1 Wniosek z lematu o gęstości

Lemat 1.1 *(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 $x_1, \dots, x_n$ będzie bazą M jako przetrzeni wektorowej nad k. Wtedy na mocy lematu o gęstości istnieje $\alpha \in R$ takie że $\alpha x_i = f(x_i)$. Jako że $x_1, \dots, x_n$ jest bazą oznacza to że $\alpha = f$. Jako że f był dowolny oznacza to że $R = \mathrm{End}_k(M)$. $\square$

2 Twierdzenie Wedderburna

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

Lemat 2.1 *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. $\square$

Lemat 2.2 *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. $\square$

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 2.3 *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 reprezentaty 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 nieizomorficze, 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 założnia 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 nieparzystago n grupa D_n ma dwie reprezentacje jednowymiarowe, pochodzące z reprezentacji $\mathbb{Z}_2$. Jest też $(n-1)/2$ różnych reprezentaci 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.

3 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 3.1 *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 3.2 *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.

4 Charaktery

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

Uwaga: W przypadku pierscienia grupowgo 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 reprezentaję 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 naiwyższej potędze jest równy 1. Takie liczby nazywamy *liczbami algebraicznymi całkowitymi.* Nieco ogólniej mówimy że są to elementy całkowite nad $\mathbb{Z}$. Na mocy Lematu 5.2 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 5.3) 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).

5 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 5.1 *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 5.2 *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 $R[a_1a_2]$ i $R[a_1 + a_2]$ są skończenie generowalne.

Lemat 5.3 *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 współczniki 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 $q = -l_0 \in \mathbb{Z}$. $\square$