

**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

<b>Wprowadzenie</b> . . . . .	5
<b>1. Wiadomości wstępne</b> . . . . .	7
1.1. Oznaczenia . . . . .	7
1.2. Grupy proste . . . . .	7
1.3. Twierdzenia o izomorfizmie . . . . .	7
1.4. Komutant i abelianizacja . . . . .	8
1.5. Działanie grupy na zbiorze . . . . .	8
<b>2. Prostota grupy alternującej <math>A_n</math></b> . . . . .	11
<b>3. Lemat Iwasawy</b> . . . . .	13
3.1. Prymitywne działanie grupy . . . . .	13
3.2. Lemat Iwasawy . . . . .	16
<b>4. Prostota specjalnej rzutowej grupy liniowej <math>PSL_n(k)</math></b> . . . . .	17
<b>Bibliografia</b> . . . . .	19



# 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 oznaczane 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 definicję 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,  $\varphi: G \rightarrow H$  homomorfizm,  $K = \ker \varphi$  oraz  $H' = \text{im} \varphi$ .*

*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  $H_2 \leq H_1$ .

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 1.3.3** (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  $[G, G] \leq H$ .

**Definicja 1.4.2.** Przekształcenie kanoniczne  $G \rightarrow G/[G, G]$  (rzutowanie na grupę ilorazową) nazywamy abelianizacją.

O abelianizacji (w przeciwieństwie do twierdzenia o komutancie) nie będzie więcej wspomniane 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 zauważmy prosty fakt:

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

## 1.5. Działanie grupy na zbiorze

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

**Definicja 1.5.1.** Niech  $G$  będzie grupą, a  $X$  – zbiorem. Mówimy, że  $\rho$  jest działaniem grupy  $G$  na zbiorze  $X$ , jeżeli dla każdego  $g \in G$  przyporządkowane jest przekształcenie  $\rho_g: X \rightarrow X$ , takie, że:

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

Jeżeli sposób działania ( $\rho$ ) 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  $X \rightarrow X$ , 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  $\rho$  jest działaniem  $G$  na  $X$  wtedy i tylko wtedy, gdy  $\rho$  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  $\rho$  jest działaniem grupy  $G$  na zbiorze  $X$  oraz  $x \in X$ . Wówczas:

- a) Stabilizatorem punktu  $x$  (grupą izotropii  $x$ ) nazwiemy zbiór elementów  $\{g \in G : x^g = x\}$ . Stabilizator punktu  $x$  oznaczamy  $G_x$ .
- b) Orbitą punktu  $x$  nazwiemy podzbiór  $X$  równy  $\{y \in X : \exists g \in G x^g = y\}$ . Orbitę punktu  $x$  oznaczamy  $G(x)$ .

Podstawowe własności tych obiektów przedstawia następujący fakt:

**Fakt 1.5.1.** Załóżmy, że  $\rho$  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 rozbiecie 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  $\rho$  jest działaniem grupy  $G$  na zbiorze  $X$ .

- a)  $\rho$  jest działaniem tranzytywnym (przechodnim), jeżeli wszystkie elementy  $X$  tworzą jedną orbitę.
- b)  $\rho$  jest działaniem wiernym, jeżeli  $\rho$  jest iniekcją jako homomorfizm  $G \rightarrow S_X$ .
- c)  $\rho$  jest działaniem nietrywialnym, jeżeli  $\rho$  nie jest zerowe jako homomorfizm  $G \rightarrow S_X$ .

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

**Twierdzenie 1.5.2.**

Załóżmy, że  $\rho$  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  $\rho$  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  $x_1, x_2, \dots, x_k$  to reprezentanci wszystkich orbit działania  $\rho$ .



## 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 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  $\rho$  jest działaniem grupy  $G$  na zbiorze  $X$ .

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

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  $X = \{1, 2, \dots, n\}$ , 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  $(a_1, a_2, \dots, a_n)$  na  $(b_1, b_2, \dots, b_n)$ , gdyż jak założyliśmy w definicji, wszystkie  $a_i$  jak i wszystkie  $b_i$  są parami różne. Stąd również działanie  $S_n$  jest  $k$ -tranzytywne dla każdego  $k \leq n$ .

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  $i = 1, 2, \dots, (n-2)$  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  $(a_1, a_2, \dots, a_{n-2})$  na  $(b_1, b_2, \dots, b_{n-2})$ . Stąd działanie  $S_n$  jest  $k$ -tranzytywne dla każdego  $k \leq n-2$ .

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

**Definicja 3.1.2.** Załóżmy, że  $\rho$  jest działaniem grupy  $G$  na zbiorze  $X$ .

Systemem bloków działania  $\rho$  nazywamy podział zbioru  $X$  zachowywany przez  $\rho$ , 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  $\rho$  jest działaniem grupy  $G$  na zbiorze  $X$ .

$\rho$  nazywamy prymitywnym, jeśli nie istnieje nietrywialny system bloków działania  $\rho$ .

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

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

- a) Jeżeli  $\rho$  jest prymitywne, to jest tranzytywne.
- b) Jeżeli  $\rho$  jest 2-tranzytywne, to jest prymitywne.

*Dowód.*

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

Ad b) Załóżmy nie wprost, że  $\rho$  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  $\rho$  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  $\rho$  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  $|Y_1| \leq |Y_2|$ . Analogicznie  $|Y_2| \leq |Y_1|$ , zatem  $|Y_1| = |Y_2|$ .  $\square$

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  $\rho$  jest tranzytywnym działaniem grupy  $G$  na zbiorze  $X$  oraz  $x \in X$ . Wówczas  $\rho$  jest prymitywne wtedy i tylko wtedy, gdy  $G_x$  jest maksymalną podgrupą  $G$ , tzn. nie istnieje podgrupa  $H$  grupy  $G$ , że  $G_x \subsetneq H \subsetneq G$ .*

*Dowód.* Zauważmy najpierw, że warstwy (lewostronne)  $G_x$  odpowiadają jednoznacznie elementom zbioru  $X$  – bijekcja zadana jest wzorem  $\zeta: gG_x \mapsto x^g$ . 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  $\zeta$  jest suriekcją, gdyż działanie jest tranzytywne, stąd rzeczywiście  $\zeta$  jest bijekcją.

Przejdźmy teraz do dalszej części dowodu

$\Rightarrow$ )

Załóżmy nie wprost, że  $G_x$  nie jest maksymalna, czyli istnieje  $H$ , takie, że  $G_x \subsetneq H \subsetneq G$ . 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 rozbięciu zbioru warstw  $G_x$ , czyli również rozbięciu 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  $(x^{g_i})^f = x^{fg_i} = f g_i G_x$ . Ale warstwy  $f g_1 G_x$  oraz  $f g_2 G_x$  zawierają się w jednej warstwie  $H$ , gdyż  $(f g_1)^{-1} f g_2 = g_1^{-1} f^{-1} f g_2 = g_1^{-1} g_2 \in H$ .

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

$\Leftarrow$ )

Tutaj również przeprowadzimy dowód nie wprost. Załóżmy, że  $\rho$  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  $\{g \in G: \forall y \in Y y^g \in Y\}$ ). 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 tę samą wielkość, więc również  $|Y| \geq 2$ .

Zauważmy, że  $H = \{g \in G: x^g \in Y\} = K$ . 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  $G_x \subsetneq H \subsetneq G$ . 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.  $\square$

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,  $\rho$  – 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  $K \not\leq H$ , gdyż  $k_0 \notin H$ , stąd również  $H \not\leq HK$ .

Z lematu 3.1.2 otrzymujemy, że  $H$  jest podgrupą maksymalną w  $G$ .  $H \leq HK$ , 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  $\rho$  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  $g^{-1}Bg = k^{-1}h^{-1}Bhk = k^{-1}Bk \leq BK$ . Wszystkie sprzężenia  $B$  generują  $G$  i są zawarte w  $BK \leq G$ , 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  $B/B \cap K$  jak i  $G/K$  są abelowe. Z twierdzenia o komutancie wnioskujemy, że  $K \geq [G, G] = G$ , 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

[A] C, *D*, E