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, specjalna rzutowa grupa 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.

1.1. Oznaczenia

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.

Jeżeli H oraz K są podgrupami grupy G, to przez $HK = H \cdot K$ będzie oznaczana podgrupa G generowana przez wszystkie elementy postaci $h \cdot k$, gdzie $h \in H$ oraz $k \in K$.

W związku z tym oznaczeniem warto przytoczyć twierdzenie:

Twierdzenie 1.1.1.
Jeżeli H oraz K są podgrupami grupy G, przy czym K jest podgrupą normalną, to $HK = \{hk : h \in H, k \in K\}$.

1.2. Grupy proste

Przypomnijmy teraz podstawową definicji w tej pracy.

Definicja 1.2.1. *Nietrywialną grupę G nazwiemy* grupą prostą, *jeżeli nie ma ona podgrup normalnych różnych od $\{e\}$ oraz samej siebie.*

Fakt 1.2.1. *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.

1.3. Twierdzenia o izomorfizmie

Przejdźmy teraz do podstawowych twierdzeń o izomorfizmie.

Twierdzenie 1.3.1 (Pierwsze twierdzenie o izomorfizmie)**.**
Niech G, H – grupy, $\varphi: G \to H$ homomorfizm, $K = \ker\varphi$ oraz $H' = \mathrm{im}\varphi$.
Wówczas zachodzi izomorfizm

$$G/K \simeq H'$$

Twierdzenie 1.3.2 (Drugie twierdzenie o izomorfizmie).
Niech G – grupa, H_1, H_2 podgrupy normalne G, przy czym $H_2 \leqslant H_1$.
Wówczas $H_2 \trianglelefteq H_1$, $H_1/H_2 \trianglelefteq G/H_2$ i zachodzi izomorfizm

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

Twierdzenie 1.3.3 (Trzecie twierdzenie o izomorfizmie).
Niech G – grupa, H_1 podgrupa normalna G, H podgrupa G.
Wówczas $H \cap H_1 \trianglelefteq H$ oraz zachodzi izomorfizm

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

1.4. Komutant i abelianizacja

Poniżej przedstawionych jest kilka użytecznych wiadomości o komutancie.

Definicja 1.4.1. *Niech G będzie dowolną grupą. Wówczas* komutantem grupy G *nazywamy podgrupę G generowaną przez wszystkie elementy postaci $aba^{-1}b^{-1}$, gdzie $a, b \in G$. Komutant grupy G oznaczamy przez $[G, G]$.*

Twierdzenie 1.4.1 (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 1.4.2. *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 1.4.3. Grupą doskonałą *nazwiemy dowolną grupę, która jest równa swojemu komutantowi.*

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

Fakt 1.4.1. *Nieprzemienne grupy proste są grupami doskonałymi.*

1.5. Działanie grupy na zbiorze

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

Definicja 1.5.1. *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 1.5.2. *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 1.5.1 (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 1.5.3. *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 1.5.1. *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 1.5.4. *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 $G \to S_X$.*

c) ρ jest działaniem nietrywialnym*, jeżeli ρ nie jest zerowe jako homomorfizm $G \to S_X$.*

Jak to zostało wcześniej zapowiedziane, na koniec przytoczmy kilka ważnych twierdzeń pokazujących zależność między orbitami a stabilizatorami.

Twierdzenie 1.5.2.
Załóżmy, że ρ jest działaniem grupy G na zbiorze X oraz $x, y \in X$ należą do jednej orbity. Wówczas grupy G_x oraz G_y są wzajemnie sprzężone.

Twierdzenie 1.5.3 (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 1.5.4 (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

Zanim udowodnimy główną tezę tego rozdziału, czyli fakt, że A_n jest grupą prostą dla $n \geqslant 5$, przypomnimy znane własności o tej grupie oraz udowodnimy kilka mniej znanych.

2.1. Przypomnienie wiadomości o S_n oraz A_n

W poprzednim rozdziale wprowadziliśmy definicję grupy S_X symetrii zbioru X. Ważnym przypadkiem szczególnym jest sytuacja, gdy X jest zbiorem skończonym o n elementach. Wówczas, jako że grupy symetrii zbiorów równolicznych są izomorficzne, grupę S_X będziemy oznaczać S_n i bez straty ogólności przyjmiemy, że jej elementami są permutacje zbioru $\{1, 2, \cdots, n\}$.

Fakt 2.1.1. *Rozmiar grupy S_n wynosi $n!$.*

Ważnym sposobem przedstawienia elementów grupy S_n jest rozkład na cykle.

Definicja 2.1.1. *Permutację $\sigma \in S_n$ nazwiemy* cyklem długości k*, jeżeli istnieją różne elementy $c_1, c_2, \cdots, c_k \in \{1, 2, \cdots, n\}$ takie, że*

$$\sigma(x) = \begin{cases} c_{i+1}, & \textit{jeżeli } x = c_i \\ c_1, & \textit{jeżeli } x = c_k \\ x, & \textit{w przeciwnym przypadku} \end{cases}$$

Wówczas permutację σ zapisujemy jako $(c_1, c_2, \cdots, c_k)$.

Oczywiście zapis cyklu nie jest jednoznaczny – $(c_1, c_2, \cdots, c_k) = (c_k, c_1, c_2, \cdots, c_{k-1}) = (c_2, c_3, \cdots, c_k, c_1)$. Ponadto ten zapis ma tylko sens, gdy wiemy, w jakiej grupie symetrii ten cykl się znajduje.

Dla $\sigma \in S_n$, jeżeli weźmiemy element zbioru $\{1, 2, \cdots, n\}$, będziemy na niego działać permutacją σ tak długo, aż dojdziemy do niego samego, to z otrzymanych elementów możemy stworzyć cykl. Powtarzając tę procedurę z niewybranymi jeszcze elementy dostaniemy rozkład na cykle:

Twierdzenie 2.1.1.
Każdą permutację $\sigma \in S_n$ można przedstawić jako iloczyn rozłącznych cykli, czyli takich $(c_1, c_2, \cdots, c_k)$, $(d_1, d_2, \cdots, d_l)$, że $\{c_1, c_2, \cdots, c_k\} \cap \{d_1, d_2, \cdots, d_l\} = \emptyset$ przy czym każdy element ze zbioru $\{1, 2, \cdots, n\}$ znajduje się w pewnym cyklu. Przedstawienie jest jednoznaczne z dokładnością do kolejności cykli.

Przejdźmy teraz do zdefiniowania podgrupy A_n grupy S_n. Załóżmy do końca tego rozdziału, że $n \geqslant 2$.

Definicja 2.1.2. Transpozycją *nazwiemy dowolny cykl długości 2.*

Transpozycję są cegiełkami, z których można budować permutacje, tzn.

Twierdzenie 2.1.2.
Każda permutacja jest iloczynem pewnej liczby transpozycji.

Rozkład permutacji na transpozycje nie musi być jednoznaczny. Np. $(1,2)(2,4)(4,2) = (1,2)$ oraz $(1,2)(2,3)(3,4)(4,1) = (4,2)(2,3)$. Jednoznaczna natomiast jest parzystość liczby transpozycji w rozkładzie.

Definicja 2.1.3. *Permutację o parzystej liczbie transpozycji w rozkładzie nazwiemy* parzystą, *w przeciwnym przypadku –* nieparzystą. *Podgrupę wszystkich permutacji parzystych grupy S_n nazywamy* grupą alternującą *i oznaczamy A_n.*

Poprawność definicji wynika z twierdzenia:

Twierdzenie 2.1.3.
Parzystość liczby transpozycji w rozkładzie permutacji na transpozycje nie zależy od rozkładu. Permutacje o parzystej liczbie transpozycji tworzą podgrupę normalną grupy S_n indeksu 2, czyli rozmiaru $n!/2$.

Warto tu jeszcze wspomnieć o tym, które cykle są permutacjami parzystymi, a które nie. Mianowicie, trochę wbrew swojej nazwie, cykle o długości nieparzystej są parzyste, a o długości parzystej – nieparzyste. Stąd prawdziwy jest fakt:

Fakt 2.1.2. *Permutacja $\sigma \in S_n$ jest parzysta wtedy i tylko wtedy, kiedy w rozkładzie na cykle zawiera parzystą liczbę cykli o parzystej długości.*

2.2. Klasy sprzężoności S_n i A_n

W celu udowodnienia prostoty grupy A_n musimy zbadać klasy sprzężoności tej grupy. Najpierw zajmiemy się jednak prostszym problemem – klasami sprzężoności S_n.

Definicja 2.2.1. Typem cyklowym *permutacji $\sigma \in S_n$ nazwiemy listę długości cykli występujących w σ, tzn. ciąg $(1^{i_1}, 2^{i_2}, \cdots, n^{i_n})$, gdzie i_k to liczba cykli długości k w rozkładzie σ na cykle rozłączne.*

W celu uproszczenia zapisu można omijać długości cykli, które nie występują w rozkładzie. Dla przykładu typem cyklowym transpozycji jest $(1^{n-2}, 2^1)$, a identyczności – (1^n).

Okazuje się, że w grupie S_n typ cyklowy jednoznacznie wskazuje na klasę sprzężoności:

Twierdzenie 2.2.1.
Permutacje $\pi, \sigma \in S_n$ są wzajemnie sprzężone wtedy i tylko wtedy, gdy ich indeks cyklowy jest taki sam.

Dowód. Niech $\lambda = (c_1, c_2, \cdots, c_k)$ będzie cyklem w S_n, $c_{k+1} = c_1$ oraz $\gamma \in S_n$. Wówczas $(\gamma^{-1}\lambda\gamma)(\gamma(c_i)) = (\lambda\gamma)(c_i) = \gamma(c_{i+1})$, na pozostałych elementach $\gamma^{-1}\lambda\gamma$ jest stałe, zatem $\gamma^{-1}(c_1, c_2, \cdots, c_k)\gamma = (\gamma(c_1), \gamma(c_2), \cdots, \gamma(c_k))$. Stąd również

$$\gamma\Big(c_1^1, c_2^1, \cdots, c_{k^1}^1\Big) \cdots \Big(c_1^m, c_2^m, \cdots, c_{k^m}^m\Big)\gamma^{-1} =$$

$$= \gamma\Big(c_1^1, c_2^1, \cdots, c_{k^1}^1\Big)\gamma^{-1}\gamma\cdots\gamma^{-1}\gamma\Big(c_1^m, c_2^m, \cdots, c_{k^m}^m\Big)\gamma^{-1} =$$

$$= \Big(\gamma(c_1^1), \gamma(c_2^1), \cdots, \gamma(c_{k^1}^1)\Big)\cdots\Big(\gamma(c_1^m), \gamma(c_2^m), \cdots, \gamma(c_{k^m}^m)\Big)$$

Jeżeli cykle $\Big(c_1^1, c_2^1, \cdots, c_{k^1}^1\Big)\cdots\Big(c_1^m, c_2^m, \cdots, c_{k^m}^m\Big)$ były rozłączne, to również powstałe po sprzężeniu cykle są rozłączne. Jest ich tyle samo i mają te same długości, zatem rzeczywiście sprzężenie zachowuje typ permutacji.

Wystarczy jeszcze pokazać, że permutacje o tym samym typie są sprzężone. Niech $\pi = \Big(c_1^1, c_2^1, \cdots, c_{k^1}^1\Big)\cdots\Big(c_1^m, c_2^m, \cdots, c_{k^m}^m\Big)$ oraz $\sigma = \Big(d_1^1, d_2^1, \cdots, d_{k^1}^1\Big)\cdots\Big(d_1^m, d_2^m, \cdots, d_{k^m}^m\Big)$. Wówczas permutacja $\gamma\colon c_i^j \mapsto d_i^j$ jest taka, że $\gamma\pi\gamma^{-1} = \sigma$. □

Klasy sprzężoności permutacji parzystych w S_n mogą zostać rozbite na kilka mniejszych w A_n, gdyż $A_n \leqslant S_n$, czyli w A_n jest mniejszy wybór elementów, którymi możemy sprzęgać. Okazuje się, że rzeczywiście niektóre z tych klas rozpadają się na dwie:

Twierdzenie 2.2.2.
Typy cyklowe permutacji parzystych, które zawierają cykl parzysty lub dwa cykle nieparzyste o tej samej długości (możliwe, że o długości 1) odpowiadają jednej klasie sprzężoności w S_n. Pozostałe typy permutacji parzystych odpowiadają dwóm równolicznym klasom sprzężoności w S_n.

Dowód. TODO □

Zanim udowodnimy prostotę grup A_n pokażemy jeszcze dwa przydatne lematy.

Lemat 2.2.1. *Dla $n \geqslant 5$ nietrywialne klasy sprzężoności (klasy elementów różnych od elementu neutralnego) A_n mają rozmiar co najmniej n.*

Dowód. TODO □

Lemat 2.2.2. *Dla $n \geqslant 5$ cykle długości 3 generują całą grupę A_n*

Dowód. Każdą permutację $\sigma \in A_n$ można przedstawić w postaci iloczynu parzystej liczby transpozycji $\sigma = \lambda_1\lambda_2\cdots\lambda_{2m-1}\lambda_{2m} = (\lambda_1\lambda_2)\cdots(\lambda_{2m-1}\lambda_{2m})$. Stąd wystarczy przedstawić iloczyn dwóch transpozycji $\lambda_1\lambda_2$ jako iloczyn cykli długości 3, a dostaniemy tezę.

Jeżeli $\lambda_1 = \lambda_2$, to $\lambda_1\lambda_2 = \mathrm{id}$. Gdy λ_1 i λ_2 są rozłączne, czyli $\lambda_1 = (a, b)$, $\lambda_2 = (c, d)$, to $\lambda_1\lambda_2 = (a, c, d)(a, c, b)$. Jeżeli natomiast λ_1 i λ_2 mają jeden element wspólny, czyli $\lambda_1 = (a, b)$, $\lambda_2 = (a, c)$, to $\lambda_1\lambda_2 = (a, b, c)$. □

2.3. Prostota A_n

Jesteśmy już gotowi, żeby udowodnić twierdzenie:

Twierdzenie 2.3.1 (O prostocie A_n)**.**
Grupa alternująca A_n jest prosta dla $n \geqslant 5$.

Dowód. Dowód przeprowadzimy przez indukcję ze względu na n

Pokażemy najpierw, że grupa A_5 jest prosta.

Na podstawie faktu 2.1.2 wiemy, że elementy A_5 mają jeden z następujących typów cyklowych: $(1^5), (1^2, 3^1), (1^1, 2^2)$ lub (5^1). z twierdzenia 2.2.2 każdy z pierwszych czterech odpowiada jednej klasie sprzężoności, a ostatni dwóm – równolicznym. Stąd klasy sprzężoności A_5 mają rozmiary: 1, 20, 15, 12, 12.

Załóżmy nie w prost, że H jest nietrywialną, właściwą podgrupą normalną A_5. Wówczas H musi być sumą pewnych klas sprzężoności A_5, w tym klasy sprzężoności elementu neutralnego. Ponadto rozmiar H musi być dzielnikiem rozmiaru $A_5 = 60$. Najmniejszy nietrywialny możliwy rozmiar sumy klas sprzężoności wraz z trywialną wynosi 13. Stąd $|H| = 15$, $|H| = 20$ lub $|H| = 30$. Ale żaden podzbiór multibioru $\{1, 12, 12, 15, 20\}$ zawierający jedynkę nie sumuje się do potencjalnego rozmiaru H, zatem takie H nie może istnieć – A_5 jest grupą prostą.

Załóżmy zatem, że $n \geqslant 6$ oraz grupa A_{n-1} jest prosta. Pokażemy, że A_n również jest prosta.

Załóżmy nie w prost, że H jest nietrywialną, właściwą podgrupą A_n.

Jeżeli H zawiera pewną nietrywialną permutację σ, która ma punkt stały $a \in \{1, 2, \cdots, n\}$, to niech $K = H_a$. Wówczas $K \simeq A_{n-1}$ oraz (np. z trzeciego twierdzenia o izomorfizmie) $H \cap K$ jest podgrupą normalną w K. Ale $\sigma \in H \cap K$ oraz K jest grupą prostą, zatem z założenia indukcyjnego $H \cap K = K$. Stąd H zawiera pewien element o typie $(1^{n-3}, 3^1)$, a zatem z twierdzenia 2.2.2 wszystkie, gdyż $n - 3 \geqslant 3$. Ale z lematu 2.2.2 cykle o długości 3 generują całe A_n, stąd $H = A_n$ – sprzeczność z właściwością H.

Jeżeli natomiast żaden nietrywialny element H nie ma punktu stałego, to $|H| \leqslant n$. W przeciwnym przypadku istniałyby dwie różne permutacje $\pi, \sigma \in H$ takie, że $\pi(1) = \sigma(1)$. Wtedy $\gamma = \pi\sigma^{-1} \neq \mathrm{id}$, $\gamma \in H$ oraz $\gamma(1) = 1$ – sprzeczność. Stąd rzeczywiście $|H| \leqslant n$. Ale z lematu 2.2.1 H jako nietrywialna suma pewnej liczby klas sprzężoności w tym trywialnej musiałaby mieć rozmiar co najmniej $n + 1$. Stąd w tym przypadku również otrzymujemy sprzeczność.

We wszystkich przypadkach otrzymaliśmy sprzeczność, czyli rzeczywiście A_n jest grupą pierwszą, czyli z indukcji A_n jest grupą pierwszą dla wszystkich $n \geqslant 5$. $\square$

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 działanie 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 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 (z S_n). 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. Jest to własność 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.*

Teraz jesteśmy już gotowi na wprowadzenie pojęcia prymitywności.

Definicja 3.1.4. *Załóżmy, że ρ jest działaniem grupy G na zbiorze X.*
ρ nazywamy prymitywnym*, jeśli nie istnieje nietrywialny system bloków działania ρ.*

Aby lepiej zrozumieć tą własność, pokażemy, że rzeczywiście jest to własność pomiędzy tranzytywnością oraz 2-tranzytywnością.

Twierdzenie 3.1.1. *Załóżmy, że ρ jest nietrywialnym działaniem grupy G na zbiorze X. Wówczas:*

a) Jeżeli ρ jest prymitywne, to jest tranzytywne.

b) Jeżeli ρ jest 2-tranzytywne, to jest prymitywne.

*Dowód.*Ad a) Załóżmy nie wprost, że ρ nie jest tranzytywne. Wówczas rozbicie X na orbity daje nietrywialny system bloków. Rzeczywiście, z nieprzechodniości dostajemy, że ilość bloków wynosi co najmniej 2 a z nietrywialności ρ – któryś blok ma co najmniej 2 elementy. Ostatecznie ρ permutuje elementy orbit, więc w szczególności je zachowuje. Znaleźliśmy nietrywialny system bloków działania ρ, czyli sprzeczność – ρ nie jest prymitywne. Stąd ρ musi być tranzytywne.

Ad b) Załóżmy nie wprost, że ρ nie jest prymitywne. Wówczas istnieje nietrywialny system bloków $\mathfrak{A} = \{Y_i : i \in I\}$, w którym istnieją $Y_1, Y_2 \in \mathfrak{A}$ takie, że $|Y_1| > 1$. Niech więc $x, y \in Y_1, z \in Y_2$ gdzie $x \neq y$. Z 2-tranzytywności możemy odwzorować parę (x, y) na parę (x, z), co daje sprzeczność z definicją systemu bloków. Stąd ρ musi być prymitywne. □

Oczywiście możliwe jest, że grupa działa tranzytywnie a nie prymitywnie, lub prymitywnie, a nie 2-tranzytywnie.

Jako pierwszy przykład możemy rozważyć naturalne działanie czteroelementowej grupy $H = \langle (1,2)(3,4), (1,3)(2,4) \rangle$ będącej podgrupą S_4 na zbiorze 4 elementowym. Jak łatwo widać jest ono przechodnie. Nie jest jednak prymitywne, gdyż zachowuje ono np. system bloków $\{\{1,2\},\{3,4\}\}$.

Jako drugi przykład rozważmy działanie A_3 na zbiorze $\{1,2,3\}$. Jak pokazaliśmy wcześniej nie jest ono 2-tranzytywne, ale jest tranzytywne. To, że jest to również działanie prymitywne wynika z następującego lematu:

Lemat 3.1.1. *Załóżmy, że ρ jest tranzytywnym działaniem grupy G na zbiorze X. Wówczas w dowolnym systemie bloków wszystkie bloki są równych rozmiarów.*

Dowód. Rzeczywiście, jeżeli Y_1, Y_2 są blokami, to skoro możemy odwzorować $y_1 \in Y_1$ na $y_2 \in Y_2$, To całe Y_1 musi być przekształcone w Y_2 (z własności systemu bloków), stąd $|Y_1| \leqslant |Y_2|$. Analogicznie $|Y_2| \leqslant |Y_1|$, zatem $|Y_1| = |Y_2|$. □

W tym przypadku bloki w nietrywialnym systemie bloków muszą mieć rozmiary 1 i 2, czyli różne, więc nietrywialny system bloków nie może istnieć.

Udowodnijmy teraz jeszcze jedno stwierdzenie, które jest użyteczne w dowodzie lematu Iwasawy.

Lemat 3.1.2. *Załóżmy, że ρ jest tranzytywnym działaniem grupy G na zbiorze X oraz $x \in X$. Wówczas ρ jest prymitywne wtedy i tylko wtedy, gdy G_x jest maksymalną podgrupą G, tzn. nie istnieje podgrupa H grupy G, taka że $G_x \lneq H \lneq G$.*

Dowód. Zauważmy najpierw, że warstwy (lewostronne) G_x odpowiadają jednoznacznie elementom zbioru X – bijekcja zadana jest wzorem $\zeta\colon gG_x \mapsto x^g$. Funkcja ta jest dobrze określona oraz jest iniekcją, gdyż $g_1G_x = g_2G_x \iff g_1^{-1} \cdot g_2 = h$ dla pewnego $h \in G_x \iff x^{g_1^{-1} \cdot g_2} = x^h = x \iff x^{g_1} = x^{g_2}$. Ponadto ζ jest suriekcją, gdyż działanie jest tranzytywne. Stąd rzeczywiście ζ jest bijekcją.

Przejdźmy teraz do dalszej części dowodu

$\Rightarrow$)

Załóżmy nie w prost, że G_x nie jest maksymalna, czyli istnieje H, takie, że $G_x \lneq H \lneq G$. Skoro H zawiera G_x, to warstwy H są sumami pewnych warstw G_x – jeżeli $g_1G_x = g_2G_x \iff g_1^{-1} \cdot g_2 \in G_x$ to również $g_1^{-1} \cdot g_2 \in H \iff g_1H = g_2H$. Stąd warstwy H odpowiadają rozbiciu zbioru warstw G_x, czyli również rozbiciu zbioru X. Zauważmy jeszcze, że działanie G zachowuje warstwy H. Jest tak dlatego, że dla $g_1H = g_2H$ zachodzi $g_1^{-1} \cdot g_2 \in H$. Punkt $g_iG_x = x^{g_i}$ przy działaniu elementem f grupy G przechodzi na $(x^{g_i})^f = x^{fg_i} = fg_iG_x$. Ale warstwy fg_1G_x oraz fg_2G_x zawierają się w jednej warstwie H, gdyż $(fg_1)^{-1}fg_2 = g_1^{-1}f^{-1}fg_2 = g_1^{-1}g_2 \in H$.

Otrzymaliśmy zatem system bloków, który na dodatek jest nietrywialny, gdyż H zawiera się ściśle pomiędzy G_x a G. Zatem działanie ρ nie jest prymitywne – sprzeczność. Stąd taka grupa H nie istnieje – G_x jest maksymalną podgrupą G.

$\Leftarrow$)

Tutaj również przeprowadzimy dowód nie w prost. Załóżmy, że ρ nie działa prymitywnie na X, czyli istnieje pewien nietrywialny system bloków $\mathfrak{A}$. Niech $Y \in \mathfrak{A}$ takie, że $x \in Y$ oraz niech H będzie stabilizatorem całego zbioru Y (czyli zbiorem $\{g \in G\colon \forall_{y \in Y} y^g \in Y\}$). Skoro $\mathfrak{A}$ jest nietrywialne, to $Y \neq X$ oraz istnieje blok rozmiaru co najmniej 2. Ale z poprzedniego lematu wiemy, że wszystkie bloki mają tą samą wielkość, więc również $|Y| \geqslant 2$.

Zauważmy, że $H = \{g \in G\colon x^g \in Y\} \stackrel{def}{=} K$. Oczywiście $H \subseteq K$, gdyż elementy H zachowują zbiór Y. Z drugiej strony, jeżeli jakiś element z Y trafia z powrotem do Y, to całe Y jest zachowywane, gdyż Y jest elementem systemu bloków. Stąd rzeczywiście $H = K$.

Na koniec wystarczy zobaczyć, że skoro $\{x\} \subsetneq Y \subsetneq X$, to $G_x \lneq H \lneq G$. Jest tak dlatego, że H, w przeciwieństwie do G_x, zawiera elementy odwzorowujące x na jakiś inny element zbioru Y ale nie zawiera elementów, które odwzorowują x na elementy spoza Y (które istnieją). Stąd G_x nie jest maksymalne – sprzeczność. Stąd to działanie musi być prymitywne. □

Teraz jesteśmy już gotowi na sformułowanie i dowód lematy Iwasawy.

3.2. Lemat Iwasawy

Twierdzenie 3.2.1. *Załóżmy, że G jest skończoną [dowolną?] grupą doskonałą, ρ – wiernie oraz prymitywnie działanie G na zbiorze X. Załóżmy dodatkowo, że dla pewnego $x \in X$ stabilizator G_x zawiera normalną podgrupę abelową A, której sprzężenia w G generują całe G. Wówczas grupa G jest prosta.*

Dowód. Załóżmy przeciwnie, że w G istnieje właściwa, nietrywialna podgrupa normalna K. Skoro G działa wiernie oraz K jest nietrywialna, to $x_0^{k_0} \neq x_0$ dla pewnego $k_0 \in K$. Niech $H = G_{x_0}$. Dostajemy, że $K \nleq H$, gdyż $k_0 \notin H$, stąd również $H \lneq HK$.

Z lematu 3.1.2 otrzymujemy, że H jest podgrupą maksymalną w G. $H \lneq HK$, więc $HK = G$. Stąd (i z twierdzenia 1.1.1) każdy element $g \in G$ jest postaci $g = hk$, gdzie $h \in H$ oraz $k \in K$.

Skoro działanie ρ jest prymitywne, a więc tranzytywne, to z twierdzenia 1.5.2 dostajemy, że G_x jest sprzężone z H. Z założenia dodatkowo wynika, że H zawiera podgrupę B sprzężoną do A, ponadto B jest normalną podgrupą abelową H, której sprzężenia (w G) generują całe G. Sprzężenia B są postaci $g^{-1}Bg = k^{-1}h^{-1}Bhk = k^{-1}Bk \leqslant BK$. Wszystkie sprzężenie B generują G i są zawarte w $BK \leqslant G$, stąd $G = BK$.

Korzystając z trzeciego twierdzenia o izomorfizmie dostajemy:

$$G/K = BK/K \simeq B/B \cap K$$

Ale grupa ilorazowa grupy abelowej jest abelowa, stąd zarówno $B/B \cap K$ jaki i G/K są abelowe. Z twierdzenia o komutancie wnioskujemy, że $K \geqslant [G,G] = G$, gdyż G jest grupą doskonałą – dostaliśmy sprzeczność z założeniem, że K jest właściwą podgrupą G, stąd G jest grupą prostą. $\square$

Zastosowania lematu Iwasawy znajdują się w dalszej części pracy.

Rozdział 4

Prostota specjalnej rzutowej grupy liniowej $PSL_n(k)$

Bibliografia

[Wil09] Robert A. Wilson, *The Finite Simple Groups*, Springer, 2009.

[Bia87] Andrzej Białynicki-Birula, *Zarys algebry*, Państwowe Wydawnictwo Naukowe, 1987.

[Lan73] Serge Lang, *Algebra*, Państwowe Wydawnictwo Naukowe, 1973.

[Kar76] M. I. Kargapołow, J. I. Mierzlakow, *Podstawy teorii grup*, Państwowe Wydawnictwo Naukowe, 1976.

[Bag02] Czesław Bagiński, *Wstęp do teorii grup*, Script, 2002.

[Neu03] Peter M. Neumann, Gabrielle A. Stoy, Edward C. Thompson, *Groups and Geometry*, Oxford Science Publications, 2003.