Teoria grup

Jan Dereziński

Katedra Metod Matematycznych Fizyki
Uniwersytet Warszawski
Hoża 74, 00-682, Warszawa
e-mail jan.derezinski@fuw.edu.pl

15 stycznia 2011

rok 2010/11, semestr zimowy

1 Podstawowe własności grup

1.1 Definicja

Grupa to niepusty zbiór G wyposażony w

(1) działanie $G \times G \ni (g,h) \mapsto g \cdot h \in G$ mające własność *łączności*

$$g(gh)k = g(hk), \quad g,h,k \in G.$$

(2) wyróżniony element $e \in G$, zwany elementem neutralnym, spełniający

$$eg = ge = g, \quad g \in G.$$

(3) odwzorowanie $G \ni g \mapsto g^{-1} \in G$, zwane odwrotnością spełniające

$$gg^{-1} = g^{-1}g = e, \quad g \in G.$$

Czyli gupa jest czwórką $(G, \cdot, e, ^{-1})$. Notacja powyższa nosi nazwę *multiplikatywnej*.

Mówimy, że grupa jest *nietrywialna*, gdy jest różna od grupy składającej się jedynie z elementu neutralnego.

Element neutralny w notacji multiplikatywnej jest często oznaczany przez 1 lub $\mathbb{1}$.

Możliwe jest też sformułowanie słabszych aksjomatów, w ktorych grupa jest zbiorem wyposażonym jedynie w łączne działanie i dwa warunki zapewniające istnienie elementu neutralnego i odwrotności.

Mówimy, że grupa jest *przemienna* lub *abelowa*, gdy

$$gh = hg, \quad g,h \in G.$$

Dla grup abelowych stosujemy często notację *addytywną*, w której grupa to $(G, +, 0, -)$.

1.2 Podgrupy

Niech G będzie grupą. Niepusty podzbiór $H \subset G$ nazywamy *podgrupą* gdy jest zamknięty ze względu na mnożenie i branie odwrotności. Zawiera wtedy element neutralny i ze względu na mnożenie i odwrotność dziedziczone z G jest grupą.

Mówimy, że podgrupa jest *nietrywialna*, gdy jest różna od grupy składającej się jedynie z elementu neutralnego, jak również od grupy G.

Jeśli rodzina $H_\alpha \subset G$ składa się z podgrup, to $\cap_\alpha H_\alpha$ jest też podgrupą. Dlatego, dla dowolnego podzbioru $X \subset G$ istnieje najmniejsza podgrupa zawierająca X. Oznaczamy ją przez $\mathrm{Gr}(X)$ i nazywamy *podgrupą generowaną przez X*.

Grupę generowaną przez jeden element nazywamy *grupą cykliczną*. Są to grupy $\mathbb{Z}_n$, $n \in \mathbb{N}$ i $\mathbb{Z}$.

Mówimy, że $g \in G$ ma *rząd* $n \in \mathbb{N} \cap \{\infty\}$, gdy $n = \#\mathrm{Gr}(g)$. Jeśli rząd g jest równy $n \in \mathbb{N}$, to $\mathrm{Gr}(g) = \{e, g, \dots, g^{n-1}\}$ jest podgrupą w G izomorficzną z $\mathbb{Z}_n$. Jeśli rząd g jest równy ∞, to $\mathrm{Gr}(g) = \{\dots, g^{-1}, e, g, g^2, \dots\}$ jest podgrupą izomorficzną z $\mathbb{Z}$.

1.3 Homomorfizmy

Niech G, H będą grupami. Odwzorowanie $\phi : G \to H$ jest *homomorfizmem*, gdy

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2), \quad g_1, g_2 \in G.$$

Stwierdzenie 1.1 *Jeśli ϕ jest homomorfizmem, to*

$$\phi(e_G) = e_H, \quad \phi(g^{-1}) = \phi(g)^{-1}.$$

Dowód.

$$\begin{aligned}
\phi(e_G)e_H &= \phi(e_G^2)\phi(e_G)^{-1} = \phi(e_G)\phi(e_G)^{-1} = e_H. \\
\phi(g^{-1}) &= \phi(g^{-1})\phi(g)\phi(g)^{-1} = \phi(g^{-1}g)\phi(g)^{-1} \\
= \phi(e_G)\phi(g)^{-1} &= e_H\phi(g)^{-1} = \phi(g)^{-1}.
\end{aligned}$$

□

Bijektywny homomorfizm nazywamy *izomorfizmem*.

Jeśli $G = H$, to homomorfizm nazywamy *endomorfizmem* a izomorfizm *automorfizmem*. Automorfizmy grupy G tworzą grupę oznaczaną $\mathrm{Aut}(G)$.

Liczbę elementów zbioru X oznaczamy przez $\#X$ w szczególności, liczbę elementów grupy nazywamy *rzędem grupy*.

1.4 Działanie

Niech X będzie zbiorem. Przez $S(X)$ oznaczamy zbiór bijekcji na zbiorze X. Wtedy $S(X)$ jest grupą ze składaniem i elementem neutralnym równym id, gdzie $\mathrm{id}(x) = x$, $x \in X$.

Niech G będzie grupą. Homomorfizm $G \to S(X)$ nazywamy *działaniem grupy G na zbiorze X*.

Innymi słowy, rodzina

$$G \ni g \mapsto \tau_g \in S(X) \tag{1.1}$$

jest działaniem, gdy

$$\tau_g(\tau_h(x)) = \tau_{gh}(x), \quad g, h \in G.$$

Stosujemy też często notację uproszczoną:

$$G \times X \ni (g, x) \mapsto gx \in X.$$

W tej notacji własności homomorficzności i łączności naturalnie się zapisują:

$$g(hx) = (gh)x, \quad ((gh)k)x = (g(hk))x, \quad g, h, k \in G, \ x \in X.$$

Dlatego też, zbyteczne jest pisanie nawiasów.

Jeśli $x \in X$, to

$$G^x := \{g \in G \ : \ \tau_g(x) = x\}$$

jest podgrupą w G zwaną *grupą izotropii elementu* x.

Niech $\tau : G \times X \to X$, $\tilde{\tau} : G \times \tilde{X} \to \tilde{X}$, będą działaniami. Mówimy, że bijekcja $\phi : X \to \tilde{X}$ jest *izomorfizmem działań* τ *i* $\tilde{\tau}$, gdy

$$\tilde{\tau}_g(\phi(x)) = \phi\left(\tau_g(x)\right), \quad g \in G, \ x \in X.$$

1.5 Orbity

Niech $\tau : G \to X$ będzie działaniem. Definiujemy relację

$$x \sim_\tau y \ \Leftrightarrow \exists_{g \in G} \tau_g(x) = y.$$

Stwierdzenie 1.2 *$\sim_\tau$ jest relacją równoważności.*

Klasy abstrakcji tej relacji nazywamy *orbitami działania* τ. Klasę abstrakcji dla elementu $x \in X$ nazywamy *orbitą elementu* x i oznaczamy $\tau_G(x)$.

Jeśli x, y należą do tej samej orbity, to grupy izotropii G^x i G^y są do siebie *sprzężone*, to znaczy istnieje $g \in G$ takie, że $G^x = gG^y g^{-1}$.

Mówimy, że działanie τ jest *tranzytywne*, gdy posiada dokładnie jedną orbitę. Mówimy też wtedy, że X jest *przestrzenią jednorodną* dla grupy G.

1.6 Warstwy

Niech H będzie podgrupą grupy G. Wtedy H działa na G przez *lewe mnożenie*

$$\lambda_h(g) := hg, \quad g \in G, \ h \in H.$$

Orbity tego działania mają postać

$$Hg := \{hg \ : \ h \in H\}, \ g \in G,$$

i są nazywane *lewymi warstwami podgrupy* H. Zbiór lewych warstw jest oznaczany przez $H\backslash G$.

H działa na G również przez *prawe mnożenie*

$$\rho_h(g) := gh^{-1}, \quad g \in G,\ h \in H.$$

Orbity tego działania mają postać

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

i są nazywane *prawymi warstwami podgrupy* H. Zbiór prawych warstw jest oznaczany przez G/H.

$G \ni g \mapsto g^{-1} \in G$ jest izomorfizmem dla tych działań.

W szczególności, możemy wziąć $H = G$ i dostajemy działanie grupy G na sobie samej. Jest to działanie tranzytywne. Każdemu elementowi $g \in G$ odpowiada inna bijekcja na G. Dlatego też dostajemy

Twierdzenie 1.3 (Cayley) *Każda grupa jest izomorficzna z podgrupą w $S(G)$.*

Następujący wzór definiuje działanie grupy G na G/H:

$$g(kH) := (gk)H, \quad g, k \in G.$$

Działanie to jest tranzytywne. Grupą izotropii elementu jednostkowego jest H.

Niech H_1 i H_2 będą podgrupami. Wtedy działania G na G/H_1 i G/H_2 są izomorficzne wtedy i tylko wtedy gdy H_1 jest sprzężona do H_2.

Twierdzenie 1.4 (Podstawowe twierdzenie o przestrzeniach jednorodnych) *Niech $\tau : G \times X \to X$ będzie działaniem tranzytywnym i $x \in X$. Wtedy wzór*

$$\phi(gG^x) := \tau_g(x)$$

definiuje izomorfizm τ i działania G na przestrzeni warstw G/G^x. Jeśli X jest zbiorem skończonym, to $\#G = \#X\ \#G^x$.

Wniosek:

Twierdzenie 1.5 (Lagrange) *Jeśli G jest grupą skończoną i H jej podgrupą, to*

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

Dowód. Stosujemy Twierdzenie 1.4 do działania G na G/H, zauważając, że $G^e = H$. □

Liczbę $\#G/H$ nazywamy *indeksem podgrupy* H.

1.7 Klasy sprzężoności

Niech $g \in G$. Kładziemy

$$\mathrm{Inn}_g(h) := ghg^{-1}, \quad h \in G.$$

Wtedy Inn_g jest automorfizmem grupy G nazywanym *automorfizmem wewnętrznym.*

$$G \ni g \mapsto \mathrm{Inn}_g \in \mathrm{Aut}(G)$$

jest homomorfizmem.

Grupa G działa na sobie samej przez automorfizmy wewnętrzne. Orbity względem tego działania nazywają się *klasami sprzężoności.*

1.8 Iloczyn grup

Niech K, H będą grupami. Wtedy $K \times H$ jest grupą z iloczynem

$$(k_1, h_1)(k_2, h_2) := (k_1 k_2, h_1 h_2).$$

$K \times H$ z takim iloczynem nazywamy *iloczynem (zewnętrznym) grupy K i H*. Zauważmy, że $K \times \{e_H\}$, $\{e_K\} \times H$ są podgrupami, które komutują, ich przecięcie to $\{(e_K, e_H)\}$ i generują razem $K \times H$.

Latwo pokazać, że jeśli n, m są liczbami względnie pierwszymi, to

$$\mathbb{Z}_m \times \mathbb{Z}_n \ni (i, j) \mapsto (in + jm) \in \mathbb{Z}_{nm}$$

jest izomorfizmem. Każda skończona grupa abelowa jest iloczyne grup postaci $\mathbb{Z}^{p^k}$, gdzie p są liczbami pierwszymi.

1.9 Podgrupy normalne

Niech N będzie podgrupą w G. Mówimy, że N jest *podgrupą normalną*, gdy

$$g \in G,\ n \in N \ \Rightarrow\ gng^{-1} \in N.$$

Równoważny warunek:

$$gN = Ng, \quad g \in G$$

Czyli nie ma wtedy potrzeby rozróżniać lewych i prawych warstw.

Grupę która nie posiada nietrywialnych podgrup normalnych nazywamy *grupą prostą*. Przykładami grup prostych są $\mathbb{Z}_p$ dla pierwszych p i A_n dla $n \geq 5$.

Wszystkie grupy proste skończone zostały sklasyfikowane. Dowód prostoty A_5 jako pierwszy podał Galois w 1831 r. Pełna lista jest znana od 1981 r., kiedy skonstruowano *Grupę Monstrum*. Dowód kompletności tej klasyfikacji ogłoszono w 1983 r. Za datę, kiedy powszechnie zgodzono się z tym, że dowód ten został ukończony uznaje się 2004.

Jeśli $\phi : G \to H$ jest homomorfizmem, to $\phi(G)$ jest podgrupą w H i

$$\mathrm{Ker}\phi = \{g \in G \ : \ \phi(g) = e_H\}$$

jest podgrupą normalną.

Wzór

$$(g_1 N)(g_2 N) := g_1 g_2 N$$

definiuje w G/N strukturę grupy. Odwzorowanie

$$G \ni g \mapsto gN \in G/N$$

jest homomorfizmem, którego jądrem jest N.

Jeśli $\phi : G \to H$ jest surjektywnym homomorfizmem, którego jądrem jest też N, to

$$\psi(gN) := \phi(g)$$

definiuje izomorfizm $\psi : G/N \to H$.

1.10 Iloczyn półprosty

Niech H, N będą grupami i homomorfizm $H \ni h \mapsto \alpha_h \in \mathrm{Aut}(N)$. Definiujemy *(zewnętrzny) iloczyn półprosty* $N \rtimes_\alpha H$ jako $N \times H$ wyposażone w działanie

$$(n_1, h_1)(n_2, h_2) := (n_1 \alpha_{h_1}(n_2), h_1 h_2),$$

element neutralny (e_N, e_H), i odwrotność

$$(n, h)^{-1} = (\alpha_{h^{-1}}(n^{-1}), h^{-1}).$$

Zauważmy, że $N \times e_H$ jest podgrupą normalną, zaś $e_N \times H$ jest podgrupą, ich przecięcie jest równe $\{(e_N, e_H)\}$ oraz $\mathrm{Gr}(N \cap H) = N \rtimes_\alpha H$.

Odwzorowanie

$$N \rtimes_\alpha H \ni (n, h) \mapsto h \in H$$

jest surjektywnym homomorfizmem, którego jądrem jest N.

Sytuację, gdy $\phi : G \to H$ jest surjektywnym homomorfizmem, dla którego N jest jądrem, często zapisujemy w skrócie

$$1 \to N \to G \to H \to 1. \tag{1.2}$$

Mówimy wtedy, że G *jest rozszerzeniem* N *przez* H, albo że mamy *krótki ciąg dokładny (1.2)*. Zachodzi pytanie, kiedy G jest izomorficzne iloczynowi półprostemu N i H? Zachodzi to wtedy, gdy istnieje homomorfizm injektywny $\psi : H \to G$ taki, że $\phi \circ \psi = \mathrm{id}$, $\psi(H)$ i N generują G i $\psi(H) \cap N = e_G$. Nie zawsze to ma miejsce: Weźmy

$$0 \to \mathbb{Z}_2 \to \mathbb{Z}_4 \to \mathbb{Z}_2 \to 0.$$

2 Przykłady grup

2.1 Permutacje

Jeśli X jest zbiorem skończonym, bijekcję na X często nazywamy *permutacją*. Pamiętamy, że przez $S(X)$ oznaczamy grupę bijekcji na X. Piszemy $S_n := S(\{1, 2, \dots, n\})$. Oczywiście, jeśli X ma n elementów, to $S(X)$ jest izomorficzne z S_n.

Permutację $\pi \in S_n$ nazywamy *cyklem k-elementowym*, gdy istnieją parami różne $x_1, \dots, x_k \in \{1, \dots, n\}$ takie, że

$$\pi x_i = x_{i+1},\ i = 1, \dots, k,$$

(rozumiejąc, że $k + 1 = 1$). Cykl oznaczamy przez $(x_1, \dots, x_k)$. Dwa cykle $(x_1, \dots, x_k)$ i $(y_1, \dots, y_m)$ nazywamy *rozłącznymi* jeśli zbiory $\{x_1, \dots, x_k\}$, $\{y_1, \dots, y_m\}$ są rozłączne.

Każdą permutację możemy przedstawić jako iloczyn cykli rozłącznych. Rozkład ten jest jednoznaczny (z dokładnością do kolejności). W szczególności, wyznacza on ciąg $\lambda_1, \lambda_2, \dots$ liczb z $\{0, 1, \dots\}$ takich, że $\sum_j j\lambda_j = n$ i w rozkładzie na cykle rozłączne występuje λ_j cykli j-elementowych.

*Wielomian Vandermonda stopnia n*definiujemy jako

$$V(x_1, \dots, x_n) := \prod_{i<j} (x_i - x_j).$$

Latwo sprawdzić, że dla $\pi \in S_n$,

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

Definiujemy

$$\mathrm{sgn}\pi := \frac{V(x_1, \ldots, x_n)}{V(x_{\pi(1)}, \ldots, x_{\pi(n)})}.$$

sgn : $S_n \to \{1, -1\}$. jest homomorfizmem. Jądro tego homomorfizmu nazywamy *grupą alternującą* i oznaczamy przez A_n.

2.2 Iloczyn półprosty z grupą $\mathbb{Z}_2$

Niech K będzie grupą abelową z zapisem addytywnym. Odwzorowanie $K \ni k \mapsto \beta(k) := -k \in K$ jest automorfizmem grupy K.

Dla grup $\mathbb{Z}_2^n$ jest to automorfizm identycznościowy. Jeśli nie wszystkie elementy grupy K są rzędu 2 lub 1, to jest to automorfizm nietrywialny. Możemy zdefiniować grupę $K \rtimes_\beta \mathbb{Z}_2$. W szczególności, grupa

$$D_n := \mathbb{Z}_n \rtimes_\beta \mathbb{Z}_2$$

nosi nazwę *grupy dwuściennej (dihedralnej)*. Jest ona nieabelowa dla $n \geq 3$.

2.3 Grupa permutacji 3 elementów

Mamy izomorfizm $A_3 \simeq \mathbb{Z}_3$:

$$A_3 = \{\mathrm{id},\ (123),\ (132)\}.$$

Mamy też izomorfizm $S_3 \simeq D_3 = \mathbb{Z}_3 \rtimes_\beta \mathbb{Z}_2$

S_3 posiada następujące nietrywialne podgrupy: jedną podgrupę (normalną) $\mathbb{Z}_3$ i 3 sprzężone do siebie podgrupy $\mathbb{Z}_2$. Mamy zatem 4 nieizomorficzne tranzytywne działania S_3: na zbiorze 6-, 3-, 2- i 1-elementowym

2.4 Grupa permutacji 4 elementów

Elementy grupy $\mathbb{Z}_2 \times \mathbb{Z}_2$ można oznaczyć jako $\{e, a, b, ab\}$. Automorfizmy tej grupy polegają na permutacjach $\{a, b, ab\}$. Czyli

$$\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \simeq S_3.$$

Grupę $\mathbb{Z}_2 \times \mathbb{Z}_2$ można włożyć w $A_4 \subset S_4$

$$\{\mathrm{id},\ (12)(34),\ (13)(24),\ (14)(23)\}.$$

Jest ona normalna w A_4 i w S_4. Mamy izomorfizmy

$$\begin{aligned}(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes A_3 &\simeq A_4,\\ (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes S_3 &\simeq S_4.\end{aligned}$$

2.5 Grupa obrotów $SO(3)$

Przez $SO(3)$ będziemy oznaczać grupę obrotów przestrzeni $\mathbb{R}^3$.

Lemat 2.1 *Dla każdego $A \in SO(3)\setminus\{\mathbb{1}\}$ istnieje dokładnie jedna prosta przechodząca przez 0 i $\theta \in [0, 2\pi[$ takie, że A jest obrotem wokół A o kąt θ. A jest skończonego rzędu, gdy $\theta = \frac{2\pi j}{n}$, $j = 1, \ldots, n-1$.*

Prostą opisaną w powyższym lemacie nazywamy *osią obrotu A*. Jeśli wybierzemy zwrot tej prostęj, będziemy mówili o *osi skierowanej*.

Następnie opiszemy wszystkie skończone podgrupy grupy obrotów.

Lemat 2.2 *Niech G będzie skończoną podgrupą $SO(3)$. Niech α będzie osią pewnego obrotu z G. Wtedy obroty wokół osi α należące do G stanowią grupę izomorficzną z $\mathbb{Z}_n$.*

Oś taką jak w powyższym lemacie nazywamy *osią n-krotną*.

2.6 Grupa obrotów właściwych $C_n \simeq \mathbb{Z}_n$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\frac{2\pi j}{n} & \sin\frac{2\pi j}{n} \\ 0 & -\sin\frac{2\pi j}{n} & \cos\frac{2\pi j}{n} \end{bmatrix}, \quad j = 0, \ldots, n-1. \tag{2.3}$$

2.7 Grupa dihedralna $D_n \simeq \mathbb{Z}_n \rtimes \mathbb{Z}_2$

Do (2.3) dołączamy

$$\begin{bmatrix} -1 & 0 & 0 \\ 0 & -\cos\frac{\pi j}{n} & \sin\frac{\pi j}{n} \\ 0 & \sin\frac{\pi j}{n} & \cos\frac{\pi j}{n} \end{bmatrix}, \quad j = 0, \ldots, n-1. \tag{2.4}$$

2.8 Grupa czworościanu $T \simeq A_4$

Grupa symetrii czworościanu. Permutuje

(1) 4 wierzchołki,

(2) 4 ściany,

(3) 6 krawędzi.

Ma

(1) 4 osie 3-krotne, między wierzchołkiem a przeciwległą ścianą,

(2) 3 osie 2-krotne, między środkami przeciwległych krawędzi.

2.9 Grupa sześcianu/ośmiościanu $C \simeq S_4$

Grupa symetrii sześcianu. Permutuje

(1) 8 wierzchołków/ścian,

(2) 6 ścian/wierzchołków,

(3) 12 krawędzi.

Ma

(1) 4 osie 3-krotne, między przeciwległymi wierzchołkami/ścianami,

(2) 3 osie 4-krotne, między środkami przeciwległych ścian/wierzchołków,

(3) 6 osi 2-krotnych, między środkami przeciwległych krawędzi.

2.10 Grupa dwudziestościanu/dwunastościanu) $I \simeq A_5$

Grupa symetrii dwudziestościanu. Permutuje

(1) 10 wierzchołków/ścian,

(2) 20 ścian/wierzchołków,

(3) 30 krawędzi.

Ma

(1) 6 osi 5-krotnych, między przeciwległymi wierzchołkami/ścianami,

(2) 10 osi 3-krotnych, między środkami przeciwległych ścian/wierzchołków,

(3) 15 osie 2-krotne, między środkami przeciwległych krawędzi.

2.11 Skończone podgrupy grupy obrotów

Twierdzenie 2.3 *Lista powyższa zawiera wszystkie skończone podgrupy obrotów.*

Dowód. Niech G będzie skończoną podgrupą grupy obrotów. Niech S będzie zbiorem osi skierowanychelementów z G, czyli

$$S = \{\alpha \in S^2 \ : \ g\alpha = \alpha \text{ dla pewnego } g \in G\}$$

Dla $\alpha \in S$ niech $G^{(\alpha)}$ będzie podzbiorem w G składającym się z obrotów o osi α, czyli

$$G^{(\alpha)} := \{g \in G \ : \ g\alpha = \alpha\}.$$

$$G \times S \ni (g, \alpha) \mapsto g\alpha \in S$$

jest działaniem grupy G na S. Działanie zachowuje krotność. Niech $O_1, \ldots, O_k$ będzie rozbiciem S na orbity. Niech n_i będzie krotnością elementów orbity O_i. Zakładamy, że $n_1 \leq \cdots \leq n_k$.

Zachodzi wzór

$$\sum_{j=1}^{k} \left(1 - \frac{1}{n_j}\right) = 2\left(1 - \frac{1}{\#G}\right). \tag{2.5}$$

Aby go dowieść, rozważmy

$$P := \{(\alpha, g) \in S \times (G \backslash \{\mathbb{1}\}) \ : \ g\alpha = \alpha\}.$$

Dla każdego $g \in G\backslash\{\mathbb{1}\}$ mamy dwa przecięcia osi obrotu i sfery. Dlatego

$$\#P = 2(\#G - 1). \tag{2.6}$$

Dla każdego $\alpha \in O_j$ jest $n_j - 1$ obrotów $g \in G\backslash\{\mathbb{1}\}$ takich, że $g\alpha = \alpha$. Dlatego

$$\#P = \sum_{i=1}^{k} \#O_i(n_i - 1). \tag{2.7}$$

Ale grupa izotropii $\alpha \in O_i$ jest izomorficzna z $\mathbb{Z}_{n_i}$. Dlatego

$$\#O_i = \frac{\#G}{n_i}. \tag{2.8}$$

(2.6), (2.7) i (2.8) dają razem (2.5).

Rozwiązujemy więc równanie (2.5).

$\#G \geq 2$ implikuje $2\left(1 - \frac{1}{\#G}\right) \in [1, 2[$.

$n_i \geq 2$ implikuje $1 - \frac{1}{n_i} \in [\frac{1}{2}, 1[$. Dla $k = 1$ lewa strona (2.5) < 1. Dla $k \geq 4$ lewa strona (2.5) ≥ 1. Dlatego $k = 2, 3$.

Rozważmy $k = 2$. Możemy przepisać (2.5) jako

$$\frac{1}{n_1} + \frac{1}{n_2} = \frac{2}{\#G}. \tag{2.9}$$

Wiemy, że $n_i \leq \#G$. Więc jedyne rozwiązania (2.9) to $n_1 = n_2 = \#G \in \mathbb{N}$

Rozważmy $k = 3$. Możemy przepisać (2.5) jako

$$\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} = 1 + \frac{2}{\#G}. \tag{2.10}$$

Jeśli $n_1 \geq 3$, to lewa strona (2.10) ≤ 1, co jest niemożliwe. Więc $n_1 = 2$.

Jeśli $n_2 \geq 4$, to znów lewa strona (2.10) ≤ 1, co jest niemożliwe. Więc $n_2 = 2$ lub $n_2 = 3$.

Jeśli $n_2 = 2$, to

$$n_1 = n_2 = 2, \quad n_3 = \frac{\#G}{2}.$$

Jeśli $n_2 = 3$, to dla $n_3 \geq 6$ lewa strona (2.10) ≤ 1. Dlatego $n_3 = 3$, $n_3 = 4$ lub $n_3 = 5$.

Następnie identyfikujemy powstałe możliwości z poszczególnymi grupami

- $n_1 = n_2 = n = \#G$.

  Mamy $\frac{\#G}{n_1} = \frac{\#G}{n_2} = 1$. Zatem mamy tylko jedną oś. Jest ona n-krotna. Zatem $G = C_n$.

- $n_1 = n_2 = 2$, $n_3 = n$, $\#G = 2n$.

  Mamy $\frac{\#G}{n_1} = \frac{\#G}{n_2} = n$, $\frac{\#G}{n_3} = 2$. Zatem mamy tylko jedną oś n-krotną. Zatem G zawiera C_n. Osie 2-krotne muszą być prostopadłe do niej. Jedyna możliwość to D_n.

- $n_1 = 2$, $n_2 = 3$, $n_3 = 3$, $\#G = 12$. Mamy $\frac{\#G}{n_1} = 6$, $\frac{\#G}{n_2} = 4$, $\frac{\#G}{n_3} = 4$. Wybierzmy oś 3-krotną. Musi ona przecinać sferę w dwóch różnych orbitach. Pozostałe punkty 3-krotne tworzą dwa trójkąty równoboczne w płaszczyznach prostopadłych do tej osi.

- $n_1 = 2$, $n_2 = 3$, $n_3 = 4$, $\#G = 24$.

  Mamy $\frac{\#G}{n_1} = 12$, $\frac{\#G}{n_2} = 8$, $\frac{\#G}{n_3} = 6$. Wybierzmy oś 4-krotną. Przecina ona sferę w dwóch elementach orbity O_3. Pozostałe punkty 4-krotne tworzą kwadrat w płaszczyźnie prostopadłej do tej osi.

- $n_1 = 2$, $n_2 = 3$, $n_3 = 5$, $\#G = 60$.

  Mamy $\frac{\#G}{n_1} = 30$, $\frac{\#G}{n_2} = 20$, $\frac{\#G}{n_3} = 12$. Wybierzmy oś 5-krotną. Przecina ona sferę w dwóch elementach orbity O_3. Pozostałe punkty 5-krotne tworzą dwa pięciokąty foremne w dwóch płaszczyznach prostopadłych do tej osi.

3 Grupy macierzowe

3.1 Ciała

Mówimy, że $(\mathbb{K}, +, \cdot, 1, 0\}$ jest *ciałem*, gdy $(\mathbb{K}, +, 0, -\}$ i $(\mathbb{K}^\times, \cdot, 1, {}^{-1})$ są grupami abelowymi spełniającymi

$$x(y + z) = xy + xz,$$

gdzie $\mathbb{K}^\times := \mathbb{K}\backslash\{0\}$.

Definiujemy homomorfizmy, izomorfizmy, etc. ciał w oczywisty sposób.

Najważniejszymi ciałami dla nas są $\mathbb{R}$ i $\mathbb{C}$. $\mathbb{R}$ ma jedynie automorfizm trywialny. $\mathbb{C}$ ma jeden nietrywialny automorfizm: *sprzężenie zespolone* $\mathbb{C} \ni z \mapsto \overline{z} \in \mathbb{C}$.

3.2 Przestrzenie wektorowe

Mówimy, że $(\mathcal{V}, +, 0, -)$ jest *przestrzenią wektorową nad ciałem* $\mathbb{K}$, gdy jest to grupa abelowa wyposażona w działanie $\mathbb{K} \times \mathcal{V} \ni (x, v) \mapsto xv \in \mathcal{V}$ takie, że

$$(x + y)v = xv + yv, \quad (xy)v = x(yv), \quad x, y \in \mathbb{K}, \quad v \in \mathcal{V},$$

$$x(u + v) = xu + xv, \quad x \in \mathbb{K}, \quad u, v \in \mathcal{V}.$$

Przykładem przestrzeni nad $\mathbb{K}$ są $\mathbb{K}^n$. Przestrzenie wektorowe izomorficzne z $\mathbb{K}^n$ nazywamy *przestrzeniami wymiaru n*

3.3 Odwzorowania liniowe

Homomorfizmy przestrzeni wektorowych nazywamy *odwzorowaniami liniowymi.*

Jeśli $\mathcal{V}$, $\mathcal{W}$ są przestrzeniami, to $L(\mathcal{V}, \mathcal{W})$ będzie oznaczało zbiór odwzorowań liniowych z $\mathcal{V}$ do $\mathcal{W}$. Będziemy pisać $L(\mathcal{V}) := L(\mathcal{V}, \mathcal{V})$.

$L(\mathbb{K}^n, \mathbb{K}^m)$ będziemy utożsamić z macierzami o n wierszach i m kolumnach. Dla $A \in L(\mathbb{K}^n, \mathbb{K}^m)$ przez A^*, $\overline{A}$ i $A^\#$ będziemy oznaczać macierz *hermitowsko sprzężoną, zespolenie sprzężoną i transponowaną do A.*

3.4 Ogólna grupa liniowa

Niech $A \in L(\mathbb{K}^n)$. Wzór

$$\det A := \sum_{\pi \in S_n} \mathrm{sgn}\pi A_{1,\pi(1)} \cdots A_{n,\pi(n)} \in \mathbb{K}$$

definiuje *wyznacznik* spełniający

$$\det AB = \det A \det B.$$

$GL(\mathbb{K}^n)$ definiujemy jako

$$GL(\mathbb{K}^n) := \{A \in L(\mathbb{K}^n) \ : \ \det A \neq 0\}.$$

Jest to grupa. Piszemy też

$$GL(\mathbb{K}^n) = GL(n, \mathbb{K}).$$

Wyznacznik definiuje homomorfizm

$$\det GL(\mathbb{K}^n) \to \mathbb{K}^\times.$$

Definiujemy

$$SL(\mathbb{K}^n) = SL(n, \mathbb{K}) := \{A \in GL(\mathbb{K}^n) \ : \ \det A = 1\}.$$

Można też podejść do grupy GL bardziej abstrakcyjnie. Niech $\mathcal{V}, \mathcal{W}$ będą przestrzeniami wektorowymi nad ciałem $\mathbb{K}$. Zbiór bijekcji liniowych z $\mathcal{V}$ w $\mathcal{W}$ oznaczamy przez $Gl(\mathcal{V}, \mathcal{W})$. W szczególności $GL(\mathcal{V}) := GL(\mathcal{V}, \mathcal{V})$ jest grupą. Dla $\mathcal{V} = \mathbb{K}^n$ pokrywa się to z poprzednią definicją.

3.5 Grupa ortogonalna w skończonym wymiarze

$O(\mathbb{K}^n)$ definiujemy jako

$$O(\mathbb{K}^n) := \{A \in L(\mathbb{K}^n) \ : \ A^\# A = \mathbb{1}\}.$$

(Automatycznie elementy $O(\mathbb{K}^n)$ spełniają $AA^\# = \mathbb{1}$). Jest to podgrupa w $GL(\mathbb{K}^n)$. Piszemy też

$$O(\mathbb{R}^n) = O(n).$$

Macierze ortogonalne zachowują standardowy iloczyn skalarny w $\mathbb{K}^n$.

Latwo pokazać, że wyznacznik macierzy ortogonalnych może mieć wartość ± 1, Definiujemy

$$SO(\mathbb{K}^n) := SL(\mathbb{K}^n) \cap O(\mathbb{K}^n).$$

W przypadku zespolonym piszemy też $O(n, \mathbb{C}) = O(\mathbb{C}^n)$, $SO(n, \mathbb{C}) = SO(\mathbb{C}^n)$.

W przypadku rzeczywistym piszemy też $O(n) = O(\mathbb{R}^n)$, $SO(n) = SO(\mathbb{R}^n)$. Grupa $O(n)$ ma dwie składowe spójne. Składowa spójna zawierająca jedność pokrywa się z $SO(n)$.

3.6 Grupa pseudo-ortogonalna

Rozważmy dalej przypadek rzeczywisty. Niech $q, p \in 0, 1, \ldots$. Przez $\mathbb{R}^{q,p}$ będziemy rozumieć przestrzeń $\mathbb{R}^{q+p} = \mathbb{R}^q \oplus \mathbb{R}^p$ z iloczynem zadanym przez tensor $I_{q,p} := \begin{bmatrix} -\mathbb{1} & 0 \\ 0 & \mathbb{1} \end{bmatrix}$. To znaczy,

$$vI_{q,p}v' = -\sum_{i=1}^{q} v_i v_i' + \sum_{j=q+1}^{q+p} v_j v_j'. \tag{3.11}$$

$O(\mathbb{R}^{q,p})$ definiujemy jako zbiór macierzy spełniających

$$A^{\#} I_{q,p} A = I_{q,p}.$$

(Automatycznie spełniają one $AI_{q,p}A^{\#} = I_{q,p}$). Jest to grupa. Piszemy też

$$O(\mathbb{R}^{q,p}) = O(q,p).$$

Macierze pseudoortogonalne zachowują iloczyn pseudoskalarny w $\mathbb{R}^{q,p}$.

Wyznacznik macierzy pseudo-ortogonalnych może mieć wartość ± 1, Definiujemy

$$SO(\mathbb{R}^{q,p}) = SO(q,p) := \{A \in O(\mathbb{R}^{q,p}) \ : \ \det A = 1\}.$$

Jeśli $q = 1$, grupę $O(\mathbb{R}^{q,p})$ nazywamy grupą Lorentza. Ma ona cztery składowe spójne. Spójna składowa jedności jest nazywana ortoczasową grupą Lorentza i jest oznaczana $SO^{\uparrow}(\mathbb{R}^{q,p})$

3.7 Abstrakcyjne podejście do grup (pseudo-)ortogonalnych

Można też podejść bardziej abstrakcyjnie. Niech $\mathcal{V}$, $\mathcal{W}$ będą przestrzeniami wektorowymi z formą symetryczną, którą dla $v, v' \in \mathcal{V}$ oznaczamy $v \cdot v'$. Zbiór bijekcji liniowych z $\mathcal{V}$ w $\mathcal{W}$ spełniających

$$Av \cdot Av' = v \cdot v'$$

oznaczamy przez $O(\mathcal{V}, \mathcal{W})$. W szczególności $O(\mathcal{V}) := O(\mathcal{V}, \mathcal{V})$ jest grupą.

Dla $\mathcal{V} = \mathbb{R}^n$ każdą niezdegenerowaną formę symetryczną można sprowadzić do postaci (3.11), i wtedy $\mathcal{V}$ nazywamy $\mathbb{R}^{q,p}$. Więc obie definicje sie w tym wypadku pokrywają.

Dla $\mathcal{V}$ każdą niezdegenerowaną formę można sprowadzić do postaci (3.11) z $q = 0$.

Dla przestrzenie nieskończenie wymiarowych z reguły zakładamy, że forma symetryczna jest dodatnio określona i nazywamy ją iloczynem skalarnym. Zakładamy też z reguły, że przestrzenie są zupełne, czyli że są *rzeczywistymi przestrzeniami Hilberta.*

3.8 Grupa unitarna w skończonym wymiarze

$U(\mathbb{C}^n)$ definiujemy jako

$$U(\mathbb{C}^n) := \{A \in L(\mathbb{C}^n) \ : \ A^* A = \mathbb{1}\}.$$

(Automatycznie elementy $U(\mathbb{C}^n)$ spełniają $AA^* = \mathbb{1}$). Jest to podgrupa w $GL(\mathbb{C}^n)$. Piszemy też

$$U(\mathbb{C}^n) = U(n).$$

Macierze unitarne zachowują standardowy iloczyn skalarny w $\mathbb{C}^n$.

Latwo pokazać, że wyznacznik macierzy unitarnych ma moduł 1. Definiujemy

$$SU(\mathbb{C}^n) := SL(\mathbb{C}^n) \cap U(\mathbb{C}^n).$$

3.9 Grupa pseudo-unitarna

Niech $q, p \in 0, 1, \ldots$. Przez $\mathbb{C}^{q,p}$ będziemy rozumieć przestrzeń $\mathbb{C}^{q+p} = \mathbb{C}^q \oplus \mathbb{C}^p$ z iloczynem zadanym przez tensor $I_{q,p} := \begin{bmatrix} -\mathbb{1} & 0 \\ 0 & \mathbb{1} \end{bmatrix}$. To znaczy,

$$\overline{v} I_{q,p} v' = -\sum_{i=1}^{q} \overline{v}_i v'_i + \sum_{j=q+1}^{q+p} \overline{v}_j v'_j. \tag{3.12}$$

$U(\mathbb{C}^{q,p})$ definiujemy jako zbiór macierzy spełniających

$$A^* I_{q,p} A = I_{q,p}.$$

(Automatycznie spełniają one $A I_{q,p} A^* = I_{q,p}$). Jest to grupa. Piszemy też

$$U(\mathbb{C}^{q,p}) = U(q, p).$$

Macierze pseudo-unitarne zachowują iloczyn pseudoskalarny w $\mathbb{C}^{q,p}$.

Wyznacznik macierzy pseudo-unitarnych ma moduł 1. Definiujemy

$$SU(\mathbb{C}^{q,p}) = SU(q, p) := \{A \in U(\mathbb{C}^{q,p}) \ : \ \det A = 1\}.$$

3.10 Abstrakcyjne podejście do grup (pseudo-)unitarnych

Można też podejść bardziej abstrakcyjnie. Niech $\mathcal{V}$, $\mathcal{W}$ będą zespolonymi przestrzeniami wektorowymi z wyróżnioną formą hermiowską, którą dla $v, v' \in \mathcal{V}$ oznaczamy $\overline{v} \cdot v'$. Zbiór bijekcji liniowych z $\mathcal{V}$ w $\mathcal{W}$ spełniających

$$\overline{Av} \cdot Av' = \overline{v} \cdot v'$$

oznaczamy przez $U(\mathcal{V}, \mathcal{W})$. W szczególności $U(\mathcal{V}) := U(\mathcal{V}, \mathcal{V})$ jest grupą.

Dla $\mathcal{V} = \mathbb{C}^n$ każdą niezdegenerowaną formę hermitowską można sprowadzić do postaci (3.12), i wtedy $\mathcal{V}$ nazywamy $\mathbb{C}^{q,p}$. Więc obie definicje sie w tym wypadku pokrywają.

Dla przestrzenie nieskończenie wymiarowych z reguły zakładamy, że forma hermitowska jest dodatnio określona i nazywamy ją iloczynem skalarnym. Zakładamy też z reguły, że przestrzenie są zupełne, czyli że są *(zespolonymi) przestreniami Hilberta*

3.11 Grupa symplektyczna w skończonym wymiarze

W przestrzeni $\mathbb{K}^{2n} = \mathbb{K}^n \oplus \mathbb{K}^n$ wprowadzamy macierz $J = \begin{bmatrix} 0 & \mathbb{1} \\ -\mathbb{1} & 0 \end{bmatrix}$. Grupa $Sp(\mathbb{K}^n) = Sp(n, \mathbb{K})$ jest zdefiniowana jako

$$Sp(\mathbb{K}) := \{A \in L(\mathbb{K}^n) \ : \ A^{\#} J A = J\}$$

(Automatycznie elementy $Sp(\mathbb{K}^n)$ spełniają $A J A^{\#} = J$). Jest to podgrupa w $GL(\mathbb{K}^n)$. Macierze symplektyczne zachowują standardową formę symplektyczną w $\mathbb{K}^n$.

$$v \omega v' = \sum_{i=1}^{n} (v_i v'_{i+n} - v_{i+n} v'_i). \tag{3.13}$$

Latwo pokazać, że wyznacznik macierzy symplektycznych jest równy 1. Dlatego $Sp(\mathbb{K}^n)$ jest podgrupą w $SL(\mathbb{K}^n)$.

3.12 Abstrakcyjne podejście do grup symplektycznych

Można też podejść bardziej abstrakcyjnie. Niech $\mathcal{V}$, $\mathcal{W}$ będą przestrzeniami wektorowymi z formą symetryczną, którą np. dla $v, v' \in \mathcal{V}$ oznaczamy $v\omega v'$. Zbiór bijekcji liniowych z $\mathcal{V}$ w $\mathcal{W}$ spełniających

$$Av\omega\, Av' = v\omega v'$$

oznaczamy przez $Sp(\mathcal{V}, \mathcal{W})$. W szczególności $Sp(\mathcal{V}) := Sp(\mathcal{V}, \mathcal{V})$ jest grupą.

Każdą niezdegenerowaną formę symetryczną można sprowadzić do postaci (3.13). Więc obie definicje się w tym wypadku pokrywają.

3.13 Grupy afiniczne

Niech $\mathcal{V}$ będzie przestrzenią wektorową. Odwzorowaniem afinicznym na $\mathcal{V}$ nazywamy odwzorowanie postaci

$$\mathcal{V} \ni v \mapsto w + Av \in \mathcal{V}$$

gdzie $w \in \mathcal{V}$ i $A \in L(\mathcal{V})$. Odwzorowania afiniczne dla których $A \in GL(\mathcal{V})$ tworzą grupę z działaniem

$$(w_1, A_1)(w_2, A_2) := (w_1 + A_1 w_2, A_1 A_2)$$

elementem neutralnym $(0, \mathbb{1})$ i odwrotnością $(w, A)^{-1} = (A^{-1}w, A^{-1})$. Grupę tę nazywamy *afinicznym rozszerzeniem grupy* $GL(\mathcal{V})$.

Grupa $GL(\mathcal{V})$ działa na elementy z $\mathcal{V}$ w oczywisty sposób. Czyli dostajemy homomorfizm

$$GL(\mathcal{V}) \ni A \mapsto A \in \mathrm{Aut}(\mathcal{V}),$$

gdzie z prawej $\mathcal{V}$ jest traktowana jako grupa z dodawaniem. Latwo widzimy, że grupa afiniczna jest iloczynem półprostym $\mathcal{V} \rtimes GL(\mathcal{V})$.

Często w zastosowaniach spotykamy grupy w których $GL(\mathcal{V})$ jest zastąpione jej podgrupą. Na przykład, grupa Poincarego jest afinicznym rozszerzeniem grupy Lorentza $\mathbb{R}^{1,3} \rtimes O(1,3)$.

3.14 Grupy Liego

Mówimy, że G jest *grupą Liego*, jeśli jest to grupa będąca rozmaitością (gładką) i odwzorowania

$$\begin{aligned} G \times G \ni (g,h) &\mapsto gh \in G \\ G \ni g &\mapsto g^{-1} \in G \end{aligned}$$

są gładkie.

Wszystkie rozważane w tej sekcji grupy dla skończenie wymiarowych $\mathcal{V}$ nad ciałem $\mathbb{K} = \mathbb{R}$ lub $\mathbb{C}$ są grupami Liego.

Oto wymiary wybranyh grup Liego

(1) $\dim SL(\mathbb{R}^n) = \dim SU(\mathbb{C}^n) = n^2 - 1$,

(2) $\dim SO(\mathbb{R}^n) = \frac{n(n-1)}{2}$,

(3) $\dim Sp(\mathbb{R}^{2n} = \frac{2n(2n+1)}{2}$.

4 Koincydencje wśród grup macierzowych

4.1 $SL(2,\mathbb{K}) \simeq Sp(2,\mathbb{K})$

Niech
$$J := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

Zauważmy, że dla $A \in L(\mathbb{K}^2)$ mamy
$$AJA^{\#} = (\det A)J.$$

4.2 $SU(2)/\mathbb{Z}_2 \simeq SO(3)$

Utożsamiamy $\mathbb{R}^3$ z macierzami hermitowskimi 2×2 o śladzie 0:
$$\mathbb{R}^3 \ni (x,y,x) \mapsto X = \begin{bmatrix} z & x + \mathrm{i}y \\ x - \mathrm{i}y & -z \end{bmatrix}.$$

Zauważmy, że
$$-\det X = x^2 + y^2 + z^2,$$
czyli wyznacznik zadaje standardowy iloczyn skalarny.

Dla $A \in SU(2)$ kładziemy
$$\rho_A X := AXA^*.$$

Wtedy
$$\det \rho_A X = \det X.$$

Zatem ρ_A zachowuje iloczyn skalarny.
$$SU(2) \ni A \mapsto \rho_A \in SO(3).$$
jest surjektywnym homomorfizmem. Jego jądrem jest $\pm\mathbb{1}$.

4.3 $SL(2,\mathbb{R})/\mathbb{Z}_2 \simeq SO(1,2)$, $SL(2,\mathbb{C})/\mathbb{Z}_2 \simeq SO(3,\mathbb{C})$,

Utożsamiamy $\mathbb{K}^3$ z macierzami 2×2 o śladzie 0:
$$\mathbb{K}^3 \ni (x,y,x) \mapsto X = \begin{bmatrix} z & x + y \\ x - y & -x \end{bmatrix}.$$

Zauważmy, że
$$-\det X = -x^2 + y^2 + z^2.$$

Dla $\mathbb{K} = \mathbb{R}$ wyznacznik zadaje iloczyn pseudoskalarny o sygnaturze $(1,2)$. Dla $\mathbb{K} = \mathbb{C}$ jest to zwykły iloczyn skalarny.

Dla $A \in SL(2,\mathbb{K})$ kładziemy
$$\rho_A X := AXA^{-1}.$$

Wtedy

$$\det \rho_A X = \det X.$$

Zatem ρ_A zachowuje iloczyn (pseudo-)skalarny.

$$SL(2,\mathbb{R}) \ni A \mapsto \rho_A \in SO(1,2),$$
$$SL(2,\mathbb{C}) \ni A \mapsto \rho_A \in SO(3,\mathbb{C}),$$

są surjektywnymi homomorfizmami. Ich jądrem jest $\pm 1\!\!1$.

4.4 $SL(2,\mathbb{C})/\mathbb{Z}_2 \simeq SO(1,3)$

Utożsamiamy $\mathbb{R}^4$ z macierzami 2×2 hermitowskimi

$$\mathbb{R}^3 \ni (t,x,y,x) \mapsto X = \begin{bmatrix} t+z & x+\mathrm{i}y \\ x-\mathrm{i}y & t-z \end{bmatrix}.$$

Zauważmy, że

$$-\det X = -t^2 + x^2 + y^2 + z^2,$$

czyli wyznacznik zadaje iloczyn pseudo-skalarny.

Dla $A \in SL(2,\mathbb{C})$ kładziemy

$$\rho_A X := AXA^*.$$

Wtedy

$$\det \rho_A X = \det X.$$

Zatem ρ_A zachowuje iloczyn pseudo-skalarny.

$$SL(2,\mathbb{C}) \ni A \mapsto \rho_A \in SO^{\uparrow}(1,3).$$

jest surjektywnym homomorfizmem. Jego jądrem jest $\pm 1\!\!1$.

4.5 $(SL(2,\mathbb{R}) \times SL(2,\mathbb{R}))/\mathbb{Z}_2 \simeq SO(2,2)$, $(SL(2,\mathbb{C}) \times SL(2,\mathbb{C}))/\mathbb{Z}_2 \simeq SO(4,\mathbb{C})$,

Utożsamiamy $\mathbb{K}^4$ z macierzami 2×2:

$$\mathbb{K}^3 \ni (t,x,y,x) \mapsto X = \begin{bmatrix} t+z & x+y \\ x-y & t-z \end{bmatrix}.$$

Zauważmy, że

$$-\det X = -t^2 - x^2 + y^2 + z^2.$$

Dla $\mathbb{K} = \mathbb{R}$ wyznacznik zadaje iloczyn pseudoskalarny o sygnaturze $(2,2)$. Dla $\mathbb{K} = \mathbb{C}$ jest to zwykły iloczyn skalarny.

Dla $(A,B) \in SL(2,\mathbb{K})$ kładziemy

$$\rho_{(A,B)} X := AXB^{-1}.$$

Wtedy

$$\det \rho_{(A,B)} X = \det X.$$

Zatem $\rho_{(A,B)}$ zachowuje iloczyn (pseudo-)skalarny.

$$\begin{aligned} SL(2,\mathbb{R}) \times SL(2,\mathbb{R}) \ni (A,B) \mapsto \rho_{(A,B)} \in SO(2,2), \\ SL(2,\mathbb{C}) \times SL(2,\mathbb{R}) \ni (A,B) \mapsto \rho_{A} \in SO(4,\mathbb{C}), \end{aligned}$$

są surjektywnymi homomorfizmami. Ich jądrem jest $\pm\mathbb{1}$.

4.6 $(SU(2) \times SU(2))/\mathbb{Z}_2 \simeq SO(4)$

Utożsamiamy $\mathbb{R}^4$ z macierzami zespolonymi 2×2 spełniającymi $\overline{X} = JXJ$ w następujący sposób:

$$\mathbb{R}^4 \ni (t,x,y,x) \mapsto X = \begin{bmatrix} \mathrm{i}t + z & x + \mathrm{i}y \\ x - \mathrm{i}y & \mathrm{i}t - z \end{bmatrix}.$$

Zauważmy, że

$$-\det X = t^2 + x^2 + y^2 + z^2.$$

Czyli zadaje standardowy iloczyn skalarny.

Dla $(A,B) \in SU(2) \times SU(2)$ kładziemy

$$\rho_{(A,B)} X := AXB^{-1}.$$

Wtedy

$$\det \rho_{(A,B)} X = \det X.$$

Zatem $\rho_{(A,B)}$ zachowuje iloczyn skalarny.

$$SU(2) \times SU(2) \ni (A,B) \mapsto \rho_{(A,B)} \in SO(4).$$

jest surjektywnym homomorfizmem. Jego jądrem jest $\pm\mathbb{1}$.

5 Reprezentacje grup

5.1 Definicja

Niech G będzie grupą a $\mathcal{V}$ przestrzenią liniową. *Reprezentacją grupy G na przestrzeni $\mathcal{V}$* nazywamy homomorfizm $\pi : G \to Gl(\mathcal{V})$. Będziemy też często pisać, że para $(\pi, \mathcal{V})$ jest reprezentacją grupy G.

Innymi słowy, $G \ni g \mapsto \pi(g) \in L(\mathcal{V})$ jest reprezentacją, gdy

$$\pi(g_1 g_2) = \pi(g_1)\pi(g_2), \quad g_1, g_2 \in G.$$

Jeśli $\mathcal{V}$ jest przestrzenią Hilberta, to *reprezentacją unitarną grupy G na przestrzeni $\mathcal{V}$* nazywamy homomorfizm $\pi : G \to U(\mathcal{V})$.

W szczególności, $G \ni g \mapsto \mathbb{1}_{\mathcal{V}} \in L(\mathcal{V})$ jst reprezentacją. Nazywamy ją *reprezentacją trywialną*.

5.2 Suma prosta

Niech $\mathcal{V}_1$, $\mathcal{V}_2$ będą przestrzeniami liniowymi. Wtedy $\mathcal{V}_1 \times \mathcal{V}_2$ ma strukturę przestrzeni wektorowej, oznaczane przez $\mathcal{V}_1 \oplus \mathcal{V}_2$ i nazywanej *sumą prostą przestrzeni* $\mathcal{V}_1$ *i* $\mathcal{V}_2$.

Jeśli $A_i \in L(\mathcal{V}_i)$, to $A_1 \oplus A_2 \in L(\mathcal{V}_1 \oplus \mathcal{V}_2)$ jest zdefiniowany jako

$$(A_1 \oplus A_2)(v_1, v_2) := (A_1 v_1, A_2 v_2).$$

Niech $(\pi_i, \mathcal{V}_i)$ będą reprezentacjami na przestrzeniach $\mathcal{V}_i$. Wtedy

$$\pi_1 \oplus \pi_2(g) := \pi_1(g) \oplus \pi_2(g)$$

definiuje reprezentację na przestrzeni $\mathcal{V}_1 \oplus \mathcal{V}_2$ zwaną *sumą prostą reprezentacji* π_1 *i* π_2. Będziemy pisać

$$m\pi = \underbrace{\pi \oplus \cdots \oplus \pi}_{m \text{ razy}}.$$

5.3 Równoważność

Niech $(\pi, \mathcal{V}_\pi)$, $(\rho, \mathcal{V}_\rho)$ będą reprezentacjami G. Mówimy, że operator U *splata* π i ρ, jeśli

$$U\pi(g) = \rho(g)U, \quad g \in G. \tag{5.14}$$

Mówimy, że π, ρ są reprezentacjami *równoważnymi*, gdy istnieje $U \in Gl(\mathcal{V}_\pi, \mathcal{V}_\rho)$ splatający π i ρ. Piszemy wtedy $\pi \simeq \rho$.

Jeśli dodatkowo przestrzenie te są przestrzeniami Hilberta, mówimy, że π, ρ są *unitarnie równoważne*, gdy istnieje $U \in U(\mathcal{V}_\pi, \mathcal{V}_\rho)$ splatający π i ρ.

Twierdzenie 5.1 *Niech $\mathcal{V}_\pi$, $\mathcal{V}_\rho$ będą skończenie wymiarowymi przestrzeniami Hilberta. Niech $(\pi, \mathcal{V}_\pi)$, $(\rho, \mathcal{V}_\rho)$ będą reprezentacjami unitarnymi. Wtedy ich równoważność jest równoważna unitarnej równoważności.*

Dowód. Niech $A \in GL(\mathcal{V}_\pi, \mathcal{V}_\rho)$ splata π i ρ. Wtedy $A^* \in GL(\mathcal{V}_\rho, \mathcal{V}_\pi)$ splata ρ i π. Zatem $A^*A \in GL(\mathcal{V}_\pi)$ splata π z sobą. To samo jest prawdą dla $(A^*A)^{-1/2}$. Zatem operator unitarny $(AA^*)^{-1/2}A$ splata π z ρ. $\square$

5.4 Nieprzywiedlność

Niech $(\pi, \mathcal{V})$ będzie reprezentacją G. Mówimy, że podprzestrzeń $\mathcal{V}_1 \subset \mathcal{V}$ jest *niezmiennicza dla* $(\pi, \mathcal{V})$, gdy jest niezmiennicza względem $\pi(g)$, $g \in G$. Połóżmy $\pi_1 := \pi\Big|_{\mathcal{V}_1}$. Wtedy $(\pi_1, \mathcal{V}_1)$ jest też reprezentacją. Mówimy, że $(\pi_1, \mathcal{V}_1)$ jest *podreprezentacją* reprezentacji $(\pi, \mathcal{V})$.

Twierdzenie 5.2 *Jeśli $(\pi, \mathcal{V})$ jest unitarna i $\mathcal{V}_1$ jest niezmiennicza dla $(\pi, \mathcal{V})$, to $\mathcal{V}^\perp$ jest też niezmiennicza dla $(\pi, \mathcal{V})$.*

Mówimy, że $(\pi, \mathcal{V})$ jest *nieprzywiedlna*, gdy nie istnieje nietrywialna podprzestrzeń w $\mathcal{V}$ niezmiennicza względem π.

Mówimy, że $(\rho, \mathcal{V})$ jest *całkowicie rozkładalna*, gdy $\rho \simeq \oplus_{i=1}^n \pi_i$, gdzie π_i są nieprzywiedlne.

Twierdzenie 5.3 *Niech* $(\pi, \mathcal{V})$ *będzie reprezentacją unitarną w skończenie wymiarowej przestrzeni. Wtedy* $(\pi, \mathcal{V})$ *jest całkowicie rozkładalna.*

Dowód. Załóżmy, że $\mathcal{V}$ jest przywiedlna. Wtedy posiada nietrywialną podprzestrzeń niezmienniczą $\mathcal{V}_1$. $\mathcal{V}_2 := \mathcal{V}_1^{\perp}$ jest też niezmiennicza. Kontynuując dostaniemy rozkład. □

Jeśli weźmiemy reprezentację $\mathbb{R} \ni t \mapsto \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} \in L(\mathbb{C}^2)$, to $\mathbb{C} \oplus \{0\}$ jest przestrzenią niezmienniczą, która nie posiada dopełniającej niezmienniczej. Dlatego jest to reprezentacja przywiedlna, ale nie jest całkowicie rozkładalna. Nie jest natomiast unitarna.

5.5 Reprezentacje jednowymiarowe

Rozważmy reprezentacje w jednowymiarowej przestrzeni zespolonej. Takie reprezentacje mają wartości w grupie $GL(\mathbb{C})$, która pokrywa się z multiplikatywną grupą liczb zespolonych $\mathbb{C}^{\times}$. W $\mathbb{C}$ mamy z dokładnością do proporcjonalności tylko jeden iloczyn skalarny. Reprezentacja jest unitarna (bądź unitaryzowalna) gdy ma wartości w $U(\mathbb{C}) = \{z \in \mathbb{C} \ : \ |z| = 1\}$.

Każda reprezentacja jednowymiarowa jest nieprzywiedlna. Jeśli $G \ni g \mapsto \chi(g) \in \mathbb{C}^{\times}$ jest jednowymiarową reprezentacją zaś $G \ni g \mapsto \pi(g)$ jest dowolną reprezentacją, to

$$\chi\pi(g) := \chi(g)\pi(g)$$

jest też reprezentacją. Jeśli π jest nieprzywiedlne, to $\chi\pi$ też. W szczególności, reprezentacje jednowymiarowe dowolnej grupy tworzą grupę ze względu na mnożenie.

Dla grupy $\mathbb{Z}_n$, dla $m = 0, \dots, n-1$,

$$\mathbb{Z}_n \ni k \mapsto \mathrm{e}^{\frac{\mathrm{i}2\pi km}{n}} \in \mathbb{C}^{\times}$$

jest reprezentacją. Jest ona zawsze unitarna. Ogólniej

$$\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_p} \ni (k_1, \dots, k_p) \mapsto \mathrm{e}^{\frac{\mathrm{i}2\pi k_1 m_1}{n_1}} \cdots \mathrm{e}^{\frac{\mathrm{i}2\pi k_p m_p}{n_p}} \in \mathbb{C}^{\times}$$

jest reprezentacją unitarną. Latwo się przekonać, że wszystkie nieprzywiedlne reprezentacje grupy $\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_p}$ są tej postaci.

Dla grupy $\mathbb{Z}$, dla dowolnego $\mu \in \mathbb{C}$

$$\mathbb{Z} \ni k \mapsto \mathrm{e}^{k\mathrm{i}\mu} \in \mathbb{C}^{\times}$$

jest reprezentacją. Jest ona unitarna wtedy i tylko wtedy gdy μ jest rzeczywiste. W szczególności, nie wszystkie reprezentacje $\mathbb{Z}$ są unitaryzowalne.

5.6 Reprezentacje permutacyjne

Niech grupa G działa na zbiorze X. Niech δ_x będzie bazą kanoniczną w $l^2(X)$. Wtedy

$$\pi(g)\delta_x := \delta_{gx}, \quad g \in G, \ x \in X,$$

lub równoważnie

$$\pi(g)f(x) := f(g^{-1}x), \quad g \in G, \ x \in X,$$

definiuje reprezentację unitarną na $l^2(X)$.

Jeśli X jest skończone, to reprezentacja ta jest przywiedlna, bo przesrtrzeń rozpięta na wektorze $\sum_x \delta_x$ jest niezmiennicza.

5.7 Podstawowe reprezentacje grupy permutacji

Rozważmy powyższą konstrukcję dla grupy S_n działającej na $\{1, \ldots, n\}$. Zatem rozważamy S_n działającą na $\mathbb{C}^n$,

$$\pi\delta_i := \delta_{\pi i}.$$

Niech $\mathcal{V}_n = \{f \in \mathbb{C}^n \ : \ f_1 + \ldots + f_n = 0\} = \{(1, \ldots, 1)\}^\perp$. Reprezentacja π obcięta do $\mathcal{V}$ bywa nazywana *reprezentacją standardową grupy* S_n.

Twierdzenie 5.4 *Reprezentacja standardowa jest nieprzywiedlna dla* $n \geq 2$

Dowód. Twierdzenie jest oczywiste dla grupy S_2, dla której wymiar reprezentacji jest równy 1.

Załóżmy, że twierdzenie jest prawdziwe dla $n-1$. Bazą przestrzeni $\mathcal{V}_n$ jest $e_1 = \delta_1 - \delta_n, \ldots, e_{n-1} := \delta_{n-1} - \delta_n$. Rozważmy grupę $S_{n-1} \subset S_n$. Działa one na bazę $e_1, \ldots, e_{n-1}$ jak reprezentacja permutacyjna. Dlatego też, z założenia indukcyjnego, jej jedyne nietrywialne podprzestrzenie niezmiennicze są rozpięte przez $e_1 + \ldots + e_{n-1} = \delta_1 + \ldots + \delta_{n-1} - (n-1)\delta_n$ oraz jej dopełnienie ortogonalne. Latwo się przekonać, że jakikolwiek element $S_n \backslash S_{n-1}$ nie zachowuje obu podprzestrzeni. □

Zauważmy, że dla grupy A_3, reprezentacja standardowe na $\mathcal{V}_3$ jest przywiedlna. Dla A_4, reprezentacja standardowa jest nieprzywiedlna na $\mathcal{V}_3$. Dlatego też, Twierdzenie 5.4 jest słuszne jeśli zastąpimy S_n przez A_n i $n \geq 4$ (z takim samym dowodem).

Zatem dla dowolnej grupy permutacji znamy już 4 reprezentacje nieprzywiedlne.

(1) trywialna, (1-wymiarowa),

(2) sgn, (1-wymiarowa),

(3) standardowa, ($d-1$-wymiarowa),

(4) sgn×standardowa, ($d-1$-wymiarowa).

Dla małych n niektóre z nich się pokrywają: Dla S_2, (1)=(4), (2)=(3). Dla S_3, (3)=(4).

Począwszy od S_4, wszystkie cztery reprezentacje są różne.

5.8 Lematy Schura

Twierdzenie 5.5 (Pierwszy Lemat Schura) *Niech* $(\pi, \mathcal{V})$ *będzie nieprzywiedlną unitarną reprezentacją* G. *Niech* A *splata* $(\pi, \mathcal{V})$ *z samą sobą. Wtedy* $A = c\mathbb{1}$ *dla pewnego* $c \in \mathbb{C}$.

Dowód. Niech A będzie niezerowym operatorem splatającym $(\pi, \mathcal{V})$ z sobą. A^* też splata. Jeden z operatorów $A + A^*$ i $\mathrm{i}(A - A^*)$ jest niezerowy i oba splatają. Zatem można założyć, że A jest samosprzężony. Jeśli A nie jest równy $\lambda\mathbb{1}$, to znaczy, że istnieją $\lambda_1 \neq \lambda_2$ w spektrum A.

Załóżmy dla uproszczenia, że $\dim \mathcal{V} < \infty$. Wtedy $\mathrm{Ker}(A - \lambda_1)$ jest nietrywialną podprzestrzenią niezmienniczą, co jest sprzecznością. $\Box$

Twierdzenie 5.6 (Drugi Lemat Schura) *Niech $(\pi, \mathcal{V}_\pi)$, $(\rho, \mathcal{V}_\rho)$ będą nieprzywiedlnymi unitarnymi reprezentacjami G. Jeśli istnieje $A \neq 0$ splatający $(\pi, \mathcal{V}_\pi)$ z $(\rho, \mathcal{V}_\rho)$, to $(\pi, \mathcal{V}_\pi)$ jest unitarnie równoważna $(\rho, \mathcal{V}_\rho)$.*

Dowód. Niech $A \neq 0$. $A^*A \neq 0$ splata $(\pi, \mathcal{V}_\pi)$ z sobą. Dlatego $A^*A = \lambda_1 \mathbb{1}$, $\lambda_1 \neq 0$. Podobnie, AA^* splata $(\rho, \mathcal{V}_\rho)$ z sobą. Dlatego $A^*A = \lambda_2 \mathbb{1}$. Mamy $\lambda_1^2 \mathbb{1} = A^*AA^*A = \lambda_2 A^*A = \lambda_2\lambda_1 \mathbb{1}$. Zatem $\lambda_1 = \lambda_2 =: \lambda$. Więc $U := \lambda^{-\frac{1}{2}} A$ jest unitarny. $\Box$

5.9 Iloczyn tensorowy I

Najpierw wprawadźmy iloczyn tensorowy w "naiwny" sposób.

Oznaczmy bazę kanoniczną $\mathbb{C}^n$ przez e_i, $i = 1, \dots, n$, zaś bazę kanoniczną $\mathbb{C}^m$ przez f_j, $j = 1, \dots, m$. Przestrzeń $\mathbb{C}^n \otimes \mathbb{C}^m$ można zdefiniować jako $\mathbb{C}^{nm}$ z bazą $e_i \otimes f_j$, $i = 1, \dots, n, j = 1, \dots, m$. Czyli elementy $\mathbb{C}^n \otimes \mathbb{C}^m$ są postaci $\sum_{i,j=1}^n t_{ij} e_i \otimes f_j$.

Jeśli $v = \sum_{i=1}^n v_i e_i, = \sum_{j=1}^m v_j f_j$, to kładziemy

$$v \otimes w := \sum_{i=1}^n \sum_{j=1}^m v_i w_j e_i \otimes f_j.$$

Niech A będzie operatorem na $\mathbb{C}^n$ a B operatorem na $\mathbb{C}^m$. Przez $A \otimes B$ rozumiemy operator na $\mathbb{C}^n \otimes \mathbb{C}^m$, którego macierz jest równa

$$(A \otimes B)_{ij,kl} = A_{ik} B_{jl}.$$

Jeśli A i B są unitarne/hermitowskie, to $A \otimes B$ też.

5.10 Iloczyn tensorowy II

Wprowadźmy teraz iloczyn tensorowy w sposób niezależny od bazy. Niech $\mathcal{V}$, $\mathcal{W}$ będą przestrzeniami. Dla uproszczenia, będziemy zakładać, że są skończenie wymiarowe.

Niech $\mathcal{Z}$ będzie przestrzenią skończonych kombinacji liniowych wektorów (v, w), $v \in \mathcal{V}$, $w \in \mathcal{W}$. W przestrzeni tej wyróżniamy podprzestrzeń $\mathcal{Z}_0$ rozpiętą na wektorach

$$\begin{aligned} (\lambda v, w) - \lambda(v, w), &\qquad (v, \lambda w) - \lambda(v, w), \\ (v_1 + v_2, w) - (v_1, w) - (v_2, w), &\qquad (v, w_1 + w_2) - (v, w_1) - (v, w_2). \end{aligned}$$

Definiujemy $\mathcal{V} \otimes \mathcal{W} := \mathcal{Z}/\mathcal{Z}_0$. Jeśli $v \in \mathcal{V}$, $w \in \mathcal{W}$, to definiujemy $v \otimes w := (v, w) + \mathcal{Z}_0$.

$\mathcal{V} \otimes \mathcal{W}$ jest przestrzenią wektorową. $\otimes$ jest działaniem spełniającym warunki

$$\begin{aligned} (\lambda v) \otimes w = \lambda v \otimes w, &\qquad v \otimes (\lambda w) - \lambda v \otimes w, \\ (v_1 + v_2) \otimes w - v_1 \otimes w - v_2 \otimes w, &\qquad v \otimes (w_1 + w_2) - v \otimes w_1 - v \otimes w_2. \end{aligned}$$

Wektory postaci $v \otimes w$ nazywają się *tensorami prostymi*. Nie są to wszystkie wektory w $\mathcal{V} \otimes \mathcal{W}$, ale rozpinają $\mathcal{V} \otimes \mathcal{W}$.

Pokażmy, że powyższa definicja jest rółnoważna definicji "naiwnej".

Twierdzenie 5.7 *Jeśli e_i, $i = 1, \dots, n$ jest bazą w $\mathcal{V}$, zaś f_j, $j = 1, \dots, m$ bazą w $\mathcal{W}$, to $e_i \otimes f_j$, $i = 1, \dots, n, j = 1, \dots, m$. jest bazą w $\mathcal{V} \otimes \mathcal{W}$.*

Dowód. Latwo sprawdzamy, że $e_i \otimes f_j$ rozpinają $\mathcal{V} \otimes \mathcal{W}$. Trzeba pokazać ich liniową niezależność. Niech

$$\sum_{i,j} t^{ij} e_i \otimes f_j = 0. \tag{5.15}$$

Niech $e^1, \dots, e^n$ będzie bazą dualną do $e_1, \dots, e_n$, tzn

$$\langle e^i | e_j \rangle = \delta^i_j.$$

Podobnie, niech $f^1, \dots, f^m$ będzie bazą dualną do $f_1, \dots, f_m$. Zdefiniujmy funkcjonał p^{ij} na $\mathcal{Z}$ wzorem

$$\langle p^{ij} | (v, w) \rangle = \langle e^i | v \rangle \langle f^j | w \rangle.$$

Sprawdzamy, że $p^{ij} = 0$ na $\mathcal{Z}_0$. Zatem p^{ij} jest dobrze określony na $\mathcal{V} \otimes \mathcal{W} = \mathcal{Z} / \mathcal{Z}_0$. Stosując p^{ij} do (5.15) dostajemy $t^{ij} = 0$. $\square$

Twierdzenie 5.8 *Jeśli $\mathcal{V}$ i $\mathcal{W}$ są przestrzeniami Hilberta, to $\mathcal{V} \otimes \mathcal{W}$ posiada jedyny iloczyn skalarny taki, że*

$$(v_1 \otimes w_1 | v_2 \otimes w_2) = (v_1 | v_2)(w_1 | w_2). \tag{5.16}$$

Jeśli e_i, $i = 1, \dots, n$ jest bazą ortonormalną w $\mathcal{V}$, zaś f_j, $j = 1, \dots, m$ bazą ortonormalną w $\mathcal{W}$, to $e_i \otimes f_j$, $i = 1, \dots, n, j = 1, \dots, m$. jest bazą ortonormalną w $\mathcal{V} \otimes \mathcal{W}$.

Dowód. Najpierw sprawdzamy, że jeśli iloczyn skalarny o własności (5.16) istnieje, to część twierdzenia o bazach ortonormalnych musi być prawdziwa. $\square$

Twierdzenie 5.9 *Niech A będzie operatorem na $\mathcal{V}$ i B operatorem na $\mathcal{W}$. Wtedy istnieje dokładnie jeden operator $A \otimes B$ na $\mathcal{V} \otimes \mathcal{W}$ taki, że*

$$(A \otimes B) v \otimes w := (Av) \otimes (Bw).$$

Dowód. Wystarczy zdefiniować $A \otimes B$ w bazie:

$$(A \otimes B) e_i \otimes f_j := (Ae_i) \otimes (Bf_j).$$

$\square$

Niech $(\pi, \mathcal{V})$, $(\rho, \mathcal{W})$ będą reprezentacjami. *Iloczynem tensorowym tych reprezentacji* nazywamy reprezentację $\pi \otimes \rho$ w przestrzeni $\mathcal{V} \otimes \mathcal{W}$

$$(\pi \otimes \rho)(g) = \pi(g) \otimes \rho(g).$$

Zauważmy, że $m\pi$ jest równoważne $\pi \otimes 1\!\!1_{\mathbb{C}^m}$.

5.11 Reprezentacja grupy permutacji

Twierdzenie 5.10 *Dla $\sigma \in S_n$ istnieje dokładnie jeden operator $\Theta(\sigma) \in L(\otimes^n \mathcal{V}$, dla którego*

$$\Theta(\sigma) v_1 \otimes \cdots \otimes v_n = v_{\sigma^{-1}1} \otimes \cdots \otimes v_{\sigma^{-1}n}.$$

$$S_n \ni \sigma \mapsto \Theta(\sigma) \in L(\mathcal{V}^{\otimes n})$$

jest reprezentacją.

Dowód. Wystarczy wybrać bazę $e_1, \ldots, e_m$ w $\mathcal{V}$ i położyć

$$\Theta(\sigma) e_{i_1} \otimes \cdots \otimes e_{i_n} = e_{i_{\sigma^{-1}1}} \otimes \cdots \otimes e_{i_{\sigma^{-1}n}}$$

To definiuje jednoznacznie operator $\Theta(\sigma)$.

Pokażmy, że $\Theta(\pi)\Theta(\sigma) = \Theta(\pi\sigma)$. Niech $v_1, \ldots, v_n \in \mathcal{V}$ i $w_i := v_{\sigma^{-1}i}$. Wtedy

$$\begin{aligned}
\Theta(\pi)\Theta(\sigma) v_1 \otimes \cdots \otimes v_n &= \Theta(\pi) w_1 \otimes \cdots \otimes w_n \\
&= w_{\pi^{-1}1} \otimes \cdots \otimes w_{\pi^{-1}n} \\
&= w_{\sigma^{-1}\pi^{-1}1} \otimes \cdots \otimes w_{\sigma^{-1}\pi^{-1}n} \\
&= w_{(\pi\sigma)^{-1}1} \otimes \cdots \otimes w_{(\pi\sigma)^{-1}n}.
\end{aligned}$$

Jeśli $\mathcal{V}$ jest przestrzenią Hilberta, jest to reprezentacja unitarna.

Jest to reprezentacja przywiedlna. W szczególności, można podać rzuty ortogonalne na podprzestrzenie na których reprezentacja jest trywialna i znakową:

$$\begin{aligned}
\Theta^n_{\mathrm{s}} &:= \frac{1}{n!} \sum_{\sigma \in S_n} \Theta(\sigma), \\
\Theta^n_{\mathrm{a}} &:= \frac{1}{n!} \sum_{\sigma \in S_n} \mathrm{sgn}\sigma \Theta(\sigma).
\end{aligned}$$

Kładziemy $\otimes^n_{\mathrm{s/a}} \mathcal{V} := \Theta^n_{\mathrm{s/a}} \otimes^n \mathcal{V}$.

Zauważmy, że

$$\begin{aligned}
\Theta^2_{\mathrm{s}} &:= \frac{1}{2}(\mathbb{1} + \Theta(\tau)), \\
\Theta^2_{\mathrm{a}} &:= \frac{1}{2}(\mathbb{1} - \Theta(\tau)).
\end{aligned}$$

Zatem $\mathbb{1} = \Theta^2_{\mathrm{s}} + \Theta^2_{\mathrm{a}}$. Czyli każdy 2-tensor można rozłożyć na część symetryczną i antysymetryczną: $\otimes^2 \mathcal{V} = \otimes^2_{\mathrm{s}} \mathcal{V} \oplus \otimes^2_{\mathrm{a}} \mathcal{V}$.

Jeśli $t \in \otimes^n \mathcal{V}$, to

$$t = \sum t_{i_1,\ldots,i_n} e_{i_1} \otimes \cdots \otimes e_{i_n}.$$

Wtedy

$$\begin{aligned}
\Theta_{\mathrm{s}} t &= \sum t_{(i_1,\ldots,i_n)} e_{i_1} \otimes \cdots \otimes e_{i_n}, \\
\Theta_{\mathrm{a}} t &= \sum t_{[i_1,\ldots,i_n]} e_{i_1} \otimes \cdots \otimes e_{i_n},
\end{aligned}$$

gdzie

$$\begin{aligned} t_{(i_1,\dots,i_n)} &= \frac{1}{n!}\sum_{\sigma\in S_n} t_{i_{\sigma i},\dots,i_{\sigma n}}, \\ t_{[i_1,\dots,i_n]} &= \frac{1}{n!}\sum_{\sigma\in S_n} \mathrm{sgn}\sigma t_{i_{\sigma i},\dots,i_{\sigma n}}. \end{aligned}$$

5.12 Charaktery

Załóżmy, że π jest reprezentacją na skończenie wymiarowej przestrzeni $\mathcal{V}$. Charakterem reprezentacji π nazywamy funkcję na G równą

$$\chi_\pi(g) := \mathrm{Tr}\pi(g).$$

Mamy $\dim \mathcal{V} = \chi_\pi(e)$,

$$\begin{aligned} \chi_\pi(g) &= \chi_\pi(hgh^{-1}), \quad g,h\in G; \\ \chi_{\pi\oplus\rho} &= \chi_\pi + \chi_\rho, \\ \chi_{n\pi} &= n\chi_\pi, \\ \chi_{\pi\otimes\rho} &= \chi_\pi\chi_\rho, \\ \chi_{\overline{\pi}} &= \overline{\chi}_\pi, \\ \chi_{\otimes^2_{\mathrm{s}}\pi} &= \frac{1}{2}\left(\chi_\pi(g)^2 + \chi_\pi(g^2)\right); \\ \chi_{\otimes^2_{\mathrm{a}}\pi} &= \frac{1}{2}\left(\chi_\pi(g)^2 - \chi_\pi(g^2)\right). \end{aligned}$$

6 Reprezentacje grup skończonych

W tej sekcji wszystkie grupy są skończone.

6.1 Unitaryzowalność

Twierdzenie 6.1 *Niech G będzie grupą skończoną a $(\pi,\mathcal{V}_\pi)$ jej reprezentacją. Wtedy istnieje iloczyn skalarny na $\mathcal{V}_\pi$ taki, że π jest reprezentacją unitarną.*

Dowód. Wybierzmy dowolny iloczyn skalarny $(\cdot|\cdot)_0$ w $\mathcal{V}_\pi$. Wtedy

$$(v|w) := \frac{1}{\#G}\sum_{g\in G}(\pi(g)v|\pi(g)w)_0$$

jest też iloczynem skalarnym. Mamy

$$(\pi(h)v|\pi(h)w) = \frac{1}{\#G}\sum_{g\in G}(\pi(hg)v|\pi(hg)w)_0 = (v|w).$$

Zatem π jest reprzentacją unitarną. $\square$

Stąd wniosek, że każda reprezentacja grupy skończonej w skończenie wymiarowej przestrzeni jest całkowici rozkładalna.

6.2 Relacje ortogonalności

Unitarna równoważność reprezentacji jest relacją równoważności. Przez $\hat{G}$ będziemy oznaczali zbiór klas abstrakcji względem tej relacji. W praktyce dla każdego elementu $\hat{G}$ wybierzemy reprezentanta $(\pi, \mathcal{V}_\pi)$. Wybierzemy również bazę ortonormalną $e_{\pi,1}, \ldots, e_{\pi,d_\pi}$, gdzie $d_\pi := \dim \mathcal{V}_\pi$. Możemy wtedy zapisać π jako macierz

$$[\pi_{ij}(g)]_{i,j=1,\ldots,d_\pi}, \quad g \in G.$$

Czyli

$$\pi_{ij}(g) = (e_{\pi,i}|\pi(g)e_{\pi,j}).$$

Mamy też charaktery nieprzywiedlne

$$\chi_\pi(g) := \sum_{i=1}^{d_\pi} \pi_{ii}(g) = \mathrm{Tr}\pi(g)$$

W $l^2(G)$ będziemy używać iloczynu skalarnego

$$(f|f') := \frac{1}{\#G} \sum \overline{f(g)} f'(g).$$

Twierdzenie 6.2 *Niech $\pi, \pi' \in \hat{G}$.*

$$(\pi_{ij}|\pi'_{km}) = \frac{1}{\#G} \sum_{g\in G} \overline{\pi_{ij}(g)}\pi'_{km}(g) \quad = \quad \frac{1}{d_\pi}\delta_{\pi,\pi'}\delta_{ik}\delta_{jm}, \tag{6.17}$$

$$(\chi_\pi|\chi_{\pi'}) = \frac{1}{\#G} \sum_{g\in G} \overline{\chi_\pi(g)}\chi_{\pi'}(g) \quad = \quad \delta_{\pi,\pi'}. \tag{6.18}$$

Lemat 6.3 *Niech π, π' będą reprezentacjami. Niech H będzie operatorem z $\mathcal{V}_{\pi'}$ do $\mathcal{V}_\pi$. Zdefiniujmy*

$$\langle H \rangle := \frac{1}{\#G} \sum_{g\in G} \pi(g^{-1}) H \pi'(g).$$

Wtedy $\langle H \rangle$ splata π' i π. W szczególności, jeśli π, π' są nieprzywiedlne, to $\langle H \rangle$ jest niezerowe jedynie, gdy są one równoważne i wtedy (przyjmując, że $\mathcal{V}_\pi = \mathcal{V}_{\pi'}$) mamy

$$\langle H \rangle = \frac{\mathrm{Tr} H}{d_\pi} \mathbb{1}_{\mathcal{V}_\pi}. \tag{6.19}$$

Dowód.

$$\begin{aligned}
\pi(h)\langle H \rangle &= \frac{1}{\#G} \sum_{g\in G} \pi(hg^{-1}) H \pi'(g) \\
&= \frac{1}{\#G} \sum_{g\in G} \pi((gh^{-1})^{-1}) H \pi'(gh^{-1})\pi'(h) \; = \; \langle H \rangle \pi'(h).
\end{aligned}$$

Nastę[pnie stosujemy Lemat Schura. Pokażmy na koniec (6.19). Wiemy, że $\langle H\rangle = c1\!\!1_{\mathcal{V}_\pi}$. Zatem

$$cd_\pi = \mathrm{Tr}\langle H\rangle = \frac{1}{\#G}\sum_{g\in G}\mathrm{Tr}\pi(g^{-1})H\pi(g) = \mathrm{Tr}H.$$

□

Dowód Twierdzenia 6.2 Stosujemy Lemat 6.3 do $H = |e_{\pi,j})(e_{\pi',m}|$.

$$\begin{aligned}\frac{1}{\#G}\sum_{g\in G}\pi(g^{-1})|e_{\pi,j})(e_{\pi',m}|\pi'(g) &= \frac{1}{d_\pi}1\!\!1_{\mathcal{V}_\pi}\delta_{\pi,\pi'}\mathrm{Tr}|e_{\pi j})(e_{\pi,m}| \\ &= \frac{1}{d_\pi}1\!\!1_{\mathcal{V}_\pi}\delta_{\pi,\pi'}\delta_{jm}.\end{aligned}$$

Następnie obkładamy obie strony przez $(e_{\pi,i}|\cdots|e_{\pi',k})$, dostając (6.17). Aby pokazać (6.18), liczymy:

$$(\chi_\pi|\chi_{\pi'}) = \sum_{i=1}^{d_\pi}\sum_{j=1}^{d_{\pi'}}(\pi_{ii}|\pi'_{jj}) = \sum_{i=1}^{d_\pi}(\pi_{ii}|\pi_{ii}) = \delta_{\pi\pi'}\frac{d_\pi}{d_\pi}.$$

□

6.3 Rozkład reprezentacji

Niech $(\rho, \mathcal{W})$ będzie reprezentacją grupy G na przestrzeni wymiaru d_ρ. Wiemy, że

$$\rho \simeq \underset{\pi\in\hat{G}}{\oplus} m_\pi\pi. \tag{6.20}$$

Zatem

$$d_\rho = \sum_{\pi\in\hat{G}} m_\pi d_\pi. \tag{6.21}$$

Mamy też rozkład przestrzeni $\mathcal{W}$ na sumę prostą ortogonalną $\mathcal{W} = \oplus_{\pi\in\hat{G}}\mathcal{W}_\pi$ taki, że $\rho\Big|_{\mathcal{W}_\pi}$ jest równoważna $m_\pi\pi$, oraz rzuty ortogonalne $Q_\pi$na $\mathcal{W}_\pi$. Oczywiście, $\mathcal{W}_\pi = \mathrm{Ran}Q_\pi$,

$$\sum_{\pi\in\hat{G}} Q_\pi = 1\!\!1, \quad Q_\pi^* = Q_\pi, \quad Q_\pi Q_{\pi'} = Q_\pi.$$

Pokażemy, że liczby m_π, podprzestrzenie $\mathcal{W}_\pi$ i rzuty Q_π są wyznaczone jednoznacznie. Pokażemy, jak je łatwo znajdować.

Pamiętamy, że charakter ρ jest zdefiniowany jako $\chi_\rho(g) := \mathrm{Tr}\rho(g)$, $g \in G$.

Twierdzenie 6.4 *Dla* $\pi \in \hat{G}$

$$m_\pi = \frac{1}{\#G}\sum_{g\in G}\overline{\chi_\pi(g)}\chi_\rho(g) \tag{6.22}$$

$$= (\chi_\pi|\chi_\rho), \tag{6.23}$$

$$Q_\pi = \frac{d_\pi}{\#G}\sum_{g\in G}\overline{\chi_\pi(g)}\pi(g). \tag{6.24}$$

Dowód. Niech ρ spełnia (6.20). Wtedy

$$\rho = \sum m_\pi \rho_\pi.$$

Następnie relacja ortogonalności charakterów implikuje (6.22).

Możemy znaleźć bazę ortonormalną w $\mathcal{W}_\pi$ $e_{\pi,i,p}$, $i = 1, \ldots, d_\pi$, $p = 1, \ldots, m_\pi$ taką, że

$$\rho(g) e_{\pi,i,p} = \sum_{j=1}^{d_\pi} \pi_{ji}(g) e_{\pi,j,p}.$$

Wtedy

$$\begin{aligned}
\frac{d_\pi}{\#G} \sum_{g\in G} \overline{\chi_{\pi'}(g)} \rho(g) e_{\pi,i,p} &= \frac{d_\pi}{\#G} \sum_{g\in G} \sum_{k=1}^{d_{\pi'}} \sum_{j=1}^{d_\pi} \overline{\pi'_{kk}(g)} \pi_{ji}(g) e_{\pi,j,p} \\
&= \delta_{\pi,\pi'} \sum_{k,j=1}^{d_\pi} \delta_{kj} \delta_{ki} e_{\pi,j,p} \; = \; \delta_{\pi,\pi'} e_{\pi,i,p}.
\end{aligned}$$

6.4 Reprezentacja regularna

Jeśli grupa G działa na zbiorze X, to wiąże się z tym unitarna reprezentacja grupy G na przestrzeni $l^2(X)$ zadana przez

$$\lambda(g) f(x) := f(g^{-1}x), \quad g \in G, \; x \in X.$$

W szczególności, rozważmy $X = G$. Iloczyn skalarny w $l^2(G)$ normalizujemy

$$(f|f') := \frac{1}{\#G} \sum \overline{f(g)} f'(g).$$

Dostajemy reprezentację na $l^2(G)$ zwaną *(lewą) reprezentacją regularną*. Mamy też *prawą reprezentację regularną*

$$\rho(g) f(h) := f(hg), \quad g, h \in G.$$

Twierdzenie 6.5 (1) $\lambda \simeq \underset{\pi\in\hat{G}}{\oplus} d_\pi \pi$.

(2) $\#G = \sum_{\pi\in\hat{G}} d_\pi^2$. *Funkcje* $\sqrt{d_\pi}\pi_{ij}$ *stanowią bazę ortonormalną w* $l^2(G)$.

Dowód. Charakter reprezentacji regularnej jest równy

$$\chi_\lambda(g) = \#G \; \delta_e(g).$$

Stąd

$$m_\pi = (\chi_\lambda|\chi_\pi) = \chi_\pi(e) = d_\pi.$$

To pokazuje (1), z którego na mocy (6.21) wynika (2).

Wiemy, że $\{\sqrt{d_\pi}\pi_{ij} \;:\; \pi \in \hat{G}, \; i, j = 1, \ldots, d_\pi\}$ stanowią układ ortonormalny. (2) oznacza, że liczba jego elementów równa jest wymiarowi $l^2(G) = \#G$. Zatem jest to baza ortonormalna. □

6.5 Liczba reprezentacji nieprzywiedlnych

Twierdzenie 6.6 *Liczba klas sprzężoności jest równa liczbie reprezentacji nieprzywiedlnych.*

Dowód. Niech $l^2_{\mathrm{cent}}(G)$ będzie podprzesterzenią $l^2(G)$ składającą się z funkcji stałych na klasach sprzężoności. Wiemy, że χ_π, $\pi \in \hat{G}$, stanowią układ ortonormalny w $l^2_{\mathrm{cent}}(G)$. Pokażemy, że jest to baza ortonormalna.

Najpierw zauważmy, że z Lematu (6.3) wynika, że

$$\langle \pi(g) \rangle = \frac{\chi_\pi(g)}{d_\pi} \mathbb{1}_{\mathcal{V}_\pi}. \tag{6.25}$$

Niech $f \in l^2_{\mathrm{cent}}(G)$.

$$\begin{aligned}
f(g) &= \sum_{\pi\in\hat{G}} \sum_{i,j}^{d_\pi} f_{\pi,ij}\pi_{ij}(g) \\
&= \frac{1}{\#G} \sum_{h\in G} \sum_{\pi\in\hat{G}} \sum_{i,j}^{d_\pi} f_{\pi,ij}\pi_{ij}(hgh^{-1}) \\
&= \sum_{\pi\in\hat{G}} \sum_{i,j}^{d_\pi} f_{\pi,ij}(e_{\pi,i}|\langle\pi(g)\rangle e_{\pi,j}) \\
&= \sum_{\pi\in\hat{G}} \sum_{i}^{d_\pi} f_{\pi,ii}\frac{\chi_\pi(g)}{d_\pi},
\end{aligned}$$

gdzie w ostatnim kroku skorzystaliśmy z (6.25). Zatem $l^2_{\mathrm{cent}}(G)$ jest rozpięte przez χ_π, $\pi \in \hat{G}$. □

7 Algebry łączne

7.1 Definicja

Niech $\mathfrak{A}$ będzie przestrzenią wektorową nad ciałem $\mathbb{K}$. Mówimy, że $\mathfrak{A}$ jest *algebrą* jeśli jest wyposażona w działanie

$$\mathfrak{A} \times \mathfrak{A} \ni (A, B) \mapsto AB \in \mathfrak{A}$$

spełniające

$$\begin{aligned}
&A(B + C) = AB + AC, \quad (B + C)A = BA + CA, \\
&(\alpha\beta)(AB) = (\alpha A)(\beta B).
\end{aligned}$$

Jeśli w dodatku

$$A(BC) = (AB)C,$$

to mówimy, że jest to *algebra łączna*. (W praktyce, skracamy nazwę, przez *algebrę* rozumiejąc algebrę łączną).

Mówimy, że $\mathfrak{A}$ jest *algebrą przemienną* gdy $A, B \in \mathfrak{A}$ implikuje $AB = BA$.

Centrum algebry $\mathfrak{A}$ jest zdefiniowane jako

$$\mathfrak{Z}(\mathfrak{A}) = \{A \in \mathfrak{A} \ : \ AB = BA, \ B \in \mathfrak{A}\}.$$

7.2 Podalgebry

Ustalmy algebrę $\mathfrak{A}$. $\mathfrak{B} \subset \mathfrak{A}$ nazywmy *podalgebrą* gdy jest to podprzestrzeń liniowa i $A, B \in \mathfrak{B} \Rightarrow AB \in \mathfrak{B}$. Oczywiście, podalgebra jest również algebrą.

Jeśli rodzina $\mathfrak{B}_\alpha \subset \mathfrak{A}$ składa się z podalgebr, to $\cap_\alpha \mathfrak{B}_\alpha$ jest też podgrupą. Dlatego, dla dowolnego podzbioru $\mathfrak{B} \subset \mathfrak{A}$ istnieje najmniejsza podalgebra zawierająca $\mathfrak{B}$. Oznaczamy ją przez $\mathrm{Alg}(\mathfrak{B})$ i nazywamy *podalgebrą generowaną przez* $\mathfrak{B}$.

Niech $\mathcal{V}$ będzie przestrzenią wektorową nad $\mathbb{K}$. Oczywiście, zbiór liniowych odwzorowań w $\mathcal{V}$, oznaczany przez $L(\mathcal{V})$, jest algebrą.

Podalgebry w $L(\mathcal{V})$ nazywane są *konkretnymi algebrami.*

7.3 Identyczność

Identyczność algebry $\mathfrak{A}$ to element $\mathbb{1} \in \mathfrak{A}$ taki, że

$$A = \mathbb{1}A = A\mathbb{1}, \quad A \in \mathfrak{A}.$$

Każda algebra ma najwyżej jedną identyczność. W rzeczy samej, jeśli $\mathbb{1}_1, \mathbb{1}_2$ są identycznościami, to

$$\mathbb{1}_1 = \mathbb{1}_1\mathbb{1}_2 = \mathbb{1}_2.$$

Mówimy, że $\mathfrak{A}$ jest *unitalna* albo *z jedynką*, jeśli posiada identyczność. W dalszym ciągu, dla $\lambda \in \mathbb{C}$ będziemy po prostu pisać λ zamiast $\lambda\mathbb{1}$.

Zawsze można do algebry $\mathfrak{A}$ dołączyć jedynkę. Dostajemy wtedy algebrę $\mathfrak{A}_\mathbf{1}$, jako przestrzeń wektorow równą $\mathfrak{A} \oplus \mathbb{C}$ z działaniem

$$(A, \lambda)(B, \mu) := (AB + \lambda B + \mu A, \lambda\mu).$$

7.4 Idempotenty

$P \in \mathfrak{A}$ nazywa się *idempotentem* gdy $P^2 = P$. $P\mathfrak{A}P$ jest podalgebrą zwaną *algebrą zredukowaną.*

Identyczność jest idempotentem.

Idempotent P nazywa się *minimalnym* gdy $P\mathfrak{A}P$ jest jednowymiarowa.

7.5 Sumy proste

Jeśli $\mathfrak{A}_1$, $\mathfrak{A}_2$ są algebrami, możemy zdefiniować $\mathfrak{A}_1 \oplus \mathfrak{A}_2$.

Jeśli $\mathfrak{A}$ jest algebrą i $P \in \mathfrak{A} \cap \mathfrak{A}'$ jest idempotentem, to oczywiście $P\mathfrak{A} = P\mathfrak{A}P$ jest podalgebrą. $\mathfrak{A}$ jest naturalnie izomorficzna z $P\mathfrak{A} \oplus (1 - P)\mathfrak{A}$.

7.6 Homomorfizmy

Niech $\mathfrak{A}$, $\mathfrak{B}$ będą algebrami. Odwzorowanie $\phi : \mathfrak{A} \to \mathfrak{B}$ nazywa się *homomorfizmem* gdy jest liniowe i zachowuje mnożenie, to znaczy

(1) $\phi(\lambda A) = \lambda\phi(A)$;

(2) $\phi(A + B) = \phi(A) + \phi(B)$;

(3) $\phi(AB) = \phi(A)\phi(B)$.

Jeśli ϕ jest homomorfizmem i P jest idempotentem, to $\phi(P)$ jest idempotentem.

Homomorfizm $\mathfrak{A}$ w $L(\mathcal{V})$ jest nazywany *reprezentacją* $\mathfrak{A}$ *na* $\mathcal{V}$.

Jeśli $\mathfrak{A}, \mathfrak{B}$ są algebrami unitalnymi i $\phi : \mathfrak{A} \to \mathfrak{B}$ jest homomorfizmem, mówimy, że ϕ jest *unitalny* gdy

$$\phi(\mathbb{1}_{\mathfrak{A}}) = \mathbb{1}_{\mathfrak{B}}.$$

7.7 Lewa regularna reprezentacja

Regularna reprezentacja

$$\mathfrak{A} \ni A \mapsto \lambda(A) \in L(\mathfrak{A})$$

jest zdefiniowana przez

$$\lambda(A)B := AB, \quad A, B \in \mathfrak{A}.$$

Jeśli $\mathfrak{A}$ jest unitalna, to λ jest injektywna. Jeśli $\mathfrak{A}$ nie jest unitalna, to λ może być rozszerzona do reprezentacji

$$\mathfrak{A} \ni A \mapsto \lambda_{\mathbf{1}}(A) \in L(\mathfrak{A}_{\mathbf{1}})$$

w oczywisty sposób. $\lambda_{\mathbf{1}}$ jest injektywna.

W obu przypadkach widzimy, że każda algebra jest izomorficzna z konkretną algebrą.

7.8 Ideały

$\mathfrak{B}$ jest *lewym ideałem* algebry $\mathfrak{A}$ jeśli jest liniową podprzestrzenią w $\mathfrak{A}$ i $A \in \mathfrak{A}$, $B \in \mathfrak{B} \Rightarrow AB \in \mathfrak{B}$. Podobnie definiujemy prawy ideał.

Jeśli $A \in \mathfrak{A}$, to $\mathfrak{A}A$ jest lewym ideałem

$\mathfrak{B}$ nazywa się *ideałem dwustronnym*, lub po prostu *ideałem*, gdy jest lewym i prawym ideałem.

Mówimy, że ideał $\mathfrak{I}$ jest *właściwy* gdy $\mathfrak{I} \neq \mathfrak{A}$. Mówimy, że ideał $\mathfrak{I}$ jest *nietrywialny* gdy $\mathfrak{I} \neq \mathfrak{A}$ i $\mathfrak{I} \neq \{0\}$.

Twierdzenie 7.1 *Jądro homomorfizmu jest ideałem. Jeśli $\mathfrak{I}$ jest ideałem w $\mathfrak{A}$, to $\mathfrak{A}/\mathfrak{I}$ ma naturalną strukturę algebry. Odwzorowanie*

$$\mathfrak{A} \ni A \mapsto A + \mathfrak{I} \in \mathfrak{A}/\mathfrak{I}$$

jest homomorfizmem, którego jądro jest równe $\mathfrak{I}$.

7.9 Przykłady podalgebr w $L(\mathbb{K}^n)$

(1) Algebra górnotrójkątna.

(2) Algebra nil-górnotrójkątna.

(3) Algebra blokowa $L(\mathbb{K}^{p_1}) \oplus \cdots \oplus L(\mathbb{K}^{p_k})$, $n = p_1 + \cdots p_k$.

(4) Algebra $L(\mathbb{K}^p) \otimes \mathbb{1}$, $n = pq$.

(5) Lewa regularna reprezentacja $L(\mathbb{K}^{d_1}) \oplus \cdots \oplus L(\mathbb{K}^{d_k})$ działa w $L(\mathbb{K}^n)$ dla $n = d_1^2 + \cdots d_k^2$.

7.10 $*$-algebry

Załóżmy, że $\mathbb{K}$ jest $\mathbb{R}$ lub $\mathbb{C}$.

Definicja 7.2 *Mówimy, że algebra $\mathfrak{A}$ jest* $*$-algebrą *gdy jest wyposażona w antyliniowe odwzorowanie $\mathfrak{A} \ni A \mapsto A^* \in \mathfrak{A}$ takie, że $(AB)^* = B^*A^*$, $A^{**} = A$ i $A \neq 0$ implikuje $A^*A \neq 0$. $*$ nazywa się* inwolucją.

Mówimy, że ideał $\mathfrak{I}$ jest $*$-ideałem, *gdy jest $*$-niezmienniczy.*

Niech $\mathcal{V}$ będzie przestrzenią Hilberta. Zbiór operatorów ograniczonych na $\mathcal{V}$, oznaczany $B(\mathcal{V})$ ze sprzężeniem hermitowskim tworzy $*$-algebrę. Każda podalgebra w $B(\mathcal{V})$ niezmiennicza względem $*$ jest też $*$-algebrą.

Definicja 7.3 *$*$-Algebry takie są zwane* konkretnymi $*$-algebrami.

Definicja 7.4 *Jeśli $\mathfrak{A}$, $\mathfrak{B}$ są $*$-algebrami, to homomorfizm $\pi : \mathfrak{A} \to \mathfrak{B}$ spełniający $\pi(A^*) = \pi(A)^*$ nazywa się* $*$-homomorfizmem. *(Również definiujem* $*$-isomorfizmy, $*$-automorfizmy,*, etc.)*

Twierdzenie 7.5 *Każda skończenie wymiarowa zespolona $*$-algebra $\mathfrak{N}$ jest $*$-izomorficzna z*

$$\overset{k}{\underset{i=1}{\oplus}} L(\mathbb{C}^{p_i}).$$

W szczególności, $\mathfrak{N}$ posiada jedynkę.

Zdefiniujmy $\dim(\mathfrak{N}) = [p_1, \dots, p_k]$. $\mathfrak{N}$ jest przemienna jeśli p_i są równe 1 lub 0.

Niech P_i będzie rzutem na $L(\mathbb{C}^{p_i}$. Centrum algebry $\mathfrak{N}$ składa się z elementów postaci

$$\sum_i c_i P_i, \quad c_i \in \mathbb{C}.$$

P_i są nazywane *minimalnymi rzutami centralnymi.*

7.11 Reprezentacje skończenie wymiarowych $*$-algebr

Lemat 7.6 *Niech $\phi : L(\mathbb{C}^p) \to L(\mathbb{C}^n)$ będzie unitalnym $*$- homomorfizmem. Wtedy $n = qp$, $q \in \mathbb{N}$, i ϕ jest unitarnie równoważny homomorfizmowi*

$$L(\mathbb{C}^p) \ni A \mapsto A \otimes \mathbb{1}_q \in L(\mathbb{C}^p \otimes \mathbb{C}^q).$$

Dowód. Niech $e_1, \dots, e_p$ będzie bazą w $\mathbb{C}^p$ a $e^1, \dots, e^p$ bazą dualną. $L(\mathbb{C}^p)$ jest rozpięta przez operatory $|e_i\rangle\langle e_j|$. Niech $f_{11}, \dots, f_{1q}$ będzie bazą w $\mathrm{Ran}\phi\left(|e_1\rangle\langle e^1|\right)$. Niech $f_{ij} := \phi\left(|e_i\rangle\langle e^1|\right) f_{1j}$. Sprawdzamy, że f_{ij} stanowią bazę. Jeśli f^{ij} jest bazą dualną, to

$$\phi\left(|e_i\rangle\langle e^j|\right) = \sum_{j=1}^{q} |f_{ik}\rangle\langle f^{jk}|.$$

Twierdzenie 7.7 *Każda unitalna reprezentacja algebry* $\overset{k}{\underset{i=1}{\oplus}} L(\mathbb{C}^{p_i})$ *na* $\mathbb{C}^n$ *jest unitarnie równoważna reprezentacji w* $\oplus_{i=1}^k \mathbb{C}^{p_i} \otimes \mathbb{C}^{q_i}$

$$\phi(A_1, \ldots, A_k) := \oplus_{i=1}^k A_i \otimes \mathbb{1}_{q_i}.$$

Mamy $n = \sum_{i=1}^k p_i q_i$ *oraz* $q_i = \frac{1}{p_i} \mathrm{Tr}\phi(P_i)$.

Dla reprezentacji regularnej mamy $p_i = q_i$. W szczególności, w tym wypadku

$$n = \sum_i p_i^2.$$

7.12 $*$-homomorfizmy skończenie wymiarowych $*$-algebr

Niech $\mathfrak{N}$, $\mathfrak{M}$ będą skończenie wymiarowymi $*$-algebrami. Niech $P_1, \ldots$, $Q_1, \ldots$ będą minimalnymi rzutami centralnymi $\mathfrak{N}$ i odpowiednio $\mathfrak{M}$.

Każdy homomorfizm $\alpha : \mathfrak{N} \to \mathfrak{M}$, gdzie $\dim \mathfrak{N} = [n_1, \ldots, n_p]$, $\dim \mathfrak{M} = [m_1, \ldots, m_q]$, określony jest przez macierz $[t_{ij}]$, gdzie $i = 1, \ldots, q,\ j = 1, \ldots, p$ i

$$\sum_j t_{ij} n_j \le m_i.$$

Mamy $=$ zamiast $\le$ jeśli α jest unitalna. Będziemy pisać $\mathrm{Diag}(\alpha) = [t_{ij}]$. Mamy $t_{ij} = \mathrm{Tr} Q_i \phi(P_j)$.

8 Algebra grupowa

8.1 Algebra grupowa

Niech G będzie skończoną grupą. Przez $C(G)$ będziemy oznaczali zbiór funkcji zespolonych na G. Jest on rozpięty przez funkcje δ_g, $g \in G$,

$$\delta_g(h) := \begin{cases} 1, & g = h, \\ 0, & g \neq h. \end{cases}$$

$C(G)$ jest wyposażone w dwa łączne iloczyny: mnożenie punktowe i splot:

$$\begin{aligned} FG(g) &:= F(g)G(g), \\ FG(g) &:= \sum_h F(gh^{-1})G(h). \end{aligned}$$

Mamy również inwolucję

$$F^*(g) := \overline{F(g^{-1})}. \tag{8.26}$$

Twierdzenie 8.1 $C(G)$ *ze splotem i sprzężeniem (8.26) jest* $*$*-algebrą.*

Dowód. Niech $F \in C(G)$ będzie różne od zera. Liczymy

$$F^* * F(g) = \sum_{h \in G} \overline{F(hg^{-1})} F(h).$$

W szczególności,

$$F^* * F(e) = \sum_{h \in G} = |F(h)|^2 \neq 0.$$

□

Mamy naturalne zanurzenie $G \in g \mapsto \delta_g \in C(G)$, przy czym mnożenie przechodzi na splot:

$$\delta_g * \delta_h \quad := \quad \delta_{gh}.$$

Niech π będzie reprezentacją G na $\mathcal{V}$. Wtedy $\tilde{\pi}(\delta_g) := \pi(g)$ rozszerza się przez liniowość do reprezentacji algebry splotowej $C(G)$ na $\mathcal{V}$. Jeśli reprezentacja jest unitarna, to $\tilde{\pi}$ jest $*$-reprezentacją.

W przyszłości będziemy po prostu pisać π zamiast $\tilde{\pi}$.

8.2 Postać algebry splotowej

Zdefiniujmy odwzorowanie liniowe

$$\phi : C(G) \to \bigoplus_{\pi \in \hat{G}} L(\mathcal{V}_\pi) \subset L\left(\bigoplus_{\pi \in \hat{G}} \mathcal{V}_\pi\right)$$

przez

$$\begin{aligned} \phi(\delta_g) \quad &:= \quad \bigoplus_{\pi \in \hat{G}} \pi(g) \\ &= \quad \bigoplus_{\pi \in \hat{G}} \sum_{i,j=1}^{d_\pi} \pi_{ij}(g) |e_{\pi,i})(e_{\pi,j}| \end{aligned}$$

Twierdzenie 8.2 *ϕ jest $*$-izomorfizmem.*

Dowód. Oczywiste jest, że $|e_{\pi,i})(e_{\pi,j}|$, $i,j = 1,\ldots,d_\pi$, $\pi \in \hat{G}$ rozpina $L\left(\bigoplus_{\pi \in \hat{G}} \mathcal{V}_\pi\right)$. Ale $\phi^{-1}\left(|e_{\pi,i})(e_{\pi,j}|\right)(g) = \pi_{ij}(g)$, której jak pokazaliśmy, stanowią bazę $l^2(G)$. □

Niech $\mathbb{1}_\pi$ oznacza rzut na $\mathcal{V}_\pi$. Niech

$$C_{\mathrm{cent}}(G) := \{F \in C(G) \ : \ F(ghg^{-1}) = F(h), \quad h, g \in G\}$$

Innymi słowy, $C_{\mathrm{cent}}(G)$ składa się z funkcji stałych na klasach sprzężoności grupy G.

Twierdzenie 8.3 *$C_{\mathrm{cent}}(G)$ jest centrum algebry splotowej $C(G)$. Jest rozpięte przez $\phi^{-1}(\mathbb{1}_\pi)$, $\pi \in \hat{G}$. Mamy*

$$\mathbb{1}_\pi \quad = \quad \phi\left(\frac{\#G}{d_\pi}\sum_{g\in G}\overline{\chi_\pi(g)}\delta_g\right).$$

Rozważmy lewą reprezentację regularną λ grupy G na $l^2(G)$. Rozszerza się ona do reprezentacji $\lambda : C(G) \to L(l^2(G))$.

Twierdzenie 8.4 *Z lewej F, F' są traktowane jako elementy $l^2(G)$, z prawej, jako elementy algebry $C(G)$:*

$$(F|F') \quad = \quad \sum_{\pi\in\hat{G}} d_\pi \mathrm{Tr}\pi(F)^*\pi(F') = \mathrm{Tr}\lambda(F)^*\lambda(F').$$