SZCZEGÓLNE PODGRUPY SKOŃCZONEGO INDEKSU W GRUPIE WARKOCZY B_3

BARTŁOMIEJ BYCHAWSKI

Streszczenie. W pracy konstruujemy interesujący geometrycznie przykład grupy o niskiej randze posiadającej podgrupy wysokiej rangi.

1. Wprowadzenie

W niniejszej pracy przedstawimy w postaci jawnej szczególne podgrupy wysokiej rangi i skończonego indeksu w grupie warkoczy. Motywacja stojąca za rozważaniami takich problemów jest geometryczna. Pośród wszystkich grup abelowych możemy wyróżnić tzw. *grupy powierzchni* i *grupy rozmaitości trójwymiarowych*, pochodzące od tzw. grup podstawowych tych przestrzeni [4]. O ile te pierwsze można wypisać jawnie i ich struktura jest zrozumiała od dawna [3], to te drugie nastręczają znacznie więcej problemów. Nie podejmujemy się tutaj omawiać pełnej ich listy, związanej z jedynym z rozwiązanych Problemów Milenijnych, z Hipotezą Poincaré [2], poprzestaniemy na powtórzeniu informacji, że o wielu z nich wiadomo, że są wirtualnie dość prostej postaci, oraz że bardzo ważnym niezmiennikiem tych grup jest ich ranga (wszystkie niezbędne definicje pojawią się niżej). Na podstawie prywatnej komunikacji od Andrzeja Czarneckiego i Katarzyny Krawiec pojawiło się pytanie: czy pomimo poważnych ograniczeń, jakie niesie bycie grupą rozmaitości trójwymiarowej, można znaleźć interesujące przykłady takich grup

(1) rangi 2, oraz
(2) wirtualnie $\mathbb{Z} \times F_2$ (a więc wirtualnie rangi 3), oraz
(3) podane w możliwie jawnej postaci.

Ponownie, poprzestaniemy na powtórzeniu informacji, że pozytywna odpowiedź ma znaczenie dla tzw. rozkładów Heegaarda.

Ogólny problem znalezienia grupy niskiej rangi będącej wirtualnie wysokiej rangi jest znany i najlepszym przykładem jest grupa wolna na dwóch generatorach, która wirtualnie jest grupą wolną na n generatorach, dla każdego $n \geqslant 2$, co wynika z tw. Nielsena-Schreiera [8]. F_2 nie jest jednak wirtualnie $\mathbb{Z} \times F_2$ (na podstawie tego samego twierdzenia). Prezentowana poniżej grupa warkoczy ten warunek spełnia, co więcej w [7] można przeczytać, że jest ona grupą podstawową dopełnienia węzła trójlistnika, a więc grupą podstawową rozmaitości trójwymiarowej

Praca napisana pod kierunkiem dra Piotra Miski w IMUJ.

z brzegiem. Po raz trzeci powtarzając jedynie zasłyszaną informację dodamy, że geometrycznie najciekawszy byłby przykład grupy będącej dodatkowo grupą podstawową rozmaitości bez brzegu, ale jego prezentacja nie jest tak elegancka i przejrzysta jak ta pokazana poniżej.

Celem niniejszej pracy jest wyznaczenie szczególnej podgrupy grupy warkoczy B_3 poprzez wyznaczenie zbioru jej generatorów oraz wykazanie, że jest to podgrupa normalna o skończonym indeksie. Następnie, korzystając z twierdzenia Nielsena-Schreiera (i jego wspomnianego zastosowania) udowodnimy, że dla dowolnego $n \geqslant 2$ grupa B_3 jest wirtualnie rangi n, ale nie jest wirtualnie rangi 1 (czyli wirtualnie cykliczna). Przy okazji uzyskamy rezultat, że grupa $SL_2(\mathbb{Z})$ jest wirtualnie wolna rangi 2, a więc również wirtualnie wolna dowolnej rangi $n \geqslant 2$. Praca jest inspirowana artykułem [6].

2. Podstawowe definicje

Większość definicji i pojęć w pracy opierać będziemy na książce [1], gdzie czytelnik znajdzie wszystkie podstawowe fakty z teorii grup. Będziemy starać się podawać wszystkie definicje i twierdzenia niezbędne do pracy, ale powstrzymamy się, na przykład, przed zdefiniowaniem, czym jest grupa, odsyłając Czytelnika w razie potrzeby do wspomnianej książki.

Grupy będziemy rozumieć przede wszystkim jako dane przez *prezentacje*: jako grupy słów na skończonym zbiorze liter (lub generatorów), wydzielone przez skończony zbiór relacji. Zapisywać je będziemy jako $\langle a_1, \ldots, a_n \mid r_1, \ldots, r_m \rangle$. Działanie wewnątrz takiej grupy będziemy zamiennie zapisywać przez konkatenację słów lub symbol $\cdot$, a więc używając zapisu multiplikatywnego, i zatem oczywiście oznaczając odwrotność elementu x przez x^{-1}. Słowo puste, czyli element neutralny oznaczać będziemy przez e - to w której grupie jest ono rozpatrywane wynikać będzie z kontekstu.

Grupę o pustym zbiorze relacji, a więc wolną na literach $a_1, \ldots, a_n$, oznaczamy przez F_n.

Jeśli z kontekstu będzie wynikać, że rozważamy podgrupę pewnej grupy X zawierającej elementy $x_1, \ldots, x_p$, zapis $\langle x_1, \ldots, x_p \rangle$ będzie oznaczać podgrupę X generowaną przez te elementy (a nie grupę wolną na tych literach).

Rangą grupy G, którą będziemy oznaczać $\operatorname{rank}(G)$, nazywamy najmniejszą możliwą moc zbioru generatorów pośród wszystkich możliwych prezentacji grupy. Odnotujmy, że będziemy korzystać bez dowodu z faktu, że F_n ma rangę n, podobnie jak grupa $\mathbb{Z}^n$, n-tek liczb całkowitych.

Nieco podobnie definiujemy *długość słowa* x w grupie o prezentacji $\langle a_1, \ldots, a_n \mid r_1, \ldots, r_m \rangle$ jako

$$\min \left\{ |k_1| + \ldots + |k_q| \mid x = a_{p_1}^{k_1} \cdot \ldots \cdot a_{p_q}^{k_q} \right\}$$

Słowo x jest zapisane w *zwartej formie*, jeżeli w wyrażeniu $a_{p_1}^{k_1} \cdot \ldots \cdot a_{p_q}^{k_q}$ nie występują obok siebie litery a_i i a_i^{-1}. Zauważmy, że ani zwarta forma elementu, ani jego najkrótszy możliwy zapis nie są dane jednoznacznie nawet w jednej ustalonej prezentacji (choć oczywiście długość słowa jest dobrze określona, i jest osiągana na słowie zapisanym w zwartej formie).

Zauważmy też drobną nieścisłość: długość właściwie powinna przysługiwać elementowi w grupie, nie słowu będącemu jedynie jego zapisem, ponieważ obliczamy ją właśnie po wszystkich słowach równych temu elementowi. Jednak "długość słowa" brzmi naturalniej niż "długość elementu" i mając nadzieję, że nie spowoduje to nieporozumień (i nie chcąc wprowadzać słowa "norma") będziemy stosować powyższe nazewnictwo.

W wypowiedzi i zastosowaniach Lematu 3.3 będziemy korzystać z działania grupy na zbiorze. Mówimy, że grupa G *działa na zbiór* X gdy istnieje odwzorowanie $G \times X \to X$ (które będziemy zapisywać $(g, x) \mapsto g.x$) takie, że:

(1) $\forall x \in X \; e.x = x$
(2) $\forall g_1, g_2 \in G \; \forall_{x \in X} \; g_1. (g_2.x) = (g_1 \cdot g_2) .x$

Zauważmy, że $x = e.x = (g \cdot g^{-1}) .x = g. (g^{-1}.x)$ co oznacza, że $g.x$ jest surjekcją. Ponieważ również $x = g^{-1}. (g.x)$, $g.x$ jest też injekcją, a zatem bijekcją dla każdego $g \in G$.

Wreszcie, będziemy mówić, że grupa G jest *wirtualnie* grupą H (lub: ma wirtualnie pewną własność), jeżeli H jest podgrupą G i *indeks* $[G : H]$, czyli moc zbioru warstw ${}^{G}/_{H}$, jest skończony (lub: istnieje w G podgrupa skończonego indeksu o rozważanej własności). Jak omówiliśmy we Wprowadzeniu, skupimy uwagę na pokazaniu, że pewne grupy są wirtualnie $\mathbb{Z} \times F_2$, oraz że są wirtualnie pewnej rangi.

3. Grupy macierzy

Grupę macierzy o wyrazach w $\mathbb{Z}$ o rozmiarach 2×2 i wyznaczniku równym 1 z działaniem mnożenia macierzy będziemy oznaczać $SL_2(\mathbb{Z})$

W obliczeniach i prezentacjach poniżej będziemy przyjmować następujące oznaczenia:

$$A_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \qquad A_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \qquad B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

Lemat 3.1. *Te trzy macierze z $SL_2(\mathbb{Z})$ spełniają następujące zależności:*

(1) $$A_1^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \qquad A_2^n = \begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix}$$

(2) $$A_1 \cdot A_2^{-1} \cdot A_1 = B$$

(3) $$B^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \qquad B^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Dowód. (1) Indukcyjnie sprawdzamy, że

$$\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & n-1 \\ 0 & 1 \end{bmatrix}$$

co dowodzi wzoru dla A_1. Podobnie sprawdzamy A_2.
(2) Rachunek pokazuje, że

$$A_1 \cdot A_2^{-1} \cdot A_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = B$$

(3) Trywialne. □

Ze względu na dwie ostatnie równości otrzymujemy relację w podgrupie $\langle A_1, A_2 \rangle$, co pokazuje że podgrupa ta nie jest wolna.

Zbadamy teraz, w jaki sposób elementy A_1, A_2 oraz B wpływają na daną macierz przy przemnożeniu z lewej i prawej strony.

(1) $$A_1 \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ c & d \end{bmatrix} \qquad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot A_1 = \begin{bmatrix} a & a+b \\ c & c+d \end{bmatrix}$$

(2) $$A_2 \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ a+c & b+d \end{bmatrix} \qquad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot A_2 = \begin{bmatrix} a+b & b \\ c+d & d \end{bmatrix}$$

(3) $$B \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} c & d \\ -a & -b \end{bmatrix} \qquad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot B = \begin{bmatrix} -b & a \\ -d & c \end{bmatrix}$$

Wykorzystując te wzory, pokażemy następujące twierdzenie.

Twierdzenie 3.2. $SL_2(\mathbb{Z}) = \langle A_1, A_2 \rangle$

Dowód. Dowód, że każda macierz $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ należy do $\langle A_1, A_2 \rangle$ przeprowadzimy za pomocą indukcji względem $|a| + |c|$.

Na początku zauważmy, że $|a| + |c| > 0$ bo inaczej $a = 0 = c$, co daje: $\left|\begin{smallmatrix} 0 & b \\ 0 & d \end{smallmatrix}\right| = 0$, więc taka macierz nie należy do $SL_2(\mathbb{Z})$.

Baza indukcji: niech $|a| + |c| = 1$.

(1) $a = 1$ oraz $c = 0$. Wyznacznik $1 = \left|\begin{smallmatrix} 1 & b \\ 0 & d \end{smallmatrix}\right| = 1 \cdot d - b \cdot 0 = d$ oznacza, biorąc pod uwagę poprzednie wnioski, że
$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = A_1^b$$

(2) $a = (-1)$ oraz $c = 0$. W tym wypadku
$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -1 & b \\ 0 & d \end{bmatrix} = B^2 \cdot \begin{bmatrix} 1 & -b \\ 0 & -d \end{bmatrix}$$
więc sprowadziliśmy ten przypadek do wcześniej już rozwiązanego.

(3) $a = 0$ oraz $|c| = 1$. W tym wypadku
$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 0 & b \\ c & d \end{bmatrix} = B \cdot \begin{bmatrix} -c & -d \\ 0 & -b \end{bmatrix}$$
co również sprowadza się do wcześniej rozwiązanych przypadków.

Dowód bazy indukcji jest zakończony. Krok indukcyjny: zauważmy na początku, że jeśli $|a|+|c|>1$ to $a,c\neq 0$. Gdyby $a=0$ lub $c=0$, to z $1=ad-bc$ otrzymalibyśmy odpowiednio $|c|=1$ lub $|a|=1$, czyli $|a|+|c|=1$. Bez straty ogólności (ze względu na możliwość mnożenia z lewej strony przez B) załóżmy, że $|a|\geqslant|c|$. Zapiszmy naszą macierz na dwa następujące sposoby

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = A_1 \cdot \begin{bmatrix} a-c & b-d \\ c & d \end{bmatrix} = A_1^{-1} \cdot \begin{bmatrix} a+c & b+d \\ c & d \end{bmatrix}$$

i rozważmy dwa przypadki:

(1) $sgn\,(a) = sgn\,(c)$. W tym przypadku zachodzi $|a-c| = |a|-|c|$, a stąd $|a-c|+|c| = |a| < |a|+|c|$, więc na mocy założenia indukcyjnego macierz $\left[\begin{smallmatrix} a-c & b-d \\ c & d \end{smallmatrix}\right]$ należy do $\langle A_1, A_2\rangle$, co oznacza, że macierz $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ także należy do tej grupy, co kończy dowód kroku indukcyjnego w tym przypadku.

(2) $sgn\,(a) \neq sgn\,(c)$. W tym przypadku zachodzi $|a+c| = |a|-|c|$, a stąd $|a+c|+|c| = |a| < |a|+|c|$, więc na mocy założenia indukcyjnego macierz $\left[\begin{smallmatrix} a+c & b+d \\ c & d \end{smallmatrix}\right]$ należy do $\langle A_1, A_2\rangle$ co oznacza, że macierz $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ także należy do tej grupy, co kończy dowód kroku indukcyjnego w tym przypadku.

W konsekwencji dowód całego twierdzenia jest zakończony. □

Warto zauważyć, że grupa $SL_2(\mathbb{Z})$ nie może zostać wygenerowana przez mniejszą liczbę generatorów: nie jest cykliczna, gdyż oznaczałoby to, że jest abelowa, tymczasem generatory A_1 i A_2 nie komutują:

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \qquad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$

Twierdzenie 3.3 (Ping-Pong Lemma)**.** *Jeśli grupa G działa na zbiór X, i istnieją takie $a,b\in G$ oraz $A,B\subseteq X$, że $A\nsubseteq B$, $B\nsubseteq A$ i dla każdego $n\in\mathbb{Z}\setminus\{0\}$ zachodzi $a^n.B\subseteq A$, $b^n.A\subseteq B$, to grupa $\langle a,b\rangle$ jest wolna.*

Dowód. Załóżmy nie wprost, że grupa $\langle a,b\rangle$ nie jest wolna. Oznacza to, że istnieje w niej pewna relacja, czyli nietrywialne słowo równe identyczności - niech będzie to S. Mamy dwa przypadki, pierwszy gdy słowo S zapisane w pewnej zwartej formie ma pierwszą literę różną od ostatniej (przy czym w tym miejscu traktujemy a i a^{-1} jak tą samą literę), oraz przypadek drugi, gdy pierwsza i ostatnia litera są takie same.

Przypadek pierwszy sprowadza się do drugiego następująco. Bez straty ogólności (przez symetrię w założeniach lematu), niech pierwszą literą będzie a, ostatnią b. W takim wypadku mamy $a^{j_1}\cdot\ldots\cdot b^{k_s}=e$. Sprzęgając to wyrażenie przez element $a^{sgn(j_1)}$ otrzymujemy

$$a^{j_1+sgn(j_1)}\cdot\ldots\cdot b^{k_s}\cdot a^{sgn(j_1)} = a^{sgn(j_1)}\cdot e\cdot a^{-sgn(j_1)} = e$$

A skoro $j_1+sgn\,(j_1)\neq 0$ to wystarczy nam rozważyć przypadek drugi.

Ponownie, bez straty ogólności, możemy założyć, że nasze słowo zaczyna się i kończy na a. Mamy więc $a^{j_1} \cdot \ldots \cdot a^{j_{s-1}} \cdot b^{k_{s-1}} \cdot a^{j_s} = e$. Z założenia lematu mamy $B = e.B = \left(a^{j_1} \cdot \ldots \cdot a^{j_{s-1}} \cdot b^{k_{s-1}} \cdot a^{j_s}\right).B$. Zauważmy jednak, że $a^{j_s}.B \subseteq A$, a stąd $\left(b^{k_{s-1}} \cdot a^{j_s}\right).B = b^{k_{s-1}}.\left(a^{j_s}.B\right) \subseteq B$ z założeń lematu, i następnie

$$\left(a^{j_{s-1}} \cdot b^{k_{s-1}} \cdot a^{j_s}\right).B = a^{j_{s-1}}.\left(\left(b^{k_{s-1}} \cdot a^{j_s}\right).B\right) \subseteq A$$

Powtarzając powyższe rozumowanie do końca słowa otrzymujemy

$$B = e.B = \left(a^{j_1} \cdot \ldots \cdot a^{j_{s-1}} \cdot b^{k_{s-1}} \cdot a^{j_s}\right).B \subseteq A$$

co przeczy założeniom lematu i kończy jego dowód (formalnie indukcyjny względem długości danego słowa). □

Zdefiniujmy teraz ciekawą podgrupę $SL_2(\mathbb{Z})$, tzw. grupę Sanowa [5], $\langle A_1^2, A_2^2\rangle$.

Twierdzenie 3.4. *Grupa Sanowa jest wolna.*

Dowód. Zastosujemy Ping-Pong Lemma. Połóżmy więc $G = SL_2(\mathbb{Z})$, $a = A_1^2$, $b = A_2^2$, $X = \mathbb{R}^2$, $A = \{(x, y) \in \mathbb{R}^2 : |x| > |y|\}$, $B = \{(x, y) \in \mathbb{R}^2 : |x| < |y|\}$.

Udowodnimy teraz, że warunki lematu są spełnione. Warunki te są symetryczne, więc ich dowody także będą symetryczne. Przedstawimy dowód, że $b^n.A \subseteq B$.

Niech $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] \in A$. W tym wypadku

$$b^n.\begin{bmatrix} x \\ y \end{bmatrix} = A_2^{2n} \cdot \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 2n & 1 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ 2nx + y \end{bmatrix}$$

Teraz, znając jawną formę wyrażenia $b^n.\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]$, wystarczy pokazać, że wektor ten należy do B, czyli że $|x| < |2nx + y|$. Sprawdzamy

$$|2nx + y| \geqslant |2nx| - |y| = 2|n||x| - |y| \geqslant 2|x| - |y| = |x| + (|x| - |y|) > |x|$$

co wynika z nierówności trójkąta i definicji A. Udowodniliśmy więc, że $b^n.A \subseteq B$, analogicznie otrzymamy $a^n.B \subseteq A$, oczywiście $A \cap B = \emptyset$, tak więc grupa Sanowa spełnia założenia Ping-Pong Lemma, a zatem jest wolna. □

Warto zauważyć, że $\langle A_1^2, A_2^2\rangle \leqslant SL_2(\mathbb{Z})$ jest wolną podgrupą rangi dwa w grupie nie-wolnej, a również rangi dwa.

4. Grupy warkoczy

Zdefiniujmy wreszcie grupę warkoczy na trzech pasmach zawartą w tytule tej pracy.

Definicja 4.1. Grupę $B_3 = \langle \sigma_1, \sigma_2 \mid \sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2\rangle$ będziemy nazywać *grupą warkoczy* (na trzech pasmach).

Zdefiniujmy homomorfizm:

$$\varphi : B_3 \to SL_2(\mathbb{Z})$$

taki, że

$$\sigma_1 \mapsto A_1 \qquad \sigma_2 \mapsto A_2^{-1}$$

Udowodnijmy (szybko i jedynie dla kompletności pracy), że taki homomorfizm istnieje. Wystarczy zauważyć, że odwzorowanie między dwiema grupami danymi przez dwie prezentację i zadane na generatorach rozszerza się (w jedyny sposób) do homomorfizmu grup wtedy i tylko wtedy, gdy każda relacja pomiędzy generatorami w dziedzinie jest spełniona pomiędzy obrazami tych generatorów w przeciwdziedzinie. W naszym przypadku, jedyna relacja $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$ musi dawać relację $A_1A_2^{-1}A_1 = A_2^{-1}A_1A_2^{-1}$. Ten pierwszy iloczyn policzyliśmy w Lemacie 3.1, w punkcie (2), otrzymując macierz B. Ten drugi wynosi

$$A_2{}^{-1}A_1A_2{}^{-1} = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = B$$

a zatem φ istotnie jest homomrfizmem.

Oczywiście jest to surjekcja, ponieważ jej obraz zawiera wszystkie generatory całej grupy. Nie jest jednak injekcją, gdyż w $SL_2(\mathbb{Z})$ zachodzą relacje, których analogi nie zachodzą w B_3. Przykładem tego jest relacja wykorzystująca równość (3) z Lematu 3.1

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = B^4 = \left(A_1A_2^{-1}A_1\right)^4 = \left(A_1A_2^{-1}A_1A_2^{-1}A_1A_2^{-1}\right)^2$$
$$= \left(A_1A_2^{-1}\right)^6 = \varphi\left((\sigma_1\sigma_2)^6\right)$$

ponieważ $(\sigma_1\sigma_2)^6 \neq e$, ponieważ oznaczałoby to, że istnieje ciąg przekształceń używających relacji grupy B_3 zamieniający e w $(\sigma_1\sigma_2)^6$. Jednak niezmiennikiem każdego takiego ciągu przekształceń (składającego się z wielokrotnego dodawania bądź usuwania słowa z relacji w dowolnym miejscu danego słowa) jest liczba liter (liczonych z wykładnikami) w zapisie danego słowa. Jest tak, gdyż jedyną relacją w B_3 jest $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$ a ta relacja zachowuje powyższy niezmiennik. Dla wyrazu e suma ta jest oczywiście równa 0, zaś dla $(\sigma_1\sigma_2)^6$ wynosi ona 12 (i ta liczba powróci do nas w przyszłości). Analogicznie można również wykazać, że $\left((\sigma_1\sigma_2)^3\right)^n \neq e$ dla $n \in \mathbb{Z} \setminus \{0\}$.

Możemy teraz bliżej przyjrzeć się strukturze grupy B_3. Opiszemy jej centrum.

Twierdzenie 4.2. $(\sigma_1\sigma_2)^3 \in Z(B_3)$

Dowód. Wystarczy wykazać, że $(\sigma_1\sigma_2)^3$ jest przemienny z generatorami B_3.

Zauważmy najpierw, że dzięki relacji w B_3 możemy zapisać $(\sigma_1\sigma_2)^3 = (\sigma_2\sigma_1)^3$, tak więc dowody dla obu generatorów będą przebiegać w sposób analogiczny. Dla σ_1 mamy:

$$\sigma_1(\sigma_2\sigma_1)^3 = \sigma_1\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2\sigma_1 = (\sigma_1\sigma_2)^3\sigma_1 = (\sigma_2\sigma_1)^3\sigma_1$$

Przeliczenia dla drugiego generatora przebiegają podobnie i dowód jest zakończony. □

Przyjrzyjmy się teraz pewnej podgrupie B_3: $\langle\sigma_1^2, \sigma_2^2\rangle$. Homomorfizm φ przekształca tę grupę dokładnie na grupę $\left\langle A_1^2, A_2^{-2}\right\rangle = \langle A_1^2, A_2^2\rangle$ czyli grupę Sanowa. W Twierdzeniu 3.4 udowodniliśmy, że grupa Sanowa jest wolna. Wykorzystajmy ten fakt, żeby pokazać to samo o $\langle\sigma_1^2, \sigma_2^2\rangle$.

Twierdzenie 4.3. *Grupa* $\langle\sigma_1^2,\sigma_2^2\rangle$ *jest wolna.*

Jest to zgodne z intuicją - grupa B_3 ma mniejszy (w sensie zawierania) zbiór relacji niż $SL_2(\mathbb{Z})$, więc skoro korzystając z większego zbioru relacji nie jesteśmy w stanie stworzyć relacji w grupie Sanowa, to tym bardziej nie dokonamy tego z mniejszą liczbą relacji dla analogicznej grupy $\langle\sigma_1^2,\sigma_2^2\rangle$. Uściślijmy tę intuicję.

Dowód. Przeprowadzimy dowód nie wprost. Niech $R(\sigma_1^2,\sigma_2^2)=e$ będzie nietrywialną relacją w tej grupie. Stąd otrzymujemy:

$$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}=\varphi(e)=\varphi\left(R\left(\sigma_1^2,\sigma_2^2\right)\right)=R\left(A_1,A_2^{-1}\right)$$

Jednak, skoro $R(\sigma_1^2,\sigma_2^2)$ nie było słowem trywialnym, to także $R\left(A_1,A_2^{-1}\right)$ nie jest, a to oznacza, że $R\left(A_1,A_2^{-1}\right)$ jest relacją w grupie Sanowa, co stoi w sprzeczności z Twierdzeniem 3.4, i kończy dowód nie wprost. □

Zauważmy, że odwracając kierunek rozumowania, pokazaliśmy właśnie że odwzorowanie φ obcięte do $\langle\sigma_1^2,\sigma_2^2\rangle$ jest injekcją (nietrywialny element $R(\sigma_1^2,\sigma_2^2)$ w jądrze daje słowo $R\left(A_1,A_2^{-1}\right)$, które musi być trywialne, dając sprzeczność z nietrywialnością w dziedzinie).

Przyjrzyjmy się teraz ciekawej - i jak się przekonamy później "dużej" - podgrupie grupy B_3, mianowicie $\left\langle(\sigma_1\sigma_2)^3,\sigma_1^2,\sigma_2^2\right\rangle$.

Twierdzenie 4.4. $\left\langle(\sigma_1\sigma_2)^3,\sigma_1^2,\sigma_2^2\right\rangle\simeq\mathbb{Z}\times F_2$

Dowód. Zauważmy, że ze względu na Twierdzenie 4.2 każdy element $\left\langle(\sigma_1\sigma_2)^3,\sigma_1^2,\sigma_2^2\right\rangle$ można zapisać w postaci $\left((\sigma_1\sigma_2)^3\right)^n\cdot\sigma$ gdzie $n\in\mathbb{Z}$ oraz $\sigma\in\langle\sigma_1^2,\sigma_2^2\rangle$. Zapis ten będzie jednoznaczny, jeśli pokażemy następujący lemat

Lemat 4.5. $\left\langle(\sigma_1\sigma_2)^3\right\rangle\cap\langle\sigma_1^2,\sigma_2^2\rangle=\{e\}$

Dowód Lematu. Pokażemy od razu, że jedynym elementem w $\langle\sigma_1^2,\sigma_2^2\rangle$ należącym do centrum B_3 jest e - co wystarczy, bo Twierdzenie 4.2 implikuje, że pierwsza z grup w lemacie zawiera się w centrum. Posłużymy się w tym celu Twierdzeniem 4.3 oraz dowodem nie wprost.

Załóżmy więc, że istnieje $x\neq e$ takie, że $x\in Z(B_3)\cap\langle\sigma_1^2,\sigma_2^2\rangle$. Dowód rozłożymy na dwa symetryczne przypadki:

(1) gdy zapis $x\in\langle\sigma_1^2,\sigma_2^2\rangle$ w zwartej formie w tych generatorach kończy się na σ_1^2 lub σ_1^{-2};
(2) gdy zapis $x\in\langle\sigma_1^2,\sigma_2^2\rangle$ w zwartej formie w tych generatorach kończy się na σ_2^2 lub σ_2^{-2}.

W obu przypadkach rozumowanie przebiega analogicznie. Poniżej przedstawimy dokładny dowód dla pierwszego z nich.

Niech x kończy się na σ_1^2. Skoro $x\in Z(B_3)$, to $x\cdot\sigma_2^2=\sigma_2^2\cdot x$ a zatem $x\sigma_2^2x^{-1}\sigma_2^{-2}=e$. Ale z warunku na x, to x^{-1} zaczyna się potęgą σ_1^2, stąd powyższego słowa zawierającego podsłowo $\sigma_1^2\sigma_2^2\sigma_1^{-2}$ nie da się uprościć do słowa pustego e. Zatem $x\sigma_2^2x^{-1}\sigma_2^{-2}=e$ byłoby nietrywialną relacją, co jest sprzeczne z Twierdzeniem 4.3. Ponieważ pozostałe przypadki rozważa się analogicznie, ta sprzeczność kończy dowód nie wprost i dowodzi tezy lematu. □

Ponieważ zgodnie z uwagą nad Twierdzeniem 4.2 $(\sigma_1\sigma_2)^3$ jest nieskończonego rzędu, powyższe jednoznaczne zapisy elementów grupy $\left\langle (\sigma_1\sigma_2)^3, \sigma_1^2, \sigma_2^2 \right\rangle$ jako iloczynów $\left((\sigma_1\sigma_2)^3\right)^n \cdot \sigma$ zadaje bijekcję (i izomorfizm) między tą grupą, a grupą par $\{(n,\sigma) \mid n \in \mathbb{Z}, \sigma \in \langle \sigma_1^2, \sigma_2^2 \rangle\} \simeq \mathbb{Z} \times F_2$. Dowód twierdzenia jest zatem zakończony. □

Twierdzenie 4.6. $\left\langle (\sigma_1\sigma_2)^3, \sigma_1^2, \sigma_2^2 \right\rangle$ *jest podgrupą normalną* B_3.

Dowód. Dla ułatwienia zapisu oznaczmy $H = \left\langle (\sigma_1\sigma_2)^3, \sigma_1^2, \sigma_2^2 \right\rangle$

Wystarczy nam sprawdzić warunek $gH = Hg$ tylko dla generatorów σ_1 i σ_2. Dowody obu faktów przebiegają analogicznie, przedstawimy więc tylko jeden z nich.

Równość $\sigma_1 H = H\sigma_1$ to dwie przeciwne inkluzje $\sigma_1 H \subseteq H\sigma_1$ oraz $H\sigma_1 \subseteq \sigma_1 H$. Ponownie, bez straty ogólności przedstawimy dowód tylko tej pierwszej - dowód drugiej różni się tym, że wszystkie przeprowadzane rachunki będą "lustrzane".

Niech więc $\sigma_1\sigma \in \sigma_1 H$ i pokażemy, że $\sigma_1\sigma \in H\sigma_1$. Przeprowadzimy dowód indukcyjny ze względu na długość $\sigma \in H$ jako słowa w tej grupie. Baza indukcji jest oczywista - słowo długości 0 to element neutralny, który spełnia powyższe warunki. Przechodzimy do kroku indukcyjnego. Z założenia indukcyjnego teza zachodzi dla słów długości $n-1$. Słowo σ zapisane w zwartej formie kończy się na jeden z generatorów grupy H bądź jego odwrotność. Niech h będzie pierwszą literą tego zapisu σ i niech $\sigma = h \cdot \sigma'$, gdzie σ' to słowo złożone z ostatnich $n-1$ liter słowa σ, a zatem długości co najwyżej $n-1$. Mamy więc trzy przypadki:

(1) h jest $(\sigma_1\sigma_2)^3$ lub jego odwrotnością;
(2) h jest σ_1^2 lub jego odwrotnością;
(3) h jest σ_2^2 lub jego odwrotnością.

Przypadek pierwszy. $(\sigma_1\sigma_2)^3$ należy do $Z(B_3)$ więc zachodzi $\sigma_1 (\sigma_1\sigma_2)^3 \sigma' = (\sigma_1\sigma_2)^3 \sigma_1\sigma'$ co z założenia indukcyjnego należy do $H\sigma_1$. Analogicznie traktujemy $h = (\sigma_1\sigma_2)^{-3}$.

Przypadek drugi. Ponieważ $\sigma_1\sigma_1^2\sigma' = \sigma_1^3\sigma' = \sigma_1^2\sigma_1\sigma'$ a to już należy do $H\sigma_1$. Analogicznie dla $h = \sigma_1^{-2}$.

Przypadek trzeci. Chcemy znaleźć takie $x \in H$, żeby $\sigma_1\sigma_2^2 = x\sigma_1$, a zatem x musi być $\sigma_1\sigma_2^2\sigma_1^{-1}$. Sprawdzimy, że taki x istotnie jest w H, używając w trzeciej równości relacji w B_3.

$$\begin{aligned} x &= \sigma_1\sigma_2^2\sigma_1^{-1} = \sigma_2^{-1}\sigma_2\sigma_1\sigma_2\sigma_2\sigma_1^{-1} = \sigma_2^{-1}\sigma_1\sigma_2\sigma_1\sigma_2\sigma_1^{-1} = \\ &= \sigma_2^{-2}\sigma_2\sigma_1\sigma_2\sigma_1\sigma_2\sigma_1\sigma_1^{-2} = \sigma_2^{-2}(\sigma_1\sigma_2)^3\sigma_1^{-2} \end{aligned}$$

Dzięki temu $\sigma_1\sigma_2^2 = x\sigma_1 \in H\sigma_1$, i możemy wywnioskować, że $\sigma_1\sigma_2^2\sigma' = x\sigma_1\sigma'$, co jak wcześniej należy do $H\sigma_1$ z założenia indukcyjnego. Jak wcześniej, analogicznie traktujemy $h = \sigma_2^{-2}$. Kończy to dowód normalności grupy H w B_3. □

5. Wirtualne własności omawianych grup

Zdefiniujmy teraz odwzorowanie

$$\psi : SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}_2)$$
$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} a\,(mod2) & b\,(mod2) \\ c\,(mod2) & d\,(mod2) \end{bmatrix}$$

Jest to homomorfizm, ponieważ redukcja mod 2 jest homomorfizmem i mnożenie macierzy jest zdefiniowane przy pomocy działań w $\mathbb{Z}$. Ponadto jest to oczywiście epimorfizm.

Znany jest fakt, że grupa $SL_2(\mathbb{Z}_2)$ jest izomorficzna z grupą permutacji zbioru trójelementowego S_3 (co można pokazać wprost na sześciu elementach obu grup, lub sprawdzając prezentacje, których będziemy używać, rozumując tak jak we wcześniejszych częściach pracy).

Grupę S_3 można zaprezentować w postaci: $\left\langle \sigma_1, \sigma_2 \mid (\sigma_1\sigma_2)^3 = \sigma_1^2 = \sigma_2^2 = e \right\rangle$. Zapiszemy więc $SL_2(\mathbb{Z}_2) = \left\langle g_1, g_2 \mid (g_1 g_2)^3 = g_1^2 = g_2^2 = e \right\rangle$ gdzie $g_1 = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ oraz $g_2 = \left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right]$.

Rozważmy teraz homomorfizm $\psi \circ \varphi$ przeprowadzający

$$\sigma_1 \mapsto \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = g_1 \qquad \sigma_2 \mapsto \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = g_2$$

Tak więc generatory grupy B_3 przechodzą przez złożenie homomorfizmów na generatory grupy $SL_2(\mathbb{Z}_2)$, mamy więc epimorfizm między tymi grupami. Używając pierwszego twierdzenia o izomorfizmach zapisujemy:

$$SL_2(\mathbb{Z}_2) = \left\langle g_1, g_2 \mid (g_1 g_2)^3 = g_1^2 = g_2^2 = e \right\rangle = B_3 \Big/ \left((\sigma_1\sigma_2)^3 = \sigma_1^2 = \sigma_2^2 = e \right)$$

Gdzie ostatni zapis oznacza grupę ilorazową grupy B_3 przez najmniejszą podgrupę normalną zawierającą elementy wypisane jako relacje. Zauważmy jednak, że najmniejsza taka podgrupa normalna to na podstawie Twierdzenia 4.6 po prostu podgrupa generowana przez te elementy - $\left\langle (\sigma_1\sigma_2)^3, \sigma_1^2, \sigma_2^2 \right\rangle$. W szczególności widzimy, że podgrupa ta jest jądrem homomorfizmu $\psi\circ\varphi$. Wiedząc, że jest on epimorfizmem otrzymujemy, że indeks

$$\left[B_3 : \left\langle (\sigma_1\sigma_2)^3, \sigma_1^2, \sigma_2^2 \right\rangle \right] = |S_3| = 6$$

Oznacza to w szczególności, że grupa B_3 jest wirtualnie grupą $\mathbb{Z} \times F_2$.

Z powyższego, z poprzednich wyliczeń w $SL_2(\mathbb{Z})$, z faktu, że φ jest epimorfizmem, zaś $\psi(B^2) = \psi\left(\left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right]\right) = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right] = e$ wynika, że jądrem ψ jest podgrupa $\langle B^2, A_1^2, A_2^2 \rangle$. Rozważmy grupę $\langle B^2, A_1^2, A_2^2 \rangle \big/ \langle A_1^2, A_2^2 \rangle$. Z zapisu każdego elementu grupy $\langle B^2, A_1^2, A_2^2 \rangle$ w postaci $B^{2n} \cdot A$ gdzie $n \in \mathbb{Z}$ oraz $A \in \langle A_1^2, A_2^2 \rangle$ wynika, że grupa ilorazowa ma jedynie dwie warstwy:

$$\langle B^2, A_1^2, A_2^2 \rangle \big/ \langle A_1^2, A_2^2 \rangle = \left\{ \left\langle A_1^2, A_2^2 \right\rangle, B^2 \cdot \left\langle A_1^2, A_2^2 \right\rangle \right\}$$

Oznacza to w szczególności, że indeks $[\langle B^2, A_1^2, A_2^2 \rangle : \langle A_1^2, A_2^2 \rangle] = 2$.

Powyżej udowodniliśmy, że jądrem złożenia epimorfizmów $\psi \circ \varphi$ jest $\left\langle (\sigma_1\sigma_2)^3, \sigma_1^2, \sigma_2^2 \right\rangle$. Zatem jądrem epimorfizmu ψ jest obraz tej podgrupy po przekształceniu φ, czyli $\langle B^2, A_1^2, A_2^2 \rangle$.

Stąd wynika, że indeks

$$\left[SL_2(\mathbb{Z}) : \left\langle B^2, A_1^2, A_2^2 \right\rangle\right] = |S_3| = 6$$

Powyższe, na podstawie twierdzenia Lagrange'a daje

$$\begin{aligned}\left[SL_2(\mathbb{Z}) : \left\langle A_1^2, A_2^2 \right\rangle\right] &= \left[SL_2(\mathbb{Z}) : \left\langle B^2, A_1^2, A_2^2 \right\rangle\right] \cdot \left[\left\langle B^2, A_1^2, A_2^2 \right\rangle : \left\langle A_1^2, A_2^2 \right\rangle\right] \\ &= 6 \cdot 2 = 12\end{aligned}$$

i jest to ta sama liczba 12, której powrót anonsowaliśmy wcześniej. Widzimy więc, że $SL_2(\mathbb{Z})$ jest wirtualnie wolna. Udowodnijmy teraz w dwóch krokach, że B_3 nie jest grupą wirtualnie wolną.

Najpierw udowodnimy, że nie jest to wirtualnie grupa wolna rangi n dla $n \geqslant 2$, a następnie że grupa ta nie jest wirtualnie cykliczna.

Twierdzenie 5.1. *Grupa G posiadająca nieskończone centrum $Z(G)$ nie jest wirtualnie wolna rangi n dla $n \geqslant 2$.*

Dowód. Załóżmy nie wprost, że grupa G jest wirtualnie wolna rangi n dla pewnego $n \geqslant 2$, czyli załóżmy, że istnieje $K \leqslant G$, będące grupą wolną niecykliczną oraz indeks $[G : K]$ jest skończony. Korzystając z nieskończonej zasady szufladkowej Dirichleta wnioskujemy, że istnieje warstwa gK zawierająca nieskończenie elementów z $Z(G)$, na nasze potrzeby wystarczy, aby istniały dwa różne takie elementy. Niech tymi elementami będą $a \neq b$, czyli $a, b \in Z(G) \cap gK$, a stąd $aK = gK = bK$ co daje $b^{-1}a \in K$. Oczywiście $b^{-1}a \in Z(G)$ oraz $b^{-1}a \in Z(K)$, a skoro K była grupą wolną rangi $n \geqslant 2$, to $Z(K) = e$ i $b^{-1}a = e$, co daje $a = b$ i sprzeczność. □

Twierdzenie 5.2. *B_3 nie jest grupą wirtualnie cykliczną.*

Dowód. Przyjmijmy ponownie oznaczenie: $H = \left\langle (\sigma_1\sigma_2)^3, \sigma_1^2, \sigma_2^2 \right\rangle$. Podobnie jak wyżej przeprowadzimy dowód nie wprost. Załóżmy więc, że istnieje $K \leqslant B_3$ takie, że $K = \langle x \rangle$ oraz $[B_3 : K]$ jest skończony. Przyjrzyjmy się teraz zbiorowi $H \cap K$. Biorąc pod uwagę, że grupa $\left\langle (\sigma_1\sigma_2)^3 \right\rangle \subset H$ jest nieskończona, możemy znów skorzystać z nieskończonej zasady szufladkowej Dirichleta i stwierdzić, że wśród skończenie wielu warstw B_3/K istnieje warstwa zawierająca nieskończenie wiele elementów grupy $\left\langle (\sigma_1\sigma_2)^3 \right\rangle$. Analogicznie jak poprzednio, niech $a \neq b$ będą dwoma różnymi elementami należącymi do takiej warstwy gK. Stąd ponownie $aK = gK = bK$ i $e \neq b^{-1}a \in H \cap K$.

To przecięcie jest, jak wynika z naszych rozważań, nietrywialną podgrupą cykliczną dwóch podgrup cyklicznych, a zatem istnieje takie $n \neq 0$, że $\langle x^n \rangle = H \cap K$, oraz, z konstrukcji, takie niezerowe m, że $x^n = \left((\sigma_1\sigma_2)^3\right)^m$.

Uzasadnimy teraz następujący ciąg zależności:

$$\begin{aligned}[B_3 : K] &\overset{(1)}{\geqslant} [H : H \cap K] = \left[H : \left\langle \left((\sigma_1\sigma_2)^3\right)^m \right\rangle\right] \geqslant \\ &\overset{(2)}{\geqslant} \left[H : \left\langle \left((\sigma_1\sigma_2)^3\right) \right\rangle\right] \overset{(3)}{=} \left|\left\langle \sigma_1^2, \sigma_2^2 \right\rangle\right|\end{aligned}$$

który oczywiście przeczy założeniu, że $[B_3 : K]$ jest skończony i kończy dowód nie wprost.

Idąc od końca, równość (3) wynika z tego, że grupa $\left\langle (\sigma_1\sigma_2)^3, \sigma_1^2, \sigma_2^2 \right\rangle$ jest izomorficzna z $\left\langle (\sigma_1\sigma_2)^3 \right\rangle \times \langle \sigma_1^2, \sigma_2^2 \rangle$ (co wynika z dowodu Twierdzenia 4.4), i po wydzieleniu przez tę pierwszą podgrupę jest izomorficzny, a więc bijektywny, z drugim czynnikiem produktu.

Nierówność (2) jest ponownie konsekwencją twierdzenia Lagrange'a: oczywiście mamy $\left[H : \left\langle \left((\sigma_1\sigma_2)^3\right)^m \right\rangle\right] = m \left[H : \left\langle \left((\sigma_1\sigma_2)^3\right) \right\rangle\right]$.

Pozostaje dowód nierówności (1). Zdefiniujmy funkcję

$$f : {}^{H}/_{H \cap K} \to {}^{B_3}/_{K}$$

taką, że $f(a(H \cap K)) = aK$. Funkcja ta jest dobrze określona, ponieważ zachodzi zawieranie $a(H \cap K) \subseteq aK$, oraz warstwy są rozłączne lub sobie równe. Przejdźmy do dowodu, że odwzorowanie f jest injekcją.

Załóżmy, że $aK = f(a(H \cap K)) = f(b(H \cap K)) = bK$, gdzie $a, b \in H$. Wtedy otrzymujemy $b^{-1}a \in K$ oraz, skoro H jest grupą, to także $b^{-1}a \in H$, co w efekcie daje $b^{-1}a \in H \cap K$, a to jest znowu równoważne faktowi, że $a(H \cap K) = b(H \cap K)$. Tak więc zachodzi wynikanie

$$f(a(H \cap K)) = f(b(H \cap K)) \Rightarrow a(H \cap K) = b(H \cap K)$$

i dowód nierówności (1), a za nią całego twierdzenia, jest zakończony. □

W następnych dowodach wykorzystamy następujące klasyczne twierdzenie, którego dowodu nie zdecydujemy się przedstawiać.

Twierdzenie 5.3 (Twierdzenie Nielsena-Schreiera). *Każda podgrupa grupy wolnej jest grupą wolną. Jeśli grupa wolna F jest rangi k, a jej podgrupa G jest skończonego indeksu d w F, to G jest grupą wolną rangi $(k-1)d + 1$.*

Zauważmy, że dla $k = 2$ powyższy wzór przyjmuje postać $d + 1$. Zapowiedzianą we Wprowadzeniu konsekwencją tego twierdzenia jest następujący fakt.

Twierdzenie 5.4. *F_2 jest grupą wirtualnie wolną dowolnej rangi $n \geqslant 2$.*

Dowód. W tej części będziemy oznaczać przez $[n]$ zbiór liczb naturalnych od 0 do n. Grupa F_2 będzie dana prezentacją $\langle a, b \rangle$.

Zdefiniujmy podgrupy H_d grupy F_2, gdzie $d \in \mathbb{N}_{>0}$, następująco:

$$\left\{ a^{j_1} b^{k_1} \cdot \ldots \cdot a^{j_s} b^{k_s} \;\middle|\; k_1, \ldots, k_{s-1}, j_2, \ldots j_s \in \mathbb{Z} \setminus \{0\}, j_1, k_s \in \mathbb{Z}, d \mid \sum_{i=1}^{s} j_i \right\}$$

Łatwo udowodnić, że powyższy zbiór z działaniem dziedziczonym z F_2 faktycznie jest grupą - zbiór jest faktycznie zamknięty na działanie, oraz należą do niego odwrotności jego elementów.

Z definicji widzimy, że dla każdego $h \in H_d$ zachodzi $fhf^{-1} \in H_d$, co równoważnie daje $fH_d = H_d f$ dla każdego $f \in F_2$. Widzimy więc, że jest to dodatkowo podgrupa normalna.

Udowodnijmy teraz, że każda warstwa zbioru ${}^{F_2}\big/_{H_d}$ jest postaci: $a^m H_d$ gdzie $m \in [d-1]$. Weźmy więc dowolną warstwę:

$$\begin{aligned} a^{j_1} b^{k_1} \cdot \ldots \cdot a^{j_s} b^{k_s} H_d &= a^{j_1+\ldots+j_s} a^{-j_1-\ldots-j_s} a^{j_1} b^{k_1} \cdot \ldots \cdot a^{j_s} b^{k_s} H_d \\ &= a^{j_1+\ldots+j_s} H_d = a^{j_1+\ldots+j_s \,(mod\, d)} H_d \end{aligned}$$

Przedostatnia równość wynika z faktu, że słowo $a^{-j_1-\ldots-j_s} a^{j_1} b^{k_1} \cdot \ldots \cdot a^{j_s} b^{k_s}$ należy do grupy H_d, ponieważ suma wykładników przy wyrazach a jest równa 0. Podobnie, ostatnia równość wynika z faktu, że $a^d \in H_d$.

Pozostało udowodnić, że opisane warstwy są różne, czyli $a^{m_1} H_d = a^{m_2} H_d$ daje $m_1 = m_2$. Niech więc zachodzi ta równość zbiorów. Oznacza to, że $a^{m_1 - m_2} \in H_d$. Stąd otrzymujemy $d \mid (m_1 - m_2)$, ale skoro $m_1, m_2 \in [d-1]$, to $|m_1 - m_2| \leqslant d - 1$, a jedyna liczba podzielna przez d w tym przedziale to 0. Stąd $m_1 = m_2$.

Oznacza to, że zbiór ${}^{F_2}\big/_{H_d}$ ma dokładnie d elementów, czyli $[F_2 : H_d] = d$. Twierdzenie Nielsena-Schreiera pozwala nam więc wywnioskować, że grupa H_d jest grupą wolną rangi $d+1$.

Skoro d było dowolną dodatnią liczbą całkowitą, to $d+1$ jest dowolną liczbą całkowitą większą lub równą dwa. Dowód twierdzenia jest więc zakończony. □

Łatwą konsekwencją powyższego jest oczywiście to, że $SL_2(\mathbb{Z})$ jest wirtualnie grupą wolną dowolnej skończonej rangi $\geqslant 2$ (a rozumowanie analogiczne do dowodu Twierdzenia 5.2 pozwala pokazać, że nie jest ona wirtualnie cykliczna). Jednak wieńczącym tę pracę wnioskiem będzie następujący fakt.

Twierdzenie 5.5. *B_3 jest wirtualnie grupą dowolnej skończonej rangi $n \geqslant 2$.*

Dowód. Sama grupa B_3 jest rangi 2, jest więc trywialnie wirtualna rangi 2.

Dla $n \geqslant 3$ warunki tezy będzie spełniać grupa izomorficzna z $\mathbb{Z} \times H_{n-2} \leqslant \mathbb{Z} \times F_2 \simeq \left\langle (\sigma_1\sigma_2)^3, \sigma_1^2, \sigma_2^2 \right\rangle \leqslant B_3$. Skończony indeks tych podgrup w B_3 wynika oczywiście z twierdzenia Lagrange'a.

Dla porządku podajmy jeszcze dowód, że grupy $\mathbb{Z} \times H_{n-2} \simeq \mathbb{Z} \times F_{n-1}$ istotnie mają rangi n. Na pewno $n-1$ generatorów F_{n-1} i jeden generator grupy $\mathbb{Z}$ pozwalają wygenerować tę grupę, więc jej ranga to co najwyżej n. Dodatkowo, wiadomo że dla dowolnej grupy G i jej podgrupy normalnej H zachodzi $\operatorname{rank}(G) \geqslant \operatorname{rank}\left({}^{G}/_{H}\right)$ - wystarczy wziąć warstwy generatorów G. Stąd możemy policzyć

$$\begin{aligned} \operatorname{rank}(\mathbb{Z} \times F_{n-1}) &\geqslant \operatorname{rank}\left({}^{(\mathbb{Z} \times F_{n-1})}\big/_{\langle aba^{-1}b^{-1} \mid a, b \in \mathbb{Z} \times F_{n-1} \rangle}\right) \\ &= \operatorname{rank}\left({}^{(\mathbb{Z} \times F_{n-1})}\big/_{\langle aba^{-1}b^{-1} \mid a, b \in F_{n-1} \rangle}\right) \\ &= \operatorname{rank}\left(\mathbb{Z} \times \left({}^{F_{n-1}}\big/_{\langle aba^{-1}b^{-1} \mid a, b \in F_{n-1} \rangle}\right)\right) \\ &= \operatorname{rank}\left(\mathbb{Z} \times \mathbb{Z}^{n-1}\right) = \operatorname{rank}(\mathbb{Z}^n) = n \end{aligned}$$

Ostatecznie otrzymujemy więc $n \geqslant \operatorname{rank}(\mathbb{Z} \times F_{n-1}) \geqslant n$, czyli $\operatorname{rank}(\mathbb{Z} \times F_{n-1}) = n$. □

Literatura

[1] C. Bagiński, *Wstęp do teorii grup*, Wydawnictwo Script, 2008
[2] Clay Mathematics Institute: Millenium Problems, *Poincaré Conjecture*,
https://www.claymath.org/millennium-problems/poincar%C3%A9-conjecture (24.04.2021)
[3] A. Hatcher, *Algebraic Topology*,
http://pi.math.cornell.edu/ hatcher/AT/AT.pdf, 2002 (24.04.2021)
[4] A. Hatcher, *The Classification of 3-Manifolds - A Brief Overview*,
http://pi.math.cornell.edu/ hatcher/Papers/3Msurvey.pdf, 2004 (24.04.2021)
[5] I. N. Sanov, *A property of a representation of a free group* (w języku rosyjskim),
Doklady Akad. Nauk ZSRR 57, 1947
[6] I. Tuba, H. Wenzl, *Representations of the braid group B3 and of SL(2,Z)*,
Pacific J. Math. 197, 2001
[7] E. Weisstein, *Trefoil Knot*, MathWorld–A Wolfram Web Resource,
https://mathworld.wolfram.com/TrefoilKnot.html (24.04.2021)
[8] Wikipedia, *Nielsen-Schreier theorem*,
https://en.wikipedia.org/wiki/Nielsen-Schreier_theorem (24.04.2021)