Uniwersytet Warszawski
Wydział Matematyki, Informatyki i Mechaniki

Daniel Malinowski
Nr albumu: 292680

Metody dowodzenia prostoty grup

Praca licencjacka
na kierunku MATEMATYKA

Praca wykonana pod kierunkiem
dra hab. Zbigniewa Marciniaka
Instytut Matematyki

Czerwiec 2013

Oświadczenie kierującego pracą

Potwierdzam, że niniejsza praca została przygotowana pod moim kierunkiem i kwalifikuje się do przedstawienia jej w postępowaniu o nadanie tytułu zawodowego.

Data Podpis kierującego pracą

Oświadczenie autora (autorów) pracy

Świadom odpowiedzialności prawnej oświadczam, że niniejsza praca dyplomowa została napisana przeze mnie samodzielnie i nie zawiera treści uzyskanych w sposób niezgodny z obowiązującymi przepisami.

Oświadczam również, że przedstawiona praca nie była wcześniej przedmiotem procedur związanych z uzyskaniem tytułu zawodowego w wyższej uczelni.

Oświadczam ponadto, że niniejsza wersja pracy jest identyczna z załączoną wersją elektroniczną.

Data Podpis autora (autorów) pracy

Streszczenie

Słowa kluczowe

grupa prosta, grupa alternująca, grupa specjalna rzutowa liniowa, lemat Iwasawy

Dziedzina pracy (kody wg programu Socrates-Erasmus)

11.1 Matematyka

Klasyfikacja tematyczna

20. Group theory and generalizations

Tytuł pracy w języku angielskim

Methods of proving the simplicity of groups

Spis treści

Wprowadzenie

Rozdział 1

Wiadomości wstępne

Rozdział ten zawiera przypomnienie pewnych definicji, własności i twierdzeń omawianych na podstawowym kursie algebry I oraz ustalenie oznaczeń.

W niniejszej pracy dużymi literami alfabetu (np. G, H, K) będą oznaczane grupy. Ich elementy będą oznaczanie małymi literami alfabetu (np. g, h, k), przy czym przez e będzie zawsze oznaczany element neutralny. Rozważane grupy będą (w większości) nieprzemienne, w związku z tym będzie stosowany zapis multiplikatywny.

1.1. Grupy proste

Zacznijmy zatem od przypomnienia podstawowej definicji w tej pracy.

Definicja 1.1.1 *Nietrywialną grupę G nazwiemy* grupą prostą*, jeżeli nie ma ona podgrup normalnych różnych od $\{e\}$ oraz samej siebie.*

Fakt 1.1.1 *Jedynymi (z dokładnością do izomorfizmu) przemiennymi grupami prostymi są skończone grupy cykliczne o liczbie elementów będącą liczbą pierwszą.*

Jest to prosta konsekwencja tego, że w grupach przemiennych wszystkie podgrupy są podgrupami normalnymi.

1.2. Twierdzenia o izomorfizmie

Przejdźmy teraz do podstawowych twierdzeń o izomorfizmie.

Twierdzenie 1.2.1 (Pierwsze twierdzenie o izomorfizmie)
Niech G, H – grupy, $\varphi\colon G \to H$ homomorfizm, $K = \ker\varphi$ oraz $H' = \mathrm{im}\varphi$.
Wówczas zachodzi izomorfizm

$$G/K \simeq H'$$

Twierdzenie 1.2.2 (Drugie twierdzenie o izomorfizmie)
Niech G – grupa, H_1, H_2 podgrupy normalne G, przy czym $H_2 \leqslant H_1$.
Wówczas $H_2 \trianglelefteq H_2$, $H_1/H_2 \trianglelefteq G/H_2$ i zachodzi izomorfizm

$$(G/H_2)/(H_1/H_2) \simeq G/H_1$$

Twierdzenie 1.2.3 (Trzecie twierdzenie o izomorfizmie)
Niech G – grupa, H_1 podgrupa normalna G, H podgrupa H_1.
Wówczas $H \cap H_1 \trianglelefteq H$ oraz zachodzi izomorfizm

$$H/(H \cap H_1) \simeq H \cdot H_1/H_1$$

1.3. Komutant i abelianizacja

Poniżej przedstawionych jest kilka użytecznych wiadomości o komutancie.

Definicja 1.3.1 *Niech G będzie dowolną grupą. Wówczas* komutantem grupy G *nazywamy podgrupę G generowaną przez wszystkie elementy postacji $aba^{-1}b^{-1}$, gdzie $a, b \in G$. Komutant grupy G oznaczamy przez $[G, G]$.*

Twierdzenie 1.3.1 (O komutancie)
Komutant $[G, G]$ jest podgrupą normalną G, przy czym grupa ilorazowa $G/[G, G]$ jest grupą abelową. Ponadto dla dowolnej podgrupy normalnej $H \trianglelefteq G$ takiej, że G/H jest abelowa, zachodzi $[G, G] \leqslant H$.

Definicja 1.3.2 *Przekształcenie kanoniczne $G \to G/[G, G]$ (rzutowanie na grupę ilorazową) nazywamy abelianizacją.*

O abelianizacji (w przeciwieństwie do twierdzenia o komutancie) nie będzie więcej wspominane w tej pracy, ale ta definicja została przytoczona w celu domknięcia podstawowych faktów o komutancie. Ważniejszym dla nas pojęciem jest pojęcie grupy doskonałej:

Definicja 1.3.3 Grupą doskonałą *nazwiemy dowolną grupę, która jest równa swojemu komutantowi.*

Grupami doskonałymi zajmiemy się w dalszej części pracy – przy lemacie Iwasawy. Na razie zauważmy prosty fakt:

Fakt 1.3.1 *Nieprzemienne grupy proste są grupami doskonałymi.*

1.4. Działanie grupy na zbiorze

Na koniec tego rozdziału przyjrzyjmy się jednej z ważniejszej własności grup – ich możliwości działania na zbiorach.

Definicja 1.4.1 *Niech G będzie grupą, a X – zbiorem. Mówimy, że ρ* jest działaniem grupy G na zbiorze X, *jeżeli dla każdego $g \in G$ przyporządkowane jest przekształcenie $\rho_g \colon X \to X$, takie, że:*

- $\rho_e = \mathrm{id}_X$,
- $\rho_g \circ \rho_h = \rho(gh)$, *dla dowolnych $g, h \in G$.*

Jeżeli sposób działania (ρ) wynika z kontekstu, to zamiast $\rho_g(x)$ będziemy pisać x^g.

Zgrabniejszy opis działania grupy na zbiorze daje poniższe twierdzenie. Zanim jednak do niego przejdziemy, przypomnijmy sobie jeszcze jedną definicję.

Definicja 1.4.2 *Niech X będzie dowolnym zbiorem. Wówczas* grupą symetrii zbioru X *nazywamy zbiór bijekcji $X \to X$, wraz z operacją składania. Grupę tę oznaczamy S_X.*

Twierdzenie 1.4.1 (O działaniu grupy na zbiorze)
Niech G będzie grupą, a X – zbiorem. Wówczas ρ jest działaniem G na X wtedy i tylko wtedy, gdy ρ jest homomorfizmem z G w grupę symetrii zbioru X.

Z działaniem grupy na zbiorze związane jest dużo ważnych definicji i twierdzeń. Poniżej przytoczone są te najistotniejsze z punktu widzenia tej pracy.

Definicja 1.4.3 *Załóżmy, że ρ jest działaniem grupy G na zbiorze X oraz $x \in X$. Wówczas:*

a) Stabilizatorem punktu x (grupą izotropii x) *nazwiemy zbiór elementów* $\{g \in G \colon x^g = x\}$. *Stabilizator punktu x oznaczamy G_x.*

b) Orbitą punktu x *nazwiemy podzbiór X równy* $\{y \in X \colon \exists_{g \in G} x^g = y\}$. *Orbitę punktu x oznaczamy $G(x)$.*

Podstawowe własności tych obiektów przedstawia następujący fakt:

Fakt 1.4.1 *Załóżmy, że ρ jest działaniem grupy G na zbiorze X oraz $x, y \in X$. Wówczas:*

a) G_x jest podgrupą G.

b) $G(x)$ i $G(y)$ są równe lub rozłączne (orbity tworzą rozbicie zbioru X).

Zanim przejdziemy do ważniejszych twierdzeń opisujących orbity i stabilizatory, przypomnijmy wcześniej, jakie własności może mieć działanie grupy na zbiorze.

Definicja 1.4.4 *Załóżmy, że ρ jest działaniem grupy G na zbiorze X.*

a) ρ jest działaniem tranzytywnym (przechodnim)*, jeżeli wszystkie elementy X tworzą jedną orbitę.*

b) ρ jest działaniem wiernym*, jeżeli ρ jest iniekcją jako homomorfizm $G \to S_X$.*

Jak to zostało wcześniej zapowiedziane, na koniec przytoczmy dwa ważne twierdzenie pokazujące zależność między orbitami a stabilizatorami.

Twierdzenie 1.4.2 (O orbitach i stabilizatorach)
Załóżmy, że ρ jest działaniem grupy G na zbiorze X, przy czym X jest zbiorem skończonym. Ponadto $x \in X$. Wówczas $|G(x)| = [G : G_x]$.

Twierdzenie 1.4.3 (Równanie klas)
Przy założeniach z poprzedniego twierdzenia zachodzi

$$|X| = \sum_{i=1}^{k} [G : G_{x_i}],$$

gdzie $x_1, x_2, \cdots, x_k$ to reprezentanci wszystkich orbit działania ρ.

Rozdział 2

Prostota grupy alternującej A_n

Rozdział 3

Lemat Iwasawy

W tym rozdziale przedstawione zostanie jedno z ważniejszych narzędzi do dowodzenia prostoty grup – lemat Iwasawy. Lecz najpierw wprowadzimy nowe pojęcie – prymitywność.

3.1. Prymitywne działania grupy

Jak zostało to już wspomniane w wiadomościach wstępnych, działanie grupy G na zbiorze X jest tranzytywne, jeżeli elementy X tworzą jedną orbitę, czyli dla dowolnych $x, y \in X$ istnieje $g \in G$ takie, że $x^g = y$. Teraz uogólnimy to pojęcie.

Definicja 3.1.1 *Załóżmy, że ρ jest działaniem grupy G na zbiorze X.*
ρ jest działaniem k-tranzytywnym (k-przechodnim)*, jeżeli dla dowolnych ciągów k elementowych $(a_1, a_2, \cdots, a_k)$ oraz $(b_1, b_2, \cdots, b_k)$, które składają się z różnych elementów z X istnieje taki element g z grupy G, że $a_i^g = b_i^g$ dla każdego $i = 1, 2, \cdots, k$.*

W szczególności 1-tranzytywność to jest dokładnie to samo, co zwykła tranzytywność.

Aby lepiej zilustrować to pojęcie, policzmy ilu tranzytywne jest naturalne działanie grupy S_n oraz A_n na zbiorze $X = \{1, 2, \cdots, n\}$, tzn. takie, w którym $i^\sigma = \sigma(i)$.

Jak łatwo zauważyć, działanie S_n jest n-tranzytywne – skoro S_n składa się ze wszystkich permutacji, to zawsze możemy odwzorować ciąg $(a_1, a_2, \cdots, a_n)$ na $(b_1, b_2, \cdots, b_n)$, gdyż jak założyliśmy w definicji, wszystkie a_i jaki i wszystkie b_i są parami różne. Stąd również działanie S_n jest k-tranzytywne dla każdego $k \leqslant n$.

Natomiast w A_n nie ma wszystkich permutacji, zatem działanie A_n nie może być n-tranzytywne. Nie może być również $(n-1)$-tranzytywne, gdyż skoro mówimy na co przechodzą $n-1$ elementy X i ma to być permutacja, to wartość ostatniego elementu też jest ustalona, czyli wybór $(n-1)$ pozycji jest tak na prawdę wyborem wszystkich n pozycji, a na wszystkich elementach nie możemy dowolnie ustalić permutacji. Zauważmy jednak, że działanie A_n jest $(n-2)$-tranzytywne. Rzeczywiście, chcąc żeby a_i przeszło na b_i dla $i = 1, 2, \cdots, (n-2)$ mamy do wyboru dwie permutacje. Jedna z nich odwzorowuje $x \mapsto y, x' \mapsto y'$, a druga $x \mapsto y', x' \mapsto y$, gdzie x, x' to elementy nie wybrane na a_i, a y, y' to elementy nie wybrane na b_i. Ale te permutacje różnią się o transpozycję (y, y'), zatem jedna z nich jest parzysta, czyli należy do A_n, więc rzeczywiście możemy odwzorować $(a_1, a_2, \cdots, a_{n-2})$ na $(b_1, b_2, \cdots, b_{n-2})$. Stąd działanie S_n jest k-tranzytywne dla każdego $k \leqslant n-2$.

Wprowadzimy teraz własność prymitywności. Będzie to coś pomiędzy tranzytywnością a 2-tranzytywnością.

Definicja 3.1.2 *Załóżmy, że ρ jest działaniem grupy G na zbiorze X.*
Systemem bloków *działania ρ nazywamy podział zbioru X zachowywany przez ρ, tzn. rodzinę zbiorów $\mathfrak{A} = \{Y_i : i \in I\}$, które są niepuste, parami rozłączne, sumują się do X oraz dla dowolnych $Y \in \mathfrak{A}, x, x' \in Y$ oraz $g \in G$ oba elementy x^g oraz x'^g znajdują się razem w jednym zbiorze $Y' \in \mathfrak{A}$.*

Zauważmy, że zawsze mamy co najmniej dwa systemy bloków – jeden blok z całym zbiorem $\mathfrak{A} = \{X\}$ oraz system z wszystkimi blokami jednoelementowymi $\mathfrak{A} = \{\{x\} : x \in X\}$. W związku z tym naturalna jest definicja:

Definicja 3.1.3 Nietrywialnym systemem bloków *nazywamy dowolny system bloków, który jest różny od dwóch wyżej wspomnianych – z jednym blokiem lub z blokami jednoelementowymi.*

Rozdział 4

Prostota specjalnej rzutowej grupy liniowej $PSL_n(k)$

Bibliografia

[A] C, *D*, E