Reprezentacje grup skończonych

W. Hebisch

14 czerwca 2024

Spis treści

1 Wprowadzenie

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 działaniami 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 przestrzenie 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 rzeczywistych, G będzie 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 współrzędnych. Stąd wynika że G jest podzbiorem $\mathrm{GL}(\mathbb{R}^2)$. A więc odwzorowanie włożenia 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 prze-

sunięcia. 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 $g \in G$ definiujemy 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 endomorfizm 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 utworzyć 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.

Powiemy że reprezentacja jest wierna jeśli jedyny element G który przechodzi na operator identycznościowy to jedynka G.

Można by w podobny sposób definiować więcej 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 $f_1 f_2$ definiujemy 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 sprawdzić 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 strukturę 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 homomorfizmem z R w endomorfizmy M). Porównując to z definicją reprezentacji grupy można by mówić o reprezentacji pierścienia.

Uwaga. Analogicznie do lewego 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 endomorfizmem 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 homomorfizmem 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 rozpisanie 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 dokładniej 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 niezmienniczych, 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 $\exp(-it)$), 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 wymiarową 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 rozłożyć na sumę prostą, 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 $R[G]$

3 Twierdzenie Maschkego

Lemat 3.1 *Niech G będzie grupą skończoną mocy n, V przestrzenią wektorową nad ciałem K charakterystyki nie dzielącej n zaś ρ reprezentacją G na V. Jeśli W jest podprzestrzenią niezmienniczą dla ρ to istnieje podprzestrzeń U niezmiennicza dla ρ taka że $U + W = V$, $U \cap W = \{0\}$.*

Uwaga: Oznacza to że ρ jest równoważne sumie prostej reprezentacji działających na U i W.

Dowód: Zauważmy najpierw że istnieje operator liniowy P z V w W spełniający $P(x) = x$ dla $x \in W$. Mianowicie, możemy wybrać bazę B przestrzeni V w ten sposób że najpierw wybieramy bazę A przestrzeni W a następnie uzupełniamy ją do bazy V. Czyli $A \subset B$. Dowolny element $v \in V$ można zapisać w postaci

$$v = \sum_{b \in B} c_b b.$$

Operator P definiujemy wzorem

$$P(v) = \sum_{b \in A} c_b b.$$

Oczywiście dla $v \in W$ mamy $P(v) = v$, bo $c_b = 0$ dla $b \notin A$. Z definicji P jest operatorem liniowym. Teraz definiujemy operator Q wzorem

$$Q = \frac{1}{n} \sum_{g \in G} \rho(g) P \rho(g^{-1}).$$

Mamy

$$\begin{aligned} \rho(h)Q = \frac{1}{n} \sum_{g \in G} \rho(h)\rho(g)P\rho(g^{-1}) = \frac{1}{n} \sum_{g \in G} \rho(hg)P\rho((hg)^{-1})\rho(h) \\ = \frac{1}{n} \sum_{g \in G} \rho(g)P\rho(g^{-1})\rho(h) = Q\rho(h). \end{aligned}$$

gdzie przedostatnia równość zachodzi bo hg przebiega przez wszystkie elementy G. Teraz niech U będzie jądrem Q, tzn. $U = \{v \in V : Q(v) = 0\}$. Jeśli $v \in U$ to

$$Q\rho(g)v = \rho(g)Qv = 0,$$

czyli $\rho(g)v \in U$. A więc U jest niezmiennicze na działanie v. Jako że $Q(v) = v$ dla $v \in W$ to $U \cap V = \{0\}$. Jako że $Qv \in W$ to $QQv = Qv$, czyli

$$Q(v - Qv) = Qv - QQv = Qv - Qv = 0$$

czyli $v - Qv \in U$. A więc biorąc $w = Qv \in W$ i $u = v - w \in U$ mamy $v = u + w$ co pokazuje że $V = U + W$. □

4 Lemat Schura, wersja algebraiczna

Lemat 4.1 *Jeśli M i N są modułami, zaś ϕ jest niezerowym homomorfizmem z M w N to*

- *jeśli M jest prosty to ϕ jest różnowartościowy*
- *jeśli N jest prosty to ϕ jest na*
- *jeśli M i N są proste to ϕ jest izomorfizmem*

Dowód: Jądro $\ker(\phi)$ jest podmodułem M, jeśli M jest prosty to $\ker(\phi) = \{0\}$ lub $\ker(\phi) = M$. W drugim przypadku ϕ byłby zerowy, co jest wykluczone z założenia. A więc gdy M jest prosty to $\ker(\phi) = \{0\}$ czyli ϕ jest różnowartościowy. Podobnie, obraz $\phi(M)$ jest podmodułem N i jeśli N jest prosty to musimy mieć $\phi(M) = N$. □

Lemat 4.2 *Algebra endomorfizmów R-modułu prostego jest algebrą z dzieleniem. Jeśli R jest skończenie wymiarową algebrą nad ciałem algebraicznie domkniętym K to każdy endomorfizm modułu prostego jest operatorem mnożenia przez element K.*

Dowód: Na mocy poprzedniego lematu niezerowe endomorfizmy są odwracalne, co daje pierwszą część. Dla dowodu drugiej części zauważmy że wtedy moduł prosty M jest skończenie wymiarową przestrzenią wektorową nad ciałem K. Endomorfizm ϕ możemy przedstawić przy pomocy macierzy. Wiadomo że nad ciałem algebraicznie domkniętym macierz ma wartość własną λ i odpowiadający jej wektor własny v, tzn.

$$\phi v = \lambda v$$

czyli

$$(\phi - \lambda)v = 0$$

Jako że M jest modułem prostym oznacza to że $(\phi - \lambda)w = 0$ dla dowolnego $w \in M$. □

Lemat 4.3 *Jeśli R jest skończenie wymiarową algebrą przemienną nad ciałem algebraicznie domkniętym K to każdy R-moduł M prosty jest przestrzenią jednowymiarową nad K zaś R działa na M za pomocą mnożenia przez element K.*

Dowód: Jako że R jest przemienny, to elementy R działają za pomocą mnożenia przez element K. A więc podprzestrzenie jednowymiarowe są niezmiennicze na działanie R, czyli M jest jednowymiarowy. □

Uwaga. Jeśli G jest skończoną grupą abelową to na mocy lematu (gdy są spełnione założenia) moduły proste nad $K[G]$ (czyli reprezentacje nieprzywiedlne G) są jednowymiarow. Elementy G działają za pomocą mnożenia przez element K. A więc jeśli ρ jest reprezentacją nieprzywiedlną, to dla $g \in G$ istnieje a_g takie że $\rho(g)v = a_g v$. W grupie skończonej istnieje k_g takie że $g^{k_g} = e$ gdzie e jest jedynką w G. Wtedy mamy

$$v = \rho(e)v = \rho(g^{k_g})v = \rho(g)^{k_g}v = a_g^{k_g}v$$

czyli $a_g^{k_g} = 1$, czyli wartości a_g są pierwiastkami z 1. W szczególności, jeśli G jest skończoną grupą cykliczną to G jest izomorficzne z liczbami całkowitymi modulo k dla pewnego k. Reprezentacja grupy cyklicznej jest jednoznacznie wyznaczona przez wartość na generatorze, (tzn. 1). Poprzednie rozumowanie pokazuje że dla reprezentacji nad liczbami zespolonymi mamy

$$\rho(l)v = \exp(2\pi i l m/k)v$$

gdzie $m = 0, 1, \ldots k-1$ jest parametrem opisującym reprezentację, zaś i jest jednostką urojoną.

5 Grupa dihedralna

Niech będzie dane odwzorowanie α z $\mathbb{Z}_2$ w automorfizmy $\mathbb{Z}_n$ takie że $\alpha(0)$ to identyczność zaś $\alpha(1)(m) = -m$.

Wtedy na produkcie $\mathbb{Z}_2 \times \mathbb{Z}_n$ działanie wprowadzamy wzorem

$$(z_1, m_1)(z_2, m_2) = (z_1 z_2, \alpha(z_2)m_1 m_2).$$

Otrzymaną w ten sposób grupę oznaczamy D_n i nazywamy grupą dihedralną (przy ogólnych grupach i ogólnym α wzór wyżej definiuje produkt półprosty).

Chcemy wyznaczyć reprezentacje nieprzywiedlne D_n na ciałem liczb zespolonych, tzn. moduły proste nad $\mathbb{C}[D_n]$. Zauważmy że D_n zawiera grupę $\mathbb{Z}_n$. Niech V będzie przestrzenią reprezentacji nieprzywiedlnej ρ grupy D_n. ρ możemy potraktować jako reprezentację $\mathbb{Z}_n$. Wtedy na mocy twierdzenia Maszkego V rozpadnie się na sumę prostą reprezentacji nieprzywiedlnych $\mathbb{Z}_n$:

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_l.$$

Jako że $\mathbb{Z}_n$ jest grupą abelową zaś $\mathbb{C}$ jest ciałem algebraicznie domkniętym to V_k są jednowymiarowe. Można przyjąć że dla $v \in V_1$ i $m \in \mathbb{Z}_n$ mamy wzór

$$\rho((0,m))v = \exp(\frac{2\pi ikm}{n})v$$

gdzie k jest parametrem reprezentacji. Oznaczmy przez s element $(1,0) \in D_n$. Rozważmy teraz działanie $\mathbb{Z}_n$ na $\rho(s)V_1$. Mamy

$$\rho((0,m))\rho(s)v = \rho(s)\rho(s^{-1})\rho((0,m))\rho(s)v$$

$$= \rho(s)\rho(s^{-1}(0,m)s)v = \rho(s)\rho(-m)v$$

$$\rho(s)\exp(\frac{2\pi ik(-m)}{n})v = \exp(\frac{2\pi i(-k)m}{n})\rho(s)v.$$

Czyli $\rho(s)V_1$ jest przestrzenią reprezentacji $\mathbb{Z}_n$ z parametrem $-k$. Stosując podobne rozumowanie do reprezentacji na $\rho(s)V_1$ widać że $\rho(s)$ przeprowadzi ją na reprezentację z parameterem k. W więc

$$V = W_k \oplus W_{-k}$$

gdzie W_k jest sumą przestrzeni reprezentacji $\mathbb{Z}_n$ z parametrem k zaś W_{-k} jest sumą reprezentacji z parametrem $-k$. Mianowicie, $\rho(s)W_k \subset W_{-k}$, $\rho(s)W_{-k} \subset W_k$, zarówno W_k jak i W_{-k} są niezmiennicze na działanie $\mathbb{Z}_n$, więc suma $W_k \oplus W_{-k}$ jest niezmiennicza na działanie D_n. Jako że V jest nieprzywiedlna oznacza to równość $V = W_k \oplus W_{-k}$.

V możemy też potraktować jako przestrzeń reprezentacji $\mathbb{Z}_2$. Niech teraz v rozpina jednowymiarową podprzestrzeń niezmienniczą dla $\mathbb{Z}_2$. Piszemy $v = w_1 \oplus w_2$ gdzie $w_1 \in W_k$ zaś $w_2 \in W_{-k}$. Zakładając że $k \neq -k \mod n$ i $\rho(s)v = v$ mamy $w_2 = \rho(s)w_1$ i $w_1 = \rho(s)w_2$, a więc dwuwymiarowa podprzestrzeń rozpinana przez w_1 i w_2 jest niezmiennicza zarówno dla $\mathbb{Z}_2$ jak i dla $\mathbb{Z}_n$, a więc jest niezmiennicza dla D_n. Podobnie, jeśli $\rho(s)v = -v$, to $-w_2 = \rho(s)w_1$ i $-w_1 = \rho(s)w_2$ i również w tym przypadku podprzestrzeń rozpinana przez w_1 i w_2 jest niezmiennicza dla D_n. A więc reprezentacje nieprzywiedlne D_n są dwuwymiarowe, za wyjątkiem przypadku $k = -k \mod n$, gdy otrzymujemy reprezentacje jednowymiarowe. Ten przypadek zachodzi gdy $k = 0$, lub n jest parzyste i $k = n/2$.

6 Suma prosta

Na nieskończonym iloczynie kartezjańskim modułów mamy naturalną strukturę modułu, mianowicie operacje wykonujemy po składowych. Sumą prostą potencjalnie nieskończonej rodziny modułów M_α, $\alpha \in I$ jest podzbiór produktu kartezjańskiego M_α, $\alpha \in I$ składający się z tych elementów które mają tylko skończenie wiele składowych różnych od zera. Oznaczenie:

$$M = \bigoplus_{\alpha \in I} M_\alpha$$

Każdy z modułów M_α jest naturalnie izomorficzny z podmodułem M, dlatego zwykle możemy zakładać że $M_\alpha \subset M$. Przy takim założeniu dla $\alpha \neq \beta$ mamy $M_\alpha \cap M_\beta = \emptyset$.

Jeśli M jest modułem a M_α, $\alpha \in I$ są podmodułami M to sumą M_α nazywamy najmniejszy podmoduł $N \subset M$ taki że dla każdego $\alpha \in I$ mamy $M_\alpha \subset N$.

Jeśli M jest sumą M_α, $\alpha \in I$ oraz dla $\alpha \neq \beta$ mamy $M_\alpha \cap M_\beta = \emptyset$, to wtedy M jest izomorficzny z sumą prostą M_α, $\alpha \in I$. W tej sytuacji dalej będziemy mówić że M jest sumą prostą.

Jeśli M jest sumą prostą $M_1 \oplus M_2$ swoich podmodułów M_1 i M_2 to mówimy że M_2 jest modułem dopełniczym do M_1.

7 Moduły półproste

Najpierw potrzebujemy lemat opisujący moduły proste

Lemat 7.1 *Moduł M jest prosty wtedy i tylko wtedy gdy M jest izomorficzny z modułem postaci R/I gdzie I jest lewostronnym ideałem maksymalnym w R.*

Dowód. Niech I będzie lewostronnym ideałem maksymalnym w R i N będzie podmodułem w R/I. Wtedy $J = \{r \in R : r + I \subset N\}$ jest ideałem lewostronnym zawierającym I. Jako że I jest ideałem maksymalnym oznacza to że $J = R$ lub $J = I$. W pierwszym przypadku mamy $N = R/I$, w drugim $N = \{0\}$, a więc R/I jest modułem prostym. Jeśli M jest modułem prostym i $x \in M$, $x \neq 0$ to przyjmujemy $I = \{r : rx = 0\}$. Wtedy I jest ideałem lewostronnym w R. Zauważmy że Rx jest niezerowym podmodułem w M, czyli $Rx = M$. Innymi słowy M jest izomorficzne z R/I. Jeśli J jest ideałem lewostronnym i $I \subset J$ to Jx jest podmodułem w M, czyli $Jx = M$ lub $Jx = \{0\}$. Jeśli $Jx = M$ to dla dowolnego $r \in R$ istnieje $s \in J$ takie że $rx = sx$, czyli $(r - s)x = 0$, czyli $r - s \in I$. Jako że $I \subset J$ i $s \in J$ oznacza to że $r \in J$, czyli $J = R$. Jeśli $Jx = \{0\}$ to mamy $J = I$. Razem oznacza to że I jest ideałem maksymalnym. □

Lemat 7.2 *Następujące warunki są równoważne*

- *moduł M jest sumą prostą modułów prostych*

- *moduł M jest sumą algebraiczną modułów prostych*
- *każdy podmoduł $V \subset M$ ma podmoduł dopełniczy będący sumą prostą modułów prostych*
- *każdy podmoduł $V \subset M$ ma podmoduł dopełniczy*

Moduł spełniający jeden (a więc i wszystkie) warunki wyżej nazywamy modułem półprostym.

Dowód: Warunek pierwszy jest oczywiście silniejszy niż drugi. Warunek trzeci jest oczywiście silniejszy niż czwarty. Dla $V = \{0\}$ warunek trzeci implikuje warunek pierwszy. Pozostaje pokazać że warunek drugi implikuje trzeci i że warunek czwarty implikuje drugi.

Aby otrzymać warunek trzeci z drugiego rozważmy rodzinę S składającą się z takich modułów N że N jest sumą prostą modułów prostych i $V \cap N = \emptyset$. Zauważymy że suma V i N jest sumą prostą, tzn $V + N = V \oplus N$.

Na mocy lematu o maksymalnym łańcuchu w rodzinie S istnieje element maksymalny, tzn. taki moduł N że dla każdego modułu prostego $P \subset M$ mamy $P \cap (V \oplus N) \neq \{0\}$ (w przeciwnym razie można by dołączyć P jako kolejny składnik N przecząc maksymalności). A więc dla dowolnego modułu prostego $P \subset M$ mamy $P \subset V \oplus N$, czyli jako że M jest sumą modułów prostych to $M = V \oplus N$. Ponadto N jest sumą prostą modułów prostych co daje warunek trzeci.

Aby zakończyć dowód lematu musimy pokazać że warunek czwarty implikuje drugi.

Zauważmy najpierw że jeśli warunek czwarty jest spełniony dla M i U jest podmodułem M to warunek czwarty zachodzi dla M zastąpionego przez U. Mianowicie, jeśli V jest podmodułem U to jest też podmodułem M. Używając warunek dla M dostajemy moduł N dopełniczy do V w M. Lecz wtedy $N \cap U$ jest modułem dopełniczym do V w U. Pokażemy teraz że dowolny moduł M spełniający warunek czwarty zawiera podmoduł prosty. Mianowicie, bez utraty ogólności można przyjąć że $M = Rx$ dla pewnego $x \in M$. Niech $J = \{r \in R : rx = 0\}$. J jest ideałem lewostronnym w R. Na mocy pewnika wyboru (lematu o maksymalnym łańcuchu) istnieje ideał maksymalny I zawierający J. Wtedy $N = Ix$ jest podmodułem w $M = Rx$ takim że M/N jest izomorficzne z R/I, czyli iloraz jest modułem prostym. Na mocy warunku czwartego istnieje podmoduł P dopełniczy do M, czyli $Rx = P \oplus N$ czyli P jest izomorficzne z Rx/N czyli P jest modułem prostym. Rozważmy teraz sumę S wszystkich modułów prostych zawartych w M. Gdyby S było podmodułem właściwym to S miałby niezerowy moduł dopełniczy, a więc dopełnienie S zawierałoby moduł prosty. Lecz to jest niemożliwe z definicji S czyli M jest sumą modułów prostych czyli zachodzi warunek drugi. □

8 Lemat o gęstości

Jeśli M jest modułem to endomorfizmy M tworzą pierścień który oznaczymy przez E. M możemy potraktować jako moduł nad E. Dla zaznaczenia że pierścieniem jest E będziemy pisać M_E. Istotny dla nas jest opis endomorfizmów M_E.

Lemat 8.1 *Jeśli M jest modułem półprostym, ϕ jest endomorfizmem M_E zaś $x \in M$ to istnieje $\alpha \in R$ takie że $\phi(x) = \alpha x$.*

Dowód: $N = Rx$ jest podmodułem M, a więc na mocy półprostoty jest składnikiem prostym M. A więc rzut π_N z M na N należy do E. Wtedy

$$\pi_N(\phi(x)) = \phi(\pi_N(x)) = \phi(x)$$

czyli $\phi(x) \in N$, co daje wynik. □

Lemat 8.2 *(Jacobsona o gęstości) Jeśli M jest modułem półprostym, ϕ jest endomorfizmem M_E zaś S jest skończonym podzbiorem M. Wtedy istnieje $\alpha \in R$ takie że dla dowolnego $x \in S$ mamy $\phi(x) = \alpha x$.*

Dowód: Niech $n = |S|$ czyli $S = \{x_1, \ldots, x_n\}$.

Rozważmy n-krotną sumę prostą M^n. Na M^n rozpatrujemy odwzorowanie $\phi^{(n)}$ zadane wzorem

$$(y_1, \ldots, y_n) \mapsto (\phi(y_1), \ldots, \phi(y_n)).$$

Niech $E^{(n)}$ będzie pierścieniem endomorfizmów M^n. Zauważmy że elementy $E^{(n)}$ to macierze n na n o współczynnikach będących endomorfizmami M. Ze wzoru na $\phi^{(n)}$ wynika więc że $\phi^{(n)}$ jest homomorfizmem M^n jako modułu nad $E^{(n)}$. Moduł M^n jest oczywiście półprosty. Z poprzedniego lematu istnieje element $\alpha \in R$ taki że $\phi^{(n)}(x_1, \ldots, x_n) = \alpha(x_1, \ldots, x_n)$. Lecz to oznacza że $\phi(x_i) = \alpha x_i$. □

Lemat 8.3 *(Twierdzenie Burnsida) Jeśli M jest skończenie wymiarową przestrzenią wektorową nad ciałem algebraicznie domkniętym k, R jest podpierścieniem pierścienia $\mathrm{End}_k(M)$ który jest przestrzenia wektorową nad k i M jest R-modułem prostym nad k to $R = \mathrm{End}_k(M)$.*

Dowód: Jeśli M jest R-modułem prostym to mocy lematu Schura pierścień E R-endomorfozmów M to k. Niech $f \in \mathrm{End}_k(M) = \mathrm{End}_E(M)$ i niech $x_1, \ldots, x_n$ będzie bazą M jako przestrzeni wektorowej nad k. Wtedy na mocy lematu o gęstości istnieje $\alpha \in R$ takie że $\alpha x_i = f(x_i)$. Jako że $x_1, \ldots, x_n$ jest bazą oznacza to że $\alpha = f$. Jako że f był dowolny oznacza to że $R = \mathrm{End}_k(M)$. □

9 Twierdzenie Wedderburna

R nazywamy pierścieniem półprostym jeśli jest modułem półprostym jako lewy moduł nad sobą.

Lemat 9.1 *Jeśli R jest pierścieniem półprostym to każdy R-moduł jest półprosty.*

Dowód: Dowolny moduł jest sumą modułów postaci Rx. Moduł postaci Rx jest ilorazem R a więc na mocy półprostoty R moduł Rx jest sumą prostą modułów prostych. A więc dowolny R-moduł jest sumą modułów prostych. □

Lemat 9.2 *Jeśli R jest pierścieniem półprostym to istnieje tylko skończenie wiele klas izomorfizmu R-modułów prostych.*

Dowód: Każdy reprezentant klasy izomorfizmu R-modułów prostych jest postaci $M = R/I$ gdzie I jest ideałem maksymalnym. Na mocy półprostoty R ideał I będąc podmodułem ma podmoduł dopełniczy, czyli $R = M \oplus I$. Niech $R = \bigoplus_\alpha M_\alpha$ będzie rozkładem R na sumę prostą modułów prostych. Mamy $1 = x_1 \oplus \cdots \oplus x_l$ gdzie $x_i \in M_{\alpha_i}$. Zauważmy że $M_{\alpha_1} \oplus \cdots \oplus M_{\alpha_l}$ jest podmodułem R takim że $1 \in R$, a więc $R = M_{\alpha_1} \oplus \cdots \oplus M_{\alpha_l}$. Łatwo zauważyć że każdy podmoduł prosty M zawarty w R jest izomorficzny z jednym z M_{α_i}. Mianowicie, dla pewnego i rzutowanie z M na M_{α_i} musi być niezerowe i na mocy lematu Schura jest izomorfizmem. □

Na mocy poprzednich lematów moduł M nad pierścieniem półprostym R ma rozkład postaci

$$M = \oplus_i \oplus_{j=1}^{k_i} M_i$$

gdzie M_i przebiega zbiór reprezentantów klas równoważności R-modułów prostych. Liczby k_i nazywamy krotnościami, tzn. mówimy że moduł M_i występuje w M z krotnością M_i.

Lemat 9.3 *Jeśli R jest skończenie wymiarową algebrą półprostą nad ciałem algebraicznie domkniętym k to*

$$R \approx \mathrm{End}_k(M_1) \oplus \cdots \oplus \mathrm{End}_k(M_l)$$

gdzie M_i przebiega reprezentanty klas izomorfizmu R-modułów prostych.

Dowód: Rozważmy homomorfizm h z R w

$$\tilde{R} = \mathrm{End}_k(M_1) \oplus \cdots \oplus \mathrm{End}_k(M_l).$$

h jest różnowartościowy, bo jeśli α jest w jądrze h to mnożenie przez α daje odwzorowanie zerowe dla dowolnego modułu prostego M_i. Jako że R jest sumą

prostą modułów prostych to mnożenie przez α daje odwzorowanie zerowe na R. Lecz $\alpha = \alpha \cdot 1$, czyli wtedy $\alpha = 0$. Na mocy lematu o gęstości h jest na. Mianowicie, na mocy lematu Schura endomorfizmy M_i to ciało k. Dla $i \neq j$ moduły M_i i M_j są nieizomorficzne, więc jedyny homomorfizm między nimi jest zerowy. A więc pierścień endomorfizmów E modułu $M_1 \oplus \cdots \oplus M_l$ to suma l-kopii ciała k z działaniami po składowych. Czyli jeśli $\phi \in \tilde{R}$ to ϕ wyznacza endomorfizm $(M_1 \oplus \cdots \oplus M_l)_E$.

A więc, jeśli $x_{i,j}$, $i = 1, \ldots, l$, $j = 1, \ldots, n_l$ są takie że $x_{i,j} \in M_i$ i przy ustalonym i wektory $x_{i,j}$ tworzą bazę M_i i $\phi \in \tilde{R}$ to istnieje $\alpha \in R$ takie że $\alpha x_{i,j} = \phi x_{i,j}$. □

Uwaga. Bez założenia że ciało podstawowe jest algebraicznie domknięte pierścień $E = D_1 \oplus \ldots D_l$ gdzie D_i są algebrami z dzieleniem i w sumie wyżej musimy brać algebry endomorfizmów nad D_i.

Wniosek:

$$\dim_k R = \sum \dim_k (M_i)^2$$

gdzie M_i przebiegają klasy R modułów prostych. Innymi słowy M_i występuje w R z krotnością $\dim_k(M_i)$.

Przykład: Niech $G = S(3)$ (grupa permutacji trzech elementów). G jest izomorficzna z grupą symetrii trójkąta i łatwo sprawdzić że naturalne działanie G na trójkącie daje reprezentację nieprzywiedlną czyli prosty $k[G]$ moduł. Czyli $k[G]$ ma moduł prosty który jest przestrzenią wymiaru 2 nad k. Ponadto G ma dwie reprezentacje wymiaru 1: reprezentację trywialną i znak permutacji. G ma 6 elementów, czyli

$$6 = \dim_k k[G] = 1 + 1 + 2^2$$

czyli podane reprezentacje to wszystkie reprezentacje nieprzywiedlne G z dokładnością do równoważności.

Nieco ogólniej można rozpatrywać grupę dihedralną D_n. Dla nieparzystego n grupa D_n ma dwie reprezentacje jednowymiarowe, pochodzące z reprezentacji $\mathbb{Z}_2$. Jest też $(n-1)/2$ różnych reprezentacji nieprzywiedlnych wymiaru 2. W sumie

$$2n \dim_k k[G] = 1 + 1 + \frac{n-1}{2} 2^2.$$

Potwierdza to ze otrzymaliśmy komplet reprezentacji nieprzywiedlnych.

10 Rozkład kanoniczy reprezentacji

Ustalmy izomorfizm

$$R \approx \mathrm{End}_k(M_1) \oplus \cdots \oplus \mathrm{End}_k(M_l)$$

Niech R_i oznacza $\mathrm{End}_k(M_i)$ zaś e_i element taki że $e_i = 1$ w R_i oraz $e_i = 0$ w R_j dla $j \neq i$. Wtedy

$$1 = \sum e_i$$

oraz

$$e_i^2 = e_i$$

Ponadto e_i leżą w centrum R.

Lemat 10.1 *Jeśli M jest R modułem to e_iM to suma podmodułów M izomorficznych z M_i*

Dowód: Na M_i element e_i działa jako identyczność. Dla $j \neq i$ element e_i działa jako 0. Czyli jeśli N to suma podmodułów M izomorficznych z M_i to e_i działa na N jako identyczność. Jeśli W to moduł dopełniczy do N to W jest izomorficzny z sumą prostą modułów M_j z $j \neq i$. A więc e_i działa na W jako 0. Razem, $e_ix = x$ dla $x \in N$ i $e_ix = 0$ dla $i \in W$. □

Mamy

$$M = \oplus e_iM$$

Daje to rozkład kanoniczny M. W rozkładzie kanonicznym składniki są wyznaczone jednoznacznie. e_i wyżej nazywamy idempotentem związanym z M_i.

Lemat 10.2 *Krotności M_i w M są wyznaczone jednoznacznie*

Dowód: Na mocy poprzedniego lematu mamy

$$e_iM = \oplus_{j=1}^{k_i} M_i$$

i moduł e_iM jest wyznaczony jednoznacznie. Lecz

$$\dim_k(e_iM) = k_i \dim_k(M_i)$$

czyli k_i jest wyznaczone jednoznacznie przez wymiary nad k.

Uwaga: Jeśli $k_i > 1$ to przedstawienie e_iM jako sumy prostej M_i jest bardzo niejednoznaczne.

11 Charaktery

Definicja: Charakterem reprezentacji (modułu) nazywamy odwzorowanie $\phi_\rho(a) = \mathrm{Tr}(\rho(a))$ gdzie Tr oznacza ślad odwzorowania liniowego.

Uwaga: W przypadku pierścienia grupowego charaktery są zdefiniowane jako odwzorowania liniowe na $R[G]$. Jednakże takie odwzorowanie jest jednoznacznie wyznaczone przez wartości na bazie, tzn. elementach δ_g. Dlatego często wygodnie jest traktować charakter jako funkcję na G, której wartość w g to $\mathrm{Tr}(\rho(\delta_g))$.

Przykład: Jeśli λ jest reprezentacją regularną to

$$\phi_\lambda(\delta_g) = \begin{cases} n & \text{dla } g = e \\ 0 & \text{poza tym} \end{cases}$$

Przykład: Jeśli $G = \mathbb{Z}_n$ to nad liczbami zespolonymi mamy reprezentacji jednowymiarowe ρ_j zadanie wzorem $\rho_j(m)v = \exp(2\pi ijm/n)v$. Wtedy $\phi_{\rho_j} = \exp(2\pi ijm/n)$, czyli charakter jest homomorfizmem z G w $\mathbb{C}$.

Ogólniej, rozważmy skończenie wymiarową reprezentację ρ grupy skończonej G nad ciałem algebraicznie domkniętym k charakterystyki p nie dzielącej mocy G. Dla $g \in G$ operator $\rho(g)$ można przedstawić w postaci klatkowo-diagonalnej (rozkład Jordana). W charakterystyce 0, gdyby była nietrywialna klatka Jordana to podgrupa operatorów postaci $\rho(g)^k$ z $k \in \mathbb{Z}$ byłaby nieskończona co jest sprzeczne z tym że G jest skończona. Podobnie, w przypadku charakterystyki skończonej dla nietrywialnej klatki Jordana podgrupa operatorów postaci $\rho(g)^k$ miałaby moc podzielną przez p, co oznaczałoby że moc G jest podzielna przez p co jest sprzecznie z naszymi założeniami. A więc $\rho(g)$ można przedstawić w postaci diagonalnej. Jako że G jest skończona to istnieje k takie że $g^k = e$ (gdzie e jest jedynką w G). Jeśli ω jest elementem na diagonali w postaci diagonalnej $\rho(g)$, to $\omega^k = 1$. A więc ω jest pierwiastkiem wielomianu mającego współczynniki całkowite i takiego że współczynnik przy najwyższej potędze jest równy 1. Takie liczby nazywamy *liczbami algebraicznymi całkowitymi*. Nieco ogólniej mówimy że są to elementy całkowite nad $\mathbb{Z}$. Na mocy Lematu 12.2 suma elementów całkowitych jest całkowita. A więc wartości charakterów reprezentacji nad $\mathbb{C}$ jako sumy elementów całkowitych nad $\mathbb{Z}$ (tzn. pierwiastków z 1) są całkowite nad $\mathbb{Z}$. Innymi słowy, wartości charakterów są *liczbami algebraicznymi całkowitymi*. Wiadomo (Lemat 12.3) że liczby całkowite algebraiczne które są liczbami wymiernymi są całkowite. A więc jeśli charakter przyjmuje wartości wymierne to są one całkowite. Np. wiadomo że charaktery grup permutacji S_n przyjmują wartości całkowite (charaktery grup alternujących A_n mogą przyjmować wartości niewymierne).

Inwolucję w $k[G]$ i iloczyn skalarny dla $f = \sum_{g\in G} a_g\delta_g$ i $h = \sum_{g\in G} b_g\delta_g$ definiujemy

$$\check{f} = \sum_{g\in G} a_g\delta_{g^{-1}}$$

$$\langle f, h\rangle = \frac{1}{|G|}\sum_{g\in G} a_g b_{g^{-1}}$$

Poniżej będziemy zakładać że charakterystyka ciała k nie dzieli $|G|$, dzięki czemu $\langle f, h\rangle$ jest dobrze zdefiniowane.

Lemat 11.1 $\check{f}\check{h} = \check{h}\check{f}$

Dowód: Sprawdzamy dla $f = \delta_g$, $h = \delta_u$:

$$\check{f}\check{h} = \check{\delta}_g\check{\delta}_u = \check{\delta}_{gu} = \delta_{(gu)^{-1}} = \delta_{u^{-1}g^{-1}} = \delta_{u^{-1}}\delta_{g^{-1}}$$

$$= \check{\delta}_u\check{\delta}_g = \check{h}\check{f}.$$

W ogólnym przypadku wynik otrzymujemy przez liniowość. □

Lemat 11.2 *(Wzór Plancherela) Niech λ będzie reprezentacją regularną $k[G]$. Mamy*

$$\langle f, h\rangle = \frac{1}{|G|^2}\mathrm{Tr}(\lambda(fh))$$

Dowód: Dla $f = \delta_g$ i $h = \delta_u$ mamy $\langle f, h\rangle = 0$ dla $g \neq u^{-1}$ i $\langle f, h\rangle = \frac{1}{|G|}$ dla $g = u^{-1}$. Podobnie, $fh = \delta_{gu}$ czyli $\mathrm{Tr}(\lambda(fh)) = 0$ dla $g \neq u^{-1}$ i $\mathrm{Tr}(\lambda(fh)) = |G|$ dla $g = u^{-1}$. A więc równość zachodzi dla elementów bazy czyli przez liniowość równość zachodzi na $k[G]$. □

Lemat 11.3 *Jeśli k jest algebraicznie domknięte, M_i jest $k[G]$ modułem prostym, e_i idempotentem odpowiadającym M_i zaś χ_i charakterem modułu M_i to dla $f \in k[G]$ mamy*

$$\dim_k M_i\chi_i(f) = |G|^2\langle f, e_i\rangle$$

Dowód: Na mocy twierdzenia Wedderburna M_i występuje w reprezentacji regularnej z krotnością $\dim_k M_i$. A więc mamy

$$\dim_k M_i\chi_i(f) = \mathrm{Tr}(\lambda(fe_i)) = |G|^2\langle f, e_i\rangle$$

gdzie ostatnia równość to wzór Plancherela. □

Lemat 11.4 *Jeśli k jest algebraicznie domknięte, zaś M_i jest $k[G]$-modułem prostym to jako funkcja na grupie*

$$\chi_i = \frac{|G|}{\dim_k(M_i)}\check{e}_i$$

gdzie e_i jest idempotentem związanym z M_i. W szczególności charakterystyka K nie dzieli $\dim_k(M_i)$ (zakładamy że charakterystyka K nie dzieli $|G|$).

Dowód. Dla $f = \delta_g$ mamy $|G|\langle f, e_i\rangle = \check{e}_i(g)$. A więc

$$\dim_k(M_i)\chi_i(g) = \dim_k(M_i)\chi_i(f) = |G|^2\langle f, e_i\rangle = |G|\check{e}_i(g)$$

Jako że $|G|\check{e}_i(g)$ jest niezerowe dla pewnego g to wynika stąd że charakterystyka k nie dzieli $\dim_k(M_i)$. □

Wniosek: $\langle\chi_i, \chi_j\rangle = \delta_{ij}$, gdzie $\delta_{ii} = 1$ zaś $\delta_{ij} = 0$ dla $i \neq j$. Mianowicie

$$\langle\chi_i, \chi_j\rangle = \frac{|G|^2}{\dim_k(M_i)\dim_k(M_j)}\langle\check{e}_i, \check{e}_j\rangle$$

$$= \frac{1}{\dim_k(M_i)\dim_k(M_j)}\mathrm{Tr}(\lambda(e_j\check{e}_i)).$$

Gdy $i \neq j$ to $e_j e_i = 0$ czyli $\langle \chi_i, \chi_j \rangle = 0$. Dla $i = j$ element $e_i e_i = e_i$ przechodzi na identyczność w $e_i k[G]$ które jest sumą prostą $\dim_k(M_i)$ kopii M_i. A więc $\check{e}_i$ przechodzi na identyczność w $\check{e}_i k[G]$ które ma wymiar $\dim_k(M_i)^2$, czyli $\mathrm{Tr}(\lambda(\check{e}_i)) = \dim_k(M_i)^2$ co daje $\langle \chi_i, \chi_i \rangle = 1$.

Lemat 11.5 *Jeśli ciało k jest charakterystyki 0 to $k[G]$ moduły są izomorficzne wtedy i tylko wtedy gdy ich charaktery są równe. W szczególności gdy ciało k jest algebraicznie domknięte, η jest charakterem $k[G]$ modułu N zaś M_i jest $k[G]$-modułem prostym z charakterem χ_i to M_i występuje w N z krotnością $\langle \chi_i, \eta \rangle$.*

Dowód: Druga cześć wynika z zależności $\langle \chi_i, \chi_j \rangle = \delta_{ij}$. Mianowicie, rozkładając N na moduły proste mamy

$$N = \oplus_i k_i M_i,$$

$$\eta = \sum_i k_i \chi_i,$$

$$\langle \eta, \chi_j \rangle = \sum_i k_i \langle \chi_i, \chi_j \rangle = k_j.$$

Daje to wynik dla ciała algebraicznie domkniętego. Ponadto mamy

$$\langle \eta, \eta \rangle = \sum_{i,j} k_i k_j \langle \chi_i, \chi_j \rangle = \sum_i k_i^2 > 0.$$

Gdy k jest tylko charakterystyki 0 to można rozumować podobnie. Mianowicie, jak dla ciała algebraicznie domkniętego rozpatrujemy moduły proste M_i i ich charaktery χ_i. Niech K będzie algebraicznym domknięciem k. Traktując M_i jako moduł nad K dostaniemy ten sam charakter, ale moduł nie musi być prosty jako moduł nad K. Ze wzoru wyżej dostaniemy że

$$\langle \chi_i, \chi_i \rangle > 0.$$

Trzeba jeszcze pokazać że $\langle \chi_i, \chi_j \rangle = 0$ dla $i \neq j$. Traktując M_i i M_j jako moduły nad K widać że $\langle \chi_i, \chi_j \rangle \neq 0$ implikuje że w rozkładzie nad K jest wspólny czynnik, czyli istnieje niezerowy homomorfizm modułów H nad $K[G]$. Homomorfizm modułów możemy reprezentować macierzą nad K. To że macierz reprezentuje homomorfizm jest równoważne temu że rozwiązuje układ równań

$$\rho_i(\delta_g) H = H \rho_j(\delta_g)$$

gdzie ρ_i jest reprezentacją odpowiadającą M_i zaś g przebiega elementy grupy. Ten układ równań jest układem równań liniowych. A więc, skoro ma niezerowe rozwiązanie nad K to ma też niezerowe rozwiązanie nad k. Ale niezerowe rozwiązanie nad k daje niezerowy homomorfizm modułów nad k. Jako że nad k moduły M_i i M_j są proste to z lematu Schura niezerowy homomorfizm jest izomorfizmem, czyli M_i jest izomorficzne z M_j. Czyli, jeśli M_i nie jest izomorficzne z M_j to $\langle \chi_i, \chi_j \rangle = 0$. □

12 Dodatek: całkowitość

Niech R będzie pierścieniem przemiennym. Mówimy że element $a \in R$ jest całkowity nad R jeśli jest pierwiastkiem wielomianu nad R z najwyższym współczynnikiem równym 1.

Lemat 12.1 *a jest całkowity wtedy i tylko wtedy gdy $R[a]$ jest skończenie generowalnym R-modułem.*

Dowód: Jeśli $a^n + c_{n-1}a^{n-1} + \cdots + c_0 = 0$ to możemy wyliczyć a^l dla $l \geq n$ w terminach a^i dla $i = 0, \ldots, n-1$, czyli $R[a]$ jest generowane przez a^i, $i - 0, \ldots, n-1$ nad R. Jeśli $R[a]$ jest skończenie generowalnym R-modułem to można wybrać n takie że a^i, $i = 0, \ldots, n-1$ są generatorami $R[a]$. Zapisując a^n w terminach generatorów dostaniemy potrzebne równanie.

Lemat 12.2 *Jeśli R jest pierścieniem noetherowskim to suma i iloczyn elementów całkowitych są całkowite.*

Dowód. $R[a_1]R[a_2]$ jest skończenie generowalnym modułem nad R. Jako że R jest noethereowski to również $R[a_1 a_2]$ i $R[a_1 + a_2]$ są skończenie generowalne.

Lemat 12.3 *Jeśli liczba wymierna q jest liczbą algebraiczną całkowitą to jest liczbą całkowitą, tzn. $q \in \mathbb{Z}$.*

Dowód: Z definicji, q jest pierwiastkiem wielomianu $P(x)$ o współczynnikach całkowitych i takiego że współczynnik przy najwyższej potędze x jest równy 1. Z własności wielomianów nad liczbami wymiernymi $P(x)$ ma wtedy czynnik liniowy o współczynnikach wymiernych którego pierwiastkiem jest q. Ale wielomiany o współczynnikach całkowitych mają jednoznaczny rozkład na czynniki nierozkładalne i czynniki liniowy ma współczynniki całkowite. Dokładniej, istnieją wielomiany P_1 i l o współczynnikach całkowitych, takie że $P(x) = P_1(x)l(x)$, l jest liniowy i $l(q) = 0$. Współczynnik P przy najwyższej potędze x jest równy produktowi współczynników P_1 i l przy najwyższej potędze x. A więc współczynnik przy najwyższej x w l jest równy 1 lub -1. Bez utraty ogólności można przyjąć że jest on równy 1. A więc

$$l(x) = x + l_0$$

gdzie $l_0 \in \mathbb{Z}$. Jako że $l(q) = 0$ oznacza to że $q = -l_0 \in \mathbb{Z}$. □

13 Iloczyn tensorowy

Niech R będzie pierścieniem przemiennym, zaś M i N będą R-modułami. Powiemy że moduł V jest iloczynem tensorowym modułów M i N (co oznaczamy pisząc $V = M \otimes N$) jeśli zadana jest operacja dwuliniowa oznaczana przez $\otimes$

z $M \times N$ w V mająca następującą własność: jeśli η jest operacją dwuliniową z $M \times N$ w pewien R-moduł W to istnieje dokładnie jedna operacja liniowa ϕ z V w W taka że

$$\eta(m, n) = \phi(m \otimes n).$$

Zauważmy najpierw że z definicji wyżej wynika że jeśli produkt tensorowy istnieje to jest wyznaczony jednoznacznie z dokładnością do izomorfizmu. Mianowicie, jeśli V_1 z $\otimes_1$ oraz V_2 z $\otimes_2$ są dwoma różnymi produktami tensorowymi to na mocy własności definicyjnej istnieją jedyne odwzorowania liniowe ϕ_1 i ϕ_2 takie że

$$m \otimes_2 n = \phi_1(m \otimes_1 n)$$

i

$$m \otimes_1 n = \phi_2(m \otimes_2 n)$$

Wtedy

$$m \otimes_1 n = \phi_2(\phi_1(m \otimes_1 n)).$$

Lecz na mocy definicji istnieje dokładnie jedno odwzorowanie liniowe mające własność wyżej czyli $\phi_2\phi_1$ to identyczność. Podobnie $\phi_1\phi_2$ to identyczność, czyli V_1 jest izomorficzne z V_2.

Lemat 13.1 *Produkt tensorowy istnieje.*

Dowód. Niech H będzie modułem wolnym z bazą $M \times N$. By oznaczenia były bardziej sugestywne zamiast (m, n) będziemy pisać $m \otimes n$. W module H definiujemy podmoduł I jako podmoduł generowany przez elementy następujących postaci:

$$(a_1m_1 + a_2m_2) \otimes n - a_1m_1 \otimes n - a_2m_2 \otimes n$$

$$m \otimes (a_1n_1 + a_2n_2) - a_1m \otimes n_1 - a_1m \otimes n_2$$

i przyjmujemy $M \otimes N = H/I$. Operacje $\otimes$ definiujemy jako klasę $m \otimes n = (m, n)$ w module ilorazowym H/I. Łatwo sprawdzić że $\otimes$ jest operacją dwuliniową: wydzielenie przez podmoduł I zapewnia potrzebne równości. Jeśli W jest modułem z definicji iloczynu tensorowego zaś η jest operacją dwuliniową z $M \times N$ w W to definiujemy ϕ w ten sposób że

$$\phi(m \otimes n) = \eta(m, n)$$

Aby ϕ było dobrze zdefiniowane musimy sprawdzić że ϕ znika na I. Lecz to wynika z dwuliniowości η. Zauważmy że powyższa definicja ϕ jest wymuszona przez definicję iloczynu tensorowego, skąd wynika że ϕ jest wyznaczone jednoznacznie. □

14 Własności iloczynu tensorowego

Lemat 14.1 *Jeśli M, N, K są R-modułami to $M \otimes N$ jest izomorficzne z $N \otimes M$, $(M \otimes N) \otimes K$ jest izomorficzne z $M \otimes (N \otimes K)$. Jeśli $M = M_1 \oplus M_2$ i $N = N_1 \oplus N_2$ to $M \otimes N$ jest izomorficzne z $(M_1 \otimes N) \oplus (M_2 \otimes N)$ i $M \otimes N$ jest izomorficzne z $(M \otimes N_1) \oplus (M \otimes N_2)$.*

Dowód. Wynika to używając własność definicyjną. Np. dla $(M_1 \otimes N) \oplus (M_2 \otimes N)$ mamy operacje $\otimes_i$ z $M_i \times N$ w $M_i \otimes N$ i jest spełniona własność produktu tensorowego dla $M_i \times N$. Pokażemy że $(M_1 \otimes N) \oplus (M_2 \otimes N)$ spełnia własność produktu tensorowego. Operację $\otimes$ definiujemy wzorem

$$(m_1 \oplus m_2) \otimes n = (m_1 \otimes_1 n) \oplus (m_2 \otimes_2 n).$$

Rozważamy teraz operację dwuliniową η z $M \times N$ w W. Ograniczenie η do $M_1 \times N$ daje operację η_1 z $M_1 \times N$ w W. Podobnie ograniczenie η do $M_2 \times N$ daje operację η_2 z $M_2 \times N$ w W. Z własności iloczynu tensorowego dla $M_i \otimes N$ istnieją ϕ_i takie że

$$\eta_i(m, n) = \phi_i(m \otimes_i n)$$

dla $m \in M_i$ i $n \in N$. Wtedy definiując ϕ wzorem

$$\phi(t_1 \oplus t_2) = \phi_1(t_1) + \phi_2(t_2)$$

gdzie $t_i \in M_i \otimes N$ mamy

$$\eta(m_1 \oplus m_2, n) = \eta_1(m_1, n) + \eta_2(m_2, n) = \phi_1(m_1 \otimes_1 n) + \phi_2(m_2 \otimes_2 n)$$

$$= \phi((m_1 \otimes_1 n) \oplus (m_2 \otimes_2 n)) = \phi((m_1 \oplus m_2) \otimes n)$$

gdzie ostatnia równość to definicja $\otimes$ z $M \times N$ w $(M_1 \otimes N) \oplus (M_2 \otimes N)$. A więc dla $(M_1 \otimes N) \oplus (M_2 \otimes N)$ z powyżej zdefiniowanym $\otimes$ spełniona jest własność iloczynu tensorowego, czyli mamy izomorfizm z $M \otimes N$. Pozostałe izomorfizmy mają podobne dowody, więc je pominiemy. □

Lemat 14.2 *Jeśli $M = \oplus_\alpha M_\alpha$ to $M \otimes N$ jest izomorficzny z $\oplus_\alpha (M_\alpha \otimes N)$. Jeśli $N = \oplus_\alpha N_\alpha$ to $M \otimes N$ jest izomorficzny z $\oplus_\alpha (M \otimes N_\alpha)$.*

Dowód jest podobny do poprzedniego.

Lemat 14.3 *$M \otimes R$ jest izomorficzne z M. Podobnie $R \otimes M$ jest izomorficzne z M.*

Dowód: Operację $\otimes$ z $M \times R$ w M definiuję wzorem $m \otimes a = am$. Niech η będzie operacją dwuliniową z $M \times R$ w W i niech $\phi(m) = \eta(m, 1)$. Oczywiście ϕ jest operacją liniową. Mam

$$\eta(m, a) = \eta(am, 1) = \phi(am) = \phi(m \otimes a)$$

czyli jest spełniona własność iloczynu tensorowego. □

Lemat 14.4 *Jeśli M jest modułem wolnym z bazą $\{e_\alpha\}$ zaś N jest modułem wolnym z bazą $\{f_\beta\}$ to $M \otimes N$ jest modułem wolnym z bazą $\{e_\alpha \otimes f_\beta\}$*

Dowód: jest to bezpośredni wniosek z lematów 14.2 i 14.3. □

Wniosek: Jeśli R to ciało to $\dim(M \otimes N) = \dim(M)\dim(N)$.

Przykład: Jeśli $R = \mathbb{Z}$, zaś p i q to względnie pierwsze liczby całkowite dodatnie to $R/(pR) \otimes R/(qR)$ to moduł zerowy. Mianowicie skoro p i q są względnie pierwsze to istnieją liczby całkowite a i b takie że $1 = ap + bq$. Teraz dla $u \otimes v \in R/(pR) \otimes R/(qR)$ mamy

$$u \otimes v = (ap + bq)(u \otimes v) = ap(u \otimes v) + bq(u \otimes v)$$

$$= a(pu \otimes v) + b(u \otimes qv).$$

Lecz $pu = 0$ w $R/(pR)$ i $qv = 0$ w $R/(qR)$ czyli powyższy element to 0. Jako że elementy postaci $u \otimes v$ generują $R/(pR) \otimes R/(qR)$ to produkt tensorowy jest zerowy.

Lemat 14.5 *Jeśli dla $i = 1, 2$ M_i, N_i są R-modułami, zaś $\phi_i : M_i \to N_i$ są homomorfizmami to istnieje dokładnie jeden homomorfizm $\phi : (M_1 \otimes M_2) \to (N_1 \otimes N_2)$ taki że*

$$\phi(m_1 \otimes m_2) = \phi_1(m_1) \otimes \phi_2(m_2)$$

Dowód: $\phi_1(m_1) \otimes \phi_2(m_2)$ jest odwzorowaniem dwuliniowym z $M_1 \times M_2$ w $N_1 \otimes N_2$ a więc ϕ istnieje i jest jednoznaczne z własności definicyjnej iloczynu tensorowego $M_1 \otimes M_2$. □

W dalszym ciągu odwzorowanie ϕ wyżej będziemy oznaczać przez $\phi_1 \otimes \phi_2$.

Lemat 14.6 *Jeśli dla $i = 1, 2$ M_i, N_i, V_i są R-modułami, zaś $\phi_i : M_i \to N_i$ i $\psi_i : N_i \to V_i$ są homomorfizmami to*

$$(\psi_1 \otimes \psi_2)(\phi_1 \otimes \phi_2) = (\psi_1\phi_1) \otimes (\psi_2\phi_2)$$

Dowód: Bezpośrednie sprawdzenie z własności definicyjnej. □

Lemat 14.7 *Jeśli M_i, N_i wyżej są skończenie wymiarowymi przestrzeniami wektorowymi nad ciałem k i $M_i = N_i$ to*

$$\mathrm{Tr}(\phi_1 \otimes \phi_2) = \mathrm{Tr}(\phi_1)\mathrm{Tr}(\phi_2)$$

Dowód. Niech $\{e_i\}$ będzie bazą M_1, $\{f_j\}$ bazą M_2 zaś $\{e_i^*\}$ i $\{f_j^*\}$ będą bazami dualnymi. Wtedy $\{e_i^* \otimes f_j^*\}$ jest bazą $M_1^* \otimes M_2^*$ dualną do $\{e_i \otimes f_j\}$. Mamy

$$\mathrm{Tr}(\phi_1 \otimes \phi_2) = \sum_{i,j} \langle (\phi_1 \otimes \phi_2)(e_i \otimes f_j), e_i^* \otimes f_j^* \rangle = \sum_{i,j} \langle (\phi_1(e_i) \otimes \phi_2(f_1), e_i^* \otimes f_j^* \rangle$$

$$= \sum_{i,j} \langle \phi_1(e_i), e_i^* \rangle \langle \phi_2(f_j), f_j^* \rangle = \left(\sum_i \langle \phi_1(e_i), e_i^* \rangle \right) \left(\sum_j \langle \phi_2(f_j), f_j^* \rangle \right)$$

$$= \mathrm{Tr}(\phi_1)\mathrm{Tr}(\phi_2).$$

□

15 Produkt tensorowy reprezentacji

Jeśli R i S są algebrami nad k to na $R \otimes_k S$ (gdzie $\otimes_k$ oznacza że produkt tensorowy liczymy biorąc k jako pierścień) można wprowadzić strukturę pierścienia wzorem

$$(r_1 \otimes_k s_1)(r_2 \otimes_k s_2) = (r_1 r_2) \otimes_k (s_1 s_2)$$

Własność produktu tensorowego pozwala pokazać że tak określone mnożenie jednoznacznie rozszerza się na $R \otimes_k S$ i spełnia aksjomaty mnożenia w pierścieniu.

Lemat 15.1 *Jeśli G i H są grupami to $k[G] \otimes_k k[H]$ jest izomorficzne z $k[G \times H]$.*

Dowód: Elementy δ_g, $g \in G$ dają bazę $k[G]$, elementy δ_h, $h \in H$ dają bazę $k[H]$, zaś elementy δ_{gh}, $g \in G, h \in H$ dają bazę w $k[G \times H]$. Na mocy wcześniejszego lematu $\delta_g \otimes \delta_h$ daje bazę $k[G] \otimes_k k[H]$. A więc przyporządkowanie

$$\delta_g \otimes \delta_h \mapsto \delta_{gh}$$

daje izomorfizm $k[G] \otimes_k k[H]$ z $k[G \times H]$ jako przestrzeni liniowych. Trzeba sprawdzić że zachowuje się mnożenie. Lecz

$$(\delta_{g_1} \otimes \delta_{h_1})(\delta_{g_2} \otimes \delta_{h_2}) = \delta_{g_1 g_2} \otimes \delta_{h_1 h_2}$$

i w $G \times H$ mamy $(g_1 h_1)(g_2 h_2) = (g_1 g_2)(h_1 h_2)$ czyli faktycznie mnożenie jest zachowane. □

Jeśli M jest R-modułem zaś N jest S-modułem to na $M \otimes_k N$ mamy naturalną strukturę $R \otimes_k S$-modułu:

$$(r \otimes s)(m \otimes n) = rm \otimes sn.$$

Lemat 15.2 *Niech ciało k będzie algebraicznie domknięte, R będzie skończenie wymiarową algebrą nad k zaś M prostym R-modułem. Jeśli V jest niezerowym podmodułem w $M \oplus M$ to albo $V = M \oplus M$ albo $V = \{0\} \oplus M$ albo istnieje $a \in k$ takie że V to zbiór elementów postaci $v \oplus av$ gdzie $v \in M$.*

Dowód: Rozważmy rzut z V na pierwszy składnik sumy prostej. Jako że M jest modułem prostym to obraz to moduł zerowy albo całe M. Jeśli obraz to moduł zerowy to V jest zawarte w $\{0\} \oplus M$ które jest izomorficzne z M. Czyli V jako niezerowy podmoduł modułu prostego $\{0\} \oplus M$ jest równe $\{0\} \oplus M$. A więc pozostaje rozpatrzeć przypadek gdy obraz V przez rzut na pierwszy składnik sumy to M, czyli dla każdego $v_1 \in M$ istnieje $v_2 \in M$ takie że $v_1 \oplus v_2 \in V$. Przy ustalonym $v_1 \oplus v_2 \in V$ elementy $w \in M$ takie że $v_1 \oplus (w + v_2) \in V$ tworzą podmoduł H w M. Zauważmy że H nie zależy od v_1, bo $w \in H$ wtedy i tylko wtedy gdy $0 \oplus w \in V$. Jeśli H to całe M to $V = M \oplus M$. A więc pozostaje rozpatrzeć przypadek gdy H to moduł zerowy. Wtedy V jest wykresem odwzorowania liniowego z M w M. Na mocy lematu Schura takie odwzorowanie to mnożenie przez element $a \in k$ (to jest jedyne miejsce gdzie w tym lemacie używamy skończoność wymiaru M i algebraiczną domkniętość k). Czyli elementy V są postaci $v \oplus av$. □

Lemat 15.3 *Jeśli k jest algebraicznie domknięte, M jest prostym R-modułem który ma skończony wymiar nad k zaś N jest prostym S-modułem to $M \otimes_k N$ jest prostym $R \otimes_k S$-modułem.*

Dowód: Niech V będzie podmodułem $M \otimes_k N$. Ustalmy bazę $\{f_\alpha\}$ przestrzeni N nad k. Wtedy V zawiera element v postaci

$$\sum m_\alpha \otimes f_\alpha$$

Jeśli wszystkie m_α są proporcjonalne nad k tzn. jeśli istnieje m i a_α takie że $m_\alpha = a_\alpha m$ to mogę napisać

$$v = \sum m_\alpha \otimes f_\alpha = \sum a_\alpha m \otimes f_\alpha = \sum m \otimes a_\alpha f_\alpha = m \otimes n$$

gdzie $n = \sum a_\alpha f_\alpha$. Jako że M i N są modułami prostymi to podmoduł nad R generowany przez m to całe M, podmoduł nad S generowany przez n to całe N czyli podmoduł nad $R \otimes_k S$ generowany przez $m \otimes n$ to całe $M \otimes_k N$. Jeśli istnieją α i β takie że m_α i m_β nie są proporcjonalne nad k to na mocy poprzedniego lematu podmoduł nad R generowany przez $m_\alpha \oplus m_\beta$ to $M \oplus M$ i w szczególności zawiera element postaci $0 \oplus m$. Wtedy biorąc odpowiednią kombinację liniową v dostanę niezerowy element z mniejszą ilością składników w sumie. A więc indukcyjnie dostanę w V element postaci $m \otimes n$. □

Jeśli G jest grupą zaś M i N są $k[G]$ modułami to na $M \otimes_k N$ (gdzie $\otimes_k$ oznacza że produkt tensorowy liczymy biorąc k jako pierścień) można w naturalny sposób wprowadzić strukturę $k[G]$ modułu. Mianowicie niech $\lambda(g)$ oznacza operator mnożenia przez δ_g w M zaś $\eta(g)$ oznacza operator mnożenia przez δ_g w N. Wtedy przyporządkowanie

$$g \mapsto \lambda(g) \otimes \eta(g)$$

zadaje reprezentację G na $M \otimes_k N$, czyli zadaje strukturę $k[G]$-modułu.

Lemat 15.4 *Jeśli dla $i = 1, 2$ λ_i są reprezentacjami G nad k zaś χ_i są odpowiednimi charakterami to $\chi(g) = \chi_1(g)\chi_2(g)$ jest charakterem dla $\lambda_1 \otimes \lambda_2$. Podobnie $\chi(g) = \chi_1(g) + \chi_2(g)$ jest charakterem dla $\lambda_1 \oplus \lambda_2$.*

Dowód: Mamy

$$\chi(g) = \mathrm{Tr}(\lambda_1 \otimes \lambda_2(g)) = \mathrm{Tr}(\lambda_1(g))\mathrm{Tr}(\lambda_2(g)) = \chi_1(g)\chi_2(g)$$

Dla sumy jest podobnie. □

Z lematu wynika że charaktery tworzą półpierścień. Niekiedy wygodnie jest rozszerzyć ten półpierścień do pierścienia, tzn. rozpatrzeć moduł nad $\mathbb{Z}$ generowany przez charaktery modułów prostych z naturalnym mnożeniem.

Produkt tensorowy reprezentacji często jest rozkładalny. W szczególności w $M \otimes M$ podmoduł generowany przez elementy postaci $v \otimes v$ (oznaczany przez $S^2(M)$) jest niezmienniczy na działanie G. Podobnie $(M \otimes M)/S^2(M)$ (oznaczane przez $\Lambda^2(M)$) jest izomorficzne z podmodułem $(M \otimes M)$.

Bez dowodu podamy

Lemat 15.5 *Jeśli χ jest charakterem M, η jest charakterem $S^2(M)$ zaś ϕ jest charakterem $\Lambda^2(M)$ to*

$$\eta(g) = (\chi(g)^2 + \chi(g^2))/2$$
$$\phi(g) = (\chi(g)^2 - \chi(g^2))/2$$

16 Reprezentacje indukowane

16.1 Iloczyn tensorowy nad pierścieniem nieprzemiennym

Dotychczas rozpatrywaliśmy produkty tensorowe nad pierścieniem przemiennym. Było to spowodowane tym że zwykła definicja odwzorowania dwuliniowego prowadzi do warunku typu przemienności na pierścień. Nad pierścieniem nieprzemiennym potrzebujemy słabszy warunek. Po pierwsze rozważamy prawy R-moduł M i lewy R-moduł N. Bez dodatkowych założeń nad pierścieniem nieprzemiennym $M \otimes N$ jest tylko grupą abelową. Powiemy że odwzorowanie η z $M \times N$ w grupę abelową W jest prawie dwuliniowe jeśli spełnia następujące warunki:

- η jest addytywne ze względu na pierwszy argument
- η jest addytywne ze względu na drugi argument
- $\eta(ma, n) = \eta(m, an)$

Powiemy że para grupa abelowa V i odwzorowanie prawie dwuliniowe $\otimes$ z $M \times N$ w V jest iloczynem tensorowym M i N wtedy i tylko wtedy gdy dla dowolnego odwzorowania prawie dwuliniowego η z $M \times N$ w grupę abelową W istnieje dokładnie jeden homomorfizm grup abelowych ϕ taki że

$$\eta(m, n) = \phi(m \otimes n)$$

Tak jak w przypadku pierścienia przemiennego pokazujemy że tak określony iloczyn tensorowy jest wyznaczony jednoznacznie z dokładnością do izomorfizmu grup abelowych.

Lemat 16.1 *Wyżej określony iloczyn tensorowy istnieje.*

Dowód: Grupa abelowa to moduł nad $\mathbb{Z}$. Niech $H = N \otimes_{\mathbb{Z}} N$ gdzie $\mathbb{Z}$ traktujemy jako podpierścień R generowany przez 1. Miech I będzie podgrupą W generowaną przez elementy postaci $(ma) \otimes n - m \otimes (an)$ gdzie $m \in M$, $n \in N$, $a \in R$. Bierzemy $V = H/I$. Łatwo sprawdzić że $\otimes$ jako operacja z $M \times N$ w V jest prawie dwuliniowe. Jak poprzednio, dla prawie dwuliniowego η definiuję ϕ wzorem

$$\phi(m \otimes n) = \eta(m, n).$$

Jako że η jest prawie dwuliniowe to ϕ znika na I, czyli mamy dobrze zdefiniowany homomorfizm grup abelowych z V w W. Określenie ϕ jest wymuszone przez definicję iloczynu tensorowego czyli ϕ jest wyznaczone jednoznacznie. □

Jeśli M jest dodatkowo lewym modułem nad pierścieniem S to na $M \otimes N$ można wprowadzić strukturę lewego S modułu wzorem

$$s(m \otimes n) = (sm) \otimes n.$$

Podobnie jeśli N jest dodatkowo prawym modułem nad pierścieniem S to na $M \otimes N$ można wprowadzić strukturę prawego S modułu wzorem

$$(m \otimes n)s = m \otimes (ns).$$

Lemat 16.2 *Jeśli M jest prawym S modułem, N jest lewym S modułem i prawym R-modułem zaś V jest lewym R-modułem to $(M \otimes_S N) \otimes_R V$ jest izomorficzne z $M \otimes_S (N \otimes_R V)$.*

Dowód: Przez własność definicyjną. □

Jeśli pierścień R jest przemienny to lewy R-moduł można traktować jako prawy R moduł i odwrotnie. Wtedy nasza konstrukcja produktu tensorowego nad R daje R moduł i można sprawdzić że $\otimes$ jest dwuliniowe. Podobnie dla dwuliniowego η również ϕ będzie dwuliniowe. A więc w przypadku pierścienia przemiennego nowa definicja daje ten sam wynik co stara. Ogólniej, jeśli R zawiera w centrum pierścień przemienny S (czyli R jest algebrą nad S) to w konstrukcji wyżej możemy zastąpić $\mathbb{Z}$ przez S: jako moduł H bierzemy $M \otimes_S N$, I definiujemy jak poprzednio ale teraz jest modułem nad S i $V = H/I$. Tak zbudowane V spełnia warunek definicyjny iloczynu tensorowego czyli jest izomorficzne z iloczynem tensorowym.

Gdy $M = S$ zaś R jest podpierścieniem S to M ma naturalną strukturę lewego i prawego S-modułu czyli też prawego R-modułu. W takim przypadku powyższa konstrukcja jest nazywana rozszerzeniem skalarów z R do S. Mianowicie, z R-modułu N dostajemy S moduł $S \otimes_R N$.

16.2 Definicja i własności reprezentacji indukowanej

W kontekście teorii reprezentacji, gdy H jest podgrupą G to $k[H]$ jest podpierścieniem $k[G]$ i moduł otrzymany przez rozszerzanie skalarów z $k[H]$ do $k[G]$ nazywamy modułem indukowanym (lub reprezentacją indukowaną).

Lemat 16.3 *(Indukcja etapami) Jeśli U jest podgrupą H, H jest podgrupą G zaś M jest $k[U]$ modułem to $k[G] \otimes_{k[U]} M$ jest izomorficzne z $k[G] \otimes_{k[H]} (k[H] \otimes_{k[U]} M)$.*

Dowód: $k[G] \otimes_{k[H]} k[H]$ jest izomorficzne z $k[G]$ zaś reszta wynika z łączności iloczynu tensorowego. □

Podamy teraz bardziej konkretną konstrukcję reprezentacji indukowanej. w przypadku gdy podgrupa H grupy G jest skończona. Niech M będzie $k[H]$ modułem czyli reprezentacją H. Niech W będzie przestrzenią funkcji na G o wartościach w M takich że są niezerowe tylko dla skończenie wielu g zaś V będzie podprzestrzenią W funkcji na G spełniających warunek

$$v(gh^{-1}) = \delta_h v(g)$$

gdzie mnożenie przez δ_h to działanie reprezentacji.

Można sprawdzić że V jest podprzestrzenią dopełniczą do I (tu istotne jest że H jest skończone) gdzie I jest podprzestrzenią W generowaną przez elementy których wartość w g jest dana wzorem

$$w(gh^{-1}) - \delta_h w(g)$$

gdzie $w \in W$ jest dowolny.

Zauważmy teraz że W jest izomorficzne z $k[G] \otimes_k M$ zaś I jest podmodułem z konstrukcji iloczynu tensorowego. Dokładniej, w $k[G]$ mamy

$$\delta_g \delta_s = \delta_{gs}$$

co daje

$$(v\delta_s)(g) = v(gs^{-1})$$

A więc rzeczywiście I to podprzestrzeń z definicji iloczynu tensorowego. Teraz V jest izomorficzne z W/I, czyli faktycznie V daje nam iloczyn tensorowy $K[G] \otimes_{k[S]} M$. Podobnie jak dla I sprawdzamy że

$$(\delta_g v)(h) = v(g^{-1}h)$$

co daje jawnie działanie G w przestrzeni reprezentacji indukowanej.

Ogólniej, jako V można wziąść przestrzeń funkcji na G o wartościach w M które są niezerowe tylko na skończenie wielu warstwach gH.

Druga konstrukcja reprezentacji indukowanej pozwala pokazać że ma ona dodatkową własność. Mianowicie, rozważmy podział G na warstwy lewostronne względem podgrupy S. Przestrzeń warstw oznaczamy przez G/S. Wtedy jeśli $\sigma_1, \sigma_2 \in G/S$, przy ustalonym $g \in G$ dla pewnego $u \in \sigma_1$ mamy $gu \in \sigma_2$ to dla dowolnego $u \in \sigma_1$ mamy $gu \in \sigma_2$. A więc biorąc jako V_σ podprzestrzeń V składającą się z funkcji które są zerem poza warstwą σ mamy $\delta(g)V_{\sigma_1} = V_{\sigma_2}$. Innymi słowy G permutuje przestrzenie V_σ. Ponadto

$$V = \oplus_\sigma V_\sigma.$$

Dodatkowo, warunek nałożony na V oznacza że reprezentacja S w przestrzeni V_e jest równoważna z wyjściową reprezentacją M.

Lemat 16.4 *Niech będzie dana reprezentacja λ grupy G na W, $W = \oplus_\sigma W_\sigma$ i G tranzytywnie permutuje przestrzenie W_σ. Ustalmy pewne σ_0 i niech*

$$S = \{g \in G : \delta_g W_{\sigma_0} = W_{\sigma_0}\}.$$

Wtedy reprezentacja na W jest izomorficzna z reprezentacją indukowaną z reprezentacji S na W_{σ_0}.

Dowód: Zauważmy że ponieważ G tranzytywnie permutuje przestrzenie W_σ to zbiór σ można utożsamić ze zbiorem warstw lewostronnych G/S. Oznaczmy przez η działanie reprezentacji indukowanej na V. Zdefiniujemy odwzorowanie liniowe ϕ z W do V. Robimy to dla każdej podprzestrzeni W_σ z osobna. Niech $u \in \sigma$. Bierzemy

$$\phi(x) = \eta(u)\lambda(u^{-1})x$$

dla $x \in W_\sigma$. Ten wzór ma sens bo $\lambda(u^{-1})x \in W_e = V_e$. Widać że $\phi(x) \in V_\sigma$. Jeśli us jest innym elementem σ to

$$\eta(us)\lambda((us)^{-1}) = \eta(u)\eta(s)\lambda(s^{-1})\lambda(u^{-1})$$

Lecz na $W_e = V_e$ dla $s \in S$ działania η i λ są równe, czyli $\eta(s)\lambda(s^{-1})$ to identyczność i wartość ϕ nie zależy od wyboru u. Jeśli $g \in G$ to biorąc gu jako reprezentant $g\sigma$ mam

$$\phi(\lambda(g)x) = \eta(gu)\lambda((gu)^{-1})\lambda(g)x = \eta(g)\eta(u)\lambda(u^{-1})\lambda(g^{-1})\lambda(g)x$$

$$= \eta(g)\eta(u)\lambda(u^{-1})x = \eta(g)\phi(x)$$

czyli ϕ zadaje homomorfizm reprezentacji (operator splatający). Lecz z określenia widać że ϕ na każdym W_σ jest izomorfizmem przestrzeni liniowych czyli skoro W i V są sumami prostymi to ϕ jest izomorfizmem przestrzeni liniowych. czyli jest izomorfizmem (równoważnością) reprezentacji. □

Lemat 16.5 *Niech N będzie abelowym dzielnikiem normalnym w G. Niech χ będzie charakterm N. Niech M oznacza podgrupę G składającą się z elementów takich że $\chi(g^{-1}ng) = \chi(n)$ dla wszystkich $n \in N$. Wtedy χ rozszerza się do charakteru M który również ozanczymy przez χ. Niech θ będzie reprezentacją nieprzywiedlną M trywialną na N. Wtedy reprezentacja indukowana z produktu tensorowego $\chi \otimes \theta$ (który tu redukuje się do zwykłego mnożenia) jest nieprzywiedlna. Ponadto każda reprezentacja nieprzywiedlna G jest takiej postaci.*

Dowód zostawiam jako ćwiczenie.

Lemat 16.6 *Jeśli R jest zbiorem reprezentantów G/S, χ jest charakterem reprezentacji S na M rozszerzonym przez 0 na G, zaś η jest charakterem reprezentacji indukowanej to*

$$\eta(g) = \sum_{r\in R} \chi(r^{-1}gr) = \frac{1}{|S|}\sum_{u\in G} \chi(u^{-1}gu)$$

Dowód: Niech $V = \oplus\delta_r M$ będzie przestrzenią reprezentacji indukowanej. Zauważmy że albo $\delta_g\delta_r M = \delta_r M$ albo $\delta_g\delta_r M \cap \delta_r M = \{0\}$. W drugim przypadku podprzestrzeń $\delta_r M$ daje zerowy wkład do śladu. W pierwszym mamy

$$\mathrm{Tr}(\delta_g)|_{\delta_r M} = \mathrm{Tr}(\delta_{r^{-1}}\delta_g\delta_r)|_M = \mathrm{Tr}(\delta_{r^{-1}gr})|_M = \chi(r^{-1}gr).$$

Przy tym w pierwszym przypadku $r^{-1}gr \in S$, w drugim $r^{-1}gr \notin S$, czyli $\chi(r^{-1}gr) = 0$. A więc

$$\eta(g) = \mathrm{Tr}(\delta_g) = \sum_{r:r^{-1}gr\in S} \mathrm{Tr}(\delta_g)|_{\delta_r M} = \sum_{r:r^{-1}gr\in S} \chi(r^{-1}gr) = \sum_r \chi(r^{-1}gr)$$

co daje pierwszą równość. Druga wynika z pierwszej zapisując elementy $u \in G$ w postaci $u = rs$ i sumując najpierw po s:

$$\sum_u \chi(u^{-1}gu) = \sum_r\sum_s \chi(s^{-1}r^{-1}grs) = \sum_r\sum_s \chi(r^{-1}gr) = |S|\sum_r \chi(r^{-1}gr).$$

□

17 Reprezentacje indukowane a charaktery

Funkcję ϕ na G nazywamy centralną jeśli dla dowolnego $u \in G$ mamy $\phi(g) = \phi(u^{-1}gu)$. Jak pokazaliśmy wcześniej charaktery są funkcjami centralnymi.

Niech S będzie podgrupą grupy skończonej G. Dla funkcji centralnej ϕ na S oznaczymy przez $\mathrm{Ind}(\phi)$ (lub $\mathrm{Ind}_S^G(\phi)$ jeśli trzeba zaznaczyć grupy) funkcję zadaną wzorem

$$\mathrm{Ind}(\phi)(g) = \sum_{r\in R} \chi(r^{-1}gr) = \frac{1}{|S|}\sum_{s\in G} \chi(s^{-1}gs)$$

gdzie R jest zbiorem reprezentantów dla G/S. Jako że ϕ jest funkcją centralną $\chi(r^{-1}gr)$ nie zależy od wyboru reprezentanta r dla warstwy lewostronnej, czyli $\mathrm{Ind}(\phi)$ jest dobrze zdefiniowane. Ponadto $\mathrm{Ind}(\phi)$ jest funkcją centralną: dla $u \in G$ zbiór $\{ur : r \in R\}$ jest też zbiorem reprezentantów dla warstw, więc

$$\mathrm{Ind}(\phi)(u^{-1}gu) = \sum_{r\in R} \chi(r^{-1}u^{-1}gur) = \sum_{r\in R} \chi((ur)^{-1}g(ur))$$

$$= \sum_{r\in R} \chi(r^{-1}gr) = \mathrm{Ind}(\phi)(g).$$

Definiujemy również operację Res która jest ograniczeniem funkcji z G do S, tzn. dla ϕ będącego funkcją na G funkcja $\mathrm{Res}(\phi)$ jest funkcją na S i dla $s \in S$ mamy $\phi(s) = \mathrm{Res}(\phi)$.

Lemat 17.1 *(Prawo wzajemności Frobeniusa) Jeśli ψ jest funkcją centralną na S zaś ϕ jest funkcją centralną na G to*

$$\langle \psi, \mathrm{Res}(\phi)\rangle = \langle \mathrm{Ind}(\psi), \phi\rangle$$

Oznaczmy przez $R(G)$ pierścień z mnożeniem punktowym generowany przez charaktery. Elementy $R(G)$ nazywamy charakterami wirtualnymi.

Lemat 17.2 *(Twierdzenia Artina) Każdy element $\phi \in R(G)$ jest wymierną kombinacją liniową charakterów indukowanych z podgrup cyklicznych. Dokładniej, $|G|\phi$ jest całkowitą kombinacją liniową charakterów indukowanych z podgrup cyklicznych.*

Dowód: Pokażemy to w kilku krokach.

Krok 1: Wystarczy pokazać wynik dla charakteru trywialnego. Mianowicie, zakładając że

$$|G|1 = \sum k_i \mathrm{Ind}(\chi_i)$$

mamy

$$|G|\psi = |G| \cdot 1 \cdot \psi = \sum k_i \psi \mathrm{Ind}(\chi_i) = \sum k_i \mathrm{Ind}(\mathrm{Res}(\psi)\chi_i))$$

$\mathrm{Res}(\psi)\chi_i$ jako produkt charakterów jest charakterem. Charaktery grupy cyklicznej można przedstawić jako sumę charakterów jednowymiarowych, czyli

$$\mathrm{Res}(\psi)\chi_i = \sum_j l_j \chi_j$$

co oznacza że ψ jest sumą charakterów indukowanych z charakterów podgrup cyklicznych. A więc wystarczy pokazać że $|G|$ jest całkowitoliczbową kombinacją liniową charakterów indukowanych z charakterów podgrup cyklicznych.

Krok 2. Niech $g \in G$. Niech C będzie grupę cykliczną generowaną przez g. Niech $\alpha_C(u) = 1$ dla u będących generatorem C i $\alpha_C(u) = 0$ poza tym. Niech N_C będzie normalizatorem C, tzn. $N_C = \{s \in G : s^{-1}Cs \subset C\}$. Dla $s \notin N_C$ mamy $s^{-1}gs \notin C$ czyli $\alpha_C(s^{-1}gs) = 0$, zaś dla $s \in N_C$ element $s^{-1}gs$ jest generatorem C, czyli $\alpha_C(s^{-1}gs) = 1$. A więc

$$\mathrm{Ind}(\alpha_C)(g) = \frac{1}{|C|}\sum_{s\in G}\alpha_C(s^{-1}gs) = \frac{1}{|C_g|}\sum_{s\in N_g}\alpha_C(s^{-1}gs) = \frac{|N_C|}{|C|}$$

czyli dla u w sprzężonych z generatorem C mamy

$$\frac{|G||C|}{|N_C|}\mathrm{Ind}(\alpha_C)(u) = |G|$$

zaś dla pozostałych u mamy $\mathrm{Ind}(\alpha_C)(u) = 0$. Niech U będzie zbiorem reprezentantów klas sprzężoności podgrup cyklicznych G. Wtedy dla każdego $u \in G$

$$\sum_{C\in U}\frac{|G||C|}{|N_C|}\mathrm{Ind}(\alpha_C)(u) = |G|.$$

Mianowicie, u generuje dokładnie jedną podgrupę cykliczną i ta podgrupa jest sprzężona z dokładnie jednym elementem U, a więc przy ustalonym u w sumie wyżej dokładnie jeden składnik jest niezerowy. Oczywiście $|G||C|/|N_C|$ jest liczbą całkowitą.

Krok 3. Na mocy poprzedniego kroku wystarczy pokazać że α_C jest kombinacją liniową z całkowitoliczbowymi współczynnikami charakterów podgrup (siłą rzeczy cyklicznych) C. Jeśli $|C| = l$ i l można zapisać jako produkt $l = km$ z względnie pierwszymi k i m, to $C = C_1 \times C_2$ jest produktem grup, $C_1 = k$, $C_2 = m$. Mamy $\alpha_C = \tilde{\alpha}_{C_1}\tilde{\alpha}_{C_2}$ gdzie $\tilde{\alpha}_{C_i}$ jest rozszerzeniem α_{C_i} na produkt zgodnie ze wzorem $\tilde{\alpha}_{C_i}(g_1, g_2) = \alpha_{C_i}(g_i)$. W podobny sposób można rozszerzać charaktery. Indukcyjnie możemy zakładać że wynik jest prawdziwy dla mniejszych grup cyklicznych, czyli że zachodzi dla C_i. Wtedy α_{C_i} jest kombinacją charakterów, rozszerzenie charakterów do produktu oznacza że również $\tilde{\alpha}_{C_i}$ jest kombinacją charakterów i w końcu α_C jako produkt jest kombinacją charakterów.

Krok 4. Teraz wystarcza rozważać C z mocą postaci p^k gdzie p jest liczbą pierwszą. Elementy C nie będące generatorami tworzą podgrupę H mocy p^{k-1}. A więc α_C jest różnicą charakteru trywialnego C i charakteru trywialnego H.

□

Komentarz: Powyżej wystarczy wziąść tylko maksymalne podgrupy cykliczne. Ponadto wystarczy wziąść tylko jeden reprezentant w klasie sprzężoności podgrup cyklicznych. Dla grupy $SL(2,q)$ oznacza to że wystarczą trzy albo cztery podgrupy: podgrupa macierzy diagonalnych, podgrupa mocy $q+1$ składająca się z macierzy diagonalizujących się nad $F(q^2)$ i jedna lub dwie podgrupy generowane przez elementy typu $-N$ (jeśli każdy element $F(p)$ jest kwadratem w $F(q)$ to potrzebne są dwie podgrupy, w przeciwnym razie wystarcza jedna). Bezpośredni rachunek pokazuje że faktycznie wystarczy jedna podgrupa typu $-N$. Przy tym dla q będącego potęgą otrzymuje się wielokrotności charakterów indukowanych z $\tilde{N}$. Jako że charaktery odpowiednich reprezentacji nieprzywiedlnych nie pojawiają się w innych reprezentacjach to widać że potrzeba dzielenia by otrzymać wszystkie charaktery. Patrząc na charaktery indukowane z podgrupy mocy $q+1$ widać że potrzebne jest odejmowanie by otrzymać charaktery nieprzywiedlne.

Lemat 17.3 *Charaktery grupy $S(n)$ permutacji zbioru n-elementowego przyjmują wartości całkowite wymierne.*

Dowód: Charaktery przyjmują wartości będące całkowitymi liczbami algebraicznymi. A więc trzeba pokazać że wartości są wymierne (całkowita liczba algebraiczna która jest wymierna jest liczbą całkowitą). Na mocy twierdzenia Artina wystarczy pokazać że charaktery indukowane z podgrup cyklicznych są wymierne. Pokażemy to w kilku krokach.

Krok 1. Jeśli g jest generatorem podgrupy cyklicznej i ma więcej niż jeden cykl w rozkładzie na cykle rozłączne możemy użyć indukcję etapami. Mianowicie rozważamy podgrupę $S(n)$ która zachowuje cykle g jako zbiory. Ta podgrupa jest produktem grup G_c permutacji elementów cyklu c. Robiąc indukcję etapami widać że wystarczy pokazać wynik dla G_c, czyli można zakładać że g jest pojedynczym cyklem.

Krok 2. Jeśli generator g jest cyklem długości l którą można zapisać jako produkt $l = km$ z względnie pierwszymi k i m to g można potraktować jako permutacją produktu zbiorów k elementowego i m elementowego, tak że g działa po składowych jako cykl długości k i cykl długości m. Znowu robimy indukcję etapami, najpierw w produkcie grup permutacji zbioru k elementowego i m elementowego, a potem do permutacji zbioru l elementowego. Indukcja w produkcie daje produkt charakterów, więc to sprowadza problem do cyklu który jest potęgą liczby pierwszej.

Krok 3. Niech cykl g długości p^k gdzie p jest liczbą pierwszą będzie generatorem podgrupy cyklicznej C. Elementy C które nie są generatorami tworzą podgrupę H mocy p^{k-1}. Jeśli $h \in H$ i $u^{-1}hu \in C$ to $u^{-1}hu$ nie jest generatorem C, czyli $u^{-1}hu \in H$. Ponadto obcięcie charakteru C do H jest charakterem H. A więc z wzoru na charakter indukowany wynika że charakter indukowany na klasie h z H będzie wielokrotnością charakteru indukowanego z C. Czyli przez

indukcję po k wystarczy pokazać że charakter indukowany na klasie generatora jest wymierny.

Krok 4. Niech g będzie generatorm podgrupy cyklicznej C mocy p^k zaś χ będzie charakterem C. $u^{-1}gu \in C$ oznacza że $u^{-1}gu$ jest generatorem C. Z wzoru na charakter indukowany wynika że charakter indukowany jest wielokrotnością sumy wartości χ na generatorach. Zauważmy że suma wartości χ po całym C jest wymierna bo jeśli χ jest charakterem trywialnym to jest to liczba całkowita, jeśli χ jest nietrywialny jest to wielokrotność sumy pierwiastków z 1 która wynosi 0. Suma wartości χ na generatorach to różnica sumy wartości χ na C i sumy wartości χ na elementach nie będących generatorami. Ale elementy nie będące generatorami tworzą podgrupę H, χ obcięte do H jest charakterem H, czyli suma po H jest wymierna. □

Niech p będzie liczbą pierwszą. Mówimy że element $g \in G$ jest p-elementem jeśli rząd g jest potęgą p. Mówimy że g jest p-regularny jeśli rząd p jest względnie pierwszy z p.

Mówimy że podgrupa grupy G jest p-elementarna jeśli jest produktem grupy cyklicznej rzędu względnie pierwszego z p i podgrupy rzędu będącego potęgą p (p-podgrupy).

Uwaga: p-podgrupa może być nieprzemienna. Jednakże z definicji produktu grup elementy grupy cyklicznej i p-podgrupy muszą komutować w podgrupie p-elementarnej.

Lemat 17.4 *(Twierdzenia Brauera) Każdy element $R(G)$ jest kombinacją liniową z całkowitymi współczynnikami charakterów jednowymiarowych podgrup p-elementarnych (z dowolnym p).*

Dowód lematu 17.4 można znaleźć w literaturze, np. [1] paragraf 10 rozdziału XVIII dowód Twierdzenia 15, lub [2] paragrafy 12.6 i 12.7.

Uwaga: Istnieją nieprzemienne p-grupy. Takie grupy muszą mieć reprezentacje nieprzywiedlne wymiaru większego niż 1, a więc w twierdzeniu Brauera trzeba uwzględniać charaktery podgrup. Innymi słowy, w przeciwieństwie do twierdzenia Artina nie można się ograniczyć do maksymalnych podgrup p-elementarnych.

Uwaga: W praktyce przy wyznaczaniu klas sprzężoności elementów również można wyliczyć komutant (a przynajmniej jego moc). Często podgrupy p-elementarne są małymi rozszerzeniami podgrup cyklicznych i łatwo je wyliczyć. Wtedy stosowanie twierdzenia Brauera wymaga podobnego wysiłku jak twierdzenie Artina a daje mocniejszy wynik. Ale czasami p-podgrupy są duże i skomplikowane.

Przykład: Niech q i r będą liczbami pierwszymi takimi że r dzieli $q-1$ (np. $r=3$, $q=7$). Wtedy istnieja $a \neq 0$ takie że $a^r = 1$ modulo q ($a=2$ działa dla $r=3$, $q=7$). A więc mnożenie przez a daje automorfizm $\mathbb{Z}_q$ którego r-ta potęga jest identycznością. Używając ten automorfizm możemy zbudować produkt półprosty $G = \mathbb{Z}_r \ltimes \mathbb{Z}_q$. G ma dwie wyróżnione podgrupy: obraz $\mathbb{Z}_q$ który

oznaczymy przez Q oraz obraz $\mathbb{Z}_r$ który oznaczymy przez R. Q jest podgrupą normalną. Dowolny element $G - Q$ generuje podgrupę sprzężoną z R. A więc właściwe podgrupy G są cykliczne, samo G nie jest grupą p-elementarną dla żadnego p. Lemat 17.4 mówi więc że dowolny charakter G jest kombinacją liniową o współczynnikach z $\mathbb{Z}$ charakterów indukowanych z podgrup cyklicznych, oczywiście jest to mocniejszy wynik niż dany przez lemat 17.2. Zobaczmy jeszcze jak przedstawić charakter trywialny G jako $\mathbb{Z}$-liniową kombinację charakterów indukowanych z podgrup cyklicznych.

Minus suma charakterów indukowanych z nietrywialnych charakterów R daje 1 ma $G-Q$, $-(r-1)q$ w e i 0 poza tym. Charakter indukowany z nietrywialnego charakteru χ grupy Q daje sumę po orbicie działania R na χ. Biorąc minus sumę z charakterów indukowanych z reprezentów orbit dostaniemy minus sumę nietrywialnych charakterów Q, czyli 1 na $Q - \{e\}$, $-(q-1)$ w e i 0 poza tym. Dodając te dwie sumy dostaniemy 1 na $G-\{e\}$ i $-(r-1)q-(q-1) = -rq+1$ w e, czyli trzeba jeszcze skorygować wartość w e. Suma charakterów indukowanych z charakterów R to rq w e i 0 poza tym. Dodając to do powyższego dostaniemy 1 na całym G.

Lemat 17.5 *Każda reprezentacja nieprzywiedlna grupy nilpotentnej G jest indukowana z jednowymiarowej reprezentacji podgrupy.*

Dowód. Dowód przez indukcję ze względu na moc G. Niech λ będzie reprezentacją nieprzywiedlną G na przestrzeni W. Jeśli λ nie jest wierna to istnieje nietrywialna podgrupa $H \subset G$ taka że λ obcięte do H jest trywialne. Wtedy H jest dzielnikiem normalnym zaś reprezentacja jest złożeniem homomorfizmu ilorazowego π z G na G/H z reprezentacją η grupy G/H. G/H ma mniej elementów niż G więc z założenia indukcyjnego istnieje podgrupa $N \subset G/H$ i reprezentacja jednowymiarowa ϕ grupy N takie że η jest indukowana z ϕ. Wtedy λ jest indukowana z reprezentacji $\phi \circ \pi$ podgrupy $\pi^{-1}(N)$, co daje wynik w tym przypadku.

A więc można zakładać że λ jest wierna. Grupa nilpotentna ma nietrywialne centrum Z. Jeśli $Z = G$ to G jest przemienna i reprezentacje G są jednowymiarowe, co daje wynik. W przeciwnym razie niech h będzie elementem G który przy odwzorowaniu ilorazowym z G w G/Z przechodzi na nietrywialny element centrum G/Z. Niech H będzie podgrupą G generowaną przez Z i h. H jest przemienna i jest dzielnikiem normalnym G. Mianowicie niech $g \in G$. Z wyboru h mamy $ghZ = hgZ$, czyli $h^{-1}g^{-1}hg \in Z$ co implikuje $g^{-1}hg \in H$. Oczywiście dla $z \in Z$ mamy $g^{-1}zg \in Z \subset H$ co oznacza że działanie automorfizmów wewnętrznych na generatory H daje elementy H, czyli H faktycznie jest dzielnikiem normalnym. Można więc zastosować lemat 16.5 z którego wynika że λ jest indukowana z reprezentacji $\chi \otimes \theta$ podgrupy $M \subset G$. Gdyby $M = G$ to charakter χ z lematu 16.5 byłby niezmienniczy na automorfizmy wewnętrzne. Ale $h \notin Z$ toteż dla pewnego $g \in G$ mamy $h^{-1}g^{-1}hg \in Z - \{e\}$. Jako że λ jest wierna i na Z λ jest wielokrotnością χ, to $\chi(h^{-1}g^{-1}hg) \neq 1$, czyli $\chi(h) \neq \chi(g^{-1}hg)$ czyli $g \notin M$. A więc M jest nietrywialną podgrupą i z założenia indukcyjnego $\chi \otimes \theta$ jest indukowane z jednowymiarowej reprezentacji ψ pewnej podgrupy M. Ale

wtedy na mocy lematu 16.3 o indukowaniu etapami λ jest indukowana z ψ. $\square$

Lemat 17.6 *Każda reprezentacja nieprzywiedlna grupy p-elementarnej jest indukowana z jednowymiarowej reprezentacji podgrupy.*

Dowód: Grupa p-elementarna jest produktem grupy cyklicznej C i p-grupy N. Reprezentacja ρ produktu $C \times N$ jest produktem tensorowym reprezentacji nieprzywiedlnych η grupy C i reprezentacji ϕ grupy N. Jako że C jest cykliczna to η jest jednowymiarowa. Wystarczy więc pokazać że ϕ jest indukowana z jednowymiarowej reprezentacji ψ podgrupy M bo wtedy ρ jest indukowana z produktu tensorowego $\eta \otimes \psi$ który jest jednowymiarową reprezentacją $C \times M$.

A więc wystarczy pokazać lemat w przypadku gdy G jest p-grupą. Wiadomo że p-grupa jest nilpotentna. A więc wynik otrzymujemy z lematu 17.5. $\square$

Dla grupy $SL(2,q)$ z opisu komutantów elementów widać że jeśli składnik cykliczny zawiera nietrywialną klasę sprzężoności to cała podgrupa p-elementarna będzie albo cykliczna albo będzie podgrupą $\tilde{N}$. Widać że wymienione podgrupy są p-elementarne. Dla nieparzystego q moc $SL(2,q)$ jest podzielna przez 8, a więc $SL(2,q)$ zawiera nieprzemienną 2-podgrupę.

Jeśli dla każdego $g \in G$ mamy równość $g^m = e$ i m jest najmniejszą liczbą całkowitą o tej własności to m nazywamy wykładnikiem G.

Lemat 17.7 *Niech m będzie wykładnikiem G i ciało k charakterystyki 0 zawiera pierwiastek pierwotny stopnia m z 1. Dowolną reprezentację G można zrealizować nad k.*

Dowód: Charaktery grupy G przyjmują wartości w k. Jeśli K jest większym ciałem, W jest $K[G]$ modułem to oznaczmy przez ψ charakter W. Na mocy twierdzenia Brauera

$$\psi = \sum n_j \mathrm{Ind}(\phi_j)$$

gdzie ϕ_j są jednowymiarowymi charakterami podgrup p-elementarnych. Moduł N_j odpowiadający charakterowi jednowymiarowemu ϕ_i oczywiście można zrealizować nad k. Oznaczmy przez $\mathrm{Ind}(N_j)$ moduł indukowanym z N_j. Oczywiście również $\mathrm{Ind}(N_j)$ można zrealizować nad k. A więc $\mathrm{Ind}(N_j)$ jest sumą prostą kopii $k[G]$-modułów prostych M_i. Niech χ_i będzie charakterem M_i. Istnieją liczby całkowite $k_{j,i}$ takie że

$$\mathrm{Ind}(\phi_j) = \sum_i k_{j,i}\chi_i.$$

Wtedy

$$\psi = \sum_j n_j(\sum_i k_{j,i}\chi_i) = \sum_i(\sum_j n_j k_{j,i})\chi_i$$

Z rozkładu kanonicznego wynika że suma $|G|$ kopii W jest sumą prostą M_i, czyli $|G|\psi$ jest kombinacją liniową χ_i o współczynnikach będących nieujemnymi

liczbami całkowitymi. Lecz χ_i są liniowo niezależnie nad $\mathbb{Q}$ więc przedstawienie ψ jako kombinacji liniowej χ_i jest jednoznaczne, więc $c_i = \sum_j n_j k_{j,i}$ są liczbami dodatnimi. Jako sumy liczb całkowitych są całkowite. A więc W jest izomorficzne z rozszerzeniem skalarów

$$\oplus_i \oplus_1^{c_i} M_i$$

czyli M można zrealizować nad k. □

18 Reprezentacje charakterystyki skończonej

W przypadku gdy charakterystyka p ciała nie dzieli mocy grupy i ciało jest dostatecznie duże teoria w charakterystyce p jest izomorficzna z teorią w charakterystyce 0. Dokładniej, niech m będzie wykładnikiem G, tzn. taką najmniejszą liczbą całkowitą dodatnią że dla każdego $g \in G$ mamy $g^m = e$. Pokazaliśmy że wtedy każda reprezentacja grupy G daje się zrealizować nad ciałem $K = \mathbb{Q}(e_m)$ gdzie e_m jest pierwiastkiem pierwotnym stopnia m z 1. Niech A będzie podpierścieniem w K składajacym się z elementów całkowitych nad $\mathbb{Z}$ i niech $\mathbf{m}$ będzie ideałem maksymalnym w A zawierającym p. Wtedy pierścień ilorazowy $A/\mathbf{m}$ jest ciałem F charakterystyki p zawierającym pierwiastek pierwotny stopnia e_m z 1.

Niech B będzie podpierścieniem K składającym się z elementów które można zapisać jako ułamek z mianownikiem nie należącym do $\mathbf{m}$. Redukcja modulo $\mathbf{m}$ jest dobrze zdefiniowana na B (jest to największy podpierścień K na którym redukcja modulo $\mathbf{m}$ jest dobrze zdefiniowana). B jest tak zwanym pierścieniem lokalnym. Co istotniejsze B jest pierścieniem ideałów głównych.

Lemat 18.1 *Niech k będzie ciałem zaś R będzie pierścieniem takim że k jest ciałem ułamków R. Niech ρ będzie reprezentacją grupy skończonej G na skończenie wymiarowej przestrzeni wektorowej V nad k. Wtedy V zawiera skończenie generowalny R moduł W który generuje V nad k.*

Dowód: Niech B będzie bazą V. B jest zbiorem skończonym. Definiujemy S wzorem

$$S = \bigcup_{g \in G} \rho(B).$$

Jako że G jest skończona to również S jest zbiorem skończonym. Jako W bierzemy podmoduł V traktowanego jako R-moduł generowany przez S. Oczywiście W jest skończnie generowalny. Jako że W zawiera B to W generuje V nad k. □

Bez dowodu przypomnijmy znany fakt z algebry:

Lemat 18.2 *Niech R będzie pierścieniem ideałów głównych zaś k ciałem ułamków R. Każdy podmoduł modułu wolnego nad R jest modułem wolnym. Jeśli W jest skończenie generowalnym modułem beztorsyjnym nad R (np. W jest podmodułem przestrzeni wektorowej nad k) to W jest modułem wolnym. Jeśli W_1 i W_2 są skończenie generowanymi podmodułami nad R przestrzeni wektorowej V nad k takimi że $kW_i = V$ to istnieją elementy $a \in K$, $b \in R$ takie ze $abW_1 \subset W_2 \subset aW_1$.*

Pierścień A zdefiniowany wyżej zwykle nie jest pierścieniem ideałów głównych. Jednakże łatwo można to poprawić używając większy pierścień. Niech B będzie podpierścieniem K składającym się z elementów które można zapisać jako ułamek z mianownikiem nie należącym do $\mathbf{m}$. Redukcja modulo $B\mathbf{m}$ jest dobrze zdefiniowana na B (jest to największy podpierścień K na którym redukcja modulo $\mathbf{m}$ jest dobrze zdefiniowana). B jest tak zwanym pierścieniem lokalnym. Co istotniejsze B jest pierścieniem ideałów głównych. Przy tym w B istnieje jedyny z dokładnością do stowarzyszenia (czyli mnożenia przez elementy odwracalne w B) element pierwszy π taki że $B\mathbf{m} = B\pi$. Przy tym każdy element $b \in B$ można zapisać jednoznacznie jako $b = u\pi^l$ gdzie $l \geq 0$, $l \in \mathbb{Z}$, zaś u jest elementem odwracalnym w B.

Lemat 18.3 *Niech M będzie skończenie generowalnym $K[G]$ modułem gdzie G jest grupą skończoną zaś p, K, B i F jest jak wyżej. Zakładamy że p nie dzieli mocy G. W M wybieramy $B[G]$-podmoduł E który generuje M jako przestrzeń wektorową nad K. Niech $\tilde{E}$ będzie $F[G]$-modułem otrzymanym przez redukcję modulo $B\mathbf{m}$. Klasa izomorfizmu $\tilde{E}$ nie zależy od wyboru E spełniającego warunki wyżej.*

Dowód: Niech E_1 i E_2 będą dwoma różnymi wyborami dla E. Zauważmy najpierw że jeśli $a \in K$ zaś $E_1 = aE_2$ to E_1 i E_2 są izomorficzne jako $B[G]$ moduły więc redukcja też daje izomorficzne moduły. Ogólnie na mocy lematu 18.2 istnieją $a \in K$ i $b \in B$ takie że $abE_1 \subset E_2 \subset aE_1$. Bazując na już udowodnionej części można zakładać że $a = 1$, czyli $bE_1 \subset E_2 \subset E_1$. Zapiszmy $b = u\pi^l$ gdzie u jest odwracalne w B. Jako że u jest odwracalny mamy $bE_1 = u\pi^l E_1 = \pi^l E_1$, więc wystarcza rozważać przypadek gdy $\pi^l E_1 \subset E_2 \subset E_1$. Najpierw rozważmy przypadek gdy $\pi E_1 \subset E_2 \subset E_1$. Niech $T = E_1/E_2$. Jako że $\pi E_1 \subset E_2$, to $B[G]$-moduł T można traktować jako $F[G]$ moduł. Mamy też ciąg dokładny $F[G]$ modułów:

$$0 \to \pi T \to \tilde{E}_2 \to \tilde{E}_1 \to T \to 0$$

gdzie odwzorowania (strzałki) są zadane przez inkluzje $B[G]$ modułów. Ale każdy $F[G]$ moduł jest sumą prostą modułów prostych, przy tym składniki proste są wyznaczone jednoznacznie. A więc ciąg dokładny wyżej prowadzi do izomorfizmów

$$\mathrm{Im}(\tilde{E}_2) \oplus T \approx \tilde{E}_1, \quad T \oplus \mathrm{Im}(\tilde{E}_2) \approx \tilde{E}_2,$$

gdzie $\mathrm{Im}(\tilde{E}_2)$ oznacza obraz $\tilde{E}_2$ i konsekwentnie $\tilde{E}_1$ jest izomorficzne z $\tilde{E}_2$ co daje wynik w przypadku gdy $\pi E_1 \subset E_2 \subset E_1$.

Wynik w przypadku $\pi^l E_1 \subset E_2 \subset E_1$ pokażemy przez indukcję ze względu na l. Pokazaliśmy już wynik dla $l = 1$, więc trzeba jeszcze pokazać wynik dla $l + 1$. Czyli zakładamy że $\pi^{l+1} E_1 \subset E_2 \subset E_1$. Niech $E_3 = E_2 + p^l E_1$. Mamy $p^l E_1 \subset E_3 \subset E_1$, czyli z założenia indukcyjnego $\tilde{E}_3$ jest izomorficzne z $\tilde{E}_1$. Mamy też $\pi E_3 = \pi E_2 + \pi^{l+1} E_1$. Jako że $\pi^{l+1} E_1 \subset E_2$ to $\pi E_3 \subset E_2 \subset E_3$. Na mocy przypadku $l = 1$ moduł $\tilde{E}_2$ jest izomorficzny z $\tilde{E}_3$. Ale $\tilde{E}_3$ jest izomorficzny z $\tilde{E}_1$, czyli $\tilde{E}_2$ jest izomorficzny z $\tilde{E}_1$. □

Uwaga: Wynik powyższego lematu zachodzi dla ogólniejszych ciał K. Po zamianie sformułowania pozostaje on prawdziwy dla dowolnych p. Dokładniej, dla danych E_1 i E_2 istnieje $F[G]$-moduł N taki że $\tilde{E}_1 \oplus N$ jest izomorficzne z $\tilde{E}_2 \oplus N$.

Lemat 18.4 *Niech M będzie $K[G]$ modułem prostym zaś K, B, G, p i E będą jak w poprzednim lemacie. Wtedy $\tilde{E}$ jest $F[G]$ modułem prostym.*

Dowód: Jeśli M ma nad K wymiar l to $\tilde{E}$ ma wymiar l nad F. M występuje z krotnością l w $K[G]$, więc $\tilde{E}$ też występuję z krotnością l w $F[G]$. Mianowicie, używając δ_g, z $g \in G$ jako bazę B-modułu redukcja $K[G]$ daje $F[G]$. Ale na mocy lematu 18.3 inne B-moduły generujące $K[G]$ nad K dają izomorficzną redukcję. W szczególności można rozłożyć $K[G]$ na $K[G]$-moduły proste i w każdym z modułów prostych M_i wybrać $B[G]$ moduł E_i generujący M_i nad K. Suma prosta kopii E_i daje $B[G]$-moduł zawarty w $K[G]$ i generujący $K[G]$ nad K. Widać że redukcja sumy prostej daje sumę prostą, czyli $\tilde{E}$ pojawi się w redukcji z krotnością l.

Skoro $\tilde{E}$ występuje w $F[G]$ z krotnością l to składniki nieprzywiedlne $\tilde{E}$ występują w $F[G]$ z krotnością co najmniej l. A więc na mocy twierdzenia Wedderburna dowolny niezerowy składnik nieprzywiedlny $\tilde{E}$ musi mieć wymiar co najmniej l. Jako że $\tilde{E}$ ma wymiar l oznacza to że $\tilde{E}$ jest modułem prostym. □

Lemat 18.5 *Redukcja modulo* $\mathbf{m}$ *zadaje wzajemnie jednoznaczną odpowiedniość między charakterami reprezentacji nieprzywiedlnych G nad K i charakterami reprezentacji nieprzywiedlnych G nad F.*

Dowód: Licząc ślad w bazie odpowiedniego modułu widać że redukcja charakteru jest charakterem redukcji modułu. Czyli wynik jest prostym wnioskiem z Lematu 18.4 □

19 Dodatek, krótko o grupach krystalograficznych

Idealny kryształ to periodyczna kolekcja atomów. Interesują nas symetrie kryształu. Fizycznie najważniejsze są kryształy w przestrzeni trójwymiarowej. Mate-

matycznie możemy rozważać dowolne $\mathbb{R}^n$ jako przestrzeń. Z definicji symetriami są przesunięcia o okresy co daje $\mathbb{Z}^n$ jako podgrupę grupy symetrii G. Jest to podgrupa normalna. Iloraz H grupy G przez $\mathbb{Z}^n$ jest grupą skończoną. Działanie G na $\mathbb{Z}^n$ przez automorfizmy wewnętrzne daje reprezentację H na $\mathbb{Z}^n$. Przy tym jest to reprezentacja wierna, bo przekształcenie afiniczne komutujące z przesunięciami jest samo przesunięciem.

Pierwszym krokiem do wyznaczenia możliwych grup symetrii jest wyznaczenie grup skończonych które mają wierną reprezentacje na $\mathbb{Z}^n$.

Tradycyjne podejście dla $\mathbb{R}^3$ wyglądało następująco:

- wyznaczenie grup mających reprezentacje na $\mathbb{R}^3$
- sprawdzenie które z nich mają reprezentacje na $\mathbb{Z}^3$
- wyznaczenie klas równoważności reprezentacji na $\mathbb{Z}^3$

Znając reprezentacje pozostawało wyznaczyć możliwe struktury G, co we współczesnym języku sprowadza się do policzenia odpowiednich grup homologii H.

Wyniki tej analizy są dość długie i dostępne w książkach, nie będziemy ich tu powtarzać.

Jest prosta sztuczka która pozwala uzyskać istotną informację o grupie H. Mianowicie H zachowuje $2\mathbb{Z}^n$ co prowadzi do reprezentacji H nad Z_2 (można też wziąść inną liczbę pierwszą). Jądro tego homomorfizmu jest grupą rozwiązalną. Dla $n = 3$ obraz to podgrupa grupy $SL(3, 2)$. Grupa $SL(3, 2)$ jest grupą prostą – można pokazać że jest ona izomorficzna z ilorazem grupy $SL(2, 7)$ przez centrum. Jednak obraz H musi być właściwą podgrupą $SL(3, 2)$ która jest rozwiązalna. Taki argument pozwala to pokazać że dla $\mathbb{Z}^3$ całe H jest rozwiązalne.

Literatura

[1] S. Lang, Algebra, PWN, 1984.

[2] P-P. Serre, Reprezentacje liniowe grup skończonych, PWN, 1988.