

**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**

Praca ta zawiera dowody prostoty dwóch najprostszych rodzin (nieprzemiennych) grup prostych – grup alternujących oraz specjalnych rzutowych grup liniowych. Dowód prostoty  $A_n$  używa jedynie narzędzi znanych z podstawowego kursu Algebry I, natomiast dowód prostoty  $PSL_n(k)$  wprowadza nowe pojęcia –  $k$ -tranzytywność oraz prymitywność działania grupy i używa lematu Iwasawy.

## **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

<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
2.1. Przypomnienie wiadomości o $S_n$ oraz $A_n$ . . . . .	11
2.2. Klasy sprzężoności $S_n$ i $A_n$ . . . . .	12
2.3. Prostota $A_n$ . . . . .	14
<b>3. Lemat Iwasawy</b> . . . . .	17
3.1. Prymitywne działanie grupy . . . . .	17
3.2. Lemat Iwasawy . . . . .	20
<b>4. Prostota specjalnej rzutowej grupy liniowej <math>PSL_n(k)</math></b> . . . . .	21
4.1. Grupy liniowe . . . . .	21
4.2. Prostota $PSL_n(k)$ . . . . .	22
4.3. Dodatkowe informacje o $PSL_n(k)$ oraz lemacie Iwasawy . . . . .	24
<b>Bibliografia</b> . . . . .	27



# Wprowadzenie

Grupy proste są jednymi z ważniejszych pojęć w teorii grup. Badając ich strukturę możemy poznać własności np. wszystkich skończonych grup, gdyż grupy proste są budulcem, z których zbudowane są inne grupy, co wyraża następujące (nie omawiane dalej w pracy) twierdzenie:

**Twierdzenie** (Jordana – Höldera [Bia87, tw. II.11.9.]).

*Jeżeli  $G$  jest grupą skończoną, to istnieje w niej skończony ciąg podgrup*

$$G = G_n > G_{n-1} > \dots > G_1 > G_0 = \{e\}$$

*taki, że  $G_{i-1}$  jest podgrupą normalną  $G_i$  oraz  $G_i/G_{i-1}$  jest grupą prostą dla  $i = 1, \dots, n$ .*

*Ponadto dla każdego innego ciągu podgrup*

$$G = H_m > H_{m-1} > \dots > H_1 > H_0 = \{e\}$$

*spełniającego powyższe warunki zachodzi  $n = m$  oraz  $G_i/G_{i-1} \simeq H_{\pi(i)}/H_{\pi(i)-1}$  dla  $i = 1, \dots, n$  oraz pewnej permutacji indeksów  $\pi \in S_n$ .*

W związku z tym, klasyfikacja skończonych grup prostych była istotnym zagadnieniem w matematyce, począwszy od pierwszej połowy XIX wieku, kiedy to E. Galois sformułował podstawowe pojęcia teorii grup i udowodnił m.in. prostotę grup  $A_n$ , aż do zakończenia dowodu klasyfikacyjnego na początku lat 80' ubiegłego wieku. Uprozczone sformułowanie tego twierdzenia brzmi:

**Twierdzenie** (Twierdzenie klasyfikacyjne skończonych grup prostych).

*Jeśli grupa  $G$  jest skończoną grupą prostą, to  $G$  jest izomorficzna z jedną z następujących grup:*

- 1. grupą cykliczną  $C_p$  rzędu  $p$ , będącego liczbą pierwszą;*
- 2. grupą alternującą  $A_n$ , dla  $n \geq 5$ ;*
- 3. grupą prostą typu Liego, należącą do jednej z 16 nieskończonych rodzin skończonych grup prostych;*
- 4. jedną z 26 sporadycznych grup prostych.*

W tej pracy zajmiemy się czymś znacznie prostszym – udowodnimy prostotę dwóch najprostszych rodzin (nieprzemiennych) grup prostych – grup alternujących oraz specjalnych rzutowych grup liniowych. Poniżej znajduje się dokładniejszy opis zawartości poszczególnych rozdziałów.

Rozdział pierwszy, *Wiadomości wstępne*, zawiera przypomnienie różnych definicji, twierdzeń oraz własności znanych z podstawowego kursu Algebry I, do których będziemy się odwoływali w dalszej części pracy lub też zostały tam zamieszczone w celu podsumowania wiedzy

na dany temat. Poszczególne przypomniane tematy to definicja grupy prostej, twierdzenia o izomorfizmie, komutant i abelianizacja oraz działanie grupy na zbiorze.

Kolejny rozdział, *Prostota grupy alternującej*  $A_n$ , zaczyna się od definicji grupy symetrycznej, cykli oraz grupy alternującej. Następnie wprowadzimy pojęcie typu permutacji oraz pokażemy jego związek z klasami sprzężoności w grupie  $S_n$  oraz w grupie  $A_n$ . Na koniec udowodnimy główny wynik tego rozdziału – twierdzenie, że grupa alternująca  $A_n$  jest prosta dla  $n = 3$  oraz  $n \geq 5$ .

Rozdział *Lemat Iwasawy* wprowadza nowe pojęcia –  $k$ -tranzytywność oraz prymitywność działania grupy na zbiorze. Wykażemy w nim związki między tymi pojęciami, maksymalność grup izotropii przy działaniu prymitywnym, a także lemat Iwasawy – jedno z podstawowych narzędzi do dowodzenia prostoty grup.

Ostatni rozdział, *Prostota specjalnej rzutowej grupy liniowej*  $PSL_n(k)$ , pokazuje zastosowanie lematu Iwasawy. Zaczyna się on od definicji grup liniowych, a następnie, korzystając z lematu Iwasawy oraz pomocniczych stwierdzeń dowodzi, że grupa  $PSL_n(k)$  jest prosta poza przypadkiem  $n = 2$  oraz  $|k| \leq 3$ .

Na koniec pracy pokazujemy jeszcze jedno zastosowanie lematu Iwasawy – alternatywny dowód prostoty grup alternujących.



# 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 wielkimi 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  $A$  oraz  $B$  są podzbiorami grupy  $G$ , to przez  $AB$  będzie oznaczany podzbiór iloczynów  $\{a \cdot b : a \in A, b \in B\} \subseteq G$ .

Przy okazji tego oznaczenia warto przytoczyć twierdzenie:

#### **Twierdzenie 1.1.1.**

*Jeżeli  $H$  oraz  $K$  są podgrupami grupy  $G$ , przy czym  $K$  jest podgrupą normalną, to  $HK$  jest podgrupą grupy  $G$ .*

### 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.*

**Stwierdzenie 1.2.1.** *Jedynymi (z dokładnością do izomorfizmu) przemiennymi grupami prostymi są skończone grupy cykliczne, których rząd jest liczbą pierwszą.*

Jest to prosta konsekwencja tego, że w grupach przemiennych wszystkie podgrupy są normalne oraz że każda inna grupa przemienna ma właściwą podgrupę cykliczną.

### 1.3. Twierdzenia o izomorfizmie

Przejdźmy teraz do podstawowych twierdzeń o izomorfizmie.

**Twierdzenie 1.3.1** (Pierwsze twierdzenie o izomorfizmie [Bia87, tw. II.4.5.]).

*Niech  $\varphi: G \rightarrow H$  będzie homomorfizmem grup. Oznaczmy  $K = \ker \varphi$  oraz  $H' = \operatorname{im} \varphi$ . Wówczas ma miejsce izomorfizm*

$$G/K \simeq H'. \quad \square$$

**Twierdzenie 1.3.2** (Drugie twierdzenie o izomorfizmie [Bia87, tw. II.4.6. a)]).

Niech  $G$  będzie grupą,  $H_1, H_2$  jej podgrupami normalnymi, przy czym  $H_2 \leq H_1$ . Wówczas  $H_2 \trianglelefteq H_1$ ,  $H_1/H_2 \trianglelefteq G/H_2$  i ma miejsce izomorfizm

$$(G/H_2)/(H_1/H_2) \simeq G/H_1. \quad \square$$

**Twierdzenie 1.3.3** (Trzecie twierdzenie o izomorfizmie [Bia87, tw. II.4.6. b)]).

Niech  $G$  będzie grupą,  $H$  oraz  $H_1$  – jej podgrupami, przy czym  $H_1$  jest podgrupą normalną w  $G$ . Wówczas  $H \cap H_1$  jest podgrupą normalną w  $H$  oraz ma miejsce izomorfizm

$$H/(H \cap H_1) \simeq HH_1/H_1. \quad \square$$

## 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 [Bia87, tw. II.7.2-5.]).

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  $[G, G] \leq H$ .  $\square$

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

W skrajnym przypadku abelianizacja grupy jest trywialna, co prowadzi do ważnego pojęcia 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:

**Stwierdzenie 1.4.1.** Nieprzemienne grupy proste są grupami doskonałymi.  $\square$

## 1.5. Działanie grupy na zbiorze

Na koniec tego rozdziału przyjrzymy się użytecznej własności grup – możliwości działania na zbiorach.

**Definicja 1.5.1.** Niech  $G$  będzie grupą, a  $X$  – zbiorem. Mówimy, że  $\rho$  jest działaniem grupy  $G$  na zbiorze  $X$ , jeśli każdemu elementowi  $g \in G$  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 następujące twierdzenie. Zanim jednak do niego przejdziemy, przypomnijmy 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 [Bia87, str. 79]).

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  $X$ .  $\square$

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 następujące stwierdzenie:

**Stwierdzenie 1.5.1** ([Bia87, tw. II.1.3.a,b]). 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  $X$ ).  $\square$

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 homomorfizmem stałym  $G \rightarrow S_X$ .

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

**Twierdzenie 1.5.2** ([Bia87, tw. II.1.3.c]).

Założmy, 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 sprzężone w grupie  $G$ .

**Twierdzenie 1.5.3** (O orbitach i stabilizatorach [Bag02, stw. 11.3.]).

Założmy, że  $\rho$  jest działaniem grupy  $G$  na zbiorze  $X$  oraz  $x \in X$ . Wówczas  $|G(x)| = [G : G_x]$ .

**Twierdzenie 1.5.4** (Równanie klas [Lan73, str. 37]).

Zakładając dodatkowo, że  $G$  jest grupą skończoną, prawdziwa jest równość

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

gdzie  $x_1, x_2, \dots, x_k$  są reprezentantami wszystkich orbit działania  $\rho$ .



## Rozdział 2

# Prostota grupy alternującej $A_n$

Zanim wykażemy główną tezę tego rozdziału, czyli twierdzenie, że  $A_n$  jest grupą prostą dla  $n \geq 5$ , 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 przyjmujemy, że jej elementami są permutacje zbioru  $\{1, 2, \dots, n\}$ .

W przypadku elementów z  $S_n$ , będziemy się trzymać odwrotnej konwencji zapisu mnożenia permutacji, tzn.  $(\pi\sigma)(a) = \sigma(\pi(a))$  dla  $a \in \{1, 2, \dots, n\}$ .

**Stwierdzenie 2.1.1.** *Rzęd grupy  $S_n$  wynosi  $n!$ .*  $\square$

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  $c_1, c_2, \dots, c_k \in \{1, 2, \dots, n\}$  takie, że*

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

Cykle zapisujemy w postaci  $(c_1, c_2, \dots, c_k)$ . Oczywiście zapis cyklu nie jest jednoznaczny; następujące zapisy:  $(c_1, c_2, \dots, c_k) = (c_k, c_1, c_2, \dots, c_{k-1}) = (c_2, c_3, \dots, c_k, c_1)$  reprezentują ten sam cykl.

Dla  $\sigma \in S_n$  oraz  $x \in \{1, 2, \dots, n\}$  zbiór  $\{x, \sigma(x), \sigma^2(x), \dots\} \subseteq \{1, \dots, n\}$  jest skończony, zatem istnieją liczby  $k < l \leq n$  takie, że  $\sigma^k(x) = \sigma^l(x)$ , a stąd  $\sigma^{l-k}(x) = x$ . Jeśli  $d$  jest najmniejszą liczbą całkowitą dodatnią taką, że  $\sigma^d(x) = x$ , to mamy cykl  $(x, \sigma(x), \dots, \sigma^{d-1}(x))$ . Powtarzając tę procedurę z niewybranymi jeszcze elementami  $x$ , dostaniemy twierdzenie:

**Twierdzenie 2.1.1** (Rozkład na cykle).

*Każdą permutację  $\sigma \in S_n$  można przedstawić jako iloczyn rozłącznych cykli, czyli takich  $(c_1, c_2, \dots, c_k), (d_1, d_2, \dots, d_l)$ , że  $\{c_1, c_2, \dots, c_k\} \cap \{d_1, d_2, \dots, d_l\} = \emptyset$ , przy czym każdy element ze zbioru  $\{1, 2, \dots, n\}$  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  $n \geq 2$ .

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

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

**Twierdzenie 2.1.2** ([Bag02, stw. 3.7.]).

*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, którą można przedstawić w postaci iloczynu parzystej liczby transpozycji, nazwiemy permutacją 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** ([Bag02, stw. 3.8.]).

*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 rzędu  $n!/2$ .*

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 prawdziwe jest:

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

## 2.2. Klasy sprzężoności $S_n$ i $A_n$

W celu udowodnienia prostoty grupy  $A_n$  zbadamy klasy sprzężoności tej grupy. Najpierw zajmijmy 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  $\sigma$ , tzn. ciąg  $(1^{i_1}, 2^{i_2}, \dots, n^{i_n})$ , gdzie  $i_k$  to liczba cykli długości  $k$  w rozkładzie  $\sigma$  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 sprzężone wtedy i tylko wtedy, gdy ich indeks cyklowy jest taki sam.*

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

$$\gamma(c_1^1, c_2^1, \dots, c_{k_1}^1) \cdots (c_1^m, c_2^m, \dots, c_{k_m}^m)\gamma^{-1} =$$

$$\begin{aligned}
&= \gamma(c_1^1, c_2^1, \dots, c_{k_1}^1) \gamma^{-1} \gamma \cdots \gamma^{-1} \gamma(c_1^m, c_2^m, \dots, c_{k_m}^m) \gamma^{-1} = \\
&= (\gamma^{-1}(c_1^1), \gamma^{-1}(c_2^1), \dots, \gamma^{-1}(c_{k_1}^1)) \cdots (\gamma^{-1}(c_1^m), \gamma^{-1}(c_2^m), \dots, \gamma^{-1}(c_{k_m}^m))
\end{aligned}$$

Jeżeli cykle  $(c_1^1, c_2^1, \dots, c_{k_1}^1), \dots, (c_1^m, c_2^m, \dots, c_{k_m}^m)$  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  $\pi = (c_1^1, c_2^1, \dots, c_{k_1}^1) \cdots (c_1^m, c_2^m, \dots, c_{k_m}^m)$  oraz  $\sigma = (d_1^1, d_2^1, \dots, d_{k_1}^1) \cdots (d_1^m, d_2^m, \dots, d_{k_m}^m)$ . Wówczas permutacja  $\gamma: d_i^j \mapsto c_i^j$  jest taka, że  $\gamma\pi\gamma^{-1} = \sigma$ .  $\square$

Klasy sprzężoności permutacji parzystych w  $S_n$  mogą rozpaść się na kilka mniejszych w  $A_n$ , gdyż  $A_n \leq S_n$ , 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 o parzystej długości lub dwa cykle o tej samej nieparzystej długości (możliwe, że o długości 1) odpowiadają jednej klasie sprzężoności w  $A_n$ . Pozostałe typy permutacji parzystych odpowiadają dwóm równolicznym klasom sprzężoności w  $A_n$ .*

*Dowód.* Zauważmy najpierw, że jeżeli  $\sigma \in A_n$  jest centralizowane przez pewną nieparzystą permutację  $\gamma$  (tzn.  $\sigma = \gamma\sigma\gamma^{-1}$ ), to  $\sigma$  jest sprzężona w  $A_n$  ze wszystkimi permutacjami o tym samym typie cyklowym. Jest tak dlatego, że z każdą taką permutacją  $\psi$  permutacja  $\sigma$  jest sprzężona w  $S_n$  przez pewną permutację  $\pi$ , tzn.  $\psi = \pi\sigma\pi^{-1}$ . Ale również  $\psi = \pi\gamma\sigma\gamma^{-1}\pi^{-1} = (\pi\gamma)\sigma(\pi\gamma)^{-1}$ . Jedną z permutacji  $\pi$  lub  $\pi\gamma$  jest parzysta, więc rzeczywiście  $\psi$  oraz  $\sigma$  są sprzężone w  $A_n$ .

Jeżeli  $\sigma$  ma w rozkładzie na cykle rozłączne cykl parzystej długości  $\lambda$ , to jest przez niego centralizowana (a jest on permutacją nieparzystą), a jeżeli ma dwa cykle o tej samej nieparzystej długości  $(c_1, c_2, \dots, c_m)$  oraz  $(d_1, d_2, \dots, d_m)$ , to jest centralizowana przez nieparzystą permutację  $(c_1, d_1)(c_2, d_2) \dots (c_m, d_m)$ , czyli rzeczywiście  $\sigma$  jest sprzężona ze wszystkimi elementami o tym samym typie cyklowym.

W przypadku, gdy  $\sigma$  nie jest centralizowana przez żadną nieparzystą permutację, to permutacje o tym samym typie cyklowym co  $\sigma$  rozpadają się na dwie klasy sprzężoności –  $\{\lambda\sigma\lambda^{-1}: \lambda \in S_n \setminus A_n\}$  oraz  $\{\pi\sigma\pi^{-1}: \pi \in A_n\}$ . Są one równoliczne, gdyż są sprzężone w  $S_n$ .

Z takim przypadkiem mamy do czynienia, gdy  $\sigma$  w rozkładzie na cykle rozłączne ma tylko cykle o różnych nieparzystych długościach. Przy centralizowaniu każdy taki cykl musi przejść na cykl o tej samej długości, czyli na siebie. Ponadto pierwsze elementy z cykli muszą przejść na elementy ze swoich cykli, a obraz pozostałych elementów jest już przez to wyznaczony jednoznacznie. W związku z tym,  $\sigma$  może być centralizowane tylko przez permutacje, które są równe iloczynowi potęg cykli z rozkładu  $\sigma$ , a zatem tylko przez permutacje parzyste.  $\square$

Zanim udowodnimy prostotę grup  $A_n$  pokażemy jeszcze dwa przydatne lematy.

**Lemat 2.2.1.** *Dla  $n \geq 5$  klasy sprzężoności elementów nietrywialnych  $A_n$  mają co najmniej  $n$  elementów.*

*Dowód.* Niech  $\sigma \in A_n$ ,  $\sigma \neq \text{id}$ . Oszacujmy ile permutacji ma ten sam typ cyklowy  $\tau$  co  $\sigma$ .

Jeżeli  $\sigma$  zawiera cykl długości  $k \geq 3$ , to permutacji o typie  $\tau$ , których rozkład na cykle rozłączne zawiera cykl  $(1, a_1, a_2, \dots, a_k)$  jest co najmniej tyle, ile wyborów  $a_1$  i  $a_2$ , czyli

$(n-1)(n-2)$ . Stąd i z poprzedniego twierdzenia, w klasie sprzężoności  $\sigma$  jest co najmniej  $\frac{(n-1)(n-2)}{2} \geq n$  elementów (bo  $n \geq 5$ ).

W przeciwnym przypadku  $\sigma$  zawiera co najmniej dwa cykle długości 2. Analogicznie dostajemy, że samych permutacji o typie  $\tau$ , których rozkład na cykle rozłączne zawiera cykle  $(1, a)$  oraz  $(2, b)$  jest co najmniej  $(n-2)(n-3)$ , więc z poprzedniego twierdzenia w tym przypadku również rozmiar klasy sprzężoności  $\sigma$  wynosi co najmniej  $(n-2)(n-3) \geq n$ .  $\square$

**Lemat 2.2.2.** *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  $\lambda_1 \lambda_2 = \text{id}$ . Gdy  $\lambda_1$  i  $\lambda_2$  są rozłączne,  $\lambda_1 = (a, b)$ ,  $\lambda_2 = (c, d)$ , to  $\lambda_1 \lambda_2 = (a, c, d)(a, c, b)$ . Jeżeli natomiast  $\lambda_1$  i  $\lambda_2$  mają jeden element wspólny,  $\lambda_1 = (a, b)$ ,  $\lambda_2 = (a, c)$ , to  $\lambda_1 \lambda_2 = (a, b, c)$ .  $\square$

## 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  $n \geq 5$ .*

*Dowód.* Dowód przeprowadzimy przez indukcję ze względu na  $n$ .

Pokażemy najpierw, że grupa  $A_5$  jest prosta.

Na podstawie Stwierdzenia 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 wprost, 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 rząd  $H$  musi być dzielnikiem rzędu  $A_5$  równego 60. Najmniejszy nietrywialny możliwy rozmiar sumy klas sprzężoności wraz z trywialną wynosi 13. Stąd  $|H| = 15$ ,  $|H| = 20$  lub  $|H| = 30$ . Ale żaden podzbiór multizbioru  $\{1, 12, 12, 15, 20\}$  zawierający jedynekę nie sumuje się do potencjalnego rzędu  $H$ , zatem takie  $H$  nie może istnieć –  $A_5$  jest grupą prostą.

Pokażemy teraz, że jeśli  $n \geq 6$  oraz grupa  $A_{n-1}$  jest prosta, to również  $A_n$  jest prosta.

Załóżmy nie wprost, że  $H$  jest nietrywialną, właściwą podgrupą normalną w  $A_n$ .

Jeżeli  $H$  zawiera pewną nietrywialną permutację  $\sigma$ , która ma punkt stały  $a \in \{1, 2, \dots, n\}$ , to niech  $K = (A_n)_a$ . Wówczas  $K \simeq A_{n-1}$  oraz (np. z trzeciego twierdzenia o izomorfizmie)  $H \cap K$  jest podgrupą normalną w  $K$ . Ale  $e \neq \sigma \in H \cap K$  oraz  $K$  jest grupą prostą, zatem z założenia indukcyjnego  $H \cap K = K$ . Wobec tego  $H$  zawiera pewien element o typie  $(1^{n-3}, 3^1)$ , więc także wszystkie elementy tego typu, na mocy twierdzenia 2.2.2, gdyż  $n-3 \geq 3$ . Ale z lematu 2.2.2 cykle o długości 3 generują całą  $A_n$ , stąd  $H = A_n$  – sprzeczność z założeniem, że  $H$  jest podgrupą właściwą.

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



We wszystkich przypadkach otrzymaliśmy sprzeczność, czyli rzeczywiście  $A_n$  jest grupą prostą. W takim razie, z indukcji,  $A_n$  jest grupą prostą dla wszystkich  $n \geq 5$ .  $\square$

Można się jeszcze zastanawiać, jak wygląda  $A_n$  dla  $n < 5$ . Z twierdzenia 2.1.3 wiemy, że  $|A_n| = n!/2$ . Zatem  $A_2$  jest grupą trywialną.  $A_3$  ma 3 elementy – jest grupą cykliczną o 3 elementach, więc jest prosta. Natomiast grupa  $A_4$  nie jest prosta – jej czteroelementowa podgrupa  $H = \langle (1, 2)(3, 4), (1, 3)(2, 4) \rangle$  jest normalna, gdyż składa się ze wszystkich elementów o rzędzie  $\leq 2$ .



## 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  $X$ .

Powiemy, że  $\rho$  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  $a_i^g = b_i$  dla każdego  $i = 1, 2, \dots, k$ .

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

Aby zilustrować to pojęcie, policzmy jaki jest stopień tranzytywności naturalnego działania  $S_n$  oraz  $A_n$  na zbiorze  $X = \{1, 2, \dots, n\}$ , tzn. takiego, 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 także 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 ustalimy na co przejdzie pierwsze  $n-1$  elementów  $X$  i ma to być permutacja, to obraz ostatniego elementu też jest ustalony, 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 (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 różne od wszystkich  $a_i$ , a  $y, y'$  to elementy różne od wszystkich  $b_i$ . 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. Jest to własność 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  $X$ .

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

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

*Dowód b).* Załóżmy nie wprost, że  $\rho$  nie jest prymitywne. Wówczas istnieje nietrywialny system bloków  $\mathfrak{A}$ , w którym istnieją  $Y_1 \neq Y_2$  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.  $\square$

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.** *Założmy, 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  $G$ , taka 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 surjekcją, gdyż działanie jest tranzytywne. Stąd rzeczywiście  $\zeta$  jest bijekcją.

Przejdźmy teraz do dalszej części dowodu.

$\Rightarrow$ )

Założmy 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 także  $g_1^{-1} \cdot g_2 \in H \iff g_1H = g_2H$ . Stąd warstwy  $H$  odpowiadają rozbiciu zbioru warstw  $G_x$ , czyli również rozbiciu zbioru  $X$ . Zauważmy jeszcze, że działanie  $\rho$  zachowuje zbiór warstw  $H$ . 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 system bloków, który na dodatek jest nietrywialny, ponieważ  $H$  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 także przeprowadzimy dowód nie wprost. Założmy, że  $\rho$  nie działa prymitywnie na  $X$  – istnieje pewien nietrywialny system bloków  $\mathfrak{A}$ . Niech  $Y \in \mathfrak{A}$  będzie tym blokiem, który zawiera  $x$  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, ponieważ  $\rho$  jest tranzytywne, więc również  $|Y| \geq 2$ .

Zauważmy, że  $H = \{g \in G: x^g \in Y\} \stackrel{\text{def}}{=} K$ . 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, bo  $Y$  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). Otrzymujemy, że  $G_x$  nie jest maksymalne – sprzeczność. Zatem to działanie musi być prymitywne.  $\square$

Teraz jesteśmy już gotowi na sformułowanie i dowód lematu Iwasawy.

### 3.2. Lemat Iwasawy

**Twierdzenie 3.2.1.** *Załóżmy, że  $G$  jest grupą doskonałą, natomiast  $\rho$  jest wiernym oraz prymitywnym działaniem  $G$  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 pewnych  $k_0 \in K$  oraz  $x_0 \in X$ . Niech  $H = G_{x_0}$ . Dostajemy, że  $K \not\leq H$ , gdyż  $k_0 \notin H$ , stąd również  $H \subsetneq HK$ .

Z lematu 3.1.2 otrzymujemy, że  $H$  jest podgrupą maksymalną w  $G$ , a z twierdzenia 1.1.1, że  $HK$  jest podgrupą  $G$ .  $H \subsetneq HK$ , więc  $HK = G$ . Wobec tego każdy element  $g \in G$  jest postaci  $g = hk$ , gdzie  $h \in H$  oraz  $k \in K$ .

Skoro działanie  $\rho$  jest prymitywne, czyli również tranzytywne, to z twierdzenia 1.5.2 dostajemy, że każda grupa izotropii  $G_x$  jest sprzężona 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, więc 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  $G$ , zatem  $G$  jest grupą prostą.  $\square$

## Rozdział 4

# Prostota specjalnej rzutowej grupy liniowej $PSL_n(k)$

W tym rozdziale pokażemy zastosowania udowodnionego powyżej lematy Iwasawy. Wykażemy prostotę grupy  $PSL_n(k)$  oraz zaproponujemy alternatywny dowód prostoty  $A_n$ .

### 4.1. Grupy liniowe

Zacznijmy od przypomnienia definicji grup liniowych.

**Definicja 4.1.1.** Pełną grupą liniową  $GL_n(k)$  nazywamy grupę kwadratowych macierzy odwracalnych stopnia  $n$  nad ciałem  $k$ , wraz z operacją mnożenia macierzy i macierzą jednostkową  $I_n$  jako element neutralny.

Oprócz  $GL_n(k)$  ważne są również inne grupy liniowe –  $PGL_n(K)$ ,  $SL_n(k)$  oraz  $PSL_n(k)$ . Zanim je zdefiniujemy, przypomnimy pewne wiadomości z algebry liniowej.

**Stwierdzenie 4.1.1.** Wyznacznik  $\det: GL_n(k) \rightarrow k^*$  jest homomorfizmem grup, gdzie  $k^* = k \setminus \{0\}$  jest grupą multiplikatywną ciała  $k$ .

**Stwierdzenie 4.1.2** ([Bia87, str. 47]). Centrum  $Z_n$  grupy  $GL_n(k)$  składa się z macierzy postaci  $\lambda I_n$ , gdzie  $\lambda \in k^*$ .

Centrum jest oczywiście podgrupą normalną. Stąd poprawna jest

**Definicja 4.1.2.** Rzutową grupą liniową  $PGL_n(k)$  nazywamy grupę ilorazową  $GL_n(k)/Z_n$ .

**Definicja 4.1.3.** Specjalną grupą liniową  $SL_n(k)$  nazywamy jądro funkcji  $\det: GL_n(k) \rightarrow k^*$ . Innymi słowy  $SL_n(k)$  to macierze o wyznaczniku równym 1.

W  $SL_n(k)$  prawdziwe jest, analogiczne od powyższego, stwierdzenie o jego centrum.

**Stwierdzenie 4.1.3.** Centrum  $SZ_n$  grupy  $SL_n(k)$  składa się z macierzy postaci  $\lambda I_n$ , gdzie  $\lambda \in k^*: \lambda^n = 1$ .

Jesteśmy teraz gotowi na zdefiniowanie obiektu badań tego rozdziału.

**Definicja 4.1.4.** Specjalną rzutową grupą liniową  $PSL_n(k)$  nazywamy iloraz  $SL_n(k)/SZ_n$ .

W celu zastosowania lematu Iwasawy, zajmijmy się macierzami elementarnymi postaci  $E_{ij}(a) = I_n + a\Delta_{ij}$ , gdzie  $a \in k$ ,  $i \neq j$  oraz  $\Delta_{ij}$  to macierz składająca się z jedynki na pozycji  $(i, j)$  oraz samych zer.

Udowodnimy o tych macierzach 2 lematy.

**Lemat 4.1.1.** *Macierze  $E_{ij}(a)$  dla  $i \neq j$  generują grupę  $SL_n(k)$ .*

*Dowód.* Oczywiście  $E_{ij}(a) \in SL_n(k)$  dla  $i \neq j$ . Ponadto  $E_{ij}(a)^{-1} = E_{ij}(-a)$ , zatem aby pokazać, że każdy element  $M \in SL_n(k)$  jest iloczynem macierzy  $E_{ij}(a)$ , wystarczy dowieść, że jak będziemy mnożyć  $M$  z lewej strony przez macierze  $E_{ij}(a)$ , to dostaniemy identyczność. Ale mnożenie przez  $E_{ij}(a)$  to dodanie do  $j$ -tego wiersza  $a$  krotność  $i$ -tego wiersza. Dzięki zastosowaniu eliminacji Gaussa możemy w ten sposób doprowadzić  $M$  do postaci diagonalnej, a nawet postaci diagonalnej z jedynkami na przekątnej poza pozycją  $(n, n)$ , ponieważ dodając  $i$ -ty wiersz do  $(i+1)$ -go, a następnie odpowiednio odejmując od  $i$ -tego  $c$  krotność  $(i+1)$ -wszego dostajemy na przekątnej jedynkę. Ale wówczas ostatnia pozycja również będzie równa 1, gdyż  $\det(M) = 1$ , a mnożenie przez  $E_{ij}(a)$  wyznacznika nie zmienia.  $\square$

**Lemat 4.1.2.** *Macierze  $E_{ij}(a)$  dla  $i \neq j$  są komutantami pewnych elementów z  $SL_n(k)$  dla  $n > 2$  lub  $|k| > 3$ .*

*Dowód.* Gdy  $n > 2$ , to weźmy  $m \leq n$  takie, że  $m \neq i$  oraz  $m \neq j$ . Wówczas

$$\begin{aligned} [E_{mj}(1), E_{im}(-a)] &= E_{mj}(1)E_{im}(-a)E_{mj}(1)^{-1}E_{im}(-a)^{-1} = \\ &= E_{mj}(1)E_{im}(-a)E_{mj}(-1)E_{im}(a) = \\ &= (I_n + \Delta_{mj})(I_n - a\Delta_{im})(I_n - \Delta_{mj})(I_n + a\Delta_{im}) = \\ &= (I_n + \Delta_{mj} - a\Delta_{im})(I_n - \Delta_{mj} + a\Delta_{im}) = I_n + a\Delta_{ij} = E_{ij}(a) \end{aligned}$$

gdyż  $\Delta_{ab}\Delta_{bc} = \Delta_{ac}$  oraz  $\Delta_{ab}\Delta_{dc} = 0$  dla  $b \neq d$ .

W przypadku, gdy  $n = 2$  oraz  $|k| > 3$ , w  $k$  istnieje element  $x$  różny od 0, 1, -1. Wtedy  $x^2 \neq 1$  i dla  $y = \frac{a}{1-x^{-2\epsilon}}$  gdzie  $\epsilon = i - j \in \{-1, 1\}$  zachodzi

$$\begin{aligned} [E_{ij}(y), x\Delta_{11} + x^{-1}\Delta_{22}] &= \\ &= E_{ij}(y)(x\Delta_{11} + x^{-1}\Delta_{22})E_{ij}(y)^{-1}(x\Delta_{11} + x^{-1}\Delta_{22})^{-1} = \\ &= (I_n + y\Delta_{ij})(x\Delta_{11} + x^{-1}\Delta_{22})(I_n - y\Delta_{ij})(x^{-1}\Delta_{11} + x\Delta_{22}) = \\ &= (x\Delta_{11} + x^{-1}\Delta_{22} + yx^\epsilon\Delta_{ij})(x^{-1}\Delta_{11} + x\Delta_{22} - yx^{-\epsilon}\Delta_{ij}) = \\ &= \Delta_{11} + \Delta_{22} + y(1 - x^{-2\epsilon})\Delta_{ij} = I_n + a\Delta_{ij} = E_{ij}(a) \end{aligned}$$

$\square$

## 4.2. Prostota $PSL_n(k)$

**Twierdzenie 4.2.1.** *Grupa  $PSL_n(k)$  jest prosta dla  $n \geq 2$  i dowolnego ciała  $k$ , poza przypadkiem, gdy  $n = 2$  oraz  $|k| \leq 3$ .*



*Dowód.* Rozważmy działanie  $\rho$  grupy  $SL_n(k)$  na  $X$  – zbiorze jednowymiarowych podprzestrzeni  $k^n$  przez domnażanie, tzn. dla  $M \in SL_n(k)$  oraz  $v \in k^n, v \neq 0$  definiujemy  $\langle v \rangle^M = \langle Mv \rangle$ .

Wówczas dla  $M \in SZ_n$  zachodzi  $\langle v \rangle^M = \langle Mv \rangle = \langle \lambda v \rangle = \langle v \rangle$ . Zatem  $SZ_n \subset \ker \rho$ . Jeżeli natomiast  $M \in SL_n(k) \setminus SZ_n$ , to albo  $M$  ma niezerowy element  $a_{ij}$  dla  $i \neq j$ , więc przekształca podprzestrzeń rozpinaną przez wektor standardowy  $e_j$  na inną, albo  $M$  ma tylko elementy na przekątnej, ale dla pewnych  $i \neq j$  zachodzi  $a_{ii} \neq a_{jj}$  – wówczas  $\langle e_i + e_j \rangle^M = \langle a_{ii}e_i + a_{jj}e_j \rangle \neq \langle e_i + e_j \rangle$ . Stąd  $SZ_n = \ker \rho$ , czyli  $\rho$  indukuje wierne działanie  $\tilde{\rho}$  grupy  $SL_n(k)/SZ_n = PSL_n(k)$  na tym samym zbiorze.

Zauważmy również, że działanie  $\rho$ , a więc także  $\tilde{\rho}$ , jest 2-tranzytywne, stąd prymitywne. Jest tak, gdyż za pomocą mnożenia przez odpowiednią macierz, możemy przekształcić dowolną bazę  $k^n$  na inną. Dlatego chcąc przekształcić  $\langle v_i \rangle$  na  $\langle w_i \rangle$  dla  $i = 1, 2$  dopełniamy  $v_i$  do bazy  $v_1, \dots, v_n$  oraz  $w_i$  do bazy  $w_1, \dots, w_n$  i mnożymy  $w_n$  przez pewną stałą tak, żeby wyznacznik macierzy  $A$  o kolumnach  $v_i$  był równy wyznacznikowi macierzy  $B$  o kolumnach  $w_i$ . Dzięki temu macierz  $BA^{-1} \in SL_n(k)$  przekształca  $\langle v_i \rangle$  na  $\langle w_i \rangle$  dla  $i = 1, 2, \dots, n$ .

Rozważmy teraz stabilizator  $H$  punktu  $\langle e_1 \rangle$  przy działaniu  $\rho$ .  $H$  składa się z tych macierzy o wyznaczniku 1, które stabilizują  $\langle e_1 \rangle$ , czyli w pierwszej kolumnie mają wektor  $(\lambda, 0, 0, \dots, 0)$ , gdzie  $\lambda \in k^*$ .

Niech  $A$  będzie podzbiorem  $H$  macierzy o postaci blokowej  $\begin{pmatrix} 1 & v_{n-1} \\ 0_{n-1} & I_{n-1} \end{pmatrix}$ . Wówczas  $A$  jest abelową podgrupą  $H$ . Rzeczywiście:

$$\begin{pmatrix} 1 & v_{n-1} \\ 0_{n-1} & I_{n-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & w_{n-1} \\ 0_{n-1} & I_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & v_{n-1} + w_{n-1} \\ 0_{n-1} & I_{n-1} \end{pmatrix}$$

Zatem iloczyn elementów z  $A$  należy do  $A$ , jest przemienny oraz biorąc  $w_{n-1} = -v_{n-1}$  otrzymujemy, że odwrotność elementów z  $A$  również należy do  $A$ .

Ponadto  $A$  jest podgrupą normalną  $H$ , gdyż

$$\begin{aligned} & \begin{pmatrix} \lambda & w_{n-1} \\ 0_{n-1} & A_{n-1} \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & v_{n-1} \\ 0_{n-1} & I_{n-1} \end{pmatrix} \cdot \begin{pmatrix} \lambda & w_{n-1} \\ 0_{n-1} & A_{n-1} \end{pmatrix} = \\ & = \begin{pmatrix} \lambda^{-1} & w'_{n-1} \\ 0_{n-1} & A_{n-1}^{-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & v_{n-1} \\ 0_{n-1} & I_{n-1} \end{pmatrix} \cdot \begin{pmatrix} \lambda & w_{n-1} \\ 0_{n-1} & A_{n-1} \end{pmatrix} = \\ & = \begin{pmatrix} \lambda^{-1} & w'_{n-1} \\ 0_{n-1} & A_{n-1}^{-1} \end{pmatrix} \cdot \begin{pmatrix} \lambda & \lambda w_{n-1} + v_{n-1} A_{n-1} \\ 0_{n-1} & A_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & v'_{n-1} \\ 0_{n-1} & I_{n-1} \end{pmatrix} \end{aligned}$$

dla odpowiednio dobranych  $w'_{n-1}$  oraz  $v'_{n-1}$ .

Pokażemy teraz, że sprzężenia  $A$  w  $SL_n(k)$  zawierają wszystkie macierze elementarne  $E_{ij}(a)$  (dla  $i \neq j$ ). Dzięki temu oraz lematowi 4.1.1 będziemy wiedzieć, że sprzężenia  $A$  generują całe  $SL_n(k)$ .

Gdy  $n = 2$ , to  $E_{12}(a) \in A$  oraz

$$\begin{aligned} & \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \\ & \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} = E_{21}(a) \end{aligned}$$

Natomiast, gdy  $n \geq 3$  oraz  $j \neq m$  to z przechodniości naturalnego działania grupy  $A_n$  na zbiorze  $\{1, 2, \dots, n\}$  otrzymujemy pewien element  $\pi \in A_n$  taki, że  $\pi(1) = j$ . Niech  $l = \pi^{-1}(m) \neq 1$  oraz  $P_\pi$  – macierz permutacji  $\pi$ , tzn.  $P_\pi$  zawiera jedynki na pozycjach  $(i, \pi(i))$  a poza tym same zera. Wówczas z parzystości  $\pi$  dostajemy, że  $\det(P_\pi) = 1$ , czyli  $P_\pi \in SL_n(k)$  oraz

$$\begin{aligned} (P_\pi)^{-1} E_{1l}(a) P_\pi &= P_{\pi^{-1}}(I_n + a\Delta_{1l}) P_\pi = \\ &= I_n + P_{\pi^{-1}}(a\Delta_{1\pi(l)}) = I_n + a\Delta_{\pi(1)\pi(l)} = I_n + a\Delta_{jm} = E_{jm}(a) \end{aligned}$$

Przechodząc teraz do działania  $\tilde{\rho}$  widzimy, że stabilizatorem punktu  $\langle e_1 \rangle$  przy tym działaniu jest  $\tilde{H} = H/SZ_n \leq PSL_n(k)$ . Ponadto  $\tilde{A} = A/SZ_n$  jest abelową podgrupą normalną  $\tilde{H}$  oraz sprzężenia  $\tilde{A}$  generują  $PSL_n(k)$ , gdyż  $\tilde{g}\tilde{A}\tilde{g}^{-1} = (gAg^{-1})/SZ_n$ .

Udowodniliśmy zatem, że działanie  $\tilde{\rho}$  grupy  $PSL_n(k)$  na zbiorze  $X$  jest wierne, prymitywne oraz stabilizator  $\tilde{H}$  punktu  $\langle e_1 \rangle$  zawiera przemianą podgrupę normalną  $\tilde{A}$ , której sprzężenia generują całe  $PSL_n(k)$ .

Żeby skorzystać z lematu Iwasawy wystarczy pokazać, że  $PSL_n(k)$  jest grupą doskonałą, gdy  $n > 2$  lub  $|k| > 3$ . Ale z lematu 4.1.1 dostajemy, że macierze  $E_{ij}(a)$  generują  $SL_n(k)$ , zatem również elementy  $E_{ij}(a) \cdot SZ_n$  generują  $PSL_n(k)$ . Ponadto z lematu 4.1.2 wiemy, że dla  $n > 2$  lub  $|k| > 3$  macierze  $E_{ij}(a)$  są komutantami macierzy z  $SL_n(k)$ , więc także elementy  $E_{ij}(a) \cdot SZ_n$  są komutantami elementów z  $PSL_n(k)$ . Stąd zarówno grupa  $SL_n(k)$  jak i grupa  $PSL_n(k)$  jest grupą doskonałą.

Założenia lematu Iwasawy dla grupy  $PSL_n(k)$  są spełnione, zatem jest to grupa prosta.  $\square$

### 4.3. Dodatkowe informacje o $PSL_n(k)$ oraz lemacie Iwasawy

Na koniec tej pracy wspomnimy jeszcze o dwóch rzeczach – udowodnimy, że rzeczywiście grupy  $PSL_2(\mathbb{F}_2)$  oraz  $PSL_2(\mathbb{F}_3)$  nie są proste, a także podamy alternatywny dowód prostoty grup  $A_n$  dla  $n \geq 5$  – tym razem korzystając z lematu Iwasawy.

**Stwierdzenie 4.3.1.**  *$PSL_2(\mathbb{F}_2)$  oraz  $PSL_2(\mathbb{F}_3)$  nie są grupami prostymi.*

*Dowód.* W przypadku  $PSL_2(\mathbb{F}_2)$  zauważmy, że działanie  $\tilde{\rho}$ , takie jak w dowodzie poprzedniego twierdzenia, jest wiernym działaniem 2-przechodnim na zbiorze  $\{\langle e_1 \rangle, \langle e_2 \rangle, \langle e_1 + e_2 \rangle\}$ . Ale jak wcześniej pokazaliśmy, działanie 2-przechodnie na zbiorze 3 elementowym jest też 3-przechodnie, stąd  $\tilde{\rho}$  zadaje bijekcję między  $PSL_2(\mathbb{F}_2)$  a  $S_3$ , czyli  $PSL_2(\mathbb{F}_2) \simeq S_3$  nie jest grupą prostą.

Natomiast dla  $PSL_2(\mathbb{F}_2)$  działanie  $\tilde{\rho}$  jest wiernym działaniem 2-przechodnim na zbiorze 4 elementowym  $\{\langle e_1 \rangle, \langle e_2 \rangle, \langle e_1 + e_2 \rangle, \langle e_1 - e_2 \rangle\}$ . Zatem  $|PSL_2(\mathbb{F}_2)| \geq 12$ , gdyż mamy 12 możliwości wyboru par elementów  $(a, b)$ , na które ma przejść para  $(\langle e_1 \rangle, \langle e_2 \rangle)$ . Ponadto z wierności  $\tilde{\rho}$  otrzymujemy, że  $PSL_2(\mathbb{F}_2)$  jest izomorficzne z pewną podgrupą  $S_4$ , czyli  $PSL_2(\mathbb{F}_2)$  to  $A_4$  lub  $S_4$ . Ale  $\tilde{\rho}$  nie jest 4-przechodnie, bo jeśli zarówno  $\langle e_1 \rangle$  jak i  $\langle e_2 \rangle$  przechodzi na siebie, to również  $\langle e_1 + e_2 \rangle$  jak i  $\langle e_1 - e_2 \rangle$  przechodzi na siebie. Stąd  $PSL_2(\mathbb{F}_2) \simeq A_4$  nie jest grupą prostą.  $\square$

Teraz zobaczymy jak łatwo udowodnić prostotę  $A_n$  dla  $n \geq 5$  korzystając z lematu Iwasawy oraz dwóch prostych faktów o cyklach długości 3.

**Twierdzenie 2.3.1** (O prostocie  $A_n$ ).

*Grupa alternująca  $A_n$  jest prosta dla  $n \geq 5$ .*

*Dowód (II sposób).* Zauważmy najpierw, że dla  $n \geq 5$  cykle długości 3 są komutantami pewnych elementów z  $A_n$ . Rzeczywiście, dla parami różnych  $a, b, c, d, e \in \{1, 2, \dots, n\}$  mamy

$$\begin{aligned} [(b, c, d)(a, c, e)] &= (b, c, d)(a, c, e)(d, c, b)(e, c, a) = \\ &= (b, e, a, c, d)(d, a, e, c, b) = (a, b, c)(d)(e) = (a, b, c) \end{aligned}$$

Zatem z lematu 2.2.2 grupa  $A_n$  jest doskonała.

Rozważmy działanie  $\rho$  grupy  $A_n$  na trójelementowych podzbiorach zbioru  $\{1, 2, \dots, n\}$ , w którym po prostu przestawiam elementy zbioru  $\{1, 2, \dots, n\}$ , tzn dla  $\sigma \in A_n$  mamy  $\{a, b, c\}^\sigma = \{\sigma(a), \sigma(b), \sigma(c)\}$ . Wówczas jest to działanie wierne. Ponadto stabilizatorem zbioru  $\{1, 2, 3\}$  jest podgrupa  $H$  permutacji parzystych, która osobno permutuje zbiór  $\{1, 2, 3\}$  i osobno  $\{4, 5, \dots, n\}$ . Zatem  $A = \langle (1, 2, 3) \rangle \leq H$  jest oczywiście przemienną grupą, ale jest również podgrupą normalną  $H$ , gdyż  $(1, 2, 3)$  jest przemienne z permutacjami  $\{4, 5, \dots, n\}$  oraz sprzężenia  $A$  permutacjami zbioru  $\{1, 2, 3\}$  zachowują  $A$  ( $\langle (1, 2, 3) \rangle \trianglelefteq S_3$ ).

Ponadto z twierdzenia 2.2.2 wszystkie cykle długości 3 są sprzężone w  $A_n$  dla  $n \geq 5$  (co można udowodnić prościej, wprost), a z lematu 2.2.2 generują one całe  $A_n$ . Stąd sprzężenia  $A$  generują całą grupę  $A_n$ .

Możemy zatem skorzystać z lematu Iwasawy – dostajemy, że  $A_n$  jest grupą prostą dla  $n \geq 5$ , czyli tezę.  $\square$



# 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. Kargapólow, J. I. Mierzłakow, *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.