

Uniwersytet Warszawski
Wydział Matematyki, Informatyki i Mechaniki

Arkadiusz Męcel

Nr albumu: 234204

Rozkład Bruhat i algebry Hecke

Praca magisterska
na kierunku MATEMATYKA

Praca wykonana pod kierunkiem
prof. Jana Oknińskiego
Instytut Matematyki

Sierpień 2010

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

Celem pracy jest prezentacja podstawowych zagadnień związanych z abstrakcyjnymi odpowiednikami rozkładu Bruhat grupy algebraicznej na warstwy podwójne względem jej podgrup Borela. Zasadniczą motywację stanowi przykład rozkładu grupy macierzy nieosobliwych nad ciałem na warstwy podwójne względem podgrupy macierzy górnotrójkątnych. Obok rozdziału wprowadzającego zasadnicze pojęcia i wyniki niezbędne do prowadzenia dalszych rozważań, cała praca składa się z trzech części. Pierwsza część dotyczy rozkładu Bruhat w teorii grup. Omawiamy podstawowe przykłady oraz prezentujemy zarys pochodzącej od Titsa teorii grup z BN -parą. Druga część dotyczy algebr Hecke. Dowodzimy twierdzenie Titsa o deformacji, pozwalające na ustalenie związku pomiędzy reprezentacjami grupy permutacji zbioru n -elementowego i reprezentacjami grup macierzy odwracalnych nad ciałem skończonym. W trzeciej części omawiamy analog rozkładu Bruhat w przypadku półgrupowym.

Słowa kluczowe

podgrupa Borela, rozkład Bruhat, BN -para, grupa Weyla, algebra Hecke, monoid Rennera

Dziedzina pracy (kody wg programu Socrates-Erasmus)

11.1 Matematyka

Klasyfikacja tematyczna

Według AMS:

- 20-XX Group theory and generalizations
- 20Cxx Representation theory of groups
- 20C08 Hecke algebras and their representations
- 20Exx Structure and classification of infinite or finite groups
- 20E42 Groups with a BN -pair; buildings
- 20Mxx Semigroups
- 20M10 General structure theory
- 20M20 Semigroups of transformations, etc.

Tytuł pracy w języku angielskim

The Bruhat decomposition and Hecke algebras.

Spis treści

1. Niektóre pojęcia i fakty przygotowawcze	7
1.1. Elementy teorii półgrup	8
1.2. Elementy teorii algebr skończone wymiarowych	13
1.3. Elementy teorii reprezentacji grup skończonych	16
1.4. Elementy geometrii algebraicznej	18
2. Rozkład Bruhat	23
2.1. Działanie podgrupy $B_n(\mathbb{K})$ na $Gl_n(\mathbb{K})$	25
2.2. Podgrupy Borela w $Gl_n(\mathbb{K})$	30
2.3. Systemy Titsa	32
2.4. $Gl_n(\mathbb{F}_q)$	35
2.5. Warunek wymiany i prezentacja grupy Weyla	38
3. Algebry Hecke	47
3.1. Generatory i stałe strukturalne w $\mathcal{H}_{\mathbb{C}}(G, B)$	51
3.2. Prezentacja algebry Hecke	54
3.3. Algebry generyczne i ich specjalizacje	58
3.4. $\mathcal{H}_{\mathbb{C}}(G, B) \simeq \mathbb{C}[W]$	65
4. Monoid Rennera	71
4.1. Analog rozkładu Bruhat w $M_n(\mathbb{K})$	73
4.2. Pełen monoid liniowy	74
4.3. Struktura półgrupowa monoidu Rennera	82
Bibliografia	87

Wprowadzenie

W 1954r. F. Bruhat zauważył ([Bru54]), że rozkład klasycznej grupy Liego G (nad ciałem liczb zespolonych) na warstwy podwójne względem jej podgrupy Borela B można ściśle związać z pewną grupą, generowaną przez skończony zbiór symetrii przestrzeni euklidesowej, nazywaną grupą Weyla grupy G . W szczególności pokazał on, że elementy grupy Weyla W , indeksują warstwy tego rozkładu, tj.

$$G = \bigsqcup_{w \in W} BwB.$$

Zjawisko to, choć odkryte w późnym stadium rozwoju klasycznej (nad $\mathbb{R}$ i nad $\mathbb{C}$) teorii grup Liego, odpowiednio zrozumiane i uogólnione, wykorzystane zostało w pracach Chevalleya i Titsa odgrywając kluczową rolę w rodzącej się wówczas teorii grup algebraicznych oraz w znajdującym się wówczas w niemal półwiecznym zastoju problemie klasyfikacji skończonych grup prostych.

Celem pracy jest prezentacja podstawowych zagadnień związanych z abstrakcyjnymi odpowiednikami rozkładu Bruhat. Zasadniczą motywację stanowi przykład rozkładu grupy macierzy nieosobliwych nad ciałem na warstwy podwójne względem podgrupy macierzy górnotrójkątnych. Punktem wyjścia jest klasyczny rozkład Bruhat znany z teorii grup algebraicznych. Uogólnienia, które zaprezentujemy idą natomiast w dwóch zasadniczych kierunkach:

- przejścia z teorii grup algebraicznych do teorii grup abstrakcyjnych,
- przejścia z teorii grup algebraicznych do teorii monoidów algebraicznych.

Obok zagadnienia samego istnienia rozkładu Bruhat omawiamy także jedno z klasycznych jego zastosowań. Mieści się ono w teorii reprezentacji grup skończonych i polega na próbie ustalenia związku pomiędzy grupą G , a odpowiadającą jej grupą Weyla (indeksującą warstwy rozkładu Bruhat grupy G). Wyniki te pochodzą od Titsa i związane są z tzw. algebrami Hecke.

Praca składa się z czterech rozdziałów. W pierwszym rozdziale wprowadzamy zasadnicze pojęcia i wyniki niezbędne do prowadzenia dalszych rozważań. Rozdział drugi dotyczy rozkładu Bruhat w teorii grup. Omawiamy podstawowe przykłady oraz prezentujemy zarys pochodzącej od Titsa teorii grup z BN-parą. Rozdział trzeci dotyczy algebr Hecke. Dowodzimy twierdzenie Titsa o deformacji, pozwalające na ustalenie związku pomiędzy reprezentacjami grupy permutacji zbioru n -elementowego i reprezentacjami grup macierzy odwracalnych nad ciałem skończonym. Rozdział czwarty poświęcony jest analogowi rozkładu Bruhat w przypadku półgrupowym.

Podziękowania

Praca ta mogła powstać głównie dzięki mojemu promotorowi, prof. J. Oknińskiemu, któremu bardzo dziękuję za wprowadzenie mnie w tematykę teorii półgrup oraz w zagadnienie rozkładu Bruhat, za dzielenie się swoim doświadczeniem w tych dziedzinach, a przede wszystkim za pełne wyrozumiałość i cierpliwość nadzorowanie kolejnych etapów powstawania tej pracy. Słowa podziękowania kieruję także w kierunku opiekunów seminarium magisterskiego „Klasyczne struktury algebraiczne”, w ramach którego powstała ta praca: prof. E. Puczyłowskiego oraz prof. J. Matczuka.

Rozdział 1

Niektóre pojęcia i fakty przygotowawcze

Celem tego rozdziału jest przedstawienie podstawowych pojęć i wyników niezbędnych do prowadzenia właściwych, z punktu widzenia całej pracy, rozważań. W kolejnych paragrafach omawiamy:

- w paragrafie 1.1 – elementy teorii półgrup,
- w paragrafie 1.2 – elementy teorii algebr skończenie wymiarowych,
- w paragrafie 1.3 – elementy teorii reprezentacji grup skończonych.
- w paragrafie 1.4 – elementy geometrii algebraicznej.

Rozdział ten ma charakter wprowadzający, brak w nim zatem dowodów zdecydowanej większości cytowanych przez nas twierdzeń. Są to jednak wyniki dobrze znane. Po ich dowody odsyłamy do stosownych monografii. Konstrukcje i wyniki pozostające w obrębie podstaw teorii grup, pierścieni, modułów, przestrzeni liniowych oraz algebr (objęte na MIM UW dwoma semestrami algebry liniowej oraz trzema semestrami algebry) przyjmujemy dalej bez szerszego komentarza za [BiB87].

Poniżej podajemy szereg oznaczeń, które będziemy wykorzystywali w dalszym ciągu pracy bez szerszego komentarza.

- $\mathbb{K}$ – dowolne ciało
- $\mathbb{Q}$ – ciało liczb wymiernych
- $\mathbb{C}$ – ciało liczb zespolonych
- $\mathbb{F}_p$ – ciało skończone o p elementach, p – liczba pierwsza
- $M_n(\mathbb{K})$ – zbiór macierzy wymiaru $n \times n$ nad ciałem $\mathbb{K}$
- $Gl_n(\mathbb{K})$ – grupa macierzy odwracalnych nad $\mathbb{K}$
- $B_n(\mathbb{K})$ – grupa odwracalnych macierzy górnotrójkątnych
- $U_n(\mathbb{K})$ – grupa macierzy unipotentnych górnotrójkątnych
- $T_n(\mathbb{K})$ – grupa odwracalnych macierzy diagonalnych
- S_n – grupa macierzy permutacyjnych

1.1. Elementy teorii półgrup

Celem tego paragrafu jest wprowadzenie podstawowych pojęć i wyników związanych z teorią półgrup. Standardowym odnośnikiem jest monografia Howiego [How76].

Definicja 1.1 (Półgrupa, monoid). Zbiór S z działaniem $\circ : S \times S \rightarrow S$ nazwiemy **półgrupą** jeśli $\circ$ jest łączne. Jeśli istnieje $e \in S$, że dla każdego $s \in S$ zachodzą równości:

$$e \circ s = s \circ e = s,$$

to półgrupę taką nazywamy **monoidem**, e zaś **jedynką** w tym monoidzie.

Definicja 1.2 (Półgrupa z dołączonym zerem lub jedynką). Niech S będzie półgrupą. Bierzemy pewne dwa elementy $\theta, 1 \notin S$ i określamy zbiory:

$$S^1 := S \cup \{1\}, \quad S^0 := S \cup \{\theta\},$$

i rozszerzamy działanie $\circ$ tak, że 1 jest w S^1 jedynką, zaś θ jest w S^0 obustronnym zerem.

Podobnie jak w teorii pierścieni, także w teorii półgrup wprowadzane jest pojęcie ideału.

Definicja 1.3 (Ideał). Niech $\emptyset \neq I \subseteq S$. Zbiór I nazwiemy:

- **ideałem prawostronnym**, piszemy $I <_r S$, jeśli $IS \subseteq I$,
- **ideałem lewostronnym**, piszemy $I <_l S$, jeśli $SI \subseteq I$,
- **ideałem dwustronnym**, piszemy $I \triangleleft S$, jeśli $SI \subseteq S \wedge IS \subseteq S$.

Definicja 1.4 (Ideał główny). Niech $a \in S$. Wówczas zbiór

$$aS^1 := a(S \cup \{1\}) = aS \cup \{a\}$$

nazywamy **ideałem głównym** prawostronnym w S . Analogicznie określamy S^1a – ideał główny lewostronny w S oraz S^1aS^1 – ideał główny dwustronny w S .

Definicja 1.5 (Iloraz Reesa). Niech $I \triangleleft S$. W zbiorze $(S \setminus I) \cup \{\theta\}$ określamy następujące działanie:

$$a \circ b = \begin{cases} ab & , \text{ o ile } ab \notin I, \\ \theta & , \text{ o ile } ab \in I \end{cases} \quad \text{dla } a, b \in S.$$

Co więcej, dla każdego $a \in (S \setminus I) \cup \{\theta\}$

$$a \circ \theta = \theta \circ a = \theta.$$

Wówczas działanie $\circ$ jest łączne na zbiorze $(S \setminus I) \cup \{\theta\}$. Uzyskaną w ten sposób półgrupę oznaczamy przez S/I i nazywamy **ilorazem Reesa** półgrupy S przez ideał $I \triangleleft S$.

O ile w przypadku każdej grupy G zbiór jej podgrup normalnych tworzy kratę izomorficzną z kratą kongruencji na G , o tyle w przypadku półgrup ideały tworzą kratę izomorficzną jedynie z pewną podkratą w $\text{Con}(S)$. Pojęcie **kongruencji** przynależy do algebry uniwersalnej. W przypadku półgrup oznacza ono relację równoważności ρ na S spełniającą warunek:

$$(a, b) \in \rho \Rightarrow \forall_{c \in S} \quad [((ac, bc) \in \rho) \wedge ((ca, cb) \in \rho)].$$

Na zbiorze ilorazowym S/ρ określić można działanie o postaci: $[a] \circ [b] = [ab]$. Wynik działania jest niezależny od wyboru reprezentantów. Uzyskujemy zatem półgrupę ilorazową, oznaczaną przez S/ρ . Jest jasne, że izomorficzna kopia kraty ideałów zawarta jest w kracie kongruencji S . Istotnie, jeśli $I \triangleleft S$, to odpowiada mu kongruencja ρ_I na S postaci:

$$(a, b) \in \rho_I \Leftrightarrow [(a, b \in I) \vee (a = b, a \in S \setminus I)].$$

Łatwo widzieć, że nie każda kongruencja musi być ideałem. Dowolna grupa G jest półgrupą, tymczasem jedyny ideał w G to cała grupa G .

Pojęcie ideału w sposób naturalny prowadzi do konkretnych relacji równoważności związanych z daną podgrupą.

Definicja 1.6 (Relacje Greena). *Niech S będzie półgrupą, $a, b \in S$. Określamy następujące relacje na S :*

$$a\mathcal{L}b \Leftrightarrow S^1a = S^1b \quad (1.1)$$

$$a\mathcal{R}b \Leftrightarrow aS^1 = bS^1 \quad (1.2)$$

$$a\mathcal{J}b \Leftrightarrow S^1aS^1 = S^1bS^1 \quad (1.3)$$

Są to relacje równoważności. Przecięcie $\mathcal{R} \cap \mathcal{L}$ oznaczamy jako $\mathcal{H}$. Sumę, a więc najmniejszą relację równoważności zawierającą $\mathcal{R}$ oraz $\mathcal{L}$, oznaczamy przez $\mathcal{D}$. Jeśli $a \in S$ to symbolami $\mathcal{J}_a, \mathcal{L}_a, \mathcal{R}_a, \mathcal{H}_a, \mathcal{D}_a$ oznaczać będziemy klasy abstrakcji elementu a odpowiednio względem relacji $\mathcal{J}, \mathcal{L}, \mathcal{R}, \mathcal{H}$ oraz $\mathcal{D}$.

Z definicji widać od razu, że skoro $\mathcal{R} \subseteq \mathcal{J}$ oraz $\mathcal{L} \subseteq \mathcal{J}$, to $\mathcal{D} \subseteq \mathcal{J}$. Zawieranie to może być właściwe, przykładem jest następująca półgrupa ([And52]):

$$S = \left\{ \begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix} : a, b \in \mathbb{R}, a, b > 0 \right\} \subseteq Gl_2(\mathbb{R}). \quad (1.4)$$

Wiele kluczowych obserwacji dotyczących półgrup pochodzi z opisu ich $\mathcal{D}$ -klas. Mają one wyjątkowo regularną strukturę. Podstawowym powodem jest przemienność definiujących $\mathcal{D}$ relacji $\mathcal{R}$ i $\mathcal{L}$. Sprawdzenie tego faktu jest czysto rachunkowe. Przypomnijmy, że przez przemienność relacji rozumiemy równość następujących złożań relacji:¹

$$\mathcal{L} \circ \mathcal{R} = \mathcal{R} \circ \mathcal{L}.$$

Zachodzi następujący fakt.

Uwaga 1.7. *Niech $\mathcal{A}, \mathcal{B}$ – relacje równoważności na zbiorze X . Wówczas:*

$$\mathcal{A} \circ \mathcal{B} = \mathcal{B} \circ \mathcal{A} \Rightarrow \mathcal{A} \circ \mathcal{B} = \mathcal{A} \vee \mathcal{B}.$$

Relację $\mathcal{D}$ można więc opisać jako złożenie $\mathcal{R}$ oraz $\mathcal{L}$. Ma ono bardzo regularną strukturę. Każda $\mathcal{D}$ -klasa jest sumą rozłączną pewnej liczby $\mathcal{R}$ -klas oraz pewnej liczby $\mathcal{L}$ -klas. Wiemy już, że:

$$a\mathcal{D}b \Leftrightarrow \exists_{c \in S} (a, c) \in \mathcal{L}, (c, b) \in \mathcal{R} \Leftrightarrow \mathcal{R}_a \cap \mathcal{L}_b \neq \emptyset \Leftrightarrow \mathcal{R}_b \cap \mathcal{L}_a \neq \emptyset.$$

¹Złożenie $\mathcal{A} \circ \mathcal{B}$ relacji równoważności $\mathcal{A}, \mathcal{B}$ na zbiorze X określamy następującym warunkiem:

$$(x, y) \in \mathcal{A} \circ \mathcal{B} \Leftrightarrow \exists_{z \in X} [(x, z) \in \mathcal{A}, (z, y) \in \mathcal{B}].$$

Jest to, co łatwo sprawdzić, również relacja równoważności.

Przecięcie $\mathcal{R}$ -klasy oraz $\mathcal{L}$ -klasy jest więc zawsze albo puste (wtedy klasy te leżą w różnych $\mathcal{D}$ -klasach), albo jest $\mathcal{H}$ -klasą. Clifford i Preston zaproponowali w [Cli61] następujący model obrazujący opisaną przez nas sytuację.

Definicja 1.8 (Egg-box pattern). *Każda $\mathcal{D}$ -klasa w półgrupie S jest postaci „pudełka na jajka”, w którym rzędy reprezentowane są przez $\mathcal{R}$ -klasy, zaś kolumny przez $\mathcal{L}$ -klasy. Każda powstała w ten sposób przegródka jest pojedynczą $\mathcal{H}$ -klasą. Jeśli półgrupa S posiada element zerowy, wówczas tworzy on osobną $\mathcal{D}$ -klasę.*

$\mathcal{H}_x$	$\mathcal{H}_y$						

Jeśli, podobnie jak na rysunku powyżej, element $x \in S$ należy do pewnej przegródki w „pudełku”, wówczas cały wiersz, który go zawiera, równy jest $\mathcal{R}_x$, cała kolumna zaś to $\mathcal{L}_x$. Zgodnie z definicją $\mathcal{R}$, biorąc element $y \in \mathcal{R}_x \setminus \mathcal{H}_x$ znajdziemy elementy r, r' w S^1 , że $xr = y$, oraz $yr' = x$. Niech $\rho_r : S \rightarrow S$ będzie określone wzorem $\rho_r(s) = sr$. Jest to przekształcenie $\mathcal{L}_x$ na $\mathcal{L}_y$. W „pudełku” oznacza to, że ρ_r nie tylko przenosi x na y , ale całą kolumnę z $\mathcal{L}$ -klasą elementu x , na $\mathcal{L}$ -klasę elementu y . Przekształcenie to zachowuje jednocześnie $\mathcal{R}$ -klasy. Można także sprawdzić, że $\rho_{r'} : S \rightarrow S$, określone wzorem $\rho_{r'}(s) = sr'$, przenosi $\mathcal{L}_y$ z powrotem na $\mathcal{L}_x$. Stąd już można pokazać, że $\rho_r|_{\mathcal{L}_x}, \rho_{r'}|_{\mathcal{L}_y}$ są wzajemnie odwrotnymi bijekcjami zachowującymi $\mathcal{R}$ klasy. Analogiczne twierdzenie wysłowić można na temat przekształceń $\mathcal{R}$ -klas (będziemy je oznaczać przez λ), zachowujących $\mathcal{L}$ -klasy. Fakty te znane są jako lematy Greena.

Efekt tych rozważań jest następujący: biorąc dowolne elementy x, y (już niekoniecznie w tej samej $\mathcal{R}$ -klasie) możemy wskazać bijekcję pomiędzy $\mathcal{H}_x$, a $\mathcal{H}_y$. Mechanizm tego faktu łatwo zobaczyć na modelu „pudełka”.

$\mathcal{H}_x$	ρ_s	$\mathcal{H}_c$					
		λ_t					
		$\mathcal{H}_y$					

Istotnie, skoro $x\mathcal{D}y$, to istnieje $c \in S$, że $x\mathcal{R}c$ oraz $c\mathcal{L}y$. Istnieją więc $s, t, s', t' \in S^1$, że:

$$xs = c, \quad cs' = x, \quad tc = y, \quad t'y = c.$$

Wystarczy zatem wziąć najpierw przekształcenie ρ_s , ono przeprowadzi $\mathcal{H}_x$ na $\mathcal{H}_c$ (bijektywnie, bo $\rho_{s'}$ jest odwrotne), a dalej pójść przez λ_t i przeprowadzić $\mathcal{H}_c$ na $\mathcal{H}_y$. Rozumując analogicznie, moglibyśmy najpierw użyć przekształcenia λ_t , a później dopiero przekształcenia ρ_s . Wówczas nie przechodzilibyśmy przez element c , ale przez element należący do $\mathcal{L}_x \cap \mathcal{R}_y$.

Rozważania naszkicowane powyżej pozwalają określić nie tylko własności $\mathcal{D}$ klas, ale także samych $\mathcal{H}$ klas w nich leżących. Zachodzi następujący, prosty fakt.

Uwaga 1.9. *Jeśli $x, y \in S$ oraz $xy \in \mathcal{H}_x$, to $\rho_y|_{\mathcal{H}_x}$ jest bijekcją $\mathcal{H}_x$ na siebie. Jeśli $xy \in \mathcal{H}_y$, to $\lambda_x|_{\mathcal{H}_y}$ jest bijekcją $\mathcal{H}_y$ na siebie.*

Konsekwencją tego faktu jest następujące twierdzenie.

Twierdzenie 1.10 (Green). *Jeśli H jest $\mathcal{H}$ klasą w półgrupie S , to albo $H^2 \cap H = \emptyset$, albo $H^2 = H$ i H jest podgrupą w S .*

Jeśli $\mathcal{H}$ -klasa H półgrupy S jest grupą, wówczas jedynka H jest idempotentem w S . Wynika stąd, że w każdej H klasie S może leżeć co najwyżej jeden idempotent e . Zgodnie z twierdzeniem Greena, jeśli w $\mathcal{H}$ -klasie H znajdziemy idempotent, wówczas H musi być grupą.

Przejdziemy teraz do opisu półgrup składających się z dokładnie jednej nietrywialnej $\mathcal{J}$ -klasy. Termin „nietrywialna” rozumiemy tutaj dwojako. W klasie półgrup nie posiadających elementu zerowego są to takie półgrupy S , które posiadają dokładnie jedną $\mathcal{J}$ -klasę (równą całemu S). W klasie półgrup zawierających element zerowy będą to takie, które posiadają dokładnie dwie $\mathcal{J}$ -klasy: $\{0\}$ oraz $S \setminus \{0\}$. Półgrupy proste i 0-proste, o nich bowiem mowa, zdefiniujemy jednak najpierw w tradycyjny sposób.

Definicja 1.11 (Półgrupa prosta, 0 – prosta). *Półgrupę S nazywamy prostą wtedy i tylko wtedy, gdy S nie jest jednoelementowa i S jest jedynym ideałem w S . Półgrupę S nazwiemy 0 – prostą wtedy i tylko wtedy, gdy S posiada element zerowy, $S^2 \neq 0$ oraz każdy ideał w S równy jest S lub $\{0\}$.*

Każda półgrupa prosta S jest, po przejściu do S^0 półgrupą 0-prostą. Stąd dowody twierdzeń dotyczących półgrup 0-prostych łatwo przenosić na proste. W związku z tym naszą uwagę poświęcimy jedynie półgrupom 0-prostym.

Fakt, że półgrupy 0-proste składają się z jedynie dwóch $\mathcal{J}$ -klas nie wynika wprost z definicji. Jedną z dróg do wykazania tego rezultatu jest sformułowanie twierdzenia strukturalnego Reesa-Suschkewitscha, opisującego strukturę półgrup 0-prostych.

Każdą półgrupę skończoną S można podzielić na segmenty, struktura których będzie łatwa do opisanie. Wprowadzamy w tym celu naturalny porządek na zbiorze ideałów półgrupy S . Minimalne elementy niezerowe w tym porządku nazywać będziemy **ideałami 0-minimalnymi**. Okazuje się, że ideał taki ma albo zerowe mnożenie, albo jest półgrupą 0-prostą. Co więcej, jeśli S nie ma zera, wówczas taki ideał minimalny jest jedyny i nazywamy go **jądrem** $K(S)$ półgrupy S . $K(S)$ jest zatem półgrupą prostą.

Wiemy, że ideał to pewien podzbiór I półgrupy S , a iloraz Reesa to zbiór $(S \setminus I) \cup \{0\}$. Biorąc zatem ideał 0-minimalny I półgrupy skończonej S i biorąc iloraz S/I , wytniemy z S „najmniej” jak to możliwe. Postępując analogicznie można poszukać ideału 0-minimalnego J w ilorazie S/I i uzyskać iloraz $(S/I)/J$, a dalej iloraz ten dzielić przez ideał 0-minimalny itd. W ten sposób wycinalibyśmy ideały 0-minimalne w kolejnych ilorazach. Skoro S jest skończona, cała procedura byłaby skończona. Dostalibyśmy zatem podział S na sumę rozłączną „składników” 0-minimalnych. Aby uzasadnić i sformalizować tę drogę działania potrzeba następującego stwierdzenia:

Uwaga 1.12. *Jeśli I, J są ideałami półgrupy S takimi, że $I \subseteq J$ oraz takimi, że nie istnieje ideał K w S , dla którego $I \subsetneq K \subsetneq J$, to J/I jest albo 0-prosty, albo $(J/I)^2 = 0$ (czyli ma zerowe mnożenie).*

Jeśli w półgrupie S istnieje ideał 0-minimalny I , którego następnikiem² będzie ideał J , to J/I będzie 0-minimalny. W ten sposób biorąc (skończony) łańcuch wstępujący ideałów w S uzyskujemy rozkład S na rozłączne składniki 0-minimalne. Zbiory te można scharakteryzować przy pomocy $\mathcal{J}$ -klas.

Najprostszymi, z punktu widzenia porządku, ideałami w półgrupie są ideały główne postaci

$$J(a) = S^1 a S^1. \quad (1.5)$$

Ideały te są w naturalny sposób związane z $\mathcal{J}$ -klasami w S . Dlatego w zbiorze $S/\mathcal{J}$ wprowadza się następujący porządek:

$$\mathcal{J}_a \leq \mathcal{J}_b \Leftrightarrow J(a) \subseteq J(b). \quad (1.6)$$

Jeśli $\mathcal{J}_a$ jest minimalną niezerową $\mathcal{J}$ -klasą względem takiego porządku w S , to $J(a)$ jest minimalnym ideałem w S . Wówczas, o ile S nie ma elementu zerowego, mamy: $J(a) = \mathcal{J}_a = K(S)$. W przypadku, gdy $\mathcal{J}_a$ nie jest minimalną $\mathcal{J}$ -klasą, wówczas określa się zbiór:

$$I(a) = \{b \in J(a) \mid \mathcal{J}_b < \mathcal{J}_a\}.$$

Jest to zbiór niepusty, więcej – ideał w S . Łatwo sprawdzić, że $J(a) = \mathcal{J}_a \cup I(a)$ jest sumą rozłączną. Łatwo zobaczyć, że jeśli K jest ideałem w S takim, że:

$$I(a) \subseteq K \subseteq J(a),$$

to $K = I(a)$. Z uwagi 1.12 wynika zatem, że $J(a)/I(a)$ jest 0-prosty lub ma zerowe mnożenie. Półgrupy: $K(S)$ oraz $J(a)/I(a)$, $a \in S$ są zatem tymi „najmniejszymi kawałkami”, na które podzielić można półgrupę skończoną S . Nazywamy je **faktorami głównymi** w S . Łatwo widzieć, że faktor główny $J(a)/I(a)$ to nic innego tylko $\mathcal{J}_a$ z dołączonym zerem. Stąd w przypadku każdej półgrupy skończonej 0-prostej istotnie mamy tylko jedną niezerową $\mathcal{J}$ -klasę. Wyraża to jeszcze raz następujący fakt.

Uwaga 1.13. *Jeśli J jest $\mathcal{J}$ -klasą w półgrupie S , to albo J jest jądrem S albo zbiór:*

$$I = \{x \in S \mid \mathcal{J}_x \subseteq J\}$$

jest niepusty i jest ideałem w J . Iloraz J/I jest wówczas 0-prosty lub ma zerowe mnożenie.

²Następnikiem w porządku określonym w zbiorze ideałów przez inkluzję. Zbiór ideałów jest skończony, stąd wiemy, że następnik istnieje.

W 1928 roku Suschkewitsch podał klasyfikację wszystkich skończonych półgrup 0-prostych. Wynik ten rozwinął Rees w 1940r. Okazuje się, że każda skończona półgrupa 0-prosta jest izomorficzna z tzw. **półgrupą typu macierzowego**.

Definicja 1.14 (Półgrupa typu macierzowego). Niech G będzie grupą z jedynką e oraz X, Y – niepustymi zbiorami. Przez P będzie macierzą rozmiaru $|Y| \times |X|$ o wyrazach z $G \cup \{0\} = G^0$, przy czym żaden wiersz ani kolumna P nie jest zerowa. Na zbiorze $S = (G \times X \times Y) \cup \{\theta\}$ określamy następujące działanie:

$$(g_1, x_1, y_1)(g_2, x_2, y_2) = \begin{cases} (g_1 p_{y_1 x_2} g_2, x_1, y_2), & p_{y_1 x_2} \neq 0, \\ 0, & p_{y_1 x_2} = 0 \end{cases}$$

$$(g_1, x_1, y_1)\theta = \theta(g_1, x_1, y_1) = \theta\theta = \theta.$$

Czym jest w istocie zdefiniowany obiekt? Element $a = (g, x_1, y_1) \in S$ utożsamiać można z macierzą rozmiarów $|X| \times |Y|$ o współczynnikach w G^0 . Jedyny niezerowy element tej macierzy znajduje się w wierszu x_1 i kolumnie y_1 i wynosi g . Nietrudno zobaczyć, że iloczyn $c = ab$ dwóch elementów $a, b \in S$ odpowiada, po przejściu do reprezentujących elementy S macierzy $A = (a_{xy}), B = (b_{xy}), C = (c_{xy})$, zwykłemu iloczynowi macierzy postaci $C = A \cdot P \cdot B$. Innymi słowy:

$$(c_{x,y}) = (a_{xy}) \cdot P \cdot (b_{xy}).$$

W ten sposób zdefiniowana struktura jest rzeczywiście półgrupą. Obok terminu „półgrupa typu macierzowego” w literaturze używa się także określenia „**półgrupa Reesa**”. W dalszej części pracy półgrupę tę oznaczać będziemy przez $\mathcal{M}[G^0; X, Y; P]$. Półgrupy typu macierzowe są, jak się okazuje, 0-proste ([How76], Lemma 2.3). Zachodzi też twierdzenie odwrotne:

Twierdzenie 1.15 (Rees, Suschkewitsch [How76], 2.11). Niech S będzie skończoną półgrupą 0-prostą. Wówczas istnieją: grupa skończona G , zbiory skończone X, Y , oraz macierz $P \in M_{|Y| \times |X|}(G^0)$, że $S \simeq \mathcal{M}[G^0; X, Y; P]$.

Powyższe sformułowanie jest słabsze niż to, którego oryginalnie użył Rees. Wynik z 1940r. obejmował nie tylko skończone, ale także pewną klasę nieskończonych półgrup 0-prostych, tzw. całkowicie 0-prostych. W czwartym rozdziale rozważać będziemy przykład nieskończonego monoidu macierzy $M_n(\mathbb{K})$ nad ciałem. Faktory główne tego monoidu będą, w przypadku gdy $|\mathbb{K}| = \infty$, półgrupami 0-prostymi nieskończonymi. Mimo to wykażemy, że ich opis objęty jest ogólniejszą wersją twierdzenia Reesa-Suschkewitscha.

1.2. Elementy teorii algebr skończenie wymiarowych

Przytoczymy podstawowe definicje i fakty związane w teorią algebr skończenie wymiarowych. Do klasycznych źródeł z tej tematyki należy np. monografia Pierce’a [Pie82]. Będziemy się także opierać o pierwsze rozdziały [Cur81].

Zacniemy od ustalenia znaczenia terminu „**pierścień**”. Standardowa definicja mówi o uporządkowanej piątce $(\underline{R}, 0, -, +, \cdot)$, gdzie $(\underline{R}, 0, -, +)$ jest grupą abelową, zaś $(\underline{R}, \cdot)$ jest półgrupą. Struktury te związane są przez aksjomaty obustronnej rozdzielności mnożenia względem dodawania. Zbiór $\underline{R}$ nazywamy **nośnikiem** R . W dalszym ciągu będziemy zakładać, że R jest pierścieniem łącznym z jedynką.

Jeśli R jest pierścieniem z jedyneką 1_R , wówczas grupę abelową M wraz z operacją $\phi : R \times M \rightarrow M$ ($\phi(r, m)$ oznaczamy dalej przez rm) nazywamy **R -modułem** lewostronnym ozn. ${}_R M$ (odpowiednio prawostronnym dla operacji $M \times R \rightarrow M$, ozn. M_R) jeśli dla każdych $r, s \in R$ oraz $v, w \in M$ prawdziwe są następujące równości:

$$\begin{array}{ll} r(v+w) = rv+rw & \text{odp. } (v+w)r = vr+wr \\ (r+s)v = rv+sv & \text{odp. } v(r+s) = vr+vs \\ (rs)v = r(sv) & \text{odp. } v(rs) = (vr)s \\ 1_R v = v & \text{odp. } v 1_R = v \end{array}$$

Niech K będzie pierścieniem przemiennym z 1. Powiemy, że A jest **K -algebrą** jeśli A jest:

1. lewostronnym K -modułem z działaniem dodawania $+$
2. pierścieniem, w którym dodawanie jest tożsame z $+$
3. dla każdych $a_1, a_2 \in A, k \in K$ spełniony jest warunek:

$$k(a_1 a_2) = (k a_1) a_2 = a_1 (k a_2).$$

W przypadku gdy $K = \mathbb{K}$ jest ciałem, wówczas A ma strukturę przestrzeni liniowej nad $\mathbb{K}$. Można wówczas mówić o **wymiarze algebry** A nad $\mathbb{K}$. W dalszym ciągu tego paragrafu zakładamy, że $\mathbb{K}$ jest ciałem algebraicznie domkniętym, zaś wymiar algebry A nad ciałem $\mathbb{K}$ jest skończony. Analogicznie do definicji R -modułu można wprowadzić definicję modułu nad algebrą.

Niech M będzie A -modułem. Mówimy, że jest on **prosty**, jeśli nie zawiera żadnych właściwych³ A -podmodułów. Mówimy, że M jest **półprosty** jeśli spełniony jest jeden z równoważnych warunków:

- (a) dla każdego A -podmodułu N modułu M istnieje A -podmoduł N' , że $M = N \oplus N'$
- (b) moduł M jest sumą prostą A -modułów prostych,
- (c) moduł M jest sumą A -modułów prostych.

Algebrę A nazywamy **półprostą**, jeśli spełniony jest jeden z następujących, równoważnych warunków:

- (a) lewostronny A -moduł ${}_A A$ jest półprosty,
- (b) każdy lewostronny A -moduł jest półprosty,
- (c) prawostronny A -moduł A_A jest półprosty,
- (d) każdy prawostronny A -moduł jest półprosty.

Twierdzenie 1.16 (Wedderburn). *Niech A będzie skończenie wymiarową algebrą nad ciałem algebraicznie domkniętym $\mathbb{K}$. Niech $\omega(A)$ będzie sumą wszystkich ideałów nilpotentnych algebry A . Następujące warunki są równoważne:*

- (a) A jest algebrą półprostą,

³Podmoduł właściwy $N \subset M$ jest różny od 0 oraz od M .

(b) $\omega(A) = 0$,

(c) istnieją liczby naturalne $m, n_1, n_2, \dots, n_m$, oraz algebry z dzieleniem $D_1, D_2, \dots, D_m$ takie, że:

$$A \simeq M_{n_1}(D_1) \oplus M_{n_2}(D_2) \oplus \dots \oplus M_{n_m}(D_m). \quad (1.7)$$

(d) Jeśli M jest prostym A -modułem, to M jest izomorficzna ze składnikiem prostym ${}_A A$.

Z twierdzenia Wedderburna wynika, że jeśli A jest półprosta, wówczas A -moduły proste M, N są izomorficzne wtedy i tylko wtedy, gdy $M' \simeq M$, $N' \simeq N$ oraz $M', N' \subseteq M_{n_i}(D_i)$, gdzie $M_n(D)$ jest jednym ze składników prostych sumy. Ideał $\omega(A)$ nazywa się **radykałem Wedderburna** algebry A . Z punktu (d) twierdzenia Wedderburna wynika, że liczby n_i są wymiarami wszystkich możliwych prostych A -modułów (zarówno prawostronnych, jak i lewostronnych). Zbiór $\{n_1, n_2, \dots, n_m\}$ nazywać będziemy dalej **niezmiennikami numerycznymi** algebry A .

W teorii algebr skończenie wymiarowych ważną rolę odgrywają **elementy idempotentne**, a więc takie $e \in A$, że $e^2 = e$. Jeśli A jest algebrą półprostą i rozważymy rozkład (1.7) algebry A na sumę prostą algebr, tak jak w punkcie (c) twierdzenia Wedderburna, wówczas istnieją takie idempotenty $e_1, e_2, \dots, e_m \in A$, że

$$M_{n_i}(D_i) \simeq e_i A \quad (1.8)$$

oraz $1 = e_1 + e_2 + \dots + e_m$. Elementy e_i mają tę własność, że są:

- **ortogonalne**, tj. $e_i e_j = \begin{cases} 0 & i = j \\ 1 & i \neq j \end{cases}$,
- **centralne**, tj. $e_i a = a e_i$, dla każdego $a \in A$.

W dalszych rozważaniach interesować nas będzie związek pomiędzy algebrą A , a algebrą eAe , gdzie $e \in A$ jest dowolnym elementem idempotentnym. Zachodzi następujące twierdzenie:

Twierdzenie 1.17 ([Cur81], 5.13). *Niech A będzie skończenie wymiarową algebrą nad ciałem $\mathbb{K}$, zaś $\omega(A)$ niech będzie radykałem Wedderburna algebry A . Jeśli $e = e^2 \in A$, wówczas*

$$\omega(eAe) = e\omega(A)e \quad (1.9)$$

W szczególności, jeśli A jest półprosta, wówczas eAe jest półprosta dla każdego $e = e^2 \in A$.

Szczególnymi przykładami algebr są algebry grupowe i półgrupowe.

Definicja 1.18 (Algebra grupowa (półgrupowa)). *Jeśli G jest grupą (półgrupą), zaś $\mathbb{K}$ jest ciałem, wówczas algebrą grupową (półgrupową) $\mathbb{K}[G]$ nazywamy zbiór wszystkich skończonych sum formalnych postaci:*

$$\left\{ \sum_{x \in G} a_x x \mid a_x \in \mathbb{K} \right\},$$

z działaniami dodawania i mnożenia zdefiniowanymi w następujący sposób:

$$\sum a_x x + \sum b_x x = \sum (a_x + b_x) x, \quad \sum a_x x \cdot \sum b_y y = \sum_{x,y} a_x b_y xy.$$

Pierścień $\mathbb{K}[G]$ jest $\mathbb{K}$ -algebrą z naturalnym mnożeniem przez skalary.

W przypadku, gdy G jest monoidem algebra $\mathbb{K}[G]$ ma jedynekę. Dostajemy ją przy naturalnym zanurzeniu $\mathbb{K} \rightarrow \mathbb{K}[G]$. Będziemy ją zwykle utożsamiać z jedyneką grupy G . W przypadku gdy półgrupa G ma zero θ zasadne jest wydzielenie z $\mathbb{K}[G]$ ideału $\mathbb{K}\theta$. Iloraz $\mathbb{K}[G]/\mathbb{K}\theta = \mathbb{K}_0[G]$ nazywamy **ściągniętą algebrą półgrupową**.

Niech G będzie grupą skończoną, zaś $\mathcal{F}_{\mathbb{K}}(G) = \{f \mid f : G \rightarrow \mathbb{K}\}$. Elementowi $x = \sum_{g \in G} a_g g \in \mathbb{K}[G]$ w sposób jednoznaczny odpowiada element $\Phi(x) \in \mathcal{F}_{\mathbb{K}}(G)$, zadany wzorem:

$$\Phi(x)(g) = a_g. \quad (1.10)$$

I odwrotnie, każdej funkcji $f \in \mathcal{F}_{\mathbb{K}}(G)$ odpowiada element $\Psi(f) \in \mathbb{K}[G]$ zadany wzorem:

$$\Psi(f) = \sum_{g \in G} f(g)g. \quad (1.11)$$

Łatwo widzieć, że przyporządkowania $x \rightarrow \Phi(x)$ oraz $f \rightarrow \Psi(f)$ są wzajemnie odwrotnymi bijekcjami zbiorów, tzn. dla każdego $x \in \mathbb{C}[G]$ oraz dla każdej funkcji $f \in \mathcal{F}_{\mathbb{K}}(G)$ zachodzą równości

$$\Psi(\Phi(x)) = x, \quad \Phi(\Psi(f)) = f \quad (1.12)$$

Na zbiorze $\mathcal{F}_{\mathbb{K}}(G)$ można wprowadzić naturalną strukturę $\mathbb{K}$ -algebry izomorficznej z $\mathbb{K}[G]$. Jeśli $f \in \mathcal{F}_{\mathbb{K}}(G)$, wówczas dla $k \in \mathbb{K}$ funkcja $k \cdot f$ określona jest wzorem: $(k \cdot f)(g) = kf(g)$, gdzie lewa strona jest iloczynem dwóch elementów z $\mathbb{K}$. Podobnie jeśli $f, f' \in \mathcal{F}_{\mathbb{K}}(G)$, wówczas dla każdego $g \in G$ wartość funkcji $f + f'$ w punkcie g równa jest $f(g) + f'(g)$. Łatwo widzieć, że zdefiniowaliśmy w ten sposób na $\mathcal{F}_{\mathbb{K}}(G)$ strukturę przestrzeni liniowej izomorficznej z $\mathbb{C}[G]$. Zdefiniowane wyżej przekształcenia Φ, Ψ stają się w ten sposób izomorfizmami przestrzeni liniowych.

Niech $f, f' \in \mathcal{F}_{\mathbb{K}}(G)$. Określamy następującą operację: $\star : \mathcal{F}_{\mathbb{K}}(G) \times \mathcal{F}_{\mathbb{K}}(G) \rightarrow \mathcal{F}_{\mathbb{K}}(G)$:

$$(f \star f')(g) := \sum_{h \in G} f(gh)f'(h^{-1}), \quad g \in G. \quad (1.13)$$

Łatwo sprawdzić, że operacja $\star$ wprowadza na $\mathcal{F}_{\mathbb{K}}(G)$ strukturę $\mathbb{K}$ -algebry. Łatwo także widzieć, że dla $x, y \in \mathbb{C}[G]$ oraz $f, f' \in \mathcal{F}_{\mathbb{K}}(G)$ zachodzą równości:

$$\Phi(xy) = \Phi(x) \star \Phi(y), \quad \Psi(f \star f') = \Phi(f)\Phi(f'). \quad (1.14)$$

Stąd $\mathbb{C}[G] \simeq \mathcal{F}_{\mathbb{K}}(G)$ jest izomorfizmem $\mathbb{K}$ -algebr.

Twierdzenie 1.19 (Maschke). *Jeśli G jest grupą to algebra $\mathbb{K}[G]$ jest półprosta wtedy i tylko wtedy, gdy charakterystyka ciała $\mathbb{K}$ nie dzieli $|G|$.*

1.3. Elementy teorii reprezentacji grup skończonych

Definicja 1.20 (Reprezentacja grupy). *Niech V będzie skończenie wymiarową przestrzenią liniową nad ciałem $\mathbb{K}$, $Gl_{\mathbb{K}}(V)$ niech będzie grupą izomorfizmów liniowych przestrzeni V (izomorficzną z $Gl_n(\mathbb{K})$, dla pewnego $n \in \mathbb{N}$), zaś G niech będzie grupą. Parę (V, ρ) , gdzie $\rho : G \rightarrow Gl_{\mathbb{K}}(V)$ jest homomorfizmem, nazywamy reprezentacją grupy G .*

Także samą przestrzeń V , oraz samo przekształcenie ρ nazywać będziemy reprezentacją G . Reprezentacja ρ określa lewostronne działanie G na V postaci:

$$g \cdot v = \rho_g v = \rho(g)(v).$$

Mamy stąd następujące równości:

$$\begin{aligned} (hg)v &= \rho_{hg} \cdot v = (\rho_h \circ \rho_g)v = h \cdot (g \cdot v), & (h, g \in G, v \in V) \\ g \cdot (v_1 + v_2) &= \rho_g(v_1 + v_2) = \rho_g v_1 + \rho_g v_2 = g \cdot v_1 + g \cdot v_2, & (g \in G, v_1, v_2 \in V) \\ g \cdot (tv) &= \rho_g tv = t\rho_g v = t(g \cdot v), & (g \in G, t \in \mathbb{K}, v \in V) \end{aligned}$$

Jeśli istnieje podprzestrzeń liniowa $W \subseteq V$ taka, że dla każdego $g \in G$ mamy $\rho_g(W) \subseteq W$, wówczas przestrzeń W traktować można jako samodzielną reprezentację traktując ρ jako przekształcenie z G do W . Parę (W, ρ) nazywamy wówczas **podreprezentacją** reprezentacji (V, ρ) .⁴ Jeśli $\rho : G \rightarrow V$ ma tę własność, że V jest jedyną niezerową podreprezentacją V , wówczas (V, ρ) nazywamy **reprezentacją nieprzywiedlną** grupy G .

Niech $\rho_1 : G \rightarrow V$ oraz $\rho_2 : G \rightarrow W$ będą reprezentacjami grupy G . Przekształcenie liniowe $\phi : V \rightarrow W$ nazywamy **równoważnością reprezentacji** grupy G jeśli dla każdego $g \in G$ mamy równość $\rho_1(g) \circ \phi = \phi \circ \rho_2(g)$. Mówimy wtedy, że reprezentacje V, W (jak również ρ_1, ρ_2) są **równoważne**. Łatwo pokazać, że jądro i obraz równoważności reprezentacji są podreprezentacjami grupy G (odpowiednio w V i W).

Twierdzenie 1.21. *Niech $\phi : G \rightarrow Gl_{\mathbb{K}}(V)$ będzie nietrywialną reprezentacją grupy skończonej G , przy czym $\mathbb{K}$ jest ciałem charakterystyki 0. Istnieją wówczas podreprezentacje nieprzywiedlne $U_1, U_2, \dots, U_r \subseteq V$, że:*

$$V = U_1 \oplus \dots \oplus U_r.$$

W rzeczywistości, jeśli dana jest reprezentacja $\rho : G \rightarrow V$, którą można rozłożyć na sumy proste:

$$V = U_1 \oplus \dots \oplus U_r = W_1 \oplus \dots \oplus W_s,$$

wówczas $s = r$, a liczba W_j równoważnych z ustalonym W_k równa jest (z dokładnością do przenumowania) liczbie U_j równoważnych z U_k . Oznacza to w szczególności, że każda grupa skończona ma skończenie wiele reprezentacji nieprzywiedlnych, które z odpowiednimi wielokrotnościami wchodzi do rozkładu dowolnej reprezentacji. Aby sformalizować te obserwacje wprowadzimy pojęcie charakteru. W dalszym ciągu pracować będziemy nad ciałem algebraicznie domkniętym $\mathbb{C}$.

Definicja 1.22. *Niech G będzie grupą skończoną i niech $\rho : G \rightarrow Gl_{\mathbb{K}}(V)$ będzie skończone wymiarową reprezentacją grupy G nad ciałem $\mathbb{C}$. Charakterem elementu g przy tej reprezentacji nazywamy ślad macierzy ρ_g (jest on niezależny od wyboru bazy). **Charakterem reprezentacji** ρ nazywamy funkcję $\chi_\rho : G \rightarrow \mathbb{C}$ określoną wzorem $\chi_\rho(g) = \text{tr} \rho_g$. Charaktery reprezentacji nieprzywiedlnych nazywamy **charakterami nieprzywiedlnymi**.*

Łatwo widzieć, że każda reprezentacja ρ wyznacza na V strukturę lewostronnego $\mathbb{C}[G]$ -modułu. Określamy ją przez liniowe rozszerzenie mnożenia $gv := \rho_g(v)$. Podobnie, każdy lewostronny $\mathbb{C}[G]$ -moduł X wyznacza pewną reprezentację grupy G . Istotnie, każdy $\mathbb{C}[G]$ -moduł ma strukturę przestrzeni liniowej nad $\mathbb{C}$, a reprezentację $\rho_X : G \rightarrow X$ można określić jako: $\rho(g) = gx$. Co więcej, ρ_1, ρ_2 są reprezentacjami równoważnymi wtedy i tylko

⁴Samą podprzestrzeń W , zgodnie z przyjętą konwencją, także nazywamy podreprezentacją V .

wtedy, gdy odpowiadające im $\mathbb{C}[G]$ -moduły są izomorficzne.

Szczególą rolę odgrywa reprezentacja odpowiadająca $\mathbb{C}[G]$ -modułowi $\mathbb{C}[G]$. Nazywamy ją **reprezentacją regularną** $\rho_{reg} : G \rightarrow \mathbb{C}[G]$ grupy G . Wówczas $\rho_{reg}(g)$ jest taką macierzą permutacyjną, że $\rho_{reg}(g)(e_h) = e_{gh}$, dla każdych $g, h \in G$. Łatwo udowodnić, że:

$$\chi_{\rho_{reg}}(g) = \begin{cases} |G| & \text{jeśli } g = e \\ 0 & \text{jeśli } g \neq e \end{cases} \quad (1.15)$$

Każdej reprezentacji, w szczególności reprezentacji nieprzywiedlnej $\rho : G \rightarrow Gl_{\mathbb{K}}(V)$, odpowiada więc z jednej strony pewien $\mathbb{C}[G]$ -moduł M , z drugiej zaś charakter nieprzywiedlny χ_{ρ} . Będziemy czasem mówić, że charakter nieprzywiedlny χ jest wyznaczony przez pewien $\mathbb{C}[G]$ -moduł M . Okazuje się, że M jest prosty. Zachodzi ważne twierdzenie:

Twierdzenie 1.23. *Niech G będzie grupą skończoną, zaś $\chi_1, \chi_2, \dots, \chi_r$ będą różnymi charakterami nieprzywiedlnymi nad $\mathbb{C}$. Wówczas:*

- Każda nieprzywiedlna reprezentacja G występuje w rozkładzie $\mathbb{C}[G]$ na składniki nieprzywiedlne.
- Krotność n_j , z jaką każdy nieprzywiedlny składnik V_j o charakterze χ_j występuje w $\mathbb{C}[G]$ równa jest:

$$n_j = \dim_{\mathbb{C}} V_j = \chi_j(1_G).$$

Zgodnie z twierdzeniem Maschke algebra $\mathbb{C}[G]$ jest półprosta, zatem każdy prosty $\mathbb{C}[G]$ -moduł jest w pewnej składowej jednorodnej (będącej sumą prostą izomorficznych modułów prostych o krotności równej n_j) A_i tak, że $\mathbb{C}[G]$ jest jako moduł równy $A_1 \oplus \dots \oplus A_r$. Co więcej, dla każdego $1 \leq i \leq r$ istnieje idempotent e_i , że $A_i \simeq e_i \mathbb{C}[G] \simeq \mathbb{C}[G] e_i$. Łatwo widzieć, że $e_i A_j = \delta_{ij} A_j$. Stąd powiemy, że charakterowi nieprzywiedlnemu χ odpowiada centralny idempotent $e \in \mathbb{C}[G]$, jeśli moduł prosty M odpowiadający χ leży w eA .⁵ Dany jest on wzorem ([Cur81], 9.21):

$$e = \chi_j(1) |G|^{-1} \sum_{x \in G} \chi_j(x^{-1}) x. \quad (1.16)$$

1.4. Elementy geometrii algebraicznej

Niech $\mathbb{K}$ będzie ciałem algebraicznie domkniętym. Punkty n – wymiarowej przestrzeni afinicznej $A_{\mathbb{K}}^n$ identyfikujemy z:

$$\{(a_1, a_2, \dots, a_n) \mid a_i \in \mathbb{K}\}.$$

Niech I będzie ideałem pierścienia wielomianów $\mathbb{K}[x_1, x_2, \dots, x_n]$. Przyjmujemy następującą definicję:

$$\mathcal{V}(I) := \{a = (a_1, a_2, \dots, a_n) \in \mathbb{K}^n \mid f(a) = 0, \text{ dla wszystkich } f \in I\}.$$

Każdy zbiór zdefiniowany w powyższy sposób nazywać będziemy **zbiorem algebraicznym**⁶ Każdy zbiór algebraiczny można opisać przy pomocy skończenie wielu równań postaci $f_i = 0$, $1 \leq i \leq n$, gdzie n jest pewną liczbą naturalną, zaś $f_i \in \mathbb{K}[x_1, x_2, \dots, x_n]$. Mówi o tym poniższe twierdzenie.

⁵Idempotent e ma własność opisaną w (1.8), a więc wydziela z $\mathbb{C}[G]$ jeden z bloków prostych.

⁶Dokładniej, zdefiniowane obiekty nazywane są zbiorami algebraicznymi afinicznymi. Pojęcie zbioru algebraicznego przynależy w geometrii algebraicznej obiektom, które „lokalnie” mają strukturę zbiorów afinicznych. W dalszym ciągu pracy pisząc „zbiór algebraiczny” będziemy mieli zawsze na myśli zbiór algebraiczny afiniczny.

Twierdzenie 1.24 (Hilberta o bazie). *Niech $R[x_1, x_2, \dots, x_n]$ będzie pierścieniem wielomianów o współczynnikach z pierścienia R . Jeżeli każdy ideał $I < R$ jest skończenie generowany, to także każdy ideał $J < R[x_1, x_2, \dots, x_n]$ jest skończenie generowany.*

Rozważmy rodzinę $\mathcal{A}$ wszystkich zbiorów algebraicznych zawartych w $A_{\mathbb{K}}^n$. Widzimy, że zbiór pusty oraz cała przestrzeń $A_{\mathbb{K}}^n$ należą do $\mathcal{A}$. Rodzina ta jest ponadto zamknięta zarówno ze względu na operację przecięcia dowolnej liczby zbiorów, jak i ze względu na operację sumy skończonej liczby zbiorów. Widać stąd, że w $A_{\mathbb{K}}^n$ możliwe jest wprowadzenie topologii. Zbiorami domkniętymi są w tej topologii elementy rodziny $\mathcal{A}$. Bazę zaś stanowi rodzina zbiorów postaci:

$$V_f = \{x \in A_n(\mathbb{K}) \mid f(x) \neq 0\}, \quad f \in \mathbb{K}[x_1, x_2, \dots, x_n].$$

Topologię określoną wyżej nazywamy **topologią Zariskiego** na przestrzeni $A_{\mathbb{K}}^n$. Jeśli $X \subseteq A_{\mathbb{K}}^n$ jest dowolnym zbiorem algebraicznym, wówczas topologia Zariskiego na X jest dziedziczona z topologii Zariskiego na $A_{\mathbb{K}}^n$.

Dla zbioru algebraicznego X określić można podzbiór $\mathbb{K}[x_1, x_2, \dots, x_n]$ postaci:

$$\mathcal{I}(X) := \{f \in \mathbb{K}[x_1, x_2, \dots, x_n] \mid f(x) = 0, \text{ dla wszystkich } x \in X\}.$$

Twierdzenie 1.25 (Hilberta o zerach). *Niech $I \triangleleft \mathbb{K}[x_1, x_2, \dots, x_n]$. Wówczas*

$$I = \mathcal{I}(\mathcal{V}(I)) \Leftrightarrow I = \sqrt{I}, \quad \text{gdzie } \sqrt{I} = \{f \in \mathbb{K}[x_1, x_2, \dots, x_n] \mid \exists m \in \mathbb{N}_+ (f^m \in I)\}.$$

Ważnym wnioskiem z twierdzenia o zerach jest istnienie jednoznacznej odpowiedniości pomiędzy zbiorami algebraicznymi $\mathcal{V}(I)$ w $A_{\mathbb{K}}^n$, a **ideałami radykalnymi** w $\mathbb{K}[x_1, x_2, \dots, x_n]$ tj. takimi ideałami $I \in \mathbb{K}[x_1, x_2, \dots, x_n]$, dla których $I = \sqrt{I}$. Bijeckja ta odwraca inkluzję, tzn. $I \subseteq J \Leftrightarrow \mathcal{V}(I) \supseteq \mathcal{V}(J)$.

Z twierdzeń Hilberta wynika także obserwacja, że każdy zbiór algebraiczny X można rozłożyć na skończoną sumę $X = X_1 \cup X_2 \cup \dots \cup X_s$, gdzie $X_i = \mathcal{V}(P_i)$, przy czym P_i są ideałami pierwszymi. Składniki $\mathcal{V}(P_i)$, nazywane **rozmaitościami algebraicznymi**, mają ważną topologiczną własność – są **nierozkładalne**. Oznacza to, że $\mathcal{V}(P_i)$ nie można przedstawić jako sumy dwóch różnych właściwych podzbiorów domkniętych w topologii Zariskiego (w przeciwieństwie do spójności nie zakładamy, że są to podzbiory rozłączne). Własność ta charakteryzuje rozmaitości.

Definicja 1.26. *Niech $X \subseteq A_{\mathbb{K}}^n$ będzie zbiorem algebraicznym. **Pierścieniem funkcji regularnych** X , oznaczanym dalej symbolem⁷ $\mathbb{K}[X]$, nazywamy iloraz*

$$\mathbb{K}[x_1, x_2, \dots, x_n] / \mathcal{I}(X).$$

Morfizmem zbioru algebraicznego $V \subseteq A_{\mathbb{K}}^n$ do przestrzeni $A_{\mathbb{K}}^m$ nazywamy funkcję $\phi : V \rightarrow A_{\mathbb{K}}^m$, która każdemu $x \in V$ przyporządkowuje $(f_1(x), f_2(x), \dots, f_m(x))$, gdzie $f_i \in \mathbb{K}[V]$. Jeśli dla wszystkich $x \in X$ obraz $\phi(x)$ należy do pewnej rozmaitości algebraicznej $Y \subseteq A_{\mathbb{K}}^m$, to ϕ nazywamy morfizmem z rozmaitości X do Y . Jest to przekształcenie ciągłe w topologii Zariskiego.

⁷Występuje tu konflikt oznaczeń z definicją 1.18. Nie powinno to jednak prowadzić do jakichkolwiek nieporozumień.

Przez wymiar rozmaitości algebraicznej X określamy wymiar X rozumianej jako przestrzeni topologicznej⁸. **Wymiar** dowolnego **zbioru algebraicznego** określa się jako supremum z wymiarów jego składowych nierozkładalnych.

W dalszej części rozważań wykorzystamy standardowy (choć nietrywialny) wynik związany z teorią wymiaru zbiorów algebraicznych.

Twierdzenie 1.27. *Niech X będzie rozmaitością algebraiczną, zaś Y niech będzie właściwym, domkniętym i nieredukowalnym podzbiorem X . Wówczas $\dim(Y) < \dim(X)$.*

Twierdzenie to mówi, nieprecyzyjnie rzecz biorąc, że jeśli jeden zbiór algebraiczny zawiera się w drugim, to do opisania mniejszego potrzeba mniej równań, niż do opisania większego. Dowód tw. 1.27 stosunkowo łatwo wynika⁹ z następującej obserwacji:

Uwaga 1.28. *Niech $W \subseteq V$ będą rozmaitościami algebraicznymi. Wówczas $\mathbb{K}[W] = \mathbb{K}[V]/P$, gdzie P jest pewnym ideałem pierwszym w $\mathbb{K}[V]$.*

Na podstawie twierdzeń Hilberta: o zerach i o bazie wiadomo, że $X \subset A^n$ jest rozmaitością wtedy i tylko wtedy, gdy $\mathbb{K}[X] = A_{\mathbb{K}}^n/P$, gdzie $P \triangleleft \mathbb{K}[x_1, x_2, \dots, x_n]$ jest ideałem pierwszym. Nie ma jednak, a priori, żadnego powodu, by podobna odpowiedniość przenosiła się z $A_{\mathbb{K}}^n$ na dowolną rozmaitość algebraiczną. To właśnie stw. 1.28 jest zasadniczą trudnością w dowodzie tw. 1.27. Dowód stw. 1.28 bazuje na ściśle algebraicznych rozważaniach. Polega on na utożsamieniu wymiaru zbioru algebraicznego V z pewnym niezmiennikiem pierścienia funkcji regularnych $\mathbb{K}[V]$. Ze względu na zasadnicze znaczenie tw. 1.27 dla dalszych rozważań, omówimy teraz krótko naturę tego utożsamienia.

Niech P będzie ideałem pierwszym pierścienia przemiennej R . Przez wysokość P , ozn. $h(P)$, rozumiemy supremum (o ile istnieje) po takich $n \in \mathbb{N}$, że:

$$P_0 \subsetneq P_1 \subsetneq \dots \subsetneq P_n = P,$$

gdzie P_i są ideałami pierwszymi w R . Niech I będzie dowolnym ideałem w R . Oznaczmy przez $\mathcal{P}(I)$ rodzinę ideałów pierwszych pierścienia R zawartych w ideale I . Jeśli istnieje $\sup\{h(P) \mid P \in \mathcal{P}(I)\}$, wówczas liczbę tę nazywamy **wysokością ideału I** i oznaczamy ją symbolem $h(I)$. Wreszcie, jeśli istnieje $n = \sup\{h(P) \mid P \in \mathcal{P}(R)\}$ z wysokości wszystkich ideałów pierwszych pierścienia R wówczas mówimy, że R ma **wymiar Krulla** równy n . Można udowodnić, że wymiar zbioru algebraicznego V równy jest wymiarowi Krulla pierścienia $\mathbb{K}[V]$. Uwaga 1.28 w łatwy sposób wynika z następującego wyniku Krulla

Twierdzenie 1.29 (Krull). *Niech R będzie pierścieniem noetherowskim. Niech $f \in R$ będzie elementem nieodwracalnym, który nie jest dzielnikiem zera. Wówczas każdy minimalny ideał pierwszy R , który jest zawarty w ideale (f) generowanym przez element f ma wysokość 1.*

Dowód można znaleźć np. w [Ati69] (Coll. 11.17).

Pierścienie funkcji regularnych rozmaitości algebraicznych nad ciałem algebraiczne domkniętym są skończenie generowanymi pierścieniami noetherowskimi. W szczególności, można do

⁸Wymiar topologiczny to supremum ze wszystkich liczb naturalnych n takich, że istnieje łańcuch

$$X_0 \subsetneq X_1 \subsetneq \dots \subsetneq X_n$$

nierozkładalnych podzbiorów domkniętych X .

⁹Patrz [Hum75], 3.2.

nich stosować tw. Krulla.

W dalszej części tego paragrafu interesować nas będzie możliwość wprowadzenia struktury grupowej (półgrupowej) na zbiorze algebraicznym. Odnotujmy zatem następującą uwagę ([Hum75], 2.4).

Uwaga 1.30. *Jeśli $V \subseteq A_{\mathbb{K}}^n$ oraz $W \subseteq A_{\mathbb{K}}^m$ są algebraiczne, to także $V \times W \subseteq A_{\mathbb{K}}^{m+n}$ jest zbiorem algebraicznym. Odpowiadającym mu pierścieniem funkcji regularnych jest $\mathbb{K}[V] \otimes_{\mathbb{K}} \mathbb{K}[W]$.*

Obserwacja ta pozwala rozważać morfizmy postaci $V \times V \rightarrow V$. W szczególności, jeżeli zbiór V posiada strukturę półgrupy lub grupy abstrakcyjnej, wtedy możemy pytać o „zgodność” tej struktury ze strukturą zbioru algebraicznego. Rozważymy teraz dwa zasadnicze przykłady takiej sytuacji.

Przykład 1.31. Pełen monoid liniowy.

Rozważmy zbiór macierzy $M_n(\mathbb{K})$ rozumiany jako zbiór algebraiczny izomorficzny z $A_{\mathbb{K}}^{n^2}$. Pierścień funkcji regularnych tego zbioru utożsamiamy z pierścieniem wielomianów n^2 zmiennych postaci $\mathbb{K}[x_{ij}]$, $1 \leq i, j \leq n$. Niech $\phi : M_n(\mathbb{K}) \times M_n(\mathbb{K}) \rightarrow M_n(\mathbb{K})$ będzie zwykłym mnożeniem macierzowym, a więc jeśli $A = (a_{ij})$, $B = (b_{ij})$ oraz $C = \phi(A, B) = (c_{ij})$ wtedy $c_{ij} = \sum_{l=1}^n a_{il}b_{lj}$. Nietrudno widzieć, że ϕ jest zatem morfizmem zbiorów algebraicznych. Struktury: półgrupowa i algebraiczna są w przypadku $M_n(\mathbb{K})$ zgodne, tj. mnożenie półgrupowe jest morfizmem zbiorów algebraicznych. Trójkę $(M_n(\mathbb{K}), \phi, Id)$ nazywamy pełnym liniowym monoidem algebraicznym.

Przykład 1.32. Pełna grupa liniowa

Rozważmy grupę $Gl_n(\mathbb{K})$. Ma ona strukturę zbioru algebraicznego. Dowód polega na zauważeniu, że wyznacznik należy do pierścienia funkcji regularnych w $M_n(\mathbb{K})$ (jest funkcją wielomianową). Wówczas $Gl_n(\mathbb{K})$ utożsamić można ze zbiorem rozwiązań równania $\det(A)y = 1$ rozważanego w $M_n(\mathbb{K}) \times A_{\mathbb{K}}^1$. Pierścień $\mathbb{K}[Gl_n(\mathbb{K})]$ funkcji regularnych na $Gl_n(\mathbb{K})$ generowany jest przez obcięcie n^2 funkcji regularnych x_{ij} , generujących $\mathbb{K}[M_n(\mathbb{K})]$ (patrz przykład 1.31), oraz przez funkcję $(\det)^{-1}$. Można pokazać, że funkcje $\phi : Gl_n(\mathbb{K}) \times Gl_n(\mathbb{K}) \rightarrow Gl_n(\mathbb{K})$ oraz $^{-1} : Gl_n(\mathbb{K}) \rightarrow Gl_n(\mathbb{K})$ określające odpowiednio: mnożenie i odwracanie elementów $Gl_n(\mathbb{K})$ są morfizmami zbiorów algebraicznych. W szczególności struktury: grupowa i algebraiczna są, w przypadku $Gl_n(\mathbb{K})$, zgodne.

Przykłady te są motywacją dla następującej definicji:

Definicja 1.33. *Niech $(Gl_n(\mathbb{K}), \phi, ^{-1}, Id)$ będzie pełną grupą liniową nad ciałem $\mathbb{K}$. Niech G będzie taką podgrupą grupy $Gl_n(\mathbb{K})$, która jest domknięta jako podzbiór algebraiczny w $Gl_n(\mathbb{K})$. Wówczas każdą grupę G' izomorficzną z G nazywamy **liniową grupą algebraiczną**.*

W dalszym ciągu zdefiniowane obiekty nazywać będziemy „grupami algebraicznymi”. Jest to pewne nadużycie terminologii. W geometrii algebraicznej rozważa się bardziej abstrakcyjną definicję grupy algebraicznej niż 1.33, patrz. [Hum75], (7.1). Ze względu jednak na to, że w pracy tej zajmujemy się wyłącznie liniowymi grupami algebraicznymi, pojęcie „grupy algebraicznej” nie powinno prowadzić do żadnych nieporozumień.

Mówimy, że grupa algebraiczna jest **spójna** lub **nierozkładalna**, jeśli jest spójna lub nierozkładalna jako zbiór algebraiczny. Można pokazać, że jeśli grupa algebraiczna G jest, jako zbiór algebraiczny, nierozkładalna, wtedy musi być także spójna. Co więcej, składowe spójne dowolnej grupy algebraicznej G są nierozkładalne jako rozmaitości algebraiczne. Jest ich zatem skończenie wiele. Składowa spójna G' jedynki grupy G jest podgrupą w G . Składowe spójne grupy G są, jak się okazuje, warstwami G względem podgrupy izomorficznej z G' .

Sformułujemy teraz szczególny przypadek klasycznego rezultatu teorii reprezentacji grup algebraicznych, twierdzenie Lie-Kolchina, charakteryzujący spójne grupy rozwiązalne. Przypomnijmy najpierw definicję grupy rozwiązalnej.

Definicja 1.34. *Niech G będzie grupą. Powiemy, że G jest **rozwiązalna** gdy istnieje ciąg podgrup*

$$\{1\} = H_0 \leq H_1 \leq H_2 \leq \dots \leq H_{k-1} \leq H_k = G,$$

że dla każdego $1 \leq i \leq k$ spełnione są następujące warunki:

1. $H_{i-1} \triangleleft H_i$
2. H_i/H_{i-1} jest grupą abelową.

Twierdzenie 1.35 (Lie-Kolchin). *Każda domknięta spójna i rozwiązalna podgrupa $Gl_n(\mathbb{K})$ jest sprzężona z pewną podgrupą $B_n(\mathbb{K})$.*

Dowód można znaleźć w [Gec03], 3.1.7. lub w [Hum75], 17.6.¹⁰

Definicja 1.36. *Podgrupą Borela grupy afinicznej G nazwiemy element maksymalny w zbiorze tych podgrup w G , które są domknięte, spójne i rozwiązalne.*

Przez stwierdzenie 'element maksymalny' rozumiemy tutaj element maksymalny w zbiorze uporządkowanym częściowo przez relację inkluzji. Dla każdej grupy algebraicznej G pojęcie to jest dobrze określone. Na mocy tw. 1.27 nie jest możliwe, by istniał nieskończony łańcuch wstępujący spójnych i domkniętych podgrup grupy algebraicznej $G \subset A_{\mathbb{K}}^n$. Cała przestrzeń afiniczna $A_{\mathbb{K}}^n$ jest bowiem wymiaru n .¹¹

Podgrupy Borela B grupy algebraicznej G będą obiektem naszego szczególnego zainteresowania. W pewnych ściśle określonych przypadkach warstwy podwójne grupy algebraicznej G względem podgrupy Borela B indeksowane będą elementami pewnej grupy związanej z G . Odnotujmy w tym miejscu jeden istotny fakt związany z podaną wyżej definicją podgrupy Borela.

Twierdzenie 1.37 (Borel). *Niech B i B' będą dwiema podgrupami Borela grupy algebraicznej G . Wówczas istnieje $g \in G$ takie, że $gBg^{-1} = B'$.*

Dowód tego twierdzenia, jak i szczegółowe wprowadzenie do teorii podgrup Borela (z punktu widzenia zastosowań w geometrii algebraicznej), znaleźć można na przykład w [Gec03] (rozdział trzeci).

¹⁰Twierdzenie 1.35 jest w istocie szczególnym przypadkiem tw. Lie-Kolchina. Obydwa źródła zawierają ogólniejsze jego sformułowania.

¹¹Krótki dowód tego faktu znaleźć można na przykład w [Lom04].

Rozdział 2

Rozkład Bruhat

Niech G będzie grupą i $H \leq G$. Wówczas można określić działanie iloczynu $H \times H$ na G :

$$(h_1, h_2)g = h_1gh_2^{-1}, \quad h_1, h_2 \in H, g \in G. \quad (2.1)$$

Działanie to prowadzi do **rozkładu grupy na warstwy podwójne** postaci:

$$G = \bigsqcup_{x \in X} HxH,$$

gdzie X jest pewnym zbiorem. W rozdziale tym interesować nas będą sytuacje, gdy na X wprowadzić można strukturę algebraiczną związaną ze strukturą grupy G . Zasadniczą motywację stanowi następujący rezultat.

Twierdzenie 2.1. *Dla dowolnego ciała $\mathbb{K}$ ma miejsce następujący rozkład grupy $Gl_n(\mathbb{K})$:*

$$Gl_n(\mathbb{K}) = \bigsqcup_{\sigma \in S_n} B_n(\mathbb{K})\sigma B_n(\mathbb{K}), \quad (2.2)$$

gdzie S_n jest grupą macierzy permutacyjnych.

Dowód tego faktu przedstawimy w paragrafie 2.1. Rozkłady podobne do (2.2) nazywać będziemy rozkładami Bruhat. Nazwa pochodzi od nazwiska francuskiego matematyka François Bruhat (1929–2007). Zajmował się on teorią reprezentacji grup i algebr Liego oraz teorią grup algebraicznych. Jednym z jego wczesnych wyników był następujący rezultat.

Twierdzenie 2.2 (Bruhat, [Bru54]). *Rozważmy następujące serie prostych grup Liego¹:*

$$\begin{aligned} A &= \{A_n \mid A_n = Sl_{n+1}(\mathbb{C}) \quad , n = 1, 2, 3, \dots\} \\ B &= \{B_n \mid B_n = SO_{2n+1}(\mathbb{C}) \quad , n = 2, 3, 4, \dots\} \\ C &= \{C_n \mid C_n = Sp_{2n}(\mathbb{C}) \quad , n = 2, 3, 4, \dots\} \\ D &= \{D_n \mid D_n = SO_{2n}(\mathbb{C}) \quad , n = 4, 5, 6, \dots\} \end{aligned}$$

Wówczas jeśli $G \in A \cup B \cup C \cup D$ jest podgrupą $Gl_m(\mathbb{K})$ oraz $B = G \cap B_m(\mathbb{C})$, $T = G \cap T_m(\mathbb{C})$, to oznaczając przez $N(T)$ normalizator grupy T w G , a przez W – iloraz $N(T)/T$, dostajemy rozkład G na warstwy podwójne $\{BwB \mid w \in W\}$ ² postaci

$$G = \bigsqcup_{w \in W} BwB. \quad (2.3)$$

¹Przypomnijmy, że grupa Liego nad ciałem $\mathbb{C}$, to zbiór mający zgodne struktury grupy i rozmaitości różniczkowej nad $\mathbb{C}$. Zgodność polega na tym, że mnożenie i odwracanie są różniczkowalne klasy C^∞ . Prosta grupa Liego to taka spójna grupa Liego, która nie posiada nietrywialnych spójnych dzielników normalnych.

²Jest to pewne nadużycie oznaczeń. Zauważmy jednak, że jeśli $n_1, n_2 \in N(T)$ oraz $n_1n_2^{-1} \in T$, to $Bn_1B = Bn_2B$. Wynika to z faktu, że w przypadku każdej z tych grup $T = B \cap N(T) \triangleleft N(T)$.

W twierdzeniu Bruhat grupą indeksującą warstwy podwójne G względem B jest grupa $N(T)/T$. Obiekt ten, zwany **grupą Weyla** grupy Liego G pojawił się po raz pierwszy w rozważaniach Weyla z połowy lat 20. XX wieku, kiedy to udowodnione zostało przezeń następujące twierdzenie:

Twierdzenie 2.3 (Weyl (1926), [Wey56]). *Każda skończona wymiarowa prosta algebra Liego $\mathfrak{g}$ nad $\mathbb{C}$ jest, z dokładnością do izomorfizmu, wyznaczona przez pewną skończoną grupę W permutacji jednowymiarowych podprzestrzeni algebry Liego $\mathfrak{g}$. Grupa W jest izomorficzna z grupą skończoną generowaną przez symetrie przestrzeni euklidesowej E^n .*

Publikacje Bruhat zwróciły uwagę Chevalleya, który zastosował rozkład Bruhat do poszukiwania skończonych grup prostych.³ W szczególności, pokazał on ([Che55], [Che58]), że jeśli $\mathbb{K}$ jest ciałem różnym od $\mathbb{F}_2, \mathbb{F}_3$, to z każdą prostą algebrą Liego nad $\mathbb{K}$ związać można grupę prostą G . W zależności od ciała Chevalley uzyskał w ten sposób:

- dla $\mathbb{K} = \mathbb{C}$ – wszystkie proste grupy Liego nad $\mathbb{C}$,
- dla $\mathbb{K} = \overline{\mathbb{K}}$ – wszystkie proste grupy algebraiczne nad $\mathbb{K}$,
- dla $|\mathbb{K}| < \infty$ – wszystkie znane wówczas skończone grupy proste nieabelowe, a także nieznanne wcześniej serie skończonych grup prostych

Uogólnienie związane było z jednej strony z samą techniką dowodu, który, w przeciwieństwie do oryginalnego dowodu Bruhat, jednym ciągiem rozumowań obejmował wszystkie serie prostych grup Liego i nie tylko te grupy; z drugiej zaś strony wynik Chevalleya dotyczył grup Liego nad dowolnym ciałem różnym od $\mathbb{F}_2, \mathbb{F}_3$. W szczególności, Chevalley skonstruował nieznanne dotąd przykłady skończonych grup prostych ([Che55]), otwierając tym samym nowy rozdział w historii problemu ich klasyfikacji. Wyniki Chevalleya dały przykłady rozkładów Bruhat poza teorią grup Liego. Dalsze uogólnienia, pozwalające na rozważanie rozkładu Bruhat w przypadku grup abstrakcyjnych (i pozwalające na dalsze postępy w problemie klasyfikacji skończonych grup prostych), pochodzą z początku lat 60' z prac Titsa, o których powiemy dalej.

W kolejnych paragrafach tego rozdziału przedstawimy:

- w paragrafie 2.1 – dowód twierdzenia 2.1;
- w paragrafie 2.2 – omówienie, na podstawie grupy $GL_n(\mathbb{K})$, podstawowych pojęć potrzebnych do rozważania rozkładu Bruhat w klasie grup algebraicznych,
- w paragrafie 2.3 – systemy Titsa, a więc grupy skończone związane czterema aksjomatami zapewniającymi istnienie analogu rozkładu Bruhat;
- w paragrafie 2.4 – dowód faktu, że $GL_n(\mathbb{K})$ jest systemem Titsa z BN-parą⁴ $(B_n(\mathbb{K}), N_n(\mathbb{K}))$, gdzie $N_n(\mathbb{K})$ jest normalizatorem $T_n(\mathbb{K})$ w $GL_n(\mathbb{K})$ ⁵;
- w paragrafie 2.5 – opis abstrakcyjnego odpowiednika grupy Weyla (określonego w paragrafie 2.3) przy pomocy generatorów i relacji.

³Na podstawie [Cur67] oraz [Abr89] (str. 335-336).

⁴Stosowne definicje pojawiają się w paragrafie 2.3.

⁵A więc grupą macierzy mających dokładnie jeden element niezerowy w każdym wierszu i w każdej kolumnie.

2.1. Działanie podgrupy $B_n(\mathbb{K})$ na $Gl_n(\mathbb{K})$

Celem tego paragrafu jest dowód twierdzenia 2.1. Składa się on z dwóch części:

Lemat 2.4. *Niech $A \in Gl_n(\mathbb{K})$. Wówczas istnieje $P \in S_n$ oraz $L, M \in B_n(\mathbb{K})$, że:*

$$A = LPM.$$

Lemat 2.5. *Niech $\sigma_1, \sigma_2 \in S_n$. Wówczas:*

$$B_n(\mathbb{K})\sigma_1 B_n(\mathbb{K}) = B_n(\mathbb{K})\sigma_2 B_n(\mathbb{K}) \Rightarrow \sigma_1 = \sigma_2$$

Zanim przystąpimy do dowodu wprowadzimy pewne dodatkowe oznaczenia. Jeśli $A \in M_n(\mathbb{K})$, to i -ty wiersz macierzy A oznaczать będziemy przez $w_i(A)$, natomiast j -tą kolumnę macierzy A oznaczать będziemy przez $k_j(A)$. Symbolem e_k oznaczать będziemy k -ty wektor bazy standardowej $\mathbb{K}^n$.

Ustalmy $n \in \mathbb{N}$. Dla każdego $1 \leq t \leq n$ rozważać będziemy funkcje:

$$\begin{aligned} l_t : Gl_n(\mathbb{K}) &\rightarrow \{1, 2, \dots, n\} \\ q_t : Gl_n(\mathbb{K}) &\rightarrow M_n(\mathbb{K}) \end{aligned}$$

Założmy, że $A = (a_{ij}), 1 \leq i, j \leq n$ jest macierzą odwracalną. Wówczas:

•

$$l_t(A) := \min\{k \mid a_{kt} \neq 0\}, \quad 1 \leq t \leq n.$$

Funkcje l_i są dobrze określone, ponieważ każda kolumna macierzy odwracalnej jest niezerowa. Dla przykładu, jeśli

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 4 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 3 & 0 \end{pmatrix},$$

$$\text{to } l_1(A) = 2, l_2(A) = 1, l_3(A) = 4, l_4(A) = 2.$$

•

$$q_t(A) := B = (b_{ij}), 1 \leq i, j \leq n, \quad \text{gdzie } b_{ij} = \begin{cases} 1 & , i = l_t \wedge j = t \\ a_{ij} & , i \neq l_t \wedge j \neq t \\ 0 & , \text{w przeciwnym przypadku} \end{cases}.$$

Warto odnotować, że $A \in Gl_n(\mathbb{K}) \not\Rightarrow q_t(A) \in Gl_n(\mathbb{K})$. Przykład:

$$q_1\left(\begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}\right) = \begin{pmatrix} \mathbf{0} & 0 & 1 \\ \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & 0 & 0 \end{pmatrix}.$$

Definicja 2.6. *Niech $A \in M_n(\mathbb{K})$, zaś $t \in \{1, 2, \dots, n\}$. O macierzy A powiemy, że jest **t -zredukowana** wtedy i tylko wtedy, gdy:*

$$A = q_1(A) = q_2(A) = \dots q_t(A).$$

Przykład macierzy 2-zredukowanej.

$$\begin{pmatrix} 0 & 0 & 3 & 4 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 6 & 1 & 3 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 5 & 1 & 2 \end{pmatrix}$$

Jest jasne, że macierz A jest n -zredukowana wtedy i tylko wtedy, gdy $A \in S_n$.

Przez $B_n^-(\mathbb{K})$ oznaczać będziemy macierze dolnotrójkątne. Zauważmy, że:

$$A \in B_n^-(\mathbb{K}) \Leftrightarrow A \cdot \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \end{pmatrix} \in B_n(\mathbb{K}). \quad (2.4)$$

Wprowadziwszy niezbędne oznaczenia przechodzimy do dowodu lematów 2.4 i 2.5.

Dowód. (Lemat 2.4)

Niech $A \in Gl_n(\mathbb{K})$. Wystarczy udowodnić, że istnieją macierze:

$$\begin{aligned} X^{(1)}, X^{(2)}, \dots, X^{(n)} &\in B_n^-(\mathbb{K}) \\ Y^{(1)}, Y^{(2)}, \dots, Y^{(n)} &\in B_n(\mathbb{K}), \text{ że:} \end{aligned}$$

- (i) $A^{(1)} := X^{(1)} A Y^{(1)}$, gdzie macierz $A^{(1)}$ jest 1-zredukowana,
- (ii) $A^{(t)} := X^{(t)} A^{(t-1)} U^{(t)}$, gdzie $1 < t \leq n$ oraz macierz $A^{(t)}$ jest t -zredukowana.

Istotnie, wówczas macierz:

$$A^{(n)} = X^{(n)} X^{(n-1)} \dots X^{(2)} X^{(1)} \cdot A \cdot Y^{(1)} Y^{(2)} \dots Y^{(n-1)} Y^{(n)}$$

jest n -zredukowana, a więc jest macierzą permutacyjną. Dostajemy zatem tezę lematu 2.4, ponieważ zgodnie z wzorem (2.4) istnieje macierz permutacyjna P taka, że:

$$P A^{(n)} = \underbrace{\left(P X^{(n)} X^{(n-1)} \dots X^{(2)} X^{(1)} \right)}_{B_n(\mathbb{K})} \cdot A \cdot \underbrace{\left(Y^{(1)} Y^{(2)} \dots Y^{(n-1)} Y^{(n)} \right)}_{B_n(\mathbb{K})},$$

a stąd:

$$A = \underbrace{\left(P X^{(n)} X^{(n-1)} \dots X^{(2)} X^{(1)} \right)^{-1}}_{B_n(\mathbb{K})} \cdot \underbrace{\left(P A^{(n)} \right)}_{S_n} \cdot \underbrace{\left(Y^{(1)} Y^{(2)} \dots Y^{(n-1)} Y^{(n)} \right)^{-1}}_{B_n(\mathbb{K})}.$$

Rozumowanie jest indukcyjne. Niech $1 \leq i, j \leq n$. Elementy macierzy A oznaczać będziemy przez $a_{i,j}$. Dla $1 \leq t \leq n$ elementy macierzy $A^{(t)}$ oznaczać będziemy przez $a_{i,j}^{(t)}$, zaś elementy macierzy $X^{(t)}, Y^{(t)}$ przez $x_{i,j}^{(t)}, y_{i,j}^{(t)}$.

1. (Krok 1.) Niech $t = 1$.

Niech $k_1(A)$ składa się z elementów $a_{1,1}, a_{2,1}, \dots, a_{l_1,1}, \dots, a_{n,1}$. Wówczas kładziemy:

$$X^{(1)} := \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & x_{l_1, l_1}^{(1)} & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & x_{l_1+1, l_1}^{(1)} & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & x_{n, l_1}^{(1)} & 0 & \dots & 1 \end{pmatrix} \in B_n^-(\mathbb{K}),$$

gdzie:

$$x_{p, l_1}^{(1)} = \begin{cases} (a_{l_1, 1})^{-1} & , \quad p = l_1 \\ -(a_{l_1, 1})^{-1} a_{p, 1} & , \quad p > l_1 \end{cases},$$

Łatwo sprawdzić, że $k_1(X^{(1)}A) = e_{l_1}$.

Aby zakończyć krok 1. wystarczy znaleźć macierz $Y^{(1)}$ spełniającą następujące warunki:

$$k_1(X^{(1)}A) = k_1(X^{(1)}AY^{(1)}) = e_{l_1} \quad (2.5)$$

$$w_1(X^{(1)}AY^{(1)}) = e_1 \quad (2.6)$$

Łatwo sprawdzić, że jest to macierz postaci:

$$Y^{(1)} := \begin{pmatrix} 1 & y_{1,2}^{(1)} & y_{1,3}^{(1)} & \dots & y_{1,n}^{(1)} \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \in B_n(\mathbb{K}),$$

gdzie $y_{1,q}^{(1)} = -a_{l_1,q}$, $q > 1$.

W ten sposób macierz $A^{(1)} = X^{(1)}AY^{(1)}$ jest 1-zredukowana. Krok 1 został zakończony.

2. (Krok indukcyjny.) Ustalmy $1 < t < n$. Niech $l_i := l_i(A^{(i-1)})$, $1 < i \leq t$. Załóżmy, że $A^{(i)}$ jest, dla $1 \leq i < t$, macierzą i -zredukowaną, a więc:

$$\begin{aligned} w_{l_1}(A^{(i)}) &= e_1, & w_{l_2}(A^{(i)}) &= e_2, & \dots, & & w_{l_i}(A^{(i)}) &= e_i \\ k_1(A^{(i)}) &= e_{l_1}, & k_2(A^{(i)}) &= e_{l_2}, & \dots, & & k_i(A^{(i)}) &= e_{l_i} \end{aligned} \quad (2.7)$$

Zacznijmy od konstrukcji macierzy $X^{(t)}$. Niech $k_t(A^{(t-1)})$ składa się z elementów $a_{1,t}^{(t-1)}, a_{2,t}^{(t-1)}, \dots, a_{l_t,t}^{(t-1)}, \dots, a_{n,t}^{(t-1)}$. Wówczas kładziemy:

$$X^{(t)} := \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & x_{l_t, l_t}^{(t)} & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & x_{l_t+1, l_t}^{(t)} & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & x_{n, l_t}^{(t)} & 0 & \dots & 1 \end{pmatrix} \in B_n^-(\mathbb{K}),$$

gdzie dla $1 \leq i \leq t$:

$$x_{p, l_t}^{(t)} = \begin{cases} (a_{l_t, t}^{(t-1)})^{-1} & , p = l_t \\ -(a_{l_t, t}^{(t-1)})^{-1} a_{p, t}^{(t-1)} & , p > l_t \end{cases}.$$

Łatwo sprawdzić, że: $k_i(A^{(t-1)}) = k_i(X^{(t)} A^{(t-1)}) = e_{l_i}$, dla $1 \leq i \leq t$. Istotnie, z założenia indukcyjnego wynika, że $k_i(A^{(t-1)}) = e_{l_i}$, co więcej $\{l_1, l_2, \dots, l_t\}$ są parami różne. W szczególności, jeśli $1 \leq i < t$, to w każdej z kolumn $k_i(A^{(t-1)})$, element $a_{l_t, i}^{(t-1)}$ równy jest 0. Podobnie jak w kroku 1. macierz $X^{(t)}$ zamienia $k_t(A^{(t-1)})$ na wektor jednostkowy e_{l_t} .

Pozostała nam jeszcze konstrukcja macierzy $Y^{(t)}$, spełniającej warunki:

$$k_i(X^{(t)} A^{(t-1)}) = k_i(X^{(t)} A^{(t-1)} Y^{(t)}) = e_{l_i}, 1 \leq i \leq t \quad (2.8)$$

$$w_{l_t}(X^{(t)} A^{(t-1)} Y^{(t)}) = e_t \quad (2.9)$$

Łatwo widzieć, że warunki (2.8), (2.9) są spełnione przez macierz:

$$Y^{(t)} := \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & y_{t, t+1}^{(t)} & \dots & y_{t, n}^{(t)} \\ 0 & 0 & 0 & \dots & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 0 & \dots & 1 \end{pmatrix} \in B_n(\mathbb{K}),$$

gdzie $y_{t, q}^{(t)} = -a_{l_t, q}^{(t-1)}$, $q > t$.

Zatem macierz $A^{(t)} = X^{(t)} A^{(t-1)} Y^{(t)}$ jest t -zredukowana. To kończy krok indukcyjny. Lemat 2.4 został zatem udowodniony.

□

Dowód. (Lemat 2.5)

Założmy, że dla pewnych $\sigma_1, \sigma_2 \in S_n$ mamy:

$$B_n(\mathbb{K}) \sigma^{(1)} B_n(\mathbb{K}) = B_n(\mathbb{K}) \sigma_2 B_n(\mathbb{K}).$$

Istnieją więc macierze $A, B \in B_n(\mathbb{K})$, że:

$$A\sigma_1 B = \sigma_2.$$

Zgodnie z algorytmem Gaussa:

- istnieje ciąg $W_1, W_2, \dots, W_n$ macierzy takich, że dla każdego $1 \leq i \leq n$ macierz W_i jest iloczynem macierzy elementarnych operacji wierszowych na $W_{i+1} \dots W_n A$. Dokładniej, macierz $W_{i+1} \dots W_n A$ jest górnotrójkątna, zatem $k_i(W_{i+1} \dots W_n A)$ jest postaci:

$$\begin{pmatrix} x_{1,i} \\ x_{2,i} \\ \vdots \\ x_{i,i} \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Macierz W_i jest iloczynem operacji elementarnych $W_{1,i}W_{2,i} \dots W_{i,i}$, które polegają kolejno na:

- $W_{i,i}$ – na pomnożeniu i -tego wiersza przez $(x_{i,i})^{-1}$,
- $W_{j,i}$ – na odjęciu od j -tego wiersza i -tego wiersza przemnożonego przez stałą x_{ji} , gdzie $1 \leq j < i$.

W ten sposób $k_i(W_i W_{i+1} \dots W_n A) = e_i$.⁶

- istnieje ciąg $K_1, K_2, \dots, K_n$ macierzy takich, że dla każdego $1 \leq i \leq n$ macierz K_i jest iloczynem macierzy elementarnych operacji kolumnowych na $BK_1 \dots K_{i-1}$. Dokładniej, macierz $BK_1 \dots K_{i-1}$ jest górnotrójkątna, zatem $w_i(BK_1 \dots K_{i-1})$ jest postaci:

$$(0 \quad \dots \quad y_{i,i} \quad y_{i,i+1} \quad \dots \quad y_{i,n}).$$

Macierz K_i jest iloczynem operacji elementarnych $K_{i,i}K_{i,i+1} \dots K_{i,n}$, które polegają kolejno na:

- $K_{i,i}$ – na pomnożeniu i -tej kolumny przez $(y_{i,i})^{-1}$,
- $K_{i,j}$ – na odjęciu od j -tej kolumny i -tej kolumny przemnożonej przez stałą $y_{i,j}$, gdzie $i < j \leq n$.

W ten sposób $w_i(BK_1 \dots K_{i-1}K_i) = e_i$.⁷

Korzystamy tu z faktu, że A, B są elementami $B_n(\mathbb{K})$. Wiadomo, że postać zredukowana, zarówno wierszowa jak i kolumnowa, macierzy należącej do $B_n(\mathbb{K})$ jest identycznością. Iloczyn $W_1 W_2 \dots W_n A$ prowadzi do postaci wierszowej zredukowanej. Iloczyn $BK_1 K_2 \dots K_n$ prowadzi do postaci kolumnowej zredukowanej. Stąd:

$$(W_1 W_2 \dots W_n) \sigma_1 (K_1 K_2 \dots K_n) = \sigma_2$$

⁶Wyjaśnia to przyjętą przez nas numerację. Algorytm Gaussa (w części wykorzystującej jedynie operacje wierszowe) działa od n . wiersza „w górę”.

⁷Wyjaśnia to przyjętą przez nas numerację. Algorytm Gaussa (w części wykorzystującej jedynie operacje kolumnowe) działa od 1. kolumny „w prawo”.

Założmy, że chcąc uzyskać σ_2 z σ_1 wykonujemy najpierw operacje kolumnowe $K_1, K_2, \dots, K_n$, a później operacje wierszowe $W_n, W_{n-1}, \dots, W_1$. Pokażemy, że dla $1 \leq i \leq n$, $k_i(\sigma_1) = k_i(\sigma_2)$.

Dowód jest indukcją ze względu na i .

- $k_1(\sigma_1) = k_1(\sigma_2)$. Zgodnie z tym jak określiliśmy macierze K_i widzimy, że jedynie operacja $K_{1,1}$ może zmienić pierwszą kolumnę σ_1 . Założmy, że tak jest i $K_{1,1}$ polega na przemnożeniu $k_1(\sigma_1)$ przez $0 \neq a \in \mathbb{K}$. Rozważmy teraz operacje W_j . Działają one kolejno na macierzy $W_{j+1} \dots W_{n-1} W_n \sigma_1 K_1 K_2 \dots K_n$, przy czym

$$k_1(\sigma_1 K_1 K_2 \dots K_n) = a k_1(\sigma).$$

Założmy, że niezerowy element $k_1(\sigma_1)$ znajduje się w wierszu l_1 . Wówczas wszystkie operacje postaci $W_{i,j}$, gdzie $j > l_1$ nie mają wpływu na kolumnę $a k_1(\sigma)$. Operacja W_{l_1, l_1} polega na przemnożeniu wiersza l_1 przez pewną stałą $0 \neq b \in \mathbb{K}$. Łatwo widzieć, że operacje postaci $w_{i,j}$, gdzie $j \leq l_i$ oraz $(i, j) \neq (l_i, l_i)$ muszą być identycznościami, w przeciwnym razie w $k_1(\sigma_2)$ znajdowałyby się przynajmniej dwa elementy niezerowe.⁸ Widzimy zatem, że $k_1(\sigma_2) = b a k_1(\sigma_1)$. Stąd $b a = 1$ i pierwsza część dowodu jest zakończona.

- Założmy, że $k_i(\sigma_1) = k_i(\sigma_2)$, dla $1 \leq i < m \leq n$. Wykażemy, że $k_m(\sigma_1) = k_m(\sigma_2)$. Założmy, że niezerowy element $k_i(\sigma_1)$ znajduje się w wierszu l_i . Zauważmy, że mnożenie σ_1 kolejno przez macierze $K_1, K_2, \dots, K_n$ może sprawić, że $k_m(\sigma_1 K_1 K_2 \dots K_n)$ będzie miała niezerowe elementy w wierszach $t_1, t_2, \dots, t_s \subseteq \{l_1, l_2, \dots, l_{m-1}\}$. Niech $l = \max(t_1, t_2, \dots, t_s, l_m)$. Zauważmy, że skoro $A \sigma_1 B$ jest macierzą permutacyjną, zatem po wykonaniu operacji $W_n, W_{n-1}, \dots, W_1$ dostaniemy $k_m(\sigma_2) = e_l$. Na mocy założenia indukcyjnego istnieje takie $s < m$, że $k_s(\sigma_1) = k_s(\sigma_2) = e_l$. Jeśli, wbrew tezie $l > l_m$, wówczas $k_s(\sigma_2) = k_m(\sigma_2) = e_l$. Stąd sprzeczność z założeniem, że $\sigma_2 \in S_n$.

□

2.2. Podgrupy Borela w $Gl_n(\mathbb{K})$

Niech G będzie grupą algebraiczną nad ciałem algebraicznie domkniętym $\mathbb{K}$. Przypomnijmy, że zgodnie z definicją 1.36 podgrupę $B \leq G$ nazywamy podgrupą Borela w G jeśli jest ona maksymalną domkniętą, spójną i rozwiązalną podgrupą G . Celem tego paragrafu będzie dowód następującego faktu:

Twierdzenie 2.7. *Niech $\mathbb{K} = \overline{\mathbb{K}}$. Wówczas każda podgrupa Borela grupy $Gl_n(\mathbb{K})$ jest, z dokładnością do sprzężenia, równa $B_n(\mathbb{K})$.*

Na podstawie poprzedniego paragrafu wiemy, że w $Gl_n(\mathbb{K})$ zachodzi rozkład na warstwy podwójne względem podgrupy $B_n(\mathbb{K})$. Rozkład ten, podobnie jak rozkłady wymienione w twierdzeniu 2.2, nazwalismy rozkładem Bruhat. W klasie grup algebraicznych rozkładem Bruhat nazywamy rozkład na warstwy podwójne względem podgrupy Borela.

Dowód. (Twierdzenie 2.7)

Należy dowieść, że $B_n(\mathbb{K})$ jest domkniętą, spójną i rozwiązalną podgrupą $Gl_n(\mathbb{K})$. Jeśli warunki te są spełnione, to na mocy tw. Lie-Kolchina (tw. 1.35) jest ona maksymalną podgrupą $Gl_n(\mathbb{K})$ o tych własnościach.

⁸Istotną rolę gra tutaj kolejnych wykonywanych operacji: „z dołu do góry”.

- $B_n(\mathbb{K})$ jest domkniętą i spójną podgrupą $Gl_n(\mathbb{K})$.

Istotnie, zauważmy że zachodzi następujący związek pomiędzy pierścieniami funkcji regularnych $Gl_n(\mathbb{K})$ oraz $B_n(\mathbb{K})$

$$\mathbb{K}[B_n(\mathbb{K})] \simeq \mathbb{K}[Gl_n(\mathbb{K})]/(x_{ij}, i > j)$$

Ideał $(x_{ij}, i > j)$ jest pierwszy w $\mathbb{K}[Gl_n(\mathbb{K})]$. Stąd na mocy uwagi 1.28 $B_n(\mathbb{K})$ jest nierozkładalnym podzbiorem domkniętym $Gl_n(\mathbb{K})$. W komentarzu do definicji 1.33 (grupy algebraicznej) stwierdziliśmy jednak, że jeśli grupa algebraiczna jest nierozkładalna, to musi być też spójna.

- $B_n(\mathbb{K})$ jest grupą rozwiązalną.

Rozważmy homomorfizm $h : B_n(\mathbb{K}) \rightarrow (\mathbb{K}^*)^n$ postaci:

$$h((a_{ij})) = (a_{11}, a_{22}, \dots, a_{nn}).$$

Jest on dobrze określony, bo $a_{ii} \neq 0$, $i = 1, 2, \dots, n$ (inaczej wyznacznik macierzy byłby zerowy). Jest to epimorfizm, którego jądrem jest grupa $U_n(\mathbb{K})$. Iloraz jest grupą abelową. Z definicji 1.34 (grupy rozwiązalnej) widać, że wystarczy teraz pokazać rozwiązalność grupy $U_n(\mathbb{K})$. Niech:

$$N_i = \{(a_{kl}) \in M_n(\mathbb{K}) \mid a_{kl} = 0, \text{ dla } l - k < i\}, \quad i = 1, 2, \dots, n.$$

Określamy ciąg $\{I\} = I + N_n \leq I + N_{n-1} \leq \dots \leq I + N_2 \leq I + N_1 = U_n(\mathbb{K})$.

Zgodnie z definicją 1.34 wykażemy, że dla $1 \leq i \leq n-1$:

- $I + N_{i+1} \triangleleft I + N_i$
- $(I + N_i)/(I + N_{i+1})$ jest grupą abelową.

Łatwo widzieć, że dla każdych $1 \leq i, j \leq n$:

$$N_i \cdot N_j \subset N_{\min\{i+j, n\}}. \quad (2.10)$$

Niech $X \in I + N_i$, zaś $A \in I + N_{i+1}$, $1 \leq i \leq n-1$. Wtedy na mocy (2.10):

$$(X^{-1}AX) - I = X^{-1}(A - I)X \in (I + N_i)(N_{i+1})(I + N_i) \subseteq N_{i+1},$$

zatem $I + N_{i+1} \triangleleft I + N_i$.

Pozostaje udowodnić, że iloraz $(I + N_i)/(I + N_{i+1})$ jest grupą abelową.

Rozważmy macierze $A = I - A', B = I - B'$, gdzie $A', B' \in N_i$. Chcemy pokazać, że $ABA^{-1}B^{-1} \in I + N_{i+1}$. Zauważmy, że $(A')^{n-i} = 0$, $(B')^{n-i} = 0$. Stąd:

$$A^{-1} = I + A' + (A')^2 + \dots + (A')^{n-i-1}, \quad B^{-1} = I + B' + (B')^2 + \dots + (B')^{n-i-1}.$$

Zatem:

$$ABA^{-1}B^{-1} = (I - A')(I - B')(I + A' + \dots + (A')^{n-i-1})(I + B' + \dots + (B')^{n-i-1}). \quad (2.11)$$

Na mocy (2.10) wiadomo, że macierze $A'B', B'A', (A')^2, (B')^2 \in N_{i+1}$. Jeśli zatem pomnożymy nawiasy w (2.11) otrzymamy:

$$ABA^{-1}B^{-1} = I - A' - B' + A' + B' + T = I + T, \quad T \in N_{i+1}.$$

Zatem grupa $(I + N_i)/(I + N_{i+1})$ istotnie jest abelowa. Grupa $U_n(\mathbb{K})$, a wraz z nią $Gl_n(\mathbb{K})$, jest zatem rozwiązalna. □

2.3. Systemy Titsa

Jak wspomnieliśmy we wprowadzeniu do tego rozdziału, rozkład na warstwy podwójne, zaobserwowany po raz pierwszy przez Bruhat, został przez Chevalleya wykorzystany do konstrukcji nieznanych wcześniej serii skończonych grup prostych. Rozumowania Chevalleya obciążone były jednak narzędziami wykraczającymi poza teorię grup skończonych – przede wszystkim metodami geometrii algebraicznej. Na początku lat 60' J. Tits opublikował serię prac (m.in [Tit62], [Tit64]), w których wyniki Chevalleya zostały uproszczone i przeniesione na grunt teorii grup abstrakcyjnych. Przyglądając się strukturze grup wprowadzonych przez Chevalleya i posiadających rozkład Bruhat, Tits wyodrębnił zestaw czterech aksjomatów, które spełniać musi grupa skończona, aby mógł w niej zachodzić analog rozkładu na warstwy podwójne. Omówieniu tej aksjomatyki poświęcony jest niniejszy paragraf.

Zacniemy od dowodu następującej uwagi technicznej.

Uwaga 2.8. *Niech G będzie grupą, zaś B, N niech będą takimi podgrupami G , że $G = \langle B, N \rangle$. Załóżmy ponadto, że $B \cap N \triangleleft N$. Wówczas jeśli $n_1, n_2 \in N$ i $n_1 n_2^{-1} \in B \cap N$ (n_1, n_2 są reprezentantami ustalonego elementu w ilorazie $N/(B \cap N)$), to warstwy podwójne Bn_1B, Bn_2B elementów n_1, n_2 względem podgrupy B są równe.*

Dowód. Zauważmy, że skoro w tezie lematu mówimy o warstwach, a więc orbitach działania grupy $H \times H$ na G (zgodnie z (2.1)) to jeśli, wbrew tezie, $Bn_1B \neq Bn_2B$, wówczas

$$Bn_1B \cap Bn_2B = \emptyset. \tag{2.12}$$

Wiemy jednak, że $n_1 n_2^{-1} \in B \cap N$. W szczególności, istnieje $b \in B$, że $n_1 n_2^{-1} = b$. Stąd $n_1 = bn_2 \in Bn_2 \subseteq Bn_2B$. Sprzeczność z (2.12). □

Jeśli $N/(B \cap N) = W$, wówczas każda z warstw postaci $BnB, n \in N$ wyznaczona jest jednoznacznie przez pewien element $w \in W$. W dalszych rozważaniach warstwę odpowiadającą elementowi $w \in W$ oznaczать będziemy przez Bn_wB lub po prostu przez BwB .

Definicja 2.9 (Tits (1962)). *Niech G będzie grupą skończoną. Mówimy, że G jest **systemem Titsa** (lub **grupą z BN-parą**⁹) jeśli istnieją podgrupy $B, N \leq G$, spełniające następujące warunki:*

- **(BN1)** $G = \langle B, N \rangle$,
- **(BN2)** $B \cap N$ jest podgrupą normalną w N , oraz iloraz $W := N/(B \cap N)$, zwany **grupą Weyla** G , jest grupą generowaną przez skończony zbiór S elementów rzędu 2,

⁹Terminu BN-para używał oryginalnie Tits.

- **(BN3)** $n_s B n_s \neq B$ jeśli $s \in S$,
- **(BN4)** $n_s B n_w \subseteq B n_s n_w B \cup B n_w B$ dla każdego $s \in S$ oraz $w \in W$.

Odnotujmy od razu równoważne sformułowania aksjomatów **(BN3)**, **(BN4)**:

- **(BN3)** $(B n_s B)(B n_s B) \neq B$, $s \in S$,
- **(BN4)** $(B n_s B)(B n_w B) \subseteq B n_w B \cup B n_s n_w B$, $s \in S, w \in S$.

Zasadniczym przykładem systemu Titsa jest, jak wykażemy w następnym paragrafie, grupa macierzy odwracalnych nad ciałem skończonym.

Przykład 2.10. Niech $\mathbb{F}_q$ będzie ciałem q -elementowym, gdzie q jest liczbą pierwszą, zaś $G = Gl_n(\mathbb{F}_q)$. Niech:

- $B := B_n(\mathbb{F}_q)$ – podgrupa złożona ze wszystkich macierzy górnotrójkątnych in $Gl_n(\mathbb{F}_q)$,
- $N := N_n(\mathbb{F}_q)$ – podgrupa złożona ze wszystkich macierzy mających dokładnie jeden niezerowy wyraz w każdym wierszu i kolumnie

Grupa G wraz z podgrupami B, N tworzą system Titsa. Grupa Weyla jest izomorficzna z grupą macierzy permutacyjnych, generowaną przez transpozycje (a więc macierze zamiany dwóch sąsiednich wierszy).

Powyższy przykład pokazuje jaka jest intuicja dla pojęć występujących w definicji systemu Titsa. Grupa B ma być abstrakcyjnym odpowiednikiem macierzy górnotrójkątnych, czy ogólniej – podgrupy Borela grupy algebraicznej. Spodziewamy się zatem, że abstrakcyjny rozkład Bruhat będzie miał następującą postać:

$$G = \bigcup_{w \in W} B n_w B.$$

Zanim przystąpimy do dowodu twierdzenia o istnieniu rozkładu Bruhat w każdym systemie Titsa, wprowadzimy jeszcze jedno niezwykle istotne pojęcie.

Niech $1 \neq w \in W$. Element ten można zapisać jako iloczyn dodatnich potęg pewnej ilości elementów z S (wynika to z faktu, że W jest generowana przez involucje). Takich przedstawień jest oczywiście nieskończenie wiele. Wśród nich istnieją przedstawienia o najmniejszej długości, a więc takie, do których użyto takiej liczby $l(w)$ generatorów, że w nie można zapisać w postaci iloczynu mniej niż $l(w)$ generatorów. Przedstawienia takie nazywamy **postaciami zredukowanymi** $w \in W$. Możliwe jest oczywiście, aby dany element $w \in W$ miał wiele różnych postaci zredukowanych. Liczba naturalna $l(w)$ jest mu jednak przyporządkowana jednoznacznie (można założyć, że element neutralny W zapisuje się za pomocą 0 generatorów). W ten sposób określona zostaje **funkcja długości** $l : W \rightarrow \mathbb{N}$. Istnienie tej funkcji pozwala na stosowanie dowodów indukcyjnych. Ich podstawą jest następująca uwaga.

Uwaga 2.11. Zauważmy też, że jeśli mamy $w \in W$, które nie jest jednością, wówczas możemy znaleźć takie $s \in S$, że $l(sw) + 1 = l(w)$.

Dowód. Wystarczy rozważyć dowolną postać zredukowaną w postaci:

$$w = s_{i_1} s_{i_2} \dots s_{i_{l(w)}}, \quad s_{i_k} \in S.$$

Wówczas $s_{i_1} w$ ma długość o 1 mniejszą niż w . □

Twierdzenie 2.12 (Rozkład Bruhat). Niech G będzie grupą z BN -parą. Wówczas G rozkłada się na sumę rozłącznych warstw podwójnych postaci:

$$G = \bigcup_{w \in W} Bn_w B. \quad (2.13)$$

Dowód. Wykażemy najpierw równość zbiorów występujących po obydwu stronach (2.13). Jest jasne, że suma warstw $Bn_w B, w \in W$ zawarta jest w G . Pozostaje wykazać inkluzję przeciwną. W tym celu wystarczy uzasadnić, że $BNB \leq G$. Istotnie, wówczas na mocy **(BN1)** podgrupa BNB musi być równa całej grupie G .

Zbiór BNB jest zamknięty na operacje grupowe. Istotnie, po pierwsze, w zbiorze tym jest jedynka grupy G . Jest on ponadto zamknięty na branie elementu odwrotnego. Dla elementów $b_1, b_2 \in B, n \in N$ mamy: $(b_1 n b_2)^{-1} = b_2^{-1} n^{-1} b_1^{-1} \in BNB$. Pozostaje uzasadnić, że BNB jest zamknięty na mnożenie. Z pewnością $B(BNB) \subseteq BNB$. Wystarczy więc pokazać, że $N(BNB) \subseteq BNB$. Skoro jednak N jest generowana przez $N \cap B$ oraz przez wybrany zbiór reprezentantów elementów grupy ilorazowej W , nazwijmy je n_w , wystarczy pokazać, że $n_w(BNB) \subseteq BNB$ (oczywiście $(N \cap B)(BNB) \subseteq BNB$). Z aksjomatu **(BN4)**, dla każdego $n_w, w \in W$ mamy:

$$n_s(Bn_w B) = (n_s B n_w) B \subseteq B n_s n_w B \cup B n_w B \subseteq BNB.$$

W jest generowana przez zbiór S , zatem

$$n_s(BNB) \subseteq BNB, s \in S \Rightarrow n_w(BNB) \subseteq BNB, w \in W.$$

Stąd $BNB \leq G$. Pierwsza część dowodu jest więc zakończona. Pozostaje udowodnić, że dla $x, y \in W$:

$$Bn_x B = Bn_y B \Rightarrow x = y. \quad (2.14)$$

Istotnie, rozkład (2.13) pochodzi od działania $B \times B$ na G , zatem warstwy $Bn_w B$ są, dla $w \in W$, równe lub rozłączne. Załóżmy, że $l(x) \leq l(y)$. Dowiedzimy teraz (2.14). Stosujemy indukcję ze względu na $l(x)$.

- (Krok 1) $l(x) = 0$. Jeśli $l(x) = 0$, wtedy $x = 1$, zatem $B = Bn_x B = Bn_y B$. Stąd $n_y \in B \cap N$, a zatem n_y przechodzi przy homomorfizmie naturalnym $N \rightarrow N/(N \cap B)$ na jedynkę grupy W , czyli $y = 1$.
- (Krok 2) $l(x) > 0$. Zgodnie z uwagą 2.11 istnieje $s \in S$, że $l(sx) < l(x)$. Jeśli, wbrew tezie, $x \neq y$, to $sx \neq sy$ oraz $sx \neq y$ (y ma większą długość). Długość sx jest mniejsza niż długość x , zatem z założenia indukcyjnego:

$$Bn_s n_x B \neq Bn_s n_y B, \quad Bn_s n_x B \neq Bn_y B. \quad (2.15)$$

Korzystając z **(BN4)** widzimy jednak, zgodnie z (2.15), że:

$$(Bn_s n_x B) \cap (Bn_s B)(Bn_y B) \subseteq Bn_s n_x B \cap Bn_s n_y B = \emptyset \quad (2.16)$$

Z drugiej strony dla dowolnych $s \in S, x \in W$:

$$(Bn_s n_x B) \subseteq (Bn_s B)(Bn_x B). \quad (2.17)$$

Porównanie (2.16) i (2.17) prowadzi do wniosku, że $Bn_x B \neq Bn_y B$. Dostaliśmy zatem sprzeczność z założeniem. Dowód jest zakończony. Warto odnotować, że ani razu nie skorzystaliśmy do tej pory z **(BN3)**.

□

W kontekście poprzednich paragrafów naturalne jest następujące pytanie: czy grupa algebraiczna nad ciałem algebraicznie domkniętym (a więc grupa nieskończona) może spełniać aksjomaty systemu Titsa? Przy jakich warunkach rozkład Bruhat jest rozkładem grupy algebraicznej na warstwy podwójne względem jej podgrupy Borela? Wśród tych grup klasycznych, które posiadają rozkład Bruhat, wszystkie, choć są nieskończone, spełniają **(BN1) – (BN4)**. Dla przykładu, jeśli G jest klasyczną grupą Liego nad $\mathbb{C}$, wówczas występujące w sformułowaniu twierdzenia 2.2 grupy $B, N(T)$ tworzą BN-parę w G . Iloraz $N(T)/T$ jest grupą Weyla grupy G . Dowód twierdzenia 2.12 nie korzysta ze skończoności grupy G . Widać zatem, że jeśli grupa nieskończona spełnia aksjomaty systemu Titsa, wówczas zachodzi w niej rozkład Bruhat.

W teorii grup algebraicznych o rozkładzie Bruhat mówi się w kontekście tzw. grup reduktywnych. O klasie tej można mówić bez konieczności wcześniejszego definiowania BN-par. Nie będziemy jednak zatrzymywać się dłużej przy tym zagadnieniu. Dokładne omówienie tej tematyki znaleźć można np. w [Gec03], par. 1.7, lub w [Hum75], rozdz. 28.

Definicja 2.13. Powiemy, że podgrupa T spójnej grupy algebraicznej G jest **torusem maksymalnym** w G jeśli jest maksymalną spójną podgrupą G izomorficzną z domkniętą podgrupą $T_n(\mathbb{K})$, dla pewnego n .

Definicja 2.14. Powiemy, że podgrupa $R_u(G)$ spójnej grupy algebraicznej G jest **radykałem unipotentnym** spójnej grupy algebraicznej G , jeśli $R_u(G)$ jest maksymalną domkniętą spójną i unipotentną podgrupą normalną w G . Spójną grupą algebraiczną G nazywamy **reduktywną**, jeśli $R_u(G) = \{1\}$.

W każdej tak zdefiniowanej grupie reduktywnej można wprowadzić strukturę BN-pary. Grupy reduktywne są tą klasą grup algebraicznych, w których zachodzi rozkład Bruhat na warstwy podwójne względem podgrupy Borela:

Twierdzenie 2.15. Niech G będzie grupą reduktywną, zaś B, T niech będą odpowiednio: podgrupą Borela w G oraz torusem maksymalnym w G . Wówczas grupa G rozkłada się na sumę warstw podwójnych względem B postaci:

$$G = \bigsqcup_{w \in W} BwB, \quad (2.18)$$

dla $W = N(T)/T$, gdzie $N(T)$ jest normalizatorem T w G .

2.4. $Gl_n(\mathbb{F}_q)$

Celem tego krótkiego paragrafu jest uzasadnienie, że jeśli $G = Gl_n(\mathbb{F}_q)$, wówczas podgrupy:

- $B := B_n(\mathbb{F}_q)$ – podgrupa $Gl_n(\mathbb{F}_q)$ złożona ze wszystkich macierzy górnotrójkątnych,
- $N := N_n(\mathbb{F}_q)$ – podgrupa $Gl_n(\mathbb{F}_q)$ złożona ze wszystkich macierzy mających dokładnie jeden niezerowy wyraz w każdym wierszu i kolumnie,

zadają strukturę BN-pary na G . Grupa Weyla jest izomorficzna z grupą macierzy permutacyjnych, generowaną przez transpozycje (a więc macierze zamiany dwóch sąsiednich wierszy).

Niech $\{e_1, e_2, \dots, e_n\}$ będzie bazą przestrzeni liniowej $\mathbb{F}_q^n$. Sprawdzamy kolejne aksjomaty BN-pary:

- (BN 1) Wykażemy, że $\langle B, N \rangle = G$.

Ze standardowego kursu algebry liniowej wiadomo, że G jest generowana przez macierze diagonalne, należące do N , oraz przez macierze elementarne postaci:

$$E = \mathbf{E}_{ij}(c) = I + c\mathbf{e}_{ij}, \quad i \neq j, c \in \mathbb{F}_q,$$

gdzie $\mathbf{e}_{ij}$ jest jedynką macierzową¹⁰. Pozostaje uzasadnić, że macierze ze zbioru E można generować przy pomocy elementów z B i N .

Podgrupa B zawiera oczywiście wszystkie macierze postaci $\{\mathbf{E}_{ij}(c) \mid i < j, c \in \mathbb{F}_q\}$. Wiadomo, że wiersze i kolumny dowolnej macierzy można permutować przy pomocy macierzy z N . Łatwo zatem widzieć, że dla dowolnej macierzy elementarnej $\mathbf{E}_{ij}(c) \in E$ istnieją takie macierze permutacyjne $P, Q \in N$, że $P\mathbf{E}_{ij}(c)Q \in B$. Zatem $G = \langle B, N \rangle$. Zatem każda macierz z E jest generowana przez elementy z B i N , co kończy dowód.

- (BN 2) Łatwo widzieć, że $B \cap N$ to grupa macierzy diagonalnych. Zauważmy, że każda macierz z grupy N permutuje proste $\text{lin}\{e_1\}, \text{lin}\{e_2\}, \dots, \text{lin}\{e_n\}$. Mamy więc homomorfizm z N do grupy permutacji S_n . Jego jądrem jest podgrupa macierzy diagonalnych $B \cap N = T$. Fakt, że S_n jest generowana przez elementy rzędu 2 (transpozycje) jest elementarny.
- (BN 3) Spełniony w sposób oczywisty.
- (BN 4) Chcemy udowodnić, że:

$$n_s B n_w \subseteq B n_s n_w B \cup B n_w B, \quad s \in S, w \in W. \quad (2.19)$$

Mnożąc (2.19) z prawej strony przez n_w^{-1} widzimy, że wystarczy udowodnić inkluzję postaci:

$$n_s B \subseteq B n_s B' \cup B B', \quad \text{gdzie } B' := n_w B n_w^{-1}, s \in S, w \in W. \quad (2.20)$$

Niech G_i będzie, dla $1 \leq i \leq n$, taką podgrupą G , której działanie¹¹ jest niezmiennicze na podprzestrzeni¹² $\text{lin}\{e_i, e_{i+1}\}$ i stałe na pozostałych wektorach bazy $\{e_1, e_2, \dots, e_n\}$ przestrzeni $\mathbb{F}_q^n$. Łatwo widzieć, że jest to podgrupa izomorficzna z $Gl_2(\mathbb{F}_q)$. Co więcej, dla $1 \leq i \leq n$ zachodzi równość:

$$G_i B = B G_i. \quad (2.21)$$

Istotnie, łatwo widzieć, że zarówno lewa, jak i prawa strona równości (2.21) składa się z dokładnie tych macierzy $g \in G$, których działanie na wektorach bazowych $\mathbb{F}_q^n$ opisać można, dla $1 \leq i \leq n$, w następujący sposób:

$$\begin{aligned} g e_j &\in \text{lin}\{e_1, e_2, \dots, e_j\} \quad , \text{ dla każdego } j \neq i \\ g e_i &\in \text{lin}\{e_1, e_2, \dots, e_{i+1}\}. \end{aligned}$$

Grupa $W \simeq S_n$ generowana jest przez transpozycje $s_1 = (1, 2)$, $s_2 = (2, 3)$, $s_3 = (3, 4)$, $\dots$, $s_{n-1} = (n-1, n)$, $s_n = (n, 1)$. Działanie s_i na $\mathbb{F}_q^n$ polega, dla $1 \leq i \leq n$, na permutacji

¹⁰Jedynka macierzowa $\mathbf{e}_{ij}$ to taka macierz, w której na miejscu (i, j) stoi 1, a na pozostałych miejscach stoją zera.

¹¹Z każdą macierzą odwracalną należącą do $Gl_n(\mathbb{F}_q)$ związany jest izomorfizm liniowy przestrzeni $\mathbb{F}_q^n$.

¹²Gdy $i = n$, wówczas chodzi o podprzestrzeń $\text{lin}\{e_n, e_1\}$.

wektorów bazowych e_i, e_{i+1} . Na pozostałych wektorach bazowych s_i jest stałe. Stąd $s_i \in G_i$. Element ten można utożsamiać z macierzą $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in Gl_2(\mathbb{F}_q)$. Na mocy (2.21) widzimy, że $s_i B \subseteq B G_i$. Stąd inkluzja (2.20) będzie spełniona jeśli dla każdego $1 \leq i \leq n$ zachodzić będzie inkluzja:

$$G_i \subseteq B B' \cup B s_i B'.$$

W szczególności, wystarczy pokazać, że dla każdego $1 \leq i \leq n$:

$$G_i \subseteq (B \cap G_i)(B' \cap G_i) \cup (B \cap G_i)s_i(B' \cap G_i). \quad (2.22)$$

Jeśli G_i utożsamiamy z $Gl_2(\mathbb{F}_q)$, to $B \cap G_i$ utożsamiać możemy z podgrupą B_2 macierzy górnotrójkątnych w $Gl_2(\mathbb{F}_q)$. Niech B_2^- oznacza grupę macierzy dolnotrójkątnych w $Gl_2(\mathbb{F}_q)$.

Uwaga 2.16. *Rozważmy grupę $G' = B' \cap G_i = n_w B n_w^{-1} \cap G$. Wówczas $G' \simeq B_2$ lub $G' \simeq B_2^-$. $G' \simeq B_2$ gdy $n_w B n_w^{-1} \cap G_i$ przeprowadza wektor e_i na siebie, zaś $G' \simeq B_2^-$ gdy $n_w B n_w^{-1} \cap G_i$ przeprowadza na siebie wektor e_{i+1} .*

Dowód. Podgrupa $n_w B n_w^{-1} \cap G_i$ stabilizuje podprzestrzeń $w^{-1} \text{lin}\{e_i, e_{i+1}\}$ i jest niezmiennicza na prostych $\text{lin}\{n_w^{-1} e_k\}$, gdzie $k \notin \{i, i+1\}$. Stąd $n_w^{-1} \text{lin}\{e_i\} = \text{lin}\{e_k\}$ oraz $n_w^{-1} \text{lin}\{e_{i+1}\} = \text{lin}\{e_l\}$ dla pewnego $k \neq l, 1 \leq k, l \leq n$. Stąd $B \cap w^{-1} G_i w$ trzyma w miejscu albo $\text{lin}\{e_k\}$, albo $\text{lin}\{e_l\}$. Wynika to z definicji podgrupy B . Stąd $n_w B n_w^{-1} \cap G_i$ jest niezmiennicza na podprzestrzeni $\text{lin}\{e_i\}$ lub $\text{lin}\{e_{i+1}\}$. $\square$

Na mocy uwagi 2.16 widzimy, że inkluzja (2.22) przybiera jedną z dwóch postaci:

$$Gl_2(\mathbb{F}_q) \subseteq B_2 \cup B_2 s_i B_2 \quad (2.23)$$

$$Gl_2(\mathbb{F}_q) \subseteq B_2 B_2^- \cup B_2 s_i B_2^-, \quad (2.24)$$

gdzie s_i utożsamiamy z macierzą $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in Gl_2(\mathbb{F}_q)$.

Inkluzję (2.23) dowodzimy w następujący sposób. Jeśli $g \in Gl_2(\mathbb{F}_q) \setminus B_2$, to g jest postaci:

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad c \neq 0. \quad (2.25)$$

Macierze $E_{12}(t)$, gdzie $t \in \mathbb{F}_q$ nie należą do zbioru macierzy opisanych przez (2.25), a więc:

$$E_{12}(-ac^{-1})g = \begin{pmatrix} 0 & * \\ * & * \end{pmatrix}.$$

Stąd już wynika, że:

$$s_i E_{12}(-ac^{-1})g \in \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} g \in B \Rightarrow g \in B_2 s_i B_2.$$

W ten sposób dowiedliśmy inkluzję (2.23), a nawet więcej:

$$Gl_2(\mathbb{F}_q) = B_2 \cup B_2 s_i B_2 \quad (2.26)$$

Inkluzję (2.24) dostajemy zauważając, że $s_i^2 = 1$ oraz $s_i B_2 s_i = B_2^-$. Stąd na mocy (2.26) mamy:

$$Gl_2(\mathbb{F}_q) = Gl_2(\mathbb{F}_q) s_i = B_2 s_i \cup B_2 s_i B_2 s_i \subseteq B_2 s_i \cup B_2 B_2^-.$$

Dostajemy w ten sposób inkluzję (2.24). Zachodzi zatem inkluzja (2.23) lub (2.24), a więc także (2.22). Zatem warunek **(BN4)** jest spełniony.

2.5. Warunek wymiany i prezentacja grupy Weyla

Niewiele miejsca poświęciliśmy dotychczas opisowi grupy Weyla indeksującej warstwy rozkładu Bruhat. Paragraf ten poświęcimy dowodowi następującej jej charakteryzacji.

Twierdzenie 2.17. *Grupa Weyla W generowana jest przez elementy $s_1, s_2, \dots, s_n$ i określa ją zbiór następujących równości:*

$$s_i^2 = 1, \quad 1 \leq i \leq n \quad (2.27)$$

$$(s_i s_j)^{k_{ij}} = (s_j s_i)^{k_{ij}} \quad , \quad o \text{ ile } m_{ij} = 2k_{ij}, \quad i \neq j \quad (2.28)$$

$$(s_i s_j)^{k_{ij}} s_i = (s_j s_i)^{k_{ij}} s_j \quad , \quad o \text{ ile } m_{ij} = 2k_{ij} + 1, \quad i \neq j \quad (2.29)$$

gdzie m_{ij} jest rzędem elementu $s_i s_j$ w W .

Zacniemy od wykazania, że grupa Weyla spełnia równości (2.27)–(2.29). Jest to, jak się okazuje, własność przysługująca każdej grupie skończonej generowanej przez zbiór inwolucji. W dowodzie tego faktu przyda nam się wprowadzenie dodatkowych oznaczeń.

Definicja 2.18. *Niech G będzie grupą skończoną generowaną przez skończony zbiór inwolucji $S = \{s_1, s_2, \dots, s_n\}$. Niech $1 \neq g \in G$. Wówczas przez $\mathcal{R}(g)$ oznaczać będziemy zbiór wszystkich postaci zredukowanych elementu g . Wprowadzamy także następujące oznaczenia:*

$$\begin{aligned} \mathcal{R}(G) &= \bigcup_{g \in G \setminus \{1\}} \mathcal{R}(g) \\ \mathcal{R}_k(G) &= \bigcup_{g \in G: l(g)=k} \mathcal{R}(g), \quad \text{gdzie } k > 1 \end{aligned}$$

Będziemy też mówili, że elementy $x, y \in \mathcal{R}_k(G)$ (czy ogólniej: $x, y \in \mathcal{R}(G)$) są **równe w G** jeśli istnieje $g \in G$, że $x, y \in \mathcal{R}(g)$.

Dowód twierdzenia 2.17 rozpoczniemy od następującego lematu:

Lemat 2.19. *Niech G będzie grupą skończoną generowaną przez parę inwolucji r, s , przy czym rząd elementu rs wynosi m . Niech $1 \neq g \in G$. Wówczas:*

- jeśli m jest liczbą parzystą, równą $2k$, wówczas

$$|\mathcal{R}(g)| > 1 \Leftrightarrow g = (rs)^k = (sr)^k,$$

- jeśli m jest liczbą nieparzystą, równą $2k + 1$, wówczas

$$|\mathcal{R}(g)| > 1 \Leftrightarrow g = (rs)^k r = (sr)^k s.$$

Dowód. Niech $1 \neq g \in G$. Wówczas każdy element $\mathcal{R}(g)$ musi być w jednej z następujących postaci:

$$(rs)^{k_1} \vee (sr)^{k_2} \vee (rs)^{k_3} r \vee (sr)^{k_4} s, \quad (2.30)$$

gdzie $k_1, k_2, k_3, k_4 \in \mathbb{N}$. Istotnie, postać zredukowana $x \in \mathcal{R}(g)$ wyznaczona jest jednoznacznie przez pierwszy element określającego ją słowa (złożonego z liter r, s), ponieważ x jest określonej długości, równej $l(g)$, co więcej x nie może zawierać podśłów postaci rr, ss . Żadne dwa

elementy $\mathcal{R}(g)$ nie mogą się zaczynać tą samą literą. Widać stąd, że $|\mathcal{R}(g)| \leq 2$. Jeśli zachodzi równość, wówczas zgodnie z możliwościami przedstawionymi w (2.30):

$$\mathcal{R}(g) = \{(rs)^{k_1}, (sr)^{k_2}\} \quad \text{albo} \quad \mathcal{R}(g) = \{(rs)^{k_3}r, (sr)^{k_4}s\}, \quad k_1, k_2, k_3, k_4 \in \mathbb{N}.$$

Jeśli $(rs)^{k_1} = (sr)^{k_2}$, to oznaczając przez k rząd elementu rs widzimy, że $k_1 < k$ (inaczej nie byłoby to wyrażenie zredukowane), a także $k_2 < k+1$, zatem $k_1 + k_2 \leq 2k-1$. Mnożąc równość obustronnie przez $(rs)^{k-k_1}$ dostajemy $1 = (rs)^{k-k_1}(rs)^{k_1} = (sr)^{k_1+k_2-k}$. Stąd $k_1 + k_2 = k$. Wiemy, że $l((rs)^{k_1}) = l((sr)^{k_2})$ (elementy te są w $\mathcal{R}(g)$, dla pewnego $g \in G$, muszą mieć zatem identyczną długość, równą $l(g)$). Stąd $k_1 = k_2$. Podobnie rozumiemy w przypadku równości $(rs)^{k_3}r = (sr)^{k_4}s$. Zakładając, że rząd elementu rs to $2k_3+1$, otrzymujemy równość $k_3 = k_4$. $\square$

Widzimy więc, że grupa Weyla spełnia równości (2.27)–(2.29). Zasadniczą trudnością jest pokazanie, że $\langle S | (2.27) - (2.29) \rangle$ jest prezentacją tejże grupy. Warto zaznaczyć, że fakt ten nie znalazł się w pierwszej pracy Titsa dotyczącej BN-par, a został uzasadniony dopiero dwa lata później, niezależnie przez samego Titsa ([Tit64]), jak i (pracującego w tym samym ośrodku, co Bruhat) H. Matsumoto ([Mat64]). W naszych rozważaniach oprzemy się na metodzie wykorzystanej przez Matsumoto. Zaczniemy od następującego lematu technicznego.

Lemat 2.20. *Niech $s \in S$ będzie jednym z generatorów W . Wówczas dla każdego $w \in W$:*

$$l(sw) \geq l(w) \Rightarrow sBw \subseteq BswB \quad (2.31)$$

$$l(sw) \leq l(w) \Rightarrow sBw \cap BwB \neq \emptyset. \quad (2.32)$$

Dowód. Dowodzimy (2.31). Rozumowanie jest indukcją ze względu na $l(w)$.

Dla $l(w) = 0$ teza jest oczywista (w jest jedyneką). Niech $l(w) > 0$. Na mocy uwagi 2.11 istnieje takie $s' \in S$, że $w = w's'$ oraz $l(w') \leq l(w) - 1$. Załóżmy, że teza jest fałszywa dla w . Wówczas na mocy (BN4) mamy:

$$sBw \cap BwB \neq \emptyset \Rightarrow sBw' \cap BwBs' \neq \emptyset. \quad (2.33)$$

Skoro $l(sw) \geq l(w)$ i $sw = sw's'$, to także $l(sw') \geq l(w')$. Inaczej bowiem

$$l(sw) \leq l(sw') + 1 < l(w') + 1 \leq l(w)$$

i dochodzimy do sprzeczności z założeniem indukcyjnym. Jeśli natomiast $l(sw') \geq l(w')$, wówczas z założenia indukcyjnego $sBw' \subseteq Bsw'B$, a więc zgodnie z (2.33) dostajemy:

$$Bsw'B \cap BwBs' \neq \emptyset.$$

Z (BN4) wynika także zawieranie:

$$wBs' \subseteq Bws'B \cup BwB.$$

Warstwa $Bsw'B$ ma niepuste przecięcie ze zbiorem $BwBs'$, zgodnie z (BN4) zawartym w sumie dwóch warstw podwójnych BwB oraz $Bws'B$. Stąd albo $Bsw'B = Bws'B$, albo $Bsw'B = BwB$. Na mocy twierdzenia 2.12 (o rozkładzie Bruhat) oznacza to, że albo zachodzi równość $sw' = ws'$, albo $sw' = w$. Żadna z tych równości nie może mieć jednak miejsca. Istotnie, z równości $sw' = ws'$ wynika, że $sw's' = w \Rightarrow w = sw \Rightarrow s = 1$. Tymczasem rząd elementu s wynosi 2. Jeśli natomiast zachodzi równość $sw' = w$, wówczas $w' = sw$ i, zgodnie

z założeniem indukcyjnym, $l(w') = l(sw) \geq l(w) > l(w')$. Sprzeczność. Skoro zatem nieprawdziwa jest zarówno równość $sw' = ws'$, jak i $sw' = w$, dostajemy ostatecznie sprzeczność z przypuszczeniem, że (2.31) jest nieprawdą.

Dowodzimy (2.32). Korzystając z **(BN4)** widzimy, że $sBs \subseteq B \cup BsB$. Na mocy **(BN3)** mamy więc:

$$sBs \cap BsB \neq \emptyset \Rightarrow sB \cap BsBs \neq \emptyset \Rightarrow sBw \cap BsBsw \neq \emptyset. \quad (2.34)$$

Skoro tymczasem $l(ssw) = l(w) \geq l(sw)$, stąd z (2.31):

$$BsBsw \subseteq BwB. \quad (2.35)$$

Zestawiając (2.34) i (2.35) widzimy, że $sBw \cap BwB \neq \emptyset$. □

Warto zauważyć, że w dowodzie (2.32) po raz pierwszy skorzystaliśmy z aksjomatu **(BN3)**. Jako wniosek dostajemy następujące twierdzenie.

Twierdzenie 2.21. *Niech $w \in W$ oraz $s \in S$. Wówczas:*

$$l(sw) \neq l(w) \quad (2.36)$$

$$l(sw) = l(w) \pm 1 \quad (2.37)$$

$$l(sw) < l(w) \Rightarrow sB \subseteq BwBw^{-1}B. \quad (2.38)$$

Dowód. Gdyby dla pewnych $s \in S, w \in W$ zachodziły jednocześnie (2.31) i (2.32), wówczas $BswB \cap BwB \neq \emptyset$. Zatem na mocy twierdzenia 2.12 (o rozkładzie Bruhat) $sw = w \Rightarrow s = 1$. Tymczasem element s ma rząd 2. To dowodzi (2.36)

Łatwo uzasadnić także równość (2.37). Zauważmy, że jeśli $l(sw) > l(w)$, to na pewno $l(sw) = l(w) + 1$, bo istnieje zapis sw przy pomocy $l(w) + 1$ generatorów. Z (2.36) wiadomo, że $l(sw) \neq l(w)$. Jeśli $l(sw) < l(w) = l(ssw)$, to podobnie jak wyżej, $l(sw) + 1 = l(ssw) = l(w)$.

Inkluzja (2.38) jest natychmiastowym wnioskiem z (2.32). □

Definicja 2.22 (Matsumoto). *Niech W będzie grupą skończoną generowaną przez zbiór $S = \{s_1, s_2, \dots, s_n\}$ elementów rzędu 2. Powiemy, że S spełnia **warunek wymiany**, jeśli:*

$$(l(s_{i_1} \dots s_{i_m}) = m \wedge l(s_{i_0} s_{i_1} \dots s_{i_m}) < m + 1) \Rightarrow \exists k : s_{i_1} \dots s_{i_k} = s_{i_0} \dots s_{i_{k-1}}.$$

Twierdzenie 2.23 (Matsumoto). *Niech W będzie grupą skończoną generowaną przez zbiór $S = \{s_1, s_2, \dots, s_n\}$ elementów rzędu 2 spełniający warunek wymiany. Dla każdej pary (i, j) , $i \neq j$ niech m_{ij} będzie rzędem elementu $s_i s_j$. Wówczas dla $i \neq j$ spełnione są równości (2.28) i (2.29).*

Niech M będzie monoidem z jednością e zawierającym zbiór elementów $\{m_1, \dots, m_n\}$ spełniających równości¹³ (2.28) i (2.29). Istnieje wówczas przekształcenie $f : W \rightarrow M$ takie, że:

$$f(1) = e, \quad f(s_i) = m_i, \quad f(s_{i_1} \dots s_{i_s}) = m_{i_1} \dots m_{i_s}, \quad (2.39)$$

gdzie $1 \leq i \leq n$, oraz $s_{i_1} \dots s_{i_s} \in \mathcal{R}(W)$.

¹³Chodzi oczywiście o analogiczne równości, tj. takie, że w (2.28), (2.29) zamiast s_i piszemy m_i , dla $1 \leq i \leq n$. Liczby m_{ij} są rzędami elementów $s_i s_j$ w W .

Zanim przystąpimy do dowodu poczynimy w tym miejscu krótki komentarz. Aby uzasadnić, że $\langle s_1, s_2, \dots, s_n \mid (2.27) - (2.29) \rangle$ jest prezentacją grupy Weyla, trzeba wziąć dowolną grupę G zawierającą elementy $g_1, g_2, \dots, g_n$ spełniające równości (2.27)–(2.29) i wykazać, że istnieje homomorfizm $f : W \rightarrow G$ zadany wzorem $f(s_i) = g_i$, $1 \leq i \leq n$. Funkcja $f : W \rightarrow M$ występująca w tezie twierdzenia Matsumoto nie jest homomorfizmem monoidów. Wiemy o niej tylko tyle, że „przenosi” do M wszystkie postaci zredukowane elementów z W . Jak się dalej okaże, korzystając z twierdzenia 2.21 dowodzi się, że w przypadku grupy Weyla W przekształcenie opisane w twierdzeniu Matsumoto jest, dla $M = G$, homomorfizmem grup. By móc skorzystać z twierdzenia Matsumoto będziemy musieli oczywiście wykazać, że generatory grupy Weyla spełniają warunek wymiany.

Dowód. (Twierdzenie Matsumoto)

Naszym celem jest wykazanie, że przekształcenie $f : W \rightarrow M$, opisane zgodnie z (2.39), jest dobrze określone, tj. jeśli dwa elementy $\mathcal{R}(W)$ są równe w W :

$$s_{j_1} \dots s_{j_l} = s_{i_1} \dots s_{i_l}, \quad (2.40)$$

wówczas:

$$m_{j_1} \dots m_{j_l} = m_{i_1} \dots m_{i_l}. \quad (2.41)$$

Dowód będzie indukcją ze względu na ze względu na długość równych w W elementów $\mathcal{R}(W)$. Dla elementów $\mathcal{R}_1(W)$ teza wynika z definicji funkcji f . Bierzemy $l > 1$ i zakładamy, że dla $t < l$ funkcja f jest dobrze określona dla wszystkich równych w W par elementów ze zbiorów $\mathcal{R}_t(W)$. Weźmy parę równych w W elementów $\mathcal{R}_l(W)$, tak jak w równości (2.40):

$$s_{j_1} \dots s_{j_l} = s_{i_1} \dots s_{i_l}.$$

Mnożąc z lewej strony przez s_{j_1} dostajemy:

$$s_{j_2} \dots s_{j_l} = s_{j_1} s_{i_1} \dots s_{i_l}.$$

Widać, że $l(s_{j_1} s_{i_1} \dots s_{i_l}) < l + 1$, zatem zgodnie z warunkiem wymiany istnieje liczba k , gdzie $1 \leq k \leq l$, że:

$$s_{j_1} s_{i_1} \dots s_{i_{k-1}} = s_{i_1} \dots s_{i_k}. \quad (2.42)$$

Wstawiając (2.42) do (2.40) dostajemy:

$$s_{j_1} \dots s_{j_l} = (s_{i_1} \dots s_{i_k}) \dots s_{i_l} = (s_{j_1} s_{i_1} \dots \widehat{s_{i_k}}) \dots s_{i_l}, \quad (2.43)$$

gdzie symbol $\widehat{s_{i_k}}$ oznacza brak czynnika s_{i_k} . Skracając s_{j_1} uzyskujemy:

$$s_{j_2} \dots s_{j_l} = s_{i_1} \dots \widehat{s_{i_k}} \dots s_{i_l}.$$

Zauważmy, że $s_{j_2} \dots s_{j_l} \in \mathcal{R}_{l-1}(W)$. Istotnie, zgodnie z (2.37)

$$l - 1 \geq l(s_{j_2} \dots s_{j_l}) = l(s_{j_1} (s_{j_1} s_{j_2} \dots s_{j_l})) = l(s_{j_1} s_{j_2} \dots s_{j_l}) \pm 1 = l \pm 1.$$

Wynika stąd, że także $s_{i_1} \dots \widehat{s_{i_k}} \dots s_{i_l} \in \mathcal{R}_{l-1}(W)$. Z założenia indukcyjnego mamy zatem:

$$m_{j_2} \dots m_{j_l} = m_{i_1} \dots \widehat{m_{i_k}} \dots m_{i_l}.$$

Po domnożeniu (półgrupowym) stronami przez m_{j_1} dostajemy:

$$m_{j_1} \dots m_{j_l} = m_{j_1} m_{i_1} \dots \widehat{m_{i_k}} \dots m_{i_l}. \quad (2.44)$$

Chcemy wykazać formułę (2.41). Pozostaje zatem dowieść, że:

$$m_{i_1} \dots m_{i_l} = m_{j_1} m_{i_1} \dots \widehat{m_{i_k}} \dots m_{i_l}.$$

Rozumowanie rozbijamy na dwa przypadki:

- Niech $k < l$. Wówczas równość (2.42) przybiera postać:

$$s_{j_1} s_{i_1} \dots s_{i_{k-1}} = s_{i_1} \dots s_{i_k}.$$

Jest to równość w $\mathcal{R}_k(W)$. W przeciwnym razie mielibyśmy sprzeczność z założeniem, że (2.40) jest równością pomiędzy elementami z $R_l(W)$. Z założenia indukcyjnego:

$$m_{i_1} \dots m_{i_k} = m_{j_1} m_{i_1} \dots m_{i_{k-1}}. \quad (2.45)$$

Podstawiając (2.45) do (2.44) dostajemy tezę:

$$m_{i_1} \dots m_{i_l} = m_{j_1} \dots m_{j_l}.$$

- Niech $k = l$. Równość (2.43) przybiera wówczas postać:

$$s_{j_1} s_{i_1} \dots s_{i_{l-1}} = s_{i_1} \dots s_{i_l}. \quad (2.46)$$

Równość (2.44) przybiera natomiast równość:

$$m_{j_1} m_{i_1} \dots m_{i_{l-1}} = m_{j_1} \dots m_{j_l}.$$

Teza sprowadza się zatem do wykazania równości:

$$m_{j_1} m_{i_1} \dots m_{i_{l-1}} = m_{i_1} \dots m_{i_l}$$

Podsumowując te rozważania widzimy, że implikacja:

$$s_{j_1} \dots s_{j_l} = s_{i_1} \dots s_{i_l} \Rightarrow m_{j_1} \dots m_{j_l} = m_{i_1} \dots m_{i_l} \quad (2.47)$$

jest nieprawdziwa tylko wtedy, gdy nieprawdziwa jest implikacja:

$$s_{i_1} \dots s_{i_l} = s_{j_1} s_{i_1} \dots s_{i_{l-1}} \Rightarrow m_{i_1} \dots m_{i_l} = m_{j_1} m_{i_1} \dots m_{i_{l-1}}. \quad (2.48)$$

Intuicyjnie poprzednik implikacji (2.48) „powstaje” z poprzednika implikacji (2.47) w wyniku trzech „operacji”:

- poprzez przeniesienie całej prawej strony poprzednika (2.47) na lewą stronę poprzednika (2.48) – tj. przez zamianę $s_{j_1} \dots s_{j_l}$ na $s_{i_1} \dots s_{i_l}$,
- poprzez dopisanie do prawej strony poprzednika (2.47) pierwszego z generatorów stojących po lewej stronie poprzednika (2.47) – tj. przez dopisanie do $s_{i_1} \dots s_{i_l}$ generatora s_{j_1} (z lewej strony),
- poprzez wymazanie ostatniego generatora z prawej strony poprzednika (2.47) – tj. zamiast $s_{j_1} s_{i_1} \dots s_{i_l}$ dostajemy $s_{j_1} s_{i_1} \dots s_{i_{l-1}}$.

Prowadząc analogiczne rozumowanie¹⁴ widzimy, że implikacja (2.48) ostatnia implikacja jest nieprawdziwa tylko wtedy, gdy nieprawdziwa jest implikacja:

$$s_{j_1}s_{i_1}\dots s_{i_{l-1}} = s_{i_1}s_{j_1}s_{i_1}\dots s_{i_{l-2}} \Rightarrow m_{j_1}m_{i_1}\dots m_{i_{l-1}} = m_{i_1}m_{j_1}m_{i_1}\dots m_{i_{l-2}}.$$

Powyższa implikacja jest nieprawdziwa tylko wtedy, gdy nieprawdziwa jest implikacja:

$$s_{i_1}s_{j_1}s_{i_1}\dots s_{i_{l-2}} = s_{j_1}s_{i_1}s_{j_1}s_{i_1}\dots s_{i_{l-3}} \Rightarrow m_{i_1}m_{j_1}m_{i_1}\dots m_{i_{l-2}} = m_{j_1}m_{i_1}m_{j_1}m_{i_1}\dots m_{i_{l-3}},$$

Warto odnotować, że w poprzednikach wszystkich wymienionych tu implikacji znajdują się równości pomiędzy elementami $\mathcal{R}(W)$ (dowód analogiczny jak w przypadku poprzednika (2.48)).

Kontynuujemy to rozumowanie i widzimy, że ostatecznie teza kroku indukcyjnego jest nieprawdziwa tylko wtedy, gdy nieprawdziwa jest implikacja:

$$s_{i_1}s_{j_1}s_{i_1}\dots = s_{j_1}s_{i_1}s_{j_1}\dots \Rightarrow m_{i_1}m_{j_1}m_{i_1}\dots = m_{j_1}m_{i_1}m_{j_1}\dots, \quad (2.49)$$

gdzie $s_{i_1}s_{j_1}s_{i_1}\dots, s_{j_1}s_{i_1}s_{j_1}\dots \in \mathcal{R}(w)$, gdzie $w \in \langle s_{i_1}, s_{j_1} \rangle \leq W$.

W tym miejscu korzystamy z lematu 2.19. Elementy $\mathcal{R}(\langle s_{i_1}, s_{j_1} \rangle)$ są równe w $\langle s_{i_1}, s_{j_1} \rangle$ (def. 2.18) wtedy i tylko wtedy, gdy wiążą je równości postaci (2.28) oraz (2.29). Założyliśmy jednak, że analogiczne równości spełnione są także przez elementy $\{m_1, \dots, m_n\}$. Zatem (2.49) jest prawdą, a wraz z nią także (2.47). Krok indukcyjny został zatem zakończony. $\square$

Twierdzenie 2.24. *Niech G będzie skończonym systemem Titsa, zaś W związaną z nim podgrupą Weyla generowaną przez zbiór $S = \{s_1, \dots, s_n\}$. Zbiór S spełnia warunek wymiany.*

Dowód. Zaczniemy od dowodu pewnego uogólnienia aksjomatu (BN4).

Lemat 2.25. *Niech $w \in W$ i niech $w' = s_{j_1}s_{j_2}\dots s_{j_p}$ będzie iloczynem generatorów ze zbioru S . Wówczas:*

$$wBw' \subseteq \bigcup Bws_{j_{q_1}}s_{j_{q_2}}\dots s_{j_{q_t}}B, \quad (2.50)$$

gdzie suma wzięta jest po wszystkich podciągach rosnących postaci $1 \leq q_1 < q_2 < \dots < q_t \leq p$ oraz ciągu pustym.¹⁵

Dowód. Indukcja po p . Wykorzystując dwukrotnie (BN 4) widzimy, że:

$$\begin{aligned} wBs_1s_2 &\subseteq B(ws_2) \cup B(ws_1Bs_2) \\ &\subseteq B(BwB) \cup B(Bws_2B) \cup B(Bws_1B) \cup B(Bws_1s_2B). \end{aligned}$$

Podobnie jeśli założymy, że dla $p > 2$ mamy:

$$wBs_{j_1}s_{j_2}\dots s_{j_p} \subseteq \bigcup Bws_{j_{q_1}}s_{j_{q_2}}\dots s_{j_{q_t}}B,$$

wówczas:

$$\begin{aligned} (wBs_{j_1}s_{j_2}\dots s_{j_p})s_{j_{p+1}} &\subseteq \bigcup B(ws_{j_{q_1}}s_{j_{q_2}}\dots s_{j_{q_t}}Bs_{j_{p+1}}) \\ &\subseteq \bigcup B(Bws_{j_{q_1}}s_{j_{q_2}}\dots s_{j_{q_t}}B) \cup B(Bws_{j_{q_1}}s_{j_{q_2}}\dots s_{j_{q_t}}s_{j_{p+1}}B). \end{aligned}$$

Dostajemy w ten sposób sumę po wszystkich rosnących podciągach ciągu $(1, 2, \dots, p+1)$. $\square$

¹⁴Według podanej wyżej intuicji stosujemy podaną „modyfikację” po raz kolejny.

¹⁵Składnikiem sumy (2.50) jest także BwB .

Pokażemy teraz, że zbiór generatorów grupy Weyla spełnia warunek wymiany. Niech $w = s_{i_1} s_{i_2} \dots s_{i_m}$, gdzie $l(w) = m$ oraz niech $l(s_{i_0} w) < m + 1$. Warunek wymiany będzie spełniony jeśli znajdziemy takie $k, 1 \leq k \leq m$, że $s_{i_1} \dots s_{i_k} = s_{i_0} \dots s_{i_{k-1}}$. Korzystając z (2.36) widzimy, że $l(s_{i_0} w) < l(w)$, zatem z (2.38):

$$s_{i_0} B \subseteq B w B w^{-1} B. \quad (2.51)$$

Skorzystamy teraz z lematu 2.25. Zauważmy, że $w^{-1} = s_{i_m} s_{i_{m-1}} \dots s_{i_2} s_{i_1}$. Stąd:

$$B w B w^{-1} B \subseteq \bigcup B w s_{j_{q_1}} s_{j_{q_2}} \dots s_{j_{q_t}} B, \quad (2.52)$$

gdzie

$$m \geq q_1 > q_2 > \dots > p_t \geq 1.$$

Mnożąc (2.51) z lewej strony przez B widzimy, że $B s_{i_0} B$ leży w sumie warstw podwójnych znajdujących się po prawej stronie inkluzji (2.52). Korzystając zatem z twierdzenia 2.12 (o rozkładzie Bruhat) dostajemy, że:

$$s_{i_0} = w s_{j_{q_1}} s_{j_{q_2}} \dots s_{j_{q_t}},$$

dla pewnego podciągu malejącego $\{q_i\}$, $1 \leq i \leq t$ ciągu $(m, m-1, \dots, 1)$. Skoro $l(s_{i_0}) = 1$ oraz $l(ws) = l(w) \pm 1$ (na mocy (2.37)), to $t = m - 1$, a więc:

$$s_{i_0} = w s_{i_m} \dots \widehat{s_{i_j}} \dots s_{i_1},$$

gdzie jeden z czynników (o indeksie i_j) został pominięty. Wstawiając $w = s_{i_1} s_{i_2} \dots s_{i_m}$ dostajemy:

$$\begin{aligned} s_{i_0} &= (s_{i_1} \dots s_{i_m}) (s_{i_m} \dots \widehat{s_{i_j}} \dots s_{i_1}) \\ &= s_{i_1} \dots s_{i_{j-1}} s_{i_j} s_{i_{j-1}} \dots s_{i_1} \\ &= s_{i_1} \dots s_{i_{j-1}} s_{i_j} (s_1 \dots s_{i_{j-1}})^{-1}. \end{aligned}$$

Mnożąc z prawej strony przez $s_1 \dots s_{i_{j-1}}$ dostajemy zatem warunek wymiany:

$$s_{i_0} \dots s_{i_{j-1}} = s_1 \dots s_{i_j}.$$

□

Dowód. (Twierdzenie 2.17)

Wiemy, że grupa Weyla spełnia równości (2.27)–(2.29). Niech G będzie dowolną grupą zawierającą zbiór elementów $\{g_1, \dots, g_n\}$ spełniających w G równości analogiczne¹⁶ do (2.27)–(2.29). Generatory grupy Weyla spełniają warunek wymiany, zatem na mocy twierdzenia Matsumoto istnieje przekształcenie $f : W \rightarrow G$ takie, że $f(1_W) = 1_G$, $f(s_i) = g_i$, dla $1 \leq i \leq n$ oraz

$$f(s_{i_1} s_{i_2} \dots s_{i_m}) = g_{i_1} g_{i_2} \dots g_{i_m}, \quad (2.53)$$

dla wszystkich postaci zredukowanych $s_{i_1} s_{i_2} \dots s_{i_m}$. Jeśli udowodnimy, że f jest homomorfizmem, wówczas dowód twierdzenia 2.17 będzie zakończony. Wystarczy więc wykazać, że:

$$f(sw) = f(s)f(w), \quad s \in S, w \in W. \quad (2.54)$$

¹⁶W równościach (2.27)–(2.29) zamiast s_i wstawiamy g_i , $1 \leq i \leq n$.

Niech $w = s_{i_1} s_{i_2} \dots s_{i_m}$, $s_{i_j} \in S$, przy czym $l(w) = m$. Łatwo widzieć, że (2.53) jest spełnione, gdy $l(sw) > l(w)$. Istotnie, w takim przypadku także postać $ss_{i_1} s_{i_2} \dots s_{i_m}$ jest zredukowana i teza wynika z (2.52).

Jeśli natomiast założymy, że $l(sw) < l(w)$, wówczas także $l(sw) < l(ssw)$. Zatem $f(ssw) = f(s)f(sw)$. Zarówno s , jak i $f(s)$ są inwolucjami, zatem

$$f(s)f(w) = f(s)f(ssw) = f(sw),$$

co kończy dowód. □

* * *

Podsumujmy wyniki zebrane w tym rozdziale. Pokazaliśmy, że jeśli rozważamy rozkład grupy G na warstwy podwójne względem podgrupy H , wówczas w ściśle określonych warunkach warstwy tego rozkładu indeksowane są przez grupę generowaną przez skończony zbiór inwolucji. Zasadniczym przykładem jest rozkład grupy macierzy odwracalnych $GL_n(\mathbb{K})$ na warstwy podwójne względem podgrupy macierzy górnotrójkątnych $B_n(\mathbb{K})$. Rozkład ten indeksowany był przez grupę permutacji zbioru n -elementowego. Zaobserwowanie takich rozkładów, najpierw w klasie grup Liego, potem w klasie grup algebraicznych, wreszcie natomiast w klasie systemów Titsa, miało istotny wpływ na postęp w pracach nad problemem klasyfikacji skończonych grup prostych w latach 50' i 60' XX. wieku.¹⁷

¹⁷Szersze omówienie tego zagadnienia znaleźć można np. w artykule przeglądowym Curtisa [Cur67].

Rozdział 3

Algebry Hecke

W naszych dotychczasowych rozważaniach przyglądaliśmy się zjawisku rozkładu Bruhat, występującym zarówno w klasycznym przypadku grupy macierzy odwracalnych nad ciałem, jak i w ogólnym środowisku systemów Titsa. Celem tego rozdziału jest prezentacja związku pomiędzy systemem Titsa G , a odpowiadającą mu grupą Weyla W .

W ciągu całego tego rozdziału zakładamy, że G jest skończoną grupą z BN-parą, zaś W jest odpowiadającą G podgrupą Weyla generowaną przez skończony zbiór inwolucji S . Zgodnie z twierdzeniem 2.12 rozpatrywać można rozkład Bruhat grupy G na warstwy podwójne względem B postaci:

$$G = \bigsqcup_{w \in W} BwB.$$

Będziemy czasem mówili, że B jest podgrupą Borela w G , przyjmując te nazewnictwo jako naturalne uogólnienie przypadku znanego z teorii grup algebraicznych. Warstwy podwójne grupy G względem podgrupy B nazywać będziemy krótko (B, B) -warstwami.

Rozważmy zbiór funkcji: $\mathcal{F}_{\mathbb{C}}(G) = \{f \mid f : G \rightarrow \mathbb{C}\}$. Zbiór ten można, zgodnie z rozważaniami poczynionymi w paragrafie 1.2¹, wyposażyć w strukturę $\mathbb{C}$ -algebry, w której mnożenie zdefiniowane jest przez spłot² za pomocą formuły (1.13). Uzyskujemy w ten sposób algebrę izomorficzną z algebrą grupową $\mathbb{C}[G]$.

Interesuje nas opis takiego podzbioru $\mathcal{F}_{\mathbb{C}}(G, B) \subset \mathcal{F}_{\mathbb{C}}(G)$, który zawiera funkcje stałe na (B, B) -warstwach rozkładu Bruhat grupy G . Zgodnie z utożsamieniem (1.11) $\mathcal{F}_{\mathbb{C}}(G, B)$ odpowiada pewien podzbiór $\mathcal{H}_{\mathbb{C}}(G, B) \subseteq \mathbb{C}[G]$. Wykażemy dalej, że $\mathcal{H}_{\mathbb{C}}(G, B)$ jest podalgebrą algebry $\mathbb{C}[G]$. Celem tego rozdziału jest dowód twierdzenia Titsa mówiącego, że

$$\mathcal{H}_{\mathbb{C}}(G, B) \simeq \mathbb{C}[W], \tag{3.1}$$

gdzie W jest podgrupą Weyla grupy G .

* * *

Uzasadnimy teraz, że $\mathcal{H}_{\mathbb{C}}(G, B)$ jest w istocie podalgebrą algebry $\mathbb{C}[G]$. Przypomnijmy, że zgodnie z (1.10) każdemu elementowi $x \in \mathbb{C}[G]$ odpowiada w sposób jednoznaczny element

¹Komentarz do definicji 1.18.

²Istotne jest tu założenie, że G jest grupą skończoną.

$\Phi(x) \in \mathcal{F}_{\mathbb{C}}(G)$. Podobnie każdej funkcji $f \in \mathcal{F}_{\mathbb{C}}(G)$ odpowiada element $\Psi(f) \in \mathbb{C}[G]$. Z odpowiedniości pomiędzy $\mathbb{C}[G]$ i $\mathcal{F}_{\mathbb{C}}(G)$ będziemy teraz korzystać.

Przy tej okazji wprowadzimy też wygodną dla dalszych rozważań notację. Niech G będzie grupą skończoną i $H \subseteq G$. Wówczas:

$$[H] := \sum_{h \in H} h \in \mathbb{C}[G].$$

Jeśli $H \leq G$, wówczas $[H]$ utożsamiać można z elementem $\mathbb{C}[H]$.

Lemat 3.1. *Niech G będzie skończoną grupą z BN-parą. Wówczas $\mathcal{H}_{\mathbb{C}}(G, B)$ jest podalgebrą w $\mathbb{C}[G]$. Co więcej:*

$$\mathcal{H}_{\mathbb{C}}(G, B) \simeq e_B \mathbb{C}[G] e_B,$$

gdzie $e_B \in \mathbb{C}[B]$ jest centralnym idempotentem odpowiadającym charakterowi trywialnemu grupy B .

Dowód. Na podstawie (1.16) wiemy, że e_B dany jest wzorem:

$$e_B = \chi(1)|B|^{-1} \sum_{x \in B} \chi(x^{-1})x = |B|^{-1} \sum_{x \in B} x = |B|^{-1}[B]. \quad (3.2)$$

Zgodnie z utożsamieniem (1.10), elementowi $e_B \in \mathbb{C}[G]$ odpowiada funkcja $\Phi(e_B) : \mathbb{C} \rightarrow G$. W dowodzie będziemy kilkakrotnie korzystali z formuły (1.12) mówiącej, że Φ i Ψ są wzajemnie odwrotnymi bijekcjami zbiorów, oraz z formuły (1.14) mówiącej, że Φ i Ψ są homomorfizmami algebr.

Rozważmy zbiór:

$$\Phi(e_B) \star \mathcal{F}_{\mathbb{C}}(G) \star \Phi(e_B) := \{f \in \mathcal{F}_{\mathbb{C}}(G) \mid f = \Phi(e_B) \star f' \star \Phi(e_B), f' \in \mathcal{F}_{\mathbb{C}}(G)\}.$$

Wykażemy, że zachodzi następująca równość zbiorów:

$$\Phi(e_B) \star \mathcal{F}_{\mathbb{C}}(G) \star \Phi(e_B) = \mathcal{F}_{\mathbb{C}}(G, B). \quad (3.3)$$

Rozważmy element $x = \sum_{g \in G} a_g g \in \mathbb{C}[G]$. Jeśli wykażemy, że $\Phi(e_B) \star \Phi(x) \star \Phi(e_B) \in \mathcal{F}_{\mathbb{C}}(G, B)$, otrzymamy wówczas jedną z inkluzji w postulowanej przez nas równości (3.3).

Jeśli $B = \{b_1, b_2, \dots, b_n\}$, wówczas funkcji $|B|^2 \cdot \Phi(e_B) \star \Phi(x) \star \Phi(e_B)$ odpowiada:

$$\begin{aligned} \Psi(|B|^2 \cdot \Phi(e_B) \star \Phi(x) \star \Phi(e_B)) &\stackrel{(1.14)}{=} |B|^2 \cdot \Psi(\Phi(e_B)) \Psi(\Phi(x)) \Psi(\Phi(e_B)) = \\ &\stackrel{(1.12)}{=} |B|^2 \cdot e_B x e_B = [B]x[B] = \\ &= \sum_{g \in G} a_g \left(\sum_{1 \leq i, j \leq n} b_i g b_j \right). \end{aligned}$$

Wśród elementów postaci $b_i g b_j$ pewne mogą być sobie równe. Innymi słowy, nie każdy element $x \in G$ musi się przedstawiać jednoznacznie jako $x = b_i g b_j$, dla pewnych $g \in G$, $1 \leq i, j \leq n$. Wiemy jednak, że zgodnie z wzorem (2.1) grupa $B \times B$ działa na G . Z podstawowego kursu teorii grup wiadomo, że jeśli grupa skończona A działa na zbiorze X , to dla $x \in X$ moc

orbity Ax równa jest ilorazowi $|A|/|A_x|$, gdzie $A_x = \{a \in A \mid ax = x\}$ jest podgrupą izotropii elementu x . W szczególności, jeśli przez s_g oznaczymy moc podgrupy izotropii elementu g przy działaniu $B \times B$ na G , wówczas otrzymamy:

$$|B|^2 \cdot e_B x e_B = [B]x[B] = \sum_{g \in G} a_g s_g [BgB].$$

Dowodzi to, że $\Phi(e_B) \star \Phi(x) \star \Phi(e_B) \in \mathcal{F}_{\mathbb{C}}(G, B)$. Istotnie, jeśli dwa elementy g_1, g_2 grupy G są w tej samej (B, B) -warstwie BgB , wówczas:

$$(\Phi(e_B) \star \Phi(x) \star \Phi(e_B))(g_1) = (\Phi(e_B) \star \Phi(x) \star \Phi(e_B))(g_2) = a_g s_g.$$

Odwrotnie, jeśli funkcja $f : G \rightarrow \mathbb{C}$ jest stała na (B, B) -warstwach, a więc należy do $\mathcal{F}_{\mathbb{C}}(G, B)$, wówczas zgodnie z (1.11) w $\mathbb{C}[G]$ odpowiada jej element postaci:

$$\Psi(f) = \sum_{g \in G} a_g [BgB] = \sum_{g \in G} \frac{a_g}{s_g} \left(\sum_{1 \leq i, j \leq n} b_i g b_j \right) = |B|^2 \cdot e_B \left(\sum_{g \in G} \frac{a_g}{s_g} g \right) e_B,$$

gdzie $a_g \in \mathbb{C}$, zaś s_g jest rzędem podgrupy izotropii elementu $g \in G$ przy działaniu $B \times B$ na G . Jeśli przyjmiemy $x = \sum_{g \in G} \frac{|B|^2 \cdot a_g}{s_g} g \in \mathbb{C}[G]$ wówczas, zgodnie z (1.12) i (1.14) dostajemy:

$$f = \Phi(\Psi(f)) = \Phi(e_B x e_B) = \Phi(e_B) \star \Phi(x) \star \Phi(e_B).$$

W ten sposób dowiedliśmy (3.3).

Zgodnie z (1.14) przekształcenia Φ, Ψ są wzajemnie odwrotnymi homomorfizmami algebr. Stąd:

$$\Phi(e_B \mathbb{C}[G] e_B) = \Phi(e_B) \star \mathcal{F}_{\mathbb{C}}(G) \star \Phi(e_B) = \mathcal{F}_{\mathbb{C}}(G, B),$$

czyli ostatecznie, zgodnie z definicją $\mathcal{H}_{\mathbb{C}}(G, B)$, dostajemy:

$$e_B \mathbb{C}[G] e_B = \Psi(\Phi(e_B \mathbb{C}[G] e_B)) = \Psi(\mathcal{F}_{\mathbb{C}}(G, B)) = \mathcal{H}_{\mathbb{C}}(G, B).$$

Wiadomo, że $e_B \mathbb{C}[G] e_B$ jest podalgebrą w $\mathbb{C}[G]$, zatem także $\mathcal{H}_{\mathbb{C}}(G, B)$ jest podalgebrą w $\mathbb{C}[G]$, co kończy dowód. □

Definicja 3.2 (Algebra Hecke). *Podalgebrę $\mathcal{H}_{\mathbb{C}}(G, B)$ algebry $\mathbb{C}[G]$ określoną w lemacie 3.1 nazywamy **algebrą Hecke** systemu Titsa G .*

Uwaga 3.3. $\mathcal{H}_{\mathbb{C}}(G, B)$ jest algebrą półprostą.

Dowód. Teza wynika natychmiast z twierdzenia 1.17. □

Pojęcie „algebry Hecke” pojawiało się w matematyce stopniowo.³ Sama idea przejścia od rozważania własności pierścienia R , do własności pierścienia eRe , gdzie $e = e^2 \in R$, pochodzi od Schura i sięga początków XX wieku. Oryginalne motywacje leżące u podstaw omawianej tu teorii związane są jednak z osobą niemieckiego matematyka Ericha Hecke’go. Jest on znany głównie z wyników w algebraicznej teorii liczb. Z jego nazwiskiem związane jest zasadnicze dla teorii form modularnych pojęcie tzw. operatora Hecke⁴, wprowadzonego w [Hec37].

³Dokładniejszy zarys historyczny znaleźć można w [Sol90].

⁴Przykładowym źródłem są tu rozdziały II. i III. monografii Langa, [Lan76].

Gdy termin „pierścień Hecke” pojawił się po raz pierwszy w pracach G. Shimury ([Shi59]) i T. Tamagawy ([Tam63]), dotyczył on właśnie zagadnień związanych z tym operatorem, a przynależących raczej do analitycznej teorii liczb i teorii form modularnych.

Pierwsza istotna praca dotycząca „pierścieni Hecke”, związana w sposób bezpośredni z pojęciem określonym w 3.2, a więc z funkcjami stałymi na warstwach podwójnych pewnych grup⁵, pochodzi od Iwahoriego ([Iwa64]). Wiele z uzyskanych w tej pracy wyników okazało się kluczowymi dla zastosowań nie leżących już w obrębie teorii liczb. Algebry Hecke okazały się bowiem przydatnym narzędziem dla stosunkowo różnych od siebie dziedzin matematyki.⁶ Poniżej wymieniamy kilka z nich.

- Teoria reprezentacji tzw. skończonych grup typu Lie ([Cur87], rozdział 8). Związek wyrażony w (3.1) pozwala na zrozumienie związku pomiędzy teorią reprezentacji $\mathbb{C}[G]$ i $\mathbb{C}[W]$. W przypadku omówionym w paragrafie 2.4, a więc gdy G jest grupą macierzy odwracalnych nad ciałem skończonym, twierdzenie to daje ważny związek⁷ pomiędzy teorią reprezentacji grupy permutacji zbioru skończonego ([Ful08], rozdział 4.) i teorią reprezentacji grupy macierzy odwracalnych nad ciałem p-elementowym ([Ful08], rozdział 6).
- Teoria węzłów, gdzie zasadniczą rolę gra tzw. wielomian Jonesa. Do definicji tego obiektu Vaughn Jones wykorzystał algebry Hecke. ([Jon87]).
- Algebry Temperleya-Lieba. Występują one w teorii węzłów, fizyce statystycznej oraz fizyce kwantowej. Pojęcie algebry Hecke było ważnym elementem na drodze do odkrycia tzw. grup kwantowych. Zasadniczym odnośnikiem z tej tematyki jest praca Jimbo [Jim86].

Rozdział ten poświęcimy, zgodnie z wcześniejszą zapowiedzią, dowodowi twierdzenia Titsa orzekającego izomorfizm (3.1). Nie jest to wynik elementarny, dlatego na drodze do pełnego dowodu zaprezentujemy szereg własności algebr Hecke. I tak w kolejnych paragrafach przedstawimy:

- w paragrafie 3.1 – opis generatorów i stałych strukturalnych algebry $\mathcal{H}_{\mathbb{C}}(G, B)$,
- w paragrafie 3.2 – opis algebry Hecke przy pomocy generatorów i relacji,
- w paragrafie 3.3 – pojęcie algebry generycznej systemu Titsa,
– dowód twierdzenia Titsa o deformacji,
- w paragrafie 3.4 – dowód wzoru (3.1).

W naszych rozważaniach opieramy się na [Cur81] i [Cur87].

⁵Są to wówczas jeszcze, podobnie jak we wcześniejszych pracach Hecke’a i innych, grupy nieskończone, na których określona jest miara Haara pozwalająca na stosowanie splotu.

⁶Istnieją też zastosowania algebr Hecke w informatyce. Przykładem jest praca Diaconisa, [Dia00].

⁷Nie był to oczywiście pierwszy wynik tego typu. Teoria reprezentacji $GL_n(\mathbb{F}_p)$ od początku związana była z teorią reprezentacji S_n . Relacja ta znana jest dziś pod nazwą odpowiedniości Schura-Weyla.

3.1. Generatory i stałe strukturalne w $\mathcal{H}_{\mathbb{C}}(G, B)$

Naszym pierwszym celem będzie wykazanie, że $\mathcal{H}_{\mathbb{C}}(G, B)$ posiada bazę $\{a_{w_i} \mid 1 \leq i \leq |W|\}$. Wyznamy też **stałe strukturalne** $\mathcal{H}_{\mathbb{C}}(G, B)$, a więc takie liczby zespolone μ_{ijk} , że:

$$a_{w_i} a_{w_j} = \sum_{k=1}^{|W|} \mu_{ijk} a_{w_k}, \quad 1 \leq i, j \leq |W|.$$

Definicja 3.4. Niech G będzie skończonym systemem Titsa, B – podgrupą Borela. Wówczas dla każdego $x \in G$ określamy **indeks x w B** poprzez:

$$\text{ind}(x) = |B : (xBx^{-1} \cap B)|.$$

Łatwo sprawdzić, że $\text{ind}(x)$ opisuje liczbę warstw lewostronnych (lub prawostronnych) grupy B zawartych w warstwie podwójnej BxB . Istotnie, jeśli $A \subseteq G$ oraz dla każdego $a \in A$ warstwa Ba zawarta jest w A , wówczas A jest sumą pewnych warstw lewostronnych Bx . Zbiór takich warstw oznaczmy przez $(B \setminus A)$. Rozważmy przekształcenie zbiorów

$$\phi : (xBx^{-1} \cap B \setminus B) \rightarrow (B \setminus BxB)$$

zadane wzorem:

$$\phi((xBx^{-1} \cap B)b) = Bxb, \quad b \in B.$$

Przekształcenie to jest dobrze określone. Istotnie, jeśli $b, b' \in B$ wówczas:

$$(xBx^{-1} \cap B)b = (xBx^{-1} \cap B)b' \Leftrightarrow b'b^{-1} \in xBx^{-1} \cap B \Leftrightarrow b'b^{-1} \in x^{-1}Bx \Leftrightarrow Bxb' = Bxb.$$

Powyższy rachunek pokazuje jednocześnie, że przekształcenie to jest injekcją. Moc dziedziny tego przekształcenia to dokładnie $\text{ind}(x)$. Aby pokazać, że $\text{ind}(x) = |(B \setminus BxB)|$ wystarczy wykazać, że ϕ jest surjekcją. Ponieważ jednak Bxb jest warstwą lewostronną, zawiera się ona w BxB . Każdą warstwę lewostronną uzyskujemy w ten sposób.

Uzyskaliśmy zatem formułę:

$$\text{ind}(x) = |(B \setminus BxB)| = \frac{|BxB|}{|B|}. \quad (3.4)$$

Wynika stąd, że jeśli elementy $x_1, x_2 \in BxB$, wtedy $\text{ind}(x_1) = \text{ind}(x_2)$. Funkcja ind jest zatem stała na (B, B) -warstwach⁸ grupy G . Zgodnie z twierdzeniem o rozkładzie Bruhat z każdą (B, B) -warstwą G można zwi  zać jednoznacznie pewien element $w \in W$. Mo  emy zatem okre  lić stałe $\text{ind}(w) := \text{ind}(g)$, gdzie $g \in BwB, w \in W$. Zauwa  my,   e daj   one pe  n   informacj   o funkcji ind na G . W dalszym ci  gu naszych rozwa  a   b  d   one pe  nić bardzo wa  n   rol  .

Twierdzenie 3.5. Niech $1 \leq i \leq |W|$, gdzie $w_i \in W$. Nast  puj  ce elementy algebry $\mathcal{H}_{\mathbb{C}}(G, B)$:

$$a_{w_j} := \text{ind}(w_j) e_B w_j e_B, \quad 1 \leq j \leq |W| \quad (3.5)$$

tworz   baz   przestrzeni $\mathcal{H}_{\mathbb{C}}(G, B)$.

⁸Widzimy wi  c,   e $\text{ind} \in \mathcal{H}_{\mathbb{C}}(G, B)$.

Dowód. Rozważmy element $[B]x[B]$, dla $x \in G$. Wówczas zgodnie z przyjętymi wcześniej oznaczeniami:

$$[B]x[B] = \sum_{b, b' \in B} bxb'.$$

Sprawdźmy, jaki współczynnik stoi przy x . Już w dowodzie lematu 3.1 wykazaliśmy, że jest to pewna liczba s_x , taka sama dla wszystkich elementów warstwy BxB . Udowodnimy teraz, że stała ta związana jest z $\text{ind}(x)$. Zauważmy, że dla każdego $b' \in B$:

$$x = bxb' \Leftrightarrow b \in xBx^{-1} \cap B.$$

Stąd przy x stoi współczynnik

$$|B|^{-2} \cdot |xBx^{-1} \cap B| = (|B| \cdot \text{ind}(x))^{-1}.$$

Ten sam współczynnik stoi przy dowolnym elemencie $y = b_1xb_2 \neq x$. Wynika to z faktu, że $BxB = ByB$. Rozumowanie jest analogicznie, jak w dowodzie lematu 3.1. Innymi słowy dla każdego $x \in G$ dostajemy formułę:

$$[B]x[B] = \frac{|B|}{\text{ind}(x)} [BxB]. \quad (3.6)$$

Niech $D_i := Bw_iB$, gdzie $1 \leq i \leq |W|$. Zgodnie z twierdzeniem o rozkładzie Bruhat, dla każdego $x \in G$ istnieje takie $1 \leq j \leq |W|$, że $BxB = Bw_jB = D_j$. Zatem wstawiając formułę (3.6) do definicji (3.5) dostajemy:

$$a_{w_j} = \text{ind}(w_j)e_Bw_je_B = \text{ind}(w_j) \cdot |B|^{-2} \sum_{x \in D_j} \frac{|B|}{\text{ind}(x)} \cdot x = |B|^{-1} [Bw_jB]. \quad (3.7)$$

Na podstawie (3.7) jest jasne, że każdy element $\mathcal{H}_{\mathbb{C}}(G, B)$ jest kombinacją liniową a_{w_j} , gdzie $1 \leq j \leq |W|$. Widać też, że skoro Bw_jB są parami rozłączne, to elementy $a_{w_j}, 1 \leq j \leq |W|$ są liniowo niezależne. Zatem rzeczywiście tworzą one bazę $\mathcal{H}_{\mathbb{C}}(G, B)$. Stąd też:

$$\dim_{\mathbb{C}}(\mathcal{H}_{\mathbb{C}}(G, B)) = |W|.$$

□

Niech $W = \{w_1, w_2, \dots, w_{|W|}\}$. Elementy bazy (3.5) algebry $\mathcal{H}_{\mathbb{C}}(G, B)$ oznaczać będziemy przez $\{a_{w_i}, w_i \in W\}$ lub prościej $\{a_w, w \in W\}$. Zauważmy, że po prawej stronie formuły (3.5) symbolem w_j oznaczamy pewien element algebry grupowej $\mathbb{C}[G]$. Mamy tu na myśli taki element $g \in G$, który reprezentuje warstwę Bw_iB . Konkretna postać bazy zależy od wyboru elementów w_i reprezentujących warstwy Bw_iB w $\mathbb{C}[G]$. Śledząc dowód twierdzenia 3.5 widzimy jednak, że niezależnie od tego wyboru otrzymujemy bazę $\mathcal{H}_{\mathbb{C}}(G, B)$. Elementy $\{a_{w_i}, w_i \in W\}$ nazywać będziemy **bazą standardową** $\mathcal{H}_{\mathbb{C}}(G, B)$.

Wykazaliśmy wcześniej, że $\mathcal{H}_{\mathbb{C}}(G, B)$ jest podalgebrą algebry $\mathbb{C}[G]$. Znajdziemy teraz **stałe strukturalne** tej algebry, a więc takie $\mu_{ijk} \in \mathbb{C}$, że $1 \leq i, j, k \leq |W|$ oraz:

$$a_{w_i}a_{w_j} = \sum_{k=1}^{|W|} \mu_{ijk}a_{w_k}.$$

Uwaga 3.6. Niech $w_i, w_j \in W$, dla pewnych $1 \leq i, j, \leq |W|$. Załóżmy, że istnieją takie $1 \leq i_1, i_2, \dots, i_m \leq |W|$, $m \in \mathbb{N}$, że:

$$(Bw_i B)(Bw_j B) \subseteq Bw_{i_1} B \cup Bw_{i_2} B \cup \dots \cup Bw_{i_m} B.$$

Wówczas:

$$\mu_{ijk} \neq 0 \Rightarrow k \in \{i_1, i_2, \dots, i_m\}.$$

Dowód. Fakt ten wynika natychmiast z wzoru (3.7). Istotnie, skoro dla każdego $w \in W$ mamy: $a_w = |B|^{-1}[BwB]$, to iloczyn elementów bazowych $a_{w_i} a_{w_j} = |B|^{-2}[Bw_i B][Bw_j B]$. Wymnażając $[Bw_i B][Bw_j B]$ dostaniemy element $\mathbb{C}[G]$ równy $\sum_{g \in G} \alpha_g g$, $g \in \mathbb{C}$, gdzie $\alpha_g \neq 0$ tylko wtedy, jeśli $g \in (Bw_i B)(Bw_j B)$. Wiadomo, że wartość α_g zależy jedynie od (B, B) -warstwy, w której znajduje się g , a więc α_g może być niezerowe tylko wtedy, jeśli g należy do (B, B) -warstwy zawierającej pewien element $(Bw_i B)(Bw_j B)$. $\square$

Twierdzenie 3.7. Niech $D_m = Bw_m B$, gdzie $w_m \in W$, $1 \leq m \leq |W|$. Wówczas stałe strukturalne μ_{ijk} algebry $\mathcal{H}_{\mathbb{C}}(G, B)$ opisane są, dla $1 \leq i, j, k \leq |W|$, równościami:

$$\mu_{ijk} = |B|^{-1}|D_i \cap w_k D_j^{-1}| = |B|^{-1}|Bw_i B \cap w_k (Bw_j B)^{-1}|. \quad (3.8)$$

Dowód. Dowód twierdzenia polega na wykorzystaniu przyporządkowania (1.10), a więc na interpretacji elementów x przestrzeni $\mathcal{H}_{\mathbb{C}}(G, B)$ jako elementów $\Phi(x) : G \rightarrow \mathbb{C}$ algebry $\mathcal{F}_{\mathbb{C}}(G, H)$ funkcji stałych na (B, B) -warstwach G . Chcąc uprościć nieco zapis dowodu, funkcję $\Phi(x)$ oznaczać będziemy krótko jako f_x . Wiadomo, że $\mathcal{F}_{\mathbb{C}}(G, B)$ jest przestrzenią liniową, zatem:

$$f_{a_i a_j} = f_{\sum_l \mu_{ijl} a_l} = \sum_l \mu_{ijl} f_{a_l}. \quad (3.9)$$

Zgodnie z wzorem (3.7):

$$f_{a_l} = f_{|B|^{-1}[D_l]} = |B|^{-1} \sum_{x \in D_l} f_x.$$

Dla ustalonego $1 \leq k \leq |W|$ mamy:

$$f_{a_l}(w_k) = |B|^{-1} \sum_{x \in D_l} f_x(w_k) = \begin{cases} |B|^{-1} & , l = k \\ 0 & , l \neq k. \end{cases}$$

Podstawiając ten wynik do wzoru (3.9) otrzymujemy:

$$f_{a_i a_j}(w_k) = \mu_{ijk} |B|^{-1}. \quad (3.10)$$

Z drugiej strony, na mocy (1.14):

$$f_{a_i a_j}(w_k) = (f_{a_i} \star f_{a_j})(w_k)$$

Zgodnie ze wzorem (1.13) mamy zatem:

$$f_{a_i a_j}(w_k) = \sum_{y \in G} f_{a_i}(y) f_{a_j}(y^{-1} w_k).$$

Korzystając z (3.6) widzimy jednak, że:

$$\begin{aligned} f_{a_i}(y) &\neq 0 \Leftrightarrow y \in D_i \\ f_{a_j}(y^{-1} w_k) &\neq 0 \Leftrightarrow y \in w_k D_j^{-1}. \end{aligned}$$

Stąd:

$$f_{a_i a_j}(w_k) = \sum_{y \in D_i \cap w_k D_j^{-1}} f_{a_i}(y) f_{a_j}(y^{-1} w_k). \quad (3.11)$$

Porównując (3.10) i (3.11) otrzymujemy:

$$\mu_{ijk} = |B| \sum_{y \in D_i \cap w_k D_j^{-1}} f_{a_i}(y) f_{a_j}(y^{-1} w_k).$$

Do zakończenia dowodu pozostaje pokazać, że:

$$\sum_{y \in D_i \cap w_k D_j^{-1}} f_{a_i}(y) f_{a_j}(y^{-1} w_k) = |B|^{-2} |D_i \cap w_k D_j^{-1}|.$$

Zgodnie ze wzorem (3.6), w rozwinięciu (3.5) elementu bazowego a_i przy elemencie $b_1 x b_2$ stoi współczynnik $(|B| \cdot \text{ind}(w_i))^{-1}$. Powyższe sumowanie prowadzimy po elementach z jednej warstwy, bowiem $D_i \cap w_k D_j^{-1} \subseteq D_i$, zaś $y^{-1} w_k \in D_j$. Zatem dostajemy:

$$\begin{aligned} \sum_{y \in D_i \cap w_k D_j^{-1}} f_{a_i}(y) f_{a_j}(y^{-1} w_k) &= \sum_{y \in D_i \cap w_k D_j^{-1}} \text{ind}(w_i)(e_B w_i e_B)(y) \text{ind}(w_j)(e_B w_j e_B)(y^{-1} w_k) \\ &= |D_i \cap w_k D_j^{-1}| (\text{ind}(w_i)(|B| \cdot \text{ind}(w_i))^{-1} \text{ind}(w_j)(|B| \cdot \text{ind}(w_j))) \\ &= |B|^{-2} |D_i \cap w_k D_j^{-1}|. \end{aligned}$$

□

Mnożenie elementów bazowych algebry Hecke, choć związane z mnożeniem w grupie Weyla, nie odzwierciedla go bezpośrednio. Dla przykładu, jeśli $s \in S$ jest generatorem W , to $s^2 = 1$, natomiast a_s^2 nie musi być równe a_s . Dowód formuły (3.1) wymaga głębszego wykorzystania własności grupy Weyla. Dotychczas korzystaliśmy właściwie jedynie z wyników uzyskanych w paragrafie 2.3 (rozkład Bruhat). Jak się okazuje, kluczowym krokiem na drodze do dowodu tw. Titsa jest określenie algebry Hecke przy pomocy generatorów i relacji. Jest to możliwe dzięki technikom podobnym do tych, które wprowadziliśmy w paragrafie 2.5. Zagadnieniom tym poświęcony jest następny paragraf.

3.2. Prezentacja algebry Hecke

W paragrafie tym udowodnimy następujące twierdzenie.

Twierdzenie. (Iwahori, Matsumoto) Niech G będzie skończonym systemem Titsa z grupą Weyla W generowaną przez zbiór S , zaś $\mathcal{H}_{\mathbb{C}}(G, B)$ - związaną z nią algebrą Hecke. Jeśli $S = \{s_1, s_2, \dots, s_n\}$, wówczas $\mathcal{H}_{\mathbb{C}}(G, B)$ generowana jest przez elementy $\{a_{s_i} \mid s_i \in S\}$. Jeśli $q_i = \text{ind}(a_{s_i})$, wówczas $\mathcal{H}_{\mathbb{C}}(G, B)$ określona jest przez równości:

$$a_{s_i}^2 = q_i \cdot 1 + (q_i - 1)a_{s_i}, \quad 1 \leq i \leq n, \quad (3.12)$$

$$(a_{s_i} a_{s_j})^{k_{ij}} = (a_{s_j} a_{s_i})^{k_{ij}}, \quad \text{o ile } m_{ij} = 2k_{ij}, \quad i \neq j \quad (3.13)$$

$$(a_{s_i} a_{s_j})^{k_{ij}} a_{s_i} = (a_{s_j} a_{s_i})^{k_{ij}} a_{s_j}, \quad \text{o ile } m_{ij} = 2k_{ij} + 1, \quad i \neq j \quad (3.14)$$

gdzie m_{ij} jest rzędem elementu $s_i s_j$ w W .

Dowód składa się z dwóch zasadniczych części. Po pierwsze, należy wykazać, że elementy a_{s_i} algebry Hecke spełniają równości (3.12)-(3.14). Dalej natomiast należy uzasadnić, że jeśli A jest łączną $\mathbb{C}$ -algebrą zawierającą elementy $\{a_1, \dots, a_n\}$ spełniające równości analogiczne do (3.12)-(3.14), wówczas istnieje homomorfizm $f : \mathcal{H}_{\mathbb{C}}(G, B) \rightarrow A$ taki, że $f(a_{s_i}) = a_i$.

Wykażemy najpierw, że w $\mathcal{H}_{\mathbb{C}}(G, B)$ spełniona jest równość (3.12).

Lemat 3.8. *Niech $\{a_w | w \in W\}$ będzie bazą standardową $\mathcal{H}_{\mathbb{C}}(G, B)$. Wówczas dla każdego $s \in S$:*

$$a_s^2 = q_s \cdot 1 + (q_s - 1)a_s, \text{ gdzie}$$

$$q_s = \text{ind}(a_s) = \frac{|BsB|}{|B|}.$$

Dowód. Na podstawie (BN 4) wiemy, że $(BsB)(BsB) \subseteq B \cup BsB$. Stąd, na mocy uwagi 3.6, $a_s^2 = \mu a_1 + \lambda a_s$, gdzie a_1 jest elementem bazy standardowej odpowiadającym elementowi neutralnemu $1 \in W$; $\mu, \lambda \in \mathbb{C}$, przy czym, zgodnie z tw. 3.7, $\mu = |B|^{-1}|BsB \cap BsB| = \text{ind}(s) = q_s$. Chcielibyśmy wykazać, że:

$$(\text{ind}(a_s))^2 = \text{ind}(a_s^2). \quad (3.15)$$

Wiedząc to, moglibyśmy przyłożyć ind do równości⁹ $a_s^2 = q_s a_1 + \lambda a_s$ dostając w rezultacie tezę:

$$q_s^2 = q_s \cdot 1 + \lambda q_s \Rightarrow \lambda = q_s - 1.$$

Dowodzimy zatem (3.15). Wiemy, że $a_s a_s = \sum_{w \in W} \mu_{ssw} a_w$. Na mocy twierdzenia 3.7:

$$\text{ind}(a_s a_s) = \sum_{w \in W} \mu_{ssw} \text{ind}(a_w) = \sum_{w \in W} |B|^{-1} |BsB \cap w(BsB)^{-1}| \cdot \frac{|BwB|}{|B|}.$$

Zgodnie z (3.4) $\text{ind}(a_s) = |B|^{-1} |BsB|$. Pozostaje zatem wykazać, że:

$$\sum_{w \in W} |BsB \cap wBs^{-1}B| \cdot |BwB| = |BsB| \cdot |BsB|.$$

Wiemy, że $wBs^{-1}B \subseteq Bws^{-1}B \cup BwB$ (aksjomat BN 2). Skoro $|BsB \cap wBs^{-1}B| \neq 0$, to $BsB = BwB$ lub $BsB = Bws^{-1}B$. Z twierdzenia 2.12 (o rozkładzie Bruhat) wynika, że $s = w$ lub $s = ws^{-1}$. Drugi przypadek jest jednak niemożliwy, wówczas bowiem $w = 1$, zaś $|BsB \cap Bs^{-1}B| = 0$. Zatem $s = w$ i dostajemy tezę:

$$\sum_{w \in W} |BsB \cap wBs^{-1}B| \cdot |BwB| = |BsB \cap BsB| \cdot |BsB|.$$

□

Przed nami dowód tożsamości (3.13) i (3.14). Są one tego samego typu, co równości (2.28) i (2.29) wiążące generatory grupy Weyla W . Podobnie jak w paragrafie 2.5, podstawowymi narzędziami będą warunek wymiany i twierdzenie Matsumoto (tw. 2.23). Zaczniemy od związania mnożenia elementów bazowych $\mathcal{H}_{\mathbb{C}}(G, B)$ z długościami indeksujących je elementów grupy W .

⁹Można pokazać, że przekształcenie $\text{ind} : \mathcal{H}_{\mathbb{C}}(G, B) \rightarrow \mathbb{C}$ będące $\mathbb{C}$ -liniowym rozszerzeniem definicji $\text{ind}(w), w \in W$ jest homomorfizmem algebr ([Cur81], zad. 11.19).

Twierdzenie 3.9 (Iwahori). *Niech $\{a_w\}$ będzie bazą standardową $\mathcal{H}_{\mathbb{C}}(G, B)$. Niech S będzie zbiorem generatorów grupy Weyla W systemu G . Wówczas dla każdego $s \in S$ oraz dla każdego $w \in W$ mamy:*

$$l(sw) > l(w) \Rightarrow a_s a_w = a_{sw} \quad (3.16)$$

$$l(sw) < l(w) \Rightarrow a_s a_w = q_s a_{sw} + (q_s - 1) a_w, \quad (3.17)$$

Dowód. W poprzednim paragrafie wykazaliśmy, że mnożenie na elementach bazy standardowej $\mathcal{H}_{\mathbb{C}}(G, B)$ dane jest wzorami:

$$a_u a_v = \sum_{w \in W} \mu_{uvw} a_w, \quad \text{gdzie } u, v \in W,$$

zaś $\mu_{uvw} \in \mathbb{C}$ są, zgodnie z tw. 3.7, równe:

$$\mu_{uvw} = |B|^{-1} |BuB \cap w(BvB)^{-1}|.$$

Dowodzimy implikację (3.16). Wiemy, że iloczyn $a_s a_w$ jest kombinacją liniową elementów bazy standardowej. Skoro $l(sw) > l(w)$, wówczas na mocy (2.31) dostajemy zawieranie $sBw \subseteq BswB$. Oznacza to, zgodnie z uwagą 3.6, że element $a_s a_w$ jest kombinacją liniową jednego tylko elementu bazowego, którym jest a_{sw} . Mamy zatem:

$$a_s a_w = \mu a_{sw}, \quad (3.18)$$

gdzie μ jest, zgodnie z twierdzeniem 3.7, równy:

$$\mu = |B|^{-1} |BsB \cap swBw^{-1}B| = |B|^{-1} |sBsB \cap wBw^{-1}B|.$$

Należy zatem wykazać, że współczynnik μ występujący w równości (3.18) równy jest 1. Wykażemy, że zachodzi następująca równość:

$$sBsB \cap wBw^{-1}B = B. \quad (3.19)$$

Dowodu wymaga jedynie zawieranie lewej strony w prawej. Z aksjomatu (BN 4) wynika, że $sBs \subseteq B \cup BsB$. Co więcej, $B \subseteq wBw^{-1}B$. Do wykazania (3.19) wystarczy uzasadnić, że:

$$BsB \cap wBw^{-1}B = \emptyset. \quad (3.20)$$

Założmy przeciwnie, że lewa strona (3.20) jest zbiorem niepustym. Stąd także

$$BsB \cap BwBw^{-1}B \neq \emptyset. \quad (3.21)$$

Rozważmy $s_{j_1} \dots s_{j_p} \in \mathcal{R}(w)$ (a więc postać zredukowaną w), gdzie $s_{j_k} \in S, 1 \leq k \leq p$. Wówczas, zgodnie z lematem 2.25 i formułą (2.51), mamy:

$$BwBw^{-1}B \subseteq \bigcup_y BwyB,$$

gdzie y są iloczynami czynników $s_{j_k}, 1 \leq k \leq p$ z rozkładu w^{-1} , indeksowanych dowolnymi malejącymi podciągami zbioru $\{1, \dots, p\}$. W szczególności, z (3.21) wynika, że warstwa BsB ma niepuste przecięcie z sumą warstw postaci $BwyB$. Stąd warstwa BsB musi być równa $BwyB$, gdzie y jest produktem pewnych czynników iloczynu $w = s_{j_1} \dots s_{j_p}$. Stąd $l(y) \leq l(w)$. Z twierdzenia 2.12 (o rozkładzie Bruhat) mamy: $s = wy$, a więc $w^{-1}s = y$. Skoro jednak $l(w) = p$, to:

$$l(sw) = l(w^{-1}s) = l(y) \leq p = l(w).$$

Sprzeczność z założeniem, że $l(sw) > l(w)$. Udowodniliśmy zatem równość (3.20), a wraz z nią fakt, że w równości (3.18) stała strukturalna μ równa jest 1, co kończy dowód implikacji (3.16).

Dowodzimy teraz implikację (3.17). Zakładamy więc, że $l(sw) < l(w)$. Niech $w' = sw$. Wówczas $l(sw') > l(w')$. Na mocy (3.16) dostajemy:

$$a_w = a_s a_{w'}.$$

Stąd korzystając z lematu 3.8:

$$a_s a_w = a_s^2 a_{w'} = q_s a_{w'} + (q_s - 1) a_s a_{w'} = q_s a_{sw} + (q_s - 1) a_w.$$

□

Mając w rękę twierdzenie Iwahori bez trudu wykażemy, że zbiór $\{a_s \mid s \in S\}$ generuje $\mathcal{H}_{\mathbb{C}}(G, B)$. Wystarczy jeśli będziemy umieli wygenerować każdy element bazy standardowej. Niech $w \in W$. Rozumowanie jest indukcją po długości w . Gdy $l(w) = 0$ lub $l(w) = 1$, dowód jest trywialny. Jeśli teza jest prawdziwa dla elementów długości mniejszej niż n , wówczas bierzemy dowolne $w \in W$, że $l(w) = n$ i rozważamy postać zredukowaną $w = s_1 s_2 \dots s_n$. Wiemy, że $s_2 \dots s_n$ ma długość mniejszą niż w , zatem na mocy założenia indukcyjnego umiemy go wygenerować przy pomocy elementów ze zbioru S . Korzystając z tw. 3.9 wiemy, że $a_w = a_{s_1} a_{s_2 \dots s_n}$.

Wykażemy teraz, że generatory $\{a_s \mid s \in S\}$ algebry $\mathcal{H}_{\mathbb{C}}(G, B)$ spełniają tożsamości (3.13) i (3.14). Niech $s, s' \in S$ będą różnymi generatorami grupami W i niech rząd ss' wynosi $2k$ lub $2k+1$. Zauważmy, że dla każdego $r < k$ mamy:

$$l((ss')^r s) > l((ss')^r), \quad l((ss')^{r+1}) > l((ss')^r s).$$

Istotnie długości elementów wymienionych wyżej elementów W różnią się o 1 (na mocy (2.37)). Oczywiście $ss' \neq 1$. Zatem na mocy tw. 3.9 równości (3.13) i (3.14) przybierają postać:

$$\begin{aligned} a_{(s_i s_j)^{k_{ij}}} &= a_{(s_j s_i)^{k_{ij}}} & , \text{ o ile } m_{ij} &= 2k_{ij}, & i \neq j \\ (a_{(s_i s_j)^{k_{ij}}}) a_{s_i} &= (a_{(s_j s_i)^{k_{ij}}}) a_{s_j} & , \text{ o ile } m_{ij} &= 2k_{ij} + 1, & i \neq j \end{aligned}$$

Teza wynika zatem z lematu 2.19.

Wykazaliśmy, że generatory $\mathcal{H}_{\mathbb{C}}(G, B)$ spełniają równości (3.12)-(3.14). Przejdziemy teraz do dowodu drugiej części twierdzenia Iwahori-Matsumoto, dotyczącej prezentacji algebry $\mathcal{H}_{\mathbb{C}}(G, B)$.

Twierdzenie 3.10 (Iwahori, Matsumoto). *Generatory $\{a_s \mid s \in S\}$ oraz relacje (3.12)-(3.14) zadają prezentację algebry Hecke $\mathcal{H}_{\mathbb{C}}(G, B)$.*

Dowód. Udowodnimy, że jeśli A jest łączną $\mathbb{C}$ -algebrą zawierającą elementy $\{a_1, \dots, a_n\}$ spełniające równości (3.12)-(3.14), wówczas istnieje homomorfizm algebr $f : \mathcal{H}_{\mathbb{C}}(G, B) \rightarrow A$, że $f(a_{s_i}) = a_i, 1 \leq i \leq n$. Z twierdzenia Matsumoto (2.23) oraz z formuły (2.53) wynika, że istnieje homomorfizm monoidów $f' : W \rightarrow A$ spełniający warunki analogiczne do (2.39):

$$f'(1_W) = 1_A, \quad f'(s_i) = a_i, \quad f'(s_{i_1} s_{i_2} \dots s_{i_m}) = a_{i_1} a_{i_2} \dots a_{i_m},$$

gdzie $s_{i_1}s_{i_2}\dots s_{i_m} \in \mathcal{R}(W)$. Skoro elementy $a_w, w \in W$ tworzą bazę $\mathcal{H}_{\mathbb{C}}(G, B)$, to istnieje przekształcenie liniowe $f : \mathcal{H}_{\mathbb{C}}(G, B) \rightarrow A$, że $f(a_w) = f'(w)$, dla $w \in W$. Wystarczy więc pokazać, że f to homomorfizm algebr, a więc

$$f(a_s a_w) = f(a_s) f(a_w), \quad s \in S, w \in W.$$

Niech $l(sw) > l(w)$. Wtedy postać zredukowaną elementu sw otrzymujemy z postaci zredukowanej w przemnożonej przez s . Wtedy skoro $a_{sw} = a_s a_w$, wówczas otrzymujemy tezę.

Niech $l(sw) < l(w)$. Wówczas jeśli $w' = sw$, to $l(sw') > l(w')$, a więc na mocy pierwszej części dowodu mamy:

$$f(a_w) = f(a_s a_{w'}) = f(a_s) f(a_{w'}).$$

Z założenia dotyczącego algebry A , elementy $f(a_s)$ spełniają relacje (3.12)-(3.14). Stąd:

$$\begin{aligned} f(a_s) f(a_w) &= f(a_s)^2 f(a_{w'}) \\ &= q_s f(a_{w'}) + (q_s - 1) f(a_s) f(a_{w'}) \\ &= q_s f(a_{sw}) + (q_s - 1) f(a_w). \end{aligned}$$

Z drugiej strony wiemy, że: $a_s a_w = q_s a_{sw} + (q_s - 1) a_w$. Przykładając do tej formuły funkcją f i porównując otrzymaną w ten sposób równość $f(a_s a_w) = q_s f(a_{sw}) + (q_s - 1) f(a_w)$ z uzyskanym wyżej wzorem $f(a_s) f(a_w) = q_s f(a_{sw}) + (q_s - 1) f(a_w)$, otrzymujemy tezę. Dowód całego twierdzenia jest zatem zakończony. $\square$

Ustalenie podobieństwa pomiędzy prezentacją grupy Weyla BN -pary G oraz prezentacją algebry $\mathcal{H}_{\mathbb{C}}(G, B)$ przybliża nas znacznie do dowodu izomorfizmu (3.1). Kluczowy pomysł Titsa polega na określeniu obiektu, który jest wspólnym uogólnieniem algebr $\mathbb{C}[W]$ oraz $\mathcal{H}_{\mathbb{C}}(G, B)$. Zagadnienia te przedstawimy w następnym paragrafie.

3.3. Algebry generyczne i ich specjalizacje

Naszym celem jest wykazanie, że jeśli $\mathcal{H}_{\mathbb{C}}(G, B)$ jest algebrą Hecke grupy skończonej G z BN -parą, wówczas $\mathcal{H}_{\mathbb{C}}(G, B) \simeq \mathbb{C}[W]$, gdzie W jest grupą Weyla W związaną z BN -parą. Dotychczasowe rozważania pozwoliły nam zobaczyć, że prezentacja $\mathcal{H}_{\mathbb{C}}(G, B)$ jest podobna do prezentacji W , a więc i $\mathbb{C}[W]$. Celem tego rozdziału jest uczynienie tego podobieństwa bardziej precyzyjnym. Zaczniemy od następującego faktu:

Twierdzenie 3.11. *Niech W będzie grupą Weyla związaną z systemem Titsa G , generowaną przez zbiór $S = \{s_1, s_2, \dots, s_n\}$. Przez R będziemy rozumieli dowolną przemenną $\mathbb{Q}$ -algebrę zawierającą elementy $\{u_1, u_2, \dots, u_n\}$, spełniające następującą zależność:*

$$u_i = u_j \Leftrightarrow \exists_{w \in W} (s_i = w^{-1} s_j w). \quad (3.22)$$

Niech A będzie wolnym R -modułem o bazie $\{e_w \mid w \in W\}$. Wówczas istnieje R -algebra, w której struktura R -modułu równa jest A , a mnożenie jest jednoznacznie określone formułami:

$$e_{s_i} e_w = \begin{cases} e_{s_i w}, & l(s_i w) > l(w) \\ u_i e_{s_i w} + (u_i - 1) e_w, & l(s_i w) < l(w) \end{cases}$$

Dowód tego twierdzenia zostanie przez nas pominięty. Fakt ten jest analogiczny z twierdzeniem Iwahori (tw. 3.9). Elementy $\{u_i \mid 1 \leq i \leq n\}$ są odpowiednikami stałych $q_i = \text{ind}(s_i)$ występujących w treści tw. 3.9. Warunek (3.22) jest odpowiednikiem definicji 3.4 w tym sensie, że jeśli zastąpimy ciało $\mathbb{C}$ algebrą R , wówczas istnieje homomorfizm $i : A \rightarrow R$, odpowiadający w przypadku $R = \mathbb{C}$ homomorfizmowi ind , taki, że $i(e_i) = u_i$. Dowód tw. 3.11 znaleźć można (dla ogólniejszej klasy grup) w [Cur87], tw. 68.1.

R -algebrę A otrzymaną w twierdzeniu 3.11 nazywamy **algebrą generyczną grupy Weyla W nad pierścieniem R** . Nietrudno pokazać, podobnie jak w przypadku algebry $\mathcal{H}_{\mathbb{C}}(G, B)$, że algebra ta generowana jest przez elementy postaci $\{e_s \mid s \in S\}$, a jej prezentacja zadana jest przy pomocy relacji analogicznych z (3.12)-(3.14), a więc jeśli m_{ij} jest rzędem elementu $s_i s_j$ w W , wówczas:

$$e_{s_i}^2 = q_i \cdot 1 + (q_i - 1)e_{s_i}, \quad 1 \leq i \leq n, \quad (3.23)$$

$$(e_{s_i} e_{s_j})^{k_{ij}} = (e_{s_j} e_{s_i})^{k_{ij}}, \quad \text{o ile } m_{ij} = 2k_{ij}, \quad i \neq j \quad (3.24)$$

$$(e_{s_i} e_{s_j})^{k_{ij}} e_{s_i} = (e_{s_j} e_{s_i})^{k_{ij}} e_{s_j}, \quad \text{o ile } m_{ij} = 2k_{ij} + 1, \quad i \neq j \quad (3.25)$$

W dalszym ciągu zakładamy, że $R = \mathbb{Q}[u_1, u_2, \dots, u_n]$, gdzie $\{u_i \mid 1 \leq i \leq n\}$ spełniają (3.22).

Wprowadzimy teraz pojęcie **specjalizacji pierścienia**. Niech R będzie dowolnym pierścieniem przemiennym oraz A będzie algebrą, o strukturze wolnego R -modułu postaci:

$$A = \bigoplus_{i=1}^n R a_i.$$

Specjalizacja R jest homomorfizmem $f : R \rightarrow F$, gdzie F – ciało. Przy pomocy f określić można także prawostronne działanie $\circ : F \times R \rightarrow F$ zadane wzorem:

$$a \circ r = a f(r), \quad a \in F, r \in R.$$

W ten sposób F staje się (F, R) -bimodem. Na iloczynie tensorowym $F \otimes_R A$ wprowadzić można zatem strukturę F -algebry, uzyskując:

$$F \otimes_R A = \bigoplus_{i=1}^n F a'_i, \quad a'_i = 1 \otimes a_i. \quad (3.26)$$

Powyższy zapis oznacza, że elementy $\{1 \otimes a_i \mid 1 \leq i \leq n\}$ tworzą bazę algebry $F \otimes_R A$ jako wolnego R -modułu. Tę konwencję przyjmujemy także w dalszej części rozdziału.

Algebrę $F \otimes_R A$ nazywamy **algebrą specjalizacji algebry A** , lub krócej, **specjalizacją A** , i oznaczamy ją przez A_f . Łatwo widzieć, że dla $1 \leq i, j \leq n$ stałe strukturalne r_{ijk} algebry A_f są elementami pierścienia R :

$$a_i a_j = \sum_k r_{ijk} a_k, \quad r_{ijk} \in R. \quad (3.27)$$

Algebrę specjalizacji $F \otimes_R A$ rozumieć można także jako R -algebrę, gdzie $r(1 \otimes a_i) = f(r) \otimes a_i$. Wówczas przekształcenie $f : R \rightarrow F$ rozszerza się do epimorfizmu R -algebr

$$\widehat{f} : A \rightarrow A_f \text{ tak, że } \widehat{f}(a_i) = a'_i \quad (3.28)$$

(jest to przeprowadzenie jednej bazy na drugą). W dalszych rozważaniach szczególną rolę odgrywać będą specjalizacje do ciała $\mathbb{C}$.

Naszym celem będzie pokazanie, że zarówno $\mathcal{H}_{\mathbb{C}}(G, B)$ jak i $\mathbb{C}[W]$ są specjalizacjami algebry generycznej grupy Weyla W . Okazuje się, że istnieją metody pozwalające na badanie podobieństwa pomiędzy strukturami różnych specjalizacji danej algebry A (w zależności od postaci przekształceń f). Kluczowym wynikiem będzie tu twierdzenie Titsa o deformacji.

Lemat 3.12. *Niech A będzie algebrą generyczną grupy Weyla W nad pierścieniem $R = \mathbb{Q}[u_1, u_2, \dots, u_n]$, gdzie $\{u_i \mid 1 \leq i \leq n\}$ spełniają (3.22), zaś F niech będzie dowolnym ciałem charakterystyki 0. Wówczas:*

1. *Jeśli $f' : R \rightarrow F$ jest specjalizacją taką, że $f'(u_i) = 1, 1 \leq i \leq n$, to $A_{f'} \simeq F[W]$ (jako F -algebry).*
2. *Jeśli $f'' : R \rightarrow \mathbb{C}$ jest specjalizacją taką, że $f''(u_i) = q_i = \text{ind}(s_i), 1 \leq i \leq n$, wówczas $A_{f''} \simeq \mathcal{H}_{\mathbb{C}}(G, B)$.*

Dowód. Zauważmy, że wybór pierścienia R gwarantuje, że f', f'' są dobrze określone (w pierwszym przypadku korzystamy z założenia o zerowej charakterystyce F).

Dowodzimy punkt 1. Zgodnie z twierdzeniem 3.11 oraz z notacją przyjętą w (3.26) i (3.28), elementy bazowe algebry $A_{f'}$ oznaczamy przez e_w , zaś ich obrazy $f'(e_w) = e'_w$, gdzie $w \in W$. Wiemy, że elementy bazowe algebry generycznej A mnożą się według wzorów:

$$e_{s_i} e_w = \begin{cases} e_{s_i w}, & l(s_i w) > l(w) \\ u_i e_{s_i w} + (u_i - 1) e_w, & l(s_i w) < l(w) \end{cases}$$

Po przyłożeniu do nich homomorfizmu f' obydwa wymienione wyżej przypadki staną się identyczne, ponieważ $f'(u_i) = 1$. Stąd:

$$e'_{s_i w} = f'(e_{s_i} e_w) = f'(e_{s_i}) f'(e_w) = e'_{s_i} e'_w.$$

Bijekcja $w \rightarrow e'_w$ rozszerza się zatem w sposób oczywisty do izomorfizmu $F[W] \simeq A_{f'}$.

Punkt 2. wynika natychmiast z dowodu tw. Iwahori-Matsumoto (tw. 3.10). Zgodnie z (3.28) specjalizację f'' można rozszerzyć do epimorfizmu $\widehat{f''} : A \rightarrow A_{f''}$. Algebra $A_{f''}$ będąca obrazem przy przekształceniu $\widehat{f''}$ spełnia (3.12)-(3.14). Istnieje więc homomorfizm $\mathcal{H}_{\mathbb{C}}(G, B) \rightarrow A_{f''}$. Homomorfizm ten jest w sposób oczywisty surjektywny, zatem wobec równości wymiarów $\dim_{\mathbb{C}}(\mathcal{H}_{\mathbb{C}}(G, B)) = \dim_{\mathbb{C}}(A_{f''})$ dostajemy izomorfizm $A_{f''} \simeq \mathcal{H}_{\mathbb{C}}(G, B)$. $\square$

Przypomnijmy, że K -algebrę A nazywamy **rozdzielczą** jeśli dla każdego rozszerzenia ciała $L \supset K$ algebra $A^L = L \otimes_K A$ jest półprosta ([Cur81], 7A). Jeśli A jest rozdzielczą nad K wówczas niezmiennikami numerycznymi A nazwaliśmy wymiary prostych $A^{\overline{K}}$ -modułów. Łatwo widzieć, że dwie rozdzielcze K -algebry są, po rozszerzeniu skalarów do algebraicznego domknięcia $\overline{K}$, izomorficzne nad $\overline{K}$ wtedy i tylko wtedy, gdy ich niezmienniki numeryczne są takie same. W przypadku rozdzielczych algebr specjalizacji, wyznaczenie niezmienników numerycznych jest dość nietrudne. Wykażemy następujący lemat:

Lemat 3.13. *Niech B będzie algebrą półprostą nad ciałem $\mathbb{C}$, której bazę stanowią elementy $\{b_i \mid 1 \leq i \leq n\}$, oraz niech:*

$$B = \bigoplus_{s=1}^S M_{m_s}(\mathbb{C}) \tag{3.29}$$

będzie rozkładem algebry B na algebry proste.¹⁰ Niech:

$$\mathbb{C}[T] = \mathbb{C}[t_1, t_2, \dots, t_n], \quad \mathbb{C}(T) = \mathbb{C}(t_1, t_2, \dots, t_n),$$

gdzie $\{t_i \mid 1 \leq i \leq n\}$ są algebraicznie niezależne¹¹ nad $\mathbb{C}$, zaś przez $\mathbb{C}(T)$ rozumiemy ciało ułamków pierścienia wielomianów $\mathbb{C}[T]$. Niech

$$b = \sum_{i=1}^n t_i b_i \in B^{\mathbb{C}(T)}, \quad B^{\mathbb{C}(T)} = \bigoplus_{i=1}^n \mathbb{C}(T) b_i. \quad (3.30)$$

Powiemy, że b jest **elementem ogólnym algebry $B^{\mathbb{C}(T)}$ w bazie $\{b_i \mid 1 \leq i \leq n\}$** . Rozważmy endomorfizm algebry $B^{\mathbb{C}(T)}$ zadany wzorem $x \rightarrow bx$. Jeśli przyjmiemy, że wielomian charakterystyczny¹² tego endomorfizmu to $p(x) = \text{char}_{B^{\mathbb{C}(T)}/B}(b)$, wówczas łatwo widzieć, że $p(x) \in \mathbb{C}[T][x]$.¹³ Niech:

$$p(x) = \prod_{s=1}^{S'} p_s(x)^{p_s} \quad (3.31)$$

będzie rozkładem¹⁴ $p(x)$ na parami niestowarzyszone¹⁵ czynniki pierwsze $\{p_s(x)\}$ w $\mathbb{C}[T][x]$. Wówczas:

- a) Zachodzi równość $S = S'$, zaś wykładniki $\{p_s \mid 1 \leq s \leq S'\}$ są niezmiennikami numerycznymi algebry B ,
- b) $\deg(p_s(x)) = p_s$,
- c) Jeśli $p(x) = \prod_{v=1}^V q_v(x)^{q_v}$ jest rozkładem¹⁶ $p(x)$ na czynniki pierwsze w $\mathbb{C}[T][x]$, przy czym $q_v(x)$ są unormowane w $\mathbb{C}[T][x]$ oraz $\deg(q_v(x)) = q_v$, wówczas $V = S'$, co więcej wielomiany $\{q_v(x)\}$ są parami niestowarzyszone i dla każdego $q_v(x)$ istnieje stowarzyszony z nim wielomian $p_s(x)$.

Dowód. Nietrudno sprawdzić, że teza lematu nie zależy od wyboru bazy algebry B . Pierwszym krokiem dowodu będzie sprawdzenie punktów (a) oraz (b) tezy lematu w przypadku, gdy B jest $\mathbb{C}$ -algebrą prostą wymiaru $n = m^2$ postaci $B = M_m(\mathbb{C})$. W tym przypadku każde dwa B -moduły proste (niezerowe) są izomorficzne i mają wymiar m . Algebra B ma strukturę $\mathbb{C}$ -modułu postaci:

$$B = \bigoplus_{1 \leq i, j \leq m} \mathbb{C} E_{ij},$$

gdzie $\{E_{ij} \mid 1 \leq i, j \leq m\}$ jest bazą $M_m(\mathbb{C})$ złożoną z jedynek macierzowych.¹⁷ Przyjmijmy, że $T = \{t_{ij} \mid 1 \leq i, j \leq m\}$ są elementami algebraicznie niezależnymi nad $\mathbb{C}$. Rozważamy element ogólny $b \in B^{\mathbb{C}(T)}$ względem bazy złożonej z jedynek macierzowych:

$$b = \sum_{1 \leq i, j \leq m} t_{ij} E_{ij}. \quad (3.32)$$

¹⁰Zgodnie z twierdzeniem Artina-Wedderburna (tw. 1.16).

¹¹tzn., że nie istnieje niezerowy wielomian $f \in \mathbb{C}[x_1, x_2, \dots, x_n]$, że $f(t_1, t_2, \dots, t_n) = 0$.

¹²Z definicji jest to $\det(M - xI)$, gdzie M jest macierzą endomorfizmu $B^{\mathbb{C}(T)}$ w bazie $\{b_i \mid 1 \leq i \leq n\}$ nad ciałem $\mathbb{C}(T)$.

¹³Zgodnie z (3.29) $bb_i \in \mathbb{C}[T]$, zatem jeśli macierz endomorfizmu $x \rightarrow bx$ w bazie $\{b_i \mid 1 \leq i \leq n\}$ oznaczmy przez M , wówczas $M \in M_n(\mathbb{C}[T])$.

¹⁴Chodzi o rozkład wielomianu jednej zmiennej x o współczynnikach z $\mathbb{C}[T]$.

¹⁵Przypomnijmy, że jeśli pierścień R jest dziedziną całkowitości, wówczas elementy $a, b \in R$ są stowarzyszone wtedy i tylko wtedy, gdy istnieje element odwracalny $c \in R^*$, że $a = cb$.

¹⁶Podobnie jak w (3.31), chodzi o rozkład wielomianu jednej zmiennej x o współczynnikach z $\mathbb{C}[T]$.

¹⁷Jedynka macierzowa E_{ij} to macierz, której jedyny niezerowy element znajduje się w wierszu i i kolumnie j . Element ten równy jest 1.

Rozważmy też wielomian charakterystyczny elementu b , a więc $\text{char}_{B^{\mathbb{C}(T)}/B}(b)$. Chcemy wykazać, że:

a') $\text{char}_{B^{\mathbb{C}(T)}/B}(b) = (p_1(x))^m$, gdzie $p_1(x)$ jest wielomianem nierozkładalnym w $\mathbb{C}[T][x]$.

b') $\deg(p_1(x)) = m$

Rozważmy przekształcenie $f : B^{\mathbb{C}(T)} \rightarrow B^{\mathbb{C}(T)}$ zadane wzorem:

$$f(a) = ba, \quad a \in B^{\mathbb{C}(T)}.$$

Szukamy macierzy przekształcenia f w bazie $\{E_{ij}\}$. Kolejność elementów bazowych wyznaczona jest przez porządek leksykograficzny na zbiorze par indeksów opisujących elementy bazowe (a więc kolejno $E_{11}, E_{21}, E_{31}, \dots, E_{n1}, E_{12}, E_{22}, \dots, E_{m2}, \dots, E_{mm}$). Macierz M przekształcenia f ma wówczas postać:

$$M = \begin{pmatrix} (t_{ij}) & 0 & \dots & 0 & 0 \\ 0 & (t_{ij}) & \dots & 0 & 0 \\ & & \dots & & \\ 0 & 0 & \dots & (t_{ij}) & 0 \\ 0 & 0 & \dots & 0 & (t_{ij}) \end{pmatrix}, \quad (3.33)$$

gdzie blok (t_{ij}) jest postaci:

$$\begin{pmatrix} t_{11} & t_{12} & \dots & t_{1m} \\ t_{21} & t_{22} & \dots & t_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ t_{m1} & t_{m2} & \dots & t_{mm} \end{pmatrix} \in M_m(\mathbb{C}[T]).$$

Istotnie, macierz M należy do $M_{m^2}(\mathbb{C}[T])$. Jeśli ponumerujemy jej kolumny parami (i, j) , gdzie $1 \leq i, j \leq m$, zgodnie z porządkiem leksykograficznym (tak samo ponumerowana jest baza B), wówczas w kolumnie (k, l) znajdują się współrzędne elementu bE_{kl} w bazie $\{E_{ij}\}$. Zgodnie z (3.32) wiadomo natomiast, że:

$$bE_{kl} = \sum_{1 \leq i, j \leq m} t_{ij} E_{ij} E_{kl} = \sum_{1 \leq i \leq m} t_{ik} E_{il}.$$

Wielomian charakterystyczny elementu b nad ciałem $\mathbb{C}$ otrzymuje się zatem, zgodnie z (3.33), przez wzięcie m -tej potęgi wielomianu charakterystycznego macierzy (t_{ij}) .

$$p(x) = \text{char}_{B^{\mathbb{C}(T)}/B}(b)(x) = (\det((t_{ij}) - xI))^m. \quad (3.34)$$

Aby udowodnić tezę w punkcie (a') wystarczy pokazać, że wielomian $f(x) = \det((t_{ij}) - xI)$ jest elementem nierozkładalnym w pierścieniu wielomianów zmiennej x o współczynnikach z $\mathbb{C}[T]$. Zauważmy najpierw, że wielomian ten jest stopnia m i współczynnik stojący przy x^m jest stopnia ± 1 . Wynika stąd, że $f(x)$ jest wielomianem pierwotnym¹⁸ w $\mathbb{C}[T][x]$. Na mocy lematu Gaussa, wielomian ten jest nierozkładalny nad $\mathbb{C}[T]$ wtedy i tylko wtedy, gdy jest nierozkładalny nad ciałem $\mathbb{C}(T)$. Rozkładalność w $\mathbb{C}(T)$ oznacza, że istnieją wielomiany zmiennej x : $g(x), h(x)$, stopni ≥ 1 , o współczynnikach z $\mathbb{C}(T)$, że $f(x) = g(x)h(x)$. Wiadomo jednak, że istnieją $a, b \in \mathbb{C}(T)$, że $g'(x) := ag(x), h'(x) := bh(x)$ są pierwotne w $\mathbb{C}[T][x]$.

¹⁸ Jeśli pierścień R ma jednoznaczność rozkładu, to zawartością elementu $f = a_n x^n + \dots + a_1 x + a_0 \in R[x]$ nazywamy element $c(f) := \text{NWD}[a_n, a_{n-1}, \dots, a_1, a_0]$. Wielomian $f \in R[x]$ nazywamy pierwotnym jeśli $c(f)$ jest elementem odwracalnym w R .

Iloczyn wielomianów pierwotnych jest, na mocy lematu Gaussa, pierwotny. Zatem możemy przyjąć, że $ab = 1$ i dostajemy rozkład $f(x) = g'(x)h'(x)$ na dwa wielomiany o współczynnikach w $\mathbb{C}[T]$. Do zakończenia dowodu punktu (a') wystarczy pokazać, że rozkład ten nie może mieć miejsca.

Rozważmy homomorfizm pierścieni $F : \mathbb{C}[T][x] \rightarrow \mathbb{C}[t_{1m}][x]$, spełniający warunki:

$$F|_{\mathbb{C}[x]} = Id, \quad F(t_{ij}) = \begin{cases} t_{ij}, & i = 1, j = m \\ 1, & i = j + 1 \\ 0, & \text{w p.p.} \end{cases}.$$

Zarówno $f(x)$, jak i $F(f(x)) = x^m - t_{1m}$ są wielomianami stopnia m . Jeśli zatem udowodnimy, że $x^m - t_{1m}$ jest nierozkładalny nad $\mathbb{C}[t_{1m}]$, będzie już z tego wynikało, że $f(x)$ nie można przedstawić w postaci iloczynu $f(x) = g'(x)h'(x)$ wielomianów stopnia ≥ 1 z $\mathbb{C}[T][x]$. Zauważmy, że element t_{1m} jest pierwszy w pierścieniu $\mathbb{C}[t_{1m}]$. Zatem z kryterium Eisensteina $x^m - t_{1m}$ jest, jako wielomian pierwotny, nierozkładalny w $\mathbb{C}[t_{1m}][x]$. Stąd $f(x)$ jest nierozkładalny w $\mathbb{C}[T]$. Dowód punktu (a') jest zakończony.

Tak, jak stwierdziliśmy w dowodzie punktu (a'), stopień wielomianu $\det((t_{ij}) - xI)$ występującego w rozkładzie (3.34) wielomianu charakterystycznego $p(x)$ wynosi m . Dostajemy zatem tezę w punkcie (b').

Uzasadnimy teraz, że teza lematu w punktach (a) i (b) jest prawdziwa dla dowolnej algebry półprostej B . Zgodnie z (3.29) B jest sumą prostą algebr prostych postaci $\{M_{m_s}, 1 \leq s \leq S\}$. Załóżmy, że bazą algebry M_{m_s} jest $\mathcal{A}_s = \{a_1^{(s)}, \dots, a_{m_s}^{(s)}\}$ oraz, że elementem ogólnym M_{m_s} względem bazy $\mathcal{A}_s$ jest element $b_s \in M_{m_s}^{\mathbb{C}(T)}$. Przyjmijmy także, że $b \in B^{\mathbb{C}(T)}$ jest elementem ogólnym algebry B względem bazy $\{a_1^{(1)}, \dots, a_{m_1}^{(1)}, a_1^{(2)}, \dots, a_{m_2}^{(2)}, \dots, a_1^{(S)}, \dots, a_{m_S}^{(S)}\}$. Na mocy (3.33) jasne jest, że:

$$\text{char}_{B^{\mathbb{C}(T)}/B}(b) = \prod_{s=1}^S \left(\text{char}_{M_{m_s}^{\mathbb{C}(T)}/M_{m_s}}(b_s) \right).$$

Zgodnie z (a') i (b') widzimy, że $\text{char}_{M_{m_s}^{\mathbb{C}(T)}/M_{m_s}}(b_s) = (p_s(x))^{m_s}$, gdzie $p_s(x)$ jest wielomianem nierozkładalnym nad $\mathbb{C}[T][x]$. Skoro m_s są niezmiennikami numerycznymi algebr M_{m_s} , zaś każdy prosty B -moduł jest dla pewnego s , zgodnie z twierdzeniem Artina-Wedderburna, prostym M_{m_s} -modułem, dowód lematu w punktach (a) i (b) jest zakończony.

Dowodzimy punkt (c). Niech $p(x) = \prod_s^{S'} p_s(x)^{p_s} = \prod_{v=1}^V q_v(x)^{q_v}$, gdzie q_v są takie, jak w tezie lematu. Wiemy, że $\{p_s(x), 1 \leq s \leq S'\}$ są parami niestowarzyszonymi elementami pierwszymi w $\mathbb{C}[T][x]$ (ich współczynniki zawierają różne od siebie elementy algebraicznie niezależne). Pierścień $\mathbb{C}[T][x]$ jest zaś dziedziną z jednoznacznością rozkładu. Jeśli więc $p_s(x)$ dzieli $q_v(x)$ (dla pewnego v), to $q_v = \deg(q_v(x)) \geq \deg(p_s(x)) = p_s$. A jeśli $q_v \neq p_s$, wówczas $p_s(x)$ musi wystąpić więcej niż p_s razy w rozkładzie $p(x)$. To jest niemożliwe. Zatem jeśli $p_s(x)$ dzieli wielomian unormowany $q_v(x)$ i $\deg(p_s(x)) = \deg(q_v(x))$, to wielomiany $q_v(x)$ oraz $p_s(x)$ muszą być stowarzyszone. $\square$

W dalszym ciągu ciało ułamków dziedziny R oznaczать będziemy przez (R) . Zanim sformułujemy kluczowe twierdzenie tego rozdziału, przytoczymy krótkie następujące dwa elementarne fakty.

Lemat 3.14. Niech $\overline{R}$ oznacza całkowite domknięcie pierścienia R . Jeśli R jest dziedziną, wówczas dla dowolnego zbioru elementów algebraicznie niezależnych $t_1, t_2, \dots, t_n$ nad algebraicznym domknięciem (R) mamy:

$$\overline{R}[t_1, t_2, \dots, t_n] = \overline{R[t_1, t_2, \dots, t_n]}$$

Dowód można znaleźć w [Bou64] (Prop. 13).

Lemat 3.15 ([Ati69], Ex. 5.2). Niech R będzie dziedziną, zaś $f : R \rightarrow \mathbb{C}$ – homomorfizmem. Wówczas f można rozszerzyć do homomorfizmu $\overline{f} : \overline{R} \rightarrow \mathbb{C}$.

Jest to łatwy wniosek z lematu Zorna. Dowód można znaleźć w [Ati69] (Ex. 5.2).

Twierdzenie 3.16 (Tits, o deformacji). Niech R będzie dziedziną całkowitości, (R) jej ciałem ułamków, zaś $f : R \rightarrow \mathbb{C}$ – homomorfizmem R w ciało $\mathbb{C}$. Niech A będzie R -algebrą ze skończoną bazą nad R , $A^{(R)} = (R) \otimes_R A$, zaś $A_f = \mathbb{C} \otimes_R A$. Jeśli $A^{(R)}$ oraz A_f są algebrami rozdzielczymi, wówczas mają one identyczne niezmienniki numeryczne.

Dowód poprzedzimy pewnym komentarzem. Twierdzenie Titsa, gdy zostanie już przez nas udowodnione, przybliży nas do bezpośredniego rozstrzygnięcia problemu postawionego na początku tego rozdziału. Widać, że jeśli tylko algebra $A^{(R)}$ jest rozdzielcza, wówczas wszystkie rozdzielcze specjalizacje A_f algebry A mają niezmienniki numeryczne identyczne z niezmiennikami $A^{(R)}$. Algebry $\mathbb{C}[W]$ oraz $\mathcal{H}_{\mathbb{C}}(G, B)$ są, na mocy lematu 3.12, specjalizacjami algebry generycznej A systemu Titsa G . Obydwie są też algebrami rozdzielczymi, bo są półproste nad ciałem algebraicznie domkniętym $\mathbb{C}$.¹⁹ W przypadku $\mathbb{C}[W]$ jest to wniosek z twierdzenia Maschke (tw. 1.19), półprostotę $\mathcal{H}_{\mathbb{C}}(G, B)$ dowodziliśmy natomiast w Uwadze 3.3, na podstawie tw. 1.17. Przypomnijmy, że lemat 3.12 dowodziliśmy dla $R = \mathbb{Q}[u_1, u_2, \dots, u_n]$, gdzie $\{u_i \mid 1 \leq i \leq n\}$ spełniają (3.22). Jeśli więc $A^{(R)}$ będzie algebrą rozdzielczą, wówczas $\mathbb{C}[W]$ oraz $\mathcal{H}_{\mathbb{C}}(G, B)$ będą miały te same niezmienniki numeryczne. Jako algebry nad ciałem algebraicznie domkniętym będą zatem izomorficzne. Plan dalszego postępowania jest zatem następujący:

1. Dowód twierdzenia Titsa o deformacji (poniżej).
2. Dowód tego, że $A^{(R)}$ jest rozdzielcza, przy czym $R = \mathbb{Q}[u_1, u_2, \dots, u_n]$ oraz elementy $\{u_i \mid 1 \leq i \leq n\}$ spełniają (3.22) (w następnym paragrafie).

Dowód. (Twierdzenie Titsa) Niech R' będzie domknięciem algebraicznym ciała (R) , natomiast $\overline{R}$ – całkowitym domknięciem R w R' . Niech $n = \dim_{(R)}(A^{(R)})$ i niech $\{t_1, t_2, \dots, t_n\}$ oraz $\{t'_1, t'_2, \dots, t'_n\}$ będą zbiorami elementów algebraicznie niezależnych odpowiednio nad R' oraz $\mathbb{C}$. Niech:

$$\begin{aligned} R[T] &= R[t_1, t_2, \dots, t_n] \\ \overline{R}[T] &= \overline{R}[t_1, t_2, \dots, t_n] \\ R'[T] &= R'[t_1, t_2, \dots, t_n] \\ \mathbb{C}[T'] &= \mathbb{C}[t'_1, t'_2, \dots, t'_n] \end{aligned}$$

¹⁹ Jest to bardzo szczególny przypadek twierdzenia, że K -algebra A jest rozdzielcza wtedy i tylko wtedy, gdy po rozszerzeniu skalarów do algebraicznego domknięcia $\overline{K}$ algebra $A^{\overline{K}}$ jest półprosta ([Cur81], 7.2).

Niech $A = \bigoplus_{i=1}^n Ra_i$, gdzie $\{a_1, a_2, \dots, a_n\}$ jest bazą wolnego R -modułu A . Wówczas element ogólny R' -algebry $A^{R'}$ jest równy $a = \sum_{i=1}^n t_i a_i$. Element ogólny algebry A_f zapisać można jako $a' = \sum_{i=1}^n t'_i a'_i$, gdzie $a'_i = 1 \otimes a_i$, $1 \leq i \leq n$ jest, zgodnie z (3.26), bazą algebry A_f .

Niech $p(x)$ będzie wielomianem charakterystycznym elementu a , zaś $p'(x)$ – wielomianem charakterystycznym elementu a' . Wówczas, zgodnie z argumentacją przytoczoną w tezie lematu 3.13, $p(x) \in R[T][x]$ (stałe strukturalne A są w R). Podobnie $p'(x) \in R[T][x]$. Przekształcenie $f : R \rightarrow \mathbb{C}$ można zatem rozszerzyć do homomorfizmu z $R[T][x]$ do $\mathbb{C}[T][x]$, oznaczanego dalej także przez f , kładąc $f(t_i) = t'_i$ oraz $f(x) = x$. Wynika stąd, że

$$f(p(x)) = p'(x). \quad (3.35)$$

Rozważmy dalej rozkład (3.31) wielomianu $p(x)$. Mamy $p(x) = \prod_{s=1}^S p_s(x)^{p_s}$, gdzie dla każdego $1 \leq s \leq S$, czynniki $p_s(x) \in R'[T][x]$. Wielomian $p(x)$ jest unormowany, a więc jego pierwiastki są całkowite nad $R[T]$. Współczynniki wielomianów $\{p_s(x)\}$, należących do $R'[T][x]$, są funkcjami symetrycznymi pierwiastków wielomianu $p(x)$. Są więc całkowite nad $R[T]$. Stąd, na mocy lematu 3.14, $p_s(x) \in \overline{R}[T][x]$, dla każdego $1 \leq s \leq S$.

Rozszerzmy teraz homomorfizm $f : R \rightarrow \mathbb{C}$ do homomorfizmu $\bar{f} : \overline{R} \rightarrow \mathbb{C}$ (lemat 3.15). Wówczas $f : R[T][x] \rightarrow \mathbb{C}[T][x]$ rozszerza się do homomorfizmu $\bar{f} : \overline{R}[T][x] \rightarrow \mathbb{C}[T][x]$. Stąd korzystając z (3.35) mamy:

$$\bar{f}(p(x)) = p'(x) = \prod \bar{f}(p_s(x))^{p_s},$$

gdzie każdy z wielomianów $\bar{f}(p_s(x))^{p_s}$ należy do $\mathbb{C}[T][x]$. Stąd skoro $p_s = \deg(p_s(x))$, dla każdego s , to $p_s = \deg(\bar{f}(p_s(x)))$. Na mocy punktu (a) lematu 3.13, wykładniki $\{p_s\}$ są zatem niezmiennikami numerycznymi $A^{(R)}$. Na mocy punktu (c) lematu 3.13 widzimy, że $\{p_s\}$ są także niezmiennikami numerycznymi A_f . To kończy dowód. $\square$

W ten sposób zrealizowaliśmy pierwszy punkt na drodze do dowodu izomorfizmu algebr $\mathbb{C}[W] \simeq \mathcal{H}_{\mathbb{C}}(G, B)$. Drugim punktem będzie, jak zapowiedzieliśmy wcześniej, dowód rozdzielczości algebry $A^{(R)}$, przy czym $R = \mathbb{Q}[u_1, u_2, \dots, u_n]$, zaś $\{u_i | 1 \leq i \leq n\}$ spełniają (3.22).

3.4. $\mathcal{H}_{\mathbb{C}}(G, B) \simeq \mathbb{C}[W]$

Celem tego paragrafu jest dowód następującego twierdzenia.

Twierdzenie 3.17. *Niech W będzie grupą Weyla związaną ze skończoną BN-parą G . Niech A będzie algebrą generyczną grupy W nad pierścieniem $R = \mathbb{Q}[u_1, u_2, \dots, u_n]$, gdzie elementy $\{u_i | 1 \leq i \leq n\}$ spełniają (3.22). Wówczas algebra $A^{(R)}$ jest rozdzielcza.*

Jak stwierdziliśmy wcześniej twierdzenie to, łącznie z twierdzeniem Titsa o deformacji, implikuje już izomorfizm $\mathbb{C}[W] \simeq \mathcal{H}_{\mathbb{C}}(G, B)$. Uzasadnienie będzie jednak wymagało bardziej szczegółowego wglądu w teorię algebr rozdzielczych. W tym celu przypominamy następującą definicję:

Definicja 3.18 (Forma śladu). Niech A będzie skończenie wymiarową algebrą nad ciałem K . Określamy następującą formę dwuliniową $T_{A/K} : A \times A \rightarrow K : T_{A/K}(a, b) = \text{Tr}(ab)$, $a, b \in A$, gdzie $\text{Tr}(ab)$ jest śladem przekształcenia liniowego $f_{ab} : A \rightarrow A$ postaci $x \rightarrow abx$, dla $x \in A$. Formę śladu $T_{A/K}(a, b)$ nazywamy **formą niezdegenerowaną** jeśli zachodzi następująca implikacja:

$$(\forall a \in A (T_{A/K}(a, b) = 0)) \Rightarrow b = 0. \quad (3.36)$$

Przypomnijmy, że jeśli zadamy przekształcenie liniowe $f : V \rightarrow V$ w pewnej bazie $\{v_1, v_2, \dots, v_n\}$ przestrzeni V , wówczas jeśli $f(v_i) = \sum_{j=1}^n \alpha_{ij} v_j$, to ślad f wyrazić²⁰ możemy w postaci sumy:

$$\text{tr}(f) = \alpha_{11} + \alpha_{22} + \dots + \alpha_{nn}. \quad (3.37)$$

Wiadomo, że $T_{A/K}$ jest niezdegenerowaną formą dwuliniową na przestrzeni liniowej A z bazą $V = \{v_1, v_2, \dots, v_n\}$ wtedy i tylko wtedy, gdy istnieje jednoznacznie wyznaczona baza $V^* = \{v_1^*, v_2^*, \dots, v_n^*\}$ przestrzeni A , że:

$$T_{A/K}(v_i, v_j^*) = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}. \quad (3.38)$$

Jest to tzw. baza dualna.²¹ Wynik ten można znaleźć w każdym standardowym kursie algebry liniowej. Ma on jednak zasadnicze znaczenie dla dalszych rozważań. Odnotujmy następujące obserwacje.

Uwaga 3.19. Niech $V = \{v_1, \dots, v_n\}$ będzie bazą algebry A nad ciałem K , zaś niech $V^* = \{v_1^*, v_2^*, \dots, v_n^*\}$ będzie bazą dualną do V . Wówczas zachodzą następujące równości:

$$T_{A/K}(a, b) = T_{A/K}(b, a), \quad a, b \in A \quad (3.39)$$

$$a = \sum_{i=1}^n T_{A/K}(a, v_i) v_i^*, \quad a \in A \quad (3.40)$$

$$\sum_{i=1}^n v_i v_i^* = 1 \quad (3.41)$$

Dowód. Równość (3.39) jest oczywista – wystarczy wykazać, że dla każdego $1 \leq i, j \leq n$ zachodzi równość: $T_{A/K}(v_i, v_j) = T_{A/K}(v_j, v_i)$. Rachunek jest identyczny, jak w przypadku dowodu równości śladów iloczynów macierzy kwadratowych AB i BA .

Równość (3.40) wynika natychmiast z (3.38). Rozważmy element bazowy $v_i \in V$ zapisany jako kombinacja liniowa elementów bazy V^* tj. $v_i = \sum_{j=1}^n \alpha_{ij} v_j^*$. Wtedy dla $1 \leq k \leq n$ mamy:

$$T_{A/K}(v_k, v_i) = \sum_{j=1}^n \alpha_{ij} T_{A/K}(v_k, v_j^*) \stackrel{(3.38)}{\Rightarrow} \alpha_{ik} = T_{A/K}(v_k, v_i) \stackrel{(3.39)}{=} T_{A/K}(v_i, v_k).$$

Innymi słowy:

$$v_i = \sum_{k=1}^n T_{A/K}(v_i, v_k) v_k^*.$$

²⁰Wynik jest niezależny od wyboru bazy V .

²¹Jest to baza dualna znana z algebry liniowej. Dokładniej, niech A^* stanowi przestrzeń liniową sprzężoną do A . Wówczas jeśli $T_{A/K}$ jest niezdegenerowana to, odwzorowanie $\psi : A \rightarrow A^*$ zadane formułą $v \rightarrow (x \rightarrow T_{A/K}(v, x))$ jest izomorfizmem przestrzeni liniowych, zaś obrazy elementów bazy V są przy tym odwzorowaniu elementami bazy dualnej V^* .

Dowodzimy (3.41). Niech lewa strona (3.41) będzie równa $e \in A$. Wówczas, z definicji $T_{A/K}$, dla każdego $a \in A$:

$$\text{tr}(ae) = \sum_{i=1}^n \text{tr}(av_i v_i^*) = \sum_{i=1}^n T_{A/K}(av_i, v_i^*).$$

Zgodnie z (3.40) wyrażenie po prawej stronie powyższej równości wynosi dokładnie $\text{tr}(a)$. Wynika to z (3.37) zastosowanego do przekształcenia $x \rightarrow ax$, dla $x \in A$, gdzie ślad obliczony jest względem bazy V^* . Stąd dla każdego $a \in A$ mamy $\text{tr}(ea) = \text{tr}(a)$. Stąd dla każdego $a \in A$:

$$\text{tr}((e-1)a) = T_{A/K}(e-1, a) \stackrel{(3.39)}{=} T_{A/K}(a, e-1) = 0.$$

Z założenia o istnieniu bazy dualnej wiemy jednak, że $T_{A/K}$ jest niezdegenerowana, zatem $e = 1$. $\square$

Forma śladu jest, jak się okazuje, wygodnym narzędziem do badania rozdzielczości algebry. Plan dowodu twierdzenia 3.17 jest następujący:

1. Dowód tego, że skończenie wymiarowa K -algebra A jest rozdzielcza wtedy, gdy $T_{A/K}$ jest formą niezdegenerowaną (tw. 3.20).
2. Dowód, że forma $T_{A^{(R)}/(R)}$ jest niezdegenerowana.

Zacniemy od punktu pierwszego.

Twierdzenie 3.20. *Niech A będzie skończenie wymiarową algebrą nad ciałem K . Wówczas A jest rozdzielcza wtedy, gdy $T_{A/K}$ jest formą niezdegenerowaną.*

Dowód. Zacniemy od wykazania, że jeśli $T_{A/K}$ jest formą niezdegenerowaną, wówczas A jest półprosta jako K -algebra. Rozważmy A -moduł lewostronny X . Wykażemy, że jest to moduł półprosty, a więc to, że każdy podmoduł Y modułu X wydziela się jako składnik prosty w X . Zrobimy to przez indukcję ze względu na wymiar X nad ciałem K . Dla wymiaru 1 teza jest oczywista. Niech X ma wymiar r . Jeśli X jest modułem prostym, wówczas nie ma czego dowodzić. Załóżmy więc, że Y jest podmodułem w X . Y ma bazę $\{y_1, y_2, \dots, y_r\}$, zaś X ma bazę $\{y_1, \dots, y_r, x_1, \dots, x_s\}$. Niech $\phi : X \rightarrow Y$ będzie rzutem modułu X na Y (jako K -modułów) dany wzorem:

$$\phi(y_i) = y_i, \quad \phi(x_j) = 0, \quad k\phi(x) = \phi(kx) \quad (3.42)$$

gdzie $k \in K$, $x \in X$, $1 \leq i \leq r$, $1 \leq j \leq s$. Określamy przekształcenie $[\phi] : X \rightarrow X$ dane wzorem:

$$[\phi](x) := \sum_{i=1}^n v_i \phi(v_i^* x). \quad (3.43)$$

Łatwo pokazać, że $[\phi]$ nie zależy od wyboru bazy $\{v_1, v_2, \dots, v_n\}$ algebry A . Sprawdźmy, że jest to homomorfizm A -modułów, tzn. dla każdego $a \in A$ oraz $x \in X$ mamy:

$$a[\phi](x) = [\phi](ax). \quad (3.44)$$

Istotnie, z (3.40) wiadomo, że dla $1 \leq i \leq n$ mamy:

$$av_i = \sum_{j=1}^n T_{A/K}(av_i, v_j^*) v_j \quad (3.45)$$

$$v_i^* a = \sum_{j=1}^n T_{A/K}(v_i^* a, v_j) v_j^* \quad (3.46)$$

Stąd dla każdego $x \in X$:

$$\begin{aligned}
a[\phi](x) &\stackrel{(3.43)}{=} \sum_{i=1}^n av_i\phi(v_i^*x) \\
&\stackrel{(3.45)}{=} \sum_{i=1}^n \sum_{j=1}^n T_{A/K}(av_i, v_j^*)v_j\phi(v_i^*x) \\
&\stackrel{(3.42)}{=} \sum_{i,j=1}^n v_j\phi(T_{A/K}(av_i, v_j^*)v_i^*x) \\
&\stackrel{(3.39)}{=} \sum_{i,j=1}^n v_j\phi(T_{A/K}(v_j^*a, v_i)v_i^*x) \\
&\stackrel{(3.46)}{=} \sum_{j=1}^n v_j\phi(v_j^*ax) \\
&\stackrel{(3.43)}{=} [\phi](ax).
\end{aligned}$$

Przekształcenie ϕ jest homomorfizmem A -modułów i identycznością na Y . Dla każdego $y \in Y$ mamy także:

$$\begin{aligned}
[\phi](y) &\stackrel{(3.43)}{=} \sum_{i=1}^n v_i\phi(v_i^*y) \\
&\stackrel{(3.44)}{=} \sum_{i=1}^n v_iv_i^*\phi(y) \\
&\stackrel{(3.42)}{=} \sum_{i=1}^n v_iv_i^*y \\
&= \left(\sum_{i=1}^n v_iv_i^* \right) y \\
&\stackrel{(3.41)}{=} y.
\end{aligned}$$

Z drugiej strony, jeśli $x \in X$, wówczas:

$$\begin{aligned}
[\phi]^2(x) &\stackrel{(3.43)}{=} [\phi] \left(\sum_{i=1}^n v_i\phi(v_i^*x) \right) \\
&\stackrel{(3.43)}{=} \sum_{i=1}^n \sum_{j=1}^n v_j\phi \left(\underbrace{v_j^*v_i\phi(v_i^*x)}_{\in Y} \right) \\
&\stackrel{(3.42)}{=} \sum_{i=1}^n \sum_{j=1}^n v_jv_j^*v_i\phi(v_i^*x) \\
&\stackrel{(3.41)}{=} \sum_{i=1}^n v_i\phi(v_i^*x) \\
&\stackrel{(3.43)}{=} [\phi](x).
\end{aligned}$$

Stąd $[\phi]^2 = [\phi]$, oraz $(Id - [\phi])^2 = Id - 2[\phi] + [\phi]^2 = 1 - [\phi]$. Zatem:

$$X = Id \cdot X = ([\phi] + Id - [\phi])X = [\phi]X + (Id - [\phi])X.$$

Zgodnie z formułą (3.44) przekształcenie $[\phi]$ jest homomorfizmem A -modułów, zatem $[\phi]X$ jest A -podmodulem X , podobnie $(Id - [\phi])X$ jest A -podmodulem X . Mają one zerowe

przecięcie. Uzyskaliśmy zatem rozkład A -modułu X na sumę prostą A -podmodułów postaci $[\phi]X \oplus (1 - [\phi])X$. Wymiary modułów $[\phi]X, (Id - [\phi])X$ są mniejsze niż wymiar X , zatem z założenia indukcyjnego są one półproste. To kończy dowód półprostoty M , wraz z nią półprostoty A .

Niech $E \supset K$ będzie rozszerzeniem ciał. Chcemy udowodnić, że jeśli $T_{A/K}$ jest formą niezdegenerowaną, to A^E jest algebrą półprostą. Wówczas A będzie algebrą rozdzielczą.

Niech $V = \{v_1, v_2, \dots, v_n\}$ będzie bazą algebry A . Zgodnie z założeniem twierdzenia oraz z formułą (3.38) istnieje baza dualna do V , tzn. $V^* = \{v_1^*, \dots, v_n^*\}$. Zgodnie z 3.26 bazę algebry A^E nad ciałem E stanowią elementy postaci $V' = \{1 \otimes v_i \mid 1 \leq i \leq n\}$. Łatwo widzieć, że bazę dualną do V' stanowią elementy postaci: $(V')^* = \{1 \otimes v_i^* \mid 1 \leq i \leq n\}$. Wobec tego forma $T_{A^E/E}$ jest niezdegenerowana (spełniony jest bowiem warunek (3.38)) Zatem algebra A^E jest półprosta, zgodnie z przedstawionym wyżej rozumowaniem. $\square$

Przejdziemy teraz do dowodu głównego wyniku tego paragrafu, a więc twierdzenia 3.17. Przypomnijmy, że zgodnie z rozważaniami z poprzedniego paragrafu fakt ten jest jedynym brakującym fragmentem stojącym pomiędzy miejscem, do którego dotarliśmy, a ostatecznym dowodem izomorfizmu $\mathcal{H}_{\mathbb{C}}(G, B) \simeq \mathbb{C}[W]$.

Dowód twierdzenia 3.17. Przypomnijmy tezę twierdzenia. Niech G będzie skończoną grupą z BN -parą, której grupa Weyla to W . Rozważamy algebrę generyczną A grupy W nad pierścieniem $R = \mathbb{Q}[u_1, u_2, \dots, u_n]$, gdzie $\{u_i \mid 1 \leq i \leq n\}$ spełniają (3.22). Mamy wykazać rozdzielczość algebry $A^{(R)}$, gdzie (R) jest ciałem ułamków pierścienia R . Zgodnie z twierdzeniem 3.20 wystarczy wykazać, że forma $T_{A^{(R)}/(R)} : A^{(R)} \times A^{(R)} \rightarrow (R)$ jest niezdegenerowana.

Założmy, że $W = \{w_1, w_2, \dots, w_n\}$. Baza algebry A to $\{e_{w_i} \mid 1 \leq i \leq n\}$ natomiast, zgodnie z (3.26), baza algebry $A^{(R)}$ składa się z elementów postaci $\{1 \otimes e_{w_i} \mid 1 \leq i \leq n\}$. Niech e_{w_i}, e_{w_j} będą, dla pewnych $1 \leq i \neq j \leq n$, elementami bazy algebry generycznej A . Pokażemy, że $T_{A^{(R)}/(R)}(1 \otimes e_{w_i}, 1 \otimes e_{w_j}) \in R$. Istotnie, rozważmy endomorfizm algebry $A^{(R)}$ postaci:

$$a \rightarrow (1 \otimes e_{w_i})(1 \otimes e_{w_j})a, \quad a \in A^{(R)}. \quad (3.47)$$

Aby policzyć ślad tego endomorfizmu wystarczy, zgodnie z (3.37), wyznaczyć k -te współrzędne obrazów elementów bazowych $\{1 \otimes e_{w_k}\}$ algebry $A^{(R)}$ przy tym endomorfizmie. Zauważmy, że:

$$(1 \otimes e_{w_i})(1 \otimes e_{w_j})(1 \otimes e_{w_k}) = 1 \otimes e_{w_i}e_{w_j}e_{w_k}.$$

Wiadomo, że $e_{w_i}e_{w_j}e_{w_k} \in A$ jest kombinacją liniową elementów bazowych $\{e_{w_s}, 1 \leq s \leq n\}$ postaci:

$$e_{w_i}e_{w_j}e_{w_k} = \sum_{s=1}^n \alpha_{ks} e_{w_s}. \quad (3.48)$$

Zgodnie z (3.27) wiadomo, że stałe strukturalne algebry generycznej A należą do pierścienia $R = \mathbb{Q}[u_1, u_2, \dots, u_n]$. Oznacza to, że także stałe $\{\alpha_{ks}, 1 \leq s \leq n\}$, występujące w wyrażeniu (3.48) należą, dla każdego $1 \leq s \leq n$, do pierścienia R . Stąd, zgodnie z (3.37), ślad endomorfizmu określonego w (3.47) też należy do R .

Niech $f : R \rightarrow F$ będzie specjalizacją pierścienia R do ciała F charakterystyki 0. Rozważmy algebrę specjalizacji A_f . Jeśli T jest formą śladu na $A^{(R)}$, zaś T_f formą śladu dla A_f , to

$$f(T(e_{w_i}, e_{w_j})) = T_f(e'_{w_i}, e'_{w_j}), \quad 1 \leq i \neq j \leq n.$$

Wynika to natychmiast z dwuliniowości śladu i z faktu, że obrazami stałych strukturalnych algebry $A^{(R)}$ są, zgodnie z (3.28), stałe strukturalne algebry A_f . Wynika stąd, że jeśli forma T_f jest niezdegenerowana, to także forma T jest niezdegenerowana. W szczególności, jeśli pokażemy, że dla konkretnej specjalizacji $f : R \rightarrow F$ forma T_f jest niezdegenerowana, wówczas dowód będzie zakończony.

Weźmy specjalizację $f' : R \rightarrow \mathbb{Q}$ tak, jak w lemacie 3.12. Otrzymujemy wówczas $A_{f'} \simeq \mathbb{Q}[W]$.²² Do zakończenia dowodu wystarczy pokazać, że $T_{f'}$ jest niezdegenerowana na $\mathbb{Q}[W]$.

Funkcja śladu $T_{f'}$ na $\mathbb{Q}[W]$, to nic innego jak charakter reprezentacji regularnej grupy W w przestrzeni liniowej nad ciałem $\mathbb{Q}$. Stąd zgodnie z (1.15):

$$T_{f'}(a_w) = \begin{cases} |W|, & w = 1 \\ 0, & w \neq 1 \end{cases}$$

Niech $h \in \mathbb{Q}[W]$. Wtedy $h = \sum_{w \in W} \lambda_w w$, gdzie $\lambda_w \in \mathbb{Q}$. Załóżmy, że $T_{f'}(hh') = 0$ dla wszystkich $h' \in \mathbb{Q}[W]$. W szczególności mamy:

$$T_{f'}\left(\sum_{w \in W} \lambda_w wx\right) = 0, \quad x \in W.$$

Jednak $T_{f'}(wx) = 0$ jeśli $w \neq x^{-1}$, zatem $|W|\lambda_{x^{-1}} = 0$ dla wszystkich $x \in W$. Stąd $\lambda_x = 0$ dla wszystkich $x \in W$. Zatem $h = 0$, a więc $T_{f'}$ jest niezdegenerowana.

* * *

W ten sposób dowód (3.1) został zakończony. Przez lata poszukiwano wzorów opisujących wprost izomorfizm pomiędzy $\mathcal{H}_{\mathbb{C}}(G, B)$, a $\mathbb{C}[W]$. Udało się to dopiero Lusztigowi w 1981r. i opisane zostało w pracy [Lus81]. Był to jeden z pierwszych wyników wykorzystujących (i zarazem motywujących powstanie) ważnego narzędzia teorii grup Coxetera, tzw. wielomiany Kazhdana-Lusztiga.²³

²²Ciało $\mathbb{Q}$ wybieramy po to, aby mieć pewność, że istnieje specjalizacja $f' : R \rightarrow \mathbb{Q}$, a więc zgodnie z tezą lematu 3.12 – bierzemy ciało charakterystyki 0.

²³O historii i znaczeniu wielomianów Kazhdana-Lusztiga przeczytać można w artykule przeglądowym F. Brenti, [Bre03].

Rozdział 4

Monoid Rennera

Na początku lat 80' XX wieku dwójka niezależnie działających matematyków: Lex Renner oraz Mohan Putcha rozpoczęła badania mające na celu przeniesienie teorii grup algebraicznych, zwłaszcza grup reduktywnych (def. 2.14), na grunt półgrupowy. Próby te okazały się owocne i zaowocowały wynikami mieszczącymi się dziś w tzw. teorii monoidów algebraicznych. Znajdują one zastosowania m.in. w teorii reprezentacji, geometrii zbiorów wypukłych, algebraicznej teorii grup.

Czym jest monoid algebraiczny? Niech $\mathbb{K} = \overline{\mathbb{K}}$. W paragrafie 1.4 rozważaliśmy przykład pełnego monoidu liniowego $M_n(\mathbb{K})$ (przykład 1.31). Jest to, jak stwierdziliśmy, zbiór algebraiczny nad ciałem $\mathbb{K}$ o tej własności, że mnożenie elementów $M_n(\mathbb{K})$ jest funkcją regularną. Przez analogię do definicji 1.33 (grupy algebraicznej) powiemy, że monoid M jest **monoidem algebraicznym** jeśli M jest podmonoidem $M_n(\mathbb{K})$ domkniętym w topologii Zariskiego na $M_n(\mathbb{K})$.

W każdym monoidzie M wyróżnić można grupę elementów odwracalnych $U(M)$. Jeśli monoid M ma strukturę zbioru algebraicznego, wówczas $U(M)$ jest grupą algebraiczną. Niech B będzie podgrupą Borela $U(M)$. Wówczas możemy rozważać działanie $B \times B$ na M zadane, podobnie jak w (2.1), wzorem:

$$(b_1, b_2)m = b_1mb_2^{-1}, \quad b_1, b_2 \in B, m \in M. \quad (4.1)$$

Orbity działania (4.1) nazywać będziemy, podobnie jak w rozdziale 3., **(B, B) -warstwami** M .

Określiwszy działanie (4.1) możemy pytać: czy istnieje analog rozkładu Bruhat monoidu M w przypadku półgrupowym? Jeśli tak, to w jaki sposób rozkład ten związany jest z strukturą półgrupową monoidu M ? Celem tego rozdziału jest rozważenie tych zagadnień w przypadku pełnego monoidu liniowego. W szczególności, udowodnimy następujące twierdzenie pochodzące od Rennera [Ren95].

Twierdzenie 4.1. *Niech $M_n(\mathbb{K})$ będzie pełnym monoidem liniowym, zaś $B_n(\mathbb{K})$ niech będzie podgrupą macierzy górnortrójkątnych w $M_n(\mathbb{K})$. Wówczas ma miejsce następujący rozkład $M_n(\mathbb{K})$ na $(B_n(\mathbb{K}), B_n(\mathbb{K}))$ -warstwy:*

$$M_n(\mathbb{K}) = \bigcup_{\sigma \in R_n} B_n(\mathbb{K})\sigma B_n(\mathbb{K}), \quad (4.2)$$

gdzie R_n jest półgrupą złożoną ze wszystkich macierzy mających w każdym wierszu i w każdej kolumnie co najwyżej niezerowy element równy 1.

Półgrupa R_n będzie nazywana dalej **monoidem Rennera**. Pokażemy też, że istnieje ścisły związek pomiędzy strukturą półgrupową $M_n(\mathbb{K})$, a strukturą półgrupową R_n .

Twierdzenie 4.2. *Rozważmy relację Greena $\mathcal{J}$ (definicja 1.6) na $M_n(\mathbb{K})$, oznaczaną dalej przez $\mathcal{J}_1$, oraz relację Greena $\mathcal{J}$ na R_n , oznaczaną dalej przez $\mathcal{J}_2$. Zbiór ilorazowy relacji $\mathcal{J}_1$ oznaczmy przez $\mathcal{M}$, zaś zbiór abstrakcji relacji $\mathcal{J}_2$ przez $\mathcal{R}$. Niech M będzie dowolną $\mathcal{J}_1$ -klasą na $M_n(\mathbb{K})$. Wówczas istnieje dokładnie jedna $\mathcal{J}_2$ -klasa R na R_n , że $R \subset M$. Co więcej:*

$$M_n(\mathbb{K}) = \bigcup_{M \in \mathcal{M}} M = \bigcup_{M \in \mathcal{M}} \left(\bigcup_{\sigma \in \mathcal{R} \cap M} B_n(\mathbb{K}) \sigma B_n(\mathbb{K}) \right).$$

Włączając te zagadnienia do naszej pracy chcemy pokazać, że rozważanie rozkładu Bruhat w przypadku półgrupowym nie jest motywowane jedynie chęcią uogólnienia określonych wyników teorii grup, ale może być także źródłem wyników strukturalnych nie związanych bezpośrednio z teorią grup.

Oczywiście, poszukiwania półgrupowych uogólnień rozmaitych konstrukcji znanych z teorii grup nie ograniczyły się jedynie do wyróżnienia klasy monoidów algebraicznych czy do prób rozstrzygnięcia pytań o istnienie analogu rozkładu Bruhat. Pytano także o istnienie półgrupowych analogów grup reduktywnych, systemów Titsa, algebr Hecke itd. 30 lat badań nad monoidami algebraicznymi pozwoliło odpowiedzieć twierdząco na wiele z wymienionych wyżej pytań. Dla przykładu, M. Putcha pokazał w [Put93], że jeśli rozważymy półgrupowy analog algebry Hecke pełnego monoidu macierzy, zdefiniowany w następujący sposób:

$$\mathcal{H}_{\mathbb{C}}(M, B) := e\mathbb{C}[M]e, \quad e = |B|^{-1}[B],$$

gdzie $M = M_n(\mathbb{F}_q)$, $B = B_n(\mathbb{F}_q)$ wówczas ma miejsce analog dowodzonego przez nas w rozdziale 3. twierdzenia Titsa:

$$\mathcal{H}_{\mathbb{C}}(M, B) \simeq \mathbb{C}[R_n].$$

Związłą prezentację powyższych zagadnień znaleźć można np. w artykule Solomona [Sol95].

W kolejnych paragrafach tego rozdziału przedstawimy:

- w paragrafie 4.1 – dowód twierdzenia 4.1,
- w paragrafie 4.2 – omówienie struktury półgrupowej pełnego monoidu liniowego,
- w paragrafie 4.3 – omówienie struktury półgrupowej monoidu Rennera R_n ,
– dowód twierdzenia 4.2.

Zasadniczym punktem odniesienia będzie dla nas monografia Oknińskiego [Okn98].

4.1. Analog rozkładu Bruhat w $M_n(\mathbb{K})$

Celem tego krótkiego paragrafu jest dowód twierdzenia 4.1. Naśladuje on dowód twierdzenia 2.1 przedstawiony w rozdziale 2. Aby uzyskać tezę udowodnimy następujące dwa lematy:

Lemat 4.3. *Niech $A \in M_n(\mathbb{K})$. Wówczas istnieje $P \in S_n$ oraz $L, M \in B_n(\mathbb{K})$, że:*

$$A = LPM. \quad (4.3)$$

Lemat 4.4. *Niech $\sigma_1, \sigma_2 \in R_n$. Wówczas:*

$$B_n(\mathbb{K})\sigma_1 B_n(\mathbb{K}) = B_n(\mathbb{K})\sigma_2 B_n(\mathbb{K}) \Rightarrow \sigma_1 = \sigma_2$$

Zanim przystąpimy do dowodu przypomnijmy oznaczenia stosowane w rozdziale 2. Jeśli $A \in M_n(\mathbb{K})$, wówczas i -ty wiersz macierzy A oznaczamy przez $w_i(A)$, zaś j -tą kolumnę A oznaczamy przez $k_j(A)$. Bazę standardową przestrzeni $\mathbb{K}^n$ oznaczamy przez $e_1, e_2, \dots, e_n$. Niech $1 \leq i \leq n$. Określamy funkcję $l_i : M_n(\mathbb{K}) \rightarrow \{0, 1, \dots, n\}$:

$$l_i(A) = \begin{cases} \min\{k \mid a_{ki} \neq 0\} & , \text{ jeśli } k_i(A) \text{ nie jest zerowa,} \\ 0 & , \text{ w przeciwnym przypadku.} \end{cases}$$

Dowód. (Lemat 4.3)

Weźmy macierz $A \in M_n(\mathbb{K})$. Rozkład (4.3) uzyskujemy w n krokach. W pierwszym kroku patrzymy na $k_1(A)$. Jeśli jest to kolumna zerowa, wówczas kładziemy $X^{(1)} := Id, Y^{(1)} := Id$ i przechodzimy do następnego kroku. Jeśli $w_1(A)$ nie jest zerowa, wówczas podobnie jak w dowodzie lematu 2.4 można wskazać macierze $X^{(1)} \in B_n^-(\mathbb{K})$ i $Y^{(1)} \in B_n(\mathbb{K})$, że:

$$k_1(X^{(1)}AY^{(1)}) = e_{l_1}, \quad w_1(X^{(1)}AY^{(1)}) = e_1.$$

W $t+1$. kroku dysponujemy macierzą $A^{(k)} := X^{(t)}A^{(t-1)}Y^{(t)}$. Wśród jej pierwszych t kolumn występują wektory zerowe lub jednostkowe. Jeśli $k_i(A^{(t)})$ nie jest zerowa dla $1 \leq i \leq t$, wówczas $w_{l_i}(A^{(t)}) = e_i$. W kroku tym patrzymy na kolumnę $k_{t+1}(A^{(t)})$. Jeśli jest ona zerowa, wówczas kładziemy $X^{(t+1)} := Id, Y^{(t+1)} := Id, A^{(t+1)} := X^{(t+1)}A^{(t)}Y^{(t+1)}$ i przechodzimy do kolejnego (o ile $k+1 \leq n$) kroku. W przeciwnym przypadku niech $l_{k+1} := l_{k+1}(A^{(t)})$. Znajdujemy dalej macierze $X^{(t+1)} \in B_n^-(\mathbb{K}), Y^{(t+1)} \in B_n(\mathbb{K})$, takie, że:

$$k_i(X^{(t+1)}A^{(t)}Y^{(t+1)}) = \begin{cases} k_i(A^{(t)}) & , i \leq t \\ e_{l_{t+1}} & , i = t+1 \end{cases}$$

$$w_{l_i}(X^{(t+1)}A^{(t)}Y^{(t+1)}) = e_i, \quad \text{jeśli } l_i \neq 0, 1 \leq i \leq t+1.$$

Macierze takie można wskazać wprost, podobnie jak w dowodzie lematu 2.4. Dalsze rozumowanie także jest analogiczne. Po n krokach otrzymujemy macierz:

$$A^{(n)} = X^{(n)}X^{(n-1)} \dots X^{(2)}X^{(1)} \cdot A \cdot Y^{(1)}Y^{(2)} \dots Y^{(n-1)}Y^{(n)},$$

która w każdym wierszu i w każdej kolumnie ma co najwyżej jeden element niezerowy równy 1. Jest to zatem element R_n . Dostajemy zatem tezę lematu 4.3, ponieważ zgodnie z wzorem (2.4) istnieje macierz permutacyjna P , że:

$$PA^{(n)} = \underbrace{\left(PX^{(n)}X^{(n-1)} \dots X^{(2)}X^{(1)} \right)}_{B_n(\mathbb{K})} \cdot A \cdot \underbrace{\left(Y^{(1)}Y^{(2)} \dots Y^{(n-1)}Y^{(n)} \right)}_{B_n(\mathbb{K})},$$

a stąd:

$$A = \underbrace{\left(PX^{(n)} X^{(n-1)} \dots X^{(2)} X^{(1)} \right)^{-1}}_{B_n(\mathbb{K})} \cdot \underbrace{\left(PA^{(n)} \right)}_{R_n} \cdot \underbrace{\left(Y^{(1)} Y^{(2)} \dots Y^{(n-1)} Y^{(n)} \right)^{-1}}_{B_n(\mathbb{K})}.$$

□

Dowód jednoznaczności rozkładu, a więc lematu 4.4, jest analogiczny z dowodem lematu 2.5. Dowód twierdzenia 4.1 jest zatem zakończony.

4.2. Pełen monoid liniowy

Paragraf ten poświęcony jest omówieniu struktury półgrupowej pełnego monoidu macierzy nad ciałem. Interesować nas będzie postać klas Greena, struktura ideałów oraz prezentacja Reesa czynników głównych tego monoidu. Dla większej przejrzystości zapisu elementy zbioru $M_n(\mathbb{K})$ będziemy w tym rozdziale oznaczali małymi, a nie jak dotychczas – wielkimi, literami.

Przypomnijmy podstawowe oznaczenia z algebry liniowej. Przez **rzęd** $rz(a)$ macierzy kwadratowej $a \in M_n(\mathbb{K})$ rozumiemy wymiar przestrzeni liniowej nad $\mathbb{K}$ rozpiętej przez kolumny a . Wiadomo, że wielkość ta równa jest wymiarowi przestrzeni rozpiętej przez wiersze tejże macierzy. Podzbiór $M_n(\mathbb{K})$ zawierający macierze rzędu nie większego niż j oznaczać będziemy dalej przez M_j . Macierz a rzędu $j \leq n$ można przy pomocy **elementarnych operacji** wierszowych (odp. kolumnowych) przekształcić do **zredukowanej postaci** wierszowej (odp. kolumnowej). Postać ta ma następujące własności:

1. Współczynnik wiodący każdego niezerowego wiersza (odp. każdej niezerowej kolumny) wynosi 1.
2. Dla każdego $i \leq j$, współczynnik wiodący $i + 1$. wiersza (odp. kolumny) znajduje się w kolumnie (odp. wierszu) o indeksie dalszym niż współczynnik wiodący z wiersza (odp. kolumny) i .
3. Współczynnik wiodący niezerowego wiersza (odp. kolumny) A jest jedynym niezerowym elementem kolumny (odp. wiersza) go zawierającej.

Przykład 4.5. *Przykłady macierzy kwadratowych w formie zredukowanej:*

- *wierszowej:*

$$\begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 5 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

- *kolumnowej:*

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & 1 & 0 & 0 \end{pmatrix}$$

Wiadomo, że każdej macierzy nad ciałem $\mathbb{K}$ odpowiada dokładnie jedna postać kolumnowa (odp. wierszowa). Przez X_j (odp. Y_j) oznaczamy będziemy zbiór wszystkich elementów $M_n(\mathbb{K})$ rzędu j będących w zredukowanej formie kolumnowej (odp. wierszowej). Łatwo widzieć, że jeśli $e \in X_j \cap Y_j$, wówczas $e = e_j = \begin{pmatrix} id_j & 0 \\ 0 & 0 \end{pmatrix}$, gdzie $id_j \in Gl_j(\mathbb{K})$ jest macierzą identyczności.

Niech $a \in M_n(\mathbb{K})$. Algorytm Gaussa pozwala jednoznacznie określić skończony i uporządkowany ciąg operacji wierszowych (odp. kolumnowych) prowadzących dla każdej macierzy A do uzyskania zredukowanej formy wierszowej (odp. kolumnowej). Operacje te to: mnożenie wiersza (odp. kolumny) przez niezerowy skalar, dodawanie wielokrotności jednego wiersza do drugiego (odp. dla kolumn) oraz zamiana wierszy (odp. zamiana kolumn). Są one opisane przez odpowiednie macierze przekształceń elementarnych. Przekształcenie dowolnej macierzy kwadratowej do zredukowanej postaci kolumnowej (odp. wierszowej) polega na przemnożeniu jej z prawej (odp. z lewej) strony przez macierz będącą iloczynem macierzy operacji elementarnych. Macierz złożenia operacji kolumnowych oznaczamy będziemy przez k_a (odp. macierz złożenia operacji wierszowych oznaczamy przez w_a). Oczywiście k_a (odp. w_a) to macierz odwracalna. Aby uzyskać zredukowaną formę wierszową (odp. kolumnową) macierzy a należy ją przemnożyć z lewej strony przez w_a (odp. z prawej strony przez k_a). Wiemy już, że iloczyn $w_a \cdot a \cdot k_a$ jest macierzą postaci $\begin{pmatrix} id_j & 0 \\ 0 & 0 \end{pmatrix}$, ozn. e_a gdzie $\mathbf{rz}(e_a) = \mathbf{rz}(a)$.

Wprowadziwszy niezbędne oznaczenia możemy przejść do sformułowania pierwszego twierdzenia tego paragrafu.

Twierdzenie 4.6. Niech $a, b \in M_n(\mathbb{K})$. Wówczas równoważne są następujące warunki:

1. $Gl_n(\mathbb{K})aGl_n(\mathbb{K}) = Gl_n(\mathbb{K})bGl_n(\mathbb{K})$
2. $M_n(\mathbb{K})aM_n(\mathbb{K}) = M_n(\mathbb{K})bM_n(\mathbb{K})$
3. $\mathbf{rz}(a) = \mathbf{rz}(b)$

Dowód. Implikacja (1) $\Rightarrow$ (2) jest oczywista. Zaczniemy więc od dowodu (2) $\Rightarrow$ (3). Zgodnie z (2) istnieją macierze $p, q, r, s \in M_n(\mathbb{K})$, że $a = pbq$, $b = ras$. Zauważmy, że zachodzą następujące nierówności: $\mathbf{rz}(a) \geq \mathbf{rz}(ras) = \mathbf{rz}(b)$. Analogicznie pokazujemy nierówność $\mathbf{rz}(b) \geq \mathbf{rz}(a)$. W rezultacie $\mathbf{rz}(a) = \mathbf{rz}(b)$. W przypadku implikacji (3) $\Rightarrow$ (1) podamy dwa uzasadnienia. Pierwszy korzysta bezpośrednio z wprowadzonych oznaczeń, drugi natomiast pozwoli nam na istotne uproszczenia w dowodach faktów, które sformułujemy w dalszej części paragrafu.

Dowód 1. implikacji (3) $\Rightarrow$ (1)

Założmy, że $\mathbf{rz}(a) = \mathbf{rz}(b) = j$. Stąd $e_a = e_b \Leftrightarrow w_a \cdot a \cdot k_a = w_b \cdot b \cdot k_b$. Zatem:

$$\begin{aligned} a &= (w_a^{-1}w_b) \cdot b \cdot (k_bk_a^{-1}) \in Gl_n(\mathbb{K})bGl_n(\mathbb{K}) \\ b &= (w_b^{-1}w_a) \cdot a \cdot (k_ak_b^{-1}) \in Gl_n(\mathbb{K})aGl_n(\mathbb{K}) \end{aligned}$$

Stąd oczywiście $Gl_n(\mathbb{K})aGl_n(\mathbb{K}) = Gl_n(\mathbb{K})bGl_n(\mathbb{K})$.

Dowód 2. implikacji (3) $\Rightarrow$ (1)

Założmy, że $\mathbf{rz}(a) = \mathbf{rz}(b) = j$. Oznacza to, że przestrzenie liniowe nad $\mathbb{K}$ rozpięte przez kolumny tych macierzy są izomorficzne. Oznaczmy je jako $a\mathbb{K}^n, b\mathbb{K}^n$. Można wskazać macierz

odwracalną $g \in Gl_n(\mathbb{K})$ taką, że $ga\mathbb{K}^n = b\mathbb{K}^n$.

Niech $E = \{e_1, e_2, \dots, e_n\}$ będzie taką bazą $\mathbb{K}^n$, że $b(e_1), b(e_2), \dots, b(e_j)$ jest bazą przestrzeni $b\mathbb{K}^n$. Możemy wybrać teraz pewną bazę $F = \{f_1, f_2, \dots, f_n\}$ przestrzeni $\mathbb{K}^n$, aby $ga(f_i) = b(e_i)$ dla $1 \leq i \leq j$. Innymi słowy, wybieramy dwie bazy $\mathbb{K}^n$ tak, by po zastosowaniu przekształceń a, b obrazy pierwszych j wektorów dawały bazy $a\mathbb{K}^n, b\mathbb{K}^n$ i to takie bazy, by g obcięta do pierwszych j wierszy i kolumn była macierzą przejścia między tymi bazami:

$$\begin{array}{ccc}
 \overbrace{a(f_1), a(f_2), \dots, a(f_j), \dots}^{\text{baza } a\mathbb{K}^n} & \xrightarrow[\substack{g(a(f_i)) = b(e_i) \\ g \in Gl_n(\mathbb{K})}]{} & \overbrace{b(e_1), b(e_2), \dots, b(e_j), \dots}^{\text{baza } b\mathbb{K}^n} \\
 \uparrow a & & \uparrow b \\
 f = (f_1, f_2, \dots, f_j, \dots, f_n) & \xleftarrow[\substack{h(e_i) = f_i \\ h \in Gl_n(\mathbb{K})}]{} & e = (e_1, e_2, \dots, e_j, \dots, e_n)
 \end{array} \quad (***)$$

Jest zatem oczywiste, że biorąc macierz $h \in Gl_n(\mathbb{K})$ przejścia pomiędzy bazami E, F przestrzeni $\mathbb{K}^n$ dostaniemy równość: $b = gah$. Stąd $b \in Gl_n(\mathbb{K})aGl_n(\mathbb{K})$. Analogicznie $a \in Gl_n(\mathbb{K})bGl_n(\mathbb{K})$. Zatem tak, jak chcieliśmy $Gl_n(\mathbb{K})aGl_n(\mathbb{K}) = Gl_n(\mathbb{K})bGl_n(\mathbb{K})$. $\square$

Twierdzenie 4.6 można przetłumaczyć na język $\mathcal{J}$ -klas Greena monoidu $M_n(\mathbb{K})$.

Twierdzenie 4.7. *Relacje Greena na $M_n(\mathbb{K})$ mają następującą postać:*

$$\begin{array}{llll}
 a\mathcal{J}b & \Leftrightarrow & Gl_n(\mathbb{K})aGl_n(\mathbb{K}) = Gl_n(\mathbb{K})bGl_n(\mathbb{K}) & \Leftrightarrow & rz(A) = rz(B) \\
 a\mathcal{R}b & \Leftrightarrow & aGl_n(\mathbb{K}) = bGl_n(\mathbb{K}) & \Leftrightarrow & Im(a) = Im(b) \\
 a\mathcal{L}b & \Leftrightarrow & Gl_n(\mathbb{K})a = Gl_n(\mathbb{K})b & \Leftrightarrow & ker(a) = ker(b).
 \end{array} \quad (4.4)$$

Dowód. Rozumowanie prowadzone jest oddzielnie dla każdej z relacji Greena wymienionych w (4.4).

- $a\mathcal{J}b \Leftrightarrow Gl_n(\mathbb{K})aGl_n(\mathbb{K}) = Gl_n(\mathbb{K})bGl_n(\mathbb{K}) \Leftrightarrow rz(a) = rz(b)$

Fakt ten wynika bezpośrednio z twierdzenia 4.6.

- $a\mathcal{R}b \Leftrightarrow aGl_n(\mathbb{K}) = bGl_n(\mathbb{K}) \Leftrightarrow Im(a) = Im(b)$

Rozumowanie jest analogiczne do dowodu 2. implikacji $(3) \Rightarrow (1)$ twierdzenia 4.6. Niech $Im(a) = Im(b)$. Przestrzeń liniowa nad $\mathbb{K}$ rozpięta przez kolumny tych macierzy są zatem identyczne. Przyjmując więc oznaczenia z diagramu $(***)$, $g = Id$. Stąd $ah = b$, $bh^{-1} = a$ dla pewnej $h \in Gl_n(\mathbb{K})$. Stąd $aGl_n(\mathbb{K}) = bGl_n(\mathbb{K})$. Nietrudno widzieć, że prawdziwa jest implikacja $aGl_n(\mathbb{K}) = bGl_n(\mathbb{K}) \Rightarrow aM_n(\mathbb{K}) = bM_n(\mathbb{K})$. Pozostaje uzasadnić, że $a\mathcal{R}b \Rightarrow Im(a) = Im(b)$. Istotnie: $Im(a) = (aM_n(\mathbb{K}))\mathbb{K}^n = (bM_n(\mathbb{K}))\mathbb{K}^n = Im(b)$.

- $a\mathcal{L}b \Leftrightarrow Gl_n(\mathbb{K})a = Gl_n(\mathbb{K})b \Leftrightarrow ker(a) = ker(b)$

Założmy, że $ker(a)$ ma wymiar $n-j$ i jest równa z $ker(b)$. Wybieramy bazę $u_1, u_2, \dots, u_n$ przestrzeni $\mathbb{K}^n$ tak, by ostatnie $n-j$ wektorów było bazą $ker(a)$. Skoro $ker(a) = ker(b)$,

to $b(u_i) = 0, i > j$, zaś obrazy pozostałych wektorów u_i są dla $i \leq j$ liniowo niezależne. Istnieje zatem $g \in Gl_n(\mathbb{K})$, że $g(b(u_i)) = a(u_i)$, dla $i > j$. Stąd $gb = a$. Istotnie, na wektorach bazowych $\mathbb{K}^n$ mają one izomorficzne jądra oraz obrazy. Dostajemy zatem równość $Gl_n(\mathbb{K})a = Gl_n(\mathbb{K})b$. Implikacja $Gl_n(\mathbb{K})a = Gl_n(\mathbb{K})b \Rightarrow M_n(\mathbb{K})a = M_n(\mathbb{K})b$ jest oczywista. Jeśli natomiast $M_n(\mathbb{K})a = M_n(\mathbb{K})b$, to na mocy tw. 4.6 mamy równość $\mathbf{r}z(a) = \mathbf{r}z(b)$. Łatwo widać, że $b(\ker(a)) = 0$. Stąd $\ker(a) \subseteq \ker(b)$. Równość rzędów wymusza jednak, by zawieranie powyższe musi być równością. To kończy dowód. $\square$

Nietrudno wykazać, że macierze przynależące do tej samej $\mathcal{L}$ -klasy to takie, które są równoważne z punktu widzenia elementarnych operacji na kolumnach. Podobnie przynależność dwóch macierzy do tej samej $\mathcal{R}$ -klasy oznacza, że jedną można sprowadzić do drugiej przy pomocy elementarnych operacji na wierszach. Innymi słowy, zbiór reprezentantów klas, na jakie dzieli $M_n(\mathbb{K})$ relacje $\mathcal{R}, \mathcal{L}$ to nic innego, jak zbiory macierzy w postaciach zredukowanych. Wniosujemy stąd, że w pełnym monoidzie liniowym mamy $n + 1$ $\mathcal{J}$ -klas. Zbiory reprezentantów $\mathcal{R}$ i $\mathcal{L}$ w obrębie $\mathcal{J}$ klasy macierzy rzędu j oznaczać będziemy odpowiednio przez $\mathbf{X}_j$ oraz $\mathbf{Y}_j$.¹

Dwóm relacjom Greena nie poświęciliśmy dotąd żadnej uwagi, mianowicie: $\mathcal{D}$ oraz $\mathcal{H}$. Ich opis jest jednak ściśle ze sobą związany. Kluczowe jest wykazanie, że w $M_n(\mathbb{K})$ relacje $\mathcal{D}$ i $\mathcal{J}$ pokrywają się. W paragrafie 1.1 odnotowaliśmy, że $\mathcal{D} \subseteq \mathcal{J}$. Pokazaliśmy też przykład półgrupy, opisaną w (1.4), w której zawieranie to jest właściwe. Charakteryzacja tych półgrup, w których $\mathcal{J} = \mathcal{D}$ jest delikatnym problemem i nie będziemy go dokładniej rozwijać. W przypadku $M_n(\mathbb{K})$ wykazanie inkluzji $\mathcal{J} \subseteq \mathcal{D}$ nie jest jednak trudne. Wprowadźmy następującą definicję.

Definicja 4.8. Niech S będzie półgrupą. Na zbiorze $\mathcal{L}$ -klas i $\mathcal{R}$ -klas półgrupy S wprowadzamy relację porządku postaci:

- $\mathcal{L}_a \leq \mathcal{L}_b \Leftrightarrow S^1 a \subseteq S^1 b$,
- $\mathcal{L}_a \leq \mathcal{L}_b \Leftrightarrow aS^1 \subseteq bS^1$.

Mówimy, że półgrupa S :

- **spełnia $\min_L$** $\Leftrightarrow$ w każdym niepustym zbiorze lewostronnych ideałów głównych S istnieje minimalny element niezerowy,
- **spełnia $\min_R$** $\Leftrightarrow$ w każdym niepustym zbiorze prawostronnych ideałów głównych S istnieje minimalny element niezerowy.

Lemat 4.9. Jeśli S jest monoidem spełniającym $\min_R$ oraz $\min_L$, to $\mathcal{D} = \mathcal{J}$.

Dowód. Zawieranie $\mathcal{D} \subseteq \mathcal{J}$ zachodzi zawsze, zatem pozostaje wykazać zawieranie $\mathcal{J} \subseteq \mathcal{D}$. Niech $a\mathcal{J}b$. Wówczas istnieją takie $p, q, r, s \in S$, że:

$$paq = b, \quad rbs = a. \quad (4.5)$$

Wynika stąd, że:

$$X := \{x \in S : \exists_{y \in S} (xay = b)\} \neq \emptyset.$$

¹Są to, zgodnie z przyjętymi wcześniej oznaczeniami, zbiory złożone z macierzy w formie zredukowanej: wierszowej – dla $\mathcal{R}$ -klas i kolumnowej – dla $\mathcal{L}$ -klas.

Stąd niepusty jest także podzbiór $\Lambda := \{\mathcal{L}_x \mid x \in X\}$ złożony z $\mathcal{L}$ -klas elementów należących do X . Warunek $\min_L$ pozwala nam wybrać minimalny element względem porządku określonego na $\mathcal{L}$ -klasach S , zgodnie z definicją 4.8. Niech będzie to element $\mathcal{L}_u$, dla pewnego $u \in X$. Zgodnie z definicją zbioru X możemy wybrać element $v \in S$, że $uav = b$. Zauważmy, że:

$$uruavsv = urbsv = uav = b \Rightarrow \mathcal{L}_{uru} \in \Lambda.$$

Łatwo widzieć, że $\mathcal{L}_{uru} \leq \mathcal{L}_u$, a stąd wobec minimalności $\mathcal{L}_u$ w Λ dostajemy:

$$\mathcal{L}_u = \mathcal{L}_{uru} \leq \mathcal{L}_{ru} \leq \mathcal{L}_u.$$

Stąd $ru\mathcal{L}_u$, a więc także² $ruav\mathcal{L}uav$. Wobec (4.5) dostajemy:

$$rb\mathcal{L}b.$$

Analogiczny argument, tym razem wykorzystujący $\min_R$ pokazuje, że $bs\mathcal{R}b$. Stąd $rb\mathcal{S}\mathcal{R}rb$, czyli zgodnie z (4.5) $a\mathcal{R}rb$. Ostatecznie otrzymujemy:

$$a\mathcal{R}rb \quad \wedge \quad rb\mathcal{L}b \quad \Rightarrow \quad (a, b) \in \mathcal{R} \circ \mathcal{L}.$$

Na mocy uwagi 1.7 zachodzi równość $\mathcal{R} \circ \mathcal{L} = \mathcal{D}$, co oznacza, że $a\mathcal{D}b$, a więc $\mathcal{J} \subseteq \mathcal{D}$. $\square$

Uwaga 4.10. *Pelen monoid liniowy spełnia warunki $\min_R$ oraz $\min_L$.*

Dowód. Wystarczy pokazać, że w każdym niepustym zbiorze ideałów głównych prawostronnych (odp. lewostronnych) istnieje niezerowy element minimalny. Istotnie, niech $a, b \in M_n(\mathbb{K})$. Wówczas:

$$Gl_n(\mathbb{K})a \not\subseteq Gl_n(\mathbb{K})b \Rightarrow \ker(b) \not\subseteq \ker(a) \Rightarrow \dim(\ker(b)) < \dim(\ker(a)).$$

Podobnie jeśli $c, d \in M_n(\mathbb{K})$, to:

$$cGl_n(\mathbb{K}) \subseteq dGl_n(\mathbb{K}) \Rightarrow \text{Im}(c) \not\subseteq \text{Im}(d) \Rightarrow \dim(\text{Im}(c)) < \dim(\text{Im}(d)).$$

Zarówno więc każdy łańcuch ideałów lewostronnych jak i każdy łańcuch ideałów prawostronnych mają długość równą co najwyżej $n + 1$. To kończy dowód. $\square$

Na mocy lematu 4.9 widzimy zatem, że w przypadku monoidu $M_n(\mathbb{K})$ relacje $\mathcal{J}$ i $\mathcal{D}$ są tożsame. Równość $\mathcal{J} = \mathcal{D}$ pozwala uprościć poszukiwania $\mathcal{H}$ -klas w $M_n(\mathbb{K})$. Możemy bowiem skorzystać z modelu „egg-boxu” (zgodnie z definicją 1.8). Każda $\mathcal{H}$ -klasa jest przecięciem $\mathcal{R}$ -klas i $\mathcal{L}$ -klas zawierających macierze ustalonego rzędu. Zbiory te oznaczamy przez $\mathcal{L}_j, \mathcal{R}_j$. Rozważmy następujące działania:

- lewostronne $\phi_L : Gl_n(\mathbb{K}) \times \mathcal{R}_j \rightarrow \mathcal{R}_j$,
- prawostronne $\phi_R : \mathcal{L}_j \times Gl_n(\mathbb{K}) \rightarrow \mathcal{L}_j$,

zadane wzorami:

$$\phi_L(a, \mathcal{R}_b) = \mathcal{R}_{ab}, \quad \phi_R(\mathcal{L}_c, a) = \mathcal{L}_{ca}, \quad a \in Gl_n(\mathbb{K}), b \in \mathcal{R}_j, c \in \mathcal{L}_j$$

Łatwo sprawdzić, że działania te są dobrze określone tj. nie zależą od wyboru reprezentantów $\mathcal{L}$, $\mathcal{R}$ -klas. Działania ϕ_L oraz ϕ_R są tranzytywne odpowiednio na $\mathcal{R}_j$ i na $\mathcal{L}_j$. Istotnie, każde

²Łatwo sprawdzić, że jeśli $a, b, c \in S$, to $a\mathcal{L}b \Rightarrow ac\mathcal{L}bc$ oraz $a\mathcal{R}b \Rightarrow ca\mathcal{R}cb$.

dwie macierze $x_1, x_2 \in X_j$ (odp. $y_1, y_2 \in Y_j$) będące w postaci zredukowanej kolumnowej (odp. wierszowej) można przeprowadzić na siebie przy pomocy elementarnych operacji na wierszach (odp. na kolumnach). Nietrudno pokazać, że stabilizatorem działania ϕ_L jest grupa

$$P_j := \begin{pmatrix} Gl_j(\mathbb{K}) & * \\ 0 & Gl_{n-j}(\mathbb{K}) \end{pmatrix},$$

zaś stabilizatorem ϕ_R jest grupa

$$P_j^- := \begin{pmatrix} Gl_j(\mathbb{K}) & 0 \\ * & Gl_{n-j}(\mathbb{K}) \end{pmatrix}.$$

W ten sposób zbiór $\mathcal{R}_j$ identyfikować można z warstwami lewostronnymi P_j w $Gl_n(\mathbb{K})$, zaś zbiór $\mathcal{L}_j$ z warstwami prawostronnymi P_j^- . Widać więc, że jeśli $e_j = \begin{pmatrix} id_j & 0 \\ 0 & 0 \end{pmatrix}$, gdzie $id_j \in Gl_j(\mathbb{K})$ jest macierzą identyczności, wówczas każda $\mathcal{H}$ -klasa w $M_j \setminus M_{j-1}$ jest postaci:

$$xP_j e_j P_j^- y = x \begin{pmatrix} id_j & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} Gl_j(\mathbb{K}) & 0 \\ 0 & id_{n-j}(\mathbb{K}) \end{pmatrix} \begin{pmatrix} id_j & 0 \\ 0 & 0 \end{pmatrix} y, \quad x \in X_j, y \in Y_j.$$

Opis klas Greena monoidu $M_n(\mathbb{K})$ jest zatem zakończony.

* * *

Przejdziemy teraz do opisu czynników głównych monoidu $M_n(\mathbb{K})$. W paragrafie 1.1 pojęcie to określone zostało jedynie w klasie półgrup skończonych. Był to iloraz Reesa kolejnych (w sensie porządku częściowego) ideałów półgrupy S . Zasadniczą motywacją dla takiej definicji była uwaga 1.12. Jest ona prawdziwa dla dowolnej półgrupy. W szczególności, jeśli półgrupa jest nieskończona, ale posiada skończenie wiele ideałów, wówczas określenie czynników głównych nie przedstawia żadnej trudności. Tak będzie w przypadku monoidu $M_n(\mathbb{K})$. Nasze rozważania zaczniemy od dowodu następującej uwagi.

Uwaga 4.11. Niech $M_j = \{a \in M_n(\mathbb{K}) \mid rz(a) \leq j\}$, $j = 0, 1, 2, \dots, n$. Wówczas

$$0 = M_0 \subset M_1 \subset M_2 \subset \dots \subset M_n = M_n(\mathbb{K}) \quad (4.6)$$

jest kratą ideałów monoidu $M_n(\mathbb{K})$.

Dowód. Jeśli macierz a należy do ideału $I \triangleleft M_n(\mathbb{K})$, to $J_a \subset I$ (patrz (1.5)). Istotnie, jeśli $b \in J_a$, to $b \in M_n(\mathbb{K})aM_n(\mathbb{K}) \subset M_n(\mathbb{K})IM_n(\mathbb{K}) \subseteq I$. Oczywiście mnożąc a obustronnie przez odpowiednio elementy $M_n(\mathbb{K})$ możemy dowolnie obniżyć rząd tej macierzy. Zatem I zawiera wszystkie macierze o rzędzie nie większym od rzędu a . Domnażaniem macierzy nie można powiększyć rzędu, co dowodzi, że M_i są, dla $1 \leq i \leq n$, jedynymi ideałami w $M_n(\mathbb{K})$. Struktura kratowa zbioru ideałów jest oczywista. $\square$

Faktorami głównymi monoidu $M_n(\mathbb{K})$ będą zatem ilorazy Reesa postaci M_j/M_{j-1} , gdzie $j = 1, 2, \dots, n$, a więc zbiory wszystkich macierzy rzędu j z elementem zerowym³. Łatwo widzieć, że faktory główne $M_n(\mathbb{K})$ nie są półgrupami z zerowym mnożeniem, zatem na mocy uwagi 1.12 są to półgrupy 0-proste. W paragrafie 1.1 sformułowaliśmy twierdzenie Reesa-Suschkewitscha (tw. 1.15) klasyfikujące wszystkie skończone półgrupy 0-proste. Pozwalało ono opisać półgrupy 0-proste przy pomocy półgrup typu macierzowego $\mathcal{M}[G^0; X, Y; P]$ (def.

³Element zerowy faktora nie jest macierzą $0 \in M_n(\mathbb{K})$. Jest to zero w sensie definicji 1.5.

1.14). Definiując $\mathcal{M}[G^0; X, Y; P]$ zakładaliśmy, że skończone są zarówno grupa G , jak i zbiory X, Y . Jeśli opuścimy to założenie, otrzymamy wówczas klasę półgrup⁴ zawierającą nie tylko skończone półgrupy 0-proste, ale także z pewne półgrupy nieskończone. Należą do nich, jak się okazuje, także faktory główne $M_n(\mathbb{K})$.

Do zdefiniowania nowej klasy półgrup potrzebne jest wyróżnienie szczególnego podzbioru w zbiorze idempotentów dowolnej półgrupy. Jak wiadomo, idempotent jest to taki element e półgrupy S , że $e = e^2$. W zbiorze idempotentów danej półgrupy S rozważać możemy częściowy porządek postaci:

$$e \leq f \Leftrightarrow ef = e \wedge fe = e, \quad \text{gdzie } e = e^2, f = f^2. \quad (4.7)$$

Niezerowe elementy minimalne tego porządku, o ile istnieją, nazywamy **idempotentami prymitywnymi**.

Definicja 4.12. *Półgrupę 0-prostą nazwiemy **całkowicie 0-prostą** jeśli zawiera ona idempotent prymitywny.*

Twierdzenie 4.13 (Rees (1940)). *Niech S będzie półgrupą. Następujące warunki są równoważne:*

- S jest całkowicie 0-prostą,
- istnieją: grupa G , zbiory X, Y , oraz macierz $P \in M_{|Y| \times |X|}(G^0)$, że $S \simeq \mathcal{M}[G^0; X, Y; P]$.

Dowód twierdzenia Reesa można znaleźć w [How76], 2.5. Przejdziemy teraz do opisu faktorów głównych monoidu $M_n(\mathbb{K})$.

Twierdzenie 4.14. *Niech M_j/M_{j-1} będzie faktorem głównym w półgrupie $M_n(\mathbb{K})$. Wówczas M_j/M_{j-1} jest izomorficzny z całkowicie 0-prostą półgrupą $\mathcal{M}(Gl_j^0(\mathbb{K}), X_j, Y_j, Q_j)$, gdzie $Q_j = (q_{yx})$ jest zdefiniowana w następujący sposób dla $x \in X_j, y \in Y_j$:*

$$q_{yx} = \begin{cases} yx, & \text{jeśli } \mathbf{r}z(yx) = j \\ 0, & \text{jeśli } \mathbf{r}z(yx) \neq j \end{cases}$$

Dowód. W pierwszej części dowodu wskażemy półgrupy izomorficzne z faktorami głównymi $M_n(\mathbb{K})$. Będą one wykorzystane w dowodzie całego twierdzenia.

Lemat 4.15. *Niech $0 < j < n$. Jeśli $e \in Y_j$ jest idempotentną macierzą diagonalną rzędu j postaci $\begin{pmatrix} I_j & 0 \\ 0 & 0 \end{pmatrix}$, to przez G_j oznaczając będziemy podgrupę elementów odwracalnych monoidu $eM_n(\mathbb{K})e$. Grupa ta jest izomorficzna z $Gl_j(\mathbb{K})$. Każda macierz xgy , gdzie $x \in X_j, y \in Y_j, g \in G_j$, ma rząd j i każdą macierz $M \in M_n(\mathbb{K})$ rzędu j można jednoznacznie przedstawić w tej postaci.*

Dowód. Wykażemy najpierw, że:

$$U(eM_n(\mathbb{K})e) \simeq Gl_j(\mathbb{K}). \quad (4.8)$$

⁴Poprawność definicji mnożenia półgrupowego podana w 1.14 nie zależy od skończoności G, X, Y . Interpretacja elementów półgrupy typu macierzowego jako macierzy nieskończonych o wymiarach $|X| \times |Y|$ jest także możliwa, ponieważ każda taka macierz ma tylko jeden niezerowy element, a więc iloczyn takiej macierzy z P jest dobrze określony.

Istotnie, obustronne przemnożenie $M \in M_n(\mathbb{K})$ przez e zeruje pierwszej j wierszy i kolumn M . Innymi słowy $eM_n(\mathbb{K})e \simeq M_j(\mathbb{K})$. Stąd $U(eM_n(\mathbb{K})e) \simeq Gl_j(\mathbb{K})$.

Pokażemy teraz, że każdą macierz a rzędu j można przedstawić w postaci:

$$a = xgy \quad , \text{ gdzie } x \in X_j, y \in Y_j, g \in G_j. \quad (4.9)$$

Zauważmy, że istnieje $b \in M_n(\mathbb{K})$, że $\ker(a) = \ker(b)$ oraz $\text{Im}(b) = e\mathbb{K}^n$. Istotnie, zgodnie z twierdzeniem 4.7, b jest taką macierzą, która leży w $\mathcal{H}$ -klasie równej przecięciu $\mathcal{L}_a$ oraz $\mathcal{R}_e$. Skoro $\text{Im}(b) = e\mathbb{K}^n$, to $b = eb$. Innymi słowy, jedynie pierwsze j wierszy macierzy b to wiersze niezerowe. Natomiast skoro $\ker(a) = \ker(b)$, zatem zgodnie z twierdzeniem 4.7 istnieje macierz $y \in Y_j$ w postaci zredukowanej wierszowej taka, że

$$\ker(y) = \ker(a) = \ker(b). \quad (4.10)$$

Widzimy, że $y\mathcal{L}b$, a stąd istnieje macierz $t \in M_n(\mathbb{K})$, że $y = tb$. Zauważmy, że skoro jedynie pierwsze j wierszy macierzy b to wiersze niezerowe, podobnie jak jedynie pierwsze j wierszy macierzy y to wiersze niezerowe, to macierz t jest elementem G_j . Zgodnie z (4.10) widzimy także, że $y\mathcal{L}a$, a więc istnieje macierz $c \in M_n(\mathbb{K})$, że $cy = a$. Łatwo widzieć, że można dobrać taką macierz c , która ma jedynie pierwsze j kolumn niezerowych. Istotnie, skoro y ma jedynie pierwsze j wierszy niezerowych, to kolumny od $j+1$ -wszej do n -tej nie mają wpływu na postać iloczynu cy . Można więc założyć, że są one zerowe, a więc $c = ce$. Widzimy zatem, że:

$$a = cy = (ce)tb. \quad (4.11)$$

Chcemy tak zmodyfikować rozkład (4.11), aby przedstawić a w postaci (4.9). Wystarczy więc przedstawić ce jako element X_jG_j . Doprowadźmy macierz ce do postaci kolumnowej zredukowanej. Zgodnie z (4.4) istnieje macierz $h \in M_n(\mathbb{K})$, że $ceh \in X_j$. Skoro jednak jedynie pierwsze j kolumn macierzy ce to kolumny niezerowe, podobnie jak jedynie pierwsze j kolumn macierzy ceh to kolumny niezerowe ($ceh \in X_j$), można zatem zakładać, że $h \in G_j$. Macierz h ma swoją odwrotność w G_j , a więc taką macierz h' , że $hh' = e$. Zatem $ce = ce e = ce hh' \in X_jG_j$. Przyjmując zatem $x = ceh, g = h', y = tb$, uzyskujemy rozkład (4.9) macierzy a .

Pokażemy teraz jednoznaczność przedstawienia (4.9). Jeśli $x \in X_j, y \in Y_j, g \in G_j$, to $x\mathcal{L}e$ oraz $y\mathcal{R}e$. Istnieją zatem macierze $u, v \in Gl_n(\mathbb{K})$, że $uv = e = yv$. Zachodzi następująca nierówność $\mathbf{r}z(xgy) \geq \mathbf{r}z(uxgyv) = \mathbf{r}z(g) = j$. Zatem $\mathbf{r}z(xgy) = j$. Załóżmy teraz, że dla pewnych $x' \in X_j, y' \in Y_j, g' \in G_j$ zachodzi równość $xgy = x'g'y'$. Skoro $\mathbf{r}z(xgy) = \mathbf{r}z(x) = j$, to $\text{Im}(xgy) = \text{Im}(x)$. Analogicznie dla x' , zatem $\text{Im}(x) = \text{Im}(x')$. Stąd $x\mathcal{R}x'$, a więc $x = x'$. Analogicznie $y = y'$. Jeśli mimo to $y(g - g')y = 0$, wówczas:

$$g - g' = e(g - g')e = u(x(g - g')y)v = u0v = 0.$$

To kończy dowód lematu. □

Przechodzimy do dowodu twierdzenia 4.14. Określamy następujące przekształcenie:

$$\mathcal{M}(Gl_j(\mathbb{K})^0, X_j, Y_j, Q_j) \ni (g, x, y) \xrightarrow{\phi_j} xgy \in M_j/M_{j-1}. \quad (4.12)$$

Wykażemy, że ϕ_j opisuje izomorfizm pólgrup. Istotnie,

$$\begin{aligned}
\phi_j(g, x, y)\phi_j(g', x', y') &= (xgy)(x'g'y') = \\
&= \begin{cases} xgyx'g'y' & \in M_j/M_{j-1} \quad , \text{ jeśli } \mathbf{rz}(yx') = j, \\ \theta & \in M_j/M_{j-1} \quad , \text{ jeśli } \mathbf{rz}(yx') \neq j \end{cases} \\
\phi_j((g, x, y)(g', x', y')) &= \phi_j(gq_{yx'}g', x, y') = \\
&= \begin{cases} xg(yx')g'y' & \in M_j/M_{j-1} \quad , \text{ jeśli } \mathbf{rz}(yx') = j, \\ xg(0)g'y' = \theta & \in M_j/M_{j-1} \quad , \text{ jeśli } \mathbf{rz}(yx') \neq j \end{cases}
\end{aligned}$$

Przekształcenie ϕ_j jest zatem homomorfizmem. Na mocy lematu 4.15 wiemy jednak, że zbiory $\{xgy \mid x \in X_j, y \in Y_j, g \in G_j\}$, $M_j \setminus M_{j-1}$ są ze sobą w bijekcji. W ten sposób ϕ_j jest, dla każdego $1 \leq j \leq n$, izomorfizmem pomiędzy $\mathcal{M}(Gl_j(\mathbb{K}), X_j, Y_j, Q_j)$, a faktorem głównym M_j/M_{j-1} monoidu $M_n(\mathbb{K})$. Dowód twierdzenia jest zatem zakończony. $\square$

Pełen opis klas Greena monoidu $M_n(\mathbb{K})$ zbliża nas do dowodu twierdzenia 4.2. Aby móc go rozpocząć, potrzebujemy jeszcze opisu klas Greena w monoidzie Rennera R_n . Temu zagadnieniu poświęcony jest następny paragraf.

4.3. Struktura półgrupowa monoidu Rennera

Celem tego paragrafu jest opis klas Greena monoidu R_n oraz dowód twierdzenia 4.2. Przypomnijmy, że monoid Rennera R_n jest podmonoidem $M_n(\mathbb{K})$ złożonym ze wszystkich macierzy, które w każdym wierszu i w każdej kolumnie mają co najwyżej jeden niezerowy element równy 1. Naszym pierwszym celem będzie dowód następującego twierdzenia.

Twierdzenie 4.16. *Niech dla $0 \leq i \leq n$ zbiory T_i będą określone jako przecięcia R_n z kolejnymi elementami łańcucha M_i ideałów monoidu $M_n(\mathbb{K})$. Wówczas T_i są jedynymi ideałami w R_n . Tworzą one łańcuch postaci:*

$$0 = T_0 \subset T_1 \subset T_2 \subset \dots \subset T_n = R_n. \quad (4.13)$$

Faktory T_j/T_{j-1} są całkowicie 0-prostymi półgrupami z prezentacją

$$\mathcal{M}(S_j, \binom{n}{j}, \binom{n}{j}, id_{\binom{n}{j}}), \quad (4.14)$$

gdzie S_j jest grupą permutacji zbioru j -elementowego, zaś $id_{\binom{n}{j}} \in M_{\binom{n}{j}}(\mathbb{K})$ – macierzą identyczności.

Dowód. Rozpoczniemy od opisu ideałów monoidu R_n . Nietrudno zauważyć, że $T_j \subset R_n$ są, dla każdego $1 \leq j \leq n$ ideałami w R_n . Argument jest identyczny jak w dowodzie uwagi 4.8. Wykażemy teraz, że T_j są jedynymi ideałami w R_n . Weźmy element $a \in T_j \setminus T_{j-1}$. Wtedy, podobnie jak w lemacie 4.15,

$$e_a = w_a \cdot a \cdot k_a, \text{ gdzie } w_a \in X_j, k_a \in Y_j,$$

zaś $e_a = e_j$ jest macierzą postaci $\begin{pmatrix} id_j & 0 \\ 0 & 0 \end{pmatrix}$. Zatem każdy element T_j należy do $\mathcal{J}_{e_j}$. Półgrupa T_j/T_{j-1} jest więc 0-prosta, a to oznacza, że T_j są jedynymi ideałami w R_n . Co więcej, po utożsamieniu e_a z elementem $id_j \in G_j$, dostajemy:

$$T_j \setminus T_{j-1} = (X_j \cap R_n)(G_j \cap R_n)(Y_j \cap R_n). \quad (4.15)$$

Łatwo widzieć, że $G_j \cap R_n \simeq S_j$, oraz $|X_j \cap R_n| = |Y_j \cap R_n| = \binom{n}{j}$. Co więcej, jeśli $x \in X_j \cap R_n$, oraz $y \in Y_j \cap R_n$, wówczas $yx = e_j$ lub $\mathbf{r}z(yx) < j$ zatem analogiczne, jak w (4.12) możemy określić przekształcenie:

$$\psi_j : \mathcal{M}(S_j(\mathbb{K}), \binom{n}{j}, \binom{n}{j}, id_{\binom{n}{j}}) \ni (g, x, y) \xrightarrow{\psi_j} xgy \in T_j/T_{j-1}. \quad (4.16)$$

Naśladując rozumowanie z dowodu tw. 4.14 wykazujemy, że ψ_j jest homomorfizmem półgrup. Na mocy (4.15) jest to izomorfizm. Faktory główne monoidu R są zatem izomorficzne z półgrupą typu macierzowego opisaną w (4.14). $\square$

Przejdziemy teraz do opisu relacji Greena na R_n . Są one, jak się okazuje, wiernym odbiciem relacji Greena na $M_n(\mathbb{K})$. Udowodnimy następujące twierdzenie pomocnicze.

Twierdzenie 4.17. *Niech S będzie całkowicie 0-prostą podpółgrupą całkowicie 0-prostej półgrupy M . Jeśli $\mathcal{S}, \mathcal{S}_S$ oznaczają jedną z relacji Greena $\mathcal{R}, \mathcal{L}, \mathcal{H}$, odpowiednio na M oraz na S , wówczas $\mathcal{S}|_S = \mathcal{S}_S$.*

Dowód. Wykażemy najpierw następujący lemat.

Lemat 4.18. *Niech S będzie półgrupą całkowicie 0-prostą. Wówczas każda niezerowa $\mathcal{R}$ -klasa i każda niezerowa $\mathcal{L}$ -klasa półgrupy S zawiera idempotent prymitywny.*

Dowód. Zgodnie z twierdzeniem Reesa wystarczy pokazać tezę dla każdej półgrupy typu macierzowego $M = \mathcal{M}[G^0; X, Y; P]$ (takiej, jaka występuje w treści twierdzenia 4.14⁵). Przypomnijmy, że mnożenie w M opisane jest następującym wzorem:

$$(g_1, x_1, y_1)(g_2, x_2, y_2) = \begin{cases} (g_1 p_{y_1 x_2} g_2, x_1, y_2), & p_{y_1 x_2} \neq 0, \\ 0 & , \quad p_{y_1 x_2} = 0 \end{cases}$$

$$(g_1, x_1, y_1)\theta = \theta(g_1, x_1, x_2) = \theta\theta = \theta,$$

przy czym $g_1, g_2 \in G^0$, $x_1, x_2 \in X$, $y_1, y_2 \in Y$ oraz $P = (p_{yx})$ dla $y \in Y, x \in X, p_{yx} \in G^0$.

Zauważmy, że jeśli $p_{yx} \neq 0$, to:

$$(p_{yx}^{-1}, x, y)(p_{yx}^{-1}, x, y) = (p_{yx}^{-1} p_{yx} p_{yx}^{-1}, x, y) = (p_{yx}^{-1}, x, y).$$

Element (p_{yx}^{-1}, x, y) jest zatem idempotentem w M . Jest to, jak się okazuje, idempotent prymitywny w M . Istotnie, jeśli $(a, x', y') \leq (p_{yx}^{-1}, x, y)$ jest idempotentem w M , wówczas zgodnie z (4.7):

$$(p_{yx}^{-1}, x, y)(a, x', y') = (a, x', y'), \quad (a, x', y')(p_{yx}^{-1}, x, y) = (a, x', y'),$$

wówczas mamy równości:

$$(p_{yx}^{-1} p_{yx'} a, x, y') = (a, x', y'), \quad (a p_{y'x} p_{yx}^{-1}, x', y) = (a, x', y').$$

Stąd: $x = x', y = y'$. Skoro jednak (a, x, y) jest idempotentem, to:

$$(a, x, y)(a, x, y) = (a p_{yx} a, x, y) = (a, x, y),$$

⁵Zgodnej z definicją 1.14 przy opuszczeniu założenia o skończoności zbiorów X, Y, G

zatem o ile $a \neq 0$, wówczas $ap_{yx}a = 1 \Rightarrow a = p_{yx}^{-1}$. Istotnie więc element (p_{yx}^{-1}, x, y) jest idempotentem prymitywnym w $M = \mathcal{M}[G^0; X, Y; P]$.

Każda $\mathcal{R}$ -klasa w $M = \mathcal{M}[G^0; X, Y; P]$ równa jest $\{(g, x, y) \mid y \in Y, g \in G\}$. Podobnie każda $\mathcal{L}$ -klasa równa jest $\{(g, x, y) \mid x \in X, g \in G\}$.⁶ Wobec założenia o niezerowości każdego wiersza i każdej kolumny macierzy P , występującego w definicji 1.14 widzimy, że każda $\mathcal{R}$ -klasa i każda $\mathcal{L}$ -klasa monoidu M zawiera idempotent prymitywny. Z twierdzenia Reesa wynika zatem, że w każdej półgrupie całkowicie 0-prostej S każda niezerowa $\mathcal{R}$ -klasa i każda niezerowa $\mathcal{L}$ -klasa S zawiera idempotent prymitywny. $\square$

Przechodzimy do dowodu twierdzenia 4.17. Jest jasne, że jeśli dla $a, b \in S$ mamy $a\mathcal{R}_S b$, to $a\mathcal{R}b$. Z drugiej strony, jeśli $a\mathcal{R}b$, wówczas będąc całkowicie 0-prostą półgrupa S zawiera idempotent prymitywny e . Zgodnie z lematem 4.18 możemy tak wybrać e , aby $eS = aS$. Wtedy $a\mathcal{R}e$, a więc także $b\mathcal{R}e$. Stąd $b = eb \in eS$, skąd $b \in aS$. Podobnie dowodzimy, że $a \in bS$, a zatem $a\mathcal{R}_S b$. Analogiczne rozumowanie przeprowadzamy dla przypadku $\mathcal{L}$ oraz $\mathcal{H}$ -klas. $\square$

Twierdzenie 4.19. *Relacje Greena $\mathcal{J}, \mathcal{R}, \mathcal{L}, \mathcal{H}$ na R są obcięciem odpowiadających im relacji Greena na $M_n(\mathbb{K})$.*

Dowód. Istotnie, elementy danej klasy Greena na R mają ten sam rząd, np. równy j . Na mocy twierdzenia 4.16 są one zatem elementami tego samego faktora głównego $W_j = T_j/T_{j-1}$ monoidu R . Ten zaś jest półgrupą całkowicie 0-prostą i stanowi podpółgrupę faktora głównego $F_j = M_j/M_{j-1}$ monoidu $M_n(\mathbb{K})$. F_j jest także całkowicie 0-prosty. Teza wynika zatem z twierdzenia 4.17. Warto zauważyć także, że:

$$\mathcal{J}_a = S_n a S_n, \quad \mathcal{R}_a = a S_n, \quad \mathcal{L}_a = S_n a. \quad (4.17)$$

$\square$

Opisaliśmy strukturę półgrupową monoidu Rennera R_n . Jesteśmy przygotowani do przeprowadzenia dowodu twierdzenia 4.2. Jest ono teraz prostym wnioskiem z twierdzenia 4.19. Zgodnie z oznaczeniami przyjętymi w tezie twierdzenia 4.2 widzimy, że rodzina $\mathcal{M}$ wszystkich $\mathcal{J}$ -klas na $M_n(\mathbb{K})$ równa jest rodzinie $\{F_0, F_1, \dots, F_n\}$, gdzie $F_i \subset M_n(\mathbb{K})$ jest zbiorem macierzy rzędu i (tw. 4.7). Podobnie rodzina $\mathcal{R}$ wszystkich $\mathcal{J}$ -klas Greena na R równa jest $\{W_0, W_1, \dots, W_n\}$ gdzie $T_i = R_n \cap W_i$ (tw. 4.19). Wiadomo zatem, że:

$$M_n(\mathbb{K}) = \bigcup_{i=0}^n F_i.$$

Należy udowodnić, że jeśli $\{W_i \mid 0 \leq i \leq n\}$ stanowi zbiór $\mathcal{J}$ -klas w R , wówczas:

$$F_i = \bigcup_{\sigma \in W_i} B_n(\mathbb{K}) \sigma B_n(\mathbb{K}).$$

Wobec (4.15) wiemy, że $W_i = S_n e_i S_n$. Zgodnie z twierdzeniem 4.1 zbiór $F_i = M_i \setminus M_{i-1}$ macierzy rzędu i jest sumą warstw rozkładu Bruhat. Istotnie, jeśli dana jest warstwa $B_n(\mathbb{K}) \sigma B_n(\mathbb{K})$, $\sigma \in R_n$, wówczas wszystkie elementy tej warstwy mają ten sam rząd. Z drugiej strony F_i jest $\mathcal{J}$ -klasą elementu e_i w $M_n(\mathbb{K})$, zatem mogą się w niej znajdować tylko te elementy R_n , które

⁶Ogólniej, jeśli półgrupa S jest całkowicie 0-prosta, wówczas jeśli $a \neq 0$, to $\mathcal{R}_a = aS \setminus \{0\}$, $\mathcal{L}_a = Sa \setminus \{0\}$. Fakt ten jest istotnym krokiem w dowodzie twierdzenia Reesa. Dowód jest czysto rachunkowy ([How76], 3.2.5 i 3.2.6).

pochodzą z obcięcia F_i do R_n . Zgodnie z twierdzeniem 4.18, są to dokładnie elementy z W_i . To kończy dowód twierdzenia 4.2.

* * *

Analiza porównawcza budowy monoidu $M_n(\mathbb{K})$ i odpowiadającego mu monoidu Rennera R pokazała, że struktura tego ostatniego jest, nadużywając nieco terminologii, obcięciem struktury $M_n(\mathbb{K})$. Fakt ten jest przykładem znacznie szerszego zjawiska związanego z półgrupami liniowymi. Oczywiście, jeśli weźmiemy dowolną podpółgrupę $S \subseteq M_n(\mathbb{K})$ nie powinniśmy spodziewać się, że wszystkie ideały S będą równe $M_i \cap S$. Takie przeniesienie struktury półgrupy z $M_n(\mathbb{K})$ nie jest własnością każdej podpółgrupy. W przypadku ogólnym zagadnienie to jest znacznie bardziej skomplikowane. Mimo to idea badania tego jak półgrupa S wypełnia kolejne egg-boxy⁷ $M_n(\mathbb{K})$ prowadzi do głębokich uogólnień uzyskanych tu wyników. Po szczegóły odsyłamy do rozdziału 3. w [Okn98].

⁷W przypadku monoidu Rennera idea ta realizowana jest właśnie przez twierdzenie 4.2.

Bibliografia

- [Abr89] ABRAMIENKO P., BROWN K.: *Buildings. Theory and Applications*, Graduate Texts in Mathematics (248), Springer (1989).
- [And52] ANDERSEN O.: *Ein Bericht über die Struktur abstrakter Halbgruppen*, Praca doktorska, Hamburg (1952).
- [Ati69] ATIYAH M.F., MACDONALD I.G.: *Introduction to commutative algebra*, Addison-Wesley, Reading (1969).
- [BiB87] BIAŁYNICKI-BIRULA A.: *Zarys algebry*, PWN, Warszawa (1987).
- [Bor91] BOREL A.: *Linear algebraic groups*, Graduate Texts in Mathematics (126), Springer (1991).
- [Bou64] BOURBAKI N.: *Éléments de mathématique. Algèbre commutative V*, Hermann, Paryż (1964).
- [Bre03] BRENTI F.: *Kazhdan-Lusztig polynomials: History. Problems, and Combinatorial Invariance*, Seminaire Lotharingien de Combinatoire 49 (2003), Article B49b.
- [Bru54] BRUHAT F.: *Représentations induites des groupes de Lie semi-simples connexes*, C.R. Acad. Sci. Paris 238 (1954), 437-439.
- [Che58] CHEVALLEY C.: *Séminaire Chevalley*, Tomy I and II, École Normale Supérieure, Paryż (1958).
- [Che55] CHEVALLEY C.: *Sur certains groupes simples*, Tohoku Math. J. 7 (1955), 14-66.
- [Cli61] CLIFFORD A. H., PRESTON G. B.: *The algebraic theory of semigroups*, American Mathematical Society (1961).
- [Lan76] LANG S.: *Introduction to modular forms*, A Series of Comprehensive Studies in Mathematics, No. 222, Springer-Verlag, Berlin and New York (1976).
- [Lom04] COQUAND T., LOMBARDI H.: *A short proof for the Krull dimension of a polynomial ring*, American Math. Monthly 112 (2005), no. 9, 826-829.
- [Cur67] CURTIS C.W.: *The Classical Groups as a Source of Algebraic Problems*, The American Mathematical Monthly, 74 (1967), 80-91.
- [Cur81] CURTIS C.W., REINER I.: *Methods of Representation Theory, with applications to finite groups and orders*, tom 1., Wiley, Nowy Jork (1981).
- [Cur87] CURTIS C.W., REINER I.: *Methods of Representation Theory, with applications to finite groups and orders*, tom 2., Wiley, Nowy Jork (1987).

- [Dia00] DIACONIS P., RAM A.: *Analysis of systematic scan Metropolis algorithms using Iwahori-Hecke algebra techniques*, Michigan Math. J. 48 (2000), 157-190.
- [Dro94] DROZD Y.A., KIRICHENKO V.V.: *Finite dimensional algebras*, Springer, Berlin (1994).
- [Ful08] FULTON W., HARRIS J.: *Representation Theory: A First Course.*, Graduate texts in mathematics (129), Springer (2008).
- [Gec03] GECK M.: *An Introduction to Algebraic Geometry and Algebraic Groups*, Oxford Graduate Texts in Mathematics 10, Nowy Jork (2003).
- [Hec37] HECKE E.: *Über modulfunktionen und Dirichletscher Reihen mit Eulerscher Produktentwicklung*, Math. Ann. 114 (1937), 1-28, 316-351.
- [How76] HOWIE J.M.: *An introduction to semigroup theory*, Londyn (1976).
- [Hum75] HUMPHREYS J.E.: *Linear algebraic groups*, Graduate Texts in Mathematics (21), Springer (1975).
- [Iwa64] IWAHORI N.: *On the structure of a Hecke ring of a Chevalley group over a finite field*, J. Fac. Sci. Univ. Tokyo, Sec 1, 10 (1964), 215-236.
- [Jim86] JIMBO M.: *A q -analogue of $U(\mathfrak{gl}(N+1))$, Hecke algebra, and the Yang-Baxter equation*, Lett. Math. Phys. 11 (1986), 247-252.
- [Jon87] JONES V.F.R.: *Hecke Algebra Representations of Braid Groups and Link Polynomials*, Ann. Math. 126 (1987), 335-388.
- [Lus81] LUSZTIG G.: *On a theorem of Benson and Curtis*, J. Algebra 71 (1979), 490-498.
- [Mat64] MATSUMOTO H.: *Générateurs et relations des groupes de Weyl généralisés*, C.R. Acad. Sci. Paris 258 (1964), 3419-3422.
- [Okn98] OKNIŃSKI J.: *Semigroups of matrices*, Series in algebra (6), World Scientific (1998).
- [Pie82] PIERCE R.S.: *Associative algebras*, Graduate Texts in Mathematics (88), Springer (1982).
- [Put93] PUTCHA M.S.: *Sandwich Matrices, Solomon algebras, and Kazhdan-Lusztig polynomials*, Trans. Amer. Math. Soc. 340 (1993), 415-428.
- [Ren86] RENNER L.: *Analogue of the Bruhat decomposition for algebraic monoids*, J. Algebra 101 (1986), 303-338.
- [Ren95] RENNER L.: *Analogue of the Bruhat decomposition for algebraic monoids II. The length function and the trichotomy*, J. Algebra 175(1995), 697-714.
- [Shi59] SHIMURA G.: *Sur les intégrales attachées aux formes automorphes*, J. Math. Soc. Japan 11 (1959), 291-311.
- [Shi71] SHIMURA G.: *Introduction to the arithmetic theory of automorphic functions*, Princeton Univ. Press, Princeton (1971).
- [Sol90] SOLOMON L.: *The Bruhat decomposition, Tits system and Iwahori ring for the monoid of matrices over a finite field*, Geometriae Dedicata 36 (1990), 15-49.

- [Sol95] SOLOMON L.: *An introduction to reductive monoids*, Semigroups, Formal Languages and Groups, 295-352.
- [Tam63] TAMAGAWA T.: *On the ζ -functions of a division algebra*, Ann. of Math., 77 (1963), 387-405.
- [Tit64] TITS J.: *Algebraic and abstract simple groups*, Ann. of Math. 80 (1964), 313-329.
- [Tit62] TITS J.: *Théorème de Bruhat et sous-groupes paraboliques*, C.R. Acad. Sci. Paris 254 (1962), 2910-2912.
- [Wey56] WEYL H.: *Theorie der Darstellung kontinuierlicher half-einfacher Gruppen durch lineare Transformationen*, Selecta Hermann Weyl, Birkhäuser, Basel (1956).