Wykład 1

W. Hebisch

26 lutego 2023

1 Wrowadzenie

Grupy pojawiły się w matematyce jako symetrie różnych obiektów. Od początku prowadziło to do badania działania grup na różnych strukturach matematycznych. My będziemy się zajmować działniami liniowymi, tzn. gdy elementy grupy działają jako odwzorowania liniowe na przestrzeni wektorowej nad ciałem czy ogólniej na modułach. W pierwszej części będziemy się zajmować głównie grupami skończonymi i ich działaniem na przestrzeniach wektorowych nad ciałem. Wyniki przyjmują najprostszą postać na ciałem liczb zespolonych czy ogólniej nad ciałem algebraicznie domkniętym charakterystyki 0. Ale teorię łatwo można uogólnić na znacznie większą klasę ciał. Pierwsza część używa metody czysto algebraiczne.

W drugiej części będziemy się zajmować grupami nieskończonymi. Tutaj ograniczymy się głównie do reprezentacji unitarnych (w przeciwnym wypadku teoria byłby zbyt skomplikowana). Tu będą potrzebne przestrzeni Hilberta i operatory na przestrzeniach Hilberta, w szczególności przestrzeni L^2.

2 Podstawowe definicje

2.1 Definicja reprezentacji

Niech R będzie pierścieniem przemiennym z jedynką zaś V modułem nad R. Przez $\mathrm{GL}(V)$ oznaczymy grupę odwracalnych endomorfizmów V.

Definicja. Reprezentacją grupy G na V nazywamy homomorfizm $\rho : G \to \mathrm{GL}(V)$

Komentarz. Na wstępnych wykładach często rozważa się tylko przypadek gdy pierścień R to ciało liczb zespolonych. Ale ogólniejsza teoria nie jest trudniejsza (można argumentować że jest łatwiejsza bo pozbywamy się zbędnych założeń), a pozwala pokazać zjawiska które się nie pojawią dla ciała liczb zespolonych i stosuje się do większej liczby problemów.

Przykłady.

1. Niech $R = \mathbb{R}$ będzie ciałem liczb rzeczywstych, G bedzie grupą izometrii płaszczyzny przeprowadzających zbiór $A = \{(1,0),(0,1),(-1,0),(0,-1)\}$ na siebie. Łatwo zauważyć że taka izometria musi przeprowadzać średnią A na siebie.

Ale średnia A to $(0,0)$, czyli takie izometrie zachowują początek układu współrzednych. Stąd wynika że G jest podzbiorem $\mathrm{GL}(\mathbb{R}^2)$. A więc odwzorowanie włożenienia z G w $\mathrm{GL}(\mathbb{R}^2)$ daje nam reprezentację G na $V = \mathbb{R}^2$.

2. Ogólniej, izometrie ustalonej figury geometrycznej tworzą grupę (zwykle skończoną). Izometrię $V = \mathbb{R}^n$ można zapisać jako sumę elementu $\mathrm{GL}(V)$ i przesunięcia. Zapominając o przesunięciu dostaniemy homomorfizm z G w $\mathrm{GL}(V)$, czyli reprezentację na V.

3. Niech R i G będą dowolne. Jako V przyjmujemy przestrzeń wszystkich funkcji na G o wartościach w R. V ma naturalną strukturę modułu nad G: dodawanie wykonujemy dodając wartości w punktach. Podobnie mnożenie przez element z R wykonujemy mnożąc wartości w punktach. Dla ustalonego $g \in G$ definujemy odwzorowanie $\rho(g) : V \to V$ wzorem:

$$(\rho(g)f)(x) = f(g^{-1}x).$$

Łatwo zauważyć że $\rho(g)$ jest dobrze zdefiniowane, tzn. dla $f \in V$ wzór definiuje element V. Ponadto to odwzorowanie spełnia $\rho(g)(f_1 + f_2) = \rho(g)f_1 + \rho(g)f_2$ i dla $r \in R$ mamy $\rho(g)(rf) = r\rho(g)f$, czyli $\rho(g)$ jest endomorfizmem V. Następnie dla $g_1, g_2 \in G$ mamy

$$\begin{aligned}\rho(g_1)(\rho(g_2)f)(x) = (\rho(g_2)f)(g_1^{-1}x) = f(g_2^{-1}g_1^{-1}x)\\ = f((g_1g_2)^{-1}x) = (\rho(g_1g_2)f)(x).\end{aligned}$$

A więc $\rho(g_1)\rho(g_2) = \rho(g_1g_2)$ czyli ρ daje homomorfizm z G w endomorfizmy G. Łatwo zauważyć że jedynka grupy G przechodzi na endomorfim identycznościowy V. A więc $\rho(g^{-1})$ jest odwrotnością $\rho(g)$, czyli ρ przyjmuje wartości w $\mathrm{GL}(V)$, czyli daje reprezentację G na V.

4) Jeśli dla każdego elementu G wartość $\rho(g)$ zdefiniujemy jako identyczność na V to otrzymamy reprezentację G na V. Tą reprezentację nazywamy reprezentacją *trywialną*.

Jeśli mamy zadane reprezentacje ρ_i, $i = 1, 2$ grupy G na modułach V_i, $i = 1, 2$ to możemy utwożyć sumę prostą $V = V_1 \oplus V_2$ i zdefiniować reprezentację ρ na V wzorem

$$\rho(g)(v_1, v_2) = (\rho_1(g)v_1, \rho_2(g)v_2).$$

Tą reprezentację nazywamy sumą prostą ρ_1 i ρ_2 i oznaczamy przez $\rho_1 \oplus \rho_2$.

Jeśli W jest podmodułem V niezmienniczym na działanie wszystkich $\rho(g)$, to możemy zdefiniować reprezentację η grupy G na W wzorem

$$\eta(g) = \rho(g)|_W.$$

gdzie $|_W$ oznacza obcięcie operatora do W. Mówimy że reprezentacja η jest podreprezentacją ρ.

Przykład.

5) Niech V będzie modułem z przykładu 3. Jako W przyjmiemy zbiór funkcji które są różne od zera tylko w skończenie wielu punktach. Łatwo zauważyć że W jest podmodułem V i że W jest niezmienniczy na działanie G. Obcięcie ρ do W daje nam reprezentację λ którą nazywamy *reprezentacją regularną* G.

Jeśli mamy zadane reprezentacje ρ_i, $i = 1, 2$ grupy G na modułach V_i, $i = 1, 2$ izomorfizm $h : V_1 \to V_2$ spełniający

$$h(\rho_1(g)) = \rho_2(h(g))$$

to mówimy że V_1 jest *równoważne* V_2. Często nie ma potrzeby rozróżniania równoważnych reprezentacji.

Można by w podobny sposób definiować wiecej pojęć, ale dalej będziemy używać nieco ogólniejszej terminologii modułów.

2.2 Pierścień grupowy

Moduł W z przykładu 5 ma bogatsze własności: ma naturalną strukturę pierścienia. Mianowicie niech δ_g będzie funkcję na G która przyjmuje w punkcie g wartość 1 a w pozostałych punktach wartość 0. Wtedy definiujemy

$$\delta_{g_1}\delta_{g_2} = \delta_{g_1 g_2}.$$

Łatwo zauważyć W jest modułem wolnym z bazą $\{\delta_g : g \in G\}$:

$$f(x) = \sum f(g)\delta_g(x)$$

gdzie suma jest skończona bo tylko dla skończenie wielu g mamy $f(g) \neq 0$. To pozwala zdefiniować mnożenie rozszerzając podany wyżej wzór dla δ_g. Mianowicie, niech

$$f_1 = \sum_g a_g \delta_g,$$
$$f_2 = \sum_h b_h \delta_h.$$

Wtedy produkt $f_1 f_2$ definujemy wzorem

$$f_1 f_2 = \sum_{gh} a_g b_h \delta_{gh} = \sum_s \left(\sum_{gh=s} a_g b_h \right) \delta_s$$

to znaczy linowo rozszerzamy mnożenie z bazy na całe W. Mamy

$$\sum_{gh=s} a_g b_h = \sum_g a_g b_{g^{-1}s},$$

czyli wzór na mnożenie można zapisać w postaci

$$f_1 f_2 = \sum_s \left(\sum_g a_g b_{g^{-1}s} \right) \delta_s.$$

Dla $f_1 = \delta_g$ daje to

$$\delta_g f_2 = \sum_s b_{g^{-1}s} \delta_s,$$

czyli

$$(\delta_g f_2)(x) = b_{g^{-1}x}$$

Ale $b_h = f_2(h)$ czyli mamy

$$(\delta_g f_2)(x) = f_2(g^{-1}x) = (\rho(g)f_2)(x).$$

Czyli $\rho(g)$ to operator mnożenia przez δ_g.

Jako że mnożenie wprowadziliśmy jako liniowe rozszerzenie mnożenia z bazy W to łatwo spradzić że jest on rozdzielne względem dodawania:

$$f_1(f_2 + f_3) = f_1 f_2 + f_1 f_3,$$
$$(f_1 + f_2)f_3 = f_1 f_3 + f_2 f_3.$$

Ponadto mnożenie jest łączne:

$$f_1(f_2 f_3) = (f_1 f_2)f_3.$$

Widać też że δ_e gdzie e jest elementem neutralnym w G jest jedynką dla naszego mnożenia:

$$\delta_e f = f\delta_e = f.$$

A więc moduł W z mnożeniem wprowadzonym wyżej mnożeniem faktycznie jest pierścieniem. Nazywamy go *pierścieniem grupowym* G i oznaczamy przez $R[G]$.

Definicja. Niech R będzie pierścieniem (niekoniecznie przemiennym) zaś M jest grupą abelową. Mówimy że M jest (lewym) modułem nad R jeśli zadane jest mnożenie elementów $m \in M$ przez elementy $r \in R$ spełniające następujące warunki:

$$r_1(r_2 m) = (r_1 r_2)m,$$
$$(r_1 + r_2)m = r_1 m + r_2 m,$$
$$r(m_1 + m_2) = rm_1 + rm_2,$$

Jeśli R jest pierścieniem z jedynką to dodatkowo żądamy by $1m = m$.

Zauważmy że jeśli pierścień R_1 jest podpierścieniem pierścienia R_2 to moduł M nad R_2 można potraktować jako moduł nad R_1, po prostu mnożąc tylko przez elementy z R_1. Nieco ogólniej mając homomorfizm h z R_1 w R_2 można zdefiniować mnożenie przez elementy $r \in R_1$ wzorem

$$rm = h(r)m$$

Zauważmy że każdą grupę abelową można potraktować jako moduł na liczbami całkowitymi $\mathbb{Z}$ definiując mnożenie przez liczbę całkowitą dodatnią za pomocą dodawania, zaś mnożenie przez -1 jako branie elementu odwrotnego. Z drugiej strony, dla dowolnego pierścienia z jedynką R istnieje dokładnie jeden homomorfizm z $\mathbb{Z}$ w R co na modułach nad R daje stukturę modułu nad $\mathbb{Z}$. Łatwo sprawdzić że mnożenie przez elementy $\mathbb{Z}$ otrzymane w ten sposób jest identyczne z mnożeniem pochodzącym ze struktury grupy abelowej.

Uwaga. Niech M będzie grupą abelową i dla r z pierścienia R są zadane odwzorowania $\rho(r)$ które są endomorfizmami M i spełniają równości

$$\rho(r_1)\rho(r_2)m = \rho(r_1 r_2)m,$$
$$\rho(r_1)m + \rho(r_2)m = \rho(r_1 + r_2)m$$

Wtedy wzór $rm = \rho(r)m$ zadaje ma M strukturę modułu nad R. Odwrotnie, jeśli M jest modułem nad R zaś ρ jest zadane wzorem $\rho(r)m = rm$, to ρ spełnia wzory wyżej (czyli jest homomofizmem z R w endomofizmy M). Porównując to z definicją reprezentacji grupy można by mówić o reprezentacji pierścienia.

Uwaga. Analogicznie do lewgo modułu można by zdefiniować prawy moduł, pisząc w definicji elementy R z prawej strony. Dla pierścieni przemiennych daje to niewiele nowego, ale jeśli R nie jest przemienny to różnica może być istotna.

Definicja. Jeśli M_i, $i = 1, 2$ są modułami nad R i h jest odwzorowaniem z M_1 w M_2 to mówimy że h jest homomorfizmem jeśli h jest homomorfizmem M_1 w M_2 traktowanymi jako grupy abelowe i dla każdego $m \in M_1$ i każdego $r \in R$ zachodzi równość $h(rm) = rh(m)$.

Jeśli $M_1 = M_2$ i h jest homomorfizm z M_1 w M_2 to mówimy że h jest endomorfizmem. Jeśli h jest homomorfizm i ma odwrotność która też jest homomorfizmem to mówimy że h jest izomorfizmem.

Lemat 2.1 *Niech V będzie lewym modułem nad pierścieniem grupowym $R[G]$. wtedy wzór*

$$\rho(g)m = \delta_g m$$

zadaje reprezentację na V traktowanym jako moduł nad R.

Odwrotnie, jeśli dany jest moduł V nad R i reprezentacja ρ grupy G na V, to na V można wprowadzić dokładnie jedną strukturę $R[G]$ modułu taką że ρ jest dane wzorem wyżej.

Dowód. Na mocy definicji modułu $\rho(g)$ przeprowadza sumy na sumy, czyli jest endomorfizmen grupy abelowej. R jest podpierścieniem $R[G]$ i dla $r \in R$ mamy $\delta_g rm = r\delta_g m$, a więc $\rho(g)$ jest endomorfizmem V traktowanego jako moduł nad R.

Mnożenie w $R[G]$ jest łączne, więc mamy

$$\rho(g_1)(\rho(g_2)m) = \delta_{g_1}(\delta_{g_2}m) = (\delta_{g_1}\delta_{g_2})m = \delta_{g_1 g_2}m = \rho(g_1 g_2)m$$

czyli ρ jest homomorfizem z G w endomorfizmy V traktowanego jako moduł nad R. δ_e jest jedynką w $R[G]$, więc zgodnie z naszą definicją δ_e przechodzi na operator identycznościowy I na V. Wzór $\rho(g^{-1})\rho(g) = I$ oznacza że $\rho(g) \in \mathrm{GL}(V)$, a więc ρ jest reprezentacją G na V traktowanym jak moduł nad R.

Gdy mamy zadaną reprezentację ρ grupy G na V to dla

$$f_1 = \sum_g a_g \delta_g$$

piszemy

$$f_1 m = \sum_g a_g \rho(g) m. \tag{1}$$

Dla

$$f_2 = \sum_h b_h \delta_h$$

mamy

$$f_1(f_2 m) = \sum_g a_g \rho(g) \left(\sum_h b_h \rho(h) m \right) = \sum_g a_g \sum_h b_h \rho(g)\rho(h) m =$$

$$\sum_g a_g \sum_h b_h \rho(gh) m = \sum_s \left(\sum_{gh=s} \right) \rho(s) m = (f_1 f_2) m$$

gdzie piewsza równość to użycie (1), druga zachodzi bo $\rho(h)$ jest endomorfizmem modułu, trzecia wynika z tego że ρ jest reprezentacją, czwarta to pogrupowanie wyrazów sumy, piąta używa wzór na mnożenie w $R[G]$ i (1). Równość $(f_1 + f_2)m = f_1 m + f_2 m$ łatwo wynika z przez rzopisanie obu stron używając (1). Równość $f_1(m_1 + m_2) = f_1 m_1 + f_1 m_2$ wynika z tego że dla każdego $g \in G$ odwzorowanie $\rho(g)$ spełnia $\rho(g)(m_1 + m_2) = \rho(g)m_1 + \rho(g)m_2$. A więc wzór (1) faktycznie zadaje na V strukturę modułu nad $R[G]$. Widać też że

$$\rho(g)m = \delta_g m$$

czyli wzór z pierwszej części lematu daje nam z powrotem reprezentację ρ. □

Każdy pierścień można potraktować jako lewy moduł nad samym sobą, po prostu licząc rm za pomocą mnożenia w pierścieniu. Traktując $R[G]$ jako lewy moduł nad sobą otrzymujemy moduł odpowiadający reprezentacji regularnej, tzn. reprezentacji z przykładu 5.

Definicja. Niech M będzie modułem nad R. Podgrupę abelową $N \subset M$ nazywamy podmodułem jeśli jest zamknięta na mnożenie przez elementy R.

Uwaga. Dla reprezentacji pokrywa się to z pojęciem podreprezentacji.

Przykład. Moduł V nad R z przykładu 3 ma podmoduł $W = R[G]$. Na mocy lematu V można potraktować jako moduł nad $R[G]$. Oczywiście W jest zamknięty na mnożenie przez elementy $R[G]$, więc jest podmodułem nad $R[G]$.

Definicja. Mówimy że moduł M nad R jest prosty jeśli nie ma nietrywialnych podmodułów, tzn. jedyne jego podmoduły to M i moduł zerowy ($\{0\}$).

Uwaga. Dla reprezentacji odpowiada to pojęciu reprezentacji nieprzywiedlnej.

Szukanie podmodułów $R[G]$ jest równoważnie szukaniu podmodułów nad R które są niezmiennicze na działanie G. Jeśli R jest ciałem jest to równoważne

szukaniu podprzestrzeni niezmienniczych. Popatrzmy teraz dokładnije na przykład 1. Twierdzimy że grupa z tego przykładu nie ma jednowymiarowych podprzestrzeni niezmienniczych. Grupa G zawiera odwzorowanie ϕ zadane wzorem $\phi((x,y)) = (-x,y)$ (tzn. odbicie względem osi y). ϕ ma dokładnie dwie podprzestrzenie niezmiennicze: $A = \{(0,y) : y \in \mathbb{R}\}$ i $B = \{(y,0) : y \in \mathbb{R}\}$. Ale G zawiera również odwzorowanie ψ zadane wzorem $\psi((x,y)) = (y,x)$. Widać że ani A ani B nie jest zachowane przez ψ, więc nie ma podprzestrzeni jednowymiarowych zachowywanych przez całe G. Podprzestrzeń dwuwymiarowa jest jedna, jest to całe $V = \mathbb{R}^2$. Podprzestrzeń zerowymiarowa to podprzestrzeń składająca się tylko z wektora zerowego. A więc V jako moduł nad $R[G]$ jest modułem prostym.

To czy działanie grupy prowadzi do modułu prostego zależy od pierścienia R. Rozważmy grupę obrotów płaszczyzny $\mathbb{R}^2$. Widać że nie ma jednowymiarowych podprzestrzeni niezmieniczych, każdą prostą przechodzącą przez $(0,0)$ można trochę obrócić dostając inną prostą. A więc jak przed chwilą odpowiedni moduł nad $R[G]$ jest prosty. Jednakże, pracując nad ciałem liczb zespolonych obroty to odwzorowania zadane macierzami postaci

$$\begin{bmatrix} \cos(t) & -\sin(t) \\ \sin(t) & \cos(t) \end{bmatrix}$$

i można je traktować jako odwzorowania $\mathbb{C}^2$. Wtedy $(1,i)$ jest wektorem własnym wszystkich odwzorowań wyżej (z wartością własną $\exp(-t)$), a więc rozpina jednowymiarową podprzestrzeń niezmienniczą. Czyli nad liczbami zespolonymi odpowiedni moduł *nie* jest prosty.

Przykład. Niech $G = \mathbb{Z}$ z dodawaniem. G jest generowane przez pojedynczy element, tzn. przez 1. Rozważmy reprezentację ρ grupy G na module V nad pierścieniem R. Niech $A = \rho(1)$. Reprezentacja jest jednoznacznie wyznaczona przez A i podmoduły niezmiennicze dla G to dokładnie podmoduły niezmiennicze dla A. Z drugiej strony, jeśli A jest odwracalnym endomorfizmem V to wzór $\rho(1) = A$ jednoznacznie zadaje reprezentację. A więc badanie podmodułów dla $R[G]$ jest równoważne badaniu podmodułów niezmienniczych dla odwracalnego A. W pełnej ogólności jest to trudne zadanie. Jeśli R jest ciałem algebraicznie domkniętym zaś V jest skończenie wyniarową przestrzenią wektorową nad R to twierdzenie o rozkładzie Jordana daje dokładny opis modułów nad $R[G]$: moduły proste to przestrzenie wymiaru 1, klatki Jordana dają moduły które nie są proste, ale nie daje się ich rozłożych na sumę prostę, cały moduł jest sumą prostą klatek. Ogólnej, gdy R jest ciałem zaś V jest skończenie wymiarową przestrzenią wektorową nad V moduły proste odpowiadają algebraicznym rozszerzeniom R generowanym przez pojedynczy element (równoważnie generowanym przez zero wielomianu nieprzywiedlnego), zamiast klatek Jordana rozpatruje się moduły cykliczne a cały moduł rozpada się na sumę prostą modułów cyklicznych.

Uwaga. Jest to przykład pokazujący możliwe komplikacje dla stosunkowo prostej grupy. W dalszym ciągu będziemy przyjmować założenia które pozwolą nam ograniczyć się do sumy prostej modułów prostych lub tak zwanej całki prostej (dla grup ciągłych).

Podam jeszcze mały słowniczek między terminologią modułów a reprezentacji:

Reprezentacje	Moduły
reprezentacja	moduł
podreprezentacja	podmoduł
suma prosta	suma prosta
reprezentacja nieprzywiedlna	moduł prosty
operator splatający	homomorfizm
równoważność	izomorfizm
reprezentacja regularna	$R[G]$ jako moduł nad sobą
reprezentacja trywialna	R jako moduł nad $R[G]$