1 Reprezentacje indukowane

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 centalnej ϕ na S oznaczymy przez $\mathrm{Ind}(\phi)$ (lub $\mathrm{Ind}_S^G(\phi)$ jeśli trzeba zaznaczyć grupy) funkcję zadaną wzorem

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

gdzie R jest zbiorem reprezentantów dla G/S. Jako że ϕ jest funkcją centalną $\chi(r^{-1}gr)$ nie zależy od wyboru reprezentanta r dla warstwy lewostronnej, czyli $\mathrm{Ind}(\phi)$ jest dobrze zdefiniowane. Ponadto $\mathrm{Ind}(\phi)$ jest funkcją centalną: dla $u \in G$ zbiór $\{ur : r \in R\}$ jest też zbiorem reprezentatów 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 1.1 *(Prawo wzajemności Frobeniusa) Jeśli ψ jest funkcją centalną na S zaś ϕ jest funkcją centralną na G to*

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

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

Lemat 1.2 *(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.*

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 1.3 *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 perwszymi 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 generatorm 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 będzię 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 charkter 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 obciete do H jest charakterm H, czyli suma po H jest wymierna. $\square$

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 cykliczniej rzędu względnie pierwszego z p i podgrupy rzędu będącego potegą 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 1.4 *(Twierdzenia Brauera) Każdy element $R(G)$ jest kombinacją liniową z całkowitymi współczynnikami charakterów jednowymiarowych podgrup p-elementarnych (z dowolnym p).*

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 ograniczyc 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 twiedzenie Artina a daje mocniejszy wynik. Ale czasami p-podgrupy są duże i skomplikowane.

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 1.5 *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 wspólczynnikach 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. □

2 Kondensacja

Niech μ będzie idempotentem w pierścieniu A tzn. $\mu^2 = \mu$. Wtedy $A_\mu = \mu A \mu$ jest podalgebrą w A zaś $I_\mu = A\mu$ jest lewym ideałem. Przy założeniu że A jest pierścieniem z jedynką I_μ jest składnikiem prostym A. W tym celu zauważmy że $(1-\mu)$ też jest idempotentem, bo

$$(1-\mu)^2 = 1 - 2\mu + \mu^2 = 1 - \mu.$$

Mamy $(1-\mu)\mu = \mu - \mu^2 = 0$. Teraz widać że $(1-\mu)A$ jest modułem dopełniczym do μA w A. Mianowicie, dla $a \in A$ mamy $a = (1-\mu)a + \mu a$, czyli $A = (1-\mu)A + \mu A$. Jeśli $a \in \mu A$ to $\mu a = a$. Jeśli $a \in (1-\mu)A$ to $\mu a = 0$. Czyli $\mu A \cap (1-\mu)A = \{0\}$, czyli suma jest prosta.

Można też pokazać że jeśli A jest pierścieniem z jedynką zaś ideał I jest składnikiem prostym w A to istnieje idempotent μ taki że $I = A\mu$.

I_μ możemy potraktować jako prawy A_μ moduł:

$$(A\mu)(\mu A \mu) \subset A\mu$$

czyli mnożenie z prawej strony elementów I_μ przez elementy A_μ daje elementy I_μ.

Przypominam że N i M są lewymi A-modułami to przez $\mathrm{Hom}(N, M)$ oznaczamy $\mathbb{Z}$-moduł homomorfizmów z N w M.

Lemat 2.1 *Jeśli M jest lewym A-modułem to* $\mathrm{Hom}(I_\mu, M)$ *jest naturalnie izomomorficzne z A_μ-podmodułem $\mu M \subset M$ modułu M. Izomorfizm przyporządkowuje homomorfizmowi ϕ element $\phi(\mu)$.*

Dowód. Niech $\iota(\phi) = \phi(\mu)$. ι zadaje homomorfizm z $\mathrm{Hom}(I_\mu, M)$ w M. Jako że $\mu = \mu\mu$ to $\phi(\mu) = \phi(\mu\mu) = \mu\phi(\mu)$ czyli wartości są w μM. μ jest generatorem I_μ, więc to ι jest różnowartościowe. Jeśli $m \in \mu M$ to definiuję ϕ wzorem $\phi(a\mu) = am$. Takie ϕ jest dobrze zdefiniowane, bo jeśli $a\mu = 0$ to $a\mu M = \{0\}$ a więc $am = 0$. Oznacza to że mamy odwzorowanie odwrotne do ι, czyli ι jest izomorfizmem. □

Teraz definiujemy dwa odzworowania między modułami. Jeśli M jest lewym A-modułem to przez $\mathrm{Res}(M)$ będziemy oznaczać μM które traktujemy jako lewy A_μ-moduł. Jeśli N jest lewym A_μ-modułem to przez $\mathrm{Ind}(N)$ oznaczamy moduł $I_\mu \otimes_{A_\mu} N$. Jako że I_μ jest lewym A-modułem (i prawym A_μ-modułem) to $\mathrm{Ind}(N)$ jest lewym A-modułem.

Lemat 2.2 *Jeśli N jest A_μ modułem to* $\mathrm{Res}(\mathrm{Ind}(N))$ *jest izomorficzne z N.*

Dowód. Jako lewe A_μ moduły mamy równość

$$\begin{aligned}\mu\mathrm{Ind}(N) &= \mu(I_\mu \otimes_{A_\mu} N) = \mu((1-\mu)I_\mu \oplus \mu I_\mu) \otimes_{A_\mu} N \\ &= \mu((1-\mu)I_\mu \otimes_{A_\mu} N) \oplus \mu((\mu I_\mu) \otimes_{A_\mu} N).\end{aligned}$$

Mnożenie przez μ daje zero w $(1-\mu)I_\mu$ a więc również w $(1-\mu)I_\mu \otimes_{A_\mu} N$ czyli piewszy składnik sumy wyżej to moduł zerowy. $\mu I_\mu = A_\mu$ czyli $(\mu I_\mu) \otimes_{A_\mu} N$ jest izomorficzne z N jako A_μ moduł. Na A_μ module mnożenie przez μ daje identyczność, czyli drugi składnik jest izmomorficzy z N. □

Lemat 2.3 *Jeśli M jest lewym A-modułem to istnieje naturalne odwzorowanie z* $\mathrm{Ind}(\mathrm{Res}(M))$ *na $A\mu M$. Jeśli $A = A\mu A$ to jest to izomorfizm z M.*

Dowód. Na mocy własności iloczynu tensorowego istnieje odzworowanie ψ takie że dla $a \in I_\mu$ i $m \in \mu M$ mamy

$$\psi(a \otimes \phi) = am$$

Widać że ψ jest A-liniowe. Jako że $m \in \mu M$ oznacza że $m = \mu\tilde{m}$ dla $\tilde{m} \in M$ to $am \in A\mu M$, czyli obraz ψ jest zawarty w $A\mu M$. Jeśli $w \in A\mu M$ to istnieją a_i i m_i takie że $w = \sum a_i\mu m_i$. Wtedy $a_i\mu \in I_\mu$, $\mu m_i \in \mu M$ i

$$\psi(\sum(a_i\mu) \otimes (\mu m_i)) = \sum a_i\mu\mu m_i = w$$

czyli obraz ψ to $A\mu M$. Jeśli $A\mu A = A$ to istnieją a_i, b_i takie że $1 = \sum a_i\mu b_i$. Definiujemy odwzorowanie prawie dwuliniowe $\otimes$ z $I_\mu \times \mu A$ w A wzorem $a\mu \otimes \mu b =$

$a\mu b$. Niech η będzie odwzorowaniem prawie dwuliniowym z $I_\mu \times \mu A$ w grupę abelową W. Definiujemy homomorfizm ϕ z A jako grupy abelowej w W wzorem

$$\phi(t) = \sum \eta(ta_i\mu, \mu b_i).$$

Mamy

$$\phi(a\mu \otimes \mu b) = \phi(a\mu b) = \sum \eta(a\mu b a_i \mu, \mu bi)$$

Jako że η jest prawie dwuliniowe to $\eta(a\mu b a_i \mu, \mu b_i) = \eta(a\mu, \mu b a_i \mu b_i)$, czyli

$$\phi(a\mu \otimes \mu b) = \sum \eta(a\mu, \mu b a_i \mu b_i) = \eta(a\mu, \mu b \sum a_i \mu b_i) = \eta(a\mu, \mu b)$$

A więc ϕ spełnia równość z definicji iloczynu tensorowego. Jako że elementy $a\mu \otimes \mu b = a\mu b$ generują A jako grupę abelową takie ϕ jest jedyne, czyli A jest izomorficzne z iloczynem tensorowym $I_\mu \otimes_{A_\mu} \mu A$. Z definicji ψ wyżej dla a_i, b_i jak wyżej mamy

$$\sum \psi(a_i\mu \otimes \mu b_i) = \sum a_i \mu b_i = 1$$

czyli zdefiniowane wyżej ψ jest identyczne z podanym izomorfizmem $I_\mu \otimes \mu A$ z A. Teraz z łączności iloczynu tensorowego dla dowolnego modułu M mamy izomorfizm M i $I_\mu \otimes_{A_\mu} \mu M$. Przy tym z własności tensorowania odwzorowań ten izomorfizm jest zadany przez ψ. $\square$

Wniosek. Jeśli A-moduł M jest prosty to A_μ moduł μM jest albo prosty albo zerowy. Jeśli $A\mu A = A$ to jest 1-1 odpowiedniość między prostymi A-modułami i prostymi A_μ modułami.

Prostym przykładem idempotenta jest element μ algebry grupowej grupy skończonej taki że $\mu(g) = \frac{1}{|S|}$ dla $g \in S$ i $\mu(g) = 0$ dla $g \notin S$ gdzie S jest podgrupą G. Wtedy algebra A_μ składa się z funkcji które są dwustronnie niezmiennicze na przesunięcia względem S.