową

$$\phi_2 : T^{\times 2} \longrightarrow T : (t^m, t^n) \longmapsto t^{m+n}$$

o elemencie neutralnym danym przez operację 0-argumentową

$$\phi_0 : \{\bullet\} \longrightarrow T : \bullet \longmapsto t^0$$

oraz z operacją 1-argumentową

$$\phi_1 : T \curvearrowright : t^n \longmapsto t^{-n},$$

przy czym zakładamy, że

$$\forall_{m,n \in \mathbb{Z}} : (t^m = t^n \iff m = n).$$

Rozważmy stowarzyszony z tą grupą monoid $(T_{\geq 0} := \{t^n\}_{n \in \mathbb{N}}, \phi_2, \phi_0)$ i niech $(\mathbb{K}, +_{\mathbb{K}}, \cdot_{\mathbb{K}}, \mathbf{P}_{\mathbb{K}}, \text{Inv}_{\mathbb{K}}, \bullet \mapsto 0_{\mathbb{K}}, \bullet \mapsto 1_{\mathbb{K}})$ będzie ciałem. **Zbiór wielomianów o współczynnikach z $\mathbb{K}$** to zbiór odwzorowań

$$\mathbb{K}[t] := \{ w : T_{\geq 0} \longrightarrow \mathbb{K} \mid \exists_{N \in \mathbb{N}} \forall_{n > N} : w(t^n) = 0_{\mathbb{K}} \}.$$

W szczególności odwzorowanie

$$\mathbf{0} : T_{\geq 0} \longrightarrow \mathbb{K} : t^n \longmapsto 0_{\mathbb{K}}$$

określamy mianem **wielomianu zerowego**. Wielomiany o 1-elementowym przeciwobrazie $\mathbb{K} \setminus \{0_{\mathbb{K}}\}$,

$$\lambda_n t^n : T_{\geq 0} \longrightarrow \mathbb{K} : t^m \longmapsto \begin{cases} \lambda_n & \text{dla } m = n \\ 0_{\mathbb{K}} & \text{dla } m \neq n \end{cases}$$

zadane dla dowolnych $\lambda_n \in \mathbb{K}$ i $n \in \mathbb{N}$, nazywamy **jednomianami**. ▲

Powyższa definicja każe w oczywisty sposób utożsamiać wielomiany z rodzinami elementów $\mathbb{K}$ indeksowanymi przez $\mathbb{N}$ (czyli ciągami) o skończonym nośniku. Ta ostatnia cecha nadaje sens wygodnemu zapisowi wielomianów, który będziemy od-tąd stosować.

NOTACJA 3. W notacji Def. 6, 67, 11 i 24 wielomian $w \in \mathbb{K}[t]$ zadany przez układ warunków

$$w(t^n) := \begin{cases} \lambda_n & \text{dla } n \leq N \\ 0_{\mathbb{K}} & \text{dla } n > N \end{cases},$$

określonych dla pewnych elementów $\lambda_n \in \mathbb{K}$ oraz pewnej liczby $N \in \mathbb{N}$, będziemy zapisywać zamiennie w postaci sumy skończonej

$$w = \sum_{n=0}^N \lambda_n t^n$$

lub też sumy nieskończonej

$$w = \sum_{n=0}^{\infty} \lambda_n t^n,$$

przy czym w tej ostatniej kładziemy $\forall_{n \geq N} : \lambda_n = 0_{\mathbb{K}}$. W tym zapisie elementy $\lambda_n \in \mathbb{K}$ noszą miano **współczynników wielomianu** w , element $t \in T$ zaś – jego **zmiennej (formalnej)**.

* * *

Możemy już teraz dokonać istotnego rozróżnienia.

DEFINICJA 25. W notacji Def. 6, 67, 11 i 24 **funkcja wielomianowa stowarzyszona z wielomianem** $w = \sum_{n=0}^N \lambda_n t^n \in \mathbb{K}[t]$ to odwzorowanie

$$F_w : \mathbb{K} \circlearrowleft : \mu \mapsto \lambda_0 +_{\mathbb{K}} (\lambda_1 \cdot_{\mathbb{K}} \mu) +_{\mathbb{K}} (\lambda_2 \cdot_{\mathbb{K}} \mu^2) +_{\mathbb{K}} \cdots +_{\mathbb{K}} (\lambda_N \cdot_{\mathbb{K}} \mu^N),$$

przy czym dla dowolnego $n \in \mathbb{N} \setminus \{0\}$ określamy **n -tą potęgę** elementu $\mu \in \mathbb{K}$ jako

$$\mu^n := \underbrace{\mu \cdot_{\mathbb{K}} \mu \cdot_{\mathbb{K}} \cdots \cdot_{\mathbb{K}} \mu}_{n \text{ razy}}.$$

Rozszerzając ten zapis na $n = 0$, jak następuje:

$$\mu^0 := 1_{\mathbb{K}},$$

możemy przepisać F_w w zwartej postaci

$$F_w : \mathbb{K} \circlearrowleft : \mu \mapsto \sum_{n=0}^N \lambda_n \cdot_{\mathbb{K}} \mu^n \equiv \sum_{n=0}^{\infty} \lambda_n \cdot_{\mathbb{K}} \mu^n.$$

Zero wielomianu $w \in \mathbb{K}[t]$ to dowolny element $\mu \in \mathbb{K}$ o własności

$$F_w(\mu) = 0_{\mathbb{K}}.$$

▲

Zbiór wielomianów jest nośnikiem naturalnej struktury algebraicznej.

DEFINICJA 26. W notacji Def. 6, 67, 11 i 24 **pierścień wielomianów o współczynnikach z ciała** $\mathbb{K}$ to szóstka

$$(\mathbb{K}[t], \boxplus, \odot, P_{\mathbb{K}[t]}, \bullet \mapsto 0, \bullet \mapsto 1_{\mathbb{K}} t^0),$$

w której $\boxplus$ i $\odot$ są operacjami 2-argumentowymi na $\mathbb{K}[t]$ określonymi, jak następuje:

$$\begin{aligned} \boxplus & : \mathbb{K}[t]^{\times 2} \longrightarrow \mathbb{K}[t] : \left(\sum_{m=0}^{\infty} \lambda_m t^m, \sum_{n=0}^{\infty} \mu_n t^n \right) \mapsto \sum_{n=0}^{\infty} (\lambda_n +_{\mathbb{K}} \mu_n) t^n, \\ \odot & : \mathbb{K}[t]^{\times 2} \longrightarrow \mathbb{K}[t] : \left(\sum_{m=0}^{\infty} \lambda_m t^m, \sum_{n=0}^{\infty} \mu_n t^n \right) \mapsto \sum_{n=0}^{\infty} \left(\sum_{\substack{k,l=0 \\ k+l=n}}^n \lambda_k \cdot_{\mathbb{K}} \mu_l \right) t^n, \end{aligned}$$

a $P_{\mathbb{K}[t]}$ jest operacją 1-argumentową na $\mathbb{K}[t]$ daną przez

$$P_{\mathbb{K}[t]} : \mathbb{K}[t] \circlearrowleft : \sum_{n=0}^{\infty} \lambda_n t^n \mapsto \sum_{n=0}^{\infty} (-\lambda_n) t^n.$$

▲

Bez trudu dowodzimy

TWIERDZENIE 4.1. *Pierścień wielomianów o współczynnikach z dowolnego ciała jest dziedziną całkowitości.*

■

Dodatkową strukturę na zbiorze $\mathbb{K}[t]$ opisuje

STWIERDZENIE 14. W notacji Def. 6, 67, 11 i 24 struktura modułu nad pierścieniem $(\mathbb{K}, +_{\mathbb{K}}, \cdot_{\mathbb{K}}, P_{\mathbb{K}}, \bullet \mapsto 0_{\mathbb{K}}, \bullet \mapsto 1_{\mathbb{K}})$ na grupie $(\mathbb{K}[t], \boxplus, P_{\mathbb{K}[t]}, \bullet \mapsto \mathbf{0})$ to odwzorowanie

$$\ell_{\mathbb{K}[t]} : \mathbb{K} \times \mathbb{K}[t] \longrightarrow \mathbb{K}[t] : \left(\lambda, \sum_{n=0}^{\infty} \lambda_n t^n \right) \mapsto \sum_{n=0}^{\infty} (\lambda \cdot_{\mathbb{K}} \lambda_n) t^n =: \lambda \cdot \sum_{n=0}^{\infty} \lambda_n t^n$$

o własnościach

$$\lambda \cdot (\mu \cdot w) = (\lambda \cdot_{\mathbb{K}} \mu) \cdot w, \quad 1_{\mathbb{K}} \cdot w = w,$$

$$(\lambda +_{\mathbb{K}} \mu) \cdot w = \lambda \cdot w \boxplus \mu \cdot w, \quad \lambda \cdot (w_1 \boxplus w_2) = \lambda \cdot w_1 \boxplus \lambda \cdot w_2,$$

wypisanych dla dowolnych $\lambda, \mu \in \mathbb{K}$ oraz $w, w_1, w_2 \in \mathbb{K}[t]$. ■

Strukturalny związek między wielomianami i stowarzyszonymi z nimi funkcjami wielomianowymi opisuje dokładnie poniższe oczywiste

STWIERDZENIE 15. Przyjmijmy notację Def. 6, 67, 11, 24, 25 i 26. Odwzorowanie

$$\text{ev}_{\lambda} : \mathbb{K}[t] \longrightarrow \mathbb{K} : w \mapsto F_w(\lambda),$$

określone dla dowolnego elementu $\lambda \in \mathbb{K}$, jest homomorfizmem pierścienia wielomianów o współczynnikach z ciała $\mathbb{K}$ w pierścień $(\mathbb{K}, +_{\mathbb{K}}, \cdot_{\mathbb{K}}, P_{\mathbb{K}}, \mathbf{0}_{\mathbb{K}}, \mathbf{1}_{\mathbb{K}})$ przez to ciało określany. Odwzorowanie to określamy mianem **homomorfizmu ewaluacji**. ■

Mamy też praktyczne

STWIERDZENIE 16. Przyjmijmy notację Def. 6, 67, 11, 24 i 26. Odwzorowanie

$$j : \mathbb{K} \longrightarrow \mathbb{K}[t] : \lambda \mapsto \lambda t^0$$

jest kanonicznym monomorfizmem pierścienia $(\mathbb{K}, +_{\mathbb{K}}, \cdot_{\mathbb{K}}, P_{\mathbb{K}}, \mathbf{0}_{\mathbb{K}}, \mathbf{1}_{\mathbb{K}})$ w pierścień wielomianów o współczynnikach z ciała $\mathbb{K}$. ■

Powyższy monomorfizm pozwala nam utożsamić $\mathbb{K}$ z jego obrazem w $\mathbb{K}[t]$ i tym samym usprawiedliwia zapis

$$\sum_{n=0}^{\infty} \lambda_n t^n \equiv \lambda_0 + \sum_{n=1}^{\infty} \lambda_n t^n.$$

Skończoność nośnika rodziny, indeksowanej przez $\mathbb{N}$, współczynników wielomianu motywuje poniższą

DEFINICJA 27. W notacji Def. 6, 67, 11, 24 i 26 **stopień wielomianu** $w = \sum_{n=0}^{\infty} \lambda_n t^n \neq \mathbf{0}$ to liczba

$$\deg w := \min \{ N \in \mathbb{N} \mid \forall_{n > N} : \lambda_n = 0_{\mathbb{K}} \}.$$

Pojęcie to rozszerzamy na wielomian zerowy, dołączając do zbioru $\mathbb{N}$ stopni wielomianów niezerowych liczbę

$$\deg \mathbf{0} =: -\infty$$

spełniającą (z definicji) proste relacje

$$(-\infty) + (-\infty) = -\infty, \quad (-\infty) + n = -\infty, \quad -\infty < n,$$

wypisane dla dowolnego $n \in \mathbb{N}$.

▲

Elementarne własności funkcji $\deg$ w odniesieniu do operacji algebraicznych na $\mathbb{K}[t]$ zbiera

STWIERDZENIE 17. *Przyjmijmy notację Def. 6, 67, 11, 24, 26 i 27. Dla dowolnych $\lambda \in \mathbb{K}^\times$ oraz $w_1, w_2 \in \mathbb{K}[t]$ prawdziwe są relacje*

- (i) $\deg(w_1 \boxplus w_2) \leq \max(\deg w_1, \deg w_2)$, przy czym $\deg w_1 \neq \deg w_2 \implies \deg(w_1 \boxplus w_2) = \max(\deg w_1, \deg w_2)$;
- (ii) $\deg(w_1 \odot w_2) = \deg w_1 + \deg w_2$;
- (iii) $\deg(\lambda \cdot w) = \deg w$.

■

Algebraiczny sens stopnia wielomianu wyjawia

TWIERDZENIE 4.2 (Algorytm Euklidesa). *Przyjmijmy notację Def. 6, 67, 11, 24, 26 i 27. Para $((\mathbb{K}[t], \boxplus, \odot, \mathbf{P}_{\mathbb{K}[t]}, \bullet \mapsto \mathbf{0}, \bullet \mapsto 1_{\mathbb{K}} t^0), \deg)$ jest dziedziną euklidesową. Ponadto elementy $q, r \in \mathbb{K}[t]$, o których mowa w Def. 21, są określone jednoznacznie.*

■

Dowód: W świetle Tw. 4.1 jedynym, co należy pokazać, jest to, że funkcja $\deg$ spełnia aksjomaty (ED1) oraz (ED2). Drugi z nich jest spełniony w sposób oczywisty, pozostaje zatem upewnić się, że jest też spełniony aksjomat (ED1). Zaczniemy od dowodu istnienia wielomianów $q, r \in \mathbb{K}[t]$. W tym celu ustalmy $b \in \mathbb{K}[t]$, przy czym $\beta := \deg b \geq 0$. Przeprowadzimy teraz (mocną) indukcję względem $\alpha := \deg a$. İlkroć $\alpha < \beta$, para $(q, r) := (\mathbf{0}, a)$ spełnia (ED1). Niechaj zatem $\alpha \geq \beta$, przy czym zakładamy, że dla każdego $\forall \tilde{a} \in \mathbb{K}[t] : (\deg \tilde{a} < \alpha \implies \text{(ED1)})$. Zapiszmy

$$a := \sum_{k=0}^{\alpha} \lambda_k t^k, \quad \lambda_\alpha \neq 0_{\mathbb{K}}, \quad b := \sum_{l=0}^{\beta} \mu_l t^l, \quad \mu_\beta \neq 0_{\mathbb{K}}.$$

Wówczas dla

$$\begin{aligned} \underline{a} := a \boxplus ((-\lambda_\alpha \cdot_{\mathbb{K}} \mu_\beta^{-1}) t^{\alpha-\beta} \odot b) &= \lambda_0 + \lambda_1 t^1 + \lambda_2 t^2 + \dots + \lambda_{\alpha-\beta-1} t^{\alpha-\beta-1} \\ &\quad + (\lambda_{\alpha-\beta} - (\lambda_\alpha \cdot_{\mathbb{K}} \mu_0 \cdot_{\mathbb{K}} \mu_\beta^{-1})) t^{\alpha-\beta} \\ &\quad + (\lambda_{\alpha-\beta+1} - (\lambda_\alpha \cdot_{\mathbb{K}} \mu_1 \cdot_{\mathbb{K}} \mu_\beta^{-1})) t^{\alpha-\beta+1} + \dots \\ &\quad + (\lambda_{\alpha-1} - (\lambda_\alpha \cdot_{\mathbb{K}} \mu_{\beta-1} \cdot_{\mathbb{K}} \mu_\beta^{-1})) t^{\alpha-1} \end{aligned}$$

stwierdzamy $\deg \underline{a} < \alpha$, co wobec założenia indukcyjnego oznacza, że

$$\underline{a} = (\underline{q} \odot b) \boxplus \underline{r}$$

dla pewnych $\underline{q}, \underline{r} \in \mathbb{K}[t]$ o własności $\deg \underline{r} < \deg b = \beta$. Jest zatem

$$a = \underline{a} \boxplus (\lambda_\alpha \cdot_{\mathbb{K}} \mu_\beta^{-1}) t^{\alpha-\beta} \odot b = \underline{q} \odot b \boxplus \underline{r} \boxplus (\lambda_\alpha \cdot_{\mathbb{K}} \mu_\beta^{-1}) t^{\alpha-\beta} \odot b$$

$$= (\underline{q}(\lambda_\alpha \cdot_{\mathbb{K}} \mu_\beta^{-1}) t^{\alpha-\beta}) \odot b \boxplus \underline{r},$$

co daje nam požądane

$$q := \underline{q}(\lambda_\alpha \cdot_{\mathbb{K}} \mu_\beta^{-1}) t^{\alpha-\beta}, \quad r := \underline{r}.$$

Niechaj teraz zachodzi równość

$$\tilde{q} \odot b \boxplus \tilde{r} = a = q \odot b \boxplus r,$$

a wtedy

$$(\tilde{q} \boxplus P_{\mathbb{K}[t]}(q)) \odot b = r \boxplus P_{\mathbb{K}[t]}(\tilde{r}).$$

Jeśli teraz było $\tilde{q} \boxplus P_{\mathbb{K}[t]}(q) \neq \mathbf{0}$, to wobec $b \neq \mathbf{0}$ zachodziłaby nierówność

$$\deg((\tilde{q} \boxplus P_{\mathbb{K}[t]}(q)) \odot b) = \deg(\tilde{q} \boxplus P_{\mathbb{K}[t]}(q)) + \beta \geq \beta,$$

gdy tymczasem

$$\deg(r \boxplus P_{\mathbb{K}[t]}(\tilde{r})) \leq \max(\deg r, \deg P_{\mathbb{K}[t]}(\tilde{r})) < \beta,$$

czyli sprzeczność. Stąd wniosek, że konieczne $\tilde{q} = q$, a wtedy także $\tilde{r} = r$, co kończy dowód. $\square$

4.3. Podzielność i algebraiczna domkniętość

Określimy obecnie na zbiorze $\mathbb{K}[t]$ relację, która pozwoli opisać rozkład dowolnego wielomianu o współczynnikach z $\mathbb{C}$ (wzgl. $\mathbb{R}$) na czynniki nierozkładalne, będące odpowiednikami czynników pierwszych znanych z arytmetyki liczb naturalnych, i w ten sposób da nam możliwość wysłowienia fundamentalnego twierdzenia charakteryzującego $\mathbb{C}[t]$.

DEFINICJA 28. Przyjmijmy notację Def. 21 i niech $(R, +_R, \cdot_R, P_R, \mathbf{0}_R, \mathbf{1}_R)$ będzie pierścieniem. Mówimy, że $a \in R$ **dzieli** $b \in R$ lub też że a jest **dzielnikiem** b (lub też że b jest **krotnością** a), co zapisujemy jako $a \mid b$, gdy

$$a \mid b \iff \exists c \in R : b = a \cdot_R c.$$

▲

Oczywiste własności tak zdefiniowanej relacji podzielności w pierścieniu zbiera

STWIERDZENIE 18. W notacji Def. 21 i 28 a dla pierścienia przemennego R zachodzi

- (i) $\forall a \in R : a \mid a$ (zwrotność);
- (ii) $\forall a, b, c \in R : (a \mid b \wedge b \mid c) \implies a \mid c$ (przechodność);
- (iii) $\forall a, b, c, d \in R : (a \mid b \wedge c \mid d) \implies a \cdot_R c \mid b \cdot_R d$ (mnożalność);
- (iv) $\forall a, b, c \in R : (a \mid b \wedge a \mid c) \implies a \mid b +_R c$;
- (v) $\forall a \in R : \mathbf{1}_R \mid a \mid \mathbf{0}_R$;
- (vi) jeśli R jest dziedziną całkowitości, wówczas $\forall a, b \in R : (a \cdot_R c \mid b \cdot_R c \implies a \mid b)$ (prawo skracania).

■

Punktem wyjścia do zastosowania powyższej relacji w interesującym nas kontekście algebraicznym jest

STWIERDZENIE 19 (Twierdzenie Bezouta). *Przyjmijmy notację Def. 6, 67, 11, 24, 26, 25 i 28. Dla dowolnego $w \in \mathbb{K}[t]$ oraz $\lambda \in \mathbb{K}$ prawdziwą jest następująca równoważność*

$$F_w(\lambda) = 0_{\mathbb{K}} \iff (t \boxplus P_{\mathbb{K}}(\lambda)) \mid w, \text{ tj. } \exists_{w_1 \in \mathbb{K}[t]} : w = (t \boxplus P_{\mathbb{K}}(\lambda)) \odot w_1.$$

■

Dowód: Na mocy Tw. 4.2, w którym kładziemy $R := \mathbb{K}[t]$ oraz $a = w$ i $b = (t \boxplus P_{\mathbb{K}}(\lambda))$, istnieją $q, r \in \mathbb{K}[t]$ spełniające równość $w = q \odot (t \boxplus P_{\mathbb{K}}(\lambda)) \boxplus r$, przy czym $\deg r < \deg(t \boxplus P_{\mathbb{K}}(\lambda)) = 1$, czyli $r = \mu$ dla pewnego $\mu \in \mathbb{K}$. Tożsamość $0_{\mathbb{K}} = F_w(\lambda) = \mu$ daje tezę. $\square$

Z powyższego wyciągamy proste a użyteczne wnioski

COROLLARIUM 1. *W notacji Def. 6, 67, 11, 24, 26, 25 i 27 zachodzi, co następuje:*

- (i) $\forall_{w \in \mathbb{K}[t]} : |\{ \lambda \in \mathbb{K} \mid F_w(\lambda) = 0_{\mathbb{K}} \}| \leq \deg w$, czyli liczba zer wielomianu nie przekracza jego stopnia.
- (ii) Niechaj $n \in \mathbb{N} \setminus \{0\}$ i niech $S \subset \mathbb{K}$ spełnia relację $|S| > n$, a przy tym niech $\sum_{k=0}^n \lambda_k \cdot \mu^k = 0_{\mathbb{K}}$ dla każdego $\mu \in S$. Wówczas $\forall_{k \in \overline{0, n}} : \lambda_k = 0_{\mathbb{K}}$.

■

Wprowadzimy jeszcze

DEFINICJA 29. W notacji Def. 6, 67, 11, 24, 25 i 26 **krotność zera** $\lambda \in F_w^{-1}(\{0_{\mathbb{K}}\})$ wielomianu $w \in \mathbb{K}[t]$ to liczba

$$\kappa(\lambda | w) := \max \left\{ n \in \mathbb{N} \mid (t + P_{\mathbb{K}}(\lambda))^n \mid w \right\},$$

przy czym $\kappa(\lambda | w) = 0$ oznacza, że $F_w(\lambda) \neq 0_{\mathbb{K}}$.

▲

Zgromadzone pojęcia pozwalają wysłowić

STWIERDZENIE 20. *Przyjmijmy notację Def. 6, 67, 11, 24, 26, 25, 27 oraz 29. Poniższe zdania są równoważne:*

- (i) $\forall_{w \in \mathbb{K}[t]} \exists_{\lambda \in \mathbb{K}} : F_w(\lambda) = 0_{\mathbb{K}}$ (istnienie pierwiastka).
- (ii) $\forall_{w \in \mathbb{K}[t]} \exists_{\substack{\mu \in \mathbb{K} \setminus \{0_{\mathbb{K}}\} \\ \lambda_1, \lambda_2, \dots, \lambda_n \in \mathbb{K}, n \in \mathbb{N} \setminus \{0\}}} : w = \mu \odot \odot_{i=1}^n (t + P_{\mathbb{K}}(\lambda_i))$ (rozkład na czynniki liniowe).
- (iii) $\forall_{w \in \mathbb{K}[t] \setminus \{0\}} : \sum_{\lambda \in \{ \mu \in \mathbb{K} \mid F_w(\mu) = 0_{\mathbb{K}} \}} \kappa(\lambda | w) = \deg w$ (związek między krotnościami a stopniem).

■

Dowód:

- (i) $\Rightarrow$ (ii) Prosta konsekwencja Stw. 19.
- (ii) $\Rightarrow$ (iii) Wynika bezpośrednio z Def. 29.
- (iii) $\Rightarrow$ (i) Oczywiście.

□

Powyższe rozważania pozwalają nam wyróżnić ważną klasę ciał.

DEFINICJA 30. Ciało algebraicznie domknięte to takie, w którym są spełnione warunki Stw. 20.

▲

O tym, że algebraiczna domkniętość jest cechą nietrywialną (tj. że istnieją ciała nie należące do tej klasy) przekonują nas

PRZYKŁAD(Y) 14. Poniższe ciała są algebraicznie niedomknięte:

- (1) $\mathbb{Q}, \mathbb{R}$ (wystarczy rozważyć wielomian $t^2 + 1 \in \mathbb{Q} \cap \mathbb{R}$);
- (2) $\mathbb{Q}[\sqrt{2}]$ (wystarczy rozpatrzyć $t^2 - 3$).

✓

Dotychczasowa dyskusja prowadzi nas wprost do fundamentalnego

TWIERDZENIE 4.3 (Podstawowe Twierdzenie Algebry). *Ciało liczb zespolonych jest algebraicznie domknięte.*

■

Dowód: Wszystkie opisane w literaturze dowody tego twierdzenia odwołują się do własności topologicznych zbioru $\mathbb{C}$ (wzgl. $\mathbb{R}$) lub też konstrukcji algebraicznych (teoria Galois i in.), których szczegółowa dyskusja wykracza w istotny sposób poza ramy niniejszego kursu. Nie chcąc pozostawić Czytelnika bez dowodu, przedstawiamy rozumowanie geometryczne korzystające z pojęć wprowadzonych w Przykł. 5 (3). Jego pojęcie wymaga znajomości elementarnych własności topologicznych płaszczyzny $\mathbb{R}^2$ tudzież okręgu (jednostkowego) $\mathbb{S}^1$, co czyni z niego doskonałe ćwiczenie do wykładu analizy matematycznej na drugim roku studiów (na którym przedstawione zostaną również alternatywne formy dowodu, wykorzystujące podstawy teorii funkcji zmiennej zespolonej).

Nie tracąc ogólności rozważań, przyjmujemy następującą postać wielomianu:

$$w = t^n + \lambda_{n-1} t^{n-1} + \lambda_{n-2} t^{n-2} + \dots + \lambda_0,$$

przy czym $\lambda_{n-1}, \lambda_{n-2}, \dots, \lambda_0 \in \mathbb{C}$. Jeśli zbiór $F_w^{-1}(\{0\}) \subset \mathbb{C}$ zer wielomianu w jest pusty, to dla dowolnego $r \in \mathbb{R}_{\geq 0}$ obrazem odcinka $I = [0, 1]$ względem odwzorowania

$$\gamma_r : I \longrightarrow \mathbb{R}^{\times 2} : s \longmapsto \frac{F_w(r \cdot e^{i2\pi s}) \cdot F_w(r)^{-1}}{|F_w(r \cdot e^{i2\pi s}) \cdot F_w(r)^{-1}|}$$

jest pętla o bazie $z_* := (1, 0)$ zawarta w okręgu jednostkowym $\mathbb{S}^1$. Zmieniając parametr r w sposób ciągły definiujemy homotopię

$$\gamma_\cdot : I^{\times 2} \longrightarrow \mathbb{R}^{\times 2}$$

pętli o bazie z_* , a ponieważ $\gamma_0 = \varepsilon_{z_*}$, przeto

$$\forall_{r \in \mathbb{R}_{\geq 0}} : [\gamma_r]_{\sim} = [\varepsilon_{z_*}]_{\sim} \in \pi_1(\mathbb{S}^1; z_*).$$

Dobrawszy

$$r > \max \left(1, \sum_{k=0}^{n-1} |\lambda_k| \right),$$

otrzymujemy, dla $z \in \mathbb{C}$ o module $|z| := r$, nierówność

$$|z^n| = r \cdot |z^{n-1}| > \left(\sum_{k=0}^{n-1} |\lambda_k| \right) \cdot |z^{n-1}| > \sum_{k=0}^{n-1} |\lambda_k| \cdot |z^k| \geq \left| \sum_{k=0}^{n-1} \lambda_k \cdot z^k \right|,$$

która pokazuje, że żaden z rodziny wielomianów

$$w_u := t^n \boxplus u \odot \sum_{k=0}^{n-1} \lambda_k t^k$$

indeksowanej przez zbiór $[0, 1] \ni u$ nie ma zera na okręgu $O(0; r)$, co pozwala określić przyporządkowanie

$$\gamma_r^u : I \longrightarrow \mathbb{R}^{\times 2} : s \longmapsto \frac{F_{w_u}(r \cdot e^{i2\pi s}) \cdot F_{w_u}(r)^{-1}}{|F_{w_u}(r \cdot e^{i2\pi s}) \cdot F_{w_u}(r)^{-1}|}.$$

To ostatnie definiuje homotopię

$$\gamma_r : I^{\times 2} \longrightarrow \mathbb{R}^{\times 2}$$

pętli o bazie z_* przeprowadzające pętlę

$$\gamma_r^0 : I \longrightarrow \mathbb{R}^{\times 2} : s \longmapsto e^{i2\pi ns}$$

w pętlę $\gamma_r^1 \equiv \gamma_r$. Pierwsza z nich należy przy tym do n -tej potęgi $[\omega]_~^n$ generatora $[\omega]_~$ grupy $\pi_1(\mathbb{S}^1; z_*) \cong \mathbb{Z}$ (patrz: Def. 33). Skoro jednak

$$[\omega]_~^n = [\gamma_r^0]_~ = [\gamma_r^1]_~ \equiv [\gamma_r]_~ = [\varepsilon_{z_*}]_~,$$

to musi być $n = 0$, co oznacza, że jedynymi wielomianami nie posiadającymi zer w $\mathbb{C}$ są wielomiany stałe $w = \lambda \in \mathbb{C}^\times$. $\square$

Tę część wykładu zakończymy wypisując najbardziej elementarne konsekwencje Tw. 4.3.

COROLLARIUM 2. *Przyjmijmy notację Def. 6, 67, 11, 14, 24, 26, 25, 27 oraz 29. Prawdziwe są poniższe zdania:*

- (i) $\forall_{\substack{w \in \mathbb{C}[t] \\ n := \deg w \geq 1}} \exists_{\substack{\alpha \in \mathbb{C}^\times \\ z_1, z_2, \dots, z_n \in \mathbb{C}}} : w = \alpha \odot \odot_{i=1}^n (t - z_i);$
- (ii) $\forall_{\substack{w \in \mathbb{R}[t] \\ n := \deg w \geq 1}} \exists_{\substack{a \in \mathbb{R}^\times \\ k, l \in \mathbb{N}, k+2l=n \\ x_1, x_2, \dots, x_k \in \mathbb{R} \\ (p_1, q_1), (p_2, q_2), \dots, (p_l, q_l) \in \mathbb{R}^{\times 2}, p_j^2 - 4q_j < 0}} : w = a \odot \odot_{i=1}^k (t - x_i) \odot \odot_{j=1}^l (t^2 + p_j t + q_j);$
- (iii) $\forall_{w \in \mathbb{R}[t]} : \deg w - \sum_{z \in \{ r \in \mathbb{R} \mid F_w(r) = 0 \}} \kappa(r|w) \in 2\mathbb{N};$ *w szczególności*
 $\deg w \in 2\mathbb{N} + 1 \implies \exists_{r \in \mathbb{R}} : F_w(r) = 0.$

■

Dowód: Jedynym punktem wymagającym jakiegokolwiek komentarza jest (ii). Zauważmy, że dla dowolnego $w \in \mathbb{R}[t] \subset \mathbb{C}[t]$ (traktowanego jako wielomian o współczynnikach zespolonych, na co pozwala Stw. 2) zachodzi

$$\forall_{z \in \mathbb{C}} : \overline{F_w(z)} = F_w(\bar{z}),$$

skąd wniosek

$$F_w(z) = 0 \implies F_w(\bar{z}) = 0,$$

który przy $\Im(z) \neq 0$ prowadzi do konkluzji

$$(t - z) \sqcap (t - \bar{z}) \mid w.$$

Ale też

$$(t - z) \sqcap (t - \bar{z}) = t^2 - 2\Re(z)t + |z|^2,$$

przy czym $(-2\Re(z))^2 - 4 \cdot 1 \cdot |z|^2 = 4(\Re(z)^2 - \Re(z)^2 - \Im(z)^2) = -4\Im(z)^2 < 0$. $\square$

4.4. Dodatkowe własności dziedzin ideałów głównych

W niniejszym kursie pierścieni wielomianów (i ogólniej – pierścienie ideałów głównych) odgrywa rolę pomocniczą i z tej to przyczyny powstrzymujemy się od rozwinięcia teorii pierścieni w stopniu szerszym, niż wymagają tego przyszłe jej zastosowania. Na zakończenie rozdziału omówimy kilka aspektów tej teorii o istotnym znaczeniu praktycznym dla późniejszej dyskusji struktury endomorfizmów przestrzeni wektorowych. Zaczniemy od wprowadzenia dodatkowych pojęć powiązanych z zagadnieniem podzielności.

DEFINICJA 31. Przyjmijmy notację Def. 21 oraz 28 i niech $\{r_n\}_{n \in \overline{1, N}}$, $N \in \mathbb{N}$ będzie rodziną elementów pierścienia przemennego R . **Największy wspólny dzielnik** elementów r_i to zbiór

$$\begin{aligned} \text{NWD}(r_1, r_2, \dots, r_N) := \{ r \in R \mid \forall_{i \in \overline{1, N}} : \text{NWD}(r_1, r_2, \dots, r_N) \mid r_i \\ \wedge \forall_{s \in R} : \left(\forall_{i \in \overline{1, N}} : s \mid r_i \implies s \mid r \right) \}. \end{aligned}$$

Ilekoć $1_R \in \text{NWD}(r_1, r_2, \dots, r_N)$, mówimy, że elementy r_i są **względnie pierwsze**.

▲

Należy zaznaczyć, że możliwe są zarówno sytuacje, w których zdefiniowany powyżej zbiór jest pusty, jak i takie, w których zawiera on więcej niż jeden element. Jest przy tym jasnym, że w tym ostatnim przypadku każde dwa jego elementy $d_1, d_2 \in \text{NWD}(r_1, r_2, \dots, r_N)$ spełniają relacje $d_1 \mid d_2$ oraz $d_2 \mid d_1$ i dowolny element pierścienia dzielący i zarazem dzielony przez element zbioru $\text{NWD}(r_1, r_2, \dots, r_N)$ sam do zbioru tego należy.

Wygodnej charakteryzacji największego wspólnego dzielnika dostarcza

STWIERDZENIE 21. *Przyjmijmy notację Def. 21, 22, 28 i 31. Element pierścienia $d \in R$ należy do $\text{NWD}(r_1, r_2, \dots, r_N)$ wtedy i tylko wtedy, gdy $\langle d \rangle_R$ jest najmniejszym ideałem głównym zawierającym ideał $\langle r_1 \rangle_R +_R \langle r_2 \rangle_R +_R \dots +_R \langle r_N \rangle_R$, tj. $\langle d \rangle_R$ jest zawarty w każdym ideałem głównym zawierającym $\langle r_1 \rangle_R +_R \langle r_2 \rangle_R +_R \dots +_R \langle r_N \rangle_R$.*

■

Dowód: Relacja $\langle r_1 \rangle_R +_R \langle r_2 \rangle_R +_R \cdots +_R \langle r_N \rangle_R \subset \langle r \rangle_R$ zapisana dla pewnego elementu $r \in R$ implikuje $\forall_{i \in \overline{1, N}} : \langle r_i \rangle_R \subset \langle r \rangle_R$, gdyż $\langle r_i \rangle_R \ni 0_R$, a stąd $\langle r_i \rangle_R \subset \langle r_1 \rangle_R +_R \langle r_2 \rangle_R +_R \cdots +_R \langle r_N \rangle_R$. Zarazem domkniętość ideału $\langle r_1 \rangle_R +_R \langle r_2 \rangle_R +_R \cdots +_R \langle r_N \rangle_R$ względem operacji 2-argumentowych pierścienia sprawia, że prawdziwa jest implikacja odwrotna, w konsekwencji więc stwierdzamy równoważność

$$\langle r_1 \rangle_R +_R \langle r_2 \rangle_R +_R \cdots +_R \langle r_N \rangle_R \subset \langle r \rangle_R \iff \forall_{i \in \overline{1, N}} : \langle r_i \rangle_R \subset \langle r \rangle_R .$$

Jest też prawdziwą równoważność

$$\forall_{x, y \in R} : (\langle x \rangle_R \subset \langle y \rangle_R \iff y \mid x) ,$$

oto bowiem z jednej strony inkluzja $\langle x \rangle_R \subset \langle y \rangle_R$ implikuje $x = x \cdot_R 1_R \in \langle y \rangle_R$, czyli $x = y \cdot_R q$ dla pewnego $q \in R$, z drugiej zaś ta ostatnia równość oznacza, że $\langle x \rangle_R \equiv \langle y \cdot_R q \rangle_R \subset \langle y \rangle_R$. Możemy zatem zapisać

$$\langle r_1 \rangle_R +_R \langle r_2 \rangle_R +_R \cdots +_R \langle r_N \rangle_R \subset \langle r \rangle_R \iff \forall_{i \in \overline{1, N}} : r \mid r_i ,$$

co oznacza, że element generujący dowolny ideał pierścienia R , który zawiera $\langle r_1 \rangle_R +_R \langle r_2 \rangle_R +_R \cdots +_R \langle r_N \rangle_R$, jest wspólnym dzielnikiem elementów r_i i każdy taki wspólny dzielnik generuje ideał o rzeczonyj własności. W świetle tych obserwacji prawdziwość tezy stwierdzenia staje się oczywista, jako że każdy dzielnik elementów r_i dzieli dowolny element ich największego wspólnego dzielnika. $\square$

Dyskusję zamyka kluczowe z punktu widzenia przyszłych zastosowań

STWIERDZENIE 22. *Przyjmijmy notację Def. 21, 22, 28 i 31. Niechaj R będzie dziedziną ideałów głównych. Wówczas największy wspólny dzielnik dowolnej rodziny $\{r_n\}_{n \in \overline{1, N}}$, $N \in \mathbb{N}$ elementów R jest zbiorem niepustym, którego dowolny element $d \in \text{NWD}(r_1, r_2, \dots, r_N)$ spełnia warunek*

$$\exists_{\{q_n\}_{n \in \overline{1, N}} \subset R} : d = \sum_{n=1}^N q_n \cdot_R r_n .$$

■

Dowód: Skoro R jest dziedziną ideałów głównych, to ideał $\langle r_1 \rangle_R +_R \langle r_2 \rangle_R +_R \cdots +_R \langle r_N \rangle_R$ jest główny, a zatem na mocy Stw. 21 zachodzi równość

$$\langle d \rangle_R = \langle r_1 \rangle_R +_R \langle r_2 \rangle_R +_R \cdots +_R \langle r_N \rangle_R ,$$

z której wynika już wprost istnienie elementów $q_n \in R$ zadających pożądaną rozkład elementu $d = d \cdot_R 1_R \in \langle d \rangle_R$. $\square$

* * *

Literatura uzupełniająca: Elementarne własności pierścienia wielomianów o współczynnikach z ciała zostały wyczerpująco omówione w książkach Langa [Lan02, Rozdz. IV] i Cohna [Coh82, Rozdz. 6]. Bardziej zaawansowaną problematykę, w szczególności zaś tematykę rozszerzeń algebraicznych ciał, autorzy ci dyskutują, odpowiednio, w [Lan02, Rozdz. V, VI] oraz [Coh89, Rozdz. 3] i [Coh91, Rozdz. 5, 9].

Grupy

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 6.

5.1. Struktura grupy i jej transport

Zacniemy od rozpisania i rozszerzenia definicji grupy.

DEFINICJA 32. **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**;
- $\phi_1 : G \rightarrow G$ 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)

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

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

(G3) (fundamentalna własność ϕ_1)

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

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

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 (wypisany wraz z równoważnym zdaniem logicznym)

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

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) 15.

- (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:

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

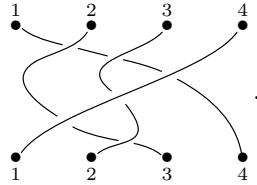
zapisanej dla dowolnego $f \in \text{Map}(S, G)$, oraz z działaniem 0-argumentowym $\tilde{\phi}_0$ indukowanym przez ϕ_0 wedle formuły:

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

- (5) 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 $\Pi \subset \mathbb{R}^{x3}$, zakładając przy tym, że proste Λ_+ i Λ_- wyznaczone przez zbiory Σ_+ i Σ_- , odpowiednio, są do siebie równoległe. Punktom ze zbioru $\Sigma_{\pm}$ przypiszemy indeksy naturalne od 1 do n , w kolejności ich ułożenia na prostej $\Lambda_{\pm}$, 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 $\overline{1, n}$, która liczbie $k \in \overline{1, n}$ 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 $\mathbb{R}^{x3}$ 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



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

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



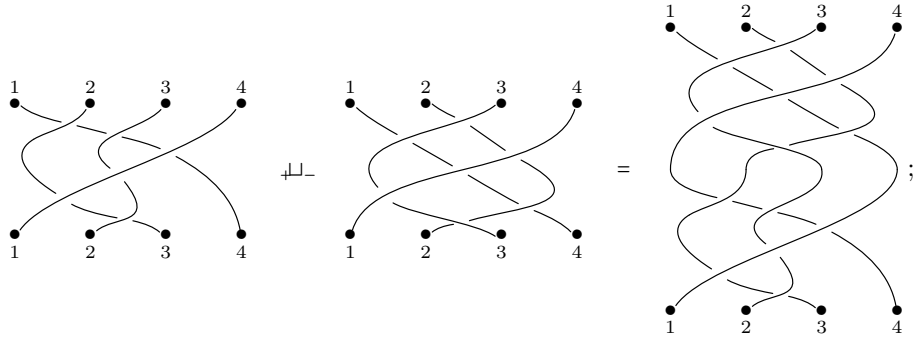
Jak jasno wynika z opisu ogólnego i powyższej ilustracji, różnica między warkoczami a indukowanymi przez nie permutacjami z $\mathfrak{S}_n$ polega na tym, że w w procesie indukcji tracona jest informacja o tym, czy ścieżka wychodząca z punktu odpowiadającego elementowi nośnika permutacji opisywanej 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

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

złożona z następujących elementów:

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

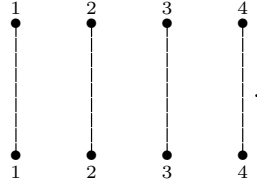


- operacja 1-argumentowa $\text{Inv} : \mathfrak{B}_n \longrightarrow \mathfrak{B}_n : [w] \mapsto [R(w)]$ przyporządkowuje klasie izotopii warkocza w klasę izotopii warkocza $R(w)$ otrzymanego przez odbicie w w prostej $\Lambda_0 \subset \Pi$ równoległej do Λ_+ i

leżącej w połowie odległości między Λ_+ i Λ_- , np.

$$R \left(\begin{array}{cccc} 1 & 2 & 3 & 4 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ 1 & 2 & 3 & 4 \end{array} \right) = \begin{array}{cccc} 1 & 2 & 3 & 4 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ 1 & 2 & 3 & 4 \end{array} ;$$

- element neutralny 1 względem $\star$ będący klasą izotopii warkoczy 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 odpowiednim diagramie warkoczowym ponad pasmem o indeksie wyższym, i o pozostałych pasmach niesplecionych,

$$\tau_i \doteq \begin{array}{ccccccc} 1 & 2 & \dots & i-1 & i & i+1 & i+2 & \dots & n \\ \cdot & \cdot & & \cdot & \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot & \cdot & \cdot & \cdot & & \cdot \\ 1 & 2 & \dots & i-1 & i & i+1 & i+2 & \dots & n \end{array}.$$

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

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

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

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

✓

NOTACJA 4. Dwa najbardziej rozpowszechnione zapisy dla grup to

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

- zapis masyplikatywny $(\phi_2, \phi_1, e) \equiv (\cdot \equiv M, \text{Inv} \equiv (\cdot)^{-1}, \mathbf{1})$ (mnożenie, odwrotność, jedyńska), 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 $(\phi_2, \phi_1, e) \equiv (+ \equiv A, P \equiv -(\cdot), \mathbf{0})$ (przeciwność, dodawanie, zero), w którym wprowadzamy pojęcie **krotności**

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

$$(5.1) \quad \forall_{g \in G} : 0g := \mathbf{0},$$

o oczywistych własnościach:

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

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

* * *

STWIERDZENIE 23. *W dowolnej grupie element neutralny oraz element odwrotny do danego są określone jednoznacznie.*

■

STWIERDZENIE 24. *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 25. *W notacji (masyplikatywnej) Def. 32 zachodzi*

- (i) $\text{Inv} \circ \text{Inv} = \text{id}_G$;
- (ii) $\text{Inv} \circ M = M \circ (\text{Inv} \times \text{Inv}) \circ \tau_G$;

$$(iii) \quad \forall_{g,h,k \in G} : g \cdot h = k \iff g = k \cdot h^{-1} \iff h = g^{-1} \cdot k.$$

■

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. 24), co w świetle Stw. 23 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. 23.

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 33. 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) 16.

- (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 7.

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

✓

DEFINICJA 34. W notacji Def. 32 **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:

$$(SG1) \quad \phi_2 : H^{\times 2} \longrightarrow H \subset G;$$

$$(SG2) \quad \phi_1 : H \longrightarrow H \subset G.$$

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



PRZYKŁAD(Y) 17.

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

- (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 przesunień 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, przesunień 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 ,

$$(5.2) \quad \mathfrak{A}_X := [\mathfrak{S}_X, \mathfrak{S}_X].$$

W dziale 7 zapoznamy się z alternatywną definicją tej podgrupy, wysłowioną w terminach znaku tworzących ją permutacji.



STWIERDZENIE 26. *Każda podgrupa grupy danej jest grupą.*

■

Użyteczne własności podgrup zbiera

STWIERDZENIE 27. *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 35. W notacji Def. 32 **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 przemienności (wypisany wraz z równoważnym zdaniem logicznym):

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

Jak poprzednio w oczywisty sposób wyróżniamy

- **monomorfizmy** (homomorfizmy 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, $G^{(2)} \equiv G^{(1)} \circlearrowright$);
- **automorfizmy** (bijektywne homomorfizmy wewnętrzne).

▲

PRZYKŁAD(Y) 18.

- (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 $\sqrt[n]{1} \longrightarrow \mathbb{Z}/n\mathbb{Z} : e^{i\frac{2\pi k}{n}} \mapsto [k]_n, \quad n \in \mathbb{N} \setminus \{0, 1\}$ 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 $\mathbb{Z}/(2n+1)\mathbb{Z} \ni [k]_{2n+1} \mapsto 2[k]_{2n+1}$ 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 $\phi_1 : G \ni$ zadaje izomorfizm między grupą G a przeciwną do niej.

✓

Proste własności homomorfizmu w odniesieniu do pozostałych elementów struktury grupy zbiera

STWIERDZENIE 28. W notacji Def. 35 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. 23 daje tezę.

□

Szczególny typ homomorfizmów grup opisuje

STWIERDZENIE 29. 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 30. Grupa automorfizmów wewnętrznych grupy przemiennej jest trywialna.

■

PRZYKŁAD(Y) 19.

- (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 36. W notacji Def. 35 **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 31. W notacji Def. 35 i 36 $\text{Ker } \chi$ 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 32. W notacji Def. 35 i 36 $\text{Im } \chi$ 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) 20.

- (1) Jądrem epimorfizmu z przykładu 18(2) jest **grupa specjalna ortogonalna stopnia 2 nad $\mathbb{R}$** , o nośniku dopuszczającym naturalną parametryzację:

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

- (2) Jądrem epimorfizmu $|\cdot|$ z przykładu 18(6) jest podgrupa $U(1) \subset \mathbb{C}^\times$.
 (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. 29 jest podgrupa $\mathcal{Z}(G) \subset G$.

✓

Przyjrzymy się bliżej jądro homomorfizmu.

STWIERDZENIE 33. W notacji Def. 35 i 36 χ jest monomorfizmem $\iff \mathrm{Ker} \chi = \{e^{(1)}\}$.

■

Dowód:

$$\begin{aligned} \Rightarrow \quad & \chi(e^{(1)}) = e^{(2)}, \text{ zatem } \chi(g) = e^{(2)} \text{ implikuje } g = e^{(1)} \text{ wobec iniektywności } \chi. \\ \Leftarrow \quad & \chi(g) = \chi(h) \iff \chi(g \cdot_{(1)} \mathrm{Inv}^{(1)}(h)) = e^{(2)}, \text{ ale wobec trywialności } \mathrm{Ker} \chi \\ & \text{to implikuje } g \cdot_{(1)} \mathrm{Inv}^{(1)}(h) = e^{(1)}, \text{ czyli } g = h. \end{aligned}$$

□

5.2. Warstwy i grupy ilorazowe

Przypomnijmy następujące pojęcie znane z kursu analizy matematycznej.

DEFINICJA 37. Niechaj X, Y będą zbiorami i niech będzie dane odwzorowanie $f : X \longrightarrow Y$. **Poziomica** (albo **przeciwbraz**) **podzbioru** $Z \subset f(X)$ **względem** f to podzbiór

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

▲

STWIERDZENIE 34. W notacji Def. 35, 36 i 37

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

■

Odpowiedzi na pytanie o postać pozostałych poziomów dostarcza

STWIERDZENIE 35. W notacji Def. 35, 36 oraz 37 i dla dowolnego $g \in G^{(1)}$ słuszną jest formuła

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

■

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 38. W notacji Def. 34 **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 36. W notacji Def. 34 i 38 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 39. W notacji Def. 38 **indeksem (lewostronnym) podgrupy H w grupie G** nazywamy moc zbioru warstw (lewostronnych) względem H w G ,

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

▲

STWIERDZENIE 37. W notacji Def. 34 i 38 relacja na G zadana, jak następuje:

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

jest relacją równoważności.

■

Dowód:

- (1) Na mocy Stw. 26 $e \in H$, 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. 26 $h \in H \implies h^{-1} \in H$, 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 3. *Dowolna podgrupa grupy danej zadaje rozkład tej ostatniej na sumę rozłączną równolicznych warstw (względem tejże podgrupy).*

■

PRZYKŁAD (Y) 21.

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

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

✓

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

COROLLARIUM 4. (Twierdzenie Lagrange'a) *Przyjmijmy notację Def. 32 i 34. 39. Wówczas zachodzi tożsamość*

$$(5.3) \quad |G| = |H| \cdot (G : H) .$$

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 38. W notacji Def. 34, 35, 36 i 38 zachodzi

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

albo – równoważnie –

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

■

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

DEFINICJA 40. W notacji Def. 34 i 38 **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) 22.

- (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 39. *Każda podgrupa grupy przemiennej jest normalna.*

■

Dyskusja istnienia dzielników normalnych grupy danej prowadzi do naturalnej

DEFINICJA 41. **Grupa prosta** to taka, która nie posiada podgrup normalnych właściwych i nietrywialnych, tj. różnych od całej grupy i od podgrupy trywialnej.

▲

PRZYKŁAD(Y) 23. 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 40. *W notacji Def. 34, 38 i 40 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: $\text{Inv}_{G/H}(gH) := g^{-1}H$;
- jedynka: $\mathbf{1}_{G/H} := H$.

■

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 $\odot$ 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 . □

DEFINICJA 42. W notacji Def. 34 i 38 oraz Stw. 40 **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) 24.

- (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 adekwatnie³ – **grupą klas automorfizmów**)

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

✓

5.3. 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

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

Wyraża ona, w połączeniu ze Stw. 38, zapowiedziane wcześniej utożsamienie pomiędzy dzielnikami normalnymi a jądrami homomorfizmów. Jej abstrakcję opisuje

DEFINICJA 43. Niechaj $(G^{(\alpha)}, \phi_2^{(\alpha)}, \phi_1^{(\alpha)}, \phi_0^{(\alpha)})$, $\alpha \in \{1, 2, 3\}$ będzie trójką grup i niech $\chi_{(\beta)} : G^{(\beta)} \longrightarrow G^{(\beta+1)}$, $\beta \in \{1, 2\}$ będzie parą homomorfizmów grup. Piątkę

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

nazywamy **ciągiem dokładnym (grup)**, jeżeli

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

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

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

³Należy zauważyć, że elementami $\text{Out}(G)$ nie są automorfizmy zewnętrzne G , lecz ich warstwy w $\text{Aut}(G)$.

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**⁴ (możliwym wtedy tylko, gdy $G^{(1)}$ jest przemienna).

▲

PRZYKŁAD(Y) 25. Niechaj $(G, \phi_2, \phi_1, \phi_0)$ będzie dowolną grupą, $H \subset G$ zaś – jej dzielnikiem normalnym. Wówczas diagram

$$(5.4) \quad 1 \longrightarrow H \xrightarrow{J_H} G \xrightarrow{\pi_{G/H}} G/H \longrightarrow 1$$

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 liczb (rzeczywistych). Wobec oczywistej relacji

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

wypisanej dla epimorfizmu grup z Przykł. 18 (6), dostajemy – na mocy Tw. 5.1 –

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

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 struktury modułu nad pierścieniem w Rozdz. 8 oraz wybranych zagadnień algebry homologicznej w Rozdz. 14.

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.

⁴Rozszerzenia centralne grup odgrywają istotną rolę w opisie symetrii kwantowej teorii pola.

Zacznijmy od twierdzenia podsumowującego dyskusję struktury jądra homomorfizmu.

TWIERDZENIE 5.1 (Pierwsze twierdzenie o izomorfizmie). *W notacji Def. 35, 36 i 42 oraz Stw. 40 $\text{Ker } \chi$ jest dzielnikiem normalnym $G^{(1)}$, a nadto istnieje kanoniczny izomorfizm grup*

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

■

Dowód: Pierwsza część twierdzenia wynika wprost ze Stw. 38, 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

$$(5.5) \quad \chi(h) = \chi(g \cdot_{(1)} k) = \chi(g) \cdot_{(2)} \chi(k) = \chi(g) \cdot_{(2)} e^{(2)} = \chi(g).$$

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

Jest ono także injektywne, co wynika z następującego rozumowania (wykorzystującego Stw. 38):

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

Na koniec przekonujemy się, że λ_χ jest homomorfizmem grup,

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

□

Prostą konsekwencją powyższego twierdzenia jest

COROLLARIUM 5. *Niechaj $(G, \phi_2, \phi_1, \phi_0)$ będzie grupą i przyjmijmy notację Przykł. 5 (2), Stw. 29 i 40 oraz Def. 42. Istnieje kanoniczny izomorfizm grup*

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

■

Dowód: Na mocy Stw. 29 oraz Przykł. 20 (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 5.2 (O uniwersalności rzutu kanonicznego). *W notacji Def. 35, 36 i 42 oraz Stw. 40 (dla $H = \text{Ker } \chi$) istnieje dokładnie jeden **monomorfizm indukowany***

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

o własności

$$(5.6) \quad \chi = \tilde{\chi} \circ \pi_{G^{(1)}/\text{Ker } \chi}.$$

Indukuje on – wedle Tw. 5.1 – 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 $j_{\text{Im } \chi} : \text{Im } \chi \rightarrow G^{(2)}$ 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. (5.5). 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

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

□

Kolejnym ważnym wynikiem jest

TWIERDZENIE 5.3 (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: 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 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 widzieć, 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. 31). Tw. 5.1 odniesione do φ przesądza o istnieniu pożądanego izomorfizmu kanonicznego,

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

□

5.4. Iloczyn półprosty grup w algebrze i geometrii

Powyższe twierdzenie, pozornie dość abstrakcyjne, opisuje szeroką klasę fizycznie istotnych struktur określanych mianem iloczynów (pół)prostych grup. Dla ich omówienia konieczne będzie wprowadzenie dodatkowych pojęć, które poprzędzimy 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 rachunek⁵:

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

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 44. 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 $G = H \bullet K$.

▲

O naturalności pojęcia dopełnienia w kontekście naszych rozważań przekonuje

STWIERDZENIE 41. *Każde dopełnienie podgrupy normalnej grupy danej jest kanonicznie izomorficzne z grupą ilorazową warstw względem tejże podgrupy (w grupie).*

⁵W istocie przemycamy tutaj strukturę modułu grupy ruchów euklidesowych na zbiorze $\mathbb{R}^2$. O strukturach takich powiemy więcej już wkrótce.

■

Dowód: W świetle Tw. 5.3 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 42. *Przyjmijmy notację Def. 44. 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 45. Przyjmijmy notację Def. 44. 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

$$G = H \rtimes K.$$

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 43. *W notacji Def. 44 i 45 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 (dziedziczoną z G) zadawaną przez działanie

$$\begin{aligned} \phi_2^\times : (H \times K) \times (H \times K) &\longrightarrow H \times K : ((h_1, k_1), (h_2, k_2)) \longmapsto (h_1 \cdot h_2, k_1 \cdot k_2) \\ \text{o elemencie neutralnym } (e_H, e_K) \text{ (czyli tutaj } (e_G, e_G)) \text{ oraz przez odwrotność} \\ \phi_1^\times : H \times K &\curvearrowright : (h, k) \longmapsto (h^{-1}, k^{-1}). \end{aligned}$$

■

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,

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

□

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) 26.

$$(1) \quad \mathrm{O}(2, \mathbb{R}) = \mathrm{SO}(2, \mathbb{R}) \rtimes \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\} \cong \mathrm{SO}(2, \mathbb{R}) \rtimes \mathbb{Z}/2\mathbb{Z}.$$

- (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: Dopelnienie 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 $\Im(z) = 0$,

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

Oczywiście odbicie to nie jest obrotem, mamy zatem rozkład

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

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 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) Prosty, lecz zarazem pobudzający wyobraźnię przykładów iloczynów półprostych grup dostarcza niskowymiarowa topologia, z którą zetknęliśmy się w Przykł. 5 (3) 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 $([a^m]_{\sim}, [b^n]_{\sim})$, 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 wnętrze $I^{\times 2}$) 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 $(0, 1) \sim_X (0, 0)$, $X \in \{\mathbb{T}^2, \text{KB}\}$. Otrzymujemy w ten sposób następującą relację

$$(5.7) \quad \begin{aligned} [a \circ b \circ \bar{a}]_{\sim} &= [b]_{\sim} & \iff & [a]_{\sim} \star [b]_{\sim} \star \text{Inv}([a]_{\sim}) = [b]_{\sim} \\ & & \iff & [a]_{\sim} \star [b]_{\sim} = [b]_{\sim} \star [a]_{\sim} \end{aligned}$$

dla torusa i analogiczną relację

$$(5.8) \quad \begin{aligned} [a \circ \bar{b} \circ \bar{a}]_{\sim} &= [b]_{\sim} & \iff & [a]_{\sim} \star \text{Inv}([b]_{\sim}) \star \text{Inv}([a]_{\sim}) = [b]_{\sim} \\ & & \iff & \text{Inv}([a]_{\sim}) \star [b]_{\sim} \star [a]_{\sim} = \text{Inv}([b]_{\sim}) \end{aligned}$$

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

$$(5.9) \quad \prod_{k=1}^N ([a]_{\sim}^{m_k} \cdot [b]_{\sim}^{n_k}) = [\varepsilon_{x^*}]_{\sim}$$

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 (5.7),

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

oraz – odpowiednio – 5.8

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

bez trudu przepisujemy relację (5.9) 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,

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

✓

5.5. Rozszerzenia homomorfizmów a ich jednostronna odwracalność

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 46. 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 $\chi : H^{(1)} \rightarrow G^{(2)}$. **Rozszerzeniem homomorfizmu χ do grupy $G^{(1)}$** nazywamy dowolny homomorfizm $\tilde{\chi} : G^{(1)} \rightarrow G^{(2)}$ 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 44. *Przyjmijmy notację Def. 40. 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 przypuścimy, 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. $\square$

Z sytuacji opisanej w powyższym stwierdzeniu możemy wyabstrahować

DEFINICJA 47. 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

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

Ileokroć 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 5.4 (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:

$$(5.10) \quad G^{(1)} = \text{Ker } \tilde{\chi} \cdot_{(1)} H^{(1)}.$$

Biorąc pod uwagę surjektywność χ , dostajemy

$$g \in G^{(1)} \implies \exists_{h \in H^{(1)}} : \tilde{\chi}(g) = \chi(h) \equiv \tilde{\chi}(h) \implies \tilde{\chi}(g \cdot_{(1)} h^{-1}) = e^{(2)}$$

$$\iff g \cdot_{(1)} h^{-1} \in \text{Ker } \tilde{\chi} \implies g = (g \cdot_{(1)} h^{-1}) \cdot_{(1)} h \in \text{Ker } \tilde{\chi} \cdot_{(1)} H^{(1)},$$

co wobec oczywistej relacji

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

daje pożądaną równość (5.10). 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- $\text{Ker } \tilde{\chi}$.

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 $n_2^{-1} \cdot_{(1)} n_1 = h_2 \cdot_{(1)} h_1^{-1} \in N \cap H^{(1)} = \text{Ker } \chi \implies \chi(h_2 \cdot_{(1)} h_1^{-1}) = e^{(2)} \iff \chi(h_2) = \chi(h_1)$.

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 45. *Przyjmijmy notację Tw. 5.4 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. 27 (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

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

a zatem teza stwierdzenia wynika z Tw. 5.4 (ii). □

Warto zaznaczyć, że dotychczasowe wyniki dotyczące rozszerzeń epimorfizmów ustanawiają naturalną podstawę analizy rozszerzeń odwzorowań (R -)liniowych w kontekście teorii modułów nad pierścieniem (w tej liczbie także przestrzeni wektorowych). Pełnią one także kluczową rolę w dyskusji zagadnienia jednostronnej odwracalności homomorfizmów, która z kolei pokazuje dowodnie naturalność (i powszechność) struktury iloczynu półprostego grup.

DEFINICJA 48. W notacji Def. 35 **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 precyzuje⁶

STWIERDZENIE 46. *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

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



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

TWIERDZENIE 5.5 (O jednostronnej odwracalności homomorfizmu). *W notacji Def. 35 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. 5.1. Jest przy tym oczywistym, że każda lewostronna odwrotność χ jest rozszerzeniem λ_χ^{-1} do $G^{(2)}$ i *vice versa*. W świetle Tw. 5.4 rozszerzenie takie istnieje (i jest określone jednoznacznie) wtedy i tylko wtedy, gdy istnieje w $G^{(2)}$ dopełnienie normalne N obrazu χ modulo $\text{Ker } \lambda_\chi^{-1} = \{e^{(2)}\}$. Oznaczmy to rozszerzenie przez $\chi_L^{-1}(N)$. Na mocy Stw. 45 zachodzi równość $\text{Ker } \chi_L^{-1}(N) = N \cdot_{(2)} \text{Ker } \lambda_\chi^{-1} = N$.

⁶Związki te stają się równoważnościami, gdy rozważamy zbiory bez struktury algebraicznej. Nie każda jednak jednostronna odwrotność jest homomorfizmem.

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

$$(5.11) \quad G^{(1)} = \text{Ker } \chi \rtimes H.$$

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 (5.11)

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

a ponadto χ_H jest iniekcją, 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 odwzorowanie χ_H^{-1} spełnia warunek $\chi \circ \chi_H^{-1} = \text{id}_{G^{(2)}}$, widzimy zatem, że każdemu dopełnieniu H jądra χ w $G^{(1)}$ odpowiada 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

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

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 $G^{(1)}$.

□

O znaczeniu związku między jednostronnymi odwrotnościami homomorfizmów a iloczynami (pół)prostymi grup przekonamy się pełniej przy okazji dyskusji zagadnienia rozszczepialności ciągów dokładnych modułów nad pierścieniem w Rozdz. 8.

5.6. Grupy ilorazowe i ciągi dokładne w obrazie homomorfizmu

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

TWIERDZENIE 5.6 (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

$$\chi : G/H_2 \longrightarrow G/H_1 : gH_2 \longmapsto gH_1.$$

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

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

gdyż

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

Wobec surjektywności χ teza przyjmuje teraz oczywistą postać

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

por. Tw. 5.1. □

Niniejszy dział, poświęcony abstrakcyjnym własnościom grup, zamknijemy opisem transportu ciągów dokładnych typu (5.4) względem homomorfizmów grup.

TWIERDZENIE 5.7 (O homomorficznym przeciwobrazie normalnego ciągu dokładnego grup). *W notacji Def. 35, 42 oraz 43 i dla dowolnego dzielnika normalnego $H^{(2)} \subset G^{(2)}$ istnieje kanoniczny monomorfizm indukowany*

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

który czyni przemiennym diagram

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

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 $g \in G^{(1)}$)

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

Stąd wynika – na mocy Tw. 5.2 – istnienie kanonicznego monomorfizmu (indukowanego)

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

który oznaczamy jako $\bar{\chi}$. Przemienność diagramu jest teraz treścią definicji $\bar{\chi}$ – istotnie, $\bar{\chi}$ to w świetle Tw. 5.2 (jedyne) monomorfizm spełniający warunek

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

por. (5.6).

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. $\square$

Ostatnie twierdzenie znajdzie zastosowanie w dyskusji elementarnych zagadnień algebry homologicznej w Rozdz. 14.

PRZYKŁAD(Y) 27. 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)

$$\begin{array}{ccccc}
 & & 6\mathbb{Z} & & \\
 & & \downarrow & & \\
 2\mathbb{Z} & \rightarrow & \mathbb{Z} & \twoheadrightarrow & \mathbb{Z}/2\mathbb{Z} \\
 \downarrow & & \downarrow & & \downarrow \cong \\
 \{[0]_6, [2]_6, [4]_6\} & \rightarrow & \mathbb{Z}/6\mathbb{Z} & \twoheadrightarrow & (\mathbb{Z}/6\mathbb{Z})/\{[0]_6, [2]_6, [4]_6\}
 \end{array}$$

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 (pół)prostemu

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

✓

*

*

*

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

Działanie grupy na zbiorze

Zasada symetrii jest bezsprzecznie jedną z podstawowych zasad nowoczesnej fizyki, porządkującą – w duchu prac Wignera – strukturę teorii fizycznych (w terminach tzw. teorii reprezentacji grup symetrii) i wyjaśniającą – za Noether – głęboki sens matematyczny fizycznych zasad zachowania. W połączeniu z zasadą lokalności prowadzi ona wprost do mechanizmu cechowania symetrii globalnych, fundamentalnego dla obowiązującego opisu teoretycznego (części) oddziaływań elementarnych, jak również dla modeli fizyki matematycznej stanowiących rozwijane obecnie propozycje kwantowego opisu oddziaływań grawitacyjnych.

6.1. Struktura zbioru z działaniem grupy i jej transport

Punktem wyjścia do strukturalnego zrozumienia zasady symetrii jest wprowadzenie pojęcia działania grupy na zbiorze.

DEFINICJA 49. Przyjmijmy notację Def. 32. Niechaj X będzie zbiorem i niech $(G, \phi_2, \phi_1, \phi_0)$ będzie grupą. **Lewostronne działanie grupy G na zbiorze X** to odwzorowanie

$$\lambda : G \times X \longrightarrow X : (g, x) \longmapsto g \triangleright x$$

spełniające następujące aksjomaty (wyrażone przez diagramy przemienne i równoważne zdania logiczne):

(IDG1) (homomorficzność działania)

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

(IDG2) (trywialność działania elementu neutralnego)

$$\begin{array}{ccc} \{\bullet\} \times X & \xrightarrow{\phi_0 \times \text{id}_X} & G \times X \\ & \searrow \text{pr}_2 & \downarrow \lambda \\ & & X \end{array} \quad \equiv \quad \forall_{x \in X} : e \triangleright x = x.$$

Parę (X, λ) określamy mianem **zbioru z działaniem lewostronnym G** (lub też – z angielska – **lewostronnym G -zbiorem**).

Prawostronne działanie grupy G na zbiorze X to odwzorowanie

$$\varrho : X \times G \longrightarrow X : (x, g) \longmapsto x \triangleleft g$$

spełniające następujące aksjomaty (wyrażone przez diagramy przemienne i równoważne zdania logiczne):

(rDG1) (homomorficzność działania)

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

(rDG2) (trywialność działania elementu neutralnego)

$$\begin{array}{ccc}
 X \times \{\bullet\} & \xrightarrow{\text{id}_X \times \phi_0} & X \times G \\
 \searrow \text{pr}_1 & & \downarrow \varrho \\
 & & X
 \end{array} \quad \equiv \quad \forall_{x \in X} : x \triangleleft e = x.$$

Parę (X, ϱ) określamy mianem **zbioru z działaniem prawostronnym** G (lub też **prawostronnym G -zbiorem**). G (lub też **prawostronnym G -zbiorem**). ▲

Jako prosty wniosek z powyższej definicji otrzymujemy

STWIERDZENIE 47. W notacji Def. 32 i 49 oznaczmy – dla dowolnego $g \in G$

$$\lambda_g : X \longrightarrow X : x \longmapsto g \triangleright x, \quad \varrho_g : X \longrightarrow X : x \longmapsto x \triangleleft g.$$

Wówczas odwzorowanie dane wzorem

$$\lambda : G \longrightarrow \text{Map}(X, X) : g \longmapsto \lambda_g$$

jest homomorfizmem monoidu (G, ϕ_2, ϕ_0) w monoid $(\text{Map}(X, X), \circ, \bullet \longmapsto \text{id}_X)$ odwzorowań zbioru X w siebie (ze składaniem odwzorowań oraz odwzorowaniem tożsamościowym jako elementem neutralnym). Homomorfizm ten określamy mianem **lewostronnej realizacji** (albo inaczej **reprezentacji**) grupy G na zbiorze X indukowanej przez działanie λ . Analogicznie odwzorowanie dane wzorem

$$\varrho : G \longrightarrow \text{Map}(X, X) : g \longmapsto \varrho_g$$

jest homomorfizmem monoidu $(G, \phi_2^{\text{opp}}, \phi_0)$ w monoid $(\text{Map}(X, X), \circ, \bullet \longmapsto \text{id}_X)$. Homomorfizm ten określamy mianem **prawostronnej realizacji** (albo inaczej **reprezentacji**) grupy G na zbiorze X indukowanej przez działanie ϱ . ■

NOTACJA 5. O ile nie będzie to prowadziło do nieporozumień, będziemy czasem używać pojęcia „działanie” w odniesieniu do odwzorowania λ . (wzgl. ϱ).

* * *

Obraz realizacji grupy daje się opisać dużo precyzyjniej.

STWIERDZENIE 48. W notacji Def. 32 i 49 dowolna realizacja lewostronna (względnie prawostronna) G na X jest homomorfizmem tejże grupy (względnie grupy do niej przeciwnej) w grupę symetryczną na X . I odwrotnie, każdy taki homomorfizm definiuje pewną realizację grupy G na X .

■

Dowód: Istnieje wzajemnie jednoznaczna odpowiedniość pomiędzy homomorfizmami grup i homomorfizmami odnośnych monoidów, jedyną zatem nietrywialną częścią powyższego stwierdzenia jest ta mówiąca o bijektywnym charakterze odwzorowań λ_g i ϱ_g dla dowolnego $g \in G$. Ich surjektywność jest prostą konsekwencją tożsamości

$$\lambda_g \circ \lambda_{g^{-1}} = \lambda_{g \cdot g^{-1}} = \lambda_e = \text{id}_X = \varrho_e = \varrho_{g^{-1} \cdot g} = \varrho_g \circ \varrho_{g^{-1}},$$

oto bowiem otrzymujemy – dla dowolnego $x \in X$ –

$$x = \lambda_g \circ \lambda_{g^{-1}}(x) \in \text{Im } \lambda_g$$

oraz

$$x = \varrho_g \circ \varrho_{g^{-1}}(x) \in \text{Im } \varrho_g.$$

Injektywność odwzorowania λ_g dla dowolnego $g \in G$ stwierdzamy w bezpośrednim rachunku:

$$\lambda_g(x) = \lambda_g(y) \implies x = \lambda_{g^{-1}} \circ \lambda_g(x) = \lambda_{g^{-1}} \circ \lambda_g(y) = y,$$

w którym $x, y \in X$ są dowolne. Analogiczny rachunek dowodzi injektywności ϱ_g . □

Kolejny wynik pozwala nam ograniczyć się w dalszych rozważaniach, bez jakiegokolwiek straty ogólności, do działań lewostronnych¹. Oto bowiem

STWIERDZENIE 49. *W notacji Def. 32 i 49 izomorfizm grup $\phi_1 : (G, \phi_2, \phi_1, \phi_0) \xrightarrow{\cong} (G, \phi_2^{\text{opp}}, \phi_1, \phi_0)$ indukuje kanoniczną bijekcję między zbiorami $\text{Mor}_L(G, X)$ lewostronnych i $\text{Mor}_R(G, X)$ prawostronnych działań grupy G na zbiorze X , daną wzorem*

$${}^L\phi_1^* : \text{Mor}_L(G, X) \xrightarrow{\sim} \text{Mor}_R(G, X) : \lambda \mapsto \lambda \circ \phi_1.$$

■

Dowód: Odwrotnością ${}^L\phi_1^*$ jest odwzorowanie

$${}^R\phi_1^* : \text{Mor}_R(G, X) \longrightarrow \text{Mor}_L(G, X) : \varrho \mapsto \varrho \circ \phi_1,$$

por. Stw. 25 (ii). □

PRZYKŁAD(Y) 28.

- (1) **Działanie trywialne:** $\lambda : G \longrightarrow \mathfrak{S}_X : g \mapsto \text{id}_X$.
- (2) Naturalne działanie grupy symetrycznej $\mathfrak{S}_X$ na zbiorze X poprzez permutacje jego elementów: $\lambda = \text{id}_{\mathfrak{S}_X}$.

¹Odstępstwem od reguły będzie dyskusja wiązek głównych o grupie strukturalnej G , co do których zwyczajowo zakłada się, że tzw. włókno typowe jest przestrzenią z (regularnym) działaniem prawostronnym G .

- (3) Działanie grupy $\mathbb{Z}$ (z dodawaniem) na zbiorze $\mathbb{R}$ przez przesunięcia, $\lambda = T : \mathbb{Z} \longrightarrow \mathfrak{S}_{\mathbb{R}} : n \longmapsto T_n$, gdzie $T_n : \mathbb{R} \ni r \longmapsto r + n$. Innym typem działania tej samej grupy $\mathbb{Z}$ na tym samym zbiorze $\mathbb{R}$ jest odwzorowanie $\lambda = (-1)^{\cdot} : \mathbb{Z} \longrightarrow \mathfrak{S}_{\mathbb{R}} : n \longmapsto (-1)^n$, gdzie $(-1)^n : \mathbb{R} \ni r \longmapsto (-1)^n \cdot r$. Przykłady te dokumentują możliwość istnienia *całkowicie różnych* realizacji *tej samej* grupy na *tym samym* zbiorze.
- (4) **Działanie dołączone** grupy G na sobie: $\lambda = \text{Ad} : G \longrightarrow \text{Inn}(G) \subset \mathfrak{S}_G$. Elementy $g, \text{Ad}_h(g) \in G$ nazywamy **(wzajem) sprzężonymi**. Określenie to przenosimy także na podgrupy nazywając podgrupę $\text{Ad}_g(H)$ **podgrupą sprzężoną względem podgrupy $H \subset G$** .
- (5) **Działanie (lewostronne) regularne** grupy G na sobie: $\lambda = \ell : G \longrightarrow \mathfrak{S}_G : g \longmapsto \ell_g$, gdzie $\ell_g : G \ni h \longmapsto g \cdot h$.
- (6) Działanie grupy symetrycznej $\mathfrak{S}_X$ na $\text{Map}(X, Y)$, dla dowolnej pary zbiorów X, Y , poprzez **cofnięcie** względem odwrotności permutacji,

$$(\cdot)^* \circ \text{Inv} : \mathfrak{S}_X \longrightarrow \mathfrak{S}_{\text{Map}(X, Y)} : \sigma \longmapsto (\sigma^{-1})^*,$$

$$(\sigma^{-1})^* : \text{Map}(X, Y) \ni f \longmapsto f \circ \sigma^{-1}.$$

Jego złożenie z działaniem dowolnej grupy G na X prowadzi do realizacji tejże grupy na $\text{Map}(X, Y)$, szczególnie istotnej w kontekście fizycznym (w którym najczęściej zbiór X jest nośnikiem dodatkowej struktury, np. struktury topologicznej lub różniczkowej, jak to ma miejsce choćby w przypadku czasoprzestrzeni, na której działa grupą izometrii, albo też wiązki pól rozważanego modelu dynamiki, na której to wiązce działa grupa symetrii teorii pola).

- (7) Działanie grupy $\mathbb{R}/2\pi\mathbb{Z} \cong \text{U}(1)$ na płaszczyźnie $\mathbb{R}^2 \cong \mathbb{C}$ przez obrót o środku $(0, 0)$, wedle definicji

$$R_{\cdot} : \mathbb{R}/2\pi\mathbb{Z} \longrightarrow \mathfrak{S}_{\mathbb{C}} : [\theta] \longmapsto R_{[\theta]} \equiv R_{\theta},$$

$$R_{\theta} : \mathbb{C} \ni z \longmapsto e^{-i\theta} \cdot z.$$

W opisie kartezjańskim otrzymujemy znajome formuły:

$$\begin{aligned} \Re(R_{\theta}(z)) &= \frac{e^{-i\theta} \cdot z + \overline{e^{-i\theta} \cdot z}}{2} \\ &= \frac{(\cos \theta - i \sin \theta) \cdot (\Re(z) + i \Im(z)) + (\cos \theta + i \sin \theta) \cdot (\Re(z) - i \Im(z))}{2} \\ &= \cos \theta \cdot \Re(z) + \sin \theta \cdot \Im(z), \\ \Im(R_{\theta}(z)) &= \cos \theta \cdot \Im(z) - \sin \theta \cdot \Re(z), \end{aligned}$$

które możemy przedstawić zwięźle w zapisie macierzowym:

$$\begin{pmatrix} \Re(R_{\theta}(z)) \\ \Im(R_{\theta}(z)) \end{pmatrix} = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} \cdot \begin{pmatrix} \Re(z) \\ \Im(z) \end{pmatrix}.$$

Zapis ten ilustruje ciąg izomorfizmów grup $\mathbb{R}/2\pi\mathbb{Z} \cong \text{U}(1) \cong \text{SO}(2, \mathbb{R})$.

- (8) Naturalne działanie grupy obrotów w przestrzeni $\mathbb{R}^3$ o środku w punkcie o współrzędnych $(0, 0, 0)$ ogranicza się do dowolnej 2-sfery o środku w tymże punkcie.

(9) Niechaj $(G, \cdot, (\cdot)^{-1}, \bullet \mapsto e)$ będzie dowolną grupą i niech

$$H_n := \{ (g_1, g_2, \dots, g_n) \in G^{\times n} \mid \gamma_1 \cdot g_2 \cdots g_n = e \}.$$

Grupa $\mathfrak{B}_n$ warkoczy o n pasmach z Przykł. 15 (5) działa na H_n w sposób określony jednoznacznie przez działanie generatorów grupy:

$$\begin{aligned} [\tau_i] &\triangleright (g_1, g_2, \dots, g_{i-1}, g_i, g_{i+1}, g_{i+2}, \dots, g_n) \\ &:= (g_1, g_2, \dots, g_{i-1}, g_{i+1}, \text{Ad}_{g_{i+1}}^{-1}(g_i), g_{i+2}, g_{i+3}, \dots, g_n). \end{aligned}$$

✓

Zgodnie z ogólną logiką wykładu dyskusję wstępną zakończymy opisem odwzorowań między nośnikami działania grupy, zgodnych z tą strukturą.

DEFINICJA 50. Przyjmijmy notację Def. 32 i 49 i niech $(X^{(\alpha)}, \lambda^{(\alpha)})$, $\alpha \in \{1, 2\}$ będą zbiorami z działaniem lewostronnym grupy G . **Odwzorowanie lewostronnie G -ekwiwariantne** (albo inaczej **lewostronne G -odwzorowanie**, wzgl. **lewostronny G -homomorfizm**) $(X^{(1)}, \lambda^{(1)})$ w $(X^{(2)}, \lambda^{(2)})$ to odwzorowanie

$$f : X^{(1)} \longrightarrow X^{(2)}$$

spełniające aksjomat (wyrażony przez diagram przemienności i równoważne zdanie logiczne):

$$(1GE) \quad \begin{array}{ccc} G \times X^{(1)} & \xrightarrow{\lambda^{(1)}} & X^{(1)} \\ \text{id}_G \times f \downarrow & & \downarrow f \\ G \times X^{(2)} & \xrightarrow{\lambda^{(2)}} & X^{(2)} \end{array} \quad \equiv \quad \forall_{(g,x) \in G \times X^{(1)}} : f \circ \lambda_g^{(1)}(x) = \lambda_g^{(2)} \circ f(x).$$

Jeśli f jest przy tym bijekcją, to mówimy o **G -ekwiwariantnym izomorfizmie zbiorów z działaniem lewostronnym**.

Odwzorowanie prawostronnie G -ekwiwariantne definiujemy analogicznie.

▲

PRZYKŁAD(Y) 29.

- (1) Niechaj $\Delta_{(0,0)}$ będzie zbiorem trójkątów na płaszczyźnie o jednym z wierzchołków w punkcie $(0,0)$. Na zbiorze tym grupa $\text{GL}(2, \mathbb{R})$ odwracalnych przekształceń liniowych punktów płaszczyzny działa w naturalny sposób: obrazem punktu trójkąta o współrzędnych (x, y) względem działania macierzy $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}(2, \mathbb{R})$ jest punkt płaszczyzny o współrzędnych $(a \cdot x + b \cdot y, c \cdot x + d \cdot y)$. Odwzorowanie $A : \Delta_{(0,0)} \longrightarrow \mathbb{R}_{>0}$ przyporządkowujące trójkątowi jego pole powierzchni jest $\text{GL}(2, \mathbb{R})$ -ekwiwariantne względem rzeczonego działania na $\Delta_{(0,0)}$ i następującego działania na $\mathbb{R}_{>0}$:

$$\text{GL}(2, \mathbb{R}) \times \mathbb{R}_{>0} \longrightarrow \mathbb{R}_{>0} : \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, r \right) \longmapsto (a \cdot d - b \cdot c) \cdot r.$$

- (2) Dla pary grup $(G^{(\alpha)}, \phi_2^{(\alpha)}, \phi_1^{(\alpha)}, \phi_0^{(\alpha)})$, $\alpha \in \{1, 2\}$ dowolny komomorfizmy $\chi : G^{(1)} \longrightarrow G^{(2)}$ jest odwzorowaniem $G^{(1)}$ -ekwiwariantnym względem działania dołączonego,

$$\chi : (G^{(1)}, \text{Ad}) \longrightarrow (G^{(2)}, \text{Ad} \circ (\chi \times \text{id}_{G^{(2)}})) ,$$

przy czym

$$\text{Ad} : G^{(1)} \times G^{(1)} \longrightarrow G^{(1)} : (g, h) \longmapsto \text{Ad}_g(h) ,$$

por. Przykł. 22 (2), jak również względem działania lewostronnego regularnego,

$$\chi : (G^{(1)}, \ell) \longrightarrow (G^{(2)}, \ell \circ (\chi \times \text{id}_{G^{(2)}})) ,$$

przy czym

$$\ell : G^{(1)} \times G^{(1)} \longrightarrow G^{(1)} : (g, h) \longmapsto g \cdot h ,$$

por. Przykł. 28 (5). W tym ostatnim przypadku konkretnym przykładem jest automorfizm antypodalny $\alpha : \text{U}(1) \ni u \longmapsto -u$ na okręgu jednostkowym $\text{U}(1) \cong \mathbb{S}^1$.

- (3) Niechaj $(G, \phi_2, \phi_1, \phi_0)$ będzie grupą, $(\mathbb{K}, A, M, P, \text{Inv}, \mathbf{0}, \mathbf{1})$ zaś – dowolnym ciałem, traktowanym jako zbiór z trywialnym działaniem $\lambda_0 : G \times \mathbb{K} \longrightarrow \mathbb{K} : (g, k) \longmapsto k$. **Funkcje klas grupy G o wartościach z ciała $\mathbb{K}$** są definiowane jako odwzorowania G -ekwiwariantne

$$f : (G, \text{Ad}) \longrightarrow (\mathbb{K}, \lambda_0) .$$

Konkretnym przykładem takiej funkcji jest znak permutacji $\text{sgn} : \mathfrak{S}_X \longrightarrow \{-1, 1\}$.

✓

Elementarnej charakteryzacji odwzorowań G -ekwiwariantnych dostarcza

STWIERDZENIE 50. *Odwrotność dowolnego bijektywnego odwzorowania G -ekwiwariantnego jest także odwzorowaniem G -ekwiwariantnym.*

■

Dowód: Przykładając odwrotność f do obu stron równości

$$f \circ \lambda_g^{(1)}(x) = \lambda_g^{(2)} \circ f(x) ,$$

zapisanej dla dowolnych $g \in G$ oraz $x \in X^{(1)}$ i definiującej odwzorowanie G -ekwiwariantne, otrzymujemy

$$\lambda_g^{(1)}(x) = \text{id}_{X^{(1)}} \circ \lambda_g^{(1)}(x) = f^{-1} \circ f \circ \lambda_g^{(1)}(x) = f^{-1} \circ \lambda_g^{(2)} \circ f(x) ,$$

skoro jednak dla każdego $x \in X^{(1)}$ istnieje, i to dokładnie jedno, $y \in X^{(2)}$ o własności

$$x = f^{-1}(y) ,$$

a przy tym $X^{(2)} = f(X^{(1)})$, to wnioskujemy, że

$$\lambda_g^{(1)} \circ f^{-1}(y) = f^{-1} \circ \lambda_g^{(2)}(y)$$

dla dowolnych $g \in G$ i $y \in X^{(2)}$.

□

Dalszej charakteryzacji tych odwzorowań dokonamy po wprowadzeniu dodatkowych pojęć.

6.2. Stratyfikacja grupy i G -zbioru indukowana przez działanie

Zbadamy teraz anatomię działania grupy na zbiorze zarówno od strony grupy, jak i od strony zbioru, po to by sklasyfikować w naturalny sposób typy działań i ostatecznie powiązać obie składowe opisu w terminach teorii mocy. Zaczniemy dyskusję od strony grupy.

DEFINICJA 51. W notacji Def. 32 i 49 **stabilizator** (lub **grupa izotropii**) **elementu** $x \in X$ nośnika działania grupy G to zbiór

$$G_x := \{ g \in G \mid g \triangleright x = x \}.$$

▲

PRZYKŁAD(Y) 30.

- (1) Cała grupa G jest stabilizatorem dowolnego elementu nośnika reprezentacji trywialnej.
- (2) Stabilizatorem elementu $x \in X$ względem naturalnego działania $\mathfrak{S}_X$ jest zbiór wszystkich tych permutacji σ elementów X , których **nośnik**

$$\text{supp}(\sigma) := \{ y \in X \mid \sigma(y) \neq y \},$$

nie zawiera x . I tak, np.,

$$(\mathfrak{S}_3)_1 = \{\text{id}_{\{1,2,3\}}, (23)\} \cong \mathbb{Z}_2.$$

- (3) Stabilizatorem dowolnego elementu $\mathbb{R}$ względem działania T z Przykł. 28 (3) jest grupa trywialna. Stabilizatorem każdego elementu $r \neq 0$ względem działania $(-1)^\cdot$ z tego samego przykładu jest podgrupa $2\mathbb{Z} \subset \mathbb{Z}$. W przypadku $r = 0$ stabilizatorem względem tego działania jest pełna grupa $\mathbb{Z}$.
- (4) Stabilizator elementu $g \in G$ względem działania dołączonego Ad z Przykł. 28 (4) określamy mianem **centralizatora** g i oznaczamy jako

$$C_G(g) := \{ h \in G \mid \text{Ad}_h(g) = g \}.$$

Ogólniej, dla dowolnego podzbioru $S \subset G$ definiujemy centralizator S jako podgrupę

$$C_G(S) := \{ g \in G \mid \forall_{x \in S} : \text{Ad}_g(x) = x \}.$$

- (5) Stabilizatorem dowolnego punktu x 2-sfery o środku w punkcie o współrzędnych $(0, 0, 0)$ względem (ograniczenia) działania grupy obrotów z Przykł. 28 (8) jest podgrupa obrotów (płaskich) wokół osi przechodzącej przez x oraz przez punkt o współrzędnych $(0, 0, 0)$.
- (6) Stabilizatorem dowolnego wierzchołka n -kąta foremnego względem działania jego grupy symetrii D_{2n} jest podgrupa (izomorficzna z) $\mathbb{Z}_2$ generowana przez odbicie symetryczne względem dwusiecznej kąta przy tymże wierzchołku.

✓

Mamy oczywiste

STWIERDZENIE 51. *Stabilizator dowolnego elementu nośnika działania grupy jest podgrupą tej ostatniej.* ■

Ponadto

STWIERDZENIE 52. *W notacji Def. 32, 36 i 49 zachodzi tożsamość*

$$\text{Ker } \lambda = \bigcap_{x \in X} G_x.$$

PRZYKŁAD(Y) 31.

- (1) $\text{Ker } \lambda = G$ dla trywialnego działania λ grupy G na dowolnym zbiorze.
- (2) Jądro naturalnego działania $\mathfrak{S}_X$ na X jest trywialne.
- (3) $\text{Ker } T = \{0\}$ oraz $\text{Ker } (-1) = 2\mathbb{Z}$ dla działań T i (-1) grupy $\mathbb{Z}$ na $\mathbb{R}$ z Przykł. 28 (3).
- (4) $\text{Ker } \text{Ad} = \mathcal{Z}(G)$ dla działania dołączonego grupy G na sobie z Przykł. 28 (4). Działanie regularne z Przykł. 28 (5) ma jądro trywialne. ✓

W następnej kolejności zajmiemy się relacjami, jakie działanie grupy wprowadza w nośniku realizacji. W tym celu będziemy potrzebować dodatkowego pojęcia, które określa

DEFINICJA 52. W notacji Def. 32 i 49 **orbita elementu** $x \in X$ **względem działania** λ to zbiór

$$G \triangleright x := \{ \lambda_g(x) \mid g \in G \}.$$

PRZYKŁAD(Y) 32.

- (1) Orbitą elementu $x \in X$ względem działania trywialnego grupy G na X jest singleton $\{x\}$.
- (2) Orbitą elementu $x \in X$ względem naturalnego działania $\mathfrak{S}_X$ na X jest X .
- (3) Zbiór $\{-r, r\}$ jest orbitą działania (-1) grupy $\mathbb{Z}$ na $\mathbb{R}$ z Przykł. 28 (3).
- (4) Orbitę elementu $g \in G$ względem działania dołączonego grupy G na sobie z Przykł. 28 (4) określamy mianem **klasy sprzężoności** g i oznaczamy jako

$$C(g) := \{ \text{Ad}_h(g) \mid h \in G \}.$$

- (5) Orbitą elementu $g \in G$ względem działania regularnego grupy G na sobie z Przykł. 28 (5) jest G . Orbitą tegoż $g \in G$ względem działania regularnego podgrupy H na grupie G ,

$$\ell. : H \times G \longrightarrow G : (h, g) \longmapsto h \cdot g,$$

jest warstwa prawostronna Hg .

- (6) Orbitą elementu $z \in \mathbb{C}$ względem działania R grupy $\mathbb{R}/2\pi\mathbb{Z}$ z Przykł. 28 (7) jest okrąg $|z|U(1)$.
 (7) Orbitą dowolnego punktu $x \in \mathbb{R}^3$ względem naturalnego działania grupy obrotów w $\mathbb{R}^3$ (względem punktu o współrzędnych $(0,0,0)$) jest 2-sfera o środku w punkcie o współrzędnych $(0,0,0)$ i promieniu $|x|$.

✓

Możemy już teraz wysłowić

STWIERDZENIE 53. W notacji Def. 32 i 49 relacja na $X \ni x, y$ zadana, jak następuje:

$$x \sim_\lambda y \iff x \in G \triangleright y,$$

jest relacją równoważności. Działanie grupy zadaje zatem rozkład nośnika na sumę rozłączną orbit względem tego działania.

■

Dowód:

- (1) $x = e \triangleright x \in G \triangleright x \implies x \sim_\lambda x$.
- (2) $x \sim_\lambda y \iff \exists_{g \in G} : x = g \triangleright y \implies g^{-1} \triangleright x = g^{-1} \triangleright (g \triangleright y) = (g^{-1} \cdot g) \triangleright y = e \triangleright y = x \implies y \sim_\lambda x$.
- (3) $(x \sim_\lambda y \wedge y \sim_\lambda z) \iff \exists_{g_1, g_2 \in G} : (x = g_1 \triangleright y \wedge y = g_2 \triangleright z) \implies x = g_1 \triangleright (g_2 \triangleright z) = (g_1 \cdot g_2) \triangleright z \implies x \sim_\lambda z$.

□

Wprowadzenie pojęć stabilizatora i orbity pozwala w naturalny sposób sklasyfikować działania grupy na zbiorze.

DEFINICJA 53. W notacji Def. 32, 49, 51 i 52 oraz Stw. 53 działanie λ nazywamy

- **trywialnym**, jeśli $\forall_{g \in G} : \lambda_g = \text{id}_X$, tj. wszystkie orbity działania są jednoelementowe;
- **przechodnim** (lub **tranzytywnym**), jeśli $\forall_{x, y \in X} : x \sim_\lambda y$, tj. zbiór X jest pojedynczą orbitą $G \triangleright x = X$ (dowolnego) swojego elementu $x \in X$;
- **wolnym**, jeśli $\forall_{g, h \in G} : g \triangleright x = h \triangleright x \implies g = h$, tj. $\forall_{x \in X} : G_x = \{e\}$, co oznacza, że odwzorowanie λ_g nie ma punktów stałych dla $g \in G \setminus \{e\}$, a wtedy określamy X mianem **przestrzeni jednorodnej**;
- **wiernym** (lub **efektywnym**), jeśli $\forall_{g, h \in G} : (g \neq h \implies \exists_{x \in X} : g \triangleright x \neq h \triangleright x)$, czyli $\text{Ker } \lambda = \{e\}$, a wtedy grupa G jest kanonicznie izomorficzna z podgrupą $\text{Im } \lambda \subset \mathfrak{S}_X$;
- **regularnym**, jeśli jest ono przechodnie i wolne, a wtedy określamy X mianem G -torsora lub **głównej przestrzeni jednorodnej**.

▲

PRZYKŁAD(Y) 33.

- (1) Ograniczenie działania grupy na zbiorze do jądra tego działania jest działaniem trywialnym. W szczególności działanie dołączone grupy przemiennej na sobie jest tego typu.
- (2) Działanie grupy alternującej na zbiorze n -elementowym jest przechodnie dla każdego $n \geq 3$, por. Stw. 64. Tego typu jest też działanie grupy diedralnej rzędu $2n$ na zbiorze wierzchołków n -kąta foremnego. To samo dotyczy (indukowanego) działania lewostronnego regularnego grupy G na zbiorze warstw G/H względem podgrupy $H \subset G$.
- (3) Antypodalne działanie grupy odbić względem punktu o współrzędnych $(0, 0, 0) \in \mathbb{R}^3$ (izomorficznej z $\mathbb{Z}_2$) na dowolnej 2-sferze o środku w tym punkcie jest wolne. Tę własność ma również działanie regularne dowolnej grupy na sobie.
- (4) Działanie dołączone grupy G na sobie z Przykł. 28 (4) jest wierne wtedy i tylko wtedy, gdy $\mathcal{Z}(G) = \{e\}$. Podobnie, (indukowane) działanie lewostronne regularne grupy G na zbiorze warstw G/H względem podgrupy $H \subset G$ jest tego typu wtedy i tylko wtedy, gdy $\bigcap_{g \in G} gHg^{-1} = \{e\}$.
- (5) Zbiór izomorfizmów $\text{Iso}(G^{(1)}, G^{(2)})$ pomiędzy dowolnymi dwiema grupami $G^{(1)}$ i $G^{(2)}$ jest torskorem grupy $\text{Aut}(G^{(1)})$ względem działania prawostronnego

$$\varrho : \text{Iso}(G^{(1)}, G^{(2)}) \times \text{Aut}(G^{(1)}) \longrightarrow \text{Iso}(G^{(1)}, G^{(2)}) : (\chi, \alpha) \longmapsto \chi \circ \alpha.$$

Jest on zarazem torskorem grupy $\text{Aut}(G^{(2)})$ względem działania lewostronnego

$$\lambda : \text{Aut}(G^{(2)}) \times \text{Iso}(G^{(1)}, G^{(2)}) \longrightarrow \text{Iso}(G^{(1)}, G^{(2)}) : (\alpha, \chi) \longmapsto \alpha \circ \chi.$$

✓

W bezpośredniej konsekwencji Stw. 38 i 40 oraz Tw. 5.1 wyprowadzamy

STWIERDZENIE 54. *Przyjmijmy notację Def. 32, 36 i 42 oraz Przykł. 5 (1). Istnieje kanoniczny monomorfizm grup*

$$G/\text{Ker } \lambda \rightarrow \mathfrak{S}_X,$$

który indukuje wierne działanie grupy ilorazowej na X według wzoru

$$\tilde{\lambda} : G/\text{Ker } \lambda \times X \longrightarrow X : (g\text{Ker } \lambda, x) \longmapsto g \triangleright x.$$

■

Dostajemy ponadto

STWIERDZENIE 55. *Stabilizatory elementów z tej samej (dowolnej) orbity działania grupy są jej podgrupami wzajem sprzężonymi, a więc – w szczególności – izomorficznymi.*

■

Dowód: Z jednej strony

$$\forall_{\substack{x \in X \\ (g, h) \in G \times G_x}} : \text{Ad}_g(h) \triangleright (g \triangleright x) = (g \cdot h \cdot g^{-1} \cdot g) \triangleright x = g \triangleright (h \triangleright x) = g \triangleright x,$$

a zatem $\text{Ad}_g(G_x) \subset G_{g \triangleright x}$. Z drugiej strony

$$\begin{aligned} \forall_{\substack{x \in X \\ (g,h) \in G \times G_{g \triangleright x}}} : \text{Ad}_{g^{-1}}(h) \triangleright x &= (g^{-1} \cdot h \cdot g) \triangleright x = g^{-1} \triangleright (h \triangleright (g \triangleright x)) \\ &= g^{-1} \triangleright (g \triangleright x) = x, \end{aligned}$$

a zatem $\text{Ad}_{g^{-1}}(G_{g \triangleright x}) \subset G_x \iff G_{g \triangleright x} \subset \text{Ad}_g(G_x)$. Ostatecznie więc

$$G_{g \triangleright x} = \text{Ad}_g(G_x).$$

□

Zgromadzone dotychczas fakty i pojęcia stanowią podstawę do sformułowania kilku istotnych stwierdzeń, które szczegółowo charakteryzują działanie grupy na zbiorze.

TWIERDZENIE 6.1 (O klasyfikacji orbit). *Przyjmijmy notację Def. 32, 38, 49, 51 oraz 52 i rozważmy, dla dowolnego elementu $x \in X$, zbiór warstw G/G_x z działaniem*

$$[\ell] : G \times (G/G_x) \longrightarrow G/G_x : (g, hG_x) \longmapsto (g \cdot h)G_x.$$

Istnieje kanoniczny G -ekwiwariantny izomorfizm

$$G/G_x \xrightarrow{\sim} G \triangleright x,$$

stąd też zachodzi tożsamość

$$|G| = |G_x| \cdot |G \triangleright x|.$$

W szczególności więc moc dowolnej orbity w skończonym zbiorze z działaniem grupy skończonej jest dzielnikiem mocy tejże grupy.

■

Dowód: Pożądane odwzorowanie ma postać

$$f_x : G/G_x \longrightarrow G \triangleright x : gG_x \longmapsto g \triangleright x.$$

Jest ono dobrze określone, gdyż dla dowolnego reprezentanta $h \in gG_x$ możemy zapisać $h = g \cdot k$ dla pewnego $k \in G_x$, a w takim razie $g \triangleright x = g \triangleright (k \triangleright x) = (g \cdot k) \triangleright x = h \triangleright x$. Jego G -ekwiwariantność sprawdzamy w bezpośrednim rachunku:

$$f_x \circ [\ell](h, gG_x) = f_x((h \cdot g)G_x) = (h \cdot g) \triangleright x = \lambda(h, g \triangleright x) = \lambda(h, f_x(gG_x)).$$

Ponieważ zaś jest ono jawnie surjektywne, przeto pozostaje pokazać, że jest injekcją, czego dowodzimy, jak następuje:

$$\begin{aligned} f_x(gG_x) = f_x(hG_x) &\iff g \triangleright x = h \triangleright x \iff (h^{-1} \cdot g) \triangleright x = x \iff h^{-1} \cdot g \in G_x \\ &\iff g \in hG_x \iff gG_x = hG_x. \end{aligned}$$

Ostatnia część tezy dowodzonego twierdzenia jest – w świetle powyższego – bezpośrednim następstwem Cor. 4, oto bowiem na mocy (5.3) dostajemy

$$|G| = |G_x| \cdot (G : G_x) = |G_x| \cdot |G \triangleright x|.$$

□

Twierdzenie powyższe znajduje bezpośrednie zastosowanie w następującym wyniku, wykorzystywanym w rozważaniach natury enumeracyjnej (prowadzonych w terminach teorii mocy) dotyczących zbiorów z działaniem grup skończonych.

STWIERDZENIE 56. (Lemat Cauchy’ego–Frobeniusa, zwany też Lematem (nie od) Burnside’a) *Przyjmijmy notację Def. 32 i 49, a ponadto oznaczmy przez*

$$X/G := \{ G \triangleright x \mid x \in X \}$$

zbiór orbit działania grupy G na zbiorze X i przez

$$X^g := \{ x \in X \mid g \triangleright x = x \}$$

zbiór punktów stałych odwzorowania λ_g . Wówczas zachodzi tożsamość

$$|G| \cdot |X/G| = \sum_{g \in G} |X^g|.$$

■

Dowód: Wykorzystując Stw. 53 zapiszemy

$$\begin{aligned} \sum_{g \in G} |X^g| &= \sum_{g \in G} \sum_{G \triangleright x \in X/G} |(G \triangleright x)^g| = \sum_{G \triangleright x \in X/G} |\{ (g, y) \in G \times (G \triangleright x) \mid g \triangleright y = y \}| \\ &= \sum_{G \triangleright x \in X/G} \sum_{y \in G \triangleright x} |\{ g \in G \mid g \triangleright y = y \}| = \sum_{G \triangleright x \in X/G} \sum_{y \in G \triangleright x} |G_y|, \end{aligned}$$

a dalej – wobec Stw. 55 –

$$\sum_{g \in G} |X^g| = \sum_{G \triangleright x \in X/G} \sum_{y \in G \triangleright x} |G_x| = \sum_{G \triangleright x \in X/G} |G \triangleright x| \cdot |G_x|,$$

czyli też – na mocy Tw. 6.1 –

$$\sum_{g \in G} |X^g| = \sum_{G \triangleright x \in X/G} |G| = |G| \cdot |X/G|.$$

□

6.3. Modele struktury zbioru z działaniem grupy

W podsumowaniu niniejszej części wykładu dokonamy abstrakcji fundamentalnych cech działania przechodniego, które z jednej strony określają strukturę grupy w odwołaniu do własności dowolnego elementu nośnika działania, z drugiej zaś – ustalają swego rodzaju uniwersalny model zbioru z działaniem przechodnim. Zaczniemy od przestudiowania tego pierwszego aspektu.

STWIERDZENIE 57. (Lemat Frattiniego) *Przyjmijmy notację Def. 32, 34, 44, 49 i 51. Jeśli ograniczenie działania grupy G na zbiorze X do podgrupy $H \subset G$ jest działaniem przechodnim, to wówczas – dla dowolnego elementu $x \in X$ – zachodzi relacja*

$$G = H \cdot G_x.$$

Jeśli ponadto ograniczenie to jest działaniem wolnym, to jest

$$G = H \bullet G_x.$$

■

Dowód: Ustalmy (dowolnie) $x \in X$. Przechodność działania H implikuje dla dowolnego $g \in G$ istnienie pewnego $h \in H$ spełniającego warunek $g \triangleright x = h \triangleright x$, co oznacza $h^{-1} \cdot g \in G_x \iff g \in h G_x$, skąd też wynika pierwsza z dowodzonych relacji.

Jeśli działanie H na X jest ponadto wolne, tj. dla dowolnego $x \in X$ zachodzi $H_x = \{e\}$, to otrzymujemy dodatkowy warunek

$$H \cap G_x \equiv H_x = \{e\},$$

co w sumie odtwarza definicję iloczynu rozłącznego H i G_x . $\square$

Mamy też oczywiste

COROLLARIUM 6. *Przyjmijmy notację Def. 32, 38, 49, 51 i 52 oraz Tw. 6.1. Ilekroć działanie grupy G na zbiorze X jest przechodnie, spełniona jest równość*

$$|X| = (G : G_x).$$

■

Na koniec opiszemy uniwersalną postać zbioru z działaniem przechodnim.

TWIERDZENIE 6.2 (O ekwiwariantnym izomorfizmie zbiorów z działaniem). *Przyjmijmy notację Def. 32 oraz Przykł. 29 (2). Dowolny zbiór z działaniem przechodnim grupy G jest G -ekwiwariantnie izomorficzny z parą $(G/H, [\ell])$, w której $H \subset G$ jest pewną podgrupą, natomiast $[\ell]$ jest naturalnym działaniem indukowanym przez ℓ na zbiorze warstw,*

$$[\ell] : G \times (G/H) \longrightarrow G/H : (g, hH) \longmapsto (g \cdot h)H.$$

Dowolny zbiór z działaniem wolnym tejże grupy jest G -ekwiwariantnie izomorficzny z parą $(G \times S, \ell \times \text{id}_S)$, w której S jest pewnym zbiorem. Jeśli działanie G na zbiorze jest regularne, to wówczas zbiór ten jest G -ekwiwariantnie izomorficzny z parą (G, ℓ) .

■

Dowód: W pierwszym przypadku przechodność λ , którą można wysłowić zdaniem $X = G \triangleright x$, prawdziwym dla dowolnego $x \in X$, pozwala zastosować wprost Tw. 6.1, co prowadzi do oczywistego wyboru G -ekwiwariantnego izomorfizmu zbiorów z działaniem:

$$f_x : G/G_x \longrightarrow X : gG_x \longmapsto g \triangleright x.$$

Podgrupą, o której mowa w treści twierdzenia, jest zatem $H = G_x$.

W drugim przypadku, tj. dla działania wolnego λ , wybieramy (dowolnie) po jednym elemencie $y_{G \triangleright x} \in G \triangleright x$ z każdej z orbit $G \triangleright x$ działania G , na jakie rozwarstwia się X . Otrzymujemy w ten sposób zbiór

$$S_{X/G} := \{ y_{G \triangleright x} \mid G \triangleright x \in X/G \}.$$

Następnie odwzorowujemy zbiór $G \times S_{X/G}$ w X wedle przepisu

$$f_{S_{X/G}} : G \times S_{X/G} \longrightarrow X : (g, y_{G \triangleright x}) \longmapsto g \triangleright y_{G \triangleright x}.$$

I tym razem proponowane odwzorowanie jest jawnie surjektywne i G -ekwiwariantne jak w tezie twierdzenia, a przy tym injektywne, bowiem

$$f_{S_{X/G}}(g, y_{G \triangleright x}) = f_{S_{X/G}}(h, y_{G \triangleright z}) \iff g \triangleright y_{G \triangleright x} = h \triangleright y_{G \triangleright z}$$

$$\iff y_{G \triangleright z} = (h^{-1} \cdot g) \triangleright y_{G \triangleright x} \in G \triangleright y_{G \triangleright x},$$

co jednak oznacza – wobec definicji zbioru $S_{X/G}$ – koniunkcję równości

$$y_{G \triangleright z} = y_{G \triangleright x} \quad \wedge \quad h^{-1} \cdot g = e,$$

które pozwalają podsumować nasz rachunek jednym zdaniem:

$$f_{S_{X/G}}(g, y_{G \triangleright x}) = f_{S_{X/G}}(h, y_{G \triangleright z}) \iff (g, y_{G \triangleright x}) = (h, y_{G \triangleright z}).$$

Tak oto odwzorowanie $f_{S_{X/G}}$ zadaje pożądaną G -ekwiwariantny izomorfizm między $(G \times S_{X/G}, \ell \times \text{id}_{S_{X/G}})$ i (X, λ) .

Tezę dotyczącą działania regularnego otrzymujemy jako szczególny przypadek ostatniej konstrukcji. $\square$

* * *

Literatura uzupełniająca: Gładkie wprowadzenie do książki Romana w kontekście ostatnich wykładów daje podręcznik Armstronga [[Arm88](#)].

Grupa symetryczna jako model grupy ogólnej

Nasze studia dotychczasowe eksponują rolę grup symetrycznych w opisie działania grup dowolnych na zbiorach. Nadto sama już definicja grupy symetrycznej podpowiada naturalny, jawny opis jej realizacji, z którego w bezpośredni sposób możemy wywieść pełną wiedzę o strukturze grupy. Te obserwacje uzasadniają pytanie o to, które z grup mogą być traktowane jako grupy symetryczne i jako takie poddają się – przynajmniej w zasadzie – elementarnej analizie. Pełnej a w istocie swej dość banalnej odpowiedzi na to pytanie dostarcza

TWIERDZENIE 7.1 (Twierdzenie Cayleya). *Każda grupa jest izomorficzna z podgrupą grupy symetrycznej na pewnym zbiorze.* ■

Dowód: Przywołując Przykł. 28 (5), stwierdzamy istnienie homomorfizmu $\ell : G \longrightarrow \mathfrak{S}_G : g \longmapsto \ell_g$. Pozostaje upewnić się, że jest on iniektywny. Załóżmy, że $\ell_g = \text{id}_G$, a wtedy – w szczególności – $e = \text{id}_G(e) = \ell_g(e) = g \cdot e = g$, co oznacza, że $\text{Ker } \ell = \{e\}$. Na mocy Stw. 1 i 31 istnieje pożądaný izomorfizm $\ell : G \xrightarrow{\cong} \text{Im } \ell \subset \mathfrak{S}_G$. □

Powyższe skłania nas do dokładniejszego zbadania struktury grupy symetrycznej jako modelowej struktury grupowej.

7.1. Permutacje i orbity – szczegóły anatomii

Wprowadzamy

DEFINICJA 54. W notacji Przykł. 5 (1) **rzęd permutacji** $\sigma \in \mathfrak{S}_X$ elementów zbioru X , który oznaczamy symbolem $\text{ord}(\sigma)$, to najmniejsza z liczb naturalnych N o własności

$$\sigma^N = \text{id}_X$$

lub ∞ , jeśli liczba taka nie istnieje.

Nośnik permutacji σ to zbiór

$$\text{supp}(\sigma) := \{ x \in X \mid \sigma(x) \neq x \}.$$

▲

Zanim przejdziemy do zbadania nośnika permutacji w duchu rozważań z Rozdz. 6, wypowiemy użyteczne

STWIERDZENIE 58. *Permutacje o nośnikach rozłącznych są przemienne, czyli – w notacji Przykł. 5 (1) i 17 (5) oraz Def. 54 a dla dowolnych $\sigma_1, \sigma_2 \in \mathfrak{S}_X$ –*

zachodzi

$$\text{supp}(\sigma_1) \cap \text{supp}(\sigma_2) = \emptyset \implies [\sigma_1, \sigma_2] = \text{id}_X.$$

■

Dowód: Dokonajmy rozkładu X na podzbiory rozłączne:

$$X = \text{supp}(\sigma_1) \cup \text{supp}(\sigma_2) \cup \tilde{X},$$

gdzie $\tilde{X} := C_X(\text{supp}(\sigma_1) \cup \text{supp}(\sigma_2))$. Zauważmy, że każda ze składowych rozłącznych X jest zachowywana przez obie permutacje, tj.

$$\forall_{\alpha \in \{1,2\}} : \left(\sigma_\alpha(\text{supp}(\sigma_1)) = \text{supp}(\sigma_1) \wedge \sigma_\alpha(\text{supp}(\sigma_2)) = \text{supp}(\sigma_2) \wedge \sigma_\alpha(\tilde{X}) = \tilde{X} \right).$$

W przypadku $\tilde{X}$ jest to oczywistą konsekwencją tożsamości

$$(7.1) \quad \sigma_\alpha|_{\tilde{X}} = \text{id}_{\tilde{X}}$$

wynikającej z $\tilde{X} \cap \text{supp}(\sigma_\alpha) = \emptyset$. Załóżmy teraz, że dla $x \in \text{supp}(\sigma_1)$, spełniającego oczywistą tożsamość $\sigma_2(x) = x \in \text{supp}(\sigma_1)$, zachodzi $\sigma_1(x) = y \in \text{supp}(\sigma_2) \cup \tilde{X}$. Otrzymujemy na tej podstawie

$$x = \text{id}_X(x) = \sigma_1^{-1} \circ \sigma_1(x) = \sigma_1^{-1}(y) = \sigma_1^{-1} \circ \sigma_1(y) = \text{id}_X(y) = y \in \text{supp}(\sigma_2),$$

czyli sprzeczność. Podobnie wykazujemy zachowywanie nośnika σ_2 przez obie permutacje. Jest zatem $\sigma_1(x) = y \in \text{supp}(\sigma_1)$, a w takim razie

$$\sigma_1 \circ \sigma_2(x) = \sigma_1(x) = y = \sigma_2(y) = \sigma_2 \circ \sigma_1(x).$$

Analogicznie dowodzimy przemienności obu permutacji w przypadku $x \in \text{supp}(\sigma_2)$. Na koniec dla dowolnego $\tilde{x} \in \tilde{X}$ bez trudu pokazujemy

$$\sigma_1 \circ \sigma_2(\tilde{x}) = \sigma_1(\tilde{x}) = \tilde{x} = \sigma_2(\tilde{x}) = \sigma_2 \circ \sigma_1(\tilde{x}),$$

korzystając z równości (7.1). □

Charakterystykę nośnika permutacji zaczniemy od

STWIERDZENIE 59. W notacji Przykł. 5 (1) oraz Def. 54 a dla ustalonego elementu $x \in X$ zbioru skończonego X ciąg

$$y_n^{(x)} : \mathbb{N} \longrightarrow X : n \longmapsto y_n^{(x)} := \sigma^n(x), \quad \sigma^0 \equiv \text{id}_X$$

jest okresowy, tj. istnieje liczba naturalna $N_x \leq |X|$ o własności $\forall_{n \in \mathbb{N}} : y_{n+N_x}^{(x)} = y_n^{(x)}$. Zachodzi równość

$$\text{ord}(\sigma) = \text{NWW} \left\{ \min \{ N_x \in \overline{0, |X|} \mid \forall_{n \in \mathbb{N}} : y_{n+N_x}^{(x)} = y_n^{(x)} \} \mid x \in X \right\},$$

przy czym prawa strona jest najmniejszą wspólną wielokrotnością liczb $\min \{ N_x \in \overline{0, |X|} \mid \forall_{n \in \mathbb{N}} : y_{n+N_x}^{(x)} = y_n^{(x)} \}$.

Ponadto relacja na $X \ni x, y$ określona przez warunek

$$x \sim_\sigma y \iff \exists_{n \in \mathbb{N}} : y = \sigma^n(x)$$

jest relacją równoważności. ■

Dowód: Zaczniemy od okresowości ciągu $(y_n^{(x)})_{n \in \mathbb{N}}$. Skończoność X oznacza, że ciąg ten nie może być różnowartościowy, zatem $\exists_{(k, N_x) \in \mathbb{N} \times \mathbb{N}_{>0}} : y_{k+N_x}^{(x)} = y_k^{(x)}$. Skoro jednak $y_{k+N_x}^{(x)} = \sigma^k(y_{N_x}^{(x)})$, to otrzymujemy równość $\sigma^k(y_{N_x}^{(x)}) = \sigma^k(y_0^{(x)})$, która z racji różnowartościowości σ^k (będącej pochodną różnowartościowości σ) implikuje równość $y_{N_x}^{(x)} = y_0^{(x)}$, na tej zaś podstawie wnioskujemy, że

$$\forall n \in \mathbb{N} : y_{n+N_x}^{(x)} = \sigma^n(y_{N_x}^{(x)}) = \sigma^n(y_0^{(x)}) = y_n^{(x)},$$

co wyraża pożądaną własność. Formuła określająca $\text{ord}(\sigma)$ jest oczywista.

Przejdziemy teraz do dowodu zwrotności, symetrii i przechodniości $\sim_\sigma$. Pierwsza z nich jest oczywistą konsekwencją równości $x = \text{id}_X(x) = \sigma^0(x)$. Drugą wyprowadzamy z następującego rozumowania: niech $x \sim_\sigma y$, tj. $y = \sigma^n(x)$ dla pewnego $n \in \mathbb{N}$, przy czym z uwagi na N -okresowość ciągu $(x_n)_{n \in \mathbb{N}}$ możemy założyć, że $r := N - n \geq 0$, a wtedy $x = x_0 = x_N = x_{r+n} = \sigma^r(x_n) = \sigma^r(y)$, czyli ostatecznie $y \sim_\sigma x$. I wreszcie ilekroć $x \sim_\sigma y$ oraz $y \sim_\sigma z$, czyli $\exists_{m, n \in \mathbb{N}} : (y = \sigma^m(x) \wedge z = \sigma^n(y))$, wówczas $z = \sigma^n \circ \sigma^m(x) = \sigma^{m+n}(x)$, co oznacza właśnie, że $x \sim_\sigma z$. $\square$

Wprowadzamy

DEFINICJA 55. W notacji Przykł. 5 (1) oraz Stw. 59 σ -orbita elementu $x \in X$ to jego klasa równoważności $[x]_{\sim_\sigma}$ względem relacji $\sim_\sigma$. ▲

Wprost ze Stw. 59 dedukujemy

COROLLARIUM 7. W notacji Przykł. 5 (1) i Def. 55 a dla dowolnych $\sigma \in \mathfrak{S}_X$ oraz $x \in X$ odnośna σ -orbita ma postać

$$[x]_{\sim_\sigma} = \{x, \sigma(x), \sigma^2(x), \dots, \sigma^{L-1}(x)\}.$$

dla pewnej liczby $L \in \mathbb{N}$. Przy tym $\sigma(\sigma^{L-1}(x)) = x$. Dowolne dwie takie σ -orbity albo się pokrywają, albo są rozłączne.

Ponadto dowolny podzbiór $Y \subset X$ jest niezmienniczy względem σ wtedy i tylko wtedy, gdy Y jest sumą mnogościową pewnej liczby σ -orbit. ■

Nasze wnioski dotyczące struktury σ -orbity podpowiadają poniższą

DEFINICJA 56. W notacji Przykł. 5 (1) **cykl o długości L** na zbiorze X to permutacja $\gamma \in \mathfrak{S}_X$ o własności $\gamma^L = \text{id}_X$ oraz nośniku

$$\text{supp}(\gamma) := \{x_k := \gamma^k(x)\}_{k \in \overline{0, L-1}}$$

będącym pojedynczą orbitą o mocy L . Cykl tej postaci zapisujemy jako

$$(x_0 \ x_1 \ x_2 \ \dots \ x_{L-1}) \equiv (x_1 \ x_2 \ \dots \ x_{L-1} \ x_0) \equiv (x_2 \ x_3 \ \dots \ x_{L-1} \ x_0 \ x_1) = \dots$$
▲

O pierwszoplanowej roli wprowadzonego tu pojęcia przekonuje nas

TWIERDZENIE 7.2 (O rozkładzie permutacji na cykle rozłączne). *Dowolną permutację elementów zbioru skończonego można przedstawić jako złożenie cykli o nośnikach rozłącznych, przy czym rozkład taki jest jednoznaczny z dokładnością do kolejności cykli.*

■

Dowód: Niechaj

$$(7.2) \quad \text{supp}(\sigma) = \bigcup_{k=1}^n X_k \subset X$$

będzie rozkładem nośnika $\sigma \in \mathfrak{S}_X$ na sumę rozłączną σ -orbit X_k . Dla dowolnego $k \in \overline{1, n}$ możemy określić odwzorowania

$$\gamma_k(x) := \begin{cases} \sigma(x) & \text{dla } x \in X_k \\ x & \text{dla } x \in X \setminus X_k \end{cases} ,$$

tak że $X_k = \text{supp}(\gamma_k)$, a przy tym $\forall_{k, l \in \overline{1, n}}^{k \neq l} : X_k \cap X_l = \emptyset$. Jak wynika wprost z konstrukcji (oraz z Cor. 7), $\{\gamma_k\}_{k \in \overline{1, n}}$ jest wówczas rodziną cykli o nośnikach wzajemnie rozłącznych, które spełniają oczekiwaną tożsamość

$$\sigma = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_n ,$$

co kończy konstruktywny dowód istnienia rozkładu. Pozostaje zatem przekonać się o jego jednoznaczności.

Niech teraz

$$\sigma = \tilde{\gamma}_1 \circ \tilde{\gamma}_2 \circ \cdots \circ \tilde{\gamma}_{\tilde{n}}$$

będzie dowolnym takim rozkładem σ , przy czym zakładamy, że w rodzinie $\{\tilde{\gamma}_l\}_{l \in \overline{1, \tilde{n}}}$ nie ma cykli o nośnikach pustych. Otrzymujemy wtedy rozkład

$$(7.3) \quad \text{supp}(\sigma) = \bigcup_{l=1}^{\tilde{n}} \tilde{X}_l$$

na rozłączne podzbiory $\tilde{X}_l := \text{supp}(\tilde{\gamma}_l) \neq \emptyset$. Te ostatnie są pojedynczymi σ -orbitami, na których $\sigma|_{\tilde{X}_l} = \tilde{\gamma}_l|_{\tilde{X}_l}$, wobec czego (na mocy Cor. 7) rozkład (7.3) musi się pokrywać z rozkładem (7.2), tj. $\tilde{n} = n$ i istnieje $\varrho \in \mathfrak{S}_n$ o własności

$$\forall_{l \in \overline{1, n}} : \tilde{X}_l = X_{\varrho(l)} .$$

Ponieważ jest też

$$\tilde{\gamma}_l|_{\tilde{X}_l} = \sigma|_{\tilde{X}_l} \equiv \sigma|_{X_{\varrho(l)}} = \gamma_{\varrho(l)}|_{X_{\varrho(l)}} \equiv \gamma_{\varrho(l)}|_{\tilde{X}_l}$$

oraz

$$\tilde{\gamma}_l|_{X \setminus \tilde{X}_l} = \text{id}_{X \setminus \tilde{X}_l} \equiv \text{id}_{X \setminus X_{\varrho(l)}} = \gamma_{\varrho(l)}|_{X \setminus X_{\varrho(l)}} \equiv \gamma_{\varrho(l)}|_{X \setminus \tilde{X}_l} ,$$

przeto

$$\forall_{l \in \overline{1, n}} : \tilde{\gamma}_l = \gamma_{\varrho(l)} ,$$

co dowodzi rzeczonyj jedności rozkładu. □

Ostatni wynik uzasadnia wprowadzenie

DEFINICJA 57. Przyjmijmy notację Przykł. 5 (1), Def. 54 i 56 oraz Tw. 7.2. Niechaj

$$\sigma = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_m , \quad m \in \mathbb{N}$$

będzie rozkładem permutacji $\sigma \in \mathfrak{S}_X$ elementów zbioru skończonego X na cykle γ_i o niepustych nośnikach rozłącznych i o długości L_i i oznaczmy

$$N := \max_{i \in \overline{1, n}} \{L_i, 1\}.$$

Typ permutacji σ to N -tka liczb naturalnych

$$\text{typ}(\sigma) := (n_1, n_2, \dots, n_N)$$

w której n_j o indeksie $j > 1$ jest liczbą cykli o długości j w rozkładzie, natomiast $n_1 := |\text{C}_X \text{supp}(\sigma)|$.

▲

Przed przystąpieniem do dalszej analizy, wprowadzimy wygodny zapis permutacji. W praktyce będziemy najczęściej rozpatrywać permutacje zbioru skończonego X , o elementach $x_i \in X$ ponumerowanych liczbami naturalnymi ze zbioru $\overline{1, |X|} \ni i$. Ustanawiamy dla nich

NOTACJA 6. Zapis

$$\sigma \equiv \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 & x_9 & x_{10} \\ x_7 & x_3 & x_1 & x_5 & x_2 & x_6 & x_4 & x_{10} & x_8 & x_9 \end{pmatrix}$$

przedstawia permutację $\sigma \in \mathfrak{S}_X$ zbioru 10-elementowego $X \ni x_i$, która elementowi x_i o indeksie $i \in \overline{1, 10}$ z wiersza górnego przyporządkowuje element z wiersza dolnego leżący bezpośrednio pod nim, czyli $\sigma : x_1 \mapsto x_7, x_2 \mapsto x_3, x_3 \mapsto x_1, x_4 \mapsto x_5, x_5 \mapsto x_2, x_6 \mapsto x_6, x_7 \mapsto x_4, x_8 \mapsto x_{10}, x_9 \mapsto x_8, x_{10} \mapsto x_9$.

Innym sposobem zapisania tej samej permutacji, odwołującym się wprost do tezy Tw. 7.2, jest rozkład na cykle o niepustych nośnikach wzajem rozłącznych

$$\sigma = (x_1 x_7 x_4 x_5 x_2 x_3)(x_8 x_{10} x_9),$$

w którym opuszczamy znak złożenia cykli. Znak ten będziemy również opuszczać w zapisie permutacji jako superpozycji dowolnych cykli, także z uwzględnieniem cykli trywialnych typu (x_6) (jednoelementowych).

* * *

Możemy już teraz określić bezpośredni związek pomiędzy typem permutacji a jej przynależnością do ustalonej orbity działania dołączonego grupy symetrycznej na sobie.

STWIERDZENIE 60. *Typ permutacji elementów zbioru skończonego jest stały na klasach sprzężoności i różny dla różnych klas sprzężoności w grupie symetrycznej na tymże zbiorze.*

■

Dowód: Niechaj σ i ϱ będą dwiema permutacjami elementów X i niech

$$\sigma := \gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_n, \quad n \in \mathbb{N}$$

będzie rozkładem σ na cykle γ_i o niepustych nośnikach wzajem rozłącznych i o długościach L_i , o którym mówi Tw. 7.2. Oznaczmy

$$s_i := \sum_{j=0}^i L_j,$$

wprowadzając dla wygody zapisu dodatkowe oznaczenie

$$L_0 := 0.$$

Wypiszmy dalej poszczególne cykle rozkładu w jawnej postaci,

$$\gamma_i := (x_{s_{i-1}+1} x_{s_{i-1}+2} \dots x_{s_i}),$$

a następnie uzupełnijmy podzbiór

$$\bigcup_{k=1}^n \text{supp}(\gamma_k) = \{x_1, x_2, \dots, x_{s_n}\}$$

o punkty (parami różne) $x_{s_n+j} \in \mathbb{C}_X \text{supp}(\sigma)$, $j \in \overline{1, N}$, $N := |\mathbb{C}_X \text{supp}(\sigma)|$, przepisując zarazem σ w równoważnej postaci

$$\begin{aligned} \sigma &\equiv (x_1 x_2 \dots x_{s_1})(x_{s_1+1} x_{s_1+2} \dots x_{s_2}) \dots (x_{s_{n-1}+1} x_{s_{n-1}+2} \dots x_{s_n})(x_{s_n+1})(x_{s_n+2}) \\ (7.4) \quad &\dots (x_{s_n+N}). \end{aligned}$$

Na potrzeby niniejszego rozumowania wprowadzimy specjalne określenie na rozkłady tego rodzaju – będziemy je mianowicie nazywać **kompletnymi rozkładami na cykle rozłączne**. Załóżmy dalej, że $\varrho \in C(\sigma) \subset \mathfrak{S}_X$, czyli że istnieje permutacja $\xi \in \mathfrak{S}_X$ spełniająca relację

$$\varrho = \xi \circ \sigma \circ \xi^{-1},$$

którą możemy zapisać jako

$$\begin{aligned} \varrho &= \xi \circ (x_1 x_2 \dots x_{s_1}) \circ \xi^{-1} \circ \xi \circ (x_{s_1+1} x_{s_1+2} \dots x_{s_2}) \circ \xi^{-1} \circ \dots \circ \xi \\ &\quad \circ (x_{s_{n-1}+1} x_{s_{n-1}+2} \dots x_{s_n}) \circ \xi^{-1} \circ \xi \circ (x_{s_n+1}) \circ \xi^{-1} \circ \xi \circ (x_{s_n+2}) \circ \xi^{-1} \circ \dots \circ \xi \\ &\quad \circ (x_{s_n+N}) \circ \xi^{-1}. \end{aligned}$$

Permutację ξ możemy zawsze przepisać jako

$$\xi = \begin{pmatrix} x_1 & x_2 & \dots & x_{s_n+N} \\ x_{\widehat{\xi}(1)} & x_{\widehat{\xi}(2)} & \dots & x_{\widehat{\xi}(s_n+N)} \end{pmatrix}$$

dla pewnej permutacji $\widehat{\xi} \in \mathfrak{S}_{|X|}$, a wtedy

$$\xi^{-1} = \begin{pmatrix} x_{\widehat{\xi}(1)} & x_{\widehat{\xi}(2)} & \dots & x_{\widehat{\xi}(s_n+N)} \\ x_1 & x_2 & \dots & x_{s_n+N} \end{pmatrix}$$

i z łatwością przekonujemy się o prawdziwości formuł

$$\xi \circ \gamma_i \circ \xi^{-1} = (x_{\widehat{\xi}(s_{i-1}+1)} x_{\widehat{\xi}(s_{i-1}+2)} \dots x_{\widehat{\xi}(s_i)}), \quad i \in \overline{1, n}$$

oraz

$$\xi \circ (x_{s_n+j}) \circ \xi^{-1} = (x_{\widehat{\xi}(s_n+j)}), \quad j \in \overline{1, N},$$

z których wynika wprost pierwsza część tezy.

Dowód implikacji odwrotnej przebiega podobnie. Niech σ ma opisaną powyżej postać i niech ϱ będzie permutacją tego samego typu, o rozkładzie

$$\begin{aligned} \varrho &= (y_1 y_2 \dots y_{s_1})(y_{s_1+1} y_{s_1+2} \dots y_{s_2}) \dots (y_{s_{n-1}+1} y_{s_{n-1}+2} \dots y_{s_n})(y_{s_n+1})(y_{s_n+2}) \\ &\quad \dots (y_{s_n+N}), \end{aligned}$$

przy czym wprost z konstrukcji wynikają równości $y_k = x_{\widehat{\zeta}(k)}$, $k \in \overline{1, s_n + N}$ spełnione dla pewnej permutacji $\widehat{\zeta} \in \mathfrak{S}_{|X|}$. Indukowana przez tę ostatnią permutacja elementów X ,

$$\zeta := \begin{pmatrix} x_1 & x_2 & \cdots & x_{s_n+N} \\ x_{\widehat{\zeta}(1)} & x_{\widehat{\zeta}(2)} & \cdots & x_{\widehat{\zeta}(s_n+N)} \end{pmatrix} \equiv \begin{pmatrix} x_1 & x_2 & \cdots & x_{s_n+N} \\ y_1 & y_2 & \cdots & y_{s_n+N} \end{pmatrix},$$

zadaje poszukiwane sprzężenie,

$$\varrho = \zeta \circ \sigma \circ \zeta^{-1}.$$

□

Łącząc tezy Stw. 58 i Tw. 7.2 otrzymujemy

COROLLARIUM 8. *W notacji Przykł. 5 (1) oraz Def. 54 a dla dowolnej permutacji $\sigma \in \mathfrak{S}_X$ o rozkładzie*

$$\sigma = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_n, \quad n \in \mathbb{N}$$

na cykle γ_i o nośnikach rozłącznych o długości L_i zachodzi równość

$$\text{ord}(\sigma) = \text{NWW}(L_1, L_2, \dots, L_n).$$

■

Dowód: Wystarczy zauważyć, że rząd cyklu jest równy jego długości. □

Innym prostym a użytecznym wnioskiem z udowodnionego Tw. 7.2 jest

COROLLARIUM 9. *Dowolną permutację elementów zbioru skończonego można przedstawić jako złożenie pewnej liczby transpozycji, czyli cykli o długości 2.*

■

Dowód: Stwierdzenie to zostało zapowiedziane w Przykł. 16 (1). W świetle Tw. 7.2 należy jedynie wykazać, że dowolny cykl ma rozkład na transpozycje. Istotnie, łatwo stwierdzamy równość

$$(x_0 x_1 x_2 \dots x_{L-1}) = (x_0 x_1)(x_1 x_2) \cdots (x_{L-2} x_{L-1}).$$

□

Stąd już tylko krok do

STWIERDZENIE 61. *W notacji Przykł. 16 (1) grupa symetryczna $\mathfrak{S}_n$ na zbiorze $\overline{1, n}$ jest generowana przez każdy z poniższych zbiorów transpozycji:*

- (i) $\{ (1 i) \mid i \in \overline{2, n} \};$
- (ii) $\{ (i i+1) \mid i \in \overline{1, n-1} \}.$ Permutacje te określamy mianem **transpozycji prostych**.

■

Dowód:

Ad (i) Wystarczy zauważyć, że dla dowolnych $i, j \in \overline{2, n}$, $j \neq i$ zachodzi

$$(ij) = (1j)(1i)(1j),$$

reszta wynika bezpośrednio z Cor. 9.

Ad (ii) Niechaj $H \subset \mathfrak{S}_n$ będzie podgrupą generowaną przez transpozycje liczb sąsiednich,

$$H = \langle (12), (23), \dots, (n-1n) \rangle.$$

Zauważmy, że $(12) \in H$, a nadto, dla dowolnego $k \in \overline{2, n-1}$,

$$(1k) \in H \implies (1k+1) = (kk+1)(1k)(kk+1) \in H,$$

zatem teza wynika wprost z punktu (i). □

7.2. Grupa symetryczna w terminach generatorów i relacji

Treść udowodnionego stwierdzenia wskazuje na logiczną alternatywę dla dokonanego przez nas na wstępie wyboru sposobu określenia struktury algebraicznej grupy symetrycznej. Dotychczasowy jej opis odwoływał się wprost do istnienia nośnika działania grupy, a więc *de facto* był opisem *realizacji* grupy $\mathfrak{S}_X$ na zbiorze X , w którym elementy grupy $\mathfrak{S}_X$ są utożsamiane z konkretnymi wyznaczanymi przez nie (jako odwzorowania bijektywne) relacjami na zbiorze X , mnożenie grupowe zaś – ze składaniem takich relacji. Ten schemat myślenia o grupie symetrycznej wynika bezpośrednio z samej jej definicji, nie jest jednak bynajmniej sposobem jedynym. Przywołując Def. 33, możemy na podstawie Stw. 61 pokusić się o zadanie struktury algebraicznej na $\mathfrak{S}_X$ w terminach listy generatorów i zupełnego zestawu spełnianych przez nie relacji, w oderwaniu od „anatomii” ich działania na X . Zaczniemy od ustalenia relacji spełnianych przez transpozycje proste.

STWIERDZENIE 62. W notacji Przykł. 16 (1) i Stw. 61 generatory

$$\tau_i := (ii+1), \quad i \in \overline{1, n-1}$$

grupy symetrycznej $\mathfrak{S}_n$ spełniają następujące relacje, wypisane dla dowolnych indeksów $i, j \in \overline{1, n-1}$,

$$\begin{aligned} \tau_i^2 &= \text{id}_X, \\ (7.5) \quad |i-j| = 1 &\implies (\tau_i \circ \tau_j)^3 = \text{id}_X, \\ |i-j| \geq 2 &\implies (\tau_i \circ \tau_j)^2 = \text{id}_X. \end{aligned}$$

■

Dowód: Relacje z pierwszej linii wynikają z inwolutywności transpozycji, te z ostatniej zaś – ze Stw. 58. Pozostaje sprawdzić relacje z linii środkowej. Wobec ich niezmienniczości względem zamiany indeksów i, j możemy przyjąć $j = i+1$, a wtedy

$$\begin{aligned} (\tau_i \circ \tau_j)^3 &\equiv ((ii+1)(i+1i+2))^3 = (ii+1i+2)^3 = (ii+1i+2)(ii+2i+1) \\ &= \text{id}_X. \end{aligned}$$

□

Uważny Czytelnik natychmiast skojarzy powyższe relacje z relacjami spełnianymi przez generatory grupy warkoczowej z Przykł. 15 (5) i bez trudu zinterpretuje opuszczenie relacji z pierwszej linii przy przejściu do $\mathfrak{B}_n$.

O zupełności wypisanego zestawu relacji zaświadcza

TWIERDZENIE 7.3 (Grupa symetryczna w terminach generatorów i relacji). *Przyjmijmy notację Def. 32 i 35, Przykł. 16 (1) oraz Stw. 61. 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 $i, j \in \overline{1, n-1}$,

$$g_i^2 = e,$$

$$(7.6) \quad |i - j| = 1 \implies (g_i \cdot g_j)^3 = e,$$

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

Wówczas istnieje jedyny homomorfizm grup

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

o własności

$$(7.7) \quad \forall_{i \in \overline{1, n-1}} : \chi(g_i) = \tau_i.$$

Homomorfizm ten jest izomorfizmem.

■

Dowód: Każdy element G_n można zapisać jako iloczyn generatorów g_i , postulujemy zatem, dla dowolnego $g \in G_n$ o rozkładzie

$$(7.8) \quad g = g_{i_1} \cdot g_{i_2} \cdot \dots \cdot g_{i_N},$$

zadawanym przez pewną rodzinę $\{i_k\}_{k \in \overline{1, N}}$, $N \in \mathbb{N}$ indeksów $i_k \in \overline{1, n-1}$ ($N = 0$ oznacza, że $g = e$), co następuje:

$$(7.9) \quad \chi(g) := \tau_{i_1} \circ \tau_{i_2} \circ \dots \circ \tau_{i_N}.$$

Odwzorowanie to jest dobrze określone, jeśli bowiem

$$g = g_{i_1} \cdot g_{i_2} \cdot \dots \cdot g_{i_{\tilde{N}}}$$

jest dowolnym innym rozkładem¹ g , to musi istnieć sekwencja operacji algebraicznych wykorzystujących *wyłącznie* układ (7.6) relacji między generatorami g_i (wszak układ ten jest *zupełny*), która przeprowadza pierwszy rozkład na drugi, a

¹Przykładem niejednoznaczności rozkładu jest równość $g_1 \cdot g_2 \cdot g_3 = g_3 \cdot g_2 \cdot g_1 \cdot g_2 \cdot g_3 \cdot g_1 \cdot g_2$, wynikająca z przejścia $g_3 \cdot g_2 \cdot g_1 \cdot g_2 \cdot g_3 \cdot g_1 \cdot g_2 = g_3 \cdot g_2 \cdot g_1 \cdot g_2 \cdot (g_2 \cdot g_1) \cdot (g_2 \cdot g_1) \cdot (g_2 \cdot g_1) \cdot g_3 \cdot g_1 \cdot (g_1 \cdot g_3) \cdot (g_1 \cdot g_3) \cdot g_2 = g_3 \cdot g_2 \cdot g_1 \cdot g_2^2 \cdot g_1 \cdot g_2 \cdot g_1 \cdot g_2 \cdot g_1 \cdot g_3 \cdot g_1^2 \cdot g_3 \cdot g_1 \cdot g_3 \cdot g_2 = g_3 \cdot g_2 \cdot g_1^2 \cdot g_2 \cdot g_1 \cdot g_2 \cdot g_1 \cdot g_2 \cdot g_3 \cdot g_2 = g_3 \cdot g_2^2 \cdot g_1 \cdot g_2 \cdot g_1^2 \cdot g_3 \cdot g_2 = g_3 \cdot g_1 \cdot g_2 \cdot g_3 \cdot g_2 = g_3 \cdot g_1 \cdot g_2 \cdot g_3 \cdot g_2 \cdot (g_2 \cdot g_3) \cdot (g_2 \cdot g_3) \cdot (g_2 \cdot g_3) \equiv g_3 \cdot g_1 \cdot g_2 \cdot g_3 \cdot g_2^2 \cdot g_3 \cdot g_2 \cdot g_3 \cdot g_2 \cdot g_3 = g_3 \cdot g_1 \cdot g_2 \cdot g_3^2 \cdot g_2 \cdot g_3 \cdot g_2 \cdot g_3 = g_3 \cdot g_1 \cdot g_2^2 \cdot g_3 \cdot g_2 \cdot g_3 = g_3 \cdot g_1 \cdot g_3 \cdot (g_1 \cdot g_1) \cdot g_2 \cdot g_3 \equiv (g_3 \cdot g_1)^2 \cdot g_1 \cdot g_2 \cdot g_3 = g_1 \cdot g_2 \cdot g_3$.

wówczas – wobec (symbolicznej) tożsamości $\chi(7.6)=(7.5)$ – sekwencja obrazów tych samych operacji algebraicznych względem odwzorowania χ przeprowadza permutację zapisaną po prawej stronie (7.9) w

$$\chi(g_{\tilde{i}_1} \cdot g_{\tilde{i}_2} \cdots g_{\tilde{i}_N}) = \tau_{\tilde{i}_1} \cdot \tau_{\tilde{i}_2} \cdots \tau_{\tilde{i}_N},$$

ustalając tym samym równość tych permutacji.

Łatwo przekonujemy się, że χ jest homomorfizmem grup. Istotnie, iloczyn dowolnych dwóch elementów $g^{(\alpha)} \in G_n$, $\alpha \in \{1, 2\}$ o rozkładach, odpowiednio, $g^{(\alpha)} = g_{i_1^{(\alpha)}} \cdot g_{i_2^{(\alpha)}} \cdots g_{i_{N(\alpha)}^{(\alpha)}}$, można zawsze sprowadzić do postaci $g_{i_1^{(1)}} \cdot g_{i_2^{(1)}} \cdots g_{i_{N(1)}^{(1)}} \cdot g_{i_1^{(2)}} \cdot g_{i_2^{(2)}} \cdots g_{i_{N(2)}^{(2)}}$ poprzez pewną sekwencję operacji algebraicznych wykorzystujących (wyłącznie) relacje (7.6), a w takim razie – na mocy wcześniejszego rozumowania – uzyskujemy pożądaną równość

$$\chi(g^{(1)} \cdot g^{(2)}) = \tau_{i_1^{(1)}} \circ \tau_{i_2^{(1)}} \circ \cdots \circ \tau_{i_{N(1)}^{(1)}} \circ \tau_{i_1^{(2)}} \circ \tau_{i_2^{(2)}} \circ \cdots \circ \tau_{i_{N(2)}^{(2)}} = \chi(g^{(1)}) \circ \chi(g^{(2)}).$$

Jeśli teraz $\tilde{\chi}$ jest dowolnym innym homomorfizmem spełniającym warunki $\forall_{i \in \overline{1, n-1}} : \tilde{\chi}(g_i) = \tau_i$, to zachodzi równość

$$\tilde{\chi}(g) = \tilde{\chi}(g_{i_1}) \circ \tilde{\chi}(g_{i_2}) \circ \cdots \circ \tilde{\chi}(g_{i_N}) = \tau_{i_1} \circ \tau_{i_2} \circ \cdots \circ \tau_{i_N} = \chi(g),$$

która dowodzi jedyności χ .

Pozostaje wykazać, że χ jest bijekcją. Zważywszy, że podgrupa $\chi(G_n)$ zawiera wszystkie generatory $\mathfrak{S}_n$, zachodzi relacja $\chi(G_n) = \mathfrak{S}_n$, a stąd nierówność

$$|G_n| \geq |\mathfrak{S}_n| = n!.$$

Dla zakończenia dowodu wyprowadzimy nierówność przeciwną stosując indukcję względem n . Nierówność

$$|G_1| \leq |\mathfrak{S}_1|$$

jest trywialnie spełniona, załóżmy zatem, że także

$$|G_{n-1}| \leq |\mathfrak{S}_{n-1}|,$$

czyli $G_{n-1} \cong \mathfrak{S}_{n-1}$. Grupę G_{n-1} możemy przy tym wybrać jako podgrupę G_n postaci

$$G_{n-1} := \langle g_2, g_3, \dots, g_{n-1} \rangle \subset G_n.$$

Uwzględniwszy Cor. 4 (oraz założenie indukcyjne), przepisemy tezę indukcyjną w postaci

$$\begin{aligned} (G_n : G_{n-1}) &\equiv \frac{1}{(n-1)!} |\mathfrak{S}_{n-1}| \cdot (G_n : G_{n-1}) = \frac{1}{(n-1)!} |G_{n-1}| \cdot (G_n : G_{n-1}) \\ &= \frac{1}{(n-1)!} |G_n| \leq \frac{1}{(n-1)!} |\mathfrak{S}_n| = n. \end{aligned}$$

Ażeby oszacować liczbę warstw (prawostronnych) względem G_{n-1} w G_n , zbadajmy zachowanie ich rodziny

$$\mathcal{H} := \{H_i\}_{i \in \overline{1, n}}$$

złożonej z warstw szczególnego rodzaju:

$$H_1 := G_{n-1}, \quad H_2 := H_1 g_1, \quad H_3 := H_2 g_2, \quad \dots, \quad H_n := H_{n-1} g_{n-1}$$

względem (indukowanego) działania prawostronnego grupy G_n , które jest jednoznacznie określone przez działanie generatorów. Wprost z definicji dostajemy

$$\forall_{i \in \overline{1, n-1}} : \left(H_i g_i = H_{i+1} \in \mathcal{R} \wedge H_{i+1} g_i = H_i g_i^2 = H_i \in \mathcal{R} \right).$$

Rozważmy teraz warstwy $H_j g_i$ dla $j \notin \{i, i+1\}$. Mamy oczywistą równość

$$\forall_{i \in \overline{2, n-1}} : H_1 g_i = H_1 \in \mathcal{R}.$$

Przechodzimy zatem do przypadku $j > 1$, w którym możemy zapisać

$$H_j = H_1 h_j, \quad h_j := g_1 \cdot g_2 \cdot \dots \cdot g_{j-1}.$$

Zauważmy, że ilekroć $i \geq j+1 (> 2)$, wówczas

$$h_j \cdot g_i = g_i \cdot h_j,$$

czyli też

$$H_j g_i = (H_1 g_i) h_j = H_1 h_j = H_j \in \mathcal{R},$$

gdy natomiast $j-1 > i \geq 1$, to

$$\begin{aligned} h_j \cdot g_i &= h_i \cdot g_i \cdot g_{i+1} \cdot (g_{i+2} \cdot g_{i+3} \cdot \dots \cdot g_{j-1}) \cdot g_i = h_i \cdot (g_i \cdot g_{i+1} \cdot g_i) \\ &\quad \cdot (g_{i+2} \cdot g_{i+3} \cdot \dots \cdot g_{j-1}) = h_i \cdot (g_{i+1} \cdot g_i \cdot g_{i+1}) \cdot (g_{i+2} \cdot g_{i+3} \cdot \dots \cdot g_{j-1}) \\ &= g_{i+1} \cdot h_i \cdot g_i \cdot g_{i+1} \cdot (g_{i+2} \cdot g_{i+3} \cdot \dots \cdot g_{j-1}) = g_{i+1} \cdot h_j, \end{aligned}$$

czyli też

$$H_j g_i = (H_1 g_{i+1}) h_j = H_1 h_j = H_j \in \mathcal{R}.$$

Ostatecznie więc stwierdzamy, że rodzina $\mathcal{R}$ jest zachowywana przez zbiór generatorów G_n ,

$$\forall_{\substack{i \in \overline{1, n-1} \\ j \in \overline{1, n}}} : H_j g_i \in \mathcal{R},$$

a zatem przez całą grupę,

$$\forall_{\substack{j \in \overline{1, n} \\ g \in G_n}} : H_j g \in \mathcal{R}.$$

W szczególności

$$\forall_{g \in G_n} : G_{n-1} g \equiv H_1 g \in \mathcal{R},$$

co pokazuje, że

$$G_n/G_{n-1} = \{H_1, H_2, \dots, H_n\} \implies |G_n/G_{n-1}| \leq n.$$

□

7.3. Parzystość permutacji

Godzi się podkreślić, że w odróżnieniu od poprzednio dyskutowanego rozkładu na cykle *rozłączne* rozkład na transpozycje (na które nie możemy w ogólności narzucić ograniczającego założenia o rozłączności nośników) jest wysoce niejednoznaczny. Jako przykład podamy

$$\begin{aligned} (12)(23)(12) &= (12)(23)(12)(23)(23) = (13) = (12)(13)(23) \\ &= (13)(12)(13)(23)(13). \end{aligned}$$

Ostatnia obserwacja staje się źródłem pytania o istnienie niezmiennika rozkładu permutacji na transpozycje. Takim niezmiennikiem okazuje się być parzystość liczby czynników rozkładu.

TWIERDZENIE 7.4 (O parzystości permutacji). *W notacji Przykł. 16 (1) i dla permutacji $\sigma \in \mathfrak{S}_X$ elementów zbioru skończonego X o dwóch rozkładach*

$$\tau_1 \circ \tau_2 \circ \dots \circ \tau_m = \sigma = \tilde{\tau}_1 \circ \tilde{\tau}_2 \circ \dots \circ \tilde{\tau}_n$$

na transpozycje $\{\tau_i\}_{i \in \overline{1,m}}$ i $\{\tilde{\tau}_j\}_{j \in \overline{1,n}}$ zachodzi

$$(-1)^m = (-1)^n.$$

■

Dowód: Podstawę dowodu stanowi

LEMAT 7.5. *Przyjmijmy notację Przykł. 16 (1) oraz Stw. 59 i dla dowolnej permutacji $\sigma \in \mathfrak{S}_X$ zbioru skończonego X oznaczmy przez $\mathcal{N}(\sigma)$ liczbę σ -orbit w X . Niech też $\tau_{x,y} \equiv (x y) \in \mathfrak{S}_X$ będzie transpozycją pewnych elementów $x, y \in X$, a wtedy*

$$\mathcal{N}(\tau_{x,y} \circ \sigma) - \mathcal{N}(\sigma) = \begin{cases} -1 & \text{dla } x \not\sim_{\sigma} y \\ +1 & \text{dla } x \sim_{\sigma} y \end{cases}.$$

■

Dowód: Niech $\sigma = \gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_n$ będzie kompletnym rozkładem σ na cykle rozłączne (uwzględniającym trywialne cykle jednoelementowe odpowiadające punktom stałym σ), jak w (7.4). Zważywszy, że każdy z podzbiorów $\{x_{s_{i-1}+1}, x_{s_{i-1}+2}, \dots, x_{s_i}\}$ występujących w definicji cyklu γ_i jest σ -orbitą oraz że ich suma mnogościowa zadaje rozkład zbioru X , stwierdzamy

$$\mathcal{N}(\sigma) = n.$$

Rozpatrzmy teraz po kolei oba przypadki. Niech najpierw $x \not\sim_{\sigma} y$, co oznacza, że każdy z elementów x, y należy do zbioru definiującego inny cykl rozkładu, np. (bez straty ogólności wobec przemienności cykli)

$$\gamma_1 = (x_1 \equiv x x_2 \dots x_{L_1}), \quad \gamma_2 = (x_{L_1+1} \equiv y x_{L_1+2} \dots x_{L_1+L_2}).$$

Dostajemy wówczas

$$\begin{aligned} \tau_{x,y} \circ \gamma_1 \circ \gamma_2 &\equiv (x_1 x_{L_1+1})(x_1 x_2 \dots x_{L_1})(x_{L_1+1} x_{L_1+2} \dots x_{L_1+L_2}) \\ &= (x_1 x_2 \dots x_{L_1} x_{L_1+1} x_{L_1+2} \dots x_{L_1+L_2}), \end{aligned}$$

i jasnym jest, że wskutek takiej konkatenacji liczba cykli w rozkładzie $\tau_{x,y} \circ \sigma$ jest mniejsza o jeden od $\mathcal{N}(\sigma)$.

Jeśli teraz $x \sim_\sigma y$, to x i y należą do zbioru definiującego pojedynczy cykl, np.

$$\gamma_1 = (x_1 \equiv x \ x_2 \ \dots \ x_m \ x_{m+1} \equiv y \ x_{m+2} \ \dots \ x_{L_1}).$$

Tym razem wyznaczamy

$$\begin{aligned} \tau_{x,y} \circ \gamma_1 &= (x_1 \ x_{m+1})(x_1 \ x_2 \ \dots \ x_m \ x_{m+1} \ x_{m+2} \ \dots \ x_{L_1}) \\ &= (x_1 \ x_2 \ \dots \ x_m)(x_{m+1} \ x_{m+2} \ \dots \ x_{L_1}), \end{aligned}$$

więc liczba cykli w rozkładzie przyrasta o jeden w efekcie opisanego rozklejenia cyklu zawierającego oba elementy x, y . $\square$

Na mocy lematu zachodzi równość

$$\begin{aligned} \mathcal{N}(\sigma) &= \mathcal{N}(\tau_1 \circ \tau_2 \circ \dots \circ \tau_m) = \varepsilon_1 + \mathcal{N}(\tau_2 \circ \tau_3 \circ \dots \circ \tau_m) \\ &= \varepsilon_1 + \varepsilon_2 + \mathcal{N}(\tau_3 \circ \tau_4 \circ \dots \circ \tau_m) = \dots = \sum_{k=1}^m \varepsilon_k + \mathcal{N}(\text{id}_X) \end{aligned}$$

dla pewnych liczb $\varepsilon_k \in \{-1, 1\}$, $k \in \overline{1, m}$, a ponadto $\mathcal{N}(\text{id}_X) = |X|$, gdyż id_X -orbitami są zbiory jednoelementowe zawierające poszczególne elementy X . Biorąc pod uwagę tożsamość $(-1)^{\varepsilon_k} = -1$, wyprowadzamy relację

$$(-1)^{\mathcal{N}(\sigma)} = (-1)^m \cdot (-1)^{|X|},$$

czyli ostatecznie

$$(-1)^m = (-1)^{\mathcal{N}(\sigma) - |X|} = (-1)^n.$$

$\square$

Ostatni wynik nadaje sens poniższej

DEFINICJA 58. W notacji Przykł. 16 (1) **znakiem permutacji** $\sigma \in \mathfrak{S}_X$ elementów zbioru skończonego X nazywamy liczbę

$$\text{sgn}(\sigma) := (-1)^n,$$

gdzie n jest liczbą czynników w dowolnym rozkładzie σ na transpozycje. $\blacktriangle$

Mamy oczywiste

STWIERDZENIE 63. W notacji Przykł. 16 (1) i Def. 58 znak permutacji jest homomorfizmem

$$\text{sgn} : \mathfrak{S}_X \longrightarrow \{-1, 1\}$$

grupy symetrycznej $\mathfrak{S}_X$ na zbiorze skończonym X w grupę $(\{-1, 1\}, \cdot, \text{id}_{\{-1, 1\}}, \bullet \mapsto 1)$. Jest to jedyny homomorfizm $\mathfrak{S}_X$ w $\{-1, 1\}$ przyjmujący wartość -1 na dowolnej transpozycji. $\blacksquare$

W odwołaniu do Stw. 31 formułujemy (alternatywną wobec (5.2))

DEFINICJA 59. W notacji Przykł. 16(1) i Def. 58 **grupa alternująca na zbiorze X** to podgrupa

$$\mathfrak{A}_X := \text{Ker sgn} \subset \mathfrak{S}_X.$$

W analogii do grupy symetrycznej stosujemy zapis skrócony $\mathfrak{A}_n$ w przypadku $X = \overline{1, n}$. ▲

Zgodność powyższej definicji z wcześniejszą, podaną w Przykł. 17(5), jest natychmiastową konsekwencją następującego

STWIERDZENIE 64. *Grupa alternująca na dowolnym zbiorze X jest generowana przez cykle o długości 3. Każdy taki cykl można przedstawić jako komutator dwóch transpozycji.* ■

Dowód: Dla dowolnych $a, b, c, d \in X$ zachodzi

$$(a b)(b c) = (a b c) \quad \wedge \quad (a b)(c d) \equiv (a b)(b c)(b c)(c d) = (a b c)(b c d),$$

co w połączeniu z obserwacją, że $\mathfrak{A}_X$ jest generowana przez złożenia par transpozycji, daje pierwszą część dowodzonej tezy. Część druga wynika wprost z równości

$$\text{sgn}([\sigma_1, \sigma_2]) = \text{sgn}(\sigma_1)^2 \cdot \text{sgn}(\sigma_2)^2 = 1,$$

słusznej dla dowolnych $\sigma_1, \sigma_2 \in \mathfrak{S}_X$ a implikującej relację $[\mathfrak{S}_X, \mathfrak{S}_X] \subset \mathfrak{A}_X$, oraz z tożsamości

$$(a b c) = [(a b), (a c)],$$

która na mocy części pierwszej implikuje relację odwrotną. □

* * *

Literatura uzupełniająca: Bardziej wnikliwą analizę struktury grupy symetrycznej, jej podgrup oraz relacji z innymi grupami (skończonymi) Czytelnik znajdzie w pracy Romana [Rom12]. Związki z grupami warkoczy i inne mniej trywialne aspekty rzeczony struktury zostały opisane w monografii Kassela i Turaeva [KT08].

Część 3

Struktury złożone

Dotychczasowe rozważania, w których skupiliśmy się na prostych (tj. grupo- i pierścieniopodobnych) strukturach algebraicznych, dostarczają naturalnych schematów myślenia i opisu niezbędnych do rygorystycznej dyskusji tak istotnych z fizycznego punktu widzenia zagadnień jak symetria i niezmienniczość (wzgl. współzmienniczość). Zarazem przygotowują one grunt pod konstrukcję obiektów bardziej złożonych, w której kluczową rolę odgrywa oddziaływanie kilku wzajem uzgodnionych struktur algebraicznych. Ostatnia część wykładu, poświęcona zbadaniu istotnie nowych relacji indukowanych w obecności działania grupy na zbiorze, jak dotąd rozpatrywanym bez dodatkowej struktury algebraicznej, daje nam przedsmak tematyki, jaką podejmiemy w dalszej części kursu. Zajmiemy się w niej strukturami modulo- i algebropodobnymi znajdującymi bezpośrednie zastosowanie w nowoczesnym opisie formalnym zjawisk fizycznych. Pojęciem porządkującym dalszą część dyskursu jest działanie struktur algebraicznych na sobie, będące szczególnym przykładem następującej abstrakcji pojęcia działania grupy na zbiorze:

DEFINICJA 60. Niechaj X i Ω będą zbiorami. **Realizacja zbioru Ω na zbiorze X** to odwzorowanie

$$\mathcal{R} : \Omega \longrightarrow \text{Map}(X, X) : \omega \longmapsto \mathcal{R}_\omega.$$

Z powyższym stowarzyszamy **lewostronne działanie zbioru Ω na zbiorze X** dane przez

$$\ell : \Omega \times X \longrightarrow X : (\omega, x) \longmapsto \mathcal{R}_\omega(x) \equiv \omega \triangleright x,$$

jak również **prawostronne działanie zbioru Ω na zbiorze X** dane przez

$$\wp : X \times \Omega \longrightarrow X : (x, \omega) \longmapsto \mathcal{R}_\omega(x) \equiv x \triangleleft \omega.$$

Zbiór X określamy mianem **nośnika działania**, natomiast zbiór Ω – mianem **dziedziny operatorów**.

▲

Ileokroć któryś ze zbiorów X, Ω występujących w powyższej definicji sam jest nośnikiem struktury algebraicznej, naturalnym staje się wyróżnienie tych realizacji (a więc także działań), które są w oczywistym znaczeniu zgodne z ową strukturą. Tak właśnie będzie w przypadkach studiowanych w dalszej części kursu.

Elementy teorii modułów

Jedną z najbardziej fundamentalnych i zarazem pojemnych struktur algebraicznych zbudowanych na relacji działania jest struktura modułu nad pierścieniem¹, łącząca w swej definicji struktury elementarne: grupy przemiennej oraz pierścienia. Z czysto matematycznego punktu widzenia jej omówienie jest o tyle zasadne, że pozwala na uprawianie algebry liniowej na dowolnych grupach przemiennej, a oprócz tego dostarcza wiedzy o najbardziej ogólnych własnościach przestrzeni wektorowych, niewymagających bogatszej struktury ciała na dziedzinie operatorów. Wyposaża nas ono także w aparat pojęciowy przydatny w dyskusji elementów algebry homologicznej (rozwiniętej w Rozdz. 14), która znajduje szerokie zastosowanie w klasycznej i kwantowej teorii pól (w szczególności – teorii z tzw. symetrią cechowania). Z fizykalnego (ale nie nie-matematycznego) punktu widzenia struktura modułu jest również dużo bardziej adekwatna i naturalna niżli struktura przestrzeni wektorowej, o czym przekonuje nas chociażby dyskusja klasycznej teorii pola zbudowanej na pojęciu wiązki wektorowej nad czasoprzestrzenią². Na tym jednak nie koniec, oto bowiem, jak przekonamy się niebawem, analiza samych przestrzeni wektorowych wyprowadza nas – na stosunkowo wczesnym etapie – poza wyjściową kategorię, wprost do kategorii modułów nad pierścieniem. Z tych to przyczyn teoria modułów stanowi właściwy punkt wyjścia do wszystkich naszych przyszłych studiów w ramach kursu algebry.

8.1. Struktury elementarne i ich transport

Zacniemy od pojęcia podstawowego:

DEFINICJA 61. Przyjmijmy notację Def. 21 i 32. **Moduł lewostronny nad pierścieniem** R (zwany też z angielska **R -modułem lewostronnym**) to para $((G, \phi_2 = +_G, \phi_1 = -(\cdot), \phi_0 : \bullet \mapsto 0_G), \ell)$ złożona z grupy przemiennej $(G, \phi_2 = +_G, \phi_1 = -(\cdot), \phi_0 : \bullet \mapsto 0_G)$ oraz z **lewostronnego działania pierścienia** R , o elementach określanych mianem **skalarów**, na grupie G

$$\ell : R \times G \longrightarrow G : (r, g) \mapsto r \triangleright g$$

spełniającego następujące aksjomaty (wyrażone przez diagramy przemienne i równoważne zdania logiczne):

¹Bardziej ogólną jest struktura grupy z operatorami, której nośnik jest wprawdzie także grupą, lecz w ogólności nieprzemiennej, patrz: [Bou07b, Rozdz. I §4.2]. Okoliczności, w których nośnik działania jest wyposażony w uboższą jeszcze strukturę algebraiczną, nie są zwykle oddzielnie dyskutowane.

²Zasada superpozycji rozwiązań klasycznych zagadnień liniowych, którą zwykle przywołuje się dla uzasadnienia roli przestrzeni wektorowych w fizyce (klasycznej), jest tutaj *pochodną* struktury modułu nad pierścieniem funkcji gładkich na czasoprzestrzeni, jaką niesie zbiór cięć wiązek wektorowej pól fizycznych.

(lRM1) (G, ℓ) jest zbiorem z lewostronnym działaniem monoidu (R, M, ϕ_0^M) , tj.

$$\begin{array}{ccc} R \times R \times G & \xrightarrow{\text{id}_R \times \ell} & R \times G \\ M \times \text{id}_G \downarrow & & \downarrow \ell \\ R \times G & \xrightarrow{\ell} & G \end{array} \quad \equiv \quad \forall_{r,s \in R} \forall_{g \in G} : r \triangleright (s \triangleright g) = (r \cdot_R s) \triangleright g$$

oraz

$$\begin{array}{ccc} \{\bullet\} \times G & \xrightarrow{\phi_0^M \times \text{id}_G} & R \times G \\ & \searrow \text{pr}_2 & \downarrow \ell \\ & & G \end{array} \quad \equiv \quad \forall_{g \in G} : 1_R \triangleright g = g;$$

(lRM2) (rozdzielność działania względem dodawania skalarów)

$$\begin{array}{ccc} R \times R \times G & \xrightarrow{(\ell \text{opr}_{1,3}, \ell \text{opr}_{2,3})} & G \times G \\ A \times \text{id}_G \downarrow & & \downarrow \phi_2 \\ R \times G & \xrightarrow{\ell} & G \end{array} \quad \equiv \quad \forall_{r,s \in R} \forall_{g \in G} : \begin{array}{l} (r +_R s) \triangleright g \\ = (r \triangleright g) +_G (s \triangleright g) \end{array};$$

(lRM3) (rozdzielność działania względem dodawania grupowego)

$$\begin{array}{ccc} R \times G \times G & \xrightarrow{(\ell \text{opr}_{1,2}, \ell \text{opr}_{1,3})} & G \times G \\ \text{id}_R \times \phi_2 \downarrow & & \downarrow \phi_2 \\ R \times G & \xrightarrow{\ell} & G \end{array} \quad \equiv \quad \forall_{r \in R} \forall_{g,h \in G} : \begin{array}{l} r \triangleright (g +_G h) \\ = (r \triangleright g) +_G (r \triangleright h) \end{array}.$$

Analogicznie, **moduł prawostronny nad pierścieniem** R (zwany też **R -modułem prawostronnym**) to para $((G, \phi_2 = +_G, \phi_1, \phi_0 : \bullet \mapsto 0_G), \wp)$, w której $\wp$ jest odwzorowaniem

$$\wp : G \times R \longrightarrow G : (g, r) \mapsto g \triangleleft r,$$

zwanym **prawostronnym działaniem pierścienia** skalarów R na grupie G i spełniającym oczywiste prawostronne odpowiedniki powyższych aksjomatów:

(rRM1) $(G, \wp)$ jest zbiorem z prawostronnym działaniem monoidu (R, M, ϕ_0^M) , tj.

$$\begin{array}{ccc} G \times R \times R & \xrightarrow{\wp \times \text{id}_R} & G \times R \\ \text{id}_G \times M \downarrow & & \downarrow \wp \\ G \times R & \xrightarrow{\wp} & G \end{array} \quad \equiv \quad \forall_{r,s \in R} \forall_{g \in G} : (g \triangleleft r) \triangleleft s = g \triangleleft (r \cdot_R s)$$

oraz

$$\begin{array}{ccc}
G \times \{\bullet\} & \xrightarrow{\text{id}_G \times \phi_0^M} & G \times R \\
& \searrow \text{pr}_1 & \downarrow \wp \\
& & G
\end{array} \quad \equiv \quad \forall_{g \in G} : g \triangleleft 1_R = g;$$

(rRM2)

$$\begin{array}{ccc}
G \times R \times R & \xrightarrow{(\wp \circ \text{pr}_{1,2}, \wp \circ \text{pr}_{1,3})} & G \times G \\
\text{id}_G \times A \downarrow & & \downarrow \phi_2 \\
G \times R & \xrightarrow{\wp} & G
\end{array} \quad \equiv \quad \forall_{r,s \in R} \forall_{g \in G} : \quad \begin{array}{l} g \triangleleft (r +_R s) \\ = (g \triangleleft r) +_G (g \triangleleft s) \end{array};$$

(rRM3)

$$\begin{array}{ccc}
G \times G \times R & \xrightarrow{(\wp \circ \text{pr}_{1,3}, \wp \circ \text{pr}_{2,3})} & G \times G \\
\phi_2 \times \text{id}_R \downarrow & & \downarrow \phi_2 \\
G \times R & \xrightarrow{\wp} & G
\end{array} \quad \equiv \quad \forall_{r \in R} \forall_{g,h \in G} : \quad \begin{array}{l} (g +_G h) \triangleleft r \\ = (g \triangleleft r) +_G (h \triangleright r) \end{array}.$$

▲

Dla pełniejszego zrozumienia struktury modułu warto poddać jego aksjomatykę prostej reinterpretacji. W tym celu wprowadzamy

DEFINICJA 62. Przyjmijmy notację Def. 21 i 32. **Pierścień endomorfizmów grupy przemiennej** G to pierścień

$$(\text{End}(G), \tilde{\phi}_2, \circ, \tilde{\phi}_1, \tilde{\phi}_0, \bullet \mapsto \text{id}_G),$$

którego nośnikiem jest zbiór $\text{End}(G) \subset \text{Map}(G, G)$ endomorfizmów grupy G z operacjami $\tilde{\phi}_n$, $n \in \{0, 1, 2\}$ jak w Przykł. 15 (4) dla $S := G$

▲

Zapowiedziana reinterpretacja przyjmuje postać oczywistego

STWIERDZENIE 65. W notacji Def. 21, 32 i 61 oznaczmy – dla dowolnego $r \in R$ –

$$\ell_r : G \longrightarrow G : g \longmapsto r \triangleright g, \quad \wp_r : G \longrightarrow G : g \longmapsto g \triangleleft r.$$

Powyższe odwzorowania bywają nazywane **homotetiami o skali** r ,

indexdziałanie!pierścienia!homotetia

patrz:

[Bou07b, Rozdz. II §4.2]. Obraz odwzorowania

$$\ell. : R \longrightarrow \text{Map}(G, G) : r \longmapsto \ell_r$$

jest zawarty w podzbiorze $\text{End}(G) \subset \text{Map}(G, G)$ i jako taki zadaje homomorfizm pierścienia R w pierścień endomorfizmów G . Podobnie obraz odwzorowania

$$\wp. : R \longrightarrow \text{Map}(G, G) : r \longmapsto \wp_r$$

jest zawarty w podzbiorze $\text{End}(G) \subset \text{Map}(G, G)$ i określa homomorfizm **pierścienia przeciwnego do R** w pierścień endomorfizmów G .

I odwrotnie, każdy homomorfizm pierścienia (wzgl. pierścienia przeciwnego) w pierścień endomorfizmów danej grupy przemiennej zadaje na niej strukturę R -modułu lewostronnego (wzgl. prawostronnego).

■

Jak w przypadku działania grupy na zbiorze możemy bez jakiejkolwiek straty ogólności ograniczyć nasze rozważania (tymczasowo) do modułów lewostronnych, o czym przekonuje proste

STWIERDZENIE 66. *Przyjmijmy notację Def. 21, 32 i 61. Struktura modułu lewostronnego nad pierścieniem R na grupie G indukuje na tej ostatniej w kanoniczny sposób strukturę modułu prawostronnego nad pierścieniem przeciwnym do R i vice versa.*

■

PRZYKŁAD(Y) 34.

- (1) Grupa trywialna niesie strukturę modułu nad dowolnym pierścieniem. Jest to tzw. **moduł trywialny**, który będziemy oznaczać symbolem $\mathbf{0}$.
- (2) Grupa przemienne (R, A, P, ϕ_0^A) definiowana przez dowolny pierścień $(R, A = +, M = \cdot, P = -(\cdot), \phi_0^A : \bullet \mapsto 0_R, \phi_0^M : \bullet \mapsto 1_R)$ jest modułem lewostronnym nad R z działaniem $\ell : R \times R \rightarrow R : (r, s) \mapsto r \cdot s$. Ogólniej, dla dowolnego $n \in \mathbb{N} \setminus \{0\}$ grupa $(R^{\times n}, A^n, P^n, \phi_0^{A^n})$ zdefiniowana przez pierścień R , z operacjami określonymi „współrzędna po współrzędnej”:

$$A^n((x_1, x_2, \dots, x_n), (y_1, y_2, \dots, y_n)) := (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n),$$

$$P^n(x_1, x_2, \dots, x_n) := (-x_1, -x_2, \dots, -x_n),$$

$$\phi_0^{A^n}(\bullet) := (0_R, 0_R, \dots, 0_R),$$

dla $(x_1, x_2, \dots, x_n), (y_1, y_2, \dots, y_n) \in R^{\times n}$, niesie naturalną strukturę modułu lewostronnego nad R z działaniem

$$\ell^n : R \times R^{\times n} \rightarrow R^{\times n} : (r, (x_1, x_2, \dots, x_n)) \mapsto (r \cdot x_1, r \cdot x_2, \dots, r \cdot x_n),$$

dla którego będziemy używać oznaczenia $\triangleright_n$. Oczywiście zbiór $R^{\times n}$ jest także nośnikiem naturalnej struktury R -modułu prawostronnego, zadawanej przez mnożenie („współrzędna po współrzędnej”) z prawej strony przez elementy pierścienia R . Dla jawnego rozróżnienia – ważnego w dalszej części kursu – tych dwóch struktur na $R^{\times n}$ będziemy ich nośniki zapisywać odpowiednio jako ${}_R R^{\times n}$ (R -moduł lewostronny) i $R_R^{\times n}$ (R -moduł prawostronny).

- (3) Dowolny homomorfizm $\chi : R^{(1)} \rightarrow R^{(2)}$ pierścieni $(R^{(\alpha)}, M^{(\alpha)}, A^{(\alpha)}, P^{(\alpha)}, \phi_0^{M^{(\alpha)}}, \phi_0^{A^{(\alpha)}})$, $\alpha \in \{1, 2\}$ indukuje na grupie $(R^{(2)}, A^{(2)}, P^{(2)}, \phi_0^{A^{(2)}})$ strukturę modułu lewostronnego nad $R^{(1)}$ z działaniem $\ell : R^{(1)} \times R^{(2)} \rightarrow R^{(2)} : (r, s) \mapsto M^{(2)}(\chi(r), s)$.
- (4) Grupa przemienne $(G, \phi_2, \phi_1, \phi_0)$ jest nośnikiem kanonicznej struktury modułu lewostronnego nad pierścieniem endomorfizmów z Def. 62, przy czym działanie $\text{End}(G)$ jest tu zadawane przez odwzorowanie ewaluacji $\ell : \text{End}(G) \times G \rightarrow G : (\chi, g) \mapsto \chi(g) =: \text{ev}_\chi(g)$.

- (5) Grupa przemiana jest też nośnikiem struktury modułu lewostronnego nad pierścieniem $\mathbb{Z}$ z Przykł. 7, przy czym działanie $\mathbb{Z}$ jest określone przez branie krotności jak w (5.1).
- (6) Struktura modułu lewostronnego nad pierścieniem R na grupie przemiennej $(G, \phi_2, \phi_1, \phi_0)$ indukuje na grupie $(\text{Map}(S, G), \tilde{\phi}_2, \tilde{\phi}_1, \tilde{\phi}_0)$ z Przykł. 15 (4) naturalną strukturę modułu lewostronnego nad R z działaniem $\ell : R \times \text{Map}(S, G) \longrightarrow \text{Map}(S, G) : (r, f) \longmapsto r \triangleright f$, przy czym dla dowolnego $x \in S$ jest $(r \triangleright f)(x) := r \triangleright f(x)$.

✓

Szczególną i szczególnie istotną z fizykalnego punktu widzenia klasę modułów opisuje

DEFINICJA 63. W notacji Def. 11, 32, 21 i 61 **przestrzeń wektorowa nad ciałem $\mathbb{K}$** (zwana też **przestrzenią $\mathbb{K}$ -liniową**) to moduł nad pierścieniem $(\mathbb{K}, A, M, P, \mathbf{0}, \mathbf{1})$ ciała $(\mathbb{K}, A, M, P, \text{Inv}, \mathbf{0}, \mathbf{1})$. Elementy nośnika tej struktury określamy mianem **wektorów**.

▲

Nośniki struktury przestrzeni wektorowej tradycyjnie oznacza się dużymi literami z końca alfabetu łacińskiego, poczynając od V , elementy zaś tych zbiorów (czyli wektory) – odnośnymi literami małymi. W dalszej części wykładu będziemy się starali dochować wierności tej tradycji.

PRZYKŁAD(Y) 35.

- (1) Grupa trywialna jest nośnikiem struktury przestrzeni wektorowej nad dowolnym ciałem. Jest to tzw. **przestrzeń trywialna** (lub **zerowa**), którą będziemy oznaczać wprowadzonym wcześniej symbolem $\mathbf{0}$.
- (2) Dla dowolnego $n \in \mathbb{N} \setminus \{0\}$ grupa przemiana $(\mathbb{K}^{\times n}, A^n, P^n, \mathbf{0}^n)$ definiowana przez dowolne ciało $(\mathbb{K}, A, M, P, \text{Inv}, \mathbf{0}, \mathbf{1})$ na sposób opisany w Przykł. 34 (2) niesie naturalną strukturę przestrzeni wektorowej. W szczególności grupa $(\mathbb{C}, +_{\mathbb{C}}, \bullet \longmapsto 0)$ jest przestrzenią wektorową nad ciałem $\mathbb{R}$ względem działania opisanego w Def. 15.
- (3) Uogólnieniem struktury opisanej w ostatnim punkcie jest struktura przestrzeni wektorowej nad $\mathbb{K}$ na zbiorze $\mathbb{K}^{\mathbb{N}}$ ciągów o wartościach w $\mathbb{K}$ z operacjami zdefiniowanymi “wyraz po wyrazie”.
- (4) Grupa przemiana $(\mathbb{K}[t], +, -(\cdot), \bullet \longmapsto 0)$ definiowana przez pierścień wielomianów $\mathbb{K}[t]$ o współczynnikach z ciała $\mathbb{K}$ jest przestrzenią wektorową nad $\mathbb{K}$ z działaniem

$$\begin{aligned} \ell^{n+1} : \quad & \mathbb{K} \times \mathbb{K}[t] \longrightarrow \mathbb{K}[t] \\ & : \quad (r, r_0 + r_1 t + r_2 t^2 + \cdots r_n t^n) \longmapsto r \cdot r_0 + r \cdot r_1 t + r \cdot r_2 t^2 + \cdots r \cdot r_n t^n. \end{aligned}$$

✓

Możemy teraz wskazać najprostsze konsekwencje wypisanych aksjomatów.

STWIERDZENIE 67. W notacji Def. 21, 32 i 61 w module lewostronnym nad pierścieniem R zachodzą następujące tożsamości:

- (i) $\forall_{g \in G} : 0_R \triangleright g = 0_G;$

- (ii) $\forall_{r \in R} : r \triangleright 0_G = 0_G;$
- (iii) $\forall_{\substack{r \in R \\ g \in G}} : P(r) \triangleright g = \phi_1(r \triangleright g);$
- (iv) $\forall_{\substack{r \in R \\ g \in G}} : r \triangleright \phi_1(g) = \phi_1(r \triangleright g).$

■

W przypadku przestrzeni wektorowych prawdziwe jest ponadto

STWIERDZENIE 68. *W notacji Def. 11, 32 i 63 w przestrzeni wektorowej nad ciałem $\mathbb{K}$ zachodzi tożsamość*

$$\forall_{(\lambda, v) \in \mathbb{K} \times V} : \lambda \triangleright v = 0_V \implies (\lambda = 0_{\mathbb{K}} \vee v = 0_V).$$

■

Dowód: Jeśli $\lambda \neq 0_{\mathbb{K}}$, to istnieje $\text{Inv}_{\mathbb{K}}(\lambda) =: \lambda^{-1}$, a wtedy $v = 1_{\mathbb{K}} \triangleright v = (\lambda^{-1} \cdot_R \lambda) \triangleright v = \lambda^{-1} \triangleright (\lambda \triangleright v) = \lambda^{-1} \triangleright 0_V = 0_V$, przy czym ostatnia równość wykorzystuje udowodnione wcześniej Stw. 67 (ii). $\square$

O tym, że własność przestrzeni wektorowych opisana powyżej nie rozszerza się na dowolne moduły nad pierścieniem, przekonuje nas analiza prostego przypadku. Oto w $\mathbb{Z}$ -module $\mathbb{Z}/n\mathbb{Z}$ każdy element spełnia tożsamość

$$n \triangleright [k]_n = [0]_n.$$

DEFINICJA 64. W notacji Def. 21, 32, 61 i 63 **podmoduł** modułu lewostronnego $((G, \phi_2, \phi_1, \phi_0), \ell)$ nad pierścieniem R to para $((H, \phi_2, \phi_1, \phi_0), \ell)$, w której H jest podgrupą G o własności

$$(\text{IPM}) \quad \ell : R \times H \longrightarrow H \subset G.$$

Mówimy, że działanie pierścienia R zachowuje H .

W przypadku przestrzeni wektorowej nad ciałem $\mathbb{K}$ podmoduł określamy mianem **podprzestrzeni (wektorowej)**.

▲

Pojęcie podmodułu stanowi punkt wyjścia do nader istotnej konstrukcji opisanej poniżej.

STWIERDZENIE 69. *Przyjmijmy notację Def. 21, 32, 38, 42, 61 i 64 oraz Stw. 40. Struktura modułu lewostronnego nad pierścieniem R na grupie G indukuje kanoniczną strukturę modułu lewostronnego nad R na grupie ilorazowej $(G/H, +_{G/H}, P_{G/H}, H)$ względem podmodułu $H \subset G$ z operacjami (zdefiniowanymi dla dowolnych $g, g_1, g_2 \in G$)*

$$(g_1 +_G H) +_{G/H} (g_2 +_G H) := (g_1 +_G H) +_G (g_2 +_G H) = (g_1 +_G g_2) +_G H,$$

$$P_{G/H}(g +_G H) := (-g) +_G H.$$

Struktura ta jest określona przez działanie

$$\ell^{G/H} : R \times (G/H) \longrightarrow G/H : (r, g +_G H) \longmapsto (r \triangleright g) +_G H$$

i nosi nazwę modułu ilorazowego (wzgl. przestrzeni ilorazowej, gdy R jest ciałem).

■

Dowód: Określoność $\ell^{G/H}$ jest prostą konsekwencją definiującej własności (IPM) podmodułu. Oto bowiem dla dowolnego reprezentanta $k \in g +_G H$ zachodzi $\exists h \in H : k = g +_G h$, a zatem $(r \triangleright k) +_G H = (r \triangleright g) +_G (r \triangleright h) +_G H = (r \triangleright g) +_G H$, jako że $r \triangleright h \in H$. Aksjomaty modułu lewostronnego sprawdzamy w bezpośrednim rachunku. $\square$

Wyróżniamy odwzorowania transportujące strukturę modułu pomiędzy nośnikami.

DEFINICJA 65. Przyjmijmy notację Def. 21, 32, 35 oraz 61. **Homomorfizm R -modułu lewostronnego $((G^{(1)}, \phi_2^{(1)}, \phi_1^{(1)}, \phi_0^{(1)}), \ell^{(1)})$ w R -moduł lewostronny $((G^{(2)}, \phi_2^{(2)}, \phi_1^{(2)}, \phi_0^{(2)}), \ell^{(2)})$ to R -ekwiwariantny homomorfizm grup przemiennych**

$$\chi : (G^{(1)}, \phi_2^{(1)}, \phi_1^{(1)}, \phi_0^{(1)}) \longrightarrow (G^{(2)}, \phi_2^{(2)}, \phi_1^{(2)}, \phi_0^{(2)}),$$

tj. taki ich homomorfizm, który spełnia aksjomat (wyrażony przez diagram przemienności i równoważne zdanie logiczne):

$$(IRMH) \quad \begin{array}{ccc} R \times G^{(1)} & \xrightarrow{\ell^{(1)}} & G^{(1)} \\ \text{id}_R \times \chi \downarrow & & \downarrow \chi \\ R \times G^{(2)} & \xrightarrow{\ell^{(2)}} & G^{(2)} \end{array} \quad \equiv \quad \forall_{(r,g) \in R \times G^{(1)}} : \quad \begin{array}{l} \chi \circ \ell_r^{(1)}(g) \\ = \ell_r^{(2)} \circ \chi(g) \end{array} .$$

Bijektywny homomorfizm R -modułów lewostronnych, którego odwrotność jest homomorfizmem R -modułów lewostronnych, nazywamy **izomorfizmem R -modułów lewostronnych**.

Opisane homomorfizmy noszą miano **odwzorowań R -liniowych**. Wprowadzamy oznaczenie

$$\text{Hom}_R(G^{(1)}, G^{(2)}) := \{ \chi : G^{(1)} \longrightarrow G^{(2)} \mid \chi \text{ } R\text{-liniowe} \}$$

dla zbioru wszystkich odwzorowań R -liniowych z R -modułu $G^{(1)}$ w R -moduł $G^{(2)}$. W szczególnym przypadku $G^{(1)} = G^{(2)} =: G$, będziemy pisać

$$\text{End}_R(G) := \text{Hom}_R(G, G),$$

wyróżniając dodatkowo endomorfizmy (obustronnie) odwracalne, czyli automorfizmy,

$$\text{Aut}_R(G) := \{ \chi \in \text{End}_R(G) \mid \chi \text{ bijektywne} \}.$$

▲

PRZYKŁAD(Y) 36.

- (1) Odwzorowanie identycznościowe na dowolnym module lewostronnym.
- (2) Rzut kanoniczny $\text{pr}_i : R^{\times n} \longrightarrow R$ na i -ty czynnik kartezjański modułu z Przykł. 34 (2), traktowany jako nośnik kanonicznej struktury modułu nad R dla $n = 1$.

- (3) Odwzorowanie grupy przemiennej $G^{(1)}$ będącej nośnikiem struktury modułu lewostronnego nad pierścieniem R w grupę przemiennej $G^{(2)}$ dane wzorem $\mathbf{0} : G^{(1)} \rightarrow G^{(2)} : g \mapsto \phi_0^{(2)}(\bullet)$ jest odwzorowaniem R -liniowym (względem trywialnej struktury R -modułu lewostronnego na grupie trywialnej $\{\phi_0^{(2)}(\bullet)\}$). Odwzorowanie to nazywamy **homomorfizmem zerowym**.
- (4) Rzut kanoniczny $\pi_{G/H} : G \rightarrow G/H$ (nośnika struktury) modułu lewostronnego nad pierścieniem R na moduł ilorazowy G/H względem dowolnego podmodułu $H \subset G$.
- (5) Dowolny homomorfizm grup przemiennej traktowanych jako moduły lewostronne nad pierścieniem $\mathbb{Z}$ (jak w Przykł. 34 (4)) jest odwzorowaniem $\mathbb{Z}$ -liniowym.

✓

8.2. Proste własności odwzorowań R -liniowych

Szczegółowym opisem struktury odwzorowań R -liniowych zajmiemy się w dalszej części wykładu. Na obecnym etapie ograniczymy się do elementarnych spostrzeżeń.

STWIERDZENIE 70. *Przyjmijmy notację Def. 21, 32, 35, 61 oraz 65. Czwórka $(\text{Hom}_R(G^{(1)}, G^{(2)}), A \equiv +, P \equiv -(\cdot), \bullet \mapsto 0)$, w której skład wchodzi operacje punktowe*

$$A : \text{Hom}_R(G^{(1)}, G^{(2)})^{\times 2} \rightarrow \text{Hom}_R(G^{(1)}, G^{(2)}) : (\chi_1, \chi_2) \mapsto \chi_1 + \chi_2,$$

$$P : \text{Hom}_R(G^{(1)}, G^{(2)}) \rightarrow \text{Hom}_R(G^{(1)}, G^{(2)}) : \chi \mapsto -\chi,$$

określone wzorami (zapisanymi dla dowolnego $g \in G^{(1)}$)

$$(\chi_1 + \chi_2)(g) := \chi_1(g) +_{(2)} \chi_2(g), \quad (-\chi)(g) := P_{G^{(2)}}(\chi(g)),$$

oraz stała $0(g) := 0_{G^{(2)}}$, jest grupą przemiennej. Szóstka $(\text{End}_R(G), +, \circ, -(\cdot), \bullet \mapsto 0, \bullet \mapsto \text{id}_G)$ jest pierścieniem, natomiast czwórka $(\text{Aut}_R(G), \circ, (\cdot)^{-1}, \bullet \mapsto \text{id}_G)$ jest grupą.

Jeśli pierścień R jest przemiennej³, to wówczas $\text{Hom}_R(G^{(1)}, G^{(2)})$ niesie naturalną strukturę R -modułu z działaniem

$$\ell : R \times \text{Hom}_R(G^{(1)}, G^{(2)}) \rightarrow \text{Hom}_R(G^{(1)}, G^{(2)}) : (r, \chi) \mapsto r \triangleright \chi,$$

$$(r \triangleright \chi)(g) := \lambda^{(2)}(r, \chi(g)).$$

W szczególności $\text{Hom}_K(G^{(1)}, G^{(2)})$ jest nośnikiem struktury przestrzeni wektorowej nad ciałem K .

■

Powyższe stwierdzenie pozwala wysłowić prosty, lecz zarazem całkowicie ogólny argument przemawiający za wprowadzeniem struktury modułu nad pierścieniem

³Przemienność R gwarantuje, że odwzorowanie $r \triangleright \chi$ jest R -liniowe, gdy w przypadku nieprzemiennej jest $(r \triangleright \chi)(s \triangleright_{(1)} g) = r \triangleright_{(2)} \chi(s \triangleright_{(1)} g) = (r \cdot_R s) \triangleright_{(2)} \chi(g) \neq (s \cdot_R r) \triangleright_{(2)} \chi(g) = s \triangleright_{(2)} (r \triangleright \chi)(g)$.

nawet w dyskusji, w której punktem wyjścia jest struktura przestrzeni wektorowej ($R = \mathbb{K}$).

STWIERDZENIE 71. *Przyjmijmy notację Def. 21, 32, 35, 61 i 65 oraz Stw. 70. Grupa przemienności $(\text{Hom}_R(G^{(1)}, G^{(2)}), A \equiv +, P \equiv -(\cdot), \bullet \mapsto 0)$ niesie naturalną strukturę modułu lewostronnego nad pierścieniem $\text{End}_R(G^{(2)})$ oraz modułu prawostronnego nad pierścieniem $\text{End}_R(G^{(1)})$.*

■

Dowód: Rzeczoną strukturę zadaje działanie lewostronne

$$\lambda : \text{End}_R(G^{(2)}) \times \text{Hom}_R(G^{(1)}, G^{(2)}) \longrightarrow \text{Hom}_R(G^{(1)}, G^{(2)}) : (\alpha, \chi) \mapsto \alpha \circ \chi$$

oraz działanie prawostronne

$$\varrho : \text{Hom}_R(G^{(1)}, G^{(2)}) \times \text{End}_R(G^{(1)}) \longrightarrow \text{Hom}_R(G^{(1)}, G^{(2)}) : (\chi, \beta) \mapsto \chi \circ \beta,$$

dla których łatwo sprawdzić aksjomaty modułu. $\square$

Tym oto sposobem najprostsza analiza własności homomorfizmów przestrzeni wektorowych wyprowadza nas poza wyjściową kategorię, czyniąc nieodzownym jej przeniesienie na bardziej ogólny poziom teorii modułów nad pierścieniem.

Tytułem przygotowania do dalszych rozważań dowodzimy

STWIERDZENIE 72. *Każdy bijektywny homomorfizm R -modułów lewostronnych jest izomorfizmem R -modułów lewostronnych.*

■

Dowód: Niechaj $\chi : ((G^{(1)}, \phi_2^{(1)}, \phi_1^{(1)}, \phi_0^{(1)}), \ell^{(1)}) \longrightarrow ((G^{(2)}, \phi_2^{(2)}, \phi_1^{(2)}, \phi_0^{(2)}), \ell^{(2)})$ będzie takim homomorfizmem., tj. niechaj dla dowolnych $r \in R$ i $g \in G^{(1)}$ zachodzi

$$\chi \circ \ell_r^{(1)}(g) = \ell_r^{(2)} \circ \chi(g),$$

a wtedy – wobec odwracalności χ – dostajemy

$$\ell_r^{(1)}(g) = \chi^{-1} \circ \chi \circ \ell_r^{(1)}(g) = \chi^{-1} \circ \ell_r^{(2)} \circ \chi(g).$$

Skoro jednak χ jest bijekcją, to każdy element $h \in G^{(2)}$ daje się przedstawić w postaci $h = \chi(g)$ dla pewnego (i jedynego takiego) $g \in G^{(1)}$, a zatem

$$\ell_r^{(1)} \circ \chi^{-1}(h) = \chi^{-1} \circ \ell_r^{(2)}(h),$$

co kończy dowód. $\square$

Zachodzi także oczywiste

STWIERDZENIE 73. *Jądro homomorfizmu modułów lewostronnych nad dowolnym pierścieniem jest podmodułem dziedziny tegoż homomorfizmu, natomiast jego obraz jest podmodułem przeciwdziedziny.*

■

Wprowadzamy wygodną

DEFINICJA 66. W notacji Def. 21, 32, 35, 36, 42, 61 i 65 oraz Stw. 40 **koobraz homomorfizmu χ modułów nad pierścieniem** to moduł ilorazowy

$$\text{Coim } \chi := G^{(1)} / \text{Ker } \chi,$$

natomiast jego **kojądro** to moduł ilorazowy

$$\text{Coker } \chi := G^{(2)} / \text{Im } \chi.$$

▲

Wiele pojęć omówionych w Rozdz. 5, w tym pojęcie ciągu dokładnego, podnosi się w naturalny sposób do kategorii modułów nad ustalonym pierścieniem. To samo dotyczy niektórych fundamentalnych konstrukcji homomorfizmów kanonicznych oraz indukowanych, które przytaczamy poniżej bez dowodu⁴ po ich uprzednim przeformułowaniu.

TWIERDZENIE 8.1 (Pierwsze twierdzenie o izomorfizmie modułów). *W notacji Def. 21, 32, 35, 36, 42, 61 i 65 oraz Stw. 40 $\text{Ker } \chi$ jest podmodułem $G^{(1)}$, a nadto istnieje kanoniczny izomorfizm modułów*

$$\lambda_\chi : \text{Coim } \chi \xrightarrow{\cong} \text{Im } \chi,$$

który czyni przemiennym następujący diagram o wierszach i kolumnach dokładnych

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Ker } \chi & \xrightarrow{J_{\text{Ker } \chi}} & G^{(1)} & \xrightarrow{\chi} & G^{(2)} \xrightarrow{\pi_{\text{Coker } \chi}} \text{Coker } \chi \longrightarrow 0 \\ & & & & \downarrow \pi_{\text{Coim } \chi} & & \uparrow J_{\text{Im } \chi} \\ & & 0 & \longrightarrow & \text{Coim } \chi & \xrightarrow{\lambda_\chi} & \text{Im } \chi \longrightarrow 0 \\ & & & & \downarrow & & \uparrow \\ & & & & 0 & & 0 \end{array}.$$

Diagram ten opisuje kanoniczny rozkład homomorfizmu χ jak w Tw. 5.2.

■

TWIERDZENIE 8.2 (Drugie twierdzenie o izomorfizmie modułów). *Przyjmijmy notację Def. 21, 32, 35, 61 i 65. Niechaj $H, K \subset G$ niosą strukturę podmodułu G . Wówczas $K +_G H, K \cap H \subset G$ są podmodułami i istnieje kanoniczny izomorfizm modułów ilorazowych*

$$(K +_G H) / H \cong K / (K \cap H).$$

■

TWIERDZENIE 8.3 (Trzecie twierdzenie o izomorfizmie modułów). *Przyjmijmy notację Def. 21, 32, 35, 61 i 65. Niechaj $H_1 \supset H_2$ będą podmodułami G . Istnieje kanoniczny izomorfizm modułów ilorazowych*

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

■

⁴W każdym z przypadków dowód sprowadza się do bezpośredniego sprawdzenia R -liniowości stosownych homomorfizmów grup skonstruowanych w dowodach odpowiedników wypisanych twierdzeń zamieszczonych w Rozdz. 5.

TWIERDZENIE 8.4 (O liniowym przeciwobrazie normalnego ciągu dokładnego modułów). *W notacji Def. 21, 32, 35, 42, 43, 61 oraz 65 i dla dowolnego podmodułu $H^{(2)} \subset G^{(2)}$ oraz homomorfizmu R -modułów lewostronnych $\chi : G^{(1)} \rightarrow G^{(2)}$ podgrupa $\chi^{-1}(H^{(2)})$ jest podmodulem i istnieje kanoniczny monomorfizm indukowany modułów ilorazowych*

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

który czyni przemiennym diagram wypisany w treści Tw. 5.7. W szczególności jeśli χ jest surjekcją, to wówczas $\bar{\chi}$ jest izomorfizmem modułów.

■

Zanim przejdziemy do przedstawienia rozmaitych naturalnych konstrukcji wykorzystujących strukturę modułu nad pierścieniem i zbadamy własności odwzorowań liniowych, zapoznamy się z jednym jeszcze wynikiem abstrakcyjnym o niebagatelnie znaczeniu rachunkowym. Jego wyprowadzenie pozwoli nam rozbudować arsenał narzędzi logicznych szczególnie wygodnych w dyskusji struktur algebraicznych o metodę określaną mianem „pogoni wzdłuż diagramu” (z jęz. ang. „diagram chase”).

STWIERDZENIE 74. (Lemat Pięciu (Morfizmów)) *Przyjmijmy notację Def. 21, 32, 35, 43, 61 oraz 65 i rozważmy dwie piątki $((A^{(\gamma)}, \phi_2^{(\gamma)}, \phi_1^{(\gamma)}, \phi_0^{(\gamma)}), \ell^{(\gamma)})$ i $((B^{(\gamma)}, \phi_2^{(\gamma+5)}, \phi_1^{(\gamma+5)}, \phi_0^{(\gamma+5)}), \ell^{(\gamma+5)})$, $\gamma \in \overline{1, 5}$ modułów lewostronnych nad pierścieniem R , a wraz z nią – kolekcje $\alpha_\delta, \beta_\delta$, $\delta \in \overline{1, 4}$ i χ_γ , $\gamma \in \overline{1, 5}$ homomorfizmów modułów, składających się na diagram przemienny*

$$\begin{array}{ccccccccc} A^{(1)} & \xrightarrow{\alpha_1} & A^{(2)} & \xrightarrow{\alpha_2} & A^{(3)} & \xrightarrow{\alpha_3} & A^{(4)} & \xrightarrow{\alpha_4} & A^{(5)} \\ \chi_1 \downarrow & & \chi_2 \downarrow & & \chi_3 \downarrow & & \chi_4 \downarrow & & \chi_5 \downarrow \\ B^{(1)} & \xrightarrow{\beta_1} & B^{(2)} & \xrightarrow{\beta_2} & B^{(3)} & \xrightarrow{\beta_3} & B^{(4)} & \xrightarrow{\beta_4} & B^{(5)} \end{array},$$

którego wiersze są ciągami dokładnymi. Wówczas prawdziwe są następujące zdania:

- (i) *Jeśli χ_1 jest surjekcją, a χ_2 i χ_4 są injekcjami, to wtedy χ_3 jest injekcją.*
- (ii) *Jeśli χ_5 jest injekcją, a χ_2 i χ_4 są surjekcjami, to wtedy χ_3 jest surjekcją.*

W szczególności więc ilekroć χ_1, χ_2, χ_4 i χ_5 są izomorfizmami, izomorfizmem jest także χ_3 .

■

Dowód:

Ad (i) Niechaj $g \in \text{Ker } \chi_3$, a wtedy $\chi_4 \circ \alpha_3(g) = \beta_3 \circ \chi_3(g) = 0_{B^{(4)}}$, zatem – wobec injektywności χ_4 – jest $\alpha_3(g) = 0_{A^{(4)}}$, czyli $g \in \text{Ker } \alpha_3$. Skoro jednak górny wiersz diagramu jest dokładny, to $g \in \text{Im } \alpha_2$, tj. $g = \alpha_2(h)$ dla pewnego $h \in A^{(2)}$, przy czym $0_{B^{(3)}} = \chi_3(g) = \chi_3 \circ \alpha_2(h) = \beta_2 \circ \chi_2(h)$, przeto $\chi_2(h) \in \text{Ker } \beta_2$, skąd – wobec dokładności wiersza dolnego – wniosek, że $\chi_2(h) = \beta_1(k)$ dla pewnego $k \in B^{(1)}$. Ale też χ_1 jest surjekcją, toteż istnieje $l \in A^{(1)}$ spełniający równość $k = \chi_1(l)$, zatem $\chi_2(h) = \beta_1 \circ \chi_1(l) = \chi_2 \circ \alpha_1(l)$. Uwzględniając injektywność χ_2 , otrzymujemy na tej podstawie

równość $h = \alpha_1(l)$ i dalej $g = \alpha_2 \circ \alpha_1(l) = 0_{A^{(3)}}$ z racji dokładności wiersza górnego. Przedstawione rozumowanie dowodzi injektywności χ_3 .

Ad (ii) Niech teraz $g \in B^{(3)}$, a wtedy – wobec surjektywności χ_4 – zachodzi równość $\beta_3(g) = \chi_4(h)$ dla pewnego $h \in A^{(4)}$, skąd dalej, z uwagi na dokładność wiersza dolnego, $0_{B^{(5)}} = \beta_4 \circ \beta_3(g) = \beta_4 \circ \chi_4(h) = \chi_5 \circ \alpha_4(h)$, ale χ_5 jest injekcją, zatem $h \in \text{Ker } \alpha_4 = \text{Im } \alpha_3$, czyli $h = \alpha_3(k)$ dla pewnego $k \in A^{(3)}$. W takim razie jednak $\beta_3(g) = \chi_4(h) = \chi_4 \circ \alpha_3(k) = \beta_3 \circ \chi_3(k)$, co prowadzi do równości $g +_{B^{(3)}} (-\chi_3(k)) \in \text{Ker } \beta_3$, co – gdy raz jeszcze wykorzystać dokładność wiersza dolnego – daje $g = \chi_3(k) +_{B^{(3)}} \beta_2(l)$ dla pewnego $l \in B^{(2)}$. Zważywszy surjektywność χ_2 , wnioskujemy na tej podstawie, że $g = \chi_3(k) +_{B^{(3)}} \beta_2 \circ \chi_2(m) = \chi_3(k) +_{B^{(3)}} \chi_3 \circ \alpha_2(m)$ dla pewnego $m \in A^{(2)}$. Ostatecznie zatem $g = \chi_3(k +_{A^{(3)}} \alpha_2(m)) \in \text{Im } \chi_3$, co należało okazać. $\square$

8.3. Liniowa niezależność, baza i pojęcia pochodne

Dalsze nasze rozważania wytyczają strukturalnie najprostszą i najbardziej naturalną drogę od ogólnej struktury modułu nad pierścieniem do struktury przestrzeni wektorowej. Zaczniemy od pomocniczej

DEFINICJA 67. Niechaj Λ i S będą zbiorami. **Rodzina elementów zbioru S indeksowana przez zbiór Λ** to odwzorowanie $x. : \Lambda \longrightarrow S : \lambda \longmapsto x_\lambda$, przy czym element $\lambda \in \Lambda$ określamy mianem **indeksu**, zbiór Λ zaś – mianem **zbioru indeksów**. Rodzinę taką zapisujemy w postaci $\{x_\lambda\}_{\lambda \in \Lambda}$. Ilekroć S jest nośnikiem struktury monoidu o elemencie neutralnym e , wprowadzamy pojęcie **nośnika rodziny** $\{x_\lambda\}_{\lambda \in \Lambda}$ danego wzorem

$$\text{supp } \{x_\lambda\}_{\lambda \in \Lambda} := \{ \lambda \in \Lambda \mid x_\lambda \neq e \}.$$

Rodzina o nośniku skończonym to taka, której nośnik ma moc skończoną. Zbiór wszystkich takich rodzin będziemy oznaczać symbolem $\mathcal{R}_0(S)$. $\blacktriangle$

Pozwala nam ona sformułować

DEFINICJA 68. W notacji Def. 67, 21, 32 oraz 61 i dla dowolnego podzbioru $S \subset G$ modułu G **kombinacja liniowa elementów zbioru S o współczynnikach z pierścienia R** to dowolna suma (w sensie dodawania $+_G$ w grupie przemiennej G)

$$\sum_{g \in S} r_g \triangleright g,$$

wyznaczona przez rodzinę $\{r_g\}_{g \in S}$ elementów z R indeksowaną przez S , o nośniku skończonym. Elementy tej rodziny określamy mianem **współczynników kombinacji liniowej**. $\blacktriangle$

PRZYKŁAD(Y) 37.

- (1) W $\mathbb{Z}$ -module $\mathbb{Z}^{\times 2}$ z Przykł. 34 (2) element $(5, 2)$ jest kombinacją liniową $2 \triangleright (1, 1) + 3 \triangleright (1, 0)$ o współczynnikach 2 i 3.
- (2) W $\mathbb{Z}$ -module $\mathbb{Z}/9\mathbb{Z}$ z Przykł. 34 (5) element $[6]_9$ jest kombinacją liniową $4 \triangleright [7]_9 +_9 (-1) \triangleright [4]_9$ o współczynnikach 4 i -1 .
- (3) W przestrzeni $\mathbb{R}$ -liniowej $\mathbb{R}^{\times 3}$ z Przykł. 35 (2) wektor $(\pi, e, \sqrt{2})$ jest kombinacją liniową $\pi \triangleright (1, 0, 0) +_{\mathbb{R}} e \triangleright (0, 1, 0) +_{\mathbb{R}} \sqrt{2} \triangleright (0, 0, 1)$ o współczynnikach π, e i $\sqrt{2}$.
- (4) W przestrzeni $\mathbb{R}$ -liniowej $C([0, 1], \mathbb{R})$ (patrz: Przykł. 35 (5)) wektor $\sinh$ jest kombinacją liniową $\frac{1}{2} \triangleright \exp + (-\frac{1}{2}) \triangleright \exp \circ \text{Inv}_{\mathbb{R}}$ o współczynnikach $\frac{1}{2}$ i $-\frac{1}{2}$.

✓

Bez trudu dowodzimy

STWIERDZENIE 75. *Przyjmijmy notację Def. 67, 21, 32, 61 oraz 68. Podzbiór*

$$\langle S \rangle_R := \left\{ \sum_{g \in S} r_g \triangleright g \mid \{r_g\}_{g \in S} \in \mathcal{R}_0(R) \right\} \subset G$$

jest podmodułem G . Jest to najmniejszy podmoduł G zawierający S . Określamy go mianem (pod)modułu generowanego (albo rozpinanego) przez zbiór S (albo inaczej powłoki liniowej zbioru S nad R czy wreszcie powłoki R -liniowej zbioru S), ten ostatni zaś nazywamy zbiorem generatorów (lub generującym) podmodułu $\langle S \rangle_R$.

indeksmoduł nad pierścieniem!zbiór generujący Jeśli $S = \{g\}$ (jest singletonem), to odnośny moduł oznaczamy przez $\langle S \rangle_R \equiv \langle g \rangle_R$ i nazywamy modułem cyklicznym. Moduł o skończonej liczbie generatorów, tj. taki, dla którego $|S| < \infty$, nosi miano modułu skończenie generowanego.

■

Dowód: Strukturę podgrupy na $\langle S \rangle_R$ określają operacje

$$\phi_2 : \langle S \rangle_R^{\times 2} \longrightarrow \langle S \rangle_R : \left(\sum_{g \in S} r_g \triangleright g, \sum_{g \in S} s_g \triangleright g \right) \longmapsto \sum_{g \in S} (r_g +_R s_g) \triangleright g,$$

$$\phi_1 : \langle S \rangle_R \longrightarrow \langle S \rangle_R : \sum_{g \in S} r_g \triangleright g \longmapsto \sum_{g \in S} (-r_g) \triangleright g$$

oraz

$$\phi_0 : \{\bullet\} \longrightarrow \langle S \rangle_R : \bullet \longmapsto \sum_{g \in S} 0_R \triangleright g = 0_G.$$

Działanie pierścienia R zadajemy wzorem

$$(8.1) \quad \lambda : R \times \langle S \rangle_R \longrightarrow \langle S \rangle_R : \left(r, \sum_{g \in S} r_g \triangleright g \right) \longmapsto \sum_{g \in S} (r \cdot_R r_g) \triangleright g.$$

□

PRZYKŁAD(Y) 38.

- (1) Podmoduł $\langle 0_G \rangle_R = \{0_G\}$ jest modulem trywialnym.
- (2) Moduł R z Przykł. 34 (2) jest powłoką liniową elementu neutralnego 1_R . Jest to zatem moduł cykliczny.
- (3) Podmoduł $\langle [2]_6 \rangle_{\mathbb{Z}} \subset \mathbb{Z}/6\mathbb{Z}$ to $\{[0]_6, [2]_6, [4]_6\} \cong \mathbb{Z}/3\mathbb{Z}$, natomiast powłoką $\mathbb{Z}$ -liniową singletonu $\{[5]_6\}$ jest cały moduł $\mathbb{Z}/6\mathbb{Z}$.
- (4) Powłoką liniową pary wektorów $v, w \in \mathbb{R}^3$ w przestrzeni wektorowej $\mathbb{R}^3$ nad $\mathbb{R}$ jest
 - płaszczyzna przechodząca przez $(0,0,0), v$ i w , gdy ta trójka jest niewspółliniowa – jest to przykład modułu skończenie generowanego niecyklicznego;
 - prosta przechodząca przez $(0,0,0), v$ i w , gdy ta trójka jest współliniowa, a przy tym $v \neq 0$ lub $w \neq 0$;
 - singleton $\{(0,0,0)\}$, gdy $v = (0,0,0) = w$.

✓

Kolejne istotne pojęcia zbiera

DEFINICJA 69. W notacji Def. 67, 21, 32, 61 oraz 68 rodzina $\{g_\lambda\}_{\lambda \in \Lambda}$ elementów modułu G jest **liniowo niezależna nad pierścieniem R** , indexliniowa niezależność jeśli spełnia warunek

$$\forall \{r_\lambda\}_{\lambda \in \Lambda} \in \mathcal{R}_0(R) : \left(\sum_{\lambda \in \Lambda} r_\lambda \triangleright g_\lambda = 0_G \implies \forall \lambda \in \Lambda : r_\lambda = 0_R \right).$$

Podzbiór $S \subset G$ nazywamy liniowo niezależnym nad pierścieniem R , indexpodzbiór liniowo niezależny jeśli jako rodzina elementów z R indeksowana przez S jest liniowo niezależny nad R , tj. jeśli znikanie dowolnej kombinacji liniowej $\sum_{g \in S} r_g \triangleright g = 0_G$ implikuje równość $r_g = 0_R$ dla każdego $g \in S$.

Rodzinę $\{g_\lambda\}_{\lambda \in \Lambda}$ (wzgl. podzbiór $S \subset G$) nazywamy **liniowo zależną(-nym)**, jeśli nie jest liniowo niezależna(-ny).

▲

Pojęcie liniowej niezależności charakteryzuje następujące

STWIERDZENIE 76. *Przyjmijmy notację Def. 67, 21, 32, 61 oraz 68. Jeśli podzbiór $S \subset G$ jest liniowo niezależny, to równość kombinacji liniowych jego elementów jest równoznaczna z równością ich współczynników, tj.*

$$\sum_{g \in S} r_g \triangleright g = \sum_{g \in S} s_g \triangleright g \iff \forall g \in S : r_g = s_g.$$

Ponadto jeśli $R = \mathbb{K}$ jest ciałem, to liniowa zależność S jest równoważna temu, że jeden z elementów S jest kombinacją liniową pozostałych.

■

Dowód: Zachodzi równoważność $\sum_{g \in S} r_g \triangleright g = \sum_{g \in S} s_g \triangleright g \iff \sum_{g \in S} (r_g +_R P(s_g)) \triangleright g = 0_G$, która wobec liniowej niezależności S daje pożądaną równość.

Liniowa zależność S w przypadku $R = \mathbb{K}$ jest równoważna istnieniu niezerowej rodziny skalarów $\{r_g\}_{g \in S}$ o skończonym nośniku, dla której $\sum_{g \in S} r_g \triangleright g = 0_G$. Niech $g \in S$ ma tę własność, że $r_g \neq 0_{\mathbb{K}}$, a wtedy otrzymujemy

$$g = -\text{Inv}_{\mathbb{K}}(r_g) \triangleright \sum_{h \in S \setminus \{g\}} r_h \triangleright h = \sum_{h \in S \setminus \{g\}} P_{\mathbb{K}}(\text{Inv}_{\mathbb{K}}(r_g) \cdot_{\mathbb{K}} r_h) \triangleright h,$$

co kończy dowód. $\square$

PRZYKŁAD(Y) 39.

- (1) W $\mathbb{Z}$ -module $\mathbb{Z}^{\times 2}$ z Przykł. 34(2) zbiór $\{(2,0), (3,0)\}$ jest liniowo zależny, bo

$$3 \triangleright (2,0) + (-2) \triangleright (3,0) = (0,0),$$

ale zarazem nie istnieje $n \in \mathbb{Z}$ o własności $(2,0) = n \triangleright (3,0)$. Jest to przykład modułu nad pierścieniem, w których równoważność z drugiej części Stw. 76 nie jest prawdziwa.

- (2) W $\mathbb{Z}$ -module $\mathbb{Z}/n\mathbb{Z}$ z Przykł. 34(5) dowolny singleton $\{[k]_n\}$ jest liniowo zależny, patrz: uwaga pod dowodem Stw. 68.
- (3) Wielomiany $3t^2 - t^0$ i $2t^2 - 7t^0$ tworzą podzbiór liniowo niezależny modułu $\mathbb{Z}[t]$ nad $\mathbb{Z}$.
- (4) W przestrzeni $\mathbb{R}$ -liniowej $\mathbb{R}^{\times 2}$ z Przykł. 35(2) zbiór $\{(2,7), (15,-2), (1,58)\}$ jest liniowo zależny.
- (5) W przestrzeni $\mathbb{R}$ -liniowej $C([0,\pi], \mathbb{R})$ (por. Przykł. 35(5)) zbiór $\{\sin, \cos\}$ jest liniowo niezależny.

✓

Dotychczasowe rozważania doprowadzają nas wprost do kluczowego pojęcia pozwalającego dokonać precyzyjnego jakościowego rozróżnienia pomiędzy ogólnymi modułami nad pierścieniem i przestrzeniami wektorowymi.

DEFINICJA 70. Przyjmijmy notację Def. 67, 21, 32, 61 i 68 oraz Stw. 75. Rodzinę $\{g_\lambda\}_{\lambda \in \Lambda}$ elementów modułu G nad pierścieniem R nazwiemy **bazą modułu** G ,

indexmoduł nad pierścieniem! baza jeśli jest ona niepusta, liniowo niezależna nad R i generuje G . Podzbiór $S \subset G$ o tych samych własnościach określimy w ten sam sposób.

Moduł wolny (na zbiorze $\mathcal{B}$) to moduł trywialny lub taki, który posiada bazę $\mathcal{B}$.

▲

PRZYKŁAD(Y) 40.

- (1) Element neutralny 1_R jest bazą modułu R z Przykł. 34(2).
- (2) Moduł $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N} \setminus \{0\}$ nad pierścieniem $\mathbb{Z}$, choć jest cykliczny, nie posiada bazy, albowiem nie istnieje w nim podzbiór liniowo niezależny, por. uwagę pod dowodem Stw. 68.
- (3) Rodzina elementów $\{e_i\}_{i \in \overline{1,n}}$, $e_i = (\delta_{i,j}^R)_{j \in \overline{1,n}}$, gdzie

$$\delta_{i,j}^R = \begin{cases} 1_R & \text{dla } j = i \\ 0_R & \text{dla } j \neq i \end{cases}$$

jest **symbolem Kroneckera** (zwanym też **delta Kroneckera**), jest **bazą standardową** modułu wolnego $R^{\times n}$ z Przykł. 34(2).

W przypadku pierścienia $R = \mathbb{K}$ o strukturze ciała ta sama rodzina elementów (wektorów) jest bazą standardową przestrzeni wektorowej $\mathbb{K}^{\times n}$ z Przykł. 35 (2). ✓

Definiującą charakterystykę bazy modułu podaje

STWIERDZENIE 77. *Przyjmijmy notację Def. 67, 21, 32, 61, 68 i 70 oraz Stw. 75.*

Podzbiór $\mathcal{B} \subset G$ jest bazą modułu G wtedy i tylko wtedy, gdy jest spełniony warunek

$$\forall_{g \in G} \exists! \{r_h\}_{h \in \mathcal{B}} \in \mathcal{R}_0(R) : g = \sum_{h \in \mathcal{B}} r_h \triangleright h,$$

tj. gdy każdy element modułu ma jednoznaczne przedstawienie w postaci kombinacji liniowej elementów tego podzbioru. ■

Dowód:

$\Rightarrow$ Niech $\mathcal{B}$ będzie bazą G . Wówczas każdy element ma pożądane przedstawienie, gdyż $\mathcal{B}$ jest zbiorem generującym. Jego liniowa niezależność gwarantuje – na mocy Stw. 76 – jednoznaczność takiego rozkładu.

$\Leftarrow$ Istnienie rozkładu oznacza, że $\mathcal{B}$ jest zbiorem generującym, jego jednoznaczność zaś implikuje liniową niezależność elementów bazy, albowiem

$$\sum_{h \in \mathcal{B}} r_h \triangleright h = 0_G = \sum_{h \in \mathcal{B}} 0_R \triangleright h$$

prowadzi do równości $r_h = 0_R$. □

Jak stwierdziliśmy wcześniej, moduł nad pierścieniem może nie posiadać bazy, por. Przykł. 40 (2). Odpowiedzi na pytanie o istnienie bazy w przypadku przestrzeni wektorowej (i tym samym naturalnego kryterium rozróżniającego te dwie struktury) dostarcza

TWIERDZENIE 8.5 (O istnieniu bazy przestrzeni wektorowej). *Przyjmijmy notację Def. 11, 67, 21, 32, 61, 63, 68 i 70 oraz Stw. 75 i załóżmy, że V jest nietrywialną przestrzenią wektorową. Jeśli Γ jest dowolnym zbiorem generatorów V nad $\mathbb{K}$, a S – pewnym liniowo niezależnym (nad $\mathbb{K}$) podzbiorem Γ , to wtedy istnieje w V baza $\mathcal{B}$ o własności $S \subset \mathcal{B} \subset \Gamma$.* ■

Dowód: Podstawą dowodu jest Lemat Kuratowskiego–Zorna, którego sformułowanie wymaga pewnego przygotowania. Zaczniemy od przypomnienia

DEFINICJA 71. Niechaj S będzie zbiorem. **Częściowy porządek** na S to relacja $\leq \subset S \times S$ o następujących własnościach

(PO1) (zwrotność) $\forall_{x \in S} : x \leq x$;

(PO2) (antysymetria) $\forall_{x, y \in S} : (x \leq y \wedge y \leq x) \implies x = y$;

(PO3) (przechodność) $\forall_{x,y,z \in S} : ((x \leq y \wedge y \leq z) \implies x \leq z)$.

Jeśli $x \leq y$, to mówimy, że y **jest późniejszy** niż x lub też że x **jest wcześniejszy** niż y . Zbiór, na którym został określony częściowy porządek, nazywamy **zbiorem częściowo uporządkowanym**.

Liniowy porządek na S to częściowy porządek spełniający dodatkowy aksjomat

(PO4) (totalność) $\forall_{x,y \in S} : (x \leq y \vee y \leq x)$,

tj. będący relacją totalną.

Podzbiór $c \subset S$ zbioru S z częściowym porządkiem $\leq$, który jest liniowo uporządkowany (względem $\leq$), określamy mianem **łańcucha** w S . **Ograniczenie górne** łańcucha $c \subset S$ to element $x \in S$ o własności

$$\forall_{y \in c} : y \leq x.$$

Zbiór łańcuchowo zupełny to zbiór częściowo uporządkowany, w którym każdy łańcuch ma ograniczenie górne. ▲

Przykładem częściowego porządku jest relacja $\subset$ (zawierania się) określona na zbiorze 2^S podzbiorów danego zbioru S . Ten właśnie przykład odegra istotną rolę poniżej.

Możemy już teraz wysłowić

TWIERDZENIE 8.6 (Lemat Kuratowskiego–Zorna). *W każdym niepustym zbiorze S łańcuchowo zupełnym istnieje element maksymalny m o własności definiującej*

$$\forall_{x \in S} : (m \leq x \implies x = m).$$

■

Dowód twierdzenia, który można znaleźć w pracy Kuratowskiego i Mostowskiego [KM76, Rozdz. VII § 8], wykorzystuje pewnik wyboru. Warto także przeczytać wersję dowodu przedstawioną w książce Langa [Lan02, Dod. 2].

Wracając do dowodu zasadniczego, rozważamy rodzinę zbiorów

$$\mathcal{R}(\Gamma|S) := \{ X \in 2^\Gamma \mid X \supset S \wedge X \text{ liniowo niezależny nad } \mathbb{K} \}$$

z częściowym porządkiem $\subset$. Rodzina ta jest niepusta, gdyż $S \in \mathcal{R}(\Gamma|S)$, a ponadto dla dowolnego łańcucha $\{X_\lambda\}_{\lambda \in \Lambda} \subset \mathcal{R}(\Gamma|S)$ podzbiorów $S \subset X_\lambda \subset \Gamma$ (Λ jest tutaj zbiorem indeksów) zachodzi $\bigcup_{\lambda \in \Lambda} X_\lambda \in \mathcal{R}(\Gamma|S)$, bowiem $\bigcup_{\lambda \in \Lambda} X_\lambda \supset X_\lambda \supset S$, a ponadto każda kombinacja liniowa nad $\mathbb{K}$

$$\mathcal{L}(\mu.) := \sum_{v \in \bigcup_{\lambda \in \Lambda} X_\lambda} \mu_v \triangleright v$$

jest zawarta w pewnym elemencie X_λ rodziny $\{X_\lambda\}_{\lambda \in \Lambda}$ z racji skończoności nośnika rodziny jej współczynników i wobec istnienia liniowego porządku $\subset$ na $\{X_\lambda\}_{\lambda \in \Lambda}$, a zatem

$$\mathcal{L}(\mu.) = 0_G \iff \forall_{v \in \bigcup_{\lambda \in \Lambda} X_\lambda} : \mu_v = 0_{\mathbb{K}}$$

w konsekwencji liniowej niezależności X_λ . Powyższa dyskusja pokazuje, że zbiór $\mathcal{R}(\Gamma|S)$ jest łańcuchowo zupełny, więc też – na mocy Tw. 8.6 – istnieje element maksymalny

$$S \subset \mathcal{B} \subset \Gamma, \quad \forall_{X \in 2^\Gamma} : X \subset \mathcal{B}.$$

Możemy teraz rozpatrzyć podprzestrzeń $\langle \mathcal{B} \rangle_{\mathbb{K}} \subset V$. Gdyby nie zachodziła tu równość, $\langle \mathcal{B} \rangle_{\mathbb{K}} \subsetneq V$, to wówczas musiałby istnieć generator $v \in \Gamma$ o własności $v \notin \langle \mathcal{B} \rangle_{\mathbb{K}}$, w przeciwnym bowiem razie każdy wektor $w \in V$ można byłoby rozpiąć na generatorach z powłoki $\mathcal{B}$, czyli byłoby $\forall_{w \in V} : w \in \langle \mathcal{B} \rangle_{\mathbb{K}}$. Skoro jednak $v \notin \langle \mathcal{B} \rangle_{\mathbb{K}}$, to $\mathcal{B} \cup \{v\} \supset \mathcal{B} \supset S$ jest liniowo niezależny, albowiem równość

$$\sum_{w \in \mathcal{B}} \mu_w \triangleright w +_G \mu_v \triangleright v = 0_V$$

implikuje $\mu_v = 0_{\mathbb{K}}$, bo w przeciwnym razie

$$v = \sum_{w \in \mathcal{B}} P_{\mathbb{K}}(\text{Inv}_{\mathbb{K}}(\mu_v) \cdot_{\mathbb{K}} \mu_w) \triangleright w \in \langle \mathcal{B} \rangle_{\mathbb{K}}.$$

Wtedy jednak dostajemy

$$\sum_{w \in \mathcal{B}} \mu_w \triangleright w = 0_V,$$

więc też koniecznie $\forall_{w \in \mathcal{B}} : \mu_w = 0_{\mathbb{K}}$ z uwagi na liniową niezależność $\mathcal{B}$. Koniec końców stwierdzamy, że

$$\mathcal{B} \subsetneq \mathcal{B} \cup \{v\} \in \mathcal{R}(\Gamma|S),$$

co przeczy maksymalności $\mathcal{B}$ w $\mathcal{R}(\Gamma|S)$. Napotkana sprzeczność pokazuje, że musi zachodzić równość $\langle \mathcal{B} \rangle_{\mathbb{K}} = V$, a nadto $\mathcal{B} \neq \emptyset$, gdyż $V \neq \{0_V\}$, skąd wniosek, że $\mathcal{B}$ jest bazą o pożądanych własnościach. $\square$

Należy podkreślić, że powyższe twierdzenie orzeka twierdząco o istnieniu bazy w *dowolnej* przestrzeni wektorowej – istotnie, każda przestrzeń V ma zbiór generujący, np. V . Przedstawiony jego dowód, jakkolwiek szalenie elegancki, nie niesie najskromniejszej nawet sugestii odnośnie do *konstrukcji* bazy przestrzeni wektorowej. W przypadku przestrzeni skończenie generowanej (tj. takiej, w której $|\Gamma| < \infty$) niezręczność tę usuwa konstruktywny dowód poniższego

STWIERDZENIE 78. (Lemat Steinitza o wymianie) *Dowolny podzbiór liniowo niezależny skończenie generowanej przestrzeni wektorowej V nad ciałem $\mathbb{K}$ ma moc mniejszą od mocy zbioru generującego lub jej równą, a ponadto można go uzupełnić do bazy tej przestrzeni wektorami ze zbioru generującego.*

■

Dowód: Niechaj $\Gamma := \{v_1, v_2, \dots, v_n\} \subset V$ będzie zbiorem generującym przestrzeni V i niech X będzie zbiorem liniowo niezależnym w V , przy czym zakładamy, że $V \neq \{0_V\}$. Wprowadźmy oznaczenie $m_X := |X|$.

Jeśli $m_X = 0$, to bazę $\mathcal{B}$ tworzymy z elementów Γ w następującej procedurze „lustracji”: posuwając się w kierunku wzrostu indeksu naturalnego i w zbiorze wektorów v_i odrzucamy każdy z wektorów, który jest kombinacją liniową poprzedników (w szczególności v_1 odrzucamy wtedy i tylko wtedy, gdy jest wektorem zerowym). Uzyskany tym sposobem podzbiór $\{v_{i_1}, v_{i_2}, \dots, v_{i_m}\} \subset \Gamma$ jest (niepustym) zbiorem generującym V , a zarazem – wprost z konstrukcji – jest liniowo niezależny, czyli jest bazą.

Załóżmy dalej, że $0 < m_X \leq n$, przy czym $X = \{x_1, x_2, \dots, x_{m_X}\}$. Skoro Γ jest zbiorem generującym, to istnieje taka rodzina skalarów $\{\lambda_i\}_{i=1, n} \subset \mathbb{K}$, która zadaje

rozkład

$$x_1 = \sum_{i=1}^n \lambda_i \triangleright v_i.$$

Zauważmy, że rodzina ta musi mieć $\text{supp}\{\lambda_i\}_{i=\overline{1,n}} > 0$, w przeciwnym bowiem razie $x_1 = 0$, a wtedy X nie może być liniowo niezależny (bo np. nietrywialna kombinacja liniowa $1_K \triangleright x_1 +_V \sum_{j=2}^{m_X} 0_K \triangleright x_j = 0_V$ zadaje rozkład 0_V). Dokonując stosownej permutacji indeksów rodziny Γ , możemy doprowadzić do tego, by $\lambda_1 \neq 0_K$, a wtedy

$$v_1 = \lambda_1^{-1} \triangleright x_1 +_V \sum_{j=2}^n (-\lambda_1^{-1} \cdot_K \lambda_j) \triangleright v_j,$$

co oznacza, że zbiór $\Gamma^{(1)} := \{x_1\} \cup \{v_2, v_3, \dots, v_n\}$ jest zbiorem generującym V . W takim razie istnieje rodzina skalarów $\{\mu_i\}_{i=\overline{1,n}}$ o niepustym nośniku, która zadaje rozkład

$$x_2 = \mu_1 \triangleright x_1 +_V \sum_{j=2}^n \mu_j \triangleright v_j,$$

przy czym musi istnieć indeks $j > 1$ o własności $\mu_j \neq 0_K$, bo inaczej $x_2 \in \langle x_1 \rangle_K$, co przeczy liniowej niezależności X . Przeindeksowując $\{v_2, v_3, \dots, v_n\}$ odpowiednio, doprowadzamy do tego, by było $\mu_2 \neq 0_K$, a wtedy

$$v_2 = (-\mu_2^{-1} \cdot_K \mu_1) \triangleright x_1 +_V \mu_2^{-1} \triangleright x_2 +_V \sum_{j=3}^n (-\mu_2^{-1} \cdot_K \mu_j) \triangleright v_j,$$

czyli też $\Gamma^{(2)} := \{x_1, x_2\} \cup \{v_3, v_4, \dots, v_n\}$ jest zbiorem generującym V . Zastosowawszy tę procedurę m_X razy, otrzymujemy zbiór generujący $\Gamma^{(m_X)} := X \cup \{v_{m_X+1}, v_{m_X+2}, \dots, v_n\}$, przy czym drugi człon sumy jest pusty, gdy $m_X = n$. Oznaczmy

$$u_i := \begin{cases} x_i & \text{dla } 1 \leq i \leq m_X \\ v_i & \text{dla } m_X + 1 \leq i \leq n \end{cases}.$$

„Lustracja” $\Gamma^{(m_X)} \equiv \{u_i\}_{i \in \overline{1,n}}$ wedle opisanego wcześniej schematu nie eliminuje żadnego z elementów $X \subset \Gamma^{(m_X)}$ (z racji liniowej niezależności X), a zatem daje nam bazę V będącą rozszerzeniem X , zgodnie z tezą stwierdzenia.

Jeśli $m_X > n$, to wybierając z X dowolny podzbiór Y o mocy n i stosując do niego powyższe rozumowanie doprowadzamy do zastąpienia wszystkich generatorów z Γ wektorami z Y , co czyni z Y zbiór generujący V . W konsekwencji dowolny wektor $x \in X \setminus Y \neq \emptyset$ jest kombinacją liniową wektorów z Y , co przeczy liniowej niezależności X . Sprzeczność ta dowodzi tej składowej tezy, która orzeka, że $m_X \leq n$, i tym samym zamyka dowód. $\square$

Tę część wykładu zakończymy podsumowaniem własności bazy modułu wolnego.

STWIERDZENIE 79. Def. 67, 21, 32, 61, 68 i 70 oraz Stw. 75. W dowolnym module G nad pierścieniem R poniższe zdania

- (i) $\mathcal{B}$ jest bazą G .
- (ii) $\mathcal{B}$ jest maksymalnym (w sensie $\subset$) podzbiorem liniowo niezależnym G .
- (iii) $\mathcal{B}$ jest minimalnym (w sensie $\subset$) podzbiorem generującym G .

pozostają w relacji

$$(i) \implies (ii) \quad (BL)$$

oraz

$$(i) \implies (iii). \quad (BG)$$

Jeśli $R = \mathbb{K}$ jest ciałem, to także

$$(ii) \implies (i) \quad (K-LB)$$

oraz

$$(iii) \implies (i). \quad (K-GB)$$

■

Dowód:

- (BL) Baza jest z definicji zbiorem liniowo niezależnym, wystarczy zatem wykazać jego maksymalność. W tym celu rozważmy dowolny element $g \in G \setminus \mathcal{B}$. Skoro $G = \langle \mathcal{B} \rangle_R$, to istnieje $\{r_h\}_{h \in \mathcal{B}} \in \mathcal{R}_0(R)$ o własności $\sum_{h \in \mathcal{B}} r_h \triangleright h = g$, a zatem

$$P_R(1) \triangleright g +_G \sum_{h \in \mathcal{B}} r_h \triangleright h = 0_G,$$

skąd wniosek, że $\mathcal{B} \cup \{g\} \not\subseteq \mathcal{B}$ jest zbiorem liniowo zależnym.

- (BG) Baza jest z definicji zbiorem generującym, pozostaje więc udowodnić jego minimalność. Niech $g \in \mathcal{B}$ i rozważmy $\mathcal{B}' := \mathcal{B} \setminus \{g\}$. Gdyby było $\langle \mathcal{B}' \rangle_R = G$, wówczas w szczególności istniałaby rodzina $\{r_h\}_{h \in \mathcal{B}'} \in \mathcal{R}_0(R)$ o własności $\sum_{h \in \mathcal{B}'} r_h \triangleright h = g$, a wtedy mielibyśmy równość

$$P_R(1) \triangleright g +_G \sum_{h \in \mathcal{B}'} r_h \triangleright h = 0_G,$$

która przeczy liniowej niezależności $\mathcal{B}$.

- (K-LB) Załóżmy, że $\langle \mathcal{B} \rangle_{\mathbb{K}} \neq G$, czyli istnieje $g \in G \setminus \langle \mathcal{B} \rangle_{\mathbb{K}}$. Wówczas zbiór $\mathcal{B}' := \mathcal{B} \cup \{g\} \not\subseteq \mathcal{B}$ jest liniowo niezależny, gdyby bowiem $\sum_{h \in \mathcal{B}'} r_h \triangleright h = 0_G$ dla pewnej niezerowej rodziny $\{r_h\}_{h \in \mathcal{B}'} \in \mathcal{R}_0(\mathbb{K})$, to musiałoby być $g \in \text{supp} \{r_h\}_{h \in \mathcal{B}'}$ (z racji liniowej niezależności $\mathcal{B}$), a wtedy dostalibyśmy

$$g = \sum_{h \in \mathcal{B}} (-r_g^{-1} \cdot_{\mathbb{K}} r_h) \triangleright h \in \langle \mathcal{B} \rangle_{\mathbb{K}},$$

co nie jest prawdą. Jednakowoż liniowa niezależność $\mathcal{B}'$ leży w sprzeczności z założeniem o maksymalności $\mathcal{B}$.

- (K-GB) Przyjmijmy, że $\mathcal{B}$ jest liniowo zależny, czyli $\sum_{g \in \mathcal{B}} r_g \triangleright g = 0_G$ dla pewnej niezerowej rodziny $\{r_g\}_{g \in \mathcal{B}} \in \mathcal{R}_0(\mathbb{K})$. Niech $g \in \mathcal{B}$ ma własność $r_g \neq 0_R$, a wtedy, zdefiniowawszy $\mathcal{B}' := \mathcal{B} \setminus \{g\}$, otrzymujemy

$$g = \sum_{h \in \mathcal{B}'} (-r_g^{-1} \cdot_{\mathbb{K}} r_h) \triangleright h \in \langle \mathcal{B}' \rangle_{\mathbb{K}},$$

czyli $\mathcal{B}' \subsetneq \mathcal{B}$ generuje G , co przeczy minimalności $\mathcal{B}$.

□

Przykładem modułu nad pierścieniem, w którym nie jest spełnione wynikanie (K-LB) jest kanoniczny $\mathbb{Z}$ -moduł $\mathbb{Z}$ (patrz: Przykł. 34 (2)), w którym podzbiór $\{2\}$

jest w oczywisty sposób maksymalnym zbiorem liniowo niezależnym, ale nie generuje całego modułu (bo np. $1 \notin \langle 2 \rangle_{\mathbb{Z}}$). Zdanie (K-GB) traci słusność np. w przypadku $\mathbb{Z}$ -modułu $\mathbb{Z}/n\mathbb{Z}$ (patrz: Przykł. 34 (5)), w którym minimalny zbiór generujący $\{\{1\}_n\}$ nie jest liniowo niezależny (patrz: uwaga pod dowodem Stw. 68).

Chwila zastanowienia pozwala stwierdzić, że wybór bazy – ilekroć jest możliwy – nie jest w ogólności jednoznaczny. Pozostaje jednak intuicyjne pytanie o istnienie niezmiennika takiego wyboru określonego jako moc dowolnego podzbioru bazowego. Do sformułowania pierwszej odpowiedzi w tym kontekście prowadzi nas

STWIERDZENIE 80. *Przyjmijmy notację Def. 67, 21, 32, 61, 65, 68 i 70 oraz Stw. 75. Niechaj $\Lambda \neq \emptyset$ będzie zbiorem (indeksów) i niech rodzina $\mathcal{B}^{(1)} := \{g_\lambda^{(1)}\}_{\lambda \in \Lambda} \subset G^{(1)}$ będzie bazą modułu $G^{(1)}$. Dla dowolnej rodziny $\{g_\lambda^{(2)}\}_{\lambda \in \Lambda} \subset G^{(2)}$ istnieje jedyny homomorfizm R -modułów*

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

o własności

$$(8.2) \quad \forall_{\lambda \in \Lambda} : \chi(g_\lambda^{(1)}) = g_\lambda^{(2)}.$$

■

Dowód: Jest jasne, że rzeczony homomorfizm – o ile istnieje – jest określony jednoznacznie przez warunek (8.2). Istotnie, niech $\tilde{\chi}$ będzie dowolnym innym takim homomorfizmem, a wtedy dla dowolnego $g \in G^{(1)}$, o rozkładzie w bazie $\mathcal{B}^{(1)}$ danym wzorem $g = \sum_{\lambda \in \Lambda} r_\lambda \triangleright_{(1)} g_\lambda^{(1)}$ dla pewnej rodziny $\{r_\lambda\}_{\lambda \in \Lambda} \in \mathcal{R}_0(R)$, zachodzi równość

$$\begin{aligned} \tilde{\chi}(g) &= \sum_{\lambda \in \Lambda} \tilde{\chi}(r_\lambda \triangleright_{(1)} g_\lambda^{(1)}) = \sum_{\lambda \in \Lambda} r_\lambda \triangleright_{(2)} \tilde{\chi}(g_\lambda^{(1)}) = \sum_{\lambda \in \Lambda} r_\lambda \triangleright_{(2)} g_\lambda^{(2)} \\ &= \sum_{\lambda \in \Lambda} r_\lambda \triangleright_{(2)} \chi(g_\lambda^{(1)}) = \chi(g), \end{aligned}$$

przy czym skorzystaliśmy z tego, że suma występująca powyżej jest skończona, $\tilde{\chi}$ i χ zaś są odwzorowaniami R -liniowymi. Wnioskujemy zatem, że koniecznie $\tilde{\chi} = \chi$. Pozostaje więc wskazać χ . Postulujemy, dla $g \in G^{(1)}$ (dowolnego) jak wyżej,

$$\chi(g) := \sum_{\lambda \in \Lambda} r_\lambda \triangleright_{(2)} g_\lambda^{(2)}.$$

Definicja ta spełnia założenia stwierdzenia, oto bowiem

$$\begin{aligned} \chi(g_\lambda^{(1)}) &= \chi \left(1_R \triangleright_{(1)} g_\lambda^{(1)} +_{(1)} \sum_{\mu \in \Lambda \setminus \{\lambda\}} 0_R \triangleright_{(1)} g_\mu^{(1)} \right) \\ &= 1_R \triangleright_{(2)} g_\lambda^{(2)} +_{(2)} \sum_{\mu \in \Lambda \setminus \{\lambda\}} 0_R \triangleright_{(2)} g_\mu^{(2)} = 1_R \triangleright_{(2)} g_\lambda^{(2)} \\ &= g_\lambda^{(2)}, \end{aligned}$$

a przy tym χ jest oczywiście homomorfizmem R -modułów, gdyż – dla dowolnego $r \in R$ –

$$\chi(r \triangleright_{(1)} g) := \sum_{\lambda \in \Lambda} (r \cdot_R r_\lambda) \triangleright_{(2)} g_\lambda^{(2)} = r \triangleright_{(2)} \sum_{\lambda \in \Lambda} r_\lambda \triangleright_{(2)} g_\lambda^{(2)} = r \triangleright_{(2)} \chi(g),$$

patrz: (8.1). □

Powyższe stwierdzenie można wysłowić w sposób przemawiający do wyobraźni bardziej bezpośrednio: Oto każde odwzorowanie R -liniowe $\chi : G^{(1)} \rightarrow G^{(2)}$ jest jednoznacznie zadane przez wartości, jakie przyjmuje na elementach bazy $\mathcal{B}$ swej dziedziny, a zarazem dowolne odwzorowanie $\mathcal{B} \rightarrow G^{(2)}$ można rozszerzyć do odwzorowania R -liniowego o dziedzinie $G^{(1)} \supset \mathcal{B}$.

Jako istotny wniosek z tego stwierdzenia wyprowadzamy

COROLLARIUM 10. *W notacji Def. 67, 21, 32, 61 i 65 oraz Stw. 80 χ jest izomorfizmem R -modułów, jeśli rodzina $\{g_\lambda^{(2)}\}_{\lambda \in \Lambda}$ jest bazą modułu $G^{(2)}$.* ■

Dowód: Z symetrii zagadnienia wynika – na mocy ostatniego stwierdzenia – istnienie jedyne odwzorowania R -liniowego $\psi : G^{(2)} \rightarrow G^{(1)}$ o własności $\forall_{\lambda \in \Lambda} : \psi(g_\lambda^{(2)}) = g_\lambda^{(1)}$, które – jak łatwo widać – jest (obustronną) odwrotnością χ . □

Stąd też oczywiste

COROLLARIUM 11. *Dowolne dwa moduły nad tym samym pierścieniem mające bazy jednakowej mocy są izomorficzne.* ■

Powyższa analiza skłania do postawienia pytania o słuszność implikacji odwrotnej. Odpowiedź dla przypadku modułu nieskończenie generowanego zawiera

STWIERDZENIE 81. *Przyjmijmy notację Def. 21, 32 oraz 61 i niech Γ_0 będzie minimalnym podzbiorem generującym R -modułu G , przy czym zakładamy, że moc $|\Gamma_0| =: \kappa_0$ jest nieskończona (κ_0 jest stosowną liczbą kardynalną). Każdy podzbiór generujący G ma moc nie mniejszą niż κ_0 . W szczególności G nie jest skończenie generowany. Ponadto dowolne dwa minimalne zbiory generujące mają jednaką moc.* ■

Dowód: Niech Γ będzie dowolnym podzbiorem generującym G , o mocy $\kappa := |\Gamma|$. Dowolny element $g \in \Gamma$ jest kombinacją liniową (skończonej liczby elementów) Γ_0 , tj. $g \in \langle \Gamma_g \rangle_R$ dla pewnego skończonego podzbioru $\Gamma_g \subset \Gamma_0$. Prawdziwa jest równość

$$\Gamma_0 = \bigcup_{g \in \Gamma} \Gamma_g.$$

Istotnie, $U := \bigcup_{g \in \Gamma} \Gamma_g \subset \Gamma_0$, co wynika wprost z definicji, a przy tym $\langle U \rangle_R$ jest podmodułem zawierającym Γ , a zatem równym G (jako zbiór zamknięty ze względu na branie kombinacji liniowych i zarazem zawierający podzbiór generujący). Jest przeto U podzbiorem generującym G zawartym w Γ_0 , co wobec minimalności Γ_0 oznacza równość $U = \Gamma_0$. W jej konsekwencji skończona moc Γ oznaczałaby, że Γ_0 – będąc skończoną sumą mnogościową zbiorów o skończonej mocy – także jest skończony, co przeczy założeniom. Stąd wniosek, że koniecznie Γ jest nieskończony, co pozwala wykorzystać

LEMAT 8.7. *Niechaj κ_1 i κ_2 będą liczbami kardynalnymi, z których przynajmniej jedna jest nieskończona. Wówczas*

$$\kappa_1 \cdot \kappa_2 = \sup(\kappa_1, \kappa_2),$$

przy czym lewa strona określa moc iloczynu kartezjańskiego dowolnych zbiorów o mocach κ_1 i κ_2 , odpowiednio. ■

Dowód powyższego prawa arytmetyki liczb kardynalnych można znaleźć np. w [Bou06, Rozdz. III § 6.3] (patrz: Cor. 4 *ib.*), a pozwala nam ono zapisać nierówność

$$\kappa_0 = |\Gamma_0| \leq \sum_{g \in \Gamma} |\Gamma_g| \leq \aleph_0 \cdot \sum_{g \in \Gamma} 1 = \aleph_0 \cdot \kappa = \sup(\aleph_0, \kappa) = \kappa,$$

która pokazuje, że moc dowolnego zbioru generującego majoryzuje κ_0 . Jeśli przy tym także Γ jest minimalny, to na zasadzie symetrii możemy orzec, że $\kappa \leq \kappa_0$, skąd – w tym przypadku – równość $\kappa = \kappa_0$. □

Okazuje się, że równoliczność dowolnych dwóch baz modułu nad pierścieniem nie jest cechą uniwersalną. Ta konstatacja uzasadnia

DEFINICJA 72. Pierścień o cesze IBN⁵ R to taki, dla którego każde dwie bazy dowolnego modułu (wolnego) G nad tymże pierścieniem mają tę samą moc. Tę ostatnią określamy wtedy mianem **rzędu modułu** i oznaczamy symbolem $\text{rk}_R G$. ▲

Brak cechy IBN jest uznawany za patologię w kategorii pierścieni, są jednak znane przykłady struktur tego rodzaju, a nawet całe ich rodziny, patrz: prace Leavitt(-Forgettita) [Lea56, Lea57]. Określoność rzędu jest kolejną cechą wyróżniającą przestrzenie wektorowe spośród modułów. Oto bowiem zachodzi

TWIERDZENIE 8.8 (O wymiarze przestrzeni wektorowej). *Dowolne ciało ma cechę IBN, tj. dowolna przestrzeń wektorowa ma dobrze określony rząd.* ■

Dowód: Zaczniemy od tego, że na mocy Tw. 8.5 każda przestrzeń wektorowa jest modulem wolnym, możemy zatem mówić o jej bazie. Przy tym w świetle Stw. 79 każdy minimalny podzbiór generujący przestrzeni wektorowej jest jej bazą, więc udowodnione wcześniej Stw. 81 zapewnia słuszność tezy twierdzenia w przypadku przestrzeni nieskończenie generowanej. Pozostaje zająć się przypadkiem skończonym. Niech $\mathcal{B}$ będzie bazą o mocy $n < \infty$. Jak orzeka Stw. 78, dowolny zbiór Γ liniowo niezależny ma moc $m \leq n$, jeśli do tego Γ jest bazą, to – przez symetrię – także $n \leq m$, czyli ostatecznie $m = n$. □

Powyższy wynik uzasadnia

DEFINICJA 73. Przyjmijmy notację Def. 11, 32, 61 oraz 72. Rząd przestrzeni wektorowej V nad ciałem $\mathbb{K}$ określamy mianem **wymiaru ($\mathbb{K}$ -liniowego)** tej przestrzeni i oznaczamy symbolem

$$\dim_{\mathbb{K}} V := \text{rk}_{\mathbb{K}} V.$$

⁵Z jęz. ang., w którym akronim IBN pochodzi od wyrażenia „Invariant Basis Number”, które w wolnym tłumaczeniu oznacza „niezmienniczą moc bazy”.



Wprowadzony niezmiennik jest stały na klasach izomorfizmu przestrzeni wektorowych.

STWIERDZENIE 82. *Izomorficzne przestrzenie wektorowe mają ten sam wymiar.*



Dowód: Niechaj $V^{(\alpha)}$, $\alpha \in \{1, 2\}$ będą parą przestrzeni wektorowych nad ciałem $\mathbb{K}$ i niech odwzorowanie $\mathbb{K}$ -liniowe $\chi : V^{(1)} \rightarrow V^{(2)}$ będzie izomorfizmem (przestrzeni wektorowych). Wybierzmy bazę $\mathcal{B}^{(1)} := \{v_\lambda^{(1)}\}_{\lambda \in \Lambda}$ przestrzeni $V^{(1)}$ i zdefiniujmy rodzinę $\mathcal{B}^{(2)} := \{v_{\lambda \in \Lambda}^{(2)}\}_{\lambda \in \Lambda}$ wektorów z $V^{(2)}$, jak następuje:

$$\forall_{\lambda \in \Lambda} : v_\lambda^{(2)} := \chi(v_\lambda^{(1)}).$$

Pokażemy, że $\mathcal{B}^{(2)}$ jest bazą przestrzeni $V^{(2)}$. Po pierwsze zbiór ten jest koniecznie niepusty, bo cechę tę ma $\mathcal{B}^{(1)}$. Po drugie jest on zbiorem generującym $V^{(2)}$, oto bowiem dowolny wektor v z tej przestrzeni można zapisać w postaci $v = \chi(w)$ dla pewnego $w \in V^{(1)}$, ten ostatni zaś możemy przedstawić w postaci $w = \sum_{\lambda \in \Lambda} \mu_\lambda \triangleright_{(1)} v_\lambda^{(1)}$ dla pewnej rodziny $\{\mu_\lambda\}_{\lambda \in \Lambda} \in \mathcal{R}_0(\mathbb{K})$, a wtedy stwierdzamy, że

$$v = \chi\left(\sum_{\lambda \in \Lambda} \mu_\lambda \triangleright_{(1)} v_\lambda^{(1)}\right) = \sum_{\lambda \in \Lambda} \mu_\lambda \triangleright_{(2)} v_\lambda^{(2)}.$$

Łatwo też widzieć, że $\mathcal{B}^{(2)}$ jest zbiorem liniowo niezależnym, gdyż

$$\begin{aligned} \sum_{\lambda \in \Lambda} \mu_\lambda \triangleright_{(2)} v_\lambda^{(2)} = 0_{(2)} &\iff \sum_{\lambda \in \Lambda} \mu_\lambda \triangleright_{(1)} v_\lambda^{(1)} = \chi^{-1}\left(\sum_{\lambda \in \Lambda} \mu_\lambda \triangleright_{(2)} v_\lambda^{(2)}\right) = 0_{(1)} \\ &\iff \forall_{\lambda \in \Lambda} : \mu_\lambda = 0_{\mathbb{K}}. \end{aligned}$$



Ma on też (intuicyjnie) oczekiwaną cechę monotoniczności

STWIERDZENIE 83 (Bilans wymiarów). *Przyjmijmy notację Def. 11, 32, 61, 65 i 73. Niechaj V będzie przestrzenią wektorową nad ciałem $\mathbb{K}$ i niech $W \subset V$ będzie jej podprzestrzenią. Wówczas*

$$\dim_{\mathbb{K}} V = \dim_{\mathbb{K}} W + \dim_{\mathbb{K}} V/W.$$

W szczególności więc

$$\dim_{\mathbb{K}} W \leq \dim_{\mathbb{K}} V,$$

przy czym ilekroć $\dim_{\mathbb{K}} V < \infty$, równość zachodzi wtedy i tylko wtedy, gdy $W = V$.

Ogólniej, niech $\chi : V^{(1)} \rightarrow V^{(2)}$ będzie odwzorowaniem $\mathbb{K}$ -liniowym, a wtedy

$$\dim_{\mathbb{K}} V^{(1)} = \dim_{\mathbb{K}} \text{Ker } \chi + \dim_{\mathbb{K}} \text{Im } \chi.$$



Dowód: Wynikanie pierwszej równości (więc też i nierówności) z drugiej jest oczywistą konsekwencją istnienia normalnego ciągu dokładnego dla dowolnej podprzestrzeni $W \subset V$ (będącej automatycznie dzielnikiem normalnym przestrzeni V),

$$(8.3) \quad \mathbf{0} \longrightarrow W \xrightarrow{j_W} V \xrightarrow{\pi_{V/W}} V/W \longrightarrow \mathbf{0},$$

które implikuje

$$\begin{aligned} \dim_{\mathbb{K}} V &= \dim_{\mathbb{K}} \operatorname{Ker} \pi_{V/W} + \dim_{\mathbb{K}} \operatorname{Im} \pi_{V/W} = \dim_{\mathbb{K}} \operatorname{Im} j_W + \dim_{\mathbb{K}} \operatorname{Im} \pi_{V/W} \\ &\equiv \dim_{\mathbb{K}} W + \dim_{\mathbb{K}} V/W. \end{aligned}$$

W przypadku ogólnym oznaczmy jako $\{v_\lambda^{(2)}\}_{\lambda \in \Lambda^{(2)}}$ bazę podprzestrzeni $\operatorname{Im} \chi \subset V^{(2)}$ i jako $\{v_\nu^{(1)}\}_{\nu \in \Lambda^{(1)}}$ bazę podprzestrzeni $\operatorname{Ker} \chi \subset V^{(1)}$. Niech też $\{v_\lambda\}_{\lambda \in \Lambda^{(2)}}$ będzie podzbiorem $V^{(1)}$ określonym przez warunki

$$\forall_{\lambda \in \Lambda^{(2)}} : \chi(v_\lambda) = v_\lambda^{(2)}.$$

Twierdzimy, że zbiór $\Gamma^{(1)} := \{v_\lambda\}_{\lambda \in \Lambda^{(2)}} \cup \{v_\nu^{(1)}\}_{\nu \in \Lambda^{(1)}}$ jest bazą $V^{(1)}$. Istotnie, weźmy dowolny $v \in V^{(1)}$, a wtedy $\chi(v) \in \operatorname{Im} \chi$ możemy przedstawić jednoznacznie jako kombinację liniową elementów bazy

$$\chi(v) = \sum_{\lambda \in \Lambda^{(2)}} \mu_\lambda \triangleright_{(2)} v_\lambda^{(2)}$$

o współczynnikach z pewnej rodziny $\{\mu_\lambda\}_{\lambda \in \Lambda^{(2)}} \in \mathcal{R}_0(\mathbb{K})$, czyli

$$\chi(v) = \sum_{\lambda \in \Lambda^{(2)}} \mu_\lambda \triangleright_{(2)} \chi(v_\lambda) = \chi \left(\sum_{\lambda \in \Lambda^{(2)}} \mu_\lambda \triangleright_{(1)} v_\lambda \right),$$

skąd wniosek, że

$$v +_{(1)} \sum_{\lambda \in \Lambda^{(2)}} (-\mu_\lambda) \triangleright_{(1)} v_\lambda \in \operatorname{Ker} \chi,$$

a zatem istnieje jednoznaczny rozkład

$$v +_{(1)} \sum_{\lambda \in \Lambda^{(2)}} (-\mu_\lambda) \triangleright_{(1)} v_\lambda = \sum_{\nu \in \Lambda^{(1)}} \zeta_\nu \triangleright_{(1)} v_\nu^{(1)}$$

dla pewnej rodziny $\{\zeta_\nu\}_{\nu \in \Lambda^{(1)}} \in \mathcal{R}_0(\mathbb{K})$. Przepisawszy powyższą równość w postaci

$$v = \sum_{\lambda \in \Lambda^{(2)}} \mu_\lambda \triangleright_{(1)} v_\lambda +_{(1)} \sum_{\nu \in \Lambda^{(1)}} \zeta_\nu \triangleright_{(1)} v_\nu^{(1)},$$

stwierdzamy, iż – w rzeczy samej – $\Gamma^{(1)}$ jest podzbiorem generującym $V^{(1)}$. Pozostaje pokazać, że jest on liniowo niezależny. W tym celu rozważmy rozkład

$$0_{(1)} = \sum_{\lambda \in \Lambda^{(2)}} \mu_\lambda \triangleright_{(1)} v_\lambda +_{(1)} \sum_{\nu \in \Lambda^{(1)}} \zeta_\nu \triangleright_{(1)} v_\nu^{(1)}.$$

Przykładając χ do obu stron równości, otrzymujemy równość pochodną

$$0_{(2)} = \chi(0_{(1)}) = \sum_{\lambda \in \Lambda^{(2)}} \mu_\lambda \triangleright_{(2)} \chi(v_\lambda) +_{(2)} \sum_{\nu \in \Lambda^{(1)}} \zeta_\nu \triangleright_{(2)} \chi(v_\nu^{(1)}) = \sum_{\lambda \in \Lambda^{(2)}} \mu_\lambda \triangleright_{(2)} v_\lambda^{(2)},$$

która implikuje

$$\forall_{\lambda \in \Lambda^{(2)}} : \mu_\lambda = 0_{\mathbb{K}}$$

wobec liniowej niezależności $\{v_\lambda^{(2)}\}_{\lambda \in \Lambda^{(2)}}$. Jest zatem także

$$0_{(1)} = \sum_{\nu \in \Lambda^{(1)}} \zeta_\nu \triangleright_{(1)} v_\nu^{(1)},$$

co oznacza, że

$$\forall_{\nu \in \Lambda^{(1)}} : \zeta_\nu = 0_{\mathbb{K}}$$

z racji liniowej niezależności $\{v_\nu^{(1)}\}_{\nu \in \Lambda^{(1)}}$. Na mocy Stw. 79 $\Gamma^{(1)}$ jest zatem bazą $V^{(1)}$ i zachodzi równość

$$\dim_{\mathbb{K}} V = |\Lambda^{(1)}| + |\Lambda^{(2)}| = \dim_{\mathbb{K}} \text{Ker } \chi + \dim_{\mathbb{K}} \text{Im } \chi.$$

□

Wprowadzamy

DEFINICJA 74. Przyjmijmy notację Def. 11, 32, 61, 72 oraz 73. **Kowymiar podprzestrzeni** $W \subset V$ przestrzeni wektorowej V nad ciałem $\mathbb{K}$ to liczba

$$\text{codim}_{\mathbb{K}}^{(V)} W := \dim_{\mathbb{K}} (V/W).$$

Podprzestrzeń kowymiaru 1 określamy mianem **hiperpłaszczyzny**.

▲

8.4. Produkt i suma prosta modułów jako struktury uniwersalne

Po omówieniu podstawowych aspektów „anatomii” modułu nad pierścieniem, ze szczególnym uwzględnieniem specyfiki przestrzeni wektorowych nad ciałem, przejdziemy obecnie do dyskusji rozmaitych naturalnych operacji na modułach takich jak produkt, suma prosta oraz iloczyn tensorowy. Uważny Czytelnik dostrzeże z łatwością strukturalne związki między tymi operacjami (szczególniej: dwiema pierwszymi) a rozpatrywanymi wcześniej konstrukcjami iloczynu rozłącznego oraz iloczynu prostego grup. Jako miarę naturalności przedstawianych konstrukcji, pozwalającą uniknąć konieczności uzasadniania rozważań nad nimi *a posteriori*, w odwołaniu do konkretnych sytuacji o znaczeniu matematycznym lub fizycznym, w których występują i odgrywają znaczącą rolę, przyjmijmy ich uniwersalność – definicję tego konstruktu, przykrojoną do ram niniejszego kursu, podajemy poniżej. Godzi się zawczasu podkreślić istotną jego cechę swoistą: oto wyróżnia on nośnik struktury określonego rodzaju (np. moduł nad pierścieniem) poprzez precyzyjne scharakteryzowanie jego własności względem odwzorowań transportujących ową strukturę (np. homomorfizmów modułów). Ten schemat myślenia o obiektach, nie tylko zresztą algebraicznych, jest konkretną realizacją pewnej głębszej idei opisu bytów matematycznych, jaką jest teoria kategorii⁶ [ML71], przedstawiająca rzeczony schemat nad szczegółową specyfikacją i jawną rekonstrukcją struktury wewnętrznej bytów opisywanych.

⁶Warto przy tej okazji wspomnieć, że teoria ta, współtworzona od podstaw przez wychowanka Uniwersytetu Warszawskiego i późniejszego aktywnego bourbakistę Samuela Eilenberga (wraz z Saundersem Mac Lanem) na gruncie – m.in. – rezultatów erlangenckiego programu Kleina opisu geometrii oraz fundamentalnych studiów Noether, Tannaki, Kreina i wielu innych nad związkami między strukturami algebraicznymi i klasami ich realizacji, stanowi – obok logiki, teorii mnogości, teorii przestrzeni Banacha i tzw. przestrzeni polskich, jak również algebry homologicznej – oryginalny a przy tym wysoce niebanalny przyczynek Polskiej Szkoły Matematycznej do rozwoju matematyki nowoczesnej.

DEFINICJA 75. Przyjmijmy notację Def. 2, 10 oraz 67 i ustalmy rodzinę $\mathcal{S} := \{\mathcal{S}^{(\lambda)}\}_{\lambda \in \Lambda}$ struktur algebraicznych tego samego rodzaju $\mathfrak{R}$,

$$\mathcal{S}^{(\lambda)} := (S^{(\lambda)}, \phi_{k_1}^{(\lambda)}, \phi_{k_2}^{(\lambda)}, \dots, \phi_{k_N}^{(\lambda)}),$$

oznaczając przy tym $S := \{S^{(\lambda)}\}_{\lambda \in \Lambda}$.

Rozważmy najpierw zbiór $\text{Hom}_{\mathfrak{R}}(\cdot, S)$ wszystkich rodzin $\chi := \{\chi^{(\lambda)}\}_{\lambda \in \Lambda}$ homomorfizmów struktur rodzaju $\mathfrak{R}$ o wspólnej dla całej rodziny dziedzinie i o przeciwdziedzinie S , tj. – dla ustalonej χ –

$$\forall_{\lambda \in \Lambda} : \chi^{(\lambda)} : X \longrightarrow S^{(\lambda)}$$

są homomorfizmami struktur rodzaju $\mathfrak{R}$, co będziemy zapisywać zwięźle w postaci $\chi^{(\lambda)} \in \text{Hom}_{\mathfrak{R}}(X, S^{(\lambda)})$ oraz $\chi \in \text{Hom}_{\mathfrak{R}}(X, S)$. Dla dowolnych $\chi \in \text{Hom}_{\mathfrak{R}}(X, S)$ oraz $\gamma \in \text{Hom}_{\mathfrak{R}}(Y, S)$ określamy **homomorfizm przed-kładający γ w χ** jako pewien homomorfizm $\Phi \in \text{Hom}_{\mathfrak{R}}(X, Y)$ o własności (wyrażonej przez diagram przemienności i równoważne zdanie logiczne)

$$\begin{array}{ccc} X & & \\ \Phi \downarrow & \searrow \chi & \\ Y & \xrightarrow{\gamma} & S \end{array} \quad \equiv \quad \forall_{\lambda \in \Lambda} : \chi^{(\lambda)} = \gamma^{(\lambda)} \circ \Phi.$$

Struktura terminalna (zwana też **końcową**) **dla zbioru** $\text{Hom}_{\mathfrak{R}}(\cdot, S)$ to para

$$(\mathcal{T}, \tau := \{\tau^{(\lambda)}\}_{\lambda \in \Lambda})$$

złożona ze struktury $\mathcal{T}$ rodzaju $\mathfrak{R}$ o nośniku T oraz rodziny $\tau \in \text{Hom}_{\mathfrak{R}}(T, S)$ o następującej własności: dla dowolnej struktury $\mathcal{X}$ rodzaju $\mathfrak{R}$ o nośniku X oraz dowolnej rodziny $\xi \in \text{Hom}_{\mathfrak{R}}(X, S)$ istnieje dokładnie jeden homomorfizm indukowany $\Phi \in \text{Hom}_{\mathfrak{R}}(X, T)$ przed-kładający τ w ξ , co będziemy zapisywać za pomocą diagramu przemienności

$$(8.4) \quad \begin{array}{ccc} X & & \\ \Phi \downarrow & \searrow \xi & \\ T & \xrightarrow{\tau} & S \end{array},$$

w którym przerywana cięciwa strzałki symbolizuje „istnienie i jedyność”.

Rozpatrzmy następnie zbiór $\text{Hom}_{\mathfrak{R}}(S, \cdot)$ wszystkich rodzin $\theta := \{\theta^{(\lambda)}\}_{\lambda \in \Lambda}$ homomorfizmów struktur rodzaju $\mathfrak{R}$ o wspólnej dla całej rodziny przeciwdziedzinie i o dziedzinie S , tj. – dla ustalonej θ –

$$\forall_{\lambda \in \Lambda} : \theta^{(\lambda)} : S^{(\lambda)} \longrightarrow O$$

są homomorfizmami struktur rodzaju $\mathfrak{R}$, tj. $\theta \in \text{Hom}_{\mathfrak{R}}(S, O)$. Dla dowolnych $\theta \in \text{Hom}_{\mathfrak{R}}(S, O)$ oraz $\zeta \in \text{Hom}_{\mathfrak{R}}(S, Z)$ określamy **homomorfizm po-kładający θ w ζ** jako pewien homomorfizm $\Psi \in \text{Hom}_{\mathfrak{R}}(O, Z)$ o własności (wyrażonej przez

diagram przemienny i równoważne zdanie logiczne)

$$\begin{array}{ccc}
 & Z & \\
 \uparrow \Psi & \swarrow \zeta & \\
 O & \xleftarrow{\theta} & S
 \end{array} \quad \equiv \quad \forall_{\lambda \in \Lambda} : \Psi \circ \theta^{(\lambda)} = \zeta^{(\lambda)}.$$

Struktura inicjalna (zwana też **początkową**) dla zbioru $\text{Hom}_{\mathfrak{R}}(S, \cdot)$ to para

$$(\mathcal{I}, \iota := \{\iota^{(\lambda)}\}_{\lambda \in \Lambda})$$

złożona ze struktury $\mathcal{I}$ rodzaju $\mathfrak{R}$ o nośniku I oraz rodziny $\iota \in \text{Hom}_{\mathfrak{R}}(S, I)$ o następującej własności: dla dowolnej struktury $\mathcal{U}$ rodzaju $\mathfrak{R}$ o nośniku U oraz dowolnej rodziny $v \in \text{Hom}_{\mathfrak{R}}(S, U)$ istnieje dokładnie jeden homomorfizm indukowany $\Psi \in \text{Hom}_{\mathfrak{R}}(I, U)$ po-kładający ι w v , co opisuje diagram przemienny

$$(8.5) \quad \begin{array}{ccc}
 & U & \\
 \uparrow \Psi & \swarrow v & \\
 I & \xleftarrow{\iota} & S
 \end{array} .$$

Struktury terminalne i inicjalne (stowarzyszone z daną rodziną $\mathcal{I}$) noszą miano **struktur uniwersalnych**. ▲

Sens uniwersalności łatwo wysławić w języku potocznym: oto elementy dowolnej rodziny odwzorowań transportujących strukturę rodzaju $\mathfrak{R}$ do $\mathcal{I}$ (wzgl. z $\mathcal{I}$) są przeprowadzane, za pośrednictwem homomorfizmów indukowanych, przez struktury terminalne (wzgl. inicjalne). Na pytanie o istnienie struktur uniwersalnych nie ma uniwersalnej odpowiedzi – tej trzeba każdorazowo poszukiwać w interesującym nas kontekście algebraicznym. Można natomiast bardzo konkretnie skwantyfikować swobodę ich wyboru (będącą miarą ich jednoznaczności), co czyni poniższe

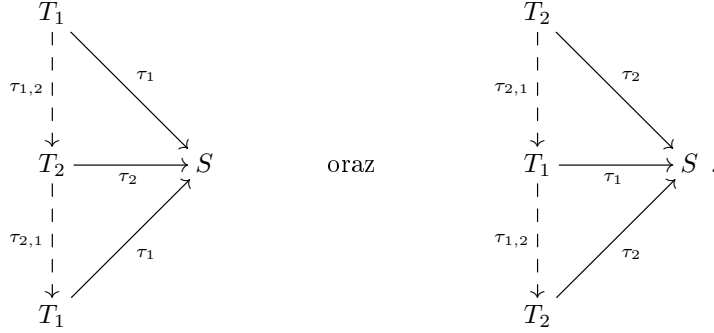
TWIERDZENIE 8.9 (O jednoznaczności struktur uniwersalnych). *Przyjmijmy notację Def. 2, 10, 67 oraz 75. Niechaj $(\mathcal{T}_\alpha, \tau_\alpha)$, $\alpha \in \{1, 2\}$ będą dwiema strukturami terminalnymi dla $\text{Hom}_{\mathfrak{R}}(\cdot, S)$ i niech $(\mathcal{I}_\beta, \iota_\beta)$, $\beta \in \{1, 2\}$ będą dwiema strukturami inicjalnymi dla $\text{Hom}_{\mathfrak{R}}(S, \cdot)$. Istnieją jednoznacznie określone izomorfizmy struktury rodzaju $\mathfrak{R}$*

$$\tau_{1,2} : \mathcal{T}_1 \xrightarrow{\cong} \mathcal{T}_2, \quad \iota_{1,2} : \mathcal{I}_1 \xrightarrow{\cong} \mathcal{I}_2.$$

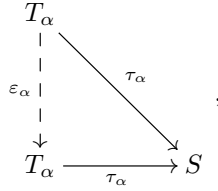
■

Dowód: Przeprowadzimy dowód dla struktur terminalnych, pozostawiając Czytelnikowi koncepcyjnie w pełni analogiczny dowód dla struktur inicjalnych. Połóżmy w opisie struktury terminalnej w Def. 75 najpierw $(\mathcal{X}, \xi) := (\mathcal{T}_1, \tau_1)$ (nośnik T_1) i $(\mathcal{T}, \tau) := (\mathcal{T}_2, \tau_2)$ (nośnik T_2), a następnie – na odwrót – $(\mathcal{X}, \xi) := (\mathcal{T}_2, \tau_2)$ i $(\mathcal{T}, \tau) := (\mathcal{T}_1, \tau_1)$. Korzystając każdorazowo z definiującej własności struktury

terminalnej $(\mathcal{T}, \tau)$, stwierdzamy istnienie pary *jedynych* homomorfizmów indukowanych, domykających odnośnie dwa diagramy przemienne, które złożymy ze sobą na dwa sposoby, jak następuje:



Jak wynika wprost z konstrukcji, $\tau_{2,1} \circ \tau_{1,2} \in \text{End}_{\mathfrak{R}}(T_1)$ oraz $\tau_{1,2} \circ \tau_{2,1} \in \text{End}_{\mathfrak{R}}(T_2)$ (czyli w szczególności oba złożenia są homomorfizmami struktury rodzaju $\mathfrak{R}$). Z drugiej jednakowoż strony możemy położyć $(\mathcal{X}, \xi) := (\mathcal{T}_\alpha, \tau_\alpha)$ i $(\mathcal{T}, \tau) := (\mathcal{T}_\alpha, \tau_\alpha)$ dla $\alpha \in \{1, 2\}$, uzyskując odnośnie diagramy



w których homomorfizmy indukowane muszą – wobec swej jedyności – przyjąć prostą postać $\varepsilon_\alpha = \text{id}_{T_\alpha}$ (co stwierdzamy zauważając, że homomorfizmy identycznościowe spełniają kryteria definicyjne). Ten sam argument (jednoznaczność określenia homomorfizmów indukowanych) pozwala nam zapisać tożsamości

$$\tau_{2,1} \circ \tau_{1,2} = \text{id}_{T_1} \quad \wedge \quad \tau_{1,2} \circ \tau_{2,1} = \text{id}_{T_2},$$

na podstawie których wnioskujemy, że $\tau_{1,2}$ jest pożądanym jedynym izomorfizmem struktur terminalnych (o odwrotności $\tau_{2,1}$). $\square$

Praktyczny sens udowodnionego twierdzenia jest oczywisty: każde dwie struktury uniwersalne możemy utożsamić, i to w jednoznaczny sposób (zgodny z niesioną przez nie strukturą algebraiczną), za pośrednictwem stosownego izomorfizmu $\tau_{1,2}$ (wzgl. $\iota_{1,2}$).

Możemy już teraz w pełni świadomie wysławić

DEFINICJA 76. Przyjmijmy notację Def. 2, 10, 67 oraz 75. **Produkt rodziny struktur** $\mathcal{S}$ rodzaju $\mathfrak{R}$ to struktura terminalna

$$\left(\prod_{\lambda \in \Lambda} \mathcal{S}^{(\lambda)}, \{\varpi_\lambda\}_{\lambda \in \Lambda} \right)$$

dla zbioru $\text{Hom}_{\mathfrak{R}}(\cdot, S)$. Homomorfizm ϖ_λ określamy przy tym mianem **rzutu kanonicznego na (składową) $\mathcal{S}^{(\lambda)}$** .

Koprodukt rodziny struktur $\mathcal{S}$ rodzaju $\mathfrak{R}$ to struktura inicjalna

$$\left(\coprod_{\lambda \in \Lambda} \mathcal{S}^{(\lambda)}, \{j_\lambda\}_{\lambda \in \Lambda} \right)$$

dla zbioru $\text{Hom}_{\mathfrak{R}}(S, \cdot)$. Homomorfizm j_λ określamy przy tym mianem **włożenia kanonicznego (składowej)** $\mathcal{S}^{(\lambda)}$.

Koprodukt struktur z rodzaju $\mathfrak{R} \in \{\text{grupy przemienne, moduły nad pierścieniem } R\}$ jest najczęściej określamy mianem **sumy prostej**. ▲

Ilustracji wprowadzonych dotychczas pojęć i konstrukcji abstrakcyjnych dostarcza poniższy przykład, którego dokładne zrozumienie w części początkowej dotyczącej produktu stanowi podstawę dalszych naszych rozważań poświęconych modułom.

PRZYKŁAD(Y) 41. Rozważmy strukturę algebraiczną rodzaju trywialnego (tj. „pustego”), której nośnikami są zbiory bez jakichkolwiek wyróżnionych operacji wieloargumentowych i dla której homomorfizmami są dowolne odwzorowania między zbiorami. W tym szczególnym przypadku produktem zbiorów z rodziny $\{S^{(\lambda)}\}_{\lambda \in \Lambda}$ jest **produkt kartezjański** [KM76, Rozdz. IV § 6]

$$\prod_{\lambda \in \Lambda} S^{(\lambda)} := \{ f : \Lambda \longrightarrow \bigcup_{\lambda \in \Lambda} S^{(\lambda)} \mid \forall_{\lambda \in \Lambda} : f(\lambda) \in S^{(\lambda)} \}$$

wraz z rodziną $\{\varpi_\lambda := \text{pr}_\lambda\}_{\lambda \in \Lambda}$ rzutów kanonicznych na składowe $S^{(\lambda)}$,

$$\text{pr}_\mu : \prod_{\lambda \in \Lambda} S^{(\lambda)} \longrightarrow S^{(\mu)} : f \longmapsto f(\mu).$$

Należy zwrócić uwagę, że w przypadku skończonego zbioru indeksów $\Lambda \equiv \overline{1, n}$ produkt kartezjański sprowadza się do standardowego iloczynu kartezjańskiego⁷ i zapisuje w postaci

$$\times_{k=1}^n S^{(k)} = \{ (x_1, x_2, \dots, x_n) \mid \forall_{k \in \overline{1, n}} : x_k \in S^{(k)} \},$$

przy czym

$$\text{pr}_l : \times_{k=1}^n S^{(k)} \longrightarrow S^{(l)} : (x_1, x_2, \dots, x_n) \longmapsto x_l.$$

Dla dowolnej rodziny odwzorowań

$$\{f^{(\lambda)} : X \longrightarrow S^{(\lambda)}\}_{\lambda \in \Lambda}$$

znajdujemy jedyne odwzorowanie

$$\Phi : X \longrightarrow \prod_{\lambda \in \Lambda} S^{(\lambda)}$$

przedkładające rzuty kanoniczne pr_λ w odwzorowania $f^{(\lambda)}$, a mianowicie

$$x \longmapsto \Phi(x), \quad \Phi(x)(\lambda) := f^{(\lambda)}(x).$$

Koproduktem jest tutaj natomiast **suma rozłączna**⁸

$$\bigsqcup_{\lambda \in \Lambda} S^{(\lambda)} := \{ (x, \lambda) \mid x \in S^{(\lambda)} \wedge \lambda \in \Lambda \}$$

⁷Por. uwagi pod definicją w traktacie Kuratowskiego i Mostowskiego, jak również Konw. 1.

⁸N.B. Ilekroć $x \in S^{(\lambda)} \cap S^{(\mu)}$, $\lambda \neq \mu$, wówczas $(x, \lambda) \neq (x, \mu)$.

wraz z injekcjami (włączeniami) kanonicznymi

$$j_\mu : S^{(\mu)} \longrightarrow \bigsqcup_{\lambda \in \Lambda} S^{(\lambda)} : x \longmapsto (x, \mu).$$

Z dowolną rodziną odwzorowań

$$\{g^{(\lambda)} : S^{(\lambda)} \longrightarrow Y\}_{\lambda \in \Lambda}$$

stowarzyszymy jedyne odwzorowanie

$$\Psi : \bigsqcup_{\lambda \in \Lambda} S^{(\lambda)} \longrightarrow Y$$

po-kładające injekcje kanoniczne j_λ w odwzorowania $g^{(\lambda)}$, a mianowicie

$$(x, \lambda) \longmapsto \Psi(x, \lambda) := g^{(\lambda)}(x).$$

✓

Zwieńczeniem obecnej dyskusji jest szczegółowe *wyprowadzenie* postaci produktu i koproduktu dla struktury z rodzaju moduł nad pierścieniem.

DEFINICJA 77. Przyjmijmy notację Def. 67, 21, 32, 61 i 75 oraz Przykł. 41. Niechaj

$$\mathcal{M} := \{\mathcal{M}^{(\lambda)}\}_{\lambda \in \Lambda}, \quad \mathcal{M}^{(\lambda)} := \left((G^{(\lambda)}, \phi_2^{(\lambda)}, \phi_1^{(\lambda)}, \phi_0^{(\lambda)}), \ell^{(\lambda)} \right)$$

będzie rodziną modułów nad pierścieniem R . **Produkt modułów z rodziny $\mathcal{M}$** to para

$$(\mathcal{M}^\square, \{\text{pr}_\lambda\}_{\lambda \in \Lambda}), \quad \mathcal{M}^\square := \left(\left(\prod_{\lambda \in \Lambda} G^{(\lambda)}, \phi_2^\square, \phi_1^\square, \phi_0^\square \right), \ell^\square \right),$$

w której $\phi_n^\square$, $n \in \{0, 1, 2\}$ to *kanonicznie indukowane* operacje grupowe, $\ell^\square$ zaś to *kanonicznie indukowane* działanie R na produkcie kartezjańskim $\prod_{\lambda \in \Lambda} G^{(\lambda)}$. ▲

Poświęcimy obecnie trochę czasu na bezpośrednie uzasadnienie i wyjaśnienie powyższej definicji w odwołaniu do wcześniejszej definicji produktu struktur algebraicznych jako struktury terminalnej. Oto więc rozważamy zbiór $G^\square := \prod_{\lambda \in \Lambda} G^{(\lambda)}$ z rzutami kanonicznymi $\text{pr}_\lambda : G^\square \longrightarrow G^{(\lambda)}$. Dodawania grupowe⁹

$$\phi_2^{(\lambda)} : G^{(\lambda)} \times G^{(\lambda)} \longrightarrow G^{(\lambda)}$$

zadają – dla dowolnego indeksu $\lambda \in \Lambda$ – odwzorowania

$$\phi_2^{(\lambda)} \circ (\text{pr}_\lambda \times \text{pr}_\lambda) : G^\square \times G^\square \longrightarrow G^{(\lambda)},$$

co wobec terminalności pary $(G^\square, \{\text{pr}_\lambda\}_{\lambda \in \Lambda})$, w której $G^\square$ traktowane jest jako struktura trywialna (czyli „goły” zbiór), oznacza istnienie jedyne odwzorowania (*a priori* bez dodatkowych własności względem operacji grupowych i działań określonych dla poszczególnych składowych rodziny)

$$\phi_2^\square : G^\square \times G^\square \longrightarrow G^\square$$

o własności

$$(8.6) \quad \text{pr}_\lambda \circ \phi_2^\square = \phi_2^{(\lambda)} \circ (\text{pr}_\lambda \times \text{pr}_\lambda).$$

⁹Opisywana konstrukcja produktu po opuszczeniu działań $\ell^{(\lambda)}$ stosuje się także do grup nieprzemienne.

Zauważmy, że jeśli tylko $\phi_2^\square$ jest poprawnie określonym dodawaniem na $G^\square$ a rzuty pr_λ są homomorfizmami grup transportującymi owo dodawanie w dodawanie w poszczególnych składowych $G^{(\lambda)}$, czego mozolnie dowodzimy poniżej, to tożsamość (8.6) identyfikuje operację $\phi_2^\square$ jako „dodawanie po współrzędnych”. Łatwo przy tym stwierdzamy, że homomorficzność rzutów wynika bezpośrednio z założenia, że $\phi_2^\square =: +_\square$ jest pożądaną operacją grupową, oto bowiem (8.6) implikuje równość

$$\text{pr}_\lambda(g +_\square h) = \text{pr}_\lambda(g) +_{(\lambda)} \text{pr}_\lambda(h),$$

słuszną dla dowolnych dwóch elementów $g, h \in G^\square$ a oznaczającą właśnie, że pr_λ są homomorfizmami grup. Wystarczy zatem sprawdzić definiujące własności dodawania grupowego w odniesieniu do odwzorowania $\phi_2^\square$. W pierwszej kolejności zbadamy jego łączność. Biorąc dowolne $g, h, k \in G^\square$, obliczamy – wykorzystując po drodze (przy przejściu z linii 2. do linii 3.) łączność operacji $\phi_2^{(\lambda)}$ –

$$\begin{aligned} \text{pr}_\lambda \circ \phi_2^\square (\phi_2^\square(g, h), k) &= \phi_2^{(\lambda)} \circ (\text{pr}_\lambda \times \text{pr}_\lambda) (\phi_2^\square(g, h), k) \\ &\equiv \phi_2^{(\lambda)} (\text{pr}_\lambda \circ \phi_2^\square(g, h), \text{pr}_\lambda(k)) \\ &= \phi_2^{(\lambda)} \left(\phi_2^{(\lambda)} \circ (\text{pr}_\lambda \times \text{pr}_\lambda)(g, h), \text{pr}_\lambda(k) \right) \\ &\equiv \phi_2^{(\lambda)} \left(\phi_2^{(\lambda)} (\text{pr}_\lambda(g), \text{pr}_\lambda(h)), \text{pr}_\lambda(k) \right) \\ &= \phi_2^{(\lambda)} \left(\text{pr}_\lambda(g), \phi_2^{(\lambda)} (\text{pr}_\lambda(h), \text{pr}_\lambda(k)) \right) \\ &\equiv \phi_2^{(\lambda)} \left(\text{pr}_\lambda(g), \phi_2^{(\lambda)} \circ (\text{pr}_\lambda \times \text{pr}_\lambda)(h, k) \right) \\ &= \phi_2^{(\lambda)} (\text{pr}_\lambda(g), \text{pr}_\lambda \circ \phi_2^\square(h, k)) \\ &\equiv \phi_2^{(\lambda)} \circ (\text{pr}_\lambda \times \text{pr}_\lambda) (g, \phi_2^\square(h, k)) \\ &= \text{pr}_\lambda \circ \phi_2^\square (g, \phi_2^\square(h, k)). \end{aligned}$$

Tym sposobem otrzymujemy dwa odwzorowania

$$G^\square \times G^\square \times G^\square \xrightarrow[\phi_2^\square \circ (\text{id}_{G^\square} \times \phi_2^\square)]{\phi_2^\square \circ (\phi_2^\square \times \text{id}_{G^\square})} G^\square \xrightarrow{\text{pr}_\lambda} G^{(\lambda)},$$

których obrazy pokrywają się, dając odwzorowanie $\phi_2^{(\lambda)} \circ (\text{id}_{G^{(\lambda)}} \times \phi_2^{(\lambda)}) \circ (\text{pr}_\lambda \times \text{pr}_\lambda \times \text{pr}_\lambda)$. Raz jeszcze przywołując terminalność pary $(G^\square, \{\text{pr}_\lambda\}_{\lambda \in \Lambda})$, wnioskujemy, że istnieje dokładnie jedno odwzorowanie

$$\alpha^\square : G^\square \times G^\square \times G^\square \longrightarrow G^\square$$

przez nie indukowane, które przed-kłada pr_λ w $\phi_2^{(\lambda)} \circ (\text{id}_{G^{(\lambda)}} \times \phi_2^{(\lambda)}) \circ (\text{pr}_\lambda \times \text{pr}_\lambda \times \text{pr}_\lambda)$,

$$\text{pr}_\lambda \circ \alpha^\square = \phi_2^{(\lambda)} \circ (\text{id}_{G^{(\lambda)}} \times \phi_2^{(\lambda)}) \circ (\text{pr}_\lambda \times \text{pr}_\lambda \times \text{pr}_\lambda),$$

a ponieważ zarówno $\phi_2^\square \circ (\phi_2^\square \times \text{id}_{G^\square})$, jak i $\phi_2^\square \circ (\text{id}_{G^\square} \times \phi_2^\square)$ spełniają ten warunek, przeto koniecznie

$$\phi_2^\square \circ (\phi_2^\square \times \text{id}_{G^\square}) = \alpha^\square = \phi_2^\square \circ (\text{id}_{G^\square} \times \phi_2^\square),$$

co dowodzi łączności $\phi_2^\square$.

Analogicznie wykazujemy przemienność $\phi_2^\square$, korzystając z przemienności $\phi_2^{(\lambda)}$. Oto bowiem, dla dowolnych $g, h \in G^\square$,

$$\begin{aligned} \text{pr}_\lambda \circ (\phi_2^\square \circ \tau_{G^\square}(g, h)) &= \phi_2^{(\lambda)} \circ (\text{pr}_\lambda \times \text{pr}_\lambda)(h, g) \equiv \phi_2^{(\lambda)}(\text{pr}_\lambda(h), \text{pr}_\lambda(g)) \\ &= \phi_2^{(\lambda)}(\text{pr}_\lambda(g), \text{pr}_\lambda(h)) \equiv \phi_2^{(\lambda)} \circ (\text{pr}_\lambda \times \text{pr}_\lambda)(g, h) \\ &= \text{pr}_\lambda \circ \phi_2^\square(g, h), \end{aligned}$$

skąd równość odwzorowań

$$G^\square \times G^\square \xrightarrow[\phi_2^\square]{\phi_2^\square \circ \tau_{G^\square}} G^\square \xrightarrow{\text{pr}_\lambda} G^{(\lambda)},$$

tożsamy z $\phi_2^{(\lambda)} \circ (\text{pr}_\lambda \times \text{pr}_\lambda)$, czyli wobec jednoznaczności określenia indukowanego przezeń odwzorowania

$$\beta^\square : G^\square \times G^\square \longrightarrow G^\square$$

o własności

$$\text{pr}_\lambda \circ \beta^\square = \phi_2^{(\lambda)} \circ (\text{pr}_\lambda \times \text{pr}_\lambda)$$

mamy pożądaną identyczność

$$\phi_2^\square \circ \tau_{G^\square} = \beta^\square = \phi_2^\square.$$

Następnie rozważamy elementy neutralne w każdej z grup składowych,

$$\phi_0^{(\lambda)} : \{\bullet\} \longrightarrow G^{(\lambda)} : \bullet \longmapsto e^{(\lambda)},$$

i zapominając jak uprzednio o strukturze algebraicznej na rozważanych zbiorach, stowarzyszymy z nimi jedyne odwzorowanie

$$\phi_0^\square : \{\bullet\} \longrightarrow G^\square : \bullet \longmapsto e^\square$$

o własności

$$\text{pr}_\lambda \circ \phi_0^\square = \phi_0^{(\lambda)}.$$

W ten sposób wyróżniamy element $e^\square$ zbioru $G^\square$, o sugestywnej postaci uogólnionego ciągu (o indeksach z Λ) elementów neutralnych z grup składowych. Jego własności względem dodawania $\phi_2^\square$ sprawdzamy w bezpośrednim rachunku. Biorąc dowolny element $g \in G^\square$, otrzymujemy

$$\begin{aligned} \text{pr}_\lambda \circ \phi_2^\square(e^\square, g) &= \phi_2^{(\lambda)} \circ (\text{pr}_\lambda \times \text{pr}_\lambda)(e^\square, g) \equiv \phi_2^{(\lambda)}(\text{pr}_\lambda \circ \phi_0^\square(\bullet), \text{pr}_\lambda(g)) \\ &= \phi_2^{(\lambda)}(\phi_0^{(\lambda)}(\bullet), \text{pr}_\lambda(g)) \equiv \phi_2^{(\lambda)}(e^{(\lambda)}, \text{pr}_\lambda(g)) = \text{pr}_\lambda(g) \\ &\equiv \text{pr}_\lambda \circ \text{pr}_2(e^\square, g), \end{aligned}$$

stąd zaś równość odwzorowań

$$\{\bullet\} \times G^\square \xrightarrow[\text{pr}_2]{\phi_2^\square \circ (\phi_0^\square \times \text{id}_{G^\square})} G^\square \xrightarrow{\text{pr}_\lambda} G^{(\lambda)},$$

pokrywających się z $\phi_2^{(\lambda)} \circ (\phi_0^{(\lambda)} \times \text{pr}_\lambda)$. Znowu więc znajdujemy jedyne odwzorowanie

$$\varepsilon^\square : \{\bullet\} \times G^\square \longrightarrow G^\square$$

spełniające warunek

$$\mathrm{pr}_\lambda \circ \varepsilon^\square = \phi_2^{(\lambda)} \circ (\phi_0^{(\lambda)} \times \mathrm{pr}_\lambda),$$

a zatem

$$\phi_2^\square \circ (\phi_0^\square \times \mathrm{id}_{G^\square}) = \varepsilon^\square = \mathrm{pr}_2.$$

Podobnie dowodzimy tożsamości

$$\phi_2^\square \circ (\mathrm{id}_{G^\square} \times \phi_0^\square) = \mathrm{pr}_1,$$

co w sumie pokazuje dowodnie, że $e^\square$ jest elementem neutralnym dodawania $\phi_2^\square$.

Bez trudu rekonstruujemy też operację brania przeciwności w $G^\square$, biorąc za punkt wyjścia odnośne operacje w składowych

$$\phi_1^{(\lambda)} : G^{(\lambda)} \curvearrowright.$$

Rozumując jak wcześniej, tworzymy rodzinę odwzorowań

$$\phi_1^{(\lambda)} \circ \mathrm{pr}_\lambda : G^\square \longrightarrow G^{(\lambda)},$$

z którymi możemy związać jedyne odwzorowanie

$$\phi_1^\square : G^\square \curvearrowright$$

o własności

$$\mathrm{pr}_\lambda \circ \phi_1^\square = \phi_1^{(\lambda)} \circ \mathrm{pr}_\lambda,$$

która identyfikuje $\phi_1^\square$ jako „branie przeciwności po współrzędnych”. Trzeba jeszcze tylko upewnić się, że odwzorowanie to nadaje monoidowi przemienemu $(G^\square, \phi_2^\square, \phi_0^\square)$ strukturę grupy przemiennej. Z rachunku

$$\begin{aligned} \mathrm{pr}_\lambda \circ \phi_2^\square (\phi_1^\square(g), g) &= \phi_2^{(\lambda)} \circ (\mathrm{pr}_\lambda \times \mathrm{pr}_\lambda) (\phi_1^\square(g), g) \equiv \phi_2^{(\lambda)} (\mathrm{pr}_\lambda \circ \phi_1^\square(g), \mathrm{pr}_\lambda(g)) \\ &= \phi_2^{(\lambda)} (\phi_1^{(\lambda)} \circ \mathrm{pr}_\lambda(g), \mathrm{pr}_\lambda(g)) = e^{(\lambda)} = \phi_0^{(\lambda)}(\bullet) = \mathrm{pr}_\lambda \circ \phi_0^\square(\bullet), \end{aligned}$$

wykonanego dla dowolnego $g \in G^\square$ a wskazującego na równość odwzorowań

$$\{\bullet\} \times G^\square \xrightarrow[\phi_0^\square \circ \mathrm{pr}_1]{\phi_2^\square \circ (\phi_1^\square, \mathrm{id}_{G^\square}) \circ \mathrm{pr}_2} G^\square \xrightarrow{\mathrm{pr}_\lambda} G^{(\lambda)},$$

identycznych z $\phi_0^{(\lambda)} \circ \mathrm{pr}_1$, wywodzimy wniosek o istnieniu jedyne odwzorowania

$$\mu^\square : \{\bullet\} \times G^\square \longrightarrow G^\square$$

o własności

$$\mathrm{pr}_\lambda \circ \mu^\square = \phi_0^{(\lambda)} \circ \mathrm{pr}_1.$$

Ostatecznie więc stwierdzamy słuszność tożsamości

$$\phi_2^\square \circ (\phi_1^\square, \mathrm{id}_{G^\square}) \circ \mathrm{pr}_2 = \mu^\square = \phi_0^\square \circ \mathrm{pr}_1.$$

Analogiczne wnioskowanie prowadzi do jej symetrycznego odpowiednika

$$\phi_2^\square \circ (\mathrm{id}_{G^\square}, \phi_1^\square) \circ \mathrm{pr}_2 = \mu^\square = \phi_0^\square \circ \mathrm{pr}_1,$$

co potwierdza identyfikację $\phi_1^\square$ jako operacji brania przeciwności.

Na koniec wreszcie indukujemy na zrekonstruowanej powyżej grupie przemiennej strukturę modułu nad pierścieniem R ze struktur składowych. W tym celu z każdego z działań

$$\ell^{(\lambda)} : R \times G^{(\lambda)} \longrightarrow G^{(\lambda)}$$

budujemy odwzorowanie

$$\ell^{(\lambda)} \circ (\text{id}_R \times \text{pr}_\lambda) : R \times G^\Gamma \longrightarrow G^{(\lambda)},$$

co daje nam jedyne odwzorowanie

$$\ell^\Gamma : R \times G^\Gamma \longrightarrow G^\Gamma$$

o własności

$$\text{pr}_\lambda \circ \ell^\Gamma = \ell^{(\lambda)} \circ (\text{id}_R \times \text{pr}_\lambda).$$

Z tej ostatniej odczytujemy definicję ℓ^Γ jako „działania po współrzędnych”. W żmudnym, lecz poza tym absolutnie trywialnym rachunku przekonujemy się, że tak zdefiniowane odwzorowanie spełnia aksjomaty działania, i tym samym zamykamy kanoniczną konstrukcję modułu na produkcie kartezjańskim G^Γ .

O ile konstrukcja produktu modułów postępuje automatycznie po dokonaniu narzucającego się wyboru nośnika G^Γ , o tyle konstrukcja koproduktu, który będziemy w dalszej części kursu nazywać sumą prostą modułów, wymaga pewnej dozy inwencji oraz rozlicznych sprawdzeń (jednoznaczności konstrukcji). Zaznaczamy zawniasu, że poniższa konstrukcja stosuje się wyłącznie do grup przemiennej, co będziemy podkreślać pisząc $e^{(\lambda)}$ w notacji addytywnej jako $0_{(\lambda)}$.

DEFINICJA 78. Przyjmijmy notację Def. 67, 21, 32, 61, 75 i 77. **Suma prosta modułów z rodziny $\mathcal{M}$** to para

$$(\mathcal{M}^\sqcup, \{j_\lambda\}_{\lambda \in \Lambda}), \quad \mathcal{M}^\oplus := \left(\left(\bigoplus_{\lambda \in \Lambda} G^{(\lambda)}, \phi_2^\Gamma, \phi_1^\Gamma, \phi_0^\Gamma \right), \ell^\Gamma \right),$$

w której $\mathcal{M}^\oplus$ jest podmodulem produktu modułów $\mathcal{M}^\Gamma$ z rodziny $\mathcal{M}$ o nośniku

$$(8.7) \quad \bigoplus_{\lambda \in \Lambda} G^{(\lambda)} := \{ g \in G^\Gamma \mid |\{ \lambda \in \Lambda \mid \text{pr}_\lambda(g) \neq 0_{(\lambda)} \}| < \infty \}$$

(czyli $\text{pr}_\lambda(g)$ jest równe elementowi neutralnemu dla prawie wszystkich indeksów) i w której $j_\lambda : G^{(\lambda)} \longrightarrow G^\Gamma$ są iniekcjami kanonicznymi spełniającymi warunki

$$(8.8) \quad \forall_{\substack{\lambda, \mu \in \Lambda \\ g_\mu \in G^{(\mu)}}} : \text{pr}_\lambda \circ j_\mu(g_\mu) := \begin{cases} g_\mu & \text{dla } \lambda = \mu \\ 0_{(\lambda)} & \text{dla } \lambda \neq \mu \end{cases}.$$

▲

Pokażemy najpierw, że odwzorowania j_λ są homomorfizmami oraz że mają cechę uniwersalności. Na początku ustalmy (dowolnie) indeks $\mu \in \Lambda$ i obliczmy – dla dowolnych $g_\mu, h_\mu \in G^{(\mu)}$ –

$$\begin{aligned} \text{pr}_\lambda \circ \phi_2^\Gamma \circ (j_\mu \times j_\mu)(g_\mu, h_\mu) &= \phi_2^{(\lambda)} \circ (\text{pr}_\lambda \times \text{pr}_\lambda) \circ (j_\mu \times j_\mu)(g_\mu, h_\mu) \\ &= \phi_2^{(\lambda)} \circ ((\text{pr}_\lambda \circ j_\mu) \times (\text{pr}_\lambda \circ j_\mu))(g_\mu, h_\mu) \\ &= \begin{cases} \phi_2^{(\mu)}(g_\mu, h_\mu) & \text{dla } \lambda = \mu \\ \phi_2^{(\lambda)}(0_{(\lambda)}, 0_{(\lambda)}) = 0_{(\lambda)} & \text{dla } \lambda \neq \mu \end{cases} \end{aligned}$$

$$= \text{pr}_\lambda \circ j_\mu \circ \phi_2^{(\mu)}(g_\mu, h_\mu),$$

dowodząc tym samym równości dwóch rodzin odwzorowań

$$G^{(\mu)} \times G^{(\mu)} \xrightarrow[j_\mu \circ \phi_2^{(\mu)}]{\phi_2^\square \circ (j_\mu \times j_\mu)} G^\square \xrightarrow{\text{pr}_\lambda} G^{(\lambda)}$$

identycznych z $\psi^{(\lambda)} : (g_\mu, h_\mu) \mapsto \begin{cases} \phi_2^{(\mu)}(g_\mu, h_\mu) & \text{dla } \lambda = \mu \\ 0_{(\lambda)} & \text{dla } \lambda \neq \mu \end{cases}$. W konsekwencji terminalności pary $(G^\square, \{\text{pr}_\lambda\}_{\lambda \in \Lambda})$ równość ta implikuje istnienie jedynej rodziny odwzorowań

$$\alpha^{(\mu)} : G^{(\mu)} \times G^{(\mu)} \longrightarrow G^\square$$

o własności

$$\forall_{\lambda \in \Lambda} : \text{pr}_\lambda \circ \alpha^{(\mu)} = \psi^{(\lambda)}.$$

Na tej podstawie wnioskujemy o równości

$$\phi_2^\square \circ (j_\mu \times j_\mu) = j_\mu \circ \phi_2^{(\mu)},$$

która wyraża homomorficzny charakter j_μ . Dowód uniwersalności j_λ wymaga, iż-
byśmy z dowolną rodziną homomorfizmów grup (przebiegających)

$$\chi^{(\lambda)} : G^{(\lambda)} \longrightarrow X$$

określoną dla dowolnej grupy przemiennej X potrafili stowarzyszyć odwzorowanie

$$H : \bigoplus_{\lambda \in \Lambda} G^{(\lambda)} \longrightarrow X$$

spełniające relacje

$$(8.9) \quad \forall_{\lambda \in \Lambda} : H \circ j_\lambda = \chi^{(\lambda)}$$

oraz udowodnić, że odwzorowanie o tej własności jest dane jednoznacznie. Postulujemy, dla dowolnego $g \in \bigoplus_{\lambda \in \Lambda} G^{(\lambda)}$,

$$H(g) := \sum_{\lambda \in \Lambda} \chi^{(\lambda)} \circ \text{pr}_\lambda(g).$$

Zauważmy, że suma w powyższej definicji jest skończona, por. (8.7), zatem definicja ma sens. Sprawdzamy też bez trudu (8.9), wybrawszy dowolnie $g_\lambda \in G^{(\lambda)}$,

$$\begin{aligned} H \circ j_\lambda(g_\lambda) &= \sum_{\mu \in \Lambda} \chi^{(\mu)} \circ \text{pr}_\mu \circ j_\lambda(g_\lambda) \\ &\equiv \chi^{(\lambda)} \circ \text{pr}_\lambda \circ j_\lambda(g_\lambda) +_X \sum_{\mu \in \Lambda \setminus \{\lambda\}} \chi^{(\mu)} \circ \text{pr}_\mu \circ j_\lambda(g_\lambda) \\ &= \chi^{(\lambda)}(g_\lambda) +_X \sum_{\mu \in \Lambda \setminus \{\lambda\}} \chi^{(\mu)}(0_{(\mu)}) = \chi^{(\lambda)}(g_\lambda). \end{aligned}$$

Dowodzimy następnie jedyności H . Niechaj $\tilde{H} : \bigoplus_{\lambda \in \Lambda} G^{(\lambda)} \longrightarrow X$ będzie dowolnym innym takim odwzorowaniem, a wtedy różnica odwzorowań

$$H - \tilde{H} : \bigoplus_{\lambda \in \Lambda} G^{(\lambda)} \longrightarrow X : g \mapsto H(g) +_X P_X \circ \tilde{H}(g),$$

będąca homomorfizmem grup przemiennej (przypomnijmy, że rzuty kanoniczne są homomorfizmami grup przemiennej), spełnia tożsamości

$$(H - \tilde{H}) \circ j_\lambda(g_\lambda) = H \circ j_\lambda(g_\lambda) +_X P_X(\tilde{H} \circ j_\lambda(g_\lambda)) = \chi^{(\lambda)}(g_\lambda) +_X P_X(\chi^{(\lambda)}(g_\lambda))$$

$$= 0_X.$$

Możemy stąd wyciągnąć prosty wniosek:

$$\bigcup_{\lambda \in \Lambda} J_\lambda(G^{(\lambda)}) \subset \text{Ker}(H - \tilde{H}).$$

Jednakowoż $\text{Ker}(H - \tilde{H})$ jest – na mocy Stw. 31 – podgrupą $\bigoplus_{\lambda \in \Lambda} G^{(\lambda)}$, tj. podzbiorem domkniętym ze względu na operację brania skończonych sum jego elementów, każdy zaś element $g \in \bigoplus_{\lambda \in \Lambda} G^{(\lambda)}$ jest taką właśnie sumą skończoną elementów z różnych $J_\lambda(G^{(\lambda)})$. Ażeby się o tym przekonać, rozważmy odwzorowanie

$$\iota^\oplus : \bigoplus_{\lambda \in \Lambda} G^{(\lambda)} \ni g \longmapsto \sum_{\lambda \in \Lambda} J_\lambda \circ \text{pr}_\lambda(g),$$

które jest dobrze określone z tych samych powodów co H i które wobec homomorficzności rzutów kanonicznych spełnia tożsamości

$$\text{pr}_\lambda \circ \iota^\oplus(g) \equiv \text{pr}_\lambda \circ \sum_{\mu \in \Lambda} J_\mu \circ \text{pr}_\mu(g) = \sum_{\mu \in \Lambda} (\text{pr}_\lambda \circ J_\mu)(\text{pr}_\mu(g)) = \text{pr}_\lambda(g).$$

Te ostatnie – jak w poprzednio dyskutowanych przypadkach (tj. w konsekwencji terminalności produktu kartezjańskiego) – prowadzą do równości

$$(8.10) \quad \iota^\oplus = \text{id}_{\bigoplus_{\lambda \in \Lambda} G^{(\lambda)}},$$

zadającej rzeczony rozkład g na skończoną sumę

$$(8.11) \quad g = \sum_{\lambda \in \Lambda} J_\lambda \circ \text{pr}_\lambda(g).$$

Wracając do zasadniczego wyводу, stwierdzamy, że jedynym podzbiorem $\bigoplus_{\lambda \in \Lambda} G^{(\lambda)}$ zawierającym $\bigcup_{\lambda \in \Lambda} J_\lambda(G^{(\lambda)})$ i domkniętym względem operacji brania sum skończonych jest cały zbiór $\bigoplus_{\lambda \in \Lambda} G^{(\lambda)}$,

$$\text{Ker}(H - \tilde{H}) = \bigoplus_{\lambda \in \Lambda} G^{(\lambda)},$$

czyli też ostatecznie

$$H = \tilde{H}.$$

Należy podkreślić, że nigdzie w dotychczasowej dyskusji koproduktu nie brałimy pod uwagę dodatkowej struktury R -modułu na nośniku grupy przemiennej, możemy przeto podsumować tę jej część stwierdzeniem, że oto czwórka

$$\left(\bigoplus_{\lambda \in \Lambda} G^{(\lambda)}, \phi_2^\square, \phi_1^\square, \phi_0^\square \right)$$

stanowi spójną definicję sumy prostej grup przemiennej. Jako że działanie pierścienia R w jawny sposób zachowuje podgrupę $\bigoplus_{\lambda \in \Lambda} G^{(\lambda)} \subset G^\square$, dla naszych celów wystarczy jeszcze tylko upewnić się, że zarówno iniekcje kanoniczne J_λ , jak też jedyny homomorfizm grup H są odwzorowaniami R -liniowymi. W tym drugim przypadku własność ta jest bezpośrednim następstwem R -liniowości rzutów kanonicznych pr_λ oraz odwzorowań $\chi^{(\lambda)}$. W przypadku pierwszym R -liniowości stwierdzamy na gruncie terminalności produktu kartezjańskiego oraz dowiedzionych

własności odwzorowań ℓ^Γ i $\ell^{(\lambda)}$, stosując sprawdzoną strategię rozważań wcześniejszych. Punktem wyjścia jest obserwacja (wysłowiona dla dowolnych $\lambda, \mu \in \Lambda$ oraz $(r, g_\mu) \in R \times G^{(\mu)}$)

$$\begin{aligned} \text{pr}_\lambda \circ \ell^\Gamma \circ (\text{id}_R \times j_\mu)(r, g_\mu) &= \ell^{(\lambda)} \circ (\text{id}_R \times \text{pr}_\lambda) \circ (\text{id}_R \times j_\mu)(r, g_\mu) \\ &\equiv \ell^{(\lambda)} \circ (\text{id}_R \times \text{pr}_\lambda \circ j_\mu)(r, g_\mu) = (\text{pr}_\lambda \circ j_\mu) \circ \ell^{(\mu)}(r, g_\mu), \end{aligned}$$

wskazująca na równość dwóch rodzin odwzorowań

$$R \times G^{(\mu)} \xrightarrow[\text{j}_\mu \circ \ell^{(\mu)}]{\ell^\Gamma \circ (\text{id}_R \times \text{j}_\mu)} \bigoplus_{\nu \in \Lambda} G^{(\nu)} \xrightarrow{\text{pr}_\lambda} G^{(\lambda)},$$

identycznych z $r^{(\lambda)} : (r, g_\mu) \mapsto \begin{cases} \ell^{(\mu)}(r, g_\mu) & \text{dla } \lambda = \mu \\ 0_{(\lambda)} & \text{dla } \lambda \neq \mu \end{cases}$. Terminalność pary $(G^\Gamma, \{\text{pr}_\lambda\}_{\lambda \in \Lambda})$ przesądza w tej sytuacji o istnieniu jedynej rodziny odwzorowań

$$\rho^{(\mu)} : R \times G^{(\mu)} \longrightarrow \bigoplus_{\nu \in \Lambda} G^{(\nu)} \subset G^\Gamma$$

o własności

$$\forall \lambda \in \Lambda : \text{pr}_\lambda \circ \rho^{(\mu)} = r^{(\lambda)}.$$

Stąd ostatecznie wyprowadzamy pożądaną równość

$$j_\lambda \circ \ell^{(\lambda)} = \ell^\Gamma \circ (\text{id}_R \times j_\lambda)$$

wyrażającą R -liniowość iniekcji kanonicznych.

Warto zwrócić uwagę, że o ile definicja obu rozpatrywanych struktur uniwersalnych: produktu oraz sumy prostej modułów stawia je na pozycjach obiektów wzajem „dualnych” (co odzwierciedla odwrócenie strzałek w odnośnych diagramach przemiennych precyzujących sens uniwersalności), o tyle bezpośrednia konstrukcja w ramach teorii modułów nad pierścieniem uwypukla ich wewnątrzstrukturalne powinowactwo, prowadząc wprost do

COROLLARIUM 12. *Produkt i suma prosta skończonej rodziny modułów nad pierścieniem pokrywają się.*

■

NOTACJA 7. W przypadku skończonej rodziny $\{G^{(k)}\}_{k \in \overline{1, n}}$, $n \in \mathbb{N}$ modułów nad pierścieniem R będziemy czasem stosować zapis

$$\bigoplus_{k \in \overline{1, n}} G^{(k)} \equiv \underset{*}{G^{(1)}} \underset{*}{\oplus} \underset{*}{G^{(2)}} \oplus \dots \oplus G^{(n)}.$$

8.5. Suma prosta – związek z sumą algebraiczną i rodzinami rzutów, warunki rozszczepialności modułu

W dalszej części wykładu zajmiemy się prostą, konstruktywną charakteryzacją modułów o strukturze sumy prostej. Zaczniemy od istotnego

STWIERDZENIE 84. *Przyjmijmy notację Def. 67, 21, 32, 61, 75, 77 i 78. Niechaj $((H, \phi_2^H, \phi_1^H, \phi_0^H), \ell^H)$ będzie modulem nad pierścieniem R i niech $\{\chi^{(\lambda)}\}_{\lambda \in \Lambda}$ będzie rodziną odwzorowań R -liniowych $\chi^{(\lambda)} : G^{(\lambda)} \rightarrow H$, indukującą – według Diag. 8.5 – jedyne odwzorowanie R -liniowe $\chi : \bigoplus_{\lambda \in \Lambda} G^{(\lambda)} \rightarrow H$ pokładające iniekcje kanoniczne j_λ w odwzorowania $\chi^{(\lambda)}$. Na to by χ był izomorfizmem R -modułów, potrzeba i wystarcza, iżby istniała rodzina $\{\psi^{(\lambda)}\}_{\lambda \in \Lambda}$ odwzorowań R -liniowych $\psi^{(\lambda)} : H \rightarrow G^{(\lambda)}$ o następujących własnościach:*

$$(DS1) \quad \forall_{\lambda, \mu \in \Lambda} : \psi^{(\lambda)} \circ \chi^{(\mu)} = \begin{cases} \text{id}_{G^{(\lambda)}} & \text{dla } \lambda = \mu \\ 0 & \text{dla } \lambda \neq \mu \end{cases} ;$$

(DS2)

$$\forall_{h \in H} : \left(\left| \{ \lambda \in \Lambda \mid \psi^{(\lambda)}(h) \neq 0_{(\lambda)} \} \right| < \infty \quad \wedge \quad h = \sum_{\lambda \in \Lambda} \chi^{(\lambda)} \circ \psi^{(\lambda)}(h) \right).$$

■

Dowód:

$\Rightarrow$ Jeśli χ jest izomorfizmem, to istnieje izomorfizm odwrotny $\chi^{-1} : H \rightarrow \bigoplus_{\lambda \in \Lambda} G^{(\lambda)}$, a wtedy naturalnym (z punktu widzenia konstrukcji struktur uniwersalnych) staje się rozważenie rodziny odwzorowań R -liniowych

$$\psi^{(\mu)} : H \xrightarrow{\chi^{-1}} \bigoplus_{\lambda \in \Lambda} G^{(\lambda)} \xrightarrow{\text{pr}_\mu} G^{(\mu)},$$

które spełniają tożsamości

$$\psi^{(\lambda)} \circ \chi^{(\mu)} \equiv \text{pr}_\lambda \circ \chi^{-1} \circ \chi \circ j_\mu = \text{pr}_\lambda \circ j_\mu.$$

Z tych ostatnich wynika już wprost własność (DS1), patrz: (8.8). Skończoność nośnika rodziny $\{\psi^{(\lambda)}(h)\}_{\lambda \in \Lambda}$ jest tutaj natychmiastową konsekwencją definicji sumy prostej. Ponadto zachodzi

$$\chi^{(\lambda)} \circ \psi^{(\lambda)} = \chi \circ j_\lambda \circ \text{pr}_\lambda \circ \chi^{-1},$$

co w połączeniu z (8.11) implikuje drugą część zdania (DS2),

$$\begin{aligned} \sum_{\lambda \in \Lambda} \chi_\lambda \circ \psi_\lambda(h) &\equiv \sum_{\lambda \in \Lambda} \chi \circ j_\lambda \circ \text{pr}_\lambda \circ \chi^{-1}(h) = \chi \left(\sum_{\lambda \in \Lambda} j_\lambda \circ \text{pr}_\lambda (\chi^{-1}(h)) \right) \\ &= \chi(\chi^{-1}(h)) = h. \end{aligned}$$

$\Leftarrow$ Ilekroć prawdziwe jest zdanie (DS2), możemy zdefiniować odwzorowanie jawnie R -liniowe

$$\psi(h) := \sum_{\lambda \in \Lambda} j_\lambda \circ \psi^{(\lambda)}(h)$$

modułu H w $\bigoplus_{\lambda \in \Lambda} G^{(\lambda)}$. Wobec homomorficzności χ i na mocy (DS2) zachodzi

$$\chi \circ \psi(h) = \sum_{\lambda \in \Lambda} \chi \circ j_\lambda \circ \psi^{(\lambda)}(h) = \sum_{\lambda \in \Lambda} \chi^{(\lambda)} \circ \psi^{(\lambda)}(h) = h.$$

Z drugiej strony dla dowolnego $g \in \bigoplus_{\lambda \in \Lambda} G^{(\lambda)}$ otrzymujemy wobec (DS1)

$$\psi^{(\lambda)} \circ \chi(g) = \psi^{(\lambda)} \circ \chi \left(\sum_{\mu \in \Lambda} j_\mu \circ \text{pr}_\mu(g) \right) \equiv \psi^{(\lambda)} \left(\sum_{\mu \in \Lambda} \chi^{(\mu)} \circ \text{pr}_\mu(g) \right) = \text{pr}_\lambda(g),$$

a stąd

$$\psi \circ \chi(g) \equiv \sum_{\lambda \in \Lambda} j_\lambda \circ \psi^{(\lambda)} \circ \chi(g) = \sum_{\lambda \in \Lambda} j_\lambda \circ \text{pr}_\lambda(g) = g,$$

co pokazuje, że ψ jest homomorfizmem odwrotnym do χ .

□

Zajmiemy się teraz ważnym przypadkiem szczególnym, kiedy to sumę prostą tworzą podmoduły modułu danego.

DEFINICJA 79. Przyjmijmy notację Def. 67, 21, 32, 61, 64, 75, 77 i 78 oraz Przykł. 18 (7). Niechaj $((G, \phi_2, \phi_1, \phi_0), \ell)$ będzie modulem nad pierścieniem R i niech $\{G^{(\lambda)}\}_{\lambda \in \Lambda}$ będzie rodziną jego podmodułów. G jest sumą prostą wszystkich modułów z tej rodziny, jeśli jedyne odwzorowanie $j_\oplus : \bigoplus_{\mu \in \Lambda} G^{(\mu)} \rightarrow G$ pokładające – według Diag. 8.5 – injekcje kanoniczne $j_\lambda : G^{(\lambda)} \rightarrow \bigoplus_{\mu \in \Lambda} G^{(\mu)}$ we włożenia standardowe $j_{G^{(\lambda)}} : G^{(\lambda)} \rightarrow G$ jest izomorfizmem modułów, lub też – co na jedno wychodzi – jeśli dowolny element $g \in G$ ma jednoznaczny rozkład w postaci

$$g = \sum_{\lambda \in \Lambda} g^{(\lambda)}, \quad g^{(\lambda)} \in G^{(\lambda)},$$

zadawany przez rodzinę $\{g^{(\lambda)}\}_{\lambda \in \Lambda}$ o nośniku skończonym. Sumę prostą opisanego typu określamy mianem **wewnętrznej sumy prostej podmodułów**, natomiast niezerowe elementy rozkładu $g^{(\lambda)}$ to **składowe z podmodułu $G^{(\lambda)}$** . Będziemy tu (najczęściej) stosować zapis uproszczony

$$G = \bigoplus_{\lambda \in \Lambda} G^{(\lambda)},$$

w którym kanoniczny izomorfizm między modułami po obu stronach znaku równości został opuszczony.

▲

Wygodnym jest mieć do dyspozycji kilka równoważnych praktycznych definicji wewnętrznej sumy prostej. Dostarcza ich poniższe

STWIERDZENIE 85. Przyjmijmy notację Def. 67, 21, 32, 61, 64, 75, 77, 78 oraz 79 i oznaczmy przez

$$\sum_{\lambda \in \Lambda} G^{(\lambda)} := \left\{ \sum_{\mu \in \Lambda} g_\mu \mid \{g_\mu\}_{\mu \in \Lambda} \in \mathcal{R}_0(G) \wedge \forall_{\mu \in \Lambda} : g_\mu \in G^{(\mu)} \right\}$$

sumę algebraiczną podmodułów z rodziny $\{G^{(\lambda)}\}_{\lambda \in \Lambda}$. Poniższe zdania są równoważne

- (i) $\sum_{\lambda \in \Lambda} G^{(\lambda)} = \bigoplus_{\lambda \in \Lambda} G^{(\lambda)}$.
- (ii) $\forall_{\mu \in \Lambda} : G^{(\mu)} \cap \sum_{\lambda \in \Lambda \setminus \{\mu\}} G^{(\lambda)} = \{0_G\}$.
- (iii) $\forall_{\{g_\lambda\}_{\lambda \in \Lambda} \in \mathcal{R}_0(G)} : \left(\left(\forall_{\lambda \in \Lambda} : g_\lambda \in G^{(\lambda)} \wedge \sum_{\lambda \in \Lambda} g_\lambda = 0_G \right) \implies \forall_{\lambda \in \Lambda} : g_\lambda = 0_G \right)$.

■

Dowód:

- (i)⇒(ii) Załóżmy, przeciwnie, że $G^{(\mu)} \cap \sum_{\lambda \in \Lambda \setminus \{\mu\}} G^{(\lambda)} \ni g_\mu \neq 0_G$, a wówczas element $g_\mu \in G$ miałby dwa rozkłady, mianowicie

$$g_\mu = g_\mu +_G \sum_{\lambda \in \Lambda \setminus \{\mu\}} 0_{(\lambda)}, \quad 0_{(\lambda)} \equiv 0_G,$$

wynikający z relacji $g_\mu \in G^{(\mu)}$, oraz – dla pewnej niezerowej rodziny $\{g_\lambda\}_{\lambda \in \Lambda \setminus \{\mu\}}$ o elementach $g_\lambda \in G^{(\lambda)}$ –

$$g_\mu = 0_{(\mu)} +_G \sum_{\lambda \in \Lambda \setminus \{\mu\}} g_\lambda, \quad 0_{(\mu)} \equiv 0_G,$$

wynikający z relacji $g_\mu \in \sum_{\lambda \in \Lambda \setminus \{\mu\}} G^{(\lambda)}$. Istnienie takich dwóch istotnie różnych rozkładów przeczyłoby jednak wprost Def. 79.

- (ii)⇒(iii) Niech dla pewnej rodziny $\{g_\lambda\}_{\lambda \in \Lambda} \in \mathcal{R}_0(G)$ o elementach $g_\lambda \in G^{(\lambda)}$ zachodzi relacja

$$\sum_{\lambda \in \Lambda} g_\lambda = 0_G.$$

Powyższą relację możemy przepisać, dla dowolnego $\mu \in \Lambda$, w postaci

$$g_\mu = \sum_{\lambda \in \Lambda \setminus \{\mu\}} P_G(g_\lambda),$$

wtedy jednak widać, że $g_\mu \in G^{(\mu)} \cap \sum_{\lambda \in \Lambda \setminus \{\mu\}} G^{(\lambda)}$, więc też na mocy (ii) jest $g_\mu = 0_G$ i wniosek taki wyciągamy w odniesieniu do każdego elementu rodziny, odtwarzając tym samym (iii).

- (iii)⇒(i) Niech między pewnymi rodzinami $\{g_\lambda\}_{\lambda \in \Lambda}, \{h_\lambda\}_{\lambda \in \Lambda} \in \mathcal{R}_0(G)$ o elementach $g_\lambda, h_\lambda \in G^{(\lambda)}$ zachodzi relacja

$$\sum_{\lambda \in \Lambda} g_\lambda = \sum_{\lambda \in \Lambda} h_\lambda,$$

którą przepiszemy w postaci

$$\sum_{\lambda \in \Lambda} (g_\lambda +_G P_G(h_\lambda)) = 0_G.$$

Na podstawie (iii) wnioskujemy wtedy, że $\forall_{\lambda \in \Lambda} : g_\lambda = h_\lambda$, skąd wynika (i).

□

Prostą a ważną konsekwencją powyższego jest

STWIERDZENIE 86. *Przyjmijmy notację Def. 67, 21, 32, 61, 64, 68, 75, 78 i 79 oraz Stw. 75. Niechaj $((G, \phi_2, \phi_1, \phi_0), \ell)$ będzie R -modułem wolnym o bazie $\{g_\lambda\}_{\lambda \in \Lambda}$, a wtedy G jest sumą prostą swych podmodułów*

$$G = \bigoplus_{\lambda \in \Lambda} \langle g_\lambda \rangle_R.$$

■

Relacje między sumą algebraiczną, sumą prostą oraz przecięciem (pod)modułów zwięźle ujmuje

STWIERDZENIE 87. Przyjmijmy notację Def. 21, 32, 43, 61, 64, 65 i 78 oraz Przykł. 18 (7). Niechaj H_α , $\alpha \in \{1, 2\}$ będą dwoma podmodułami modułu G nad pierścieniem R i niech

$$\begin{aligned} j_1 &: H_1 \longrightarrow H_1 +_G H_2 : h_1 \longmapsto h_1 +_G 0_G, \\ j_2 &: H_2 \longrightarrow H_1 +_G H_2 : h_2 \longmapsto 0_G +_G h_2, \\ j_1^\cap &: H_1 \cap H_2 \longrightarrow H_1 \longrightarrow H_1 \oplus H_2 : h \longmapsto h \longmapsto (h, 0_G), \\ j_2^\cap &: H_1 \cap H_2 \longrightarrow H_2 \longrightarrow H_1 \oplus H_2 : h \longmapsto h \longmapsto (0_G, h) \end{aligned}$$

oznaczając iniekcje kanoniczne. Wówczas poniższy ciąg R -modułów jest dokładny:

$$0 \longrightarrow H_1 \cap H_2 \xrightarrow{j_1^\cap + j_2^\cap} H_1 \oplus H_2 \xrightarrow{j_1 \circ \text{pr}_1 + \text{P}_G \circ j_2 \circ \text{pr}_2} H_1 +_G H_2 \longrightarrow 0.$$

■

Dowód: Najpierw dowodzimy iniektywności $j_1^\cap + j_2^\cap$ licząc, dla dowolnego $h \in H_1 \cap H_2$,

$$(0_G, 0_G) = (j_1^\cap + j_2^\cap)(h) \equiv j_1^\cap(h) +_\oplus j_2^\cap(h) = (h, 0_G) +_\oplus (0_G, h) = (h, h) \iff h = 0_G,$$

a następnie – suriektywności $j_1 \circ \text{pr}_1 + \text{P}_G \circ j_2 \circ \text{pr}_2$ znajdując, dla dowolnego $h_1 +_G h_2 \in H_1 +_G H_2$,

$$\begin{aligned} h_1 +_G h_2 &= (h_1 +_G 0_G) +_G (0_G +_G h_2) = j_1(h_1) +_G j_2(h_2) \\ &= (j_1 \circ \text{pr}_1 + \text{P}_G \circ j_2 \circ \text{pr}_2)(h_1, \text{P}_G(h_2)). \end{aligned}$$

Na koniec wykazujemy równość $\text{Ker}(j_1 \circ \text{pr}_1 + \text{P}_G \circ j_2 \circ \text{pr}_2) = \text{Im}(j_1^\cap + j_2^\cap)$ w bezpośrednim rachunku (w którym $h_\alpha \in H_\alpha$, $\alpha \in \{1, 2\}$)

$$\begin{aligned} 0_G &= (j_1 \circ \text{pr}_1 + \text{P}_G \circ j_2 \circ \text{pr}_2)(h_1, h_2) = h_1 +_G \text{P}_G(h_2) \\ \iff h_1 &= h_2 \in H_1 \cap H_2 \iff (h_1, h_2) = (j_1^\cap + j_2^\cap)(h_1). \end{aligned}$$

□

Warto prześledzić konsekwencje rozkładu modułu na sumę prostą rodziny jego podmodułów w kontekście Stw. 84. Tytułem przygotowania do tej dyskusji rozważymy

DEFINICJA 80. Przyjmijmy notację Def. 67, 21, 32, 61, 64, 65 i 80. Niechaj $((G, \phi_2, \phi_1, \phi_0), \ell)$ będzie modułem nad pierścieniem R . **Rzut** (lub **operator rzutu**) to **idempotentny** endomorfizm π modułu G , tj. taki, który spełnia tożsamość (w $\text{End}_R(G)$)

$$\pi \circ \pi = \pi.$$

Rodzinę $\{\pi_\lambda\}_{\lambda \in \Lambda}$ określamy mianem **rodziny rzutów komplementarnych** (lub **dopełniających**¹⁰), jeśli spełnione są warunki

$$\forall_{\lambda, \mu \in \Lambda} : (\lambda \neq \mu \implies \pi_\lambda \circ \pi_\mu = 0) .$$

▲

Możemy już teraz sformułować nader istotne

STWIERDZENIE 88. *Przyjmijmy notację Def. 67, 21, 32, 61, 64, 75, 78, 79 i 80. Jeśli moduł G nad pierścieniem R jest sumą prostą rodziny $\{G^{(\lambda)}\}_{\lambda \in \Lambda}$ swoich podmodułów, wówczas rzuty kanoniczne $\text{pr}_\mu : G = \bigoplus_{\lambda \in \Lambda} G^{(\lambda)} \longrightarrow G^{(\mu)}$ na podmoduły $G^{(\mu)}$ wraz z iniekcjami kanonicznymi $j_\mu : G^{(\mu)} \longrightarrow G$ indukują rodzinę rzutów komplementarnych*

$$\pi_\mu := j_\mu \circ \text{pr}_\mu : G \hookrightarrow G \quad : \quad \sum_{\lambda \in \Lambda} g_\lambda \mapsto g_\mu + \sum_{\lambda \in \Lambda \setminus \{\mu\}} 0_G \equiv g_\mu$$

o własności

$$\forall_{g \in G} : g = \sum_{\lambda \in \Lambda} \pi_\lambda(g) ,$$

którą będziemy też zapisywać w postaci¹¹

$$(8.12) \quad \sum_{\lambda \in \Lambda} \pi_\lambda = \text{id}_G$$

I odwrotnie, każda rodzina $\{\pi_\lambda\}_{\lambda \in \Lambda} \subset \text{End}_R(G)$ rzutów komplementarnych o własności (8.12) określonych na module G nad pierścieniem R zadaje rozkład G na sumę prostą

$$G = \bigoplus_{\lambda \in \Lambda} \pi_\lambda(G) .$$

Rodzinę rzutów komplementarnych o własności będziemy nazywać **zupełną**.

■

Dowód: Niech $G = \bigoplus_{\lambda \in \Lambda} G^{(\lambda)}$, a wtedy dowolny element $g \in G$ ma jednoznaczny rozkład $g = \sum_{\lambda \in \Lambda} g_\lambda$ na składowe $g_\lambda \in G^{(\lambda)}$, zatem tożsamość (8.12) jest automatycznie spełniona. Pozostaje sprawdzić, że rzuty kanoniczne są wzajemnie komplementarnymi idempotentami. Dla dowolnego g o rozkładzie jak wyżej wyznaczamy

$$\pi_\mu \circ \pi_\mu(g) \equiv \pi_\mu \circ \pi_\mu \left(\sum_{\lambda \in \Lambda} g_\lambda \right) = \pi_\mu(g_\mu) ,$$

co wobec jednoznaczności rozkładu każdego z elementów G , a więc w szczególności

$$g_\mu = g_\mu + \sum_{\lambda \in \Lambda \setminus \{\mu\}} 0_G ,$$

¹⁰Bourbaki używa w odniesieniu do odwzorowań π_λ określenia „rzuty ortogonalne”, my jednak rezerwujemy to określenie dla pewnego typu rzutów komplementarnych w przestrzeni z iloczynem skalarnym, patrz: Rozdz. 9.

¹¹Należy podkreślić, że w przypadku nieskończonej rodziny modułów zapis ten jest umowny, oto bowiem suma w nim występująca jest nieskończona. Skończoną jest natomiast każda z sum w równości poprzedniej.

daje pożądaną wynik

$$\pi_\mu \circ \pi_\mu(g) = \pi_\mu \left(g_\mu +_G \sum_{\lambda \in \Lambda \setminus \{\mu\}} 0_G \right) = g_\mu = \pi_\mu(g).$$

Analogicznie pokazujemy komplementarność wzajemną π_μ i π_ν dla dowolnych $\mu \neq \nu$,

$$\pi_\nu \circ \pi_\mu(g) = \pi_\nu(g_\mu) = \pi_\nu \left(g_\mu +_G 0_{(\nu)} +_G \sum_{\lambda \in \Lambda \setminus \{\mu, \nu\}} 0_G \right) = 0_{(\nu)} = 0(g).$$

Niechaj teraz $\{\pi_\lambda\}_{\lambda \in \Lambda}$ będzie rodziną rzutów komplementarnych o własności (8.12). Ta ostatnia oznacza, że

$$G \subset \sum_{\lambda \in \Lambda} \pi_\lambda(G),$$

a ponieważ zachodzi także zawieranie odwrotne, przeto

$$G = \sum_{\lambda \in \Lambda} \pi_\lambda(G).$$

Niechaj teraz będzie dana dowolna rodzina $\{\pi_\lambda(g_\lambda)\}_{\lambda \in \Lambda} \in \mathcal{R}_0(G)$ elementów $g_\lambda \in G$ o własności

$$\sum_{\lambda \in \Lambda} \pi_\lambda(g_\lambda) = 0_G.$$

Wykorzystując komplementarność rzutów π_λ , wyliczamy wtedy, dla każdego $\mu \in \Lambda$ z osobna,

$$0_G = \pi_\mu(0_G) = \pi_\mu \left(\sum_{\lambda \in \Lambda} \pi_\lambda(g_\lambda) \right) = \sum_{\lambda \in \Lambda} \pi_\mu \circ \pi_\lambda(g_\lambda) = \pi_\mu \circ \pi_\mu(g_\mu) = \pi_\mu(g_\mu).$$

Na mocy Stw. 85 jest zatem

$$\bigoplus_{\lambda \in \Lambda} \pi_\lambda(G) = \sum_{\lambda \in \Lambda} \pi_\lambda(G) = G.$$

□

Wysłowimy teraz proste acz ważne corollarium ostatniego stwierdzenia, będące rozwinięciem dyskusji naturalnego związku między (wewnętrznymi) sumami prostymi modułów a operatorami rzutowymi i tym samym przygotowujące grunt pod dalszą część wykładu.

STWIERDZENIE 89. *Przyjmijmy notację Def. 21, 32, 36, 61, 78, 79 i 80. Niechaj $\pi \in \text{End}_R(G)$ będzie rzutem. Wówczas*

(i) *odwzorowanie*

$$\text{id}_G - \pi : G \rightarrow G : g \mapsto g +_G P_G \circ \pi(g)$$

jest rzutem;

(ii) $\text{Ker}(\text{id}_G - \pi) = \text{Im } \pi$ oraz $\text{Im}(\text{id}_G - \pi) = \text{Ker } \pi$;

(iii) $G = \text{Ker } \pi \oplus \text{Im } \pi$, przy czym dla dowolnego elementu $g \in G$ o rozkładzie $g = g_1 +_G g_2$ na składowe $g_1 \in \text{Ker } \pi$ i $g_2 \in \text{Im } \pi$ zachodzi równość $g_2 = \pi(g)$.

■

Dowód:

Ad (i) Sprawdzamy, dla dowolnego $g \in G$,

$$\begin{aligned}
 (\text{id}_G - \pi) \circ (\text{id}_G - \pi)(g) &= (\text{id}_G - \pi)(g +_G P_G \circ \pi(g)) \\
 &= g +_G P_G \circ \pi(g) +_G P_G \circ \pi(g +_G P_G \circ \pi(g)) \\
 &= g +_G P_G \circ \pi(g) +_G P_G \circ \pi(g) +_G \pi \circ \pi(g) \\
 &= g +_G P_G \circ \pi(g) +_G P_G \circ \pi(g) +_G \pi(g) \\
 &= g +_G P_G \circ \pi(g) \equiv (\text{id}_G - \pi)(g).
 \end{aligned}$$

Ad (ii) Bezpośrednim rachunkiem dowodzimy też tożsamości

$$(8.13) \quad \pi \circ (\text{id}_G - \pi) = 0 = (\text{id}_G - \pi) \circ \pi,$$

które w połączeniu z oczywistą równością

$$\text{id}_G = \pi_G + (\text{id}_G - \pi).$$

oznaczają, wobec Stw. 88, że

$$(8.14) \quad G = \text{Im}(\text{id}_G - \pi) \oplus \text{Im} \pi.$$

Ponadto (8.13) implikuje

$$\text{Im}(\text{id}_G - \pi) \subset \text{Ker} \pi$$

oraz

$$\text{Im} \pi \subset \text{Ker}(\text{id}_G - \pi).$$

Niech $g \in \text{Ker} \pi$, a wtedy

$$g \equiv (\pi_G +_G (\text{id}_G - \pi))(g) = \pi_G(g) +_G (\text{id}_G - \pi)(g) = (\text{id}_G - \pi)(g) \in \text{Im}(\text{id}_G - \pi),$$

czyli $\text{Ker} \pi \subset \text{Im}(\text{id}_G - \pi)$, więc też ostatecznie

$$(8.15) \quad \text{Ker} \pi = \text{Im}(\text{id}_G - \pi).$$

Dowód równości

$$\text{Ker}(\text{id}_G - \pi) = \text{Im} \pi,$$

przebiega analogicznie.

Ad (iii) Żądaną tożsamość otrzymujemy wprost z (8.14) podstawiając (8.15). Jednoznaczny rozkład dowolnego $g \in G$ na składowe z $\text{Ker} \pi$ i $\text{Im} \pi$ to teraz

$$g \equiv (\pi_G +_G (\text{id}_G - \pi))(g) = (\text{id}_G - \pi)(g) +_G \pi(g),$$

skąd wynika ostatnia część tezy dowodzonego punktu stwierdzenia. $\square$

Dotychczasowe nasze rozważania w naturalny sposób prowadzą do pytania o istnienie rozkładu modułu na sumę prostą zadawanego przez dowolny jego podmoduł. Jak się okaże, twierdząca odpowiedź na to pytanie jest kolejnym wyróżnikiem strukturalnym przestrzeni wektorowych pośród modułów ogólnych. Zanim jednak przekonamy się o tym, wprowadźmy niezbędne pojęcia.

DEFINICJA 81. Przyjmijmy notację Def. 21, 32, 61, 64, 75, 78 i 79. **Dopełnienie proste** podmodułu $H_1 \subset G$ modułu G nad pierścieniem R to podmoduł $H_2 \subset G$ o własności

$$G = H_1 \oplus H_2.$$

Podmoduł $H_1 \subset G$ posiadający dopełnienie proste w G nazywamy **składnikiem prostym** G .

▲

Przywoławszy konstrukcję i kanoniczne przykłady krótkich ciągów dokładnych z Rozdz. 5, uświadamiamy sobie bez trudu, że są one właściwym narzędziem formalnym pozwalającym precyzyjnie sformułować warunki istnienia dopełnienia prostego. Przekonuje nas o tym

TWIERDZENIE 8.10 (O rozszczepialności modułu). *Przyjmijmy notację Def. 21, 32, 43, 61, 64, 75, 78 i 79 oraz Przykł. 25. Niechaj $((G^{(\alpha)}, \phi_2^{(\alpha)}, \phi_1^{(\alpha)}, \phi_0^{(\alpha)}), \ell^{(\alpha)})$, $\alpha \in \{1, 2, 3\}$ będą trzema modułami nad pierścieniem R i niech*

$$(8.16) \quad \mathbf{0} \longrightarrow G^{(1)} \xrightarrow{\chi^{(1)}} G^{(2)} \xrightarrow{\chi^{(2)}} G^{(3)} \longrightarrow \mathbf{0}$$

będzie krótkim ciągiem dokładnym modułów. Poniższe warunki są wówczas równoważne.

- (i) $\text{Im } \chi^{(1)}$ jest składnikiem prostym modułu $G^{(2)}$.
- (ii) Istnieje odwzorowanie R -liniowe $\rho : G^{(2)} \longrightarrow G^{(1)}$ będące lewostronną odwrotnością $\chi^{(1)}$, tj. takie, że $\rho \circ \chi^{(1)} = \text{id}_{G^{(1)}}$ (odwzorowanie takie nosi miano **retrakcji liniowej stowarzyszonej z $\chi^{(1)}$**).
- (iii) Istnieje odwzorowanie R -liniowe $\sigma : G^{(3)} \longrightarrow G^{(2)}$ będące prawostronną odwrotnością $\chi^{(2)}$, tj. takie, że $\chi^{(2)} \circ \sigma = \text{id}_{G^{(3)}}$ (odwzorowanie takie nosi miano **cięcia liniowego stowarzyszonego z $\chi^{(2)}$**).

Ileokroć są one spełnione, odwzorowanie

$$\chi^{(1)} \circ \text{pr}_1 + {}_{(2)}\sigma \circ \text{pr}_2 : G^{(1)} \oplus G^{(3)} \longrightarrow G^{(2)}$$

*jest izomorfizmem R -modułów (zadającym rozkład przeciwdziedziny na sumę prostą podmodułów). O ciągu dokładnym mającym tę własność mówimy, że **rozszczepia się** (albo że jest **rozszczepiony**), trójkę $(G^{(2)}, \chi^{(1)}, \chi^{(2)})$ zaś nazywamy **trywialnym rozszerzeniem modułu $G^{(3)}$ przez moduł $G^{(1)}$** , por. Def. 43.*

■

Dowód:

- (i) $\Leftrightarrow$ (ii) Ileokroć $H^{(2)} := \text{Im } \chi^{(1)}$ jest składnikiem prostym $G^{(2)}$, istnieje – na mocy Stw. 88 – operator rzutu $\pi \in \text{End}_R(G^{(2)})$ na tenże obraz, dla którego spełniona jest – w świetle Stw. 89 – tożsamość

$$(8.17) \quad \pi(G^{(2)}) = H^{(2)}.$$

Oznaczmy przez $\chi_{H^{(2)}}^{(1)-1}$ izomorfizm będący odwrotnością monomorfizmu $\chi^{(1)}$ określoną na $H^{(2)}$ w zgodzie z Tw. 8.1. Łatwo sprawdzamy, że homomorfizm

$$\chi_{H^{(2)}}^{(1)-1} \circ \pi : G^{(2)} \longrightarrow G^{(1)}$$

jest poszukiwaną retrakcją liniową stowarzyszoną z $\chi^{(1)}$, oto bowiem dla dowolnego $g^{(1)} \in G^{(1)}$ istnieje – z racji (8.17) – $g^{(2)} \in G^{(2)}$ o własności

$$\chi^{(1)}(g^{(1)}) = \pi(g^{(2)}),$$

a zatem

$$\begin{aligned} \chi_{H^{(2)}}^{(1)-1} \circ \pi \circ \chi^{(1)}(g^{(1)}) &\equiv \chi_{H^{(2)}}^{(1)-1} \circ \pi \circ \pi(g^{(2)}) = \chi_{H^{(2)}}^{(1)-1} \circ \pi(g^{(2)}) \\ &= \chi_{H^{(2)}}^{(1)-1} \circ \chi^{(1)}(g^{(1)}) = g^{(1)}. \end{aligned}$$

I odwrotnie, dowolna taka retrakcja ρ definiuje odwzorowanie R -liniowe

$$\chi^{(1)} \circ \rho \in \text{End}_R(G^{(2)}),$$

które spełnia tożsamość

$$(\chi^{(1)} \circ \rho) \circ (\chi^{(1)} \circ \rho) \equiv \chi^{(1)} \circ (\rho \circ \chi^{(1)}) \circ \rho = \chi^{(1)} \circ \text{id}_{G^{(1)}} \circ \rho = \chi^{(1)} \circ \rho,$$

jest zatem operatorem rzutu, a przy tym dla dowolnego elementu obrazu $g^{(2)} = \chi^{(1)}(g^{(1)}) \in H^{(2)}$ obliczamy

$$\chi^{(1)} \circ \rho(g^{(2)}) = \chi^{(1)} \circ (\rho \circ \chi^{(1)})(g^{(1)}) = \chi^{(1)} \circ \text{id}_{G^{(1)}}(g^{(1)}) = \chi^{(1)}(g^{(1)}) = g^{(2)},$$

więc też

$$\text{Im}(\chi^{(1)} \circ \rho) \supset H^{(2)}.$$

Jest też oczywiście

$$\text{Im}(\chi^{(1)} \circ \rho) \subset H^{(2)},$$

przeto $\chi^{(1)} \circ \rho$ jawi się być rzutem na $\text{Im}(\chi^{(1)} \circ \rho) = H^{(2)}$, a w konsekwencji $H^{(2)}$ jest składnikiem prostym $G^{(2)}$ na mocy Stw. 89.

(i) $\Leftrightarrow$ (iii) Jeśli $G^{(2)} = H^{(2)} \oplus D$, to wtedy iniekcja kanoniczna $j_D : D \rightarrow G^{(2)}$ definiuje homomorfizm R -modułów

$$\chi^{(2)} \circ j_D : D \rightarrow G^{(3)}.$$

Nietrudno się przekonać, że wobec istnienia rozkładu

$$G^{(2)} = H^{(2)} \oplus D = \text{Ker } \chi^{(2)} \oplus D,$$

będącego konsekwencją dokładności ciągu rozważanego, $\chi^{(2)} \circ j_D$ jest izomorfizmem. W rzeczy samej, po pierwsze jest to monomorfizm, bowiem

$$\text{Ker}(\chi^{(2)} \circ j_D) = D \cap \text{Ker } \chi^{(2)} = \{0_{(2)}\},$$

przy czym ostatnia równość wynika wprost ze specjalizacji Stw. 85 (ii) do przypadku $\Lambda = \{1, 2\}$, w którym

$$(848) \quad G^{(1)} \oplus G^{(2)} \iff (G = G^{(1)} +_G G^{(2)} \quad \wedge \quad G^{(1)} \cap G^{(2)} = \{0_G\}).$$

Jest to także epimorfizm, gdyż z racji surjektywności $\chi^{(2)}$ dla dowolnego $g^{(3)} \in G^{(3)}$ możemy znaleźć $h \in G^{(2)}$ o własności $\chi^{(2)}(h) = g^{(3)}$, który po rozbiciu na składowe $h_1 \in \text{Ker } \chi^{(2)}$ i $h_2 \in D$ do postaci $h = h_1 +_{(2)} h_2$ daje nam

$$\chi^{(2)}(h_2) = \chi^{(2)}(h) = g^{(3)}.$$

Odwrotność izomorfizmu $\chi^{(2)} \circ j_D$, złożona z j_D jest pożądanym cięciem liniowym stowarzyszonym z $\chi^{(2)}$. Istotnie,

$$\chi^{(2)} \circ (j_D \circ (\chi^{(2)} \circ j_D)^{-1}) \equiv (\chi^{(2)} \circ j_D) \circ (\chi^{(2)} \circ j_D)^{-1} = \text{id}_{G^{(3)}}.$$

I odwrotnie, jeśli tylko istnieje takowe cięcie σ , to wtedy odwzorowanie R -liniowe

$$\sigma \circ \chi^{(2)} \in \text{End}_R(G^{(2)})$$

jest rzutem, albowiem spełnia tożsamość

$$(\sigma \circ \chi^{(2)}) \circ (\sigma \circ \chi^{(2)}) \equiv \sigma \circ (\chi^{(2)} \circ \sigma) \circ \chi^{(2)} = \sigma \circ \text{id}_{G^{(3)}} \circ \chi^{(2)} = \sigma \circ \chi^{(2)}.$$

Jego jądro zawiera $H^{(2)}$, gdyż

$$\text{Ker}(\sigma \circ \chi^{(2)}) \supset \text{Ker} \chi^{(2)} = \text{Im} \chi^{(1)} \equiv H^{(2)},$$

ale też dla dowolnego $g \in \text{Ker}(\sigma \circ \chi^{(2)})$ stwierdzamy, że

$$0_{(3)} = \chi^{(2)}(0_{(2)}) = \chi^{(2)}((\sigma \circ \chi^{(2)})(g)) \equiv (\chi^{(2)} \circ \sigma) \circ \chi^{(2)}(g) = \chi^{(2)}(g),$$

skąd

$$\text{Ker}(\sigma \circ \chi^{(2)}) \subset \text{Ker} \chi^{(2)} = H^{(2)}.$$

Ostatecznie zatem

$$\text{Ker}(\sigma \circ \chi^{(2)}) = H^{(2)},$$

czyli $H^{(2)}$ jest obrazem operatora rzutowego $\text{id}_{G^{(2)}} - \sigma \circ \chi^{(2)}$ (patrz: Stw. 89 (i) i (ii)) i jako taki ma dopełnienie proste $\text{Im}(\sigma \circ \chi^{(2)}) \equiv \text{Im} \sigma$, wedle Stw. 89 (iii).

Jak wynika wprost z powyższej analizy, przy spełnionych równoważnych warunkach (i)-(iii) znajdujemy rozkład

$$G = \chi^{(1)}(G^{(1)}) \oplus \sigma(G^{(3)}),$$

a to jawny dowód prawdziwości ostatniej części tezy twierdzenia. $\square$

Godzi się zauważyć, że ostatnie twierdzenie jest naturalną reinkarnacją Tw. 5.5 w strukturalnie bogatszym kontekście teorii grup przemennych z działaniem pierścienia.

Proste kryterium rozszczepialności modułu dostarcza

STWIERDZENIE 90. *Przyjmijmy notację Def. 21, 32, 43, 61, 64, 75, 78 i 79, Przykł. 25 oraz Tw. 8.10. Jeśli moduł $G^{(3)}$ jest wolny, wówczas krótki ciąg dokładny (8.16) rozszczepia się, tj. zachodzi*

$$G^{(2)} \cong G^{(1)} \oplus G^{(3)}.$$

■

Dowód: Niechaj $\{g_\lambda^{(3)}\}_{\lambda \in \Lambda}$ będzie bazą modułu $G^{(3)}$, z którą z racji surjektywności $\chi^{(2)}$ możemy stowarzyszyć rodzinę $\{g_\lambda^{(2)}\}_{\lambda \in \Lambda}$ elementów modułu $G^{(2)}$, jak następuje:

$$\forall \lambda \in \Lambda : \chi^{(2)}(g_\lambda^{(2)}) = g_\lambda^{(3)}.$$

Jedyne odwzorowanie R -liniowe $\sigma : G^{(3)} \longrightarrow G^{(2)}$ o własności

$$\forall \lambda \in \Lambda : \sigma(g_\lambda^{(3)}) = g_\lambda^{(2)},$$

o którego istnieniu orzeka Stw. 80, jest ciągiem liniowym stowarzyszonym z $\chi^{(2)}$, oto bowiem dla dowolnego elementu $g \in G^{(3)}$ o rozkładzie (w bazie) $g = \sum_{\lambda \in \Lambda} r_\lambda \triangleright_{(3)}$ $g_\lambda^{(3)}$ stwierdzamy równość

$$\begin{aligned} \chi^{(2)} \circ \sigma(g) &= \chi^{(2)} \left(\sum_{\lambda \in \Lambda} r_\lambda \triangleright_{(2)} \sigma(g_\lambda^{(3)}) \right) = \chi^{(2)} \left(\sum_{\lambda \in \Lambda} r_\lambda \triangleright_{(2)} g_\lambda^{(2)} \right) \\ &= \sum_{\lambda \in \Lambda} r_\lambda \triangleright_{(3)} \chi^{(2)}(g_\lambda^{(2)}) = \sum_{\lambda \in \Lambda} r_\lambda \triangleright_{(3)} g_\lambda^{(3)} = g. \end{aligned}$$

Teza stwierdzenia wynika teraz wprost z Tw. 8.10. $\square$

Użytecznym uzupełnieniem opisu modułów rozszczepiających się na sumę prostą swych podmodułów jest poniższe oczywiste

STWIERDZENIE 91. *Przyjmijmy notację Def. 67, 21, 32, 61, 64, 68, 70, 75, 78 i 79 oraz Stw. 75. Niechaj $\mathcal{B}^{(\lambda)} \subset G^{(\lambda)}$, $\lambda \in \Lambda$ będą bazami podmodułów $G^{(\lambda)} \subset G$ R -modułu G . Jeśli moduł ten ma rozkład na sumę prostą*

$$G = \bigoplus_{\lambda \in \Lambda} G^{(\lambda)},$$

wówczas zbiór

$$\mathcal{B} := \bigcup_{\lambda \in \Lambda} \mathcal{B}^{(\lambda)}$$

jest jego bazą.¹² W szczególności więc rząd modułu (nad ciałem o cesze IBN) będącego sumą prostą podmodułów jest sumą rządów tychże podmodułów. $\blacksquare$

Nasza analiza prowadzi nas wprost do istotnego wyróżnika (pod)przestrzeni wektorowych.

COROLLARIUM 13. *Każda podprzestrzeń przestrzeni wektorowej ma dopełnienie proste.* $\blacksquare$

Dowód: Wystarczy rozważyć normalny ciąg dokładny (8.3) stowarzyszony z daną podprzestrzenią $W \subset V$ przestrzeni V . Na mocy Tw. 8.5 przestrzeń ilorazowa V/W jest modulem wolnym, a zatem można zastosować Stw. 90. Otrzymujemy w ten sposób kanoniczny rozkład

$$V = W \oplus \widetilde{W}, \quad \widetilde{W} \cong V/W.$$

$\square$

Tę część dyskusji zamknijmy pożytecznym wynikiem natury buchalteryjnej.

¹²W analogiczny sposób tworzymy (jako sumy teoriomnogościowe odnośnych podzbiorów składników prostych po zbiorze indeksów) podzbiory generujące oraz liniowo niezależne G .

STWIERDZENIE 92. („Kwantowy” bilans wymiarów) *Przyjmijmy notację Def. 11, 32, 61, 63, 64, 73, 78 i 79. Niechaj V_α , $\alpha \in \{1, 2\}$ będą dwiema podprzestrzeniami przestrzeni wektorowej V nad ciałem $\mathbb{K}$. Wówczas prawdziwą jest równość*

$$\dim_{\mathbb{K}} V_1 + \dim_{\mathbb{K}} V_2 = \dim_{\mathbb{K}}(V_1 +_V V_2) + \dim_{\mathbb{K}}(V_1 \cap V_2).$$

■

Dowód: Rozpatrzmy krótki ciąg dokładny z treści Stw. 87, w którym kładziemy $H_\alpha := V_\alpha$, i zastosujmy Stw. 90 (tudzież Cor. 13), aby dostać

$$V_1 \oplus V_2 \cong (V_1 +_V V_2) \oplus (V_1 \cap V_2).$$

Przywoławszy Stw. 91 oraz 82, wyliczamy

$$\begin{aligned} \dim_{\mathbb{K}} V_1 + \dim_{\mathbb{K}} V_2 &= \dim_{\mathbb{K}}(V_1 \oplus V_2) = \dim_{\mathbb{K}}((V_1 +_V V_2) \oplus (V_1 \cap V_2)) \\ &= \dim_{\mathbb{K}}(V_1 +_V V_2) + \dim_{\mathbb{K}}(V_1 \cap V_2). \end{aligned}$$

□

Warto zwrócić uwagę, że powyższe stwierdzenie bywa wykorzystywane jako wygodne kryterium istnienia rozkładu przestrzeni wektorowej na sumę prostą jej podprzestrzeni.

PRZYKŁAD(Y) 42. Doskonałej ilustracji tez zgromadzonych w ostatniej części wykładu dostarcza analiza porównawcza dwóch prostych przykładów $\mathbb{Z}$ -modułu, a mianowicie nieizomorficznych grup przemennych rzędu 4.

Pierwsza z nich to grupa cykliczna

$$C_4 := \{0, g, 2g, 3g\} \cong \mathbb{Z}/4\mathbb{Z}$$

o tabelce dodawania

+	0	g	2g	3g
0	0	g	2g	3g
g	g	2g	3g	0
2g	2g	3g	0	g
3g	3g	0	g	2g

Grupa ta jest nośnikiem struktury modułu nad pierścieniem $\mathbb{Z}$ z działaniem

$$\ell : \mathbb{Z} \times C_4 \longrightarrow C_4 : x \longmapsto nx.$$

Jedynym podmodułem właściwym C_4 jest

$$H := \{0, 2a\} \cong \mathbb{Z}/2\mathbb{Z}.$$

Jest jasnym, że H nie posiada dopełnienia w C_4 . Istotnie, dopełnienie takie nie może zawierać g ani $3g$, bo jako podmoduł zawierałoby wtedy także wszystkie elementy postaci ng wzgl. $3ng$, czyli cały moduł C_4 , co oznaczałoby nietrywialne przecięcie $H \cap C_4 = H \neq \{0\}$ podmodułu H z jego dopełnieniem. Ponieważ zaś z definicji nie może zawierać $2g$, przeto nie istnieje.

$\mathbb{Z}$ izomorfizmu $H \cong \mathbb{Z}/2\mathbb{Z}$ wynika istnienie ciągu dokładnego $\mathbb{Z}$ -modułów

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\chi} C_4 \xrightarrow{\psi} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0,$$

w którym odwzorowania $\mathbb{Z}$ -liniowe χ i ψ są określone (jednoznacznie) na generatorach odnośnych grup, jak następuje:

$$\chi([1]_2) = 2a, \quad \psi(g) = [1]_2.$$

Zauważmy, że jest to jedyny wybór gwarantujący dokładność wypisanego ciągu modułów. Spróbujemy teraz skonstruować retrakcję liniową $\rho : C_4 \rightarrow \mathbb{Z}/2\mathbb{Z}$ monomorfizmu χ . Tożsamość definiująca

$$(8.19) \quad \rho \circ \chi = \text{id}_{\mathbb{Z}/2\mathbb{Z}}$$

narzuca wybór wartości ρ na podzbiorze $\chi(\mathbb{Z}/2\mathbb{Z}) = \{0, 2a\}$ w postaci

$$\rho(0) = [0]_2, \quad \rho(2g) = [1]_2.$$

Położmy następnie $\rho(g) = [k]_2$, $k \in \{0, 1\}$, a wtedy

$$[1]_2 = \rho(2g) = 2\rho(g) = 2[k]_2 = [2k]_2 = [0]_k,$$

czyli sprzeczność. Wnioskujemy na tej podstawie, że retrakcja liniowa χ nie istnieje, co obrazuje pierwszą część tezy Tw. 8.10. Część druga orzeka o nieistnieniu cięcia liniowego $\sigma : \mathbb{Z}/2\mathbb{Z} \rightarrow C_4$ epimorfizmu ψ . Odnośna tożsamość definiująca,

$$(8.20) \quad \psi \circ \sigma = \text{id}_{\mathbb{Z}/2\mathbb{Z}}$$

pozostawia nam dwie możliwości:

$$\sigma([1]_2) \in \{g, 3g\}.$$

W obu przypadkach dostajemy

$$0 = \sigma([0]_2) = \sigma(2[1]_2) = 2\sigma([1]_2) = 2g,$$

czyli sprzeczność, która pokazuje, że σ nie istnieje.

Drugi z interesujących nas przykładów to **grupa czwórkowa Kleina**¹³

$$V := \{0, g, h, g+h\},$$

czyli najmniejsza niecykliczna grupa przemienna, o tabelce dodawania

+	0	g	h	g+h
0	0	g	h	g+h
g	g	0	g+h	h
h	h	g+h	0	g
g+h	g+h	h	g	0

I w tym przypadku mamy rozważamy strukturę modułu nad pierścieniem $\mathbb{Z}$ z działaniem

$$\ell : \mathbb{Z} \times V \rightarrow V : x \mapsto nx,$$

natrafiając przy tym na trzy podmoduły właściwe:

$$G := \{0, g\}, \quad H := \{0, h\}, \quad S := \{0, g+h\},$$

z których każdy jest izomorficzny z $\mathbb{Z}/2\mathbb{Z}$. Bez trudu wykazujemy prawdziwość następujących relacji

$$(8.21) \quad V = G \oplus H = S \oplus G = H \oplus S,$$

korzystając z kryterium (ii) ze Stw. 85 w wersji (8.18). Oto więc

$$G \cap H = \{0\} = S \cap G = H \cap S,$$

¹³W zachodniej literaturze bywa ona nazywana z niemiecka “Vierergruppe” (nie mylić, nawet w wymowie, z “Führergruppe”), stąd też standardowe oznaczenie jej nośnika.

a do tego

$$g = g + 0 = 0 + g = h + (g + h), \quad h = 0 + h = (g + h) + g = h + 0,$$

co potwierdza słuszność Równ. (8.21). Możemy zatem zapisać

$$\mathbf{V} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z},$$

a ponieważ automorfizmy $\mathbf{V}$ zadane (na generatorach g, h) wzorami

$$\begin{aligned} \alpha_1(g) &:= g, & \alpha_1(h) &:= g + h, \\ \alpha_2(g) &:= h, & \alpha_2(h) &:= g + h \end{aligned}$$

przeprowadzają poszczególne rozkłady w siebie nawzajem wedle schematu

$$\alpha_1(G \oplus H) = G \oplus S, \quad \alpha_2(G \oplus H) = H \oplus S,$$

istnienie dowolnego z tych rozkładów jest równoważne istnieniu pozostałych. Możemy przeto ograniczyć dalsze rozważania do jednego z nich, np. do

$$\mathbf{V} = G \oplus H.$$

Dotychczasowa dyskusja uzasadnia konstrukcję ciągu dokładnego $\mathbb{Z}$ -modułów

$$\mathbf{0} \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\chi} \mathbf{V} \xrightarrow{\psi} \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbf{0}.$$

I tym razem dokładność ciągu wymusza na nas konkretną postać odwzorowań $\mathbb{Z}$ -liniowych χ i ψ , które są określone na generatorach odnośnych grup, jak następuje:

$$\chi([1]_2) = g, \quad \psi(g) = [0]_2, \quad \psi(h) = [1]_2.$$

Ograniczenie retrakcji liniowej $\rho : \mathbf{V} \longrightarrow \mathbb{Z}/2\mathbb{Z}$ monomorfizmu χ do podmodułu $\chi(\mathbb{Z}/2\mathbb{Z}) = \{0, g\}$ jest – jak uprzednio – wyznaczone jednoznacznie przez warunek (8.19),

$$\rho(0) = [0]_2, \quad \rho(g) = [1]_2,$$

i dopuszcza dwa rozszerzenia do $\mathbf{V}$, określone przez wartości przyjmowane na drugim generatorze,

$$\rho(h) \in \{[0]_2, [1]_2\}.$$

Bez trudu przekonujemy się, że każde z rozszerzeń prowadzi do definicji homomorfizmu $\mathbb{Z}$ -modułów będącego lewostronną odwrotnością χ . Analogicznie stwierdzamy, że ciągi liniowe $\sigma : \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbf{V}$ epimorfizmu ψ musi spełniać warunki

$$\sigma([0]_2) = 0, \quad \sigma([1]_2) \in \{h, g + h\},$$

przy czym każdy z wyborów definiuje prawostronną odwrotność ψ . W sumie raz jeszcze zyskujemy bezpośrednie potwierdzenie – tym razem wprost – tezy Tw. 8.10.

✓

8.6. Macierzowy opis modułów rozzszczepionych i ich homomorfizmów

Spożytkujemy obecnie zgromadzone elementy opisu modułu nad pierścieniem oraz konstrukcje produktu i sumy prostej modułów w szczegółowej dyskusji struktury odwzorowań R -liniowych, która w naturalny sposób doprowadzi nas do macierzowej realizacji tych odwzorowań. Ich najbardziej elementarne własności zostały już omówione w Stw. 70 i 71. Rozpoczętą wtedy wstępną charakterystykę homomorfizmów uzupełniamy o użyteczne

STWIERDZENIE 93. *Przyjmijmy notację Def. 21, 32, 35, 61 oraz 65. Niechaj $((G^{(\alpha)}, \phi_2^{(\alpha)}, \phi_1^{(\alpha)}, \phi_0^{(\alpha)}), \ell^{(\alpha)})$, $\alpha \in \{1, 2, 3\}$ będą trzema modułami nad pierścieniem R . Dowolne odwzorowanie R -liniowe $\Phi \in \text{Hom}_R(G^{(1)}, G^{(2)})$ indukuje homomorfizm grup przemiennych*

$$\text{Hom}_R(\Phi, G^{(3)}) : \text{Hom}_R(G^{(2)}, G^{(3)}) \longrightarrow \text{Hom}_R(G^{(1)}, G^{(3)}) : \chi \longmapsto \chi \circ \Phi.$$

Analogicznie, dowolne odwzorowanie R -liniowe $\Psi \in \text{Hom}_R(G^{(2)}, G^{(3)})$ określa homomorfizm grup przemiennych

$$\text{Hom}_R(G^{(1)}, \Psi) : \text{Hom}_R(G^{(1)}, G^{(2)}) \longrightarrow \text{Hom}_R(G^{(1)}, G^{(3)}) : \chi \longmapsto \Psi \circ \chi.$$

■

Dowód: Dla dowolnych dwóch $\chi_1, \chi_2 \in \text{Hom}_R(G^{(2)}, G^{(3)})$ dostajemy równość

$$\begin{aligned} \text{Hom}_R(\Phi, G^{(3)})(\chi_1 + \chi_2) &= (\chi_1 + \chi_2) \circ \Phi = \chi_1 \circ \Phi + \chi_2 \circ \Phi \\ &= \text{Hom}_R(\Phi, G^{(3)})(\chi_1) + \text{Hom}_R(\Phi, G^{(3)})(\chi_2). \end{aligned}$$

Dowód homomorficzności $\text{Hom}_R(G^{(1)}, \Psi)$ przebiega identycznie. □

Wprowadzone powyżej obiekty pozwalają nam dokonać związanej parafrazy warunków definiujących struktury uniwersalne dla rodziny modułów.

STWIERDZENIE 94. *Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 75, 77 i 78. Niechaj $\{G^{(\lambda)}\}_{\lambda \in \Lambda}$ będzie rodziną R -modułów i niech G będzie dowolnym R -modułem. Homomorfizmy*

$$\begin{aligned} \text{Hom}_R(j, G) &: \text{Hom}_R\left(\bigoplus_{\lambda \in \Lambda} G^{(\lambda)}, G\right) \longrightarrow \prod_{\lambda \in \Lambda} \text{Hom}_R(G^{(\lambda)}, G) : \chi \longmapsto \chi \circ j, \\ \chi \circ j &: \Lambda \longrightarrow \bigcup_{\lambda \in \Lambda} \text{Hom}_R(G^{(\lambda)}, G) : \lambda \longmapsto \chi \circ j_\lambda \end{aligned}$$

oraz

$$\begin{aligned} \text{Hom}_R(G, \text{pr}) &: \text{Hom}_R\left(G, \prod_{\lambda \in \Lambda} G^{(\lambda)}\right) \longrightarrow \prod_{\lambda \in \Lambda} \text{Hom}_R(G, G^{(\lambda)}) : \chi \longmapsto \text{pr} \circ \chi, \\ \text{pr} \circ \chi &: \Lambda \longrightarrow \bigcup_{\lambda \in \Lambda} \text{Hom}_R(G, G^{(\lambda)}) : \lambda \longmapsto \text{pr}_\lambda \circ \chi, \end{aligned}$$

indukowane – odpowiednio – przez rzuty kanoniczne na moduły składowe i ich włożenia kanoniczne, są izomorfizmami grup przemiennych. Określamy je mianem izomorfizmów kanonicznych.

■

Dowód: O istnieniu homomorfizmów odwrotnych do wypisanych przesądzaają definicje odnośnych struktur uniwersalnych. I tak, np., rodzinie $\{\chi^{(\lambda)}\}_{\lambda \in \Lambda}$ odwzorowań R -liniowych $\chi^{(\lambda)} : G^{(\lambda)} \rightarrow G$ przypisane jest jedyne odwzorowanie R -liniowe $\chi : \bigoplus_{\lambda \in \Lambda} G^{(\lambda)} \rightarrow G$ o własności $\chi \circ j_\lambda = \chi^{(\lambda)}$, któremu homomorfizm $\text{Hom}_R(j, G)$ przyporządkowuje na powrót wyjściową rodzinę odwzorowań. $\square$

W dalszej części wykładu ograniczymy uwagę do modułów mających rozkład na sumy proste swoich podmodułów. Punktem wyjścia do naszej dyskusji jest tutaj

COROLLARIUM 14. *Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 75 oraz 78 i niechaj $\{G^{(\alpha|\lambda_\alpha)}\}_{\lambda_\alpha \in \Lambda_\alpha}$, $\alpha \in \{1, 2\}$ będą dwiema rodzinami R -modułów o sumach prostych, odpowiednio, $G^{(\alpha)\oplus} := \bigoplus_{\lambda_\alpha \in \Lambda_\alpha} G^{(\alpha|\lambda_\alpha)}$. Odwzorowanie*

$$\begin{aligned} \mathcal{M} &: \text{Hom}_R(G^{(1)\oplus}, G^{(2)\oplus}) \rightarrow \prod_{(\lambda_2, \lambda_1) \in \Lambda_2 \times \Lambda_1} \text{Hom}_R(G^{(1|\lambda_1)}, G^{(2|\lambda_2)}) \\ &: \chi \mapsto \text{pr} \circ \chi \circ j, \end{aligned}$$

$$\begin{aligned} \text{pr} \circ \chi \circ j &: \Lambda_2 \times \Lambda_1 \rightarrow \bigcup_{(\lambda_2, \lambda_1) \in \Lambda_2 \times \Lambda_1} \text{Hom}_R(G^{(1|\lambda_1)}, G^{(2|\lambda_2)}) \\ &: (\lambda_2, \lambda_1) \mapsto \text{pr}_{\lambda_2} \circ \chi \circ j_{\lambda_1} =: \mathcal{M}(\chi)_{\lambda_1}^{\lambda_2} \end{aligned}$$

jest monomorfizmem grup przemennych. Ilekroć zbiór indeksów Λ_2 jest skończony, $\mathcal{M}$ jest izomorfizmem. ■

Dowód: Wprost z konstrukcji sumy prostej modułów wynika, że $G^{(2)\oplus} \subset \prod_{\lambda_2 \in \Lambda_2} G^{(2|\lambda_2)}$, a zatem każde odwzorowanie R -liniowe $\chi : G \rightarrow G^{(2)\oplus}$ jest zarazem elementem $\text{Hom}_R(G, \prod_{\lambda_2 \in \Lambda_2} G^{(2|\lambda_2)})$. Przy tym zawieranie przechodzi w równość dla skończonego zbioru indeksów. Teza jest więc następstwem Stw. 94. $\square$

Przeciwdziedzina monomorfizmu $\mathcal{M}$ okazuje się być bardzo wygodnym modelem w analizie odwzorowań R -liniowych. Mając to na uwadze, zajmiemy się obecnie rekonstrukcją i formalizacją struktury algebraicznej indukowanej na grupach przemennych typu $\prod_{(\lambda_2, \lambda_1) \in \Lambda_2 \times \Lambda_1} \text{Hom}_R(G^{(1|\lambda_1)}, G^{(2|\lambda_2)})$ przez naturalne operacje algebraiczne na homomorfizmach R -modułów (takie jak np. dodawanie i składanie). W tym celu musimy wprowadzić kilka nowych pojęć.

DEFINICJA 82. Przyjmijmy notację Def. 67 oraz Przykł. 41 i niechaj Λ_1, Λ_2 będą zbiorami, $S := \{S^{(\lambda_2, \lambda_1)}\}_{(\lambda_2, \lambda_1) \in \Lambda_2 \times \Lambda_1}$ zaś niech będzie rodziną zbiorów indeksowaną przez zbiór $\Lambda_2 \times \Lambda_1$. **Macierz typu $\Lambda_2 \times \Lambda_1$ o wyrazach ze zbioru**

$$S^\cup := \bigcup_{(\lambda_2, \lambda_1) \in \Lambda_2 \times \Lambda_1} S^{(\lambda_2, \lambda_1)}$$

to dowolne odwzorowanie

$$M \in \prod_{(\lambda_2, \lambda_1) \in \Lambda_2 \times \Lambda_1} S^{(\lambda_2, \lambda_1)},$$

które będziemy identyfikować z jego zbiorem wartości zapisywanym w postaci

$$(M_{\lambda_1}^{\lambda_2} \equiv M(\lambda_2, \lambda_1))_{(\lambda_2, \lambda_1) \in \Lambda_2 \times \Lambda_1}.$$

O zbiorze tym można myśleć jako o “dwuwymiarowym” rozkładzie (“tablicy”) elementów zbioru $S^\cup$ nad dziedziną $\Lambda_2 \times \Lambda_1$. W tym samym “geometrycznym” duchu podrodzinę

$$M_{\bullet}^{\lambda_2} := (M_{\lambda_1}^{\lambda_2})_{\lambda_1 \in \Lambda_1}$$

określamy mianem **wiersza macierzy M o indeksie λ_2** , natomiast podrodzinę

$$M_{\lambda_1}^{\bullet} := (M_{\lambda_1}^{\lambda_2})_{\lambda_2 \in \Lambda_2}$$

nazywamy **kolumną macierzy M o indeksie λ_1** . Zbiór wszystkich macierzy opisanego rodzaju oznaczamy symbolem

$$\text{Mat}(S; \Lambda_2 \times \Lambda_1) \equiv \prod_{(\lambda_2, \lambda_1) \in \Lambda_2 \times \Lambda_1} S^{(\lambda_2, \lambda_1)},$$

a w przypadku $N_\alpha := |\Lambda_\alpha| < \infty$, $\alpha \in \{1, 2\}$ także symbolem

$$\text{Mat}(S; N_2 \times N_1) \equiv \prod_{(n_2, n_1) \in \overline{1, N_2} \times \overline{1, N_1}} S^{(n_2, n_1)}.$$

Macierz kwadratowa o wyrazach z $S^\cup$ to macierz typu $\Lambda \times \Lambda$ dla pewnego zbioru indeksów Λ . Podrodzina

$$(M_\lambda^\lambda)_{\lambda \in \Lambda}$$

wyrazów macierzy kwadratowej M nosi miano **przekątnej M** . Zbiór macierzy kwadratowych zapisujemy jako

$$\text{Mat}(S; \Lambda) \equiv \prod_{\lambda, \mu \in \Lambda} S^{(\lambda, \mu)},$$

a w przypadku $N := |\Lambda| < \infty$ także jako

$$\text{Mat}(S; N) \equiv \prod_{m, n \in \overline{1, N}} S^{(m, n)}.$$

Elementy $\text{Mat}(S; N)$ nazywamy **macierzami kwadratowymi stopnia N o wyrazach z $S^\cup$** . ▲

Zbadamy następnie okoliczności, w których $\text{Mat}(S; \Lambda_2 \times \Lambda_1)$ jest nośnikiem naturalnej struktury algebraicznej. Najprostszą taką sytuację opisuje

STWIERDZENIE 95. *W notacji Def. 32, 77 i 82 struktura grupy przemiennej $(G^{(\lambda_2, \lambda_1)}, +_{(\lambda_2, \lambda_1)}, P_{(\lambda_2, \lambda_1)}, \bullet \mapsto 0_{(\lambda_2, \lambda_1)})$ na każdym ze zbiorów $S^{(\lambda_2, \lambda_1)} \equiv G^{(\lambda_2, \lambda_1)}$ z rodziny $S \equiv G$ indukuje na zbiorze macierzy $\text{Mat}(G; \Lambda_2 \times \Lambda_1)$ kanoniczną strukturę grupy przemiennej*

$$(\text{Mat}(G; \Lambda_2 \times \Lambda_1), \phi_2^\square \equiv \boxplus_G, \phi_1^\square \equiv P_G, \phi_0^\square : \bullet \mapsto \mathbf{0}_{\Lambda_2 \times \Lambda_1}),$$

którą na zbiorze wartości odwzorowań z $\text{Mat}(G; \Lambda_2 \times \Lambda_1)$ realizują następujące operacje, określone “wyraz po wyrazie” i zwane **dodawaniem macierzy**

$$\begin{aligned} \boxplus_G &: \text{Mat}(G; \Lambda_2 \times \Lambda_1)^{\times 2} \longrightarrow \text{Mat}(G; \Lambda_2 \times \Lambda_1) \\ &: ((M_{\lambda_1}^{\lambda_2})_{(\lambda_2, \lambda_1) \in \Lambda_2 \times \Lambda_1}, (N_{\mu_1}^{\mu_2})_{(\mu_2, \mu_1) \in \Lambda_2 \times \Lambda_1}) \end{aligned}$$

$$\longmapsto (M_{\lambda_1}^{\lambda_2} +_{(\lambda_2, \lambda_1)} N_{\lambda_1}^{\lambda_2})_{(\lambda_2, \lambda_1) \in \Lambda_2 \times \Lambda_1}$$

oraz braniem przeciwności macierzowej

$$\begin{aligned} P_G &: \text{Mat}(G; \Lambda_2 \times \Lambda_1) \curvearrowright \\ &: (M_{\lambda_1}^{\lambda_2})_{(\lambda_2, \lambda_1) \in \Lambda_2 \times \Lambda_1} \longmapsto (P_{(\lambda_2, \lambda_1)}(M_{\lambda_1}^{\lambda_2}))_{(\lambda_2, \lambda_1) \in \Lambda_2 \times \Lambda_1}, \end{aligned}$$

a wraz z nimi element neutralny dla dodawania macierzy $\boxplus_G$ dany przez macierz zerową

$$0_{\Lambda_2 \times \Lambda_1} := (0_{(\lambda_2, \lambda_1)})_{(\lambda_2, \lambda_1) \in \Lambda_2 \times \Lambda_1}.$$

■

Obecność dodatkowej struktury na G pozwala – bywa – wzbogacić wprowadzoną powyżej strukturę grupy przemiennej na $\text{Mat}(G; \Lambda_2 \times \Lambda_1)$. Dość ogólnego przykładu dostarcza

STWIERDZENIE 96. *Przyjmijmy notację Def. 32 i 82, Stw. 95 i niech $S^{(\alpha)} := \{S^{(\alpha|\lambda_{\alpha+1}, \lambda_\alpha)}\}_{(\lambda_{\alpha+1}, \lambda_\alpha) \in \Lambda_{\alpha+1} \times \Lambda_\alpha}$, $\alpha \in \{1, 2\}$ będą dwiema rodzinami zbiorów. Dla dowolnego $|\Lambda_2| < \infty$ rodzina odwzorowań*

$$f := \{f_{\lambda_3, \lambda_1}^{\lambda_2} : S^{(2|\lambda_3, \lambda_2)} \times S^{(1|\lambda_2, \lambda_1)} \longrightarrow G^{(\lambda_3, \lambda_1)}\}_{(\lambda_3, \lambda_2, \lambda_1) \in \Lambda_3 \times \Lambda_2 \times \Lambda_1}$$

definiuje (lewostronne) mnożenie macierzy z $\text{Mat}(S^{(1)}; \Lambda_2 \times \Lambda_1)$ przez macierze z $\text{Mat}(S^{(2)}; \Lambda_3 \times \Lambda_2)$ wzdłuż f dane wzorem:

$$\begin{aligned} \boxplus_f &: \text{Mat}(S^{(2)}; \Lambda_3 \times \Lambda_2) \times \text{Mat}(S^{(1)}; \Lambda_2 \times \Lambda_1) \longrightarrow \text{Mat}(G; \Lambda_3 \times \Lambda_1) \\ &: ((M_{\lambda_2}^{\lambda_3})_{(\lambda_3, \lambda_2) \in \Lambda_3 \times \Lambda_2}, (N_{\lambda_1}^{\lambda_2})_{(\lambda_2, \lambda_1) \in \Lambda_2 \times \Lambda_1}) \\ &\longmapsto \left(\sum_{\lambda_2 \in \Lambda_2} f_{\lambda_3, \lambda_1}^{\lambda_2} (M_{\lambda_2}^{\lambda_3}, N_{\lambda_1}^{\lambda_2}) \right)_{(\lambda_3, \lambda_1) \in \Lambda_3 \times \Lambda_1}. \end{aligned}$$

Mnożenie macierzy jest zatem określone wedle schematu “wiersze przez kolumny”.

Jeśli ponadto zbiory $S^{(\alpha|\lambda_{\alpha+1}, \lambda_\alpha)} \equiv G^{(\alpha|\lambda_{\alpha+1}, \lambda_\alpha)}$ są nośnikami odnośnych struktur grupy przemiennej $(G^{(\alpha|\lambda_{\alpha+1}, \lambda_\alpha)}, +_{(\alpha|\lambda_{\alpha+1}, \lambda_\alpha)}, P_{(\alpha|\lambda_{\alpha+1}, \lambda_\alpha)}, \bullet \longmapsto 0_{(\alpha|\lambda_{\alpha+1}, \lambda_\alpha)})$, odwzorowania $f_{\lambda_3, \lambda_1}^{\lambda_2}$ zaś są $\mathbb{Z}$ -dwuliniowe, tj. spełniając, dla dowolnych elementów $g^{(\alpha|\lambda_{\alpha+1}, \lambda_\alpha)}, h^{(\alpha|\lambda_{\alpha+1}, \lambda_\alpha)} \in G^{(\alpha|\lambda_{\alpha+1}, \lambda_\alpha)}$, $\alpha \in \{1, 2\}$, tożsamości

$$\begin{aligned} &f_{\lambda_3, \lambda_1}^{\lambda_2} (g^{(2|\lambda_3, \lambda_2)} +_{(2|\lambda_3, \lambda_2)} h^{(2|\lambda_3, \lambda_2)}, g^{(1|\lambda_2, \lambda_1)} +_{(1|\lambda_2, \lambda_1)} h^{(1|\lambda_2, \lambda_1)}) \\ &= f_{\lambda_3, \lambda_1}^{\lambda_2} (g^{(2|\lambda_3, \lambda_2)}, g^{(1|\lambda_2, \lambda_1)}) +_{(\lambda_3, \lambda_1)} f_{\lambda_3, \lambda_1}^{\lambda_2} (g^{(2|\lambda_3, \lambda_2)}, h^{(1|\lambda_2, \lambda_1)}) \\ &+_{(\lambda_3, \lambda_1)} f_{\lambda_3, \lambda_1}^{\lambda_2} (h^{(2|\lambda_3, \lambda_2)}, g^{(1|\lambda_2, \lambda_1)}) +_{(\lambda_3, \lambda_1)} f_{\lambda_3, \lambda_1}^{\lambda_2} (h^{(2|\lambda_3, \lambda_2)}, h^{(1|\lambda_2, \lambda_1)}), \end{aligned}$$

to mnożenie $\boxplus_f$ jest homomorfizmem grup przemiennej, tj. splata ze sobą dodawanie macierzy w $\text{Mat}(G^{(1)}; \Lambda_2 \times \Lambda_1) \ni M_1, M_2, M$ oraz w $\text{Mat}(G^{(2)}; \Lambda_3 \times \Lambda_2) \ni N_1, N_2, N$ z dodawaniem macierzy w $\text{Mat}(G; \Lambda_3 \times \Lambda_1)$, co wyrażają równości

$$\begin{aligned} (M_1 \boxplus_{G^{(1)}} M_2) \boxplus_f N &= (M_1 \boxplus_f N) \boxplus_G (M_2 \boxplus_f N), \\ M \boxplus_f (N_1 \boxplus_{G^{(2)}} N_2) &= (M \boxplus_f N_1) \boxplus_G (M \boxplus_f N_2). \end{aligned}$$

Przyjmijmy, że są dane rodziny grup przemennych $(G^{(\alpha|\lambda_{\alpha+1}, \lambda_{\alpha})}, +_{(\alpha|\lambda_{\alpha+1}, \lambda_{\alpha})}, P_{(\alpha|\lambda_{\alpha+1}, \lambda_{\alpha})}, \bullet \mapsto 0_{(\alpha|\lambda_{\alpha+1}, \lambda_{\alpha})})$, $\alpha \in \{1, 2, 3\}$ oraz $(G^{(\beta+1, \beta|\lambda_{\beta+2}, \lambda_{\beta})}, +_{(\beta+1, \beta|\lambda_{\beta+2}, \lambda_{\beta})}, P_{(\beta+1, \beta|\lambda_{\beta+2}, \lambda_{\beta})}, \bullet \mapsto 0_{(\beta+1, \beta|\lambda_{\beta+2}, \lambda_{\beta})})$, $\beta \in \{1, 2\}$ wraz z rodzinami odwzorowań

$$f(2, 1) := \left\{ f(2, 1)_{\lambda_3, \lambda_1}^{\lambda_2} : G^{(2|\lambda_3, \lambda_2)} \times G^{(1|\lambda_2, \lambda_1)} \longrightarrow G^{(2, 1|\lambda_3, \lambda_1)} \right\}_{(\lambda_3, \lambda_2, \lambda_1) \in \Lambda_3 \times \Lambda_2 \times \Lambda_1},$$

$$f(3, 2) := \left\{ f(3, 2)_{\lambda_4, \lambda_2}^{\lambda_3} : G^{(3|\lambda_4, \lambda_3)} \times G^{(2|\lambda_3, \lambda_2)} \longrightarrow G^{(3, 2|\lambda_4, \lambda_2)} \right\}_{(\lambda_4, \lambda_3, \lambda_2) \in \Lambda_4 \times \Lambda_3 \times \Lambda_2}$$

oraz rodzinami odwzorowań $\mathbb{Z}$ -dwuliniowych

$$f(1) := \left\{ f(1)_{\lambda_4, \lambda_1}^{\lambda_2} : G^{(3, 2|\lambda_4, \lambda_2)} \times G^{(1|\lambda_2, \lambda_1)} \longrightarrow G^{(\lambda_4, \lambda_1)} \right\},$$

$$f(3) := \left\{ f(3)_{\lambda_4, \lambda_1}^{\lambda_3} : G^{(3|\lambda_4, \lambda_3)} \times G^{(2, 1|\lambda_3, \lambda_1)} \longrightarrow G^{(\lambda_4, \lambda_1)} \right\}$$

o własności (wyrażonej przez rodzinę diagramów przemennych)

$$\begin{array}{ccc} G^{(3|\lambda_4, \lambda_3)} \times G^{(2|\lambda_3, \lambda_2)} \times G^{(1|\lambda_2, \lambda_1)} & \xrightarrow{f(3, 2)_{\lambda_4, \lambda_2}^{\lambda_3} \times \text{id}_{G^{(1|\lambda_2, \lambda_1)}}} & G^{(3, 2|\lambda_4, \lambda_2)} \times G^{(1|\lambda_2, \lambda_1)} \\ \downarrow \text{id}_{G^{(3|\lambda_4, \lambda_3)}} \times f(2, 1)_{\lambda_3, \lambda_1}^{\lambda_2} & & \downarrow f(1)_{\lambda_4, \lambda_1}^{\lambda_2} \\ G^{(3|\lambda_4, \lambda_3)} \times G^{(2, 1|\lambda_3, \lambda_1)} & \xrightarrow{f(3)_{\lambda_4, \lambda_1}^{\lambda_3}} & G^{(\lambda_4, \lambda_1)} \end{array}.$$

Wówczas, o ile $|\Lambda_2|, |\Lambda_3| < \infty$, dla dowolnych macierzy $M^{(\alpha)} \in \text{Mat}(G^{(\alpha)}; \Lambda_{\alpha+1} \times \Lambda_{\alpha})$, $\alpha \in \{1, 2, 3\}$ zachodzą tożsamości

$$M^{(3)} \begin{smallmatrix} \square \\ f(3) \end{smallmatrix} (M^{(2)} \begin{smallmatrix} \square \\ f(2, 1) \end{smallmatrix} M^{(1)}) = (M^{(3)} \begin{smallmatrix} \square \\ f(3, 2) \end{smallmatrix} M^{(2)}) \begin{smallmatrix} \square \\ f(1) \end{smallmatrix} M^{(1)}.$$

W szczególności struktura pierścienia $(R, +_R, \cdot_R, P_R, \bullet \mapsto 0_R)$ na zbiorze R indukuje strukturę pierścienia na zbiorze $\text{Mat}(R; N)$ macierzy kwadratowych stopnia N o wyrazach z R . Dodawanie macierzy $\boxplus_R$ jest tu określone jak wyżej (“wyraz po wyrazie”) i ma element neutralny dany przez macierz zerową $\mathbf{0}_N \equiv (M_n^m = 0_R)_{m, n \in \overline{1, N}}$, natomiast obustronnie względem niego rozdzielne i łączne mnożenie macierzy określamy wzorem

$$\boxdot_R : \text{Mat}(R; N)^{\times 2} \longrightarrow \text{Mat}(R; N)$$

$$: \left((A_l^k)_{k, l \in \overline{1, N}}, (B_n^m)_{m, n \in \overline{1, N}} \right) \mapsto \left(\sum_{k=1}^N A_k^m \cdot_R B_n^k \right)_{m, n \in \overline{1, N}},$$

przy czym elementem neutralnym dla mnożenia jest **macierz jednostkowa**

$$\mathbf{1}_N := (\delta_{m, n}^R)_{m, n \in \overline{1, N}}.$$

Branie przeciwności P_R jest także zdefiniowane jak uprzednio (“wyraz po wyrazie”). Pierścień ten,

$$(\text{Mat}(R; N), \boxplus_R, \boxdot_R, P_R, \bullet \mapsto \mathbf{0}_N, \bullet \mapsto \mathbf{1}_N),$$

określamy mianem **pierścienia macierzowego stopnia N nad R** .
indexpierścień!macierzowy stopnia N Niesie on strukturę modułu nad R zadaną przez działanie

$$\ell : R \boxtimes \text{Mat}(R; N) \longrightarrow \text{Mat}(R; N)$$

$$: \left(r, (A_n^m)_{m,n \in \overline{1,N}} \right) \mapsto (r \cdot_R A_n^m)_{m,n \in \overline{1,N}} =: r \triangleright_{(N)} (A_n^m)_{m,n \in \overline{1,N}}.$$

Elementy odwracalne pierścienia $\text{Mat}(R; N)$ określamy mianem **macierzy odwracalnych (stopnia N o współczynnikach z R)**. Tworzą one **grupę główną liniową (macierzy) stopnia N o współczynnikach z R** , której nośnik będziemy oznaczać symbolem $\text{GL}(R; N)$.

■

W następnej kolejności rozpatrzmy odwzorowania między grupami macierzowymi transportujące opisaną powyżej strukturę algebraiczną a indukowane przez odwzorowania między zbiorami, z których pochodzą elementy macierzy.

STWIERDZENIE 97. *Przyjmijmy notację Def. 32 i 82 oraz Stw. 95 i 96. Rodzina homomorfizmów grup przemiennej*

$$\chi := \{ \chi^{(\lambda_2, \lambda_1)} : G^{(\lambda_2, \lambda_1)} \longrightarrow H^{(\lambda_2, \lambda_1)} \}$$

indukuje homomorfizm grup przemiennej

$$\begin{aligned} [\chi] &: \text{Mat}(G; \Lambda_2 \times \Lambda_1) \longrightarrow \text{Mat}(H; \Lambda_2 \times \Lambda_1) \\ &: (M_{\lambda_1}^{\lambda_2})_{(\lambda_2, \lambda_1) \in \Lambda_2 \times \Lambda_1} \mapsto (\chi^{(\lambda_2, \lambda_1)}(M_{\lambda_1}^{\lambda_2}))_{(\lambda_2, \lambda_1) \in \Lambda_2 \times \Lambda_1}. \end{aligned}$$

Jeśli wszystkie homomorfizmy $\chi^{(\lambda_2, \lambda_1)}$ są izomorfizmami, to $[\chi]$ także jest izomorfizmem.

Przyjmijmy, że jest dana rodzina homomorfizmów grup przemiennej

$$\chi := \{ \chi^{(\lambda_3, \lambda_1)} : G^{(\lambda_3, \lambda_1)} \longrightarrow H^{(\lambda_3, \lambda_1)} \}$$

oraz dwie rodziny odwzorowań

$$\begin{aligned} \gamma &:= \{ \gamma_{\lambda_3, \lambda_1}^{\lambda_2} : G^{(2|\lambda_3, \lambda_2)} \times G^{(1|\lambda_2, \lambda_1)} \longrightarrow G^{(\lambda_3, \lambda_1)} \}_{(\lambda_3, \lambda_2, \lambda_1) \in \Lambda_3 \times \Lambda_2 \times \Lambda_1}, \\ \eta &:= \{ \eta_{\lambda_3, \lambda_1}^{\lambda_2} : H^{(2|\lambda_3, \lambda_2)} \times H^{(1|\lambda_2, \lambda_1)} \longrightarrow H^{(\lambda_3, \lambda_1)} \}_{(\lambda_3, \lambda_2, \lambda_1) \in \Lambda_3 \times \Lambda_2 \times \Lambda_1} \end{aligned}$$

zadające – odpowiednio – mnożenie $\boxtimes_\gamma$ macierzy z $\text{Mat}(G^{(1)}; \Lambda_2 \times \Lambda_1)$ przez macierze z $\text{Mat}(G^{(2)}; \Lambda_3 \times \Lambda_2)$ oraz mnożenie $\boxtimes_\eta$ macierzy z $\text{Mat}(H^{(1)}; \Lambda_2 \times \Lambda_1)$ przez macierze z $\text{Mat}(H^{(2)}; \Lambda_3 \times \Lambda_2)$. Niech będą też dane dwie rodziny homomorfizmów grup przemiennej

$$\chi^{(\alpha)} := \{ \chi^{(\alpha|\lambda_{\alpha+1}, \lambda_\alpha)} : G^{(\alpha|\lambda_{\alpha+1}, \lambda_\alpha)} \longrightarrow H^{(\alpha|\lambda_{\alpha+1}, \lambda_\alpha)} \}, \quad \alpha \in \{1, 2\}$$

o własności (wyrażonej przez rodzinę diagramów przemiennej)

$$\begin{array}{ccc} G^{(2|\lambda_3, \lambda_2)} \times G^{(1|\lambda_2, \lambda_1)} & \xrightarrow{\chi^{(2|\lambda_3, \lambda_2)} \times \chi^{(1|\lambda_2, \lambda_1)}} & H^{(2|\lambda_3, \lambda_2)} \times H^{(1|\lambda_2, \lambda_1)} \\ \downarrow \gamma_{\lambda_3, \lambda_1}^{\lambda_2} & & \downarrow \eta_{\lambda_3, \lambda_1}^{\lambda_2} \\ G^{(\lambda_3, \lambda_1)} & \xrightarrow{\chi^{(\lambda_3, \lambda_1)}} & H^{(\lambda_3, \lambda_1)} \end{array}.$$

Wówczas, o ile $|\Lambda_2| < \infty$, dla dowolnych $M \in \text{Mat}(G^{(2)}; \Lambda_3 \times \Lambda_2)$ i $N \in \text{Mat}(G^{(1)}; \Lambda_2 \times \Lambda_1)$ spełniona jest tożsamość

$$[\chi](M \boxdot_{\gamma} N) = [\chi^{(2)}](M) \boxdot_{\gamma} [\chi^{(1)}](N).$$

■

Dowód: Pierwsza część tezy jest oczywista, skupimy zatem uwagę na części drugiej. Obliczamy wprost z definicji:

$$\begin{aligned} \left([\chi](M \boxdot_{\gamma} N) \right)_{\lambda_1}^{\lambda_3} &= \chi^{(\lambda_3, \lambda_1)} \left(\sum_{\lambda_2 \in \Lambda_2} \gamma_{\lambda_3, \lambda_1}^{\lambda_2} (M_{\lambda_2}^{\lambda_3}, N_{\lambda_1}^{\lambda_2}) \right) \\ &= \sum_{\lambda_2 \in \Lambda_2} \chi^{(\lambda_3, \lambda_1)} \circ \gamma_{\lambda_3, \lambda_1}^{\lambda_2} (M_{\lambda_2}^{\lambda_3}, N_{\lambda_1}^{\lambda_2}) \\ &= \sum_{\lambda_2 \in \Lambda_2} \eta_{\lambda_3, \lambda_1}^{\lambda_2} (\chi^{(2| \lambda_3, \lambda_2)}(M_{\lambda_2}^{\lambda_3}), \chi^{(1| \lambda_2, \lambda_1)}(N_{\lambda_1}^{\lambda_2})) \\ &= \left([\chi^{(2)}](M) \boxdot_{\eta} [\chi^{(1)}](N) \right)_{\lambda_1}^{\lambda_3}. \end{aligned}$$

□

Możemy już teraz wypowiedzieć istotne

STWIERDZENIE 98. Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 75, 78 i 82, Cor. 14 oraz Stw. 95 i 96. Oznaczmy przez

$$\mathcal{H}^{(2,1)} := \left\{ \text{Hom}_R(G^{(1| \lambda_1)}, G^{(2| \lambda_2)}) \right\}_{(\lambda_2, \lambda_1) \in \Lambda_2 \times \Lambda_1}$$

rodzinę grup przemennych

$$\mathcal{H}^{(2,1| \lambda_2, \lambda_1)} := \text{Hom}_R(G^{(1| \lambda_1)}, G^{(2| \lambda_2)}).$$

Odwzorowanie $\mathcal{M}$ zdefiniowane w Cor. 14 jest monomorfizmem grup przemennych (przechodzącym w izomorfizm dla Λ_2 skończonego)

$$\mathcal{M} : (\text{Hom}_R(G^{(1)\oplus}, G^{(2)\oplus}), +, -(\cdot), \bullet \mapsto \mathbf{0})$$

$$\xrightarrow{\cong} (\text{Mat}(\mathcal{H}^{(2,1)}; \Lambda_2 \times \Lambda_1), \boxplus_{\mathcal{H}}, \boxminus_{\mathcal{H}}, \bullet \mapsto \mathbf{0}_{\Lambda_2 \times \Lambda_1}),$$

który będziemy określać mianem **macierzowej realizacji odwzorowania R -liniowego $G^{(1)\oplus}$ w $G^{(2)\oplus}$** . Jawnie $\mathbb{Z}$ -dwuliniowe operacje złożenia homomorfizmów

$$\circ : \mathcal{H}^{(3,2| \lambda_3, \lambda_2)} \times \mathcal{H}^{(2,1| \lambda_2, \lambda_1)} \longrightarrow \mathcal{H}^{(3,1| \lambda_3, \lambda_1)}$$

$$: (\chi^{(3,2| \lambda_3, \lambda_2)}, \chi^{(2,1| \lambda_2, \lambda_1)}) \longmapsto \chi^{(3,2| \lambda_3, \lambda_2)} \circ \chi^{(2,1| \lambda_2, \lambda_1)}$$

określają, o ile $|\Lambda_2| < \infty$, mnożenie macierzy

$$\odot \equiv \boxtimes : \text{Mat}(\mathcal{H}^{(3,2)}; \Lambda_3 \times \Lambda_2) \times \text{Mat}(\mathcal{H}^{(2,1)}; \Lambda_2 \times \Lambda_1) \longrightarrow \text{Mat}(\mathcal{H}^{(3,1)}; \Lambda_3 \times \Lambda_1)$$

$$: \left((\mathcal{M}(\chi)_{\lambda_2}^{\lambda_3})_{(\lambda_3, \lambda_2) \in \Lambda_3 \times \Lambda_2}, (\mathcal{M}(\psi)_{\mu_1}^{\mu_2})_{(\mu_2, \mu_1) \in \Lambda_2 \times \Lambda_1} \right)$$

$$\longmapsto \left(\sum_{\lambda_2 \in \Lambda_2} \mathcal{M}(\chi)_{\lambda_2}^{\lambda_3} \circ \mathcal{M}(\psi)_{\lambda_1}^{\lambda_2} \right)_{(\lambda_3, \lambda_1) \in \Lambda_3 \times \Lambda_1}$$

o własnościach

$$(\mathcal{M}(\chi_1) \boxplus_{\mathcal{H}^{(3,2)}} \mathcal{M}(\chi_2)) \odot \mathcal{M}(\psi) = (\mathcal{M}(\chi_1) \odot \mathcal{M}(\psi)) \boxplus_{\mathcal{H}^{(3,1)}} (\mathcal{M}(\chi_2) \odot \mathcal{M}(\psi)),$$

$$\mathcal{M}(\chi) \odot (\mathcal{M}(\psi_1) \boxplus_{\mathcal{H}^{(2,1)}} \mathcal{M}(\psi_2)) = (\mathcal{M}(\chi) \odot \mathcal{M}(\psi_1)) \boxplus_{\mathcal{H}^{(3,1)}} (\mathcal{M}(\chi) \odot \mathcal{M}(\psi_2))$$

oraz

$$(8.22) \quad \mathcal{M}(\chi \circ \psi) = \mathcal{M}(\chi) \odot \mathcal{M}(\psi),$$

wypisanych dla dowolnych odwzorowań $\chi_1, \chi_2, \chi \in \text{Hom}_R(G^{(2)\oplus}, G^{(3)\oplus})$ i $\psi, \psi_1, \psi_2 \in \text{Hom}_R(G^{(1)\oplus}, G^{(2)\oplus})$. Mnożenie to jest łączne w sensie wyrażonym przez tożsamość

$$(8.23) \quad (\mathcal{M}(\zeta) \odot \mathcal{M}(\chi)) \odot \mathcal{M}(\psi) = \mathcal{M}(\zeta) \odot (\mathcal{M}(\chi) \odot \mathcal{M}(\psi)),$$

słuszną, przy $|\Lambda_2|, |\Lambda_3| < \infty$, dla dowolnych odwzorowań $\zeta \in \text{Hom}_R(G^{(3)\oplus}, G^{(4)\oplus})$, $\chi \in \text{Hom}_R(G^{(2)\oplus}, G^{(3)\oplus})$ i $\psi \in \text{Hom}_R(G^{(1)\oplus}, G^{(2)\oplus})$.

■

Dowód: Pierwsza część tezy dowodzonego stwierdzenia stanowi proste przeformułowanie tezy Cor. 14 uwzględniające treść Def. 82. Z kolei łączność mnożenia macierzowego, którą wyraża formuła (8.23), jest – wobec łączności operacji składania homomorfizmów – bezpośrednim następstwem relacji (8.22). Pozostaje zatem sprawdzić słusność tej ostatniej. Czynimy to w bezpośrednim rachunku, korzystając przy tym z tożsamości (8.10),

$$\begin{aligned} \mathcal{M}(\chi \circ \psi)_{\lambda_1}^{\lambda_3} &= \text{pr}_{\lambda_3} \circ (\chi \circ \psi) \circ j_{\lambda_1} = \text{pr}_{\lambda_3} \circ \chi \circ \left(\sum_{\lambda_2 \in \Lambda_2} j_{\lambda_2} \circ \text{pr}_{\lambda_2} \right) \circ \psi \circ j_{\lambda_1} \\ &\equiv \sum_{\lambda_2 \in \Lambda_2} (\text{pr}_{\lambda_3} \circ \chi \circ j_{\lambda_2}) \circ (\text{pr}_{\lambda_2} \circ \psi \circ j_{\lambda_1}) \\ &= \sum_{\lambda_2 \in \Lambda_2} \mathcal{M}(\chi)_{\lambda_2}^{\lambda_3} \circ \mathcal{M}(\psi)_{\lambda_1}^{\lambda_2} = (\mathcal{M}(\chi) \odot \mathcal{M}(\psi))_{\lambda_1}^{\lambda_3}. \end{aligned}$$

□

Dla ujednolicenia opisu homomorfizmów modułów z rozkładem na sumy proste podmodułów i samych modułów, a zarazem celem przygotowania gruntu pod dalsze rozważania, formułujemy

STWIERDZENIE 99. Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 75, 78 i 82, Cor. 14 oraz Stw. 95, 96 i 98. Niechaj $\{G^{(\alpha|\lambda_\alpha)}\}_{\lambda_\alpha \in \Lambda_\alpha}$, $\alpha \in \{1, 2\}$ będą dwiema rodzinami R -modułów o sumach prostych $G^{(\alpha)\oplus} := \bigoplus_{\lambda_\alpha \in \Lambda_\alpha} G^{(\alpha|\lambda_\alpha)}$ i wprowadźmy zapis

$$G^{(\alpha)} := \{G^{(\alpha|\lambda_\alpha, \mu)}\}_{(\lambda_\alpha, \mu) \in \Lambda_\alpha \times \{\bullet\}}, \quad G^{(\alpha|\lambda_\alpha, \bullet)} := G^{(\alpha|\lambda_\alpha)}.$$

Istnieje trywialny monomorfizm¹⁴ R -modułów (przechodzący w izomorfizm dla $|\Lambda_\alpha| < \infty$)

$$\mathcal{M} : \left(G^{(\alpha)\oplus}, \phi_2^{(\alpha)\sqcap}, \phi_1^{(\alpha)\sqcap}, \phi_0^{(\alpha)\sqcap} \right)$$

¹⁴Jest jasnym, że wypisany monomorfizm to tylko inny, równoważny sposób zapisu elementów modułu mającego rozkład na sumę prostą podmodułów, pozwalający na wykorzystanie wcześniejszych konstrukcji dotyczących odwzorowań R -liniowych.

$$\begin{aligned} &\longrightarrow (\text{Mat}(G^{(\alpha)}; \Lambda_\alpha \times \{\bullet\}), \boxplus_{G^{(\alpha)}}, \text{P}_{G^{(\alpha)}}, \bullet \longmapsto \mathbf{0}_{\Lambda_\alpha \times \{\bullet\}}) \\ &: \quad g \longmapsto \text{pr}(g), \end{aligned}$$

$$\text{pr}(g) \quad : \quad \Lambda_\alpha \times \{\bullet\} \quad : \quad (\lambda_\alpha, \bullet) \longmapsto \text{pr}_{\lambda_\alpha}(g) =: \mathcal{M}(g)^{\lambda_\alpha},$$

który będziemy określać mianem **macierzowej realizacji elementu R -modułu $G^\oplus$** .

Ilekoć $|\Lambda_1| < \infty$, jawnie $\mathbb{Z}$ -dwuliniowe odwzorowanie ewaluacji

$$\text{ev} : \mathcal{H}^{(2,1|\lambda_2,\lambda_1)} \times G^{(1|\lambda_1)} \longrightarrow G^{(2|\lambda_2)} \quad : \quad (\chi, g) \longmapsto \chi(g)$$

określa mnożenie macierzy

$$\begin{aligned} \odot \equiv \boxtimes_{\text{ev}} &: \text{Mat}(\mathcal{H}^{(2,1)}; \Lambda_2 \times \Lambda_1) \times \text{Mat}(G^{(1)}; \Lambda_1 \times \{\bullet\}) \longrightarrow \text{Mat}(G^{(2)}; \Lambda_2 \times \{\bullet\}) \\ &: \quad \left((\mathcal{M}(\chi)^{\lambda_2}_{\lambda_1})_{(\lambda_2, \lambda_1) \in \Lambda_2 \times \Lambda_1}, (\mathcal{M}(g)^{\mu_1})_{\mu_1 \in \Lambda_1} \right) \\ &\quad \longmapsto \left(\sum_{\lambda_1 \in \Lambda_1} \mathcal{M}(\chi)^{\lambda_2}_{\lambda_1} (\mathcal{M}(g)^{\lambda_1}) \right)_{\lambda_2 \in \Lambda_2} \end{aligned}$$

o własnościach

$$\begin{aligned} (\mathcal{M}(\chi_1) \boxplus_{\mathcal{H}^{(2,1)}} \mathcal{M}(\chi_2)) \odot \mathcal{M}(g) &= (\mathcal{M}(\chi_1) \odot \mathcal{M}(g)) \boxplus_{G^{(2)}} (\mathcal{M}(\chi_2) \odot \mathcal{M}(g)), \\ \mathcal{M}(\chi) \odot (\mathcal{M}(g_1) \boxplus_{G^{(1)}} \mathcal{M}(g_2)) &= (\mathcal{M}(\chi) \odot \mathcal{M}(g_1)) \boxplus_{G^{(2)}} (\mathcal{M}(\chi) \odot \mathcal{M}(g_2)) \end{aligned}$$

oraz

$$(8.24) \quad \mathcal{M}(\chi(g)) = \mathcal{M}(\chi) \odot \mathcal{M}(g),$$

wypisanych dla dowolnych $\chi_1, \chi_2, \chi \in \text{Hom}_R(G^{(1)\oplus}, G^{(2)\oplus})$ i $g, g_1, g_2 \in G^{(1)\oplus}$. ■

Dowód: I w tym przypadku jedyną nietrywialną relacją jest (8.24). Poddajemy ją bezpośredniej weryfikacji:

$$\begin{aligned} \mathcal{M}(\chi(g))^{\lambda_2} &= \text{pr}_{\lambda_2} \circ \chi(g) = \text{pr}_{\lambda_2} \circ \chi \left(\sum_{\lambda_1 \in \Lambda_1} \lambda_{\lambda_1} \circ \text{pr}_{\lambda_1}(g) \right) \\ &\equiv \sum_{\lambda_1 \in \Lambda_1} (\text{pr}_{\lambda_2} \circ \chi \circ \lambda_{\lambda_1}) (\text{pr}_{\lambda_1}(g)) = \sum_{\lambda_1 \in \Lambda_1} \mathcal{M}(\chi)^{\lambda_2}_{\lambda_1} (\mathcal{M}(g)^{\lambda_1}) \\ &= (\mathcal{M}(\chi) \odot \mathcal{M}(g))^{\lambda_2}. \end{aligned}$$

□

Powyższe obserwacje pozwalają na szczególnie dogodne i naturalne zarazem przeformułowanie opisu modułów wolnych – w tym przestrzeni wektorowych – w terminach operacji macierzowych. W tej swojej odsłonie algebra liniowa ujawnia

rozliczne powiązania z problematyką o istotnym znaczeniu fizykalnym (jak np. teoria liniowych równań różniczkowych, w tym także cząstkowych, znajdująca zastosowanie w opisie zjawisk o naturze liniowej, mechanika macierzowa, algebraiczna teoria systemów całkowalnych, modele macierzowe fizyki statystycznej oraz grawitacji kwantowej, macierzowe sformułowanie M-teorii, lagranżowski opis oddziaływań fundamentalnych *etc.*), a przy tym poddaje się prostej algorytmizacji, która wydatnie usprawnia rachunki. Niebagatelne znaczenie praktyczne algebry macierzowej oraz mnogość technik rachunkowych, jakich dostarcza, usprawiedliwiają czas poświęcony na jej dyskusję w dalszej części niniejszego kursu. Zaczniemy od prostych obserwacji pozwalających na identyfikację zasadniczych elementów opisu macierzowego modułów wolnych nad pierścieniem przemennym.

TWIERDZENIE 8.11 (O macierzy elementu modułu wolnego i odwzorowania R -liniowego). *Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 68, 70, 75, 78 i 82, Cor. 14 oraz Stw. 75, 95, 96, 97, 98 i 99. Niechaj $((G^{(\alpha)}, +_{(\alpha)}, P_{(\alpha)}, \bullet \mapsto 0_{(\alpha)}), \ell^{(\alpha)})$, $\alpha \in \{1, 2, 3\}$ będą trzema modułami nad pierścieniem przemennym¹⁵ R . Wybór bazy $\mathcal{B}^{(\alpha)} := \{g_{(\alpha|\lambda_\alpha)}\}_{\lambda_\alpha \in \Lambda_\alpha}$ w $G^{(\alpha)}$ określa rodzinę izomorfizmów R -modułów*

$$\varrho^{(\alpha|\lambda_\alpha)} : \underline{G}^{(\alpha|\lambda_\alpha)} := \langle g_{(\alpha|\lambda_\alpha)} \rangle_R \xrightarrow{\cong} R : r \triangleright_{(\alpha)} g_{(\alpha|\lambda_\alpha)} \mapsto r,$$

która indukuje monomorfizm R -modułów (przechodzący w izomorfizm dla $|\Lambda_\alpha| < \infty$)

$$[\varrho^{(\alpha)}] \circ \mathcal{M} : G^{(\alpha)} \xrightarrow{\cong} \text{Mat}(\underline{G}^{(\alpha)}, \Lambda_\alpha \times \{\bullet\}) \xrightarrow{\cong} \text{Mat}(R, \Lambda_\alpha \times \{\bullet\})$$

$$: g \mapsto \text{pr}(g) \mapsto [g]^{\mathcal{B}^{(\alpha)}},$$

przy czym dla $g = \sum_{\lambda_\alpha \in \Lambda_\alpha} r^{\lambda_\alpha} \triangleright_{(\alpha)} g_{(\alpha|\lambda_\alpha)}$ jest

$$[g]^{\mathcal{B}^{(\alpha)}}(\lambda_\alpha, \bullet) := r^{\lambda_\alpha},$$

a ponadto dla każdych dwóch elementów $g_1, g_2 \in G^{(\alpha)}$ zachodzi tożsamość

$$[g_1 +_{(\alpha)} g_2]^{\mathcal{B}^{(\alpha)}} = [g_1]^{\mathcal{B}^{(\alpha)}} \boxplus_R [g_2]^{\mathcal{B}^{(\alpha)}}.$$

Macierz $[g]^{\mathcal{B}^{(\alpha)}}$ nosi miano **macierzy elementu g względem bazy $\mathcal{B}^{(\alpha)}$** . Ograniczenie monomorfizmu do jego obrazu w $\text{Mat}(R, \Lambda_\alpha \times \{\bullet\})$ określa izomorfizm

$$\rho_{\mathcal{B}^{(\alpha)}} : G^{(\alpha)} \xrightarrow{\cong} \bigoplus_{\lambda_\alpha \in \Lambda_\alpha} R.$$

Każde dwa wybory, $\mathcal{B}^{(\alpha)}$ i $\mathcal{B}^{(\beta)}$, współokreślają rodzinę izomorfizmów grup przemennych

$$\varrho^{(\beta, \alpha|\lambda_\beta, \lambda_\alpha)} : \underline{\mathcal{H}}^{(\beta, \alpha|\lambda_\beta, \lambda_\alpha)} := \text{Hom}_R(\underline{G}^{(\alpha|\lambda_\alpha)}, \underline{G}^{(\beta|\lambda_\beta)}) \xrightarrow{\cong} R : \psi \mapsto \psi^{\lambda_\beta}_{\lambda_\alpha},$$

gdzie

$$\psi(g_{(\alpha|\lambda_\alpha)}) =: \psi^{\lambda_\beta}_{\lambda_\alpha} \triangleright_{(\beta)} g_{(\beta|\lambda_\beta)}.$$

Rodzina ta indukuje monomorfizm grup przemennych

$$[\varrho^{(\beta, \alpha)}] \circ \mathcal{M} : \text{Hom}_R(G^{(\alpha)}, G^{(\beta)}) \xrightarrow{\cong} \text{Mat}(\underline{\mathcal{H}}^{(\beta, \alpha)}; \Lambda_\beta \times \Lambda_\alpha)$$

¹⁵Założenie o przemienności pierścienia można opuścić za cenę bardziej skomplikowanej struktury mультыпликатывnej na zbiorze macierzy rozważanych.

$$\xrightarrow{\cong} \text{Mat}(R; \Lambda_\beta \times \Lambda_\alpha)$$

$$: \quad \chi \mapsto \text{pr} \circ \chi \circ j \mapsto [\chi]_{\mathcal{B}^{(\alpha)}}^{\mathcal{B}^{(\beta)}},$$

przy czym dla χ określonego wzorami

$$\chi(g_{(\alpha|\lambda_\alpha)}) = \sum_{\lambda_\beta \in \Lambda_\beta} \chi_{\lambda_\alpha}^{\lambda_\beta} \triangleright_{(\beta)} g_{(\beta|\lambda_\beta)},$$

słusznymi, o ile $|\Lambda_\beta| < \infty$, dla wszystkich $\lambda_\alpha \in \Lambda_\alpha$, jest

$$(8.25) \quad [\chi]_{\mathcal{B}^{(\alpha)}}^{\mathcal{B}^{(\beta)}}(\lambda_\beta, \lambda_\alpha) := \chi_{\lambda_\alpha}^{\lambda_\beta}.$$

Dla każdych dwóch odwzorowań R -liniowych $\chi_1, \chi_2 \in \text{Hom}_R(G^{(\alpha)}, G^{(\beta)})$ zachodzi tożsamość

$$[\chi_1 + \chi_2]_{\mathcal{B}^{(\alpha)}}^{\mathcal{B}^{(\beta)}} = [\chi_1]_{\mathcal{B}^{(\alpha)}}^{\mathcal{B}^{(\beta)}} \boxplus_R [\chi_2]_{\mathcal{B}^{(\alpha)}}^{\mathcal{B}^{(\beta)}}.$$

Macierz $[\chi]_{\mathcal{B}^{(\alpha)}}^{\mathcal{B}^{(\beta)}}$ nosi miano **macierzy odwzorowania R -liniowego g względem baz $\mathcal{B}^{(\alpha)}$ i $\mathcal{B}^{(\beta)}$** .

Ilekoć $|\Lambda_2| < \infty$, dla dowolnych odwzorowań R -liniowych $\chi^{(\alpha+1, \alpha)} \in \text{Hom}_R(G^{(\alpha)}, G^{(\alpha+1)})$, $\alpha \in \{1, 2\}$ spełniona jest tożsamość

$$(8.26) \quad [\chi^{(3,2)} \circ \chi^{(2,1)}]_{\mathcal{B}^{(1)}}^{\mathcal{B}^{(3)}} = [\chi^{(3,2)}]_{\mathcal{B}^{(2)}}^{\mathcal{B}^{(3)}} \boxplus_R [\chi^{(2,1)}]_{\mathcal{B}^{(1)}}^{\mathcal{B}^{(2)}},$$

a ponadto dla dowolnych $g \in G^{(2)}$ i $\chi \in \text{Hom}_R(G^{(2)}, G^{(3)})$ prawdziwą jest równość

$$(8.27) \quad [\chi(g)]_{\mathcal{B}^{(2)}}^{\mathcal{B}^{(3)}} = [\chi]_{\mathcal{B}^{(2)}}^{\mathcal{B}^{(3)}} \boxplus_R [g]_{\mathcal{B}^{(2)}}^{\mathcal{B}^{(2)}}.$$

■

Dowód: Tezy twierdzenia stanowią bezpośrednią konsekwencję definicji oraz Stw. 98 i 99 podpartych Stw. 86 oraz obserwacją, odniesioną do Stw. 97, że oto w przypadku przemienne pierścienia R izomorfizmy $[\varrho^{(2,1)}]$, $[\varrho^{(3,2)}]$ oraz $[\varrho^{(3,1)}]$ razem z $\circ$ i $\cdot_R$ czynią przeminnym każdy ze stosownej rodziny diagramów

$$\begin{array}{ccc} \underline{\mathcal{H}}^{(3,2|\lambda_3, \lambda_2)} \times \underline{\mathcal{H}}^{(2,1|\lambda_2, \lambda_1)} & \xrightarrow{\varrho^{(3,2|\lambda_3, \lambda_2)} \times \varrho^{(2,1|\lambda_2, \lambda_1)}} & R \times R \\ \downarrow \circ & & \downarrow \cdot_R \\ \underline{\mathcal{H}}^{\varrho^{(3,1|\lambda_3, \lambda_1)}} & \xrightarrow{\varrho^{(3,1|\lambda_3, \lambda_1)}} & R \end{array}.$$

□

W świetle powyższych obserwacji zasadne wydaje się ustalenie macierzowego obrazu procedury zmiany wyboru bazy, tak w dziedzinie, jak i w przeciwdziedzinie odwzorowania R -liniowego. Odpowiedzi dostarcza

STWIERDZENIE 100. Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 68, 70, 75, 78 i 82, Cor. 14, Stw. 75, 95, 96, 97, 98 i 99 oraz Tw. 8.11. Niechaj $\mathcal{B} = \{g_m\}_{m \in \overline{1, N}}$ będzie bazą modułu G nad pierścieniem (przemiennym) R , i niech będzie dana macierz

$$M := (M_n^m)_{m, n \in \overline{1, N}} \in \text{Mat}(R; N).$$

Zbiór $\mathcal{B}' := \{h_n\}_{n \in \overline{1, N}}$ złożony z elementów G określonych wzorami

$$h_n := \sum_{m=1}^N M_n^m \triangleright g_m$$

jest bazą G wtedy i tylko wtedy, gdy

$$M \in \text{GL}(R; N),$$

tj. gdy M jest macierzą odwracalną. W takim przypadku prawdziwą jest tożsamość

$$M = [\text{id}_G]_{\mathcal{B}}^{\mathcal{B}'}.$$

Powyższą macierz określamy mianem **macierzy przejścia z bazy $\mathcal{B}'$ do bazy $\mathcal{B}$** .

■

Dowód: Tożsamość stanowiąca ostatnią część tezy jest oczywista. Pozostaje zatem udowodnić pierwszą jej część.

$\Rightarrow$ Niechaj rodzina $\{h_n\}_{n \in \overline{1, N}}$ będzie bazą G . Na mocy Stw. 80 istnieje dokładnie jeden endomorfizm $\chi \in \text{End}_R(G)$ o własności

$$\forall_{n \in \overline{1, N}} : \chi(g_n) = h_n \equiv \sum_{m=1}^N M_n^m \triangleright g_m,$$

dla którego wprost z definicji (8.25) zachodzi równość

$$[\chi]_{\mathcal{B}}^{\mathcal{B}} = M,$$

czyli M jest macierzą odwzorowania χ względem bazy $\mathcal{B}$. Zgodnie z Cor. 10, odwzorowanie χ jest automorfizmem, czyli istnieje $\psi \in \text{End}_R(G)$ spełniający tożsamości

$$\psi \circ \chi = \text{id}_G = \chi \circ \psi.$$

Odwracalność M wynika teraz wprost z Równ. (8.26) – poszukiwaną odwrotnością jest $[\psi]_{\mathcal{B}}^{\mathcal{B}}$.

$\Leftarrow$ Niechaj $M \in \text{GL}(R; N)$ i niech $N = (N_n^m)_{m, n \in \overline{1, N}}$ będzie jej odwrotnością. Wówczas

$$g_m \equiv \sum_{n=1}^N \delta_{n,m}^R \triangleright g_n = \sum_{k,n=1}^N (M_k^n \cdot_R N_n^m) \triangleright g_n = \sum_{k=1}^N N_m^k \triangleright h_k,$$

co pokazuje, że $\mathcal{B}'$ jest układem generującym.

Założmy dalej, że dla pewnej rodziny $\{r^m\}_{m \in \overline{1, N}} \subset R$ zachodzi równość

$$\sum_{m=1}^N r^m \triangleright h_m = 0_G,$$

którą możemy przepisać w postaci

$$\sum_{n=1}^N \left(\sum_{m=1}^N r^m \cdot_R M_m^n \right) \triangleright g_n = 0_G.$$

Liniowa niezależność $\mathcal{B}$ pozwala wtedy stwierdzić

$$\sum_{m=1}^N r^m \cdot_R M_m^n = 0_R,$$

więc też

$$r^k \equiv \sum_{m=1}^N r^m \cdot_R \delta_{m,k}^R = \sum_{m,n=1}^N r^m \cdot_R M_m^n \cdot_R N_n^k = \sum_{n=1}^N 0_R \cdot_R N_n^k = 0_R,$$

skąd wniosek, że zbiór $\mathcal{B}'$ jest liniowo niezależny. Ostatecznie więc jest on bazą G .

□

Z połączenia ostatniego stwierdzenia z formułami (8.26) i (8.27) wyprowadzamy bez trudu proste acz poręczne

STWIERDZENIE 101. *Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 68, 70, 75, 78 i 82, Cor. 14, Stw. 75, 95, 96, 97, 98 i 99 oraz Tw. 8.11. Niechaj $\mathcal{B}_1^{(\alpha)}, \mathcal{B}_2^{(\alpha)}$, $\alpha \in \{1, 2\}$ będą dwiema dowolnymi bazami skończenie generowanego modułu $G^{(\alpha)}$ nad pierścieniem (przemiennym) R . Dla dowolnego odwzorowania R -liniowego $\chi \in \text{Hom}_R(G^{(1)}, G^{(2)})$ i dowolnych elementów $g^{(\alpha)} \in G^{(\alpha)}$ spełnione są formuły przejścia (między bazami)*

$$\begin{aligned} [\chi]_{\mathcal{B}_2^{(1)}}^{\mathcal{B}_2^{(2)}} &= [\text{id}_{G^{(2)}}]_{\mathcal{B}_1^{(2)}}^{\mathcal{B}_2^{(2)}} \square_R [\chi]_{\mathcal{B}_1^{(1)}}^{\mathcal{B}_1^{(2)}} \square_R [\text{id}_{G^{(1)}}]_{\mathcal{B}_2^{(1)}}^{\mathcal{B}_1^{(1)}}, \\ [g^{(\alpha)}]_{\mathcal{B}_2^{(\alpha)}}^{\mathcal{B}_2^{(\alpha)}} &= [\text{id}_{G^{(\alpha)}}]_{\mathcal{B}_1^{(\alpha)}}^{\mathcal{B}_2^{(\alpha)}} \square_R [g^{(\alpha)}]_{\mathcal{B}_1^{(\alpha)}}^{\mathcal{B}_1^{(\alpha)}}, \end{aligned}$$

przy czym

$$[\text{id}_{G^{(\alpha)}}]_{\mathcal{B}_1^{(\alpha)}}^{\mathcal{B}_2^{(\alpha)}} \square_R [\text{id}_{G^{(\alpha)}}]_{\mathcal{B}_2^{(\alpha)}}^{\mathcal{B}_1^{(\alpha)}} = \mathbf{1}_{\text{rk}_R(G^{(\alpha)})} = [\text{id}_{G^{(\alpha)}}]_{\mathcal{B}_2^{(\alpha)}}^{\mathcal{B}_1^{(\alpha)}} \square_R [\text{id}_{G^{(\alpha)}}]_{\mathcal{B}_1^{(\alpha)}}^{\mathcal{B}_2^{(\alpha)}}.$$

■

Warto w tym momencie zauważyć, w odniesieniu do przestrzeni wektorowych nad ciałem $\mathbb{K}$, że wszelka nietrywialna struktura macierzy (dowolnego) odwzorowania $\mathbb{K}$ -liniowego jest związana z wyborem baz w dziedzinie oraz w przeciwdziedzinie (a ściślej – w obrazie) tegoż odwzorowania. Mówi o tym

STWIERDZENIE 102. *(O postaci kanonicznej (macierzy) odwzorowania $\mathbb{K}$ -liniowego) Przyjmijmy notację Def. 67, 21, 32, 35, 36, 61, 63, 65, 68, 70, 73, 75, 78 i 82, Cor. 14, Stw. 75, 95, 96, 97, 98 i 99 oraz Tw. 8.11. Dla dowolnych dwóch skończenie wymiarowych przestrzeni wektorowych $V^{(\alpha)}$, $\alpha \in \{1, 2\}$ nad ciałem $\mathbb{K}$, i dla dowolnego odwzorowania $\mathbb{K}$ -liniowego $\chi \in \text{Hom}_{\mathbb{K}}(V^{(1)}, V^{(2)})$ istnieje taki wybór odnośnych baz $\mathcal{B}^{(\alpha)}$, przy którym macierz χ przyjmuje kanoniczną postać blokową*

$$[\chi]_{\mathcal{B}^{(1)}}^{\mathcal{B}^{(2)}} = \begin{pmatrix} \mathbf{1}_r & \mathbf{0}_{r \times k} \\ \mathbf{0}_{(D^{(2)}-r) \times r} & \mathbf{0}_{(D^{(2)}-r) \times k} \end{pmatrix},$$

gdzie $\mathbf{0}_{m \times n} \in \text{Mat}(\mathbb{K}; m \times n)$ jest macierzą o wszystkich wyrazach równych $0_{\mathbb{K}}$ i gdzie

$$r := \dim_{\mathbb{K}} \text{Im } \chi, \quad k := \dim_{\mathbb{K}} \text{Ker } \chi, \quad D^{(2)} := \dim_{\mathbb{K}} V^{(2)}.$$

■

Dowód: Bazę $\mathcal{B}^{(1)}$ otrzymujemy jak $\Gamma^{(1)}$ w dowodzie Stw. 83. Baza $\mathcal{B}^{(2)}$ powstaje z uzupełnienia odnośnej bazy $\text{Im } \chi$ do bazy $V^{(2)}$. □

Rola, jaką odgrywa wymiar obrazu odwzorowania $\mathbb{K}$ -liniowego, także w dalszej części wykładu, usprawiedliwia wprowadzenie dla niego specjalnej nazwy i osobnego oznaczenia.

DEFINICJA 83. Przyjmijmy notację Def. 11, 32, 35, 36, 61, 63, 64, 65, 72 i 73. Niechaj $V^{(\alpha)}$, $\alpha \in \{1, 2\}$ będą dwiema dowolnymi skończenie wymiarowymi przestrzeniami wektorowymi nad ciałem $\mathbb{K}$, i niech $\chi \in \text{Hom}_{\mathbb{K}}(V^{(1)}, V^{(2)})$ będzie dowolnym odwzorowaniem $\mathbb{K}$ -liniowym. **Rząd odwzorowania $\mathbb{K}$ -liniowego** to wymiar jego obrazu, oznaczany jako

$$\text{rk } \chi := \dim_{\mathbb{K}} \text{Im } \chi.$$

▲

Elementarne własności rzędu odwzorowania R -liniowego podaje

STWIERDZENIE 103. Przyjmijmy notację Def. 11, 32, 35, 36, 61, 63, 64, 65, 72, 73 i 83. Prawdziwe są następujące zdania:

- (i) $\text{rk } \chi \leq \min\{\dim_{\mathbb{K}} G^{(1)}, \dim_{\mathbb{K}} G^{(2)}\}$;
- (ii) jeśli $\dim_{\mathbb{K}} G^{(1)} < \infty$, to $\text{rk } \chi = \dim_{\mathbb{K}} G^{(1)} \iff \chi$ jest iniektywny;
- (iii) jeśli $\dim_{\mathbb{K}} G^{(2)} < \infty$, to $\text{rk } \chi = \dim_{\mathbb{K}} G^{(2)} \iff \chi$ jest suriektywny.

Dowód: Wszystkie wypisane (nie)równości wynikają wprost z koniunkcji bilansów wymiarów

$$\dim_{\mathbb{K}} G^{(1)} = \dim_{\mathbb{K}} \text{Ker } \chi + \text{rk } \chi,$$

$$\dim_{\mathbb{K}} G^{(2)} = \text{rk } \chi + \dim_{\mathbb{K}} (G^{(2)} / \text{Im } \chi) \equiv \text{rk } \chi + \dim_{\mathbb{K}} \text{Coker } \chi.$$

□

■

W związku z opisaną odpowiednością między odwzorowaniami R -liniowymi między modułami wolnymi i ich macierzowymi realizacjami wprowadzamy także

DEFINICJA 84. Przyjmijmy notację Def. 11, 67, 21, 32, 61, 63, 68, 75 i 82, Stw. 75 oraz Przykł. 41 i niech $\mathbb{K}$ będzie ciałem. **Rząd macierzy** $M \in \text{Mat}(\mathbb{K}; N_1 \times N_2)$ to wymiar powłoki $\mathbb{K}$ -liniowej jej kolumn,

$$\text{rk } M := \dim_{\mathbb{K}} \langle M_{\bullet 1}^{\bullet}, M_{\bullet 2}^{\bullet}, \dots, M_{\bullet N_2}^{\bullet} \rangle_{\mathbb{K}},$$

przy czym kolumny traktujemy tutaj jako elementy przestrzeni wektorowej $\text{Mat}(\mathbb{K}, N_1 \times 1) \equiv \mathbb{K}^{\times N_1}$, czyli tzw. **wektory kolumnowe**.



Zachodzi oczywiście

STWIERDZENIE 104. Przyjmijmy notację Def. 11, 67, 21, 32, 35, 61, 63, 65, 68, 70, 75, 78, 82, 84 i 83, Przykł. 41, Cor. 14, Stw. 75, 95, 96, 97, 98 i 99 oraz Tw. 8.11. Niechaj $V^{(1)}$ i $V^{(2)}$ będą dwiema przestrzeniami wektorowymi skończonego wymiaru nad ciałem $\mathbb{K}$, o bazach – odpowiednio – $\mathcal{B}^{(1)}$ i $\mathcal{B}^{(2)}$, i niech $\chi : V^{(1)} \rightarrow V^{(2)}$ będzie odwzorowaniem $\mathbb{K}$ -liniowym. Wówczas zachodzi tożsamość

$$\mathrm{rk} \chi = \mathrm{rk} [\chi]_{\mathcal{B}^{(1)}}^{\mathcal{B}^{(2)}}.$$



W dalszej części kursu, równoległe do naturalnego kierunku jego rozwoju abstrakcyjnego, będziemy rozwijać i wykorzystywać poczynione tu obserwacje dotyczące prostego związku między odwzorowaniami R -liniowymi i macierzami, w tym w szczególności tymi o wyrazach z pierścienia R .

8.7. Równania liniowe

Przedyskutowany powyżej problem algebraicznego opisu transformacji bazy w module wolnym ma swoje naturalne uogólnienie, jakim jest *zagadnienie odwrotne* dla zadanego odwzorowania R -liniowego $\chi \in \mathrm{Hom}_R(G^{(1)}, G^{(2)})$ między dwoma R -modułami lewostronnymi $G^{(1)}$ i $G^{(2)}$, polegające na wyznaczeniu przeciwobrazu $\chi^{-1}(\{\nu\})$ ustalonego elementu $\nu \in G^{(2)}$ przeciwdziedziny χ . Jego rozwiązanie sprowadza się do znalezienia wszystkich elementów $x \in G^{(1)}$ dziedziny χ spełniających równanie

$$\chi(x) = \nu \iff x \in \chi^{-1}(\{\nu\}).$$

Motywacji do rozważania tego typu zagadnień dostarcza chociażby geometria afiniczna czy teoria równań różniczkowych wyższego stopnia oraz cząstkowych. Ich dyskusję zaczniemy od

DEFINICJA 85. Przyjmijmy notację Def. 21, 32, 35, 37, 61 i 65. Niechaj $((G^{(\alpha)}, +_{(\alpha)}, \mathbf{P}_{(\alpha)}, \bullet \mapsto 0_{(\alpha)}), \ell^{(\alpha)})$, $\alpha \in \{1, 2\}$ będą dwoma R -modułami nad pierścieniem R i niech $\chi : G^{(1)} \rightarrow G^{(2)}$ będzie odwzorowaniem R -liniowym. Ustalmy element $\nu \in G^{(2)}$. **Równanie liniowe niejednorodne z niejednorodnością** ν to równanie postaci

$$\chi(x) = \nu,$$

w którym x jest **niewiadomą**, z założenia należącą do $G^{(1)}$. W szczególnym przypadku $\nu = 0_{(2)}$ mówimy o **równaniu liniowym jednorodnym**.

Dowolny element $g \in G^{(1)}$, dla którego powyższe równanie obraca się w tożsamość po podstawieniu $x := g$, nosi miano **rozwiązania równania liniowego (niejednorodnego)**. Zbiór

$$\mathcal{R}(\chi, \nu) := \chi^{-1}(\{\nu\})$$

nazywamy **zbiorem rozwiązań równania liniowego (niejednorodnego)**. Ilekroć $\mathcal{R}(\chi, \nu) = \emptyset$, równanie określamy jako **sprzeczne**.



Przywoławszy Stw. 35, otrzymujemy natychmiast prosty opis zbioru rozwiązań niesprzecznego równania liniowego.

STWIERDZENIE 105. *Przyjmijmy notację Def. 21, 32, 35, 36, 37, 42, 61, 65 i 85 oraz Stw. 40. Niechaj $g_* \in G^{(1)}$ będzie dowolnym rozwiązaniem równania liniowego niejednorodnego*

$$\chi(x) = \nu.$$

Wówczas

$$\mathcal{R}(\chi, \nu) = g_* +_{(1)} \mathcal{R}(\chi, 0_{(2)}) \equiv g_* +_{(1)} \text{Ker } \chi \in G^{(1)} / \text{Ker } \chi.$$

Równanie powyższe ma zatem dokładnie jedno rozwiązanie wtedy i tylko wtedy, gdy ma przynajmniej jedno rozwiązanie i χ jest monomorfizmem. ■

Należy podkreślić, że zbiór $\mathcal{R}(\chi, 0_{(2)})$ nigdy nie jest pusty, zawiera bowiem w szczególności **rozwiązanie trywialne równania jednorodnego**

$$0_{(1)} \in \mathcal{R}(\chi, 0_{(2)}).$$

W przypadku, gdy mamy do czynienia z modułami wolnymi (w szczególności gdy $R = \mathbb{K}$ jest ciałem), dyskusję zagadnienia istnienia i jednoznaczności rozwiązań równania liniowego wygodnie jest przenieść w dziedzinę algebry macierzowej, odwołując się przy tym do fundamentalnego Tw. 8.11. Ten tok rozumowania prowadzi nas wprost do

DEFINICJA 86. Przyjmijmy notację Def. 67, 21, 32, 61, 64, 68, 75 i 82, Stw. 75, 95 i 96 oraz Przykł. 41 i niech R będzie pierścieniem przemiennym. Dla dowolnych liczb $N_1, N_2 \in \mathbb{N} \setminus \{0\}$ ustalmy elementy $M \in \text{Mat}(R; N_1 \times N_2)$ oraz $\nu \in \text{Mat}(R; N_1 \times 1) \equiv R^{\times N_1}$. **Niejednorodny układ równań liniowych o współczynnikach z R o macierzy M i niejednorodności ν** (zwany dalej w skrócie niejednorodnym układem równań liniowych, ilekroć obiekty definiujące R, M, ν są znane) to równanie macierzowe

$$(8.28) \quad M \odot x = \nu,$$

w którym x jest **niewiadomą**, z założenia należącą do $\text{Mat}(R; N_2 \times 1) \equiv R^{\times N_2}$. W szczególnym przypadku $\nu = \mathbf{0}_{N_1 \times 1}$ mówimy o **jednorodnym układzie równań liniowych**.

Dowolny element $g \in \text{Mat}(R; N_2 \times 1)$, dla którego powyższe równanie obraca się w tożsamość po podstawieniu $x := g$, nosi miano **rozwiązania (niejednorodnego) układu równań liniowych**. Zbiór

$$\mathcal{R}(M, \nu) := \{ g \in \text{Mat}(R; N_2 \times 1) \mid M \odot g = \nu \}$$

nazywamy **zbiorem rozwiązań (niejednorodnego) układu równań liniowych**. Ilekroć $\mathcal{R}(M, \nu) = \emptyset$, układ równań określamy jako **sprzeczny**.

Wprowadzamy ponadto pojęcia pomocnicze: **jądro macierzy** to podmoduł

$$\text{Ker } M := \mathcal{R}(M, \mathbf{0}_{N_1 \times 1}) \subset \text{Mat}(R; N_2 \times 1),$$

obraz macierzy to podmoduł

$$\text{Im } M := \langle M^\bullet_1, M^\bullet_2, \dots, M^\bullet_{N_2} \rangle_R \subset \text{Mat}(R; N_1 \times 1),$$

natomiast **macierz rozszerzona niejednorodnego układu równań liniowych** to macierz

$$[M | \nu] \in \text{Mat}(R; N_1 \times (N_2 + 1))$$

o kolumnach

$$[M | \nu]^\bullet_i := M^\bullet_i, \quad i \in \overline{1, N_2}, \quad [M | \nu]^\bullet_{N_2+1} := \nu,$$

tj. macierz otrzymana przez dostawienie niejednorodności ν do kolumn macierzy M jako kolumny o indeksie $N_2 + 1$. ▲

Przepisawszy układ równań liniowych (8.28) w postaci

$$(8.29) \quad \sum_{i=1}^{N_2} x^i \triangleright_{(N_1)} M^\bullet_i = \nu,$$

bądź też – dla $x^{N_2+1} := -\mathbf{1}_R$ – w postaci równoważnej

$$\sum_{i=1}^{N_2+1} x^i \triangleright_{(N_1)} M^\bullet_i = \mathbf{0}_{N_1 \times 1},$$

gdzie zarówno suma jak i działanie $\triangleright$ są wyprowadzonymi wcześniej operacjami „współrzędna po współrzędnej” z Przykł. 34 (2), spostrzegamy natychmiast, że pytanie o istnienie rozwiązania układu można równie dobrze rozumieć jako pytanie o przynależność niejednorodności układu do powłoki liniowej zbioru kolumn jego macierzy. Obserwację tę precyzuje i rozszerza (w przypadku, gdy $R = \mathbb{K}$ jest ciałem) następujące

STWIERDZENIE 106. (Twierdzenie Kroneckera–Capelliego albo¹⁶ Twierdzenie Rouchégo–Fonteného) *Przyjmijmy notację Def. 11, 67, 21, 32, 61, 63, 64, 68, 75, 82, 84 i 86, Stw. 75, 95 i 96 oraz Przykł. 41 i niech $\mathbb{K}$ będzie ciałem. Układ równań liniowych*

$$M \odot x = \nu$$

ma rozwiązanie wtedy i tylko wtedy, gdy spełniony jest jeden z równoważnych warunków:

- (i) $\nu \in \text{Im } M$;
- (ii) $\text{rk } [M | \nu] = \text{rk } M$.

Układ ten ma dokładnie jedno rozwiązanie wtedy i tylko wtedy, gdy rząd jego macierzy jest równy rzędowi macierzy rozszerzonej i zarazem maksymalny, tj.

$$\text{rk } [M | \nu] = N_2 = \text{rk } M.$$
■

Dowód: Równoważność istnienia rozwiązania z warunkiem (i) staje się oczywista w świetle wcześniejszej naszej reinterpretacji układu równań liniowych z niejednorodnością, a stwierdzenie dotyczące jednoznaczności rozwiązania jest prostą konsekwencją koniunkcji warunku (ii) i bilansu wymiarów

$$\text{rk } M = N_2 - \dim_{\mathbb{K}} \text{Ker } M,$$

¹⁶Dруга назва, historycznie najbardziej bodaj usprawiedliwiona, jest używana w krajach francuskojęzycznych.

rozpatrywanej w połączeniu ze Stw. 105. Wystarczy zatem udowodnić równoważność (i) $\iff$ (ii). Implikacja $\nu \in \langle M_1^\bullet, M_2^\bullet, \dots, M_{N_2}^\bullet \rangle_{\mathbb{K}} \implies \langle M_1^\bullet, M_2^\bullet, \dots, M_{N_2}^\bullet, \nu \rangle_{\mathbb{K}} = \langle M_1^\bullet, M_2^\bullet, \dots, M_{N_2}^\bullet \rangle_{\mathbb{K}}$ nie wymaga wyjaśnień. Dla uzyskania implikacji odwrotnej zauważmy, że równość wypisanych powłok $\mathbb{K}$ -liniowych oznacza istnienie, dla dowolnych $\xi \in \mathbb{K}$ i $\{\xi^j\}_{j \in \overline{1, N_2}} \subset \mathbb{K}$, rodziny $\{\lambda^i\}_{i \in \overline{1, N_2}}$ elementów ciała $\mathbb{K}$ spełniającej równość

$$\sum_{i=1}^{N_2} \xi^i \triangleright_{(N_1)} M_i^\bullet + \xi \triangleright_{(N_1)} \nu = \sum_{j=1}^{N_2} \lambda^j \triangleright_{(N_1)} M_j^\bullet,$$

zapisaną w konwencji Przykł. 34 (2). Wybierając dowolne $\xi \neq 0_{\mathbb{K}}$, otrzymujemy równość

$$\nu = \sum_{i=1}^{N_2} (\xi^{-1} \cdot_{\mathbb{K}} (\lambda^i - \xi^i)) \triangleright_{(N_1)} M_i^\bullet,$$

która kończy dowód. $\square$

8.8. Elementy teorii form wieloliniowych i wyznaczników

Warto zwrócić uwagę, że warunek maksymalności rzędu macierzy M można zinterpretować jako warunek liniowej niezależności jej kolumn. To spostrzeżenie każe nam zastanowić się nad okolicznościami, w których układ kolumn macierzy o wyrazach z ciała $\mathbb{K}$ albo – ogólniej – z pierścienia przemennego R jest liniowo niezależny. Wygodnych narzędzi formalnych do takiej analizy dostarcza teoria wyznaczników, która pozwala też zgrabnie zapisać rozwiązania odnośnych układów równań liniowych, gdy te istnieją. Teoria ta stanowi specjalizację teorii odwzorowań wieloliniowych na modułach nad R . Mając na względzie przyszłe zastosowania tej szerszej teorii w dyskusji dwoistości i form kwadratowych, wykorzystamy nadarzającą się tutaj sposobność do zbudowania stosownie poszerzonej bazy pojęciowej. W celu wyrobienia sobie elementarnych intuicji odnośnie do pojawiających się tu struktur matematycznych rozwiążemy konkretne zagadnienie polegające na ustaleniu algebraicznych warunków liniowej zależności nad ciałem $\mathbb{K}$ kolumn macierzy

$$\begin{pmatrix} M_1^1 & M_2^1 \\ M_1^2 & M_2^2 \end{pmatrix} \in \text{Mat}(\mathbb{K}; 2).$$

Założymy przy tym – dla uczynienia zagadnienia nietrywialnym – że jedna z kolumn, np. $M_2^\bullet$, jest niezerowa, a więc np. $M_2^2 \neq 0_{\mathbb{K}}$. Z warunku liniowej zależności kolumn,

$$\lambda \triangleright_{(2)} M_1^\bullet \boxplus_{\mathbb{K}} \mu \triangleright_{(2)} M_2^\bullet = \mathbf{0}_{2 \times 1}, \quad (\lambda, \mu) \in \mathbb{K}^{\times 2} \setminus \{(0_{\mathbb{K}}, 0_{\mathbb{K}})\},$$

w którego zapisie $\triangleright_{(2)}$ symbolizuje działanie $\mathbb{K}$ na kolumny polegające na „mnożeniu po współrzędnej” z Przykł. 34 (2), wyprowadzamy równość

$$\mu = -\lambda \cdot_{\mathbb{K}} M_1^2 \cdot_{\mathbb{K}} (M_2^2)^{-1},$$

a stąd

$$\begin{aligned} 0_{\mathbb{K}} &= \lambda \cdot_{\mathbb{K}} M_1^1 +_{\mathbb{K}} \mu \cdot_{\mathbb{K}} M_2^1 = \lambda \cdot_{\mathbb{K}} M_1^1 - \lambda \cdot_{\mathbb{K}} M_2^2 \cdot_{\mathbb{K}} (M_2^2)^{-1} \cdot_{\mathbb{K}} M_2^1 \\ &= \lambda \cdot_{\mathbb{K}} (M_2^2)^{-1} \cdot_{\mathbb{K}} (M_1^1 \cdot_{\mathbb{K}} M_2^2 - M_2^1 \cdot_{\mathbb{K}} M_1^2). \end{aligned}$$

Równość $\lambda = 0_{\mathbb{K}}$ pociąga za sobą równość $\mu = 0_{\mathbb{K}}$ i z tego powodu musimy ją wykluczyć, co pozwala przepisać powyższe w równoważnej postaci

$$M_1^1 \cdot_{\mathbb{K}} M_2^2 - M_2^1 \cdot_{\mathbb{K}} M_1^2 = 0_{\mathbb{K}}.$$

Potraktujmy wyrażenie po lewej stronie równości jako wynik odwzorowania w $\mathbb{K}$ kolumn macierzy M ,

$$\varphi(M_1^\bullet, M_2^\bullet) := M_1^1 \cdot_{\mathbb{K}} M_2^2 - M_2^1 \cdot_{\mathbb{K}} M_1^2.$$

Odwzorowanie to jest jawnie $\mathbb{Z}$ -dwuliniowe,

$$\varphi(M_1^\bullet \boxplus_{\mathbb{K}} N_1^\bullet, M_2^\bullet) = \varphi(M_1^\bullet, M_2^\bullet) +_{\mathbb{K}} \varphi(N_1^\bullet, M_2^\bullet),$$

$$\varphi(M_1^\bullet, M_2^\bullet \boxplus_{\mathbb{K}} N_2^\bullet) = \varphi(M_1^\bullet, M_2^\bullet) +_{\mathbb{K}} \varphi(M_1^\bullet, N_2^\bullet),$$

i R -jednorodne w każdym z argumentów,

$$\varphi(\lambda \triangleright M_1^\bullet, M_2^\bullet) = \lambda \cdot_{\mathbb{K}} \varphi(M_1^\bullet, M_2^\bullet) = \varphi(M_1^\bullet, \lambda \triangleright M_2^\bullet),$$

a ponadto antysymetryczne względem transpozycji argumentów,

$$\varphi(M_2^\bullet, M_1^\bullet) = -\varphi(M_1^\bullet, M_2^\bullet).$$

Przeprowadzona analiza skłania nas do wypowiedzenia

DEFINICJA 87. Przyjmijmy notację Def. 21, 32, 35, 61 oraz 65 i niech R będzie pierścieniem przemiennym. Niechaj $G^{(\alpha)}$, $\alpha \in \overline{1, n}$ oraz G będą modułami nad pierścieniem przemiennym R . **Odwzorowanie n -liniowe nad R** to dowolne odwzorowanie

$$\varphi : G^{(1)} \times G^{(2)} \times \dots \times G^{(n)} \longrightarrow G,$$

które jest R -liniowe (tj. $\mathbb{Z}$ -liniowe i R -jednorodne) względem każdego swojego argumentu, czyli spełnia warunek

$$\begin{aligned} & \forall_{i \in \overline{1, n}} \forall_{(g_1, g_2, \dots, g_{i-1}, g_{i+1}, g_{i+2}, \dots, g_n) \in \times_{\beta \in \overline{1, n} \setminus \{i\}} G^{(\beta)}} \\ & : \varphi(g_1, g_2, \dots, g_{i-1}, \cdot, g_{i+1}, g_{i+2}, \dots, g_n) \in \text{Hom}_R(G^{(i)}, G). \end{aligned}$$

Zbiór wszystkich takich odwzorowań oznaczamy symbolem

$$\mathbb{L}_R(G^{(1)}, G^{(2)}, \dots, G^{(n)}; G).$$

W przypadku, gdy $\forall_{\alpha \in \overline{1, n}} : G^{(\alpha)} = H$, mówimy o **odwzorowaniu n -liniowym na H** , a odnośny zbiór zapisujemy jako

$$\mathbb{L}_R^n(H; G) \equiv \mathbb{L}_R(\underbrace{H, H, \dots, H}_{n \text{ razy}}; G).$$

Jeśli ponadto $G = R$, to mamy do czynienia z **formami n -liniowymi** oznaczanymi – odpowiednio – jako

$$\mathbb{L}_R(G^{(1)}, G^{(2)}, \dots, G^{(n)}) \quad \text{lub} \quad \mathbb{L}_R^n(H).$$

▲

Bez trudu stwierdzamy prawdziwość poniższego

STWIERDZENIE 107. Przyjmijmy notację Def. 21, 32, 35, 61, 65 i 87. Zbiór $\mathcal{L}_R(G^{(1)}, G^{(2)}, \dots, G^{(n)}; G)$ (a zatem także zbiory $\mathcal{L}_R^n(H; G)$, $\mathcal{L}_R(G^{(1)}, G^{(2)}, \dots, G^{(n)})$ i $\mathcal{L}_R^n(H)$) jest nośnikiem struktury R -modułu z operacjami grupowymi

$$\begin{aligned} \phi_2 &: \mathcal{L}_R(G^{(1)}, G^{(2)}, \dots, G^{(n)}; G)^{\times 2} \longrightarrow \mathcal{L}_R(G^{(1)}, G^{(2)}, \dots, G^{(n)}; G) \\ &: (\varphi_1, \varphi_2) \longmapsto \varphi_1 + \varphi_2, \\ \phi_1 &: \mathcal{L}_R(G^{(1)}, G^{(2)}, \dots, G^{(n)}; G) \curvearrowright : \varphi \longmapsto -\varphi, \\ \phi_0 &: \{\bullet\} \longrightarrow \mathcal{L}_R(G^{(1)}, G^{(2)}, \dots, G^{(n)}; G) : \bullet \longmapsto 0, \end{aligned}$$

określonymi wzorami

$$\begin{aligned} (\varphi_1 + \varphi_2)(g^{(1)}, g^{(2)}, \dots, g^{(n)}) &:= \varphi_1(g^{(1)}, g^{(2)}, \dots, g^{(n)}) +_G \varphi_2(g^{(1)}, g^{(2)}, \dots, g^{(n)}), \\ (-\varphi)(g^{(1)}, g^{(2)}, \dots, g^{(n)}) &:= P_G(\varphi_1(g^{(1)}, g^{(2)}, \dots, g^{(n)})), \\ 0(g^{(1)}, g^{(2)}, \dots, g^{(n)}) &:= 0_G, \end{aligned}$$

oraz z działaniem pierścienia

$$\begin{aligned} \ell &: R \times \mathcal{L}_R(G^{(1)}, G^{(2)}, \dots, G^{(n)}; G) \longrightarrow \mathcal{L}_R(G^{(1)}, G^{(2)}, \dots, G^{(n)}; G) \\ &: (r, \varphi) \longmapsto r \triangleright \varphi, \end{aligned}$$

określonym formułą

$$(r \triangleright \varphi)(g^{(1)}, g^{(2)}, \dots, g^{(n)}) := r \triangleright_G \varphi(g^{(1)}, g^{(2)}, \dots, g^{(n)}).$$

■

W przypadku odwzorowania n -liniowego na pojedynczym R -module zasadnym jest pytanie o własności symetrii tegoż odwzorowania, tj. jego zachowanie względem działania grupy symetrycznej $\mathfrak{S}_n$ na zbiorze jego argumentów.

DEFINICJA 88. Przyjmijmy notację Def. 21, 32, 35, 61, 65 i 87. Odwzorowanie $\varphi \in \mathcal{L}_R^n(H; G)$ nazywamy

- **symetrycznym**, jeśli $\forall_{\sigma \in \mathfrak{S}_n} : \varphi \circ \sigma = \varphi$ – ich zbiór oznaczamy symbolem $\mathcal{L}_R^{n, \text{sym}}(H; G)$ (wzgl. $\mathcal{L}_R^{n, \text{sym}}(H)$);
- **skośnie symetrycznym** (lub **antysymetrycznym**), jeśli $\forall_{\sigma \in \mathfrak{S}_n} : \varphi \circ \sigma = \text{sgn}(\sigma) \varphi$ – ich zbiór oznaczamy symbolem $\mathcal{L}_R^{n, \text{antysym}}(H; G)$ (wzgl. $\mathcal{L}_R^{n, \text{antysym}}(H)$);
- **alternującym**, jeśli

$$\forall_{\substack{i, j \in \overline{1, n} \\ i < j}} : (g^{(i)} = g^{(j)} \implies \varphi(g^{(1)}, g^{(2)}, \dots, g^{(n)}) = 0_G);$$

ich zbiór oznaczamy symbolem $\mathcal{L}_R^{n, \text{alt}}(H; G)$ (wzgl. $\mathcal{L}_R^{n, \text{alt}}(H)$).

▲

PRZYKŁAD(Y) 43.

(1) Dla dowolnego pierścienia przemiennego R odwzorowanie

$$\delta : \underbrace{R^N \times R^N \times \dots \times R^N}_{n \text{ razy}} \longrightarrow R : (g^{(1)}, g^{(2)}, \dots, g^{(n)}) \longmapsto g_1^{(1)} \cdot_R g_2^{(2)} \cdot_R \dots \cdot_R g_n^{(n)},$$

w którego definicji $g_j^{(i)}$ jest współczynnikiem przy e_j w rozkładzie $g^{(i)}$ w bazie standardowej $\{e_j\}_{j \in \overline{1, N}}$ R -modułu R^N , jest n -liniowe i symetryczne.

(2) Pochodna stopnia n odwzorowania $F \in C^k(\mathbb{R}^{N_1}, \mathbb{R}^{N_2})$ w punkcie $p \in \mathbb{R}^{N_1}$ dziedziny jest symetrycznym odwzorowaniem n -liniowym

$$D^n F(p) : \underbrace{R^{N_1} \times R^{N_1} \times \dots \times R^{N_1}}_{n \text{ razy}} \longrightarrow \mathbb{R}^{N_2},$$

określonym jednoznacznie przez wartości przyjmowane na łańcuchach elementów bazy (standardowej) $\mathbb{R}^{N_1}$ (przy oznaczeniu x^i na i -tą współrzędną kartezjańską argumentu F)

$$D^n F(p)(e_{i_1}, e_{i_2}, \dots, e_{i_n}) := \frac{\partial^n F}{\partial x^{i_1} \partial x^{i_2} \dots \partial x^{i_n}}(p), \quad i_1, i_2, \dots, i_n \in \overline{1, N_1}.$$

(3) **Komutator macierzy**

$$[\cdot, \cdot] : \text{Mat}(R; N)^{\times 2} \longrightarrow \text{Mat}(R; N) : (M, N) \longmapsto M \odot N - N \odot M$$

jest skośnie symetrycznym odwzorowaniem 2-liniowym.

(4) **Iloczyn wektorowy**

$$\mathbb{R}^3 \times \mathbb{R}^3 \longrightarrow \mathbb{R}^3 : \left(\sum_{i=1}^3 v^i e_i, \sum_{j=1}^3 w^j e_j \right) \longmapsto v \times w$$

o rozkładzie w bazie (standardowej) $\mathbb{R}$ -modułu $\mathbb{R}^3$

$$v \times w = (v^2 w^3 - v^3 w^2) e_1 +_{\mathbb{R}^3} (v^3 w^1 - v^1 w^3) e_2 +_{\mathbb{R}^3} (v^1 w^2 - v^2 w^1) e_3,$$

jest skośnie symetrycznym odwzorowaniem 2-liniowym.

(5) **Nawias Poissona**

$$\begin{aligned} \{\cdot, \cdot\}_{\text{P.B.}} & : C^\infty(\mathbb{R}^2, \mathbb{R})^{\times 2} \longrightarrow C^\infty(\mathbb{R}^2, \mathbb{R}) \\ & : (f_1, f_2) \longmapsto \frac{\partial f_1}{\partial x^1} \frac{\partial f_2}{\partial x^2} - \frac{\partial f_2}{\partial x^1} \frac{\partial f_1}{\partial x^2} =: \{f_1, f_2\}_{\text{P.B.}} \end{aligned}$$

jest skośnie symetrycznym odwzorowaniem 2-liniowym (dla $C^\infty(\mathbb{R}^2; \mathbb{R})$ traktowanego jako przestrzeni wektorowa nad $\mathbb{R}$). Struktura ta odgrywa istotną rolę w mechanice klasycznej (a także – w połączeniu z tą z punktu (3) powyżej – w mechanice kwantowej). Jej uogólnieniem, istotnym w pewnych sformułowaniach M-teorii, jest **nawias Nambu–Poissona**

$$\begin{aligned} \{\cdot, \cdot, \cdot\}_{\text{N.-P.B.}} & : C^\infty(\mathbb{R}^3, \mathbb{R})^{\times 3} \longrightarrow C^\infty(\mathbb{R}^3, \mathbb{R}) \\ & : (f_1, f_2, f_3) \longmapsto \sum_{\sigma \in \mathfrak{S}_3} \text{sgn}(\sigma) \frac{\partial f_1}{\partial x^{\sigma(1)}} \frac{\partial f_2}{\partial x^{\sigma(2)}} \frac{\partial f_3}{\partial x^{\sigma(3)}} \\ & =: \{f_1, f_2, f_3\}_{\text{N.-P.B.}} \end{aligned}$$

✓

Związek między odwzorowaniami skośnie symetrycznymi i alternującymi ustala

STWIERDZENIE 108. *Każde alternujące odwzorowanie n -liniowe jest skośnie symetryczne. Każda skośnie symetryczna forma n -liniowa nad ciałem o charakterystyce różnej od 2 jest alternująca.* ■

Dowód: Niech $\varphi \in \mathbb{L}_R^{n,\text{alt}}(H; G)$, a wtedy dla dowolnych $i, j \in \overline{1, n}$, $i < j$ oraz $g_k, g, h \in H$, $k \in \overline{1, n} \setminus \{i, j\}$ otrzymujemy równość

$$\begin{aligned}
 0_G &= \varphi(g_1, g_2, \dots, g_{i-1}, g +_H h, g_{i+1}, g_{i+2}, \dots, g_{j-1}, g +_H h, g_{j+1}, g_{j+2}, \dots, g_n) \\
 &= \varphi(g_1, g_2, \dots, g_{i-1}, g, g_{i+1}, g_{i+2}, \dots, g_{j-1}, g, g_{j+1}, g_{j+2}, \dots, g_n) \\
 &\quad +_G \varphi(g_1, g_2, \dots, g_{i-1}, h, g_{i+1}, g_{i+2}, \dots, g_{j-1}, h, g_{j+1}, g_{j+2}, \dots, g_n) \\
 &\quad +_H \varphi(g_1, g_2, \dots, g_{i-1}, g, g_{i+1}, g_{i+2}, \dots, g_{j-1}, h, g_{j+1}, g_{j+2}, \dots, g_n) \\
 &\quad +_H \varphi(g_1, g_2, \dots, g_{i-1}, h, g_{i+1}, g_{i+2}, \dots, g_{j-1}, g, g_{j+1}, g_{j+2}, \dots, g_n) \\
 &= \varphi(g_1, g_2, \dots, g_{i-1}, g, g_{i+1}, g_{i+2}, \dots, g_{j-1}, h, g_{j+1}, g_{j+2}, \dots, g_n) \\
 &\quad +_H \varphi(g_1, g_2, \dots, g_{i-1}, h, g_{i+1}, g_{i+2}, \dots, g_{j-1}, g, g_{j+1}, g_{j+2}, \dots, g_n),
 \end{aligned}$$

którą po uwzględnieniu dowolności argumentów możemy przepisać w postaci

$$\varphi \circ \tau_{i,j} = -\varphi \equiv \text{sgn}(\tau_{i,j}) \varphi.$$

Pierwsza część tezy wynika teraz wprost z Cor. 9.

Jeśli $\varphi \in \mathbb{L}_{\mathbb{K}}^{n,\text{antysym}}(H)$ nad ciałem $\mathbb{K}$, to stwierdzamy, co następuje (przy oznaczeniach jak wyżej):

$$\begin{aligned}
 &\varphi(g_1, g_2, \dots, g_{i-1}, g, g_{i+1}, g_{i+2}, \dots, g_{j-1}, g, g_{j+1}, g_{j+2}, \dots, g_n) \\
 &\equiv \varphi \circ \tau_{i,j}(g_1, g_2, \dots, g_{i-1}, g, g_{i+1}, g_{i+2}, \dots, g_{j-1}, g, g_{j+1}, g_{j+2}, \dots, g_n) \\
 &= \text{sgn}(\tau_{i,j}) \cdot_{\mathbb{K}} \varphi(g_1, g_2, \dots, g_{i-1}, g, g_{i+1}, g_{i+2}, \dots, g_{j-1}, g, g_{j+1}, g_{j+2}, \dots, g_n) \\
 &\equiv -\varphi(g_1, g_2, \dots, g_{i-1}, g, g_{i+1}, g_{i+2}, \dots, g_{j-1}, g, g_{j+1}, g_{j+2}, \dots, g_n).
 \end{aligned}$$

Możemy zatem zapisać (w notacji (5.1))

$$2\varphi(g_1, g_2, \dots, g_{i-1}, g, g_{i+1}, g_{i+2}, \dots, g_{j-1}, g, g_{j+1}, g_{j+2}, \dots, g_n) = 0_{\mathbb{K}},$$

co przy $\varphi(g_1, g_2, \dots, g_{i-1}, g, g_{i+1}, g_{i+2}, \dots, g_{j-1}, g, g_{j+1}, g_{j+2}, \dots, g_n) \neq 0_{\mathbb{K}}$, a więc odwracalnym, implikuje $1_{\mathbb{K}} +_{\mathbb{K}} 1_{\mathbb{K}} \equiv 21_{\mathbb{K}} = 0_{\mathbb{K}}$, czyli $\text{char}(\mathbb{K}) = 2$. □

Koniunkcja warunków wieloliniowości i alternowania narzuca bardzo ciasne więzy strukturalne na odwzorowania n -liniowe, o czym przekonuje nas

STWIERDZENIE 109. *Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65 i 87. Niechaj $\varphi \in \mathbb{L}_R^{n,\text{alt}}(H; G)$ i niech $\mathcal{H} := \{h^{(i)}\}_{i \in \overline{1, n}}$ będzie rodziną elementów R -modułu H . Wówczas dla dowolnej rodziny $\{g^{(i)}\}_{i \in \overline{1, n}}$ złożonej z elementów $g^{(i)} =$*

$$\begin{aligned}
& \sum_{j=1}^n r^i_j \triangleright_H h^{(j)} \text{ powłoki } R\text{-liniowej } \mathcal{H} \text{ zachodzi tożsamość} \\
& \varphi(g^{(1)}, g^{(2)}, \dots, g^{(n)}) \\
& = \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma) (r^1_{\sigma(1)} \cdot_R r^2_{\sigma(2)} \cdot_R \dots \cdot_R r^n_{\sigma(n)}) \triangleright_G \varphi(h^{(1)}, h^{(2)}, \dots, h^{(n)}).
\end{aligned}$$

■

Dowód: Wykorzystując R -liniowość φ w każdym argumentie z osobna, przepisujemy

$$\begin{aligned}
& \varphi(g^{(1)}, g^{(2)}, \dots, g^{(n)}) \\
& \equiv \varphi\left(\sum_{j_1=1}^n r^1_{j_1} \triangleright_H h^{(j_1)}, \sum_{j_2=1}^n r^2_{j_2} \triangleright_H h^{(j_2)}, \dots, \sum_{j_n=1}^n r^n_{j_n} \triangleright_H h^{(j_n)}\right) \\
& = \sum_{j_1=1}^n \sum_{j_2=1}^n \dots \sum_{j_n=1}^n (r^1_{j_1} \cdot_R r^2_{j_2} \cdot_R \dots \cdot_R r^n_{j_n}) \triangleright_G \varphi(h^{(j_1)}, h^{(j_2)}, \dots, h^{(j_n)}).
\end{aligned}$$

Ilekcioć $j_k = j_l$ dla dwóch indeksów $k \neq l$, prawa strona równości zeruje się, gdyż para $h^{(j_k)} = h^{(j_l)}$ jest anihilowana przez alternujące odwzorowanie φ . W takim razie sekwencje indeksów $(j_1, j_2, \dots, j_n)$ dające niezerowy wkład do kombinacji R -liniowej po prawej stronie równości stanowią permutacje zbioru $\overline{1, n}$. Przy tym ewidentnie każda permutacja z $\mathfrak{S}_\sigma$ występuje, i to dokładnie raz, w rzeczonyj kombinacji, a zatem tę ostatnią możemy przepisać w postaci

$$\begin{aligned}
& \varphi(g^{(1)}, g^{(2)}, \dots, g^{(n)}) \\
& \equiv \sum_{\sigma \in \mathfrak{S}_n} (r^1_{\sigma(1)} \cdot_R r^2_{\sigma(2)} \cdot_R \dots \cdot_R r^n_{\sigma(n)}) \triangleright_G \varphi(h^{(\sigma(1))}, h^{(\sigma(2))}, \dots, h^{(\sigma(n))}).
\end{aligned}$$

Po uwzględnieniu skośnej symetrii φ otrzymujemy tezę. □

Powyższe stwierdzenie pokazuje dowodnie, że ograniczenie alternującego odwzorowania n -liniowego do powłoki liniowej dowolnego n -elementowego podzbioru modułu, na którym definiujemy owo odwzorowanie, jest w sposób jednoznaczny określone przez obraz zbioru generującego względem tego odwzorowania. Obserwacja ta nabiera szczególnego znaczenia w przypadku modułów wolnych, na których skupimy uwagę w dalszej części wykładu.

Celem ustalenia bezpośredniego związku z wyjściowym zagadnieniem rozwiązywalności niejednorodnych układów równań liniowych (w opisie macierzowym), a zarazem dla wyrobienia sobie intuicji, którą następnie przeniesiemy na sytuacje bardziej skomplikowane, zaczniemy od zbadania struktury alternujących form wieloliniowych na modelowym module wolnym

$$H := R^{\times m} \equiv \oplus_{k=1}^m R.$$

Ciąg oczywistych utożsamień

$$\operatorname{Mat}(R; m \times n) \equiv \bigoplus_{k=1}^n \bigoplus_{l=1}^m R = \bigoplus_{k=1}^n \operatorname{Mat}(R; m \times 1) = \bigotimes_{i=1}^n R^{\times m},$$

wyrażających możliwość traktowania macierzy wskazanego typu jako n -składnikowych układów elementów modułu H zadawanych przez kolumny tychże macierzy,

pozwala nam przy tym używać w dyskusji form wieloliniowych na równych prawach z zapisem wyjściowym (wykorzystującym układów elementów dziedziny H) zapisu macierzowego, tj. w szczególności ewaluować formy wieloliniowe na macierzach. Kluczowe dla naszych rozważań jest

STWIERDZENIE 110. *Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 68, 70, 75, 77 i 87 oraz Przykł. 34 (2), 40 (3) i 41. Niechaj $\varphi \in \mathbb{L}_R^{n, \text{alt}}(R^{\times m})$. Wówczas $\varphi \equiv 0$, jeśli $n > m$, gdy zaś $n \leq m$, to forma φ jest jednoznacznie określona przez wartości przyjmowane przezeń na $\binom{m}{n}$ układach $(e_{i_1}, e_{i_2}, \dots, e_{i_n})$ elementów bazy standardowej $\{e_i\}_{i \in \overline{1, m}}$ R -modułu $R^{\times m}$ uporządkowanych przez relację $1 \leq i_1 < i_2 < \dots < i_n \leq m$. W szczególności przy $m = n$ formę φ zadaje pojedynczy skalar $\varphi(e_1, e_2, \dots, e_n)$.*

■

Dowód: Potraktujmy dowolny układ n elementów $g_i = \sum_{j=1}^m M_i^j \triangleright_n e_j$, $i \in \overline{1, n}$ jako układ kolumn macierzy $M = (M_i^j)_{(j,i) \in \overline{1, m} \times \overline{1, n}} \in \text{Mat}(R; m \times n)$. Stosując rozumowanie analogiczne do tego użytego w dowodzie poprzednim, możemy wtedy zapisać

$$\begin{aligned} \varphi(M) &= \sum_{j_1=1}^n \sum_{j_2=1}^n \cdots \sum_{j_n=1}^n (M_1^{j_1} \cdot_R M_2^{j_2} \cdot_R \cdots \cdot_R M_n^{j_n}) \cdot_R \varphi(e_{j_1}, e_{j_2}, \dots, e_{j_n}) \\ &= \sum_{(j_1, j_2, \dots, j_n) \in \binom{\overline{1, m}}{n}} \sum_{\sigma \in \mathfrak{S}_n} \text{sgn}(\sigma) (M_{\sigma(1)}^{j_1} \cdot_R M_{\sigma(2)}^{j_2} \cdot_R \cdots \cdot_R M_{\sigma(n)}^{j_n}) \\ &\quad \cdot_R \varphi(e_{j_1}, e_{j_2}, \dots, e_{j_n}), \end{aligned}$$

przy czym $\binom{\overline{1, m}}{n}$ jest zbiorem n -elementowych kombinacji bez powtórzeń elementów zbioru $\overline{1, m}$. Istotnie, każdy inny układ wektorów bazowych jest bądź to anihilowany przez φ (jeśli zawiera powtórzenia), bądź też sprowadza się do jednego z układów wyróżnionych przez stosowaną permutację argumentów formy (jeśli nie zawiera powtórzeń). Uwzględnienie tej ostatniej ewentualności prowadzi do konieczności wysumowania czynników skalarnych pochodzących od wszystkich permutacji n -elementowego zbioru wskaźników z ustalonej kombinacji $(j_1, j_2, \dots, j_n)$. Należy w tym miejscu podkreślić, że uzyskane w ten sposób wyrażenie skalarne

$$R(M; (j_1, j_2, \dots, j_n)) := \sum_{\sigma \in \mathfrak{S}_n} \text{sgn}(\sigma) (M_{\sigma(1)}^{j_1} \cdot_R M_{\sigma(2)}^{j_2} \cdot_R \cdots \cdot_R M_{\sigma(n)}^{j_n}) \in R$$

charakteryzuje *wyłącznie* argumenty formy φ , nie zaś – ją samą. Przepisawszy wynik powyższego rachunku w zwartej postaci

$$\varphi(M) = \sum_{(j_1, j_2, \dots, j_n) \in \binom{\overline{1, m}}{n}} R(M; (j_1, j_2, \dots, j_n)) \cdot_R \varphi(e_{j_1}, e_{j_2}, \dots, e_{j_n}),$$

odtworzymy tezę stwierdzenia. W szczególności jest jasnym, że przy $n > m$ forma φ anihiluje dowolny układ elementów modułu H , gdyż nie można wybrać spośród m indeksów bazy standardowej n indeksów wzajem *różnych*. □

Jak pokazuje ostatnie stwierdzenie, do w pełni jednoznacznego określenia formy maksymalnego rzędu (tj. formy o maksymalnej liczbie argumentów) na module $R^{\times m}$ potrzeba i wystarcza ustalenie wartości przyjmowanej przez nią na układzie

bazowym. Ta konstatacja prowadzi nas wprost do podstawowego celu praktycznego naszych analiz, jakim jest

DEFINICJA 89. Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 68, 70, 75, 77, 82 i 87 oraz Przykł. 34 (2), 40 (3) i 41. Niech R będzie pierścieniem przemennym i niech $N \in \mathbb{N} \setminus \{0\}$. **Wyznacznik macierzy kwadratowej stopnia N o wyrazach z R to alternująca forma N -liniowa**

$$\det_{(N)} : \text{Mat}(R; N) \equiv \bigotimes_{i=1}^N R^{\times N} \longrightarrow R$$

spełniająca **warunek normalizacyjny**

$$\det_{(N)}(\mathbf{1}_N) \equiv \det_{(N)}(e_1, e_2, \dots, e_N) := 1_R.$$

▲

Dotychczasowe nasze rozważania upewniają nas, że forma taka, o ile istnieje, jest dana jednoznacznie. Pozostaje zatem sprawdzić, czy warunek normalizacyjny jest niesprzeczny z warunkami N -liniowości i alternowania. Twierdząca odpowiedź na tak postawione pytanie jest treścią poniższego

TWIERDZENIE 8.12 (O istnieniu wyznacznika). *Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 82, 87 i 89 oraz Przykł. 34 (2) i 41. Wyznacznik macierzy kwadratowej M dowolnego stopnia $N \in \mathbb{N} \setminus \{0\}$ o wyrazach z pierścienia przemennego R istnieje i jest dany wzorem rekurencyjnym*

$$(8.30) \quad \det_{(N)}(M) = \sum_{j=1}^N (-1)^{i+j} M_{\#j}^i \cdot_R \det_{(N-1)}(M_{\#j}^{\#i}),$$

zapisanym, dla dowolnego $i \in \overline{1, N}$, przy użyciu macierzy $M_{\#j}^{\#i} \in \text{Mat}(R; N-1)$ otrzymanej z M przez usunięcie $M_{\bullet}^i$ (i -tego wiersza) i $M_{\bullet_j}^{\bullet}$ (j -tej kolumny). Wyznacznik tej ostatniej określamy mianem **minora (głównego) macierzy M** . Wypisany wzór to **rozwinięcie Laplace’a wyznacznika macierzy M według i -tego wiersza**.

■

Dowód: Zastosujemy (mocną) indukcję względem stopnia N . Połóżmy

$$\det_{(1)} := \text{id}_R$$

(co ma sens, gdyż $\det_{(1)}(1_R) = 1_R$) i przyjmijmy, że teza twierdzenia jest prawdziwa dla dowolnego stopnia $n < N$, przy czym $N \geq 2$. Postulujemy wówczas postać wyznacznika jak w treści twierdzenia. Wobec jednoznaczności $\det_{(N)}$ stwierdzonej wcześniej wystarczy teraz pokazać, że tak zadane odwzorowanie jest w istocie alternującą formą N -liniową określoną na kolumnach macierzy M .

Zacniemy od sprawdzenia N -liniowości wyznacznika. W tym celu ustalmy (dowolnie) wskaźnik $k \in \overline{1, N}$ i rozważmy zależność składnika $(-1)^{i+j} M_{\#j}^i \cdot_R \det_{(N-1)}(M_{\#j}^{\#i})$ sumy występującej po prawej stronie znaku równości w Równ. (8.30) od $M_{\bullet_k}^{\bullet}$. Ilekroć $j \neq k$, wyraz $M_{\#j}^i$ nie należy do $M_{\bullet_k}^{\bullet}$, gdy tymczasem $M_{\#j}^{\#i}$ zawiera kolumnę $M_{\bullet_k}^{\#i}$ i zależy od niej (a zatem także od $M_{\bullet_k}^{\bullet}$) R -liniowo. W przeciwnym razie, tj. przy $j = k$, to wyraz $M_{\#j}^i \equiv M_{\bullet_k}^i$ zależy R -liniowo od $M_{\bullet_k}^{\bullet}$, natomiast

$M_{\#j}^{\#i} \equiv M_{\#k}^{\#i}$ jest od tej kolumny niezależny, albowiem zawiera wszystkie (skrótowe) kolumny M poza tą jedną właśnie. W obu przypadkach mamy do czynienia z R -liniową zależnością od $M_k^\bullet$, a ponieważ wyrażenie definiujące $\det_{(N)}(M)$ zależy od poszczególnych składników $(-1)^{i+j} M_j^i \cdot_R \det_{(N-1)}(M_{\#j}^{\#i})$ liniowo, przeto zależność jego od $M_k^\bullet$ jest (R) -liniowa.

Niech teraz $M_i^\bullet = M_j^\bullet$ dla pewnej pary wskaźników $i \neq j$. Jeśli $l \notin \{i, j\}$, to $M_{\#l}^{\#k}$ zawiera identyczne kolumny $M_{\#i}^{\#k\bullet}$ i $M_{\#j}^{\#k\bullet}$, a zatem $\det_{(N-1)}(M_{\#l}^{\#k}) = 0_R$ na mocy założenia indukcyjnego. Odnośne rozwinięcie Laplace'a według k -tego wiersza redukuje się więc do postaci sumy dwuskładnikowej

$$\begin{aligned} \det_{(N)}(M) &= (-1)^{k+i} M_i^k \cdot_R \det_{(N-1)}(M_{\#i}^{\#k}) + (-1)^{k+j} M_j^k \cdot_R \det_{(N-1)}(M_{\#j}^{\#k}) \\ &\equiv (-1)^{k+i} M_i^k \cdot_R [\det_{(N-1)}(M_{\#i}^{\#k}) + (-1)^{j-i} \det_{(N-1)}(M_{\#j}^{\#k})]. \end{aligned}$$

Jedyną różnicą między macierzami $M_{\#i}^{\#k}$ i $M_{\#j}^{\#k}$ jest pozycja kolumny $M_{\#j}^{\#k\bullet} = M_{\#i}^{\#k\bullet}$ – oto w $M_{\#i}^{\#k}$ pojawia się ona jako kolumna o indeksie $j-1$, w $M_{\#j}^{\#k}$ zaś jest kolumną o indeksie $i-1$. Biorąc pod uwagę założenie o tym, że $\det_{(N-1)}$ jest formą alternującą, a zatem skośnie symetryczną, stwierdzamy równość

$$\det_{(N-1)}(M_{\#j}^{\#k}) = (-1)^{j-i+1} \det_{(N-1)}(M_{\#i}^{\#k}),$$

która prowadzi do wniosku, że także $\det_{(N)}$ jest formą alternującą.

I wreszcie na koniec zauważamy, że jedyny niezerowy przyczynik do rozwinięcia Laplace według i -tego wiersza, które definiuje $\det_{(N)}(\mathbf{1}_N)$, pochodzi od indeksu $j = i$, gdyż $(\mathbf{1}_N)_j^i = \delta_{i,j}^R$. Wobec tego wprost z założenia $\det_{(N-1)}(\mathbf{1}_{N-1}) = 1_R$ wyprowadzamy pożądaną równość

$$\det_{(N)}(\mathbf{1}_N) = (-1)^{i+i} \delta_{i,i}^R \cdot_R \det_{(N-1)}((\mathbf{1}_N)_{\#i}^{\#i}) \equiv (-1)^{2i} \delta_{i,i}^R \cdot_R \det_{(N-1)}(\mathbf{1}_{N-1}) = 1_R.$$

□

Wygodnie będzie wprowadzić na tym etapie operację zamiany miejscami wyrazów macierzy $M \in \text{Mat}(R; N_1 \times N_2)$ sprowadzającą się do lustrzanego odbicia wyrazów macierzy w prostej wyznaczonej przez wyrazy macierzy o wskaźnikach M_i^i , $i \in \overline{1, \min(N_1, N_2)}$. Operacji tej nadamy głębszy sens algebraiczny w dalszej części wykładu, teraz natomiast spełni ona swoją funkcję pomocniczą.

DEFINICJA 90. Przyjmijmy notację Def. 67, 21 i 82 oraz Przykł. 41 i niech $M \in \text{Mat}(R; N_1 \times N_2)$. **Macierz transponowana do M** to macierz $M^T \in \text{Mat}(R; N_2 \times N_1)$ o wyrazach

$$(M^T)_j^i := M_i^j, \quad (i, j) \in \overline{1, N_2} \times \overline{1, N_1}.$$

▲

Mamy oczywiste

STWIERDZENIE 111. Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 82, 87 i 89, Przykł. 34 (2) i 41. Odwzorowanie

$$\text{Mat}(R; N) \ni M \mapsto M^T,$$

zwane **transpozycją macierzy**, jest inwolutywnym antymultiplikatywnym automorfizmem R -modułu $\text{Mat}(R; N)$, tj. spełnia tożsamości

$$(M_1 \boxplus M_2)^T = M_1^T \boxplus M_2^T, \quad (M_1 \odot M_2)^T = M_2^T \odot M_1^T,$$

$$(r \triangleright_{(N)} M)^T = r \triangleright_{(N)} M^T$$

oraz

$$(M^T)^T = M,$$

wypisane dla dowolnych $M, M_1, M_2 \in \text{Mat}(R; N)$ i $r \in R$, a także

$$\mathbf{1}_N^T = \mathbf{1}_N.$$

■

Możemy już teraz wysławić

STWIERDZENIE 112. Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 82, 87, 89 i 90 oraz Przykł. 34 (2) i 41. Dla dowolnej macierzy $M \in \text{Mat}(R; N)$ zachodzi tożsamość

$$\det_{(N)}(M^T) = \det_{(N)}(M).$$

W szczególności więc wyznacznik jest alternującą formą N -liniową określoną na wierszach macierzy i słuszne jest **rozwiniecie Laplace'a wyznacznika macierzy M według i -tej kolumny**

$$\det_{(N)}(M) = \sum_{j=1}^N (-1)^{i+j} M_{i \cdot}^j \cdot_R \det_{(N-1)}(M_{\neq i}^{\neq j}).$$

■

Dowód: Odwołując się do dowodu Stw. 110 i definicji macierzy transponowanej, możemy zapisać

$$\begin{aligned} \det_{(N)}(M^T) &= \sum_{\sigma \in \mathfrak{S}_N} \text{sgn}(\sigma) M_1^{\sigma(1)} \cdot_R M_2^{\sigma(2)} \cdot_R \cdots \cdot_R M_N^{\sigma(N)} \\ &\equiv \sum_{\sigma \in \mathfrak{S}_N} \text{sgn}(\sigma) M_{\sigma^{-1}(1)}^{\sigma(1)} \cdot_R M_{\sigma^{-1}(2)}^{\sigma(2)} \cdot_R \cdots \cdot_R M_{\sigma^{-1}(N)}^{\sigma(N)}. \end{aligned}$$

Ponieważ jednak σ jest bijekcją, przeto $\{\sigma(1), \sigma(2), \dots, \sigma(N)\} = \{1, 2, \dots, N\}$, a stąd (wobec przemienności R)

$$\begin{aligned} \det_{(N)}(M^T) &= \sum_{\sigma \in \mathfrak{S}_N} \text{sgn}(\sigma) M_{\sigma^{-1}(1)}^1 \cdot_R M_{\sigma^{-1}(2)}^2 \cdot_R \cdots \cdot_R M_{\sigma^{-1}(N)}^N \\ &= \sum_{\sigma \in \mathfrak{S}_N} \text{sgn}(\sigma^{-1}) M_{\sigma^{-1}(1)}^1 \cdot_R M_{\sigma^{-1}(2)}^2 \cdot_R \cdots \cdot_R M_{\sigma^{-1}(N)}^N \\ &= \sum_{\sigma^{-1} \in \mathfrak{S}_N} \text{sgn}(\sigma^{-1}) M_{\sigma^{-1}(1)}^1 \cdot_R M_{\sigma^{-1}(2)}^2 \cdot_R \cdots \cdot_R M_{\sigma^{-1}(N)}^N \\ &\equiv \det_{(N)}(M). \end{aligned}$$

□

Szczególną pozycję wyznacznika w teorii alternujących form wieloliniowych ujawnia

STWIERDZENIE 113. Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 82, 87 i 89 oraz Przykł. 34 (2) i 41. Niechaj G będzie modułem nad pierścieniem

przemennym R i niech $\{g^{(i)}\}_{i \in \overline{1, N}}$ będzie rodziną elementów G , a ponadto niech $M \in \text{Mat}(R; N)$. Zapišmy

$$\begin{pmatrix} h^{(1)} \\ h^{(2)} \\ \vdots \\ h^{(N)} \end{pmatrix} := M \triangleright \begin{pmatrix} g^{(1)} \\ g^{(2)} \\ \vdots \\ g^{(N)} \end{pmatrix},$$

co oznacza, że

$$h^{(i)} := \sum_{j=1}^N M_{ij} \triangleright_G g^{(j)},$$

i niech $\varphi \in \mathbb{L}_R^{N, \text{alt}}(G; H)$. Wówczas

$$\varphi(h^{(1)}, h^{(2)}, \dots, h^{(N)}) = \det_{(N)}(M) \triangleright_H \varphi(g^{(1)}, g^{(2)}, \dots, g^{(N)}).$$

■

Dowód: Wystarczy dokonać rozwinięcia wyrażenia

$$\varphi \left(\sum_{j_1=1}^N M_{j_1}^1 \triangleright_G g^{(j_1)}, \sum_{j_2=1}^N M_{j_2}^2 \triangleright_G g^{(j_2)}, \dots, \sum_{j_N=1}^N M_{j_N}^N \triangleright_G g^{(j_N)} \right)$$

jak w dowodzie Stw. 110, a następnie przywołać tezę Stw. 112. □

O przydatności powyższego stwierdzenia zaświadcza

STWIERDZENIE 114. (Wzór wyznacznikowy Cauchy'ego) *Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 68, 70, 75, 77, 82, 87 i 89, Przykł. 34 (2), 40 (3) i 41 oraz Stw. 96. Dla dowolnych dwóch macierzy $M_1, M_2 \in \text{Mat}(R; N)$ zachodzi tożsamość*

$$\det_{(N)}(M_1 \odot M_2) = \det_{(N)}(M_1) \cdot_R \det_{(N)}(M_2),$$

tj. wyznacznik jest odwzorowaniem moltiplikatywnym.

■

Dowód: Położywszy $G := R^{\times N}$, $\varphi := \det_{(N)}$ oraz $g^{(i)} := e_i$ (baza standardowa) w treści Stw. 113, dostajemy

$$\begin{pmatrix} h^{(1)} \\ h^{(2)} \\ \vdots \\ h^{(N)} \end{pmatrix} = (M_1 \odot M_2) \triangleright \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_N \end{pmatrix} \equiv M_1 \triangleright \begin{pmatrix} f^{(1)} \\ f^{(2)} \\ \vdots \\ f^{(N)} \end{pmatrix}.$$

gdzie

$$\begin{pmatrix} f^{(1)} \\ f^{(2)} \\ \vdots \\ f^{(N)} \end{pmatrix} := M_2 \triangleright \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_N \end{pmatrix},$$

a stąd

$$\det_{(N)}(h^{(1)}, h^{(2)}, \dots, h^{(N)}) = \det_{(N)}(M_1 \odot M_2) \cdot_R \det_{(N)}(e_1, e_2, \dots, e_N)$$

i zarazem

$$\begin{aligned}\det_{(N)}(h^{(1)}, h^{(2)}, \dots, h^{(N)}) &= \det_{(N)}(M_1) \cdot_R \det_{(N)}(f^{(1)}, f^{(2)}, \dots, f^{(N)}) \\ &= \det_{(N)}(M_1) \cdot_R \det_{(N)}(M_2) \cdot_R \det_{(N)}(e_1, e_2, \dots, e_N).\end{aligned}$$

Biorąc pod uwagę normalizację wyznacznika, otrzymujemy ostatecznie żadaną równość. $\square$

Wprowadzimy teraz kolejne pojęcie pomocnicze, które da nam możliwość wypowiedzenia w zwartej formie relacji między wyznacznikiem macierzy kwadratowej a jej odwrotnością w pierścieniu $\text{Mat}(R; N)$.

DEFINICJA 91. Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 82, 87 i 89, Przykł. 34 (2) i 41 oraz Tw. 8.12 i niech $M \in \text{Mat}(R; N)$ będzie dowolną macierzą kwadratową. **Dopełnienie algebraiczne wyrazu M^i_j macierzy** (kwadratowej) M to skalar postaci

$$\widetilde{M}^i_j := (-1)^{i+j} \det_{(N-1)}(M^{\#j}_{\#i}).$$

Macierz $\widetilde{M} \in \text{Mat}(R; N)$ o wypisanych powyżej wyrazach jest nazywana **macierzą dopełnień algebraicznych macierzy M** . $\blacktriangle$

Możemy już teraz sformułować fundamentalne

TWIERDZENIE 8.13 (O odwracalności macierzy). *Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 82, 87, 89 i 91, Przykł. 34 (2) i 41 oraz Tw. 8.12 i niech $M \in \text{Mat}(R; N)$ będzie dowolną macierzą kwadratową. Prawdziwą jest relacja*

$$M \odot \widetilde{M} = \det_{(N)}(M) \triangleright_{(N)} \mathbf{1}_N = \widetilde{M} \odot M.$$

W szczególności M jest odwracalna w pierścieniu $\text{Mat}(R; N)$ wtedy i tylko wtedy, gdy jej wyznacznik $\det_{(N)}(M)$ jest odwracalny w pierścieniu R . Zachodzi wówczas tożsamość

$$M^{-1} := \text{Inv}_{\text{Mat}(R; N)}(M) = \text{Inv}_R(\det_{(N)}(M)) \triangleright_{(N)} \widetilde{M}.$$

$\blacksquare$

Dowód: Rozważmy wyrażenie

$$(M \odot \widetilde{M})^i_j = \sum_{k=1}^N M^i_k \cdot_R \widetilde{M}^k_j \equiv \sum_{k=1}^N (-1)^{k+j} M^i_k \cdot_R \det_{(N-1)}(M^{\#j}_{\#k}).$$

Jeśli $i = j$, to otrzymujemy

$$(M \odot \widetilde{M})^i_j = \sum_{k=1}^N (-1)^{i+k} M^i_k \cdot_R \det_{(N-1)}(M^{\#i}_{\#k}),$$

czyli rozwinięcie wyznacznika M według i -tego wiersza. Pozostaje zatem upewnić się, że dla dowolnego $j \neq i$ zachodzi równość $(M \odot \widetilde{M})^i_j = 0_R$. Niech $\underline{M}(j \rightarrow i)$ oznacza macierz o wierszach $\underline{M}(j \rightarrow i)^k_{\bullet} = M^k_{\bullet}$ dla każdego $k \neq j$ oraz $\underline{M}(j \rightarrow i)^j_{\bullet} = M^i_{\bullet}$ (tj. taką, która powstaje z M poprzez zastąpienie j -tego wiersza i -tym wierszem tej samej macierzy), której wyznacznik jest tożsamościowo równy zeru (z

racji równości wierszy o indeksach i oraz j). Jak łatwo widać, $\underline{M}(j \rightarrow i)^{\#j}_{\#k} = M^{\#j}_{\#k}$ dla dowolnego $k \in \overline{1, N}$, a zatem

$$\begin{aligned} (M \odot \widetilde{M})^i_{j \neq i} &= \sum_{k=1}^N (-1)^{j+k} M^i_k \cdot_R \det_{(N-1)}(M^{\#j}_{\#k}) \\ &= \sum_{k=1}^N (-1)^{j+k} M^i_k \cdot_R \det_{(N-1)}(\underline{M}(j \rightarrow i)^{\#j}_{\#k}) \\ &= \sum_{k=1}^N (-1)^{j+k} \underline{M}(j \rightarrow i)^j_k \cdot_R \det_{(N-1)}(\underline{M}(j \rightarrow i)^{\#j}_{\#k}) \\ &= \det_{(N)}(\underline{M}(j \rightarrow i)) = 0_R. \end{aligned}$$

Ostatecznie więc wyprowadzamy równość

$$M \odot \widetilde{M} = \det_{(N)}(M) \triangleright_{(N)} \mathbf{1}_N,$$

a ponieważ także (wprost z definicji)

$$\widetilde{M^T} = \widetilde{M}^T,$$

toteż na mocy Stw. 111 oraz 112

$$(\widetilde{M} \odot M)^T = M^T \odot \widetilde{M}^T = M^T \odot \widetilde{M^T} = \det_{(N)}(M^T) \triangleright_{(N)} \mathbf{1}_N = \det_{(N)}(M) \triangleright_{(N)} \mathbf{1}_N.$$

Dokonując transpozycji obu stron uzyskanej równości i uwzględniając inwolutywność tej operacji, otrzymujemy drugą część pożądaną równości.

Prawdziwość części tezy określającej warunek konieczny i wystarczający odwracalności M jest w świetle wcześniejszych uwag oczywista, oto bowiem odwracalność wyznacznika M w R oznacza, że macierz $X := \text{Inv}_R(\det_{(N)}(M)) \triangleright_{(N)} \widetilde{M}$ spełnia tożsamości

$$\begin{aligned} M \odot X &= \text{Inv}_R(\det_{(N)}(M)) \triangleright_{(N)} (M \odot \widetilde{M}) \\ &= \text{Inv}_R(\det_{(N)}(M)) \triangleright_{(N)} (\det_{(N)}(M) \triangleright_{(N)} \mathbf{1}_N) \\ &= (\text{Inv}_R(\det_{(N)}(M)) \cdot_R \det_{(N)}(M)) \triangleright_{(N)} \mathbf{1}_N = \mathbf{1}_R \triangleright_{(N)} \mathbf{1}_N = \mathbf{1}_N \end{aligned}$$

i (wyprowadzaną podobnie)

$$X \odot M = \mathbf{1}_N,$$

a ponadto dla dowolnej $M \in \text{GL}(R; N)$ o odwrotności M^{-1} otrzymujemy – na mocy definicji wyznacznika oraz Stw. 114 –

$$\mathbf{1}_R = \det_{(N)}(\mathbf{1}_N) = \det_{(N)}(M \odot M^{-1}) = \det_{(N)}(M) \cdot_R \det_{(N)}(M^{-1}),$$

skąd wniosek, że $\det_{(N)}(M^{-1})$ jest odwrotnością wyznacznika $\det_{(N)}(M)$. $\square$

Dotychczasowe nasze rozważania prowadziliśmy w bardzo ograniczonym kontekście algebraicznym, a mianowicie dla modułów modelowych postaci $R^{\times N}$. Nic nie stoi jednak na przeszkodzie, iżby uogólnić uzyskane tu konstrukcje i wyprowadzone z nich wnioski na całą klasę R -modułów wolnych wykorzystując w tym celu izomorfizmy $[\varrho^{(\alpha)}] \circ \mathcal{M}$ i $[\varrho^{(\beta, \alpha)}] \circ \mathcal{M}$ z treści Tw. 8.11, indukowane w obecności bazy. Idąc tym tropem, możemy stowarzyszyć z dowolnym endomorfizmem modułu wolnego skalarny niezmiennik wyboru bazy, który wprowadza

DEFINICJA 92. Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 68, 70, 72, 75, 77, 82 i 87 oraz Przykł. 34 (2), 40 (3) i 41. Niechaj G będzie modulem wolnym nad pierścieniem przemiennym R , niech $\mathcal{B}$ będzie dowolną jego bazą i niech $\chi \in \text{End}_R(G)$. **Wyznacznik endomorfizmu** χ to skalar

$$\det \chi := \det_{\text{rk}_R G}([\chi]_{\mathcal{B}}^{\mathcal{B}}).$$

▲

Z połączenia Stw. 101 i 114 wysnuwamy istotne

STWIERDZENIE 115. *Wyznacznik endomorfizmu modułu wolnego nad pierścieniem przemiennym nie zależy od wyboru bazy modułu.*

■

Nie koniec jednak na tym, oto bowiem pozostając w klasie modułów wolnych możemy dokonać dalszej abstrakcji pojęcia wyznacznika, z której wyłania się ciekawa a zarazem całkowicie naturalna interpretacja pojęcia bazy modułu.

STWIERDZENIE 116. *Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 68, 70, 72, 75, 77 i 87 oraz Przykł. 41. Niechaj G, H będą dwoma modułami nad pierścieniem przemiennym R , przy czym o G zakładamy ponadto, że jest wolny i skończenie generowany. Niech $\mathcal{B} = \{g^{(i)}\}_{i \in \overline{1, N}}$, $N \equiv \text{rk}_R(G) \in \mathbb{N}$ będzie dowolną bazą G , a wtedy*

$$\forall_{h \in H} \exists!_{\Delta_h \in \mathbb{L}_R^{N, \text{alt}}(G; H)} : \Delta_h(g^{(1)}, g^{(2)}, \dots, g^{(N)}) = h.$$

■

Dowód: Na mocy Stw. 109 ustalenie obrazu układu generującego względem alternującego odwzorowania wieloliniowego zadaje to odwzorowanie całkowicie jednoznacznie. Jest zatem jasnym, że odwzorowanie, o którym mowa w treści powyższego stwierdzenia, jest jedyne, o ile tylko istnieje. Wykorzystując jednoznaczny rozkład dowolnych N elementów $\gamma^i \in G$, $i \in \overline{1, N}$ w bazie $\mathcal{B}$,

$$\gamma^i := \sum_{j=1}^N r^i_j \triangleright_G g^{(j)}, \quad r^i_j \in R,$$

położmy

$$\Delta_h(\gamma^1, \gamma^2, \dots, \gamma^N) := \det_{(N)} \left((r^i_j)_{i, j \in \overline{1, N}} \right) \triangleright_H h.$$

Łatwo sprawdzamy, że tak określone odwzorowanie $G^{\times N} \rightarrow H$ ma wszystkie potrzebne własności. □

Jako prosty wniosek z powyższego stwierdzenia dostajemy

COROLLARIUM 15. *Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 68, 70, 72, 75, 77 i 87, Przykł. 41 oraz Stw. 107. Niechaj G będzie skończenie generowanym modulem wolnym rzędu $\text{rk}_R(G) := N \in \mathbb{N}$ nad pierścieniem przemiennym R . Moduł $\mathbb{L}_R^{N, \text{alt}}(G)$ jest wolny i ma rząd jednostkowy,*

$$\text{rk}_R \left(\mathbb{L}_R^{N, \text{alt}}(G) \right) = 1.$$

■

Dowód: Wybierzmy (dowolnie) bazę $\mathcal{B} := \{g^{(i)}\}_{i \in \overline{1, N}}$, $N \equiv \text{rk}_R(G) \in \mathbb{N}$ modułu G i stowarzyszymy z nią alternującą formę N -liniową $\Delta_{\mathcal{B}}$ na G określoną jednoznacznie przez warunek

$$\Delta_{\mathcal{B}}(g^{(1)}, g^{(2)}, \dots, g^{(N)}) := 1_R.$$

Wówczas dla dowolnej formy $\varphi \in \mathbb{L}_R^{N, \text{alt}}(G)$ zachodzi tożsamość

$$\varphi = \varphi(g^{(1)}, g^{(2)}, \dots, g^{(N)}) \triangleright \Delta_{\mathcal{B}},$$

którą sprawdzamy w bezpośrednim rachunku. $\square$

Przedstawione tu rozumowanie prowadzi do

DEFINICJA 93. Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 68, 70, 72, 75, 77 i 87, Przykł. 41, Stw. 107 oraz dowodu Cor. 15. Niechaj G będzie modulem wolnym rzędu $\text{rk}_R G := N \in \mathbb{N}$ nad pierścieniem przemiennym R . **Wyznacznik na module** G to dowolna alternująca forma N -liniowa $\Delta_{\mathcal{B}}$ spełniająca warunek

$$\Delta_{\mathcal{B}}(\mathcal{B}) := \Delta_{\mathcal{B}}(g^{(1)}, g^{(2)}, \dots, g^{(N)}) := 1_R$$

dla pewnej bazy $\mathcal{B} := \{g^{(i)}\}_{i \in \overline{1, N}}$ modułu G , przy czym zapis powyższy *implycite* wyróżnia porządek na $\mathcal{B}$ wyznaczony przez ustaloną (dowolnie) numerację jej elementów. $\blacktriangle$

W świetle powyższych rozważań możemy *utożsamiać* dowolną bazę $\mathcal{B}$ (skończenie generowanego) modułu wolnego G nad pierścieniem przemiennym R ze stowarzyszonym z nią wyznacznikiem $\Delta_{\mathcal{B}}$ na G . W tym podejściu transformacje bazy odpowiadają odwracalnym elementom R , oto bowiem rozumując jak w dowodzie Cor. 15, otrzymujemy tożsamość

$$\Delta_{\mathcal{B}_2} = \Delta_{\mathcal{B}_2}(\mathcal{B}_1) \triangleright \Delta_{\mathcal{B}_1}$$

dla każdej pary $\mathcal{B}_\alpha$, $\alpha \in \{1, 2\}$ baz G , a ponadto – jak poucza dowód Stw. 116 w połączeniu z treścią Stw. 100 i Tw. 8.13 –

$$\Delta_{\mathcal{B}_2}(\mathcal{B}_1) = \det_{\text{rk}_R G}([\text{id}_G]_{\mathcal{B}_1}^{\mathcal{B}_2}).$$

Właściwym podsumowaniem tej części naszej dyskusji, określającym prosty związek między wyznacznikiem endomorfizmu modułu wolnego i (dowolnym) wyznacznikiem na tymże module, jest poniższe

STWIERDZENIE 117. (O współmienniczości wyznacznika na module względem endomorfizmu) *Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 68, 70, 72, 75, 77, 87, 92 i 93, Przykł. 41, Stw. 107 oraz dowodu Cor. 15. Niechaj G będzie modulem wolnym rzędu $\text{rk}_R G := N \in \mathbb{N}$ nad pierścieniem przemiennym R , niech $\Delta_{\mathcal{B}} \in \mathbb{L}_R^{N, \text{alt}}(G)$ będzie wyznacznikiem na G stowarzyszonym z (dowolną) bazą $\mathcal{B}$ modułu G i niech $\chi \in \text{End}_R(G)$ będzie jego endomorfizmem. **Cofnięcie wyznacznika $\Delta_{\mathcal{B}}$ wzdłuż endomorfizmu χ , indexwyznacznik!modułu nad pierścieniem!cofnięcie wzdłuż endomorfizmu zdefiniowane wzorem***

$$\chi^* \Delta_{\mathcal{B}} := \Delta_{\mathcal{B}} \circ (\chi \times \chi \times \dots \times \chi) \in \mathbb{L}_R^{N, \text{alt}}(G),$$

spełnia tożsamość

$$(8.31) \quad \chi^* \Delta_{\mathcal{B}} = \det \chi \triangleright \Delta_{\mathcal{B}}.$$

■

Dowód: Zgodnie z tezą Stw. 109 dla zweryfikowania tożsamości (8.31) wystarczy porównać wynik ewaluacji każdej z form na bazie $\mathcal{B} := \{g^{(i)}\}_{i \in \overline{1, N}}$. Niech $[\chi]_{\mathcal{B}}^{\mathcal{B}} := (\chi^i_j)_{i, j \in \overline{1, N}}$ będzie macierzą χ względem bazy $\mathcal{B}$. Rozumując jak w dowodzie Stw. 100 i przywołując treść Stw. 100 i Tw. 8.13, bez trudu wyliczamy

$$\begin{aligned} \chi^* \Delta_{\mathcal{B}}(\mathcal{B}) &\equiv \Delta_{\mathcal{B}}(\chi(g^{(1)}), \chi(g^{(2)}), \dots, \chi(g^{(N)})) \\ &= \Delta_{\mathcal{B}}\left(\sum_{i_1=1}^N \chi^1_{i_1} \triangleright_G g^{(i_1)}, \sum_{i_2=1}^N \chi^2_{i_2} \triangleright_G g^{(i_2)}, \dots, \sum_{i_N=1}^N \chi^N_{i_N} \triangleright_G g^{(i_N)}\right) \\ &= \det_{(N)}([\chi]_{\mathcal{B}}^{\mathcal{B}}) \cdot_R \Delta_{\mathcal{B}}(\mathcal{B}) \equiv \det \chi \cdot \Delta_{\mathcal{B}}(\mathcal{B}). \end{aligned}$$

□

Prostej geometrycznej ilustracji tezy udowodnionego tu stwierdzenia dostarcza kurs analizy matematycznej (wzgl. geometrii różniczkowej), w swej części poświęconej całkowaniu na rozmaitościach różniczkowych. Wyznacznik (lokalnie wolnego) $C^\infty(M, \mathbb{R})$ -modułu cięć gładkich wiązki stycznej rozmaitości M pojawia się tam jako forma objętości na M .

Zgromadzona wiedza pozwala nam sformułować prosty warunek ilościowy jednoznacznej rozwiązywalności niejednorodnego układu równań liniowych o współczynnikach z ciała. Aby to uczynić, wysłowimy najpierw istotne (i bardziej ogólne)

STWIERDZENIE 118. (Wzory Cramera) *Przyjmijmy notację Def. 67, 21, 32, 35, 61, 64, 65, 68, 70, 75, 77, 82, 86 i 89, Stw. 75, 95 i 96 oraz Przykł. 34 (2), 40 (3) i 41. Niechaj R będzie pierścieniem przemiennym i niech $M \in \text{Mat}(R; N)$ będzie macierzą kwadratową o wyrazach z R . Załóżmy, że element $g = (g^i)_{i \in \overline{1, N}} \in \text{Mat}(R; N \times 1)$ jest rozwiązaniem niejednorodnego układu równań liniowych*

$$M \odot x = \nu.$$

Wówczas spełnione są tożsamości

$$\forall_{i \in \overline{1, N}} : g^i \cdot_R \det_{(N)}(M) = \det_{(N)}(M^\bullet_1, M^\bullet_2, \dots, M^\bullet_{i-1}, \nu, M^\bullet_{i+1}, M^\bullet_{i+2}, \dots, M^\bullet_N).$$

■

Dowód: Korzystając z Równ. (8.29) oraz z R -liniowości wyznacznika, przepisujemy

$$\begin{aligned} &\det_{(N)}(M^\bullet_1, M^\bullet_2, \dots, M^\bullet_{i-1}, \nu, M^\bullet_{i+1}, M^\bullet_{i+2}, \dots, M^\bullet_N) \\ &= \sum_{j=1}^N g^j \cdot_R \det_{(N)}(M^\bullet_1, M^\bullet_2, \dots, M^\bullet_{i-1}, M^\bullet_j, M^\bullet_{i+1}, M^\bullet_{i+2}, \dots, M^\bullet_N). \end{aligned}$$

Wobec własności alternowania jedyny nietrywialny przyczynik do sumy pochodzi od składnika o indeksie $j = i$ i odtwarza wzór z treści dowodzonego stwierdzenia. □

Bezpośrednią a istotną dla nas konsekwencją powyższego jest

STWIERDZENIE 119. *Przyjmijmy notację Def. 11, 67, 21, 32, 35, 61, 63, 65, 68, 70, 75, 77, 82 i 87 oraz Przykł. 34 (2), 40 (3) i 41. Niech $\mathbb{K}$ będzie ciałem i niech $M \in \text{Mat}(\mathbb{K}; N)$, $N \in \mathbb{N}$ będzie macierzą kwadratową o wyrazach z $\mathbb{K}$. Kolumny M są liniowo zależne wtedy i tylko wtedy, gdy $\det_{(N)}(M) = 0$.* ■

Dowód:

$\Rightarrow$ Liniowa zależność kolumn oznacza istnienie nietrywialnego układu $(\lambda^1, \lambda^2, \dots, \lambda^N) \in \mathbb{K}^{\times N} \setminus \{(0_{\mathbb{K}}, 0_{\mathbb{K}}, \dots, 0_{\mathbb{K}})\}$ skalarów, dla których spełniona jest tożsamość

$$\sum_{i=1}^N \lambda^i \triangleright_N M^\bullet_i = \mathbf{0}_{N \times 1}.$$

W świetle Stw. 118 implikuje to układ równości

$$\forall_{i \in \overline{1, N}} : \lambda^i \cdot_{\mathbb{K}} \det_{(N)}(M)$$

$$= \det_{(N)}(M^\bullet_1, M^\bullet_2, \dots, M^\bullet_{i-1}, \mathbf{0}_{N \times 1}, M^\bullet_{i+1}, M^\bullet_{i+2}, \dots, M^\bullet_N) = 0_{\mathbb{K}}.$$

Wobec odwracalności (przynajmniej) jednego ze skalarów λ^i wnioskujemy na tej podstawie, że

$$\det_{(N)}(M) = 0_{\mathbb{K}}.$$

$\Leftarrow$ Załóżmy, że kolumny M są liniowo niezależne, a wtedy istnieje macierz $(\Lambda^j_i)_{i,j \in \overline{1, N}} \in \text{Mat}(\mathbb{K}; N)$ zadająca rozkład elementów e_i , $i \in \overline{1, N}$ bazy standardowej przestrzeni $\mathbb{K}^{\times N}$ w bazie $\{M^\bullet_j\}_{j \in \overline{1, N}}$, według wzoru

$$e_i = \sum_{j=1}^N \Lambda^j_i \triangleright_N M^\bullet_j.$$

Na mocy Stw. 113 i 112 dostajemy

$$1_{\mathbb{K}} = \det_{(N)}(\mathbf{1}_N) \equiv \det_{(N)}(e_1, e_2, \dots, e_N) = \det_{(N)}(\Lambda^T) \cdot_{\mathbb{K}} \det_{(N)}(M),$$

skąd wniosek, że

$$\det_{(N)}(M) \neq 0_{\mathbb{K}}.$$

□

Naszą dyskusję (niejednorodnych) układów równań liniowych wieńczy

STWIERDZENIE 120. *Przyjmijmy notację Def. 11, 67, 21, 32, 35, 61, 63, 64, 65, 68, 70, 75, 77, 82, 84, 86 i 87, Przykł. 34 (2), 40 (3) i 41 oraz Stw. 95 i 96. Niech $\mathbb{K}$ będzie ciałem i niech $M \in \text{Mat}(\mathbb{K}; N)$, $N \in \mathbb{N}$ będzie macierzą kwadratową o wyrazach z $\mathbb{K}$. Niejednorodny układ równań liniowych*

$$M \odot x = \nu$$

ma dokładnie jedno rozwiązanie wtedy i tylko wtedy, gdy spełniony jest jeden z równoważnych warunków

- (i) $\text{rk } M = N$;
- (ii) $\text{Ker } M = \{\mathbf{0}_{N \times 1}\}$;
- (iii) $\det_{(N)}(M) \neq 0_K$.

■

Na zakończenie niniejszego rozdziału przedstawimy proste przykładowe rachunki wyznaczników macierzowych, z którymi przyjdzie nam się spotykać nieraz w toku dalszej nauki.

PRZYKŁAD(Y) 44.

- (1) Wyznacznik **macierzy górnotrójkątnej**, tj. macierzy $M \in \text{Mat}(R; N)$ o wszystkich wyrazach pod przekątną równych zeru,

$$\forall_{m > n \in \overline{1, N}} : M_{n,m}^m = 0_R.$$

Zachodzi

$$\det_{(N)}(M) = M_{1,1}^1 \cdot_R M_{2,2}^2 \cdot_R \cdots \cdot_R M_{N,N}^N.$$

Istotnie, rozwinięcie Laplace'a wyznacznika według pierwszej kolumny przyjmuje prostą postać

$$\det_{(N)}(M) = M_{1,1}^1 \cdot_R \det_{(N-1)}(M_{j \neq 1}^{\#1}).$$

Takie samo rozwinięcie dla minora $\det_{(N-1)}(M_{j \neq 1}^{\#1})$ daje wynik

$$\det_{(N-1)}(M_{j \neq 1}^{\#1}) = M_{2,2}^2 \cdot_R \det_{(N-2)}(M_{j \neq 1,2}^{\#1,2}),$$

przy czym $M_{j \neq 1,2}^{\#1,2} \in \text{Mat}(R; N-2)$ jest macierzą otrzymaną z M poprzez usunięcie kolumn i wierszy o indeksach 1, 2. Wykonawszy tę samą procedurę (rozwinięcia Laplace'a według pierwszej kolumny) N razy dla kolejnych macierzy zredukowanych, otrzymujemy pożądaną wartość. Pozostaje on słuszny także w odniesieniu do **macierzy dolnotrójkątnych**, zdefiniowanych w sposób analogiczny.

- (2) Wyznacznik **macierzy blokowo trójkątnej**, tj. macierzy T otrzymanej z opisanej powyżej macierzy górno- wzgl. dolnotrójkątnej poprzez zastąpienie wyrazów macierzami stosownego wymiaru,

$$M_n^m \in \text{Mat}(R; D_m \times D_n), \quad D_m, D_n \in \mathbb{N}.$$

Wyznacznik ten jest iloczynem wyznaczników podmacierzy leżących na przekątnej,

$$\det_{(D_1+D_2+\dots+D_N)}(T) = \prod_{n=1}^N \det_{(D_n)}(M_n^n).$$

Wynik ten wyprowadzimy dla przypadku macierzy blokowo górnotrójkątnej o $N = 2$, pozostawiając dowód ogólny (przez indukcję) Czytelnikowi. Zdefiniujmy odwzorowanie

$$(M_1^1, M_1^2, M_2^2) \mapsto \det_{(D_1+D_2)} \begin{pmatrix} M_1^1 & M_1^2 \\ \mathbf{0}_{D_2 \times D_1} & M_2^2 \end{pmatrix} =: \mathcal{D}(M_1^1, M_1^2, M_2^2).$$

Dla ustalonych macierzy M_2^1 i M_2^2 otrzymujemy tym sposobem alternującą formę D_1 -liniową określoną na kolumnach macierzy M_1^1 , przeto – przywołując argumenty z dowodu Stw. 110 – możemy zapisać

$$\mathcal{D}(M_1^1, M_2^1, M_2^2) = \det_{(D_1)}(M_1^1) \cdot_R \mathcal{D}(\mathbf{1}_{D_1}, M_2^1, M_2^2).$$

Ustalając M_2^1 i rozumując analogicznie, stwierdzamy dalej, że

$$\mathcal{D}(\mathbf{1}_{D_1}, M_2^1, M_2^2) = \det_{(D_2)}(M_2^2) \cdot_R \mathcal{D}(\mathbf{1}_{D_1}, M_2^1, \mathbf{1}_{D_2}).$$

Zauważmy, że $\mathcal{D}(\mathbf{1}_{D_1}, M_2^1, \mathbf{1}_{D_2})$ jest wyznacznikiem macierzy górnotrójkątnej o wszystkich wyrazach na przekątnej równych 1_R , korzystając zatem z poprzedniego wyniku, orzekamy równość

$$\mathcal{D}(\mathbf{1}_{D_1}, M_2^1, \mathbf{1}_{D_2}) = 1_R,$$

która zamyka dowód.

- (3) **Wyznacznik (macierzy) Vandermonda**, tj. wyznacznik macierzy postaci

$$V(x_1, x_2, \dots, x_N) := \begin{pmatrix} 1_R & 1_R & \cdots & 1_R \\ x_1 & x_2 & \cdots & x_N \\ x_1^2 & x_2^2 & \cdots & x_N^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{N-1} & x_2^{N-1} & \cdots & x_N^{N-1} \end{pmatrix} \in \text{Mat}(R; N),$$

jest równy

$$\det_{(N)}(V(x_1, x_2, \dots, x_N)) = \prod_{i=1}^{N-1} \prod_{j=i+1}^N (x_j - x_i),$$

✓

8.9. Moduły sprzężone, formy dwuliniowe oraz pary dwoiste

Pośród form wieloliniowych odnajdujemy odwzorowania szczególnej postaci

$$\begin{aligned} \varphi &: G^{(1)} \times G^{(2)} \times \cdots \times G^{(N)} \longrightarrow R \\ &: (g^{(1)}, g^{(2)}, \dots, g^{(N)}) \longmapsto \sum_{n=1}^N \sum_{i_n=1}^{M_n} \alpha_{i_1, i_2, \dots, i_N} \cdot_R \varphi^{i_1}(g^{(1)}) \cdot_R \varphi^{i_2}(g^{(2)}) \\ &\quad \cdot_R \cdots \cdot_R \varphi^{i_N}(g^{(N)}), \end{aligned}$$

gdzie $\varphi^{i_n} \in \mathbb{L}_R(G^{(n)})$. W szczególności konstruktywna dyskusja wyznaczników macierzowych podpowiada przykład struktury

$$\begin{aligned} \delta &: G^{\times N} \longrightarrow R \\ &: (g_1, g_2, \dots, g_N) \longmapsto \sum_{\sigma \in \mathfrak{S}_N} \text{sgn}(\sigma) \varphi^1(g_{\sigma(1)}) \cdot_R \varphi^2(g_{\sigma(2)}) \cdot_R \cdots \cdot_R \varphi^N(g_{\sigma(N)}) \end{aligned}$$

określonej przy użyciu form (1-)liniowych $\varphi^n \in \mathbb{L}_R(G)$. Ta obserwacja sygnalizuje istotną rolę odgrywaną przez formy (1-)liniowe w ogólniejszej teorii form wieloliniowych, która zostanie precyzyjnie opisana w części wykładu poświęconej dyskusji iloczynowi tensorowego. Tymczasem warto odnotować jedną jeszcze okoliczność wyróżniającą wskazane tu odwzorowania. Oto o ile nie istnieją naturalne powody, dla których można by było spodziewać się na grupach odwzorowań R -liniowych

$\text{Hom}_R(G^{(1)}, G^{(2)})$ w ogólności (tj. dla dowolnych R -modułów $G^{(\alpha)}$, $\alpha \in \{1, 2\}$ i bez narzucania ograniczających warunków na R) struktury modułu nad pierścieniem innym niż $\mathbb{Z}$, czyli po prostu stwierdzonej już struktury grupy przemiennej, o tyle formy (1-)liniowe $\text{Hom}_R(G, R)$ stanowią wyjątek od tak rozumianej reguły.

DEFINICJA 94. Przyjmijmy notację Def. 21, 32, 35, 61, 65 i 70 oraz Przykł. 34 (2) i niech G będzie dowolnym R -modulem lewostronnym. **Forma liniowa** (lub inaczej **funkcjonał liniowy**) na G to dowolny element zbioru $\text{Hom}_R(G, {}_R R)$. Ten ostatni jest nośnikiem naturalnej struktury grupy przemiennej

$$(\text{Hom}_R(G, {}_R R), +, -(\cdot), \bullet \mapsto 0),$$

opisanej w Stw. 70, na której jest określone *prawostronne* działanie pierścienia R

$$\wp^* : \text{Hom}_R(G, {}_R R) \times R \longrightarrow \text{Hom}_R(G, {}_R R) : (\varphi, r) \mapsto \varphi \triangleleft r,$$

$$\forall_{g \in G} : (\varphi \triangleleft r)(g) := \varphi(g) \triangleleft r \equiv \varphi(g) \cdot_R r.$$

Tak zadana struktura R -modułu prawostronnego

$$((\text{Hom}_R(G, {}_R R), +, -(\cdot), \bullet \mapsto 0), \wp^*)$$

nosi miano **modułu sprzężonego do G** ,

indexmoduł nad pierścieniem!sprzężony wzgl. **przestrzeni sprzężonej** w przypadku, gdy $R = \mathbb{K}$ jest ciałem. W tym kontekście stosujemy oznaczenie

$$G^* := \text{Hom}_R(G, {}_R R).$$

▲

Należy zwrócić uwagę, że struktura R -modułu prawostronnego na G^* pokrywa się w przypadku pierścienia przemiennego ze strukturą R -modułu (lewostronnego) na zbiorze $\text{Hom}_R(G, {}_R R)$ zadawaną przez działanie

$$\ell^* : R \times \text{Hom}_R(G, {}_R R) \longrightarrow \text{Hom}_R(G, {}_R R) : (r, \varphi) \mapsto r \triangleright \varphi,$$

$$\forall_{g \in G} : (r \triangleright \varphi)(g) := r \cdot_R \varphi(g).$$

Ta mniej ogólna sytuacja, nierzadko przyjmowana za punkt wyjścia do dyskusji struktury liniowej na module sprzężonym w ramach pierwszorocznego kursu algebry, w oczywisty sposób nie pozwala rozpoznać jako naturalnej struktury R -modułu *prawostronnego* na G^* .

PRZYKŁAD(Y) 45.

- (1) ${}_R R^* \cong {}_R R$, czyli też w szczególności $\mathbb{K}^* \cong \mathbb{K}$ dla ciała $\mathbb{K}$. Istotnie, rozważmy odwzorowanie

$$\varphi. : {}_R R \longrightarrow {}_R R^* : r \mapsto \varphi_r,$$

$$\forall_{s \in R} : \varphi_r(s) := s \cdot_R r.$$

Jest ono jawnie R -liniowe, oto bowiem dla dowolnych $p, q, r, s, t \in R$ otrzymujemy

$$\begin{aligned} \varphi_{(r \triangleleft p) + {}_R (s \triangleleft q)}(t) &= t \cdot_R ((r \cdot_R p) + {}_R (s \cdot_R q)) = ((t \cdot_R r) \cdot_R p) + {}_R ((t \cdot_R s) \cdot_R q) \\ &= (\varphi_r(t) \cdot_R p) + {}_R (\varphi_s(t) \cdot_R q) = (\varphi_r \triangleleft p + \varphi_s \triangleleft q)(t). \end{aligned}$$

Ażeby zanalizować własności φ , przywołajmy Stw. 80, na mocy którego każda forma liniowa jest w pełni określona przez wartości przyjmowane przez nią na bazie dziedziny, czyli (np.) na elemencie 1_R . Niech zatem dla ustalonej formy φ zachodzi $\varphi(1_R) := r$, a wtedy możemy napisać $\varphi = \varphi_r \in \text{Im } \varphi$, czyli φ jest epimorfizmem. Ponadto równość $\varphi_r = \varphi_s$ implikuje – po dokonaniu ewaluacji obu jej stron na 1_R – równość argumentów $r = s$, skąd wniosek, że φ jest także monomorfizmem. Ostatecznie więc odwzorowanie to zadaje pożądany izomorfizm R -modułów.

- (2) To, jak istotny jest wybór pierścienia przy określaniu nośnika struktury sprzężonej dla ustalonego nośnika struktury wyjściowej, pokazuje przykład grupy przemiennej $(\mathbb{Q}, +_{\mathbb{Q}}, P_{\mathbb{Q}}, [(0, 1)])$ traktowanej to jako $\mathbb{Q}$ -moduł, a wówczas $\text{Hom}_{\mathbb{Q}}(\mathbb{Q}, \mathbb{Q}) \cong \mathbb{Q}$ (patrz: wyżej), to znowu jako $\mathbb{Z}$ -moduł, a wtedy $\text{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) = \{0\}$. O słuszności tej ostatniej równości przekonuje następujący prosty argument: niech $\varphi \in \text{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z})$ i założmy, że dla pewnej liczby $q \in \mathbb{Q}$ zachodzi $\varphi(q) = n \in \mathbb{N} \setminus \{0\}$ (co zawsze można osiągnąć, jeśli tylko $\varphi \neq 0$); wobec $\mathbb{Z}$ -liniowości φ a dla dowolnego $N_q > n$ dostajemy wtedy $n = \varphi(N_q \triangleright (q \cdot_{\mathbb{Q}} [(1, N_q)])) = N_q \cdot \varphi(q \cdot_{\mathbb{Q}} [(1, N_q)]) \in N_q \cdot \mathbb{N}$, co oznacza, że $N_q \mid n$, ale $N_q > n$, więc sprzeczność, skąd też pożądany wniosek $\varphi \equiv 0$.
- (3) Przykładów form liniowych na przestrzeniach wektorowych dostarcza następująca lista:
- (i) $0 : V \longrightarrow \mathbb{K} : v \longmapsto 0_{\mathbb{K}}$ dla dowolnych V i $\mathbb{K}$ (**funkcjonał zerowy**);
 - (ii) $v^i : V \longrightarrow \mathbb{K} : \sum_{n=1}^N \lambda^n \triangleright v_n \longmapsto \lambda^i$ dla $V, \mathbb{K}$ jak wyżej (przy $\dim_{\mathbb{K}} V = N < \infty$) oraz dla dowolnej bazy $\{v_n\}_{n \in \overline{1, N}}$ przestrzeni V ;
 - (iii) $\int_{[0, 1]} : C([0, 1], \mathbb{R}) \longrightarrow \mathbb{R} : f \longmapsto \int_0^1 dt f(t)$.

✓

Natychmiastową konsekwencją definicji modułu sprzężonego oraz Stw. 94 jest

STWIERDZENIE 121. *Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 75, 77 i 78. Niechaj $\{G^{(\lambda)}\}_{\lambda \in \Lambda}$ będzie rodziną modułów lewostronnych nad pierścieniem R i niech $j_{\lambda} : G^{(\lambda)} \longrightarrow G$, $\lambda \in \Lambda$ będą włożeniami kanonicznymi. Istnieje kanoniczny izomorfizm R -modułów prawostronnych*

$$\text{Hom}_R(j, R) : \left(\bigoplus_{\lambda \in \Lambda} G^{(\lambda)} \right)^* \longrightarrow \prod_{\lambda \in \Lambda} G^{(\lambda)*} : \varphi \longmapsto \varphi \circ j,$$

który w przypadku skończonego zbioru indeksów, $\Lambda = \overline{1, N}$, przybiera postać

$$\left(\bigoplus_{n=1}^N G^{(n)} \right)^* \cong \bigoplus_{n=1}^N G^{(n)*}.$$

■

Ograniczenie rozważań do kategorii przestrzeni wektorowych umożliwia najbardziej zgrubne porównanie dowolnej przestrzeni z przestrzenią do niej sprzężoną, co czynimy w

STWIERDZENIE 122. *Przyjmijmy notację Def. 11, 32, 35, 61, 63, 65, 72, 73 i 94 oraz Przykł. 45 (1) i niech V będzie dowolną przestrzenią wektorową nad*

ciałem $\mathbb{K}$. Wówczas

$$\dim_{\mathbb{K}} V \leq \dim_{\mathbb{K}} V^*.$$

Na to, iżby przestrzeń V^* miała wymiar skończony, potrzeba i wystarcza, aby $\dim_{\mathbb{K}} V < \infty$, a wtedy $\dim_{\mathbb{K}} V^* = \dim_{\mathbb{K}} V$. ■

Dowód: Na mocy Tw. 8.5 V ma bazę $\mathcal{B} = \{v_\lambda\}_{\lambda \in \Lambda}$, która określa izomorfizm

$$V \cong \bigoplus_{\lambda \in \Lambda} \langle v_\lambda \rangle_{\mathbb{K}} \cong \bigoplus_{\lambda \in \Lambda} \mathbb{K}.$$

Ten pozwala nam zapisać, korzystając ze Stw. 94,

$$V^* \cong \left(\bigoplus_{\lambda \in \Lambda} \mathbb{K} \right)^* \cong \text{Hom}_{\mathbb{K}} \left(\bigoplus_{\lambda \in \Lambda} \mathbb{K}, \mathbb{K} \right) \cong \prod_{\lambda \in \Lambda} \text{Hom}_{\mathbb{K}}(\mathbb{K}, \mathbb{K}) \cong \prod_{\lambda \in \Lambda} \mathbb{K}^* \cong \prod_{\lambda \in \Lambda} \mathbb{K} \supset \bigoplus_{\lambda \in \Lambda} \mathbb{K} \cong V.$$

W świetle Stw. 82 i 83 wnioskujemy na tej podstawie o słuszności nierówności

$$\dim_{\mathbb{K}} V^* \geq \dim_{\mathbb{K}} V = |\Lambda|.$$

Takż warunkiem koniecznym skończoności wymiaru V^* jest $\dim_{\mathbb{K}} V < \infty$, a zarazem jego spełnienie gwarantuje równość $\bigoplus_{\lambda \in \Lambda} \mathbb{K} = \prod_{\lambda \in \Lambda} \mathbb{K}$, która pociąga za sobą istnienie izomorfizmu $V^* \cong V$, przesądzające o równości wymiarów. □

Wyjątkowość struktury opisanej w Def. 94 w kontekście teorii odwzorowań R -liniowych każe nam przyjrzeć się jej nieco dokładniej, co też uczynimy poniżej. Zaczniemy od precyzyjniejszego scharakteryzowania relacji między wzajem sprzężonymi strukturami liniowymi G i G^* . W tym celu wprowadzimy kilka nowych pojęć, które okażą się przydatne także w dalszej części wykładu.

DEFINICJA 95. Przyjmijmy notację Def. 21, 32, 35, 61 i 65. Niechaj $((G^{(1)}, \phi_2^{(1)} \equiv +_{(1)}, \phi_1^{(1)} \equiv P_{(1)}, \phi_0^{(1)} : \bullet \mapsto 0_{(1)}, \ell^{(1)} \equiv \triangleright_{(1)})$ (wzgl. $((G^{(2)}, \phi_2^{(2)} \equiv +_{(2)}, \phi_1^{(2)} \equiv P_{(2)}, \phi_0^{(2)} : \bullet \mapsto 0_{(2)}, \wp^{(2)} \equiv \triangleleft_{(2)})$ będzie modułem lewostronnym (wzgl. prawostronnym) nad pierścieniem $R^{(1)}$ (wzgl. $R^{(2)}$) i niech $((G, \phi_2 \equiv +_G, \phi_1 \equiv P_G, \phi_0 : \bullet \mapsto 0_G, \ell \equiv \triangleright, \wp \equiv \triangleleft)$ będzie $(R^{(1)}, R^{(2)})$ -**bimodułem**, tj. grupą przemianą ze strukturą modułu lewostronnego nad $R^{(1)}$ oraz modułu prawostronnego nad $R^{(2)}$ uzgodnionymi wzajemnie w sensie wyrażonym przez diagram przemienności (wypisany wraz z równoważnym zdaniem logicznym)

$$\begin{array}{ccc} R^{(1)} \times G \times R^{(2)} & \xrightarrow{\text{id}_{R^{(1)}} \times \wp} & R^{(1)} \times G \\ \ell \times \text{id}_{R^{(2)}} \downarrow & & \downarrow \ell \\ G \times R^{(2)} & \xrightarrow{\wp} & G \end{array} \quad \equiv \quad \forall_{(r,g,s) \in R^{(1)} \times G \times R^{(2)}} : \begin{array}{l} (r \triangleright g) \triangleleft s \\ = r \triangleright (g \triangleleft s) \end{array}.$$

Odwzorowanie $\beta : G^{(1)} \times G^{(2)} \longrightarrow G$ nazywamy **dwuliniowym** (lub też **biliniowym**), ilekroć spełnia warunki wyrażone przez następujące diagramy przemienności (wypisane wraz z równoważnymi zdaniami logicznymi)

(BL1) ($\mathbb{Z}$ -liniowość w pierwszym argumentcie)

$$\begin{array}{ccc}
G^{(1) \times 2} \times G^{(2)} & \xrightarrow{\phi_2^{(1)} \times \text{id}_{G^{(2)}}} & G^{(1)} \times G^{(2)} \\
(\beta \circ \text{pr}_{1,3}, \beta \circ \text{pr}_{2,3}) \downarrow & & \downarrow \beta \\
G^{\times 2} & \xrightarrow{\phi_2} & G
\end{array}
\quad \begin{array}{l} \forall_{(g,h,k) \in G^{(1) \times 2} \times G^{(2)}} \\ \equiv \\ : \beta(g +_{(1)} h, k) = \beta(g, k) +_G \beta(h, k) \end{array} ;$$

(BL2) ($\mathbb{Z}$ -liniowość w drugim argumentcie)

$$\begin{array}{ccc}
G^{(1)} \times G^{(2)} \times 2 & \xrightarrow{\text{id}_{G^{(1)}} \times \phi_2^{(2)}} & G^{(1)} \times G^{(2)} \\
(\beta \circ \text{pr}_{1,2}, \beta \circ \text{pr}_{1,3}) \downarrow & & \downarrow \beta \\
G^{\times 2} & \xrightarrow{\phi_2} & G
\end{array}
\quad \begin{array}{l} \forall_{(g,h,k) \in G^{(1)} \times G^{(2)} \times 2} \\ \equiv \\ : \beta(g, h +_{(2)} k) = \beta(g, h) +_G \beta(g, k) \end{array} ;$$

(BL3) (jednorodność w pierwszym argumentcie)

$$\begin{array}{ccc}
R^{(1)} \times G^{(1)} \times G^{(2)} & \xrightarrow{\ell^{(1)} \times \text{id}_{G^{(2)}}} & G^{(1)} \times G^{(2)} \\
\text{id}_{R^{(1)}} \times \beta \downarrow & & \downarrow \beta \\
R^{(1)} \times G & \xrightarrow{\ell} & G
\end{array}
\quad \begin{array}{l} \forall_{(r,g,h) \in R^{(1)} \times G^{(1)} \times G^{(2)}} \\ \equiv \\ : \beta(r \triangleright_{(1)} g, h) = r \triangleright_G \beta(g, h) \end{array} ;$$

(BL4) (jednorodność w drugim argumentcie)

$$\begin{array}{ccc}
G^{(1)} \times G^{(2)} \times R^{(2)} & \xrightarrow{\text{id}_{G^{(1)}} \times \wp^{(2)}} & G^{(1)} \times G^{(2)} \\
\beta \times \text{id}_{R^{(2)}} \downarrow & & \downarrow \beta \\
G \times R^{(2)} & \xrightarrow{\wp} & G
\end{array}
\quad \begin{array}{l} \forall_{(g,h,r) \in G^{(1)} \times G^{(2)} \times R^{(2)}} \\ \equiv \\ : \beta(g, h_{(2)} \triangleleft r) = \beta(g, h)_G \triangleleft r \end{array} .$$

Zbiór wszystkich odwzorowań 2-liniowych opisanego typu będziemy oznaczać symbolem

$$\mathbf{L}_{(R^{(1)}, R^{(2)})}(G^{(1)}, G^{(2)}; G).$$

▲

Ważnej charakterystyki odwzorowań dwuliniowych dostarcza

DEFINICJA 96. Przyjmijmy notację Def. 21, 32, 35, 61, 65 i 95. **Odwzorowanie $R^{(2)}$ -liniowe prawostronnie stowarzyszone z β** to odwzorowanie

$$r_\beta : G^{(2)} \longrightarrow \text{Hom}_{R^{(1)}}(G^{(1)}, G) : g \longmapsto \beta(\cdot, g),$$

natomiast **odwzorowanie $R^{(1)}$ -liniowe lewostronnie stowarzyszone z β** to odwzorowanie

$$l_\beta : G^{(1)} \longrightarrow \text{Hom}_{R^{(2)}}(G^{(2)}, G) : g \longmapsto \beta(g, \cdot).$$

Odwzorowanie β określamy mianem **prawostronnie** (wzgl. **lewostronnie**) **zwyrodniałego** (lub **zdegenerowanego**), jeśli odwzorowanie r_β (wzgl. l_β) jest nie-iniektywne, tj. $\text{Ker } r_\beta \neq \{0_{(2)}\}$ (wzgl. $\text{Ker } l_\beta \neq \{0_{(1)}\}$). Ilekroć β jest prawo- lub

lewostronnie zwyrodniałe, mówimy, że jest ono **zwyrodniałe**. W przeciwnym razie mamy do czynienia z **odwzorowaniem niezwyrodniałym**. Prawostronnie (wzgl. lewostronnie) niezwyrodniałe odwzorowanie β nazwiemy **prawostronnie** (wzgl. **lewostronnie**) **nieosobliwym**, jeśli odwzorowanie r_β (wzgl. l_β) jest także surjekcją. Odwzorowanie dwuliniowe **nieosobliwe** to takie, które jest zarazem prawo- i lewostronnie nieosobliwe.

Jeśli $R^{(1)} = R^{(2)} =: R$ i $G = R$ (z oczywistą strukturą bimodułu nad R), odwzorowanie dwuliniowe $\Phi : G^{(1)} \times G^{(2)} \rightarrow R$ nazywamy **formą dwuliniową na** $G^{(1)} \times G^{(2)}$, w zgodzie z Def. 87. Nieosobliwa forma dwuliniowa $\Delta : G^{(1)} \times G^{(2)} \rightarrow R$ nosi miano (**doskonałej**¹⁷) **dwoistości** (lub inaczej **dualności**), a odnośną trójkę $(G^{(1)}, G^{(2)}, \Delta)$ nazywamy (**doskonałą**) **parą dwoistą** (lub **dualną**). Stosujemy też wtedy wygodne oznaczenie

$$\Delta \equiv \langle \cdot, \cdot \rangle_\Delta .$$

▲

Warto podkreślić, że nazwy odwzorowań r_β i l_β mają sens, albowiem grupę przemenną $\text{Hom}_{R^{(1)}}(G^{(1)}, G)$ można traktować jako $R^{(2)}$ -moduł prawostronny z działaniem

$$\wp_{(1)}^* : \text{Hom}_{R^{(1)}}(G^{(1)}, G) \times R^{(2)} \rightarrow \text{Hom}_{R^{(1)}}(G^{(1)}, G) : (\chi, r) \mapsto \chi(\cdot)_G \triangleleft r$$

i – analogicznie – grupę przemenną $\text{Hom}_{R^{(2)}}(G^{(2)}, G)$ można traktować jako $R^{(1)}$ -moduł lewostronny z działaniem

$$\ell_{(2)}^* : R^{(1)} \times \text{Hom}_{R^{(2)}}(G^{(2)}, G) \rightarrow \text{Hom}_{R^{(2)}}(G^{(2)}, G) : (r, \chi) \mapsto r \triangleright_G \chi(\cdot) .$$

Wypiszmy też dla należytego podkreślenia znaczenia warunku nieosobliwości formy dwuliniowej

COROLLARIUM 16. *Przyjmijmy notację Def. 21, 32, 35, 61, 65 i 95. Dowlona dwoistość*

$$\Delta : G^{(1)} \times G^{(2)} \rightarrow R$$

zadaje parę izomorfizmów

$$r_\Delta : G^{(2)} \xrightarrow{\cong} G^{(1)*} , \quad l_\Delta : G^{(1)} \xrightarrow{\cong} G^{(2)*} .$$

■

PRZYKŁAD(Y) 46.

- (1) **Odwzorowanie (dwuliniowe) zerowe** $0 : G^{(1)} \times G^{(2)} \rightarrow G : (g, h) \mapsto 0_G$.
- (2) Kluczowym z punktu widzenia wykładu przykładem formy dwuliniowej jest **forma ewaluacji**

$$\langle \cdot, \cdot \rangle : G \times G^* \rightarrow R : (g, \varphi) \mapsto \varphi(g) \equiv \langle g, \varphi \rangle ,$$

wypisana w oznaczeniach Def. 94. Jak pokażemy w dalszej części wykładu, w kategorii przestrzeni wektorowych nad ciałem stanowi ona w pewnym

¹⁷Często rozważa się mniej restryktywną definicję dwoistości, nie narzucającą warunku nieosobliwości, a nawet – warunku niezwyrodnienia. Dobór terminologii wykładowej podyktowała w tym wypadku XVII-wieczna zasada „Non sunt multiplicanda entia sine necessitate”, zwana potocznie (i niesłusznie, gdyż pochodzi od irlandzkiego scholastyka Johna Ponce’a) „brzytwą Ockhama”.

(dobrze określonym) sensie kanoniczny przykład nieosobliwej formy dwuliniowej.

- (3) $G^{(1)} \times G^{(2)} \longrightarrow R : (g, h) \longmapsto \chi^{(1)}(g) \cdot_R \chi^{(2)}(h)$ dla pewnych $\chi^{(1)} \in \text{Hom}_R(G^{(1)}, {}_R R)$ i $\chi^{(2)} \in \text{Hom}_R(G^{(2)}, R_R)$.
- (4) Niechaj $\mathbb{R}_d^{(h)}[t_1, t_2, \dots, t_n]$ oznacza przestrzeń wektorową (nad $\mathbb{R}$) *jednorodnych* wielomianów stopnia d o współczynnikach rzeczywistych w $n \in \mathbb{N} \setminus \{0\}$ zmiennych t_i , $i \in \overline{1, n}$. Typowy element tej przestrzeni ma postać

$$w = \sum_{\substack{i_1, i_2, \dots, i_n=1 \\ i_1+i_2+\dots+i_n=d}}^d a_{i_1 i_2 \dots i_n} t_1^{i_1} t_2^{i_2} \dots t_n^{i_n}, \quad a_{i_1 i_2 \dots i_n} \in \mathbb{R}.$$

Oznaczmy przez D_i operator pochodnej cząstkowej względem zmiennej t_i , którego działanie na wielomianach w zmiennych $t_1, t_2, \dots, t_n$ określa jednoznacznie reguła Leibniza w połączeniu z formułami

$$\forall_{i,j \in \overline{1,n}} : D_i t_j = \delta_{i,j}^{\mathbb{R}}.$$

Dla wielomianu w o powyższym rozkładzie w bazie jednomianowej $\mathbb{R}_d^{(h)}[t_1, t_2, \dots, t_n]$ wprowadźmy oznaczenie

$$w(D) := \sum_{\substack{i_1, i_2, \dots, i_n=1 \\ i_1+i_2+\dots+i_n=d}}^d a_{i_1 i_2 \dots i_n} D_1^{i_1} \circ D_2^{i_2} \circ \dots \circ D_n^{i_n}.$$

Wówczas formuła

$$\langle \cdot, \cdot \rangle_d : \mathbb{R}_d^{(h)}[t_1, t_2, \dots, t_n] \times \mathbb{R}_d^{(h)}[t_1, t_2, \dots, t_n] \longrightarrow \mathbb{R} : (w_1, w_2) \longmapsto F_{w_1(D)w_2}(0),$$

zapisana w notacji Def. 25, zadaje niezwyrodniałą (i symetryczną) formę dwuliniową na $\mathbb{R}_d^{(h)}[t_1, t_2, \dots, t_n]$.

- (5) $C([0, 1]; \mathbb{R})^{\times 2} \longrightarrow \mathbb{R} : (f, g) \longmapsto \int_0^1 dt f(t) g(t) =: \langle f, g \rangle.$

✓

W nawiązaniu do omawianych wcześniej macierzowych realizacji odwzorowań liniowych wprowadzamy

DEFINICJA 97. Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 68, 70, 82 i 95, Stw. 75 oraz Przykł. 34 (2) i 41. Ilekroć $G^{(\alpha)}$, $\alpha \in \{1, 2\}$ są modułami wolnymi o odnośnych bazach $\mathcal{B}^{(\alpha)} := \{g^{(\alpha|\lambda_\alpha)}\}_{\lambda_\alpha \in \Lambda_\alpha}$, określamy **macierz odwzorowania dwuliniowego względem baz** $\mathcal{B}^{(1)}$ i $\mathcal{B}^{(2)}$ wzorem

$$\mathcal{B}^{(1)}[\beta]_{\mathcal{B}^{(2)}} := (\beta^{\lambda_1, \lambda_2})_{(\lambda_1, \lambda_2) \in \Lambda_1 \times \Lambda_2} \in \text{Mat}(G; \Lambda_1 \times \Lambda_2),$$

$$\beta^{\lambda_1, \lambda_2} := \beta(g^{(1|\lambda_1)}, g^{(2|\lambda_2)}).$$

▲

Zachodzi przy tym oczywiste

STWIERDZENIE 123. Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 68, 70, 82 i 95, Stw. 75 oraz Przykł. 34 (2) i 41. Odwzorowanie dwuliniowe $\beta : G^{(1)} \times G^{(2)} \longrightarrow G$ jest jednoznacznie określone przez swą macierz względem dowolnych baz $\mathcal{B}^{(\alpha)} = \{g^{(\alpha|\lambda_\alpha)}\}_{\lambda_\alpha \in \Lambda_\alpha}$ modułów $G^{(\alpha)}$, $\alpha \in \{1, 2\}$. I odwrotnie, dowolna

macierz $(\beta^{\lambda_1, \lambda_2})_{(\lambda_1, \lambda_2) \in \Lambda_1 \times \Lambda_2} \in \text{Mat}(G; \Lambda_1 \times \Lambda_2)$ zadaje odwzorowanie dwuliniowe, jak następuje:

$$\beta \left(\sum_{\lambda_1 \in \Lambda_1} r_{\lambda_1} \triangleright_{(1)} g^{(1|\lambda_1)}, \sum_{\lambda_2 \in \Lambda_2} g^{(2|\lambda_2)}_{(2)} \triangleleft s_{\lambda_2} \right) := \sum_{(\lambda_1, \lambda_2) \in \Lambda_1 \times \Lambda_2} r_{\lambda_1} \triangleright_G \beta^{\lambda_1, \lambda_2}_G \triangleleft s_{\lambda_2}.$$

Powyższe przyporządkowania określają izomorfizm grup przemennych

$$L^2_{(R^{(1)}, R^{(2)})}(G^{(1)}, G^{(2)}; G) \cong \text{Mat}(G; \Lambda_1 \times \Lambda_2),$$

który w przypadku $R^{(1)}$ i $R^{(2)}$ przemennych jest izomorfizmem $(R^{(1)}, R^{(2)})$ -bi-modułów.

■

O formach dwuliniowych można myśleć na wiele różnych a wzajem równoważnych sposobów. Niektóre z nich opisuje

STWIERDZENIE 124. *Przyjmijmy notację Def. 21, 32, 35, 61, 65, 95 i 96. Istnieją izomorfizmy grup przemennych*

$$L^2_R(G^{(1)}, G^{(2)}) \cong \text{Hom}_R(G^{(1)}, \text{Hom}_R(G^{(2)}, R_R)),$$

$$L^2_R(G^{(1)}, G^{(2)}) \cong \text{Hom}_R(G^{(2)}, \text{Hom}_R(G^{(1)}, {}_R R)),$$

które w przypadku R przemienne są izomorfizmami odnośnych R -modułów. Ponadto każda nieosobliwa forma dwuliniowa zadaje izomorfizmy grup przemennych

$$L^2_R(G^{(1)}, G^{(2)}) \cong \text{End}_R(G^{(1)}), \quad L^2_R(G^{(1)}, G^{(2)}) \cong \text{End}_R(G^{(2)}),$$

które w przypadku R przemienne są izomorfizmami odnośnych R -modułów.

■

Dowód: W pierwszym przypadku pożądane izomorfizmy przyjmują postać

$$l : L^2(G^{(1)}, G^{(2)}) \longrightarrow \text{Hom}_R(G^{(1)}, \text{Hom}_R(G^{(2)}, R_R)) : \Phi \longmapsto l_\Phi,$$

$$r : L^2(G^{(1)}, G^{(2)}) \longrightarrow \text{Hom}_R(G^{(2)}, \text{Hom}_R(G^{(1)}, {}_R R)) : \Phi \longmapsto r_\Phi.$$

Homomorfizmy odwrotne do nich przyporządkowują odwzorowaniom R -liniowym $\chi : G^{(1)} \longrightarrow \text{Hom}_R(G^{(2)}, R_R)$ i $\psi : G^{(2)} \longrightarrow \text{Hom}_R(G^{(1)}, {}_R R)$ formy dwuliniowe

$$l^{-1}(\chi) : G^{(1)} \times G^{(2)} \longrightarrow R : (g, h) \longmapsto \chi(g)(h),$$

$$r^{-1}(\psi) : G^{(1)} \times G^{(2)} \longrightarrow R : (g, h) \longmapsto \psi(h)(g).$$

W celu skonstruowania izomorfizmu $L^2_R(G^{(1)}, G^{(2)}) \cong \text{End}_R(G^{(1)})$ ustalmy nieosobliwą formę dwuliniową $\Delta \equiv \langle \cdot, \cdot \rangle_\Delta$. Dowolnemu endomorfizmowi $\chi \in \text{End}_R(G^{(1)})$ możemy teraz przypisać jawnie dwuliniowe odwzorowanie

$$\Phi_\chi : G^{(1)} \times G^{(2)} \longrightarrow R : (g, h) \longmapsto \langle \chi(g), h \rangle_\Delta,$$

które przyjmujemy za obraz χ względem rzeczzonego izomorfizmu. Odwrotność tego ostatniego konstruujemy, jak następuje. Dla dowolnej formy dwuliniowej $\Phi \in L^2_R(G^{(1)}, G^{(2)})$ i dowolnego $g \in G^{(1)}$ stwierdzamy

$$l_\Phi(g) \in G^{(2)*},$$

co wobec Cor. 16 pozwala określić element

$$l_{\Delta}^{-1} \circ l_{\Phi}(g) \in G^{(1)}$$

zależący od g w sposób jawnie (lewostronnie) R -liniowy. Tym samym z wyjściową formą dwuliniową stowarzyszymy endomorfizm

$$\chi_{\Phi} := l_{\Delta}^{-1} \circ l_{\Phi} \in \text{End}_R(G^{(1)}).$$

Dowód istnienia izomorfizmu $\mathbb{L}_R^2(G^{(1)}, G^{(2)}) \cong \text{End}_R(G^{(2)})$ przebiega analogicznie. $\square$

Powyższe stwierdzenie w znaczący sposób porządkuje dyskusję form dwuliniowych w obecności struktury pary dwoistej, sprowadzając analizę dowolnej takiej formy do analizy odnośnego endomorfizmu jednego (dowolnego) z modułów pary. Do dyskusji tej wrócimy przy okazji omawiania form kwadratowych.

Rola form dwuliniowych w fizyce i matematyce (w których pojawiają się między innymi pod postacią struktur metrycznych na geometriach riemannowskich, operatorów drugiej pochodnej przydatnych w opisie punktów krytycznych będących przedmiotem badań rachunku wariacyjnego, struktur symplektycznych na przestrzeniach stanów i wielu innych) usprawiedliwia naszą dalszą dyskusję tych obiektów, ze szczególnym naciskiem na warunki niezwyrodnienia i nieosobliwości. Celem uzyskania strukturalnie bogatszego opisu formy dwuliniowej, jak również dla lepszego zrozumienia pojęcia dwoistości wpisanego w jej definicję w kategorii przestrzeni wektorowych, wprowadzimy dodatkowe pojęcia.

DEFINICJA 98. Przyjmijmy notację Def. 21, 32, 35, 61, 64, 65 i 95 oraz Przykł. 34 (2). O elementach $g^{(\alpha)} \in G^{(\alpha)}$ modułów, na których określone jest odwzorowanie dwuliniowe $\beta : G^{(1)} \times G^{(2)} \rightarrow G$ mówimy, że **anihilują się (wzajemnie) względem** β , gdy zachodzi równość

$$\beta(g^{(1)}, g^{(2)}) = 0_G.$$

To samo powiemy o podzbiorach $H^{(\alpha)} \subset G^{(\alpha)}$, jeśli jest spełniony warunek

$$\forall_{(g^{(1)}, g^{(2)}) \in H^{(1)} \times H^{(2)}} : \beta(g^{(1)}, g^{(2)}) = 0_G.$$

Niechaj będzie dany podmoduł $H^{(1)} \subset G^{(1)}$ (wzgl. $H^{(2)} \subset G^{(2)}$). **Anihilator** $H^{(1)}$ (wzgl. $H^{(2)}$) w $G^{(2)}$ (wzgl. w $G^{(1)}$) to podmoduł $H^{(1)0} \subset G^{(2)}$ (wzgl. $H^{(2)0} \subset G^{(1)}$) złożony ze wszystkich elementów $G^{(2)}$ (wzgl. $G^{(1)}$) anihilujących dowolny element $H^{(1)}$ (wzgl. $H^{(2)}$). ▲

PRZYKŁAD(Y) 47.

- (1)
- (2)

✓

Z łatwością sprawdzamy

STWIERDZENIE 125. *Przyjmijmy notację Def. 67, 21, 32, 34, 35, 61, 64, 65, 95 i 98. Niechaj $H_1 \subset H_2$ będą podmodułami dowolnego z pary modułów $G^{(\alpha)}$, $\alpha \in \{1, 2\}$, na których określone jest odwzorowanie dwuliniowe $\beta : G^{(1)} \times G^{(2)} \rightarrow G$. Wówczas zachodzą tożsamości*

$$(i) \quad H_2 \subset (H_2^0)^0 =: H_2^{00}, \quad (ii) \quad H_2^0 \subset H_1^0,$$

$$(iii) \quad H_2^0 = (H_2^0)^{00} = (H_2^{00})^0 =: H_2^{000}.$$

Ponadto dla dowolnej rodziny $\{H_\lambda\}_{\lambda \in \Lambda}$ podmodułów $G^{(\alpha)}$ prawdziwe są równości

$$\left(\bigcup_{\lambda \in \Lambda} H_\lambda \right)^0 = \bigcap_{\lambda \in \Lambda} H_\lambda^0 = \left(\bigcup_{\lambda \in \Lambda} H_\lambda \right)_{R^{(\alpha)}}^0.$$

■

Dowód: Jedyny nietrywialny element tezy to tożsamość (iii). Na mocy (i) mamy $H_2^0 \subset (H_2^0)^{00} \equiv ((H_2^0)^0)^0$, ale też $H_2 \subset H_2^{00}$, więc wobec (ii) jest $((H_2^0)^0)^0 \equiv (H_2^{00})^0 \subset H_2^0$, a stąd w sumie wynika (iii). □

Znaczenie pojęcia anihilatora ujawnia

STWIERDZENIE 126. *Przyjmijmy notację Def. 21, 32, 34, 35, 38 61, 64, 65, 95 i 98 oraz Stw. 40. Zwyródnienie odwzorowania dwuliniowego $\beta : G^{(1)} \times G^{(2)} \rightarrow G$ jest równoważne temu, że $G^{(1)0} \neq \{0_{(2)}\}$ lub $G^{(2)0} \neq \{0_{(1)}\}$. Dowolne takie odwzorowanie zadaje jednoznacznie **niezwyródniałe odwzorowanie dwuliniowe stowarzyszone** z β , jak następuje*

$$\underline{\beta} : G^{(1)}/G^{(2)0} \times G^{(2)}/G^{(1)0} \rightarrow G : (g + {}_{(1)}G^{(2)0}, h + {}_{(2)}G^{(1)0}) \mapsto \beta(g, h).$$

■

Analiza własności anihilatora staje się szczególnie prosta w przypadku $R = \mathbb{K}$, tj. w kategorii przestrzeni wektorowych nad ciałem $\mathbb{K}$. Punkt wyjścia stanowi tutaj poniższe nader istotne

STWIERDZENIE 127. *Przyjmijmy notację Def. 11, 32, 34, 35, 38, 61, 64, 63, 65, 72, 73, 95 i 98. Niechaj $V^{(\alpha)}$, $\alpha \in \{1, 2\}$ będą dwiema przestrzeniami wektorowymi nad ciałem $\mathbb{K}$ i niech $\Phi : V^{(1)} \times V^{(2)} \rightarrow \mathbb{K}$ będzie formą dwuliniową. Przestrzeń $V^{(1)}/V^{(2)0}$ jest wymiaru skończonego wtedy i tylko wtedy, gdy własność tę ma $V^{(2)}/V^{(1)0}$, i wówczas*

$$\dim_{\mathbb{K}} (V^{(1)}/V^{(2)0}) = \dim_{\mathbb{K}} (V^{(2)}/V^{(1)0}),$$

czyli też

$$V^{(1)}/V^{(2)0} \cong V^{(2)}/V^{(1)0}.$$

■

Dowód: Niech $\underline{\Phi} : V^{(1)}/V^{(2)0} \times V^{(2)}/V^{(1)0} \rightarrow \mathbb{K}$ będzie niezwyrodniałą formą dwuliniową stowarzyszoną z Φ i niech $\dim_{\mathbb{K}} V^{(1)}/V^{(2)0} < \infty$. Injektywność $r_{\underline{\Phi}} : V^{(2)}/V^{(1)0} \rightarrow (V^{(1)}/V^{(2)0})^*$ w połączeniu z tezą Stw. 122 daje nam nierówność

$$\dim_{\mathbb{K}} (V^{(2)}/V^{(1)0}) \leq \dim_{\mathbb{K}} (V^{(1)}/V^{(2)0})^* = \dim_{\mathbb{K}} (V^{(1)}/V^{(2)0}),$$

która implikuje w szczególności równość

$$\dim_{\mathbb{K}} (V^{(2)}/V^{(1)0})^* = \dim_{\mathbb{K}} (V^{(2)}/V^{(1)0}) < \infty.$$

Ten sam zestaw argumentów w odniesieniu do odwzorowania l_{Φ} prowadzi – wobec powyższego – do nierówności odwrotnej, co w sumie implikuje relację

$$\dim_{\mathbb{K}} (V^{(2)}/V^{(1)0}) = \dim_{\mathbb{K}} (V^{(1)}/V^{(2)0}) < \infty.$$

Z symetrii zagadnienia wynika, że analogiczny ciąg implikacji można otrzymać przy założeniu $\dim_{\mathbb{K}} (V^{(2)}/V^{(1)0}) < \infty$. $\square$

Ostatni wynik motywuje

DEFINICJA 99. Przyjmijmy notację Def. 11, 32, 34, 35, 38, 61, 64, 63, 65, 72, 73, 95 i 98 oraz Stw. 127. **Rzędem formy dwuliniowej** Φ nazywamy wymiar przestrzeni $V^{(1)}/V^{(2)0}$, o ile ten ostatni jest skończony. $\blacktriangle$

Powyższe stwierdzenie pozwala ustalić dalsze elementarne własności anihilatora (pod)przestrzeni wektorowej.

STWIERDZENIE 128. *Przyjmijmy notację Def. 67, 21, 32, 34, 35, 38, 61, 64, 65, 72, 73, 74, 95 i 98. Niechaj $V^{(\alpha)}$, $\alpha \in \{1, 2\}$ będą dwiema przestrzeniami wektorowymi nad ciałem $\mathbb{K}$, niech $W \subset V^{(1)}$ będzie podprzestrzenią i niech $\Phi : V^{(1)} \times V^{(2)} \rightarrow \mathbb{K}$ będzie niezwyrodniałą formą dwuliniową. Wówczas $\dim_{\mathbb{K}} W < \infty$ wtedy i tylko wtedy, gdy $\text{codim}_{\mathbb{K}}^{(V^{(2)})} W^0 < \infty$. W tej sytuacji zachodzi równość*

$$\text{codim}_{\mathbb{K}}^{(V^{(2)})} W^0 = \dim_{\mathbb{K}} W,$$

a nadto

$$W^{00} = W.$$

■

Dowód: Skoro Φ jest niezwyrodniała, to $V^{(2)0} = \{0_{(2)}\}$, a w takim razie obcięcie Φ do $W \times V^{(2)}$ pozwala orzec, na mocy Stw. 127, równoważność

$$\dim_{\mathbb{K}} W = \dim_{\mathbb{K}} (W/V^{(2)0}) < \infty \iff \infty > \dim_{\mathbb{K}} (V^{(2)}/W^0) \equiv \text{codim}_{\mathbb{K}}^{(V^{(2)})} W^0.$$

Przy tym spełnienie któregośkolwiek z równoważnych warunków zapewnia równość

$$\dim_{\mathbb{K}} W = \text{codim}_{\mathbb{K}}^{(V^{(2)})} W^0.$$

Zarazem wobec równości (iii) z tezy Stw. 125 oraz powyższego otrzymujemy implikację

$$\text{codim}_{\mathbb{K}}^{(V^{(2)})} (W^{00})^0 \equiv \text{codim}_{\mathbb{K}}^{(V^{(2)})} W^0 < \infty \implies \dim_{\mathbb{K}} W^{00} < \infty$$

oraz równość

$$\dim_{\mathbb{K}} W^{00} = \text{codim}_{\mathbb{K}}^{(V^{(2)})} W^0,$$

która w połączeniu z poprzednio otrzymaną daje

$$\dim_{\mathbb{K}} W^{00} = \dim_{\mathbb{K}} W.$$

Ponieważ zaś $W \subset W^{00}$, przeto otrzymujemy wówczas pożądaną równość $W = W^{00}$. $\square$

Miarą naturalności wyróżnionej przez nas konstrukcji anihilatora w kontekście teorii przestrzeni wektorowych jest jej prosta strukturalna relacja względem elementarnych operacji algebraicznych, jakie możemy wykonywać na przestrzeniach wektorowych.

STWIERDZENIE 129. *Przyjmijmy notację Def. 67, 21, 32, 34, 35, 61, 64, 65, 72, 73, 95 i 98. Niechaj $V^{(\alpha)}$, $\alpha \in \{1, 2\}$ będą dwiema przestrzeniami wektorowymi nad ciałem $\mathbb{K}$, niech $X, Y \subset V^{(1)}$ będą podprzestrzeniami i niech $\Phi : V^{(1)} \times V^{(2)} \longrightarrow \mathbb{K}$ będzie formą dwuliniową. Wówczas zachodzi tożsamość*

$$(8.32) \quad (X +_{(1)} Y)^0 = X^0 \cap Y^0,$$

a ponadto ilekroć $\dim_{\mathbb{K}} X, \dim_{\mathbb{K}} Y < \infty$, także tożsamość

$$(8.33) \quad (X \cap Y)^0 = X^0 +_{(2)} Y^0.$$

■

Dowód: Prawdziwość Równ. (8.32) jest oczywista, przejdziemy zatem do dowodu Równ. (8.33). Niech $\dim_{\mathbb{K}} X, \dim_{\mathbb{K}} Y < \infty$ i oznaczmy

$$Z := X^0 +_{(2)} Y^0.$$

Na mocy (8.32) oraz Stw. 128 zachodzi równość

$$Z^0 = (X^0 +_{(2)} Y^0)^0 = X^{00} \cap Y^{00} = X \cap Y.$$

Ograniczmy Φ do $X \times Z$ i przywołajmy tezę Stw. 127 (oraz Stw. 83), aby – wobec relacji $X^0 \subset Z$ i $Z^0 \subset X$ – dostać

$$\dim_{\mathbb{K}} (X/(X \cap Y)) \equiv \dim_{\mathbb{K}} (X/Z^0) = \dim_{\mathbb{K}} (Z/X^0).$$

Dopełnienie podprzestrzeni $Z/X^0 \subset V^{(2)}/X^0$ jest – w świetle dowodu Cor. 13 – kanonicznie izomorficzne z przestrzenią

$$(V^{(2)}/X^0)/(Z/X^0) \cong V^{(2)}/Z,$$

przy czym wypisany izomorfizm wynika wprost z Tw. 8.3 i prowadzi – poprzez Stw. 83,

$$\begin{aligned} \dim_{\mathbb{K}} (V^{(2)}/X^0) &= \dim_{\mathbb{K}} (Z/X^0) + \dim_{\mathbb{K}} ((V^{(2)}/X^0)/(Z/X^0)) \\ &= \dim_{\mathbb{K}} (Z/X^0) + \dim_{\mathbb{K}} (V^{(2)}/Z), \end{aligned}$$

a wobec skończoności $\dim_{\mathbb{K}} (V^{(2)}/Z)$, wynikającej ze skończoności

$$\dim_{\mathbb{K}} (V^{(2)}/X^0) \equiv \text{codim}_{\mathbb{K}}^{(V^{(2)})} X^0 = \dim_{\mathbb{K}} X < \infty$$

oraz

$$\dim_{\mathbb{K}} (Z/X^0) = \dim_{\mathbb{K}} (X/(X \cap Y)) \leq \dim_{\mathbb{K}} X < \infty$$

– do wyniku

$$\dim_{\mathbb{K}} (X/(X \cap Y)) = \text{codim}_{\mathbb{K}}^{(V^{(2)})} X^0 - \text{codim}_{\mathbb{K}}^{(V^{(2)})} Z = \dim_{\mathbb{K}} X - \text{codim}_{\mathbb{K}}^{(V^{(2)})} Z.$$

Uwzględnivszy następvnie $\dim_{\mathbb{K}}(X \cap Y) \leq \dim_{\mathbb{K}} X < \infty$, otrzymujemy w ten sposób równość

$$\dim_{\mathbb{K}} X - \dim_{\mathbb{K}}(X \cap Y) = \dim_{\mathbb{K}} X - \operatorname{codim}_{\mathbb{K}}^{(V^{(2)})} Z,$$

z której wynika wprost równość

$$\infty > \dim_{\mathbb{K}}(X \cap Y) = \operatorname{codim}_{\mathbb{K}}^{(V^{(2)})} Z \equiv \dim_{\mathbb{K}}(V^{(2)}/Z).$$

Ta w połączeniu z

$$\infty > \dim_{\mathbb{K}}(X \cap Y) = \operatorname{codim}_{\mathbb{K}}^{(V^{(2)})} (X \cap Y)^0 \equiv \dim_{\mathbb{K}}(V^{(2)}/(X \cap Y)^0)$$

i wobec relacji

$$Z \subset Z^{00} = (X \cap Y)^0$$

pozwała stwierdzić, że

$$\dim_{\mathbb{K}}((X \cap Y)^0/Z) \leq \dim_{\mathbb{K}}(V^{(2)}/Z) < \infty,$$

a zatem z relacji

$$(V^{(2)}/Z)/((X \cap Y)^0/Z) \cong V^{(2)}/(X \cap Y)^0,$$

wynioskowanej jak poprzednio, wyprowadzamy równość

$$\dim_{\mathbb{K}}(V^{(2)}/Z) - \dim_{\mathbb{K}}((X \cap Y)^0/Z) = \dim_{\mathbb{K}}(V^{(2)}/(X \cap Y)^0) = \dim_{\mathbb{K}}(V^{(2)}/Z),$$

czyli ostatecznie

$$\dim_{\mathbb{K}}((X \cap Y)^0/Z) = 0.$$

Ostatnia równość prowadzi wprost do oczekiwanego wyniku

$$(X \cap Y)^0 = Z = X^0 + {}_{(2)}Y^0.$$

□

Udowodnione uprzednio Stw. 127 nie tylko dostarcza poręcznych narzędzi do analizy własności algebraicznych anihilatora (pod)modułu i (pod)przestrzeni wektorowej, ale także – i z fizykalnego punktu widzenia przede wszystkim – pozwala ustalić precyzyjne kryterium nieosobliwości formy dwuliniowej na parze przestrzeni wektorowych skończonego wymiaru, z którego będziemy mogli skorzystać bezpośrednio w dyskusji form dwuliniowych $\Phi : V \times V \rightarrow \mathbb{K}$ określonych na kwadracie kartezjańskim ustalonej przestrzeni wektorowej V nad ciałem $\mathbb{K}$.

STWIERDZENIE 130. *Przyjmijmy notację Def. 11, 32, 34, 35, 38, 61, 63, 64, 65, 72, 73, 95, 96 i 98. Niechaj $V^{(\alpha)}$, $\alpha \in \{1, 2\}$ będą dwiema przestrzeniami wektorowymi tego samego wymiaru skończonego nad ciałem $\mathbb{K}$,*

$$D := \dim_{\mathbb{K}} V^{(1)} = \dim_{\mathbb{K}} V^{(2)} < \infty,$$

i niech $\Phi : V^{(1)} \times V^{(2)} \rightarrow \mathbb{K}$ będzie formą dwuliniową. Poniższe zdania są wtedy równoważne:

- (i) odwzorowanie r_{Φ} jest iniektywne;
- (ii) odwzorowanie r_{Φ} jest suriektywne;
- (iii) odwzorowanie l_{Φ} jest iniektywne;
- (iv) odwzorowanie l_{Φ} jest suriektywne;
- (v) forma Φ jest niezwyrodniała.

Ileokroć są one spełnione, $(V^{(1)}, V^{(2)}, \Phi)$ jest parą dwoistą. ■

Dowód: Założenia stwierdzenia implikują na mocy Stw. 122 ciąg relacji

$$\dim_{\mathbb{K}} V^{(1)*} = \dim_{\mathbb{K}} V^{(1)} = \dim_{\mathbb{K}} V^{(2)} = \dim_{\mathbb{K}} V^{(2)*} < \infty.$$

Są przy tym spełnione bilanse wymiarów

$$\dim_{\mathbb{K}} V^{(1)} = \dim_{\mathbb{K}} \operatorname{Ker} l_{\Phi} + \dim_{\mathbb{K}} \operatorname{Im} l_{\Phi},$$

$$\dim_{\mathbb{K}} V^{(2)} = \dim_{\mathbb{K}} \operatorname{Ker} r_{\Phi} + \dim_{\mathbb{K}} \operatorname{Im} r_{\Phi}$$

dla podprzestrzeni

$$\operatorname{Im} l_{\Phi} \subset V^{(2)*}, \quad \operatorname{Im} r_{\Phi} \subset V^{(1)*}$$

wymiaru

$$\dim_{\mathbb{K}} \operatorname{Im} l_{\Phi} \leq \dim_{\mathbb{K}} V^{(2)*} = D = \dim_{\mathbb{K}} V^{(1)*} \geq \dim_{\mathbb{K}} \operatorname{Im} r_{\Phi}.$$

Zdanie (i) jest zatem równoważne ciągłowi relacji

$$D = \dim_{\mathbb{K}} V^{(2)} = \dim_{\mathbb{K}} \operatorname{Ker} r_{\Phi} + \dim_{\mathbb{K}} \operatorname{Im} r_{\Phi} = \dim_{\mathbb{K}} \operatorname{Im} r_{\Phi} \leq D,$$

którego jedynym rozwiązaniem jest

$$\dim_{\mathbb{K}} \operatorname{Im} r_{\Phi} = D = \dim_{\mathbb{K}} V^{(2)*},$$

czyli

$$\operatorname{Im} r_{\Phi} = V^{(2)*},$$

a to wyraża zdanie (ii). Analogicznie pokazujemy równoważność (iii) $\iff$ (iv).

Ponadto wobec skończoności wymiarów $V^{(1)}$ i $V^{(2)}$ (pociągającej za sobą skończoność wymiarów $V^{(1)}/V^{(2)0}$ i $V^{(2)}/V^{(1)0}$) i na mocy Stw. 127 możemy zapisać

$$\begin{aligned} \dim_{\mathbb{K}} \operatorname{Ker} l_{\Phi} &\equiv \dim_{\mathbb{K}} V^{(2)0} = \dim_{\mathbb{K}} V^{(1)} - \dim_{\mathbb{K}} (V^{(1)}/V^{(2)0}) \\ &\equiv D - \dim_{\mathbb{K}} (V^{(1)}/V^{(2)0}) = D - \dim_{\mathbb{K}} (V^{(2)}/V^{(1)0}) \\ &\equiv \dim_{\mathbb{K}} V^{(2)} - \dim_{\mathbb{K}} (V^{(2)}/V^{(1)0}) = \dim_{\mathbb{K}} V^{(1)0} \equiv \dim_{\mathbb{K}} \operatorname{Ker} r_{\Phi}, \end{aligned}$$

to zaś wprost dowodzi równoważności (i) $\iff$ (iii).

Równoważność (v) $\iff$ (i) $\wedge$ (iii) $\iff$ (i) wynika teraz wprost z definicji i zamyka dowód stwierdzenia. □

Dotychczasowa analiza przygotowuje nas należycie do wykorzystania w dalszych naszych rozważaniach wyróżnionej formy dwuliniowej, jaką jest forma ewaluacji z Przykł. 46 (2). Będziemy przy tym korzystać z tego, że forma ta jest – wprost z definicji – (dwuliniowa i) prawostronnie niezwyrodniała, gdyż $r_{\langle \cdot, \cdot \rangle} = \operatorname{id}_{G^*}$. Innymi słowy, będziemy się nieraz powoływać na (trywialne)

COROLLARIUM 17. *Przyjmijmy notację Def. 21, 32, 35, 61, 65 i 95 oraz Przykł. 46 (2). Prawdziwą jest równoważność*

$$(\forall_{g \in G} : \langle g, \varphi \rangle = 0_R) \iff \varphi = 0.$$

■

Zacniemy od zbadania naturalnego mechanizmu indukcji odwzorowań R -liniowych między modułami sprzężonymi z odwzorowań między modułami wyjściowymi. Mechanizm ten opisuje

DEFINICJA 100. Przyjmijmy notację Def. 21, 32, 35, 61, 65, 94 i 95, Stw. 94 oraz Przykł. 46 (2). Niechaj $G^{(\alpha)}$, $\alpha \in \{1, 2\}$ będą dwoma modułami lewostronnymi nad pierścieniem R i niech $\chi : G^{(1)} \rightarrow G^{(2)}$ będzie odwzorowaniem R -liniowym. **Odwzorowanie sprzężone do χ** to homomorfizm R -modułów prawostronnych

$$\chi^* := \text{Hom}_R(\chi, R) : G^{(2)*} \rightarrow G^{(1)*} : \varphi \mapsto \varphi \circ \chi,$$

czyli odwzorowanie określone formułą

$$\forall_{(g, \varphi) \in G^{(1)} \times G^{(2)*} : \langle g, \chi^*(\varphi) \rangle := \langle \chi(g), \varphi \rangle.$$

▲

O tym, że definicja ma sens (tj. że zadaje homomorfizm R -modułów prawostronnych), przekonujemy się w bezpośrednim rachunku:

$$\begin{aligned} \langle g, \chi^*(\varphi \triangleleft_{(2)} r) \rangle &= \langle \chi(g), \varphi \triangleleft_{(2)} r \rangle = \langle \chi(g), \varphi \rangle \cdot_R r \equiv \langle g, \chi^*(\varphi) \rangle \cdot_R r \\ &= \langle g, \chi^*(\varphi) \triangleleft_{(1)} r \rangle, \end{aligned}$$

przeprowadzonym dla dowolnych $(g, \varphi, r) \in G^{(1)} \times G^{(2)*} \times R$. Rachunek ten pokazuje, że

$$\langle g, \chi^*(\varphi \triangleleft_{(2)} r) - \chi^*(\varphi) \triangleleft_{(1)} r \rangle = 0_R,$$

co w świetle Cor. 17 prowadzi do pożądanej równości

$$\chi^*(\varphi \triangleleft_{(2)} r) = \chi^*(\varphi) \triangleleft_{(1)} r.$$

W podobny sposób dowodzimy podstawowego

STWIERDZENIE 131. *Przyjmijmy notację Def. 21, 32, 35, 61, 65, 94 i 100. Niechaj $G^{(\alpha)}$, $\alpha \in \{1, 2, 3\}$ będą trzema modułami lewostronnymi nad pierścieniem R oraz niech $\chi, \chi_1, \chi_2 \in \text{Hom}_R(G^{(1)}, G^{(2)})$ i $\psi \in \text{Hom}_R(G^{(2)}, G^{(3)})$. Wówczas*

$$(\chi_1 + \chi_2)^* = \chi_1^* + \chi_2^*, \quad (\psi \circ \chi)^* = \chi^* \circ \psi^*,$$

a ponadto

$$\text{id}_{G^{(\alpha)}}^* = \text{id}_{G^{(\alpha)*}}.$$

Jeśli pierścień R jest przemienny, to także, dla dowolnego $r \in R$,

$$(r \triangleright \chi)^* = r \triangleright \chi^*,$$

przy czym dla dowolnych $g \in G^{(1)}$ i $\varphi \in G^{(2)*}$ zachodzi

$$(r \triangleright \chi)(g) := r \triangleright_{(2)} \chi(g), \quad (r \triangleright \chi^*)(\varphi) := r \cdot_R \chi^*(\varphi)(\cdot).$$

■

Dowód: Wszystkie wypisane tożsamości wynikają wprost z definicji odwzorowania sprzężonego. Udowodnimy dwie z nich, a mianowicie: drugą i czwartą. Oto stwierdzamy, dla dowolnych $g \in G^{(1)}$ i $\varphi \in G^{(3)*}$,

$$\begin{aligned} \langle g, (\psi \circ \chi)^*(\varphi) \rangle &\equiv \langle (\psi \circ \chi)(g), \varphi \rangle \equiv \langle \psi(\chi(g)), \varphi \rangle \equiv \langle \chi(g), \psi^*(\varphi) \rangle \\ &\equiv \langle g, \chi^*(\psi^*(\varphi)) \rangle \equiv \langle g, \chi^* \circ \psi^*(\varphi) \rangle, \end{aligned}$$

a ponadto dla dowolnych $\xi \in G^{(2)*}$ i elementu r pierścienia przemienne R ,

$$\begin{aligned} \langle g, (r \triangleright \chi)^*(\xi) \rangle &\equiv \langle (r \triangleright \chi)(g), \xi \rangle \equiv \langle r \triangleright_{(2)} \chi(g), \xi \rangle = r \cdot_R \langle \chi(g), \xi \rangle \equiv r \cdot_R \langle g, \chi^*(\xi) \rangle \\ &\equiv \langle g, (r \triangleright \chi^*)(\xi) \rangle. \end{aligned}$$

□

Prostym a ważnym następstwem powyższych tożsamości jest

COROLLARIUM 18. *Przyjmijmy notację Def. 21, 32, 35, 61, 65, 94 i 100 oraz Przykł. 46 (2). Niechaj $G^{(\alpha)}$, $\alpha \in \{1, 2\}$ będą dwoma modułami lewostronnymi nad pierścieniem R oraz niech*

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

będzie izomorfizmem R -modułów lewostronnych. Wówczas odwzorowanie sprzężone do χ jest izomorfizmem R -modułów prawostronnych,

$$\chi^* : G^{(2)*} \xrightarrow{\cong} G^{(1)*},$$

przy czym zachodzi

$$(\chi^{-1})^* = (\chi^*)^{-1}.$$

*Ostatni izomorfizm nosi miano **izomorfizmu kontragredientnego do χ** i jest oznaczany symbolem*

$$\tilde{\chi} := (\chi^{-1})^* : G^{(1)*} \xrightarrow{\cong} G^{(2)*}.$$

Spełnia on – wprost z definicji a dla dowolnych $(g, \varphi) \in G^{(1)} \times G^{(1)}$ – tożsamość*

$$(8.34) \quad \langle \chi(g), \tilde{\chi}(\varphi) \rangle_{(2)} = \langle g, \varphi \rangle_{(1)}.$$

■

PRZYKŁAD(Y) 48.

- (1) Niechaj $C_0(\mathbb{R}; \mathbb{R})$ będzie przestrzenią wektorową (nad $\mathbb{R}$) funkcji rzeczywistych zmiennej rzeczywistej o *zwartym nośniku*. Na jej kwadracie kartezjańskim określamy formę dwuliniową

$$\langle \cdot, \cdot \rangle : C_0(\mathbb{R}; \mathbb{R}) \times C_0(\mathbb{R}; \mathbb{R}) \longrightarrow \mathbb{R} : (f, g) \longmapsto \int_{-\infty}^{\infty} dt f(t) g(t).$$

Odwzorowaniem sprzężonym do odwzorowania ($\mathbb{R}$ -liniowego) pochodnej stopnia pierwszego

$$D : C_0(\mathbb{R}; \mathbb{R}) \longrightarrow C_0(\mathbb{R}; \mathbb{R}) : f \longmapsto Df, \quad Df(t) := \frac{d}{dt} f(t)$$

jest odwzorowanie

$$D^* = -D.$$

(2) Rozważmy przestrzeń wektorową $\mathbb{R}_d^{(h)}[t_1, t_2, \dots, t_n]$ z Przykł. 46 (4). Dłowny wielomian $P \in \mathbb{R}_m^{(h)}[t_1, t_2, \dots, t_n]$ zadaje odwzorowanie $\mathbb{R}$ -liniowe

$$P(D) : \mathbb{R}_d^{(h)}[t_1, t_2, \dots, t_n] \longrightarrow \mathbb{R}_{d-m}^{(h)}[t_1, t_2, \dots, t_n] : w \longmapsto P(D)w.$$

Możemy określić **uogólnione odwzorowanie sprzężone** do $P(D)$ wzorem

$$\langle w_1, P(D)^*(w_2) \rangle_d := \langle P(D)(w_1), w_2 \rangle_{d-m},$$

zapisanym dla dowolnych $w_1 \in \mathbb{R}_d^{(h)}[t_1, t_2, \dots, t_n]$ i $w_2 \in \mathbb{R}_{d-m}^{(h)}[t_1, t_2, \dots, t_n]$. Przy tej definicji $P(D)^*$ znajdujemy bez trudu

$$P(D)^* : \mathbb{R}_{d-m}^{(h)}[t_1, t_2, \dots, t_n] \longrightarrow \mathbb{R}_d^{(h)}[t_1, t_2, \dots, t_n] : w \longmapsto P \odot w.$$

✓

Dalszej charakteryzacji algebraicznej odwzorowań sprzężonych, rzucającej światło na ich naturę, dostarcza

STWIERDZENIE 132. *Przyjmijmy notację Def. 21, 32, 34, 35, 36, 61, 64, 65, 94, 98 i 100. Niechaj $G^{(\alpha)}$, $\alpha \in \{1, 2\}$ będą dwoma modułami lewostronnymi nad pierścieniem R , niech $H \subset G^{(1)}$ będzie podmodułem i niech $\chi : G^{(1)} \longrightarrow G^{(2)}$ będzie odwzorowaniem R -liniowym. Wówczas zachodzi tożsamość*

$$\chi(H)^0 = \chi^{*-1}(H^0),$$

przy czym wypisane tu anihilatory są określone przez formę ewaluacji na – odpowiednio – $G^{(2)} \times G^{(2)*}$ i $G^{(1)} \times G^{(1)*}$. W szczególności

$$(\text{Im } \chi)^0 = \text{Ker } \chi^*.$$

■

Dowód: Teza jest tutaj bezpośrednią konsekwencją definicji χ^* , oto bowiem dla dowolnych $h \in H$ i $\varphi \in G^{(2)*}$ otrzymujemy

$$\langle \chi(h), \varphi \rangle \equiv \langle h, \chi^*(\varphi) \rangle,$$

zatem

$$\begin{aligned} \varphi \in (\text{Im } (\chi|_H))^0 &\iff \forall_{h \in H} : \langle h, \chi^*(\varphi) \rangle = 0_R \iff \chi^*(\varphi) \in H^0 \\ &\iff \varphi \in \chi^{*-1}(H^0). \end{aligned}$$

□

Pouczający przykład zgrabnego zastosowania odwzorowań sprzężonych opisuje

STWIERDZENIE 133. *Przyjmijmy notację Def. 21, 32, 34, 35, 61, 64, 65, 75, 77, 78, 94, 98 i 100. Niechaj G będzie R -modułem lewostronnym rozszczepiającym się na sumę prostą swych podmodułów $H_1, H_2 \subset G$ i niech $\text{pr}_\alpha : G \longrightarrow$*

H_α , $\alpha \in \{1, 2\}$ będą rzutami kanonicznymi na składniki proste, $j_\alpha : H_\alpha \rightarrow G$ zaś – włożeniami kanonicznymi tychże składników. Wówczas odwzorowanie R -liniowe

$$(\text{pr}_1^*, 0) + (0, \text{pr}_2^*) : H_1^* \oplus H_2^* \rightarrow G^*$$

jest izomorfizmem R -modułów (prawostronnych), przy czym

$$\text{pr}_1^* : H_1^* \rightarrow H_2^0 \subset G^*, \quad \text{pr}_2^* : H_2^* \rightarrow H_1^0 \subset G^*$$

są izomorfizmami. Ponadto endomorfizmy

$$\pi_\alpha := \text{pr}_\alpha^* \circ j_\alpha^* \in \text{End}_R(G^*)$$

są rzutami zadającymi rozkład

$$G^* = \text{pr}_1^*(H_1^*) \oplus \text{pr}_2^*(H_2^*).$$

■

Dowód: Zaczniemy od wypisania elementarnych tożsamości spełnianych przez odwzorowania pr_α i j_α ,

$$(8.35) \quad \text{pr}_\alpha \circ j_\beta = \delta_{\alpha,\beta}^R \text{id}_{H_\alpha}, \quad j_1 \circ \text{pr}_1 + j_2 \circ \text{pr}_2 = \text{id}_G.$$

Obrazem odwzorowania

$$\varphi : \{1, 2\} \rightarrow H_1^* \cup H_2^* : \alpha \mapsto \varphi_\alpha \in H_\alpha^*$$

względem $\text{pr}_\oplus^* := (\text{pr}_1^*, 0) + (0, \text{pr}_2^*)$ jest

$$\text{pr}_\oplus^*(\varphi) = \varphi_1 \circ \text{pr}_1 + \varphi_2 \circ \text{pr}_2.$$

Przywoławszy kanoniczny izomorfizm

$$\text{Hom}_R(j, R) : (H_1 \oplus H_2)^* \xrightarrow{\cong} H_1^* \oplus H_2^* : \varphi \mapsto \varphi \circ j,$$

opisany w Stw. 94, bez trudu sprawdzamy, że odwzorowanie $\text{pr}_\oplus^*$ jest jego odwrotnością, oto bowiem wobec pierwszej z tożsamości (8.35) zachodzi

$$\begin{aligned} \text{Hom}_R(j, R) \circ \text{pr}_\oplus^*(\varphi) &: \{1, 2\} \rightarrow H_1^* \cup H_2^* \\ &: \alpha \mapsto (\varphi_1 \circ \text{pr}_1 + \varphi_2 \circ \text{pr}_2) \circ j_\alpha = \varphi_\alpha \circ \text{id}_{H_\alpha} = \varphi_\alpha \end{aligned}$$

a ponadto – wobec drugiej z tożsamości (8.35) a dla $\psi \in G^*$ –

$$\text{pr}_\oplus^* \circ \text{Hom}_R(j, R)(\psi) \equiv \text{pr}_\oplus^*(\psi \circ j) \equiv \psi \circ (j_1 \circ \text{pr}_1 + j_2 \circ \text{pr}_2) = \psi.$$

Powyższa dyskusja dowodzi, że $\text{pr}_\oplus^*$ jest izomorfizmem R -modułów.

Rozważmy następnie odwzorowanie pr_1^* (analiza odwzorowania pr_2^* przebiega analogicznie). Łatwo widać, że $\text{pr}_1^*(H_1^*) \subset H_2^0 \subset G^*$ – istotnie, wprost z definicji odwzorowania sprzężonego wyprowadzamy dla $(0, h_2) \in j_2(H_2)$ równość

$$\langle (0, h_2), \text{pr}_1^*(\varphi_1) \rangle = \langle \text{pr}_1(0, h_2), \varphi \rangle = \langle 0, \varphi \rangle = 0_R.$$

Jest też $H_2^0 \subset \text{pr}_1^*(H_1^*)$, albowiem dla dowolnej formy $\varphi \in G^*$ równość $\varphi(0, h_2) = 0_R$ implikuje – z racji dwuliniowości φ i dla $(h_1, 0) \in j_1(H_1)$ –

$$\varphi(h_1, h_2) = \varphi(h_1, 0) +_R \varphi(0, h_2) = \varphi(h_1, 0) \equiv \varphi \circ j_1 \circ \text{pr}_1(h_1, h_2),$$

czyli

$$\varphi = \text{pr}_1^*(j_1^* \varphi) \in \text{Im } \text{pr}_1^*.$$

Dokonując obustronnego sprzężenia Równ. (8.35) zgodnie z regułami sformułowanymi w Stw. 131, otrzymujemy

$$j_\alpha^* \circ \text{pr}_\alpha^* = \text{id}_{H_\alpha^*}, \quad j_2^* \circ \text{pr}_1^* = 0 = j_1^* \circ \text{pr}_2^*, \quad \text{pr}_1^* \circ j_1^* + \text{pr}_2^* \circ j_2^* = \text{id}_{G^*}.$$

Odwzorowania π_α spełniają zatem relacje

$$\pi_\alpha \circ \pi_\beta = \text{pr}_\alpha^* \circ (j_\alpha^* \circ \text{pr}_\beta^*) \circ j_\beta^* = \text{pr}_\alpha^* \circ \delta_{\alpha,\beta}^R \text{id}_{H_\alpha^*} \circ j_\beta^* = \delta_{\alpha,\beta}^R \pi_\alpha$$

oraz

$$\pi_1 + \pi_2 = \text{id}_{G^*},$$

które identyfikują parę $\{\pi_1, \pi_2\}$ jako zupełną rodzinę rzutów komplementarnych. Ostatnia część tezy jest teraz prostą konsekwencją Stw. 88. $\square$

Powyższe stwierdzenie pozwala dokonać naturalnego utożsamienia

$$H_1^* \cong H_2^0, \quad H_2^* \cong H_1^0$$

form liniowych na składniku prostym $H_1 \subset G$ (wzgl. $H_2 \subset G$) z tymi formami liniowymi na całym module G , które zerują się na dopełnieniu H_2 (wzgl. H_1) tegoż składnika.

8.10. Ciągi dokładne grup odwzorowań R -liniowych i ciągi dualne

Dotychczasowe nasze rozważania ustalają ledwie najbardziej elementarne własności operacji sprzężenia – tak w odniesieniu do modułu, jak i w odniesieniu do odwzorowania R -liniowego – oraz związek modułu sprzężonego i jego podmodułów z konstrukcją anihilatora. Pogłębienie zgromadzonej przez nas wiedzy, w szczególności zaś – precyzyjna identyfikacja obrazu wyróżnionych podmodułów (takich jak obraz i jądro odwzorowania R -liniowego) oraz modułów ilorazowych, a także zbadanie warunków rozszczepialności modułu sprzężonego do danego (rozszczepialnego), wymaga użycia nowych środków formalnych. Wyjątkowo wydajnych narzędzi okazuje się tu dostarczać teoria ciągów dokładnych wprowadzona w Rozdz. 5.3. Podstawowe wyniki tej teorii znajdujące bezpośrednie zastosowanie w interesującym nas kontekście gromadzimy poniżej. O sile wysłowionych tu twierdzeń przekona nas dalsza analiza, jak również dyskusja zagadnień z dziedziny algebry homologicznej. Należy podkreślić, iż twierdzenia te stanowią doskonałą egzemplifikację podejścia kategoryjnego do opisu struktur algebraicznych, oto bowiem o własnościach obiektów algebraicznych z pewnej kategorii (w tym wypadku: modułów nad ustalonym pierścieniem oraz przestrzeni wektorowych nad ustalonym ciałem) orzekamy na gruncie analizy morfizmów (też kategorii) odwzorowujących interesujące nas obiekty w dowolny obiekt referencyjny tej samej kategorii tudzież tych odwzorowujących obiekt referencyjny w obiekty dane.

Zgromadzone tu obserwacje dokumentują w nader przekonujący sposób naturalność¹⁸ omawianych wcześniej schematów indukcji homomorfizmów: $\chi \mapsto \text{Hom}_R(\chi, G)$ oraz $\psi \mapsto \text{Hom}_R(G, \psi)$ w kontekście konstrukcji ciągów dokładnych. Zaczniemy od przeanalizowania właściwości pierwszego z tych schematów.

¹⁸W języku teorii kategorii opisane własności odwzorowania $\text{Hom}_R(\cdot, G)$, określonego – dla dowolnego modułu referencyjnego G – zarówno na modułach, jak i na odwzorowaniach R -liniowych między nimi, identyfikują to odwzorowanie jako tzw. **lewostronnie dokładny funktor kontrawariantny**. Podobnie własności odwzorowania $\text{Hom}_R(G, \cdot)$ czynią z niego **lewostronnie dokładny funktor kowariantny**.

TWIERDZENIE 8.14 (O lewostronnej dokładności $\text{Hom}_R(\cdot, G)$). *Przyjmijmy notację Def. 21, 32, 35, 43, 61, 65, 94, 95 i 100 oraz Stw. 93. Niechaj $G^{(\alpha)}$, $\alpha \in \{1, 2, 3\}$ będą trzema modułami (lewostronnymi) nad pierścieniem R i niech $\chi_{(\beta)} : G^{(\beta)} \rightarrow G^{(\beta+1)}$, $\beta \in \{1, 2\}$ będą dwoma odwzorowaniami R -liniowymi między nimi. Ciąg modułów*

$$G^{(1)} \xrightarrow{\chi_{(1)}} G^{(2)} \xrightarrow{\chi_{(2)}} G^{(3)} \rightarrow \mathbf{0}$$

jest dokładny wtedy i tylko wtedy, gdy ciąg grup przemennych

$$\mathbf{0} \rightarrow \text{Hom}_R(G^{(3)}, G) \xrightarrow{\text{Hom}_R(\chi_{(2)}, G)} \text{Hom}_R(G^{(2)}, G) \xrightarrow{\text{Hom}_R(\chi_{(1)}, G)} \text{Hom}_R(G^{(1)}, G)$$

jest dokładny dla dowolnego modułu (lewostronnego) G nad R .

W szczególności dokładność powyższego ciągu modułów implikuje dokładność ciągu modułów sprzężonych

$$\mathbf{0} \rightarrow G^{(3)*} \xrightarrow{\chi_{(2)}^*} G^{(2)*} \xrightarrow{\chi_{(1)}^*} G^{(1)*}.$$

■

Dowód:

$\Rightarrow$ Niech $\psi \in \text{Ker Hom}_R(\chi_{(2)}, G) \subset \text{Hom}_R(G^{(3)}, G)$, tj. $\psi \circ \chi_{(2)} = 0$. Skoro $\chi_{(2)}$ jest epimorfizmem, to $G^{(3)} = \text{Im } \chi_{(2)}$, czyli też $\psi(G^{(3)}) = \psi(\chi_{(2)}(G^{(2)})) = \{0_G\}$, a w takim razie $\psi = 0$, co oznacza, że – istotnie – $\text{Ker Hom}_R(\chi_{(2)}, G) = \{0\}$.

Niech teraz $\xi \in \text{Ker Hom}_R(\chi_{(1)}, G) \subset \text{Hom}_R(G^{(2)}, G)$, czyli $\xi|_{\text{Im } \chi_{(1)}} = 0$. Rozumując jak w dowodzie Tw. 5.2, możemy dokonać rozkładu

$$\xi = \tilde{\xi} \circ \pi_{G^{(2)}/\text{Im } \chi_{(1)}},$$

w którym

$$\tilde{\xi} : G^{(2)}/\text{Im } \chi_{(1)} \rightarrow G : g + {}_{(2)}\text{Im } \chi_{(1)} \mapsto \xi(g).$$

Z racji dokładności ciągu modułów jest jednak

$$G^{(2)}/\text{Im } \chi_{(1)} \equiv G^{(2)}/\text{Ker } \chi_{(2)},$$

a nadto – wobec surjektywności χ_2 – istnieje kanoniczny izomorfizm modułów

$$\tilde{\chi}_{(2)} : G^{(2)}/\text{Ker } \chi_{(2)} \xrightarrow{\cong} G^{(3)} : g + {}_{(2)}\text{Ker } \chi_{(2)} \mapsto \chi_{(2)}(g),$$

który zadaje rozkład

$$\chi_{(2)} = \tilde{\chi}_{(2)} \circ \pi_{G^{(2)}/\text{Im } \chi_{(1)}}.$$

Ostatecznie zatem

$$\xi = (\tilde{\xi} \circ \tilde{\chi}_{(2)}^{-1}) \circ (\tilde{\chi}_{(2)} \circ \pi_{G^{(2)}/\text{Im } \chi_{(1)}}) \equiv (\tilde{\xi} \circ \tilde{\chi}_{(2)}^{-1}) \circ \chi_{(2)} \in \text{Im Hom}_R(\chi_{(2)}, G),$$

co dowodzi inkluzji $\text{Ker Hom}_R(\chi_{(1)}, G) \subset \text{Im Hom}_R(\chi_{(2)}, G)$. Inkluzja odwrotna wynika wprost z tożsamości $\chi_{(2)} \circ \chi_{(1)} = 0$, będącej następstwem równości $\text{Ker } \chi_{(2)} = \text{Im } \chi_{(1)}$.

$\Leftarrow$ Dokładność ciągu grup odwzorowań R -liniowych implikuje tożsamość

$$\begin{aligned}\xi \circ \chi_{(2)} \circ \chi_{(1)} &\equiv \operatorname{Hom}_R(\chi_{(2)} \circ \chi_{(1)}, G)(\xi) = \operatorname{Hom}_R(\chi_{(1)}, G) \circ \operatorname{Hom}_R(\chi_{(2)}, G)(\xi) \\ &= 0(\xi) = 0\end{aligned}$$

dla dowolnego modułu G i dowolnego odwzorowania R -liniowego $\xi \in \operatorname{Hom}_R(G^{(3)}, G)$. Wybierając $G := G^{(3)}$ i $\xi := \operatorname{id}_{G^{(3)}}$, wnioskujemy na tej podstawie, że

$$\operatorname{Im} \chi_{(1)} \subset \operatorname{Ker} \chi_{(2)}.$$

Rozpatrując natomiast $G := \operatorname{Coker} \chi_{(1)} \equiv G^{(2)}/\operatorname{Im} \chi_{(1)}$ wraz z rzutem kanonicznym $\pi_{G^{(2)}/\operatorname{Im} \chi_{(1)}} : G^{(2)} \rightarrow G^{(2)}/\operatorname{Im} \chi_{(1)}$, otrzymujemy równość

$$\operatorname{Hom}_R(\chi_{(1)}, G^{(2)}/\operatorname{Im} \chi_{(1)})(\pi_{G^{(2)}/\operatorname{Im} \chi_{(1)}}) \equiv \pi_{G^{(2)}/\operatorname{Im} \chi_{(1)}} \circ \chi_{(1)} \equiv 0,$$

z której odczytujemy

$$\pi_{G^{(2)}/\operatorname{Im} \chi_{(1)}} \in \operatorname{Ker} \operatorname{Hom}_R(\chi_{(1)}, G^{(2)}/\operatorname{Im} \chi_{(1)}) = \operatorname{Im} \operatorname{Hom}_R(\chi_{(2)}, G^{(2)}/\operatorname{Im} \chi_{(1)})$$

i która zatem pociąga za sobą istnienie odwzorowania R -liniowego $\psi \in \operatorname{Hom}_R(G^{(3)}, G^{(2)}/\operatorname{Im} \chi_{(1)})$ o własności

$$\pi_{G^{(2)}/\operatorname{Im} \chi_{(1)}} = \psi \circ \chi_{(2)}.$$

Ostatnia równość pokazuje dowodnie, iż

$$\operatorname{Ker} \chi_{(2)} \subset \operatorname{Ker} \pi_{G^{(2)}/\operatorname{Im} \chi_{(1)}} = \operatorname{Im} \chi_{(1)},$$

co w sumie daje pożądaną równość

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

Na koniec wyznaczamy – dla rzutu kanonicznego $\pi_{G^{(3)}/\operatorname{Im} \chi_{(2)}} : G^{(3)} \rightarrow G^{(3)}/\operatorname{Im} \chi_{(2)} =: G$ –

$$\pi_{G^{(3)}/\operatorname{Im} \chi_{(2)}} \in \operatorname{Ker} \operatorname{Hom}_R(\chi_{(2)}, G^{(3)}/\operatorname{Im} \chi_{(2)}) = \{0\},$$

skąd wniosek, że

$$G^{(3)}/\operatorname{Im} \chi_{(2)} = \mathbf{0},$$

czyli też $\chi_{(2)}$ jest surjekcją.

□

Jak stwierdziliśmy w Rozdz. 8.5, konstrukcja krótkiego ciągu dokładnego pozwala na uzyskanie szczególnie zwięzłego opisu warunków rozszczepialności modułu na sumę prostą jego podmodułów. Rozpoczętą wówczas dyskusję znacząco wzbogaca

STWIERDZENIE 134. *Przyjmijmy notację Def. 21, 32, 35, 43, 61, 65, 94, 95 i 100, Stw. 93 oraz Tw. 8.14. Jeśli ciąg dokładny modułów*

$$(8.36) \quad \mathbf{0} \longrightarrow G^{(1)} \xrightarrow{\chi_{(1)}} G^{(2)} \xrightarrow{\chi_{(2)}} G^{(3)} \longrightarrow \mathbf{0}$$

rozszczenia się (tj. $\text{Im } \chi_{(1)}$ jest składnikiem prostym $G^{(2)}$), to ciąg grup przemien-
nych

$$\begin{aligned} \mathbf{0} \longrightarrow \text{Hom}_R(G^{(3)}, G) &\xrightarrow{\text{Hom}_R(\chi_{(2)}, G)} \text{Hom}_R(G^{(2)}, G) \\ &\xrightarrow{\text{Hom}_R(\chi_{(1)}, G)} \text{Hom}_R(G^{(1)}, G) \longrightarrow \mathbf{0} \end{aligned}$$

jest dokładny i rozszczepia się dla dowolnego modułu (lewostronnego) G nad pier-
ścieniem R . I odwrotnie, jeśli powyższy ciąg grup przemiennych jest dokładny dla
dowolnego R -modułu (lewostronnego) G , wówczas dokładny ciąg modułów (8.36)
rozszczenia się.

W szczególności rozszczepialność dokładnego ciągu modułów (8.36) implikuje
dokładność i rozszczepialność ciągu modułów sprzężonych

$$\mathbf{0} \longrightarrow G^{(3)*} \xrightarrow{\chi_{(2)}^*} G^{(2)*} \xrightarrow{\chi_{(1)}^*} G^{(1)*} \longrightarrow \mathbf{0}.$$

■

Dowód:

$\Rightarrow$ Skoro ciąg modułów jest rozszczepiony, to w świetle Tw. 8.10 istnieje re-
trakcja liniowa stowarzyszona z $\chi_{(1)}$, czyli odwzorowanie R -liniowe $\rho \in$
 $\text{Hom}_R(G^{(2)}, G^{(1)})$ o własności $\rho \circ \chi_{(1)} = \text{id}_{G^{(1)}}$. Dowolne odwzorowanie
 $\psi \in \text{Hom}_R(G^{(1)}, G)$ możemy zatem zapisać w postaci

$$\psi \equiv \psi \circ \text{id}_{G^{(1)}} = (\psi \circ \rho) \circ \chi_{(1)} \in \text{Im Hom}_R(\chi_{(1)}, G),$$

co pokazuje surjektywność $\text{Hom}_R(\chi_{(1)}, G)$. W świetle Tw. 8.14 przesądza
to o dokładności ciągu grup homomorfizmów.

Istnienie retrakcji liniowej pociąga za sobą także tożsamość

$$\begin{aligned} \text{Hom}_R(\chi_{(1)}, G) \circ \text{Hom}_R(\rho, G) &\equiv \text{Hom}_R(\rho \circ \chi_{(1)}, G) = \text{Hom}_R(\text{id}_{G^{(1)}}, G) \\ &= \text{id}_{\text{Hom}_R(G^{(1)}, G)}, \end{aligned}$$

słuszną dla dowolnego modułu G . Ta ostatnia oznacza jednak, że odwzo-
rowanie $\text{Hom}_R(\rho, G)$ jest cięciem liniowym stowarzyszonym z odwzoro-
waniem $\text{Hom}_R(\chi_{(1)}, G)$, którego istnienie gwarantuje rozszczepienie ciągu
grup odwzorowań R -liniowych na mocy tego samego twierdzenia.

$\Leftarrow$ Zaczniemy od udowodnienia dokładności podciągu $\mathbf{0} \longrightarrow G^{(1)} \longrightarrow G^{(2)}$,
która na mocy Tw. 8.14 gwarantuje dokładność pełnego ciągu modułów.
Połóżmy $G := G^{(1)}$. Skoro $\text{Hom}_R(\chi_{(1)}, G^{(1)})$ jest surjekcją, przeto $\text{id}_{G^{(1)}} =$
 $\psi \circ \chi_{(1)}$ dla pewnego $\psi \in \text{Hom}_R(G^{(2)}, G^{(1)})$. Stąd jednak możemy wypro-
wadzić wniosek, że $\text{Ker } \chi_{(1)} \subset \text{Ker id}_{G^{(1)}} = \{0_{(1)}\}$, który oznacza iniektyw-
ność $\chi_{(1)}$. Jest przy tym jasnym, że ψ jest retrakcją liniową stowarzyszoną
z $\chi_{(1)}$, a to na mocy Tw. 8.10 oznacza, że ciąg modułów rozszczepia się.

□

Przejdziemy obecnie do rozpatrzenia drugiego schematu indukcji homomorfi-
zmów.

TWIERDZENIE 8.15 (O lewostronnej dokładności $\text{Hom}_R(G, \cdot)$). *Przyjmijmy notację Def. 21, 32, 35, 43, 61 i 65 oraz Stw. 93. Niechaj $G^{(\alpha)}$, $\alpha \in \{1, 2, 3\}$ będą trzema modułami (lewostronnymi) nad pierścieniem R i niech $\chi_{(\beta)} : G^{(\beta)} \rightarrow G^{(\beta+1)}$, $\beta \in \{1, 2\}$ będą dwoma odwzorowaniami R -liniowymi między nimi. Ciąg modułów*

$$0 \longrightarrow G^{(1)} \xrightarrow{\chi_{(1)}} G^{(2)} \xrightarrow{\chi_{(2)}} G^{(3)}$$

jest dokładny wtedy i tylko wtedy, gdy ciąg grup przemennych

$$0 \longrightarrow \text{Hom}_R(G, G^{(1)}) \xrightarrow{\text{Hom}_R(G, \chi_{(1)})} \text{Hom}_R(G, G^{(2)}) \xrightarrow{\text{Hom}_R(G, \chi_{(2)})} \text{Hom}_R(G, G^{(3)})$$

jest dokładny dla dowolnego modułu (lewostronnego) G nad R .

■

Dowód:

$\Rightarrow$ Weźmy dowolne odwzorowanie $\psi \in \text{Ker Hom}_R(G, \chi_{(1)}) \subset \text{Hom}_R(G, G^{(1)})$, czyli takie, dla którego zachodzi $\chi_{(1)} \circ \psi = 0$. Wobec trywialności jądra $\chi_{(1)}$ ostatnia równość oznacza $\text{Im } \psi = \{0_{(1)}\}$, czyli $\psi = 0$, i tym samym pokazuje injektywność $\text{Hom}_R(G, \chi_{(1)})$.

W następnej kolejności zauważmy, że

$$\text{Hom}_R(G, \chi_{(2)}) \circ \text{Hom}_R(G, \chi_{(1)}) = \text{Hom}_R(G, \chi_{(2)} \circ \chi_{(1)}) = 0$$

w konsekwencji równości $\text{Ker } \chi_{(2)} = \text{Im } \chi_{(1)}$. W takim razie

$$\text{Im Hom}_R(G, \chi_{(1)}) \subset \text{Ker Hom}_R(G, \chi_{(2)})$$

i pozostaje tylko udowodnić zawieranie odwrotne. W tym celu wybierzmy dowolne odwzorowanie $\xi \in \text{Ker Hom}_R(G, \chi_{(2)})$, tj. spełniające warunek $\chi_{(2)} \circ \xi = 0$, z którego wynika inkluzja

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

Wobec injektywności $\chi_{(1)}$ istnieje kanoniczny izomorfizm

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

o którego istnieniu orzeka Tw. 8.1. Pozwala nam on rozłożyć ξ , jak następuje:

$$\xi = \chi_{(1)} \circ \left(\lambda_{\chi_{(1)}}^{-1} \circ \xi \right),$$

przy czym $\lambda_{\chi_{(1)}}^{-1} \circ \xi \in \text{Hom}_R(G, G^{(1)})$. Jest zatem

$$\xi \in \text{Im Hom}_R(G, \chi_{(1)}),$$

skąd

$$\text{Ker Hom}_R(G, \chi_{(2)}) \subset \text{Im Hom}_R(G, \chi_{(1)}),$$

czyli też ostatecznie

$$\text{Ker Hom}_R(G, \chi_{(2)}) = \text{Im Hom}_R(G, \chi_{(1)}).$$

$$\begin{aligned}
&\Leftarrow \text{Dokładność ciągu grup odwzorowań } R\text{-liniowych daje nam tożsamość} \\
\chi_{(2)} \circ \chi_{(1)} \circ \xi &\equiv \text{Hom}_R(G, \chi_{(2)} \circ \chi_{(1)})(\xi) = \text{Hom}_R(G, \chi_{(2)}) \circ \text{Hom}_R(G, \chi_{(1)})(\xi) \\
&= 0(\xi) = 0
\end{aligned}$$

dla dowolnego modułu G i dowolnego odwzorowania R -liniowego $\xi \in \text{Hom}_R(G, G^{(1)})$. Wybierając $G := G^{(1)}$ i $\xi := \text{id}_{G^{(1)}}$, wyprowadzamy relację

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

Wybór $G := \text{Ker } \chi_{(2)}$ wraz ze standardowym włożeniem $J_{\text{Ker } \chi_{(2)}} : \text{Ker } \chi_{(2)} \rightarrow G^{(2)}$ prowadzi do równości

$$\text{Hom}_R(\text{Ker } \chi_{(2)}, \chi_{(2)})(J_{\text{Ker } \chi_{(2)}}) \equiv \chi_{(2)} \circ J_{\text{Ker } \chi_{(2)}} \equiv 0,$$

z której wynika

$$J_{\text{Ker } \chi_{(2)}} \in \text{Ker Hom}_R(\text{Ker } \chi_{(2)}, \chi_{(2)}) = \text{Im Hom}_R(\text{Ker } \chi_{(2)}, \chi_{(1)})$$

i która zatem pociąga za sobą istnienie odwzorowania R -liniowego $\psi \in \text{Hom}_R(\text{Ker } \chi_{(2)}, G^{(1)})$ o własności

$$J_{\text{Ker } \chi_{(2)}} = \chi_{(1)} \circ \psi,$$

co z kolei dowodzi inkluzji

$$\text{Ker } \chi_{(2)} \subset \text{Im } \chi_{(1)},$$

dając ostatecznie pożądaną równość

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

I wreszcie dla $G = \text{Ker } \chi_{(1)}$ i $\text{id}_{\text{Ker } \chi_{(1)}}$ stwierdzamy

$$\text{id}_{\text{Ker } \chi_{(1)}} \in \text{Ker Hom}_R(\text{Ker } \chi_{(1)}, \chi_{(1)}) = \{0\},$$

co pozwala zidentyfikować

$$\text{Ker } \chi_{(1)} = \mathbf{0},$$

to zaś pokazuje, że $\chi_{(1)}$ jest injekcją.

□

Także drugi schemat indukcji homomorfizmów daje wgląd w zagadnienie rozszczepialności modułów.

STWIERDZENIE 135. *Przyjmijmy notację Def. 21, 32, 35, 43, 61 i 65, Stw. 93 oraz Tw. 8.15. Jeśli ciąg dokładny modułów*

$$(8.37) \quad \mathbf{0} \longrightarrow G^{(1)} \xrightarrow{\chi_{(1)}} G^{(2)} \xrightarrow{\chi_{(2)}} G^{(3)} \longrightarrow \mathbf{0}$$

rozszczepia się, to ciąg grup przemennych

$$\begin{aligned}
\mathbf{0} \longrightarrow \text{Hom}_R(G, G^{(1)}) &\xrightarrow{\text{Hom}_R(G, \chi_{(1)})} \text{Hom}_R(G, G^{(2)}) \\
&\xrightarrow{\text{Hom}_R(G, \chi_{(2)})} \text{Hom}_R(G, G^{(3)}) \longrightarrow \mathbf{0}
\end{aligned}$$

jest dokładny i rozszczepia się dla dowolnego modułu (lewostronnego) G nad pierścieniem R . I odwrotnie, jeśli powyższy ciąg grup przemennych jest dokładny dla

dowolnego R -modułu (lewostronnego) G , wówczas dokładny ciąg modułów (8.37) rozszczepia się. ■

Dowód:

$\Rightarrow$ Dokładność ciągu modułów oznacza istnienie kanonicznego izomorfizmu

$$G^{(2)} = \chi_{(1)}(G^{(1)}) \oplus \sigma(G^{(3)}),$$

w którego zapisie $\sigma \in \text{Hom}_R(G^{(3)}, G^{(2)})$ reprezentuje cięcie liniowe stowarzyszone z $\chi_{(2)}$. Tożsamość $\chi_{(2)} \circ \sigma = \text{id}_{G^{(3)}}$ implikuje surjektywność $\text{Hom}_R(G, \chi_{(2)})$, oto bowiem dowolne odwzorowanie R -liniowe $\psi \in \text{Hom}_R(G, G^{(3)})$ możemy zapisać w postaci

$$\psi = \chi_{(2)} \circ (\sigma \circ \psi) \in \text{Im } \text{Hom}_R(G, \chi_{(2)}).$$

Na mocy Stw. 94 zachodzi ponadto

$$\text{Hom}_R(G, G^{(2)}) \cong \text{Hom}_R(G, \chi_{(1)}(G^{(1)})) \oplus \text{Hom}_R(G, \sigma(G^{(3)})),$$

przy czym

$$\begin{aligned} \text{Hom}_R(G, \chi_{(2)})(\text{Hom}_R(G, \chi_{(1)}(G^{(1)}))) &\subset \text{Hom}_R(G, \chi_{(2)} \circ \chi_{(1)}(G^{(1)})) \\ &\equiv \text{Hom}_R(G, \mathbf{0}) = \{0\}. \end{aligned}$$

Co więcej, jeśli

$$\text{Hom}_R(G, \chi_{(2)})(\psi) \equiv \chi_{(2)} \circ \psi = 0$$

dla pewnego $\psi \in \text{Hom}_R(G, \sigma(G^{(3)}))$, to koniecznie $\psi = 0$, gdyż każdemu $g \in G$ możemy przyporządkować $h \in G^{(3)}$ o własności $\psi(g) = \sigma(h)$, a wtedy na podstawie rachunku

$$0_{(3)} = \chi_{(2)} \circ \psi(g) = \chi_{(2)} \circ \sigma(h) = h$$

stwierdzamy, że

$$\psi(g) = \sigma(0_{(3)}) = 0_{(2)},$$

co wobec dowolności g daje $\psi = 0$ i pokazuje injektywność $\text{Hom}_R(G, \chi_{(2)})$ ograniczonego do $\text{Hom}_R(G, \sigma(G^{(3)}))$. W takiej sytuacji wystarczy zatem pokazać, że $\text{Hom}_R(G, \chi_{(1)})$ zadaje izomorfizm

$$\text{Hom}_R(G, \chi_{(1)}) : \text{Hom}_R(G, G^{(1)}) \xrightarrow{\cong} \text{Hom}_R(G, \chi_{(1)}(G^{(1)})),$$

to jednak wynika wprost z injektywności $\chi_{(1)}$, która pozwala odwrócić to odwzorowanie na jego obrazie, tj. zdefiniować $\chi_{(1)}^{-1} \text{Im} : \text{Im } \chi_{(1)} \rightarrow G^{(1)}$, i wypisać homomorfizm odwrotny do powyższego,

$$\text{Hom}_R(G, \chi_{(1)}^{-1} \text{Im}) : \text{Hom}_R(G, \chi_{(1)}(G^{(1)})) \xrightarrow{\cong} \text{Hom}_R(G, G^{(1)}).$$

$\Leftarrow$ W świetle Tw. 8.15 jedynym, czego należy dowieść dla potwierdzenia dokładności ciągu modułów, jest surjektywność $\chi_{(2)}$. Rozważmy $G := G^{(3)}$ oraz $\text{id}_{G^{(3)}} \in \text{Hom}_R(G^{(3)}, G^{(3)})$. Wykorzystując surjektywność $\text{Hom}_R(G, \chi_{(2)})$, dobieramy $\psi \in \text{Hom}_R(G^{(3)}, G^{(2)})$, które zadaje rozkład $\text{id}_{G^{(3)}} = \chi_{(2)} \circ \psi$, ten zaś prowadzi do oczekiwanego wniosku $G^{(3)} = \text{Im } \text{id}_{G^{(3)}} \subset$

Im $\chi_{(2)}$. Odwzorowanie ψ jest przy tym – wprost z konstrukcji – ciągiem liniowym stowarzyszonym z $\chi_{(2)}$, którego istnienie zapewnia pożądane rozszczepienie ciągu modułów.

□

Wyróżniona pozycja przestrzeni wektorowych pośród modułów pozwala wypowiedzieć, w charakterze oczywistego corollarium do twierdzeń wcześniejszych,

TWIERDZENIE 8.16 (O dokładności $\text{Hom}_{\mathbb{K}}$). *Przyjmijmy notację Def. 11, 21, 32, 35, 43, 61, 63, 65, 94, 95 i 100, Stw. 94 oraz Przykł. 46 (2). Niechaj $V^{(\alpha)}$, $\alpha \in \{1, 2, 3\}$ będą trzema przestrzeniami wektorowymi nad ciałem $\mathbb{K}$ i niech $\chi_{(\beta)} : V^{(\beta)} \rightarrow V^{(\beta+1)}$, $\beta \in \{1, 2\}$ będą dwoma odwzorowaniami $\mathbb{K}$ -liniowymi między nimi. Ileż ciąg przestrzeni wektorowych*

$$0 \rightarrow V^{(1)} \xrightarrow{\chi_{(1)}} V^{(2)} \xrightarrow{\chi_{(2)}} V^{(3)} \rightarrow 0$$

jest dokładny, odnośnie ciągów grup odwzorowań $\mathbb{K}$ -liniowych

$$\begin{aligned} 0 \rightarrow \text{Hom}_{\mathbb{K}}(V^{(3)}, V) &\xrightarrow{\text{Hom}_{\mathbb{K}}(\chi_{(2)}, V)} \text{Hom}_{\mathbb{K}}(V^{(2)}, V) \\ &\xrightarrow{\text{Hom}_{\mathbb{K}}(\chi_{(1)}, V)} \text{Hom}_{\mathbb{K}}(V^{(1)}, V) \rightarrow 0, \end{aligned}$$

$$\begin{aligned} 0 \rightarrow \text{Hom}_{\mathbb{K}}(V, V^{(1)}) &\xrightarrow{\text{Hom}_{\mathbb{K}}(V, \chi_{(1)})} \text{Hom}_{\mathbb{K}}(V, V^{(2)}) \\ &\xrightarrow{\text{Hom}_{\mathbb{K}}(V, \chi_{(2)})} \text{Hom}_{\mathbb{K}}(V, V^{(3)}) \rightarrow 0, \end{aligned}$$

zapisane dla dowolnej przestrzeni wektorowej V nad $\mathbb{K}$, są dokładne i rozszczepione.

W szczególności dokładność powyższego ciągu przestrzeni wektorowych implikuje dokładność i rozszczepialność ciągu przestrzeni sprzężonych

$$0 \rightarrow V^{(3)*} \xrightarrow{\chi_{(2)}^*} V^{(2)*} \xrightarrow{\chi_{(1)}^*} V^{(1)*} \rightarrow 0.$$

■

Dowód: Treść twierdzenia jest natychmiastową konsekwencją analogicznych twierdzeń dotyczących modułów ogólnych oraz Stw. 90 rozpatrywanego w połączeniu z Tw. 8.5. □

Wykorzystamy obecnie twierdzenia udowodnione w tej części wykładu do dalszego poszerzenia i uporządkowania naszej wiedzy o algebraicznej naturze operacji sprzężenia. Zaczniemy od jej zbadania w odniesieniu do konstrukcji modułu ilorazowego.

STWIERDZENIE 136. *Przyjmijmy notację Def. 11, 21, 32, 34, 35, 38, 42, 43, 61, 63, 64, 65, 94, 95, 98 i 100, Stw. 40 i 94 oraz Przykł. 34 (2) i 46 (2). Niechaj*

G będzie modulem (lewostronnym) nad pierścieniem R i niech $H \subset G$ będzie jego podmodulem. Wówczas odwzorowanie R -liniowe

$$\pi_{G/H}^* : (G/H)^* \longrightarrow G^*$$

indukuje izomorfizm

$$(G/H)^* \cong H^0,$$

natomiast odwzorowanie R -liniowe

$$j_H^* : G^* \longrightarrow H^*$$

indukuje monomorfizm

$$G^*/H^0 \twoheadrightarrow H^*.$$

Ten ostatni jest izomorfizmem, gdy $R = \mathbb{K}$ jest ciałem. ■

Dowód: Dokładność ciągu modułów

$$H \xrightarrow{j_H} G \xrightarrow{\pi_{G/H}} G/H \longrightarrow \mathbf{0},$$

otrzymanego przez obcięcie odnośnego normalnego ciągu dokładnego, implikuje – w świetle Tw. 8.14 – dokładność ciągu grup

$$\mathbf{0} \longrightarrow (G/H)^* \xrightarrow{\pi_{G/H}^*} G^* \xrightarrow{j_H^*} H^*,$$

skąd wnioskujemy o iniektywności homomorfizmu grup

$$\pi_{G/H}^* : (G/H)^* \longrightarrow G^*,$$

a zatem – wobec Stw. 1 – także o istnieniu izomorfizmu grup

$$(G/H)^* \cong \text{Im } \pi_{G/H}^* = \text{Ker } j_H^*.$$

Przywoławszy tezę Stw. 132, otrzymujemy żądany izomorfizm

$$(G/H)^* \cong \text{Ker } j_H^* \cong H^0.$$

Ten sam indukowany ciąg grup homomorfizmów daje nam homomorfizm grup

$$j_H^* : G^* \longrightarrow H^*$$

o jądrze $\text{Ker } j_H^* \cong H^0$, a więc też monomorfizm grup

$$\widetilde{j_H^*} : G^*/H^0 \twoheadrightarrow H^*.$$

Przedłużając rzeczony ciąg grup homomorfizmów do pełnego krótkiego ciągu dokładnego w przypadku przestrzeni wektorowych, zgodnie z Tw. 8.16, uzyskujemy w ten sposób izomorfizm grup funkcjonałów liniowych nad ciałem $\mathbb{K}$. □

W następnym kroku, skupiając uwagę po raz kolejny na przestrzeniach wektorowych, znajdujemy prosty opis tych spośród nich, które są w naturalny sposób wyróżnione w obecności odwzorowania $\mathbb{K}$ -liniowego. Instrumentalną rolę w tworzeniu tego opisu odgrywają stowarzyszone z rzeczonymi przestrzeniami krótkie ciągi dokładne.

STWIERDZENIE 137. *Przyjmijmy notację Def. 11, 21, 32, 34, 35, 36, 42, 61, 63, 64, 65, 66, 94, 95, 98 i 100, Stw. 40 i 94 oraz Przykł. 34 (2) i 46 (2). Niechaj $V^{(\alpha)}$, $\alpha \in \{1, 2\}$ będą dwiema przestrzeniami wektorowymi nad ciałem $\mathbb{K}$ i niech $\chi : V^{(1)} \rightarrow V^{(2)}$ będzie odwzorowaniem $\mathbb{K}$ -liniowym. Istnieją izomorfizmy kanoniczne*

- (i) $(\operatorname{Im} \chi)^* \cong \operatorname{Im} \chi^*$;
- (ii) $(\operatorname{Ker} \chi)^* \cong \operatorname{Coker} \chi^*$;
- (iii) $(\operatorname{Coker} \chi)^* \cong \operatorname{Ker} \chi^*$;

W szczególności χ jest monomorfizmem (wzgl. epimorfizmem) wtedy i tylko wtedy, gdy χ^ jest epimorfizmem (wzgl. monomorfizmem).*

Ponadto spełniona jest nierówność

$$\operatorname{rk} \chi \leq \operatorname{rk} \chi^*,$$

która przechodzi w równość, gdy $\operatorname{rk} \chi < \infty$.

■

Dowód: Rozważmy parę krótkich ciągów dokładnych przestrzeni wektorowych

$$0 \rightarrow \operatorname{Ker} \chi \xrightarrow{J_{\operatorname{Ker} \chi}} V^{(1)} \xrightarrow{\tilde{\chi}} \operatorname{Im} \chi \rightarrow 0,$$

$$0 \rightarrow \operatorname{Im} \chi \xrightarrow{J_{\operatorname{Im} \chi}} V^{(2)} \xrightarrow{\pi_{V^{(2)}/\operatorname{Im} \chi}} \operatorname{Coker} \chi \rightarrow 0,$$

zapisanych przy użyciu odwzorowania $\mathbb{K}$ -liniowego $\tilde{\chi}$ otrzymanego z χ przez ograniczenie przeciwdziedziny i spełniającego tożsamość

$$(8.38) \quad \chi = J_{\operatorname{Im} \chi} \circ \tilde{\chi},$$

Na mocy Tw. 8.16 powyższe ciągi indukują krótkie ciągi dokładne przestrzeni sprzężonych

$$0 \rightarrow (\operatorname{Im} \chi)^* \xrightarrow{\tilde{\chi}^*} V^{(1)*} \xrightarrow{J_{\operatorname{Ker} \chi}^*} (\operatorname{Ker} \chi)^* \rightarrow 0,$$

$$0 \rightarrow (\operatorname{Coker} \chi)^* \xrightarrow{\pi_{V^{(2)}/\operatorname{Im} \chi}^*} V^{(2)*} \xrightarrow{J_{\operatorname{Im} \chi}^*} (\operatorname{Im} \chi)^* \rightarrow 0.$$

Z tych ostatnich odczytujemy wprost następujące izomorfizmy kanoniczne: wobec injektywności $\tilde{\chi}^*$,

$$(\operatorname{Im} \chi)^* \cong \operatorname{Im} \tilde{\chi}^*;$$

wobec surjektywności $J_{\operatorname{Ker} \chi}^*$,

$$(\operatorname{Ker} \chi)^* \cong V^{(1)*} / \operatorname{Ker} J_{\operatorname{Ker} \chi}^* = V^{(1)*} / \operatorname{Im} \tilde{\chi}^*;$$

wobec injektywności $\pi_{V^{(2)}/\operatorname{Im} \chi}^*$,

$$(\operatorname{Coker} \chi)^* \cong \operatorname{Im} \pi_{V^{(2)}/\operatorname{Im} \chi}^* = \operatorname{Ker} J_{\operatorname{Im} \chi}^*.$$

Izomorfizmy te sprowadzamy do pożądanej postaci na podstawie równości

$$\operatorname{Ker} J_{\operatorname{Im} \chi}^* = \operatorname{Ker} \chi^*$$

oraz

$$\operatorname{Im} \tilde{\chi}^* = \operatorname{Im} \chi^*,$$

wynikających z tożsamości

$$\chi^* = \widetilde{\chi}^* \circ J_{\text{Im } \chi}^*$$

dualnej do Równ. (8.38) oraz – odpowiednio – injektywności $\widetilde{\chi}^*$ i surjektywności $J_{\text{Im } \chi}^*$.

I wreszcie bez trudu wyprowadzamy nierówność

$$\text{rk } \chi \equiv \dim_{\mathbb{K}} \text{Im } \chi \leq \dim_{\mathbb{K}} (\text{Im } \chi)^* = \dim_{\mathbb{K}} \text{Im } \widetilde{\chi}^* = \dim_{\mathbb{K}} \text{Im } \chi^* \equiv \text{rk } \chi^*,$$

która zostaje wysycona w przypadku skończenia wymiarowym. $\square$

Na zakończenie tej części naszych rozważań możemy wysłowić prosty a ogólny wniosek porządkujący, który przekonuje nas o powszechności struktury anihilatora wśród przestrzeni wektorowych.

STWIERDZENIE 138. *Przyjmijmy notację Def. 11, 21, 32, 34, 35, 42, 61, 63, 64, 65, 94 i 95, Stw. 94 oraz Przykł. 34 (2) i 46 (2). Niechaj V będzie przestrzenią wektorową nad ciałem $\mathbb{K}$. Dowolna skończenie wymiarowa podprzestrzeń $W \subset V^*$ jest anihilatorem pewnej podprzestrzeni $U \subset V$, przy czym ta ostatnia ma kowymiar skończony i jest anihilatorem W w V .*

■

Dowód: W skończenie wymiarowej podprzestrzeni wektorowej $W \subset V^*$ wybierzmy bazę $\{w_i\}_{i \in \overline{1, p}}$ i rozważmy anihilator $W^0 \subset V$. Wprost z definicji podprzestrzeni ta jest jądrem odwzorowania $\mathbb{K}$ -liniowego

$$\nu : V \longrightarrow \mathbb{K}^p : v \longmapsto (\langle v, w_i \rangle)_{i \in \overline{1, p}},$$

a w takim razie

$$V/W^0 \equiv V/\text{Ker } \nu \cong \text{Im } \nu,$$

czyli też

$$\text{codim}_{\mathbb{K}}^{(V)} W^0 = \dim_{\mathbb{K}} \text{Im } \nu \equiv \text{rk } \nu.$$

Jednakowoż, jak pokazuje bilans wymiarów ze Stw. 103 (i), zachodzi nierówność

$$\text{rk } \nu \leq \dim_{\mathbb{K}} \mathbb{K}^p = p < \infty,$$

więc także

$$\text{codim}_{\mathbb{K}}^{(V)} W^0 \leq p < \infty.$$

W następnej kolejności rozpatrzmy anihilator $(W^0)^0 \equiv W^{00} \subset V^*$ podprzestrzeni $W^0 \subset V$. Na mocy Stw. 136 istnieje izomorfizm

$$W^{00} \cong (V/W^0)^*,$$

który w świetle Stw. 82 i 122 pozwala wypisać nierówność

$$\dim_{\mathbb{K}} W^{00} = \dim_{\mathbb{K}} (V/W^0)^* \geq \dim_{\mathbb{K}} (V/W^0) \equiv \text{codim}_{\mathbb{K}}^{(V)} W^0.$$

Nierówność ta jest wysycona wobec uzasadnionej wcześniej skończoności kowymiaru W^0 , a zatem

$$\dim_{\mathbb{K}} W^{00} = \text{codim}_{\mathbb{K}}^{(V)} W^0 \leq p = \dim_{\mathbb{K}} W.$$

Z drugiej strony mamy do czynienia z inkluzją

$$W \subset W^{00},$$

czyli ostatecznie musi zachodzić równość

$$W = W^{00},$$

która pokazuje, że przestrzeń W jest anihilatorem zdefiniowanej wyżej przestrzeni W^0 skończonego kowymiaru $\operatorname{codim}_{\mathbf{K}}^{(V)} W^0 \leq p$. $\square$

8.11. Moduł i odwzorowanie dwukrotnie sprzężone

Dwuliniowy charakter formy ewaluacji pozwala określić naturalną relację między dowolnym R -modułem G i modułem dwukrotnie doń sprzężonym, oto bowiem odwzorowanie

$$G^* \longrightarrow R : \varphi \longmapsto \langle g, \varphi \rangle,$$

zapisane dla ustalonego (dowolnie) $g \in G$, jest formą liniową na G^* , tj. elementem modułu $(G^*)^*$.

DEFINICJA 101. Przyjmijmy notację Def. 21, 32, 35, 61, 65, 70, 94 i 95 oraz Przykł. 34 (2) i 46 (2). Niechaj G będzie dowolnym R -modułem lewostronnym. **Moduł dwukrotnie sprzężony do G** to R -moduł *lewostronny*

$$G^{**} \equiv (G^*)^* = \operatorname{Hom}_R(G^*, R_R).$$

Odwzorowanie R -liniowe

$$c_G \equiv l_{\text{ev}} : G \longrightarrow G^{**} : g \longmapsto \langle g, \cdot \rangle$$

określamy mianem **homomorfizmu kanonicznego**. ▲

Godzi się podkreślić, że w ogólności c_G nie jest ani monomorfizmem, ani epimorfizmem, nawet w klasie modułów skończenie generowanych. Obserwacja ta usprawiedliwia wyszczególnienie

DEFINICJA 102. Przyjmijmy notację Def. 21, 32, 35, 61, 65, 70, 94, 95 i 101 oraz Przykł. 34 (2) i 46 (2). Moduł G nad pierścieniem R nazywamy **refleksywnym**, jeśli homomorfizm kanoniczny $c_G : G \longrightarrow G^{**}$ jest izomorfizmem. ▲

Operacja brania dwukrotnego sprzężenia rozszerza się do odwzorowań R -liniowych, co konstatuje poniższe oczywiste

STWIERDZENIE 139. *Przyjmijmy notację Def. 21, 32, 35, 61, 65, 70, 94, 101 i 100, Stw. 94 oraz Przykł. 34 (2) i 46 (2). Odwzorowanie*

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

jest homomorfizmem R -modułów lewostronnych spełniającym tożsamość wyrażoną przez diagram przemienny i równoważne zdanie logiczne

$$\begin{array}{ccc}
 G^{(1)} & \xrightarrow{\chi} & G^{(2)} \\
 \downarrow c_{G^{(1)}} & & \downarrow c_{G^{(2)}} \\
 G^{(1)*} & \xrightarrow{\chi^{**}} & G^{(2)*}
 \end{array} \quad \equiv \quad \chi^{**} \circ c_{G^{(1)}} = c_{G^{(2)}} \circ \chi.$$

■

Dowód: Jedynym faktem wymagającym sprawdzenia jest przemiennosc wypisanego diagramu. Biorąc dowolne elementy $g \in G^{(1)}$ i $\varphi \in G^{(2)*}$, otrzymujemy

$$\begin{aligned}
 (\chi^{**} \circ c_{G^{(1)}}(g))(\varphi) &= (c_{G^{(1)}}(g))(\chi^*(\varphi)) \equiv \langle g, \chi^*(\varphi) \rangle = \langle \chi(g), \varphi \rangle \\
 &= (c_{G^{(2)}} \circ \chi(g))(\varphi).
 \end{aligned}$$

□

Pemniejsze zrozumienie relacji między obiektami algebraicznymi i ich dwukrotnie sprzężonymi odpowiednikami jest możliwe w obecności dodatkowej struktury, takiej jak choćby struktura bazy na module. Jej dyskusja w kontekście relacji dwiistości, której poświęcimy najbliższy fragment wykładu, doprowadzi nas – między innymi – do elementarnej kwantyfikacji warunków refleksywności modułu tudzież przestrzeni wektorowej oraz involutywności operacji brania sprzężenia określonej na odwzorowaniach liniowych, a ponadto pozwoli dowolnemu endomorfizmowi przypisać w sposób kanoniczny kolejny (po wyznaczniku) element pierścienia skalarów.

8.12. Formy współrzędniowe i bazy (wzajem) dualne

Jak mieliśmy to już niejednokrotnie okazję docenić, obecność bazy w module pozwala na uzyskanie dodatkowego strukturalnego wglądu w jego algebraiczną anatomię. Nie inaczej jest w kontekście konstrukcji modułu sprzężonego.

STWIERDZENIE 140. *Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 70, 68, 70 i 94, Stw. 75 oraz Przykł. 40 (3) i 46 (2). Niechaj G będzie lewostronnym modulem wolnym nad pierścieniem R , o bazie $\mathcal{B} = \{g_\lambda\}_{\lambda \in \Lambda}$. W module G^* doń sprzężonym istnieje układ liniowo niezależny $\mathcal{B}^* := \{g_\lambda^*\}_{\lambda \in \Lambda}$ o własności*

$$\forall_{\lambda, \mu \in \Lambda} : \langle g_\lambda, g_\mu^* \rangle = \delta_{\lambda, \mu}^R.$$

*Jego elementy określamy mianem **form współrzędniowych** (lub **współrzędnych**) na G względem $\mathcal{B}$. Jeśli $|\Lambda| < \infty$, to $\mathcal{B}^*$ jest bazą modułu sprzężonego, zwaną **bazą dualną do $\mathcal{B}$** .*

■

Dowód: Wprowadźmy wygodne oznaczenie dla izomorfizmu

$$\chi_{\mathcal{B}} \equiv \rho_{\mathcal{B}}^{-1} : \bigoplus_{\lambda \in \Lambda} {}_R R \xrightarrow{\cong} G$$

zadawanego przez wybór bazy $\mathcal{B} = \{g_\lambda\}_{\lambda \in \Lambda}$ w R -module (lewostronnym) G , por. Tw. 8.11. Jak łatwo widać, zachodzi

$$g_\lambda = \chi_{\mathcal{B}}(d_\lambda),$$

gdzie

$$d_\lambda : \Lambda \longrightarrow R : \mu \longmapsto \delta_{\lambda, \mu}^R.$$

Oznaczmy przez δ_μ odwzorowania określone przez te same warunki, ale traktowane jako elementy $\prod_{\lambda \in \Lambda} R$. I wreszcie niech $\tilde{\delta}_\mu$ będzie obrazem odwzorowania δ_μ względem kanonicznego izomorfizmu $\prod_{\lambda \in \Lambda} R \xrightarrow{\cong} (\bigoplus_{\lambda \in \Lambda} {}_R R)^*$. Wówczas formy

$$g_\lambda^* := \tilde{\chi}_{\mathcal{B}}(\tilde{\delta}_\lambda)$$

spełniają na mocy Równ. (8.34) pożądane warunki

$$\langle g_\lambda, g_\mu^* \rangle \equiv \langle \chi_{\mathcal{B}}(d_\lambda), \tilde{\chi}_{\mathcal{B}}(\tilde{\delta}_\mu) \rangle = \langle d_\lambda, \tilde{\delta}_\mu \rangle = \delta_{\lambda, \mu}^R.$$

W szczególności więc układ $\mathcal{B}^*$ jest liniowo niezależny. Istotnie, niech $\{r^\lambda\}_{\lambda \in \Lambda} \in \mathcal{B}_0(R)$, a wtedy równość

$$\sum_{\lambda \in \Lambda} g_\lambda^* \triangleleft r^\lambda = 0$$

implikuje – dla dowolnego $\mu \in \Lambda$ –

$$0_R = \langle g_\mu, 0 \rangle = \left\langle g_\mu, \sum_{\lambda \in \Lambda} g_\lambda^* \triangleleft r^\lambda \right\rangle = \sum_{\lambda \in \Lambda} \langle g_\mu, g_\lambda^* \rangle \cdot_R r^\lambda = \sum_{\lambda \in \Lambda} \delta_{\mu, \lambda}^R \cdot_R r^\lambda = r^\mu.$$

□

Nazwę nadaną formom g_λ^* wyjaśnia

COROLLARIUM 19. *Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 70, 68, 70 i 94, Stw. 75 i 140 oraz Przykł. 40 (3) i 46 (2). Dowolny element $g \in G$ można zapisać w postaci¹⁹*

$$g = \sum_{\lambda \in \Lambda} \langle g, g_\lambda^* \rangle \triangleright g_\lambda.$$

Jeśli $|\Lambda| < \infty$, to dla dowolnej formy $\varphi \in G^*$ zachodzi formuła dualna

$$\varphi = \sum_{\lambda \in \Lambda} g_\lambda^* \triangleleft \langle g_\lambda, \varphi \rangle.$$

■

Obecność bazy dualnej pozwala ustalić macierzową realizację operacji sprzężenia odwzorowania R -liniowego.

STWIERDZENIE 141. *Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 68, 70, 75, 78, 82, 90, 94, 95 i 100, Cor. 14, Stw. 70, 75, 94, 95, 96, 97, 98, 99, 100 i 140, Tw. 8.11 oraz Przykł. 40 (3), 41 i 46 (2). Niechaj $G^{(\alpha)}$, $\alpha \in \{1, 2\}$ będą dwoma skończeniem generowanymi R -modułami lewostronnymi, o bazach $\mathcal{B}^{(\alpha)} = \{g_{(\alpha|\lambda_a)}\}_{\lambda_a \in \Lambda_\alpha}$, odpowiednio, oraz o dualnych do nich bazach $\mathcal{B}^{(\alpha)*} = \{g_{(\alpha|\lambda_a)}^*\}_{\lambda_a \in \Lambda_\alpha}$*

¹⁹Skończoność sumy jest zagwarantowana przez skończoność nośnika rodziny $\{r^\lambda\}_{\lambda \in \Lambda}$ współczynników $r^\lambda = \langle g, g_\lambda^* \rangle$ rozkładu g w bazie $\mathcal{B}$.

modułów sprzężonych $G^{(\alpha)*}$. Niech też $\chi \in \text{Hom}_R(G^{(1)}, G^{(2)})$ będzie (lewostronnym) odwzorowaniem R -liniowym określonym przez obraz bazy,

$$\chi(g_{(1|\lambda_1)}) = \sum_{\mu_2 \in \Lambda_2} \chi_{\lambda_1}^{\mu_2} \triangleright_{(2)} g_{(2|\mu_2)},$$

z którego odczytujemy postać jego macierzy

$$[\chi]_{\mathcal{B}^{(1)}}^{\mathcal{B}^{(2)}} : \Lambda_2 \times \Lambda_1 \longrightarrow R : (\mu_2, \lambda_1) \longmapsto \chi_{\lambda_1}^{\mu_2}.$$

Analogicznie, niech $\chi^* \in \text{Hom}_R(G^{(2)*}, G^{(1)*})$ będzie odwzorowaniem sprzężonym do χ zadany na bazie wzorami

$$\chi^*(g_{(2|\mu_2)}) = \sum_{\lambda_1 \in \Lambda_2} g_{(1|\lambda_1)}^* \triangleleft \chi_{\mu_2}^{\lambda_1},$$

z których wyprowadzamy postać jego macierzy

$$[\chi^*]_{\mathcal{B}^{(2)*}}^{\mathcal{B}^{(1)*}} : \Lambda_1 \times \Lambda_2 \longrightarrow R : (\lambda_1, \mu_2) \longmapsto \chi_{\mu_2}^{\lambda_1}.$$

Spełnione są tożsamości

$$\begin{aligned} [\chi]_{\mathcal{B}^{(1)}}^{\mathcal{B}^{(2)}}(\mu_2, \lambda_1) &= \langle \chi(g_{(1|\lambda_1)}), g_{(2|\mu_2)}^* \rangle_{(2)}, \\ [\chi^*]_{\mathcal{B}^{(2)*}}^{\mathcal{B}^{(1)*}}(\lambda_1, \mu_2) &= \langle g_{(1|\lambda_1)}^*, \chi^*(g_{(2|\mu_2)}) \rangle_{(1)}, \end{aligned}$$

a ponadto

$$[\chi^*]_{\mathcal{B}^{(2)*}}^{\mathcal{B}^{(1)*}} = [\chi]_{\mathcal{B}^{(1)}}^{\mathcal{B}^{(2)}}{}^T.$$

W szczególności niechaj $G := G^{(1)} \equiv G^{(2)}$ będzie skończenie generowanym modulem nad pierścieniem przemiennym R , o bazach $\mathcal{B} := \{g_n\}_{n \in \overline{1, N}}$, $N \in \mathbb{N}$ i $\mathcal{B}' := \{h_n\}_{n \in \overline{1, N}}$, i niech $\mathcal{B}^* := \{g_n^*\}_{n \in \overline{1, N}}$ oraz $\mathcal{B}'^* := \{h_n^*\}_{n \in \overline{1, N}}$ będą bazami modułu sprzężonego G^* dualnymi do – odpowiednio – $\mathcal{B}$ i $\mathcal{B}'$. Wówczas macierze przejścia $[\text{id}_G]_{\mathcal{B}'}^{\mathcal{B}}$ i $[\text{id}_{G^*}]_{\mathcal{B}'^*}^{\mathcal{B}^*}$, dane wzorami

$$\begin{aligned} [\text{id}_G]_{\mathcal{B}'}^{\mathcal{B}} &: \overline{1, N} \times \overline{1, N} \longrightarrow R : (m, n) \longmapsto \langle h_n, g_m^* \rangle, \\ [\text{id}_{G^*}]_{\mathcal{B}'^*}^{\mathcal{B}^*} &: \overline{1, N} \times \overline{1, N} \longrightarrow R : (m, n) \longmapsto \langle g_m, h_n^* \rangle, \end{aligned}$$

spełniają relację

$$[\text{id}_{G^*}]_{\mathcal{B}'^*}^{\mathcal{B}^*} = ([\text{id}_G]_{\mathcal{B}'}^{\mathcal{B}})^{-1}{}^T.$$

■

Dowód: W bezpośrednim rachunku wyznaczamy

$$\begin{aligned} \langle \chi(g_{(1|\lambda_1)}), g_{(2|\mu_2)}^* \rangle_{(2)} &= \left\langle \sum_{\nu_2 \in \Lambda_2} [\chi]_{\mathcal{B}^{(1)}}^{\mathcal{B}^{(2)}}(\nu_2, \lambda_1) \triangleright_{(2)} g_{(2|\nu_2)}, g_{(2|\mu_2)}^* \right\rangle_{(2)} \\ &= \sum_{\nu_2 \in \Lambda_2} [\chi]_{\mathcal{B}^{(1)}}^{\mathcal{B}^{(2)}}(\nu_2, \lambda_1) \cdot_R \langle g_{(2|\nu_2)}, g_{(2|\mu_2)}^* \rangle_{(2)} \\ &= \sum_{\nu_2 \in \Lambda_2} [\chi]_{\mathcal{B}^{(1)}}^{\mathcal{B}^{(2)}}(\nu_2, \lambda_1) \cdot_R \delta_{\nu_2, \mu_2}^R = [\chi]_{\mathcal{B}^{(1)}}^{\mathcal{B}^{(2)}}(\mu_2, \lambda_1) \end{aligned}$$

oraz

$$\begin{aligned}
 \langle g_{(1|\lambda_1)}, \chi^*(g_{(2|\mu_2)}) \rangle_{(1)} &= \left\langle g_{(1|\lambda_1)}, \sum_{\nu_1 \in \Lambda_1} g_{(1|\nu_1)} \triangleleft_{(1)} [\chi^*]_{\mathcal{B}^{(2)*}}^{(1)*}(\nu_1, \mu_2) \right\rangle_{(1)} \\
 &= \sum_{\nu_1 \in \Lambda_1} \langle g_{(1|\lambda_1)}, g_{(1|\nu_1)} \rangle_{(1)} \cdot_R [\chi^*]_{\mathcal{B}^{(2)*}}^{(1)*}(\nu_1, \mu_2) \\
 &= \sum_{\nu_1 \in \Lambda_1} \delta_{\lambda_1, \nu_1}^R \cdot_R [\chi^*]_{\mathcal{B}^{(2)*}}^{(1)*}(\nu_1, \mu_2) = [\chi^*]_{\mathcal{B}^{(2)*}}^{(1)*}(\lambda_1, \mu_2),
 \end{aligned}$$

więc też

$$\begin{aligned}
 [\chi^*]_{\mathcal{B}^{(2)*}}^{(1)*}(\lambda_1, \mu_2) &= \langle g_{(1|\lambda_1)}, \chi^*(g_{(2|\mu_2)}) \rangle = \langle \chi(g_{(1|\lambda_1)}), g_{(2|\mu_2)} \rangle = [\chi]_{\mathcal{B}^{(1)}}^{(2)}(\mu_2, \lambda_1) \\
 &\equiv [\chi]_{\mathcal{B}^{(1)}}^{(2)T}(\lambda_1, \mu_2).
 \end{aligned}$$

Na tej podstawie i na mocy Stw. 131 otrzymujemy na koniec

$$[\text{id}_G^*]_{\mathcal{B}'*}^{\mathcal{B}*} = [\text{id}_G^*]_{\mathcal{B}'*}^{\mathcal{B}*} = [\text{id}_G]_{\mathcal{B}}^{\mathcal{B}'T} = ([\text{id}_G]_{\mathcal{B}'}^{\mathcal{B}-1})^T.$$

□

Jak zatem widzimy, macierzową realizacją operacji sprzężenia odwzorowania R -liniowego jest transpozycja, wprowadzona wcześniej – cokolwiek *ad hoc* – na potrzeby dyskusji teorii wyznaczników.

Istnienie homomorfizmu $c_G : G \rightarrow G^{**}$ rodzi pytanie o okoliczności, w których odwzorowanie to pozwala nam kanonicznie utożsamić moduł G z podmodułem G^{**} (gdy c_G jest monomorfizmem) lub wręcz myśleć o funkcjonalach na module sprzężonym jako ewaluacjach form R -liniowych na module G na elementach tego ostatniego (ilekroć c_G jest izomorfizmem). Prostej (częściowej) odpowiedzi na to całkowicie naturalne pytanie dostarcza

STWIERDZENIE 142. *Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 70, 68, 70, 94, 95 i 101, Stw. 75 i 140 oraz Przykł. 34 (2), 40 (3) i 46 (2). Niechaj G będzie modułem lewostronnym nad pierścieniem R . Jeśli G jest wolny, to homomorfizm kanoniczny $c_G : G \rightarrow G^{**}$ jest iniektywny. Jeśli ponadto G ma bazę skończoną $\mathcal{B} := \{g_i\}_{i \in \overline{1, N}}$, to c_G jest izomorfizmem modułów, przy czym $c_G(\mathcal{B}) = \{c_G(g_i)\}_{i \in \overline{1, N}}$ jest bazą dualną do bazy $\mathcal{B}^* := \{g_i^*\}_{i \in \overline{1, N}}$ dualnej do $\mathcal{B}$. W tej sytuacji mówimy, że bazy $\mathcal{B}$ i $\mathcal{B}^*$ są **wzajem dualne**. Co więcej, każda skończona baza G^* jest bazą dualną do pewnej bazy G .*

■

Dowód: Niechaj $\mathcal{B} := \{g_\lambda\}_{\lambda \in \Lambda}$ będzie bazą G i niech $\mathcal{B}^* := \{g_\lambda^*\}_{\lambda \in \Lambda}$ będzie odnośną rodziną form współrzędniowych na G . Ilekroć $c_G(g) = 0$ dla pewnego elementu $g \in G$, zachodzą równości

$$\forall_{\lambda \in \Lambda} : 0 = c_G(g)(g_\lambda^*) \equiv \langle g, g_\lambda^* \rangle,$$

czyli wszystkie współczynniki rozkładu g w bazie $\mathcal{B}$ są równe zeru, to zaś oznacza, że $g = 0_G$.

Niech teraz $|\Lambda| =: N < \infty$, a wtedy $\mathcal{B}^*$ jest bazą G^* na mocy Stw. 140. Formy liniowe $g_\lambda^{**} := c_G(g_\lambda)$ spełniają założenia tegoż twierdzenia w odniesieniu do elementów bazy $\mathcal{B}^*$,

$$\forall_{\lambda, \mu \in \Lambda} : g_\lambda^{**}(g_\mu^*) \equiv \langle g_\lambda, g_\mu^* \rangle = \delta_{\lambda, \mu}^R,$$

przeto tworzą bazę modułu G^{**} dualną do $\mathcal{B}^*$. Skoro jednak c_G przeprowadza bazę G na bazę G^{**} , to w świetle Cor. 10 jest izomorfizmem tych modułów.

Ażeby przekonać się o słuszności ostatniej części tezy dowodzonego stwierdzenia, wystarczy rozpatrzyć bazę G^{**} dualną do danej (skończonej) bazy G^* , po czym odwzorować ją względem c_G^{-1} w bazę G . $\square$

Bijektywność homomorfizmu kanonicznego, kiedykolwiek jest faktem, pozwala w prosty sposób powiązać odwzorowanie dwukrotnie sprzężone do danego z nim samym.

STWIERDZENIE 143. *Przyjmijmy notację Def. 21, 32, 35, 61, 65, 70, 94, 101 i 100, Stw. 94 i 139 oraz Przykł. 34 (2) i 46 (2). Jeśli zarówno moduł $G^{(1)}$, jak i moduł $G^{(2)}$ ma bazę skończoną, to wówczas – utożsamiawszy $G^{(\alpha)**}$, $\alpha \in \{1, 2\}$ z $G^{(\alpha)}$ za pośrednictwem (bijektywnego) homomorfizmu kanonicznego $c_{G^{(\alpha)}}$ – możemy utożsamić odwzorowanie χ^{**} dwukrotnie sprzężone z wyjściowym χ .* $\blacksquare$

Dowód: Teza stwierdzenia wynika wprost z diagramu przemiennej ze Stw. 139. $\square$

Umiejętne wykorzystanie konstrukcji bazy dualnej umożliwia sformułowanie wygodnego warunku liniowej niezależności układu form liniowych na przestrzeni wektorowej, który wyzyskamy w dalszej części kursu.

STWIERDZENIE 144. *Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 70, 68, 70, 75, 77, 82, 87, 89 i 94, Stw. 75 oraz Przykł. 34 (2), 40 (3), 41 i 46 (2). Niechaj V będzie przestrzenią wektorową nad ciałem $\mathbb{K}$ i niech $\mathcal{R}^* := \{v_i^*\}_{i \in \overline{1, N}}$ będzie rodziną form liniowych na V . Wówczas równoważne są następujące stwierdzenia:*

- (i) *Zbiór $\mathcal{R}^*$ jest liniowo niezależny nad $\mathbb{K}$.*
- (ii) *Istnieje rodzina wektorów $\{v_i\}_{i \in \overline{1, N}} \subset V$, której elementy spełniają warunki*

$$\forall_{i, j \in \overline{1, N}} : \langle v_i, v_j^* \rangle = \delta_{i, j}^{\mathbb{K}}.$$

- (iii) *Istnieje taka rodzina wektorów $\{v_i\}_{i \in \overline{1, N}} \subset V$, dla której macierz ewaluacji*

$$M : \overline{1, N} \times \overline{1, N} \longrightarrow \mathbb{K} : (i, j) \longmapsto \langle v_i, v_j^* \rangle$$

spełnia warunek

$$\det_{(N)}(M) \neq 0_{\mathbb{K}}.$$

Powyższa teza zachowuje słuszność, gdy $\mathcal{R}^$ zastąpić rodziną $\mathcal{R} := \{v_i\}_{i \in \overline{1, N}}$ elementów przestrzeni V , a rodzinę wektorów $\{v_i\}_{i \in \overline{1, N}} \subset V$ – rodziną form liniowych $\{v_i^*\}_{i \in \overline{1, N}} \subset V^*$.* $\blacksquare$

Dowód: Ostatnia część tezy staje się oczywista, kiedy utożsamić V z obrazem tejże przestrzeni względem kanonicznego monomorfizmu $c_V : V \longrightarrow V^{**}$. Wystarczy zatem wykazać słuszność punktów (i)-(iii) w odniesieniu do rodziny $\mathcal{R}^* \subset V^*$.

(i) $\Rightarrow$ (ii) Rozważmy podprzestrzeń

$$W_{\mathcal{R}^*} := \langle \mathcal{R}^* \rangle_{\mathbb{K}} \subset V^*$$

oraz jej anihilator $W_{\mathcal{R}^*}^0 \subset V$. W świetle Stw. 138 $W_{\mathcal{R}^*}$ jest anihilatorem podprzestrzeni $W_{\mathcal{R}^*}^0$, co na mocy Stw. 136 implikuje istnienie kanonicznego izomorfizmu

$$(V/W_{\mathcal{R}^*}^0)^* \cong (W_{\mathcal{R}^*}^0)^0 = W_{\mathcal{R}^*}.$$

Skończoność wymiaru przestrzeni $W_{\mathcal{R}^*}$ pozwala na tej podstawie stwierdzić – w odwołaniu do Stw. 142 – istnienie (kanonicznego) izomorfizmu

$$V/W_{\mathcal{R}^*}^0 = (V/W_{\mathcal{R}^*}^0)^{**} \cong W_{\mathcal{R}^*}^*.$$

Skoro rodzina $\mathcal{R}^*$ jest liniowo niezależna, to – przywołując tezę Stw. 140 – możemy wybrać w $V/W_{\mathcal{R}^*}^0$ bazę $\{v_i +_V W_{\mathcal{R}^*}^0\}_{i \in \overline{1, N}}$ dualną do $\mathcal{R}^*$. Dowolny układ $\{v_i\}_{i \in \overline{1, N}}$ reprezentantów $v_i \in v_i +_V W_{\mathcal{R}^*}^0$ elementów tej bazy spełnia równania z punktu (ii).

(ii) $\Rightarrow$ (iii) Trywialne.

(iii) $\Rightarrow$ (i) Załóżmy, że zbiór $\mathcal{R}^*$ jest liniowo zależny, czyli że istnieje rodzina skalarów $\{\lambda^i\}_{i \in \overline{1, N}} \subset \mathbb{K}$ zawierająca choć jeden element niezerowy, która spełnia tożsamość

$$\sum_{j=1}^N v_j^* \triangleleft \lambda^j = 0.$$

Konsekwencją tej ostatniej jest ciąg równości

$$0_{\mathbb{K}} = \langle v_i, 0 \rangle = \left\langle v_i, \sum_{j=1}^N v_j^* \triangleleft \lambda^j \right\rangle = \sum_{j=1}^N \langle v_i, v_j^* \rangle \cdot_{\mathbb{K}} \lambda^j,$$

słusznych dla dowolnego $i \in \overline{1, N}$, który możemy przepisać w zwężłej formie macierzowej

$$M \odot \lambda = \mathbf{0}_{N \times 1}$$

używając oznaczenia

$$\lambda := (\lambda^i)_{i \in \overline{1, N}} \in \text{Mat}(\mathbb{K}; N \times 1).$$

Zgodnie z Tw. 8.13 relacja $\det_{(N)}(M) \neq 0_{\mathbb{K}}$ gwarantuje odwracalność macierzy M , ta zaś prowadzi do równości

$$\lambda = (M^{-1} \odot M) \odot \lambda = M^{-1} \odot \mathbf{0}_{N \times 1} = \mathbf{0}_{N \times 1}.$$

Powyższa równość jest sprzeczna z założeniem dotyczącym rodziny $\{\lambda^i\}_{i \in \overline{1, N}}$.

□

8.13. Ślad endomorfizmu

Obecność bazy w skończenie generowanym module nad pierścieniem przemennym pozwala stowarzyszyć z dowolnym endomorfizmem określonym na tym module kolejny (po wyznaczniku) skalarny niezmiennik wyboru bazy. Jak pokażemy niżej, oba skalary należą do rodziny niezmienników, dla których funkcjonalem generującym jest tzw. wielomian charakterystyczny endomorfizmu. Wszystkie one odegrają ważną rolę w przyszłej szczegółowej dyskusji struktury endomorfizmu.

DEFINICJA 103. Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 68, 70, 94 i 95, Stw. 70, 75, 94, 140 oraz Przykł. 40 (3) i 46 (2). Niechaj G będzie modulem nad pierścieniem przemennym R i niech $\chi \in \text{End}_R(G)$ będzie endomorfizmem G . Niech też $\mathcal{B} := \{g_n\}_{n \in \overline{1, N}}$, $N \in \mathbb{N}$ będzie dowolną bazą w G , a nadto niech $\mathcal{B}^* := \{g_n^*\}_{n \in \overline{1, N}}$ będzie bazą modułu sprzężonego G^* dualną do $\mathcal{B}$. **Ślad endomorfizmu** χ to skalar

$$\text{Tr}_G(\chi) := \sum_{n=1}^N \langle \chi(g_n), g_n^* \rangle \in R.$$

▲

Kierując się przyjętą w niniejszym kursie regułą logiczną, w pierwszym rzędzie ustalamy relację między nowo wprowadzonym obiektem a strukturą algebraiczną istniejącą na zbiorach odwzorowanych przezeń w siebie.

STWIERDZENIE 145. *Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 68, 70, 72, 94, 95 i 103, Stw. 70, 75, 94, 140 oraz Przykł. 40 (3) i 46 (2). Ślad endomorfizmu nie zależy od wyboru bazy w dziedzinie tegoż endomorfizmu. Odwzorowanie $\text{Tr}_G : \text{End}_R(G) \rightarrow R$ jest przy tym homomorfizmem R -modułów, tj. dla dowolnych $\chi_1, \chi_2, \chi \in \text{End}_R(G)$ oraz $r \in R$ są spełnione relacje*

$$\text{Tr}_G(\chi_1 + \chi_2) = \text{Tr}_G(\chi_1) +_R \text{Tr}_G(\chi_2),$$

$$\text{Tr}_G(r \triangleright \chi) = r \cdot_R \text{Tr}_G(\chi),$$

gdzie dla dowolnego $g \in G$ jest

$$(r \triangleright \chi)(g) = r \cdot_R \chi(g).$$

Ponadto zachodzi oczywista tożsamość

$$\text{Tr}_G(\text{id}_G) = \text{rk}_R(G).$$

■

Ograniczenie rozważań do klasy skończenie generowanych modułów wolnych nasuwa pytanie o istnienie prostego związku między śladem endomorfizmu a śladem endomorfizmu doń sprzężonego. Związek ten możemy łatwo ustalić korzystając z konstrukcji baz wzajem dualnych. Wynik tych dociekań wysławia poniższe

STWIERDZENIE 146. *Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 68, 70, 94, 95, 100 i 103, Stw. 70, 75, 94, 140 oraz Przykł. 40 (3) i 46 (2). Dla dowolnego endomorfizmu $\chi \in \text{End}_R(G)$ skończenie generowanego (lewostronnego) modułu wolnego G nad pierścieniem przemennym R zachodzi tożsamość*

$$\text{Tr}_{G^*}(\chi^*) = \text{Tr}_G(\chi).$$

■

Dowód: Wybierzmy w G bazę $\mathcal{B} := \{g_n\}_{n \in \overline{1, N}}$, $N = \text{rk}_R(G)$, w module sprzężonym – bazę dualną $\mathcal{B}^* := \{g_n^*\}_{n \in \overline{1, N}}$, w module zaś dwukrotnie sprzężonym – bazę $c_G(\mathcal{B})$, dualną do $\mathcal{B}^*$. Otrzymujemy wówczas spodziewaną równość

$$\text{Tr}_{G^*}(\chi^*) \equiv \sum_{n=1}^N \langle \chi^*(g_n^*), c_G(g_n) \rangle \equiv \sum_{n=1}^N \langle g_n, \chi^*(g_n^*) \rangle = \sum_{n=1}^N \langle \chi(g_n), g_n^* \rangle \equiv \text{Tr}_G(\chi).$$

□

W następnym kroku przyjrzymy się bliżej strukturze śladu endomorfizmu danego w postaci superpozycji pary odwzorowań R -liniowych, co doprowadzi nas do ustalenia najbardziej bodaj zaskakującej cechy tego niezmiennika, która – jak pokaże dalsza dyskusja – stanowi jego istotny wyróżnik.

STWIERDZENIE 147. *Przyjmijmy notację Def. 67, 21, 32, 35, 61, 65, 68, 70, 94, 95 i 103, Stw. 70, 75, 94, 140 oraz Przykł. 40 (3) i 46 (2). Niechaj $G^{(\alpha)}$, $\alpha \in \{1, 2\}$ będą dwoma skończeniem generowanymi modułami wolnymi nad pierścieniem przemennym R i niech $\chi_{1 \rightarrow 2} \in \text{Hom}_R(G^{(1)}, G^{(2)})$ oraz $\chi_{2 \rightarrow 1} \in \text{Hom}_R(G^{(2)}, G^{(1)})$ będą dwoma dowolnymi odwzorowaniami R -liniowymi. Prawdziwą jest równość*

$$\text{Tr}_{G^{(1)}}(\chi_{2 \rightarrow 1} \circ \chi_{1 \rightarrow 2}) = \text{Tr}_{G^{(2)}}(\chi_{1 \rightarrow 2} \circ \chi_{2 \rightarrow 1}),$$

która wyraża **cykliczność** śladu endomorfizmu.

■

Dowód: Wybierzmy w $G^{(\alpha)}$ i $G^{(\alpha)*}$ bazy wzajem dualne $\mathcal{B}^{(\alpha)} := \{g_{(\alpha|n_\alpha)}\}_{n_\alpha \in \overline{1, N^{(\alpha)}}}$ i $\mathcal{B}^{(\alpha)*} := \{g_{(\alpha|n_\alpha)}^*\}_{n_\alpha \in \overline{1, N^{(\alpha)}}}$, przy czym $N^{(\alpha)} := \text{rk}_R(G^{(\alpha)})$. Obliczamy wówczas

$$\begin{aligned} \text{Tr}_{G^{(1)}}(\chi_{2 \rightarrow 1} \circ \chi_{1 \rightarrow 2}) &= \sum_{n_1=1}^{N^{(1)}} \langle \chi_{2 \rightarrow 1}(\chi_{1 \rightarrow 2}(g_{(1|n_1)})), g_{(1|n_1)}^* \rangle \\ &= \sum_{n_1=1}^{N^{(1)}} \left\langle \chi_{2 \rightarrow 1} \left(\sum_{n_2=1}^{N^{(2)}} \langle \chi_{1 \rightarrow 2}(g_{(1|n_1)}), g_{(2|n_2)}^* \rangle \triangleright_{(2)} g_{(2|n_2)} \right), g_{(1|n_1)}^* \right\rangle \\ &= \sum_{n_1=1}^{N^{(1)}} \sum_{n_2=1}^{N^{(2)}} \langle \chi_{1 \rightarrow 2}(g_{(1|n_1)}), g_{(2|n_2)}^* \rangle \cdot_R \langle \chi_{2 \rightarrow 1}(g_{(2|n_2)}), g_{(1|n_1)}^* \rangle \\ &\equiv \sum_{n_2=1}^{N^{(2)}} \sum_{n_1=1}^{N^{(1)}} \langle \chi_{2 \rightarrow 1}(g_{(2|n_2)}), g_{(1|n_1)}^* \rangle \cdot_R \langle \chi_{1 \rightarrow 2}(g_{(1|n_1)}), g_{(2|n_2)}^* \rangle \\ &= \sum_{n_2=1}^{N^{(2)}} \left\langle \chi_{1 \rightarrow 2} \left(\sum_{n_1=1}^{N^{(1)}} \langle \chi_{2 \rightarrow 1}(g_{(2|n_2)}), g_{(1|n_1)}^* \rangle \triangleright_{(1)} g_{(1|n_1)} \right), g_{(2|n_2)}^* \right\rangle \\ &= \sum_{n_2=1}^{N^{(2)}} \langle \chi_{1 \rightarrow 2}(\chi_{2 \rightarrow 1}(g_{(2|n_2)})), g_{(2|n_2)}^* \rangle = \text{Tr}_{G^{(2)}}(\chi_{1 \rightarrow 2} \circ \chi_{2 \rightarrow 1}). \end{aligned}$$

□

Traktując macierze kwadratowe stopnia N jako endomorfizmy modelowego R -modułu wolnego $R^{\times N}$, dochodzimy do

DEFINICJA 104. Przyjmijmy notację Def. 67, 21 i 82, Stw. 95 oraz Przykł. 41. Niechaj R będzie pierścieniem przemiennym i niech $M \in \text{Mat}(R; N)$ będzie dowolną macierzą kwadratową stopnia N o wyrazach z R . **Ślad macierzy M** to skalar

$$\text{Tr}_{(N)}(M) := \sum_{n=1}^N M_n^n.$$

▲

Kluczowe znaczenie warunku cykliczności eksponuje

STWIERDZENIE 148. *Przyjmijmy notację Def. 67, 21, 21, 32, 35, 61, 65, 70, 82, 94 i 104, Stw. 95 oraz Przykł. 34 (2) i 41. Niechaj R będzie pierścieniem przemiennym i niech $\tau \in \text{Mat}(R; N)^*$ będzie funkcjonalem liniowym na R -module $\text{Mat}(R; N)$. Jeśli dla dowolnych dwóch macierzy $A, B \in \text{Mat}(R; N)$ funkcjonal ten spełnia równość*

$$\tau(A \odot B) = \tau(B \odot A),$$

to istnieje jedyny skalar $c_\tau \in R$ o własności

$$\tau = c_\tau \triangleright \text{Tr}.$$

Innymi słowy, podmoduł $\text{Mat}(R; N)^*$ złożony z funkcjonałów cyklicznych jest generowany przez ślad macierzowy.

■

Dowód: Punktem wyjścia do weryfikacji tezy stwierdzenia jest wygodny wybór bazy modułu $\text{Mat}(R; N) \cong R^{N \times N}$. Niech $E_{i,j}$, $i, j \in \overline{1, N}$ będzie macierzą kwadratową stopnia N o wyrazach

$$(E_{i,j})_n^m := \delta_{m,i}^R \cdot_R \delta_{n,j}^R,$$

czyli taką, której wszystkie wyrazy poza tym o indeksach (i, j) , równym 1_R , są zerami (w pierścieniu). Jest jasnym, że rodzina macierzy $\{E_{i,j}\}_{i,j \in \overline{1, N}}$ jest bazą modułu $\text{Mat}(R; N)$ – baza ta jest wprowadzoną wcześniej bazą standardową R -modułu $R^{\times 2N}$.

indeksmoduł nad pierścieniem!pierścień jako (bi)moduł standardowy!baza!standardowa
Jej elementy spełniają prostą algebrę

$$E_{i,j} \odot E_{k,l} = \delta_{j,k}^R \triangleright_{(N)} E_{i,l},$$

co też wykorzystujemy w bezpośrednim rachunku:

$$\tau(E_{i,j}) \equiv \tau(E_{i,k} \odot E_{k,j}) = \tau(E_{k,j} \odot E_{i,k}) = \delta_{i,j}^R \cdot_R \tau(E_{k,k}).$$

Wprowadźmy oznaczenie

$$c_\tau := \tau(E_{i,i}),$$

przy czym – jak pokazuje powyższy rachunek – indeks i może być wybrany dowolnie. Dokonując rozkładu dowolnej macierzy $M \in \text{Mat}(R; N)$ w bazie standardowej,

$$M = \sum_{i,j=1}^N M_j^i \triangleright_{(N)} E_{i,j},$$

wyprowadzamy oczekiwany wynik

$$\begin{aligned}\tau(M) &\equiv \tau\left(\sum_{i,j=1}^N M_j^i \triangleright_{(N)} E_{i,j}\right) = \sum_{i,j=1}^N M_j^i \cdot_R \tau(E_{i,j}) = \sum_{i,j=1}^N M_j^i \cdot_R \delta_{i,j}^R \cdot_R \tau(E_{k,k}) \\ &= \sum_{i=1}^N M_i^i \cdot_R \tau(E_{k,k}) \equiv c_\tau \cdot_R \text{Tr}_{(N)}(M).\end{aligned}$$

□

Ostatnia obserwacja identyfikuje ślad jako stosownie unormowany funkcjonal liniowy na module. Ten sposób myślenia o śladzie stanowi naturalny punkt wyjścia do uogólnień przedstawionej tu jego konstrukcji w powiązaniu z pojęciem rzędu modułu wzgl. wymiaru (patrz: Stw. 145) spotykanych w bardziej abstrakcyjnych gałęziach algebry nowoczesnej.

* * *

Literatura uzupełniająca: Najlepszym wyborem jest kombinacja wspomnianych wcześniej traktatów Bourbakiego [Bou07b], Cohna [Coh82, Coh89, Coh91] i Langa [Lan02], uzupełniona o dodatkowy tom Bourbakiego [Bou07a].

Dis legomenon: Przestrzenie wektorowe

Przestrzenie wektorowe są bez wątpienia najbardziej rozpowszechnioną w fizyce strukturą modułopodobną. Już sama mnogość ich zastosowań – od tych o charakterze czysto instrumentalnym (jak w systematycznej konstrukcji opisu oddziaływań elementarnych czy w metodach numerycznych dynamiki układów wielociałowych) aż po te odzwierciedlające immanentny charakter opisywanych zagadnień (jak w teorii względności czy w operatorowym sformułowaniu kwantowej teorii pola) – w połączeniu z bogactwem technik rachunkowych rozwijanych na potrzeby tychże zastosowań skłania do bardziej wnikliwej analizy pewnych szczególnych własności tych obiektów, nieobecnych w szerokiej kategorii modułów nad pierścieniem bądź wymagających daleko idących i – bywa – mało oczywistych ograniczających założeń strukturalnych. Analizę tę organizuje i zarazem wydatnie upraszcza sztywna struktura przestrzeni wektorowej, pozwalająca na wykorzystanie niezwykle pomocnej konstrukcji bazy i bliskiego pojęcia wymiaru, dokonywanie rozkładu przestrzeni wektorowej na składniki proste względem dowolnej jej podprzestrzeni, rozszerzanie kanonicznej struktury grupy przemiennej na zbiorze odwzorowań liniowych do struktury przestrzeni wektorowej i stosowanie wielu innych zabiegów, które w miarę potrzeb będziemy przywoływać w dalszej części kursu.

9.1. Przestrzenie ϵ -hermitowskie – struktura i jej transport

W tej części wykładu zajmiemy się formami półtoraliniowymi na przestrzeniach wektorowych. Obiekty tego typu odgrywają istotną rolę w geometrii oraz fizyce, oto bowiem – między innymi – znajdują zastosowanie w rachunku wariacyjnym, nadają sens kwantowomechanicznym funkcjom korelacji, współokreślają strukturę metryczną na rozmaitościach riemannowskich (tj. pozwalają określić pojęcie “odległości punktów” oraz “kąta między krzywymi”), stanowią podstawę ścisłego opisu pól fermionowych na czasoprzestrzeni i definiują naturalną strukturę algebraiczną (tzw. **przestrzeni symplektycznej**) na przestrzeni stanów układu dynamicznego wraz z towarzyszącą jej strukturą (**algebry Poissona**) na przestrzeni funkcji gładkich (tj. “obserwabl”) na tejże przestrzeni stanów, która stanowi punkt wyjścia do podstawowych procedur kwantowania. Spotkamy się z nimi zatem jeszcze nieraz w przyszłych odsłonach geometrii różniczkowej, rachunku różniczkowego funkcji wielu zmiennych i funkcjonałów, klasycznej i kwantowej mechaniki teoretycznej i teorii pola oraz teorii względności. Ich omawianie zaczniemy – jak zazwyczaj – od wprowadzenia niezbędnej terminologii, po czym przejdziemy do zbadania własności przestrzeni wektorowych w ich obecności. Zaczynamy od

DEFINICJA 105. Przyjmijmy notację Def. 11, 13, 21, 32, 61 i 63. Niechaj $J : \mathbb{K} \curvearrowright : \lambda \mapsto \bar{\lambda}$ będzie dowolnym sprzężeniem na ciele $\mathbb{K}$, niech V będzie przestrzenią wektorową nad $\mathbb{K}$ i ustalmy $\epsilon \in \{-1_{\mathbb{K}}, +1_{\mathbb{K}}\}$. **Forma (J) -półtoraliniowa**

na V to odwzorowanie

$$\gamma : V \times V \longrightarrow \mathbb{K},$$

które jest $\mathbb{Z}$ -liniowe względem każdego z argumentów,

$$\forall_{u,v,w \in V} : \begin{cases} \gamma(u +_V v, w) = \gamma(u, w) +_{\mathbb{K}} \gamma(v, w) \\ \gamma(u, v +_V w) = \gamma(u, v) +_{\mathbb{K}} \gamma(u, w) \end{cases}$$

i jednorodne względem pierwszego z nich

$$\forall_{v,w \in V} : \gamma(\lambda \triangleright v, w) = \lambda \cdot_{\mathbb{K}} \gamma(v, w),$$

a do tego spełnia warunek (J) -półliniowości względem drugiego z argumentów¹,

$$\forall_{v,w \in V} : \gamma(v, \lambda \triangleright w) = \gamma(v, w) \cdot_{\mathbb{K}} \bar{\lambda}.$$

W szczególności forma $\text{id}_{\mathbb{K}}$ -półtoraliniowa to forma 2-liniowa.

Forma ϵ -hermitowska na V to forma (J) -półtoraliniowa o dodatkowej własności

$$\forall_{v,w \in V} : \gamma(v, w) = \epsilon \cdot_{\mathbb{K}} \overline{\gamma(w, v)}.$$

Wyróżniamy następujące typy form ϵ -hermitowskich:

- (i) **Formy hermitowskie** o $\epsilon = 1_{\mathbb{K}}$, w tym **formy symetryczne** odpowiadające $J = \text{id}_{\mathbb{K}}$.
- (ii) **Formy skośnie hermitowskie** (lub **antyhermitowskie**) o $\epsilon = -1_{\mathbb{K}}$, w tym **formy skośnie symetryczne** (lub **antysymetryczne**) odpowiadające $J = \text{id}_{\mathbb{K}}$.

▲

PRZYKŁAD(Y) 49.

- (1)
- (2)
- (3)

✓

O tym, jak dalece ograniczające (w sensie strukturalnym) bywają warunki półtoraliniowości i hermitowskości, przekonuje studium przypadków o szczególnym znaczeniu fizycznym.

STWIERDZENIE 149. *Przyjmijmy notację Def. 11, 13, 21, 32, 61, 63 i 105. Niechaj $(\mathbb{K}, J) \in \{(\mathbb{R}, \text{id}_{\mathbb{R}}), (\mathbb{C}, \cdot)\}$ i niech Φ będzie formą J -półtoraliniową na przestrzeni wektorowej V nad ciałem $\mathbb{K}$. Prawdziwe są poniższe **formuły polaryzacyjne**:*

¹W literaturze rozpowszechniona jest konwencja, wedle której forma półtoraliniowa jest półliniowa względem pierwszego argumentu. W niniejszym kursie przyjmujemy – za Bourbakim [Bou07a] – konwencję alternatywną, a to z uwagi na możliwość naturalnego uogólnienia konstrukcji przedstawionych w tym rozdziale na szerszą klasę pierścieni. Ten wybór nie rzutuje w istotny sposób (jakościowy) na treść wypowiedzianych tu stwierdzeń.

(i) Jeśli $\mathbb{K} = \mathbb{R}$, to część symetryczna formy Φ spełnia relację

$$\forall_{v,w \in V} : \Phi(v,w) + \Phi(w,v) = \Phi(v +_V w, v +_V w) - \Phi(v,v) - \Phi(w,w),$$

w szczególności więc w przypadku formy symetrycznej

$$\forall_{v,w \in V} : \Phi(v,w) = \frac{1}{2} (\Phi(v +_V w, v +_V w) - \Phi(v,v) - \Phi(w,w)).$$

(ii) Jeśli $\mathbb{K} = \mathbb{C}$, to

$$\forall_{v,w \in V} : \Phi(v,w) = \frac{1}{4} \sum_{k=0}^3 i^k \cdot \Phi(v +_V i^k w, v +_V i^k w).$$

■

Dowód: Bezpośredni rachunek. □

Oto więc sama półtoraliniowość w przypadku zespolonym i symetryczność w przypadku rzeczywistym oznaczają, że forma jest w pełni określona przez wartości, jakie przyjmuje na przekątnej kwadratu kartezjańskiego $V \times V$. Obserwacja ta okaże się nader przydatna w naszych przyszłych rozważaniach.

Obecność (anty)automorfizmu J w definicji formy półtoraliniowej motywuje następującą

DEFINICJA 106. Przyjmijmy notację Def. 11, 13, 21, 32, 61 i 63 oraz Przykł. 35 (2). Niechaj $((V, +_V, P_V, \bullet \mapsto 0_V), \ell_V \equiv \triangleright_V)$ będzie przestrzenią wektorową nad ciałem $\mathbb{K}$ wyposażonym w inwolutywny (anty)automorfizm J . **Przestrzeń J -sprzężona** do V to przestrzeń $\mathbb{K}$ -liniowa

$$((V^J \equiv V, +_V, P_V, \bullet \mapsto 0_V), \wp)$$

o tej samej grupie przemiennej i działaniu $\mathbb{K}$ danym wzorem

$$\wp : V^J \times \mathbb{K} \longrightarrow V^J : (v, \lambda) \mapsto J(\lambda) \triangleright_V v =: v \triangleleft_{V^J} \lambda.$$

W szczególności przestrzenią J -sprzężoną do przestrzeni $\mathbb{K}$ -liniowej $\mathbb{K}$ jest grupa przemienne $(\mathbb{K}^J \equiv \mathbb{K}, +_{\mathbb{K}}, P_{\mathbb{K}}, \bullet \mapsto 0_{\mathbb{K}})$ z działaniem

$$\wp : \mathbb{K}^J \times \mathbb{K} \longrightarrow \mathbb{K}^J : (\mu, \lambda) \mapsto J(\lambda) \cdot_{\mathbb{K}} \mu.$$

Funkcjonał (J) -półliniowy (albo **forma (J) -półliniowa**) na V to $\mathbb{Z}$ -liniowe odwzorowanie

$$\varphi : V \longrightarrow \mathbb{K}^J,$$

o własności

$$\forall_{(\lambda, v) \in \mathbb{K} \times V} : \varphi(\lambda \triangleright_V v) = \varphi(v) \cdot_{\mathbb{K}} J(\lambda).$$

Zbiór wszystkich funkcyjonałów J -półliniowych na V będziemy oznaczać symbolem

$$V^{*,J} := \{ \varphi : V \longrightarrow \mathbb{K}^J \mid \varphi \text{ } (J)\text{-półliniowy} \}.$$

▲

Prostą związek między funkcyjonałami półliniowymi i dobrze nam znanymi funkcyjonałami liniowymi ustala

STWIERDZENIE 150. Przyjmijmy notację Def. 11, 13, 21, 32, 61, 63 i 106 oraz Przykł. 35 (2). Zbiór $V^{*,J}$ niesie naturalną strukturę przestrzeni $\mathbb{K}$ -liniowej z działaniem $\mathbb{K}$ określonym formułą

$$V^{*,J} \times \mathbb{K} \longrightarrow V^{*,J} : (\varphi, \lambda) \longmapsto \varphi \triangleleft \lambda,$$

$$\forall_{(v,\lambda) \in V \times \mathbb{K}} : (\varphi \triangleleft \lambda)(v) := J(\lambda) \cdot_{\mathbb{K}} \varphi(v).$$

Odwzorowanie J indukuje kanoniczny (inwolutywny) izomorfizm przestrzeni $\mathbb{K}$ -liniowych

$$J_* : V^* \longrightarrow V^{*,J} : \varphi \longmapsto J \circ \varphi.$$

■

Wprowadzone pojęcia pozwalają zwięźle wysławić

DEFINICJA 107. Przyjmijmy notację Def. 11, 13, 21, 32, 61, 63, 105 i 106 oraz Przykł. 35 (2). Niechaj γ będzie formą J -półtoraliniową na przestrzeni wektorowej V nad ciałem $\mathbb{K}$. **Odwzorowanie lewostronnie stowarzyszone z γ** to odwzorowanie $\mathbb{K}$ -liniowe

$$l_\gamma : V \longrightarrow (V^{*,J})^J : v \longmapsto \gamma(v, \cdot).$$

Odwzorowanie prawostronnie stowarzyszone z γ to odwzorowanie $\mathbb{K}$ -liniowe

$$r_\gamma : V \longrightarrow (V^*)^J : v \longmapsto \gamma(\cdot, v).$$

▲

Narzucenie warunku ϵ -hermitowskości pociąga za sobą pojawienie się oczywistej relacji między oboma odwzorowaniami stowarzyszonymi.

STWIERDZENIE 151. Przyjmijmy notację Def. 11, 13, 21, 32, 61, 63, 105, 106 i 107 oraz Przykł. 35 (2). Niechaj γ będzie formą ϵ -hermitowską na przestrzeni wektorowej V nad ciałem $\mathbb{K}$. Słuszne są tożsamości

$$l_\gamma = J_*(\epsilon \triangleright r_\gamma), \quad r_\gamma = J_*(J(\epsilon) \triangleright l_\gamma) \equiv J_*(\epsilon \triangleright l_\gamma),$$

przy czym dla dowolnego wektora $v \in V$ jest

$$(\epsilon \triangleright r_\gamma)(v) := \gamma(\cdot, v) \cdot_{\mathbb{K}} J(\epsilon) \equiv \gamma(\cdot, v) \cdot_{\mathbb{K}} \epsilon, \quad (\epsilon \triangleright l_\gamma)(v) := \epsilon \cdot_{\mathbb{K}} \gamma(v, \cdot).$$

W szczególności więc zachodzi równość

$$\text{Ker } l_\gamma = \text{Ker } r_\gamma.$$

■

Powyższa obserwacja uzasadnia

DEFINICJA 108. Przyjmijmy notację Def. 11, 13, 21, 32, 35, 36, 61, 63, 105, 106 i 107 oraz Przykł. 35 (2). **Jądro formy ϵ -hermitowskiej γ** określonej na przestrzeni wektorowej V nad ciałem $\mathbb{K}$ to podprzestrzeń

$$\text{Ker } \gamma := \text{Ker } l_\gamma \subset V.$$

Rząd formy ϵ -hermitowskiej γ to kowymiar jej jądra,

$$\text{rk } \gamma := \text{codim}_{\mathbb{K}}^{(V)} \text{Ker } \gamma.$$

Forma ϵ -hermitowska niezwyrodniała to taka, której jądro jest trywialne, $\text{Ker } \gamma = \{0_V\}$. W przeciwnym razie mamy do czynienia z **formą ϵ -hermitowską**

zwyródniałą. Forma niezwyrodniała o tej własności, że stowarzyszone odwzorowania l_γ i r_γ są izomorfizmami, jest nazywana **formą ϵ -hermitowską nieosobliwą**.

▲

Możemy już teraz sprecyzować przedmiot naszych dalszych dociekań.

DEFINICJA 109. Przyjmijmy notację Def. 11, 13, 21, 32, 35, 61, 63, 105, 106, 107 i 108 oraz Przykł. 35 (2). **Przestrzeń ϵ -hermitowska** to para $((V, +_V, P_V, \bullet \mapsto 0_V), \ell_V, \gamma)$ złożona z przestrzeni wektorowej $((V, +_V, P_V, \bullet \mapsto 0_V), \ell_V)$ nad ciałem $\mathbb{K}$ oraz formy ϵ -hermitowskiej γ na niej określonej. Przestrzeń ϵ -hermitowską nazywamy **(nie)zwyródniałą** (wzgl. **nieosobliwą**), ilekroć odnośna forma γ ma tę samą własność.

Niechaj $((V^{(\alpha)}, +_{(\alpha)}, P_{(\alpha)}, \bullet \mapsto 0_{(\alpha)}), \ell_{(\alpha)}, \gamma_{(\alpha)})$, $\alpha \in \{1, 2\}$ będą dwiema przestrzeniami ϵ -hermitowskimi nad ciałem $\mathbb{K}$. **Odwzorowanie metryczne z $V^{(1)}$ w $V^{(2)}$** to odwzorowanie $\mathbb{K}$ -liniowe

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

które spełnia aksjomat (wyrażony przez diagram przemienności i równoważne zdanie logiczne):

$$\begin{array}{ccc} V^{(1)} \times V^{(1)} & \xrightarrow{\gamma_{(1)}} & \mathbb{K} \\ \chi \times \chi \downarrow & & \parallel \text{id}_{\mathbb{K}} \\ V^{(2)} \times V^{(2)} & \xrightarrow{\gamma_{(2)}} & \mathbb{K} \end{array} \quad \equiv \quad \forall_{v, w \in V^{(1)}} : \gamma_{(2)}(\chi(v), \chi(w)) = \gamma_{(1)}(v, w).$$

Ilekroć χ jest izomorfizmem przestrzeni wektorowych, mówimy o **izometrii przestrzeni ϵ -hermitowskich**.

▲

Terminologia stosowana w teorii przestrzeni ϵ -hermitowskich ma częstokroć konotacje geometryczne i nawiązuje do pierwszoplanowej roli, jaką odgrywa nieosobliwa struktura ϵ -hermitowska w określaniu struktury metrycznej (a więc także i normy) na przestrzeniach wektorowych nad ciałami liczbowymi $\mathbb{Q}, \mathbb{R}$ i $\mathbb{C}$. Do zagadnień tych wrócimy w dalszej części kursu, a tymczasem dokończymy introdukcję elementarnych struktur algebraicznych związanych z formami ϵ -hermitowskimi.

Oto w przypadku skończenia wymiarowym bez trudu ustalamy macierzową realizację warunku ϵ -hermitowskości.

STWIERDZENIE 152. Przyjmijmy notację Def. 67, 11, 13, 21, 32, 35, 61, 63, 65, 68, 70, 75, 78, 82, 105, 106, 107, 108 i 109, Cor. 14, Stw. 75, 95, 96, 97, 98 i 99, Tw. 8.11 oraz Przykł. 35 (2). Niechaj $J : \mathbb{K} \curvearrowright : \lambda \mapsto \bar{\lambda}$ będzie inwolutywnym (anty)automorfizmem ciała $\mathbb{K}$ i niech $((V, +_V, P_V, \bullet \mapsto 0_V), \ell_V, \gamma)$ będzie przestrzenią ϵ -hermitowską skończonego wymiaru $\dim_{\mathbb{K}} V =: N < \infty$, o bazie $\mathcal{B} := \{v_i\}_{i \in \overline{1, N}}$. **Macierz formy ϵ -hermitowskiej γ względem bazy $\mathcal{B}$,**

$$[\gamma]_{\mathcal{B}} : \overline{1, N} \times \overline{1, N} \longrightarrow \mathbb{K} : (m, n) \mapsto \gamma(v_m, v_n),$$

spełnia tożsamość

$$[\gamma]_{\mathcal{B}} = \epsilon \triangleright_{(N)} [\gamma]_{\mathcal{B}}^{\dagger} \equiv \epsilon \triangleright_{(N)} \overline{[\gamma]_{\mathcal{B}}}^T,$$

przy czym dla dowolnej macierzy $M \in \text{Mat}(\mathbb{K}; N)$ określamy **sprzężenie** (J -)hermitowskie

$${}^\dagger : \text{Mat}(\mathbb{K}; N) \hookrightarrow : (M^i_j)_{i,j \in \overline{1,N}} \mapsto (\overline{M^j_i})_{i,j \in \overline{1,N}}.$$

W szczególności forma hermitowska ma **macierz hermitowską**

$$[\gamma]_{\mathcal{B}} = [\gamma]_{\mathcal{B}}^\dagger,$$

forma symetryczna – **macierz symetryczną**

$$[\gamma]_{\mathcal{B}} = [\gamma]_{\mathcal{B}}^T,$$

forma skośnie hermitowska – **macierz skośnie hermitowską** (lub antyhermitowską)

$$[\gamma]_{\mathcal{B}} = -[\gamma]_{\mathcal{B}}^\dagger,$$

i wreszcie forma skośnie symetryczna – **macierz skośnie symetryczną** (lub antysymetryczną)

$$[\gamma]_{\mathcal{B}} = -[\gamma]_{\mathcal{B}}^T.$$

I odwrotnie, każda macierz (skośnie) hermitowska (wzgl. (skośnie) symetryczna) $M \in \text{Mat}(\mathbb{K}; N)$ zadaje jednoznacznie formę (skośnie) hermitowską (wzgl. (skośnie) symetryczną) γ_M na przestrzeni V o ustalonej bazie $\mathcal{B}$ wedle wzoru

$$\gamma_M \left(\sum_{i=1}^N \lambda^i \triangleright_V v_i, \sum_{j=1}^N \mu^j \triangleright_V v_j \right) := \sum_{i=1}^N \lambda^i \cdot_{\mathbb{K}} M_{ij} \cdot_{\mathbb{K}} \overline{\mu^j}.$$

■

Reguły transformacyjne dla tak zadanej macierzy formy ϵ -hermitowskiej określające jej zachowanie przy zmianie bazy precyzuje

STWIERDZENIE 153. Przyjmijmy notację Def. 67, 11, 13, 21, 32, 35, 61, 63, 65, 68, 70, 75, 78, 82, 105, 106, 107, 108 i 109, Cor. 14, Stw. 75, 95, 96, 97, 98, 99 i 152 oraz Tw. 8.11. Niech $\mathcal{B}^{(\alpha)}$, $\alpha \in \{1, 2\}$ będą dwiema bazami przestrzeni ϵ -hermitowskiej V . Wówczas zachodzi tożsamość

$$[\gamma]_{\mathcal{B}^{(2)}} = [\text{id}_V]_{\mathcal{B}^{(2)}}^{\mathcal{B}^{(1)T}} \odot [\gamma]_{\mathcal{B}^{(1)}} \odot \overline{[\text{id}_V]_{\mathcal{B}^{(1)}}^{\mathcal{B}^{(2)}}}.$$

■

Jednym z naczelných zadań, jakie stoją przed nami w tej części wykładu, jest wykorzystanie swobody wyboru bazy w przestrzeni ϵ -hermitowskiej w celu zredukowania macierzowej realizacji odnośnej formy ϵ -hermitowskiej do możliwie najprostszej postaci wynikającej z samej jej ogólnej definicji. Kryterium “prostoty” nabierze sensu konkretnego w toku dalszej analizy własności przestrzeni ϵ -hermitowskich.

Zauważmy, że jeśli $J \neq \text{id}_{\mathbb{K}}$, to nie sposób oczekiwać struktury $\mathbb{K}$ -liniowej na zbiorze wszystkich form ϵ -hermitowskich na danej przestrzeni wektorowej nad ciałem $\mathbb{K}$. Istnieje natomiast możliwość konkatenaacji form pochodzących z różnych przestrzeni wektorowych, którą opisuje

DEFINICJA 110. Przyjmijmy notację Def. 11, 13, 21, 32, 35, 61, 63, 75, 78, 105, 106, 107, 108 i 109 oraz Przykł. 35 (2). Niechaj $\mathfrak{H}^{(\alpha)} := ((V^{(\alpha)}, +_{(\alpha)}, P_{(\alpha)}, \bullet \mapsto 0_{(\alpha)}), \ell_{(\alpha)}), \gamma_{(\alpha)})$, $\alpha \in \overline{1, N}$ będą przestrzeniami ϵ -hermitowskimi nad ciałem $\mathbb{K}$.

Zewnętrzna suma prosta przestrzeni ϵ -hermitowskich $\mathfrak{H}^{(\alpha)}$ to przestrzeń ϵ -hermitowska

$$\left(\left(\left(\bigoplus_{\alpha=1}^N V^{(\alpha)}, +_{\square}, P_{\square}, \bullet \mapsto 0_{\square} \right), \ell_{\square} \right), \bigoplus_{\alpha=1}^N \gamma_{(\alpha)} \right),$$

przy czym **suma prosta form ϵ -hermitowskich** $\bigoplus_{\alpha=1}^N \gamma_{(\alpha)}$ jest określona wzorem

$$\bigoplus_{\alpha=1}^N \gamma_{(\alpha)} \left(\sum_{\alpha=1}^N v^{(\alpha)}, \sum_{\beta=1}^N w^{(\beta)} \right) := \sum_{\alpha=1}^N \gamma_{(\alpha)}(v^{(\alpha)}, w^{(\alpha)}),$$

zapisanym dla dowolnych wektorów $v^{(\alpha)}, w^{(\alpha)} \in V^{(\alpha)}$.

▲

Obecność formy ϵ -hermitowskiej pozwala wyodrębnić z szerokiej klasy sum prostych przestrzeni ϵ -hermitowskich struktury o szczególnym znaczeniu w dyskusji dalszej wewnętrznej organizacji, jaką forma ϵ -hermitowska wprowadza w swej dziedzinie. Instrumentalną rolę w tej dyskusji odgrywa naturalny odpowiednik wprowadzonego uprzednio pojęcia anihilatora.

DEFINICJA 111. Przyjmijmy notację Def. 11, 13, 21, 32, 35, 61, 63, 64, 65, 95, 98, 105, 106, 107, 108 i 109 oraz Przykł. 34 (2) i 35 (2). Niechaj $v, w \in V$ będą wektorami z przestrzeni ϵ -hermitowskiej V . Mówimy, że wektor w jest (γ) -**ortogonalny** (lub (γ) -**prostopadły**) do wektora v , co zapisujemy symbolem

$$w \perp_{(\gamma)} v,$$

ilekroć spełniony jest warunek

$$\gamma(v, w) = 0_{\mathbb{K}}.$$

Analogicznie, dla dowolnej podprzestrzeni $W \subset V$ określamy **przestrzeń (γ) -ortogonalną** (lub (γ) -**prostopadłą**) do W jako podprzestrzeń

$$W^{\perp_{(\gamma)}} := \{ v \in V \mid \forall_{w \in W} : v \perp_{(\gamma)} w \}.$$

Idąc dalej, powiemy, że podprzestrzeń $W_1 \subset V$ jest (γ) -**prostopadła** (lub (γ) -**prostopadłą**) do podprzestrzeni $W_2 \subset V$, co zapiszemy symbolem

$$W_1 \perp_{(\gamma)} W_2,$$

jeśli spełniony jest warunek

$$\forall_{(w_1, w_2) \in W_1 \times W_2} : w_1 \perp_{(\gamma)} w_2.$$

▲

Możemy już teraz wysławić

DEFINICJA 112. Przyjmijmy notację Def. 11, 13, 21, 32, 35, 61, 63, 64, 65, 75, 78, 95, 98, 105, 106, 107, 108, 109, 110 i 111 oraz Przykł. 34 (2) i 35 (2). Niechaj $W_1, W_2 \subset V$ będą dwiema podprzestrzeniami przestrzeni ϵ -hermitowskiej V zadającymi rozkład tejsze na sumę prostą

$$V = W_1 \oplus W_2.$$

Sumę tę określamy mianem **sumy (γ) -ortogonalnej** i zapisujemy w postaci

$$V = W_1 \oplus W_2,$$

jeśli W_1 i W_2 są wzajem (γ -)ortogonalne, tj.

$$W_1 \perp_{(\gamma)} W_2.$$

▲

Mamy oczywiste

STWIERDZENIE 154. *Przyjmijmy notację Def. 11, 13, 21, 32, 35, 61, 63, 64, 65, 75, 78, 95, 98, 105, 106, 107, 108, 109, 110, 111 i 112 oraz Przykł. 34 (2) i 35 (2). Niechaj $V^{(\alpha)}$, $\alpha \in \{1, 2\}$ będą dwiema przestrzeniami ϵ -hermitowskimi i niech $\chi : V^{(1)} \rightarrow V^{(2)}$ będzie izometrią. Jeśli $W_1, W_2 \subset V^{(1)}$ są podprzestrzeniami $V^{(1)}$ zadającymi rozkład ortogonalny tej przestrzeni,*

$$V^{(1)} = W_1 \oplus W_2,$$

to wówczas $V^{(2)}$ ma rozkład

$$V^{(2)} = \chi(W_1) \oplus \chi(W_2).$$

■

Przypomnijmy, iż wybór bazy w przestrzeni wektorowej zadaje szczególny rozkład tej ostatniej na sumę prostą jej jednowymiarowych podprzestrzeni – patrz: Stw. 86. W kategorii przestrzeni ϵ -hermitowskich bywa zasadnym poddać tę konstrukcję dodatkowym ograniczeniom, co prowadzi do

DEFINICJA 113. Przyjmijmy notację Def. 67, 11, 13, 21, 32, 35, 61, 63, 64, 65, 68, 70, 75, 78, 95, 98, 105, 106, 107, 108, 109, 110, 111 i 112, Stw. 75 oraz Przykł. 34 (2) i 35 (2). **Baza ortogonalna** przestrzeni ϵ -hermitowskiej V to taka baza $\mathcal{B} := \{g_\lambda\}_{\lambda \in \Lambda}$ odnośnej przestrzeni wektorowej, której elementy spełniają relacje

$$\forall_{\lambda, \mu \in \Lambda} : (\lambda \neq \mu \implies \gamma(v_\lambda, v_\mu) = 0_{\mathbb{K}}).$$

Jeśli dodatkowo

$$\forall_{\lambda \in \Lambda} : \gamma(v_\lambda, v_\lambda) = 1_{\mathbb{K}},$$

to bazę taką określamy mianem **bazy ortonormalnej**.

▲

Jest oczywistym, że baza ortogonalna wyznacza rozkład przestrzeni ϵ -hermitowskiej na sumę ortogonalną jej jednowymiarowych podprzestrzeni danych jako powłoki $\mathbb{K}$ -liniowe elementów bazy.

Zagadnienie zwyrodnienia formy ϵ -hermitowskiej odgrywa istotną rolę w rozmaitych matematycznych i fizycznych zastosowaniach tych obiektów – oto, np., jądro pewnej wyróżnionej formy skośnie symetrycznej na przestrzeni stanów układu fizycznego (tzw. **formy presymplektycznej**) wyznacza algebrę symetrii lokalnych (tzw. **symetrii cechowania**) tegoż układu, której identyfikacja stanowi punkt wyjścia do konstrukcji – fundamentalnej w kontekście lokalnej teorii pola – fizycznej przestrzeni stanów, tj. przestrzeni orbit symetrii lokalnej z indukowaną niezwyrodniałą formą skośnie symetryczną (tzw. **formą symplektyczną**). Ta obserwacja motywuje szczegółową dyskusję warunków zwyrodnienia formy ϵ -hermitowskiej.

DEFINICJA 114. Przyjmijmy notację Def. 11, 13, 21, 32, 35, 61, 63, 64, 105, 106, 107, 108 i 109 oraz Przykł. 35 (2). **Wektor izotropowy** (lub **zerowy**) $v \in V$ w przestrzeni ϵ -hermitowskiej V to taki, który spełnia warunek

$$\gamma(v, v) = 0_{\mathbb{K}}.$$

Dowolna podprzestrzeń $W \subset V$ zawierająca wektor izotropowy $v \in W$ o własności

$$\forall_{w \in W} : \gamma(v, w) = 0_{\mathbb{K}}$$

jest określana mianem **(pod)przestrzeni izotropowej**. I wreszcie podprzestrzeń $W \subset V$, na której

$$\gamma|_{W \times W} = 0,$$

nazywamy **(pod)przestrzenią całkowicie izotropową** (lub **zerową**). Przestrzeń, na której forma ϵ -hermitowska jest niezwyrodniała, bywa nazywana **przestrzenią niezwyrodniałą** (lub **nieizotropową** wzgl. **anizotropową**). ▲

Łatwo sprawdzamy ważne z konstrukcyjnego punktu widzenia

STWIERDZENIE 155. *Każda podprzestrzeń zerowa niezwyrodniałej przestrzeni ϵ -hermitowskiej jest zawarta w pewnej maksymalnej podprzestrzeni zerowej tejże przestrzeni.* ■

Dowód: Niechaj V będzie przestrzenią ϵ -hermitowską z niezwyrodniałą formą ϵ -hermitowską i niech $W \subset V$ będzie jej dowolną podprzestrzenią zerową. Rozważmy zbiór

$$\mathcal{Z} := \{ Z \subset V \mid Z \supset W \wedge Z \text{ zerowa} \}.$$

Jest on częściowo uporządkowany względem relacji $\subset$, a przy tym łańcuchowo zupełny. Istotnie, dla dowolnego łańcucha $\{Z_\lambda\}_{\lambda \in \Lambda} \subset \mathcal{Z}$ stwierdzamy, że przestrzeń $Z^\cup := \bigcup_{\lambda \in \Lambda} Z_\lambda$ spełnia relację $W \subset Z^\cup \subset V$, a ponadto jest zerowa, oto bowiem – wobec istnienia totalnego porządku na $\mathcal{Z}$ – każde dwa wektory $v, w \in Z^\cup$ należą do pewnej przestrzeni Z_λ , a ponieważ ta jest zerowa, przeto koniecznie $\gamma(v, w) = 0_{\mathbb{K}}$. Stąd wniosek, że $Z^\cup \in \mathcal{Z}$, co dowodzi łańcuchowej zupełności $\mathcal{Z}$. Element maksymalny $\mathcal{Z}$, którego istnienie orzeka Tw. 8.6, jest poszukiwaną maksymalną podprzestrzenią zerową V zawierającą W . □

Fundamentalną własność niezwyrodniałych form ϵ -hermitowskich opisuje

STWIERDZENIE 156. *Przyjmijmy notację Def. 11, 13, 21, 32, 35, 61, 63, 64, 65, 75, 78, 95, 98, 105, 106, 107, 108, 109, 110, 111, 112 i 114 oraz Przykł. 34 (2) i 35 (2). Niechaj $W \subset V$ będzie dowolną skończone wymiarową niezwyrodniałą podprzestrzenią przestrzeni ϵ -hermitowskiej V . Wówczas*

$$V = W \oplus W^\perp.$$
■

Dowód: Skoro forma $\gamma_W := \gamma|_{W \times W}$ jest niezwyrodniała, to wobec $\dim_{\mathbb{K}} W < \infty$ odwzorowanie $r_{\gamma_W} : W \rightarrow (W^*)^J$ jest bijekcją na mocy Stw. 122 (wystarczy zastosować argumenty z dowodu Stw. 130). Jeśli zatem dla dowolnego $v \in V$ ograniczyć $r_{\gamma}(v) \in (V^*)^J$ do W , tj. wziąć $r_{\gamma}(v)|_W \in (W^*)^J$, to istnieje jedyny wektor $w \in W$ o własności

$$\forall_{u \in W} : (r_{\gamma}(v))(u) = (r_{\gamma_W}(w))(u).$$

To jednak oznacza, że

$$\gamma(u, v - w) = 0_{\mathbb{K}},$$

czyli

$$v - w \in W^{\perp}.$$

□

Z powyższego stwierdzenia możemy wysnuć ważne

COROLLARIUM 20. *Przyjmijmy notację Def. 11, 13, 21, 32, 35, 61, 63, 64, 65, 75, 78, 95, 98, 105, 106, 107, 108, 109, 110, 111, 112 i 114 oraz Przykł. 34 (2) i 35 (2). Niechaj $W \subset V$ będzie dowolną skończenie wymiarową podprzestrzenią niezwyrodniałej przestrzeni ϵ -hermitowskiej V . Wówczas równoważne są następujące stwierdzenia:*

- (i) W jest niezwyrodniała;
- (ii) $W^{\perp}$ jest niezwyrodniała;
- (iii) $V = W \oplus W^{\perp}$.

■

Dowód:

- (i) $\Rightarrow$ (iii) Wprost na mocy Stw. 156.
- (iii) $\Rightarrow$ (i) $\wedge$ (ii) Niezwyrodnienie γ oznacza trywialność jądra r_{γ} , a zatem jedynym wektorem $v \in V$ o własności

$$\forall_{u \in V} : (r_{\gamma}(v))(u) = 0_{\mathbb{K}}$$

jest wektor zerowy $v = 0_V$. Załóżmy, że $z \in W$ spełnia warunek

$$\forall_{w \in W} : \gamma(w, z) = 0_{\mathbb{K}},$$

a wtedy

$$\forall_{(w, v) \in W \times W^{\perp}} : \gamma(w +_V v, z) = \gamma(w, z) +_{\mathbb{K}} \gamma(v, z) = 0_{\mathbb{K}}.$$

Jednakowoż z racji istnienia rozkładu $V = W \oplus W^{\perp}$ każdy wektor $z \in V$ ma (jednoznaczny) rozkład na sumę elementów W i $W^{\perp}$, czyli

$$\forall_{v \in V} : 0_{\mathbb{K}} = \gamma(v, z) \equiv (r_{\gamma}(z))(v),$$

a w takim razie $z = 0_V$, co pokazuje, że forma $\gamma|_{W \times W}$ jest niezwyrodniała. Analogicznie dowodzimy niezwyrodnienia $W^{\perp}$.

(ii) $\Rightarrow$ (i) Wobec oczywistej inkluzji $W \subset W^{\perp\perp}$ niezwyrodnienie $W^{\perp}$ implikuje relację

$$W \cap W^{\perp} \subset (W^{\perp})^{\perp} \cap W^{\perp} = \{0_V\},$$

czyli też

$$W \cap W^{\perp} = \{0_V\},$$

a to oznacza, że W jest niezwyrodniała.

□

Możemy już teraz przejść do szczegółowej dyskusji cech swoistych poszczególnych typów form i przestrzeni ϵ -hermitowskich.

9.2. Przestrzenie hermitowskie

Teoria form hermitowskich ma podstawowe znaczenie w opisie struktur metrycznych na przestrzeniach wektorowych nad ciałem liczb zespolonych i jako taka znajduje zastosowanie w opisie przestrzeni stanów kwantowych teorii fizykalnych, modelowanych na przestrzeniach Hilberta (formy hermitowskie są używane m.in. w konstrukcji amplitud prawdopodobieństwa). Poniżej odpowiemy na kluczowe pytanie o kanoniczną postać formy hermitowskiej, które będzie zarazem pytaniem o wewnętrzną organizację przestrzeni wektorowej (czyli np. możliwość konstrukcji wyróżnionych baz) w obecności formy hermitowskiej. Zaczniemy zatem od fundamentalnego

TWIERDZENIE 9.1 (O bazie ortogonalnej dla formy hermitowskiej). *Przyjmijmy notację Def. 67, 11, 13, 21, 32, 35, 61, 63, 64, 65, 68, 70, 75, 78, 95, 98, 105, 106, 107, 108, 109, 110, 111, 112 i 113, Stw. 75 oraz Przykł. 11, 34 (2) i 35 (2). Niechaj V będzie skończenie wymiarową przestrzenią wektorową nad ciałem $\mathbb{K}$. Dla dowolnej formy hermitowskiej $\gamma : V \times V \rightarrow \mathbb{K}$ istnieje baza ortogonalna wtedy i tylko wtedy, gdy nie są spełnione równocześnie poniższe warunki:*

- (i) $\text{char } \mathbb{K} = 2$;
- (ii) $J = \text{id}_{\mathbb{K}}$;
- (iii) γ jest niezerową formą alternującą.

■

Dowód: Instrumentalny w dowodzie niniejszego twierdzenia jest

LEMAT 9.2. *Przyjmijmy notację Def. 11, 13, 21, 32, 35, 61, 63, 64, 105, 106, 107, 108, 109 i 114 oraz Przykł. 11 i 35 (2). Niechaj V będzie przestrzenią wektorową nad ciałem $\mathbb{K}$ i niech $\gamma : V \times V \rightarrow \mathbb{K}$ będzie niezerową formą hermitowską. Jeśli wszystkie wektory z V są izotropowe, to jest spełniona koniunkcja warunków:*

- (i) $\text{char } \mathbb{K} = 2$;
- (ii) $J = \text{id}_{\mathbb{K}}$;
- (iii) γ jest niezerową formą alternującą.

■

Dowód: Izotropowość wektorów z V jest równoznaczna z (iii). Na podstawie założeń dotyczących V obliczamy też, dla dowolnych wektorów $v, w \in V$,

$$\begin{aligned} 0_{\mathbb{K}} &= \gamma(v +_V w, v +_V w) = \gamma(v, v) +_{\mathbb{K}} \gamma(w, w) +_{\mathbb{K}} \gamma(v, w) +_{\mathbb{K}} \gamma(w, v) \\ &= \gamma(v, w) +_{\mathbb{K}} \gamma(w, v), \end{aligned}$$

skąd

$$\gamma(v, w) = -\gamma(w, v) = -\overline{\gamma(v, w)}.$$

Przy tym jednak skoro $\gamma \neq 0$, to muszą istnieć wektory $v, w \in V$ o własności

$$\gamma(v, w) = 1_{\mathbb{K}},$$

a w takim razie – dla dowolnego skłara $\lambda \in \mathbb{K}$ –

$$\lambda = \lambda \cdot_{\mathbb{K}} \gamma(v, w) = \gamma(\lambda \triangleright_V v, w) = -\overline{\gamma(\lambda \triangleright_V v, w)} = -\overline{\gamma(v, w)} \cdot_{\mathbb{K}} \bar{\lambda} = -\bar{\lambda},$$

czyli ostatecznie

$$\lambda +_{\mathbb{K}} \bar{\lambda} = 0_{\mathbb{K}}.$$

Kładąc $\lambda := 1_{\mathbb{K}}$, otrzymujemy $1_{\mathbb{K}} +_{\mathbb{K}} 1_{\mathbb{K}} = 0_{\mathbb{K}}$, a to daje (i). Wobec jednoznaczności elementu przeciwnego do danego $\lambda \in \mathbb{K}$ wnioskujemy na podstawie tożsamości

$$\lambda +_{\mathbb{K}} \lambda = \lambda \cdot_{\mathbb{K}} (1_{\mathbb{K}} +_{\mathbb{K}} 1_{\mathbb{K}}) = \lambda \cdot_{\mathbb{K}} 0_{\mathbb{K}} = 0_{\mathbb{K}},$$

o równości

$$\bar{\lambda} = \lambda,$$

która jest równoznaczna z $J = \text{id}_{\mathbb{K}}$. □

Wracamy teraz do dowodu twierdzenia zasadniczego, kładąc przy tym $\gamma \neq 0$ i stosując indukcję względem wymiaru $N := \dim_{\mathbb{K}} V$. Dla $N = 0$ teza jest w oczywisty sposób prawdziwa. Przyjmijmy przeto, że jest ona słuszna także dla $N = N_0 \geq 1$, a następnie połóżmy $N = N_0 + 1$. Jeśli koniunkcja (i) $\wedge$ (ii) $\wedge$ (iii) nie zachodzi, to na mocy lematu musi istnieć wektor $v \in V$ o własności $\gamma(v, v) \neq 0_{\mathbb{K}}$. Zwróćmy uwagę, że $\langle v \rangle_{\mathbb{K}}$ jest niezwyrodniała, przeto na mocy Stw. 156 V rozkłada się na sumę ortogonalną

$$V = \langle v \rangle_{\mathbb{K}} \oplus \langle v \rangle_{\mathbb{K}}^{\perp_{\gamma}},$$

skąd w świetle Stw. 91 wynika ograniczenie

$$\dim_{\mathbb{K}} \langle v \rangle_{\mathbb{K}}^{\perp_{\gamma}} = \dim_{\mathbb{K}} V - \dim_{\mathbb{K}} \langle v \rangle_{\mathbb{K}} = N_0 + 1 - 1 = N_0.$$

Założmy najpierw, że $\gamma|_{\langle v \rangle_{\mathbb{K}}^{\perp_{\gamma}}}$ nie spełnia (i) $\wedge$ (ii) $\wedge$ (iii), a wtedy założenie indukcyjne przewiduje istnienie bazy $\{v_i\}_{i \in \overline{2, N}}$ przestrzeni $\langle v \rangle_{\mathbb{K}}^{\perp_{\gamma}}$ ortogonalnej względem $\gamma|_{\langle v \rangle_{\mathbb{K}}^{\perp_{\gamma}}}$. W tej sytuacji układ $\{v\} \cup \{v_i\}_{i \in \overline{2, N}}$ jest bazą γ -ortogonalną V . Pozostaje zatem zbadać sytuację, gdy $\gamma^{\perp} := \gamma|_{\langle v \rangle_{\mathbb{K}}^{\perp_{\gamma}}} \neq 0$ jest alternująca, $\text{char } \mathbb{K} = 2$ i $J = \text{id}_{\mathbb{K}}$. Znajdujemy wówczas wektory $w_1, w_2 \in \langle v \rangle_{\mathbb{K}}^{\perp_{\gamma}}$ o własności $\gamma^{\perp}(w_2, w_1) \neq 0$. Zdefiniujemy $v_1 := v +_V w_1$ i dobierzmy skalar $\lambda \in \mathbb{K}$ w taki sposób, iżby było $v +_V \lambda \triangleright_V w_2 \perp_{\gamma} v_1$, czyli

$$0_{\mathbb{K}} = \gamma(v +_V \lambda \triangleright_V w_2, v +_V w_1) = \gamma(v, v) +_{\mathbb{K}} \lambda \cdot_{\mathbb{K}} \gamma(w_2, v) +_{\mathbb{K}} \gamma(v, w_1)$$

$$+_{\mathbb{K}} \lambda \cdot_{\mathbb{K}} \gamma(w_2, w_1) = \gamma(v, v) +_{\mathbb{K}} \lambda \cdot_{\mathbb{K}} \gamma(w_2, w_1).$$

Skalar taki jest dany jednoznacznie wzorem

$$\lambda = -\gamma(w_2, w_1)^{-1} \cdot_{\mathbb{K}} \gamma(v, v).$$

Obliczamy teraz, uwzględniając po drodze $w_2 \perp_{\gamma} v$ i alternujący charakter $\gamma^{\perp}$,

$$\begin{aligned} \gamma(v +_V \lambda \triangleright_V w_2, v +_V \lambda \triangleright_V w_2) &= \gamma(v, v) +_{\mathbb{K}} \lambda \cdot_{\mathbb{K}} \gamma(w_2, v) +_{\mathbb{K}} \gamma(v, w_2) \cdot \bar{\lambda} \\ &\quad +_{\mathbb{K}} \lambda \cdot_{\mathbb{K}} \gamma(w_2, w_2) \cdot_{\mathbb{K}} \bar{\lambda} \\ &= \gamma(v, v) +_{\mathbb{K}} \lambda \cdot_{\mathbb{K}} \gamma^{\perp}(w_2, w_2) \cdot_{\mathbb{K}} \bar{\lambda} = \gamma(v, v) \neq 0_{\mathbb{K}}. \end{aligned}$$

Stwierdzamy zatem, że ograniczenie $\gamma|_{(v_1)_{\mathbb{K}}^{\perp_{\gamma}}}$ nie jest formą alternującą, czyli nie jest przez nie spełniona koniunkcja (i) $\wedge$ (ii) $\wedge$ (iii), to jednak oznacza, że możemy zastosować założenie indukcyjne, zauważwszy uprzednio, że

$$\begin{aligned} \gamma(v_1, v_1) &= \gamma(v, v) +_{\mathbb{K}} \gamma(v, w_1) +_{\mathbb{K}} \gamma(w_1, v) +_{\mathbb{K}} \gamma(w_1, w_1) = \gamma(v, v) +_{\mathbb{K}} \gamma^{\perp}(w_1, w_1) \\ &= \gamma(v, v) \neq 0, \end{aligned}$$

czyli że podprzestrzeń $(v_1)_{\mathbb{K}}$ jest niezwyrodniała.

Na koniec upewniamy się, że (i) $\wedge$ (ii) $\wedge$ (iii) wyklucza istnienie bazy ortogonalnej względem γ . Załóżmy, przeciwnie, że $\{v_i\}_{i \in \overline{1, N}}$ jest taką bazą, czyli

$$\forall_{i, j \in \overline{1, N}} : \gamma(v_i, v_j) = \lambda_i \cdot_{\mathbb{K}} \delta_{i, j}^{\mathbb{K}}$$

dla pewnych skalarów $\lambda_i \in \mathbb{K}$. Skoro γ jest alternująca, to muszą zachodzić równości

$$\forall_{i \in \overline{1, N}} : \lambda_i = \gamma(v_i, v_i) = 0_{\mathbb{K}},$$

a w takim razie $\gamma \equiv 0$, co przeczy (iii). $\square$

Na podstawie powyższego twierdzenia można też wnioskować o okolicznościach, w których baza ortogonalna poddaje się normalizacji.

COROLLARIUM 21. *Przyjmijmy notację Def. 67, 11, 13, 21, 32, 35, 61, 63, 64, 65, 68, 70, 75, 78, 95, 98, 105, 106, 107, 108, 109, 110, 111, 112 i 113, Stw. 75 oraz Przykł. 34 (2) i 35 (2). Niechaj V będzie skończone wymiarową przestrzenią wektorową nad ciałem $\mathbb{K}$, wyposażoną w niezwyrodniałą formę hermitowską γ . Jeśli któryś z warunków (i), (ii) lub (iii) z tezy Tw. 9.1 nie jest spełniony, a do tego*

$$\forall_{v \in V} \exists_{\lambda \in \mathbb{K}} : \gamma(v, v) = \lambda \cdot_{\mathbb{K}} \bar{\lambda},$$

to istnieje w V baza ortonormalna względem γ . $\blacksquare$

Dowód: Niech $\{v_i\}_{i \in \overline{1, N}}$ będzie bazą ortogonalną dla γ , której istnienie gwarantuje Tw. 9.1. Wobec niezwyrodnienia γ mamy

$$\forall_{i \in \overline{1, N}} : \gamma(v_i, v_i) \neq 0_{\mathbb{K}},$$

a zatem

$$\forall_{i \in \overline{1, N}} \exists_{\lambda_i \in \mathbb{K} \setminus \{0_{\mathbb{K}}\}} : \gamma(v_i, v_i) \neq \lambda_i \cdot_{\mathbb{K}} \bar{\lambda}_i.$$

W takim razie układ $\{\lambda_i^{-1} \triangleright_V v_i\}_{i \in \overline{1, N}}$ jest poszukiwaną bazą ortonormalną. $\square$

Należy podkreślić, że założenia corollarium są spełnione, m.in., gdy $J = \text{id}_{\mathbb{K}}$ i ciało $\mathbb{K}$ jest algebraicznie domknięte, albowiem wówczas każdy skalar jest kwadratem innego. Obserwacja ta leży u podstaw procedur *ortonormalizacyjnych* dla form symetrycznych nad $\mathbb{K} = \mathbb{C}$.

Innym istotnym wnioskiem z Tw. 9.1 jest

STWIERDZENIE 157 (O postaci kanonicznej macierzy hermitowskiej). *Przyjmijmy notację Def. 67, 11, 13, 21, 32, 35, 61, 63, 65, 68, 70, 75, 78, 82, 84, 105, 106, 107, 108 i 109, Cor. 14, Stw. 75, 95, 96, 97, 98, 99 i 152, Tw. 8.11 oraz Przykł. 35 (2) i 41. Niechaj $M \in \text{Mat}(\mathbb{K}; N)$ będzie macierzą hermitowską rzędu $\text{rk } M =: r \in \mathbb{N}$. Wtedy i tylko wtedy, gdy któryś z warunków (i), (ii) lub (iii) z tezy Tw. 9.1 nie jest spełniony, istnieje macierz odwracalna $B \in \text{Mat}(\mathbb{K}; N)$ diagonalizująca M wedle formuły*

$$B^T \odot M \odot \overline{B} = \begin{pmatrix} \Lambda & \mathbf{0}_{r \times (N-r)} \\ \mathbf{0}_{(N-r) \times r} & \mathbf{0}_{(N-r) \times (N-r)} \end{pmatrix},$$

w której $\Lambda \in \text{GL}(\mathbb{K}; r)$ jest **macierzą diagonalną**

$$\Lambda = \begin{pmatrix} \lambda_1 & 0_{\mathbb{K}} & 0_{\mathbb{K}} & \cdots & 0_{\mathbb{K}} \\ 0_{\mathbb{K}} & \lambda_2 & 0_{\mathbb{K}} & \cdots & 0_{\mathbb{K}} \\ 0_{\mathbb{K}} & 0_{\mathbb{K}} & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & 0_{\mathbb{K}} \\ 0_{\mathbb{K}} & \cdots & \cdots & 0_{\mathbb{K}} & \lambda_r \end{pmatrix} =: \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_r)$$

o niezerowych wyrazach na przekątnej $\lambda_i \neq 0_{\mathbb{K}}$, $i \in \overline{1, r}$ spełniających relacje samosprężenia

$$\forall_{i \in \overline{1, r}} : \overline{\lambda_i} = \lambda_i.$$

■

Dowód: Wybierzmy w V bazę $\{v_i\}_{i \in \overline{1, N}}$ i zdefiniujmy formę hermitowską γ_M stowarzyszoną z M jak w tezie Stw. 152. Na mocy Tw. 9.1 w przestrzeni V istnieje baza $\mathcal{B}' := \{w_i\}_{i \in \overline{1, N}}$ ortogonalna względem γ_M ,

$$\forall_{i, j \in \overline{1, N}} : \gamma_M(w_i, w_j) = \lambda_i \cdot_{\mathbb{K}} \delta_{i, j}^{\mathbb{K}},$$

przy czym zawsze możemy tak uporządkować jej elementy, aby niezerowe skalary $\lambda_i \neq 0_{\mathbb{K}}$ odpowiadały pierwszym $\text{rk } \gamma_M \equiv \text{rk } M$ wektorom bazy $\mathcal{B}'$. Wówczas

$$B := [\text{id}_V]_{\mathcal{B}'}$$

jest pożądaną macierzą diagonalizującą M , jawnie odwracalną. Pozostaje upewnić się, że skalary λ_i spełniają relacje samosprężenia, wykorzystując w tym celu hermitowskość formy γ_M ,

$$\forall_{i \in \overline{1, N}} : \overline{\lambda_i} = \overline{\gamma_M(w_i, w_i)} = \gamma_M(w_i, w_i) = \lambda_i.$$

□

Celem ilustracji wypowiedzianych wcześniej tez przedstawimy obecnie prostą i dość powszechnie stosowaną konstrukcję bazy ortogonalnej dla pewnej klasy niezwyrodniałych form hermitowskich.

STWIERDZENIE 158 (Ortogonalizacja Grama–Schmidta). *Przyjmijmy notację Def. 67, 11, 13, 21, 32, 35, 61, 63, 64, 65, 68, 70, 75, 78, 82, 87, 89, 91, 95, 98, 105, 106, 107, 108, 109, 110, 111, 112 i 113, Stw. 75 oraz Przykł. 34 (2), 35 (2) i 41. Niechaj V będzie przestrzenią wektorową nad ciałem $\mathbb{K}$ wyposażoną w formę hermitowską γ i niech $\{v_i\}_{i \in I \subset \mathbb{N}} \subset V$ będzie rodziną wektorów liniowo niezależnych o tej własności, że dla dowolnego $N \in I$ podprzestrzeń $V_N := \langle v_1, v_2, \dots, v_N \rangle_{\mathbb{K}}$ jest niezwyrodniała (względem γ). Zdefiniujmy rodzinę macierzy*

$$G(N) : \overline{1, N} \times \overline{1, N} \longrightarrow \mathbb{K} : (i, j) \longmapsto \gamma(v_i, v_j),$$

indeksowaną przez liczby $N \in I$. Wektory

$$e_n := \sum_{j=1}^n \left(\left(\overline{G(n)}^n_n \right)^{-1} \cdot_{\mathbb{K}} \overline{G(n)}^n_j \right) \triangleright_V v_j, \quad n \in \overline{1, N},$$

zapisane w notacji Def. 91 i dla $\overline{G(1)}^1_1 := 1_{\mathbb{K}}$, tworzą bazę ortogonalną V_N dla dowolnego N , a przy tym

$$\forall_{n \in \overline{1, N}} : \gamma(e_n, e_n) = \left(\overline{G(n)}^n_n \right)^{-1} \cdot_{\mathbb{K}} \det_{(n)}(G(n)).$$

■

Dowód: Niezwyrodnienie $\gamma_N := \gamma|_{V_N \times V_N}$ jest – wobec $\dim_{\mathbb{K}} V_N = N < \infty$ – równoważne bijektywności odwzorowania $J_* \circ r_{\gamma_N} : V_N \longrightarrow V^*$. Macierz tego ostatniego względem baz: $\mathcal{B} := \{v_i\}_{i \in \overline{1, N}}$ w V_N i dualnej do niej $\mathcal{B}^* := \{v_i^*\}_{i \in \overline{1, N}}$ w V_N^* przyjmuje postać

$$\begin{aligned} [J_* \circ r_{\gamma_N}]_{\mathcal{B}}^{\mathcal{B}^*} &= \left(\langle J_* \circ r_{\gamma_N}(v_i), v_j^* \rangle \right)_{i, j \in \overline{1, N}} \equiv \left(\langle v_j, J_* \circ r_{\gamma_N}(v_i) \rangle \right)_{i, j \in \overline{1, N}} \\ &= \left(\overline{\gamma(v_j, v_i)} \right)_{i, j \in \overline{1, N}} = (\gamma(v_i, v_j))_{i, j \in \overline{1, N}} \equiv G(N). \end{aligned}$$

Wobec tego zerowanie się wyznacznika macierzy $G(N)$ implikowałoby nieistnienie odwrotności (macierzy) $J_* \circ r_{\gamma_N}$, co byłoby sprzeczne z wyjściowym założeniem. Argument ten pokazuje, że wektory e_n są dobrze określone.

Zauważmy dalej, że

$$\forall_{N \in I} : e_N - v_N \in V_{N-1},$$

co oznacza liniową niezależność układu $\{e_n\}_{n \in \overline{1, N}}$, z której dalej wynika, że układ ten jest bazą przestrzeni V_N . Przy tym dla każdego $n < N$ zachodzi – na mocy Tw. 8.13 –

$$\begin{aligned} \gamma(e_N, v_n) &= \left(\overline{G(N)}^N_N \right)^{-1} \cdot_{\mathbb{K}} \sum_{i=1}^N \overline{G(N)}^N_i \cdot_{\mathbb{K}} \gamma(v_i, v_n) \\ &\equiv \left(\overline{G(N)}^N_N \right)^{-1} \cdot_{\mathbb{K}} \sum_{i=1}^N \overline{G(N)}^N_i \cdot_{\mathbb{K}} G(N)^i_n \\ &= \left(\overline{G(N)}^N_N \right)^{-1} \cdot_{\mathbb{K}} \det_{(N)}(G(N)) \cdot_{\mathbb{K}} \delta_{N,n}^{\mathbb{K}} = 0_{\mathbb{K}}, \end{aligned}$$

czyli

$$e_N \perp_{\gamma} V_{N-1},$$

a zatem – w szczególności –

$$\forall_{n < N \in I} : e_N \perp_\gamma e_n.$$

Na koniec liczymy, wykorzystując wyniki wcześniejsze,

$$\begin{aligned} \gamma(e_N, e_N) &= \left(\overline{G(N)}_N^N \right)^{-1} \cdot_{\mathbb{K}} \sum_{i=1}^N \overline{G(N)}_i^N \cdot_{\mathbb{K}} \gamma(v_i, e_N) \\ &= \left(\overline{G(N)}_N^N \right)^{-1} \cdot_{\mathbb{K}} \overline{G(N)}_N^N \cdot_{\mathbb{K}} \gamma(v_N, e_N) \\ &= \gamma(v_N, e_N) = \sum_{j=1}^N \gamma(v_N, v_j) \cdot_{\mathbb{K}} J \left(\overline{G(N)}_j^N \right) \cdot_{\mathbb{K}} J \left(\overline{G(N)}_N^N \right)^{-1} \\ &= \sum_{j=1}^N J \left(\overline{G(N)}_j^N \cdot_{\mathbb{K}} G(N)_j^N \right) \cdot_{\mathbb{K}} J \left(\overline{G(N)}_N^N \right)^{-1} \\ &= J \left(\det_{(N)} (G(N)) \right) \cdot_{\mathbb{K}} J \left(\overline{G(N)}_N^N \right)^{-1} \\ &\equiv J \left(\det_{(N-1)} (G(N-1))^{-1} \cdot_{\mathbb{K}} \det_{(N)} (G(N)) \right). \end{aligned}$$

Ostatnia część tezy wynika zatem wprost z ciągu równości, wypisanego dla dowolnego $N \in I$,

$$\begin{aligned} J \left(\det_{(N)} (G(N)) \right) &= \det_{(N)} (J(G(N))) \equiv \det_{(N)} \left(\left(\overline{\gamma(v_i, v_j)} \right)_{i,j \in \overline{1,N}} \right) \\ &= \det_{(N)} \left(\left(\gamma(v_j, v_i) \right)_{i,j \in \overline{1,N}} \right) \equiv \det_{(N)} (G(N)^T) \\ &= \det_{(N)} (G(N)). \end{aligned}$$

□

Dotychczasowe nasze dociekania każą nam wyróżnić

DEFINICJA 115. Przyjmijmy notację Def. 11, 13, 21, 32, 35, 61, 63, 105, 106, 107, 108 i 109 oraz Przykł. 35 (2). Niechaj $((V, +_V, P_V, \bullet \mapsto 0_V), \ell_V, \gamma)$ będzie przestrzenią $(\epsilon = 1_{\mathbb{K}})$ -hermitowską nad ciałem $\mathbb{K}$. Jej automorfizmy określamy mianem **automorfizmów unitarnych** (lub **transformacji unitarnych**), generowaną zaś przez nie grupę

$$U(\gamma) := \text{Aut}_{\mathbb{K}}(V, \gamma)$$

nazywamy **grupą unitarną stowarzyszoną z γ** . W szczególności w przypadku przestrzeni $V := \mathbb{K}^{\times N}$, $N \in \mathbb{N}$ wyposażonej w formę hermitowską o macierzy względem bazy standardowej danej przez macierz jednostkową stopnia N otrzymujemy w ten sposób **grupę unitarną stopnia N o współczynnikach z $\mathbb{K}$** , oznaczaną symbolem

$$U(N; \mathbb{K}) \equiv U_N(\mathbb{K}).$$

Macierz transformacji unitarnej $U \in U(N; \mathbb{K})$ względem bazy standardowej nazywamy **macierzą unitarną (stopnia N)**.

▲

Mamy oczywiste

STWIERDZENIE 159. *Przyjmijmy notację Def. 11, 13, 21, 32, 35, 61, 63, 105, 106, 107, 108, 109 i 115 oraz Przykł. 35 (2). Dowolna macierz unitarna $U \in \text{Mat}(\mathbb{K}; N)$, $N \in \mathbb{N}$ spełnia tożsamość*

$$U^\dagger \odot U = \mathbf{1}_N.$$

W szczególności jest ona macierzą odwracalną.

■

Na zakończenie dyskusji form hermitowskich ograniczymy nasze rozważania do przypadków o szczególnym znaczeniu fizycznym, a mianowicie $(\mathbb{K}, J) \in \{(\mathbb{R}, \text{id}_{\mathbb{R}}), (\mathbb{C}, \cdot)\}$. Możemy w tych przypadkach określić

DEFINICJA 116. Przyjmijmy notację Def. 11, 14, 18, 13, 21, 32, 35, 61, 63, 105, 106, 107, 108 i 109 oraz Przykł. 35 (2). Niechaj $(\mathbb{K}, J) \in \{(\mathbb{R}, \text{id}_{\mathbb{R}}), (\mathbb{C}, \cdot)\}$. Formę hermitowską γ na przestrzeni wektorowej V nad $\mathbb{K}$ nazywamy **dodatnio półokreśloną** (lub po prostu **dodatnią**), co zapisujemy symbolicznie jako

$$\gamma \geq 0,$$

jeśli spełnia ona warunek

$$\forall_{v \in V} : \gamma(v, v) \geq 0.$$

Analogicznie, γ nazywamy **ujemnie półokreśloną** (lub po prostu **ujemną**), co zapisujemy symbolicznie jako

$$\gamma \leq 0,$$

jeśli spełnia ona warunek

$$\forall_{v \in V} : \gamma(v, v) \leq 0.$$

Jeżeli jedynym wektorem, dla którego powyższe nierówności ulegają wysyceniu, jest wektor zerowy, tj. zachodzi

$$\gamma(v, v) = 0 \implies v = 0_V,$$

mówimy o formie **dodatnio** lub – odpowiednio – **ujemnie określonej** i piszemy $\gamma > 0$ lub – odpowiednio – $\gamma < 0$.

▲

Ażeby móc pokusić się o sformułowanie wygodnego kryterium dodatniej określoności formy hermitowskiej, udowodnimy proste acz ważne

STWIERDZENIE 160 (Nierówność Schwarza). *Przyjmijmy notację Def. 11, 14, 18, 13, 21, 32, 35, 61, 63, 105, 106, 107, 108, 109 i 116 oraz Przykł. 35 (2). Niechaj $(\mathbb{K}, J) \in \{(\mathbb{R}, \text{id}_{\mathbb{R}}), (\mathbb{C}, \cdot)\}$. Forma hermitowska γ dodatnio półokreślona na przestrzeni wektorowej V nad $\mathbb{K}$ spełnia relację*

$$\forall_{v, w \in V} : \gamma(v, w) \cdot_{\mathbb{K}} \overline{\gamma(v, w)} \leq \gamma(v, v) \cdot_{\mathbb{K}} \gamma(w, w),$$

zwaną nierównością Schwarza.

■

Dowód: Ilekcć wektory v i w są liniowo zależne, nierówność jest trywialnie spełniona, założmy więc, że podprzestrzeń $\langle v, w \rangle_{\mathbb{K}} \subset V$ jest dwuwymiarowa i ograniczmy γ do tej podprzestrzeni, oznaczając

$$\tilde{\gamma} := \gamma|_{\langle v, w \rangle_{\mathbb{K}}}.$$

Wprost z założenia wynika, że $\tilde{\gamma}$ jest dodatnio półokreśloną formą hermitowską na $\langle v, w \rangle_{\mathbb{K}}$, istnieje zatem – na mocy Tw. 9.1 – baza $\mathcal{B} := \{v_1, v_2\}$ w $\langle v, w \rangle_{\mathbb{K}}$ ortogonalna względem $\tilde{\gamma}$, w której obliczamy

$$\det_{(2)}([\tilde{\gamma}]_{\mathcal{B}}) = \tilde{\gamma}(v_1, v_1) \cdot_{\mathbb{K}} \tilde{\gamma}(v_2, v_2) \geq 0.$$

Wobec swojej liniowej niezależności bazę tworzą także wektory $\{v, w\}$, korzystając zatem ze Stw. 112, 114 i 153, otrzymujemy pożądaný wynik

$$\begin{aligned} \gamma(v, v) \cdot_{\mathbb{K}} \gamma(w, w) - \gamma(v, w) \cdot_{\mathbb{K}} \overline{\gamma(v, w)} &\equiv \tilde{\gamma}(v, v) \cdot_{\mathbb{K}} \tilde{\gamma}(w, w) - \tilde{\gamma}(v, w) \cdot_{\mathbb{K}} \tilde{\gamma}(w, v) \\ &= \det_{(2)}([\tilde{\gamma}]_{\{v, w\}}) = \det_{(2)}\left(\left([\text{id}_{\langle v, w \rangle_{\mathbb{K}}}]_{\{v, w\}}^{\mathcal{B}}\right)^T \odot [\tilde{\gamma}]_{\mathcal{B}} \odot \overline{[\text{id}_{\langle v, w \rangle_{\mathbb{K}}}]_{\{v, w\}}^{\mathcal{B}}}\right) \\ &= \det_{(2)}\left(\left([\text{id}_{\langle v, w \rangle_{\mathbb{K}}}]_{\{v, w\}}^{\mathcal{B}}\right)^T\right) \cdot_{\mathbb{K}} \det_{(2)}\left(\overline{[\text{id}_{\langle v, w \rangle_{\mathbb{K}}}]_{\{v, w\}}^{\mathcal{B}}}\right) \cdot_{\mathbb{K}} \det_{(2)}([\tilde{\gamma}]_{\mathcal{B}}) \\ &= \det_{(2)}([\text{id}_{\langle v, w \rangle_{\mathbb{K}}}]_{\{v, w\}}^{\mathcal{B}}) \cdot_{\mathbb{K}} \overline{\det_{(2)}([\text{id}_{\langle v, w \rangle_{\mathbb{K}}}]_{\{v, w\}}^{\mathcal{B}})} \cdot_{\mathbb{K}} \det_{(2)}([\tilde{\gamma}]_{\mathcal{B}}) \geq 0. \end{aligned}$$

□

Natychmiastową konsekwencją powyższej nierówności jest

COROLLARIUM 22. *Przyjmijmy notację Def. 11, 14, 18, 13, 21, 32, 35, 61, 63, 105, 106, 107, 108, 109 i 116 oraz Przykł. 35 (2). Niechaj $(\mathbb{K}, J) \in \{(\mathbb{R}, \text{id}_{\mathbb{R}}), (\mathbb{C}, \cdot)\}$. Zbiór wektorów w przestrzeni V nad ciałem $\mathbb{K}$ izotropowych względem dodatnio półokreślonej formy hermitowskiej γ rozpina podprzestrzeń $V^{\perp \gamma}$. Forma γ jest zatem niezwyrodniała wtedy i tylko wtedy, gdy spełniony jest warunek*

$$\forall v \in V \setminus \{0_V\} : \gamma(v, v) > 0,$$

czyli, innymi słowy,

$$\gamma > 0 \iff (\gamma \geq 0 \wedge \text{Ker } \gamma = \{0_V\}).$$

■

Dowód: Każdy wektor $v \in V^{\perp \gamma}$ jest izotropowy wprost z definicji, ale też dla kaźdego wektora izotropowego v i dowolnego wektora $w \in V$ otrzymujemy nierówność

$$\gamma(v, w) \cdot_{\mathbb{K}} \overline{\gamma(v, w)} \leq \gamma(v, v) \cdot_{\mathbb{K}} \gamma(w, w) = 0,$$

która implikuje równość

$$\gamma(v, w) = 0,$$

ta zaś wobec dowolności wyboru w oznacza, że $v \in V^{\perp \gamma}$.

□

Niezwyrodniały dodatnio półokreślone formy hermitowskie dostarczają uogólnienia pojęcia “długości wektora” znanego (pod postacią wzoru Pitagorasa) z elementarnej geometrii euklidesowej przestrzeni $\mathbb{R}^{x^n}$. Omówimy je nieco dokładniej w dalszej części kursu, a tymczasem wprowadźmy jedynie

DEFINICJA 117. Przyjmijmy notację Def. 11, 13, 14, 18, 21, 32, 35, 61, 63, 105, 106, 107, 108, 109 i 116 oraz Przykł. 35 (2). Niechaj $(\mathbb{K}, J) \in \{(\mathbb{R}, \text{id}_{\mathbb{R}}), (\mathbb{C}, \cdot)\}$. Dowolną dodatnio określoną formę hermitowską γ na przestrzeni wektorowej V nad $\mathbb{K}$ określamy mianem **iloczynu skalarnego**. ▲

Możemy już teraz wypowiedzieć

STWIERDZENIE 161. Przyjmijmy notację Def. 11, 14, 18, 13, 21, 32, 35, 61, 63, 105, 106, 107, 108, 109 i 116 oraz Przykł. 35 (2). Niechaj $(\mathbb{K}, J) \in \{(\mathbb{R}, \text{id}_{\mathbb{R}}), (\mathbb{C}, \cdot)\}$ i niech V będzie przestrzenią wektorową nad $\mathbb{K}$ wymiaru $N := \dim_{\mathbb{K}} V < \infty$ wyposażoną w formę hermitowską γ . Wybierzmy w V bazę $\mathcal{B} := \{v_i\}_{i \in \overline{1, N}}$ i zdefiniujmy, dla dowolnego $n \in \overline{1, N}$,

$$G(n) := (\gamma(v_i, v_j))_{i, j \in \overline{1, n}}.$$

Prawdziwą jest równoważność

$$\gamma > 0 \iff \forall_{n \in \overline{1, N}} : \det_{(n)}(G(n)) > 0.$$
■

Dowód:

$\Rightarrow$ Skoro $\gamma > 0$, to także $\gamma_n := \gamma|_{V_n \times V_n} > 0$ dla dowolnej podprzestrzeni $V_n := \langle v_1, v_2, \dots, v_n \rangle_{\mathbb{K}}$, jest zatem γ_n dodatnio określoną formą hermitowską na V_n . Istnieje zatem w V_n – na mocy Tw. 9.1 – baza $\mathcal{B}$ ortogonalna względem γ_n , przy czym wszystkie wyrazy (diagonalne) macierzy $[\gamma_n]_{\mathcal{B}}$ są dodatnie. Z porównania wyznacznika tej macierzy z wyznacznikiem macierzy $[\gamma_n]_{\mathcal{B}'}$ formy γ_n względem bazy $\mathcal{B}' := \{v_1, v_2, \dots, v_n\}$ wynika, po uwzględnieniu odwracalności macierzy przejścia między tymi bazami, pożądana nierówność

$$\begin{aligned} \det_{(n)}(G(n)) &\equiv \det_{(n)}([\gamma_n]_{\mathcal{B}'}) \\ &= \det_{(n)}([\text{id}_{V_n}]_{\mathcal{B}'}) \cdot \overline{\det_{(n)}([\text{id}_{V_n}]_{\mathcal{B}})} \cdot {}_{\mathbb{K}} \det_{(n)}([\gamma_n]_{\mathcal{B}}) \\ &> 0. \end{aligned}$$

$\Leftarrow$ Wystarczy zastosować procedurę ortonormalizacyjną opisaną w Stw. 158 po uprzednim wykorzystaniu pierwszego kroku jego dowodu celem upewnienia się o niezwyrodnieniu V_n względem γ . □

Wykorzystując wprowadzone powyżej pojęcia, jesteśmy w stanie precyzyjnie scharakteryzować strukturę przestrzeni $(\epsilon = 1_{\mathbb{K}})$ -hermitowskiej nad ciałami liczbowymi $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$.

TWIERDZENIE 9.3 (Sylwestera prawo bezwładności). Przyjmijmy notację Def. 67, 11, 14, 18, 13, 21, 32, 35, 61, 63, 64, 65, 68, 70, 75, 78, 95, 98, 105, 106, 107, 108, 109, 110, 111, 112, 113, 116, Stw. 156 i 157 oraz Przykł. 34 (2) i 35 (2). Niechaj $(\mathbb{K}, J) \in \{(\mathbb{R}, \text{id}_{\mathbb{R}}), (\mathbb{C}, \cdot)\}$ i niech $((V, +_V, P_V, \bullet \mapsto 0_V), \ell_V, \gamma)$ będzie

przestrzeni $(\epsilon = 1_{\mathbb{K}})$ -hermitowską wymiaru $N := \dim_{\mathbb{K}} V < \infty$ nad $\mathbb{K}$. Wówczas V rozkłada się na sumę ortogonalną

$$V = V_0 \oplus V_+ \oplus V_-$$

podprzestrzeni $V_0 \subset V$ oraz niezwyrodniałych $V_{\pm} \subset V$ określonych przez warunki

$$\gamma|_{V_0 \times V_0} = 0, \quad \gamma|_{V_+ \times V_+} \geq 0, \quad \gamma|_{V_- \times V_-} \leq 0.$$

Co więcej, istnieje baza ortogonalna $\mathcal{B} := \{v_i\}_{i \in \overline{1, N}}$ przestrzeni V o tej własności, że macierz γ względem $\mathcal{B}$ ma postać

$$[\gamma]_{\mathcal{B}} = \text{diag}(\underbrace{1_{\mathbb{K}}, 1_{\mathbb{K}}, \dots, 1_{\mathbb{K}}}_{s_+ \text{ razy}}, \underbrace{-1_{\mathbb{K}}, -1_{\mathbb{K}}, \dots, -1_{\mathbb{K}}}_{s_- \text{ razy}}, \underbrace{0_{\mathbb{K}}, 0_{\mathbb{K}}, \dots, 0_{\mathbb{K}}}_{N-(s_++s_-) \text{ razy}}).$$

Przy tym wymiary $\mathbb{K}$ -liniowe $s_{\pm} := \dim_{\mathbb{K}} V_{\pm}$ nie zależą od wyboru rozkładu opisanego powyżej, a nadto spełniają tożsamości

$$s_{\pm} := \max_{\substack{W \subset V \\ \pm \gamma|_{W \times W} \geq 0 \text{ niezwyrodniała}}} \{ \dim_{\mathbb{K}} W \}, \quad s_+ + s_- = \text{rk } \gamma.$$

■

Dowód: Wybierzmy bazę ortogonalną $\mathcal{B} := \{v_i\}_{i \in \overline{1, N}}$ przestrzeni V , której istnienie orzeka Tw. 9.1. Skoro

$$\forall_{v \in V} : \gamma(v, v) \in \mathbb{R},$$

to możemy uporządkować elementy tej bazy tak, by było

$$\forall_{i \in \overline{1, s_+}} : \gamma(v_i, v_i) > 0 \quad \wedge \quad \forall_{j \in \overline{s_++1, s_++s_-}} : \gamma(v_j, v_j) < 0$$

$$\wedge \quad \forall_{k \in \overline{s_++s_-+1, N}} : \gamma(v_k, v_k) = 0$$

dla pewnych liczb naturalnych $s_{\pm} \leq N$. Mamy wtedy

$$V_+ := \langle v_1, v_2, \dots, v_{s_+} \rangle_{\mathbb{K}}, \quad V_- := \langle v_{s_++1}, v_{s_++2}, \dots, v_{s_++s_-} \rangle_{\mathbb{K}},$$

$$V_0 := \langle v_{s_++s_-+1}, v_{s_++s_-+2}, \dots, v_N \rangle_{\mathbb{K}},$$

a więc też i rozkład

$$(9.1) \quad V = V_0 \oplus V_+ \oplus V_-.$$

Ponieważ zaś

$$\forall_{i \in \overline{1, s_+}} : \gamma(v_i, v_i) = \sqrt{\gamma(v_i, v_i)}^2 \quad \wedge \quad \forall_{j \in \overline{s_++1, s_++s_-}} : \gamma(v_j, v_j) = -\sqrt{-\gamma(v_j, v_j)}^2,$$

przeto możemy wybrać jako bazę ortogonalną tę utworzoną przez wektory

$$e_i := \sqrt{\gamma(v_i, v_i)}^{-1} \triangleright_V v_i, \quad i \in \overline{1, s_+},$$

$$e_j := \sqrt{-\gamma(v_j, v_j)}^{-1} \triangleright_V v_j, \quad j \in \overline{s_++1, s_++s_-},$$

$$e_k := v_k, \quad k \in \overline{s_++s_-+1, N}.$$

Rozważmy następnie podprzestrzeń $P \subset V$, na której $\gamma|_{P \times P} \geq 0$ jest niezwyrodniała. Zachodzi oczywista relacja

$$P \cap (V_0 \oplus V_-) = \{0_V\},$$

albowiem dowolny wektor $v \in P \cap (V_0 \oplus V_-)$ spełnia warunek $\gamma(v, v) \geq 0$, a zarazem jeśli przedstawić go jako sumę $v = v_0 + v_-$ składowych $v_0 \in V_0$ i $v_- \in V_-$, to także $\gamma(v, v) = \gamma(v_-, v_-) \leq 0$, a wynikająca stąd równość $\gamma(v, v) = 0$ implikuje natychmiast (wobec znanej postaci $\gamma|_{V_- \times V_-}$ w użytej wyżej bazie ortogonalnej) $v_- = 0_V$, czyli też $v \in P \cap V_0$, a zatem $v = 0_V$ z racji niezwyrodnienia $\gamma|_{P \times P}$. W takim razie, jak poucza Stw. 85, suma

$$P +_V (V_0 \oplus V_-) \subset V = V_0 \oplus V_+ \oplus V_-$$

jest prosta, skąd dalej wniosek, wyciągnięty na podstawie Stw. 83 i 86, że

$$\dim_{\mathbb{K}} P + \dim_{\mathbb{K}} (V_0 \oplus V_-) = \dim_{\mathbb{K}} (P +_V (V_0 \oplus V_-)) \leq \dim_{\mathbb{K}} (V_+) + \dim_{\mathbb{K}} (V_0 \oplus V_-),$$

czyli

$$\dim_{\mathbb{K}} P \leq \dim_{\mathbb{K}} (V_+) = s_+.$$

Analogicznie dowodzimy relacji

$$\dim_{\mathbb{K}} N \leq \dim_{\mathbb{K}} (V_-) = s_- ,$$

spełnionej dla dowolnej podprzestrzeni $N \subset V$, na której $\gamma|_{N \times N} \leq 0$ jest niezwyrodniała.

Równość $s_+ + s_- = \text{rk } \gamma$ wynika wprost z Def. 108, dla zakończenia dowodu wystarczy zatem pokazać niezależność $s_{\pm}$ od wyboru podprzestrzeni $V_{\pm}$ w rozkładzie (9.1). Niech $\mathcal{B}' := \{w_i\}_{i \in \overline{1, N}}$ będzie bazą ortogonalną V odpowiadającą nowemu rozkładowi (w którym składnik $V_0 \equiv \text{Ker } \gamma$ pozostaje oczywiście ten sam)

$$V = V_0 \oplus W_+ \oplus W_- ,$$

przy czym

$$W_+ := \langle w_1, w_2, \dots, w_{t_+} \rangle_{\mathbb{K}} , \quad W_- := \langle w_{t_++1}, w_{t_++2}, \dots, w_{t_++t_-} \rangle_{\mathbb{K}}$$

dla pewnych liczb naturalnych $t^+, t^- \leq \text{rk } \gamma$. Pokażemy równość $s_- = t_-$. W tym celu wystarczy się przekonać, że układ

$$\{v_1, v_2, \dots, v_{s_+}, w_{t_++1}, w_{t_++2}, \dots, w_{t_++t_-}\}$$

jest liniowo niezależny, bo wtedy – na mocy Stw. 78 –

$$s_+ + t_- \leq s_+ + s_- \iff t_- \leq s_- ,$$

a z racji symetrii także

$$s_- \leq t_- ,$$

czyli ostatecznie $s_- = t_-$. Niech zatem będzie dana rodzina skalarów $\{\lambda^l\}_{l \in \overline{1, s_+ \cup t_++1, t_++t_-}}$ o własności

$$\sum_{l=1}^{s_+} \lambda^l \triangleright_V v_l +_V \sum_{m=t_++1}^{t_++t_-} \lambda^m \triangleright_V w_m = 0_V ,$$

czyli

$$v_L := \sum_{l=1}^{s_+} \lambda^l \triangleright_V v_l = - \sum_{m=t_++1}^{t_++t_-} \lambda^m \triangleright_V w_m =: v_R .$$

Wykorzystując ortogonalność baz $\mathcal{B}$ i $\mathcal{B}'$, obliczamy

$$\sum_{l=1}^{s_+} \lambda^l \cdot_{\mathbb{K}} \overline{\lambda^l} \cdot_{\mathbb{K}} \gamma(v_l, v_l) = \gamma(v_L, v_L) \equiv \gamma(v_R, v_R) = \sum_{m=t_++1}^{t_++t_-} \lambda^m \cdot_{\mathbb{K}} \overline{\lambda^m} \cdot_{\mathbb{K}} \gamma(w_m, w_m) ,$$

a ponieważ $\gamma(v_l, v_l) > 0 > \gamma(w_m, w_m)$, więc koniecznie

$$\forall_{l \in \overline{1, s_+}} : \lambda^l = 0_K \quad \wedge \quad \forall_{m \in \overline{t_+ + 1, t_+ + t_-}} : \lambda^m = 0_K.$$

□

Powyższe rozważania prowadzą do

DEFINICJA 118. Przyjmijmy notację Def. 67, 11, 13, 21, 32, 35, 61, 63, 64, 65, 68, 70, 75, 78, 95, 98, 105, 106, 107, 108, 109, 110, 111, 112, 113 i 116, Stw. 156 i 157, Tw. 9.3 oraz Przykł. 34 (2) i 35 (2). Parę liczb $(s_+, s_-) \in \mathbb{N}^{\times 2}$ zdefiniowanych w Tw. 9.3 nazywamy **sygnaturą formy hermitowskiej** γ i zapisujemy jako

$$\text{sign}(\gamma) := (s_+, s_-).$$

▲

Nader istotnym elementem teorii form hermitowskich jest ich związek z pewnymi wyróżnionymi klasami endomorfizmów ich dziedziny, analogiczny do związku między formami dwuliniowymi a endomorfizmami ich dziedziny, opisanego w Stw. 124. Rozważania dotychczasowe dają w tym kontekście natychmiastowy i strukturalnie bogaty wgląd w teorię widmową dla szerokiej klasy endomorfizmów i stanowią punkt wyjścia do dyskusji ich postaci kanonicznych. Zanim przejdziemy do szczegółowej analizy tych zagadnień, zbadamy jeszcze pokrótce formy hermitowskie o pierwszorzędym znaczeniu w geometrii różniczkowej i analizie funkcjonalnej oraz stowarzyszonych działach fizyki uprawianych nad ciałem liczb rzeczywistych, tj. formy symetryczne, jak również formy skośnie symetryczne, które spotykamy w kanonicznym opisie klasycznych i kwantowych teorii pola oraz w geometrycznym opisie pola elektromagnetycznego.

9.3. Przestrzenie symetryczne i formy kwadratowe

Naturalnym polem zastosowań form symetrycznych jest geometria różniczkowa przestrzeni topologicznych lokalnie modelowanych na (podzbiorach) przestrzeni euklidesowej $\mathbb{R}^n$ oraz analiza funkcjonalna na nich uprawiana. Pomiar odległości i upływu czasu oraz geometryczny opis propagacji światła w otaczającej nas czasoprzestrzeni to ledwie najprostsze i najbardziej oczywiste z tych zastosowań, o innych opowie przyszłosemestralny kurs geometrii różniczkowej. W niniejszym rozdziale położymy główny nacisk na te aspekty ogólnej teorii przestrzeni wektorowych wyposażonych w formy symetryczne, które nie są jedynie prostą parafrazą obserwacji poczynionych w rozdziale poprzednim w odniesieniu do szerszej klasy form hermitowskich.

Nasze rozważania zaczniemy od uporządkowania relacji pomiędzy formami symetrycznymi a pewną istotną klasą odwzorowań jednorodnych określonych na przestrzeniach wektorowych, które – jak pokażemy w Rozdz. 12 – dostarczają matematycznych narzędzi opisu pól fermionowych na czasoprzestrzeni poprzez konstrukcję struktur zwanych **algebrami Clifforda** i ich **reprezentacji spinorowych**. Odwzorowania te wprowadza

DEFINICJA 119. Przyjmijmy notację Def. 67, 11, 13, 21, 32, 35, 36, 61, 63, 64, 65, 68, 70, 75, 78, 95, 96, 98, 105, 106, 107, 108, 109, 110, 111, 112, 113, 116 i 118, Stw. 156 i 157, Tw. 9.3 oraz Przykł. 34 (2) i 35 (2). Niechaj $\mathbb{K}$ będzie ciałem

i niech V będzie przestrzenią wektorową nad $\mathbb{K}$. **Forma kwadratowa** na V to odwzorowanie

$$Q : V \longrightarrow \mathbb{K}$$

jednorodnego stopnia 2, tj. spełniające warunek

$$\forall_{(\lambda, v) \in \mathbb{K} \times V} : Q(\lambda \triangleright_V v) = \lambda^2 \cdot_{\mathbb{K}} Q(v),$$

i o tej własności, że odwzorowanie

$$\Phi_Q : V \times V \longrightarrow \mathbb{K} : (v, w) \longmapsto Q(v +_V w) - Q(v) - Q(w)$$

jest formą dwuliniową na V . Formę tę, jawnie symetryczną, określamy mianem **formy dwuliniowej stowarzyszonej z Q** . **Jądro formy kwadratowej** to podprzestrzeń

$$\text{Ker } Q := \text{Ker } \Phi_Q \subset V.$$

Formę kwadratową Q nazywamy **niezwyrodniałą** (wzgl. **zwyrodniałą**), jeśli $\text{Ker } Q = \{0_V\}$ (wzgl. $\text{Ker } Q \neq \{0_V\}$).

Wektory tudzież **(pod)przestrzenie wzajem ortogonalne** (wzgl. **izotropowe**) **względem formy kwadratowej Q** to wektory lub – odpowiednio – przestrzenie o tej samej cesze względem formy symetrycznej Φ_Q . Analogicznie definiujemy **sumę ortogonalną**, **bazę ortogonalną** oraz **bazę ortonormalną względem formy kwadratowej Q** .

indexbaza!ortonormalna!względem formy kwadratowej I wreszcie **sygnatura formy kwadratowej Q** to sygnatura formy (hermitowskiej) Φ_Q ,

$$\text{sign}(Q) := \text{sign}(\Phi_Q).$$

Przestrzeń kwadratowa to para $((V, +_V, \text{P}_V, \bullet \longmapsto 0_V), \ell_V, Q)$ złożona z przestrzeni wektorowej $((V, +_V, \text{P}_V, \bullet \longmapsto 0_V), \ell_V)$ nad ciałem $\mathbb{K}$ oraz formy kwadratowej Q na niej określonej.

▲

Związek między symetrycznymi formami dwuliniowymi a formami kwadratowymi, zasygnalizowany już w samej definicji tych ostatnich, ustala²

STWIERDZENIE 162. *Przyjmijmy notację Def. 11, 32 i 61 oraz Przykł. 11 i niech V będzie przestrzenią wektorową nad ciałem $\mathbb{K}$. Jeśli $\text{char } \mathbb{K} \neq 2$, to istnieje wzajemnie jednoznaczna odpowiedniość między formami kwadratowymi i symetrycznymi formami dwuliniowymi na V .*

■

Dowód: Warunek $\text{char } \mathbb{K} \neq 2$ gwarantuje odwracalność skalaru $2_{\mathbb{K}} := 1_{\mathbb{K}} +_{\mathbb{K}} 1_{\mathbb{K}}$ w ciele, tj. istnienie $2_{\mathbb{K}}^{-1} \in \mathbb{K}$. Możemy zatem stowarzyszyć z dowolną symetryczną formą dwuliniową Φ na V formę kwadratową

$$Q_{\Phi} : V \longrightarrow \mathbb{K} : v \longmapsto 2_{\mathbb{K}}^{-1} \cdot_{\mathbb{K}} \Phi(v, v).$$

²W przypadku $\text{char } \mathbb{K} = 2$ także można określić relację między formami kwadratowymi a symetrycznymi formami dwuliniowymi, patrz: Ref. [Bou07a, § 3, n° 4, Prop. 2]. Odpowiedniość ta nie jest jednak wzajemnie jednoznaczna.

Forma dwuliniowa stowarzyszona z Q_Φ to

$$\Phi_{Q_\Phi} = \Phi,$$

co pokazuje, że odwzorowania $Q \mapsto \Phi_Q$ i $\Phi \mapsto Q_\Phi$ są wzajem odwrotne. $\square$

O patologicznej naturze przypadku $\text{char } \mathbb{K} = 2$ zaświadcza następująca elementarna obserwacja: dla *każdej* formy kwadratowej Q na przestrzeni wektorowej V nad ciałem $\mathbb{K}$ forma dwuliniowa stowarzyszona z Q jest alternująca,

$$\forall_{v \in V} : \Phi_Q(v, v) = 0_{\mathbb{K}},$$

a zatem skośnie symetryczna. Oczywiście nie oznacza to jeszcze, że (będąc zarazem formą symetryczną) jest ona koniecznie zerowa.

W świetle powyższych argumentów podstawowe własności form kwadratowych otrzymujemy jako corollaria do stwierdzeń dotyczących form hermitowskich, udowodnionych w rozdziale poprzednim. Zaczniemy od

STWIERDZENIE 163 (Twierdzenie Lagrange'a o diagonalizacji formy kwadratowej). *W notacji Def. 11 oraz Przykł. 11 każda forma kwadratowa na przestrzeni wektorowej nad ciałem $\mathbb{K}$ o charakterystyce $\text{char } \mathbb{K} \neq 2$ ma bazę diagonalizującą.*

■

Dowód: Stwierdzenie to jest oczywistą konsekwencją Tw. 9.1. Poniżej przedstawimy jego dowód konstrukcyjny słuszny w przypadku $\dim_{\mathbb{K}} V =: N < \infty$. Jest on opisywany w literaturze pod nazwą **metody Lagrange'a diagonalizacji formy kwadratowej** (lub też **metody uzupełniania do kwadratu**).

Niech $Q \neq 0$, co jest równoważne $\Phi_Q \neq 0$. Wybierzmy dowolną bazę $\{v_i\}_{i \in \overline{1, N}}$ w przestrzeni V . Załóżmy najpierw, że

$$\forall_{i \in \overline{1, N}} : \Phi_Q(v_i, v_i) = 0_{\mathbb{K}}.$$

Wobec założenia $\Phi_Q \neq 0$ muszą istnieć elementy bazy $v_i \neq v_j$ o własności

$$\Phi_Q(v_i, v_j) \neq 0_{\mathbb{K}}.$$

Dokonując (jeśli to konieczne) permutacji elementów bazy, możemy przyjąć $j = 2 = i + 1$, a następnie definiujemy

$$\tilde{v}_1 := 2_{\mathbb{K}}^{-1} \triangleright_V (v_1 +_V v_2), \quad \tilde{v}_2 := 2_{\mathbb{K}}^{-1} \triangleright_V (v_1 +_V P_V(v_2)).$$

W nowej bazie $\{\tilde{v}_1, \tilde{v}_2\} \cup \{v_j\}_{j \in \overline{3, N}}$ zachodzą równości

$$\Phi_Q(\tilde{v}_1, \tilde{v}_1) = 2_{\mathbb{K}}^{-1} \cdot_{\mathbb{K}} \Phi_Q(v_1, v_2) = -\Phi_Q(\tilde{v}_2, \tilde{v}_2) \neq 0_{\mathbb{K}}.$$

Możemy zatem dalej rozważać sytuację, w której istnieje chociaż jeden niezerowy wyraz diagonalny w macierzy $[\Phi_Q]_{\mathcal{B}}$. Po ewentualnej permutacji indeksów dostajemy

$$\Phi_Q(v_1, v_1) \neq 0_{\mathbb{K}}.$$

Zdefiniujemy nową bazę o elementach

$$\tilde{v}_1 := v_1, \quad \forall_{j \in \overline{2, N}} : \tilde{v}_j := v_j +_V (-\Phi_Q(v_1, v_1)^{-1} \cdot_{\mathbb{K}} \Phi_Q(v_1, v_j)) \triangleright_V v_1,$$

w której obliczamy

$$\Phi_Q(\tilde{v}_1, \tilde{v}_1) \equiv \Phi_Q(v_1, v_1) \neq 0_{\mathbb{K}}$$

oraz – dla dowolnego $j \in \overline{2, N}$ –

$$\Phi_Q(\tilde{v}_1, \tilde{v}_j) \equiv \Phi_Q(v_1, v_j) - \Phi_Q(v_1, v_1)^{-1} \cdot_{\mathbb{K}} \Phi_Q(v_1, v_j) \cdot_{\mathbb{K}} \Phi_Q(v_1, v_1) = 0_{\mathbb{K}},$$

co pokazuje, że w tej nowej bazie jedynym niezerowym wyrazem w pierwszym wierszu (a więc też i w pierwszej kolumnie) macierzy formy Φ_Q jest wyraz diagonalny. Możemy teraz powtórzyć opisaną tu procedurę w odniesieniu do (formy Φ_Q ograniczonej do) podprzestrzeni $\langle \tilde{v}_2, \tilde{v}_3, \dots, \tilde{v}_N \rangle_{\mathbb{K}}$ itd., mając przy tym pewność, że wobec skończonego wymiaru V procedura diagonalizacyjna zakończy się po co najwyżej $N - 1$ krokach. $\square$

Jak jasno wynika z opisu procedury Lagrange’a, jest ona niezawodna i w każdych okolicznościach prowadzi do diagonalizacji formy kwadratowej. W szczególnych okolicznościach możemy zamiast tej – bywa – dość mozolnej procedury diagonalizacji zastosować poniższe

STWIERDZENIE 164 (Sylvestera–Jacobiego wyznacznikowy wzór na sygnaturę). *Przyjmijmy notację Def. 67, 11, 13, 21, 32, 35, 61, 63, 64, 65, 68, 70, 75, 78, 82, 87, 89, 91, 95, 98, 105, 106, 107, 108, 109, 110, 111, 112, 113, 116, 118 i 119, Stw. 75, 156, 157 i 158, Tw. 9.3 oraz Przykł. 11, 34(2), 35(2) i 41. Niechaj V będzie przestrzenią wektorową skończonego wymiaru $\dim_{\mathbb{K}} V =: N < \infty$ nad ciałem $\mathbb{K}$ o charakterystyce $\text{char } \mathbb{K} \neq 2$ wyposażoną w formę kwadratową Q i niech $\{v_i\}_{i \in \overline{1, N}} \subset V$ będzie dowolną bazą V o tej własności, że dla dowolnego $n \in \overline{1, N}$ podprzestrzeń $V_n := \langle v_1, v_2, \dots, v_n \rangle_{\mathbb{K}}$ jest niezwyrodniała względem Q , tj. wyznacznik odnośnej macierzy*

$$G(n) : \overline{1, n} \times \overline{1, n} \longrightarrow \mathbb{K} : (i, j) \longmapsto \Phi_Q(v_i, v_j),$$

jest odwracalny w $\mathbb{K}$,

$$\forall_{n \in \overline{1, N}} : \det_{(n)} G(n) \neq 0_{\mathbb{K}}.$$

Wówczas wektory

$$e_n := \sum_{j=1}^n \left(\left(\widetilde{G(n)}_n \right)^{-1} \cdot_{\mathbb{K}} \widetilde{G(n)}_j \right) \triangleright_V v_j, \quad n \in \overline{1, N},$$

zapisane w notacji Def. 91 i dla $\widetilde{G(1)}_1 := 1_{\mathbb{K}}$, tworzą bazę V diagonalizującą Q , a przy tym

$$\forall_{n \in \overline{1, N}} : Q(e_n) = 2_{\mathbb{K}}^{-1} \cdot_{\mathbb{K}} \left(\widetilde{G(n)}_n \right)^{-1} \cdot_{\mathbb{K}} \widetilde{G(n+1)}_{n+1}^{n+1},$$

gdzie $\widetilde{G(N+1)}_{N+1}^{N+1} := \det_{(N)} (G(N))$. W szczególności więc

$$\text{sign}(Q) = (p, q),$$

gdzie p jest liczbą dodatnich, q zaś – ujemnych wyrazów ciągu

$$\left(\widetilde{G(n)}_n \right)^{-1} \cdot_{\mathbb{K}} \widetilde{G(n+1)}_{n+1}^{n+1}, \quad n \in \overline{1, N}.$$

Forma Q nad ciałem $\mathbb{K} = \mathbb{R}$ jest zatem dodatnio określona, gdy

$$\forall_{n \in \overline{2, N+1}} : \widetilde{G(n)}_n^n > 0$$

i ujemnie określona, gdy

$$\forall_{n \in \overline{2, N+1}} : (-1)^n \cdot_{\mathbb{R}} \widetilde{G(n)}_n^n < 0.$$

■

Dowód: Teza jest prostym wnioskiem ze Stw. 158 i Tw. 9.3. □

Dotychczas korzystaliśmy jedynie z rezultatów wcześniejszych naszych dociekań osadzonych w kategorii form (ϵ) -hermitowskich. Prawdziwie nowej, a przy tym stosunkowo nietrywialnej wiedzy dotyczącej form symetrycznych dostarcza rodzina twierdzeń Witta, które omówimy poniżej. Tytułem przygotowania do ich sformułowania wprowadzimy

DEFINICJA 120. Przyjmijmy notację Def. 11, 13, 21, 32, 35, 61, 63, 72, 73, 105, 106, 107, 108 i 109 oraz Przykł. 35 (2). Przestrzeń wektorowa V nad ciałem $\mathbb{K}$ wyposażona w formę symetryczną γ jest nazywana **płaszczyzną hiperboliczną**, jeżeli jest niezwyrodniała (względem γ), $\dim_{\mathbb{K}} V = 2$ i istnieje w niej niezerowy wektor izotropowy $v \in V$,

$$v \neq 0_V \quad \wedge \quad \gamma(v, v) = 0_{\mathbb{K}}.$$

Przestrzeń hiperboliczna to suma ortogonalna dowolnej rodziny płaszczyzn hiperbolicznych. Forma symetryczna (wzgl. kwadratowa) na przestrzeni hiperbolicznej jest określana mianem **formy hiperbolicznej**.

Bazę $\{v, w\}$ płaszczyzny hiperbolicznej V spełniającą układ warunków

$$(9.2) \quad \gamma(v, v) = 0_{\mathbb{K}} = \gamma(w, w) \quad \wedge \quad \gamma(v, w) = 1_{\mathbb{K}}$$

nazywamy **parą hiperboliczną**. ▲

Elementarnego opisu przestrzeni hiperbolicznych dostarcza

STWIERDZENIE 165. *Przyjmijmy notację Def. 11 oraz Przykł. 11. Każda płaszczyzna hiperboliczna nad ciałem $\mathbb{K}$ o charakterystyce $\text{char } \mathbb{K} \neq 2$ ma parę hiperboliczną. I odwrotnie, dowolna dwuwymiarowa przestrzeń symetryczna o bazie spełniającej warunki (9.3) jest płaszczyzną hiperboliczną.* ■

Dowód: Niech V będzie płaszczyzną hiperboliczną o wektorze $v \neq 0_V$ izotropowym względem formy symetrycznej γ . Wobec $\text{Ker } \gamma = \{0_V\}$ musi istnieć wektor $w \notin \langle v \rangle_{\mathbb{K}}$ spełniający warunek

$$\gamma(v, w) \neq 0_{\mathbb{K}},$$

gdyż w przeciwnym razie $v \in \text{Ker } \gamma$. Położywszy

$$u := \lambda \triangleright_V v +_V w, \quad \lambda := -2_{\mathbb{K}}^{-1} \cdot_{\mathbb{K}} \gamma(v, w)^{-1} \cdot_{\mathbb{K}} \gamma(w, w),$$

bez trudu sprawdzamy, że układ $\{\gamma(v, w)^{-1} \triangleright_{\mathbb{K}} u, v\}$ jest parą hiperboliczną dla V , oto bowiem $u \notin \langle v \rangle_{\mathbb{K}}$, a ponadto

$$\begin{aligned} \gamma(\gamma(v, w)^{-1} \triangleright_{\mathbb{K}} u, \gamma(v, w)^{-1} \triangleright_{\mathbb{K}} u) &\equiv (\gamma(v, w)^{-1})^2 \cdot_{\mathbb{K}} \gamma(\lambda \triangleright_V v +_V w, \lambda \triangleright_V v +_V w) \\ &= (\gamma(v, w)^{-1})^2 \cdot_{\mathbb{K}} (\lambda^2 \cdot_{\mathbb{K}} \gamma(v, v) +_{\mathbb{K}} 2\lambda \cdot_{\mathbb{K}} \gamma(v, w) +_{\mathbb{K}} \gamma(w, w)) \end{aligned}$$

$$= (\gamma(v, w)^{-1})^2 \cdot_{\mathbb{K}} (2\lambda \cdot_{\mathbb{K}} \gamma(v, w) +_{\mathbb{K}} \gamma(w, w)) = 0_{\mathbb{K}}$$

oraz

$$\begin{aligned} \gamma(\gamma(v, w)^{-1} \triangleright_{\mathbb{K}} u, v) &\equiv \gamma(v, w)^{-1} \cdot_{\mathbb{K}} \gamma(\lambda \triangleright_V v +_V w, v) \\ &= \gamma(v, w)^{-1} \cdot_{\mathbb{K}} (\lambda \cdot_{\mathbb{K}} \gamma(v, v) +_{\mathbb{K}} \gamma(w, v)) = \gamma(v, w)^{-1} \cdot_{\mathbb{K}} \gamma(v, w) = 1_{\mathbb{K}}. \end{aligned}$$

I odwrotnie, jeżeli elementy bazy $\{v, w\}$ przestrzeni V spełniają relacje (9.3), to γ ma w tej bazie macierz

$$[\gamma]_{\{v, w\}} = \begin{pmatrix} 0_{\mathbb{K}} & 1_{\mathbb{K}} \\ 1_{\mathbb{K}} & 0_{\mathbb{K}} \end{pmatrix},$$

która jest odwracalna ($\det_{(2)}([\gamma]_{\{v, w\}}) = -1_{\mathbb{K}} \neq 0_{\mathbb{K}}$). To pokazuje, że forma γ jest niewyrodniająca, a zatem V jest w istocie płaszczyzną hiperboliczną. $\square$

Przestrzenie hiperboliczne są naturalnym elementem opisu zwyrodniałych ograniczeń niewyrodniałych form symetrycznych (lub – równoważnie – niewyrodniałych rozszerzeń zwyrodniałych form symetrycznych) i jako takie pozwalają lepiej zrozumieć geometrię zanurzeń podprzestrzeni izotropowych w niewyrodniałych przestrzeniach symetrycznych. Doskonałej ilustracji tej tezy dostarcza

STWIERDZENIE 166 (O rozszerzeniu hiperbolicznym przestrzeni izotropowej). *Przyjmijmy notację Def. 11, 13, 21, 32, 35, 61, 63, 64, 65, 72, 73, 75, 78, 95, 98, 105, 106, 107, 108, 109, 110, 111 i 112 oraz Przykł. 11, 34 (2) i Przykł. 35 (2). Niechaj V będzie przestrzenią wektorową nad ciałem $\mathbb{K}$ o charakterystyce $\text{char } \mathbb{K} \neq 2$ wyposażoną w niewyrodniałą formę symetryczną γ i niech $W \subset V$ będzie podprzestrzenią V . Oznaczmy $\gamma_W := \gamma|_{W \times W}$ i $W_0 := \text{Ker } \gamma_W$ i założymy, że wymiar W_0 jest skończony, $\dim_{\mathbb{K}} W_0 =: K < \infty$. Wybierzmy bazę $\{w_i\}_{i \in \overline{1, K}}$ w W_0 i niech D będzie dopełnieniem ortogonalnym W_0 w W ,*

$$W = W_0 \oplus D.$$

Wówczas istnieją wektory $\{v_i\}_{i \in \overline{1, K}} \subset D^\perp \subset V$ o tej własności, że dla każdego indeksu $i \in \overline{1, K}$ układ $\{v_i, w_i\}$ jest parą hiperboliczną rozpinającą płaszczyznę hiperboliczną $H_i := \langle v_i, w_i \rangle_{\mathbb{K}}$. Pary te zadają rozkład ortogonalny podprzestrzeni

$$\widetilde{W} := \langle v_1, v_2, \dots, v_K, w_1, w_2, \dots, w_K \rangle_{\mathbb{K}} +_V D \subset V$$

dany wzorem

$$\widetilde{W} = H_1 \oplus H_2 \oplus \dots \oplus H_K \oplus D.$$

■

Dowód: Oznaczmy

$$D_1 := \langle w_2, w_3, \dots, w_K \rangle_{\mathbb{K}} \oplus D.$$

Z inkluzji właściwej podprzestrzeni

$$D_1 \subsetneq W_0 \oplus D$$

wynika inkluzja właściwa ich anihilatorów,

$$D_1^{\perp \gamma} \subsetneq (W_0 \oplus D)^{\perp \gamma},$$

a stąd dalej – istnienie wektora $v_1 \in D_1^{\perp\gamma} \setminus (W_0 \oplus D)^{\perp\gamma}$, tj. takiego, który spełnia warunki

$$\forall_{j \in 2, \overline{K}} : \gamma(v_1, w_j) = 0_K, \quad \forall_{v \in D} : \gamma(v_1, v) = 0_K$$

oraz

$$\gamma(v_1, w_1) \neq 0_K.$$

Wobec izotropowości wektora w_1 podprzestrzeń $H_1 := \langle v_1, w_1 \rangle_K$ jest zatem płaszczyzną hiperboliczną, co w świetle Stw. 165 oznacza istnienie takiego wektora $u_1 \in H_1$, który tworzy wraz z w_1 parę hiperboliczną. Przy tym oczywiście

$$\widetilde{W}_1 := \langle v_1, w_1, w_2, w_3, \dots, w_K \rangle_K +_V D = H_1 \oplus \langle w_2, w_3, \dots, w_K \rangle_K \oplus D.$$

Jądrem formy symetrycznej $\gamma_{\widetilde{W}_1} := \gamma|_{\widetilde{W}_1 \times \widetilde{W}_1}$ jest

$$\text{Ker } \gamma_{\widetilde{W}_1} = \langle w_2, w_3, \dots, w_K \rangle_K,$$

wobec czego całą opisaną procedurę możemy powtórzyć w odniesieniu do podprzestrzeni izotropowej

$$\widetilde{W}_1 = \text{Ker } \gamma_{\widetilde{W}_1} \oplus D_1, \quad D_1 := H_1 \oplus D.$$

□

Zasadniczym naszym celem w niniejszym rozdziale jest wyprowadzenie kanonicznej postaci formy symetrycznej na zwyrodniałej przestrzeni wektorowej V , która odzwierciedlałaby (ewentualne) istnienie w V wektorów izotropowych, a nadto – przede wszystkim – zrozumienie swobody wyboru ortogonalnego rozkładu przestrzeni V zadawanego przez tę postać kanoniczną. Droga do tego celu wiedzie przez fundamentalny wynik teorii przestrzeni symetrycznych, jakim jest omawiane poniżej twierdzenie Witta o przedłużaniu izometrii. Twierdzenie to można uogólnić (przy pewnych założeniach odnośnie do ciała K) na przypadek dowolnej przestrzeni ϵ -hermitowskiej³, my jednak ograniczymy nasze rozważania do przestrzeni symetrycznych, co pozwoli nam skorzystać z wcześniejszych wyników ich dotyczących i tym samym wydatnie uprości ich dowody.

TIWIERDZENIE 9.4 (Twierdzenie Witta o przedłużaniu izometrii). *Przyjmijmy notację Def. 11, 13, 21, 32, 35, 61, 63, 64, 105, 106, 107, 108 i 109 oraz Przykł. 11, 35 (2). Niechaj $V^{(\alpha)}$, $\alpha \in \{1, 2\}$ będą dwiema skończone wymiarowymi przestrzeniami wektorowymi nad ciałem K o charakterystyce $\text{char } K \neq 2$, wyposażonymi w niezwyrodniałe formy symetryczne $\gamma^{(\alpha)}$, i niech $W_\alpha \subset V^{(\alpha)}$ będą ich podprzestrzeniami. Załóżmy, że istnieje izometria $V^{(1)} \cong V^{(2)}$. Wówczas dowolna izometria $\chi : W_1 \xrightarrow{\cong} W_2$ rozszerza się do izometrii $\tilde{\chi} : V^{(1)} \xrightarrow{\cong} V^{(2)}$.*

■

Dowód: Zauważmy najpierw, że wystarczy rozważyć przypadek $V^{(1)} = V^{(2)}$, oto bowiem w przypadku ogólnym możemy zawsze wykorzystać odwrotność izometrii $\sigma : V^{(1)} \xrightarrow{\cong} V^{(2)}$, której istnienie zakładamy, aby odwzorować W_2 w $\sigma^{-1}(W_2) \subset$

³Wiąże się to z pewnym wzrostem poziomu skomplikowania odnośnych dowodów – patrz: Ref. [Bou07a, § 4, n° 2,3]. Mając na względzie to, jak również konkretne fizyczne zastosowania tych twierdzeń, zdecydowaliśmy się na ich osadzenie w podkategorii przestrzeni symetrycznych.

$V^{(1)}$. Istnienie rozszerzenia izometrii $\sigma^{-1} \circ \chi : W_1 \xrightarrow{\cong} \sigma^{-1}(W_2)$ do izometrii $\widetilde{\sigma^{-1} \circ \chi} : V^{(1)} \hookrightarrow V$ da nam pożądane rozszerzenie $\widetilde{\chi} = \sigma \circ \sigma^{-1} \circ \chi$.

Niech zatem $V^{(1)} = V^{(2)} \equiv V$. Załóżmy najpierw, że W_1 jest podprzestrzenią izotropową i rozważmy rozkład ortogonalny

$$W_1 = \text{Ker}(\gamma|_{W_1 \times W_1}) \oplus D$$

jak w tezie Stw. 166. Wobec izometryczności odwzorowania χ zachodzi, na mocy Stw. 154,

$$\chi(W_1) = \chi(\text{Ker}(\gamma|_{W_1 \times W_1})) \oplus \chi(D) \equiv \text{Ker}(\gamma|_{\chi(W_1) \times \chi(W_1)}) \oplus \chi(D).$$

Niech $K := \dim_{\mathbb{K}} \text{Ker}(\gamma|_{W_1})$ i ustalmy bazę $\{z_i\}_{i \in \overline{1, K}}$ podprzestrzeni $\text{Ker}(\gamma|_{W_1 \times W_1})$. Przywołując Stw. 166, dokonujemy rozszerzenia hiperbolicznego podprzestrzeni W_1 i $\chi(W_1)$, co prowadzi do rozkładów

$$\widetilde{W}_1 = \bigoplus_{i=1}^K H_i \oplus D$$

oraz

$$\widetilde{\chi(W_1)} = \bigoplus_{i=1}^K H'_i \oplus \chi(D),$$

w których każda z płaszczyzn hiperbolicznych $H_i := \langle z_i, v_i \rangle_{\mathbb{K}}$ (wzgl. $H_i := \langle \chi(z_i), v'_i \rangle_{\mathbb{K}}$) jest współokreślana przez pewien wektor $v_i \in D^\perp$ (wzgl. $v'_i \in \chi(D)^\perp$) dopełniający z_i (wzgl. $\chi(z_i)$) do pary hiperbolicznej. Odwzorowanie $\mathbb{K}$ -liniowe o własności

$$\widetilde{\chi}|_{W_1} := \chi|_{W_1},$$

a zadane na wektorach v_i wedle wzoru

$$\widetilde{\chi}(v_i) := v'_i$$

jest rozszerzeniem izometrii χ do przestrzeni niezwyrodniałej $\widetilde{W}_1$. Istotnie, obliczamy, dla dowolnego $v \in D$ oraz $i, j \in \overline{1, K}$,

$$\gamma(\widetilde{\chi}(v_i), \widetilde{\chi}(v)) = \gamma(v'_i, \chi(v)) = 0_{\mathbb{K}} = \gamma(v_i, v),$$

$$\gamma(\widetilde{\chi}(v_i), \widetilde{\chi}(z_j)) = \gamma(v'_i, \chi(z_j)) = \delta_{i,j}^{\mathbb{K}} = \gamma(v_i, z_j),$$

$$\gamma(\widetilde{\chi}(v_i), \widetilde{\chi}(v_j)) = \gamma(v'_i, v'_j) = 0_{\mathbb{K}} = \gamma(v_i, v_j).$$

Powyższe rozumowanie pokazuje jasno, że wystarczy udowodnić tezę twierdzenia w przypadku, gdy W_1 jest podprzestrzenią niezwyrodniałą.

Założmy przeto, że W_1 (a zatem także W_2) jest niezwyrodniała. Jeśli przy tym $W_1 = W_2$, to $\chi \in \text{Aut}_{\mathbb{K}}(W_1)$ rozszerzamy trywialnie do V , kładąc

$$\widetilde{\chi} := \chi \oplus \text{id}_{W_1^\perp} : W_1 \oplus W_1^\perp \equiv V \hookrightarrow V.$$

Jeśli natomiast $W_2 \neq W_1$, to mogą zaistnieć następujące sytuacje szczególne.

Po pierwsze, może być $\dim_{\mathbb{K}} W_1 = 1 = \dim_{\mathbb{K}} W_2$, czyli $W_\alpha = \langle w_\alpha \rangle_{\mathbb{K}}$, $\alpha \in \{1, 2\}$ dla pewnych wektorów $w_1 \in W_1$ i $w_2 := \chi(w_1) \in W_2$, które spełniają relację

$$\gamma(w_2, w_2) = \gamma(w_1, w_1)$$

i rozpinają podprzestrzeń $W_{1,2} := W_1 \oplus W_2 \subset V$ wymiaru 2. Jeśli $\gamma|_{W_{1,2} \times W_{1,2}}$ jest niezwyrodniała, to wystarczy położyć $\widetilde{\chi}(w_2) := w_1$, aby uzyskać rozszerzenie χ do $W_{1,2}$ o własności $\widetilde{\chi} : W_{1,2} \xrightarrow{\cong} W_{1,2}$, które dalej rozszerza się trywialnie do

V jak poprzednio. Jeśli natomiast podprzestrzeń $W_{1,2}$ jest izotropowa, to wobec $\dim_{\mathbb{K}} \text{Ker}(\gamma|_{W_{1,2} \times W_{1,2}}) = 1$ (równość $\dim_{\mathbb{K}} \text{Ker}(\gamma|_{W_{1,2} \times W_{1,2}}) = 2$ oznaczałaby $\gamma|_{W_{1,2} \times W_{1,2}} = 0$, co przeczyłoby niezwyrodnieniu W_1) implikuje istnienie wektora $z \in \text{Ker}(\gamma|_{W_{1,2} \times W_{1,2}})$ oraz skalaru $\lambda \in \mathbb{K}$ zadających (jednoznaczny) rozkład

$$w_2 = \lambda \triangleright_V w_1 +_V z.$$

Prosty rachunek

$$\begin{aligned} \gamma(w_1, w_1) &= \gamma(w_2, w_2) = \lambda^2 \cdot_{\mathbb{K}} \gamma(w_1, w_1) +_{\mathbb{K}} 2\lambda \cdot_{\mathbb{K}} \gamma(w_1, z) +_{\mathbb{K}} \gamma(z, z) \\ &= \lambda^2 \cdot_{\mathbb{K}} \gamma(w_1, w_1) \end{aligned}$$

pokazuje, że możemy wybrać $\lambda = 1_{\mathbb{K}}$, czyli

$$w_2 = w_1 +_V z,$$

zastępując – jeśli trzeba – w_1 wektorem przeciwnym $P_V(w_1)$. Zauważmy, że wtedy

$$\gamma(w_1, w_2) = \gamma(w_1, w_1 +_V z) = \gamma(w_1, w_1).$$

Oznaczmy

$$w := w_1 +_V w_2.$$

Bez trudu sprawdzamy istnienie rozkładu ortogonalnego

$$W_1 \oplus W_2 = \langle z \rangle_{\mathbb{K}} \oplus \langle w \rangle_{\mathbb{K}}.$$

Istotnie, $w \notin \langle z \rangle_{\mathbb{K}}$, gdyż

$$\gamma(w, w) = 4\gamma(w_1, w_1) \neq 0_{\mathbb{K}} = \gamma(z, z),$$

a nadto – rzecz jasna – $\gamma(z, w) = 0_{\mathbb{K}}$. Na mocy Stw. 166 istnieje zatem wektor $v \in \langle w \rangle_{\mathbb{K}}^{\perp} \subset V$ dopełniający z do pary hiperbolicznej,

$$\gamma(v, z) = 1_{\mathbb{K}} \quad \wedge \quad \gamma(v, v) = 0_{\mathbb{K}} = \gamma(z, z).$$

Otrzymujemy rozkład ortogonalny (niezwyrodniałego) rozszerzenia hiperbolicznego

$$\langle v, z, w \rangle_{\mathbb{K}} = \langle v, z \rangle_{\mathbb{K}} \oplus \langle w \rangle_{\mathbb{K}}$$

na płaszczyznę hiperboliczną $\langle v, z \rangle_{\mathbb{K}}$ i przestrzeń niezwyrodniałą $\langle w \rangle_{\mathbb{K}}$. Zdefiniujemy odwzorowanie liniowe

$$\tilde{\chi} : \langle v, z, w \rangle_{\mathbb{K}} \hookrightarrow$$

na bazie wedle wzoru

$$\tilde{\chi} : (v, z, w) \mapsto (-v, -z, w).$$

Sprawdzamy, że jest ono rozszerzeniem χ , oto bowiem

$$\tilde{\chi}(w_1) \equiv \tilde{\chi}(2_{\mathbb{K}}^{-1} \triangleright_V (w +_V P_V(z))) = 2_{\mathbb{K}}^{-1} \triangleright_V (w +_V z) = w_2 = \chi(w_1).$$

Na koniec dokonujemy dalszego trywialnego rozszerzenia $\tilde{\chi}$ na $V = \langle v, z, w \rangle_{\mathbb{K}} \oplus \langle v, z, w \rangle_{\mathbb{K}}^{\perp}$ wedle schematu

$$\tilde{\tilde{\chi}} := \tilde{\chi} \oplus \text{id}_{\langle v, z, w \rangle_{\mathbb{K}}^{\perp}} : \langle v, z, w \rangle_{\mathbb{K}} \oplus \langle v, z, w \rangle_{\mathbb{K}}^{\perp} \hookrightarrow.$$

Pozostaje już tylko ropatrzeć przypadek $\dim_{\mathbb{K}} W_1 > 1$. Zastosujemy indukcję względem wymiaru $N := \dim_{\mathbb{K}} W_1$ podprzestrzeni W_1 . Udowodniwszy prawdziwość tezy twierdzenia dla $N = 1$, założymy następnie, że jest ono prawdziwe również dla

$N := N_0 > 1$ i niech $\dim_{\mathbb{K}} W_1 = N_0 + 1$. Przywołując Tw. 9.1, możemy dokonać rozkładu

$$W_1 = X_1 \oplus X_2,$$

przy czym $\dim_{\mathbb{K}} X_1, \dim_{\mathbb{K}} X_2 \leq N_0$. Z uwagi na izometryczność χ stwierdzamy, w odwołaniu do Stw. 154, że

$$\chi(W_1) = \chi(X_1) \oplus \chi(X_2).$$

Oznaczmy $\chi_\alpha := \chi|_{X_\alpha}$, $\alpha \in \{1, 2\}$. Na mocy założenia indukcyjnego istnieje rozszerzenie

$$\widetilde{\chi}_1 : X_1 \oplus (X_2 \oplus W_1^\perp) \equiv V \curvearrowright$$

izometrii χ_1 , a także rozszerzenie

$$\widetilde{\chi}_2 : X_2 \oplus (X_1 \oplus W_1^\perp) \equiv V \curvearrowright$$

izometrii χ_2 , przy czym wobec

$$\chi(X_2) \perp \chi(X_1) \equiv \widetilde{\chi}_1(X_1)$$

jest konieczne

$$\chi(X_2) \subset \widetilde{\chi}_1(X_2 \oplus W_1^\perp).$$

Zachodzi także trywialna inkluzja

$$\chi(X_2) \equiv \widetilde{\chi}_2(X_2) \subset \widetilde{\chi}_2(X_2 \oplus W_1^\perp),$$

a ponieważ odwzorowanie

$$\widetilde{\chi}_1 \circ \widetilde{\chi}_2^{-1} : \widetilde{\chi}_2(X_2 \oplus W_1^\perp) \longrightarrow \widetilde{\chi}_1(X_2 \oplus W_1^\perp)$$

jest izometrią (jako złożenie izometrii), przeto istnieje – znów na mocy założenia indukcyjnego – rozszerzenie izometrii identycznościowej $\text{id}_{\chi(X_2)}$ do izometrii

$$\widetilde{\text{id}_{\chi(X_2)}} : \widetilde{\chi}_2(X_2 \oplus W_1^\perp) \xrightarrow{\cong} \widetilde{\chi}_1(X_2 \oplus W_1^\perp).$$

To ostatnie pozwala skonstruować rozszerzenie χ_2 do izometrii

$$\widetilde{\widetilde{\chi}_2} := \widetilde{\text{id}_{\chi(X_2)}} \circ \widetilde{\chi}_2 : X_2 \oplus W_1^\perp \xrightarrow{\cong} \widetilde{\chi}_1(X_2 \oplus W_1^\perp).$$

Koniec końców odwzorowanie

$$\widetilde{\chi} := \chi_1 \oplus \widetilde{\widetilde{\chi}_2}$$

jest poszukiwanym rozszerzeniem χ . □

Jako prostą konsekwencję udowodnionego powyżej twierdzenia znajdujemy kolejne

TWIERDZENIE 9.5 (Twierdzenie Witta o skracaniu). *Przyjmijmy notację Def. 11, 13, 21, 32, 35, 61, 63, 64, 65, 75, 78, 105, 106, 107, 108 i 109 oraz Przykł. 11, 35 (2). Niechaj $V^{(1)}, V^{(2)}$ i V będą skończenie wymiarowymi przestrzeniami wektorowymi nad ciałem $\mathbb{K}$ o charakterystyce $\text{char } \mathbb{K} \neq 2$ wyposażonymi w formy symetryczne – odpowiednio $\gamma^{(1)}, \gamma^{(2)}$ i γ . Jeśli formy $\gamma^{(1)}, \gamma^{(2)}$ są niezwyrodniałe, a przestrzeń $V^{(1)} \oplus V$ z formą symetryczną $\gamma^{(1)} \oplus \gamma$ jest izometryczna z przestrzenią $V^{(2)} \oplus V$ z formą symetryczną $\gamma^{(2)} \oplus \gamma$, to istnieje izometria między $V^{(1)}$ (z formą symetryczną $\gamma^{(1)}$) i $V^{(2)}$ (z formą symetryczną $\gamma^{(2)}$).* ■

Dowód: Przedłużwszy izometrię identycznościową id_V do izometrii

$$\widetilde{\text{id}_V} : V^{(1)} \oplus V \xrightarrow{\cong} V^{(2)} \oplus V,$$

zgodnie z Tw. 9.4, stwierdzamy, że koniecznie

$$\widetilde{\text{id}_V}(V^{(1)}) = V^{(2)},$$

zatem $\widetilde{\text{id}_V}|_{V^{(1)}}$ jest pożądaną izometrią. $\square$

I wreszcie możemy sformułować wniosek z dotychczasowych naszych dociekań pozostający w bezpośredniej relacji z dyskutowaną wcześniej teorią form symetrycznych i kwadratowych.

TWIERDZENIE 9.6 (Twierdzenie Witta o rozkładzie). *Przyjmijmy notację Def. 11, 13, 21, 32, 35, 61, 63, 64, 65, 75, 78, 105, 106, 107, 108 i 109 oraz Przykł. 11, 35 (2). Niechaj V będzie przestrzenią wektorową skończonego wymiaru nad ciałem $\mathbb{K}$ o charakterystyce $\text{char } \mathbb{K} \neq 2$ wyposażoną w formę symetryczną γ . Przestrzeń V ma rozkład ortogonalny*

$$V = V_0 \oplus V_{\text{hip}} \oplus V_{\text{def}}$$

na podprzestrzeń zerową V_0 (na której $\gamma|_{V_0 \times V_0} = 0$), podprzestrzeń hiperboliczną V_{hip} (sumę ortogonalną pewnej liczby płaszczyzn hiperbolicznych) oraz podprzestrzeń V_{def} , na której forma jest określona, tj. taką, w której nie ma niezerowych wektorów izotropowych. Rozkład powyższy jest określony jednoznacznie z dokładnością do izometrii. $\blacksquare$

Dowód: Jest jasnym, że $V_0 = \text{Ker } \gamma$, więc składowa zerowa jest określona jednoznacznie, a ponadto mamy

$$V = V_0 \oplus V_0^\perp,$$

przy czym $V_0^\perp$ jest przestrzenią niezwyrodniałą. Jej wybór jest – w świetle Tw. 9.5 – określony z dokładnością do izometrii⁴. Będziemy dalej rozpatrywać przestrzeń $V_0^\perp$ z niezwyrodniałą formą symetryczną $\gamma_{\text{ndeg}} := \gamma|_{V_0^\perp}$. Wybierzmy w $V_0^\perp$ dowolną podprzestrzeń zerową $W_0 \subset V_0^\perp$ względem γ_{ndeg} . Na mocy Stw. 155 podprzestrzeń W_0 można zanurzyć w pewnej maksymalnej podprzestrzeni zerowej $W \subset V_0^\perp$, tę zaś – rozszerzyć do przestrzeni hiperbolicznej $V_{\text{hip}} \supset W$ zawartej w $V_0^\perp$, według Stw. 166. Korzystając ze Stw. 156, otrzymujemy przy tym rozkład

$$V_0^\perp = V_{\text{hip}} \oplus V_{\text{hip}}^\perp,$$

czyli też

$$V = V_0 \oplus V_{\text{hip}} \oplus V_{\text{hip}}^\perp.$$

Nasze rozumowanie dowodzi istnienia (być może trywialnej) składowej hiperbolicznej w rozkładzie V . Oczywiście każda taka składowa hiperboliczna zawiera pewną

⁴Podkreślimy dla uniknięcia nieporozumień: rozkład przestrzeni wektorowej na sumę prostą względem ustalonej jej podprzestrzeni *nie* jest w ogólności jednoznaczny. Wystarczy rozważyć $\langle v_1, v_2 \rangle_{\mathbb{K}} = \langle v_1 \rangle_{\mathbb{K}} \oplus \langle v_2 \rangle_{\mathbb{K}} = \langle v_1 \rangle_{\mathbb{K}} \oplus \langle v_1 + v_2 \rangle_{\mathbb{K}}$ dla wzajem liniowo niezależnych wektorów v_1, v_2 z pewnej przestrzeni wektorowej V nad ciałem $\mathbb{K}$.

maksymalną podprzestrzeń zerową (której wymiar jest połową wymiaru przestrzeni hiperbolicznej), musimy zatem upewnić się, że każde dwie maksymalne podprzestrzenie zerowe w $V_0^\perp$ są izometryczne (rozważanie podprzestrzeni zerowych w różnych, lecz wzajem izometrycznych podprzestrzeniach $V_0^\perp$ niczego nowego tu nie wnosi). W tym celu rozważmy dowolną podprzestrzeń zerową $W'_0 \subset V_0^\perp$. Odwołując się po raz kolejny do Stw. 155, zanurzamy ją w odnośnej maksymalnej przestrzeni zerowej $W' \subset V_0^\perp$. Przyjmijmy, że $\dim_{\mathbb{K}} W \leq \dim_{\mathbb{K}} W'$, a wtedy istnieje izometria W na pewną podprzestrzeń W' (wystarczy przeprowadzić bazę W na równoliczny z nią podzbiór bazy W'), którą na podstawie Tw. 9.4 możemy rozszerzyć do izometrii $V_0^\perp$ na siebie. Przeciwbraz W' względem tej izometrii jest przy tym przestrzenią zerową zawierającą W , a zatem – wobec maksymalności tej ostatniej – równą W , skąd $\dim_{\mathbb{K}} W' = \dim_{\mathbb{K}} W$. Równość tych wymiarów w przypadku $\dim_{\mathbb{K}} W \geq \dim_{\mathbb{K}} W'$ wynika natychmiast z symetrii zagadnienia i przekonuje o izometryczności dowolnych dwóch takich maksymalnych przestrzeni zerowych. Ta z kolei pociąga za sobą izometryczność odnośnych rozszerzeń hiperbolicznych H i H' . Te jednak zadają rozkłady ortogonalne

$$H \oplus H^\perp = V_0^\perp = H' \oplus (H')^\perp.$$

Dokonując rozszerzenia rzeczonyj izometrii $H \cong H'$ do izometrii $V_0^\perp$ na siebie, stwierdzamy $H^\perp \cong (H')^\perp$, co zaświadcza o jednoznaczności wyboru $V_{\text{hip}}^\perp = V_{\text{def}}$ z dokładnością do izometrii. $\square$

Godzi się na zakończenie tej części naszych rozważań dobitnie podkreślić subtelny sens ostatniego twierdzenia Witta, który kryje się w ostatniej części jego tezy. Oto przy okazji ogólnej dyskusji form ϵ -hermitowskich, a potem także hermitowskich, udało nam się wyprowadzić ich szczególnie prostą (diagonalną) postać kanoniczną wykorzystując w tym celu dowolne automorfizmy przestrzeni wektorowej będącej nośnikiem formy ϵ -hermitowskiej. Nie każdy jednak taki automorfizm jest zarazem automorfizmem wyżej uorganizowanej struktury, jaką jest struktura przestrzeni ϵ -hermitowskiej. Dopiero więc twierdzenie Witta ma charakter wewnętrzny z punktu widzenia rozpatrywanej przez nas kategorii przestrzeni ϵ -hermitowskich. Praktyczny aspekt tej dyskusji stanie się jasny, kiedy przejdziemy do omawiania automorfizmów przestrzeni wektorowej z zadaniem iloczynem skalarnym diagonalizujących jej endomorfizmy o ustalonej symetrii (np. hermitowskie bądź symetryczne). Tymczasem zamknijmy dyskusję form symetrycznych nadając imię rzeczonym automorfizmom

DEFINICJA 121. Przyjmijmy notację Def. 11, 13, 21, 32, 35, 61, 63, 105, 106, 107, 108 i 109 oraz Przykł. 35 (2). Niechaj $((V, +_V, P_V, \bullet \mapsto 0_V), \ell_V, \gamma)$ będzie przestrzenią ($\epsilon = 1$ -)hermitowską nad ciałem $\mathbb{K}$ z formą symetryczną γ . Jej automorfizmy określamy mianem **automorfizmów ortogonalnych** (lub **transformacji ortogonalnych**), generowaną zaś przez nie grupę

$$O(\gamma) := \text{Aut}_{\mathbb{K}}(V, \gamma)$$

nazywamy **grupą ortogonalną stowarzyszoną z γ** . W szczególności w przypadku przestrzeni $V := \mathbb{K}^{\times N}$, $N \in \mathbb{N}$ wyposażonej w formę symetryczną o macierzy względem bazy standardowej danej przez macierz jednostkową stopnia N otrzymujemy w ten sposób **grupę ortogonalną stopnia N o współczynnikach z $\mathbb{K}$** ,

oznaczaną symbolem

$$O(N; \mathbb{K}) \equiv O_N(\mathbb{K}).$$

Macierz transformacji ortogonalnej $O \in O(N; \mathbb{K})$ względem bazy standardowej nazywamy **macierzą ortogonalną (stopnia N)**. ▲

Prawdziwym jest

STWIERDZENIE 167. *Przyjmijmy notację Def. 11, 13, 21, 32, 35, 61, 63, 105, 106, 107, 108, 109 i 121 oraz Przykł. 35 (2). Dowolna macierz ortogonalna $O \in \text{Mat}(\mathbb{K}; N)$, $N \in \mathbb{N}$ spełnia tożsamość*

$$O^T \odot O = \mathbf{1}_N.$$

W szczególności jest ona macierzą odwracalną. ■

9.4. Formy skośnie symetryczne i przestrzenie symplektyczne

Formy skośnie symetryczne w fizyce i bliskich jej działach matematyki to przede wszystkim geometryczny opis przestrzeni stanów układów fizycznych (oraz algebr funkcji gładkich wzgl. wyróżnionych klas operatorów liniowych na nich), ale także geometryczno-kohomologiczna rekonstrukcja pola elektromagnetycznego oraz nieskończony opis grup obrotów w przestrzeni euklidesowej. Mając na względzie bogactwo zastosowań tych obiektów w obszarach, które będą przedmiotem dociekań na przyszłych kursach fizyki, a zarazem idąc śladem analiz dotychczasowych, poświęcimy nieco miejsca na ustalenie ich postaci kanonicznej. Na początek wprowadzimy

DEFINICJA 122. Przyjmijmy notację Def. 11, 13, 21, 32, 35, 61, 63, 72, 73, 105, 106, 107, 108 i 109 oraz Przykł. 35 (2). Przestrzeń wektorowa V nad ciałem $\mathbb{K}$ wyposażona w formę skośnie symetryczną ω jest nazywana **płaszczyzną symplektyczną**, jeżeli jest niezwyrodniała (względem ω) oraz $\dim_{\mathbb{K}} V = 2$. **Przestrzeń symplektyczna** to suma ortogonalna dowolnej rodziny płaszczyzn symplektycznych. Forma skośnie symetryczna na przestrzeni symplektycznej jest określana mianem **formy symplektycznej**.

Bazę $\{v, w\}$ płaszczyzny symplektycznej V spełniającą warunek

$$(9.3) \quad \omega(v, w) = 1_{\mathbb{K}}$$

nazywamy **parą symplektyczną**. ▲

Możemy teraz wypowiedzieć fundamentalne

TWIERDZENIE 9.7 (O postaci kanonicznej formy skośnie symetrycznej). *Przyjmijmy notację Def. 67, 11, 13, 21, 32, 35, 61, 63, 64, 65, 68, 70, 72, 73, 75, 78, 95, 98, 105, 106, 107, 108, 109, 110, 111, 112 i 122, Stw. 75 oraz Przykł. 34 (2) i 35 (2). Niechaj V będzie przestrzenią wektorową skończonego wymiaru $N := \dim_{\mathbb{K}} V < \infty$ nad ciałem $\mathbb{K}$ wyposażoną w formę skośnie symetryczną ω . Przestrzeń V jest wówczas sumą ortogonalną*

$$V = V_0 \oplus V_{\text{symp}}$$

na przestrzeń zerową V_0 i przestrzeń symplektyczną $V_{\text{sympł}}$ wymiaru $\dim_{\mathbb{K}} V_{\text{sympł}} = 2n \leq N$. Istnieje zatem baza $\mathcal{B} := \{v_i\}_{i \in \overline{1, N}}$ przestrzeni V , zwana **bazą symplektyczną**, w której macierz formy ω przyjmuje postać

$$[\omega]_{\mathcal{B}} = \begin{pmatrix} S & \mathbf{0}_{2n \times (N-2n)} \\ \mathbf{0}_{(N-2n) \times 2n} & \mathbf{0}_{(N-2n) \times (N-2n)} \end{pmatrix},$$

przy czym S jest **macierzą blokowo diagonalną**

$$S := \text{diag} \left(\underbrace{\begin{pmatrix} 0_{\mathbb{K}} & 1_{\mathbb{K}} \\ -1_{\mathbb{K}} & 0_{\mathbb{K}} \end{pmatrix}, \begin{pmatrix} 0_{\mathbb{K}} & 1_{\mathbb{K}} \\ -1_{\mathbb{K}} & 0_{\mathbb{K}} \end{pmatrix}, \dots, \begin{pmatrix} 0_{\mathbb{K}} & 1_{\mathbb{K}} \\ -1_{\mathbb{K}} & 0_{\mathbb{K}} \end{pmatrix}}_{n \text{ razy}} \right) \in \text{Mat}(\mathbb{K}; 2n).$$

■

Dowód: Przestrzeń V_0 jest oczywiście jądrem ω ,

$$V_0 = \text{Ker } \omega,$$

a zatem zadaje rozkład ortogonalny

$$V = V_0 \oplus V_0^{\perp \omega},$$

przy czym $V_0^{\perp \omega}$ jest już przestrzenią niezwyrodniałą. Istnieją zatem wektory $v_1, v_2 \in V_0^{\perp \omega}$ o własności

$$\omega(v_1, v_2) \neq 0_{\mathbb{K}},$$

co oznacza, że podprzestrzeń $\langle v_1, v_2 \rangle_{\mathbb{K}}$ jest płaszczyzną symplektyczną. Jako podprzestrzeń niezwyrodniała, wyznacza ona – na mocy Stw. 156 – rozkład ortogonalny

$$V_0^{\perp \omega} = \langle v_1, v_2 \rangle_{\mathbb{K}} \oplus \langle v_1, v_2 \rangle_{\mathbb{K}}^{\perp \omega},$$

przy czym – w świetle Cor. 20 – także podprzestrzeń $\langle v_1, v_2 \rangle_{\mathbb{K}}^{\perp \omega}$ jest niezwyrodniała, możemy zatem doprowadzić dowód do końca korzystając z indukcji względem wymiaru podprzestrzeni $V_0^{\perp \omega}$. □

Z powyższego wywodzimy bez trudu następujący istotny wniosek

STWIERDZENIE 168 (O postaci kanonicznej macierzy skośnie symetrycznej). *Przyjmijmy notację Def. 67, 11, 13, 21, 32, 35, 61, 63, 65, 68, 70, 75, 78, 82, 84, 105, 106, 107, 108 i 109, Cor. 14, Stw. 75, 95, 96, 97, 98, 99 i 152, Tw. 8.11 oraz Przykł. 35 (2) i 41. Niechaj $M \in \text{Mat}(\mathbb{K}; N)$ będzie macierzą skośnie symetryczną rzędu $\text{rk } M =: r \in \mathbb{N}$. Wówczas $r =: 2n \in 2\mathbb{N}$ i istnieje macierz odwracalna $B \in \text{Mat}(\mathbb{K}; N)$ sprowadzająca M do postaci*

$$B^T \odot M \odot B = \begin{pmatrix} J_r & \mathbf{0}_{r \times (N-r)} \\ \mathbf{0}_{(N-r) \times r} & \mathbf{0}_{(N-r) \times (N-r)} \end{pmatrix},$$

w której $J_r \in \text{GL}(\mathbb{K}; r)$ jest **standardową macierzą skośnie symetryczną stopnia r**

$$J_r := \begin{pmatrix} \mathbf{0}_{n \times n} & \mathbf{1}_n \\ -\mathbf{1}_n & \mathbf{0}_{n \times n} \end{pmatrix}.$$

■

Dowód: Wybierzmy w V bazę $\{v_i\}_{i \in \overline{1, N}}$ i zdefiniujmy formę skośnie symetryczną ω_M stowarzyszoną z M jak w tezie Stw. 152. Na mocy Tw. 9.7 w przestrzeni V istnieje baza $\mathcal{B}' := \{w_i\}_{i \in \overline{1, N}}$, w której macierz formy ω_M przyjmuje postać taką jak w tezie tegoż twierdzenia. Utwórzmy nową bazę $\mathcal{B}'' := \{u_i\}_{i \in \overline{1, N}}$ z wektorów

$$u_i := w_{2i-1} \quad u_{n+i} := w_{2i}, \quad i \in \overline{1, n}, \quad u_j := w_j, \quad j \in \overline{2n+1, N}.$$

Łatwo widzieć, że macierz ω_M w tak zadanej bazie ma pożądaną postać, a zatem macierz

$$B := [\text{id}_V]_{\mathcal{B}''}^{\mathcal{B}}$$

jest poszukiwaną macierzą sprowadzającą M do postaci kanonicznej, jawnie odwracalną. $\square$

Zwieńczeniem naszej krótkiej dyskusji form skośnie symetrycznych jest wzmianka o odnośnych automorfizmach. Oto więc

DEFINICJA 123. Przyjmijmy notację Def. 11, 13, 21, 32, 35, 61, 63, 105, 106, 107, 108 i 109, Stw. 168 oraz Przykł. 35 (2). Niechaj $((V, +_V, P_V, \bullet \mapsto 0_V), \ell_V, \omega)$ będzie przestrzenią ($\epsilon = 1$ -)hermitowską nad ciałem $\mathbb{K}$ z formą skośnie symetryczną ω . Jej automorfizmy określamy mianem **automorfizmów symplektycznych** (lub **transformacji symplektycznych**), generowaną zaś przez nie grupę

$$\text{Sp}(\omega) := \text{Aut}_{\mathbb{K}}(V, \omega)$$

nazywamy **grupą symplektyczną stowarzyszoną z ω** . W szczególności w przypadku przestrzeni $V := \mathbb{K}^{2n}$, $n \in \mathbb{N}$ wyposażonej w formę skośnie symetryczną o macierzy względem bazy standardowej danej przez macierz J_{2n} otrzymujemy w ten sposób **grupę symplektyczną stopnia $2n$ o współczynnikach z $\mathbb{K}$** , oznaczaną symbolem

$$\text{Sp}(2n; \mathbb{K}) \equiv \text{Sp}_{2n}(\mathbb{K}).$$

Macierz transformacji symplektycznej $S \in \text{Sp}(2n; \mathbb{K})$ względem bazy standardowej nazywamy **macierzą symplektyczną (stopnia $2n$)**. $\blacktriangle$

Bez trudu dowodzimy

STWIERDZENIE 169. Przyjmijmy notację Def. 11, 13, 21, 32, 35, 61, 63, 105, 106, 107, 108, 109 i 121, Stw. 168 oraz Przykł. 35 (2). Dowolna macierz symplektyczna $S \in \text{Mat}(\mathbb{K}; 2n)$, $n \in \mathbb{N}$ spełnia tożsamość

$$S^T \odot J_{2n} \odot S = J_{2n}.$$

W szczególności jest ona macierzą odwracalną. $\blacksquare$

Rola form ϵ -hermitowskich nie sprowadza się – bynajmniej – do opisu iloczynów skalarnych na przestrzeniach wektorowych tudzież odwzorowań dwuliniowych o ustalonej symetrii na przestrzeni stycznej do czasoprzestrzeni, względnie na przestrzeni stycznej do przestrzeni stanów układu dynamicznego. Na podobieństwo

sytuacji omówionej w Stw. 124 w przypadku form dwuliniowych można łatwo uzasadnić ich związek z endomorfizmami przestrzeni wektorowych wyposażonych w ustaloną nieosobliwą formę ϵ -hermitowską. Zanim rozwinieśmy dotychczasową dyskusję w tak określonym kierunku, poświęcimy trochę miejsca na zgłębienie anatomii endomorfizmu skończenie wymiarowej przestrzeni wektorowej.

9.5. Zagadnienie własne endomorfizmu

Endomorfizmy przestrzeni wektorowych odgrywają niezaprzeczalnie pierwszorzędną rolę w fizykalnych zastosowaniach algebry liniowej. Wystarczy przypomnieć znaczenie wyróżnionych hermitowskich endomorfizmów przestrzeni stanów skwantowanego układu dynamicznego, które opisują ładunki symetrii. Jest wśród nich operator energii określający ewolucję układu i porządkujący strukturę przestrzeni jego stanów według kryterium przynależności do podprzestrzeni odpowiadającej ustalonej wartości energii, co znajduje zastosowanie między innymi w rachunku zaburzeń. Te proste obserwacje usprawiedliwiają czas, jaki poświęcimy na zgłębienie podstawowych własności endomorfizmu i naturalnej organizacji jego dziedziny indukowanej przez jego na niej działanie. Chcąc umieścić nasze rozważania w nieco szerszym kadrze, zaczniemy od

DEFINICJA 124. Przyjmijmy notację Def. 11, 21, 23, 32, 35, 61, 63 i 65 oraz Stw. 65. Niechaj $((V, +_V, P_V, \bullet \mapsto 0_V), \ell)$ będzie przestrzenią wektorową nad ciałem $\mathbb{K}$ i niech R będzie pierścieniem, a nadto niech

$$\kappa : \mathbb{K} \longrightarrow R$$

będzie homomorfizmem pierścieni. **Realizacja pierścienia R na przestrzeni wektorowej V zgodna ze strukturą $\mathbb{K}$ -liniową** to homomorfizm pierścieni

$$\rho_R : R \longrightarrow \text{End}_{\mathbb{K}}(V)$$

o własności (wyrażonej przez diagram przemienności i równoważne zdanie logiczne)

$$\begin{array}{ccc} \mathbb{K} & \xrightarrow{\kappa} & R \\ & \searrow \ell & \downarrow \rho_R \\ & & \text{End}_{\mathbb{K}}(V) \end{array} \quad \equiv \quad \forall_{\lambda \in \mathbb{K}} : \rho_R \circ \kappa(\lambda) = \ell_{\lambda}.$$

▲

Bez trudu sprawdzamy

STWIERDZENIE 170. Przyjmijmy notację Def. 11, 21, 23, 32, 35, 61, 63, 65 i 124 oraz Stw. 65. Realizacja ρ_R pierścienia R na przestrzeni wektorowej V indukuje na V strukturę R -modułu z działaniem

$$\widehat{\rho}_R : R \times V \longrightarrow V : (r, v) \mapsto \rho_R(r)(v).$$

■

Przykładu opisanej struktury o fundamentalnym znaczeniu dla dalszej naszej dyskusji dostarcza

STWIERDZENIE 171. Przyjmijmy notację Def. 67, 11, 21, 23, 24, 32, 35, 61, 63, 65 i 124 oraz Stw. 65 i niech $\chi \in \text{End}_{\mathbb{K}}(V)$ będzie dowolnym endomorfizmem przestrzeni wektorowej V nad ciałem $\mathbb{K}$. Odwzorowanie

$$\rho_{\chi} : \mathbb{K}[t] \longrightarrow \text{End}_{\mathbb{K}}(V) : \sum_{n=0}^N \lambda_n t^n \longmapsto \ell_{\lambda_0} + \sum_{n=1}^N \ell_{\lambda_n} \circ \underbrace{\chi \circ \chi \circ \cdots \circ \chi}_{n \text{ razy}} \equiv \sum_{n=1}^N \ell_{\lambda_n} \circ \chi^n$$

określa realizację pierścienia $\mathbb{K}[t]$ na V zgodną ze strukturą $\mathbb{K}$ -liniową. Przy tym

$$\mathbb{K}[\chi] := \text{Im } \rho_{\chi} \subset \text{End}_{\mathbb{K}}(V)$$

jest podpierścieniem przemiennym. ■

Pośród realizacji pierścienia na przestrzeniach wektorowych występują typy o szczególnym znaczeniu dla naszych rozważań. Wyróżniamy je w poniższej

DEFINICJA 125. Przyjmijmy notację Def. 67, 11, 21, 23, 32, 35, 61, 63, 65, 68, 75, 77 i 124 oraz Stw. 75. Niechaj V będzie przestrzenią wektorową nad ciałem $\mathbb{K}$ i niech $\rho_R : R \longrightarrow \text{End}_{\mathbb{K}}(V)$ będzie realizacją pierścienia R na V zgodną ze strukturą $\mathbb{K}$ -liniową. Podzbiór $W \subset V$ jest **(pod)przestrzenią ρ_R -niezmienniczą**, jeśli jest spełniony warunek

$$\forall_{(r,w) \in R \times W} : \rho_R(r)(w) \in W.$$

Moduł nieprzywiedlny (lub **prosty**) to taka (niepusta) przestrzeń wektorowa, której jedynymi podprzestrzeniami R -niezmienniczymi są $\{0_V\}$ i V . Mówimy wtedy o **realizacji nieprzywiedlnej** (lub **prostej**) R na V . **Moduł całkowicie przywiedlny** (lub **półprosty**) to przestrzeń wektorowa będąca sumą prostą modułów nieprzywiedlnych. Mówimy wtedy o **realizacji całkowicie przywiedlnej** (lub **półprostej**) R na V .

indexrealizacja pierścienia na przestrzeni wektorowej zgodna ze strukturą $\mathbb{K}$ -liniową! całkowicie przywiedlna **Moduł cykliczny** to przestrzeń wektorowa V o własności

$$\exists_{v \in V} \forall_{w \in V} \exists_{r \in R} : w = \rho_R(r)(v),$$

którą zapisujemy zwięźle w postaci

$$V = \langle v \rangle_{\rho_R}.$$

Mówimy wtedy o **realizacji cyklicznej** R na V . ▲

Analiza podprzestrzeni niezmienniczych w dziedzinie zadanego endomorfizmu stanowi ważne źródło informacji o samym endomorfizmie i wewnętrznej strukturze jego dziedziny, co częstokroć ma implikacje fizyczne. Szczególnego i szczególnie ważnego z tego punktu widzenia przykładu podprzestrzeni niezmienniczej dostarcza

DEFINICJA 126. Przyjmijmy notację Def. 67, 11, 21, 23, 24, 32, 35, 61, 63, 64, 65 i 124 oraz Stw. 65 i 171. **Wektor własny endomorfizmu** χ to element $v \in V \setminus \{0_V\}$ o własności

$$\exists_{\lambda \in \mathbb{K}} : \chi(v) = \lambda \triangleright v.$$

Skalar $\lambda \in \mathbb{K}$ określony przez powyższą równość nosi miano **wartości własnej endomorfizmu** χ . Zbiór wszystkich wartości własnych χ nazywamy **widmem** (lub **spektrum**) **endomorfizmu** χ i oznaczamy symbolem

$$\mathrm{Sp} \chi := \{ \lambda \in \mathbb{K} \mid \exists_{v \in V} : \chi(v) = \lambda \triangleright v \}.$$

Przestrzeń własna endomorfizmu χ odpowiadająca wartości własnej $\lambda \in \mathrm{Sp} \chi$ to podprzestrzeń

$$V_1(\lambda; \chi) := \mathrm{Ker}(\chi - \ell_\lambda) \subset V.$$

▲

Mamy oczywiste

STWIERDZENIE 172. *Przyjmijmy notację Def. 67, 11, 21, 23, 24, 25, 32, 35, 61, 63, 64, 65, 68, 75, 77, 78, 79, 124 i 126 oraz Stw. 65, 75 i 171. Przestrzeń własna endomorfizmu χ jest ρ_χ -niezmiennicza. Jeśli $V = V_1(\lambda; \chi)$, to dla dowolnego wielomianu $w \in \mathbb{K}[t]$ zachodzi przy tym*

$$\rho_\chi(w) = \ell_{F_w(\lambda)},$$

jeśli zaś $V = \bigoplus_{i=1}^N V_1(\lambda_i; \chi)$, to dla dowolnych $v_i \in V_1(\lambda_i; \chi)$, $i \in \overline{1, N}$ jest

$$\rho_\chi(w) \left(\sum_{i=1}^N v_i \right) = \sum_{i=1}^N \ell_{F_w(\lambda_i)}(v_i) \equiv \sum_{i=1}^N F_w(\lambda_i) \triangleright v_i.$$

■

Praktyczny sens wcześniejszym uwagom o znaczeniu wyników analizy podprzestrzeni niezmienniczych endomorfizmu w dyskusji struktury wewnętrznej jego dziedziny nadaje poniższe

STWIERDZENIE 173. *Przyjmijmy notację Def. 67, 11, 21, 23, 32, 35, 61, 63, 64, 65, 68, 72, 73, 75, 77, 78, 79, 124 i 126 oraz Stw. 65. Układ wektorów własnych endomorfizmu $\chi \in \mathrm{End}_{\mathbb{K}}(V)$ odpowiadających parami różnym wartościom własnym χ jest liniowo niezależny. W szczególności, ilekroć $|\mathrm{Sp} \chi| = \dim_{\mathbb{K}} V$, istnieje baza przestrzeni V złożona z wektorów własnych χ . Bazę taką określamy mianem **bazy własnej endomorfizmu** χ . Zadaje ona rozkład*

$$V = \bigoplus_{\lambda \in \mathrm{Sp} \chi} V_1(\lambda; \chi).$$

■

Dowód: Niechaj $\{v^i\}_{i \in \overline{1, N}}$ będzie zbiorem wektorów własnych odpowiadających parami różnym wartościom własnym $\{\lambda_i\}_{i \in \overline{1, N}}$ endomorfizmu χ i niech $\{\mu_j\}_{j \in I \subset \overline{1, N}} \subset \mathbb{K}^\times$ będzie dowolną rodziną niezerowych skalarów o własności

$$(9.4) \quad \sum_{j \in I} \mu_j \triangleright v^j = 0_V$$

o minimalnej mocy, tj. taką, która spełnia warunek

$$\left(\{ \nu_k \}_{k \in J \subset \overline{1, N}} \in \mathcal{R}_0(\mathbb{K}) \quad \wedge \quad \sum_{k \in J} \nu_k \triangleright v^k = 0_V \right) \implies |J| \geq |I|.$$

Obliczając endomorfizm $\chi - \ell_{\lambda_j}$ określony dla dowolnego $j \in I$ na obu stronach równości (9.4), otrzymujemy wynik

$$\begin{aligned} 0_V &= (\chi - \ell_{\lambda_j})(0_V) = \sum_{k \in I} \mu_k \triangleright (\chi - \ell_{\lambda_j})(v^k) = \sum_{k \in I} (\mu_k \cdot_{\mathbb{K}} (\lambda_k - \lambda_j)) \triangleright v^k \\ &\equiv \sum_{k \in I \setminus \{j\}} (\mu_k \cdot_{\mathbb{K}} (\lambda_k - \lambda_j)) \triangleright v^k \end{aligned}$$

i tym samym stwierdzamy istnienie rodziny skalarów $\{\mu_k \cdot_{\mathbb{K}} (\lambda_k - \lambda_j)\}_{k \in I \setminus \{j\}}$ zadającej rozkład wektora zerowego i mniej licznej niż $\{\mu_j\}_{j \in I}$, co jest sprzeczne z założeniem o minimalnej mocy tej ostatniej. $\square$

Jakkolwiek w przypadku ogólnym endomorfizm nie określa wprost bazy (własnej) swojej dziedziny, to jednak ostatnia obserwacja uświadamia nam potrzebę zdobycia prostych narzędzi algebraicznych służących do wyznaczania widma endomorfizmu. Jak się okazuje, cel ten pozwala osiągnąć wnikliwa analiza jądra homomorfizmu ρ_χ , która dodatkowo daje wgląd w uporządkowanie struktury wewnętrznej dziedziny endomorfizmu w jego obecności (rozumiane w sensie rozkładu na sumę prostą podprzestrzeni ρ_χ -niezmienniczych) i – co nie mniej zaskakujące – pozwala w przypadku $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ rozszerzyć realizację ρ_χ na zbiór funkcji analitycznych na pewnym otoczeniu $\text{Sp } \chi \subset \mathbb{C}$. Przywoławszy zgromadzoną dotychczas wiedzę na temat struktury pierścienia $\mathbb{K}[t]$ (patrz, w szczególności: Stw. 13 oraz Tw. 4.1), łatwo weryfikujemy

STWIERDZENIE 174. *Przyjmijmy notację Def. 67, 11, 21, 23, 24, 32, 35, 61, 63, 65 i 124 oraz Stw. 65 i 171. Podpierścień $\text{Ker } \rho_\chi \subset \mathbb{K}[t]$ jest ideałem głównym pierścienia $\mathbb{K}[t]$.*

■

W dalszej części wykładu pokażemy, że ideał ten jest nietrywialny, co będzie miało daleko idące konsekwencje formalne i rachunkowe. W tym celu wprowadzamy

DEFINICJA 127. Przyjmijmy notację Def. 67, 11, 21, 24, 25, 32, 35, 61, 63, 65, 68, 70, 72, 73, 75, 77, 82, 87 i 92, Stw. 65 oraz Przykł. 34 (2), 40 (3) i 41. Niechaj χ będzie endomorfizmem skończenie wymiarowej przestrzeni wektorowej V nad ciałem $\mathbb{K}$. **Wielomian charakterystyczny endomorfizmu** χ to element $w_\chi \in \mathbb{K}[t]$ o funkcji wielomianowej

$$P_\chi := F_{w_\chi} : \mathbb{K} \curvearrowright : \lambda \longmapsto \det(\chi - \ell_\lambda).$$

▲

Badanie wielomianu charakterystycznego zaczniemy od obserwacji natury formalnej: oto stowarzyszona z nim funkcja wielomianowa generuje niezmienniki skalarne endomorfizmu, co wyraża

STWIERDZENIE 175. *Przyjmijmy notację Def. 67, 11, 21, 24, 25, 32, 35, 61, 63, 65, 68, 70, 72, 73, 75, 77, 82, 87, 92, 94, 95 i 127, Stw. 65, 70, 75, 94 i 140 oraz Przykł. 34 (2), 40 (3), 41 i 46 (2). Niechaj χ będzie endomorfizmem przestrzeni wektorowej V wymiaru $\dim_{\mathbb{K}} V =: N < \infty$ nad ciałem $\mathbb{K}$. Skalary*

$$\tau_n(\chi) := \frac{(-1)^n}{n!} \frac{d^n}{d\lambda^n} \Big|_{\lambda=0} P_\chi(\lambda), \quad n \in \overline{0, N-1}$$

zapisane w konwencji $\frac{d^0}{d\lambda^0} P_\chi(\lambda) \equiv P_\chi(\lambda)$, są niezmiennikami wyboru bazy w V , zwanymi **niezmiennikami podstawowymi endomorfizmu** χ . W szczególności

$$\tau_0(\chi) = \det \chi, \quad \tau_{N-1}(\chi) = \operatorname{Tr}_V(\chi).$$

■

Miejsce wielomianu charakterystycznego w prowadzonej przez nas dyskusji realizacji pierścienia wielomianów $\mathbb{K}[t]$ na V zgodnej ze strukturą $\mathbb{K}$ -liniową określa podstawowe

TWIERDZENIE 9.8 (Cayleya–Hamiltona). *Przyjmijmy notację Def. 67, 11, 21, 24, 25, 32, 35, 36, 61, 63, 65, 68, 70, 72, 73, 75, 77, 82, 87, 92 i 127, Stw. 65 oraz Przykł. 34 (2), 40 (3) i 41. Wielomian charakterystyczny endomorfizmu χ skończenie wymiarowej przestrzeni wektorowej V należy do jądra homomorfizmu ρ_χ ,*

$$w_\chi \in \operatorname{Ker} \rho_\chi.$$

■

Dowód: Wybierzmy w V dowolną bazę $\mathcal{B} := \{v^i\}_{i \in \overline{1, N}}$, $N := \dim_{\mathbb{K}} V$ i oznaczmy

$$H_\lambda := [\chi - \ell_\lambda]_{\mathcal{B}}^{\mathcal{B}}, \quad H := [\chi]_{\mathcal{B}}^{\mathcal{B}}.$$

Na mocy Tw. 8.13 otrzymujemy tożsamość

$$\widetilde{H}_\lambda \odot H_\lambda = P_\chi(\lambda) \triangleright_{(N)} \mathbf{1}_N,$$

którą należy rozumieć, jak następuje: oto funkcję wielomianową stowarzyszoną z wielomianem charakterystycznym można zapisać – dla dowolnie wybranego indeksu $i \in \overline{1, N}$ – w postaci sumy wyrażeń sfaktoryzowanych

$$P_\chi(\lambda) = \sum_{j=1}^N \widetilde{H}_\lambda(i, j) \cdot_{\mathbb{K}} H_\lambda(j, i)$$

na funkcję wielomianową $\widetilde{H}_\lambda(i, j)$ stopnia $N - 1$ (w zmiennej λ) i funkcję wielomianową $H_\lambda(j, i)$ stopnia 1, a ponadto dla dowolnych dwóch indeksów $k \neq i \in \overline{1, N}$ zachodzi równość

$$0_{\mathbb{K}} = \sum_{j=1}^N \widetilde{H}_\lambda(i, j) \cdot_{\mathbb{K}} H_\lambda(j, k).$$

Oznaczmy wielomian odpowiadający funkcji $\widetilde{H}_\lambda(i, j)$ jako $\widetilde{w}_{i,j}^\chi$, ten zaś odpowiadający funkcji $H_\lambda(i, j)$ – jako $w_{i,j}^\chi$. Na podstawie dotychczasowej analizy możemy zadać endomorfizm $\rho_\chi(w_\chi)$ na bazie $\mathcal{B}$ (i – co za tym idzie – na całej przestrzeni V) wzorem

$$\begin{aligned} \rho_\chi(w_\chi)(v^i) &= \rho_\chi \left(\sum_{j=1}^N \widetilde{w}_{i,j}^\chi \boxplus w_{j,i}^\chi \right) (v^i) \\ &\equiv \rho_\chi \left(\sum_{j=1}^N \widetilde{w}_{i,j}^\chi \boxplus w_{j,i}^\chi \right) (v^i) +_V \sum_{\substack{k=1 \\ k \neq i}}^N \rho_\chi \left(\sum_{j=1}^N \widetilde{w}_{i,j}^\chi \boxplus w_{j,k}^\chi \right) (v^k) \\ &\equiv \sum_{j,k=1}^N \rho_\chi(\widetilde{w}_{i,j}^\chi \boxplus w_{j,k}^\chi)(v^k) = \sum_{j,k=1}^N \rho_\chi(\widetilde{w}_{i,j}^\chi) \circ \rho_\chi(w_{j,k}^\chi)(v^k). \end{aligned}$$

Jednakowoż

$$w_{j,k}^\chi = H(j,k) - \delta_{i,j}^{\mathbb{K}} \triangleright t,$$

zatem

$$\rho_\chi(w_{j,k}^\chi) = \ell_{H(j,k)} - \ell_{\delta_{i,j}^{\mathbb{K}}} \circ \chi,$$

a w takim razie

$$\begin{aligned} \rho_\chi(w_\chi)(v^i) &= \sum_{j,k=1}^N \rho_\chi(\tilde{w}_{i,j}^\chi) (H(j,k) \triangleright v^k - \delta_{j,k}^{\mathbb{K}} \triangleright \chi(v^k)) \\ &= \sum_{j,k=1}^N \rho_\chi(\tilde{w}_{i,j}^\chi) \left(H(j,k) \triangleright v^k - \delta_{j,k}^{\mathbb{K}} \triangleright \sum_{l=1}^N H(k,l) \triangleright v^l \right) = 0_V. \end{aligned}$$

Ostatecznie więc

$$\forall_{i \in \overline{1,N}} : \rho_\chi(w_\chi)(v^i) = 0_V,$$

czyli też

$$\forall_{v \in V} : \rho_\chi(w_\chi)(v) = 0_V,$$

co daje pożądaną tożsamość

$$\rho_\chi(w_\chi) = 0.$$

□

Znalazłszy nietrywialny element $\text{Ker } \rho_\chi$, łatwo bronimy

STWIERDZENIE 176. *Przyjmijmy notację Def. 67, 11, 21, 23, 24, 32, 35, 36, 61, 63, 65 i 124 oraz Stw. 65 i 171. Istnieje wielomian $q_\chi \in \mathbb{K}[t]$ o własności*

$$\text{Ker } \rho_\chi = \langle q_\chi \rangle_{\rho_\chi},$$

określony jednoznacznie z dokładnością do współczynnika $\lambda \in \mathbb{K}^\times$ przy najwyższej potędze zmiennej. Kładąc $\lambda := 1_{\mathbb{K}}$ otrzymujemy **wielomian minimalny endomorfizmu** χ , który będziemy oznaczać symbolem p_χ .

■

Dowód: W świetle Tw. 9.8 podpierścień $\text{Ker } \rho_\chi$ jest nietrywialnym ideałem (obustronnym) w $\mathbb{K}[t]$ (należy podkreślić, że znaleziony wcześniej jego element w_χ jest wielomianem stopnia $\dim_{\mathbb{K}} V$ o niezerowym współczynniku przy najwyższej potędze, zatem różnym od wielomianu zerowego, o ile tylko V jest przestrzenią nietrywialną, co zakładamy). Ponieważ jednak $\mathbb{K}[t]$ jest na mocy Stw. 13 dziedziną ideałów głównych, przeto istnieje generator $\mathbb{K}[t]$ -podmodułu $\text{Ker } \rho_\chi \subset \mathbb{K}[t]$. Jest jasnym, że dowolne dwa generatory są tego samego stopnia, zatem swoboda wyboru q_χ sprowadza się do ustalenia współczynnika λ , o którym mowa w treści stwierdzenia. □

Jawną postać wielomianu minimalnego przedstawimy niebawem, tymczasem zaznamy dobitnie jego cechę definiującą.

COROLLARIUM 23. *Przyjmijmy notację Def. 67, 11, 21, 23, 24, 28, 32, 35, 36, 61, 63, 65 i 124 oraz Stw. 65, 171 i 176. Wielomian minimalny p_χ endomorfizmu χ dzieli dowolny wielomian z jądra homomorfizmu ρ_χ ,*

$$\forall_{w \in \text{Ker } \rho_\chi} : p_\chi \mid w.$$

■

Praktyczny sens konstrukcji wielomianu charakterystycznego, zapowiadany na wstępie tej części naszych rozważań, ujawnia

STWIERDZENIE 177. *Przyjmijmy notację Def. 67, 11, 21, 23, 24, 25, 32, 35, 61, 63, 65, 68, 70, 72, 73, 75, 77, 82, 87, 92, 124, 126 i 127, Stw. 65 i 171 oraz Przykł. 34 (2), 40 (3) i 41. Dla dowolnego endomorfizmu χ skończenie wymiarowej przestrzeni wektorowej V nad ciałem $\mathbb{K}$ zachodzi tożsamość*

$$\text{Sp } \chi = P_\chi^{-1}(\{0_{\mathbb{K}}\}).$$

■

Dowód: Wprost z definicji

$$\lambda \in \text{Sp } \chi \iff \text{Ker } (\chi - \ell_\lambda) \neq \{0_V\},$$

ale też w świetle Stw. 120 prawdziwą jest równoważność

$$\text{Ker } (\chi - \ell_\lambda) \neq \{0_V\} \iff \det(\chi - \ell_\lambda) = 0_{\mathbb{K}}.$$

□

Ostatnia nasza obserwacja uzasadnia

DEFINICJA 128. Przyjmijmy notację Def. 67, 11, 21, 24, 26, 25, 29, 32, 35, 61, 63, 64, 65, 68, 70, 72, 73, 75, 77, 82, 87, 92, 124, 126 i 127, Stw. 65 i 171 oraz Przykł. 34 (2), 40 (3) i 41. Wartość własną $\lambda \in \text{Sp } \chi$ nazywamy **zwyródniałą** (lub **zdegenerowaną**), jeśli jest ona zerem o krotności $\kappa(\lambda|w_\chi) > 1$ wielomianu charakterystycznego χ . W przeciwnym razie λ określamy mianem **niezwyródniałej** (lub **niezdegenerowanej**). Jeśli któraś z wartości własnych χ jest zwyródniałą, to mówimy o **widmie (spektrum) zwyródniałym** (lub **zdegenerowanym**), w przeciwnym razie mamy do czynienia z **widmem niezwyródniałym** (lub **niezdegenerowanym**).

▲

Tak oto dotychczasowa dyskusja daje nam do ręki wygodne narzędzie analizy widmowej endomorfizmów (skończenie wymiarowych) przestrzeni wektorowych. Na tym jednak nie kończy się rola wielomianu charakterystycznego w szczególnie interesujących dla nas przypadkach $\mathbb{K} \in \{\mathbb{C}, \mathbb{R}\}$. Ażeby się o tym przekonać, rozważmy

STWIERDZENIE 178. *Przyjmijmy notację Def. 67, 21, 11, 14, 18, 24, 25, 26, 27, 28 i 32. Niechaj $\mathbb{K} \in \{\mathbb{C}, \mathbb{R}\}$, niech $w \in \mathbb{K}[t]$ będzie dowolnym wielomianem niezerowym, $\mathcal{O}_w \subset \mathbb{C}$ – otoczeniem zbioru $F_w^{-1}(\{0\})$ jego zer i niech $f : \mathcal{O}_w \rightarrow \mathbb{C}$ będzie funkcją analityczną⁵, co do której w przypadku $\mathbb{K} = \mathbb{R}$ zakładamy dodatkowo,*

⁵Czyli taką, która daje się przedstawić w postaci granicy ciągu sum częściowych szeregu potęgowego zbieżnego na $\mathcal{O}_w$.

że jest rzeczywista, tj. spełnia warunek

$$\forall \lambda \in \mathcal{O}_w : \left(\bar{\lambda} \in \mathcal{O}_w \quad \wedge \quad f(\bar{\lambda}) = \overline{f(\lambda)} \right).$$

Istnieje dokładnie jeden wielomian $\varrho_f \in \mathbb{C}[t]$ stopnia niższego niż w ,

$$\deg \varrho_f < \deg w,$$

dla którego istnieje funkcja analityczna $\sigma : \mathcal{O}_w \longrightarrow \mathbb{C}$ spełniająca tożsamość

$$(9.5) \quad f = F_w \cdot \sigma + F_{\varrho_f}.$$

Jeśli f jest rzeczywista i $w \in \mathbb{R}[t]$, to także $\varrho_f \in \mathbb{R}[t]$. Rzeczony wielomian jest określany jako **wielomian interpolujący dla funkcji f względem wielomianu w** .

■

Dowód: Podstawową rolę w dowodzie stwierdzenia odgrywa

LEMAT 9.9. Przyjmijmy notację Def. 67, 21, 11, 24, 25, 26, 27, 32, 35, 61, 65, 70 i 94, Stw. 14 oraz Przykł. 34 (2). Ustalmy (dowolnie) liczbę $N \in \mathbb{N}^*$ i oznaczmy

$$\mathbb{K}_{N-1}[t] := \{ w \in \mathbb{K}[t] \mid \deg w \leq N-1 \} \subset \mathbb{K}[t],$$

a następnie rozważmy przestrzeń $\mathbb{K}$ -liniową

$$\left((\mathbb{K}_{N-1}[t], \oplus, \mathbb{P}_{\mathbb{K}[t]}, \bullet \longmapsto \mathbf{0}), \ell_{\mathbb{K}[t]} \right).$$

Niechaj $\{\lambda_i\}_{i \in \overline{1, r}} \subset \mathbb{K}$ będzie rodziną $r \in \overline{1, N}$ parami różnych liczb zespolonych i niech $\{k_i\}_{i \in \overline{1, r}} \subset \mathbb{N}^*$ będzie rodziną liczb naturalnych spełniających warunek

$$\sum_{i=1}^r k_i = N.$$

Zbiór $\{\varphi_i^{(p_i)}\}_{\substack{p_i \in \overline{0, k_i-1} \\ i \in \overline{1, r}}}$ form liniowych na $\mathbb{K}_{N-1}[t]$ określonych wzorami

$$\varphi_i^{(p_i)} : \mathbb{K}_{N-1}[t] \longrightarrow \mathbb{K} : w \longmapsto \frac{1}{p_i!} \frac{d^{p_i}}{d\lambda^{p_i}} \Big|_{\lambda=\lambda_i} F_w(\lambda),$$

zapisanymi w konwencji $\frac{d^0}{d\lambda^0} \Big|_{\lambda=\lambda_i} F_w(\lambda) \equiv F_w(\lambda_i)$, jest liniowo niezależny nad $\mathbb{K}$, a zatem stanowi bazę przestrzeni $\mathbb{K}_{N-1}[t]^*$.

■

Dowód: Oznaczmy

$$\begin{aligned} \psi_{p_1} &:= \varphi_1^{(p_1)}, & p_1 \in \overline{0, k_1-1}, \\ \psi_{k_1+p_2} &:= \varphi_2^{(p_2)}, & p_2 \in \overline{0, k_2-1}, \\ \psi_{k_1+k_2+p_3} &:= \varphi_3^{(p_3)}, & p_3 \in \overline{0, k_3-1}, \\ &\vdots \end{aligned}$$

$$\psi_{k_1+k_2+\dots+k_{r-1}+p_r} := \varphi_r^{(p_r)}, \quad p_r \in \overline{0, k_r-1}$$

i wprowadźmy, korzystając z tych samych oznaczeń, bazę $\mathbb{K}_{N-1}[t]$ złożoną z wielomianów

$$\begin{aligned} w_{p_1} &:= (t - \lambda_1)^{p_1}, \\ w_{k_1+p_2} &:= \frac{1}{(\lambda_2 - \lambda_1)} \cdot (t - \lambda_1)^{k_1} \square (t - \lambda_2)^{p_2}, \\ w_{k_1+k_2+p_3} &:= \frac{1}{(\lambda_3 - \lambda_1) \cdot (\lambda_3 - \lambda_2)} \cdot (t - \lambda_1)^{k_1} \square (t - \lambda_2)^{k_2} \square (t - \lambda_3)^{p_3}, \\ &\vdots \\ w_{k_1+k_2+\dots+k_{r-1}+p_r} &:= \frac{1}{(\lambda_r - \lambda_1) \cdot (\lambda_r - \lambda_2) \cdots (\lambda_r - \lambda_{r-1})} \cdot (t - \lambda_1)^{k_1} \square (t - \lambda_2)^{k_2} \\ &\quad \square \cdots \square (t - \lambda_{r-1})^{k_{r-1}} \square (t - \lambda_r)^{p_r}. \end{aligned}$$

Zwróćmy uwagę, że wielomiany te są dobrze określone na mocy założeń poczynionych w odniesieniu do liczb λ_i . Łatwo obliczamy

$$\forall_{j > \overline{i \in 0, N-1}} : \psi_i(w_j) = 0,$$

a ponadto

$$\forall_{i \in \overline{0, N-1}} : \psi_i(w_i) = 1,$$

skąd wniosek, że macierz ewaluacji

$$\Psi := (\psi_i(w_j))_{i,j \in \overline{0, N-1}}$$

jest dolnotrójkątna i zgodnie z argumentacją z Przykł. 44 (1) ma wyznacznik

$$\det_{(N)}(\Psi) = 1.$$

W świetle Stw. 144 ostatnia równość implikuje liniową niezależność układu funkcjonalów $\{\varphi_i^{(p_i)}\}_{\substack{p_i \in \overline{0, k_i-1} \\ i \in \overline{1, r}}}$. $\square$

Znalazłszy wygodną konstrukcję bazy przestrzeni $\mathbb{K}_{N-1}[t]^*$ sprzężonej do $\mathbb{K}_{N-1}[t]$, wróćmy teraz do dowodu zasadniczego. Wobec skończoności wymiaru $\dim_{\mathbb{C}} \mathbb{C}_{N-1}[t] = N < \infty$ a na mocy Stw. 142 homomorfizm kanoniczny $c_{\mathbb{C}_{N-1}[t]} : \mathbb{C}_{N-1}[t] \rightarrow \mathbb{C}_{N-1}[t]^{**}$ jest izomorfizmem, co oznacza, że każdy wielomian (stopnia nie większego niż $N-1$) może być traktowany jako funkcjonal na $\mathbb{C}_{N-1}[t]^*$ i jako taki jest jednoznacznie określony przez wartości, jakie przyjmuje na bazie tej przestrzeni. W szczególności więc istnieje dokładnie jeden wielomian $\varrho_f \in \mathbb{C}_{N-1}[t]$ spełniający układ warunków

$$\frac{1}{p_i!} \frac{d^{p_i}}{d\lambda^{p_i}} \Big|_{\lambda=\lambda_i} F_{\varrho_f}(\lambda) = c_{\mathbb{C}_{N-1}[t]}(\varrho_f)(\varphi_i^{(p_i)}) = C_i^{p_i}, \quad p_i \in \overline{0, k_i-1}, \quad i \in \overline{1, r}$$

zapisany dla dowolnego zestawu liczb $C_i^{p_i} \in \mathbb{C}$. Niechaj wielomian w , o którym mowa w treści stwierdzenia, ma rozkład

$$w = (t - \lambda_1)^{k_1} \square (t - \lambda_2)^{k_2} \square \cdots \square (t - \lambda_r)^{k_r}$$

w dotychczasowych oznaczeniach (istnienie takiego rozkładu dla pewnych wartości parametrów zapewnia Tw. 4.3). Wybierając liczby $C_i^{p_i} \in \mathbb{C}$ w postaci

$$C_i^{p_i} := \frac{1}{p_i!} \frac{d^{p_i}}{d\lambda^{p_i}} \Big|_{\lambda=\lambda_i} f(\lambda),$$

określonej przez zadaną funkcję analityczną $f : \mathcal{O}_w \longrightarrow \mathbb{C}$, otrzymujemy wynik

$$(9.6) \quad \forall_{i \in \overline{1, r}} \quad \forall_{p_i \in \overline{0, k_i-1}} : \frac{d^{p_i}}{d\lambda^{p_i}} \Big|_{\lambda=\lambda_i} (f - F_{\varrho_f})(\lambda) = 0,$$

którego słusność jest warunkiem koniecznym istnienia rozkładu 9.5. O tym, że jest to zarazem warunek wystarczający, przekonuje następujące rozumowanie. Powyższy wynik pozwala nam rozwinąć funkcję analityczną $f - F_{\varrho_f}$ w otoczeniu $\mathcal{O}_i \ni \lambda$ punktu $\lambda_i \in w^{-1}(\{0\})$ w szereg potęgowy

$$(f - F_{\varrho_f})(\lambda) = \sum_{n=0}^{\infty} c_n (\lambda - \lambda_i)^n,$$

którego pierwszych k_i współczynników jest tożsamościowo równych zeru,

$$\forall_{n \in \overline{0, k_i-1}} : c_n = 0.$$

Możemy zatem zdefiniować odwzorowanie

$$\sigma : \mathcal{O}_w \longrightarrow \mathbb{C} : \lambda \longmapsto \frac{(f - F_{\varrho_f})(\lambda)}{F_w(\lambda)},$$

którego rozwinięcie wokół dowolnego elementu λ_i zbioru $w^{-1}(\{0\})$ przybiera postać

$$\sigma(\lambda) = \prod_{\substack{j=1 \\ j \neq i}}^r (\lambda - \lambda_j)^{-k_j} \sum_{m=0}^{\infty} c_{k_i+m} (\lambda - \lambda_i)^m.$$

Zważywszy analityczny charakter mnożnika $\prod_{\substack{j=1 \\ j \neq i}}^r (\lambda - \lambda_j)^{-k_j}$ w otoczeniu λ_i , wnioskujemy, że σ jest funkcją analityczną, zgodnie z tezą stwierdzenia.

Pozostaje upewnić się, że wielomian interpolujący dla funkcji rzeczywistej względem wielomianu o współczynnikach rzeczywistych ma także współczynniki rzeczywiste. Zauważmy w tym celu, że z dowolną funkcją analityczną $F : \mathcal{O}_w \longrightarrow \mathbb{C}$ możemy stowarzyszyć nową funkcję analityczną $F^* : \mathcal{O}_w \longrightarrow \mathbb{C} : \lambda \longmapsto \overline{F(\overline{\lambda})}$, przy czym ilekroć F jest rzeczywista, zachodzi tożsamość $F^* \equiv F$. W szczególności więc $f^* \equiv f$ i $F_w^* \equiv F_w$, a zatem $F_w \cdot \sigma^* + F_{\varrho_f}^* = f^* \equiv f = F_w \cdot \sigma + F_{\varrho_f}$, co wobec analityczności σ^* i jedyności wielomianu interpolującego dla f względem w oznacza pożądaną równość $F_{\varrho_f}^* = F_{\varrho_f}$. $\square$

Powyższe stwierdzenie nadaje sens formalny

DEFINICJA 129. Przyjmijmy notację Def. 67, 11, 14, 21, 23, 24, 25, 26, 27, 28, 32, 35, 36, 61, 63, 65, 124 i 126 oraz Stw. 65, 171, 176 i 178. Niechaj χ będzie endomorfizmem skończenie wymiarowej przestrzeni wektorowej V nad ciałem $K \in \{\mathbb{C}, \mathbb{R}\}$, niech $\mathcal{O}_\chi \subset \mathbb{C}$ będzie dowolnym otoczeniem widma $\text{Sp } \chi$ i niech $f : \mathcal{O}_\chi \longrightarrow \mathbb{C}$ będzie funkcją analityczną, co do której w przypadku $K = \mathbb{R}$ zakładamy dodatkowo, że jest rzeczywista. Niech ϱ_f będzie wielomianem interpolującym dla f względem dowolnego wielomianu $w \in \text{Ker } \rho_\chi$. Wynik **ewaluacji**

funkcji f na endomorfizmie χ określamy formułą

$$f(\chi) := \rho_\chi(\varrho_f).$$

▲

Dotychczasowe nasze rozważania pozwalają sformułować istotne

STWIERDZENIE 179. *Przyjmijmy notację Def. 67, 11, 14, 21, 23, 24, 25, 26, 27, 28, 32, 35, 36, 61, 63, 64, 68, 75, 65, 72, 73, 82, 124, 126 i 129, Stw. 65, 75, 95, 96, 171, 176 i 178 oraz Przykł. 41. Niechaj χ będzie endomorfizmem przestrzeni wektorowej V skończonego wymiaru $N := \dim_{\mathbb{K}} V < \infty$ nad ciałem $\mathbb{K} \in \{\mathbb{C}, \mathbb{R}\}$, niech $\mathcal{O}_\chi \subset \mathbb{C}$ będzie dowolnym otoczeniem widma $\text{Sp } \chi$ i niech $f : \mathcal{O}_\chi \rightarrow \mathbb{C}$ będzie funkcją analityczną, co do której w przypadku $\mathbb{K} = \mathbb{R}$ założymy dodatkowo, że jest rzeczywista. Wynik ewaluacji funkcji f na endomorfizmie χ jest dobrze określony, tj. nie zależy od wyboru wielomianu $w \in \text{Ker } \rho_\chi$, względem którego określamy wielomian interpolujący ϱ_f . W szczególności możemy zawsze wybrać wielomian*

$$\varrho_f = \sum_{n=0}^{N-1} \mu_n \cdot t^n \in \mathbb{C}_{N-1}[t]$$

o współczynnikach danych wzorem

$$\begin{pmatrix} \mu_0 \\ \mu_1 \\ \mu_2 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \mu_{N-1} \end{pmatrix} = \begin{pmatrix} \Lambda_1 \\ \Lambda_2 \\ \Lambda_3 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \Lambda_r \end{pmatrix}^{-1} \odot \begin{pmatrix} f(\lambda_1) \\ f'(\lambda_1) \\ \vdots \\ f^{(k_1-1)}(\lambda_1) \\ f(\lambda_2) \\ f'(\lambda_2) \\ \vdots \\ f^{(k_2-1)}(\lambda_2) \\ \vdots \\ f(\lambda_r) \\ f'(\lambda_r) \\ \vdots \\ f^{(k_r-1)}(\lambda_r) \end{pmatrix}$$

zapisanym przy użyciu macierzy $\Lambda_i \in \text{Mat}(\mathbb{C}; k_i \times N)$ (określonych dla dowolnego $i \in \overline{1, r}$)

$$\Lambda_i$$

$$:= \begin{pmatrix} 0! & \lambda_i & \lambda_i^2 & \lambda_i^3 & \cdots & \cdots & \lambda_i^{N-1} \\ 0 & 1! & 2!\lambda_i & 3\lambda_i^2 & \cdots & \cdots & (N-1)\lambda_i^{N-2} \\ 0 & 0 & 2! & 3!\lambda_i & \cdots & \cdots & (N-1)(N-2)\lambda_i^{N-3} \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & (k_i-1)! & k_i!\lambda_i & \cdots & (N-1)(N-2)\cdots(N-k_i+1)\lambda_i^{N-k_i+1} \end{pmatrix}.$$

■

Dowód: Ostatnia część tezy jest elementarną transkrypcją warunków (9.6). Jedynym zatem orzeczeniem, które należy zweryfikować, jest to mówiące o niezależności wyniku ewaluacji f na χ od wyboru wielomianu $w \in \text{Ker } \rho_\chi$. Niech zatem

w_α , $\alpha \in \{1, 2\}$ będą dwoma takimi wielomianami, zadającymi odnośne rozkłady $f = w_\alpha \cdot \sigma_\alpha + \varrho_f^{(\alpha)}$. W świetle Cor. 23 spełnione są relacje

$$p_\chi \mid w_\alpha, \quad \alpha \in \{1, 2\},$$

które implikują tożsamość

$$\varrho_f^{(2)} - \varrho_f^{(1)} \equiv (f - \varrho_f^{(1)}) - (f - \varrho_f^{(2)}) = p_\chi \cdot \sigma_{1,2},$$

zapisaną przy użyciu pewnej funkcji analitycznej $\sigma_{1,2} : \mathcal{O}_\chi \longrightarrow \mathbb{C}$. Na mocy Tw. 9.8 otrzymujemy przeto spodziewany wynik

$$\rho_\chi(\rho_f^{(2)}) = \rho_\chi(\rho_f^{(1)}) + \rho_\chi(p_\chi) \circ \sigma_{1,2}(\chi) = \rho_\chi(\rho_f^{(1)}).$$

□

Wiedzę zgromadzoną w tym rozdziale wykorzystamy w dalszych, bardziej szczegółowych studiach struktury endomorfizmu przestrzeni wektorowej, których celem praktycznym będzie sprowadzenie go do postaci kanonicznej (zwanej też normalną) poprzez przemyślny wybór bazy w jego dziedzinie. Wybór ten, podyktowany przez rozpoczętą tu analizę widmową endomorfizmu, dostarczy czytelnego obrazu rozszczepienia dziedziny endomorfizmu na podprzestrzenie niezmiennicze względem jego działania.

9.6. Rozkład dziedziny endomorfizmu na przestrzenie pierwiastkowe

Obecność podprzestrzeni niezmienniczej w dziedzinie endomorfizmu V rodzi naturalne pytanie o niezmienniczość jej dopełnienia prostego w V . Jest jasnym, że twierdząca odpowiedź na to pytanie pozwala przedstawić rzeczony endomorfizm w szczególnie prostej postaci, a mianowicie jako sumę jego ograniczeń do każdego ze składników rozkładu dziedziny. Przedmiot zainteresowania precyzuje

DEFINICJA 130. Przyjmijmy notację Def. 67, 11, 21, 23, 32, 35, 61, 63, 64, 65, 68, 75, 77, 78 i 79 oraz Stw. 75. Niechaj V będzie przestrzenią wektorową nad ciałem $\mathbb{K}$ i niech $\chi \in \text{End}_{\mathbb{K}}(V)$ będzie endomorfizmem V . Ponadto niech $W \subset V$ będzie podprzestrzenią V o dopełnieniu prostym $\widetilde{W} \subset V$,

$$V = W \oplus \widetilde{W}.$$

Podprzestrzeń W nazywamy **podprzestrzenią redukującą dla endomorfizmu χ** , jeśli zarówno W jak i $\widetilde{W}$ są **niezmiennicze względem χ** (lub χ -**niezmiennicze**), tj. jeśli zachodzą relacje

$$\chi(W) \subset W \quad \wedge \quad \chi(\widetilde{W}) \subset \widetilde{W}.$$

Powiemy wtedy, że **podprzestrzeń W redukuje endomorfizm χ** , sam zaś endomorfizm χ będziemy określać mianem **redukowalnego względem W** .

▲

Precyzyjnych a przy tym wygodnych narzędzi do badania zagadnienia redukowalności endomorfizmu χ względem ustalonej podprzestrzeni χ -niezmienniczej jego dziedziny dostarcza sformułowanie opisu sum prostych w terminach rodzin rzutów komplementarnych (na składowe), które podaliśmy w Stw. 88.

STWIERDZENIE 180. Przyjmijmy notację Def. 67, 11, 21, 23, 32, 35, 61, 63, 64, 65, 68, 75, 77, 78, 79, 80 i 130 oraz Stw. 75 i 88. Niechaj przestrzeń wektorowa V nad ciałem $\mathbb{K}$ będzie (wewnętrzną) sumą prostą rodziny $\{V^{(\lambda)}\}_{\lambda \in \Lambda}$ swoich podprzestrzeni $V^{(\lambda)} \subset V$,

$$(9.7) \quad V = \bigoplus_{\lambda \in \Lambda} V^{(\lambda)},$$

niech $\{\pi_\lambda\}_{\lambda \in \Lambda}$ będzie stowarzyszoną z tym rozkładem zupełną rodziną rzutów komplementarnych i niech χ będzie endomorfizmem V . Rozkład (9.7) jest χ -niezmienniczy wtedy i tylko wtedy, gdy endomorfizm χ jest **przemienny** (lub **komutuje**) ze wszystkimi operatorami rzutu π_λ , tj. prawdziwą jest równoważność

$$\forall_{\lambda \in \Lambda} : \chi(V^{(\lambda)}) \subset V^{(\lambda)} \iff \forall_{\lambda \in \Lambda} : \chi \circ \pi_\lambda = \pi_\lambda \circ \chi.$$

■

Dowód:

$\Rightarrow$ Wobec tożsamości $\text{Im } \pi_\lambda = V^{(\lambda)} = \pi_\lambda(V^{(\lambda)})$ relacja $\chi(V^{(\lambda)}) \subset V^{(\lambda)}$ implikuje równość $\pi_\lambda \circ \chi \circ \pi_\lambda = \chi \circ \pi_\lambda$, z której dalej wyprowadzamy – korzystając z Równ. (8.12) – pożądane związki przemienności

$$\begin{aligned} \pi_\lambda \circ \chi &\equiv \pi_\lambda \circ \chi \circ \text{id}_V = \pi_\lambda \circ \chi \circ \sum_{\mu \in \Lambda} \pi_\mu = \sum_{\mu \in \Lambda} \pi_\lambda \circ (\chi \circ \pi_\mu) = \sum_{\mu \in \Lambda} \pi_\lambda \circ (\pi_\mu \circ \chi \circ \pi_\mu) \\ &= \sum_{\mu \in \Lambda} \delta_{\lambda, \mu}^{\mathbb{K}} \triangleright \pi_\mu \circ \chi \circ \pi_\mu = \pi_\lambda \circ \chi \circ \pi_\lambda = \chi \circ \pi_\lambda. \end{aligned}$$

$\Leftarrow$ W świetle tożsamości wypisanych w poprzednim punkcie zachodzi inkluzja $\chi(V^{(\lambda)}) = \chi \circ \pi_\lambda(V^{(\lambda)}) = \pi_\lambda \circ \chi(V^{(\lambda)}) \subset V^{(\lambda)}$.

□

Rozszczepienie przestrzeni wektorowej na sumę prostą jej podprzestrzeni niezmienniczych względem działania ustalonego endomorfizmu pozwala wyciągnąć wnioski odnośnie do struktury tego ostatniego. Oto bowiem

STWIERDZENIE 181. Przyjmijmy notację Def. 67, 11, 21, 23, 32, 35, 61, 63, 64, 65, 68, 75, 77, 78, 79 i 130, Cor. 14 oraz Stw. 75. Niechaj przestrzeń wektorowa V nad ciałem $\mathbb{K}$ będzie (wewnętrzną) sumą prostą rodziny $\{V^{(\lambda)}\}_{\lambda \in \Lambda}$ swoich podprzestrzeni $V^{(\lambda)} \subset V$ jak w Równ. (9.7) i niech χ będzie endomorfizmem V . Rozkład (9.7) jest χ -niezmienniczy wtedy i tylko wtedy, gdy obraz $\mathcal{M}(\chi)$ endomorfizmu χ względem monomorfizmu $\mathcal{M}$ zdefiniowanego w Cor. 14 leży w obrazie diagonalnego zanurzenia grupy $\prod_{\lambda \in \Lambda} \text{End}_{\mathbb{K}}(V^{(\lambda)})$ w grupie $\prod_{\lambda, \mu \in \Lambda} \text{Hom}_{\mathbb{K}}(V^{(\lambda)}, V^{(\mu)})$, czyli jest postaci⁶

$$\mathcal{M}(\chi) : \Lambda^{\times 2} \longrightarrow \bigcup_{\lambda, \mu \in \Lambda} \text{Hom}_{\mathbb{K}}(V^{(\lambda)}, V^{(\mu)}) : (\lambda, \mu) \longmapsto \delta_{\lambda, \mu}^{\mathbb{K}} \triangleright \text{pr}_\lambda \circ \chi \circ j_\lambda.$$

■

Dowód:

⁶Należy pamiętać, że wobec utożsamienia między przestrzenią wektorową i sumą prostą jej podprzestrzeni opisanego w Def. 79 przeciwdziałaniem każdego z odwzorowań j_λ jest przestrzeń V .

$\Rightarrow$ Zachowywanie przez χ rozkładu V na sumę prostą podprzestrzeni $V^{(\lambda)}$ implikuje w świetle Stw. 180 relacje $\chi \circ j_\lambda \circ \text{pr}_\lambda = j_\lambda \circ \text{pr}_\lambda \circ \chi$, które w połączeniu z Równ. (8.8) prowadzą do oczekiwanej tożsamości

$$\begin{aligned} \mathcal{M}(\chi)(\lambda, \mu) &\equiv \text{pr}_\lambda \circ \chi \circ j_\mu \equiv \text{pr}_\lambda \circ \chi \circ \pi_\mu \circ j_\mu = \text{pr}_\lambda \circ \pi_\mu \circ \chi \circ j_\mu \\ &\equiv \text{pr}_\lambda \circ (j_\mu \circ \text{pr}_\mu) \circ \chi \circ j_\mu = \delta_{\lambda, \mu}^{\mathbb{K}} \triangleright \text{id}_{V^{(\mu)}} \circ \text{pr}_\mu \circ \chi \circ j_\mu \\ &\equiv \delta_{\lambda, \mu}^{\mathbb{K}} \triangleright \text{pr}_\mu \circ \chi \circ j_\mu. \end{aligned}$$

$\Leftarrow$ Lewostronną odwrotnością monomorfizmu $\mathcal{M}$ jest odwzorowanie $\mathcal{H} : \text{Im } \mathcal{M} \rightarrow \text{End}_{\mathbb{K}}(\bigoplus_{\lambda \in \Lambda} V^{(\lambda)})$ przyporządkowujące elementowi $\psi \in \text{Im } \mathcal{M} \subset \prod_{\lambda, \mu \in \Lambda} \text{Hom}_{\mathbb{K}}(V^{(\lambda)}, V^{(\mu)})$ endomorfizm

$$\mathcal{H}(\psi) : V \curvearrowright : v \mapsto \sum_{\lambda, \mu \in \Lambda} j_\lambda \circ \psi(\lambda, \mu) \circ \text{pr}_\mu(v).$$

Stwierdzamy zatem, co następuje:

$$\begin{aligned} \chi(V^{(\lambda)}) &= \sum_{\mu, \nu \in \Lambda} j_\mu \circ \mathcal{M}(\chi)(\mu, \nu) \circ \text{pr}_\nu(V^{(\lambda)}) \\ &\equiv \sum_{\mu, \nu \in \Lambda} \delta_{\mu, \nu}^{\mathbb{K}} \triangleright j_\mu \circ \mathcal{M}(\chi)(\mu, \mu) \circ \text{pr}_\nu(V^{(\lambda)}) \\ &= \sum_{\mu \in \Lambda} j_\mu \circ \mathcal{M}(\chi)(\mu, \mu) \circ \text{pr}_\mu(V^{(\lambda)}) \\ &\equiv j_\lambda \circ \mathcal{M}(\chi)(\lambda, \lambda)(V^{(\lambda)}) \equiv j_\lambda \circ \text{pr}_\lambda \circ \chi \circ j_\lambda(V^{(\lambda)}) \\ &\equiv \pi_\lambda \circ \chi \circ j_\lambda(V^{(\lambda)}) \subset \text{Im } \pi_\lambda = V^{(\lambda)}. \end{aligned}$$

□

Warto zwrócić uwagę, że w przypadku skończenia wymiarowym powyższe stwierdzenie orzeka, że macierz endomorfizmu χ w bazie będącej konkatenacją baz podprzestrzeni $V^{(\lambda)}$ ma postać blokowo diagonalną, przy czym poszczególne bloki stanowią macierzowe realizacje endomorfizmów $\chi|_{V^{(\lambda)}} \in \text{End}_{\mathbb{K}}(V^{(\lambda)})$.

Zasadniczym celem niniejszego rozdziału jest konkretyzacja abstrakcyjnych konstrukcji opisanych w powyższym wprowadzeniu w odwołaniu do wcześniejszych naszych rozważań dotyczących widma endomorfizmu. Punktem wyjścia jest tutaj identyfikacja stosownych podprzestrzeni niezmienniczych względem endomorfizmu. Temu służy

DEFINICJA 131. Przyjmijmy notację Def. 67, 11, 21, 23, 24, 32, 35, 61, 63, 64, 65, 124 i 126 oraz Stw. 65 i 171. Niechaj V będzie przestrzenią wektorową nad ciałem $\mathbb{K}$ i niech χ będzie endomorfizmem V . Ustalmy liczbę $k \in \mathbb{N}$ i określmy endomorfizm

$$\chi_\lambda^k := \underbrace{(\chi - \ell_\lambda) \circ (\chi - \ell_\lambda) \circ \cdots \circ (\chi - \ell_\lambda)}_{k \text{ razy}},$$

przy czym stosujemy konwencję $\chi_\lambda^0 \equiv \text{id}_V$. **Uogólniona przestrzeń własna stopnia k endomorfizmu χ** (odpowiadająca wartości własnej $\lambda \in \text{Sp } \chi$) to podprzestrzeń

$$V_k(\lambda; \chi) := \text{Ker } \chi_\lambda^k \subset V.$$

Przestrzeń pierwiastkowa endomorfizmu χ (odpowiadająca wartości własnej $\lambda \in \text{Sp } \chi$) to natomiast

$$V(\lambda; \chi) := \bigcup_{k=1}^{\infty} V_k(\lambda; \chi) \subset V.$$

▲

Mamy oczywiście

STWIERDZENIE 182. *Przyjmijmy notację Def. 67, 11, 21, 23, 24, 32, 35, 61, 63, 64, 65, 72, 73, 124, 126 i 131 oraz Stw. 65 i 171. Uogólnione przestrzenie pierwiastkowe pozostają w relacjach*

$$\forall_{k \in \mathbb{N}} : V_k(\lambda; \chi) \subset V_{k+1}(\lambda; \chi).$$

W szczególności więc przestrzeń pierwiastkowa $V(\lambda; \chi)$ jest podprzestrzenią wektorową V . Przy tym jeśli $\dim_{\mathbb{K}} V < \infty$, to

$$\exists_{N \in \mathbb{N}} \forall_{k > N} : V_k(\lambda; \chi) = V_N(\lambda; \chi) \equiv V(\lambda; \chi).$$

*Najmniejszą liczbę naturalną spełniającą powyższy warunek nazwiemy **wysokością przestrzeni pierwiastkowej** $V(\lambda; \chi)$ i będziemy oznaczać jako*

$$h(\lambda; \chi) := \min \{ N \in \mathbb{N}^{\times} \mid V_N(\lambda; \chi) = V(\lambda; \chi) \}.$$

Zarówno uogólnione przestrzenie własne, jak i przestrzenie pierwiastkowe endomorfizmu χ są przestrzeniami χ -niezmienniczymi.

■

Zwieńczenie dotychczasowej dyskusji, wypuklające rolę uogólnionych przestrzeni własnych w strukturalnym opisie (dziedziny) endomorfizmu przynosi poniższe

STWIERDZENIE 183. *Przyjmijmy notację Def. 67, 11, 21, 23, 24, 32, 35, 61, 63, 64, 65, 68, 75, 77, 78, 79, 124, 126 i 131 oraz Stw. 65 i 171. Niechaj χ będzie endomorfizmem przestrzeni wektorowej V nad ciałem $\mathbb{K}$. Dowolny wielomian*

$$w \in \text{Ker } \rho_{\chi} \subset \mathbb{K}[t]$$

o rozkładzie

$$w := (t - \lambda_1)^{k_1} \square (t - \lambda_2)^{k_2} \square \dots \square (t - \lambda_r)^{k_r},$$

określonym przez liczby $r \in \mathbb{N}$ i $k_i \in \mathbb{N}$, $i \in \overline{1, r}$ oraz parami różne skalary λ_i , $i \in \overline{1, r}$, wyznacza rozkład dziedziny endomorfizmu na (wewnętrzną) sumę prostą podprzestrzeni χ -niezmienniczych

$$V = \bigoplus_{i=1}^r \text{Ker } \chi_{\lambda_i}^{k_i},$$

przy czym zachodzi

$$\forall_{i \in \overline{1, r}} : \begin{cases} \text{Ker } \chi_{\lambda_i}^{k_i} = V(\lambda_i; \chi), & \text{gdy } \lambda_i \in \text{Sp } \chi \\ \text{Ker } \chi_{\lambda_i}^{k_i} = \{0_V\}, & \text{gdy } \lambda_i \notin \text{Sp } \chi \end{cases}.$$

■

Dowód: Pokażemy najpierw, że

$$\forall_{i \in \overline{1, r}} \forall_{n \geq k_i} : \text{Ker } \chi_{\lambda_i}^n = \text{Ker } \chi_{\lambda_i}^{k_i}.$$

Zachodzi oczywiście inkluzja $\text{Ker } \chi_{\lambda_i}^{k_i} \subset \text{Ker } \chi_{\lambda_i}^n$, wystarczy zatem sprawdzić inkluzję odwrotną. Uczynimy to dla $n := k_i + 1$, a wniosek końcowy wywiedziemy na podstawie indukcji względem n . Załóżmy, przeciwnie, że istnieje wektor $v \in \text{Ker } \chi_{\lambda_i}^{k_i+1}$ o własności $v_i := \chi_{\lambda_i}^{k_i}(v) \neq 0_V$. Zauważmy, że v_i jest wówczas wektorem własnym χ odpowiadającym wartości własnej λ_i , oto bowiem

$$\chi(v_i) - \lambda_i \triangleright v_i \equiv \chi_{\lambda_i}(v_i) \equiv \chi_{\lambda_i}^{k_i+1}(v) = 0_V.$$

Wtedy jednak

$$\rho_\chi(w)(v) = \circ_{j=1, j \neq i}^r \chi_{\lambda_j}^{k_j} \circ \chi_{\lambda_i}^{k_i}(v) \equiv \circ_{j=1, j \neq i}^r \chi_{\lambda_j}^{k_j}(v_i) = \prod_{j=1, j \neq i}^r (\lambda_i - \lambda_j)^{k_j}(v_i) \neq 0_V,$$

co przeczy założeniu $w \in \text{Ker } \rho_\chi$. Widzimy zatem, że koniecznie $\text{Ker } \chi_{\lambda_i}^n = \text{Ker } \chi_{\lambda_i}^{k_i}$. W przypadku $\lambda_i \in \text{Sp } \chi$ oznacza to wprost, że $\text{Ker } \chi_{\lambda_i}^{k_i}$ jest odnośną przestrzenią pierwiastkową χ . Jeżeli natomiast $\lambda_i \notin \text{Sp } \chi$, to dla dowolnego $v \in \text{Ker } \chi_{\lambda_i}^{k_i}$ musi zachodzić

$$v_{k_i} := \chi_{\lambda_i}^{k_i-1}(v) = 0_V,$$

w przeciwnym bowiem razie byłoby

$$\chi(v_{k_i}) = \chi_{\lambda_i}(v_{k_i}) +_V \lambda_i \triangleright v_{k_i} \equiv \chi_{\lambda_i}^{k_i}(v) +_V \lambda_i \triangleright v_{k_i} = \lambda_i \triangleright v_{k_i},$$

czyli $\lambda_i \in \text{Sp } \chi$, w sprzeczności z założeniem. Jest więc

$$\chi_{\lambda_i}(\chi_{\lambda_i}^{k_i-2}(v)) = 0_V$$

i znów stwierdzamy, że wobec $\lambda_i \notin \text{Sp } \chi$ koniecznie

$$v_{k_i-1} := \chi_{\lambda_i}^{k_i-2}(v) = 0_V.$$

Tym sposobem dowodzimy ostatecznie pożądaną równość $v = 0_V$.

Dowodzimy następnie, że V istotnie rozkłada się na sumę prostą przestrzeni $\text{Ker } \chi_{\lambda_i}^{k_i}$. W tym celu rozważmy wielomiany

$$w_i := \boxplus_{j=1, j \neq i}^r (t - \lambda_j)^{k_j}.$$

Jako że skalary λ_i są parami różne, a wszystkie wielomiany są tego samego stopnia $r-1$, te ostatnie są względnie pierwsze, a zatem – na mocy Stw. 22 – istnieje rodzina wielomianów $\{q_i\}_{i \in \overline{1, r}} \subset \mathbb{K}[t]$ spełniająca warunek

$$q_1 \boxplus w_1 \boxplus q_2 \boxplus w_2 \boxplus \cdots \boxplus q_r \boxplus w_r = t^0 \in \text{NWD}(w_1, w_2, \dots, w_r).$$

Zdefiniujmy, dla dowolnego $i \in \overline{1, r}$,

$$p_i := q_i \boxplus w_i \in \mathbb{K}[t]$$

oraz

$$P_i := \rho_\chi(p_i) \in \text{End}_{\mathbb{K}}(V),$$

a wtedy

$$\sum_{i=1}^r P_i \equiv \sum_{i=1}^r \rho_\chi(p_i) = \rho_\chi(q_1 \boxplus w_1 \boxplus q_2 \boxplus w_2 \boxplus \cdots \boxplus q_r \boxplus w_r) = \rho_\chi(t^0) = \text{id}_V.$$

Ponadto ilekroć $i \neq j$, otrzymujemy

$$\begin{aligned} P_i \circ P_j &= \rho_\chi(q_i \boxplus q_j) \circ \prod_{\substack{m=1 \\ m \neq i}}^r \chi_{\lambda_m}^{k_m} \circ \prod_{\substack{n=1 \\ n \neq j}}^r \chi_{\lambda_n}^{k_n} = \rho_\chi(q_i \boxplus q_j \boxplus \prod_{\substack{m=1 \\ m \notin \{i,j\}}}^r \chi_{\lambda_m}^{k_m}) \circ \prod_{n=1}^r \chi_{\lambda_n}^{k_n} \\ &\equiv \rho_\chi(q_i \boxplus q_j \boxplus \prod_{\substack{m=1 \\ m \notin \{i,j\}}}^r \chi_{\lambda_m}^{k_m}) \circ \rho_\chi(w) = 0, \end{aligned}$$

a zatem także

$$P_i \circ P_i = P_i \circ (\text{id}_V - \sum_{\substack{j=1 \\ j \neq i}}^r P_j) = P_i - \sum_{\substack{j=1 \\ j \neq i}}^r P_i \circ P_j = P_i.$$

Endomorfizmy P_i tworzą więc zupełną rodzinę rzutów komplementarnych, która na mocy Stw. 88 zadaje rozkład dziedziny χ na (wewnętrzzną) sumę prostą

$$V = \bigoplus_{i=1}^r \text{Im } P_i.$$

Pozostaje upewnić się, że $\text{Im } P_i = \text{Ker } \chi_{\lambda_i}^{k_i}$. Po pierwsze obliczamy

$$\chi_{\lambda_i}^{k_i} \circ P_i = \rho_\chi(q_i) \circ \chi_{\lambda_i}^{k_i} \circ \prod_{\substack{j=1 \\ j \neq i}}^r \chi_{\lambda_j}^{k_j} = \rho_\chi(q_i) \circ \prod_{j=1}^r \chi_{\lambda_j}^{k_j} \equiv \rho_\chi(q_i) \circ \rho_\chi(w) = 0,$$

skąd wniosek, że

$$\text{Im } P_i \subset \text{Ker } \chi_{\lambda_i}^{k_i}.$$

Niech teraz $v \in \text{Ker } \chi_{\lambda_i}^{k_i}$, a wtedy dla dowolnego $j \neq i$ otrzymujemy

$$P_j(v) = \rho_\chi(q_j) \circ \prod_{\substack{m=1 \\ m \neq j}}^r \chi_{\lambda_m}^{k_m}(v) \equiv \rho_\chi(q_j) \circ \prod_{\substack{m=1 \\ m \notin \{i,j\}}}^r \chi_{\lambda_m}^{k_m} \circ \chi_{\lambda_i}^{k_i}(v) = 0_V,$$

czyli też

$$v \equiv \text{id}_V(v) = \sum_{j=1}^r P_j(v) = P_i(v),$$

co daje nam brakującą relację

$$\text{Ker } \chi_{\lambda_i}^{k_i} \subset \text{Im } P_i.$$

□

Godzi się w tym momencie odnotować, że konstrukcja rzutów na przestrzenie pierwiastkowe endomorfizmu wydatnie się upraszcza, gdy jego wielomian charakterystyczny rozkłada się na czynniki stopnia 1 i wyznaczone tą drogą widmo okazuje się niezwyrodniałe. Możemy wtedy zastosować

STWIERDZENIE 184. *Przyjmijmy notację Def. 67, 11, 21, 23, 24, 25, 32, 35, 61, 63, 64, 65, 68, 70, 72, 73, 75, 77, 82, 87, 92, 124, 126, 127 i 131, Stw. 65 i 171 oraz Przykł. 34 (2), 40 (3) i 41. Niechaj χ będzie endomorfizmem przestrzeni wektorowej V wymiaru $N := \dim_{\mathbb{K}} V < \infty$ nad ciałem $\mathbb{K}$, o widmie $\text{Sp } \chi := \{\lambda_i\}_{i \in \overline{1, N}}$, przy czym $\lambda_i \in \mathbb{K}$ są parami różnymi wartościami własnymi χ . Jeśli wielomian charakterystyczny χ jest postaci*

$$w_\chi = (t - \lambda_1) \square (t - \lambda_2) \square \cdots \square (t - \lambda_N),$$

to rzuty P_i , $i \in \overline{1, N}$ na podprzestrzenie pierwiastkowe $V(\lambda_i; \chi) \equiv V_1(\lambda_i; \chi) \equiv \text{Im } P_i$, występujące w rozkładzie

$$V = \bigoplus_{i=1}^N V(\lambda_i; \chi),$$

wyrażają się wzorami

$$P_i = \ell_{\Lambda_i} \circ \circ_{\substack{j=1 \\ j \neq i}}^N \chi_{\lambda_j}, \quad \Lambda_i := \prod_{\substack{j=1 \\ j \neq i}}^N (\lambda_i - \lambda_j)^{-1}.$$

■

Dowód: Zdefiniujmy wielomiany

$$\tilde{w}_i := F_{w_i}(\lambda_i)^{-1} \cdot w_i, \quad w_i := \square_{\substack{j=1 \\ j \neq i}}^N (t - \lambda_j) \in \mathbb{K}_{N-1}[t], \quad i \in \overline{1, N}$$

których obrazy względem ρ_χ przyjmują znaną postać

$$\rho_\chi(\tilde{w}_i) = P_i.$$

Ich suma

$$J := \sum_{i=1}^N \tilde{w}_i$$

spełnia warunki

$$\forall_{i \in \overline{1, N}} : F_J(\lambda_i) = \sum_{j=1}^N F_{w_j}(\lambda_j)^{-1} \cdot {}_{\mathbb{K}} F_{w_j}(\lambda_i) = F_{w_i}(\lambda_i)^{-1} \cdot {}_{\mathbb{K}} F_{w_i}(\lambda_i) = 1_{\mathbb{K}} = F_{t^0}(\lambda_i).$$

Rozumując jak w dowodzie Stw. 178, w szczególności zaś przywołując Lem. 9.9, konstatujemy, że istnieje dokładnie jeden wielomian stopnia co najwyżej $N-1$, którego funkcja wielomianowa przyjmuje ustalone wartości (jednostkowe) w $\dim_{\mathbb{K}} \mathbb{K}_{N-1}[t] = N$ punktach λ_i swej dziedziny. To jednak wobec powyższego implikuje tożsamość

$$J \equiv t^0,$$

z której odczytujemy

$$\sum_{i=1}^N P_i = \sum_{i=1}^N \rho_\chi(\tilde{w}_i) = \rho_\chi(J) \equiv \rho_\chi(t^0) = \text{id}_V.$$

W połączeniu z wynikiem, wypisanym dla $j \neq i$,

$$P_i \circ P_j = \ell_{\Lambda_i \cdot {}_{\mathbb{K}} \Lambda_j} \circ \circ_{\substack{m=1 \\ m \notin \{i, j\}}}^N \chi_{\lambda_m} \circ \rho_\chi(w_\chi) = 0,$$

pozwała ona udowodnić brakującą tożsamość

$$P_i \circ P_i = P_i$$

i tym samym zakończyć dowód. $\square$

Na zakończenie tej części wykładu omówimy dwa elementarne wnioski płynące ze Stw. 182 i 183. Pierwszy z nich stanowi prostą parafrazę tego ostatniego w kontekście algebraicznym o pierwszorzędnym znaczeniu praktycznym.

TWIERDZENIE 9.10 (O rozkładzie przestrzeni wektorowej na przestrzenie pierwiastkowe endomorfizmu). *Przyjmijmy notację Def. 67, 11, 14, 21, 23, 24, 26, 25, 32, 35, 61, 63, 64, 65, 68, 70, 72, 73, 75, 77, 78, 79, 82, 87, 92, 124, 126, 131 i 127, Stw. 65 i 171 oraz Przykł. 34 (2), 40 (3) i 41. Jeśli wielomian minimalny endomorfizmu χ przestrzeni wektorowej V skończonego wymiaru nad ciałem $\mathbb{K}$ ma rozkład na czynniki stopnia 1 w $\mathbb{K}[t]$, to V ma rozkład*

$$V = \bigoplus_{\lambda \in \text{Sp } \chi} V(\lambda; \chi).$$

W szczególności dowolny endomorfizm przestrzeni wektorowej V nad $\mathbb{K} := \mathbb{C}$ zadaje taki jej rozkład. $\blacksquare$

Dowód: Teza wynika wprost ze Stw. 183, jeśli wybrać $w := w_\chi$. $\square$

Drugi dotyczy jawnej postaci wielomianu minimalnego.

STWIERDZENIE 185. *Przyjmijmy notację Def. 67, 11, 21, 23, 24, 25, 32, 35, 36, 61, 63, 64, 65, 72, 73, 124, 126 i 131 oraz Stw. 65, 171, 176 i 182. Niechaj χ będzie endomorfizmem przestrzeni wektorowej V skończonego wymiaru nad ciałem algebraicznie domkniętym $\mathbb{K}$ i niech $h(\lambda; \chi)$ będzie wysokością przestrzeni pierwiastkowej $V(\lambda; \chi)$ odpowiadającej wartości własnej $\lambda \in \text{Sp } \chi$. Wielomian minimalny χ przyjmuje wówczas postać*

$$p_\chi = \prod_{\lambda \in \text{Sp } \chi} (t - \lambda)^{h(\lambda; \chi)}.$$

Dowód: Zaczniemy od stwierdzenia, że każdy wielomian $z \in \text{Ker } \rho_\chi \subset \mathbb{K}[t]$ ma rozkład na czynniki stopnia 1 z racji algebraicznej domkniętości $\mathbb{K}$. Jak wskazuje Stw. 183 w połączeniu z definicją wysokości przestrzeni pierwiastkowej, krotność zera $\lambda \in \text{Sp } \chi$ dowolnego wielomianu $z \in \text{Ker } \rho_\chi \subset \mathbb{K}[t]$ jest nie mniejsza niż $h(\lambda; \chi)$, wystarczy zatem sprawdzić, że wielomian zdefiniowany w tezie dowodzonego stwierdzenia istotnie należy do $\text{Ker } \rho_\chi \subset \mathbb{K}[t]$. Na mocy Tw. 9.10 przestrzeń V rozszczepia się na sumę prostą przestrzeni pierwiastkowych χ , nasze zadanie sprowadza się więc do wykazania, że obraz rzeczonego wielomianu względem ρ_χ jest zerem na każdej przestrzeni pierwiastkowej. To jednak wynika wprost z relacji $(t - \lambda)^{h(\lambda; \chi)} \mid \prod_{\mu \in \text{Sp } \chi} (t - \mu)^{h(\mu; \chi)}$, słusznej dla dowolnej wartości własnej $\lambda \in \text{Sp } \chi$, oraz z ciągu tożsamości $V(\lambda; \chi) \equiv V_{h(\lambda; \chi)}(\lambda; \chi) \equiv \text{Ker } \chi_\lambda^{h(\lambda; \chi)} \equiv \text{Ker } \rho_\chi((t - \lambda)^{h(\lambda; \chi)})$. $\square$

Jak zaznaczyliśmy na początku niniejszego rozdziału, rozkład dziedziny endomorfizmu χ na sumę prostą podprzestrzeni χ -niezmienniczych pozwala zrealizować χ jako produkt kartezjański endomorfizmów poszczególnych podprzestrzeni.

W dalszej części wykładu zastanowimy się nad swobodą wyboru bazy w każdej z przestrzeni pierwiastkowych χ , który pozwoliłby zapisać macierz χ w szczególnie prostej postaci, określonej jednoznacznie przez widmo χ (wraz z informacją o zwyrodnieniu poszczególnych jego elementów). Konstrukcyjny dowód istnienia takiej bazy stanowi centralny wynik następnego rozdziału.

9.7. Jordanowska postać normalna endomorfizmu

Istnienie w przestrzeni wektorowej bazy własnej ustalonego jej endomorfizmu to okoliczność tyleż wygodna (z praktycznego punktu widzenia, jaki często podpowiada nam fizyka) co wyjątkowa. Z drugiej strony elementarne rozważania fizyczne z rzadka tylko wyprowadzają nas poza dziedzinę zespoloną, nie wydaje się przeto nazbyt uciążliwym ograniczenie dalszej naszej dyskusji do przypadku ciała algebraicznie domkniętego. Zabieg ten nie tylko pozwala udzielić całkowicie ogólnej odpowiedzi na pytanie o postać kanoniczną endomorfizmu przestrzeni wektorowej nad dowolnym takim ciałem, ale też – w szczególności – otwiera przed nami możliwość wyjaśnienia struktury endomorfizmu rzeczywistej przestrzeni wektorowej na gruncie szczególnej relacji między przestrzeniami rzeczywistymi i zespolonymi, która nosi miano kompleksyfikacji. Niniejszy rozdział jest poświęcony przekonującemu udokumentowaniu powyższych stwierdzeń ogólnych.

Zacznijmy, jak zwykle, od wprowadzenia pojęć pomocniczych.

DEFINICJA 132. Przyjmijmy notację Def. 67, 11, 14, 16, 32, 77 i 82, Stw. 2, 95 i 96 oraz Przykł. 41. Niechaj $\lambda \in \mathbb{K}$ będzie dowolnym elementem ciała $\mathbb{K}$. **Kłatką Jordana wymiaru $N \in \mathbb{N}$ stowarzyszoną z $\lambda \in \mathbb{K}$** nazwiemy macierz

$$\mathcal{J}(\lambda, \varepsilon; N) := \begin{pmatrix} \lambda & \varepsilon_1 & 0_{\mathbb{K}} & 0_{\mathbb{K}} & \cdots & \cdots & 0_{\mathbb{K}} \\ 0_{\mathbb{K}} & \lambda & \varepsilon_2 & 0_{\mathbb{K}} & 0_{\mathbb{K}} & \cdots & 0_{\mathbb{K}} \\ 0_{\mathbb{K}} & 0_{\mathbb{K}} & \lambda & \varepsilon_3 & \ddots & \ddots & \vdots \\ \vdots & 0_{\mathbb{K}} & \ddots & \ddots & \ddots & \ddots & 0_{\mathbb{K}} \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & 0_{\mathbb{K}} \\ \vdots & \vdots & & \ddots & \ddots & \ddots & \varepsilon_{N-1} \\ 0_{\mathbb{K}} & 0_{\mathbb{K}} & \cdots & \cdots & 0_{\mathbb{K}} & 0_{\mathbb{K}} & \lambda \end{pmatrix} \in \text{Mat}(\mathbb{K}; N)$$

z dowolnym $\varepsilon := (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{N-1}) \in \{0_{\mathbb{K}}, 1_{\mathbb{K}}\}^{\times(N-1)}$. **Rzeczywista klatka Jordana wymiaru N (stowarzyszona z λ)** to macierz $\mathcal{J}_{\mathbb{R}}(\lambda, \varepsilon; N) \in \text{Mat}(\mathbb{R}; N)$ określona dla dowolnej liczby $\lambda \in \mathbb{C}$, jak następuje: jeśli $\lambda \in \iota(\mathbb{R})$, to

$$\mathcal{J}_{\mathbb{R}}(\lambda, \varepsilon; N) \equiv \mathcal{J}(\lambda, \varepsilon; N),$$

jeśli natomiast $\lambda \in \mathbb{C} \setminus \iota(\mathbb{R})$, to

$$\mathcal{J}_{\mathbb{R}}(\lambda, \varepsilon; N) := \begin{pmatrix} C_2(\lambda) & \varepsilon_1 \triangleright_{(2)} \mathbf{1}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \cdots & \cdots & \mathbf{0}_2 \\ \mathbf{0}_2 & C_2(\lambda) & \varepsilon_2 \triangleright_{(2)} \mathbf{1}_2 & \mathbf{0}_2 & \mathbf{0}_2 & \cdots & \mathbf{0}_2 \\ \mathbf{0}_2 & \mathbf{0}_2 & C_2(\lambda) & \varepsilon_3 \triangleright_{(2)} \mathbf{1}_2 & \ddots & \ddots & \vdots \\ \vdots & \mathbf{0}_2 & \ddots & \ddots & \ddots & \ddots & \mathbf{0}_2 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \mathbf{0}_2 \\ \vdots & \vdots & & \ddots & \ddots & \ddots & \varepsilon_{\frac{N}{2}-1} \triangleright_{(2)} \mathbf{1}_2 \\ \mathbf{0}_2 & \mathbf{0}_2 & \cdots & \cdots & \mathbf{0}_2 & \mathbf{0}_2 & C_2(\lambda) \end{pmatrix},$$

gdzie

$$C_2(\lambda) := \begin{pmatrix} \Re(\lambda) & \Im(\lambda) \\ -\Im(\lambda) & \Re(\lambda) \end{pmatrix}, \quad \varepsilon := (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{N-1}) \in \{0_{\mathbb{K}}, 1_{\mathbb{K}}\}^{\times(\frac{N}{2}-1)},$$

przy czym w tym ostatnim przypadku zakładamy, że $N \in 2\mathbb{N}$. ▲

Będziemy również potrzebować

DEFINICJA 133. Przyjmijmy notację Def. 67, 32, 77 i 82, Stw. 95 oraz Przykł. 41 i niech G będzie grupą. **Suma prosta macierzy** $M_\alpha \in \text{Mat}(G; N_\alpha)$, $N_\alpha \in \mathbb{N}$, $\alpha \in \{1, 2\}$ to macierz

$$M_1 \oplus M_2 := \begin{pmatrix} M_1 & \mathbf{0}_{N_1 \times N_2} \\ \mathbf{0}_{N_2 \times N_1} & M_2 \end{pmatrix} \in \text{Mat}(G; N_1 + N_2).$$
▲

Na koniec wprowadzamy

DEFINICJA 134. Przyjmijmy notację Def. 67, 11, 21, 23, 24, 32, 35, 61, 63, 64, 65, 77, 82, 124, 126, 131, 132 i 133, Stw. 95, 65 i 171 oraz Przykł. 41. Niechaj V będzie przestrzenią wektorową nad ciałem $\mathbb{K}$, niech χ będzie endomorfizmem V i niech $\lambda \in \mathbb{K}$ będzie dowolnym elementem ciała $\mathbb{K}$. **χ -seria stowarzyszona z $\lambda \in \mathbb{K}$** to rodzina wektorów $\{v^n\}_{n \in \overline{0, N-1}}$, $N \in \mathbb{N}$ z V określonych wzorami

$$v^n := \chi_\lambda^n(v^0),$$

zapisanymi w konwencji $\chi_\lambda^0 \equiv \text{id}_V$, i spełniających dodatkowy warunek

$$\chi_\lambda(v^{N-1}) = 0_V.$$
▲

Możemy już teraz wysłowić fundamentalne

TWIERDZENIE 9.11 (O jordanowskiej postaci normalnej endomorfizmu). *Przyjmijmy notację Def. 67, 11, 21, 23, 24, 32, 35, 61, 63, 64, 65, 68, 70, 72, 73, 75, 77, 78, 82, 124, 126, 131, 132, 133 i 134, Tw. 8.11, Stw. 75, 95, 96, 97, 98, 99, 65 i 171, Cor. 14 oraz Przykł. 41. Niechaj V będzie przestrzenią wektorową wymiaru $\dim_{\mathbb{K}} V =: N < \infty$ nad ciałem $\mathbb{K}$ i niech χ będzie endomorfizmem V o widmie $\text{Sp } \chi := \{\lambda_i\}_{i \in \overline{1, r}}$, $r \in \mathbb{N}$, przy czym zakładamy, że skalary λ_i są parami różne. Jeśli wielomian minimalny χ jest rozkładalny w $\mathbb{K}[t]$ na czynniki stopnia 1, to istnieje baza $\mathcal{B}_J$ przestrzeni V będąca konkatencją baz przestrzeni pierwiastkowych $V(\lambda_i; \chi)$ złożonych z χ -serii (stowarzyszonych z odpowiednimi wartościami własnymi λ_i), względem której macierz endomorfizmu przyjmuje postać blokowo diagonalną*

$$[\chi]_{\mathcal{B}_J}^{\mathcal{B}_J} = \bigoplus_{i=1}^r \mathcal{J}(\lambda_i, \varepsilon_i; \dim_{\mathbb{K}} V(\lambda_i; \chi))$$

dla pewnych $\varepsilon_i \in \{0_{\mathbb{K}}, 1_{\mathbb{K}}\}^{\times (\dim_{\mathbb{K}} V(\lambda_i; \chi) - 1)}$. Baza ta nosi miano **bazy jordanowskiej endomorfizmu χ** . ■

Dowód: Przedstawimy wyjątkowo prosty i przejrzysty dowód konstrukcyjny pochodzący od Väliaho [Väl186]. Ustalmy (dowolnie) $\lambda \in \text{Sp } \chi$ i rozważmy nierosnący ciąg podprzestrzeni $\text{Im } \chi_\lambda^n$, $n \in \mathbb{N}$,

$$V \equiv \text{Im } \chi_\lambda^0 \supset \text{Im } \chi_\lambda^1 \supset \text{Im } \chi_\lambda^2 \supset \cdots \supset \text{Im } \chi_\lambda^n \supset \cdots.$$

Jak wynika wprost z jego konstrukcji, ciąg ten jest stały począwszy od pewnego indeksu $N \in \mathbb{N}$, czyli

$$(9.8) \quad \exists_{N \in \mathbb{N}} \forall_{n > N} : \operatorname{Im} \chi_\lambda^n = \operatorname{Im} \chi_\lambda^N \not\subseteq \operatorname{Im} \chi_\lambda^{N-1}.$$

Skoro zaś $\chi_\lambda(\operatorname{Im} \chi_\lambda^N) = \operatorname{Im} \chi_\lambda^N$, to

$$(9.9) \quad \operatorname{Im} \chi_\lambda^N \cap \operatorname{Ker} \chi_\lambda = \{0_V\},$$

gdy tymczasem

$$\operatorname{Im} \chi_\lambda^{N-1} \cap \operatorname{Ker} \chi_\lambda \neq \{0_V\}.$$

Zdefiniujmy podprzestrzenie

$$S_\lambda^m := \operatorname{Im} \chi_\lambda^{m-1} \cap \operatorname{Ker} \chi_\lambda, \quad m \in \mathbb{N}^\times$$

i oznaczmy

$$d_m^0 := \dim_{\mathbb{K}} S_\lambda^m.$$

Przestrzenie S_λ^m spełniają oczywistą relację

$$\operatorname{Ker} \chi_\lambda \equiv S_\lambda^1 \supset S_\lambda^2 \supset \dots \supset S_\lambda^N \neq \{0_V\},$$

a ponadto

$$\forall_{k \in \mathbb{N}^\times} : S_\lambda^{N+k} = \{0_V\}.$$

Wyberzmy w S_λ^N dowolną bazę $\mathcal{B}^1 := \{v_{i_1}^{(1|1)}\}_{i_1 \in \overline{1, d_N^0}}$. Jako że $v_{i_1}^{(1|1)} \in \operatorname{Im} \chi_\lambda^{N-1}$,

$$\forall_{i_1 \in \overline{1, d_N^0}} \exists_{v_{i_1}^{(1|N)} \in V} : v_{i_1}^{(1|1)} = \chi_\lambda^{N-1}(v_{i_1}^{(1|N)}).$$

Określmy, dla dowolnego $i_1 \in \overline{1, d_N^0}$, wektory

$$v_{i_1}^{(1|j_1)} := \chi_\lambda^{N-j_1}(v_{i_1}^{(1|N)}), \quad j_1 \in \overline{1, N}.$$

Następnie uzupełnijmy (znów *dowolnie*) zbiór $\mathcal{B}^1 \subset S_\lambda^N$ do bazy przestrzeni $S_\lambda^{N-1} \supset S_\lambda^N$, oznaczając zbiór dodatkowych wektorów jako $\mathcal{B}^2 := \{v_{i_2}^{(2|1)}\}_{i_2 \in \overline{1, d_N^1}}$, gdzie $d_N^1 := d_{N-1}^0 - d_N^0$. Tym razem $v_{i_2}^{(2|1)} \in \operatorname{Im} \chi_\lambda^{N-2}$, zatem

$$\forall_{i_2 \in \overline{1, d_N^1}} \exists_{v_{i_2}^{(2|N-1)} \in V} : v_{i_2}^{(2|1)} = \chi_\lambda^{N-2}(v_{i_2}^{(2|N-1)}).$$

Określmy teraz, dla dowolnego $i_2 \in \overline{1, d_N^1}$, wektory

$$v_{i_2}^{(2|j_2)} := \chi_\lambda^{N-1-j_2}(v_{i_2}^{(2|N-1)}), \quad j_2 \in \overline{1, N-1}.$$

W następnej kolejności uzupełniamy (wciąż *dowolnie*) zbiór $\mathcal{B}^1 \cup \mathcal{B}^2 \subset S_\lambda^{N-1}$ do bazy przestrzeni $S_\lambda^{N-2} \supset S_\lambda^{N-1}$ dodając wektory $\mathcal{B}^3 := \{v_{i_3}^{(3|1)}\}_{i_3 \in \overline{1, d_N^2}}$, gdzie $d_N^2 := d_{N-2}^0 - d_{N-1}^0$. Rozumując jak poprzednio, stwierdzamy, że

$$\forall_{i_3 \in \overline{1, d_N^2}} \exists_{v_{i_3}^{(3|N-2)} \in V} : v_{i_3}^{(3|1)} = \chi_\lambda^{N-3}(v_{i_3}^{(3|N-2)}),$$

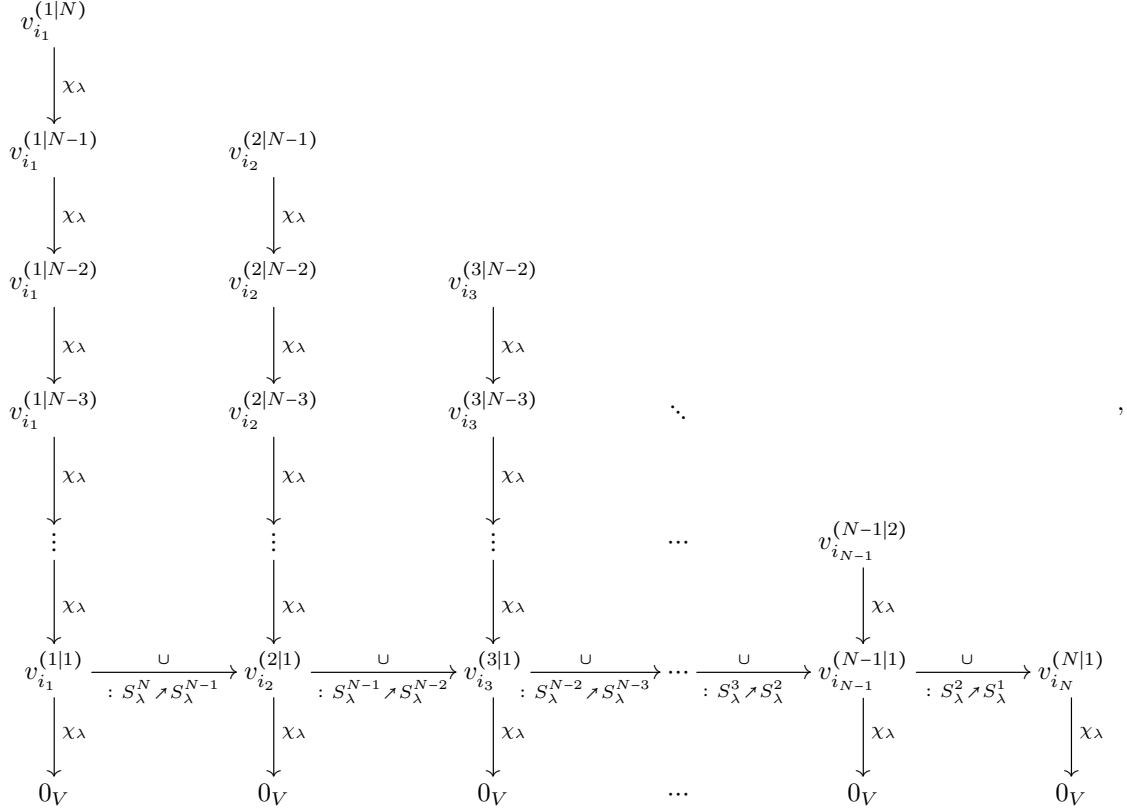
i tym sposobem otrzymujemy rodzinę wektorów

$$v_{i_3}^{(3|j_3)} := \chi_\lambda^{N-2-j_3}(v_{i_3}^{(3|N-2)}), \quad j_3 \in \overline{1, N-2}.$$

Po N iteracjach opisanej tu procedury otrzymujemy ostatecznie zbiór wektorów $\mathcal{B}^N := \{v_{i_N}^{(N|1)}\}_{i_N \in \overline{1, d_N^{N-1}}}$, które uzupełniają zbiór $\mathcal{B}^1 \cup \mathcal{B}^2 \cup \dots \cup \mathcal{B}^{N-1}$ do bazy

$S_\lambda^1 \equiv \text{Ker } \chi_\lambda$. Pokażemy, że rodzina χ -serii $\mathcal{B} := \{v_{i_n}^{(n|j_n)}\}_{\substack{i_n \in \overline{1, d_N^{n-1}} \\ j_n \in \overline{1, N+1-n} \\ n \in \overline{1, N}}}$, zobrażowana

na poniższym diagramie pogładowym



jest bazą przestrzeni $\text{Ker } \chi_\lambda^N$. W tym celu sprawdzamy najpierw, że $\mathcal{B}$ jest zbiorem liniowo niezależnym. Rozważmy zatem rodzinę skalarów $\mathcal{M} := \{\mu_{i_n}^{(n|j_n)}\}_{\substack{i_n \in \overline{1, d_N^{n-1}} \\ j_n \in \overline{1, N+1-n} \\ n \in \overline{1, N}}}$ $\subset$

$\mathbb{K}$, która zadaje rozkład wektora zerowego

$$0_V = \sum_{n=1}^N \sum_{i_n=1}^{d_N^{n-1}} \sum_{j_n=1}^{N+1-n} \mu_{i_n}^{(n|j_n)} \triangleright v_{i_n}^{(n|j_n)}.$$

Na podstawie prostego rachunku (patrz: powyższy diagram)

$$0_V = \chi_\lambda^{N-1}(0_V) = \sum_{n=1}^N \sum_{i_n=1}^{d_N^{n-1}} \sum_{j_n=1}^{N+1-n} \mu_{i_n}^{(n|j_n)} \triangleright \chi_\lambda^{N-1}(v_{i_n}^{(n|j_n)}) = \sum_{i_1=1}^{d_N^0} \mu_{i_1}^{(1|N)} \triangleright v_{i_1}^{(1|1)}$$

i biorąc pod uwagę liniową niezależność $\mathcal{B}^1$, wnioskujemy, że

$$\forall_{i_1 \in \overline{1, d_N^0}} : \mu_{i_1}^{(1|N)} = 0_{\mathbb{K}}.$$

Obliczywszy następnie

$$\begin{aligned} 0_V &= \chi_\lambda^{N-2}(0_V) = \sum_{i_1=1}^{d_N^0} \mu_{i_1}^{(1|N)} \triangleright v_{i_1}^{(1|2)} +_V \sum_{i_1=1}^{d_N^0} \mu_{i_1}^{(1|N-1)} \triangleright v_{i_1}^{(1|1)} +_V \sum_{i_2=1}^{d_N^1} \mu_{i_2}^{(2|N-1)} \triangleright v_{i_2}^{(2|1)} \\ &= \sum_{i_1=1}^{d_N^0} \mu_{i_1}^{(1|N-1)} \triangleright v_{i_1}^{(1|1)} +_V \sum_{i_2=1}^{d_N^1} \mu_{i_2}^{(2|N-1)} \triangleright v_{i_2}^{(2|1)}, \end{aligned}$$

stwierdzamy, tym razem korzystając z liniowej niezależności $\mathcal{B}^1 \cup \mathcal{B}^2$, że

$$\forall_{i_1 \in \overline{1, d_N^0}} : \mu_{i_1}^{(1|N-1)} = 0_{\mathbb{K}} \quad \wedge \quad \forall_{i_2 \in \overline{1, d_N^1}} : \mu_{i_2}^{(2|N-1)} = 0_{\mathbb{K}}.$$

Powtarzając to rozumowanie $N-1$ razy, wykazujemy trywialność wszystkich elementów rodziny $\mathcal{M}$ i tym samym – liniową niezależność $\mathcal{B}$. Pozostaje przekonać się, że $|\mathcal{B}| = \dim_{\mathbb{K}} \text{Ker } \chi_\lambda^N$. Na mocy definicji liczb d_N^{n-1} , wyprowadzamy

$$\begin{aligned} |\mathcal{B}| &= \sum_{n=1}^N (N+1-n) d_N^{n-1} \\ &\equiv d_N^0 + (d_N^0 + d_N^1) + (d_N^0 + d_N^1 + d_N^2) + \cdots + (d_N^0 + d_N^1 + \cdots + d_N^{N-1}) \\ &= \dim_{\mathbb{K}} S_\lambda^N + \dim_{\mathbb{K}} S_\lambda^{N-1} + \dim_{\mathbb{K}} S_\lambda^{N-2} + \cdots + \dim_{\mathbb{K}} S_\lambda^1 \\ &\equiv \sum_{n=1}^N \dim_{\mathbb{K}} (\text{Im } \chi_\lambda^{n-1} \cap \text{Ker } \chi_\lambda). \end{aligned}$$

W dalszych obliczeniach pomocnym okazuje się następujący

LEMAT 9.12. *Przyjmijmy notację Def. 21, 32, 35, 36, 61, 63, 65, 72 i 73. Niechaj $\chi^{(\alpha)}$, $\alpha \in \{1, 2\}$ będą endomorfizmami skończenie wymiarowej przestrzeni wektorowej V nad ciałem $\mathbb{K}$. Zachodzą tożsamości*

$$\begin{aligned} \dim_{\mathbb{K}} (\text{Im } \chi^{(1)} \cap \text{Ker } \chi^{(2)}) &= \dim_{\mathbb{K}} \text{Im } \chi^{(1)} - \dim_{\mathbb{K}} \text{Im } (\chi^{(2)} \circ \chi^{(1)}) \\ &= \dim_{\mathbb{K}} \text{Ker } (\chi^{(2)} \circ \chi^{(1)}) - \dim_{\mathbb{K}} \text{Ker } \chi^{(1)}. \end{aligned}$$

■

Dowód: Na mocy Stw. 83 spełniona jest relacja

$$\dim_{\mathbb{K}} \text{Im } \chi^{(1)} = \dim_{\mathbb{K}} \text{Ker } (\chi^{(2)}|_{\text{Im } \chi^{(1)}}) + \dim_{\mathbb{K}} \text{Im } (\chi^{(2)}|_{\text{Im } \chi^{(1)}}),$$

która implikuje wprost pierwszą z dowodzonych tożsamości. Jeśli wziąć pod uwagę także bilanse wymiarów

$$\dim_{\mathbb{K}} \text{Ker } (\chi^{(2)} \circ \chi^{(1)}) = \dim_{\mathbb{K}} V - \dim_{\mathbb{K}} \text{Im } (\chi^{(2)} \circ \chi^{(1)})$$

oraz

$$\dim_{\mathbb{K}} \text{Ker } \chi^{(1)} = \dim_{\mathbb{K}} V - \dim_{\mathbb{K}} \text{Im } \chi^{(1)},$$

to otrzymujemy na jej podstawie pożądaną równość

$$\begin{aligned} &\dim_{\mathbb{K}} \text{Ker } (\chi^{(2)} \circ \chi^{(1)}) - \dim_{\mathbb{K}} \text{Ker } \chi^{(1)} \\ &= \dim_{\mathbb{K}} V - \dim_{\mathbb{K}} \text{Im } (\chi^{(2)} \circ \chi^{(1)}) - \dim_{\mathbb{K}} V + \dim_{\mathbb{K}} \text{Im } \chi^{(1)} \end{aligned}$$

$$= \dim_{\mathbb{K}} \operatorname{Im} \chi^{(1)} - \dim_{\mathbb{K}} \operatorname{Im} (\chi^{(2)} \circ \chi^{(1)}) = \dim_{\mathbb{K}} (\operatorname{Im} \chi^{(1)} \cap \operatorname{Ker} \chi^{(2)}).$$

□

W świetle powyższego lematu dostajemy oczekiwany wynik

$$\begin{aligned} |\mathcal{B}| &= \sum_{n=1}^N \dim_{\mathbb{K}} (\operatorname{Im} \chi_{\lambda}^{n-1} \cap \operatorname{Ker} \chi_{\lambda}) = \sum_{n=1}^N (\dim_{\mathbb{K}} \operatorname{Ker} \chi_{\lambda}^n - \dim_{\mathbb{K}} \operatorname{Ker} \chi_{\lambda}^{n-1}) \\ &= \dim_{\mathbb{K}} \operatorname{Ker} \chi_{\lambda}^N - \dim_{\mathbb{K}} \operatorname{Ker} \chi_{\lambda}^0 = \dim_{\mathbb{K}} \operatorname{Ker} \chi_{\lambda}^N - \dim_{\mathbb{K}} \operatorname{Ker} \operatorname{id}_V \\ &= \dim_{\mathbb{K}} \operatorname{Ker} \chi_{\lambda}^N, \end{aligned}$$

który przekonuje nas, że $\mathcal{B}$ istotnie jest bazą podprzestrzeni $\operatorname{Ker} \chi_{\lambda}^N$.

W następnym kroku dowodzimy tożsamości

$$(9.10) \quad \operatorname{Ker} \chi_{\lambda}^N = V(\lambda; \chi).$$

Jak wynika z samej definicji przestrzeni pierwiastkowej, wystarczy sprawdzić warunek

$$(9.11) \quad \forall_{n>N} : \operatorname{Ker} \chi_{\lambda}^n = \operatorname{Ker} \chi_{\lambda}^N.$$

Założmy, przeciwnie, że dla pewnej liczby naturalnej $n > N$ istnieje wektor $v \in \operatorname{Ker} \chi_{\lambda}^n \setminus \operatorname{Ker} \chi_{\lambda}^N$, a wtedy z równości

$$\chi_{\lambda}(\chi_{\lambda}^{n-1}(v)) = 0_V$$

wywdzimy

$$\chi_{\lambda}^{n-1}(v) \in \operatorname{Im} \chi_{\lambda}^{n-1} \cap \operatorname{Ker} \chi_{\lambda}.$$

Przywołując w tym miejscu Równ. (9.8) i (9.9) (i wobec $n-1 \geq N$), konstatujemy, że

$$\chi_{\lambda}^{n-1}(v) \in \operatorname{Im} \chi_{\lambda}^N \cap \operatorname{Ker} \chi_{\lambda} = \{0_V\},$$

czyli też

$$\chi_{\lambda}^{n-1}(v) = 0_V.$$

To jednak oznacza, że

$$v \in \operatorname{Ker} \chi_{\lambda}^{n-1},$$

co ostatecznie doprowadza nas do sprzeczności. Wnioskujemy zatem, że warunek (9.11) jest spełniony.

Tożsamość (9.10) w połączeniu z tezą Tw. 9.10 pozwala stwierdzić, że dopełnienie proste W podprzestrzeni $\operatorname{Ker} \chi_{\lambda}^N$ jest – tak jak i ona sama – podprzestrzenią χ -niezmienniczą (równą sumie prostej podprzestrzeni pierwiastkowych stowarzyszonych z pozostałymi wartościami własnymi χ), co oznacza, że całą opisaną tu procedurę możemy powtórzyć dla zredukowanej wymiarowo pary $(W, \chi|_W)$, konstruując tym sposobem złożoną z χ -serii bazę jednej z pozostałych przestrzeni pierwiastkowych χ . Po $r < \infty$ krokach otrzymujemy więc bazę V będącą konkatenacją baz poszczególnych przestrzeni pierwiastkowych, z których każda jest złożona z liczby χ -serii równej wysokości odnośnej przestrzeni pierwiastkowej.

Na zakończenie niniejszego dowodu zauważamy, że dokonując rozkładu bazy $\mathcal{B}$ (dla każdej wartości własnej wziętej z osobna, w dowolnym porządku) na poszczególne χ -serie (rozstawione w dowolnej kolejności), a następnie wybierając w

obrębie każdej z nich porządek zgodny ze zwrotem pionowych strzałek na naszkicowanym wcześniej diagramie, uzyskujemy bazę (uporządkowaną), w której macierz endomorfizmu χ przybiera pożądaną postać blokowo diagonalną. $\square$

9.8. Kompleksyfikacja i rzeczywiste bazy jordanowskie

Okazuje się, że w konsekwencji istnienia prostej relacji $\iota : \mathbb{R} \longrightarrow \mathbb{C}$, opisanej w Stw. 2, możemy – adaptując prowadzący do niej schemat myślenia – wnioskować na podstawie Tw. 9.11 także odnośnie do postaci normalnej endomorfizmu przestrzeni wektorowej nad ciałem $\mathbb{R}$. W tym celu wprowadzamy

DEFINICJA 135. Niechaj $((V, +_V, P_V, \bullet \longmapsto 0_V), \ell \equiv \triangleright)$ będzie przestrzenią wektorową nad ciałem $\mathbb{R}$. **Kompleksyfikacja przestrzeni V** to przestrzeń wektorowa

$$((V^{\mathbb{C}} := V \times V, +_{V^{\mathbb{C}}}, P_{V^{\mathbb{C}}}, \bullet \longmapsto (0_V, 0_V)), \ell^{\mathbb{C}}),$$

o strukturze grupy przemiennej zadanej przez operację 2-argumentową

$$+_{V^{\mathbb{C}}} : V^{\mathbb{C}} \times V^{\mathbb{C}} \longrightarrow V^{\mathbb{C}} : ((v_1, v_2), (w_1, w_2)) \longmapsto (v_1 +_V v_2, w_1 +_V w_2)$$

oraz operację 1-argumentową

$$P_{V^{\mathbb{C}}} : V^{\mathbb{C}} \curvearrowright : (v_1, v_2) \longmapsto (P_V(v_1), P_V(v_2))$$

i z działaniem ciała $\mathbb{C}$ określonym wzorem

$$\ell^{\mathbb{C}} : \mathbb{C} \times V^{\mathbb{C}} \longrightarrow V^{\mathbb{C}}$$

$$: ((\lambda, \mu), (v_1, v_2)) \longmapsto (\lambda \triangleright v_1 +_V \mu \triangleright P_V(v_2), \lambda \triangleright v_2 +_V \mu \triangleright v_1).$$

▲

Bez trudu sprawdzamy

STWIERDZENIE 186. *Odwzorowanie*

$$\iota_V : V \longrightarrow V^{\mathbb{C}} : v \longmapsto (v, 0_V)$$

jest monomorfizmem między przestrzeniami $\mathbb{R}$ -liniowymi $((V, +_V, P_V, \bullet \longmapsto 0_V), \ell)$ i $((V^{\mathbb{C}}, +_{V^{\mathbb{C}}}, P_{V^{\mathbb{C}}}, \bullet \longmapsto (0_V, 0_V)), \ell_{\mathbb{C}} \circ \iota)$, przy czym strukturę $\mathbb{R}$ -modułu na $V^{\mathbb{C}}$ indukuje monomorfizm ciał (3.1). W szczególności jeśli $\mathcal{B}$ jest bazą przestrzeni V ,

$$V = \langle \mathcal{B} \rangle_{\mathbb{R}},$$

to $\iota_V(\mathcal{B})$ jest bazą przestrzeni $V^{\mathbb{C}}$,

$$V^{\mathbb{C}} = \langle \iota_V(\mathcal{B}) \rangle_{\mathbb{C}}.$$

■

Dowód: Jedynym stwierdzeniem wymagającym komentarza jest to dotyczące struktury bazy przestrzeni $V^{\mathbb{C}}$. Otóż jego treść wynika wprost z następującej obserwacji. Niech $\mathcal{B} := \{v^{\lambda}\}_{\lambda \in \Lambda}$. Przestrzeń $V^{\mathbb{C}}$ jest powłoką $\mathbb{C}$ -liniową zbioru

$$\tilde{\mathcal{B}} := \{(v^{\lambda}, 0_V)\}_{\lambda \in \Lambda} \cup \{(0, v_{\lambda})\}_{\lambda \in \Lambda}.$$

Zarazem $(0_V, v^\lambda) = \ell_i^{\mathbb{C}}(v^\lambda, 0_V)$, zatem

$$\langle \widetilde{\mathcal{B}} \rangle_{\mathbb{C}} \equiv \langle \{(v^\lambda, 0_V)\}_{\lambda \in \Lambda} \rangle_{\mathbb{C}} \equiv \langle \iota_V(\mathcal{B}) \rangle_{\mathbb{C}}.$$

Jest przy tym jasne, że zbiór $\iota_V(\mathcal{B})$ jest liniowo niezależny nad $\mathbb{C}$ (będąc liniowo niezależnym nad $\iota(\mathbb{R})$). $\square$

NOTACJA 8. Teza Stw. 186, w połączeniu z tezą Stw. 2, podpowiada naturalny zapis elementów przestrzeni $V^{\mathbb{C}}$. Oto utożsamiający obraz monomorfizmu ι_V z jego dziedziną, zapiszemy

$$\forall_{v \in V} : \iota_V(v) \equiv v,$$

a więc także (po opuszczeniu indeksu $V^{\mathbb{C}}$ w zapisie operacji 2-argumentowej na $V^{\mathbb{C}}$)

$$\begin{array}{ccc} \forall_{v=(v_1, v_2) \in V^{\mathbb{C}}} : v \equiv v_1 + i \triangleright v_2. \\ * & * & * \end{array}$$

Analogia z konstrukcją ciała liczb zespolonych na bazie ciała liczb rzeczywistych sięga dalej. Oto bowiem znajdujemy naturalną

DEFINICJA 136. W notacji Def. 18 i 135 **sprzężenie zespolone na przestrzeni $V^{\mathbb{C}}$** to odwzorowanie

$$\cdot : V^{\mathbb{C}} \curvearrowright : (v_1, v_2) \mapsto (v_1, P_V(v_2)) \equiv (v_1, -v_2).$$

▲

Mamy oczywiste

STWIERDZENIE 187. W notacji Def. 18, 135 i 136 **sprzężenie zespolone na przestrzeni $V^{\mathbb{C}}$ jest inwolutywnym antyizomorfizmem, tj. – w szczególności –**

$$\forall_{(\lambda, v) \in \mathbb{C} \times V^{\mathbb{C}}} : \overline{\lambda \triangleright v} = \overline{\lambda} \triangleright \overline{v}.$$

■

W następnej kolejności rozważamy

DEFINICJA 137. W notacji Def. 135 **kompleksyfikacja endomorfizmu $\chi \in \text{End}_{\mathbb{R}}(V)$** to endomorfizm $\chi^{\mathbb{C}} \in \text{End}_{\mathbb{C}}(V^{\mathbb{C}})$ dany wzorem

$$\chi^{\mathbb{C}} : V^{\mathbb{C}} \curvearrowright : (v_1, v_2) \mapsto (\chi(v_1), \chi(v_2)).$$

▲

Jak wynika wprost z powyższej definicji,

STWIERDZENIE 188. Niechaj V będzie skończenie wymiarową przestrzenią wektorową nad ciałem $\mathbb{R}$ o bazie $\mathcal{B}$ i niech $\chi \in \text{End}_{\mathbb{R}}(V)$ będzie endomorfizmem V . Macierz kompleksyfikacji $\chi^{\mathbb{C}}$ względem bazy $\iota_V(\mathcal{B})$ jest tożsama z macierzą endomorfizmu χ względem bazy $\mathcal{B}$,

$$[\chi^{\mathbb{C}}]_{\iota_V(\mathcal{B})}^{\iota_V(\mathcal{B})} \equiv [\chi]_{\mathcal{B}}^{\mathcal{B}}.$$

■

Kompleksyfikacja rzeczywistej przestrzeni wektorowej V i jej endomorfizmów pozwala zastosować wcześniejsze wyniki dotyczące jordanowskiej postaci normalnej endomorfizmu przestrzeni wektorowej nad ciałem algebraicznie domkniętym do endomorfizmu $\chi^{\mathbb{C}}$ indukowanego przez $\chi \in \text{End}_{\mathbb{R}}(V)$. Jak się okazuje, możliwa jest też transkrypcja uzyskanych tym sposobem informacji dotyczących struktury $\chi^{\mathbb{C}}$ do wyjściowej przestrzeni V , co prowadzi do wyznaczenia struktury χ . Fakt ten opisuje zasadnicze

STWIERDZENIE 189. *Przyjmijmy notację Def. 67, 11, 14 21, 23, 24, 32, 35, 61, 63, 64, 65, 68, 70, 72, 73, 75, 77, 78, 82, 124, 126, 131, 132, 133 i 134, Tw. 8.11, Stw. 75, 95, 96, 97, 98, 99, 65 i 171, Cor. 14 oraz Przykł. 41. Niechaj V będzie rzeczywistą przestrzenią wektorową wymiaru $\dim_{\mathbb{R}} V =: N < \infty$ i niech χ będzie endomorfizmem V , a nadto niech też $\text{Sp} \chi^{\mathbb{C}}$ będzie widmem kompleksyfikacji $\chi^{\mathbb{C}}$ endomorfizmu χ . Zbiór $\text{Sp} \chi^{\mathbb{C}}$ jest zachowywany przez operację sprzężenia zespolonego,*

$$(9.12) \quad \forall \lambda \in \mathbb{C} : (\lambda \in \text{Sp} \chi^{\mathbb{C}} \implies \bar{\lambda} \in \text{Sp} \chi^{\mathbb{C}}).$$

Ponadto istnieje baza $\mathcal{B}_J^{\mathbb{C}}$ przestrzeni $V^{\mathbb{C}}$ będąca konkatenacją baz przestrzeni pierwiastkowych $V^{\mathbb{C}}(\lambda; \chi^{\mathbb{C}})$ złożonych z $\chi^{\mathbb{C}}$ -serii (stowarzyszonych z odpowiednimi wartościami własnymi λ) i zawarta w $\text{Im} \iota_V$ o tej własności, że macierz endomorfizmu χ względem jej przeciwobrazu $\mathcal{B}_J$ względem monomorfizmu ι_V przyjmuje postać blokowo diagonalną

$$\begin{aligned} [\chi]_{\mathcal{B}_J}^{\mathcal{B}_J} &= \bigoplus_{\lambda \in \text{Sp} \chi^{\mathbb{C}} \cap \iota(\mathbb{R})} \mathcal{J}_{\mathbb{R}}(\lambda, \varepsilon_{\lambda}; \dim_{\mathbb{C}} V^{\mathbb{C}}(\lambda; \chi^{\mathbb{C}})) \\ &\quad \oplus \bigoplus_{\{\lambda^{\mathbb{C}}, \bar{\lambda}^{\mathbb{C}}\} \subset \text{Sp} \chi^{\mathbb{C}} \setminus \iota(\mathbb{R})} \mathcal{J}_{\mathbb{R}}(\lambda^{\mathbb{C}}, \varepsilon_{\lambda^{\mathbb{C}}}; 2 \dim_{\mathbb{C}} V^{\mathbb{C}}(\lambda^{\mathbb{C}}; \chi^{\mathbb{C}})) \end{aligned}$$

dla pewnych $\varepsilon_{\lambda} \in \{0, 1\}^{\times(\dim_{\mathbb{C}} V^{\mathbb{C}}(\lambda; \chi^{\mathbb{C}})-1)}$ i $\varepsilon_{\lambda^{\mathbb{C}}} \in \{0, 1\}^{\times(\dim_{\mathbb{C}} V^{\mathbb{C}}(\lambda^{\mathbb{C}}; \chi^{\mathbb{C}})-1)}$. Baza ta nosi miano (rzeczywistej) bazy jordanowskiej endomorfizmu χ . ■

Dowód: Zaczniemy od sprawdzenia własności (9.12). Wybierzmy w V dowolną bazę $\mathcal{B} := \{v^n\}_{n \in \overline{1, N}}$, a następnie ustalmy $\iota_V(\mathcal{B})$ jako bazę $V^{\mathbb{C}}$. Przynależność $\lambda \in \mathbb{C}$ do $\text{Sp} \chi^{\mathbb{C}}$ jest równoważna istnieniu $v \in V^{\mathbb{C}}$ o własności

$$[\chi^{\mathbb{C}}]_{\iota_V(\mathcal{B})}^{\iota_V(\mathcal{B})} \odot [v]^{\iota_V(\mathcal{B})} = \lambda \triangleright [v]^{\iota_V(\mathcal{B})}.$$

Sprzężenie zespolone powyższej równości macierzowej (“wyraz po wyrazie”) daje nam – w świetle Stw. 188, które implikuje $[\chi^{\mathbb{C}}]_{\iota_V(\mathcal{B})}^{\iota_V(\mathcal{B})} \in \text{Mat}(\iota(\mathbb{R}); N)$ – równość

$$[\chi^{\mathbb{C}}]_{\iota_V(\mathcal{B})}^{\iota_V(\mathcal{B})} \odot \overline{[v]^{\iota_V(\mathcal{B})}} = \overline{[\chi^{\mathbb{C}}]_{\iota_V(\mathcal{B})}^{\iota_V(\mathcal{B})} \odot [v]^{\iota_V(\mathcal{B})}} = \overline{\lambda \triangleright [v]^{\iota_V(\mathcal{B})}} = \bar{\lambda} \triangleright \overline{[v]^{\iota_V(\mathcal{B})}},$$

ta zaś orzeka istnienie wektora własnego $\sum_{n=1}^N \overline{[v]^{\iota_V(\mathcal{B})}}(n, \bullet) \triangleright v^n \equiv \bar{v}$ endomorfizmu $\chi^{\mathbb{C}}$ stowarzyszonego z wartością własną $\bar{\lambda}$. Powyższa konstatacja dopuszcza naturalne uogólnienie: oto sprzężenie zespolone na przestrzeni $V^{\mathbb{C}}$ ogranicza się do antyzomorfizmu

$$V^{\mathbb{C}}(\lambda; \chi^{\mathbb{C}}) \xrightarrow{\cong} V^{\mathbb{C}}(\bar{\lambda}; \chi^{\mathbb{C}}) : v \mapsto \bar{v}$$

między podprzestrzeniami pierwiastkowymi odpowiadającymi wartościom własnym wzajem zespolenie sprzężonym.

Po dokonaniu rozkładu $V^{\mathbb{C}}$ na przestrzenie pierwiastkowe, którego istnienie gwarantuje Tw. 9.10, przeszerujemy składniki proste tak, by uzyskać równoważny rozkład

$$V^{\mathbb{C}} = \bigoplus_{\lambda \in \text{Sp } \chi^{\mathbb{C}} \cap \iota(\mathbb{R})} V^{\mathbb{C}}(\lambda; \chi^{\mathbb{C}}) \oplus \bigoplus_{\{\lambda^{\mathbb{C}}, \overline{\lambda^{\mathbb{C}}}\} \subset \text{Sp } \chi^{\mathbb{C}} \setminus \iota(\mathbb{R})} \left(V^{\mathbb{C}}(\lambda^{\mathbb{C}}; \chi^{\mathbb{C}}) \oplus V^{\mathbb{C}}(\overline{\lambda^{\mathbb{C}}}; \chi^{\mathbb{C}}) \right).$$

Następnie utwórzmy bazę jordanowską $\mathcal{B}$ przestrzeni $V^{\mathbb{C}}$ wybierając w przestrzeniach pierwiastkowych $V^{\mathbb{C}}(\lambda; \chi^{\mathbb{C}})$ i $V^{\mathbb{C}}(\overline{\lambda}; \chi^{\mathbb{C}})$ (wymiaru $\dim_{\mathbb{C}} V^{\mathbb{C}}(\overline{\lambda}; \chi^{\mathbb{C}}) \equiv \dim_{\mathbb{C}} V^{\mathbb{C}}(\lambda; \chi^{\mathbb{C}}) =: n_{\lambda}$) bazy (jordanowskie) wzajem sprzężone $\{e^i := (x^i, y^i)\}_{i \in \overline{1, n_{\lambda}}}$ i – odpowiednio – $\{\overline{e^i} = (x^i, -y^i)\}_{i \in \overline{1, n_{\lambda}}}$. Tym sposobem sprowadzamy klatki jordanowskie dla $V^{\mathbb{C}}(\lambda^{\mathbb{C}}; \chi^{\mathbb{C}})$ i $V^{\mathbb{C}}(\overline{\lambda^{\mathbb{C}}}; \chi^{\mathbb{C}})$ do postaci strukturalnie identycznej (jedyną różnicą jest obecność wartości własnej $\overline{\lambda^{\mathbb{C}}}$ na przekątnej klatki dla $V^{\mathbb{C}}(\overline{\lambda^{\mathbb{C}}}; \chi^{\mathbb{C}})$, gdy tymczasem klatka dla $V^{\mathbb{C}}(\lambda^{\mathbb{C}}; \chi^{\mathbb{C}})$ ma w tym miejscu wartość własną $\lambda^{\mathbb{C}}$). Zajmiemy się najpierw klatkami odpowiadającymi rzeczywistym wartościom własnym $\lambda \in \text{Sp } \chi^{\mathbb{C}} \cap \iota(\mathbb{R})$. W świetle powyższego rozumowania w odnośnych przestrzeniach pierwiastkowych możemy zawsze wybrać bazy jordanowskie $\mathcal{B}_{\lambda} = \{e^i\}_{i \in \overline{1, n_{\lambda}}}$ złożone z elementów samosprzężonych, tj. takich, które spełniają warunki

$$\forall_{i \in \overline{1, n_{\lambda}}} \exists_{v^i \in V} : e^i = \iota_V(v^i),$$

co też czynimy. Będąc liniowo niezależnymi nad $\mathbb{C}$, wektory e^i są w szczególności liniowo niezależne nad $\iota(\mathbb{R})$, to zaś oznaczają, że wektory v^i są liniowo niezależne nad $\mathbb{R}$ i tworzą bazę przestrzeni pierwiastkowej $V(\lambda; \chi)$. Rzecz jasna, wektory odpowiadające różnym rzeczywistym wartościom własnym $\chi^{\mathbb{C}}$ są liniowo niezależne (nad $\mathbb{R}$). Macierz ograniczenia endomorfizmu χ do podprzestrzeni $V(\lambda; \chi) \subset V$ przyjmuje postać klatki jordanowskiej $\mathcal{J}_{\mathbb{R}}(\lambda, \varepsilon_{\lambda}; \dim_{\mathbb{C}} V^{\mathbb{C}}(\lambda; \chi^{\mathbb{C}}))$. Dokonawszy konkatencji tak określonych baz przestrzeni pierwiastkowych dla wszystkich wartości własnych χ (czyli dla wszystkich rzeczywistych wartości własnych $\chi^{\mathbb{C}}$), otrzymujemy w ten sposób bazę $\mathcal{B}_{\mathbb{R}}$ podprzestrzeni $\bigoplus_{\lambda \in \text{Sp } \chi^{\mathbb{C}} \cap \iota(\mathbb{R})} V(\lambda; \chi) \subset V$, a względem niej – podmacierz $\bigoplus_{\lambda \in \text{Sp } \chi^{\mathbb{C}} \cap \iota(\mathbb{R})} \mathcal{J}_{\mathbb{R}}(\lambda, \varepsilon_{\lambda}; \dim_{\mathbb{C}} V^{\mathbb{C}}(\lambda; \chi^{\mathbb{C}}))$ macierzy endomorfizmu χ . Pozostaje uzupełnić układ $\mathcal{B}_{\mathbb{R}}$ do bazy przestrzeni V . W tym celu poddamy stosownej „dekompleksyfikacji” bazę $\{e^i, \overline{e^i}\}_{i \in \overline{1, n_{\lambda^{\mathbb{C}}}}}$ przestrzeni $\mathcal{V}_{\lambda^{\mathbb{C}}} := V^{\mathbb{C}}(\lambda^{\mathbb{C}}; \chi^{\mathbb{C}}) \oplus V^{\mathbb{C}}(\overline{\lambda^{\mathbb{C}}}; \chi^{\mathbb{C}}) \subset V^{\mathbb{C}}$. Zauważmy, że zbiór wektorów

$$\iota_V(x^i) = \frac{1}{2}(e^i + {}_{v^{\mathbb{C}}} \overline{e^i}), \quad \iota_V(y^i) = \frac{1}{2i}(e^i - {}_{v^{\mathbb{C}}} \overline{e^i})$$

jest liniowo niezależny nad $\mathbb{C}$ (jako układ równoważny $\mathbb{C}$ -liniowo niezależnemu układowi $\{e^i, \overline{e^i}\}_{i \in \overline{1, n_{\lambda^{\mathbb{C}}}}}$), a zatem zbiór $\{x^i, y^i\}_{i \in \overline{1, n_{\lambda^{\mathbb{C}}}}}$ jest liniowo niezależny nad $\mathbb{R}$. Z racji $\mathbb{C}$ -liniowej niezależności baz przestrzeni pierwiastkowych $\chi^{\mathbb{C}}$ odpowiadających różnym wartościom własnym, elementy tego zbioru są także liniowo niezależne od analogicznych układów otrzymanych dla pozostałych istotnie zespolonych wartości własnych $\chi^{\mathbb{C}}$, jak również od znalezionych uprzednio wektorów v^i . Dokonajmy konkatencji zbiorów $\{x^i, y^i\}_{i \in \overline{1, n_{\lambda^{\mathbb{C}}}}}$ dla wszystkich (istotnie zespolonych) wartości własnych $\chi^{\mathbb{C}}$. Jeśli uwzględnić równoliczność uzyskanego tą drogą liniowo niezależnego zbioru wektorów z dopełnienia podprzestrzeni $\bigoplus_{\lambda \in \text{Sp } \chi^{\mathbb{C}} \cap \iota(\mathbb{R})} V(\lambda; \chi)$ w V z wymiarem tejże podprzestrzeni (równym wymiarowi $\mathbb{C}$ -liniowemu podprzestrzeni

$\oplus_{\lambda^c \in \text{Sp}_{\chi^c} \setminus \iota(\mathbb{R})} V(\lambda^c; \chi) \subset V^c$), stwierdzamy, że zbiór ten stanowi uzupełnienie $\mathcal{B}_{\mathbb{R}}$ do bazy V , którą oznaczmy symbolem $\mathcal{B}_J$. Przy tym macierz $[\chi]_{\mathcal{B}_J}^{\mathcal{B}_J}$ powstaje z macierzy χ^c względem bazy będącej konkatenacją wprowadzonych powyżej baz $\{e^i\}_{i \in \overline{1, n_\lambda}}$ poszczególnych przestrzeni pierwiastkowych $V^c(\lambda; \chi^c)$ poprzez przejście od baz jordanowskich $\{e^i, \bar{e}^i\}_{i \in \overline{1, n_{\lambda^c}}}$ w każdej z przestrzeni $V^c(\lambda^c; \chi^c) \oplus V^c(\bar{\lambda}^c; \chi^c)$ do odnośnych baz $\{\iota_V(x^i), \iota_V(y^i)\}_{i \in \overline{1, n_{\lambda^c}}}$ przy jednoczesnym zachowaniu baz $\{\iota_V(v^i)\}_{i \in \overline{1, n_\lambda}}$ przestrzeni pierwiastkowych odpowiadających rzeczywistym wartościom własnym χ^c . Wprowadźmy oznaczenia: $(e, \bar{e}) := (e^1, e^2, \dots, e^{n_{\lambda^c}}, \bar{e}^1, \bar{e}^2, \dots, \bar{e}^{n_{\lambda^c}})$, $(x, y) := (x^1, y^1, x^2, y^2, \dots, x^{n_{\lambda^c}}, y^{n_{\lambda^c}})$ i $\iota_V(x, y) := (\iota_V(x^1), \iota_V(y^1), \iota_V(x^2), \iota_V(y^2), \dots, \iota_V(x^{n_{\lambda^c}}), \iota_V(y^{n_{\lambda^c}}))$. Rzeczne przejście realizują macierze

$$[\text{id}_V|_{\mathcal{V}_{\lambda^c}}]_{(e, \bar{e})}^{\iota_V(x, y)}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & & 0 & 0 & 0 \\ i & 0 & 0 & 0 & 0 & & 0 & 0 & 0 & -i & 0 & 0 & 0 & 0 & & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & & 0 & 0 & 0 \\ 0 & i & 0 & 0 & 0 & & 0 & 0 & 0 & 0 & -i & 0 & 0 & 0 & & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & i & 0 & 0 & & 0 & 0 & 0 & 0 & 0 & -i & 0 & 0 & & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & & 0 & 0 & 0 \\ 0 & 0 & 0 & i & 0 & & 0 & 0 & 0 & 0 & 0 & 0 & -i & 0 & & 0 & 0 & 0 \\ & \vdots & & & & & \vdots & & & & & & & & & \vdots & & \\ 0 & 0 & 0 & 0 & 0 & & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & i & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & -i & 0 \\ 0 & 0 & 0 & 0 & 0 & & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & & 0 & 0 & i & 0 & 0 & 0 & 0 & 0 & & 0 & 0 & -i \end{pmatrix},$$

oraz

$$[\text{id}_V|_{\mathcal{V}_{\lambda^c}}]_{\iota_V(x, y)}^{(e, \bar{e})}$$

$$= \frac{1}{2} \begin{pmatrix} 1 & -i & 0 & 0 & 0 & 0 & 0 & 0 & & 0 & 0 & 0 & 0 & 0 & 0 & & 0 & 0 \\ 0 & 0 & 1 & -i & 0 & 0 & 0 & 0 & & 0 & 0 & 0 & 0 & 0 & 0 & & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -i & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -i & & 0 & 0 & 0 & 0 & 0 & & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & 0 & 0 & 0 & 0 & 0 & & 0 & 0 \\ & \vdots & & & & & \vdots & & & & \vdots & & & & & & \vdots & \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & 1 & -i & 0 & 0 & 0 & & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & 0 & 0 & 1 & -i & 0 & & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & 0 & 0 & 0 & 0 & 1 & -i & & 0 \\ 1 & i & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & 0 & 0 & 0 & 0 & 0 & & 0 & 0 \\ 0 & 0 & 1 & i & 0 & 0 & 0 & 0 & 0 & & 0 & 0 & 0 & 0 & 0 & & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & i & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & i & & 0 & 0 & 0 & 0 & 0 & & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & 0 & 0 & 0 & 0 & 0 & & 0 & 0 \\ & \vdots & & & & & \vdots & & & & \vdots & & & & & & \vdots & \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & 1 & i & 0 & 0 & 0 & & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & 0 & 0 & 1 & i & 0 & & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & 0 & 0 & 0 & 0 & 1 & i & & 0 \end{pmatrix}.$$

Bezpośrednim rachunkiem sprawdzamy pożądaną równość

$$\begin{aligned}
[\chi|_{((x,y))_{\mathbb{R}}}]_{(x,y)}^{(x,y)} &= [\chi^{\mathbb{C}}|_{\mathcal{V}_{\lambda^{\mathbb{C}}}}]_{\iota_V(x,y)}^{\iota_V(x,y)} \\
&= [\text{id}_V|_{\mathcal{V}_{\lambda^{\mathbb{C}}}}]_{(e,\bar{e})}^{\iota_V(x,y)} \odot [\chi^{\mathbb{C}}|_{\mathcal{V}_{\lambda^{\mathbb{C}}}}]_{(e,\bar{e})}^{(e,\bar{e})} \odot [\text{id}_V|_{\mathcal{V}_{\lambda^{\mathbb{C}}}}]_{\iota_V(x,y)}^{(e,\bar{e})} \\
&\equiv [\text{id}_V|_{\mathcal{V}_{\lambda^{\mathbb{C}}}}]_{(e,\bar{e})}^{\iota_V(x,y)} \odot \left(\mathcal{J}(\lambda^{\mathbb{C}}, \varepsilon_{\lambda^{\mathbb{C}}}; n_{\lambda^{\mathbb{C}}}) \oplus \mathcal{J}(\overline{\lambda^{\mathbb{C}}}, \varepsilon_{\lambda^{\mathbb{C}}}; n_{\lambda^{\mathbb{C}}}) \right) \odot [\text{id}_V|_{\mathcal{V}_{\lambda^{\mathbb{C}}}}]_{\iota_V(x,y)}^{(e,\bar{e})} \\
&= \mathcal{J}_{\mathbb{R}}(\lambda^{\mathbb{C}}, \varepsilon_{\lambda^{\mathbb{C}}}; 2n_{\lambda^{\mathbb{C}}}).
\end{aligned}$$

□

Macierz endomorfizmu względem bazy jordanowskiej jest nośnikiem nietrywialnej informacji o anatomii endomorfizmu, oto bowiem wskazuje na możliwość dokonania jego rozkładu na część diagonalną, jednoznacznie określaną przez jego widmo, oraz część ściśle (górną)trójkątną wyjątkowo prostej postaci. Intuicję, której źródłem jest dyskusja endomorfizmu w wyróżnionej bazie jordanowskiej, poddamy abstrakcji w dalszej części wykładu celem uzyskania lepszego wglądu w strukturę wewnętrzną endomorfizmu.

9.9. Endomorfizmy nilpotentne i diagonalizujące

Naszym celem w tej części wykładu jest dalsza systematyzacja wiedzy o strukturze endomorfizmu przestrzeni wektorowej w nawiązaniu do konstrukcji bazy jordanowskiej. Na gruncie zgromadzonych przez nas obserwacji dotyczących uporządkowania indukowanego w przestrzeni wektorowej w obecności endomorfizmu możemy dokonać abstrakcji dwóch istotnych klas endomorfizmów, które określają następujące definicje. Zaczniemy od uogólnienia pojęć napotkanych w konstrukcji bazy jordanowskiej endomorfizmu.

DEFINICJA 138. Przyjmijmy notację Def. 11, 21, 32, 35, 61, 63 i 65. Niechaj V będzie przestrzenią wektorową nad ciałem $\mathbb{K}$. **Endomorfizm nilpotentny** $\nu \in \text{End}_{\mathbb{K}}(V)$ to taki, którego pewna (skończona) potęga jest endomorfizmem zerowym, tj.

$$\exists_{n \in \mathbb{N}} : \underbrace{\nu \circ \nu \circ \dots \circ \nu}_n = 0.$$

▲

Często wygodne okazują się inne, równoważne określenia endomorfizmów tego typu, które wymieniam

STWIERDZENIE 190. Przyjmijmy notację Def. 67, 11, 21, 23, 24, 25, 32, 35, 61, 63, 64, 65, 68, 70, 72, 73, 75, 77, 82, 87, 92, 94, 95, 124 i 127, Stw. 65, 70, 75, 94, 140, 171 i 175 oraz Przykł. 34 (2), 40 (3), 41 i 46 (2). Załóżmy dodatkowo, że przestrzeń V jest wymiaru skończonego $N := \dim_{\mathbb{K}} V < \infty$. Niechaj ν będzie endomorfizmem przestrzeni V . Równoważne są następujące zdania:

- (i) ν jest nilpotentny.
- (ii) $w_{\nu} = (-1)^N t^N$.
- (iii) $\forall_{n \in \overline{0, N-1}} : \tau_n(\nu) = 0$.
- (iv) $\nu^N = 0$.

- (v) Istnieje rodzina $\{V_n\}_{n \in \overline{0, N}}$ podprzestrzeni przestrzeni V wymiaru $\dim_{\mathbb{K}} V_n = n$ o własnościach

$$\{0_V\} \equiv V_0 \subset V_1 \subset V_2 \subset \cdots \subset V_{N-1} \subset V_N \equiv V$$

oraz

$$\forall_{n \in \overline{1, N}} : \nu(V_n) \subset V_{n-1}.$$

- (vi) Istnieje baza przestrzeni V będąca konkatenacją pewnej liczby ν -serii, względem której macierz ν ma postać ściśle (górną)trójkątną.

Z każdego z nich wynika zdanie

- (vii) $\text{Sp } \nu = \{0_{\mathbb{K}}\}$.

Wynikanie odwrotne zachodzi, ilekroć wielomian minimalny ν ma w $\mathbb{K}[t]$ rozkład na czynniki liniowe. ■

Dowód:

- (i) $\Rightarrow$ (ii) Skoro $\nu^n = 0$ dla pewnego $n \in \mathbb{N}$, to $t^n \in \text{Ker } \rho_\nu$, a zatem – na mocy Cor. 23 – $p_\nu \mid t^n$. Ponieważ zaś jedynymi dzielnikami jednomianu t^n są jednomiany t^m , $m \in \overline{0, n}$, przeto koniecznie $p_\nu = t^m$ dla pewnego $m \in \overline{1, n}$. Uwzględnivszy $p_\nu \mid w_\nu$ oraz $\deg w_\nu = N$, wnioskujemy na tej podstawie, że $m \in \overline{1, N}$, co pozwala stwierdzić, tym razem w odwołaniu do Tw. 9.10, że $V = V(0_{\mathbb{K}}; \nu)$. Wprowadźmy w V bazę jordanowską $\mathcal{B}_J$, której istnienie zapewnia Tw. 9.11. W bazie tej

$$[\nu]_{\mathcal{B}_J}^{\mathcal{B}_J} = \mathcal{J}(0, \varepsilon; N)$$

dla pewnego $\varepsilon \in \{0_{\mathbb{K}}, 1_{\mathbb{K}}\}^{\times(N-1)}$, a zatem

$$\det \nu_\lambda = \det_{(N)} (\mathcal{J}(-\lambda, \varepsilon; N)) = (-\lambda)^N,$$

patrz: Przykł. 44.

- (ii) $\Leftrightarrow$ (iii) Tożsamość

$$(-1)^N \cdot t^N = w_\nu = (-1)^N \cdot t^N \boxplus \sum_{n=0}^{N-1} ((-1)^n \cdot_{\mathbb{K}} \tau_n(\nu)) \cdot t^n$$

implikuje równość

$$\sum_{n=0}^{N-1} ((-1)^n \cdot_{\mathbb{K}} \tau_n(\nu)) \cdot t^n = \mathbf{0},$$

którą możemy interpretować jako rozkład wielomianu zerowego w bazie jednomianowej przestrzeni $\mathbb{K}$ -liniowej $\mathbb{K}_{N-1}[t]$, o współczynnikach $(-1)^n \cdot_{\mathbb{K}} \tau_n(\nu)$. Liniowa niezależność elementów tej bazy daje nam wprost pożądaną układ równości $\tau_n(\nu) = 0$, $n \in \overline{0, N-1}$. Implikacja odwrotna jest oczywista.

- (ii) $\Rightarrow$ (iv) Oczywista konsekwencja Tw. 9.8.

- (iv) $\Rightarrow$ (i) Trywialne.

- (i)⇒(v) Nilpotentność ν implikuje niesurjektywność tegoż endomorfizmu, gdyby bowiem ν był surjektywny, tę samą własność miałyby dowolna jego potęga, tymczasem $\nu^n = 0$ dla pewnego $n \in \mathbb{N}$. Niesurjektywność ν oznacza, że $\dim_{\mathbb{K}} \operatorname{Im} \nu \leq N - 1$, czyli istnieje podprzestrzeń $V_{N-1} \subset V_N \equiv V$ wymiaru $\dim_{\mathbb{K}} V_{N-1} = N - 1$ o własności $\nu(V_N) \equiv \operatorname{Im} \nu \subset V_{N-1}$. Zauważając, że V_{N-1} jest ν -niezmiennicza,

$$\nu(V_{N-1}) \subset \nu(V_N) \subset V_{N-1},$$

możemy powtórzyć poprzednie rozumowanie w odniesieniu do pary $(\nu|_{V_{N-1}}, V_{N-1})$, traktując V_{N-1} jako dziedzinę (jawnie) nilpotentnego endomorfizmu $\nu|_{V_{N-1}}$. Tym sposobem po N krokach otrzymujemy pożądaną rodzinę podprzestrzeni przestrzeni V .

- (v)⇒(iv) Inkluzja $\nu(V_k) \subset V_{k-1}$ pociąga za sobą $\nu^2(V_k) \subset V_{k-2}$ i dalsze, tak że – wobec równości $V_0 = \{0_V\}$ – stwierdzamy $\nu^N = 0$.
- (ii)⇒(vi) Korzystając z Tw. 9.11, wybieramy w $V = V(0_{\mathbb{K}}; \nu)$ bazę jordanowską, względem której – jak wcześniej stwierdziliśmy –

$$[\nu]_{\mathcal{B}_J}^{\mathcal{B}_J} = \mathcal{J}(0, \varepsilon; N),$$

czyli macierz ν jest tutaj macierzą górnotrójkątną z zerami na przekątnej.

- (ii)⇐(vi) Trywialne.

Przechodząc do drugiej części tezy, udowodnimy na przykład wynikanie

- (i)⇒(vii) Z tożsamości $\nu^n(v) = 0$, spełnianej dla pewnego $n \in \mathbb{N}$ przez dowolny niezerowy wektor $v \in V$, wynika, że albo $\nu^{n-1}(v) = 0_V$, albo też $\nu^{n-1}(v)$ jest wektorem własnym ν stowarzyszonym z wartością własną $0_{\mathbb{K}}$. W pierwszym przypadku albo $\nu^{n-2}(v) = 0_V$, albo $\nu^{n-2}(v)$ jest wektorem własnym stowarzyszonym z wartością własną $0_{\mathbb{K}}$. Powtarzając to rozumowanie $n - 2$ razy, dochodzimy do wniosku, że albo $\nu(v) = 0_V$, albo $v = 0_V$, przy czym tę ostatnią ewentualność wykluczamy na podstawie założenia dotyczącego v . Ostatecznie więc istnieje wektor własny ν . Niech v będzie takim wektorem,

$$\exists \lambda \in \mathbb{K} : \nu(v) = \lambda \triangleright v.$$

Obliczamy

$$0_V = \nu^n(v) = \lambda^n \triangleright v,$$

co wobec $v \neq 0_V$ implikuje równość

$$\lambda^n = 0_{\mathbb{K}},$$

czyli też $\lambda = 0_{\mathbb{K}}$.

Wynikanie odwrotne w sytuacji, w której wielomian minimalny p_ν endomorfizmu o widmie $\operatorname{Sp} \nu = \{0_{\mathbb{K}}\}$ ma rozkład na czynniki liniowe, jest natychmiastowe, wtedy bowiem na mocy Stw. 185 jest $p_\nu = t^{h(\lambda; \chi)}$, a zatem także $\nu^{h(\lambda; \chi)} = \rho_\nu(p_\nu) = 0$, co dowodzi nilpotentności ν . $\square$

Szczegółowa analiza właściwości definiujących endomorfizmu nilpotentnego pozwala nam lepiej zrozumieć strukturę rozkładu dziedziny dowolnego endomorfizmu na sumę prostą jego przestrzeni pierwiastkowych, wyjaśniając zarazem ukryty dotąd sens algebraiczny zwyrodnienia pierwiastków wielomianu charakterystycznego.

STWIERDZENIE 191. *Przyjmijmy notację Def. 67, 11, 21, 23, 24, 25, 26, 29, 32, 35, 61, 63, 64, 65, 68, 70, 72, 73, 75, 77, 82, 87, 92, 124, 126, 127 i 131, Stw. 65 i 171 oraz Przykł. 34 (2), 40 (3) i 41. Niechaj V będzie skończone wymiarową przestrzenią wektorową nad ciałem $\mathbb{K}$ i niech χ będzie endomorfizmem V , przy czym zakładamy, że wielomian charakterystyczny χ jest rozkładalny w $\mathbb{K}[t]$ na czynniki stopnia 1. Wówczas*

$$\forall \lambda \in \text{Sp } \chi : \dim_{\mathbb{K}} V(\lambda; \chi) = \kappa(\lambda; w_{\chi}).$$

■

Dowód: Endomorfizm $\nu_{\lambda} := \chi_{\lambda}|_{V(\lambda; \chi)}$ jest jawnie nilpotentny, możemy zatem odnieść do niego punkt (ii) Stw. 190, uwzględniając przy tym χ_{λ} -niezmienniczość przestrzeni pierwiastkowych χ , orzeczoną w Stw. 182. Dostajemy

$$\begin{aligned} \prod_{\mu \in \text{Sp } \chi} (\mu - \lambda)^{\kappa(\mu; w_{\chi})} &= F_{w_{\chi}}(\lambda) = \det \chi_{\lambda} = \prod_{\mu \in \text{Sp } \chi} \det \chi_{\lambda}|_{V(\mu; \chi)} \\ &= \prod_{\mu \in \text{Sp } \chi} \det (\nu_{\mu} - \ell_{\lambda - \mu} \circ \text{id}_{V(\mu; \chi)}) = \prod_{\mu \in \text{Sp } \chi} F_{w_{\nu_{\mu}}}(\lambda - \mu) \\ &= \prod_{\mu \in \text{Sp } \chi} (-(\lambda - \mu))^{\dim_{\mathbb{K}} V(\mu; \chi)} = \prod_{\mu \in \text{Sp } \chi} (\mu - \lambda)^{\dim_{\mathbb{K}} V(\mu; \chi)}. \end{aligned}$$

□

W następnej kolejności sformalizujemy pojęcie kryjące się w treści Stw. 173.

DEFINICJA 139. Przyjmijmy notację Def. 67, 11, 21, 32, 35, 61, 65, 68, 70, 72, 73, 75, 78 i 82, Cor. 14, Stw. 75, 95, 96, 97, 98, 99 i 157 oraz Tw. 8.11. Niechaj V będzie przestrzenią wektorową wymiaru $N := \dim_{\mathbb{K}} V < \infty$ nad ciałem $\mathbb{K}$. **Endomorfizm diagonalizowalny** $\delta \in \text{End}_{\mathbb{K}}(V)$ to taki, dla którego istnieje baza $\mathcal{B}$ w V oraz rodzina skalarów $\{\lambda_i\}_{i \in \overline{1, N}} \subset \mathbb{K}$ o własności

$$[\delta]_{\mathcal{B}}^{\mathcal{B}} = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_N).$$

Tak określona baza V nosi miano **bazy diagonalizującej endomorfizm** δ .

▲

Równoważnych a wygodnych określeń endomorfizmu rzeczonego typu dostarcza

STWIERDZENIE 192. *Przyjmijmy notację Def. 67, 11, 21, 23, 24, 32, 35, 61, 63, 64, 65, 75, 78, 79, 80, 124, 126, 127 i 131 oraz Stw. 65, 88 i 171. Niechaj δ będzie endomorfizmem przestrzeni V . Równoważne są następujące zdania:*

- (i) δ jest diagonalizowalny.
- (ii) Istnieje – dla pewnego $n \in \mathbb{N}$ – zupełna rodzina $\{\pi_i\}_{i \in \overline{1, n}}$ rzutów komplementarnych oraz rodzina $\{\lambda_i\}_{i \in \overline{1, n}}$ parami różnych skalarów o własności

$$\delta = \sum_{i=1}^n \ell_{\lambda_i} \circ \pi_i.$$

Mówimy wówczas, że para $(\{\pi_i\}_{i \in \overline{1, n}}, \{\lambda_j\}_{j \in \overline{1, n}})$ określa **rozkład widmowy (lub spektralny) endomorfizmu** δ .

- (iii) Istnieje wielomian $w \in \text{Ker } \rho_\delta$ o pierwiastkach o krotności 1 rozkładalny w $\mathbb{K}[t]$ na czynniki stopnia 1.
- (iv) $\forall \lambda \in \text{Sp } \delta : V(\lambda; \delta) = V_1(\lambda; \delta)$, a nadto wielomian charakterystyczny w_δ jest rozkładalny w $\mathbb{K}[t]$ na czynniki stopnia 1.
- (v) Istnieje w V baza własna δ .

■

Dowód:

- (i) $\Rightarrow$ (ii) Niechaj $\mathcal{B} := \{v^i\}_{i \in \overline{1, N}}$ będzie bazą diagonalizującą δ i niech $\{\tilde{\pi}_i\}_{i \in \overline{1, N}}$ będzie rodzina rzutów stowarzyszoną z rozkładem

$$V = \bigoplus_{i=1}^N \langle v^i \rangle_{\mathbb{K}}$$

poprzez relacje $\langle v^i \rangle_{\mathbb{K}} = \text{Im } \tilde{\pi}_i$. Bezpośredni rachunek

$$\sum_{j=1}^N \ell_{\lambda_j} \circ \tilde{\pi}_j(v^i) = \sum_{j=1}^N (\lambda_j \cdot_{\mathbb{K}} \delta_{i,j}^{\mathbb{K}}) \triangleright v^i = \lambda_i \triangleright v^i = \delta(v^i)$$

w połączeniu ze Stw. 80 pozwala zapisać

$$\delta = \sum_{i=1}^N \ell_{\lambda_i} \circ \tilde{\pi}_i.$$

Dokonując odpowiedniej permutacji indeksów bazy, możemy zawsze pogrupować jej elementy tak, by uzyskać rozkład $\mathcal{B}$ na podrodziny $\{v^1, v^2, \dots, v^{k_1}\} \cup \{v^{k_1+1}, v^{k_1+2}, \dots, v^{k_1+k_2}\} \cup \dots \cup \{v^{k_1+k_2+\dots+k_{n-1}+1}, v^{k_1+k_2+\dots+k_{n-1}+2}, \dots, v^{k_1+k_2+\dots+k_n}\}$ o własności

$$\forall_{j \in \overline{1, n}} \forall_{v \in V} : \delta(v) = \lambda_j \triangleright v$$

$$\implies v \in \langle v^{k_0+k_1+\dots+k_{j-1}+1}, v^{k_0+k_1+\dots+k_{j-1}+2}, \dots, v^{k_0+k_1+\dots+k_j} \rangle_{\mathbb{K}},$$

przy czym przyjmujemy konwencję $k_0 \equiv 0$. Otrzymujemy wtedy rozkład

$$\delta = \sum_{j=1}^n \ell_{\lambda_j} \circ \left(\sum_{i=1}^{k_j} \tilde{\pi}_{k_0+k_1+\dots+k_{j-1}+i} \right).$$

Łatwo sprawdzić, że endomorfizmy $\pi_j := \sum_{i=1}^{k_j} \tilde{\pi}_{k_0+k_1+\dots+k_{j-1}+i}$ tworzą zupełną rodzinę rzutów komplementarnych spełniającą wszystkie warunki z punktu (ii).

- (ii) $\Rightarrow$ (iii) Prosty rachunek:

$$\begin{aligned} \left(\sum_{i=1}^n \ell_{\alpha_i} \circ \pi_i \right) \circ \left(\sum_{j=1}^n \ell_{\beta_j} \circ \pi_j \right) &= \sum_{i,j=1}^n \ell_{\alpha_i \cdot_{\mathbb{K}} \beta_j} \circ \pi_i \circ \pi_j = \sum_{i,j=1}^n \ell_{\alpha_i \cdot_{\mathbb{K}} \beta_j \cdot_{\mathbb{K}} \delta_{i,j}^{\mathbb{K}}} \circ \pi_i \\ &= \sum_{i=1}^n \ell_{\alpha_i \cdot_{\mathbb{K}} \beta_i} \circ \pi_i, \end{aligned}$$

wykonany dla dowolnych skalarów $\alpha_i, \beta_j \in \mathbb{K}$, $i, j \in \overline{1, n}$, pokazuje (na drodze indukcji), że dla wielomianu $w \in \mathbb{K}[t]$ zachodzi tożsamość

$$\rho_\delta(w) = \sum_{i=1}^n \ell_{F_w(\lambda_i)} \circ \pi_i,$$

a zatem poszukiwany wielomian można wybrać w postaci

$$w := \bigodot_{i=1}^n (t - \lambda_i).$$

(iii) $\Rightarrow$ (iv) Pierwsza część tezy jest bezpośrednią konsekwencją Stw. 183, oto bowiem istnienie wielomianu w implikuje

$$V = \bigoplus_{i=1}^n \text{Ker } \delta_{\lambda_i}^{k_i=1},$$

przy czym $V_1(\lambda_i; \delta) \equiv \text{Ker } \delta_{\lambda_i} = V(\lambda_i; \delta)$ i $\dim_{\mathbb{K}} V = \sum_{i=1}^n \dim_{\mathbb{K}} V(\lambda_i; \delta)$. Oczekiwana postać w_δ wyprowadzamy teraz wprost w bazie jordanowskiej V uzgodnionej z powyższym rozkładem.

(iv) $\Rightarrow$ (v) W świetle Tw. 9.10 otrzymujemy

$$V = \bigoplus_{i=1}^n V_1(\lambda_i; \delta),$$

zatem konkatenacja baz przestrzeni własnych $V_1(\lambda_i; \delta)$ jest bazą diagonalizującą δ .

(v) $\Rightarrow$ (i) Oczywiście.

□

Zwieńczeniem naszych dociekań jest

TWIERDZENIE 9.13 (O rozkładzie endomorfizmu na części: diagonalizowalną i nilpotentną). *Przyjmijmy notację Def. 67, 11, 21, 23, 24, 32, 35, 61, 63 i 65. Niechaj V będzie przestrzenią wektorową skończonego wymiaru nad ciałem $\mathbb{K}$ i niech χ będzie endomorfizmem V , przy czym zakładamy, że wielomian minimalny χ jest rozkładalny w $\mathbb{K}[t]$ na czynniki stopnia 1. Wówczas χ ma jednoznaczny rozkład*

$$\chi = \delta + \nu$$

na część diagonalizowalną $\delta \in \text{End}_{\mathbb{K}}(V)$ oraz część nilpotentną $\nu \in \text{End}_{\mathbb{K}}(V)$ wzajemnie przemienne,

$$\delta \circ \nu = \nu \circ \delta.$$

■

Dowód: Kluczową rolę odgrywa tutaj

LEMAT 9.14. *Przyjmijmy notację Def. 67, 11, 21, 23, 24, 32, 35, 61, 63, 64, 65, 124, 126 i 131 oraz Stw. 65 i 171. Niechaj V będzie przestrzenią wektorową skończonego wymiaru nad ciałem $\mathbb{K}$ i niech χ oraz δ będą endomorfizmami V . Jeśli δ jest diagonalizowalny, to prawdziwa jest równoważność*

$$\delta \circ \chi = \chi \circ \delta \iff (\forall_{\lambda \in \text{Sp } \delta} : \chi(V(\lambda; \delta)) \subset V(\lambda; \delta)).$$

■

Dowód:

$\Rightarrow$ Niech $v \in V(\lambda; \delta)$, czyli – na mocy Stw. 192 (patrz: punkt (iv)) – $\delta(v) = \lambda \triangleright v$, a wtedy

$$\delta(\chi(v)) \equiv \delta \circ \chi(v) = \chi \circ \delta(v) \equiv \chi(\delta(v)) = \chi(\lambda \triangleright v) = \lambda \triangleright \chi(v),$$

co oznacza właśnie, że $\chi(v) \in V_1(\lambda; \delta) = V(\lambda; \delta)$.

$\Leftarrow$ W świetle Stw. 192 (patrz: punkt (v)) dowolny wektor $v \in V$ można rozłożyć na sumę

$$v = \sum_{\lambda \in \text{Sp } \delta} v^{(\lambda)}$$

o składnikach $v^{(\lambda)} \in V(\lambda; \delta) = V_1(\lambda; \delta)$, przy czym wprost na mocy założenia jest $\chi(v^{(\lambda)}) \in V(\lambda; \delta)$, a zatem

$$\begin{aligned} \delta \circ \chi(v) &= \sum_{\lambda \in \text{Sp } \delta} \delta \circ \chi(v^{(\lambda)}) = \sum_{\lambda \in \text{Sp } \delta} \lambda \triangleright \chi(v^{(\lambda)}) = \chi \left(\sum_{\lambda \in \text{Sp } \delta} \lambda \triangleright v^{(\lambda)} \right) \\ &= \chi \left(\sum_{\lambda \in \text{Sp } \delta} \delta(v^{(\lambda)}) \right) = \chi \circ \delta(v). \end{aligned}$$

□

Wracamy teraz do dowodu zasadniczego. Wykażemy najpierw istnienie rzeczowego rozkładu. Niech $\text{Sp } \chi = \{\lambda_i\}_{i \in \overline{1, n}}$ dla pewnego $n \in \mathbb{N}$, przy czym zakładamy, że skalary λ_i są parami różne. Istnieje wówczas – na mocy Stw. 9.10 – rozkład

$$V = \bigoplus_{i=1}^n V(\lambda_i; \chi)$$

i stowarzyszona z nim zupełna rodzina rzutów komplementarnych $\{\pi_i\}_{i \in \overline{1, n}}$ o własności $\text{Im } \pi_i = V(\lambda_i; \chi)$, możemy zatem zdefiniować endomorfizm

$$\delta := \sum_{i=1}^n \ell_{\lambda_i} \circ \pi_i,$$

który w świetle Stw. 192 (patrz: punkt (ii)) jest diagonalizowalny. Przy tym dla $\nu := \chi - \delta$ otrzymujemy, przywoławszy uprzednio Stw. 180 i 182, tożsamość

$$\nu \circ \delta \equiv (\chi - \delta) \circ \delta = \chi \circ \delta - \delta \circ \delta = \delta \circ \chi - \delta \circ \delta = \delta \circ (\chi - \delta) \equiv \delta \circ \nu.$$

Ponadto, jak łatwo widać, endomorfizm ograniczony $\nu|_{V(\lambda_i; \chi)}$ jest identyczny z $\chi_{\lambda_i}|_{V(\lambda_i; \chi)}$ i jako taki zachowuje przestrzeń pierwiastkową $V(\lambda_i; \chi)$ oraz jest nilpotentny, co dowodnie pokazuje konstrukcja Väliaho bazy jordanowskiej $V(\lambda_i; \chi)$. Jest zatem ν nilpotentny na całej przestrzeni V . Pozostaje wykazać jednoznaczność uzyskanego tu rozkładu endomorfizmu χ .

Niechaj $\chi = \delta + \nu$ będzie dowolnym rozkładem określonym w tezie stwierdzenia. Wówczas dla każdej wartości własnej $\lambda \in \text{Sp } \delta$ stwierdzamy $\lambda \in \text{Sp } \chi$ i $V(\lambda; \delta) \subset V(\lambda; \chi)$. Istotnie, niech $v \in V(\lambda; \delta)$, czyli – na mocy Stw. 192 (patrz: punkt (iv)) – $\delta(v) = \lambda \triangleright v$. Wówczas $\chi(v) = (\chi - \delta)(v) + \delta(v) = \nu(v) + \lambda \triangleright v$, a zatem $\chi_\lambda(v) = \nu(v)$. Ale też – jak orzeka Lem. 9.14 – podprzestrzeń $V(\lambda; \delta)$ jest χ -niezmiennicza, czyli – wobec swej δ -niezmienniczości – także ν -niezmiennicza, gdyż $v \in V(\lambda; \delta)$ implikuje – znów na mocy Stw. 192 (patrz: punkt (iv)) i założenia $\delta \circ \nu = \nu \circ \delta$ –

$$\delta(\chi(v)) \equiv \delta \circ (\delta + \nu)(v) = (\delta + \nu) \circ \delta(v) = \chi(\lambda \triangleright v) = \lambda \triangleright \chi(v),$$

czyli $\chi(v) \in V(\lambda; \delta)$. W takim jednak razie bez trudu dowodzimy (przez indukcję) zdania

$$\forall_{n \in \mathbb{N}} : \chi_\lambda^n(v) = \nu^n(v),$$

skąd wobec nilpotentności ν wniosek $v \in V(\lambda; \chi)$. Łatwo w tym momencie przekonać się, że zachodzi równość $V(\lambda; \chi) = V(\lambda; \delta)$, oto bowiem – na gruncie Stw. 9.10 oraz udowodnionej powyżej relacji inkluzji między tymi podprzestrzeniami –

$$\begin{aligned} \bigoplus_{\tilde{\lambda} \in \text{Sp } \delta} V(\tilde{\lambda}; \chi) \oplus \bigoplus_{\mu \in \text{Sp } \chi \setminus \text{Sp } \delta} V(\mu; \chi) &\equiv \bigoplus_{\tilde{\lambda} \in \text{Sp } \chi \cap \text{Sp } \delta} V(\tilde{\lambda}; \delta) \oplus \bigoplus_{\mu \in \text{Sp } \chi \setminus \text{Sp } \delta} V(\mu; \chi) \\ &= \bigoplus_{\lambda \in \text{Sp } \chi} V(\lambda; \chi) = V = \bigoplus_{\tilde{\lambda} \in \text{Sp } \delta} V(\tilde{\lambda}; \delta) \subset \bigoplus_{\tilde{\lambda} \in \text{Sp } \delta} V(\tilde{\lambda}; \chi). \end{aligned}$$

Na tej podstawie możemy zapisać

$$\delta = \sum_{\lambda \in \text{Sp } \chi} \ell_\lambda \circ \pi_\lambda,$$

gdzie π_λ jest rzutem na podprzestrzeń $\text{Im } \pi_\lambda = V(\lambda; \chi)$, co kończy dowód. $\square$

Korzystając z konstrukcji przedstawionej w dowodzie Stw. 183, możemy podać jawne wzory na składowe: diagonalizowalną i nilpotentną χ . Oto więc w zapożyczonej z owego dowodu notacji zapiszemy

$$\delta = \sum_{i=1}^n \ell_{\lambda_i} \circ \rho_\chi(p_i) \equiv \rho_\chi(\boxplus_{i=1}^n \lambda_i \cdot p_i)$$

oraz

$$\nu = \chi - \rho_\chi(\boxplus_{i=1}^n \lambda_i \cdot p_i) \equiv \rho_\chi(t \boxplus \boxplus_{i=1}^n \mathbf{P}_K(\lambda_i) \cdot p_i).$$

9.10. Przestrzenie unitarne

Wyjątkową pozycję w opisie struktur i modelowaniu zjawisk fizyki kwantowej oraz teorii względności zajmują przestrzenie wektorowe nad $\mathbb{C}$ i – odpowiednio – nad $\mathbb{R}$ z wyróżnioną dodatnio określoną formą hermitowską, tj. z iloczynem skalarnym. Niniejsza część wykładu jest poświęcona dyskusji istotnych własności tych przestrzeni oraz ich endomorfizmów. Zaczniemy od sprecyzowania przedmiotu rozważań.

DEFINICJA 140. Przyjmijmy notację Def. 11, 13, 14, 18, 21, 32, 35, 61, 63, 105, 106, 107, 108, 109, 116 i 117 oraz Przykł. 35 (2). Niechaj $(\mathbb{K}, J) \in \{(\mathbb{R}, \text{id}_\mathbb{R}), (\mathbb{C}, \cdot)\}$. **Przestrzeń unitarna nad ciałem $\mathbb{K}$** to para $(V, (\cdot|\cdot))$ złożona z przestrzeni wektorowej V nad $\mathbb{K}$ oraz iloczynu skalarnego $(\cdot|\cdot) : V^{\times 2} \rightarrow \mathbb{K}$. Przestrzeń unitarną nad $\mathbb{R}$ (tj. rzeczywistą) określamy mianem **przestrzeni euklidesowej**⁷.

▲

Obecność iloczynu skalarnego na przestrzeni wektorowej pozwala dokonać jej metryzacji (tj. wprowadzić pojęcie odległości) i topologizacji, przy czym obie procedury są ze sobą ściśle powiązane.

⁷W części literatury jest stosowana terminologia, w której ogólna przestrzeń unitarna jest nazywana przestrzenią z iloczynem skalarnym, natomiast określenia ‘unitarna’ i ‘euklidesowa’ są zarezerwowane dla przestrzeni nad $\mathbb{C}$ i – odpowiednio – nad $\mathbb{R}$.

DEFINICJA 141. Przyjmijmy notację Def. 11, 13, 14, 18, 21, 32, 35, 61, 63, 105, 106, 107, 108, 109, 116, 117 i 140 oraz Przykł. 35 (2). Niechaj $(V, (\cdot|\cdot))$ będzie przestrzenią unitarną nad ciałem $\mathbb{K}$. **Norma indukowana na V** to odwzorowanie

$$\|\cdot\| : V \longrightarrow \mathbb{R}_{\geq 0} : v \longmapsto \sqrt{(v|v)}.$$

Zadawane przezeń odwzorowanie

$$d : V^{\times 2} \longrightarrow \mathbb{R}_{\geq 0} : (v, w) \longmapsto \|v - w\|$$

nosi miano **metryki indukowanej**. ▲

Wyjaśnienie obu nazw przynosi

STWIERDZENIE 193. Przyjmijmy notację Def. 11, 13, 14, 18, 21, 32, 35, 61, 63, 105, 106, 107, 108, 109, 116, 117, 140 i 141 oraz Przykł. 35 (2). *Norma indukowana na V jest niezwyrodniała, tj.*

$$\forall_{v \in V} : (\|v\| = 0 \iff v = 0_V) .$$

Stowarzyszona z nią metryka indukowana jest translacyjnie niezmienniczą metryką na V , tj. – w szczególności – spełnia relację

$$\forall_{u, v, w \in V} : d(v +_V u, w +_V u) = d(v, w)$$

oraz nierówność trójkąta

$$\forall_{u, v, w \in V} : d(u, v) + d(v, w) \geq d(u, w) .$$
■

Dowód: Jedynym nietrywialnym faktem jest spełnianie przez d nierówności trójkąta, ta zaś jest bezpośrednim następstwem

LEMAT 9.15 (Nierówność Minkowskiego). Przyjmijmy notację Def. 11, 13, 14, 18, 21, 32, 35, 61, 63, 105, 106, 107, 108, 109, 116, 117, 140 i 141 oraz Przykł. 35 (2). *Zachodzi relacja*

$$\forall_{v, w \in V} : \|v +_V w\| \leq \|v\| + \|w\| .$$
■

Dowód: Na podstawie Stw. 160 szacujemy

$$\begin{aligned} \|v +_V w\|^2 &\equiv (v +_V w | v +_V w) = \|v\|^2 + \|w\|^2 + (v|w) + (w|v) = \|v\|^2 + \|w\|^2 + 2\Re(v|w) \\ &\leq \|v\|^2 + \|w\|^2 + 2|(v|w)| \leq \|v\|^2 + \|w\|^2 + 2\|v\| \cdot \|w\| \equiv (\|v\| + \|w\|)^2 . \end{aligned}$$

□

□

Mamy też przydatną (np. w kontekście analizy fourierowskiej)

STWIERDZENIE 194 (Nierówność Bessela). *Przyjmijmy notację Def. 67, 11, 13, 14, 18, 21, 32, 35, 61, 63, 64, 65, 68, 95, 98, 105, 106, 107, 108, 109, 111, 116, 117, 140 i 141, Stw. 75 oraz Przykł. 34 (2) i 35 (2). Niechaj $\{v^i\}_{i \in \overline{1,n}}$ będzie układem ortonormalnym,*

$$\forall_{i,j \in \overline{1,n}} : (v^i | v^j) = \delta_{i,j}^{\mathbb{K}}.$$

Dla dowolnego wektora $w \in V$ oznaczmy

$$w_i := (w | v^i), \quad i \in \overline{1,n}.$$

Słuszną jest nierówność

$$\sum_{i=1}^n |w_i|^2 \leq \|w\|^2,$$

a ponadto

$$w - \sum_{i=1}^n w_i \triangleright v^i \in \langle v^1, v^2, \dots, v^n \rangle_{\mathbb{K}}^{\perp}.$$

■

Dowód: Wprowadźmy oznaczenie $\tilde{w} := w - \sum_{i=1}^n w_i \triangleright v^i$. Wprost z definicji

$$\begin{aligned} 0 &\leq \|\tilde{w}\|^2 \equiv (w - \sum_{i=1}^n w_i \triangleright v^i | w - \sum_{j=1}^n w_j \triangleright v^j) = (w | w) - \sum_{i=1}^n w_i \cdot (v^i | w) \\ &\quad - \sum_{j=1}^n \overline{w_j} \cdot (w | v^j) + \sum_{i,j=1}^n w_i \cdot \overline{w_j} (v^i | v^j) = \|w\|^2 - 2 \sum_{i=1}^n |w_i|^2 + \sum_{i,j=1}^n |w_i|^2 \cdot \delta_{i,j}^{\mathbb{K}} \\ &= \|w\|^2 - \sum_{i=1}^n |w_i|^2, \end{aligned}$$

co pokazuje prawdziwość nierówności. Jest też, dla dowolnego $i \in \overline{1,n}$,

$$(\tilde{w} | v^i) \equiv (w - \sum_{j=1}^n w_j \triangleright v^j | v^i) = w_i - \sum_{j=1}^n w_j \cdot (v^j | v^i) = w_i - \sum_{j=1}^n w_j \cdot \delta_{i,j}^{\mathbb{K}} = w_i - w_i = 0.$$

□

Podstawowe własności bazy ortonormalnej przestrzeni unitarnej opisuje

STWIERDZENIE 195. *Przyjmijmy notację Def. 67, 11, 13, 14, 18, 21, 32, 35, 61, 63, 64, 65, 68, 95, 98, 105, 106, 107, 108, 109, 111, 116, 117, 140 i 141, Stw. 75 i 194 oraz Przykł. 34 (2) i 35 (2). Niechaj $(V, (\cdot | \cdot))$ będzie skończone wymiarową przestrzenią unitarną nad ciałem $\mathbb{K}$ i niech $\mathcal{B} := \{v^i\}_{i \in \overline{1,n}}$ będzie układem ortonormalnym. $\mathcal{B}$ jest liniowo niezależny. Ponadto poniższe zdania są równoważne:*

- (i) $\forall_{v \in V} \left(\left(\forall_{i \in \overline{1,n}} : (w | v^i) = 0_{\mathbb{K}} \right) \implies w = 0_V \right).$
- (ii) $\mathcal{B}$ jest bazą przestrzeni V , przy czym

$$\forall_{i \in \overline{1,n}} : w = \sum_{i=1}^n (w | v^i) \triangleright v^i.$$

- (iii) $\forall_{u,w \in V} : (u | w) = \sum_{i=1}^n (u | v^i) \cdot \mathbb{K} (v^i | w).$
- (iv) $\forall_{w \in V} : \|w\|^2 = \sum_{i=1}^n |(w | v^i)|^2.$

■

Dowód: Zaczniemy od wykazania liniowej niezależności układu ortonormalnego. Niechaj $\{\lambda_i\}_{i \in \overline{1, n}} \subset \mathbb{K}$ będzie rodziną skalarów o własności

$$\sum_{i=1}^n \lambda_i \triangleright v^i = 0_V,$$

a wtedy

$$\forall_{i \in \overline{1, n}} : 0_{\mathbb{K}} = (0_V | v^i) = \left(\sum_{j=1}^n \lambda_j \triangleright v^j | v^i \right) = \sum_{j=1}^n \lambda_j \cdot_{\mathbb{K}} (v^j | v^i) = \sum_{j=1}^n \lambda_j \cdot_{\mathbb{K}} \delta_{i,j}^{\mathbb{K}} = \lambda_i.$$

Rachunek ten pokazuje słuszność pierwszej części tezy stwierdzenia. Zajmiemy się teraz równoważnymi określeniami bazy ortonormalnej.

(i) $\Rightarrow$ (ii) Dla dowolnego $w \in V$ rozważmy wektor

$$\tilde{w} := w - \sum_{i=1}^n (w | v^i) \triangleright v^i.$$

Ten spełnia tożsamości

$$\begin{aligned} (\tilde{w} | v^i) &= (w | v^i) - \sum_{j=1}^n (w | v^j) \cdot_{\mathbb{K}} (v^j | v^i) = (w | v^i) - \sum_{j=1}^n (w | v^j) \cdot_{\mathbb{K}} \delta_{i,j}^{\mathbb{K}} = (w | v^i) - (w | v^i) \\ &= 0_{\mathbb{K}}, \end{aligned}$$

słuszne dla dowolnego $i \in \overline{1, n}$, co oznacza, że $\tilde{w} = 0_V$. To jednak implikuje relację

$$w = \sum_{i=1}^n (w | v^i) \triangleright v^i$$

i tym samym pokazuje, że $\mathcal{B}$ jest układem generującym, a więc bazą.

(ii) $\Rightarrow$ (iii) Trywialny rachunek.

(iii) $\Rightarrow$ (iv) Oczywiście.

(iv) $\Rightarrow$ (i) Natychmiastowa konsekwencja Stw. 193.

□

Tak jak w przypadku ogólnych form ϵ -hermitowskich, relacja ortogonalności rozszerza się na podprzestrzenie przestrzeni unitarnej. Niezwyrodnienie iloczynu skalarowego pozwala przy tym bez trudu udowodnić następujące własności (w części dyskutowane już wcześniej).

STWIERDZENIE 196. *Przyjmijmy notację Def. 11, 13, 14, 18, 21, 32, 35, 61, 63, 64, 65, 75, 78, 95, 98, 105, 106, 107, 108, 109, 110, 111, 112, 116, 117 i 140 oraz Przykł. 34 (2) i 35 (2). Niechaj $(V, (\cdot | \cdot))$ będzie przestrzenią unitarną skończonego wymiaru nad ciałem $\mathbb{K}$ i niech $W, W_1, W_2 \subset V$ będą podprzestrzeniami V . Wówczas*

- (i) $W^\perp \subset V$ jest podprzestrzenią wektorową V .
- (ii) $(W_1 +_V W_2)^\perp = W_1^\perp \cap W_2^\perp$.
- (iii) $V = W \oplus W^\perp$.
- (iv) $(W^\perp)^\perp = W$.
- (v) $(W_1 \cap W_2)^\perp = W_1^\perp +_V W_2^\perp$.

■

Dowód: Udowodnimy jedynie te punkty, które nie były omawiane wcześniej i jawią się nieoczywistymi.

Ad (iv) Zachodzi oczywiście inkluzja $W \subset (W^\perp)^\perp$, a przy tym – na mocy punktu (iii) (i wobec skończoności wymiaru V) –

$$\dim_{\mathbb{K}} (W^\perp)^\perp = \dim_{\mathbb{K}} V - \dim_{\mathbb{K}} W^\perp = \dim_{\mathbb{K}} V - (\dim_{\mathbb{K}} V - \dim_{\mathbb{K}} W) = \dim_{\mathbb{K}} W.$$

Ad (v) W świetle punktów (ii) i (iv) jest

$$(W_1^\perp +_V W_2^\perp)^\perp = (W_1^\perp)^\perp \cap (W_2^\perp)^\perp = W_1 \cap W_2,$$

stad jednak – znowu na mocy punktu (iv) –

$$W_1^\perp +_V W_2^\perp = ((W_1^\perp +_V W_2^\perp)^\perp)^\perp = (W_1 \cap W_2)^\perp.$$

□

Istnienie iloczynu skalarnego pozwala w naturalny sposób utożsamić przestrzeń wektorową (skończonego wymiaru) ze sprzężoną do niej. Mówi o tym

STWIERDZENIE 197 (Lemat Riesza). *Przyjmijmy notację Def. 11, 13, 14, 18, 21, 32, 35, 61, 63, 65, 70, 94, 105, 106, 107, 108, 109, 116, 117 i 140 oraz Przykł. 34 (2) i 35 (2). Niechaj $(V, (\cdot|\cdot))$ będzie skończeniem wymiarową przestrzenią unitarną nad ciałem $\mathbb{K}$. Wówczas*

$$\forall_{\varphi \in V^*} \exists!_{\varphi^\dagger \in V} \forall_{v \in V} : \langle \varphi, v \rangle = (v|\varphi^\dagger).$$

Odwzorowanie

$$\mathcal{R}_V : V^* \longrightarrow V : \varphi \longmapsto \varphi^\dagger$$

jest półliniowym izomorfizmem, określanym mianem (anty)izomorfizmu Frécheta–Riesza.

■

Dowód: Skonstruujemy $\varphi^\dagger$ dla dowolnego $\varphi \in V^*$. Jeśli $\varphi = 0$, to jedynym kandydatem jest $\varphi^\dagger = 0_V$. Łatwo sprawdzamy, że ten wybór spełnia warunek definiujący. Niech teraz $\varphi \neq 0$, co oznacza, że $\text{Ker } \varphi \neq V$. Mamy wtedy – na mocy Stw. 196 – równość

$$V = \text{Ker } \varphi \oplus (\text{Ker } \varphi)^\perp,$$

czyli $(\text{Ker } \varphi)^\perp \neq V^\perp = \{0_V\}$ i każdy wektor $v \in V$ ma jednoznaczny rozkład

$$v = \kappa +_V \kappa^\perp, \quad \kappa \in \text{Ker } \varphi, \quad \kappa^\perp \in (\text{Ker } \varphi)^\perp.$$

Przy tym wobec równości $\dim_{\mathbb{K}} V = \dim_{\mathbb{K}} \text{Im } \varphi + \dim_{\mathbb{K}} \text{Ker } \varphi = \dim_{\mathbb{K}} \mathbb{K} + \dim_{\mathbb{K}} \text{Ker } \varphi = 1 + \dim_{\mathbb{K}} \text{Ker } \varphi$ (implikowanej przez Stw. 83) oraz wcześniejszej $\dim_{\mathbb{K}} (\text{Ker } \varphi)^\perp = \dim_{\mathbb{K}} V - \dim_{\mathbb{K}} \text{Ker } \varphi = 1$ jest

$$(\text{Ker } \varphi)^\perp = \langle \kappa_0 \rangle_{\mathbb{K}}$$

dla pewnego $\kappa_0 \in V \setminus \{0_V\}$. Zdefiniujmy

$$\varphi^\dagger := \frac{1}{\|\kappa_0\|^2} \cdot_{\mathbb{K}} \overline{\langle \varphi, \kappa_0 \rangle} \triangleright \kappa_0,$$

a wtedy – dla dowolnego $v = \kappa +_V \lambda \triangleright \kappa_0 \in \text{Ker } \varphi \oplus (\text{Ker } \varphi)^\perp \equiv V$ – dostajemy

$$\begin{aligned} (v|\varphi^\dagger) &= \frac{1}{\|\kappa_0\|^2} \cdot_{\mathbb{K}} \overline{\langle \varphi, \kappa_0 \rangle} \cdot_{\mathbb{K}} (\kappa +_V \lambda \triangleright \kappa_0 | \kappa_0) = \frac{1}{\|\kappa_0\|^2} \cdot_{\mathbb{K}} \langle \varphi, \kappa_0 \rangle \cdot_{\mathbb{K}} \lambda \cdot_{\mathbb{K}} (\kappa_0 | \kappa_0) \\ &= \langle \varphi, \lambda \triangleright \kappa_0 \rangle. \end{aligned}$$

Skoro jednak $\kappa \in \text{Ker } \varphi$, to możemy dodać ten wektor do $\lambda \triangleright \kappa_0$, otrzymując tym sposobem pożądaną wynik

$$(v|\varphi^\dagger) = \langle \varphi, \lambda \triangleright \kappa_0 \rangle = \langle \varphi, \kappa +_V \lambda \triangleright \kappa_0 \rangle \equiv \langle \varphi, v \rangle.$$

Jednoznaczność $\varphi^\dagger$ jest oczywistą konsekwencją niezwyrodnienia $(\cdot| \cdot)$, wystarczy zatem przekonać się o półliniowości odwzorowania $\mathcal{R}_V$ i znaleźć jego odwrotność. Ta pierwsza wynika wprost z rachunku (zapisanego dla dowolnego składowego $\lambda \in \mathbb{K}$)

$$(\lambda \triangleright \varphi)^\dagger \equiv \frac{1}{\|\kappa_0\|^2} \cdot_{\mathbb{K}} \overline{\langle \lambda \triangleright \varphi, \kappa_0 \rangle} \triangleright \kappa_0 = \frac{1}{\|\kappa_0\|^2} \cdot_{\mathbb{K}} \bar{\lambda} \cdot_{\mathbb{K}} \overline{\langle \varphi, \kappa_0 \rangle} \triangleright \kappa_0 = \bar{\lambda} \triangleright \varphi^\dagger.$$

Odwzorowanie odwrotne do $\mathcal{R}_V$ natomiast jest dane wzorem

$$\mathcal{R}_V^{-1} : V \longrightarrow V^* : v \longmapsto (\cdot|v) =: v^\dagger.$$

Istotnie, na mocy Stw. 196 zachodzi

$$(\text{Ker } v^\dagger)^\perp \equiv ((v)_{\mathbb{K}}^\perp)^\perp = \langle v \rangle_{\mathbb{K}},$$

ilekroć zatem $v \neq 0_V$, możemy wybrać (w notacji wprowadzonej wcześniej) $\kappa_0 := v$, a wtedy

$$(v^\dagger)^\dagger = \frac{1}{\|v\|^2} \cdot_{\mathbb{K}} \overline{\langle v^\dagger, v \rangle} \triangleright v = \frac{1}{\|v\|^2} \cdot_{\mathbb{K}} \overline{(v|v)} \triangleright v = v.$$

□

Wykorzystując antyizomorfizm Fréchet–Riesza, możemy przetransportować strukturę unitarną z V na V^* .

STWIERDZENIE 198. *Przyjmijmy notację Def. 11, 13, 14, 18, 21, 32, 35, 61, 63, 65, 70, 94, 105, 106, 107, 108, 109, 116, 117 i 140, Stw. 197 oraz Przykł. 34 (2) i 35 (2). Para $(V^*, (\cdot| \cdot)_*)$ złożona z przestrzeni V^* sprzężonej do V oraz odwzorowania*

$$(\cdot| \cdot)_* : V^{* \times 2} \longrightarrow \mathbb{K} : (\varphi, \psi) \longmapsto \overline{(\mathcal{R}_V(\varphi) | \mathcal{R}_V(\psi))}$$

jest przestrzenią unitarną.

■

Dowód: Półtoraliniowość odwzorowania $(\cdot| \cdot)_*$ jest oczywista, pokażemy przeto tylko, że jest ono niezwyrodniałe. Jeśli $\varphi = 0$, to także $\varphi^\dagger = 0_V$, a wtedy $(\varphi| \varphi)_* = (0_V|0_V) = 0_{\mathbb{K}}$, co jest wynikiem pożądanym. Załóżmy następnie, że $\varphi \neq 0$. Zachodzi równość

$$\begin{aligned} (\varphi| \varphi)_* &\equiv \overline{(\varphi^\dagger | \varphi^\dagger)} = (\varphi^\dagger | \varphi^\dagger) \equiv \langle \mathcal{R}_V^{-1}(\varphi^\dagger), \varphi^\dagger \rangle = \langle \varphi, \varphi^\dagger \rangle = \left\langle \varphi, \frac{1}{\|\kappa_0\|^2} \cdot_{\mathbb{K}} \overline{\langle \varphi, \kappa_0 \rangle} \triangleright \kappa_0 \right\rangle \\ &= \frac{1}{\|\kappa_0\|^2} \cdot_{\mathbb{K}} \overline{\langle \varphi, \kappa_0 \rangle} \cdot_{\mathbb{K}} \langle \varphi, \kappa_0 \rangle = \frac{|\langle \varphi, \kappa_0 \rangle|^2}{\|\kappa_0\|^2}, \end{aligned}$$

która pokazuje dowodnie, że $(\cdot| \cdot)_*$ jest odwzorowaniem dodatnim, a ponadto

$$\forall \varphi \in V^* : (\varphi \neq 0 \implies (\varphi|\varphi)_* > 0) ,$$

gdyż w przeciwnym razie dla dowolnego $v = \kappa +_V \lambda \triangleright \kappa_0 \in V$ mielibyśmy

$$\langle \varphi, v \rangle = \lambda \cdot_{\mathbb{K}} \langle \varphi, \kappa_0 \rangle = 0_{\mathbb{K}} ,$$

co oznaczałoby, że $\varphi = 0$, przeciwnie do założenia. $\square$

Zaobserwowana przez nas relacja $\mathcal{R}_V$ między wektorami i funkcjonalami liniowymi podnosi się w naturalny sposób do przestrzeni odwzorowań $\mathbb{K}$ -liniowych, o czym mówi

DEFINICJA 142. Przyjmijmy notację Def. 11, 13, 14, 18, 21, 32, 35, 61, 63, 65, 105, 106, 107, 108, 109, 116, 117 i 140 oraz Przykł. 35 (2). Niechaj $(V^{(\alpha)}, (\cdot| \cdot)_{(\alpha)})$, $\alpha \in \{1, 2\}$ będą dwiema przestrzeniami unitarnymi nad ciałem $\mathbb{K}$ i niech $\chi \in \text{Hom}_{\mathbb{K}}(V^{(1)}, V^{(2)})$ będzie odwzorowaniem $\mathbb{K}$ -liniowym między nimi. **Odwzorowanie hermitowsko sprzężone do χ** to odwzorowanie $\chi^\dagger \in \text{Hom}_{\mathbb{K}}(V^{(2)}, V^{(1)})$ o własności

$$\forall (v_1, v_2) \in V^{(1)} \times V^{(2)} : (\chi^\dagger(v_2)|v_1)_{(1)} = (v_2|\chi(v_1))_{(2)} .$$

Odwzorowanie półliniowe

$$\text{Hom}_{\mathbb{K}}(V^{(1)}, V^{(2)}) \longrightarrow \text{Hom}_{\mathbb{K}}(V^{(2)}, V^{(1)}) : \chi \longmapsto \chi^\dagger$$

nazywamy **sprzężeniem hermitowskim**. $\blacktriangle$

Definicja odwzorowania sprzężonego nie przesądza o jego istnieniu ani jednoznaczności. Sytuacja ta zmienia się radykalnie w przypadku skończenia wymiarowym.

STWIERDZENIE 199. Przyjmijmy notację Def. 11, 13, 14, 18, 21, 32, 35, 61, 63, 65, 105, 106, 107, 108, 109, 116, 117 i 140 oraz Przykł. 35 (2). Niechaj $(V^{(\alpha)}, (\cdot| \cdot)_{(\alpha)})$, $\alpha \in \{1, 2\}$ będą dwiema skończenie wymiarowymi przestrzeniami unitarnymi nad ciałem $\mathbb{K}$ i niech $\chi \in \text{Hom}_{\mathbb{K}}(V^{(1)}, V^{(2)})$ będzie dowolnym odwzorowaniem $\mathbb{K}$ -liniowym między nimi. Istnieje dokładnie jedno odwzorowanie hermitowsko sprzężone do χ . $\blacksquare$

Dowód: Jednoznaczność określenia $\chi^\dagger$ jest oczywista, a przy tym łatwo sprawdzamy, że odwzorowanie

$$\chi^\dagger := \mathcal{R}_{V^{(1)}} \circ \chi^* \circ \mathcal{R}_{V^{(2)}}^{-1}$$

spełnia warunek definiujący. Istotnie, korzystając z półoraliniowości $(\cdot| \cdot)_{(\alpha)}$ oraz z definicji odwzorowania sprzężonego, liczymy – dla dowolnych $v_\alpha \in V^{(\alpha)}$, $\alpha \in \{1, 2\}$ –

$$\begin{aligned} (\chi^\dagger(v_2)|v_1)_{(1)} &\equiv (\mathcal{R}_{V^{(1)}} \circ \chi^* \circ \mathcal{R}_{V^{(2)}}^{-1}(v_2)|v_1)_{(1)} = \overline{(v_1|\mathcal{R}_{V^{(1)}} \circ \chi^* \circ \mathcal{R}_{V^{(2)}}^{-1}(v_2))_{(1)}} \\ &= \overline{\langle \mathcal{R}_{V^{(1)}}^{-1}(\mathcal{R}_{V^{(1)}} \circ \chi^* \circ \mathcal{R}_{V^{(2)}}^{-1}(v_2)), v_1 \rangle_{(1)}} = \overline{\langle \chi^*(\mathcal{R}_{V^{(2)}}^{-1}(v_2)), v_1 \rangle_{(1)}} \\ &= \overline{\langle \mathcal{R}_{V^{(2)}}^{-1}(v_2), \chi(v_1) \rangle_{(2)}} = \overline{(\chi(v_1)|v_2)_{(2)}} = (v_2|\chi(v_1))_{(2)} . \end{aligned}$$

□

Podstawowe (i oczywiste, a dowodzone podobnie jak Stw. 131) własności operacji sprzężenia hermitowskiego opisuje

STWIERDZENIE 200. *Przyjmijmy notację Def. 11, 13, 14, 18, 21, 32, 35, 61, 63, 65, 105, 106, 107, 108, 109, 116, 117, 140 i 142 oraz Przykł. 35 (2). Niechaj $(V^{(\alpha)}, (\cdot|\cdot)_{(\alpha)})$, $\alpha \in \{1, 2, 3\}$ oraz $(V, (\cdot|\cdot))$ będą skończone wymiarowymi przestrzeniami unitarnymi. Sprzężenie hermitowskie jest inwolutywnym i antymultiplikatywnym odwzorowaniem półliniowym, tj. dla dowolnych $\chi, \chi_1, \chi_2 \in \text{Hom}_{\mathbb{K}}(V^{(1)}, V^{(2)})$ i $\chi_3 \in \text{Hom}_{\mathbb{K}}(V^{(2)}, V^{(3)})$ oraz $\lambda \in \mathbb{K}$ spełnione są tożsamości*

$$(\chi^\dagger)^\dagger = \chi, \quad (\chi_3 \circ \chi_1)^\dagger = \chi_1^\dagger \circ \chi_3^\dagger,$$

$$(\chi_1 + \chi_2)^\dagger = \chi_1^\dagger + \chi_2^\dagger, \quad (\lambda \triangleright \chi)^\dagger = \bar{\lambda} \triangleright \chi^\dagger,$$

a ponadto (ilekroć istnieje χ^{-1})

$$\text{id}_V^\dagger = \text{id}_V, \quad (\chi^{-1})^\dagger = (\chi^\dagger)^{-1}.$$

■

Bez trudu dowodzimy też

STWIERDZENIE 201. *W notacji Def. 11, 13, 14, 18, 21, 32, 35, 36, 61, 63, 64, 65, 95, 98, 105, 106, 107, 108, 109, 111, 116, 117, 140 i 142 oraz Przykł. 34 (2) i 35 (2)*

- (i) $\text{Ker } \chi^\dagger = (\text{Im } \chi)^{\perp(2)};$
- (ii) $\text{Im } \chi^\dagger = (\text{Ker } \chi)^{\perp(1)}.$

■

Dowód:

$$\text{Ad (i)} \quad v_2 \in \text{Ker } \chi^\dagger \iff \forall_{v_1 \in V^{(1)}} : 0_{\mathbb{K}} = (\chi^\dagger(v_2)|v_1)_{(1)} = (v_2|\chi(v_1))_{(2)} \iff v_2 \perp_{(2)} \text{Im } \chi.$$

Ad (ii) Wobec Stw. 196 (patrz: punkt (iv)) udowodniona powyżej tożsamość (i) implikuje

$$\text{Im } \chi^\dagger = ((\text{Im } \chi^\dagger)^{\perp(1)})^{\perp(1)} = (\text{Ker } (\chi^\dagger)^\dagger)^{\perp(1)} = (\text{Ker } \chi)^{\perp(1)}$$

□

W dalszej części wykładu skupimy uwagę na przypadku $V^{(1)} = V^{(2)}$, tj. będziemy rozpatrywać endomorfizmy przestrzeni unitarnej.

Wprowadzenie operacji sprzężenia hermitowskiego pozwala wyróżnić kilka istotnych (z punktu widzenia zastosowań, przede wszystkim tych fizycznych) typów endomorfizmów przestrzeni unitarnych.

DEFINICJA 143. Przyjmijmy notację Def. 11, 13, 14, 18, 21, 32, 35, 61, 63, 65, 105, 106, 107, 108, 109, 116, 117, 140 i 142 oraz Przykł. 35 (2). Niechaj $(V, (\cdot|\cdot))$ będzie przestrzenią unitarną nad ciałem $\mathbb{K}$. Endomorfizm $\chi \in \text{End}_{\mathbb{K}}(V)$ nazywamy

(N) **normalnym**, gdy $\chi^\dagger \circ \chi = \chi \circ \chi^\dagger$;

- (H) **samosprężonym** (lub **hermitowskim**), gdy $\chi^\dagger = \chi$ (w przypadku $\mathbb{K} = \mathbb{R}$ mówimy o endomorfizmie **symetrycznym**);
- (aH) **skośnie hermitowskim** (lub **antyhermitowskim**), gdy $\chi^\dagger = -\chi$ (w przypadku $\mathbb{K} = \mathbb{R}$ mówimy o endomorfizmie **skośnie symetrycznym** (lub **antysymetrycznym**));
- (I) **izometrycznym** (lub **izometrią**), gdy $\chi^\dagger \circ \chi = \text{id}_V$, przy czym jeśli $\dim_{\mathbb{K}} V < \infty$, to każda izometria jest endomorfizmem unitarnym (wzgl. ortogonalnym, gdy $\mathbb{K} = \mathbb{R}$) i odwrotnie, tj. spełnione są warunki

$$\chi^\dagger \circ \chi = \text{id}_V \iff \chi^\dagger \circ \chi = \text{id}_V = \chi \circ \chi^\dagger.$$

Definiujemy też endomorfizm

- (D) **dodatni** jako taki, który spełnia warunek $\forall_{v \in V} : (v|\chi(v)) \in \mathbb{R}_{\geq 0}$.

▲

Na marginesie prowadzonych tu rozważań warto zwrócić uwagę na naturalną strukturę algebraiczną obecną na zbiorach endomorfizmów izometrycznych oraz (skośnie) hermitowskich.

STWIERDZENIE 202. *Przyjmijmy notację Def. 11, 13, 14, 18, 21, 32, 35, 61, 63, 65, 105, 106, 107, 108, 109, 116, 117, 140, 142 i 143 oraz Przykł. 35 (2). Izometrie przestrzeni unitarnej V tworzą grupę, tj.*

$$\forall_{\chi_1, \chi_2 \in \text{End}_{\mathbb{K}}(V)} : (\chi_1^\dagger \circ \chi_1 = \text{id}_V = \chi_2^\dagger \circ \chi_2 \implies (\chi_1 \circ \chi_2)^\dagger \circ (\chi_1 \circ \chi_2) = \text{id}_V)$$

oraz $\text{id}_V^\dagger \circ \text{id}_V = \text{id}_V$.

Endomorfizmy hermitowskie i skośnie hermitowskie tejże przestrzeni tworzą zbiór zamknięty względem komutatora

$$[\chi_1, \chi_2]_- := \chi_1 \circ \chi_2 - \chi_2 \circ \chi_1$$

i – odpowiednio – antykomutatora

$$[\chi_1, \chi_2]_+ := \chi_1 \circ \chi_2 + \chi_2 \circ \chi_1,$$

tj.

$$\forall_{\chi_1, \chi_2 \in \text{End}_{\mathbb{K}}(V)} : ((\chi_1^\dagger = \pm \chi_1 \wedge \chi_2^\dagger = \pm \chi_2) \implies [\chi_1, \chi_2]_\mp^\dagger = \pm [\chi_1, \chi_2]_\mp).$$

■

Te pierwsze pojawiają się w przyszłych zastosowaniach jako grupy transformacji unitarnych (np. transformacje ewolucji hamiltonowskiej lub symetrii) przestrzeni stanów układów kwantowych, te drugie zaś – jako algebry endomorfizmów (skośnie) hermitowskich (np. algebry obserwabli kwantowych).

Zauważmy też, że endomorfizmy dodatnie pozostają w prostej relacji z endomorfizmami samosprężonymi.

STWIERDZENIE 203. *Każdy endomorfizm dodatni skończenie wymiarowej zespolonej przestrzeni wektorowej jest samosprężony.*

■

Dowód: Niechaj $(V, (\cdot|\cdot))$ będzie przestrzenią unitarną i niech χ będzie dowolnym jej endomorfizmem dodatnim. Odwzorowanie

$$\Phi_\chi : V^{\times 2} \longrightarrow \mathbb{C} : (v, w) \longmapsto (v|\chi(w))$$

jest formą półtoraliniową, możemy zatem odnieść do niego tezę Stw. 149 (patrz: punkt (ii)). Stwierdzamy więc, że

$$(v|\chi(w)) = \sum_{k=0}^3 i^k \cdot (v +_V i^k \triangleright w|\chi(v +_V i^k \triangleright w)) ,$$

i na tej podstawie obliczamy, przywołując definicję sprzężenia hermitowskiego i endomorfizmu dodatniego,

$$\begin{aligned} (v|\chi^\dagger(w)) &= \overline{(\chi^\dagger(w)|v)} = \overline{(w|\chi(v))} = \sum_{k=0}^3 (-1)^k \cdot i^k \cdot \overline{(w +_V i^k \triangleright v|\chi(w +_V i^k \triangleright v))} \\ &= \sum_{k=0}^3 (-1)^k \cdot i^k \cdot (w +_V i^k \triangleright v|\chi(w +_V i^k \triangleright v)) \\ &= \sum_{k \in \{0,2\}} i^k \cdot (i^k \triangleright (i^k \triangleright w +_V v)|i^k \triangleright \chi(i^k \triangleright w +_V v)) \\ &\quad - \sum_{k \in \{1,3\}} i^k \cdot (i^k \triangleright (i^{k+2} \triangleright w +_V v)|i^k \triangleright \chi(i^{k+2} \triangleright w +_V v)) \\ &= \sum_{k \in \{0,2\}} i^k \cdot (v +_V i^k \triangleright w|\chi(v +_V i^k \triangleright w)) \\ &\quad - \sum_{k \in \{1,3\}} i^k \cdot (v +_V i^{k+2} \triangleright w|\chi(v +_V i^{k+2} \triangleright w)) \\ &\equiv \sum_{k \in \{0,2\}} i^k \cdot (v +_V i^k \triangleright w|\chi(v +_V i^k \triangleright w)) \\ &\quad + \sum_{k \in \{1,3\}} i^{k+2} \cdot (v +_V i^{k+2} \triangleright w|\chi(v +_V i^{k+2} \triangleright w)) \\ &\equiv \sum_{k \in \{0,2\}} i^k \cdot (v +_V i^k \triangleright w|\chi(v +_V i^k \triangleright w)) \\ &\quad + \sum_{k \in \{1,3\}} i^k \cdot (v +_V i^k \triangleright w|\chi(v +_V i^k \triangleright w)) \\ &= (v|\chi(w)) . \end{aligned}$$

□

Warunki definiujące poszczególne typy endomorfizmów narzucają silne ograniczenia na ich widma, o czym przekonuje

STWIERDZENIE 204. *Przyjmijmy notację Def. 67, 11, 13, 14, 18, 21, 23, 24, 32, 35, 61, 63, 64, 65, 105, 106, 107, 108, 109, 116, 117, 124, 140, 142 i 143, Stw. 65 i 171 oraz Przykł. 35 (2). Niechaj $(V, (\cdot|\cdot))$ będzie skończeniem wymiarową przestrzeni unitarną nad ciałem $\mathbb{K}$ i niech $\chi \in \text{End}_{\mathbb{K}}(V)$ będzie jej endomorfizmem. Wówczas*

- (i) *jeśli χ jest samosprzężony, to $\text{Sp } \chi \subset \mathbb{R}$, jeśli zaś skośnie hermitowski, to $\text{Sp } \chi \subset i\mathbb{R}$;*
- (ii) *jeśli χ jest dodatni, to $\text{Sp } \chi \subset \mathbb{R}_{\geq 0}$;*
- (iii) *jeśli χ jest izometryczny, to $\text{Sp } \chi \subset \text{U}(1)$.*

■

Dowód: Niech $\chi(v) = \lambda \triangleright v$ dla pewnych $\lambda \in \text{Sp } \chi$ oraz $v \in V \setminus \{0_V\}$, a wtedy

Ad (i) $\overline{\lambda} \cdot \|v\|^2 = (v|\chi(v)) = (\chi^\dagger(v)|v) = (\chi(v)|v) = \lambda \cdot \|v\|^2$, więc też $\overline{\lambda} = \lambda$;

Ad (ii) $\lambda \cdot \|v\|^2 = (\chi(v)|v) = \overline{(v|\chi(v))} \in \mathbb{R}_{\geq 0}$, a zatem także $\lambda \in \mathbb{R}_{\geq 0}$;

Ad (iii) $|\lambda|^2 \cdot \|v\|^2 = (\chi(v)|\chi(v)) = \|v\|^2$, czyli $|\lambda| = 1$.

□

Powyższe stwierdzenie rodzi naturalne pytanie o prawdziwość implikacji odwrotnych. Odpowiedzi na nie dostarczy analiza widmowa endomorfizmów normalnych na zespolonych i rzeczywistych przestrzeniach unitarnych, którą zajmujemy się w dalszej części wykładu. Tytułem przygotowania poddamy teraz bardziej szczegółowej analizie pojęcie endomorfizmu normalnego, a następnie wprowadzimy konstrukcje pomocnicze, które pozwolą nam bardziej precyzyjnie opisać jego strukturę.

STWIERDZENIE 205. *Przyjmijmy notację Def. 11, 13, 14, 18, 21, 32, 35, 36, 61, 63, 64, 65, 95, 98, 105, 106, 107, 108, 109, 111, 116, 117, 131, 140, 141, 142 i 143 oraz Przykł. 34 (2) i 35 (2). Niechaj $(V, (\cdot|\cdot))$ będzie skończone wymiarową przestrzenią unitarną nad ciałem $\mathbb{C}$. Endomorfizm $\chi \in \text{End}_{\mathbb{K}}(V)$ jest normalny wtedy i tylko wtedy, gdy spełnia warunek*

$$(9.13) \quad \forall_{v \in V} : \|\chi^\dagger(v)\| = \|\chi(v)\|,$$

a wtedy

- (i) $\text{Ker } \chi^\dagger = \text{Ker } \chi$;
- (ii) $v \in \text{Ker } \chi_\lambda \implies v \in \text{Ker } \chi_\lambda^\dagger$;
- (iii) $\text{Ker } \chi = (\text{Im } \chi)^\perp$.

■

Dowód: Zaczniemy od wykazania prawdziwości równoważnego opisu endomorfizmu normalnego.

$$\Rightarrow \|\chi(v)\|^2 = (\chi(v)|\chi(v)) = (\chi^\dagger \circ \chi(v)|v) = (\chi \circ \chi^\dagger(v)|v) = \overline{(v|\chi \circ \chi^\dagger(v))} = \overline{(\chi^\dagger(v)|\chi^\dagger(v))} = \|\chi^\dagger(v)\|^2.$$

$\Leftarrow$ Rozpatrzmy formy półtoraliniowe

$$\Phi_1 : V^{\times 2} \longrightarrow \mathbb{K} : (v, w) \longmapsto (v|\chi^\dagger \circ \chi(w)),$$

$$\Phi_2 : V^{\times 2} \longrightarrow \mathbb{K} : (v, w) \longmapsto (v|\chi \circ \chi^\dagger(w)).$$

Przywołując Stw. 149 (patrz: punkt (ii)), konstatujemy, że obie one są w pełni określone przez wartości przyjmowane na przekątnej kwadratu kartezjańskiego $V \times V$, tam jednak – na mocy Stw. 200 i udowodnionej wcześniej równości (9.13) – obie formy pokrywają się,

$$\begin{aligned} \Phi_1(v, v) &= (v|\chi^\dagger \circ \chi(v)) = ((\chi^\dagger)^\dagger(v)|\chi(v)) = (\chi(v)|\chi(v)) = \|\chi(v)\|^2 = \|\chi^\dagger(v)\|^2 \\ &= (\chi^\dagger(v)|\chi^\dagger(v)) = (v|\chi \circ \chi^\dagger(v)) = \Phi_2(v, v), \end{aligned}$$

skąd też

$$(v|(\chi^\dagger \circ \chi - \chi \circ \chi^\dagger)(w)) \equiv \Phi_1(v, w) - \Phi_2(v, w)$$

$$= \frac{1}{4} \sum_{k=0}^3 i^k \cdot (\Phi_1 - \Phi_2)(v +_V i^k \triangleright w, v +_V i^k \triangleright w) = 0.$$

Wobec dowolności wektorów v i w stwierdzamy na tej podstawie tożsamość

$$\chi^\dagger \circ \chi - \chi \circ \chi^\dagger = 0.$$

Następnie sprawdzamy wymienione w treści stwierdzenia konsekwencje normalności χ .

Ad (i) W świetle Stw. 193 i na mocy wcześniej udowodnionej równoważności zachodzi $v \in \text{Ker } \chi \iff \|\chi(v)\| = 0 \iff \|\chi^\dagger(v)\| = 0 \iff v \in \text{Ker } \chi^\dagger$.

Ad (ii) Zauważmy, że dla dowolnego $\lambda \in \mathbb{C}$ zachodzi $(\ell_\lambda)^\dagger = \ell_{\bar{\lambda}}$, gdyż – dla dowolnych $v, w \in V$ –

$$((\ell_\lambda)^\dagger(v)|w) = (v|\ell_\lambda(w)) = (v|\lambda \triangleright w) = \bar{\lambda} \cdot (v|w) = (\bar{\lambda} \triangleright v|w).$$

W takim razie prawdziwą jest równość $(\chi_\lambda)^\dagger = \chi^\dagger - \ell_{\bar{\lambda}} = \chi_{\bar{\lambda}}^\dagger$, która implikuje normalność endomorfizmu χ_λ ,

$$\begin{aligned} (\chi_\lambda)^\dagger \circ \chi_\lambda &= \chi_{\bar{\lambda}}^\dagger \circ \chi_\lambda = \chi^\dagger \circ \chi - \chi^\dagger \circ \ell_{\bar{\lambda}} - \ell_{\bar{\lambda}} \circ \chi + \ell_{|\lambda|^2} = \chi \circ \chi^\dagger - \ell_{\bar{\lambda}} \circ \chi^\dagger - \chi \circ \ell_{\bar{\lambda}} + \ell_{|\lambda|^2} \\ &= \chi_\lambda \circ (\chi_\lambda)^\dagger. \end{aligned}$$

Punkt (i) odniesiony do χ_λ daje nam pożądaną tezę, oto bowiem

$$v \in \text{Ker } \chi_\lambda \iff v \in \text{Ker } \chi_{\bar{\lambda}}^\dagger.$$

Ad (iii) Prosty wniosek z połączenia punktów (i) stwierdzenia dowodzonego i Stw. 201. □

Punktem wyjścia do analizy widmowej endomorfizmu normalnego jest zbadanie rozkładu jego dziedziny na sumę prostą przestrzeni pierwiastkowych tegoż endomorfizmu. W obecności struktury unitarnej pojęcie sumy prostej zastępuje subtelniejsze pojęcie sumy ortogonalnej, wprowadzone w Def. 112. W ślad za tym idzie sublimacja stowarzyszonego pojęcia operatora rzutowego, którą omawiamy poniżej.

DEFINICJA 144. Przyjmijmy notację Def. 11, 13, 14, 18, 21, 32, 35, 36, 61, 63, 64, 65, 95, 98, 105, 106, 107, 108, 109, 111, 116, 117 i 140 oraz Przykł. 34 (2) i 35 (2). Niechaj $(V, (\cdot|\cdot))$ będzie przestrzenią unitarną nad ciałem $\mathbb{K}$. **Rzut prostopadły** (lub **ortogonalny**) o dziedzinie V to endomorfizm $\pi \in \text{End}_{\mathbb{K}}(V)$ o własnościach

$$\pi \circ \pi = \pi, \quad \text{Ker } \pi = (\text{Im } \pi)^\perp,$$

tj. rzut, dla którego rozkład dziedziny na sumę prostą jądra i obrazu jest rozkładem ortogonalnym. ▲

Równoważnej charakterystyki rzutów prostopadłych dostarcza

STWIERDZENIE 206. Przyjmijmy notację Def. 11, 13, 14, 18, 21, 32, 35, 36, 61, 63, 64, 65, 95, 98, 105, 106, 107, 108, 109, 111, 116, 117, 140, 142 i 144 oraz Przykł. 34 (2) i 35 (2). Niechaj $(V, (\cdot|\cdot))$ będzie skończenie wymiarową

przestrzeni unitarną nad ciałem $\mathbb{K}$. Rzut $\pi \in \text{End}_{\mathbb{K}}(V)$ jest prostopadły wtedy i tylko wtedy, gdy jest endomorfizmem samosprężonym, tj. spełnia warunek

$$\pi^\dagger = \pi.$$

■

Dowód:

- $\Rightarrow$ Wybierzmy (dowolnie) wektory $v, w \in V$. Jako że $(\text{id}_V - \pi)(v) \in \text{Ker } \pi$ i $\pi(w) \in \text{Im } \pi$, przeto $0_{\mathbb{K}} = ((\text{id}_V - \pi)(v)|\pi(w)) = (\pi^\dagger \circ (\text{id}_V - \pi)(v)|w)$, co wobec dowolności v i w implikuje równość $\pi^\dagger = \pi^\dagger \circ \pi$, ta zaś daje nam – na mocy Stw. 200 – tożsamość $\pi = (\pi^\dagger)^\dagger = (\pi^\dagger \circ \pi)^\dagger = \pi^\dagger \circ (\pi^\dagger)^\dagger = \pi^\dagger \circ \pi = \pi^\dagger$.
- $\Leftarrow$ Wobec równości $\pi^\dagger \circ (\text{id}_V - \pi) = \pi^\dagger - \pi^\dagger \circ \pi = \pi - \pi \circ \pi = \pi - \pi = 0$ i posilkując się Stw. 89 (patrz: punkt (ii)), stwierdzamy, że $\text{Im } \pi = (\text{Ker } \pi)^\perp = (\text{Im } (\text{id}_V - \pi))^\perp$, oto bowiem – dla dowolnych $v, w \in V$ – zachodzi równość $((\text{id}_V - \pi)(v)|\pi(w)) = (\pi^\dagger \circ (\text{id}_V - \pi)(v)|w) = (0(v)|w) = (0_V|w) = 0_{\mathbb{K}}$, a nadto $V = \text{Ker } \pi \oplus \text{Im } \pi$.

□

Możemy już teraz precyzyjnie wysłowić fundamentalne

TWIERDZENIE 9.16. (Widmowe dla endomorfizmu normalnego zespolonej przestrzeni wektorowej). *Przyjmijmy notację Def. 67, 11, 13, 14, 18, 21, 23, 24, 25, 26, 27, 28, 32, 35, 36, 61, 63, 64, 65, 75, 78, 79, 80, 88, 95, 98, 105, 106, 107, 108, 109, 111, 112, 116, 117, 124, 126, 129, 131, 140, 142, 143 i 144, Stw. 65, 171, 176 i 178 oraz Przykł. 34 (2) i 35 (2). Niechaj $(V, (\cdot|\cdot))$ będzie skończone wymiarową przestrzenią unitarną nad ciałem $\mathbb{C}$ i niech $\chi \in \text{End}_{\mathbb{C}}(V)$ będzie jej endomorfizmem o widmie $\{\lambda_i\}_{i \in \overline{1, n}} \subset \mathbb{C}$, przy czym zakładamy, że liczby λ_i są parami różne. Niech też $\Pi := \{\pi_i\}_{i \in \overline{1, n}}$ będzie rodziną rzutów na przestrzenie własne $V_1(\lambda_i; \pi_i) = \text{Im } \pi_i$ endomorfizmu χ . Jeśli χ jest normalny, to Π jest zupełną rodziną komplementarnych rzutów ortogonalnych, tj. spełnia warunki*

$$\pi_i \circ \pi_j = \delta_{i,j}^{\mathbb{K}} \triangleright \pi_i, \quad \sum_{i=1}^n \pi_i = \text{id}_V, \quad \pi^\dagger = \pi,$$

czyli przestrzeń V ma rozkład

$$V = \bigoplus_{i=1}^n V_1(\lambda_i; \chi)$$

i ortonormalną bazę własną χ , a ponadto endomorfizm χ ma rozkład widmowy

$$\chi = \sum_{i=1}^n \ell_{\lambda_i} \circ \pi_i,$$

czyli też dla dowolnej funkcji f analitycznej na pewnym otoczeniu $\text{Sp } \chi$ zachodzi równość

$$f(\chi) = \sum_{i=1}^n \ell_{F_{\varrho_f}(\lambda_i)} \circ \pi_i.$$

■

Dowód: W świetle Stw. 9.10 przestrzeń V ma rozkład

$$V = \bigoplus_{i=1}^n V(\lambda_i; \chi).$$

Musimy zatem wykazać, że dla każdej wartości własnej zachodzi równość $V(\lambda_i; \chi) = V_1(\lambda_i; \chi)$. Pomocnym okazuje się tutaj poniższy

LEMAT 9.17. *Przyjmijmy notację Def. 67, 11, 13, 14, 18, 21, 23, 24, 32, 35, 61, 63, 64, 65, 105, 106, 107, 108, 109, 116, 117, 124, 126, 131, 140, 142 i 143, Stw. 65 i 171 oraz Przykł. 35 (2). Niechaj $(V, (\cdot|\cdot))$ będzie skończone wymiarową przestrzenią unitarną nad ciałem $\mathbb{K}$ i niech χ będzie jej endomorfizmem. Jeśli χ jest normalny, to dla każdej wartości własnej $\lambda \in \text{Sp } \chi$ spełniona jest równość $V(\lambda; \chi) = V_1(\lambda; \chi)$.*

■

Dowód: Zauważmy, że

$$\forall_{v \in V} \forall_{n \in \mathbb{N}} : (\chi^n(v) = 0_V \implies \chi(v) = 0_V),$$

czego dowodzimy indukcyjnie. Oto dla $n = 2$ (pierwszy nietrywialny przypadek) otrzymujemy następujący ciąg implikacji, zapisanych dla dowolnego $v \in V$ i $w := \chi(v)$ a wykorzystujących Stw. 205: $\chi^2(v) = 0_V \iff 0_{\mathbb{K}} = \|\chi^2(v)\|^2 \equiv \|\chi(w)\|^2 = \|\chi^\dagger(w)\|^2 \equiv \|\chi^\dagger \circ \chi(v)\|^2 \iff \chi^\dagger \circ \chi(v) = 0_V \implies 0_{\mathbb{K}} = (\chi^\dagger \circ \chi(v)|v) = (\chi(v)|\chi(v)) = \|\chi(v)\|^2 \iff \chi(v) = 0_V$. Załóżmy zatem, że teza lematu jest słuszna dla wszystkich $n \in \overline{0, N-1}$, a wtedy $\chi^N(v) = 0_V \iff \chi^2(\chi^{N-2}(v)) = 0_V \implies 0_V = \chi(\chi^{N-2}(v)) = \chi^{N-1}(v)$, to jednak na mocy założenia indukcyjnego oznacza, że $\chi(v) = 0_V$.

Odnosząc powyższą obserwację do endomorfizmu χ_λ , którego normalność została wykazana w dowodzie Stw. 205, otrzymujemy tezę lematu. □

Na mocy lematu możemy zatem przepisać wcześniejszy rozkład V w postaci

$$V = \bigoplus_{i=1}^n V_1(\lambda_i; \chi).$$

Pozostaje dowieść, że powyższa suma prosta jest ortogonalna. Niech $v^i \in V_1(\lambda_i; \chi)$, $i \in \overline{1, n}$. Dla pary indeksów $i \neq j$ ze zbioru $\overline{1, n}$ otrzymujemy – wobec Stw. 205 (ii) – równość

$$\lambda_i \cdot (v^i|v^j) = (\chi(v^i)|v^j) = \overline{(v^j|\chi(v^i))} = \overline{(\chi^\dagger(v^j)|v^i)} = \overline{\lambda_j \cdot (v^j|v^i)} = \lambda_j \cdot (v^i|v^j),$$

a dalej

$$(\lambda_i - \lambda_j) \cdot (v^i|v^j) = 0,$$

czyli też – na mocy założenia $\lambda_i \neq \lambda_j$ – pożądaną tożsamość

$$(v^i|v^j) = 0.$$

Jest zatem

$$V = \bigoplus_{i=1}^n V_1(\lambda_i; \chi),$$

co w konsekwencji Stw. 88 (w połączeniu z okazaną wyżej ortogonalnością rozkładu V) jest równoznaczne z istnieniem zupełnej rodziny komplementarnych rzutów ortogonalnych na podprzestrzeń własną χ . Konkatenacja (dowolnych) baz ortonormalnych tychże przestrzeni (których istnienie gwarantuje Stw. 158) jest pożądaną ortonormalną bazą własną χ przestrzeni V . Pozostała część tezy stwierdzenia stanowi teraz natychmiastową konsekwencję równości $\chi|_{V_1(\lambda_i; \chi)} = \ell_{\lambda_i}$, $i \in \overline{1, n}$ oraz Stw. 129 i 172. $\square$

Jako prosty wniosek z twierdzenia widmowego otrzymujemy

STWIERDZENIE 207. *Def. 67, 11, 13, 14, 18, 21, 23, 24, 32, 35, 36, 61, 63, 64, 65, 95, 98, 105, 106, 107, 108, 109, 111, 116, 117, 124, 140, 142, 143 i 144, Stw. 65 i 171 oraz Przykł. 34 (2) i 35 (2). Niechaj $\chi \in \text{End}_{\mathbb{C}}(V)$ będzie endomorfizmem normalnym. Wówczas*

- (i) *jeśli $\text{Sp } \chi \subset \mathbb{R}$, to χ jest samosprężony, jeśli zaś $\text{Sp } \chi \subset i\mathbb{R}$, to χ jest skośnie hermitowski;*
- (ii) *jeśli $\text{Sp } \chi \subset \mathbb{R}_{\geq 0}$, to χ jest dodatni;*
- (iii) *jeśli $\text{Sp } \chi \subset \text{U}(1)$, to χ jest unitarny;*
- (iv) *jeśli $\text{Sp } \chi \subset \{0, 1\}$, to χ jest rzutem ortogonalnym.*

■

Dowód: Niechaj $\{\lambda_i\}_{i \in \overline{1, n}} \subset \mathbb{C}$ będzie zbiorem (parami różnych) wartości własnych endomorfizmu χ . Na mocy Tw. 9.16 endomorfizm χ ma rozkład widmowy

$$\chi = \sum_{i=1}^n \ell_{\lambda_i} \circ \pi_i, \quad \text{Im } \pi_i = V_1(\lambda_i; \chi),$$

przeto – wobec ortogonalności rzutów π_i i w świetle Stw. 200 – jest

$$\chi^\dagger = \sum_{i=1}^n \pi_i^\dagger \circ \ell_{\lambda_i}^\dagger = \sum_{i=1}^n \pi_i \circ \ell_{\overline{\lambda_i}} = \sum_{i=1}^n \ell_{\overline{\lambda_i}} \circ \pi_i.$$

Tak przygotowani możemy przejść do dowodu zasadniczego

Ad (i) $\chi^\dagger = \sum_{i=1}^n \ell_{\overline{\lambda_i}} \circ \pi_i = \sum_{i=1}^n \ell_{\lambda_i} \circ \pi_i = \chi$.

Ad (ii) Wykorzystując własności rodziny $\{\pi_i\}_{i \in \overline{1, n}}$, obliczamy

$$\begin{aligned} (v|\chi(v)) &= \left(v \left| \sum_{i=1}^n \lambda_i \triangleright \pi_i(v) \right. \right) = \sum_{i=1}^n \overline{\lambda_i} \cdot (v|\pi_i(v)) = \sum_{i=1}^n \lambda_i \cdot (v|\pi_i(v)) \\ &= \sum_{i=1}^n \lambda_i \cdot \left(\sum_{j=1}^n \pi_j(v) | \pi_i(v) \right) = \sum_{i,j=1}^n \lambda_i \cdot (\pi_j(v) | \pi_i(v)) \\ &= \sum_{i,j=1}^n \lambda_i \cdot (\pi_i^\dagger \circ \pi_j(v) | v) = \sum_{i,j=1}^n \lambda_i \cdot (\pi_i \circ \pi_j(v) | v) \\ &= \sum_{i,j=1}^n \lambda_i \cdot \delta_{i,j}^{\mathbb{C}} \cdot (\pi_i^\dagger \circ \pi_i(v) | v) = \sum_{i=1}^n \lambda_i \cdot (\pi_i(v) | \pi_i(v)) = \sum_{i=1}^n \lambda_i \cdot \|\pi_i(v)\|^2 \\ &\geq 0. \end{aligned}$$

- Ad (iii) $\chi^\dagger \circ \chi = \sum_{i=1}^n \ell_{\overline{\lambda_i}} \circ \pi_i \circ \sum_{j=1}^n \ell_{\lambda_j} \circ \pi_j = \sum_{i,j=1}^n \ell_{\overline{\lambda_i} \cdot \lambda_j} \circ \pi_i \circ \pi_j = \sum_{i,j=1}^n \ell_{\overline{\lambda_i} \cdot \lambda_j \cdot \delta_{i,j}^{\mathbb{C}}} \circ \pi_i = \sum_{i=1}^n \ell_{|\lambda_i|^2} \circ \pi_i = \sum_{i=1}^n \pi_i = \text{id}_V$. Analogiczny rachunek prowadzi do równości $\chi \circ \chi^\dagger = \text{id}_V$.
- Ad (iv) Wobec tożsamości $\chi = \ell_1 \circ \pi = \pi : V \rightarrow V_1(1; \chi)$ teza jest oczywista. $\square$

W przypadku $\mathbb{K} = \mathbb{R}$ udowodnione poprzednio twierdzenie widmowe nie jest prawdziwe, o czym można się łatwo przekonać wprost – oto np. endomorfizm $\mathbb{R}^2 \ni v \mapsto R_\theta(v)$, $\theta \in]0, 2\pi[$ ze str. 72 (tym razem traktujemy $\mathbb{R}^2$ jako przestrzeń $\mathbb{R}$ -liniową) jest normalny jako izometria naturalnej struktury euklidesowej na $\mathbb{R}^2$, zarazem jednak nie ma (niezerowych) wektorów własnych, co jest w sprzeczności z tezą Tw. 9.16. Okazuje się, że wystarczy ograniczyć się do endomorfizmów samosprzężonych, aby teza twierdzenia stała się na powrót prawdziwa. Mamy zatem

TWIERDZENIE 9.18. (Widmowe dla endomorfizmu samosprzężonego rzeczywistej przestrzeni wektorowej). *Przyjmijmy notację Def. 67, 11, 13, 14, 18, 21, 23, 24, 25, 26, 27, 28, 32, 35, 36, 61, 63, 64, 65, 75, 78, 79, 80, 88, 95, 98, 105, 106, 107, 108, 109, 111, 112, 116, 117, 124, 126, 129, 131, 140, 142, 143 i 144, Stw. 65, 171, 176 i 178 oraz Przykł. 34 (2) i 35 (2). Niechaj $(V, (\cdot|\cdot))$ będzie skończone wymiarową przestrzenią euklidesową nad ciałem $\mathbb{R}$ i niech $\chi \in \text{End}_{\mathbb{R}}(V)$ będzie jej endomorfizmem o widmie $\{\lambda_i\}_{i \in \overline{1,n}} \subset \mathbb{R}$, przy czym zakładamy, że liczby λ_i są parami różne. Niech też $\Pi := \{\pi_i\}_{i \in \overline{1,n}}$ będzie rodziną rzutów na przestrzenie własne $V_1(\lambda_i; \pi_i) = \text{Im } \pi_i$ endomorfizmu χ . Jeśli χ jest samosprzężony, to Π jest zupełną rodziną komplementarnych rzutów ortogonalnych, czyli przestrzeń V ma rozkład*

$$V = \bigoplus_{i=1}^n V_1(\lambda_i; \chi)$$

i ortonormalną bazę własną χ , a ponadto endomorfizm χ ma rozkład widmowy

$$\chi = \sum_{i=1}^n \ell_{\lambda_i} \circ \pi_i,$$

czyli też dla dowolnej rzeczywistej funkcji f analitycznej na pewnym otoczeniu $\text{Sp } \chi$ zachodzi równość

$$f(\chi) = \sum_{i=1}^n \ell_{F_{\text{eff}}(\lambda_i)} \circ \pi_i.$$

■

Dowód: Rozważmy kompleksyfikację $V^{\mathbb{C}}$ przestrzeni V i wybawszy bazę ortonormalną $\mathcal{B} = \{v^i\}_{i \in \overline{1,N}}$, $N := \dim_{\mathbb{R}} V$, której istnienie przewiduje Stw. 158, ustalmy w $V^{\mathbb{C}}$ bazę $\iota_V(\mathcal{B})$. Kładąc – dla dowolnych $\{\lambda_i\}_{i \in \overline{1,N}}, \{\mu_j\}_{j \in \overline{1,N}} \subset \mathbb{C}$ –

$$\left(\sum_{i=1}^N \lambda_i \triangleright \iota_V(v^i) \mid \sum_{j=1}^N \mu_j \triangleright \iota_V(v^j) \right)_{\mathbb{C}} := \sum_{i=1}^N \lambda_i \cdot \overline{\mu_i}$$

indukujemy na $V^{\mathbb{C}}$ strukturę przestrzeni unitarnej $(V^{\mathbb{C}}, (\cdot|\cdot)_{\mathbb{C}})$, względem której $\iota_V(\mathcal{B})$ jest bazą ortonormalną. Macierz $[\chi^{\mathbb{C}}]_{\iota_V(\mathcal{B})}^{\iota_V(\mathcal{B})} = [\chi]_{\mathcal{B}}^{\mathcal{B}}$ ma wszystkie wyrazy

rzeczywiste (wprost z konstrukcji), a przy tym jest symetryczna – istotnie, dla dowolnych $i, j \in \overline{1, N}$ otrzymujemy, na mocy Tw. 8.11,

$$[\chi]_{\mathcal{B}}^{\mathcal{B}}(j, i) \equiv \overline{[\chi]_{\mathcal{B}}^{\mathcal{B}}(j, i)} = (v^j | \chi(v^i)) = (\chi^\dagger(v^j) | v^i) = (\chi(v^j) | v^i) = [\chi]_{\mathcal{B}}^{\mathcal{B}}(i, j).$$

Jest ona zatem macierzą hermitowską, stąd zaś wniosek, że endomorfizm $\chi^{\mathbb{C}}$ jest samosprzężony, a zatem – w szczególności – normalny. Możemy przeto zastosować do niego Tw. 9.16, które pozwala zapisać

$$V^{\mathbb{C}} = \bigoplus_{\lambda \in \text{Sp } \chi^{\mathbb{C}}} V_1^{\mathbb{C}}(\lambda; \chi^{\mathbb{C}}).$$

Zauważmy także, że w świetle Stw. 177

$$\text{Sp } \chi^{\mathbb{C}} = \text{Sp } \chi.$$

Istotnie, w odwołaniu do Stw. 157 konstatujemy, że $\text{Sp } \chi^{\mathbb{C}} \subset \mathbb{R}$, a przy tym

$$\begin{aligned} F_{w_{\chi^{\mathbb{C}}}}(\lambda) &= \det(\chi^{\mathbb{C}} - \ell_{\lambda}) = \det_{(N)} \left([\chi^{\mathbb{C}}]_{\iota_V(\mathcal{B})}^{\iota_V(\mathcal{B})} - \lambda \triangleright_{(N)} \mathbf{1}_N \right) \\ &\equiv \det_{(N)} \left([\chi]_{\mathcal{B}}^{\mathcal{B}} - \lambda \triangleright_{(N)} \mathbf{1}_N \right) = F_{w_{\chi}}(\lambda). \end{aligned}$$

Jest zatem

$$V^{\mathbb{C}} = \bigoplus_{\lambda \in \text{Sp } \chi} V_1^{\mathbb{C}}(\lambda; \chi^{\mathbb{C}}),$$

a zatem także

$$\iota_V(V) \equiv \iota_V(V) \cap V^{\mathbb{C}} = \bigoplus_{\lambda \in \text{Sp } \chi} \iota_V(V) \cap V_1(\lambda; \chi^{\mathbb{C}}),$$

ponieważ jednak zachodzi relacja

$$\chi^{\mathbb{C}} \circ \iota_V = \iota_V \circ \chi,$$

a morfizm ι_V jest – jak orzeka Stw. 186 – injektywny, przeto

$$\begin{aligned} V &= (\iota_V|_{\iota_V(V)})^{-1}(\iota_V(V)) = \bigoplus_{\lambda \in \text{Sp } \chi} (\iota_V|_{\iota_V(V)})^{-1}(\iota_V(V) \cap V_1(\lambda; \chi^{\mathbb{C}})) \\ &= \bigoplus_{\lambda \in \text{Sp } \chi} V_1(\lambda; \chi). \end{aligned}$$

Bez trudu przekonujemy się przy tym, że suma w ostatnim wzorze jest ortogonalna, a to w sposób identyczny jak w dowodzie Tw. 9.16. Koniec końców otrzymujemy wynik

$$V = \bigoplus_{\lambda \in \text{Sp } \chi} V_1(\lambda; \chi),$$

równoznaczny z istnieniem zupełnej rodziny $\{\pi_{\lambda}\}_{\lambda \in \text{Sp } \chi}$ komplementarnych rzutów ortogonalnych π_{λ} na przestrzenie własne $V_1(\lambda; \chi)$. $\square$

9.11. Struktury afiniczne i kwadryki

* * *

Literatura uzupełniająca: Doskonałym sposobem na wzbogacenie i rozszerzenie zawartości merytorycznej tej części kursu jest lektura wstępnych rozdziałów traktatu Bourbakiego [Bou07a] i stosownych rozdziałów podręcznika Langa [Lan02].

Część 4

Epilegomena

Iloczyn tensorowy

Rozdział 11

Algebry Liego

Rozdział 12

Algebry Clifforda

Rozdział 13

Teoria kategorii

Rozdział 14

Elementy algebry homologicznej

Część 5

Konwencje

KONWENCJA 1. (Iloczyn kartezjański zbiorów) Mnożenie kartezjańskie zbiorów nie jest operacją łączną. W celu uniknięcia przeładowania zapisu formalnego niniejszego skryptu wskutek każdorazowego wypisywania w jawnej postaci naturalnych bijekcji pomiędzy wielokrotnymi iloczynami kartezjańskimi zbiorów różnie pogrupowanych (występującymi chociażby w diagramatycznym zapisie aksjomatyki struktur algebraicznych), np. $(X_1 \times X_2) \times X_3$ i $X_1 \times (X_2 \times X_3)$ dla trójki zbiorów X_1, X_2 i X_3 , będziemy opuszczać nawiasy określające schemat pogrupowania czynników, pisząc np. $X_1 \times X_2 \times X_3$. Pełna informacja o domyślnym schemacie pogrupowania (i ukrytej obecności stosownych bijekcji) będzie zawarta w strukturze odwzorowań o tak (niejednoznacznie) zadanej dziedzinie. I tak, np., dla odwzorowań $f_1 : X_1 \rightarrow X_4$ i $f_3 : X_3 \rightarrow X_5$ oraz $f_{i,i+1} : X_i \times X_{i+1} \rightarrow X_{i+5}$, $i \in \{1, 2\}$ skrócony zapis

$$X_4 \times X_7 \xleftarrow{f_1 \times f_{2,3}} X_1 \times X_2 \times X_3 \xrightarrow{f_{1,2} \times f_3} X_6 \times X_5$$

naależy odczytać jako

$$X_4 \times X_7 \xleftarrow{f_1 \times f_{2,3}} X_1 \times (X_2 \times X_3) \xrightarrow{\alpha_{1,2,3}} (X_1 \times X_2) \times X_3 \xrightarrow{f_{1,2} \times f_3} X_6 \times X_5,$$

przy czym utożsamienie $\alpha_{1,2,3}$ przyjmuje tu postać

$$\alpha_{1,2,3} : X_1 \times (X_2 \times X_3) \rightarrow (X_1 \times X_2) \times X_3 : (x_1, (x_2, x_3)) \mapsto ((x_1, x_2), x_3).$$

* * *

KONWENCJA 2. (Zapis odwzorowań)

- Odwzorowanie identycznościowe zbioru X w siebie zapiszemy jako

$$\text{id}_X : X \rightarrow X : x \mapsto x.$$

- Odwzorowanie zbioru X w siebie zapiszemy jako $f : X \rightarrow X$.
- Niechaj będą dane zbiory X_1, X_2, Y_1, Y_2 oraz odwzorowania $f_1 : X_1 \rightarrow Y_1$, $f_2 : X_2 \rightarrow Y_2$. Zapiszemy

$$f_1 \times f_2 : X_1 \times X_2 \rightarrow Y_1 \times Y_2 : (x_1, x_2) \mapsto (f_1(x_1), f_2(x_2)).$$

- Niechaj będą dane zbiory X, Y_1, Y_2 oraz odwzorowania $f_1 : X \rightarrow Y_1$, $f_2 : X \rightarrow Y_2$. Zapiszemy

$$(f_1, f_2) : X \rightarrow Y_1 \times Y_2 : x \mapsto (f_1(x), f_2(x)).$$

- W przypadku odwzorowania stałego $f : X \rightarrow Y : x \mapsto y_0$ zapiszemy $f \equiv y_0$.
- Transpozycję elementów zbioru X zapiszemy jako

$$\tau_X : X \times X \rightarrow X \times X : (x_1, x_2) \mapsto (x_2, x_1).$$

- Niechaj $S_1, S_2, \dots, S_N$ będą zbiorami. Kanoniczne odwzorowania rzutowe (zwane też rzutami kanonicznymi), określone na iloczynie kartezjańskim tych zbiorów i dla dowolnych indeksów $1 \leq i_1 < i_2 < \dots < i_n \leq N$, $n \in \overline{1, N}$, zapiszemy następująco

$$\text{pr}_{i_1, i_2, \dots, i_n} : \bigtimes_{i=1}^N S_i \rightarrow S_{i_1} \times S_{i_2} \times \dots \times S_{i_n} : (x_1, x_2, \dots, x_N) \mapsto (x_{i_1}, x_{i_2}, \dots, x_{i_n}).$$

* * *

KONWENCJA 3. (Diagramy przemienne) Niechaj A, B, C oraz D będą zbiorami i niech $\alpha : A \rightarrow B$, $\beta : B \rightarrow D$, $\gamma : A \rightarrow C$ oraz $\delta : C \rightarrow D$ będą odwzorowaniami pomiędzy tymi zbiorami. Diagram

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ \gamma \downarrow & & \downarrow \beta \\ C & \xrightarrow{\delta} & D \end{array}$$

nazywamy **przemiennym**, gdy zachodzi relacja

$$\beta \circ \alpha = \delta \circ \gamma.$$

W przypadku bardziej złożonym mówimy o diagramie przemienym, ilekroć każdy z zamkniętych konturów wewnątrz diagramu jest diagramem przemienym w powyższym sensie.

* * *

KONWENCJA 4. (Operacje wieloargumentowe na podzbiorach nośnika struktury algebraicznej) Niechaj S będzie zbiorem wyposażonym w operację n -argumentową $\phi_n : S^{\times n} \rightarrow S$ i niech $S_i \subset S$, $i \in \overline{1, n}$ będą podzbiorami S . Wówczas definiujemy zbiór

$$\phi_n(S_1, S_2, \dots, S_n) := \{ \phi_n(x_1, x_2, \dots, x_n) \mid \forall_{i \in \overline{1, n}} : x_i \in S_i \},$$

który będziemy nazywać **obrazem algebraicznym zbiorów** $(S_1, S_2, \dots, S_n)$ **względem operacji** ϕ_n . W szczególności możemy mówić o sumie algebraicznej podzbiorów zbioru z dodawaniem i iloczynie algebraicznym podzbiorów zbioru z mnożeniem.

* * *

PRZYKŁAD(Y) 50.

- (1) Niech S będzie zbiorem, na którym jest zadana operacja 2-argumentowa $\phi_2 := \cdot$ zwana mnożeniem. Wówczas możemy określić **iloczyn algebraiczny** dowolnych dwóch podzbiorów $S_1, S_2 \subset S$ w postaci

$$S_1 \cdot S_2 := \{ x \cdot y \mid (x, y) \in S_1 \times S_2 \}.$$

- (2) Analogicznie definiujemy **sumę algebraiczną** podzbiorów S , ilekroć na zbiorze tym jest zadana operacja 2-argumentowa $\phi_2 := +$ zwana dodawaniem,

$$S_1 + S_2 := \{ x + y \mid (x, y) \in S_1 \times S_2 \}.$$

- (3) Jeśli na S określona jest relacja 1-argumentowa $\phi_1 := -(\cdot)$ zwana braniem przeciwności, to możemy zdefiniować **przeciwność algebraiczną** dowolnego podzbioru $S_1 \subset S$ jako zbiór

$$-S_1 := \{ -s \mid s \in S_1 \}.$$

- (4) Analogicznie definiujemy **odwrotność algebraiczną** podzbioru S , zawsze gdy na zbiorze tym jest zadana operacja 1-argumentowa $\phi_1 := (\cdot)^{-1}$ zwana braniem odwrotności,

$$S_1^{-1} := \{ s^{-1} \mid s \in S_1 \}.$$

✓

Bibliografia

- [AA06] T. Andreescu and D. Andrica, *Complex numbers from A to ... Z*, Birkhäuser, 2006.
- [Arm88] M.A. Armstrong, *Groups and Symmetry*, Undergraduate Texts in Mathematics, Springer, 1988.
- [Bou06] N. Bourbaki, *Éléments de mathématique, Théorie des ensembles*, Springer, 2006.
- [Bou07a] ———, *Éléments de mathématique, Algèbre, chapitre 9*, Springer, 2007.
- [Bou07b] ———, *Éléments de mathématique, Algèbre, chapitres 1 à 3*, Springer, 2007.
- [Coh82] P.M. Cohn, *Algebra*, vol. 1, John Wiley & Sons, 1982.
- [Coh89] ———, *Algebra*, vol. 2, John Wiley & Sons, 1989.
- [Coh91] ———, *Algebra*, vol. 3, John Wiley & Sons, 1991.
- [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 prilozhenija. Tom 1: Geometrija poverkhnostej, grup preobrazovanij i polej*, Nauka, 1979.
- [DNF84] ———, *Sovremennaja geometrija: Metody i prilozhenija. Tom 3: Teorija gomologij*, Nauka, 1984.
- [KM76] K. Kuratowski and A. Mostowski, *Teoria mnogości*, Monografie Matematyczne, vol. XXVII, Państwowe Wydawnictwo Naukowe, 1976.
- [KT08] C. Kassel and V.G. Turaev, *Braid Groups*, Graduate Texts in Mathematics, vol. 247, Springer, 2008.
- [Lan02] S. Lang, *Algebra*, Graduate Texts in Mathematics, vol. 211, Springer, 2002.
- [Lea56] W.G. Leavitt, “Modules over rings of words”, Proc. AMS **7** (1956), 188–193.
- [Lea57] ———, “Modules without invariant basis number”, Proc. AMS **8** (1957), 322–328.
- [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.
- [ML71] S. Mac Lane, *Categories for the Working Mathematician*, Graduate Texts in Mathematics, vol. 5, Springer, 1971.
- [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.
- [Rom12] S. Roman, *Fundamentals of Group Theory: An Advanced Approach*, Birkhäuser, 2012.
- [Tur94] V.G. Turaev, *Quantum Invariants of Knots and 3-Manifolds*, de Gruyter Studies in Mathematics, vol. 18, Walter de Gruyter, 1994.
- [Väl86] H. Väliäho, “An elementary approach to the Jordan form of a matrix”, Amer. Math. Monthly **93** (1986), 711–714.

Indeks

- G -torsor, 93
- G -zbiór
 - homomorfizm, 89
 - lewostronny, 85
 - prawostronny, 86
- R -moduł
 - lewostronny, 115
 - prawostronny, 116
- χ -seria stowarzyszona z wartością własną, 298
- (γ) -ortogonalność
 - przestrzeni, 248
 - wektorów, 248
- (γ) -prostopadłość
 - przestrzeni, 248
 - wektorów, 248
- (anty)izomorfizm Fréchet–Riesza, 319
- ślad
 - endomorfizmu modułu nad pierścieniem, 238
 - cykliczność, 239
 - macierzy, 240
- łańcuch, 131
- ograniczenie górne, 131
- alfabet, 10
- algebra
 - Clifforda, 263
 - reprezentacja spinorowa, 263
 - Poissona, 242
- anihilator modułu nad pierścieniem, 210
- antykomutator
 - endomorfizmów przestrzeni wektorowej, 323
- argument liczby zespolonej, 29
- argument główny, 29
- niejednoznaczność, 30
- automorfizm
 - ortogonalny, 274
 - symplektyczny, 277
 - unitarny, 257
- baza
 - diagonalizująca endomorfizmu
 - diagonalizowalnego, 311
 - modułu nad pierścieniem, 129
 - standardowa, 129, 240
 - zmiana, 178
 - ortogonalna
 - względem formy kwadratowej, 264
 - przestrzeni ϵ -hermitowskiej
 - ortogonalna, 249
 - ortonormalna, 249
 - symplektyczna, 276
 - własna endomorfizmu, 280
- bijekcja, 16
- bimoduł, 205
- Cauchy’ego wzór, 194
- cecha IBN, 137
- centralizator, 91
- charakterystyka ciała, 23
- ciąg dokładny
 - grup, 66
 - krótki, 67
 - normalny, 67
 - rozszerzenie, 67
- cięcie liniowe, 160
- ciało, 14, 20
 - algebraicznie domknięte, 45
 - charakterystyka, 23
 - homomorfizm, 22
 - a monomorfizmy, 24
 - jądro, 23
 - obraz, 23
 - jedynka, 20
 - liczb zespolonych, 24
 - nietrywialność, 21
 - operacje, 20
 - potęga, 40
 - reszt *modulo*, 14
 - zero, 20
- cykl, 101
- część rzeczywista liczby zespolonej, 25
- część urojona liczby zespolonej, 25
- delta Kroneckera, 129

- diagram
 - chase, 125
 - przemienny, 340
 - warkoczowy, 51
- dopełnienie
 - normalne podgrupy, 72
 - podgrupy, 71
 - proste
 - podmodułu, 160
 - proste podgrupy, 73
- drzewa binarne, 9
- szczepienie, 10
- dwoistość (doskonała), 207
- działanie
 - grupy
 - G -torsor, 93
 - dołączone, 88
 - efektywne, 93
 - grupa izotropii, 91
 - lewostronne, 85
 - orbita, 92
 - prawostronne, 85
 - przechodnie, 93
 - przestrzeń jednorodna, 93
 - regularne, 88, 93
 - stabilizator, 91
 - transytywne, 93
 - trywialne, 87, 93
 - wierne, 93
 - wolne, 93
 - pierścienia
 - lewostronne, 115
 - prawostronne, 116
 - zbioru, 114
 - dziedzina operatorów, 114
 - nośnik, 114
- dziedzina
 - całkowitości, 35
 - euklidesowa, 35
 - norma euklidesowa, 35
 - ideałów głównych, 37
- dziedzina operatorów, 114
- dzielnik
 - elementu pierścienia, 43
 - elementy względnie pierwsze, 47
 - największy wspólny, 47
 - normalny, 64
- element neutralny, 10, 49
- elementy sprzężone grupy, 88
- endomorfizm
 - grupy, 57
 - przemiennej, 117
- idempotentny, 156
- modułu nad pierścieniem, 121
 - śląd, 238
 - a formy dwuliniowe, 209
 - cofnięcie wyznacznika, 198
 - wyznacznik, 197
- przestrzeni unitarnej
 - antyhermitowski, 323
 - antysymetryczny, 323
 - dodatni, 323
 - hermitowski, 323
 - izometria, 323
 - izometryczny, 323
 - normalny, 322
 - samosprężony, 323
 - skośnie hermitowski, 323
 - skośnie symetryczny, 323
 - symetryczny, 323
- przestrzeni wektorowej
 - χ -seria stowarzyszona z wartością
 - własną, 298
 - antykomutator, 323
 - baza jordanowska, 298
 - baza własna, 280
 - diagonalizowalny, 311
 - ewaluacja funkcji, 288
 - kompleksyfikacja, 304
 - komutator, 323
 - niezmiennik podstawowy, 282
 - nilpotentny, 308
 - przestrzeń własna, 280
 - spektrum, 280
 - wartość własna, 280
 - wektor własny, 279
 - widmo, 280
 - wielomian charakterystyczny, 281
 - wielomian minimalny, 283, 296
- ewaluacja funkcji na endomorfizmie
 - przestrzeni wektorowej, 288
- forma
 - ϵ -hermitowska, 243
 - jądro, 245
 - macierz względem bazy, 246
 - nieosobliwa, 246
 - niezwyrodniała, 245
 - rząd, 245
 - suma prosta, 248
 - zwyrodniała, 246
- n -liniowa na module nad pierścieniem, 185
 - maksymalnego rzędu, 190
- (J) -półliniowa, 244
- (J) -półtoraliniowa, 242
- antyhermitowska, 243
- antysymetryczna, 243
- dwuliniowa, 207
 - anihilacja, 210
 - anihilator, 210
 - dwoistość (doskonała), 207
 - ewaluacji, 207
 - para dwoista, 207
 - rząd, 212

- stowarzyszona z formą kwadratową, 264
- hermitowska, 243
 - dodatnia, 258
 - sygnatura, 263
 - ujemna, 258
- hiperboliczna, 267
- kwadratowa, 264
 - forma dwuliniowa stowarzyszona, 264
 - hiperboliczna, 267
 - jądro, 264
 - niezwyrodniała, 264
 - sygnatura, 264
 - zwyrodniała, 264
- liniowa na module nad pierścieniem, 203
- presymplektyczna, 249
- skośnie hermitowska, 243
- skośnie symetryczna, 243
- symetryczna, 243
- symplektyczna, 249, 275
- formuły
 - polaryzacyjne, 243
- Fréchet–Riesza (anty)izomorfizm, 319
- funkcja wielomianowa, 40
- funkcje klas grupy, 90
- funkcjonał
 - (J -)półliniowy, 244
- generator, 55
- grupa, 10, 49
 - abelowa, 11, 50
 - alternująca, 56, 112
 - generatory, 112
 - jako dzielnik normalny, 64
- Artina, 52
- automorfizmów, 59
 - wewnętrznych, 59
 - zewnętrznych, 66
- centrum, 11
- ciąg dokładny, 66
 - krótki, 67
 - normalny, 67
 - rozszerzenie, 67
- czwórkowa Kleina, 165
- diedralna, 74
- dwuścienna, 74
- działanie
 - lewostronne, 85
 - prawostronne, 85
- dzielnik normalny, 64
- element neutralny, 49
- elementy sprzężone, 88
- funkcje klas, 90
- generatory, 55
- homografii, 16, 56
- homomorfizm, 57
 - indukowany, 67
 - kanoniczny, 67
- iloczyn
 - prosty (zewnątrzny), 73
- ilorazowa, 66
- klas automorfizmów, 66
- komutant grupy, 56
- komutant podgrup, 56
- komutator, 56
- liczb zespolonych o module
 - jednostkowym, 50
- liniowa
 - główna, 172
- liniowa pełna, 16
- odwrotność, 54
- operacje, 49
- ortogonalna, 56
 - o współczynnikach z ciała, 275
 - specjalna, 61
 - stowarzyszona z formą hermitowską, 274
- pochodna grupy, 56
- podgrupa, 55
 - dopełnienie, 71
 - indeks podgrupy, 62
 - podgrupy istotnie rozłączne, 71
 - sprężona, 88
 - z dopełnieniem, 71
- podgrupa normalna, 64
- podstawowa
 - przestrzeni topologicznej, 74
- podstawowa przestrzeni topologicznej, 11
 - ścieżki, 11
 - pętle, 11
- prosta, 65
- przeciwna, 50
- przemienna, 11, 50
- realizacja
 - jako homomorfizm, 86
 - lewostronna, 86
 - prawostronna, 86
- symetryczna
 - cykl, 101
 - generatory, 105
 - permutacja, 11
 - transpozycja, 55
- symplektyczna
 - o współczynnikach z ciała, 277
 - stowarzyszona z formą hermitowską, 277
- trywialna, 50
- unitarna
 - o współczynnikach z ciała, 257
 - stowarzyszona z formą hermitowską, 257
- warkoczy, 52, 89
 - generatory, 53
 - warkocz, 51
- warstwa, 62
- zapis addytywny, 54

- krotność, 54
 - zapis mnożeniowy, 54
 - jedynka, 54
- grupa izotropii, 91
- homografia, 16, 56
- homomorfizm, 15
 - automorfizm, 15
 - inwolucja, 26
- ciało, 22
 - a monomorfizm, 24
 - jądro, 23
 - obraz, 23
- endomorfizm, 15
- epimorfizm, 15
- ewaluacji, 41
- grup, 57
 - automorfizm, 57
 - automorfizm wewnętrzny, 59
 - automorfizm zewnętrzny, 59
 - endomorfizm, 57
 - epimorfizm, 57
 - grupa automorfizmów, 59
 - grupa automorfizmów zewnętrznych, 66
 - grupa klas automorfizmów, 66
 - indukowany, 67
 - izomorfizm, 57
 - jądro, 60
 - jako homomorfizm struktur, 58
 - kanoniczny, 67
 - lewostronna odwrotność, 79
 - lewostronnie odwracalny, 79
 - monomorfizm, 57
 - obraz, 60
 - prawostronna odwrotność, 79
 - prawostronnie odwracalny, 79
 - rozszerzenie, 76
- izomorfizm, 15
- kanoniczny
 - grupy w grupę ilorazową, 66
- modułów nad pierścieniem, 121
 - automorfizm, 121
 - cięcia liniowe, 160
 - endomorfizm, 121
 - jądro, 123
 - kojądro, 124
 - koobraz, 124
 - obraz, 123
 - retrakcja liniowa, 160
 - sprężony, 216
 - struktura grupy przemiennej, 122
 - struktura modułu nad pierścieniem, 123
- monomorfizm, 15
- pierścieni, 38
- po-kładający, 141
- przed-kładający, 141
- standardowe włożenie, 58
- homotetia, 117
- ideal
 - główny, 37
 - lewostronny, 37
 - obustronny, 37
 - prawostronny, 37
- iloczyn
 - algebraiczny podzbiorów, 340
 - istotnie rozłączny podgrup, 71
 - kartezjański, 144, 339
 - półprosty podgrup, 72
 - prosty (wewnętrzny) podgrup, 73
 - prosty (zewnętrzny) grup, 73
 - skalary, 260
 - wektorowy, 187
- indeks podgrupy, 62
- injekcja, 15
- inwolucja, 26
- izometria, 246
- izomorfizm
 - kanoniczny, 229
- izotopia warkocza, 51
- jądro
 - formy
 - ϵ -hermitowskiej, 245
 - kwadratowej, 264
 - homomorfizmu, 23, 60
 - jako poziomica, 61
 - macierzy, 182
- jednomian, 39
- jednorodność
 - odwzorowania, 264
- jednostka urojona, 25
- klasa sprzężoności, 92
- klatka Jordana, 297
- rzeczywista, 297
- kombinacja liniowa, 126
- współczynniki, 126
- kompleksyfikacja
 - endomorfizmu przestrzeni wektorowej, 304
 - przestrzeni wektorowej, 303
- komutant
 - grupy, 56
 - podgrup, 56
- komutator
 - elementów grupy, 56
 - endomorfizmów przestrzeni wektorowej, 323
 - macierzy, 187
- komutowanie
 - endomorfizmów przestrzeni wektorowej, 290
- konkatenacja, 10
- koprodukt rodziny struktur, 144

- suma
 - rozłączna, 144
 - suma prosta, 144
 - modułów, 149
 - włożenie kanoniczne składowej, 144
- kowymiar podprzestrzeni wektorowej, 140
- krotność
 - elementu grupy, 54
 - elementu pierścienia, 43
 - zera wielomianu, 44
- Lagrange'a metoda diagonalizacji formy
 - kwadratowej (uzupełniania do kwadratu), 265
- Lagrange'a twierdzenie, 63
- lemat
 - nierówność Minkowskiego, 316
- liczby
 - całkowite, 8
 - Eisensteina, 36
 - naturalne, 8
 - wymierne, 8
 - zespólone, 24
 - argument, 29
 - część rzeczywista, 25
 - część urojona, 25
 - interpretacja geometryczna, 27, 30
 - jednostka urojona, 25
 - moduł, 26
 - o module jednostkowym, 28
 - pierwiastek, 30
 - sprzężenie zespolone, 26
 - symbol Eulera, 28
 - zapis kartezjański, 25
 - zapis trygonometryczny, 29
- macierz, 168
 - śląd, 240
 - antyhermitowska, 247
 - antysymetryczna, 247
 - blokowo diagonalna, 276
 - blokowo trójkątna, 201
 - branie przeciwności, 170
 - diagonalna, 255
 - dodawanie, 169
 - dolnotrójkątna, 201
 - elementu modułu nad pierścieniem
 - względem bazy, 176
 - formy ϵ -hermitowskiej względem bazy, 246
 - górnortrójkątna, 201
 - hermitowska, 247
 - jądro, 182
 - klatka Jordana, 297
 - rzeczywista, 297
 - kolumna, 169
 - komutator, 187
 - kwadratowa, 169
 - dopełnienie algebraiczne wyrazu, 195
 - macierz dopełnień algebraicznych, 195
 - przekątna, 169
 - stopnia N , 169
 - wyznacznik, 191
- mnożenie, 170
- obraz, 182
- odwzracalna, 172
- odwzorowania R -liniowego względem
 - baz, 177
- odwzorowania dwuliniowego względem
 - baz, 208
- ortogonalna, 275
- przejścia (między bazami), 178
- rząd, 180
- skośnie hermitowska, 247
- skośnie symetryczna, 247
 - standardowa, 276
- struktura pierścienia, 171
- suma
 - prosta, 298
 - symetryczna, 247
 - symplektyczna, 277
 - transponowana, 192
 - transpozycja, 56, 192
 - unitarna, 257
 - Vandermonda, 202
 - wiersz, 169
 - zerowa, 170
- magma, 9
- metryka indukowana, 316
- moduł
 - całkowicie przywiedlny, 279
 - cykliczny, 279
 - nieprzywiedlny, 279
 - półprosty, 279
 - prosty, 279
- moduł nad pierścieniem
 - lewostronny, 115
- moduł liczby zespolonej, 26
- moduł nad pierścieniem, 24
 - baza
 - zmiana, 178
 - cykliczny, 127
- forma
 - dwuliniowa, 207
 - liniowa, 203
- funkcjonał liniowa, 203
- generowany przez zbiór, 127
- grupa przemienna jako $\mathbb{Z}$ -moduł, 119
- homomorfizm, 121
 - automorfizm, 121
 - endomorfizm, 121
- kombinacja liniowa, 126
- moduł ilorazowy, 120
- odwzorowanie
 - R -liniowe, 121
 - biliniowe, 205
 - dwuliniowe, 205

- pierścień jako (bi)moduł standardowy, 118
 - baza standardowa, 129
- pierścień wielomianów, 41
- podmoduł
 - dopełnienie proste, 160
- podzbiór liniowo niezależny, 128
- podzbiór liniowo zależny, 128
- prawostronny, 116
- przestrzeń wektorowa, 119
- rodzina liniowo niezależna, 128
- rozszerzenie
 - trywialne, 160
- rzęd, 137
- skalar, 115
- skończenie generowany, 127
- trywialny, 118
- wolny, 129
- wyznacznik, 198
 - cofnięcie wzdłuż endomorfizmu, 198
- monoid, 10
 - swobodny, 10
- nawias
 - Nambu–Poissona, 187
 - Poissona, 187
- nierówność
 - Bessela, 317
 - Minkowskiego, 316
 - Schwarza, 258
 - trójkąta, 316
- niezmiennik
 - podstawowy endomorfizmu, 282
- nośnik, 7
 - działania, 114
 - permutacji, 91, 99
- norma indukowana, 316
- obraz
 - homomorfizmu, 23, 60
 - macierzy, 182
- obraz algebraiczny zbiorów względem operacji, 340
- odwrotność algebraiczna podzbioru, 341
- odwrotność homomorfizmu grup, 79
- odwzorowanie
 - R -liniowe, 121
 - rzęd, 180
 - n -liniowe
 - na module nad pierścieniem, 185
 - nad pierścieniem, 185
 - biliniowe, 205
 - dwuliniowe, 205
 - a endomorfizmy, 209
 - macierz względem baz, 208
 - nieosobliwe, 207
 - niezwyrodniałe, 207
 - zdegenerowane, 206
 - zerowe, 207
 - zwyrodniałe, 206
 - ewaluacji, 175
 - identycznościowe, 339
 - jednorodnie stopnia 2, 264
 - metryczne, 246
 - sprężone, 216
 - hermitowsko, 321
 - stowarzyszone
 - lewostronnie, 245
 - prawostronnie, 245
- operacja, 7
 - n -argumentowa, 7
 - 0-argumentowa, 7
 - przemieniana, 11
 - rozdzielna, 13
- operator rzutu, 156
- orbita
 - działania grupy, 92
 - ako klasa abstrakcji, 93
 - permutacji, 101
- ortogonalność
 - przestrzeni
 - względem formy ϵ -hermitowskiej, 248
 - względem formy kwadratowej, 264
- wektorów
 - względem formy ϵ -hermitowskiej, 248
 - względem formy kwadratowej, 264
- półgrupa, 9
- półpierścień, 13
 - tropikalny, 13
- plaszczyna
 - hiperboliczna, 267
 - symplektyczna, 275
- para
 - dwoista, 207
 - hiperboliczna, 267
 - symplektyczna, 275
- permutacja, 11
 - kompletny rozkład na cykle rozłączne, 104
 - nośnik, 91, 99
 - orbita, 101
 - rozkład na transpozycje, 105
 - rzęd, 99
 - typ, 103
 - znak, 111
 - jako homomorfizm, 111
- pierścień, 13, 33
 - Boole’a, 36
 - dziedzina
 - ideałów głównych, 37
 - endomorfizmów grupy przemiennej, 117
 - euklidesowy, 35
 - homomorfizm, 38
 - ideałów głównych, 37
 - dziedzina deałów głównych, 37

- jedynka, 33
- o cesze IBN, 137
- operacje, 33
- podpierścień, 37
- przeciwny, 117
- przemienność, 13, 35
- trywialny, 35
- wielomianów, 40
 - struktura modułu nad pierścieniem, 41
- zero, 33
- pierwiastek liczby zespolonej, 30
 - niejednoznaczność, 32
- pochodna grupy, 56
- podgrupa normalna, 64
- podzbiór liniowo zależny, 128
- podzielność, 43
 - dzielnik, 43
 - największy wspólny, 47
 - elementy względnie pierwsze, 47
 - krotność, 43
- pogoń wzdłuż diagramu, 125
- porządek
 - częściowy, 130
 - łańcuch, 131
 - element maksymalny, 131
 - element późniejszy, 131
 - element wcześniejszy, 131
 - zbiór łańcuchowo zupełny, 131
 - zbiór częściowo uporządkowany, 131
 - liniowy, 131
- potęga elementu, 40
- powłoka (R -)liniowa zbioru, 127
- poziomica, 61
- produkt
 - kartezjański, 144
 - modułów, 145
 - rodziny struktur, 143
 - kartezjański, 144
 - modułów, 145
 - rzut kanoniczny na składową, 143
- prostopadłość
 - przestrzeni
 - względem formy ϵ -hermitowskiej, 248
 - względem formy kwadratowej, 264
 - wektorów
 - względem formy ϵ -hermitowskiej, 248
 - względem formy kwadratowej, 264
- przeciwność algebraiczna podzbioru, 340
- przemienność
 - endomorfizmów przestrzeni wektorowej, 290
- przestrzeń
 - J -sprzężona, 244
 - K -liniowa, 119
 - ϵ -hermitowska, 246
 - anizotropowa, 250
 - izometria, 246
 - nieizotropowa, 250
 - nieosobliwa, 246
 - niezwyrodniała, 246, 250
 - odwzorowanie metryczne, 246
 - wektor izotropowy, 250
 - wektor zerowy, 250
 - zwyrodniała, 246
 - (γ) -ortogonalna, 248
 - (γ) -prostopadła, 248
 - anizotropowa, 250
 - euklidesowa, 315
 - hermitowska
 - iloczyn skalarny, 260
 - hiperboliczna, 267
 - izotropowa, 250
 - całkowicie, 250
 - jednorodna, 93
 - kwadratowa, 264
 - nieizotropowa, 250
 - niezmiennicza, 279, 289
 - niezwyrodniała, 250
 - ortogonalna
 - względem formy ϵ -hermitowskiej, 248
 - prostopadła
 - względem formy ϵ -hermitowskiej, 248
 - redukcja dla endomorfizmu, 289
 - symplektyczna, 242, 275
 - baza symplektyczna, 276
 - unitarna, 315
 - euklidesowa, 315
 - metryka indukowana, 316
 - norma indukowana, 316
 - rzut ortogonalny, 326
 - rzut prostopadły, 326
 - własna endomorfizmu, 280
 - uogólniona, 291
 - wektorowa, 119
 - ciało jako przestrzeń standardowa, 119
 - kompleksyfikacja, 303
 - sprzężona, 203
 - wektor, 119
 - wektor kolumnowy, 180
 - wymiar (K -liniowy), 137
 - zerowa, 119
- przestrzeń jednorodna
 - główna, 93
- przestrzeń ortogonalna
 - względem formy kwadratowej, 264
- przestrzeń prostopadła
 - względem formy kwadratowej, 264
- przestrzeń wektorowa
 - ciało jako przestrzeń standardowa
 - baza standardowa, 130
 - podprzestrzeń
 - kowymiar, 140
 - przestrzeń ilorazowa, 120
 - trywialna, 119
- równanie liniowe

- jednorodne, 181
 - rozwiązanie trywialne, 182
- niejednorodne, 181
 - rozwiązanie, 181
 - zbiór rozwiązań, 181
- niejednorodność, 181
- niewiadoma, 181
- sprzeczne, 181
- realizacja
 - endomorfizmu
 - redukowalna względem podprzestrzeni, 289
 - grupy
 - jako homomorfizm, 86
 - lewostronna, 86
 - prawostronna, 86
 - macierzowa
 - elementu modułu nad pierścieniem, 175
 - odwzorowania R -liniowego, 173
 - pierścienia na przestrzeni wektorowej
 - zgodna ze strukturą K -liniową, 278
 - cykliczna, 279
 - nieprzywiedlna, 279
 - półprosta, 279
 - prosta, 279
 - zbioru, 114
- relacje samosprzężenia, 255
- reprezentacja
 - spinorowa algebry Clifforda, 263
- retrakcja liniowa, 160
- rodzina indeksowana, 126
 - nośnik, 126
 - skończony, 126
- rodzina liniowo niezależna, 128
- rozkład
 - spektralny
 - endomorfizmu diagonalizowalnego, 311
 - widmowy
 - endomorfizmu diagonalizowalnego, 311
- rozszerzenie
 - grupy, 67
 - centralne, 67
 - homomorfizmu grup, 76
- rozszerzenie modułu trywialne, 160
- ruch euklidesowy, 70
- rzęd
 - formy
 - ϵ -hermitowskiej, 245
 - dwuliniowej, 212
 - macierzy, 180
 - modułu nad pierścieniem, 137
 - odwzorowanie R -liniowego, 180
 - permutacji, 99
- rzut, 156
 - kanoniczny, 339
 - modulo* podgrupa, 66
 - ortogonalny, 326
 - prostopadły, 326
- rodzina rzutów dopełniających, 157
 - zupełna, 157
- rodzina rzutów komplementarnych, 157
 - zupełna, 157
- słownik, 10
- singleton, 7
- spektrum endomorfizmu, 280
 - niezdegenerowane, 284
 - niezwyrodniałe, 284
- sprzężenie
 - (J) -hermitowskie, 247
 - hermitowskie, 321
 - liczby zespolonej, 26
 - zespolone, 26
 - na skompleksyfikowanej przestrzeni wektorowej, 304
- stała, 7
- stabilizator, 91
- stopień wielomianu, 41
- struktura
 - inicjalna, 142
 - końcowa, 141
 - początkowa, 142
 - terminalna, 141
 - koproduct, 144
 - product, 143
 - uniwersalna, 142
- struktura algebraiczna, 7
 - homomorfizm, 15
 - podstruktura, 7
- stwierdzenie
 - bilans wymiarów, 138
 - „kwantowy”, 164
 - lemat (nie od) Burnside'a, 96
 - lemat Cauchy'ego–Frobeniusa, 96
 - lemat Frattiniego, 96
 - lemat Pięciu (Morfizmów), 125
 - lemat Riesz, 319
 - lemat Steinitza o wymianie, 132
 - nierówność Bessela, 317
 - nierówność Schawrza, 258
 - o postaci kanonicznej (macierzy)
 - odwzorowania K -liniowego, 179
 - o postaci kanonicznej macierzy
 - hermitowskiej, 255
 - o postaci kanonicznej macierzy skośnie
 - symetrycznej, 276
 - o rozszerzeniu hiperbolicznym
 - przestrzeni izotropowej, 268
 - o współmienniczości wyznacznika na
 - module względem endomorfizmu, 198
 - ortogonalizacja Grama–Schmidta, 256
 - prawo Dedekinda, 57
 - Sylwestera–Jacobiego wyznacznikowy
 - wzór na sygnaturę, 266
 - twierdzenie Kroneckera–Capelliego, 183

- twierdzenie Lagrange'a o diagonalizacji
 - formy kwadratowej, 265
- twierdzenie Rouchégo–Fonteného, 183
- wzór wyznacznikowy Cauchy'ego, 194
- wzory Cramera, 199
- suma
 - (γ^-) ortogonalna, 248
 - algebraiczna podzbiorów, 340
 - ortogonalna
 - względem formy kwadratowej, 264
 - prosta, 144
 - form ϵ -hermitowskich, 248
 - macierzy, 298
 - modułów, 149
 - rozłączna, 144
- surjekcja, 15
- sygnatura
 - formy
 - hermitowskiej, 263
 - kwadratowej, 264
- symbol Eulera, 28
 - wzór de Moivre'a, 28
- symbol Kroneckera, 129
- symetria cechowania, 249
- teoria kategorii, 140
- transformacja
 - bazy, 178
 - ortogonalna, 274
 - symplektyczna, 277
 - unitarna, 257
- transpozycja, 55
- twierdzenie
 - algorytm Euklidesa, 42
 - Bezouta, 44
 - Cayleya, 99
 - Cayleya–Hamiltona, 282
 - grupa symetryczna w terminach generatorów i relacji, 107
 - Lagrange'a, 63
 - lemat Kuratowskiego–Zorna, 131
 - o bazie ortogonalnej dla formy hermitowskiej, 252
 - o ekwiwariantnym izomorfizmie zbiorów z działaniem, 97
 - o homomorficznym przeciwobrazie normalnego ciągu dokładnego grup, 82
 - o istnieniu bazy przestrzeni wektorowej, 130
 - o istnieniu wyznacznika, 191
 - o izomorfizmie
 - drugie (dla grup), 69
 - drugie (dla modułów), 124
 - pierwsze (dla grup), 68
 - pierwsze (dla modułów), 124
 - trzecie (dla grup), 81
 - trzecie (dla modułów), 124
 - o jednostronnej odwracalności homomorfizmu, 80
 - o jednoznaczności struktur uniwersalnych, 142
 - o jordanowskiej postaci normalnej endomorfizmu, 298
 - o klasyfikacji orbit, 95
 - o liniowym przeciwobrazie normalnego ciągu dokładnego modułów, 125
 - o macierzy elementu modułu wolnego i odwzorowania R -liniowego, 176
 - o odwracalności macierzy, 195
 - o parzystości permutacji, 110
 - o postaci kanonicznej formy skośnie symetrycznej, 275
 - o rozkładzie biegunowym i prezentacji trygonometrycznej liczby zespolonej, 29
 - o rozkładzie endomorfizmu na części: diagonalizowalną i nilpotentną, 313
 - o rozkładzie permutacji na cykle rozłączne, 101
 - o rozkładzie przestrzeni wektorowej na przestrzenie pierwiastkowe endomorfizmu, 296
 - o rozszczepialności modułu, 160
 - o rozszerzeniu epimorfizmu, 77
 - o strukturze dziedziny całkowitości na pierścieniu wielomianów, 40
 - o uniwersalności rzutu kanonicznego (dla grup), 69
 - o wymiarze przestrzeni wektorowej, 137
- Podstawowe Twierdzenie Algebry, 45
- Sylwestera prawo bezwładności, 260
- widmowe dla endomorfizmu normalnego zespolonej przestrzeni wektorowej, 327
- widmowe dla endomorfizmu samosprężonego rzeczywistej przestrzeni wektorowej, 330
- Witta
 - o przedłużaniu izometrii, 269
 - o rozkładzie, 273
 - o skracaniu, 272
- typ permutacji, 103
- układ równań
 - jednorodny, 182
 - niejednorodny, 182
 - macierz, 182
 - niejednorodność, 182
 - niewiadoma, 182
- układ równań liniowych
 - niejednorodny
 - rozwiązanie, 182
 - zbiór rozwiązań, 182
 - sprzeczny, 182
- Vierergruppe, 165

- warkocz, 51
 - diagram warkoczowy, 51
 - izotopia, 51
- warstwa, 62
- wartość własna endomorfizmu, 280
 - χ -seria stowarzyszona, 298
 - niezdegenerowana, 284
 - niezwyróżniona, 284
 - zdegenerowana, 284
 - zwyróżniona, 284
- wektor
 - (γ) -ortogonalny, 248
 - (γ) -prostopadły, 248
 - izotropowy, 250
 - kolumnowy, 180
 - ortogonalny
 - względem formy kwadratowej, 264
 - prostopadły
 - względem formy kwadratowej, 264
 - własny endomorfizmu, 279
 - zerowy, 250
- widmo endomorfizmu, 280
 - niezdegenerowane, 284
 - niezwyróżnione, 284
- wielomian, 39
 - charakterystyczny endomorfizmu, 281
 - funkcja wielomianowa, 40
 - homomorfizm ewaluacji, 41
 - interpolujący, 285
 - jednomian, 39
 - krotność zera, 44
 - minimalny endomorfizmu, 283, 296
 - pierścień wielomianów, 40
 - struktura modułu nad pierścieniem, 41
 - stopień, 41
 - współczynniki, 40
 - zero, 40
 - zerowy, 39
 - zmienna (formalna), 40
- wymiar ($\mathbb{K}$ -liniowy) przestrzeni wektorowej, 137
- wyraz, 10
- wyznacznik
 - endomorfizmu, 197
 - macierzy
 - blokowo trójkątnej, 201
 - dolnotrójkątnej, 201
 - górnortrójkątnej, 201
 - macierzy kwadratowej, 191
 - minor, 191
 - rozwinięcie Laplace'a, 191, 193
 - modułu nad pierścieniem, 198
 - Vandermonda, 202
- wzór de Moivre'a, 28
- zapis liczby zespolonej
 - kartezjański, 25
 - trygonometryczny, 29
- zbiór generujący, 127
- zbiór z działaniem grupy
 - homomorfizm, 89
 - lewostronnym, 85
 - prawostronnym, 86
- zmienna (formalna) wielomianu, 40
- znak permutacji, 111
 - jako homomorfizm, 111