Algebraiczne metody fizyki teoretycznej

Zadania zaliczeniowe

Paweł Laskoś-Grabowski

24 stycznia 2009

Zadanie 1

1. Niech $m = m_1 m_2, m_{1,2} \in \mathbb{N}$ oraz $(m_1, m_2) = 1$. Udowodnić istnienie izomorfizmu pierścieni
$$\mathbb{Z}_m \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}$$
2. Definiujemy $\mathbb{Z}_m^*$ — zbiór elementów odwracalnych względem mnożenia w $\mathbb{Z}_m$.
   (a) Pokazać, że zbiór ten tworzy grupę względem mnożenia.
   (b) Pokazać, że $\#\mathbb{Z}_m^* = \varphi(m)$
   (c) Korzystając z odpowiednich twierdzeń teorii grup udowodnić twierdzenie Eulera: $(x, m) = 1 \Rightarrow x^{\varphi(m)} \equiv 1 \mod m$.

Rozwiązanie

1. $f : \mathbb{Z}_m \to \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} : k \mapsto (k \mod m_1, k \mod m_2)$ ma funkcję odwrotną daną wzorem
$$f^{-1}(k, l) = k a_2 m_2 + l a_1 m_1$$
gdzie $a_1 m_1 + a_2 m_2 = 1$, zaś współczynniki rozkładu $a_{1,2} \in \mathbb{Z}$ są dane jednoznacznie na mocy względnej pierwszości $m_{1,2}$. Rzeczywiście, mamy
$$\begin{aligned} f \circ f^{-1}(k, l) &= f(k a_2 m_2 + l a_1 m_1) \\ &= (k a_2 m_2 + l a_1 m_1 \mod m_1, k a_2 m_2 + l a_1 m_1 \mod m_2) \\ &= (k(1 - a_1 m_1) \mod m_1, l(a_2 m_2) \mod m_2) = (k, l) \end{aligned}$$
Tożsamości $f(0) = (0, 0), f(a + b) = f(a) + f(b), f(-a) = -f(a)$ wynikają wprost z zasady wykonywania działań po współrzędnych w sumie prostej oraz z własności arytmetyki modulo. Również $f(1) = (1, 1)$ — elementowi jednostkowemu w sumie prostej. Pozostaje do sprawdzenia zachowywanie mnożenia.
$$\begin{aligned} f^{-1}(k, l) \cdot f^{-1}(p, q) &= (k a_2 m_2 + l a_1 m_1)(p a_2 m_2 + q a_1 m_1) = kp a_2^2 m_2^2 + lq a_1^2 m_1^2 \\ &= f^{-1}(kp a_2 m_2, lq a_1 m_1) = f^{-1}(kp(1 - a_1 m_1), lq(1 - a_2 m_2)) \\ &= f^{-1}(kp, lq) \end{aligned}$$
W drugim przejściu opuszczone zostały wyrazy proporcjonalne do $m_1 m_2 = m$, bo obliczenie wykonywane jest w arytmetyce $\mod m$. W ostatnim — oba opuszczenia są dozwolone w odpowiedniej kongruencji.

2. (a) Z definicji do $\mathbb{Z}_m^*$ należy $1 = 1^{-1}$ oraz elementy odwrotne. $a^{-1}b^{-1}(ba) = 1$, stąd iloczyn ba elementów odwracalnych jest odwracalny.
   (b) Zauważmy, że dla m pierwszych $\mathbb{Z}_m$ jest ciałem, stąd $\#\mathbb{Z}_m^* = m - 1$. Z kolei na mocy izomorfizmu rozważanego wyżej $\#\mathbb{Z}_{m_1 m_2}^* = \#\mathbb{Z}_{m_1}^* \cdot \#\mathbb{Z}_{m_2}^*$ dla względnie pierwszych $m_{1,2}$ (bo jedyne dzielniki zera w sumie prostej to te elementy, które mają dzielnik zera na którejś ze współrzędnych; elementy grupy multiplikatywnej muszą mieć zatem na obu współrzędnych elementy odpowiednich grup multiplikatywnych). Jest to jednocześnie rekurencyjna definicja funkcji Eulera, więc obie te funkcje są sobie równe.
   (c) $(x, m) = 1 \Rightarrow x \in \mathbb{Z}_m^*$, czyli jego rząd (multiplikatywny) jest podzielny przez rząd $\mathbb{Z}_m^*$ wynoszący $\varphi(m)$. W grupie (a więc $\mod m$) mamy zatem $x^{\varphi(m)} = x^{c \cdot ord(x)} = 1^c = 1$.

Zadanie 2

Definiujemy zbiór przekształceń działających na $\mathbb{C}$:

$$\left\{ \sigma \equiv \sigma(a, b, c, d) : \sigma(z) = \frac{az + b}{cz + d}, a, b, c, d \in \mathbb{C}, ad - bc \neq 0 \right\}$$

1. Pokazać, że nie każde σ odwzorowuje $\mathbb{C}$ na siebie.
2. Aby ominąć ten problem, definiujemy rozszerzenie $\overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ oraz działanie σ na $\overline{\mathbb{C}}$:
   (a) $c = 0 \Rightarrow \sigma(z) = \frac{az+b}{cz+d}$ na $\mathbb{C}$ oraz $\sigma(\infty) = \infty$
   (b) $c \neq 0 \Rightarrow \sigma(z) = \frac{az+b}{cz+d}$ na $\mathbb{C} \backslash \{-\frac{d}{c}\}$ oraz $\sigma(-\frac{d}{c}) = \infty, \sigma(\infty) = \frac{a}{c}$

   pokazać, że zbiór tak określonych przekształceń $\overline{\mathbb{C}}$ tworzy grupę.
3. Udowodnić, że G jest obrazem homomorficznym grupy $SL(2, \mathbb{C})$. Wyznaczyć jądro homomorfizmu.

Rozwiązanie

1. Dla $\sigma(z) = \frac{1}{z}$ nie jest możliwe $\sigma(z) = 0$.
2. $id = \sigma(1, 0, 0, 1)$, a działanie (składanie) jest łączne, bo jest łączne w grupie wszystkich bijekcji $\overline{\mathbb{C}}$. By pokazać, że elementy odwrotne należą do zbioru, rozważymy dwa przypadki jak w definicji.

   Gdy $c = 0$, to $a, d \neq 0$. Wtedy $\sigma(z) = \frac{az+b}{d}$. $z = \frac{d\sigma(z)-b}{a}$, zatem $\sigma^{-1} = \sigma(d, -b, 0, a)$. Dookreślamy jeszcze $\sigma^{-1}(\infty) = \infty$ i zauważamy, że "$ad - bc$" $= ad + b \cdot 0 = ad \neq 0$.

Gdy $c \neq 0$, to przy założeniu $z \neq -\frac{d}{c}$ stwierdzamy, że

$$\sigma(z) = \frac{az+b}{cz+d} = \frac{1}{c}\frac{caz+bc+da-da}{cz+d} = \frac{1}{c}\left(a + \frac{bc-da}{cz+d}\right)$$

$$c\sigma(z) - a = \frac{bc-da}{cz+d} \tag{$*$}$$

$$cz+d = \frac{bc-da}{c\sigma(z)-a}$$

$$z = \frac{1}{c}\left(\frac{bc-da}{c\sigma(z)-a} - d\right) = \frac{1}{c}\frac{bc-da-dc\sigma(z)+da}{c\sigma(z)-a} = \frac{-d\sigma(z)+b}{c\sigma(z)-a}$$

a więc $\sigma^{-1} = \sigma(-d, b, c, -a)$. Z niezerowości prawej strony $(*)$ argumentem σ^{-1} nie może być $\frac{a}{c}$, więc kładziemy $\sigma^{-1}(\frac{a}{c}) = \infty$ oraz $\sigma^{-1}(\infty) = -\frac{d}{c}$. Ostatecznie "$ad - bc$" $= -d \cdot -a - bc \neq 0$, czyli znów otrzymaliśmy element zbioru.

Konieczne jest jeszcze spostrzeżenie, że składanie elementów zbioru jest działaniem wewnętrznym.

$$\begin{aligned}\sigma(a,b,c,d) \circ \sigma(a',b',c',d')(z) &= \frac{a\frac{a'z+b'}{c'z+d'}+b}{c\frac{a'z+b'}{c'z+d'}+d} = \frac{(aa'+bc')z+ab'+bd'}{(ca'+dc')z+cb'+dd'} \\ &= \sigma(aa'+bc', ab'+bd', ca'+dc', cb'+dd')(z) \\ 0 \neq (ad-bc)(a'd'-b'c') &= (aa'+bc')(cb'+dd') - (ab'+bd')(ca'+dc')\end{aligned}$$

Sprawdzenie dodatkowych warunków związanych z elementem ∞ wymaga prostego rozważenia kilku przypadków.

3. $\phi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \sigma(a,b,c,d)$. Własności ϕ jako homomorfizmu zostały właściwie pokazane wyżej; warto pamiętać, że $\sigma(\alpha a, \alpha b, \alpha c, \alpha d) = \sigma(a,b,c,d)$. Na podstawie równości funkcji

$$\frac{az+b}{cz+d} = z$$

$$az+b = cz^2+dz$$

$$c = b = 0, a = d$$

wnioskujemy, że jądro ϕ równe jest $(\mathbb{C}\backslash\{0\}) \cdot \mathbb{1}$.

Zadanie 3

Niech ϕ będzie macierzową reprezentacją wymiaru n grupy G. Definiujemy reprezentację $(\psi, M(n,\mathbb{C}))$ następująco:

$$\psi(g)(A) = \phi(g)A\phi^t(g)$$

Wyrazić charakter χ_ψ za pomocą χ_ϕ.

Rozwiązanie

Jeżeli zdefiniujemy bazę przestrzeni macierzy następująco

$$\{e_{ij} : (e_{ij})_{kl} = \delta_{ik}\delta_{jl}\}$$

to ślad operatora $\mathcal{O}$ działającego na tej przestrzeni będzie zdefiniowany nastepująco: $\operatorname{Tr}\mathcal{O} = \sum_{ij}(\mathcal{O}e_{ij})_{ij}$. Zatem w naszym przypadku mamy

$$\begin{aligned}
\chi_\psi(g) = \operatorname{Tr}\psi(g) &= \sum_{ij}(\psi(g)(e_{ij}))_{ij} = \sum_{ij}(\phi(g)e_{ij}\phi^t(g))_{ij} = \sum_{ij}\sum_{kl}\phi(g)_{ik}(e_{ij})_{kl}\phi^t(g)_{lj} \\
&= \sum_{ij}\sum_{kl}\phi(g)_{ik}\delta_{ik}\delta_{jl}\phi^t(g)_{lj} = \sum_{ij}\phi(g)_{ii}\phi^t(g)_{jj} = \sum_i \phi(g)_{ii}\sum_j \phi(g)_{jj} \\
&= (\operatorname{Tr}\phi(g))^2 = \chi^2_\phi(g)
\end{aligned}$$

Zadanie 5

Ile wynosi „średnia wartość” $\frac{1}{|G|}\sum_{g\in G}\chi(g)$ charakteru nietrywialnej reprezentacji grupy skończonej G?

Rozwiązanie

Wystarczy zauważyć, że

$$\frac{1}{|G|}\sum_{g\in G}\chi(g) = \frac{1}{|G|}\sum_{g\in G}\chi(g)\tilde{\chi}^*(g) = (\chi, \tilde{\chi})$$

gdzie $\tilde{\chi}(g) = 1$ jest charakterem reprezentacji trywialnej. Zatem liczba ta jest krotnością występowania reprezentacji trywialnej w rozważanej.

Zadanie 7

Załóżmy, że $X \in \mathfrak{gl}(n, \mathbb{C})$ ma n różnych wartości własnych. Wyznaczyć wartości własne $\operatorname{ad} X$.

Rozwiązanie

Skoro macierz wymiaru n ma n wartości własnych, to ma bazę wektorów własnych, w której jest diagonalna. Rozważmy działanie $\operatorname{ad} X$ na macierz Y w tej właśnie bazie.

$$\begin{aligned}
((\operatorname{ad} X)Y)_{ij} = (XY - YX)_{ij} &= \sum_k (X_{ik}Y_{kj} - Y_{ik}X_{kj}) = \sum_k (\lambda_i\delta_{ik}Y_{kj} - Y_{ik}\lambda_k\delta_{kj}) \\
&= \lambda_i Y_{ij} - \lambda_j Y_{ij} = (\lambda_i - \lambda_j)Y_{ij}
\end{aligned}$$

Widać zatem, że wszystkie n^2 macierzy bazowych e_{ij} (p. zad. 3) to wektory własne $\operatorname{ad} X$ (z wartościami własnymi $\lambda_i - \lambda_j$). Zatem nie ma więcej wartości własnych. Dokładny rozkład na podprzestrzenie własne jest już zależny od spektrum λ_i, ale w każdym przypadku macierze e_{ii} bedą stowarzyszone z wartościami własnymi 0. Odpowiada to oczywistemu faktowi, że macierze diagonalne komutują z dowolnym X.

Zadanie 9

Niech L będzie algebrą Liego. Definiujemy

$$Der\, L = \{f \in End(L) : f[x, y] = [f(x), y] + [x, f(y)] \quad \forall\, x, y \in L\}$$

1. Pokazać, że komutator (w $\mathfrak{gl}(L)$) dwóch derywacji jest derywacją i wobec tego $Der\, L$ jest podalgebrą Liego $\mathfrak{gl}(L)$.
2. Udowodnić, że zbiór wewnętrznych derywacji L postaci $\operatorname{ad} x, x \in L$ jest ideałem w $Der\, L$.

Rozwiązanie

1. Nawias Liego jest działaniem wewnętrznym w $Der\, L$:

$$\begin{aligned}
[f,g][x,y] =& fg[x,y] - gf[x,y] = f[g(x),y] + f[x,g(y)] - g[f(x),y] - g[x,f(y)] \\
=& [fg(x),y] + [g(x),f(y)] + [f(x),g(y)] + [x,fg(y)] \\
&- [gf(x),y] - [f(x),g(y)] - [g(x),f(y)] - [x,gf(y)] \\
=& [[f,g](x),y] + [x,[f,g](y)]
\end{aligned}$$

2. $\{\operatorname{ad} x\}$ jest ideałem w $Der\, L \Leftrightarrow [Der\, L, \{\operatorname{ad} x\}] \subseteq \{\operatorname{ad} x\}$:

$$[f, \operatorname{ad} x](y) = f[x,y] - (\operatorname{ad} x)(f(y)) = [f(x),y] + [x,f(y)] - [x,f(y)] = (\operatorname{ad} f(x))(y)$$