1 Ciała skończone

Ciało skończone K ma charakterystykę skończoną, czyli istnieje p takie że p-krotne dodanie jedynki do siebie daje 0. Najmniejsze takie p jest liczbą pierwszą którą nazywamy charakterystyką K. Dodawanie 1 do siebie daje podciało F ciała K nazywane ciałem prostym. Jest ono izomorficzne z ciałem reszt modulo p. Ogólne K jest przestrzenią wektorową nad ciałem prostym czyli ma $q = p^k$ elementów dla pewnego całkowitego dodatniego k. Dla dowolnego q postaci p^k istnieje ciało skończone mocy q. Przy tym dwa ciała skończone mocy q są izomorficzne. Istnienie ciała skończonego najłatwiej pokazać rozważając wielomian $P(x) = x^q - x$. Z ogólnej teorii wiadomo że istnieje rozszerzenie ciała p elementowego nad którym $P(x)$ rozkłada się na czynniki liniowe. Przy tym dla ustalonego P rozszerzenie generowane przez pierwiastki P (tzn. ciało rozkładu) jest jednoznaczne z dokładnością do izomorfizmu. Łatwo pokazać że iloczyn i suma pierwiastków P jest pierwiastkiem P, a więc pierwiastki P dają podpierścień. Jako że pochodna $P' = -1$ jest różna od 0 pierwiastki P są wszystkie różne czyli jest ich q. Skończony pierścień bez dzielników zera jest ciałem, czyli pierwiastki P dają ciało q-elementowe które oznaczymy przez $F(q)$. Jako ciało rozkładu P ciało $F(q)$ jest wyznaczone jednoznacznie z dokładnością do izomorfizmu.

Istotną własnością którą będziemy używać jest to że grupa multyplikatywna niezerowych elementów ciała $F(q)$ jest grupą cykliczną mocy $q - 1$. Mianowicie, gdyby ta grupa nie była cykliczna to istniałoby $m < q-1$ takie że $x^m = 1$ dla wszystkich $x \in F(q) - \{0\}$. Wtedy mielibyśmy $x^{m+1} - x = 0$ dla $x \in F(q)$. Lecz wielomian stopnia $m + 1$ ma co najwyżej $m + 1$ pierwiastków, czyli $m + 1 \geq q$, co daje sprzeczność.

Dla ciał charakterystyki większej niż 2 istotną własnością jest to czy niezerowy element ciała jest kwadratem czy nie. Jako że $x^2 = (-x)^2$ to kwadratami jest dokładnie połowa niezerowych elementów ciała, czyli $(q - 1)/2$ elementów. Druga połowa nie jest kwadratem. Produkt kwadratów jest dalej kwadratem, czyli kwadraty stanowią podgrupę grupy multyplikatywnej ciała. Elementy nie będące kwadratami można otrzymać mnożąc dowolny element nie będący kwadratem przez kwadraty. Produkt dwu elementów nie będących kwadratami jest kwadratem. Istotną cechą ciała jest to czy -1 jest kwadratem. Zachodzi to dokładnie wtedy gdy $q - 1$ jest podzielne przez 4. Mianowicie, jak rząd grupy multyplikatywnej ciała jest podzielny przez 4 to istnieje element rzędu 4 (bo grupa jest cykliczna), i jego kwadrat to -1. Jeśli -1 jest kwadratem to istnieje element rzędu 4, czyli moc grupy jest podzielna przez 4. Zauważmy że w ciele $F(q^2)$ -1 zawsze jest kwadratem. Mianowicie, jeśli -1 nie jest kwadratem w $F(q)$ to rozszerzenie ciała $F(q)$ o pierwiastek z -1 jest ciałem wymiaru 2 nad $F(q)$, czyli ciałem q^2 elementowym. Ale takie ciało jest jedno z dokładnością do izomorfizmu. Ogólniej, dodanie jednego pierwiastka kwadratowego do ciała $F(q)$ jest równoważne dodaniu wszystkich. Jest to duża różnica w porównaniu np. z ciałem liczb wymiernych gdzie pierwiastki kwadratowe z liczb pierwszych są niezależne.

2 Klasy sprzężoności w $SL(2, q)$

Niech K będzie pierścieniem przemiennym. Wtedy definiujemy grupę $SL(2, K)$ jako grupę macierzy 2 na 2 o wyznaczniku 1 (macierz o wyznaczniku 1 jest odwracalna, więc faktycznie dostaniemy grupę). W dalszym ciągu będziemy rozważać $SL(2, K)$ dla $K = F(q)$ gdzie $F(q)$ jest ciałem skończonym o q elementach. Większość metod poniżej działa dla dowolnego q, ale wyniki się różnią i gdy trzeba będziemy zakładać że q jest nieparzyste (czyli $1 \neq -1$). Wtedy $SL(2, K)$ jest grupą skończoną którą oznaczymy przez $SL(2, q)$. Dowolny element $SL(2, q)$ możemy otrzymać w następujący sposób:

najpierw wybieramy niezerowy wektor z K^2 jako pierwszy wiersz macierzy. Następnie wybieramy drugi wiersz tak by wyznacznik był 1. Wyznacznik jest liniową funkcją drugiego wiersza, przy tym jeśli pierwszy wiersz jest niezerowy to jest to funkcja niezerowa, czyli wybór jest zawsze możliwy. Pierwszy wybór daje $q^2 - 1$ możliwości na pierwszy wiersz, przy drugim wyborze zbiór rozwiązań to warstwa podprzestrzeni wymiaru 1, czyli mamy q możliwości. A więc $|SL(2,q)| = q(q^2-1) = (q-1)q(q+1)$.

Element $g \in SL(2,q)$ spełnia jeden z warunków niżej:

- g ma dwie różne wartości własne w $F(q)$
- g ma dwie różne wartości własne w $F(q^2) - F(q)$
- g ma równe wartości własne

Jeśli g ma równe wartości własne $\lambda_1 = \lambda_2 = \lambda$ to $\lambda^2 = 1$ czyli $\lambda = 1$ lub $\lambda = -1$.

Jeśli dodatkowo g się diagonalizuje to $g = \pm I$ gdzie I to macierz jednostkowa. Daje to dwie jednoelementowe klasy sprzężoności.

W przeciwnym razie g jest sprzężone z elementem postaci $\pm n_c$ gdzie

$$n_c = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$$

z niezerowym c. Łatwo zauważyć że n_c jest sprzężone z n_{a^2c} dla niezerowego a. Niech $N = \{n_c : c \in F(q)\}$. Chcemy wyznaczyć przekrój klasy sprzężoności n_c z N. Zauważmy że dla $e_1 = (1,0)$ mamy $n_c e_1 = e_1$, czyli e_1 jest wektorem własnym n_c i dowolny wektor własny n_c jest proporcjonalny do e_1.

Jeśli $n_{c_1} = m^{-1} n_c m$ to dla $v = m^1 e_1$ mamy

$$n_{c_1} v = m^{-1} n_c m v = m^{-1} n_c e_1 = m^{-1} e_1 = v$$

czyli $v = a e_1$ dla pewnego $a \in F(q) - \{0\}$. Wtedy m jest postaci

$$\begin{pmatrix} a & d \\ 0 & a^{-1} \end{pmatrix}$$

(czyli należy do rozważanej później podgrupy M) i

$$m^{-1} n_c m = \begin{pmatrix} 1 & a^{-2}c \\ 0 & 1 \end{pmatrix}$$

czyli klasa sprzężoności n_c przekrojona z N to $\{n_{a^2c} : a \in F(q) - \{0\}\}$. Zauważmy że $a^2 c = (-a)^2 c$, czyli dla nieparzystego q wartość $a^2 c$ osiągniemy na dwa sposoby. Czyli $a^2 c$ przebiega $(q-1)/2$ wartości i mamy dwie orbity. Uwzględniając że $\lambda = \pm 1$ to mamy 4 kasy sprzężoności powyższej postaci. Zauważmy że z n_c komutują tylko elementy $\pm n_d$ z być może zerowym d. A więc komutant n_c ma $2q$ elementów czyli klasa sprzężoności ma $(q^2-1)/2$ elementów. Używamy tu znaną własność że moc klasy sprzężoności czyli orbity względem automorfizmów wewnętrznych to moc grupy podzielona przez moc stabilizatora punktu czyli komutanta.

Jeśli g ma dwie różne wartości własne to g jest sprzężone z macierzą postaci

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$$

Jest tu pewna subtelność: z algebry liniowej wiemy że sprzężenie będzie przy pomocy macierzy nieosobliwej, lecz my potrzebujemy wyznacznik 1. Jednakże mnożąc macierz sprzęgającą przez macierz diagonalną możemy skorygować wyznacznik tak by dostać 1. Dowolna macierz komutująca z g się diagonalizuje, czyli komutant ma $(q-1)$ elementów, a więc klasa sprzężoności ma $q(q+1)$ elementów. Widać że λ i λ^{-1} dają tą samą klasę. Z drugiej strony, macierze które są sprzężone w $SL(2,q)$ mają ten sam zbiór wartości własnych. Czyli $\{\lambda, \lambda^{-1}\}$ wyznacza dokładnie jedną klasę sprzężoności. Tutaj wykluczone jest 0 (nie ma odwrotności), 1 i -1 (wtedy wartości własne są równe). A więc mamy $(q-3)/2$ klasy tego typu.

Rozważmy teraz g z dwoma różnymi wartościami własnymi z $F(q^2) - F(q)$. Zauważmy że takie g nie ma nietrywialnych podprzestrzeni niezmienniczych nad $F(q)$ (taka podprzestrzeń dałaby wektor własny a więc i wartość własną z $F(q)$). Rozważmy teraz zbiór R macierzy nad $F(q)$ (z dowolnym wyznacznikiem) komutujących z g. Jest to pierścień. Aby macierz h nad $F(q)$ komutowała z g, h musi się diagonalizować w tej samej bazie co g. Czyli elementy R komutują ze sobą, czyli R jest pierścieniem przemiennym. Oczywiście g należy do R a więc przy naturalnym działaniu R na $F(q)^2$ R nie ma podprzestrzeni niezmienniczych, czyli $F(q)^2$ jest R-modułem prostym. Jako że R jest przemienny z lematu Schura wynika że każdy niezerowy element R jest odwracalny, czyli R jest ciałem. R zawiera macierze skalarne, czyli R jest rozszerzeniem $F(q)$. Przyporządkowanie elementowi R wartości własnej na wybranym wektorze własnym g daje homomorfizm z R w $F(q^2)$. Ale $F(q^2)$ ma wymiar 2 nad $F(q)$, czyli nie ma ciał pośrednich i R jest izomorficzne z $F(q^2)$. A więc dla dowolnego $\lambda \in F(q^2)$ w R jest macierz h z wartością własną λ. Aby h miało wyznacznik 1 λ musi być pierwiastkiem wielomianu postaci $s^2 - as + 1$ (bo druga wartość własna jest drugim pierwiastkiem wielomianu, czyli iloczyn pierwiastków to 1). Przy tym wielomian charakterystyczny h musi być nierozkładalny lub musi mieć pierwiastek podwójny. Jest $(q-3)/2$ wielomianów rozkładalnych z różnymi pierwiastkami i dwa wielomiany mające równe pierwiastki. Czyli mamy $(q-1)/2$ wielomianów nierozkładalnych jak wyżej czyli w pierwszym przypadku mamy $(q-1)$ wartości dla λ. W drugim mamy dwie możliwości. Razem komutant liczy $(q+1)$ elementów, czyli klasa sprzężoności g ma $(q-1)q$ elementów. Zauważmy że przy okazji pokazaliśmy że komutant jest izomorficzny z podgrupą grupy multyplikatywnej $F(q^2)$. Jako że grupa multyplikatywna $F(q^2)$ jest cykliczna wynika stąd że komutant jest grupą cykliczną.

Teraz zauważmy że g jak wyżej są sprzężone nad $F(q^2)$ wtedy i tylko wtedy gdy są sprzężone nad $F(q)$. Mianowicie $g_2 = u^{-1}g_1u$ jest równoważne $ug_2 - g_1u = 0$, czyli układowi równań liniowych. Układ równań liniowych o współczynnikach z $F(q)$ który ma niezerowe rozwiązanie nad $F(q^2)$ ma też rozwiązanie nad $F(q)$. Na mocy lematu Schura rozwiązanie będzie macierzą nieosobliwą. A priori wyznacznik tak otrzymanego u będzie dowolną niezerową wartością z $F(q)$. Jednakże mnożąc u przez niezerowe elementy pierścienia R wyżej otrzymamy inne rozwiązania. Tzn. jeśli $g_2 = u^{-1}g_1u$ i $h^{-1}g_1h = g_1$ to również $g_2 = (hu)^{-1}g_1(hu)$. Jako że $R - \{0\}$ ma $q^2 - 1$ elementów i $q + 1$ elementów $R - \{0\}$ ma wyznacznik 1 to wyznacznik na $R - \{0\}$ przyjmuje $q - 1$ wartości, czyli wszystkie wartości z $F(q) - \{0\}$. A więc można dobrać $h \in R - \{0\}$ by $\det(hu) = 1$. A więc jak poprzednio klasa sprzężoności g w $SL(2,q)$ jest wyznaczona przez zbiór $\{\lambda, \lambda^{-1}\}$. Nie każde $\lambda \in F(q^2) - F(q)$ daje klasę sprzężoności: wielomian charakterystyczny g ma postać $s^2 - \mathrm{Tr}(g)s + 1$ i λ musi być pierwiastkiem takiego wielomianu. Dokładniej zbiory $\{\lambda, \lambda^{-1}\}$ są w $1-1$ odpowiedniości z nierozkładalnymi wielomianami postaci wyżej. Jak liczyliśmy wyżej jest $(q-1)/2$ wielomianów nierozkładalnych, a więc $(q-1)/2$ klas jak wyżej.

Podsumujmy nasze wyliczenia klas w tabelce:

rodzaj	moc klasy	liczba klas	moc sumy klas
$\pm I$	1	2	2
$\pm n_c$	$(q^2-1)/2$	4	$2(q^2-1)$
$\lambda \in F(q) - \{0,1,-1\}$	$q(q+1)$	$(q-3)/2$	$(q-3)q(q+1)/2$
$\lambda \in F(q^2) - F(q)$	$(q-1)q$	$(q-1)/2$	$q(q-1)^2/2$
Razem		$q+4$	$(q-1)q(q+1)$

Na mocy twierdzenia Wedderburna grupa $SL(2,q)$ ma $q+4$ klasy równoważności reprezentacji nieprzywiedlnych nad $\mathbb{C}$.

Z podanego opisu klas sprzężoności wynika

Lemat 2.1 *Dla $q > 3$ jedynym nietrywialnym dzielnikiem normalnym $SL(2,q)$ jest centrum. Dla $q = 3$ jest jeszcze dzielnik normalny mocy $(q+1)(q-1) = 8$ z ilorazem mocy 3.*

Dowód. Krok 1: Jeśli dzielnik normalny H zawiera klasę typu n_c dla pewnego c to H zawiera wszystkie elementy typu n_c z dowolnym c (czyli podgrupę N). Mianowicie, przez wielokrotne mnożenie grupowe widać że H zawiera elementy postaci n_{ac} dla dowolnego $a \in F(p)$. Dla $q = p$ daje to wynik. W przeciwnym razie zauważamy że zbiór c takich że $n_c \in H$ jest przestrzenią wektorową nad $F(p)$. Gdyby była to podprzestrzeń właściwa to miałaby moc co najwyżej q/p. Ale dla $q > p > 2$ przekrój klasy sprzężoności n_c z N ma większą moc.

Krok 2: Jeśli dzielnik normalny H zawiera element postaci $-n_c$ to zawiera N i $-I$. Mianowicie, klasa sprzężoności zawiera wtedy dwa elementy $-n_{c_1}$ i $-n_{c_2}$. Mnożąc jeden przez odwrotność drugiego dostaniemy element postaci n_c z niezerowym c. A więc na mocy kroku 1 H zawiera N. Mnożąc $-n_c$ przez odwrotność n_c widzimy że $-I \in H$.

Krok 3: Dzielnik normalny H albo ma moc mniejszą lub równą $(q+1)(q-1)$ albo ma moc podzielną przez q. Mianowicie, jako że $q = p^k$ jest względnie pierwsze z $(q-1)$ i $q+1$ to albo $|H|$ jest względnie pierwsza z p i wtedy jako czynnik mocy grupy dzieli $(q+1)(q-1)$, albo $|H|$ jest podzielna przez p. Klasy elementów diagonalizowalnych nad $F(q^2)$ mają moc podzielną przez q. H zawiera również jedynkę, więc by $|H|$ była podzielna przez p musimy dobrać klasy typu $\pm n_c$. Na mocy kroków 1 i 2 widać że albo H zawiera $-I$ i cztery klasy typu n_c, albo $-I \notin H$ i H zawiera dwie klasy typu n_c. W obu przypadkach ilość elementów jest podzielna przez q.

Krok 4: Dla $q > 3$ dzielnik normalny H nie zawarty w centrum ma moc większą niż $(q+1)(q-1)$ (a więc z Kroku 3 podzielną przez q). Dla $q = 3$ dzielnik normalny nie zawarty w centrum ma moc większą lub równą $(q+1)(q-1) = 8$ przy tym istnieje dzielnik normalny mocy $(q+1)(q-1)$. Mianowicie, na mocy kroków 1 i 2 jeśli dzielnik normalny zawiera element postaci $\pm n_c$ to zawiera co namniej dwie takie klasy czyli $q^2-1 = (q+1)(q-1)$ elementów z tych klas. Razem z jedynką jest to więcej niż $(q+1)(q-1)$. A więc pozostaje rozpatrzeć pozostałe klasy sprzężoności. Klasy elementów diagonalizowalnych nad $F(q)$ mają $q(q+1)$ elementów co jest więcej niż $(q+1)(q-1)$. Pozostaje więc klasa elementu diagonalizującego się nad $F(q^2)$. Ta klasa ma $(q-1)q$ elementów. Gdyby była jeszcze jedna klasa mocy większej niż 1 do razem byłoby więcej niż $(q+1)(q-1)$ elementów. A więc jedyna pozostająca możliwość to jedna klasa $(q-1)q$ elementów, jedynka i być może $-I$. Czyli $(q-1)q+1$ elementów lub $(q-1)q+2$ elementów. Oba przypadki dają liczbę względnie pierwszą z q, czyli dzielącą $(q+1)(q-1)$. Liczba ta jest większa niż $(q+1)(q-1)/2$, czyli musiałaby zajść równość. Równość $(q-1)q+1 = (q+1)(q-1)$ daje $q = 2$ co wykluczmy bo q jest tu nieparzyste. Równość $(q-1)q+2 = (q+1)(q-1)$ daje $q = 3$. Bezpośrednie sprawdzenie pokazuje że dla $q = 3$ podane klasy elementów tworzą podgrupę mocy 8.

Krok 5. Dzielnik normalny mocy podzielnej przez q zawiera element postaci n_c. Mianowicie, wynika to z uzasadnienia kroku 3.

Krok 6. Dzielnik normalny zawierający element postaci n_c zawiera też elementy postaci

$$\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Mianowicie

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -c & 1 \end{pmatrix}$$

co daje pierwszą postać wyżej.

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

co daje drugą postać.

Krok 7. Dzielnik normalny który zawiera element postaci n_c zawiera elementy postaci

$$\begin{pmatrix} a & x \\ b & y \end{pmatrix}$$

z dowolnym a, b takim że $(a, b) \neq 0$. Mianowicie, z kroku 1 wynika że mając jedno n_c dostaniemy wszystkie elementy tej postaci. Teraz, jeśli $b \neq 0$ to

$$\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} = \begin{pmatrix} cb+1 & c \\ b & 1 \end{pmatrix}$$

gdzie czynniki są dostępne z kroku 6. Skoro $b \neq 0$ to można dobrać c tak by $cb + 1 = a$. Jeśli $b = 0$ to

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & y \\ -a & -x \end{pmatrix} = \begin{pmatrix} a & x \\ 0 & y \end{pmatrix}$$

co sprowadza problem do poprzedniego przypadku

Krok 8. Dzielnik normalny H który zawiera element postaci n_c to całe $SL(2, q)$. Mianowicie, na mocy Kroku 7 H zawiera elementy z dowolną niezerową pierwszą kolumną. Dla macierzy h pierwsza kolumna to he_1 gdzie $e_1 = (1, 0)$. Moc zbiory otrzymanych wartości to $|H|$ podzielna przez moc stabilizatora punktu. Jako że otrzymamy $q^2 - 1$ pierwszych kolumn to $|H|$ jest wielokrotnością $q^2 - 1$. Lecz $|H|$ na mocy Kroku 4 jest podzielna przez q (dla $q = 3$ z uzasadnienia w Kroku 4 wynika że dzielnik normalny o mocy niepodzielnej przez q nie zawiera elementów postaci n_c). Jako że q i $q^2 - 1 = (q - 1)(q + 1)$ są względnie pierwsze to $|H|$ jest podzielna przez $(q - 1)q(q + 1)$, czyli przez moc $SL(2, q)$. A więc H to całe $SL(2, q)$.

Kroki 3, 4, 5 i 8 razem dają lemat. □

Wniosek: Dla $q > 3$ jedyną reprezentacją jednowymiarową $SL(2, q)$ jest reprezentacja trywialna. $SL(2, 3)$ ma dwie reprezentacje jednowymiarowe.

3 Podgrupa M

Rozważmy podgrupę M grupy $SL(2,q)$ składającą się z macierzy postaci

$$A(\lambda, c) = \begin{pmatrix} \lambda & c \\ 0 & \lambda^{-1} \end{pmatrix}$$

M ma dzielnik normalny N składający się z macierzy dla których $\lambda = 1$. Dzieląc M przez N otrzymujemy grupę izomorficzną z grupą multyplikatywną ciała $F(q)$. Jest to grupa cykliczna mająca $q-1$ elementów. Składając odwzorowanie ilorazowe z jednowymiarowymi reprezentacjami otrzymamy $q-1$ reprezentacji jednowymiarowych M, a więc i $q-1$ charakterów jednowymiarowych.

N jest izomorficzne z grupą addytywną ciała $F(q)$, a więc reprezentacje nieprzywiedlne N są jednowymiarowe. Nasuwa się pytanie o reprezentacje indukowane z N. Zauważmy że w M jest większy dzielnik normalny $\tilde{N}$ generowany przez N i $\pm I$. $\tilde{N}$ jest grupą abelową, a więc reprezentacje indukowane z N rozkładają się na sumę prostą reprezentacji jednowymiarowych $\tilde{N}$. Aby móc otrzymać reprezentacje nieprzywiedlne rozważny więc reprezentacje indukowane z $\tilde{N}$. Taka reprezentacja ma wymiar $(q-1)/2$. Niech χ będzie charakterem reprezentacji $\tilde{N}$. Reprezentacja indukowana po obcięciu do N jest sumą prostą $(q-1)/2$ reprezentacji z charakterami χ_a zadanymi wzorem $\chi_a(n) = \chi(a^2 n)$ gdzie a przebiega wartości z $F(q)$ dające reprezentanty warstw. Ponieważ bierzemy tylko jedno z a i $-a$ otrzymane charaktery są różne. To oznacza że faktycznie otrzymamy w ten sposób reprezentację nieprzywiedlną M (każda nietrywialna podprzestrzeń niezmiennicza zawiera jednowymiarową podprzestrzeń z charakterem χ_a, a z jednej takiej podprzestrzeni działanie M da całą przestrzeń reprezentacji). Jeśli dwa charaktery $\tilde{N}$ są związane wzorem $\chi_2(n) = \chi_1(a^{-1}na)$ to otrzymane reprezentacje są równoważne. Charaktery $\tilde{N}$ dają cztery klasy równoważności względem tej relacji, więc otrzymamy cztery nierównoważne reprezentacje. Obliczmy charakter η reprezentacji indukowanej. Dla $m \notin \tilde{N}$ mamy $\eta(m) = 0$. Dla $m = -In$ z $n \in N$ mamy $\eta(m) = \chi(-I)\eta(n)$. A więc kluczowe jest obliczenie $\eta(n)$. Dla n_c mamy

$$\eta(n_c) = \frac{1}{2} \sum_{a \in F(q) - \{0\}} \chi(n_{a^2 c}).$$

Wyrażenie na $\eta(n_c)$ zależy od c i χ. Zauważmy że $\eta(n_c)$ przybiera dokładnie dwie wartości. Mianowicie jeśli $c_1 = b^2 c_2$ to $\eta(n_{c_1}) = \eta(n_{c_2})$. Jeśli b nie jest kwadratem to $\eta(n_{bc})$ daje drugą wartość. Podobnie, jeśli $\chi_2(n_c) = \chi_1(n_{b^2 c})$ to χ_1 i χ_2 dają to samo η. Jeśli b nie jest kwadratem i $\chi_2(n_c) = \chi_1(n_{bc})$ to wartości η zamieniają się rolami: wartość η_1 dla c będących kwadratami staje się wartością η_2 dla c nie będących kwadratami i odwrotnie. Czyli mamy dwie wartości α_1 i α_2 takie że dla ustalonego χ_0 mamy $\eta_0(n_c) = \alpha_1$ dla c będących kwadratami i $\eta_0(n_c) = \alpha_2$ dla c nie będących kwadratami.

Jeśli -1 nie jest kwadratem w $F(q)$ to mnożenie przez -1 zamienia kwadraty na elementy nie będące kwadratemi i odwrotnie. Wtedy

$$\alpha_2 = \eta_0(n_{-c}) = \frac{1}{2} \sum_{a \in F(q) - \{0\}} \chi(n_{-a^2 c}) \frac{1}{2} \sum_{a \in F(q) - \{0\}} \chi(n_{a^2 c})^{-1}$$

$$= \frac{1}{2} \sum_{a \in F(q) - \{0\}} \bar{\chi}(n_{a^2 c}) = \bar{\alpha}_1$$

Pisząc $\alpha_1 = \beta + \gamma$ gdzie β jest rzeczywiste zaś γ czysto urojone mamy $\alpha_2 = \beta - \gamma$. Mamy

$$1 + \alpha_1 + \alpha_2 = \sum_{c \in F(q)} \chi(n_c) = 0$$

czyli $\beta = \frac{-1}{2}$.

Teraz możemy użyć reguły ortogonalności dla charakterów by wyznaczyć γ. Mianowicie dla c będącego kwadratem $\eta_1(n_c) = \alpha_2$ i $\eta_1(n_{-c}) = \alpha_1$ daje inny charakter. A więc $\langle \eta_0, \eta_0 \rangle = 1$ i $\langle \eta_0, \eta_1 \rangle = 0$. Rozpisując $\langle \eta_0, \eta_0 \rangle = 1$ mamy

$$(q-1)q = ((q-1)/2)^2 + ((q-1)/2)^2 + (q-1)\alpha_1\alpha_2 + (q-1)\alpha_2\alpha_1$$

gdzie dwa pierwsze człony to wartości dla $\pm I$, kolejne to suma wartości dla $\pm I n_c$ z c będącym oraz (czwarty człon) nie będącym kwadratem. Dzieląc przez $q-1$ i uwzględniając że $\alpha_1\alpha_2 = \beta^2 - \gamma^2$ dostaniemy

$$q = (q-1)/2 + 2(\beta^2 - \gamma^2)$$

Podobnie, z $\langle \eta_0, \eta_1 \rangle = 0$ dostaniemy

$$0 = (q-1)/2 + 2(\beta^2 + \gamma^2).$$

Odejmując drugą równość od pierwszej dostaniemy $\gamma^2 = -q/4$ czyli $\gamma = \frac{i\sqrt{q}}{2}$. Oczywiście jest niejednoznaczność znaku, ale można przyjąć że wybór χ_0 był zrobiony tak że znak się zgadza.

Jeśli -1 jest kwadratem w $F(q)$ to poprzedni argument pokazuje że α_1 i α_2 są rzeczywiste. Możemy zapisać $\alpha_1 = \beta + \gamma$, $\alpha_2 = \beta - \gamma$ i jak poprzednio $\beta = -1/2$. Reguły ortogonalności działają w trochę inny sposób, bo teraz $\eta_i(n_c^{-1}) = \eta_i(n_{-c}) = \eta_i(n_c)$ a więc mamy

$$(q-1)q\langle \eta_0, \eta_0 \rangle = ((q-1)/2)^2 + ((q-1)/2)^2 + (q-1)\alpha_1^2 + (q-1)\alpha_2^2$$

co daje

$$q = (q-1)/2 + 2(\beta^2 + \gamma^2)$$

zaś $\langle \eta_0, \eta_1 \rangle$ daje

$$0 = (q-1)/2 + 2(\beta^2 - \gamma^2).$$

Odejmując drugą równość od pierwszej dostaniemy równanie $\gamma^2 = q/4$ czyli $\gamma = \frac{\sqrt{q}}{2}$. Jak poprzednio jest niejednoznaczność znaku, ale można wybrać χ_0 by znak się zgadzał.

4 Reprezentacje indukowane

Rozważmy znowu podgrupę M grupy $SL(2,q)$ składającą się z macierzy postaci

$$A(\lambda, c) = \begin{pmatrix} \lambda & c \\ 0 & \lambda^{-1} \end{pmatrix}$$

Jak to opisaliśmy M ma $q-1$ reprezentacji jednowymiarowych odpowiadających charakterom podgrupy składającej się z macierzy diagonalnych. Innymi słowy te reprezentacje pochodzą z wydzielenia M przez podgrupę macierzy postaci N_c i wzięcia reprezentacji jednowymiarowych ilorazu. Niech χ

będzie charakterem M odpowiającym takiej reprezentacji jednowymiarowej. Wtedy charakter $\mathrm{Ind}(\chi)$ reprezentacji indukowanej liczymy używając podany wcześniej lemat, biorąc sumę po reprezentantach warstw $SL(2,q)/M$. Niech $m \in M$ będzie diagonalne z dwoma różnymi wartościami własnymi i niech $m_2 = r^{-1}mr \in M$. Łatwo sprawdzić że dowolny element M mający różne wartości własne jest sprzężony w M z elementem w postaci diagonalnej, a więc zmieniając wybór r można zakładać że m_2 jest diagonalne. Wtedy re_1 albo jest wielokrotnością e_1, albo jest wielokrotnością $e_2 = (0,1)$. Jeśli re_1 jest wielokrotnością e_1 to $r \in M$ czyli jako r można wybrać jedynkę $SL(2,q)$. Jeśli re_1 jest wielokrotnością e_2 to można znaleźć diagonalne $s \in M$ tak by $sre_1 = e_2$. Jako że wyznacznik sr równa się 1 oznacza to że $sre_2 = -e_1$, czyli przy takiej normalizacji r jest wyznaczone jednoznacznie. W sumie to rozważanie pokazuje że są dokładnie dwa reprezentanty warstw $r \in SL(2,q)/M$ takie że $r^{-1}mr \in M$, przy tym przy jednym wyborze $\chi(r^{-1}mr) = \chi(m)$, przy drugim $\chi(r^{-1}mr) = \chi(m)^{-1}$. A więc $\mathrm{Ind}(\chi)(m) = \chi(m) + \chi(m)^{-1}$ dla m w postaci diagonalnej.

Jeśli m ma dwie wartości własne z $F(q^2) - F(q)$, to klasa sprzężoności ma pusty przekrój z M, czyli $\chi(m) = 0$.

Dla m postaci $\pm N_c$ możemy rozumować następująco: jeśli $r^{-1}mr \in M$ to $r^{-1}mr$ jest postaci $\pm N_{c_2}$. Każdy wektor własny m jest wielokrotnością e_1, czyli re_1 jest wielokrotnością e_1. A więc $r \in M$, czyli jest dokładnie jeden reprezentant warstw r taki że $r^{-1}mr \in M$. A więc $\mathrm{Ind}(\chi)(m) = \chi(m)$.

Jeśli $m = \pm I$ to $r^{-1}mr = m$ i każdy reprezentant daje ten sam wkład, czyli $\mathrm{Ind}(\chi)(m) = (q+1)\chi(m)$.

Licząc $\langle \mathrm{Res}(\mathrm{Ind}(\chi)), \chi \rangle$ obliczamy sumę po grupie M. Dowolny element M możemy zapisać w postaci $m = A(\lambda, c)$ i najpierw sumować po różnych wartościach c, a potem po λ. Dla λ różnego od λ^{-1} mamy

$$\sum_c \mathrm{Res}(\mathrm{Ind}(\chi))(A(\lambda,c))\chi(A(\lambda,c)^{-1})$$

$$= \sum_c (\chi(A(\lambda,c)) + \chi(A(\lambda,c)^{-1}))\chi(A(\lambda,c)^{-1}).$$

Dla $\lambda = \pm 1$ mamy

$$\sum_c \mathrm{Res}(\mathrm{Ind}(\chi))(A(\lambda,c))\chi(A(\lambda,c)^{-1})$$

$$= \left((q+1)\chi(A(\lambda,0)) + \sum_{c \neq 0} \chi(A(\lambda,c)) \right) \chi(A(\lambda,c)^{-1})).$$

Lecz $\chi(A(\lambda,c))$ nie zależy od c i $A(\lambda,0) = A(\lambda,0)^{-1}$ czyli

$$(q+1)\chi(A(\lambda,0)) + \sum_{c \neq 0} \chi(A(\lambda,c)) = (q+1)\chi(A(\lambda,0)) + (q-1)\chi(A(\lambda,0))$$

$$= 2q\chi(A(\lambda,0)) = q\chi(A(\lambda,0)) + \chi(A(\lambda,0)^{-1})$$

$$= \sum_c \left(\chi(A(\lambda,c)) + \chi(A(\lambda,c)^{-1}) \right).$$

Czyli dla dowolnego λ mamy

$$\sum_c \mathrm{Res}(\mathrm{Ind}(\chi))(A(\lambda,c))\chi(A(\lambda,c)^{-1})$$

$$= \sum_c (\chi(A(\lambda, c)) + \chi(A(\lambda, c)^{-1}))\chi(A(\lambda, c)^{-1}).$$

Sumując po λ i dzieląc przez moc M mamy

$$\langle \mathrm{Res}(\mathrm{Ind}(\chi)), \chi \rangle = \langle \chi + \check{\chi}, \chi \rangle$$

gdzie jak wcześniej $\check{\chi}(m) = \chi(m^{-1})$. Jeśli $\chi(m) \neq \chi(m^{-1})$ to z ortogonalności charakterów (wniosek po lemacie 4.4 z wykładu 4) wynika że

$$\langle \mathrm{Res}(\mathrm{Ind}(\chi)), \chi \rangle = 1$$

czyli $\mathrm{Ind}(\chi)$ zawiera tylko jedną kopię reprezentacji M z charakterem χ, a to oznacza że $\mathrm{Ind}(\chi)$ jest reprezentacją nieprzywiedlną. Przy tym takie reprezentacje otrzymane z χ_1 i χ_2 są równoważne wtedy i tylko wtedy gdy $\chi_1 = \chi_2$ lub $\check{\chi}_1 = \chi_2$ (tylko wtedy charaktery są równe). $\check{\chi} = \chi$ oznacza że $\chi(m) = \chi(m^{-1}) = \chi(m)^{-1}$, czyli χ przyjmuje tylko wartości ze zbioru $\{-1, 1\}$. Grupa multyplikatywna ciała $F(q)$ jest cykliczna, więc są tylko dwa takie charaktery. A więc powyższa procedura indukcji daje $(q-3)/2$ różne reprezentacje nieprzywiedlne wymiaru $q+1$.

Gdy $\chi(m) = \chi(m^{-1})$, to sumując po klasach mamy

$$\langle \mathrm{Ind}(\chi), \mathrm{Ind}(\chi) \rangle = \frac{1}{(q-1)q(q+1)} \left(2(q+1)^2 + 2(q^2-1) + 4(q-3)q(q+1)/2\right)$$

$$= \frac{1}{(q-1)q} \left(2(q+1) + 2(q-1) + 4(q-3)q/2\right)$$

$$= \frac{1}{(q-1)q} \left(4q + 2(q-3)q\right) = \frac{1}{(q-1)}(2(q-3)+4) = \frac{2(q-1)}{q-1} = 2.$$

Czyli $\mathrm{Ind}(\chi)$ jest sumą dwu reprezentacji nieprzywiedlnych. Ponadto $\langle \mathrm{Res}(\mathrm{Ind}(\chi)), \chi \rangle = 2$. Dla $\chi = 1$ na mocy wzajemności Frobeniusa jedną ze składowych reprezentacji jest reprezentacja trywialna, druga reprezentacja ma wymiar q. W drugim przypadku, gdy $\chi(A(\lambda, c)) = -1$ dla λ będącego generatorem grupy multyplikatywnej ciała $F(q)$ otrzymamy dwie reprezentacje wymiaru $(q+1)/2$. Mianowicie, jak pokazaliśmy $SL(2, q)$ nie ma reprezentacji jednowymiarowych z charakterem przyjmującym dwie wartości. Jako reprezentacja M $\mathrm{Ind}(\chi)$ jest sumą dwu reprezentacji jednowymiarowych (trywialnych na N) i dwu reprezentacji wymiaru $(q-1)/2$ (nietrywialnych na N). Na mocy wzajemności Frobeniusa każda składowa $\mathrm{Ind}(\chi)$ musi zawierać reprezentację jednowymiarową M z charakterem χ, a więc jedyny możliwy podział to dwie pary typu charakter χ plus reprezentacja wymiaru $(q-1)/2$ nietrywialna na N.

Reguła wzajemności Frobeniusa mówi że w ten sposób opisaliśmy wszystkie reprezentacje nieprzywiedlne $SL(2, q)$ których obcięcie do M zawiera reprezentację jednowymiarową M (trywialną na N). Pozostałe reprezentacje po obcięciu do M są sumami reprezentacji wymiaru $(q-1)/2$ (nietrywialnych na N). Chcemy opisać rozkład tych reprezentacji jako reprezentacji M. W szczególności pojawia się pytanie czy reprezentacji nieprzywiedlna $SL(2, q)$ może pozostać nieprzywiedlna po ograniczeniu do M. Innymi słowy, czy reprezentacja nieprzywiedlna M przedłuża się do reprezentacji $SL(2, q)$. To się może zdażyć (jak pokażemy dalej). Istotne dla nas jest że takie przedłużenie, o ile istnieje to jest jednoznaczne. Mianowicie, charakter η przedłużenia jest jednoznacznie wyznaczony

na klasach sprzężoności elementów z M. Niech S oznacza zbiór elementów sprzężonych z elementami postaci $\pm n_c$ z niezerowymi n_c. Nasze wcześniejsze rachunki pokazują że $|S| = (q+1)|S \cap M|$. Czyli

$$\sum_{g\in S} |\eta(g)|^2 = (q+1) \sum_{g\in S\cap M} |\eta(g)|^2 = (q+1) \left(\sum_{g\in M} |\eta(g)|^2 - 2((q-1)/2)^2 \right)$$

$$= (q+1) \left((q-1)q - (q-1)^2/2 \right) > (q-1)q(q+1)/2.$$

Dla dwu różnych przedłużeń η_1 i η_2 mamy teraz

$$\langle \eta_1, \eta_2 \rangle = \frac{1}{(q-1)q(q+1)} \sum_g \eta_1(g)\bar{\eta}_2(g)$$

Mamy

$$\sum_g \eta_1(g)\bar{\eta}_2(g) = \sum_{g\in S} |\eta|^2(g) + \sum_{g\notin S} \eta_1(g)\bar{\eta}_2(g) \geq \sum_{g\in S} |\eta|^2(g) - \sum_{g\notin S} |\eta_1(g)||\eta_2(g)|$$

$$\geq \sum_{g\in S} |\eta|^2(g) - \frac{1}{2} \sum_{g\notin S} \left(|\eta_1(g)|^2 + |\eta_2(g)|^2 \right).$$

Lecz

$$(q-1)q(q+1) = (q-1)q(q+1)\langle \eta_i, \eta_i \rangle = \sum_{g\in S} |\eta_i(g)|^2 + \sum_{g\notin S} |\eta_i(g)|^2 =$$

$$= \sum_{g\in S} |\eta(g)|^2 + \sum_{g\notin S} |\eta_i(g)|^2$$

czyli

$$\sum_{g\notin S} |\eta_i(g)|^2 = (q-1)q(q+1) - \sum_{g\in S} |\eta(g)|^2.$$

A więc

$$\sum_g \eta_1(g)\bar{\eta}_2(g) \geq \sum_{g\in S} |\eta|^2(g) - \left((q-1)q(q+1) - \sum_{g\in S} |\eta(g)|^2 \right)$$

$$= 2 \sum_{g\in S} |\eta|^2(g) - (q-1)q(q+1) > 0.$$

Czyli $\langle \eta_1, \eta_2 \rangle \neq 0$ co daje $\langle \eta_1, \eta_2 \rangle = 1$ a więc równość $\eta_1 = \eta_2$.

Przeprowadzone rozumowanie pokazuje że co najwyżej 4 reprezentacje nieprzywiedlne $SL(2,q)$ są przedłużniami reprezentacji nieprzywiedlnych M nietrywialnych na N.

Policzmy teraz na różne sposoby ile kopii reprezentacji nieprzywiedlnych M wymiaru $(q-1)/2$ (nietrywialnych na N) zawiera reprezentacja regularna $SL(2,q)$. Dla uproszczenia rachunków oznaczmy $t = (q-1)/2$. Reprezentacja regularna M zawiera $4t$ kopii reprezentacji wymiaru t. Reprezentacja regularna $SL(2,q)$ po ograniczeniu do M daje $(q+1)$ kopii reprezentacji regularnej M. A więc w sumie mamy $4(q+1)t$ kopii reprezentacji wymiaru t. Licząc otrzymane wcześniej reprezentacje mamy $(q-3)/2 = t-1$ reprezentacji nieprzywiedlnych wymiaru $q+1 = 2(t+1)$ z których każda zawiera dwie podreprezentacje M wymiaru t. Mamy też dwie reprezentacje wymiaru $t+1$

zawierające po jednej reprezentacji wymiaru t i reprezentację wymiaru $q = 2t + 1$ zawierającą dwie kopie. Razem znane reprezentacje dają

$$2(t-1)(2(t+1)) + 2(t+1) + 2(2t+1) = 4t^2 + 6t = (4t+6)t$$

kopii. Czyli reprezentacje nie zawierające charakterów M dają

$$4(q+1)t - (4t+6)t = (4(q+1) - (4t+6))t = (4q + 4 - 2(q-1) - 6)t = 2qt$$

kopii reprezentacji wymiaru t. Niech k_j będzie ilością kopii w j-tej reprezentacji. Mamy $(q+1)/2+2$ reprezentacji do rozważenia. Co najmniej $(q+1)/2-2$ mają $k_j \geq 2$. Z tych reprezentacji dostaniemy

$$t \sum_j k_j^2 \geq ((q+1)/2 - 2)4t = (2q-6)t$$

kopii reprezentacji wymiaru t. Pozostałe 4 reprezentacje dają co najmniej $4t$ kopii. Gdyby choć jedno $k_j > 2$ to dostalibyśmy co najmniej

$$(2q-6)t + 4t + (9-4)t = (2q+3)t$$

kopii, co jest za dużo. A więc $k_j \leq 2$. Gdyby były cztery reprezentacje z $k_j = 1$ to suma byłaby za mała, równość otrzymujemy gdy są dwie reprezentacje z $k_j = 1$.

Obliczenie $\langle \eta, \eta \rangle$ podobne do przeprowadzonego przy badaniu jednoznaczności rozszerzenia pokazuje że dla $k_j = 2$ muszą być dwie różne reprezentacje M. Również podobnie można pokazać że jeśli jest reprezentacja nieprzywiedlna wymiaru $(q+1)/2$ z danym znakiem charakteru w $-I$ to nie ma reprezentacji wymiaru $(q-1)/2$ z tym samy znakiem charakteru w $-I$. Pozwala to dokładniej powiedzieć kiedy pojawiają się takie reprezentacje. Mianowicie charakter χ dający reprezentację wymiaru $(q+1)/2$ ma wartość -1 na generatorze grupy $q-1$ elementowej, czyli ma wartość -1 na $-I$ gdy $(q-1)/2$ jest nieparzyste, zaś wartość 1 na $-I$ gdy $(q-1)/2$ jest parzyste.

To nam jednoznacznie wyznacza rozkład reprezentacji nieprzywiedlnych $SL(2,q)$ na reprezentacje M. Jako że charaktery są stałe na klasach sprzężoności wyznacza to jednoznacznie charaktery reprezentacji na klasach sprzężoności elementów z M.

Aby wyznaczyć wartości charakterów na pozostałych klasach sprzężoności zauważmy że jako reprezentanty klas możemy wybrać elementy komutanta wybranego elementu. Dokładniej, jeśli g ma wartość własną z $F(q^2) - F(q)$ to oznaczmy przez U komutant g. Jak pokazaliśmy wcześniej U jest grupą cykliczną mającą $q+1$ elementów. Przekrój klasy sprzężoności elementu $h \in U - \{I, -I\}$ z U jest dwuelementowy i jest to $\{h, h^{-1}\}$. U ma $q+1$ reprezentacji jednowymiarowych, czyli $q+1$ charakterów jednowymiarowych ψ_j. Dowolną reprezentację $SL(2,q)$ możemy więc rozłożyć na sumę prostą reprezentacji z charakterami ψ_j. Aby to lepiej zrozumieć rozważmy reprezentacje indukowane z charakterów ψ_j. Jak poprzednio dla reprezentacji indukowanych z M dla elementów z U o różnych wartościach własnych indukowany charakter to $\psi_j + \check{\psi}_j$. Dla $\pm I$ wartość to $(q-1)q\psi_j(\pm I)$. Reguła wzajemności Frobeniusa mówi że $\mathrm{Ind}(\psi_j)$ zawiera te reprezentacje nieprzywiedlne w których pojawia się ψ_j. Jako że ψ_j i $\check{\psi}_j$ dają równoważne reprezentacje indukowane to pojawiają się one w reprezentacjach nieprzywiedlnych z takimi samymi krotnościami. Zauważmy że $\psi_j(-I)$ musi być takie same dla wszystkich charakterów wchodzących do reprezentacji nieprzywiedlnej. Ponadto, mamy $(q+1)$ charakterów, czyli $(q+1)/2$ dla danej wartości $\psi_j(-I)$, zaś interesujące nas reprezentacje mają wymiar $(q-1)$. Teraz łatwo zgadnąć jak wyglądają charaktery reprezentacji nieprzywiedlnych: te ψ_j które się zgadzają na $-I$ pojawiają się z krotnością 2, za wyjątkiem dwu które pojawiają

się z krotnością 1. Jako że suma charakterów z ustaloną wartością w $-I$ jest zerem poza $\{I,-I\}$ to prowadzi do wartości $-(\psi_j+\check{\psi}_j)$ poza $\{I,-I\}$ gdzie ψ_j jest charakterem który pojawia się z krotnością 1. Jeśli $\psi_j=\check{\psi}_j$ i $\psi_j(-I)$ jest przeciwnego znaku jak $\chi(-I)$ w reprezentacjach wymiaru $(q+1)/2$ to oczekujmy reprezentacji wymiaru $(q-1)/2$ w której "brakuje" charakteru ψ_j, czyli na $U-\{I,-I\}$ dostaniemy $-\psi_j$. Pozostaje pokazać że dobrze zgadneliśmy.

W tym celu zauważmy że reprezentacja regularna $SL(2,q)$ rozkłada się na dwie podreprezentacje równych wymiarów, jedną na której $-I$ działa jako identyczność, drugą na której $-I$ działa jako mnożenie przez -1. Dana reprezentacja nieprzywiedlna $SL(2,q)$ należy do dokładnie jednej z podprzestrzeni zależnie od tego jak $-I$ działa w reprezentacji. Na obu tych podprzestrzeniach działa podgrupa U z charakterm który jest zerem poza $U-\{I,-I\}$. Oznacza to że te podprzestrzenie zawierają charaktery U zgadzające się na $-I$ z równymi krotnościami. Reprezentacje indukowane z M mają charaktery znikające na $U-\{I,-I\}$ a więc również charaktery U zgadzające się na $-I$ występują w nich z równymi krotnościami. Oznacza to że suma reprezentacji nieprzywiedlnych zawierających jednowymiarowe reprezentacje M zawiera nietrywialne charaktery U zgadzające się na $-I$ z równymi krotnościami. Charakter trywialny trochę komplikuje sytuację: reprezentacja trywialna zawiera tylko trywialny charakter U, zaś reprezentacja wymiaru q zawiera charakter trywialny U z krotnością 1 a pozostałe $(q-1)/2$ zgodne charaktery z krotnością 2. Jako że reprezentacja wymiaru q występuje w reprezentacji regularnej q-krotnie oznacza to że w sumie reprezentacji zawierających M charakter trywialny U pojawia się z krotnością mniejszą o $q-1$ od pozostałych charakterów.

Odejmując od reprezentacji regulanej reprezentacje zawierających jednowymiarowe reprezentacje M widzimy że suma reprezentacji wymiaru $(q-1)$ i $(q-1)/2$ zgodnych na $-I$ zawiera nietrywialne zgodne charaktery U z równymi krotnościami, zaś charakter trywialny z krotnością o $q-1$ większą od pozostałych. Jako że te reprezentacje występują w reprezentacji regularnej z krotnościami $(q-1)$ i $(q-1)/2$ odpowiednio jak weźniemy sumę reprezentacji wymiaru $(q-1)$ z krotnością 2 zaś wymiaru $(q-1)/2$ z krotnością 1 (wszystkie zgodne na $-I$), to będzie ona zawierała zgodne charaktery nietrywialne U z równymi krotnościami. A więc charakter tej sumy będzie stały na $U-\{I,-I\}$ (zero jeśli $-I$ działa jako mnożenie przez -1). Jako że charakter trywialny występuje w pełnej sumie z krotnością większą o $q-1$ po podzieleniu krotności przez $(q-1)/2$ (co zrobiliśmy wyżej) jego krotność będzie o 2 większa od innych charakterów. W więc jeśli $-I$ działa jako mnożenie przez 1 to stała w naszej sumie faktycznie będzie równa 2.

Czyli charakter tej sumy jest jednoznacznie wyznaczony przez nasze rozważania. Oznaczmy ten charakter przez $\omega_\pm$ gdzie indeks wybiera na co ma przejść $-I$.

Twierdzimy że zgadnięte wyżej charaktery są całkowitoliczbowymi kombinacjami liniowymi prawdziwych charakterów. Mianowicie oznaczmy przez η_j charakter odpowiadający ψ_j (czyli równy $-(\psi_j+\check{\psi}_j)$ na $U-\{I,-I\}$). Twierdzimy że

$$\eta_j=\omega_\pm+\theta_j-\mathrm{Ind}(\psi_j).$$

gdzie θ_j jest sumą (z krotnościami) charakterów reprezentacji nieprzywiedlnych zawierających charakter M i zawartych w $\mathrm{Ind}(\psi_j)$.

Najpierw rozpatrzmy przypadek gdy $-I$ działa jako mnożenie przez -1 i wszystkie reprezentacje wchodzące w ω_- są wymiaru $(q-1)$. Jako że krotności nietrywialnych charakterów U, zgodnych na $-I$ są równe w ω_- i w θ_j to dają one zerowy wkład na $U-\{I,-I\}$, czyli na $U-\{I,-I\}$ mamy równość. Zauważmy że θ_j nie zależy od j (z reguły wzajemności, bo charaktery odpowiednich reprezentacji M są zerem na $U-\{I,-I\}$). Charakter $\mathrm{Ind}(\psi_j)$ poza $U-\{I,-I\}$ nie zależy od j więc by pokazać równość poza $U-\{I,-I\}$ możemy wysumować po j. Mamy $(q+1)/2$ wyrazów i

η_j pojawią się dwukrotnie więc lewa strona da $\omega_\pm$ (poza $U - \{I, -I\}$ wiemy że η_j zgadzają się z prawdziwymi charakterami) czyli dostaniemy

$$\omega_\pm = \frac{q+1}{2}\omega_\pm - \sum(\theta_j - \mathrm{Ind}(\psi_j))$$

Każda z reprezentacji wymiaru $q-1$ pojawi się sumie $\mathrm{Ind}(\psi_j)$ z krotnością $q-1$, inne reprezentacje wykasują się z θ_j. Czyli nasza równość jest równoważna

$$\omega_\pm = \frac{q+1}{2}\omega_\pm - \frac{q-1}{2}\omega_\pm$$

gdzie mamy $\frac{q-1}{2}$ bo w $\omega_\pm$ jest wbudowana krotność 2. Ale równość wyżej wynika z $\frac{q+1}{2} - \frac{q-1}{2} = 1$. Czyli dostaliśmy równość w tym uproszczonym przypadku. Powyżej niejawnie zakładaliśmy że $q+1$ jest podzielne przez 4, tzn. że ψ_j się podzielą w pary. Lecz jeśli nie ma reprezentacji wymiaru $(q-1)/2$ z danym znakiem na $-I$ to jest reprezentacja wymiaru $(q+1)/2$ z tym znakiem. Czyli odpowiedni charakter χ na M ma wartość -1 na $-I$. Jak zauważyliśmy oznacza to że $(q-1)/2$ jest nieparzyste, czyli $(q+1)/2$ jest parzyste, czyli faktycznie $q+1$ jest podzielne przez 4. Jeśli pojawią się reprezentacje wymiaru $(q-1)/2$ to odpowiednie ψ_j jest sumą charakterów dwu reprezentacji. Jako że ψ_j da je tylko raz to w sumie po lewej stronie pojawią się z krotnością 1 czyli też dostaniemy właściwy wkład do sumy.

W przypadku gdy $-I$ działa jako identyczność na $U - \{I, -I\}$ jak poprzednio krotności nietrywialnych charakterów U w ω_+ i θ_j są równe. Charakter trywialny występuje w ω_+ z krotnością o 2 większą od innych. Lecz dla nietrywialnego ϕ_j reprezentacja $\mathrm{Ind}(\phi_j)$ zawiera reprezentację wymiaru q z krotnością 2. Pozostałe reprezentacje zawarte w $\mathrm{Ind}(\phi_j)$ dają równe krotności. A więc krotność trywialnego charakteru U w θ_j jest o 2 mniejsza od innych charakterów. Czyli w sumie $\omega_+ + \theta_j$ krotności zgodnych charakterów U są równe, czyli $\omega_+ + \theta_j$ jest zerem na $U - \{I, -I\}$. A więc dostaliśmy równość na $U - \{I, -I\}$.

Poza $U - \{I, -I\}$ dla nietrywialnego ψ_j człon θ_j jest taki sam. Dla trywialnego ψ_j człon θ_j różni się brakiem reprezentacji wymiaru q i obecnością charakteru trywialnego. Jeśli jak poprzednio wysumujemy wszystkie człony używając θ dla charakterów nietrywialnych to poza pożądanymi członami dostaniemy dodatkowe: po lewej stronie η_j dla trywialnego ψ_j nie odpowiada żadnej reprezentacji. Po prawej przez użycie θ_j dla innego j dostaniemy dodatkowo charakter reprezentacji wymiaru q minus charakter trywialny. Ale poza $U - \{I, -I\}$ nasze η_j i charakter reprezentacji wymiaru q minus charakter trywialny są równe, czyli te dodatkowe człony się skasują i dostaniemy równość. Reprezentacje wymiaru $(q-1)/2$ uwzględniamy jak poprzednio.

Teraz wystarcza obliczyć $\langle \eta_j, \eta_j \rangle$. Dla η_j odpowiadającym reprezentacjom wymiaru $q-1$ dostaniemy $\langle \eta_j, \eta_j \rangle = 1$. Ale wiemy że η_j jest całkowitoliczbową kombinacją liniową charakterów, czyli $\langle \eta_j, \eta_j \rangle$ jest sumą kwadratów współczynników. Czyli tylko jeden współczynnik jest niezerowy i ma on wartość bezwzględną 1, czyli jest to 1 lub -1. -1 jest niemożliwe, bo wartość w I jest dodatnia. A więc faktycznie η_j jest charakterem. Jeśli η_j odpowiada sumie dwu reprezentacji to licząc $\langle \eta_j, \eta_j \rangle$ dostaniemy 2. A więc η_j jest sumą dwu charakterów ze współczynnikami ± 1. Znowu wartość dla I pokazuje że oba współczynniki to 1. Pozostaje pokazać że składniki sumy są takie jak zgadliśmy. Lecz teoria Galois mówi że wartości obu charakterów na U muszą się zgadzać. Mianowicie, wartości charakterów są w ciele generowanym przez pierwiastki stopnia $(q-1)q(q+1)$ z jedynki. Jako że q jest względnie pierwsze z $(q-1)(q+1)$ to ta grupa jest produktem grup rzędu q i rzędu $(q-1)(q+1)$. A więc element produktu jest generatorem jeśli składowe są generatorami. Wiadomo że automorfizmy ciała generowanego przez pierwiastki z jedynki stopnia n odwzorowują generator na generator

i wybrany generator można przekształcić na dowolny inny. A więc grupa automorfizmów dla pierwiastków rzędu $(q-1)q(q+1)$ jest produktem grup dla pierwiastków rzędu q i grupy dla pierwiastków rzędu $(q-1)(q+1)$. Na N nasz charakter przyjmuje wartości w ciele generowanym przez pierwiastki stopnia q. Na U przyjmuje wartości w ciele generowanych przez pierwiastki stopnia $q+1$. A więc można niezależnie zadziałać na N i na U. Lecz grupa Galois przeprowadza charaktery na charaktery. Więc na U charakter musi być niezmienniczy na automorfizmy bo inaczej dostalibyśmy zbyt wiele charakterów. Wiedząc to widać że na U musimy mieć podaną wcześniej wartość.

Niżej podajemy w tabelce wynik naszych obliczeń. By zaoszczędzić miejsca używamy uproszczonych oznaczeń. Jako że charakter na elementach typu $-n_c$ jest wyznaczony przez wartość na n_c i wartość na $-I$ pomijamy klasy typu $-n_c$. Wartości na dwu klasach typu n_c są ze sobą związane więc podajemy tylko dla jednej. Dla charakterów wymiaru $(q+1)/2$ i $(q-1)/2$ wystarczy podanie jednego z pary.

Charakter	I	$-I$	$\lambda \in F(q)$	$\lambda \in F(q^2)$	N
tryw.	1	1	1	1	1
$\chi = 1$	q	q	1	-1	0
$\chi(\lambda) \neq \chi(\lambda)^{-1}$	$q+1$	$\chi(-1)(q+1)$	$\chi(\lambda)+\chi(\lambda)^{-1}$	0	1
$\chi(\lambda) = \chi(\lambda)^{-1}$	$(q+1)/2$	$\chi(-1)(q+1)/2$	$\chi(\lambda)$	0	$\frac{1}{2}+\gamma$
$\psi \neq \check{\psi}$	$q-1$	$\psi(-I)(q-1)$	0	$-(\psi(\lambda)+\psi(\lambda)^{-1})$	0
$\psi = \check{\psi}$	$(q-1)/2$	$\psi(-I)(q-1)/2$	0	$-\psi(\lambda)$	$\frac{-1}{2}+\gamma$