Spis treści

Przedmowa

Niniejszy tekst był początkowo przygotowany jako skrypt dla studentów w związku z prowadzonymi przeze mnie w latach 1994, 1997 i 1998 wykładami *Metod Matematycznych Fizyki* na Wydziale Fizyki Uniwersytetu Warszawskiego. Skrypt był przeznaczony głównie dla studentów drugiego roku, którzy zaliczyli wykłady Algebry i Analizy Matematycznej. Przy pisaniu skryptu wykorzystałem zadania przygotowane przez Jacka Tafla, a pomocy udzielali mi także Andrzej Okołów, Jacek Pliszka i Adam Szereszewski.

Później do skryptu zostały dołączone rozdziały poświęcone algebrom Clifforda i spinorom, oparte na wykładach z lat 2000–2008.

Z inicjatywy Pawła Nurowskiego, w roku 2011, tekst skryptu został złożony w Redakcji Księgozbioru Matematycznego IM PAN. Recenzenci zwracali uwagę na różne niedociągnięcia oraz sugerowali zmiany. Autor, będący fizykiem, nie mógł przyjąć zalecenia, aby iloczyn skalarny definiować jako zawsze dodatnio określony. Pozostało też określenie swobodnego (a nie wolnego) działania grupy, odwzorowania półliniowego (a nie antyliniowego) i kilka innych polonizmów.

Duży i cenny wkład do końcowej redakcji tekstu wniósł Paweł Nurowski. Jest on autorem niektórych dowodów. Bez jego udziału, życzliwych rad i zachęty książka ta nigdy by nie powstała.

Andrzej Trautman

Następujące książki były używane w przygotowywaniu wykładów i pisaniu skryptu:

[BR] A. O. Barut, R. Rączka, *Theory of group representations and applications*, PWN, Warszawa, 1977.

[Br] H. Boerner, *Representations of groups*, North-Holland, Amsterdam, 1963.

[Bb] N. Bourbaki, *Groupes et algèbres de Lie, Ch. 1–9*, Hermann, Masson, Paris, 1960–1982.

[BJ] M. Bryński, J. Jurkiewicz, *Zbiór zadań z algebry*, wyd. III, PWN, Warszawa, 1985.

[Ch] C. Chevalley, *Theory of Lie groups I*, Princeton Univ. Press, Princeton, 1946.

[Ha] M. Hamermesh, *Teoria grup w zastosowaniu do zagadnień fizycznych*, PWN, Warszawa, 1968.

[Ko] A. I. Kostrikin, *Wstęp do algebry*, cz. 1–3, PWN, Warszawa, 2004, 2005.

[La] S. Lang, *Algebra*, wyd. II, PWN, Warszawa, 1984.

[Lj] G. J. Ljubarskij, *Teoria grup i jej zastosowania w fizyce*, PWN, Warszawa, 1961.

[Mi] L. Michel, *Applications of group theory to quantum physics*, Lecture Notes in Physics 6, Springer, Berlin, 1970.

[SA] J.-P. Serre, *Algèbres de Lie semi-simples complexes*, Benjamin, New York, 1966.

[SF] J.-P. Serre, *Reprezentacje liniowe grup skończonych*, PWN, Warszawa, 1988.

[SL] J.-P. Serre, *Lie algebras and Lie groups*, Benjamin, New York, 1965.

[Si] B. Simon, *Representations of finite and compact groups*, Graduate Studies in Mathematics 10, Amer. Math. Soc., Providence, 1996.

[We] H. Weyl, *The theory of groups and quantum mechanics*, Dover Publ., New York, 1950.

[Wy] H. Weyl, *The classical groups*, Princeton Univ. Press, Princeton, 1946.

[Wo] W. Wojtyński, *Grupy i algebry Liego*, Biblioteka Matematyczna 60, PWN, Warszawa, 1986.

Odnośniki do tych książek są w tekście oznaczane odpowiednimi literami. Liczbami oznaczono odwołania do innych pozycji literatury, których spis jest na końcu.

I Wstępne wiadomości z algebry

1. Grupy, pierścienie, ciała i moduły

1.1. Grupy

1.1.1. Definicje i przykłady

Grupa to zbiór G z odwzorowaniem

$$G \times G \to G, \quad (a, b) \mapsto a \cdot b, \tag{1.1}$$

takim, że

(i) zachodzi prawo *łączności*: jeśli $a, b, c \in G$, to $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

(ii) istnieje element *neutralny* $e \in G$ taki, że $a \cdot e = e \cdot a = a$ dla każdego $a \in G$;

(iii) dla każdego $a \in G$ istnieje element *odwrotny* $b \in G$ taki, że $a \cdot b = b \cdot a = e$.

Odwzorowanie (1.1) nazywa się *działaniem grupowym* lub *mnożeniem* elementów; $a \cdot b$ jest *iloczynem* a i b. Zdanie „G jest grupą z działaniem (1.1)” skraca się często do „$(G, \cdot)$ jest grupą”. Znak „$\cdot$” często się opuszcza i pisze ab zamiast $a \cdot b$. Element neutralny jest niekiedy oznaczany przez 1; element odwrotny do a oznacza się przez a^{-1} (*notacja multiplikatywna*). Jeśli elementy grupy G są bijekcjami pewnego zbioru na ten sam zbiór, a działanie jest składaniem odwzorowań, to złożenie a i b bywa zapisywane jako $a \circ b$.

Jeśli $ab = ba$ dla każdej pary (a, b) elementów grupy, to grupę nazywamy *przemienną* lub *abelową*; iloczyn a i b zapisuje się wtedy często jako $a + b$ (i nazywa sumą), a element neutralny oznacza zerem; zamiast „element odwrotny” mówi się „element *przeciwny*” i zapisuje go jako $-a$ (*notacja addytywna*).

Przykład 1.1. Zbiory liczb: całkowitych $\mathbb{Z}$, wymiernych $\mathbb{Q}$, rzeczywistych $\mathbb{R}$ i zespolonych $\mathbb{C}$ są grupami przemiennymi względem dodawania; zbiory liczb dodatnich: wymiernych $\mathbb{Q}^+$ i rzeczywistych $\mathbb{R}^+$ są grupami przemiennymi względem mnożenia; zbiór $\mathbb{C}^\times$ różnych od zera liczb zespolonych jest grupą przemienną względem mnożenia. Wszystkie te grupy są nieskończone.

Jeśli G jest grupą skończoną, to liczbę $\#G$ jej elementów nazywa się *rzędem* grupy. Grupa rzędu 1 zawiera tylko element neutralny i nazywa się *grupą trywialną*; bywa ona oznaczana symbolem 1 (notacja multiplikatywna) albo 0 (notacja addytywna).

Przykład 1.2. Zbiór $\mathbb{Z}_n$ n-tych pierwiastków zespolonych z 1 jest grupą przemienną rzędu n.

Grupy pojawiły się początkowo jako grupy przekształceń zbiorów. Mówi się, że grupa G jest *grupą przekształceń* zbioru X, lub że G *działa w* X, jeśli dane jest odwzorowanie

$$G \times X \to X, \quad (a, x) \mapsto ax,$$

takie, że

$$ex = x, \quad a(bx) = (ab)x,$$

dla wszystkich $x \in X$ i $a, b \in G$.

W szczególności, dla każdego zbioru X mamy grupę $\mathfrak{S}(X)$ wszystkich bijekcji zbioru X na X. Elementem neutralnym w tej grupie jest odwzorowanie tożsamościowe id_X zbioru X na X.

Jeśli $X = \{1, \ldots, n\}$, to pisze się $\mathfrak{S}_n$ zamiast $\mathfrak{S}(X)$; jest to *n-ta grupa symetryczna* (lub *grupa permutacji* zbioru n elementów). Rząd tej grupy wynosi $n!$. Permutację

$$\pi \in \mathfrak{S}_n, \quad i \mapsto \pi(i), \quad i = 1, \ldots, n,$$

zapisuje się często jako

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \pi(1) & \pi(2) & \ldots & \pi(n) \end{pmatrix}.$$

Grupa $\mathfrak{S}_n$ działa w zbiorze X_n wszystkich funkcji $f : \mathbb{R}^n \to \mathbb{R}$. Jeśli mianowicie $f(x_1, \ldots, x_n)$ jest taką funkcją i $\pi \in \mathfrak{S}_n$, to

$$(\pi.f)(x_1, \ldots, x_n) = f(x_{\pi(1)}, \ldots, x_{\pi(n)}).$$

Funkcja $f \in X_n$ jest *symetryczna* (tzn. zamiana miejscami dwóch argumentów nie zmienia jej wartości) wtedy i tylko wtedy, gdy $\pi.f = f$ dla każdego $\pi \in \mathfrak{S}_n$. Funkcja wielomianowa

$$f_0(x_1, \ldots, x_n) = \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j) \tag{1.2}$$

jest *antysymetryczna* (zamiana miejscami dwóch argumentów zmienia wartość funkcji na przeciwną). Dla każdej permutacji π wielomian $\pi.f_0$ różni się od f_0 co najwyżej o znak:

$$\pi.f_0 = (\operatorname{sgn}\pi)f_0, \quad \operatorname{sgn}\pi \in \{1, -1\}. \tag{1.3}$$

Liczbę $\operatorname{sgn}\pi$ nazywa się *parzystością* permutacji. Permutacja π jest *parzysta* [*nieparzysta*], jeśli $\operatorname{sgn}\pi = 1$ [$\operatorname{sgn}\pi = -1$]. Permutację $\pi \in \mathfrak{S}_n$ taką, że $\pi(a_i) = a_{i+1}$ dla $i = 1, \dots, k-1$, $\pi(a_k) = a_1$ oraz $\pi(j) = j$ dla $j \notin \{a_1, \dots, a_k\}$, będziemy zapisywać jako $\lfloor a_1, \dots, a_k \rfloor$ i nazywać *cyklem*[1] o długości k (albo *k-cyklem*). Cykl o długości 2 nazywa się *transpozycją*. Transpozycja jest permutacją nieparzystą.

Łatwo pokazać (zob. zad. 1.4), że wszystkie grupy rzędu mniejszego niż 6 są przemienne.

Przykład 1.3. Grupa $\mathfrak{S}_3$ jest nieprzemienna. Istotnie, transpozycje $\lfloor 1,2 \rfloor$ i $\lfloor 2,3 \rfloor$ nie są ze sobą przemienne:

$$\lfloor 1,2 \rfloor \lfloor 2,3 \rfloor = \lfloor 1,2,3 \rfloor, \quad \lfloor 2,3 \rfloor \lfloor 1,2 \rfloor = \lfloor 1,3,2 \rfloor.$$

1.1.2. Podgrupy i morfizmy

Niepusty podzbiór H grupy G nazywa się jej *podgrupą*, jeśli $a, b \in H$ pociąga za sobą $ab^{-1} \in H$. Każda podgrupa jest grupą.

Przykład 1.4. Zbiór permutacji parzystych

$$\mathfrak{A}_n = \{\sigma \in \mathfrak{S}_n \mid \operatorname{sgn}\sigma = 1\}$$

jest podgrupą grupy $\mathfrak{S}_n$, zwaną *grupą alternującą*.

Jeśli G i H są grupami, to odwzorowanie $h : G \to H$ takie, że $h(ab) = h(a)h(b)$ dla dowolnych $a, b \in G$, nazywa się *homomorfizmem* grup.

Stwierdzenie 1.5. *Niech e_G i e_H będą elementami neutralnymi grup G i H. Jeśli $h : G \to H$ jest homomorfizmem, to $h(e_G) = e_H$; ponadto* obraz *homomorfizmu h,*

$$\operatorname{img} h = h(G),$$

jest podgrupą grupy H, a jądro *homomorfizmu h,*

$$\ker h = \{a \in G \mid h(a) = e_H\},$$

jest podgrupą grupy G.

[1] Większość autorów zapisuje taki cykl w postaci $(a_1 \dots a_k)$, co może prowadzić do nieporozumień ze względu na podobieństwo do oznaczeń dla ciągów.

Dowód. Rzeczywiście, dla każdego $a \in G$ mamy $h(e_G)h(a) = h(a) = e_H h(a)$ oraz $h(a^{-1})h(a) = h(e_G)$, więc $h(e_G) = e_H$ i $h(a)^{-1} = h(a^{-1})$; jeśli $a, b \in G$, to $h(a)h(b)^{-1} = h(ab^{-1}) \in \operatorname{img} h$; jeśli $a, b \in \ker h$, to $h(ab^{-1}) = h(a)h(b)^{-1} = e_H$, więc $ab^{-1} \in \ker h$. □

Homomorfizm grupy w tę samą grupę nazywa się *endomorfizmem*. Homomorfizm różnowartościowy nazywamy *monomorfizmem*. *Epimorfizm* to homomorfizm surjektywny. Homomorfizm wzajemnie jednoznaczny to *izomorfizm*. *Automorfizm* grupy G to izomorfizm G na G.

Przykład 1.6. Niech $\mathbb{R}^+$ oznacza grupę multiplikatywną liczb rzeczywistych dodatnich. Odwzorowanie wykładnicze $\exp : \mathbb{R} \to \mathbb{R}^+$ jest izomorfizmem grup.

Przykład 1.7. Niech $\mathbb{N} = \{0, 1, 2, \ldots\}$ oraz $0 < n \in \mathbb{N}$. Odwzorowanie

$$\mathbb{Z} \to \mathbb{Z}_n, \quad k \mapsto \exp(2\pi k\sqrt{-1}/n),$$

jest epimorfizmem; jądrem tego odwzorowania jest podgrupa $n\mathbb{Z}$ składająca się z liczb całkowitych podzielnych przez n.

1.1.3. Iloczyn grup

Mając grupy G i H, można utworzyć ich *iloczyn* (prosty, kartezjański): jest to grupa, której zbiorem elementów jest $G \times H$, a działanie określone jest wzorem

$$(a, b) \cdot (a', b') = (aa', bb'),$$

gdzie $a, a' \in G$ oraz $b, b' \in H$. „Dzielenie” grup wymaga nieco subtelniejszych rozważań.

1.1.4. Warstwy

Niech H będzie podgrupą grupy G; można wprowadzić w G relację, przyjmując

$$a \equiv b \iff a^{-1}b \in H.$$

Tak zdefiniowana relacja jest relacją równoważności: jest ona symetryczna ($a \equiv a$), zwrotna (jeśli $a \equiv b$, to $b \equiv a$) oraz przechodnia (jeśli $a \equiv b$ i $b \equiv c$, to $a \equiv c$, bo $a^{-1}c = a^{-1}b \cdot b^{-1}c$). Klasy równoważności względem tej relacji nazywają się *warstwami lewostronnymi* grupy G względem podgrupy H. Warstwę lewostronną zawierającą $a \in G$ zapisuje się jako

$$aH = \{ab \in G \mid b \in H\}.$$

Zbiór wszystkich warstw lewostronnych grupy G względem podgrupy H oznacza się przez G/H. Podobnie definiuje się *warstwy prawostronne*: są to klasy równoważności dla relacji $a \equiv b \Leftrightarrow ab^{-1} \in H$. Warstwa prawostronna zawierająca a to zbiór $Ha = \{ba \in G \mid b \in H\}$. Na ogół $aH \neq Ha$. Zbiór wszystkich warstw prawostronnych grupy G względem podgrupy H oznacza się przez $H\backslash G$. Podgrupa H jest równocześnie lewostronną i prawostronną warstwą zawierającą element neutralny. Na mocy samej definicji relacji równoważności mamy

$$aH \cap bH = \begin{cases} aH, & \text{jeśli } a^{-1}b \in H, \\ \emptyset, & \text{jeśli } a^{-1}b \notin H. \end{cases}$$

Odwzorowanie $H \to aH$ określone przez $b \mapsto ab$, $b \in H$, jest bijekcją. Wszystkie warstwy są więc zbiorami tej samej mocy. Zachodzi zatem

Twierdzenie (Lagrange'a). *Jeśli grupa G jest skończona, to*

$$\#(G/H) = \#G/\#H.$$

W szczególności rząd podgrupy jest dzielnikiem rzędu grupy.

Liczbę $\#(G/H)$ nazywa się *indeksem* podgrupy H w G.

1.1.5. Dzielniki normalne

Czy można tak zdefiniować strukturę grupy na zbiorze G/H, aby odwzorowanie kanoniczne $G \to G/H$, $a \mapsto aH$, było homomorfizmem, tzn.

$$a'H \cdot aH = a'aH\ ? \tag{1.4}$$

Trzeba najpierw sprawdzić, czy mnożenie warstw (1.4) jest dobrze określone, tzn. czy wynik nie zależy od wyboru reprezentantów a i a' w warstwach. Zastępując a przez ab, gdzie $b \in H$, otrzymuje się $a'abH = a'aH$, ale zastępując a' przez $a'b$, otrzymuje się $a'baH$; żądanie, aby ta warstwa była równa $a'aH$, oznacza istnienie $b' \in H$ takiego, że $a'ba = a'ab'$, czyli: dla dowolnych $a \in G$ i $b \in H$ istnieje $b' \in H$ takie, że $ba = ab'$. Stąd $Ha = aH$: warstwy lewostronne i prawostronne są jednakowe; jest to równoważne warunkowi

$$aHa^{-1} = H \quad \text{dla każdego } a \in G,$$

który, jak łatwo pokazać, wystarcza na to, aby (1.4) określało w zbiorze G/H strukturę grupy. Podgrupę H o tej własności nazywa się *dzielnikiem normalnym*, a zbiór G/H z mnożeniem elementów określonym wzorem (1.4) – *grupą ilorazową*. Każda podgrupa grupy przemiennej jest dzielnikiem normalnym.

Przykład 1.8. Iloraz grupy $\mathbb{Z}$ przez podgrupę $n\mathbb{Z}$ liczb podzielnych przez n jest izomorficzny multiplikatywnej grupie $\mathbb{Z}_n$ n-tych pierwiastków z 1; izomorfizm $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n$ przeprowadza warstwę zawierającą $k \in \mathbb{Z}$ w $\exp(2\pi\sqrt{-1}\,k/n)$.

Stwierdzenie 1.9. *Jeśli* $h : G \to H$ *jest homomorfizmem grup, to* $\ker h$ *jest dzielnikiem normalnym grupy* G*, a odwzorowanie*

$$G/\ker h \to \operatorname{img} h, \qquad a \ker h \mapsto h(a),$$

jest izomorfizmem grup.

Dowód. Jeśli $a \in G$ i $b \in \ker h$, to $aba^{-1} \in \ker h$, więc $\ker h$ jest dzielnikiem normalnym; odwzorowanie $a \ker h \mapsto h(a)$ jest homomorfizmem, bo $a \ker h \cdot a' \ker h = aa' \ker h \mapsto h(aa') = h(a)h(a')$; odwzorowanie to jest injektywne, gdyż jeśli $h(a) = h(a')$, to $a^{-1}a' \in \ker h$, czyli $a \ker h = a' \ker h$. □

Ważnym przykładem dzielnika normalnego grupy jest jej *centrum*,

$$\mathsf{Z}(G) = \{a \in G \mid ab = ba \text{ dla każdego } b \in G\}.$$

Jeśli grupa G jest nieskończona, to iloraz G/H może być izomorficzny z G nawet wtedy, gdy dzielnik normalny H jest nietrywialny. Niech np. G będzie grupą $\mathsf{U}(1)$ liczb zespolonych o module 1; dla każdego $n = 2, 3, \ldots$ niech $h_n : \mathsf{U}(1) \to \mathsf{U}(1)$ będzie endomorfizmem określonym wzorem $h_n(z) = z^n$. Wtedy $\operatorname{img} h_n = \mathsf{U}(1)$ oraz $\ker h_n = \mathbb{Z}_n$, więc na podstawie stwierdzenia 1.9 odwzorowanie $z\mathbb{Z}_n \mapsto z^n$ jest izomorfizmem ilorazu $\mathsf{U}(1)/\mathbb{Z}_n$ na $\mathsf{U}(1)$.

1.1.6. Rząd elementu grupy

Jeśli element a grupy ma tę własność, że $a^n \neq e$ dla każdej liczby naturalnej $n \geq 1$, to mówimy, że a jest *nieskończonego rzędu*. W przeciwnym razie istnieje najmniejsza liczba naturalna $n \geq 1$ taka, że $a^n = e$; mówimy wtedy, że a jest *rzędu* n. Zbiór $\{a, a^2, \ldots, a^n = e\}$ jest wtedy podgrupą grupy G. Na mocy twierdzenia Lagrange'a wynika stąd, że w grupie skończonej rząd każdego elementu jest dzielnikiem rzędu grupy.

1.1.7. Grupy proste

Grupę G nazywa się *prostą*, jeśli jedynymi jej dzielnikami normalnymi są G i grupa trywialna $\{e\}$. Z twierdzenia Lagrange'a wynika, że grupa skończona G, której rząd jest liczbą pierwszą, nie ma podgrup innych niż G i $\{e\}$, jest więc prosta. Np. jeśli p jest liczbą pierwszą, to grupa $\mathbb{Z}_p$ jest prosta. Co więcej, zachodzi

Stwierdzenie 1.10. *Jeśli* p *jest liczbą pierwszą, to każda grupa rzędu* p *jest izomorficzna z* $\mathbb{Z}_p$*.*

Dowód. Jeśli p jest liczbą pierwszą, a G jest grupą rzędu p, to na podstawie §1.1.6 każdy jej element $a \neq e$ jest rzędu p. Zatem $G = \{a, a^2, \ldots, a^p = e\}$, a odwzorowanie

$$G \to \mathbb{Z}_p, \quad a^k \mapsto \exp(2\pi\sqrt{-1}\,k/p), \quad k = 1, \ldots, p,$$

jest izomorfizmem. □

Wielkim osiągnięciem matematyki XX wieku było zakończenie klasyfikacji i opisu wszystkich *skończonych grup prostych*. Lista tych grup zawiera nieskończone ciągi obejmujące

- $\mathbb{Z}_p$, gdzie p jest liczbą pierwszą,
- $\mathfrak{A}_n$, $n \geqslant 5$,
- grupy proste typu Liego

oraz

- 26 „sporadycznych" grup prostych.

Pięć pierwszych grup sporadycznych zostało znalezionych przez Emila Mathieu w XIX wieku. Następne odkryto w drugiej połowie XX wieku, a ostatnia – największa wśród sporadycznych grupa *Monster* – była przewidziana i opisana dopiero w końcu XX wieku, dzięki zastosowaniu komputerów. Ma ona

$$\begin{aligned} &2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \\ &\qquad = 808017424794512875886459904961710757005754368000000000 \\ &\qquad \approx 8 \cdot 10^{53} \end{aligned}$$

elementów [28]. Robert Griess skonstruował tę grupę jako podgrupę grupy obrotów przestrzeni o wymiarze 196883 [48]. Wysuwane są przypuszczenia o związku reprezentacji grupy *Monster* z fizyką [29, 12].

1.2. Pierścienie i ciała

1.2.1. Pierścienie

Pierścień to grupa przemienna $(\mathcal{K}, +)$, w której określone jest łączne *mnożenie* elementów (1.1), rozdzielne względem dodawania, tzn. takie, że dla dowolnych $a, b, c \in \mathcal{K}$ zachodzą równości

$$(a + b) \cdot c = a \cdot c + b \cdot c, \quad c \cdot (a + b) = c \cdot a + c \cdot b.$$

Pierścień z jednością to pierścień $\mathcal{K}$ posiadający element 1, różny od elementu neutralnego 0 struktury grupy przemiennej w $\mathcal{K}$ i taki, że $1 \cdot a = a \cdot 1 = a$ dla każdego $a \in \mathcal{K}$. Pierścień z jednością ma co najmniej dwa elementy: 0 i 1.

Niech $\mathcal{K}$ będzie pierścieniem z jednością. Dla każdego $a \in \mathcal{K}$ mamy $a \cdot 0 + a = a \cdot (0+1) = a \cdot 1 = a$, więc $a \cdot 0 = 0$; podobnie pokazuje się, że $0 \cdot a = 0$. O pierścieniu mówimy, że jest *przemienny*, jeśli mnożenie jest przemienne. Np. zbiór liczb całkowitych $\mathbb{Z}$ jest pierścieniem przemiennym.

Element $a \neq 0$, dla którego istnieje $b \neq 0$ takie, że $ab = 0$, nazywa się *dzielnikiem zera*. Pierścień $\mathbb{Z}(2)$ wszystkich macierzy kwadratowych drugiego stopnia o elementach całkowitych ma dzielniki zera.

1.2.2. Ciała

Ciało to pierścień $\mathcal{K}$ z jednością taki, że zbiór $\mathcal{K}^\times = \mathcal{K} \setminus \{0\}$ jest grupą względem mnożenia. Ciało nie ma dzielników zera. Pierścień $\mathbb{Z}$ nie ma dzielników zera, ale nie jest ciałem. „Najmniejszy” pierścień $\mathbb{F}_2 = \{0, 1\}$ – w którym $1 + 1 = 0$ – jest ciałem.

Zbiory $\mathbb{R}$, $\mathbb{Q}$ i $\mathbb{C}$ są ciałami przemiennymi.

Zbiór kwaternionów $\mathbb{H}$ jest ciałem nieprzemiennym[2]: każdy element w $\mathbb{H}$ jest postaci $q = v + x\mathrm{i} + y\mathrm{j} + z\mathrm{k}$, gdzie $v, x, y, z \in \mathbb{R}$, a jednostki kwaternionowe $\mathrm{i}, \mathrm{j}, \mathrm{k}$ spełniają warunki

$$\mathrm{i}^2 = \mathrm{j}^2 = -1, \quad \mathrm{ij} + \mathrm{ji} = 0, \quad \mathrm{k} = \mathrm{ij}. \tag{1.5}$$

Wprowadzając sprzężenie $q \mapsto \bar{q} = v - x\mathrm{i} - y\mathrm{j} - z\mathrm{k}$, mamy $\bar{q}q = q\bar{q} = v^2 + x^2 + y^2 + z^2$. Jeśli $q \neq 0$, to q ma odwrotność $q^{-1} = \bar{q}/(\bar{q}q)$.

Jeśli $\mathcal{K}$ jest pierścieniem z jednością, to zbiór $\mathcal{K}(n)$ wszystkich macierzy kwadratowych stopnia n o elementach należących do $\mathcal{K}$ jest pierścieniem, którego jednością jest macierz jednostkowa I.

Przykład 1.11. Każde ciało $\mathcal{K}$ jest grupą przemienną względem dodawania; zbiór $\mathcal{K}^\times$ jest grupą względem mnożenia. Zbiór $\mathbb{H}^\times$ kwaternionów różnych od zera jest grupą nieprzemienną względem mnożenia.

1.2.3. Ideały

Jeśli $\mathcal{L}$ jest podgrupą grupy abelowej pierścienia $(\mathcal{K}, +, \cdot)$, to można utworzyć grupę ilorazową $\mathcal{K}/\mathcal{L}$, która też jest przemienna. Niech $k + \mathcal{L}$ oznacza warstwę zawierającą $k \in \mathcal{K}$; oznaczmy też

$$\mathcal{L}\mathcal{K} = \{lk \mid k \in \mathcal{K},\, l \in \mathcal{L}\}, \quad \mathcal{K}\mathcal{L} = \{kl \mid k \in \mathcal{K},\, l \in \mathcal{L}\}.$$

[2]Wielu autorów włącza przemienność do definicji ciała; wtedy zbiór kwaternionów nie jest ciałem, ale „pierścieniem z dzieleniem”. Ze względu na teorię reprezentacji grup wygodnie jest jednak uważać $\mathbb{H}$ za ciało i dopuszczać je w definicji przestrzeni wektorowych. Reprezentacje grup i algebr w takich przestrzeniach występują w naturalny sposób (zob. str. 90 i stwierdzenie 3.7, str. 89).

Czy można w ilorazie $\mathcal{K}/\mathcal{L}$ określić strukturę pierścienia w taki sposób, aby odwzorowanie kanoniczne $\mathcal{K} \to \mathcal{K}/\mathcal{L}$ było homomorfizmem pierścieni? Do tego potrzeba i wystarcza, aby podgrupa $\mathcal{L}$ była *ideałem dwustronnym* w $\mathcal{K}$, tzn. $\mathcal{L}\mathcal{K} \subset \mathcal{L}$ oraz $\mathcal{K}\mathcal{L} \subset \mathcal{L}$. Istotnie, wtedy wzór $(k + \mathcal{L}) \cdot (k' + \mathcal{L}) = kk' + \mathcal{L}$ poprawnie określa w $\mathcal{K}/\mathcal{L}$ mnożenie elementów, definiujące w tym zbiorze strukturę pierścienia.

Niech $\mathcal{K} = \mathbb{Z}$ będzie pierścieniem liczb całkowitych; podgrupa $\mathcal{L} = n\mathbb{Z}$ liczb podzielnych przez $n \in \mathbb{N}$ jest ideałem dwustronnym pierścienia $\mathbb{Z}$. Pierścień $\mathbb{Z}/n\mathbb{Z}$ jest przemienny i ma n elementów; jako grupa jest on izomorficzny grupie $\mathbb{Z}_n$ pierwiastków stopnia n z 1.

1.2.4. Ciała $\mathbb{F}_p$

Kiedy pierścień $\mathbb{Z}/n\mathbb{Z}$ jest ciałem? Aby to rozstrzygnąć, można się posłużyć następującym stwierdzeniem, będącym konsekwencją *algorytmu Euklidesa* znajdowania największego wspólnego dzielnika pary liczb całkowitych:

Stwierdzenie 1.12. *Jeśli $p, q \in \mathbb{Z}$, to równanie*

$$px + qy = 1 \tag{1.6}$$

ma rozwiązanie w liczbach całkowitych x, y wtedy i tylko wtedy, gdy liczby p i q są względnie pierwsze.

Dowód. Przypomnijmy, że jeśli $m, n \in \mathbb{Z}$ i $n > 0$, to reszta z dzielenia m przez n jest liczbą całkowitą r taką, iż $0 \leqslant r < n$ i $m = ns + r$, gdzie $s \in \mathbb{Z}$. (Np. jeśli $m = -7$ i $n = 3$, to $r = 2$.) Jeśli $r = 0$, to n dzieli m, co zapisuje się w postaci $n \mid m$.

Niech p i q będą liczbami całkowitymi, z których przynajmniej jedna nie jest zerem; istnieje wtedy ich *największy wspólny dzielnik*, tzn. taka liczba naturalna d, która dzieli p i q oraz ma tę własność, że jeśli $d' \mid p$ i $d' \mid q$, to $d' \mid d$. Zbiór $Z = \{px' + qy' \mid x', y' \in \mathbb{Z}\}$ zawiera liczby dodatnie; niech

$$d = px + qy \tag{1.7}$$

będzie najmniejszą z nich. Dzieląc p przez d, otrzymuje się

$$p = ds + r, \quad \text{gdzie} \quad 0 \leqslant r < d,$$

czyli

$$r = p - ds = p(1 - xs) - qys \in Z;$$

ale $0 \leqslant r < d$, więc $r = 0$. Zatem $d \mid p$. Podobnie pokazuje się, że $d \mid q$. Jeśli d' jest dowolnym dzielnikiem p i q, to d' dzieli (1.7), więc d jest największym wspólnym dzielnikiem p i q. W szczególności, jeśli p i q są względnie pierwsze, to $d = 1$ i równość (1.7) przyjmuje postać (1.6). □

Wniosek. *Pierścień $\mathbb{Z}/p\mathbb{Z}$ jest ciałem wtedy i tylko wtedy, gdy p jest liczbą pierwszą.*

Dowód. Jeśli p jest liczbą pierwszą, to odwrotnością elementu $q + p\mathbb{Z}$, gdzie $q \not\equiv 0 \bmod p$, jest element $y + p\mathbb{Z}$ taki, że zachodzi (1.6). Jeśli p nie jest liczbą pierwszą, czyli $p = rs$, gdzie $r, s > 1$, to

$$(r + p\mathbb{Z})(s + p\mathbb{Z}) = p\mathbb{Z}. \qquad \square$$

Jeśli p jest liczbą pierwszą, to ciało $\mathbb{Z}/p\mathbb{Z}$ oznacza się przez $\mathbb{F}_p$.

O ciele $\mathcal{K}$ mówimy, że ma *charakterystykę* p, jeśli p jest najmniejszą (dodatnią) liczbą naturalną taką, że $ps = 0$ dla każdego $s \in \mathcal{K}$. Np. ciało $\mathbb{F}_p$ ma charakterystykę p. Jeśli nie ma takiej liczby $p \neq 0$, że $ps = 0$ dla każdego $s \in \mathcal{K}$, to mówimy, że ciało $\mathcal{K}$ ma *charakterystykę* 0.

1.2.5. Zbiory uporządkowane

Zbiór E z relacją $\preccurlyeq$ zwrotną, przechodnią i taką, że dla dowolnych $x, y, z \in E$ zachodzi warunek

$$\text{jeśli} \quad x \preccurlyeq y \text{ i } y \preccurlyeq x, \quad \text{to} \quad x = y,$$

nazywa się zbiorem (częściowo) *uporządkowanym.* Zbiór jest *liniowo uporządkowany*, jeśli ponadto dla każdej pary $x, y \in E$ mamy $x \preccurlyeq y$ lub $y \preccurlyeq x$. Jeśli $X \subset E$, to element $a \in X$ taki, że $a \preccurlyeq x$ dla każdego $x \in X$, nazywa się elementem *najmniejszym* w X. Element *minoryzujący* zbiór X to taki element $a \in E$, że $a \preccurlyeq x$ dla każdego $x \in X$. Podobnie definiuje się elementy *największe* i *majoryzujące. Kres dolny* zbioru X to element $\inf X$ największy spośród elementów minoryzujących zbiór X. Podobnie definiuje się *kres górny* $\sup X$. *Krata* to zbiór uporządkowany, którego każdy skończony podzbiór posiada oba kresy. Każdy zbiór liniowo uporządkowany jest kratą.

1.2.6. Pierścienie Boole'a

Ważnym przykładem kraty jest *pierścień Boole'a*, tzn. taki pierścień $(E, +, \cdot)$, którego każdy element a jest *idempotentny*, tzn. $a^2 = a$. Wykorzystując równości $(-a)^2 = -a$ oraz $(a + b)^2 = a + b$, $a, b \in E$, otrzymuje się

$$a + a = 0 \quad \text{oraz} \quad ab = ba.$$

W pierścieniu Boole'a w naturalny sposób wprowadza się relację uporządkowania, definiując

$$a \preccurlyeq b \iff ab = a.$$

Łatwo sprawdzić następujące fakty:

(i) $\inf\{a, b\} = ab$ oraz $\sup\{a, b\} = a + ab + b$,

(ii) 0 jest najmniejszym elementem w E,

(iii) jeśli pierścień ma jedność 1 (wtedy E jest *algebrą Boole'a* – ale nie algebrą w znaczeniu §2), to 1 jest elementem największym w E.

Ważnym przykładem pierścienia Boole'a jest dowolna rodzina E podzbiorów zbioru Z taka, że jeśli $X, Y \in E$, to zbiory $X + Y \overset{\text{def}}{=} (X \cup Y) \setminus (X \cap Y)$ oraz $X \cdot Y \overset{\text{def}}{=} X \cap Y$ także należą do E. Tutaj 0 oznacza $\emptyset$, $\preccurlyeq$ oznacza $\subseteq$, $\inf\{X, Y\} = X \cap Y$ itd.

1.3. Moduły i przestrzenie wektorowe

1.3.1. Moduły

Grupa przemienna $(V, +)$ jest *lewym modułem* nad pierścieniem $(\mathcal{K}, +, \cdot)$, jeśli dane jest odwzorowanie

$$\mathcal{K} \times V \to V, \quad (a, v) \mapsto a.v,$$

takie, że dla dowolnych $a, b \in \mathcal{K}$ oraz $u, v \in V$ zachodzą równości

$$a.(u+v) = a.u+a.v, \quad (a+b).u = a.u+b.u, \quad a.(b.v) = (a\cdot b).v, \quad 1.u = u.$$

Wynika stąd, że $a.0 = 0$ oraz $a.(-u) = -a.u$. Podobnie definiuje się prawy moduł: mnożenie $V \times \mathcal{K} \to V$, $(v, a) \mapsto v.a$, jest rozdzielne względem dodawania oraz $(v.a).b = v.(a \cdot b)$. Kropki $\cdot$ i . zwykle się pomija.

1.3.2. Przestrzenie wektorowe

Lewy [prawy] moduł nad ciałem nazywa się *lewą* [*prawą*] *przestrzenią wektorową*. Gdy ciało jest przemienne, mówimy po prostu o *przestrzeni wektorowej.*

Niech V będzie lewą przestrzenią wektorową nad ciałem $\mathcal{K}$; ciąg $(e_1, \ldots, e_k)$ elementów tej przestrzeni jest *liniowo niezależny*, jeśli równość $\mu_1 e_1 + \cdots + \mu_k e_k = 0$, gdzie $\mu_1, \ldots, \mu_k \in \mathcal{K}$, implikuje $\mu_1 = \cdots = \mu_k = 0$.

Jeśli przestrzeń V zawiera liniowo niezależny ciąg $(e_1, \ldots, e_m)$, a każdy ciąg zawierający więcej niż m wektorów jest liniowo zależny, to mówimy, że przestrzeń V jest *m-wymiarowa* i że $e = (e_1, \ldots, e_m)$ jest *bazą* (albo *reperem*) w V.

Jeśli ciało $\mathcal{K}$ jest przemienne, a macierz $a = (a^i{}_j)$, $a^i{}_j \in \mathcal{K}$, $i, j \in \{1, \ldots, m\}$, jest odwracalna, to ciąg

$$(e'_1, \ldots, e'_m), \quad \text{gdzie} \quad e'_j = e_i a^i{}_j \quad (\text{krócej: } e' = ea), \tag{1.8}$$

też jest bazą i każdą bazę można tak otrzymać z bazy $(e_1, \ldots, e_m)$. We wzorze (1.8) zastosowano *umowę sumacyjną* (Einsteina) względem wskaźnika i

występującego u góry i u dołu (tzn. pominięto znak sumy $\sum_i$); umowa ta, rozpowszechniona wśród fizyków, jest w tym tekście stale stosowana.

Każdy wektor $v \in V$ jest postaci $v = v^i e_i$, gdzie $v^i \in \mathcal{K}$ nazywamy itą składową wektora względem tej bazy. Zwykle zapis bazy $(e_1, \dots, e_m)$ skraca się do $(e_i)_{i=1}^m$ lub (e_i).

Przykład 1.13. Dla dowolnego ciała $\mathcal{K}$ zbiór $\mathcal{K}^m$ ma strukturę m-wymiarowej przestrzeni wektorowej nad $\mathcal{K}$. *Baza kanoniczna* w tej przestrzeni składa się z wektorów

$$\begin{aligned} e_1 &= (1, 0, \dots, 0), \\ e_2 &= (0, 1, \dots, 0), \\ &\dots \\ e_m &= (0, 0, \dots, 1). \end{aligned}$$

Zbiór $\mathbb{H}^m$ jest lewą (a także prawą) przestrzenią wektorową nad ciałem $\mathbb{H}$ o wymiarze $\dim_{\mathbb{H}} \mathbb{H}^m = m$. Można także rozpatrywać zbiór $\mathbb{H}^m$ jako przestrzeń wektorową nad $\mathbb{R}$ o wymiarze $\dim_{\mathbb{R}} \mathbb{H}^m = 4m$.

1.3.3. Odwzorowania liniowe

Niech V i W będą *lewymi* przestrzeniami wektorowymi nad ciałem $\mathcal{K}$ o wymiarach odpowiednio m i n. Odwzorowanie $h : V \to W$ nazywa się *$\mathcal{K}$-liniowym*, jeśli dla dowolnych $\lambda, \mu \in \mathcal{K}$ i $u, v \in V$ zachodzi równość

$$h(\lambda u + \mu v) = \lambda h(u) + \mu h(v).$$

Mówi się także wtedy, że h jest *homomorfizmem* V w W. Zbiór wszystkich takich homomorfizmów oznacza się przez $\mathsf{Hom}_{\mathcal{K}}(V, W)$. Jeśli ciało $\mathcal{K}$ jest ustalone w rozważaniach, to zwykle pisze się $\mathsf{Hom}(V, W)$ zamiast $\mathsf{Hom}_{\mathcal{K}}(V, W)$.

Homomorfizm, który jest bijekcją, nazywamy *izomorfizmem*. Homomorfizm $f : V \to V$ jest *endomorfizmem* przestrzeni V; piszemy $f \in \mathsf{End}\, V = \mathsf{Hom}(V, V)$.

Zbiór $\mathsf{GL}(V)$ tych wszystkich endomorfizmów przestrzeni wektorowej V, które są izomorfizmami, jest grupą i nazywa się (ogólną) *grupą liniową* przestrzeni V. Jeśli $V = \mathcal{K}^m$, to zamiast $\mathsf{GL}(V)$ piszemy $\mathsf{GL}(m, \mathcal{K})$: jest to grupa odwracalnych macierzy kwadratowych stopnia m o elementach należących do ciała $\mathcal{K}$.

Jeśli ciało $\mathcal{K}$ jest przemienne, to zbiór $\mathsf{Hom}(V, W)$ ma naturalną strukturę przestrzeni wektorowej wymiaru mn: mając bazy $(e_i)_{i=1}^m$ i $(f_k)_{k=1}^n$ w przestrzeniach odpowiednio V i W, bazę w $\mathsf{Hom}(V, W)$ można utworzyć w postaci ciągu mn odwzorowań liniowych $j_k^i : V \to W$ takich, że

$$\text{jeśli} \quad v = v^i e_i, \quad \text{to} \quad j_k^i(v) = v^i f_k. \tag{1.9}$$

Baza (e_i) w m-wymiarowej przestrzeni V nad $\mathcal{K}$ określa izomorfizm

$$e : \mathcal{K}^m \to V, \quad (v^1, \dots, v^m) \mapsto v^i e_i, \tag{1.10}$$

i na odwrót, każdy izomorfizm $\mathcal{K}^m \to V$ określa bazę w V (obraz bazy kanonicznej).

1.3.4. Przestrzenie dualne

Przestrzeń

$$V^* \stackrel{\text{def}}{=} \mathsf{Hom}(V, \mathcal{K})$$

nazywa się przestrzenią *dualną* do V lub przestrzenią *form* (liniowych) na przestrzeni V. Jeśli V jest lewą przestrzenią nad $\mathcal{K}$, to V^* ma naturalną strukturę prawej przestrzeni nad $\mathcal{K}$: jeśli $v \in V$, $\alpha \in V^*$ i $\lambda, \mu \in \mathcal{K}$, to definiując $(\alpha\mu)(v) = \alpha(v)\mu$, mamy $(\alpha\mu)(\lambda v) = \alpha(\lambda v)\mu = \lambda(\alpha\mu)(v)$. Jeśli V ma wymiar skończony, to przestrzenie V i V^* są tego samego wymiaru. Wartość formy $\alpha \in V^*$ na wektorze $v \in V$ oznacza się często przez $\langle v, \alpha \rangle$.

Jeśli (e_i) jest bazą w n-wymiarowej przestrzeni V, to *baza dualna* (e^i) do niej składa się z form e^j takich, że

$$\langle e_i, e^j \rangle = \delta_i^j, \quad i, j = 1, \dots, n,$$

gdzie *delta Kroneckera* jest określona wzorem

$$\delta_i^j = \begin{cases} 1 & \text{dla } i = j, \\ 0 & \text{dla } i \neq j. \end{cases}$$

Czasami deltę Kroneckera zapisuje się jako δ_{ij}.

Jeśli $e : \mathcal{K}^n \to V$ jest izomorfizmem odpowiadającym bazie (e_i) na mocy (1.10), to bazie dualnej odpowiada izomorfizm

$$e^{-1} : V \to \mathcal{K}^n, \quad v \mapsto (\langle v, e^1 \rangle, \dots, \langle v, e^n \rangle).$$

Wektory, formy i homomorfizmy przedstawia się często za pomocą macierzy utworzonych z ich składowych. Np. definiując $v = v^i e_i$ i $\alpha = e^i \alpha_i$ oraz zapisując $\langle v, \alpha \rangle$ w postaci

$$\begin{pmatrix} v^1 & v^2 & \dots & v^n \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}$$

uwidacznia się fakt, że jeśli wektory mnoży się przez skalary z lewej, to formy – z prawej strony.

1.3.5. Odwzorowania transponowane

Jeśli $h \in \mathsf{Hom}(V, W)$, to odwzorowanie $h^* \in \mathsf{Hom}(W^*, V^*)$ zdefiniowane wzorem[3]

$$(1.11) \qquad \langle h(v), \alpha \rangle = \langle v, h^*(\alpha) \rangle \quad \text{dla wszystkich } v \in V \text{ i } \alpha \in W^*$$

nazywa się odwzorowaniem *transponowanym* albo *dualnym* do h. Rozkładając homomorfizm $h \in \mathsf{Hom}(V, W)$ względem bazy j^i_k określonej w (1.9), $h = h_i{}^k j^i_k$, można równość (1.11) zinterpretować na podstawie

$$\begin{pmatrix} v^1 & v^2 & \dots & v^m \end{pmatrix} \begin{pmatrix} h_1{}^1 & h_1{}^2 & \dots & h_1{}^n \\ h_2{}^1 & h_2{}^2 & \dots & h_2{}^n \\ \vdots & \vdots & \vdots & \vdots \\ h_m{}^1 & h_m{}^2 & \dots & h_m{}^n \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix},$$

obliczając najpierw pierwszy – albo drugi – iloczyn dwóch spośród tych trzech macierzy.

Jeśli $f \in \mathsf{Hom}(V, W)$ i $g \in \mathsf{Hom}(U, V)$, to $f \circ g \in \mathsf{Hom}(U, W)$ oraz

$$(f \circ g)^* = g^* \circ f^* \quad \text{i} \quad \mathrm{id}_V^* = \mathrm{id}_{V^*}\,.$$

1.3.6. Wzmianka o kategoriach i funktorach

W języku *teorii kategorii* [68, 69] mówi się, że odpowiedniość

$$f \mapsto f^*, \quad V \mapsto V^*,$$

jest *funktorem kontrawariantnym* z kategorii przestrzeni wektorowych nad $\mathcal{K}$ w tę samą kategorię.

Iteracja funktora $*$, tzn. odpowiedniość $f \mapsto f^{**} \overset{\text{def}}{=} (f^*)^*$, $V \mapsto V^{**}$, jest *funktorem kowariantnym*: $(f \circ g)^{**} = f^{**} \circ g^{**}$.

Jeśli przestrzeń V ma skończony wymiar, to V, V^* i V^{**} są tego samego wymiaru; ponadto V i V^{**} można utożsamić, bo dla każdej skończenie wymiarowej przestrzeni wektorowej V istnieje *izomorfizm naturalny* $N_V : V \to V^{**}$, określony wzorem

$$(1.12) \qquad \langle \alpha, N_V(v) \rangle = \langle v, \alpha \rangle \quad \text{dla wszystkich } v \in V,\ \alpha \in V^*$$

[3] Ostrzeżenie: w literaturze fizycznej i technicznej często używa się zapisu f^* na oznaczenie sprzężenia zespolonego wielkości f. W niniejszym tekście sprzężenie zespolone jest zapisywane jako $\bar{f}$.

i mający tę własność, że jeśli $h \in \mathsf{Hom}(V, W)$, to diagram

$$\begin{tikzcd} V \arrow[r, "h"] \arrow[d, "N_V"'] & W \arrow[d, "N_W"] \\ V^{**} \arrow[r, "h^{**}"] & W^{**} \end{tikzcd}$$

jest przemienny. Po utożsamieniu V i V^{**} pomija się N_V; zamiast (1.12) można napisać $\langle \alpha, v \rangle = \langle v, \alpha \rangle$. Często stosuje się takie naturalne utożsamienia także w innych sytuacjach; teoria kategorii została rozwinięta m.in. po to, aby nadać ścisłe znaczenie pojęciu naturalności (zob. [67, str. 48]).

1.3.7. Podprzestrzenie

Jeśli U jest podzbiorem przestrzeni wektorowej V nad $\mathcal{K}$ i przestrzenią wektorową względem działań w V, to mówimy, że U jest *podprzestrzenią wektorową* w V. Można wtedy utworzyć iloraz V/U, którego elementy to klasy

$$[v] = \{v' \in V \mid v' - v \in U\};$$

często wygodnie jest pisać $v + U$ zamiast $[v]$. Iloraz V/U jest przestrzenią wektorową względem działań

$$[v] + [v'] = [v + v'], \quad \lambda[v] = [\lambda v], \quad v, v' \in V,\ \lambda \in \mathcal{K}.$$

Niech wymiary przestrzeni V i U będą równe odpowiednio m i $n \leqslant m$. Można wybrać w V bazę (e_i) *dostosowaną do* U, tzn. taką, że $(e_1, \dots, e_n)$ jest bazą w U; wtedy ciąg $([e_{n+1}], \dots, [e_m])$ jest bazą w V/U, więc $\dim(V/U) = \dim V - \dim U$. Liczbę $\dim(V/U)$ nazywa się *kowymiarem* podprzestrzeni U w V.

Ciąg homomorfizmów

$$0 \to U \xrightarrow{i} V \xrightarrow{p} V/U \to 0, \quad i(v) = v, \quad p(v) = [v],$$

jest *dokładny*, co oznacza tu, że odwzorowanie i jest injekcją, zachodzi równość $\operatorname{img} i = \ker p$, a homomorfizm p jest surjekcją.

1.3.8. Suma i suma prosta przestrzeni wektorowych

Sumą prostą przestrzeni wektorowych V i W nad $\mathcal{K}$ jest przestrzeń $V \oplus W$, której zbiór wektorów jest iloczynem kartezjańskim $V \times W$, a działania są określone wzorami $(v, w) + (v', w') = (v + v', w + w')$ i $\lambda(v, w) = (\lambda v, \lambda w)$ dla wszystkich $v, v' \in V$, $w, w' \in W$ i $\lambda \in \mathcal{K}$.

Ogólniej, jeśli $(V_\iota)_{\iota \in I}$ jest rodziną przestrzeni wektorowych, to można utworzyć ich sumę prostą $\bigoplus_{\iota \in I} V_\iota$; z definicji, składa się ona z takich ciągów

$(a_\iota)_{\iota\in I}$, gdzie $a_\iota \in V_\iota$, że tylko skończenie wiele elementów a_ι jest różnych od zera, a działania definiujemy w naturalny sposób.

Jeśli V i W są podprzestrzeniami wektorowymi przestrzeni wektorowej U, to można utworzyć ich *sumę*

$$V + W = \{v + w \mid v \in V,\ w \in W\},$$

która jest podprzestrzenią wektorową w U. Jeśli V i W są skończenie wymiarowe, to

$$\dim(V + W) = \dim V + \dim W - \dim(V \cap W).$$

Jeśli ponadto $V \cap W = \{0\}$, to także w tym wypadku mówimy, że suma ta jest prosta, i zapisujemy ją jako $V \oplus W \subset U$. Ogólniej, jeśli $(V_\iota)_{\iota\in I}$ jest rodziną podprzestrzeni wektorowych przestrzeni U, to można utworzyć ich sumę $\sum_{\iota\in I} V_\iota \subset U$.

1.3.9. Gradacja przestrzeni wektorowej

Niech $\mathcal{Z}$ oznacza pierścień $\mathbb{Z}$ albo $\mathbb{F}_2$ i niech V będzie przestrzenią wektorową nad ciałem $\mathcal{K}$. Jeśli istnieje rozkład

$$V = \bigoplus_{k\in\mathcal{Z}} V_k$$

na sumę prostą podprzestrzeni indeksowanych elementami pierścienia $\mathcal{Z}$, to mówimy, że przestrzeń V ma strukturę *przestrzeni wektorowej z gradacją* względem $\mathcal{Z}$. Np. przestrzeń wektorowa V wszystkich wielomianów zmiennej x nad $\mathbb{k} = \mathbb{R}$ lub $\mathbb{C}$ ma gradację względem $\mathbb{Z}$ taką, że $V_k = \{\lambda x^k \mid \lambda \in \mathbb{k}\}$ dla $k \in \mathbb{N}$ oraz $V_k = \{0\}$ dla $k < 0$.

1.4. Formy dwuliniowe

Niech V będzie skończenie wymiarową przestrzenią wektorową nad przemiennym ciałem $\mathcal{K}$ o charakterystyce $\neq 2$. *Forma dwuliniowa* na V to funkcja

$$h : V \times V \to \mathcal{K}$$

liniowa względem każdego argumentu z osobna. Forma dwuliniowa jest *niezdegenerowana* (lub *nieosobliwa*), jeśli $h(u, v) = 0$ dla wszystkich u implikuje $v = 0$.

1.4.1. Formy symetryczne i kwadratowe

Forma kwadratowa na V to funkcja $h : V \to \mathcal{K}$ taka, że dla wszystkich $\lambda \in \mathcal{K}$ i $u, v \in V$ zachodzi równość $h(\lambda v) = \lambda^2 h(v)$, a odwzorowanie

$$V \times V \to \mathcal{K}, \quad (u, v) \mapsto h(u, v) \overset{\text{def}}{=} \tfrac{1}{2}(h(u+v) - h(u) - h(v)),$$

jest formą dwuliniową. Jeśli ta forma jest niezdegenerowana, nazywa się ją *iloczynem skalarnym* na V.[4] Często najpierw definiuje się iloczyn skalarny jako niezdegenerowane symetryczne odwzorowanie dwuliniowe $h : V \times V \to \mathcal{K}$, a stowarzyszoną z nim formę kwadratową jako $v \mapsto h(v, v)$. Wtedy parę (V, h) nazywa się *przestrzenią kwadratową*. Dla każdego $v \in V$ odwzorowanie $V \to \mathcal{K}$, $u \mapsto h(u, v)$, jest liniowe; wygodna jest

Umowa 1.14. Jeśli h jest iloczynem skalarnym w V oraz $v \in V$, to przez $\underline{h}(v)$ oznaczamy element przestrzeni V^* taki, że

$$\langle u, \underline{h}(v) \rangle = h(u, v) \quad \text{dla każdego } u \in V.$$

Odwzorowanie $\underline{h} : V \to V^*$ jest izomorfizmem. Wprowadzając bazę (e_i) w V i bazę dualną (e^i) w V^*, możemy napisać

$$h(e_i, e_j) = h_{ij}, \quad \underline{h}(e_j) = e^i h_{ij}.$$

1.4.2. Grupy ortogonalne

Grupą automorfizmów przestrzeni kwadratowej (V, h) jest *grupa ortogonalna*

$$\mathsf{O}(V, h) = \{a \in \mathsf{GL}(V) \mid v \in V \Rightarrow h(av, av) = h(v, v)\}. \tag{1.13}$$

Jeśli $\lambda \in \mathcal{K}^\times$, to $\mathsf{O}(V, \lambda h) = \mathsf{O}(V, h)$. Jeśli $V = \mathbb{C}^n$, to pisze się $\mathsf{O}(n, \mathbb{C})$ zamiast $\mathsf{O}(V, h)$.

Jeśli (V, h) jest $(p+q)$-wymiarową rzeczywistą przestrzenią kwadratową, to istnieje w V *baza ortonormalna*, czyli taka, że jeśli $i \neq j$, to $h_{ij} = 0$, oraz

$$h_{ii} = 1 \text{ dla } 1 \leqslant i \leqslant p, \quad h_{ii} = -1 \text{ dla } p+1 \leqslant i \leqslant p+q.$$

---

[4] Matematycy, definiując iloczyn skalarny w rzeczywistych przestrzeniach wektorowych, zwykle zakładają, że stowarzyszona z nim forma kwadratowa jest *dodatnio określona*. Nadając szczególnej teorii względności postać matematyczną, Hermann Minkowski [79] wprowadził w przestrzeni $\mathbb{R}^4$ iloczyn skalarny i formę kwadratową o sygnaturze $(1, 3)$. Od tego czasu takie ogólniejsze iloczyny skalarne odgrywają ważną rolę w fizyce.

Parę (p, q) nazywa się *sygnaturą* formy h. (Poprawność tej definicji wynika z twierdzenia Sylvestera o bezwładności form kwadratowych – zob. np. [69, rozdz. XIV].) Liczbę $q-p$ nazywa się *indeksem* formy h.[5] Grupę $\mathsf{O}(V, h)$ oznacza się w tym wypadku przez $\mathsf{O}(p, q)$. W szczególności $\mathsf{O}(n) \overset{\text{def}}{=} \mathsf{O}(n, 0)$ jest grupą składającą się ze wszystkich macierzy $a \in \mathbb{R}(n)$ takich, że $a^* a = I$, gdzie a^* jest macierzą transponowaną do a.

Z przestrzenią kwadratową (V, h) nad $\mathbb{k} = \mathbb{R}$ lub $\mathbb{C}$ można w naturalny sposób związać także inne obiekty algebraiczne; przydatna będzie

Umowa 1.15. Jeśli Ω jest obiektem algebraicznym stowarzyszonym z przestrzeniami kwadratowymi, a przestrzeń (V, h) jest zespolona m-wymiarowa (lub rzeczywista, a h ma sygnaturę (p, q)) to piszemy $\Omega(m, \mathbb{C})$ (odpowiednio $\Omega(p, q)$) zamiast $\Omega(V, h)$.

Liczne zastosowania tej umowy występują w rozdziale VIII.

1.4.3. Wektory i podprzestrzenie optyczne

Wektor $v \in V$ taki, że $h(v, v) = 0$, będzie tu nazywany *wektorem optycznym*. Nazwa ta została zaproponowana przez Élie Cartana (*vecteur optique*). W anglojęzycznej literaturze fizycznej stosowana jest nazwa *null vector*. Matematycy używają w tym kontekście terminu *wektor izotropowy*. Nazwa ta nawiązuje do spostrzeżenia, że w przestrzeni wektorowej $\mathbb{C}^2$ z formą kwadratową

$$\mathbb{C}^2 \to \mathbb{C}, \quad (z, w) \mapsto z^2 + w^2,$$

pod wpływem obrotu o kąt α, wektor $(z, \mathrm{i}z)$ przechodzi na

$$\begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} z \\ \mathrm{i}z \end{pmatrix} = \exp(\mathrm{i}\alpha) \begin{pmatrix} z \\ \mathrm{i}z \end{pmatrix}.$$

Kierunek tego wektora nie zmienia się pod wpływem obrotów, jest więc on „izotropowy”. Spostrzeżenie to nie uogólnia się na przestrzenie o większej liczbie wymiarów.

Wektor $v = 0$ jest oczywiście wektorem optycznym. W przestrzeni $\mathbb{R}^2$ z iloczynem skalarnym h o sygnaturze $(1, 1)$ istnieją niezerowe wektory optyczne: jeśli $e_1, e_2 \in \mathbb{R}^2$, $h(e_1, e_1) = -h(e_2, e_2) \neq 0$ i $h(e_1, e_2) = 0$, to wektory $e_1 + e_2$ i $e_1 - e_2$ są optyczne.

[5] Wydaje się, że nie ma ogólnie przyjętej terminologii dotyczącej własności rzeczywistych form kwadratowych. Bourbaki nazywa indeksem takiej formy wymiar maksymalnych podprzestrzeni całkowicie optycznych, tzn. liczbę $\min(p, q)$ (zob. [15, §4, n°2]). Van der Waerden nazywa indeksem inercji liczbę q ujemnych kwadratów formy (zob. [117, §90]). Deligne [31] nazywa $p - q$ sygnaturą formy h.

Niech (V, h) będzie przestrzenią kwadratową nad $\Bbbk$ (= $\mathbb{R}$ lub $\mathbb{C}$) i $X \subset V$; zbiór

$$X^\perp = \{v \in V \mid x \in X \Rightarrow h(v, x) = 0\}$$

jest podprzestrzenią wektorową.

Podprzestrzeń $K \subset V$ nazywa się przestrzenią *całkowicie optyczną*, jeśli $K \subset K^\perp$; wtedy każdy element w K jest wektorem optycznym. Jeśli przestrzeń V jest m-wymiarowa, a całkowicie optyczna podprzestrzeń K ma wymiar p, to $K \subset K^\perp$ implikuje $p \leqslant m - p$. Wynika stąd, że jeśli $m = 2n$ lub $2n + 1$, to $p \leqslant n$.

Dla każdego m istnieją przestrzenie kwadratowe zawierające podprzestrzenie całkowicie optyczne maksymalnego wymiaru n. Np. jeśli V jest n-wymiarową przestrzenią rzeczywistą, to w przestrzeni $W = V \oplus V^*$ można wprowadzić naturalną formę kwadratową h, definiując, dla $v + v' \in V \oplus V^*$,

$$h(v + v', v + v') = 2\langle v, v' \rangle.$$

Forma h ma sygnaturę (n, n). Obie przestrzenie V i V^* są całkowicie optycznymi podprzestrzeniami maksymalnego wymiaru.

O formie h lub o przestrzeni (V, h) mówimy, że jest *neutralna*, jeśli V ma podprzestrzenie całkowicie optyczne maksymalnego wymiaru. Wszystkie zespolone przestrzenie kwadratowe wymiaru $\geqslant 2$ są neutralne.[6] Rzeczywista przestrzeń kwadratowa jest neutralna wtedy i tylko wtedy, gdy jej forma ma sygnaturę (n, n), $(n + 1, n)$ albo $(n, n + 1)$, $n = 1, 2, \ldots$.

1.4.4. Wektorowa przestrzeń euklidesowa

Rzeczywista przestrzeń kwadratowa (V, h) nazywa się *euklidesową przestrzenią wektorową* (krótko: *przestrzenią euklidesową*), jeśli forma kwadratowa h jest *dodatnio określona*, tzn. $h(v) > 0$ dla $v \neq 0$. Istnieje wtedy baza ortonormalna (e_i) taka, że $h(e_i, e_j) = \delta_{ij}$, więc $\underline{h}(e_i) = e^i$.

Przykład 1.16. Wektory w przestrzeni $\mathbb{R}^3$ oznacza się często literami półgrubymi, np. $\mathbf{U} = (U_x, U_y, U_z)$, $\mathbf{V} = (V_x, V_y, V_z)$, a ich (dodatnio określony) iloczyn skalarny – kropką: $\mathbf{U} \cdot \mathbf{V} = U_x V_x + U_y V_y + U_z V_z$. Wprowadza się także iloczyn „wektorowy”, $\mathbf{U} \times \mathbf{V} = (U_y V_z - U_z V_y, U_z V_x - U_x V_z, U_x V_y - U_y V_x)$, oraz iloczyn „mieszany” trzech wektorów, $(\mathbf{U} \times \mathbf{V}) \cdot \mathbf{W}$, będący miarą objętości równoległościanu, mającego te trzy wektory jako krawędzie.

---

[6] Przyjęta tu definicja różni się od tej w [15, §4, n°2]. Według Bourbakiego przestrzeń nieparzystowymiarowa nie może mieć formy neutralnej.

1.4.5. Formy i grupy symplektyczne

O formie dwuliniowej $h : V \times V \to \mathcal{K}$ mówimy, że jest *antysymetryczna*, jeśli $h(u,v) + h(v,u) = 0$ dla wszystkich $u, v \in V$. Forma *symplektyczna* to niezdegenerowana forma antysymetryczna. Jeśli w przestrzeni wektorowej istnieje forma symplektyczna, to wymiar przestrzeni jest liczbą parzystą. Jeśli h jest formą symplektyczną w przestrzeni V, to para (V, h) nazywa się *przestrzenią symplektyczną*.

Przykład 1.17. Jeśli $(e_1, \dots, e_{2l})$ jest bazą w przestrzeni wymiaru $2l$ i $u = u^\mu e_\mu$, $v = v^\nu e_\nu$, $\mu, \nu = 1, \dots, 2l$, to wzór

$$h(u,v) = u^1 v^{l+1} - u^{l+1} v^1 + \cdots + u^l v^{2l} - u^{2l} v^l$$

określa formę symplektyczną w tej przestrzeni.

Grupą automorfizmów przestrzeni symplektycznej (V, h) jest *grupa symplektyczna*

$$\mathsf{Sp}(V,h) = \{a \in \mathsf{GL}(V) \mid u, v \in V \Rightarrow h(au, av) = h(u,v)\}. \tag{1.14}$$

1.5. Iloczyny tensorowe

Niech V i W będą skończenie wymiarowymi przestrzeniami wektorowymi nad $\Bbbk = \mathbb{R}$ lub $\mathbb{C}$, o wymiarach i z bazami jak w paragrafie 1.3.3. Ich *iloczyn tensorowy* można zdefiniować jako

$$V \otimes_\Bbbk W \stackrel{\text{def}}{=} \mathsf{Hom}(V^*, W). \tag{1.15}$$

Jeśli ciało $\Bbbk$ jest ustalone w rozważaniach, to zwykle pomija się je w zapisie iloczynu tensorowego. Iloczyn tensorowy nieskończenie wymiarowych przestrzeni wektorowych wymaga innej, ogólniejszej definicji (zob. [11, rozdz. IX, §2]).

Stwierdzenie 1.18. *Odwzorowanie*

$$i : V \times W \to V \otimes W, \quad i(v,w)\alpha = \langle v, \alpha \rangle w, \quad \alpha \in V^*,$$

jest dwuliniowe i uniwersalne dla odwzorowań dwuliniowych, tzn. jeśli

$$h : V \times W \to U$$

jest dowolnym odwzorowaniem dwuliniowym, to istnieje odwzorowanie liniowe

$$h_\flat : V \otimes W \to U \quad \textit{takie, że} \quad h = h_\flat \circ i.$$

Dowód. Istotnie, bazy (e_i) w V i (f_k) w W określają bazę (j_{ik}) w $V \otimes W = \mathsf{Hom}(V^*, W)$ taką, że

$$j_{ik}(\alpha) = \langle e_i, \alpha \rangle f_k.$$

Mając h, definiuje się $h_{ik} = h(e_i, f_k)$ oraz $h_\flat$ jako odwzorowanie liniowe takie, że

$$h_\flat(j_{ik}) = h_{ik}. \qquad \square$$

Zgodnie z (1.15) pisze się

$$v \otimes w \overset{\text{def}}{=} i(v, w).$$

Posługując się stwierdzeniem 1.18, dowodzi się istnienia naturalnego izomorfizmu iloczynów tensorowych $U \otimes (V \otimes W)$ i $(U \otimes V) \otimes W$ (łączność iloczynu tensorowego – można pomijać nawiasy).

Przestrzeń *tensorów kontrawariantnych* stopnia k,

$$\bigotimes^k V = V \otimes \cdots \otimes V \quad (k \text{ czynników})$$

ma wymiar m^k: bazę tej przestrzeni można utworzyć jako ciąg, składający się z tensorów

$$e_{i_1} \otimes \cdots \otimes e_{i_k}, \quad i_1, \ldots, i_k = 1, \ldots, m.$$

Elementy iloczynu

$$\mathsf{T}^k_l(V) = (\bigotimes^k V) \otimes (\bigotimes^l V^*)$$

to *tensory o walencji* (k, l). Jeśli A jest takim tensorem, czyli

$$A = A^{i_1 \ldots i_k}_{j_1 \ldots j_l} e_{i_1} \otimes \cdots \otimes e_{i_k} \otimes e^{j_1} \otimes \cdots \otimes e^{j_l}$$

(gdzie (e^j) jest bazą w V^* dualną do (e_i)), to często używa się uproszczonego zwrotu „$A^{i_1 \ldots i_k}_{j_1 \ldots j_l}$ jest tensorem”; walencja tensora jest zakodowana w położeniu i liczbie wskaźników.

Przestrzeń $\mathsf{T}^0_k(V) = \mathsf{T}^k_0(V^*)$ jest dualna do $\mathsf{T}^k_0(V)$: jeśli $A \in \mathsf{T}^k_0(V)$ i $B \in \mathsf{T}^0_k(V)$, to

$$\langle A, B \rangle = A^{i_1 \ldots i_k} B_{i_1 \ldots i_k}.$$

1.6. Struktury rzeczywiste, zespolone i kwaternionowe

1.6.1. Kompleksyfikacja i realifikacja

Niech V będzie rzeczywistą przestrzenią wektorową; jej *kompleksyfikacja* $V^{\mathbb{C}}$ składa się ze wszystkich obiektów postaci $u + \sqrt{-1}\, v$, gdzie $u, v \in V$, z naturalnymi działaniami. Można wykazać, że przestrzeń $V^{\mathbb{C}}$ jest w naturalny sposób izomorficzna z iloczynem tensorowym $\mathbb{C} \otimes_{\mathbb{R}} V$. O przestrzeni V mówimy, że jest *formą rzeczywistą* przestrzeni $V^{\mathbb{C}}$. Jeśli przestrzeń V jest skończenie wymiarowa, to

$$\dim_{\mathbb{C}} V^{\mathbb{C}} = \dim_{\mathbb{R}} V.$$

Jeśli V jest zespoloną przestrzenią wektorową, to jej *realifikacja* $V^{\mathbb{R}}$ jest rzeczywistą przestrzenią wektorową, której zbiór wektorów i mnożenie ich przez liczby rzeczywiste są takie, jak w V. Jeśli V ma bazę $(e_1, \ldots, e_m)$, to ciąg $(e_1, \ldots, e_m, \sqrt{-1}\,e_1, \ldots, \sqrt{-1}\,e_m)$ jest bazą w $V^{\mathbb{R}}$, więc

$$\dim_{\mathbb{R}} V^{\mathbb{R}} = 2 \dim_{\mathbb{C}} V.$$

1.6.2. Struktura zespolona w rzeczywistej przestrzeni wektorowej

Niech V będzie rzeczywistą przestrzenią wektorową parzystego wymiaru. Mając endomorfizm J przestrzeni V taki, że $J \circ J = -\operatorname{id}_V$, można nadać tej przestrzeni strukturę zespolonej przestrzeni wektorowej V_J, przyjmując $\sqrt{-1}\,v = Jv$ dla każdego $v \in V$; wtedy $\dim_{\mathbb{C}} V_J = \frac{1}{2} \dim_{\mathbb{R}} V$. (Przestrzenie V i V_J mają te same zbiory wektorów.)

1.6.3. Odwzorowania półliniowe

Niech V i W będą zespolonymi przestrzeniami wektorowymi. Odwzorowanie $f : V \to W$ nazywa się *półliniowym*,[7] jeśli dla wszystkich $\lambda, \mu \in \mathbb{C}$ i $u, v \in V$ zachodzi równość

$$f(\lambda u + \mu v) = \bar{\lambda} f(u) + \bar{\mu} f(v).$$

Sprzężenie zespolone $\mathbb{C} \to \mathbb{C}$, $z \mapsto \bar{z}$, jest półliniowe.

Przestrzeń wektorową *sprzężoną* do V definiuje się jako przestrzeń $\bar{V}$, która ma ten sam zbiór elementów i strukturę grupy przemiennej co V, natomiast mnożenie wektora przez liczbę zespoloną w przestrzeni $\bar{V}$ jest poprzedzone sprzężeniem tej liczby. Obowiązuje umowa, że wektor v, rozpatrywany jako element przestrzeni $\bar{V}$, jest zapisywany w postaci $\bar{v}$, więc

$$\lambda \cdot_{\bar{V}} \bar{v} = \bar{\lambda} \cdot_V v \qquad \text{dla wszystkich } \lambda \in \mathbb{C},\ v \in V,$$

co jest równoważne równości

$$\bar{\lambda} \cdot \bar{v} = \overline{\lambda \cdot v}.$$

---

[7]Niektórzy nazywają je *antyliniowym*, co jednak prowadzi do trudności językowych, gdy trzeba określić odwzorowanie półtoraliniowe (zob. §1.6.4).

W ostatniej równości kropka po lewej stronie oznacza mnożenie w $\bar{V}$, a po prawej – w V. Odwzorowanie

$$\iota : V \to \bar{V}, \quad v \mapsto \iota(v) = \bar{v},$$

jest półliniowe i uniwersalne w tym sensie, że każde odwzorowanie półliniowe $f : V \to W$ można przedstawić jako złożenie $f = f_\flat \circ \iota$, gdzie $f_\flat : \bar{V} \to W$ jest odwzorowaniem liniowym, $f_\flat(\bar{v}) = f(v)$. Jeśli (e_i) jest bazą w przestrzeni V, to $(\overline{e_i})$ jest bazą w $\bar{V}$; zwykle pisze się $e_{\bar{i}}$ zamiast $\overline{e_i}$. Jeśli $f : V \to W$ jest odwzorowaniem liniowym, to odwzorowanie liniowe $\bar{f} : \bar{V} \to \bar{W}$ dane jest wzorem $\bar{f}(\bar{v}) = \overline{f(v)}$. Odwzorowanie $f \mapsto \bar{f}$ jest półliniowe.

Przestrzenie $(\bar{V})^*$ i $\overline{V^*}$ można utożsamić i oznaczać przez $\bar{V}^*$. Przestrzeń $\bar{\bar{V}}$ można utożsamić z V; wtedy $\bar{\bar{v}} = v$ i $\bar{\bar{f}} = f$. Jeśli (e^i) jest bazą w V^*, dualną do (e_i), to $(e^{\bar{i}})$ jest bazą w $\bar{V}^*$, dualną do $(e_{\bar{i}})$, $\overline{v^i} = \langle \bar{v}, e^{\bar{i}} \rangle$ itd.

1.6.4. Odwzorowania półtoraliniowe

Jeśli przestrzenie U, V, W są zespolone, to odwzorowanie

$$f : V \times W \to U,$$

które jest półliniowe na V i liniowe na W, nazywa się odwzorowaniem *półtoraliniowym*. Wtedy odwzorowanie $\bar{V} \times W \to U$, $(\bar{v}, w) \mapsto f(v, w)$, jest dwuliniowe.

1.6.5. Przestrzenie pseudounitarne i unitarne

Niech

$$A : V \to \bar{V}^* \tag{1.16}$$

będzie odwzorowaniem liniowym; odwzorowanie

$$V \times V \to \mathbb{C}, \quad (u, v) \mapsto (u|v) \overset{\text{def}}{=} \langle \bar{u}, Av \rangle,$$

jest półtoraliniowe. Ponadto $\overline{(u|v)} = (v|u)$ dla wszystkich $u, v \in V$ wtedy i tylko wtedy, gdy odwzorowanie A jest *hermitowskie*, tzn.

$$\bar{A}^* = A. \tag{1.17}$$

Wprowadzając macierz współczynników odwzorowania A,

$$Ae_i = e^{\bar{j}} A_{\bar{j}i},$$

i zakładając, że zachodzi (1.17), otrzymuje się

$$A_{\bar{j}i} = \langle e_{\bar{j}}, Ae_i \rangle = (e_j | e_i),$$

więc macierz $(A_{\bar{j}i})$ jest hermitowska,

$$A_{\bar{j}i} = \overline{A_{\bar{i}j}}.$$

Jeśli A jest izomorfizmem, to forma $(u, v) \mapsto (u|v)$ jest niezdegenerowana, tzn. $(u|v) = 0$ dla każdego $u \in V$ implikuje $v = 0$.

Parę (V, A), gdzie V jest przestrzenią zespoloną z niezdegenerowaną formą hermitowską (*hermitowskim iloczynem skalarnym*)

$$(u|v) = \langle \bar{u}, Av \rangle, \tag{1.18}$$

nazywa się przestrzenią *pseudounitarną*.

Jeśli forma ta jest ponadto *dodatnio określona*, tzn. $u \neq 0 \Rightarrow (u|u) > 0$, to mówimy, że odwzorowanie A definiuje w V strukturę *przestrzeni unitarnej*. Liczbę $\|u\| = (u|u)^{1/2}$ nazywa się wtedy *normą* wektora u.

Uwaga. Matematycy zwykle określają hermitowski iloczyn skalarny w ten sposób, że odwzorowanie $u \mapsto (u|v)$ jest liniowe, a $v \mapsto (u|v)$ jest półliniowe; tu przyjmuje się definicję stosowaną przez większość fizyków. Matematycy rzadko rozpatrują reprezentacje grup w przestrzeniach pseudounitarnych. W fizyce, w związku z reprezentacjami grup niezwartych, takich jak grupa Lorentza, pojawiają się w naturalny sposób przestrzenie i reprezentacje pseudounitarne. Z tego względu (czasami) celowe jest jawne uwidacznianie odwzorowania A określającego tę strukturę.

W przestrzeni unitarnej istnieją bazy *ortonormalne* (e_i), tzn. takie, że

$$(e_i|e_j) = \delta_{ij}.$$

Wtedy $(A_{\bar{j}i})$ jest macierzą jednostkową i nie występuje jawnie we wzorach.

W skończenie wymiarowej przestrzeni pseudounitarnej każdemu endomorfizmowi F odpowiada *endomorfizm sprzężony* $F^\dagger$ (względem iloczynu (1.18)) taki, że

$$(Fu|v) = (u|F^\dagger v)$$

dla każdej pary wektorów u i v. Na podstawie (1.18) mamy

$$F^\dagger = A^{-1}\bar{F}^* A. \tag{1.19}$$

Odwzorowanie $F \mapsto F^\dagger$ jest półliniowe; ponadto jeśli $F_1, F_2 \in \mathsf{End}\, V$, to $(F_1 \circ F_2)^\dagger = F_2^\dagger \circ F_1^\dagger$.

Jeśli $F = F^\dagger$, to mówimy, że endomorfizm F jest *samosprzężony* (względem iloczynu (1.18)).

Endomorfizm F jest *pseudounitarny* (względem (1.18)), jeśli $F^\dagger F = \mathrm{id}_V$; jest on wtedy odwracalny oraz $F^{-1} = F^\dagger$. Uwzględniając (1.19), można warunek pseudounitarności zapisać w postaci

$$\bar{F}^* = AF^{-1}A^{-1}. \tag{1.20}$$

Zbiór wszystkich automorfizmów pseudounitarnych tworzy *grupę pseudounitarną* $\mathsf{U}(A)$.

Gdy przestrzeń jest unitarna, zamiast „endomorfizm pseudounitarny” i „grupa pseudounitarna” mówimy oczywiście „endomorfizm unitarny” i „grupa unitarna”.

W przestrzeni $V = \mathbb{C}^{k+l}$ wprowadza się strukturę przestrzeni pseudounitarnej zdefiniowaną przez formę hermitowską o sygnaturze (k, l):

$$(u|u) = |u_1|^2 + \cdots + |u_k|^2 - |u_{k+1}|^2 - \cdots - |u_{k+l}|^2,$$

gdzie $u = (u_i) \in \mathbb{C}^{k+l}$; pisze się wtedy $\mathsf{U}(k, l)$ zamiast $\mathsf{U}(A)$. Dla $l = 0$ mówimy o strukturze unitarnej i grupie unitarnej $\mathsf{U}(k)$.

Ważne są następujące definicje i fakty związane z przestrzeniami unitarnymi. Każda podprzestrzeń wektorowa przestrzeni unitarnej jest unitarna względem ograniczenia iloczynu skalarnego do tej podprzestrzeni. Jeśli W jest podprzestrzenią przestrzeni unitarnej V, a $W^\perp$ jest podprzestrzenią ortogonalną do W, czyli

$$W^\perp = \{v \in V \mid w \in W \Rightarrow (v|w) = 0\},$$

to $V = W \oplus W^\perp$. Jeśli (F_{ij}) jest macierzą endomorfizmu F w bazie ortonormalnej, $Fe_i = \sum_j e_j F_{ji}$, to macierz endomorfizmu sprzężonego powstaje przez *sprzężenie hermitowskie*: $F^\dagger_{ij} = \overline{F_{ji}}$.

1.6.6. Struktura rzeczywista i kwaternionowa

Niech W będzie zespoloną przestrzenią wektorową. Każde odwzorowanie liniowe $C : W \to \bar{W}$ takie, że $\bar{C}C = \mathrm{id}_W$, określa *strukturę rzeczywistą* w tej przestrzeni w tym sensie, że zbiór

$$V = \{w \in W \mid \bar{w} = Cw\}$$

jest rzeczywistą podprzestrzenią w W, której kompleksyfikacja $V^{\mathbb{C}}$ jest izomorficzna z W.

Niech teraz W będzie parzystowymiarową zespoloną przestrzenią wektorową, $\dim_{\mathbb{C}} W = 2n$. Odwzorowanie liniowe $C : W \to \bar{W}$ takie, że $\bar{C}C = -\mathrm{id}_W$, pozwala wprowadzić w zbiorze W strukturę prawej, kwaternionowej przestrzeni wektorowej. Definiując mianowicie, dla każdego $w \in W$,

$$w\mathrm{i} = \sqrt{-1}\, w, \quad w\mathrm{j} = C^{-1}\bar{w},$$

otrzymuje się $(w\mathrm{i})\mathrm{i} = (w\mathrm{j})\mathrm{j} = -w$ oraz $(w\mathrm{i})\mathrm{j} + (w\mathrm{j})\mathrm{i} = 0$, więc zgodnie z (1.5) wystarczy przyjąć $w\mathrm{k} = (w\mathrm{i})\mathrm{j}$. Przy tym $\dim_{\mathbb{H}} W = n$.

2. Algebry

W niniejszym paragrafie zakłada się, że wszystkie rozpatrywane przestrzenie wektorowe są nad ciałem przemiennym $\mathbb{k}$, zwykle $\mathbb{R}$ albo $\mathbb{C}$.

2.1. Definicje i przykłady

2.1.1. Definicja

Algebra to przestrzeń wektorowa $\mathcal{A}$ z odwzorowaniem dwuliniowym

$$\mathcal{A} \times \mathcal{A} \to \mathcal{A}$$

zwanym *mnożeniem* i zapisywanym jako

$$(a, b) \mapsto a \cdot b \quad \text{albo} \quad [a, b],$$

a także na inne sposoby. Homomorfizm algebry $\mathcal{A}$ w algebrę $\mathcal{B}$ to odwzorowanie liniowe $h : \mathcal{A} \to \mathcal{B}$ takie, że $h(aa') = h(a)h(a')$ dla dowolnych $a, a' \in \mathcal{A}$. Jeśli h jest ponadto bijekcją, to mówimy, że h jest izomorfizmem algebr.

2.1.2. Algebra przeciwna

Algebra $\mathcal{A}^{\mathrm{opp}}$ ma ten sam zbiór elementów i strukturę przestrzeni wektorowej, co $\mathcal{A}$, a iloczyn $\cdot_{\mathrm{opp}}$ elementów w $\mathcal{A}^{\mathrm{opp}}$ jest taki, że

$$a \cdot_{\mathrm{opp}} b = b \cdot a, \qquad a, b \in \mathcal{A}.$$

2.1.3. Podalgebry

Podprzestrzeń $\mathcal{B}$ algebry $\mathcal{A}$ taka, że $\mathcal{B}\mathcal{B} \subset \mathcal{B}$, nazywa się *podalgebrą* algebry $\mathcal{A}$. O podzbiorze R podalgebry $\mathcal{B}$ mówimy, że ją *generuje*, jeśli $\mathcal{B}$ jest najmniejszą podalgebrą zawierającą R, tzn. jeśli $\mathcal{B}'$ jest podalgebrą w $\mathcal{A}$ i $R \subset \mathcal{B}'$, to $\mathcal{B} \subset \mathcal{B}'$. Np. pierścień $\mathbb{H}$ można rozpatrywać jako algebrę nad $\mathbb{R}$, generowaną przez zbiór $\{\mathrm{i}, \mathrm{j}\}$.

Podprzestrzeń $\mathcal{B}$ algebry $\mathcal{A}$ taka, że $\mathcal{A}\mathcal{B} \subset \mathcal{B}$ [$\mathcal{B}\mathcal{A} \subset \mathcal{B}$], nazywa się jej *ideałem lewostronnym* [*prawostronnym*]. Każdy ideał jest podalgebrą. Jeśli $\mathcal{B}$ jest ideałem dwustronnym – tzn. lewo- i prawostronnym – algebry $\mathcal{A}$, to przestrzeń ilorazowa $\mathcal{A}/\mathcal{B}$ ma strukturę algebry taką, że odwzorowanie kanoniczne $\mathcal{A} \to \mathcal{A}/\mathcal{B}$, $a \mapsto a + \mathcal{B}$, jest homomorfizmem algebr.

2.1.4. Algebry łączne

Algebra jest *łączna*, jeśli $(ab)c = a(bc)$ dla dowolnych $a, b, c \in \mathcal{A}$. Algebra może mieć jedność, tzn. element $1_{\mathcal{A}} \in \mathcal{A}$ taki, że $1_{\mathcal{A}}a = a1_{\mathcal{A}} = a$ dla każdego $a \in \mathcal{A}$.

W dalszym ciągu *zakłada się, że wszystkie rozpatrywane algebry łączne mają jedność, a homomorfizmy między nimi przeprowadzają jedności w jedności.*

Jeśli algebra $\mathcal{A}$ nad $\Bbbk$ ma jedność, to istnieje injekcja $\Bbbk \to \mathcal{A}$, $\lambda \mapsto \lambda 1_{\mathcal{A}}$, co pozwala utożsamić $\Bbbk$ z jednowymiarową podprzestrzenią w $\mathcal{A}$.

Jeśli $\mathcal{A}$ jest algebrą łączną i $n \in \mathbb{N}$, to $\mathcal{A}(n)$ oznacza algebrę (łączną) wszystkich macierzy kwadratowych stopnia n o elementach należących do $\mathcal{A}$; jej jednością jest $1_{\mathcal{A}}I$.

2.1.5. Algebry przemienne

Algebra jest *przemienna*, jeśli $ab = ba$ dla wszystkich $a, b \in \mathcal{A}$. Np. $\mathbb{C}$ jest algebrą łączną i przemienną nad $\mathbb{R}$. Zbiór kwaternionów jest łączną, ale nieprzemienną algebrą nad $\mathbb{R}$.

2.1.6. Algebry centralne

Centrum algebry $\mathcal{A}$, określone wzorem

$$\mathsf{Z}(\mathcal{A}) = \{a \in \mathcal{A} \mid ab = ba \text{ dla wszystkich } b \in \mathcal{A}\},$$

jest jej podalgebrą. Jeśli algebra $\mathcal{A}$ ma jedność, to $\Bbbk \subset \mathsf{Z}(\mathcal{A})$. Algebrę z jednością nazywamy *centralną*, jeśli $\mathsf{Z}(\mathcal{A}) = \Bbbk$. Np. algebra $\mathbb{H}$ nad $\mathbb{R}$ jest centralna; algebra $\mathbb{C}$ jest centralna nad $\mathbb{C}$, ale nie nad $\mathbb{R}$.

2.1.7. Suma prosta algebr

Sumą prostą algebr $\mathcal{A}$ i $\mathcal{B}$ jest algebra $\mathcal{A} \oplus \mathcal{B}$, której przestrzenią wektorową jest $\mathcal{A} \times \mathcal{B}$, a mnożenie elementów określamy wzorem

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2, b_1b_2) \quad \text{dla dowolnych } a_1, a_2 \in \mathcal{A},\ b_1, b_2 \in \mathcal{B}.$$

2.1.8. Iloczyn tensorowy algebr

Iloczynem tensorowym algebr $\mathcal{A}$ i $\mathcal{B}$ jest algebra, której przestrzeń wektorowa jest iloczynem tensorowym $\mathcal{A} \otimes \mathcal{B}$, a mnożenie elementów jest takie, że

$$(a_1 \otimes b_1) \cdot (a_2 \otimes b_2) = (a_1a_2) \otimes (b_1b_2) \quad \text{dla wszystkich } a_1, a_2 \in \mathcal{A},\ b_1, b_2 \in \mathcal{B}.$$

Ciało $\Bbbk$ można rozpatrywać jako algebrę nad $\Bbbk$; wtedy $\Bbbk \otimes_{\Bbbk} \Bbbk = \Bbbk$. Natomiast iloczyn $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ jest algebrą izomorficzną z $\mathbb{C} \oplus \mathbb{C}$, o czym można się przekonać, przedłużając odpowiedniości

$$\sqrt{-1} \otimes 1 \mapsto (\sqrt{-1}, \sqrt{-1}), \quad 1 \otimes \sqrt{-1} \mapsto (\sqrt{-1}, -\sqrt{-1}).$$

Iloczyn tensorowy $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{H}$ jest izomorficzny algebrze $\mathbb{C}(2)$; jej elementy były przez Williama R. Hamiltona nazywane *bikwaternionami* [52]. Aby opisać izomorfizm

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{H} \to \mathbb{C}(2), \tag{1.21}$$

wygodnie jest posługiwać się macierzami

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \varpi = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \varepsilon = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{1.22}$$

za pomocą których definiuje się *macierze Pauliego*[8]

$$\sigma_x = \varpi, \quad \sigma_y = \sqrt{-1}\,\varepsilon, \quad \sigma_z = \tau. \tag{1.23}$$

Izomorfizm (1.21) można otrzymać, przedłużając, nad ciałem $\mathbb{R}$, odpowiedniości

$$\sqrt{-1} \otimes 1 \mapsto \sqrt{-1}\,I, \quad 1 \otimes \mathrm{i} \mapsto \sigma_x/\sqrt{-1}, \quad 1 \otimes \mathrm{j} \mapsto \sigma_y/\sqrt{-1}, \quad 1 \otimes \mathrm{k} \mapsto \sigma_z/\sqrt{-1}.$$

Bikwaterniony bywają zapisywane w postaci

$$v + x\mathrm{i} + y\mathrm{j} + z\mathrm{k}, \quad \text{gdzie} \quad v, x, y, z \in \mathbb{C}.$$

2.1.9. Różniczkowanie algebry

Odwzorowanie liniowe $D : \mathcal{A} \to \mathcal{A}$ nazywa się *różniczkowaniem algebry* $\mathcal{A}$, jeśli dla wszystkich $a, b \in \mathcal{A}$ spełniona jest *reguła Leibniza*

$$D(a \cdot b) = D(a) \cdot b + a \cdot D(b).$$

Jeśli algebra $\mathcal{A}$ ma jedność $1_{\mathcal{A}}$, a D jest jej różniczkowaniem, to

$$D(1_{\mathcal{A}}) = D(1_{\mathcal{A}} \cdot 1_{\mathcal{A}}) = 2D(1_{\mathcal{A}}), \quad \text{więc} \quad D(1_{\mathcal{A}}) = 0.$$

---

[8] Wolfgang Pauli [85] wprowadził spin jako nowy stopień swobody elektronów i użył do jego opisu dwuwymiarowej zespolonej przestrzeni wektorowej, w której działają macierze (1.22).

2.2. Algebry Liego

Algebra $\mathcal{A}$ z iloczynem $[\,,\,]$ nazywa się *algebrą Liego*, jeśli dla wszystkich $a, b, c \in \mathcal{A}$ zachodzi równość

$$[a, b] + [b, a] = 0 \tag{1.24}$$

oraz *tożsamość Jacobiego*

$$[[a, b], c] + [[b, c], a] + [[c, a], b] = 0. \tag{1.25}$$

Np. jeśli $\mathcal{A}$ jest algebrą łączną, to definiując $[a, b] = ab - ba$, otrzymuje się w tym samym zbiorze $\mathcal{A}$ strukturę algebry Liego.

Jeśli dla wszystkich $a, b \in \mathcal{A}$ zachodzi (1.24), to tożsamość Jacobiego jest równoważna stwierdzeniu: dla każdego $a \in \mathcal{A}$ odwzorowanie $\mathcal{A} \to \mathcal{A}$, $b \mapsto [a, b]$, jest różniczkowaniem algebry $(\mathcal{A}, [\,,\,])$.

Jeśli (e_i) jest bazą n-wymiarowej algebry Liego, to

$$[e_j, e_k] = c^i_{jk} e_i, \qquad i, j, k = 1, \ldots, n. \tag{1.26}$$

Liczby $c^i_{jk} \in \mathbb{k}$ nazywają się *stałymi strukturalnymi* algebry Liego względem bazy (e_i). Na mocy antysymetrii nawiasu $[\,,\,]$ oraz tożsamości Jacobiego stałe strukturalne spełniają warunki

$$c^i_{jk} + c^i_{kj} = 0, \quad c^l_{jk} c^i_{ml} + c^l_{km} c^i_{jl} + c^l_{mj} c^i_{kl} = 0, \quad i, j, k, l, m = 1, \ldots, n. \tag{1.27}$$

Przykład 1.19. Przestrzeń wektorowa $\mathbb{R}^3$ z iloczynem wektorowym $\mathbf{u} \times \mathbf{v}$ jest algebrą Liego. Z tożsamości

$$(\mathbf{u} \times \mathbf{v}) \times \mathbf{w} = (\mathbf{u} \cdot \mathbf{w})\mathbf{v} - (\mathbf{v} \cdot \mathbf{w})\mathbf{u}$$

wynika tożsamość Jacobiego

$$(\mathbf{u} \times \mathbf{v}) \times \mathbf{w} + (\mathbf{v} \times \mathbf{w}) \times \mathbf{u} + (\mathbf{w} \times \mathbf{u}) \times \mathbf{v} = 0.$$

Przykład 1.20. Niech $\mathcal{K}(n)$ oznacza algebrę wszystkich macierzy kwadratowych stopnia n o elementach należących do ciała $\mathcal{K} = \mathbb{R}$, $\mathbb{C}$ albo $\mathbb{H}$. Wprowadzając w $\mathcal{K}(n)$ mnożenie elementów za pomocą komutatora $[a, b] = ab - ba$, otrzymuje się algebrę Liego $\mathfrak{gl}(n, \mathcal{K})$. Niech $\operatorname{tr} a$ oznacza ślad macierzy a; zbiory

$$\{a \in \mathfrak{gl}(n, \mathcal{K}) \mid \operatorname{tr} a = 0\} \tag{1.28}$$

są algebrami Liego dla $\mathcal{K} = \mathbb{R}$ lub $\mathbb{C}$, ale nie są takimi algebrami dla $\mathcal{K} = \mathbb{H}$ i $n > 1$, bo na przykład

$$\text{jeśli} \quad a = \begin{pmatrix} 0 & \mathrm{j} \\ -\mathrm{j} & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & \mathrm{k} \\ -\mathrm{k} & 0 \end{pmatrix}, \quad \text{to} \quad ab - ba = -2 \begin{pmatrix} \mathrm{i} & 0 \\ 0 & \mathrm{i} \end{pmatrix}. \tag{1.29}$$

Jeśli $a, b \in \mathbb{H}(n)$, to część rzeczywista śladu macierzy $ab - ba$ znika, więc zbiór

$$\mathfrak{sl}(n, \mathbb{H}) = \{a \in \mathfrak{gl}(n, \mathbb{H}) \mid \operatorname{tr} a + \operatorname{tr} \bar{a} = 0\}$$

jest algebrą Liego nad $\mathbb{R}$ o wymiarze $4n^2 - 1$. Dla $\mathcal{K} = \mathbb{R}$ lub $\mathbb{C}$ algebrę Liego (1.28) oznaczamy przez $\mathfrak{sl}(n, \mathcal{K})$.

Niech a^* oznacza macierz transponowaną do $a \in \mathfrak{gl}(n, \mathcal{K})$. Zbiór macierzy (antysymetrycznych)

$$\mathfrak{so}(n, \mathcal{K}) = \{a \in \mathfrak{gl}(n, \mathcal{K}) \mid a^* = -a\}$$

jest algebrą Liego dla $\mathcal{K} = \mathbb{R}$ i $\mathbb{C}$, ale nie jest taką algebrą dla $\mathcal{K} = \mathbb{H}$, $n > 1$, co widać z przykładu (1.29). Zwykle zapis $\mathfrak{so}(n, \mathbb{R})$ upraszcza się do $\mathfrak{so}(n)$.

Przykład 1.21. Niech K będzie ℓ-wymiarową przestrzenią wektorową nad $\mathbb{k}$ oraz $L = K^*$. W przestrzeni $V = K \oplus L$ można wprowadzić dwie naturalne, niezdegenerowane formy dwuliniowe ω_+ i ω_-,

$$\omega_\pm : V \times V \to \mathbb{k}, \qquad \omega_\pm(k + l, k' + l') = \langle k, l' \rangle \pm \langle k', l \rangle,$$

gdzie $k, k' \in K$ i $l, l' \in L$. Niech $(k_i)_{i=1}^{\ell}$ będzie bazą w K, a $(l_i)_{i=1}^{\ell}$ – bazą dualną w L, czyli

$$\langle k_i, l_j \rangle = \delta_{ij}.$$

Podprzestrzenie K i L w V są całkowicie optyczne względem obu tych form:

$$\omega_\pm(k_i, k_j) = 0, \qquad \omega_\pm(l_i, l_j) = 0 \quad \text{oraz} \quad \omega_\pm(k_i, l_j) = \delta_{ij}.$$

Każdy endomorfizm $X \in \operatorname{End} V$ można przedstawić w postaci „blokowej”

$$X = \begin{pmatrix} A & B \\ C & D \end{pmatrix}, \quad \text{gdzie} \quad A \in \operatorname{End} K,\ B \in \operatorname{Hom}(L, K) \text{ itd.} \tag{1.30}$$

Algebry Liego

$$\mathfrak{g}_\pm = \{X \in \operatorname{End} V \mid \omega_\pm(Xv, v') + \omega_\pm(v, Xv') = 0,\ \forall v, v' \in V\}$$

zawierają wszystkie macierze postaci (1.30) takie, że

$$B^* = \mp B, \qquad C^* = \mp C, \qquad D = -A^*.$$

Algebra $\mathfrak{g}_-$ to *symplektyczna algebra Liego* $\mathfrak{sp}(\ell, \mathbb{k})$.

Niech $a^\dagger = \bar{a}^*$ oznacza macierz *hermitowsko sprzężoną* do $a \in \mathfrak{gl}(n, \mathcal{K})$, gdzie $\mathcal{K} = \mathbb{C}$ lub $\mathbb{H}$. Zbiory macierzy

$$\mathfrak{su}(n) = \{a \in \mathfrak{sl}(n, \mathbb{C}) \mid a^\dagger = -a\} \quad \text{oraz} \quad \mathfrak{sp}(n) = \{a \in \mathfrak{gl}(n, \mathbb{H}) \mid a^\dagger = -a\}$$

są algebrami Liego nad $\mathbb{R}$.

Stwierdzenie 1.22. *Zbiór* $\operatorname{Der}\mathcal{A}$ *wszystkich różniczkowań algebry* $\mathcal{A}$ *nad* $\Bbbk$ *jest, względem komutatora, algebrą Liego nad* $\Bbbk$*.*

Dowód. Widać od razu, że jeśli $\lambda_1, \lambda_2 \in \Bbbk$ oraz $D_1, D_2 \in \operatorname{Der}\mathcal{A}$, to również $\lambda_1 D_1 + \lambda_2 D_2 \in \operatorname{Der}\mathcal{A}$. Jeśli $a, b \in \mathcal{A}$, to

$$\begin{aligned}[D_1, D_2](ab) &= D_1((D_2 a)b + aD_2 b) - D_2((D_1 a)b + aD_1 b) \\ &= (D_1 D_2 a)b + D_2 a D_1 b + D_1 a D_2 b + a D_1 D_2 b \\ &\quad - (D_2 D_1 a)b - D_1 a D_2 b - D_2 a D_1 b - a D_2 D_1 b \\ &= ([D_1, D_2]a)b + a[D_1, D_2]b,\end{aligned}$$

więc $[D_1, D_2] \in \operatorname{Der}\mathcal{A}$. □

Występująca w tym stwierdzeniu algebra $\mathcal{A}$ może nie być łączna. W szczególności, jeśli $\mathcal{A}$ jest algebrą Liego, to odwzorowanie

$$\operatorname{ad}(a) : \mathcal{A} \to \mathcal{A}, \quad \operatorname{ad}(a)b = [a, b],$$

jest *różniczkowaniem wewnętrznym* tej algebry.

2.3. Konstrukcja Cayleya–Dicksona

Sprzężeniem w algebrze z jednością $\mathcal{A}$ nad $\mathbb{R}$ nazywa się odwzorowanie liniowe $a \mapsto \bar{a}$ takie, że

$$\bar{\bar{a}} = a, \quad \overline{ab} = \bar{b}\bar{a}, \quad \bar{a}a = a\bar{a} \quad \text{oraz} \quad a = \bar{a} \Rightarrow a \in \mathbb{R} \subset \mathcal{A}. \tag{1.31}$$

Warunki (1.31) implikują

$$\bar{a}a \in \mathbb{R} \quad \text{oraz} \quad \operatorname{Re} a \overset{\text{def}}{=} \tfrac{1}{2}(a + \bar{a}) \in \mathbb{R}.$$

Sprzężenie jest ponadto *dobre*, jeśli

$$a \neq 0 \;\Rightarrow\; \bar{a}a > 0. \tag{1.32}$$

W łącznej algebrze z dobrym sprzężeniem każdy niezerowy element jest odwracalny, mianowicie $a^{-1} = \bar{a}(\bar{a}a)^{-1}$. Np. algebry $\mathbb{R}$, $\mathbb{C}$ i $\mathbb{H}$ są algebrami z dobrym sprzężeniem.

Jeśli algebra $\mathcal{A}$ jest łączna, to zbiór

$$\{a \in \mathcal{A} \mid \bar{a}a = 1\}$$

jest grupą.

Konstrukcja Cayleya–Dicksona pozwala zbudować z algebry $\mathcal{A}$ z dobrym sprzężeniem algebrę $\mathcal{A}^2$, także z takim sprzężeniem, o podwójnym wymiarze. W tym celu w przestrzeni wektorowej $\mathcal{A} \oplus \mathcal{A}$ wprowadza się iloczyn elementów wzorem

$$(a,b)(c,d) = (ac - d\bar{b}, \bar{a}d + cb) \tag{1.33}$$

oraz sprzężenie

$$\overline{(a,b)} = (\bar{a}, -b).$$

Jeśli 1 jest jednością w $\mathcal{A}$, to $(1,0)$ jest jednością w $\mathcal{A}^2$; ponadto $\operatorname{Re}(a,b) = (\operatorname{Re} a, 0)$. Obliczając

$$\overline{(a,b)}(a,b) = (\bar{a}a + b\bar{b}, 0) = (a\bar{a} + b\bar{b}, 0) = (a,b)\overline{(a,b)}$$

oraz

$$\begin{aligned}\overline{(a,b)(c,d)} &= \overline{(ac - d\bar{b}, \bar{a}d + cb)} = (\overline{ac - d\bar{b}}, -\bar{a}d - cb) \\ &= (\bar{c}\bar{a} - b\bar{d}, -\bar{a}d - cb) = (\bar{c}, -d)(\bar{a}, -b) = \overline{(c,d)}\,\overline{(a,b)},\end{aligned}$$

sprawdzamy, że w algebrze $\mathcal{A}^2$ spełnione są warunki (1.31) i (1.32), więc sprzężenie w tej algebrze też jest dobre.

Lemat 1.23. *Jeśli algebra $\mathcal{A}$ z dobrym sprzężeniem jest łączna, to algebra $\mathcal{A}^2$ nie ma dzielników zera.*

Dowód. Wystarczy pokazać, że jeśli $(a,b)(c,d) = 0$ i $(a,b) \neq 0$, to $(c,d) = 0$. Opierając się na (1.33), mnożąc $0 = ac - d\bar{b}$ z prawej strony przez b i korzystając z łączności algebry $\mathcal{A}$ oraz $\bar{a}d + cb = 0$, otrzymujemy

$$0 = a(cb) - d(\bar{b}b) = -(a\bar{a} + \bar{b}b)d,$$

jeśli więc $(a,b) \neq 0$, to $d = 0$. Podobnie, mnożąc $ac - d\bar{b} = 0$ z lewej strony przez $\bar{a}$, otrzymujemy $(\bar{a}a + b\bar{b})c = 0$, a stąd jeśli $(a,b) \neq 0$, to $c = 0$. □

Biorąc $\mathcal{A}_0 = \mathbb{R}$ z trywialnym sprzężeniem $\bar{a} = a$, można skonstruować ciąg $(\mathcal{A}_n)_{n\in\mathbb{N}}$ algebr ze sprzężeniem, definiując $\mathcal{A}_{n+1} = \mathcal{A}_n^2$; wtedy $\dim_{\mathbb{R}} \mathcal{A}_n = 2^n$. Zachodzą łatwe do sprawdzenia izomorfizmy algebr ze sprzężeniem:

$$\begin{aligned}&\mathcal{A}_1 \to \mathbb{C}, \quad (a,b) \mapsto a + \sqrt{-1}\,b, \qquad a,b \in \mathbb{R}, \\ &\mathcal{A}_2 \to \mathbb{H}, \quad (a + \sqrt{-1}\,b, c + \sqrt{-1}\,d) \mapsto a + \mathrm{i}b + \mathrm{j}d + \mathrm{k}c, \qquad a,b,c,d \in \mathbb{R}.\end{aligned}$$

Z definicji, algebra $\mathcal{A}_3$ to ośmiowymiarowa algebra *oktonionów* $\mathbb{O}$. Na mocy lematu algebra $\mathbb{O}$ nie ma dzielników zera, ale – jak można pokazać – nie jest łączna (zob. zad. 1.16). Algebra *sedenionów* $\mathcal{A}_4$ ma dzielniki zera.

2.4. Algebry z gradacją

Niech $\mathcal{Z}$ oznacza pierścień $\mathbb{Z}$ albo[9] $\mathbb{F}_2$ i niech $\mathcal{A}$ będzie algebrą nad ciałem $\Bbbk$. Mówimy, że $\mathcal{A}$ jest *algebrą z gradacją względem* $\mathcal{Z}$, jeśli przestrzeń wektorowa $\mathcal{A}$ ma gradację względem $\mathcal{Z}$, czyli

$$\mathcal{A} = \bigoplus_{k\in\mathcal{Z}} \mathcal{A}_k,$$

i ponadto

$$\text{jeśli} \quad a_k \in \mathcal{A}_k \text{ i } a_l \in \mathcal{A}_l, \quad \text{to} \quad a_k \cdot a_l \in \mathcal{A}_{k+l}.$$

O elementach z $\mathcal{A}_k$ mówimy, że są (jednorodne) *stopnia* k; elementy stopnia 0 i 1 algebry z gradacją względem $\mathbb{F}_2$ nazywa się, odpowiednio, elementami *parzystymi* i *nieparzystymi*.

Homomorfizm $\mathbb{Z} \to \mathbb{F}_2$ taki, że $2k + 1 \mapsto 1$, pozwala z każdej algebry z gradacją względem $\mathbb{Z}$ utworzyć algebrę z gradacją względem $\mathbb{F}_2$ przez „zapamiętywanie” tylko parzystości elementów algebry.

W dalszym tekście gradacja bez określenia pierścienia $\mathcal{Z}$ oznacza gradację względem $\mathbb{F}_2$.

Czasami wygodnie jest algebrę z gradacją

$$\mathcal{A} = \mathcal{A}_0 \oplus \mathcal{A}_1 \quad \text{zapisywać jako} \quad \mathcal{A}_0 \to \mathcal{A},$$

mimo że podalgebra $\mathcal{A}_0$ nie wyznacza części nieparzystej algebry $\mathcal{A}$.

Gradację algebry $\mathcal{A} = \mathcal{A}_0 \oplus \mathcal{A}_1$ można scharakteryzować za pomocą *automorfizmu głównego*, tzn. takiego $\alpha \in \mathsf{End}\,\mathcal{A}$, że

$$\alpha|\mathcal{A}_\epsilon = (-1)^\epsilon \operatorname{id}_{\mathcal{A}_\epsilon}, \qquad \epsilon \in \{0, 1\}.$$

Automorfizm ten jest *inwolucją*, tzn. $\alpha^2 = \operatorname{id}_{\mathcal{A}}$.

Homomorfizm algebr $f : \mathcal{A} \to \mathcal{B}$ nazywa się *homomorfizmem algebr z gradacją*, jeśli zachowuje gradację, tzn. $f(\mathcal{A}_\epsilon) \subset \mathcal{B}_\epsilon$. Piszemy

$$\mathcal{A} \approxeq \mathcal{B},$$

jeśli algebry $\mathcal{A}$ i $\mathcal{B}$ są izomorficzne jako algebry z gradacją.

Przykład 1.24. Niech $\mathcal{B}$ będzie algebrą. Poniżej używamy oznaczeń macierzy ze wzoru (1.22) (str. 38).

(i) Algebra $\mathcal{B} \to 2\mathcal{B} \overset{\text{def}}{=} \mathcal{B} \oplus \mathcal{B}$ ma gradację określoną przez automorfizm inwolutywny $\alpha : \mathcal{B} \to \mathcal{B}$ taki, że $\alpha(b_1, b_2) = (b_2, b_1)$. Odwzorowanie $\mathcal{B} \to 2\mathcal{B}$ to $b \mapsto (b, b)$.

---

[9] W wielu tekstach pisze się o gradacji względem $\mathbb{Z}_2$, ale w tej książce $\mathbb{Z}_2$ oznacza grupę, a definicja gradacji wymaga pierścienia (zob. np. (1.34) i §2.8).

(ii) Algebra $2\mathcal{B} \to \mathcal{B}(2)$ ma gradację określoną przez automorfizm $\alpha : \mathcal{B}(2) \to \mathcal{B}(2)$ taki, że $\alpha(a) = \tau a \tau^{-1}$. Odwzorowanie $2\mathcal{B} \to \mathcal{B}(2)$ przypisuje parze (b_1, b_2) macierz diagonalną z elementami b_1, b_2 na przekątnej.

Niech teraz $\Bbbk = \mathbb{R}$.

(iii) Algebra $\mathbb{R} \to \mathbb{C}$ ma gradację określoną przez sprzężenie zespolone.

(iv) Algebra $\mathbb{C} \to \mathbb{H}$ ma gradację określoną przez element $s \in \mathbb{H}$ taki, że $s^2 = -1$ i $\alpha(q) = sqs^{-1}$. Część parzysta tej algebry składa się ze wszystkich kwaternionów prostopadłych do s względem iloczynu skalarnego określonego przez formę kwadratową $q \mapsto \bar{q}q$. Gradacje odpowiadajace różnym kwaternionom są równoważne: jeśli $s^2 = s'^2 = -1$, to istnieje obrót w przestrzeni $\mathbb{R}^4 = \mathbb{H}$, przeprowadzający s w s' i rozszerzający się do izomorfizmu algebry $\mathbb{H}$ z gradacją określoną przez s na algebrę $\mathbb{H}$ z gradacją określoną przez s'. Dzięki temu można, dla uproszczenia, mówić o algebrze z gradacją $\mathbb{C} \to \mathbb{H}$.

(v) Algebra $\mathbb{R}(2)$, oprócz gradacji opisanej w (ii), ma nierównoważną jej gradację wyznaczoną przez $\alpha(a) = \varepsilon a \varepsilon^{-1}$. Podalgebra parzysta jest tu izomorficzna z $\mathbb{C}$.

(vi) Algebra $\mathbb{H} \to \mathbb{C}(2)$ ma automorfizm główny α taki, że $\alpha(a) = \varepsilon \bar{a} \varepsilon^{-1}$. Część parzysta tej algebry to

$$\operatorname{span}_{\mathbb{R}}\{I, \sqrt{-1}\,\sigma_x, \sqrt{-1}\,\sigma_y, \sqrt{-1}\,\sigma_z\} \cong \mathbb{H}.$$

Algebra przeciwna $\mathcal{A}^{\mathrm{opp}}$ do algebry z gradacją $\mathcal{A} = \bigoplus_k \mathcal{A}_k$ względem pierścienia $\mathcal{Z}$ ma tę samą strukturę przestrzeni wektorowej z gradacją co $\mathcal{A}$ i „przeciwne” mnożenie elementów:

$$\text{jeśli} \quad a \in \mathcal{A}_k \text{ i } b \in \mathcal{A}_l, \quad \text{to} \quad a \underset{\mathrm{opp}}{\cdot} b = (-1)^{kl} b \cdot a. \tag{1.34}$$

Np. algebrą przeciwną do $\mathbb{R} \to \mathbb{C}$ jest algebra $\mathbb{R} \to 2\mathbb{R}$, bo $\sqrt{-1}$ jest elementem nieparzystym, więc $\sqrt{-1} \underset{\mathrm{opp}}{\cdot} \sqrt{-1} = 1$.

Izomorfizm algebr $\beta : \mathcal{A} \to \mathcal{A}^{\mathrm{opp}}$ nazywa się *antyautomorfizmem* algebry $\mathcal{A}$. Inaczej mówiąc, antyautomorfizm algebry $\mathcal{A}$ to taki izomorfizm β struktury wektorowej tej algebry, że dla dowolnych $a, b \in \mathcal{A}$ zachodzi równość $\beta(ab) = \beta(b)\beta(a)$.

Różniczkowaniem stopnia l algebry z gradacją $\mathcal{A}$ nazywa się różniczkowanie $D : \mathcal{A} \to \mathcal{A}$ takie, że $D\mathcal{A}_k \subset \mathcal{A}_{k+l}$. Zbiór wszystkich różniczkowań algebry z gradacją tworzy algebrę Liego z gradacją: komutator $[D_1, D_2] = D_1 \circ D_2 - D_2 \circ D_1$ różniczkowania D_1 stopnia l_1 i różniczkowania D_2 stopnia l_2 jest różniczkowaniem stopnia $l_1 + l_2$.

Przykład 1.25. Algebra $\mathcal{A}$ wielomianów jednej zmiennej x o współczynnikach z ciała przemiennego $\mathcal{K}$ ma gradację względem $\mathbb{Z}$: $\mathcal{A}_k = \mathcal{K}x^k$ dla $k \geqslant 0$ i $\mathcal{A}_k = \{0\}$ dla $k < 0$. Różniczkowanie $\mathrm{d}/\mathrm{d}x$ jest stopnia -1.

2.5. Algebra tensorowa

Algebra tensorowa nad V jest, jako przestrzeń wektorowa, sumą prostą

$$\mathsf{T}(V) = \bigoplus_{k=0}^{\infty} \mathsf{T}^k(V), \quad \text{gdzie} \quad \mathsf{T}^k(V) = \bigotimes^k V, \quad \mathsf{T}^0(V) = \Bbbk.$$

Każdy element $a \in \mathsf{T}(V)$ jest (z definicji) ciągiem tensorów kontrawariantnych,

$$a = (a_0, a_1, \dots), \quad \text{gdzie} \quad a_k \in \mathsf{T}^k(V),$$

w którym prawie wszystkie elementy są zerami, tzn. istnieje $k_a \in \mathbb{N}$ o tej własności, że $k > k_a \Rightarrow a_k = 0$. Iloczyn $a \otimes b$ elementów $a = (a_k)_{k=0}^{\infty}$ i $b = (b_k)_{k=0}^{\infty}$ definiuje się wzorem

$$(a \otimes b)_k = \sum_{l=0}^{k} a_l \otimes b_{k-l}, \tag{1.35}$$

co nadaje nieskończenie wymiarowej przestrzeni $\mathsf{T}(V)$ strukturę algebry łącznej nad $\Bbbk$. Jednością tej algebry jest ciąg $(1, 0, 0, \dots)$. Algebra tensorowa ma oczywistą gradację względem $\mathbb{Z}$.

Wiele innych ważnych algebr definiuje się jako ilorazy algebry tensorowej przez jej ideały.

2.6. Algebra Grassmanna

Niech V będzie przestrzenią wektorową, a $\mathcal{A}$ – algebrą. Odwzorowanie liniowe $f : V \to \mathcal{A}$ takie, że $f(v)^2 = 0$ dla każdego $v \in V$, nazywa się *odwzorowaniem Grassmanna*.

Niech $\mathsf{J}_{\mathrm{Gr}}(V)$ będzie ideałem dwustronnym algebry $\mathsf{T}(V)$ generowanym przez zbiór wszystkich tensorów postaci $v \otimes v$, $v \in V$. (Określenie *generowany* oznacza tu najmniejszy ideał dwustronny zawierający wszystkie te elementy.) Iloraz

$$\bigwedge V \stackrel{\text{def}}{=} \mathsf{T}(V)/\mathsf{J}_{\mathrm{Gr}}(V)$$

jest łączną algebrą z gradacją względem $\mathbb{Z}$, zwaną *algebrą Grassmanna*.

Niech $\kappa : \mathsf{T}(V) \to \bigwedge V$ będzie odwzorowaniem kanonicznym, tj. $\kappa(a) = a + \mathsf{J}_{\mathrm{Gr}}(V)$. Ograniczenie odwzorowania κ do $\Bbbk \oplus V$ jest injekcją, można więc uważać $\Bbbk \oplus V$ za podprzestrzeń w $\bigwedge V$. Mnożenie elementów w $\bigwedge V$ oznacza się przez $\wedge$, tj. $\kappa(a \otimes b) = \kappa(a) \wedge \kappa(b)$.

Stwierdzenie 1.26. *Injekcja $\kappa : V \to \bigwedge V$ jest uniwersalnym odwzorowaniem Grassmanna, tzn. jeśli $f : V \to \mathcal{A}$ jest dowolnym odwzorowaniem Grassmanna, to istnieje homomorfizm algebr $f_\flat : \bigwedge V \to \mathcal{A}$ taki, że $f = f_\flat \circ \kappa$.*

Dowód. Odwzorowanie f przedłuża się do homomorfizmu algebr

$$\mathsf{T}(f) : \mathsf{T}(V) \to \mathcal{A} \quad \text{w ten sposób, że} \quad \mathsf{T}(f)(v_1 \otimes \cdots \otimes v_k) = f(v_1)\dots f(v_k).$$

Homomorfizm $\mathsf{T}(f)$ znika na $\mathsf{J}_{\mathrm{Gr}}(V)$, więc dobrze definiuje

$$f_\flat(a + \mathsf{J}_{\mathrm{Gr}}(V)) = \mathsf{T}(f)(a). \qquad \square$$

Niech V i W będą przestrzeniami wektorowymi. Wobec zawierania $W \subset \bigwedge W$ każde odwzorowanie liniowe $f : V \to W$ można rozpatrywać jako odwzorowanie Grassmanna $f : V \to \bigwedge W$, tj. $f(v) \wedge f(v) = 0$. Istnieje zatem homomorfizm algebr $\bigwedge f : \bigwedge V \to \bigwedge W$ przedłużający f. Zatem $\bigwedge$ jest funktorem z kategorii przestrzeni wektorowych w kategorię łącznych algebr z jednością.

Tensory można symetryzować i antysymetryzować. W szczególności, *odwzorowanie antysymetryzacji* $\mathsf{Alt} : \mathsf{T}(V) \to \mathsf{T}(V)$ jest określone następująco: jeśli $a \in \mathsf{T}_k(V)$ jest tensorem o składowych $a^{i_1 \dots i_k}$ względem pewnej bazy, to $\mathsf{Alt}\, a$ ma składowe

$$a^{[i_1 \dots i_k]} \overset{\text{def}}{=} \frac{1}{k!} \sum_{\pi \in \mathfrak{S}_k} (\operatorname{sgn} \pi) a^{i_{\pi(1)} \dots i_{\pi(k)}}.$$

Widać, że $\mathsf{Alt} \in \operatorname{End} \mathsf{T}(V)$ jest rzutowaniem, tj. $\mathsf{Alt} \circ \mathsf{Alt} = \mathsf{Alt}$. Przestrzeni wektorowej $\mathsf{Alt}\, V \overset{\text{def}}{=} \mathsf{Alt}(\mathsf{T}(V))$ można nadać strukturę algebry łącznej, definiując

$$\mathsf{Alt}(a) \cdot \mathsf{Alt}(b) = \mathsf{Alt}(a \otimes b) \quad \text{dla } a, b \in \mathsf{T}(V).$$

Zbiór $\Bbbk \oplus V$ jest podprzestrzenią w $\mathsf{Alt}\, V$. Dla każdego $v \in V \subset \mathsf{T}(V)$ mamy $\mathsf{Alt}(v \otimes v) = 0$, więc $f : V \to \mathsf{Alt}\, V$ jest odwzorowaniem Grassmanna, określającym izomorfizm algebry $\bigwedge V$ i *algebry zewnętrznej* $\mathsf{Alt}\, V$. Izomorfizm ten jest naturalny; nie ma potrzeby odróżniania algebr $\bigwedge V$ i $\mathsf{Alt}\, V$; tradycyjnie, nazw „algebra Grassmanna” i „algebra zewnętrzna” używa się wymiennie.

Jeśli przestrzeń V jest m-wymiarowa, to jest rozkład na sumę prostą

$$\bigwedge V = \bigoplus_{k=0}^{m} \bigwedge^k V,$$

gdzie $\bigwedge^k V$ jest przestrzenią wektorową *tensorów w pełni antysymetrycznych stopnia k*,

$$\bigwedge^k V = \{a \in \bigotimes^k V \mid a = \mathsf{Alt}\, a\}, \qquad \bigotimes^0 V = \Bbbk.$$

Elementy przestrzeni $\bigwedge^k V$ nazywa się zwykle *k-wektorami*, a elementy $\bigwedge V$ – *multiwektorami*; k-wektor jest multiwektorem jednorodnym stopnia k. Jeśli $a \in \bigwedge^k V$ i $b \in \bigwedge^l V$, to *iloczyn zewnętrzny* tych multiwektorów jest $(k+l)$-wektorem $a \wedge b = \mathsf{Alt}(a \otimes b)$ o składowych

$$(a \wedge b)^{i_1 \dots i_k j_1 \dots j_l} = a^{[i_1 \dots i_k} b^{j_1 \dots j_l]}.$$

Każdy multiwektor $a \in \bigwedge V$ jest ciągiem $(a_0, \dots, a_m)$ gdzie $a_k \in \bigwedge^k V$. Na mocy (1.35) iloczyn zewnętrzny multiwektorów a i b jest taki, że

$$(a \wedge b)_k = \sum_{l=0}^{k} a_l \wedge b_{k-l}.$$

Odwzorowanie $h \in \mathsf{Hom}(V, W)$ określa homomorfizm

$$\bigwedge^k h \in \mathsf{Hom}(\bigwedge^k V, \bigwedge^k W)$$

taki, że

$$(\bigwedge^k h)(v_1 \wedge \dots \wedge v_k) = h(v_1) \wedge \dots \wedge h(v_k) \tag{1.36}$$

dla wszystkich $v_1, \dots, v_k \in V$, oraz przedłuża się do homomorfizmu algebr $\bigwedge h : \bigwedge V \to \bigwedge W$. Dokładniej, $\bigwedge$ jest funktorem kowariantnym z kategorii przestrzeni wektorowych w kategorię algebr z gradacją.

Jeśli (e_i) jest bazą w m-wymiarowej przestrzeni V, to bazą w $\bigwedge^k V$ jest zbiór wszystkich k-wektorów postaci

$$e_{i_1} \wedge \dots \wedge e_{i_k}, \quad \text{gdzie} \quad 1 \leqslant i_1 < \dots < i_k \leqslant m. \tag{1.37}$$

Liczba takich ciągów $(i_1, \dots, i_k)$ wynosi $\binom{m}{k}$, więc

$$\dim \bigwedge V = \sum_{k=0}^{m} \binom{m}{k} = 2^m.$$

Stwierdzenie 1.27. *Ciąg wektorów $(v_1, \dots, v_k)$ jest liniowo niezależny wtedy i tylko wtedy, gdy*

$$v_1 \wedge \dots \wedge v_k \neq 0. \tag{1.38}$$

Dowód. Jeśli wektory $v_1, \dots, v_k \in V$ są liniowo zależne, to można jeden z nich przedstawić w postaci kombinacji liniowej pozostałych, więc $v_1 \wedge \dots \wedge v_k = 0$, bo $v \wedge v = 0$ dla każdego $v \in V$. Jeśli przestrzeń V jest m-wymiarowa, a wektory $v_1, \dots, v_k$ są liniowo niezależne – więc $k \leqslant m$ – to można ich zbiór uzupełnić do bazy $v_1, \dots, v_m$ w V; wtedy $v_1 \wedge \dots \wedge v_m \neq 0$ rozpina $\bigwedge^m V$ i tym bardziej zachodzi (1.38). □

Przestrzeń wektorową $\bigwedge V^*$ można utożsamić z przestrzenią dualną do $\bigwedge V$, określając *odwzorowanie obliczania*

$$\bigwedge V \times \bigwedge V^* \to \Bbbk, \qquad (a, \omega) \mapsto \langle a, \omega \rangle,$$

tak, że jeśli $v_1, \ldots, v_k \in V$ i $\alpha_1, \ldots, \alpha_k \in V^*$, to

$$\langle v_1 \wedge \cdots \wedge v_k, \alpha_1 \wedge \cdots \wedge \alpha_k \rangle = \det \langle v_i, \alpha_j \rangle. \tag{1.39}$$

Jeśli $a \in \bigwedge^k V$ i $\omega \in \bigwedge^l V^*$, przy czym $k \neq l$, to przyjmujemy $\langle a, \omega \rangle = 0$.

Jeśli $\omega \in \bigwedge^k V^*$, to zamiast $\langle v_1 \wedge \cdots \wedge v_k, \omega \rangle$ zwykle piszemy $\omega(v_1, \ldots, v_k)$; inaczej mówiąc, rozpatrujemy ω jako odwzorowanie $V \times \cdots \times V \to \Bbbk$, które jest k-liniowe i *w pełni antysymetryczne*, tzn.

$$\omega(v_{\pi(1)}, \ldots, v_{\pi(k)}) = (\operatorname{sgn} \pi)\omega(v_1, \ldots, v_k) \quad \text{dla każdego } \pi \in \mathfrak{S}_k.$$

Biorąc pod uwagę naturalny izomorfizm skończenie wymiarowych przestrzeni V i V^{**}, przestrzeń $\bigwedge^k V$ można utożsamić z przestrzenią dualną do $\bigwedge^k V^*$ i rozpatrywać k-wektor a jako odwzorowanie $V^* \times \cdots \times V^* \to \Bbbk$, które jest k-liniowe i w pełni antysymetryczne.

Algebra Grassmanna $\bigwedge V$ nad $\Bbbk$ ma naturalny antyautomorfizm („główny") β taki, że $\beta | \Bbbk \oplus V = \mathrm{id}_{\Bbbk \oplus V}$. Jeśli mianowicie $(e_1, \ldots, e_m)$ jest bazą przestrzeni V oraz $1 \leqslant i_1 < \cdots < i_k \leqslant m$, to

$$\beta(e_{i_1} \wedge \cdots \wedge e_{i_k}) = (-1)^{\frac{1}{2}k(k-1)} e_{i_1} \wedge \cdots \wedge e_{i_k}. \tag{1.40}$$

Definiując

$$\textstyle\bigwedge_\pm V = \{a \in \bigwedge V \mid \beta(a) = \pm a\},$$

otrzymujemy rozkład

$$\textstyle\bigwedge V = \bigwedge_+ V \oplus \bigwedge_- V.$$

Obliczając

$$d(m) \stackrel{\text{def}}{=} \tfrac{1}{2}(\dim \textstyle\bigwedge_+ V - \dim \bigwedge_- V), \qquad m = \dim_\Bbbk V,$$

na podstawie (1.40) oraz

$$\dim \textstyle\bigwedge^k V = \binom{m}{k},$$

otrzymujemy (zob. zad. 1.12)

$$\begin{aligned} d(m) &= \tfrac{1}{2}\left(\binom{m}{0} + \binom{m}{1} - \binom{m}{2} - \binom{m}{3} + \cdots\right) \\ &= 2^{\frac{1}{2}(m-2)}(\cos \tfrac{1}{4}m\pi + \sin \tfrac{1}{4}m\pi), \end{aligned} \tag{1.41}$$

a stąd

m	1	2	3	4	5	6	7	8
$d(m)$	1	1	0	−2	−4	−4	0	8

oraz

$$d(m+8) = 16d(m).$$

Funkcja d jest „okresową” funkcją wymiaru o okresie 8.

2.7. Algebra symetryczna

Niech $\mathsf{J}_{\mathrm{s}}(V)$ oznacza ideał algebry tensorowej $\mathsf{T}(V)$ generowany przez wszystkie elementy postaci

$$u \otimes v - v \otimes u, \quad \text{gdzie} \quad u, v \in V.$$

Algebra symetryczna nad przestrzenią V to iloraz $\mathsf{S}(V) \stackrel{\text{def}}{=} \mathsf{T}(V)/\mathsf{J}_{\mathrm{s}}(V)$. Algebra symetryczna jest łączna, przemienna i ma gradację względem $\mathbb{Z}$, $\mathsf{S}(V) = \bigoplus_{k=0}^{\infty} \mathsf{S}^k(V)$. Elementy podprzestrzeni $\mathsf{S}^k(V)$ to *tensory symetryczne* stopnia k. Surjektywne *odwzorowanie symetryzacji* $\pi : \mathsf{T}^k(V) \to \mathsf{S}^k(V)$ można określić na składowych tensorów wzorem

$$\pi(a)^{i_1 \dots i_k} = a^{(i_1 \dots i_k)} \stackrel{\text{def}}{=} \frac{1}{k!} \sum_{\pi \in \mathfrak{S}_k} a^{i_{\pi(1)} \dots i_{\pi(k)}}.$$

Mnożenie elementów algebry symetrycznej bywa oznaczane symbolem $\odot$; jest ono określone wzorem $a \odot b = \pi(a \otimes b)$. Wtedy

$$(a \odot b)^{i_1 \dots i_k j_1 \dots j_l} = a^{(i_1 \dots i_k} b^{j_1 \dots j_l)}.$$

Algebra symetryczna jest uniwersalna dla odwzorowań symetrycznych: jeśli $\mathcal{A}$ jest algebrą, a $f : V \to \mathcal{A}$ odwzorowaniem liniowym takim, że $f(u)f(v) = f(v)f(u)$ dla wszystkich $u, v \in V$, to istnieje homomorfizm algebr $f_\flat : \mathsf{S}(V) \to \mathcal{A}$ taki, że $f = f_\flat \circ \kappa$, gdzie $\kappa : V \to \mathsf{S}(V)$ jest naturalną injekcją.

2.8. Superalgebry Liego i supercentrum algebry z gradacją

W algebrach z gradacją w naturalny sposób pojawiają się „superróżniczkowania”; ich zbiór tworzy „superalgebrę Liego”, w której iloczyn elementów nieparzystych jest antykomutatorem, podobnie do tego, co w teoriach kwantowych występuje dla operatorów związanych z fermionami. Terminologia ta pochodzi od fizyków i nawiązuje do prac nad supersymetriami w teorii oddziaływań elementarnych (zob. np. [42]). Artykuł [30] jest dobrym, wczesnym przeglądem tej tematyki, napisanym dla fizyków. Niektórzy autorzy nie przyjmują nazwy „superalgebra Liego” i piszą – w tym kontekście – o algebrach Liego z gradacją, co może prowadzić do nieporozumień, gdyż występują także algebry Liego z gradacją, nie będące superalgebrami. Tematyka „super” jest rozwijana także przez matematyków (zob. np. [31, 75, 41, 113]).

2.8.1. Superróżniczkowania

Niech $\mathcal{A} = \bigoplus_k \mathcal{A}_k$ będzie algebrą z gradacją (nad $\mathbb{Z}$); odwzorowanie $D \in \mathrm{End}\,\mathcal{A}$ nazywamy *superróżniczkowaniem* stopnia l (i piszemy $D \in \mathrm{Der}_l(\mathcal{A})$), jeśli $D\mathcal{A}_k \subset \mathcal{A}_{k+l}$ oraz

$$D(ab) = (Da)b + (-1)^{kl}aDb \quad \text{dla dowolnych } a \in \mathcal{A}_k,\ b \in \mathcal{A}.$$

Każde superróżniczkowanie stopnia parzystego jest więc zwykłym różniczkowaniem; w związku z tym często zamiast „superróżniczkowanie” stopnia nieparzystego mówi się „antyróżniczkowanie” i nie wprowadza nazwy „superróżniczkowanie”.

2.8.2. Superalgebry Liego

O dwóch elementach $a \in \mathcal{A}_k$ i $b \in \mathcal{A}_l$ algebry z gradacją mówimy, że *superkomutują* (lub *superantykomutują*), jeśli $[b,a] = (-1)^{kl}[a,b]$ (odpowiednio $[b,a] = -(-1)^{kl}[a,b]$). Algebra z gradacją jest *superprzemienna* [*superantyprzemienna*], jeśli dowolne dwa jej elementy superkomutują [superantykomutują]. Np. algebra zewnętrzna jest superprzemienna.

Definicja. Algebra $\mathcal{A}$ z gradacją i z mnożeniem elementów $(a,b) \mapsto [a,b]$ takim, że $[\mathcal{A}_k, \mathcal{A}_l] \subset \mathcal{A}_{k+l}$, nazywa się *superalgebrą Liego*, jeśli jest superantyprzemienna, a odwzorowanie $b \mapsto [a,b]$, gdzie $a \in \mathcal{A}_k$, jest superróżniczkowaniem stopnia k.

Inaczej mówiąc, algebra z gradacją $(\mathcal{A}, [\,,\,])$ jest superalgebrą Liego, jeśli dla dowolnych $a \in \mathcal{A}_k$, $b \in \mathcal{A}_l$ mamy $[a,b] \in \mathcal{A}_{k+l}$, $[b,a] = -(-1)^{kl}[a,b]$ oraz spełniona jest *supertożsamość Jacobiego*

$$(-1)^{km}[a,[b,c]] + (-1)^{kl}[b,[c,a]] + (-1)^{lm}[c,[a,b]] = 0$$

dla $a \in \mathcal{A}_k,\ b \in \mathcal{A}_l,\ c \in \mathcal{A}_m$.

Niech $\mathcal{A}$ będzie łączną algebrą z gradacją. Definiując

$$\mathcal{A} \times \mathcal{A} \to \mathcal{A}, \qquad (a,b) \mapsto [a,b],$$

tak, że jeśli $a \in \mathcal{A}_k$ i $b \in \mathcal{A}_l$, to

$$[a,b] = ab - (-1)^{kl}ba, \tag{1.42}$$

nadajemy przestrzeni wektorowej $\mathcal{A}$ strukturę superalgebry Liego.

Stwierdzenie 1.28. *Jeśli* $(\mathcal{A}, \cdot)$ *jest algebrą z gradacją, to zbiór* $\mathrm{Der}\,\mathcal{A}$ *jej superróżniczkowań ma strukturę superalgebry Liego względem komutatora* (1.42).

Dowód. Przez proste sprawdzenie. □

2.8.3. Supercentrum

Używając nawiasu zdefiniowanego w (1.42), definiuje się *supercentrum* łącznej algebry z gradacją $\mathcal{A}$ jako

$$\mathsf{SZ}(\mathcal{A}) = \{a \in \mathcal{A} \mid [a, b] = 0 \text{ dla wszystkich } b \in \mathcal{A}\}.$$

Algebrę z gradacją $\mathcal{A}$ nad ciałem $\mathcal{K}$ nazywa się *supercentralną*, jeśli $\mathsf{SZ}(\mathcal{A}) = \mathcal{K}$. Algebra $\mathbb{C}$ nad $\mathbb{R}$ nie jest centralna, bo liczby urojone należą do jej centrum, ale algebra z gradacją $\mathbb{R} \to \mathbb{C}$ (zob. przykład 1.24, str. 43) jest supercentralna, bo liczby urojone są jej elementami nieparzystymi i nie należą do supercentrum: $[\sqrt{-1}, \sqrt{-1}\,] = -2$.

2.8.4. Superróżniczkowania algebry zewnętrznej

Niech

$$\operatorname{Der} \mathcal{A} = \bigoplus_k \operatorname{Der}_k \mathcal{A}$$

będzie algebrą superróżniczkowań algebry zewnętrznej $\mathcal{A} = \bigwedge V^*$, gdzie V jest przestrzenią wektorową wymiaru n. Jeżeli $k \leqslant -2$ i $D \in \operatorname{Der}_k \mathcal{A}$, to D znika na zbiorze $\Bbbk \oplus V^*$, który generuje $\mathcal{A}$, więc $D = 0$. Także jeśli $D \in \operatorname{Der}_k \mathcal{A}$ i $k \geqslant n$, to $D = 0$. Każde $D \in \operatorname{Der}_k \mathcal{A}$, gdzie $-1 \leqslant k \leqslant n-1$, jest określone przez odwzorowanie liniowe

$$D|V^* : V^* \to \textstyle\bigwedge^{k+1} V^*,$$

czyli przez pewien tensor $X \in V \otimes \bigwedge^{k+1} V^*$; piszemy $D = i(X)$, co określa izomorfizm przestrzeni wektorowych

$$i : V \otimes \textstyle\bigwedge V^* \to \operatorname{Der} \bigwedge V^*.$$

W szczególności, jeśli $k = -1$, to $i(v)$ jest *zwężaniem form z wektorem* $v \in V$; często pisze się $v \lrcorner \alpha$ zamiast $i(v)\alpha$, gdzie $\alpha \in \bigwedge V^*$. Jeśli formę $\omega \in \bigwedge^k V^*$ rozpatrujemy jako odwzorowanie antysymetryczne $V^k \to \Bbbk$, to

$$(i(v_1)\omega)(v_2, \ldots, v_k) = \omega(v_1, v_2, \ldots, v_k), \quad v_j \in V,\ j = 1, \ldots, k. \tag{1.43}$$

Niektórzy autorzy przyjmują inną umowę na temat odwzorowania dualności między $\bigwedge V$ i $\bigwedge V^*$ niż ta wynikająca z (1.39), co powoduje inną postać wzoru (1.43); zob. np. [64, tom I, str. 35, wzór na $i_X\omega$]. W niniejszym tekście została przyjęta umowa jak w [103].

Z definicji (1.43) wynika

$$\langle v \lrcorner \omega, w \rangle = \langle \omega, v \wedge w \rangle \quad \text{dla każdego } w \in \textstyle\bigwedge V,$$

co oznacza, że $v \lrcorner : \bigwedge V^* \to \bigwedge V^*$ jest odwzorowaniem transponowanym (dualnym), w znaczeniu określonym w 1.3.5 (str. 24) do odwzorowania $v \wedge : \bigwedge V \to \bigwedge V$.

Korzystając z tego, że dla skończenie wymiarowej przestrzeni V przestrzeń V^{**} jest w naturalny sposób izomorficzna z V, definicję (1.43) można zastosować do zwężania formy $\alpha \in V^*$ z multiwektorem $w \in \bigwedge V$. Wynika stąd, że

$$\text{jeśli} \quad \alpha \in V^* \text{ i } v \in V, \quad \text{to} \quad \alpha \lrcorner v = \langle v, \alpha \rangle,$$

oraz jeśli $u \in \bigwedge^k V$ i $w \in \bigwedge V$, to

$$\alpha \lrcorner (u \wedge w) = (\alpha \lrcorner u) \wedge w + (-1)^k u \wedge (\alpha \lrcorner w). \tag{1.44}$$

Jeśli $X \in V \otimes \bigwedge^{k+1} V^*$ i $Y \in V \otimes \bigwedge^{l+1} V^*$, to

$$[i(X), i(Y)] = i(X) \circ i(Y) - (-1)^{kl} i(Y) \circ i(X)$$

jest superróżniczkowaniem stopnia $k + l$, istnieje więc element

$$[X, Y] \in V \otimes \bigwedge^{k+l+1} V^* \quad \text{taki, że} \quad [i(X), i(Y)] = i([X, Y]).$$

W szczególności, jeśli $k = l = 0$, to $X, Y \in \mathsf{End}\, V$, a $[X, Y]$ jest zwykłym komutatorem endomorfizmów.

Jeśli $c \in V \otimes \bigwedge^2 V^*$, to $i(c)$ jest superróżniczkowaniem stopnia 1; jeśli (e^i) jest bazą w V^*, to

$$i(c)e^i = c^i_{jk} e^j \wedge e^k, \quad \text{gdzie} \quad c^i_{jk} + c^i_{kj} = 0,$$

a warunek $[i(c), i(c)] = 0$ jest równoważny tożsamości Jacobiego (1.27).

2.8.5. (Super)iloczyn tensorowy algebr z gradacją

Iloczyn tensorowy opisany w §2.1.8 (str. 37), zastosowany do algebr z gradacją $\mathcal{A} = \bigoplus \mathcal{A}_k$ i $\mathcal{B} = \bigoplus \mathcal{B}_k$, daje algebrę z gradacją

$$\mathcal{A} \otimes \mathcal{B} = \bigoplus (\mathcal{A} \otimes \mathcal{B})_k, \quad \text{gdzie} \quad (\mathcal{A} \otimes \mathcal{B})_k = \bigoplus_l (\mathcal{A}_l \otimes \mathcal{B}_{k-l}). \tag{1.45}$$

Bardziej interesujący jest *superiloczyn tensorowy algebr z gradacją*, tradycyjnie oznaczany przez $\mathcal{A} \hat{\otimes} \mathcal{B}$. Struktura wektorowa i gradacja tej algebry są takie, jak w (1.45), ale mnożenie uwzględnia parzystość elementów:

$$\text{jeśli} \quad a_2 \in \mathcal{A}_k \text{ i } b_1 \in \mathcal{B}_l, \quad \text{to} \quad (a_1 \otimes b_1) \cdot (a_2 \otimes b_2) = (-1)^{kl} a_1 a_2 \otimes b_1 b_2.$$

Stwierdzenie 1.29. *Jeśli V i W są skończenie wymiarowymi przestrzeniami wektorowymi, to algebry z gradacją $\bigwedge(V \oplus W)$ i $(\bigwedge V) \hat{\otimes} (\bigwedge W)$ są w naturalny sposób izomorficzne.*

Dowód. Odwzorowanie

$$V \oplus W \to (\textstyle\bigwedge V) \mathbin{\hat{\otimes}} (\textstyle\bigwedge W), \qquad (v, w) \mapsto v \otimes 1_{\bigwedge W} + 1_{\bigwedge V} \otimes w,$$

jest odwzorowaniem Grassmanna (str. 45) i rozszerza się do izomorfizmu algebr z gradacją. □

Przykład 1.30. Niech $\mathbb{R} \to \mathbb{C}$ będzie algebrą nad $\mathbb{R}$ z gradacją określoną przez sprzężenie zespolone. Wtedy algebra $\mathbb{C} \mathbin{\hat{\otimes}} \mathbb{C}$ jest izomorficzna algebrze z gradacją $\mathbb{C} \to \mathbb{H}$. Istotnie, izomorfizm $\mathbb{C} \mathbin{\hat{\otimes}} \mathbb{C} \to \mathbb{H}$ jest określony przez przedłużenie odpowiedniości

$$1 \otimes 1 \mapsto 1, \quad \sqrt{-1} \otimes 1 \mapsto \mathrm{i}, \quad 1 \otimes \sqrt{-1} \mapsto \mathrm{j}, \quad \sqrt{-1} \otimes \sqrt{-1} \mapsto \mathrm{k}.$$

2.9. Wektory i wartości własne

2.9.1. Wyznacznik endomorfizmu

Niech V będzie n-wymiarową przestrzenią wektorową nad ciałem przemiennym $\Bbbk$. Przestrzeń n-wektorów $\bigwedge^n V$ jest 1-wymiarowa, jeśli więc (e_i) jest bazą w V, to każdy n-wektor jest proporcjonalny do $e_1 \wedge \cdots \wedge e_n$. W szczególności

$$e_{i_1} \wedge \cdots \wedge e_{i_n} = \varepsilon_{i_1 \ldots i_n} e_1 \wedge \cdots \wedge e_n, \tag{1.46}$$

co definiuje *symbol Levi-Civity* $\varepsilon_{i_1 \ldots i_n}$ taki, że

$$\varepsilon_{i_1 \ldots i_n} = \varepsilon_{[i_1 \ldots i_n]} \quad \text{oraz} \quad \varepsilon_{1 \ldots n} = 1.$$

Dla każdego $a \in \operatorname{End} V$ oraz $k \in \mathbb{N}$ wzór (1.36) określa endomorfizm $\bigwedge^k a \in \operatorname{End} \bigwedge^k V$. *Wyznacznikiem* endomorfizmu $a \in \operatorname{End} V$ nazywamy element $\det a \in \Bbbk$ taki, że

$$(\textstyle\bigwedge^n a)(e_1 \wedge \cdots \wedge e_n) = (\det a)(e_1 \wedge \cdots \wedge e_n). \tag{1.47}$$

Niech $a, b \in \operatorname{End} V$; równość $\bigwedge^n (a \circ b) = (\bigwedge^n a) \circ (\bigwedge^n b)$ implikuje

$$\det(a \circ b) = \det a \cdot \det b. \tag{1.48}$$

Wyznacznik jest dobrze określony, tzn. nie zależy od bazy występującej w jego definicji; istotnie, niech $\det' a$ będzie wyznacznikiem endomorfizmu a zdefiniowanym za pomocą innej bazy (e'_i), tzn.

$$(\textstyle\bigwedge^n a)(e'_1 \wedge \cdots \wedge e'_n) = (\det' a)(e'_1 \wedge \cdots \wedge e'_n).$$

Istnieje endomorfizm odwracalny c taki, że $e'_i = c(e_i)$, $i = 1, \ldots, n$, więc

$$\det(a \circ c) = \det' a \cdot \det c,$$

czyli, wobec (1.48), mamy $\det' a = \det a$.

Jeśli (a^i_j) jest macierzą endomorfizmu a względem bazy (e_i), tj. $a(e_i) = e_j a^j_i$, to korzystając z (1.36) i (1.46), otrzymuje się wzór na obliczanie wyznaczników:

$$\det a = \varepsilon_{j_1 \ldots j_n} a^{j_1}_1 \ldots a^{j_n}_n. \tag{1.49}$$

Np. dla $n = 2$ wynika stąd, że $\det a = a^1_1 a^2_2 - a^2_1 a^1_2$.

Zamiast mówić o wyznaczniku endomorfizmu, mówi się często o wyznaczniku macierzy jego współczynników i zapisuje go w postaci

$$\det(a^i_j) = \begin{vmatrix} a^1_1 & \ldots & a^1_n \\ \ldots & \ldots & \ldots \\ a^n_1 & \ldots & a^n_n. \end{vmatrix}$$

Łatwo wydedukować z (1.49) użyteczne własności wyznaczników i sposoby ich obliczania. Np. z równości

$$\varepsilon_{i_1 \ldots i_n} = n! \delta^1_{[i_1} \ldots \delta^n_{i_n]}$$

i tożsamości

$$n\delta^1_{[i_1}\delta^2_{i_2}\delta^3_{i_3}\delta^4_{i_4}\ldots\delta^n_{i_n]} = \delta^1_{i_1}\delta^2_{[i_2}\delta^3_{i_3}\delta^4_{i_4}\ldots\delta^n_{i_n]} - \delta^1_{i_2}\delta^2_{[i_1}\delta^3_{i_3}\delta^4_{i_4}\ldots\delta^n_{i_n]} \\ + \delta^1_{i_3}\delta^2_{[i_1}\delta^3_{i_2}\delta^4_{i_4}\ldots\delta^n_{i_n]} + \cdots + (-1)^{n-1}\delta^1_{i_n}\delta^2_{[i_1}\delta^3_{i_2}\delta^4_{i_3}\ldots\delta^n_{i_{n-1}]}$$

otrzymuje się klasyczny wzór Laplace'a na obliczanie wyznaczników.

Z równości (1.48) wynika, że endomorfizm a jest odwracalny wtedy i tylko wtedy, gdy $\det a \neq 0$. *Specjalną grupę liniową* nad ciałem $\Bbbk$ definiuje się jako

$$\mathsf{SL}(n, \Bbbk) = \{a \in \Bbbk(n) \mid \det a = 1\}.$$

Jeśli V jest rzeczywistą przestrzenią wektorową, to zależnie od tego, czy wyznacznik macierzy przejścia od jednej bazy tej przestrzeni do drugiej jest liczbą dodatnią czy ujemną, mówimy, że bazy te mają zgodną albo przeciwną orientację. Orientacja takiej przestrzeni polega na wyróżnieniu jednego z dwóch zbiorów baz o zgodnej orientacji.

Jeśli (V, h) jest przestrzenią kwadratową nad $\Bbbk$, to

$$\mathsf{SO}(V, h) = \{a \in \mathsf{O}(V, h) \mid \det a = 1\}$$

jest *grupą obrotów* tej przestrzeni. Obroty *właściwe* to elementy składowej spójnej identyczności (maksymalnej spójnej podgrupy), oznaczanej przez $\mathsf{SO}_0(V, h)$. Jeśli przestrzeń V jest zespolona albo rzeczywista, a forma h jest dodatnio lub ujemnie określona, to $\mathsf{SO}(V, h) = \mathsf{SO}_0(V, h)$.

2.9.2. Wyznaczniki elementów przestrzeni $V \otimes V$ i $V^* \otimes V^*$

Wyznaczniki te można zdefiniować podobnie, ale wymaga to wyróżnienia bazy w V. Niech np. $g \in V^* \otimes V^* = \mathsf{Hom}(V, V^*)$. Wybierając bazę $e = (e_i)$ w V i bazę dualną (e^i) w V^*, definiujemy wyznacznik g względem e za pomocą wzoru

$$\det(g, e)e^1 \wedge \cdots \wedge e^n = g(e_1) \wedge \cdots \wedge g(e_n).$$

Jeśli $a \in \mathsf{GL}(V)$ i $e' = ae$, to $\det(g, e') = \det(g, e)(\det a)^2$. Niech $\mathsf{FL}(V)$ oznacza zbiór wszystkich baz w V. W rachunku tensorowym odwzorowanie $f : \mathsf{FL}(V) \to \Bbbk$ takie, że $f(ae) = (\det a)^N f(e)$, nazywa się *gęstością* o wadze N. Dla $\Bbbk = \mathbb{R}$ forma

$$\eta(e) = |\det(g, e)|^{1/2} e^1 \wedge \cdots \wedge e^n \quad \text{spełnia} \quad \eta(ae) = \eta(e) \operatorname{sgn} \det a$$

i jest używana przy określaniu całki w n-wymiarowej geometrii Riemanna opartej na tensorze metrycznym g (zob. np. [98, 107]). Jeśli $g = g_{ij} e^i \otimes e^j$, to piszemy $\det(g_{ij})$ zamiast $\det(g, e)$.

2.9.3. Wektory i wartości własne endomorfizmu

Niech V będzie zespoloną, n-wymiarową przestrzenią wektorową i $a \in \mathsf{End}\, V$. Jeśli wektor $v \in V^\times$ i liczba $\lambda \in \mathbb{C}$ spełniają warunek

$$a(v) = \lambda v,$$

to v nazywa się *wektorem własnym* endomorfizmu a odpowiadającym *wartości własnej* λ.

Lemat 1.31. *Równanie $a(v) = 0$ ma rozwiązanie $v \neq 0$ wtedy i tylko wtedy, gdy $\det a = 0$.*

Dowód. Jeśli v jest takim rozwiązaniem, to można wziąć bazę taką, że $e_1 = v$; wtedy (1.47) daje $\det a = 0$. Na odwrót, jeśli $\det a = 0$, to

$$a(e_1) \wedge \cdots \wedge a(e_n) = 0,$$

więc wektory $a(e_1), \ldots, a(e_n)$ są liniowo zależne. Oznacza to, że istnieją liczby $\mu_1, \ldots, \mu_n$, nie wszystkie równe 0, takie, że wektor

$$v = \mu_1 e_1 + \cdots + \mu_n e_n$$

jest anihilowany przez a. □

2.9.4. Twierdzenie Hamiltona–Cayleya

Wyznacznik $w_a(z) = \det(a - zI)$ jest wielomianem n-tego stopnia względem z, zwanym *wielomianem charakterystycznym* endomorfizmu a,

$$w_a(z) = (-z)^n + (-z)^{n-1} \operatorname{tr} a + \cdots + \det a.$$

Zastępując w lemacie 1.31 endomorfizm a przez $a - \lambda I$, otrzymujemy

Stwierdzenie 1.32. *Jeśli λ jest wartością własną endomorfizmu a, to $w_a(\lambda) = 0$; na odwrót, jeśli λ jest pierwiastkiem wielomianu charakterystycznego, to istnieje wektor własny endomorfizmu a, odpowiadający λ.*

Rozkładając wielomian charakterystyczny na czynniki,

$$w_a(z) = (\lambda_1 - z)^{n_1} \dots (\lambda_k - z)^{n_k}, \quad n_1 + \cdots + n_k = n,$$

można przedstawić wyznacznik endomorfizmu a w postaci

$$\det a = \lambda_1^{n_1} \dots \lambda_k^{n_k}.$$

Wymiar przestrzeni rozpiętej na wektorach własnych o wartości własnej λ_i jest $\leqslant n_i$, $i = 1, \dots, k$. Np. macierz $\left(\begin{smallmatrix} 2 & 1 \\ 0 & 2 \end{smallmatrix}\right)$ ma wielomian charakterystyczny $(2 - z)^2$ oraz jeden kierunek wektorów własnych.

Jeśli wielomian charakterystyczny w_a ma tylko pojedyncze pierwiastki, to wektory własne a rozpinają całą przestrzeń V. Takie endomorfizmy są *generyczne* w tym sensie, że ich zbiór, względem naturalnej topologii w przestrzeni $\mathsf{End}\, V \cong \mathbb{C}(n)$, jest w tej przestrzeni otwarty i gęsty. Jeśli endomorfizm a jest generyczny, to $\det a$ jest iloczynem jego wartości własnych.

Dla każdego $b \in \mathsf{End}\, V$ można rozpatrywać endomorfizm

$$w_a(b) = (-b)^n + (-b)^{n-1} \operatorname{tr} a + \cdots + I \det a \in \mathsf{End}\, V.$$

powstający przez podstawienie w wielomianie charakterystycznym w_a endomorfizmu b.

Twierdzenie (Hamiltona–Cayleya)**.** *Endomorfizm $w_a(a)$ jest zerowy dla każdego $a \in \mathsf{End}\, V$.*

Dowód. Jeśli v jest wektorem własnym a odpowiadającym wartości własnej λ, to $w_a(a)v = 0$ na mocy stwierdzenia 1.32. Jeśli endomorfizm a jest generyczny, to jego wektory własne rozpinają V, więc $w_a(a)v = 0$ dla każdego $v \in V$. Wielomian jest funkcją ciągłą, $w_a(a)$ znika dla generycznego a, stąd $w_a(a) = 0$ dla każdego a. □

Wadą powyższego rozumowania – przynajmniej w opinii niektórych osób – jest odwołanie się do argumentu topologicznego – ciągłości wielomianu – w dowodzie faktu czysto algebraicznego. Czysto algebraiczny dowód twierdzenia Hamiltona–Cayleya można znaleźć w [117].

2.10. Wyznaczniki kwaternionowe

Definicja wyznacznika na zbiorze macierzy $\mathbb{H}(n)$ wymaga specjalnych rozważań. „Zwykła” definicja nie jest dobra; np. gdyby przyjąć

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc \quad \text{dla } a, b, c, d \in \mathbb{H},$$

to byłoby

$$\det \begin{pmatrix} a & a \\ b & b \end{pmatrix} = 0, \quad \text{ale} \quad \det \begin{pmatrix} a & b \\ a & b \end{pmatrix} = ab - ba.$$

Pisząc $q = u + \mathrm{i}x + \mathrm{j}y + \mathrm{k}z = u + \mathrm{i}x + \mathrm{j}(y - \mathrm{i}z)$, można kwaternion q przedstawić w postaci macierzy o elementach zespolonych:

$$\begin{pmatrix} u + \sqrt{-1}\,x & -y - \sqrt{-1}\,z \\ y - \sqrt{-1}\,z & u - \sqrt{-1}\,x \end{pmatrix}.$$

Widać, że

$$\det \begin{pmatrix} u + \sqrt{-1}\,x & -y - \sqrt{-1}\,z \\ y - \sqrt{-1}\,z & u - \sqrt{-1}\,x \end{pmatrix} = \bar{q}q.$$

Niech teraz $A + \mathrm{j}B \in \mathbb{H}(n)$, gdzie $A, B \in \mathbb{C}(n)$. Łatwo sprawdzić, że odwzorowanie

$$g_n : \mathbb{H}(n) \to \mathbb{C}(2n), \quad g_n(A + \mathrm{j}B) = \begin{pmatrix} A & -\bar{B} \\ B & \bar{A} \end{pmatrix},$$

jest $\mathbb{R}$-liniowym monomorfizmem pierścieni. Niech

$$J = \begin{pmatrix} 0 & -I \\ I & 0 \end{pmatrix} \in \mathbb{C}(2n) \quad \text{i} \quad N \in \mathbb{C}(2n).$$

Wtedy

(1.50) $$N \in g_n(\mathbb{H}(n)) \;\Leftrightarrow\; NJ = J\bar{N},$$

więc wyznacznik macierzy $g_n(M)$ o elementach zespolonych jest liczbą rzeczywistą dla każdego $M \in \mathbb{H}(n)$.

Wyznacznik kwaternionowy macierzy $M \in \mathbb{H}(n)$ definiuje się teraz wzorem

$$\det_{\mathbb{H}} M = \det(g_n(M)).$$

Wiadomo z powyższego, że wyznacznik generycznej macierzy $N \in \mathbb{C}(2n)$ jest równy iloczynowi wartości własnych λ tej macierzy. Niech $Nv = \lambda v$, gdzie $v \in \mathbb{C}^{2n}$ jest wektorem własnym odpowiadającym λ. Na mocy (1.50) wektor $J\bar{v}$ jest też wektorem własnym, odpowiadającym wartości własnej $\bar{\lambda}$. Wektory v i $J\bar{v}$ są ortogonalne względem hermitowskiego iloczynu skalarnego $(u|v) = \sum_{i=1}^{2n} \bar{u}_i v_i$ w $\mathbb{C}^{2n}$, są więc liniowo niezależne, nawet jeśli $\bar{\lambda} = \lambda$. Zatem wektory i wartości własne macierzy N występują parami: (v, λ) i $(J\bar{v}, \bar{\lambda})$. Wynika stąd, że iloczyn wszystkich pierwiastków wielomianu w_N, a więc także wyznacznik kwaternionowy macierzy $M \in \mathbb{H}(n)$, jest liczbą nieujemną.

Zdefiniowany w ten sposób wyznacznik macierzy $M \in \mathbb{H}(n)$ jest wielomianem jednorodnym stopnia $2n$ elementów macierzy; w szczególności, jeśli $q \in \mathbb{H}$ i $\lambda, \mu \in \mathbb{R}$, to

$$\det_{\mathbb{H}} q = \bar{q}q \quad \text{i} \quad \det_{\mathbb{H}} \begin{pmatrix} \lambda & q \\ -\bar{q} & \mu \end{pmatrix} = (\lambda\mu + \bar{q}q)^2.$$

Element M pierścienia $\mathbb{H}(n)$ jest odwracalny wtedy i tylko wtedy, gdy $\det_{\mathbb{H}} M \neq 0$. Definiuje się grupy

$$\mathsf{SL}(n, \mathbb{H}) = \{M \in \mathbb{H}(n) \mid \det_{\mathbb{H}} M = 1\}.$$

Inne podejście do wyznaczników, stosujące się do wszystkich ciał nieprzemiennych, pochodzące od Jeana Dieudonnégo, jest przedstawione w [4]. Historię różnych prób zdefiniowania wyznacznika macierzy o elementach kwaternionowych można znaleźć w [5]. Przedstawiona tu definicja pochodzi od Eduarda Study'ego [105].

Zadania

1.1 Pokazać, że każda grupa ma dokładnie jeden element neutralny, a każdy element grupy ma dokładnie jeden element odwrotny.

1.2 Udowodnić, że jeśli dla każdego $a \in G$ zachodzi równość $a^2 = e$, to grupa G jest przemienna. Podać przykład takiej grupy rzędu 4.

1.3 Znaleźć grupy $\mathbb{F}_p^\times$ dla $p = 2, 3, 5$ i 7.

1.4 Wyznaczyć wszystkie, z dokładnością do izomorfizmu, grupy rzędu < 7.

Wskazówka. Pokazać najpierw, że jeśli grupa rzędu 4 posiada element rzędu 4, to jest izomorficzna grupie $\mathbb{Z}_4$. Jeśli nie ma elementu rzędu 4, to elementy $\neq e$ są rzędu 2 i grupa jest izomorficzna z $\mathbb{Z}_2 \times \mathbb{Z}_2$. W grupie rzędu 6 każdy element jest rzędu 1, 2, 3 albo 6.

1.5 Pokazać, że jeśli liczby p i q są względnie pierwsze, to grupy $\mathbb{Z}_{pq}$ i $\mathbb{Z}_p \times \mathbb{Z}_q$ są izomorficzne; pokazać, że grupy $\mathbb{Z}_2 \times \mathbb{Z}_2$ i $\mathbb{Z}_4$ nie są izomorficzne.

1.6 Mówimy, że cykle $\lfloor a_1, \ldots, a_k \rfloor$ i $\lfloor b_1, \ldots, b_l \rfloor$ są *rozłączne*, jeśli zbiory $\{a_1, \ldots, a_k\}$ oraz $\{b_1, \ldots, b_l\}$ są rozłączne. Pokazać, że cykle rozłączne są ze sobą przemienne.

1.7 Rozłożyć permutację

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 1 & 7 & 8 & 6 & 11 & 2 & 4 & 9 & 10 & 5 \end{pmatrix}$$

na iloczyn cykli rozłącznych.

1.8 Pokazać, że jeśli k jest liczbą nieparzystą, to kwadrat k-cyklu jest cyklem. Znaleźć kwadrat cyklu $\lfloor 1, 2, 3, 4 \rfloor$.

1.9 Odnosząc się do przykładu 1.20, pokazać, że

$$\begin{aligned} \dim_{\mathbb{R}} \mathfrak{so}(n) &= \dim_{\mathbb{C}} \mathfrak{so}(n, \mathbb{C}) = \tfrac{1}{2} n(n-1), \\ \dim_{\mathbb{R}} \mathfrak{su}(n) &= n^2 - 1, \\ \dim_{\mathbb{R}} \mathfrak{sp}(n) &= n(2n+1). \end{aligned}$$

1.10 Nawiązując do §2.7 (str. 49), pokazać, że

$$\dim \mathsf{S}^k(\mathbb{k}^n) = \binom{n+k-1}{k}.$$

1.11 Pokazać, że jeśli $\mathbb{k}$ jest ciałem przemiennym, to algebry $\mathbb{k}(m) \otimes \mathbb{k}(n)$ i $\mathbb{k}(mn)$ są izomorficzne.

1.12 Korzystając z $(1 + \sqrt{-1})^m = \binom{m}{0} + \binom{m}{1}\sqrt{-1} - \binom{m}{2} - \binom{m}{3}\sqrt{-1} + \cdots$, uzasadnić (1.41).

1.13 Uzupełnić przykład 1.30, uzasadniając następujące izomorfizmy algebr nad $\mathbb{R}$:

$$\begin{aligned} \mathbb{C} \otimes \mathbb{C} &= 2\mathbb{C}, & \mathbb{C} \hat{\otimes} \mathbb{C} &= \mathbb{H}, \\ \mathbb{H} \otimes \mathbb{H} &= \mathbb{R}(4), & \mathbb{H} \hat{\otimes} \mathbb{H} &= \mathbb{H}(2), \\ \mathbb{C} \otimes \mathbb{H} &= \mathbb{C}(2), & \mathbb{C} \hat{\otimes} \mathbb{H} &= 2\mathbb{H}. \end{aligned}$$

1.14 Znaleźć algebry przeciwne do algebr z gradacją (zob. str. 44 i przykład 1.24, str. 43):

$$\begin{gathered} \mathbb{R} \to \mathbb{C}, \quad \mathbb{C} \to \mathbb{H}, \quad \mathbb{H} \to 2\mathbb{H}, \quad 2\mathbb{H} \to \mathbb{H}(2), \\ \mathbb{H} \to \mathbb{C}(2), \quad \mathbb{C} \to \mathbb{R}(2), \quad \mathbb{R} \to 2\mathbb{R}, \quad 2\mathbb{R} \to \mathbb{R}(2). \end{gathered}$$

1.15 Pokazać, że

(i) odwzorowanie

$$f_n : \mathbb{C}(n) \to \mathbb{R}(2n), \quad f_n(a + \mathrm{i}b) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix},$$

jest monomorfizmem pierścieni oraz

$$f_n(\mathbb{C}(n)) = \{M \in \mathbb{R}(2n) \mid MJ = JM\}, \quad \text{gdzie} \quad J = \begin{pmatrix} 0 & -I \\ I & 0 \end{pmatrix} \in \mathbb{R}(2n);$$

(ii) dla dowolnych $a, b \in \mathbb{R}(n)$ zachodzi warunek

$$\det f_n(a + \mathrm{i}b) = |\det(a + \mathrm{i}b)|^2.$$

1.16 Nawiązując do §2.3 (str. 41), pokazać, że jeśli algebra $\mathcal{A}$ ze sprzężeniem jest czysto rzeczywista, tzn. $\bar{a} = a$ dla każdego $a \in \mathcal{A}$, to algebra $\mathcal{A}^2$ jest przemienna; jeśli algebra $\mathcal{A}$ jest przemienna, to algebra $\mathcal{A}^2$ jest łączna.

Przyjmując jako bazę algebry $\mathbb{O}$ ciąg wektorów

$$(1, 0), (\mathrm{i}, 0), (\mathrm{j}, 0), (\mathrm{k}, 0), (0, 1), (0, \mathrm{i}), (0, \mathrm{j}), (0, \mathrm{k}) \in \mathbb{H} \oplus \mathbb{H},$$

znaleźć tabliczkę mnożenia w algebrze $\mathbb{O}$ i pokazać, przez podanie przykładu, że algebra ta nie jest łączna.

1.17 Nawiązując do przykładu 1.21: (i) pokazać, że jeśli $\mathbb{k} = \mathbb{R}$, to forma ω_+ ma sygnaturę (ℓ, ℓ), (ii) znaleźć wymiary algebr $\mathfrak{g}_\pm$.

1.18 (Różniczkowania algebry macierzy są wewnętrzne.) Niech $d \in \mathcal{A} = \operatorname{End} S$, gdzie S jest n-wymiarową przestrzenią wektorową nad $\mathbb{k}$. Pokazać, że odwzorowanie $\mathcal{A} \to \mathcal{A}$, $a \mapsto [d, a]$, jest różniczkowaniem algebry $\mathcal{A}$ i, na odwrót, każde różniczkowanie algebry $\mathcal{A}$ jest tej postaci.

Wskazówka. Niech $x \in S$ oraz $y \in S^*$ będą takie, że $\langle x, y\rangle = 1$. Mając różniczkowanie D, należy zdefiniować $d \in \mathcal{A}$ wzorem $d(x') = (D(x' \otimes y))(x)$ dla każdego $x' \in S$.

1.19 Pokazać, że $\det_{\mathbb{H}} \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = 1$, choć $\det \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = -1$.