Uniwersytet Warszawski
Wydział Matematyki, Informatyki i Mechaniki

Arkadiusz Męcel
Nr albumu: 234204

Kontrprzykład do problemu izomorfizmu algebr grupowych nad dowolnym ciałem.

Praca licencjacka
na kierunku MATEMATYKA

Praca wykonana pod kierunkiem
dr Agnieszki Bojanowskiej - Jackowskiej
Instytut Matematyki

Maj 2008

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

W pracy tej dowodzimy, że istnieją grupy skończone G, H, które nie są izomorficzne, choć dla każdego ciała $\mathbb{K}$ ma miejsce izomorfizm algebr grupowych $\mathbb{K}[G] \simeq \mathbb{K}[H]$. Rezultat ten, uzyskany w 1970r. przez E. Dade, był częściową odpowiedzią na nierozwiązany aż do 2001r. tzw. problem izomorfizmu. W oryginalnym brzmieniu z początku lat 40. pytał on o prawdziwość implikacji: $\mathbb{Z}[G] \simeq \mathbb{Z}[H] \Rightarrow G \simeq H$. Opublikowany w [Dad70] dowód, przedstawiony także w monografii Passmana [Pas77], wzbogacony jest w tej pracy o szczegóły techniczne oraz stosowne wprowadzenie teoretyczne. W pracy dyskutujemy także minimalność tego kontrprzykładu.

Słowa kluczowe

problem izomorfizmu, kontrprzykład Dade, produkt półprosty grup, algebra grupowa

Dziedzina pracy (kody wg programu Socrates-Erasmus)

11.1 Matematyka

Klasyfikacja tematyczna

Według AMS:

20	Group theory and generalizations
20C	Representation theory of groups
20C05	Group rings of finite groups and their modules

Tytuł pracy w języku angielskim

A counterexample to the isomorphism problem for group rings over all fields.

Spis treści

Wprowadzenie 5

1. Niektóre pojęcia i fakty przygotowawcze 7
1.1. Produkt półprosty grup 7
1.2. Algebry grupowe 9

2. Pary nieizomorficznych grup 13
2.1. Konstrukcja grup 13
2.2. $G(p,q) \not\simeq H(p,q)$ 15

3. $\mathbb{K}[G] \simeq \mathbb{K}[H]$ 17
3.1. Ciała charakterystyki q 18
3.2. Ciała charakterystyki $\neq$ q 20
3.2.1. Układy idempotentów 20
3.2.2. $M_{q\times q}(S_j)$ 22
3.2.3. $S_1 \simeq S_2$ 23

4. Czy nie ma prostszych kontrprzykładów? 25

Bibliografia 27

Wprowadzenie

W 1940 roku G. Higman pozostawił w swojej dysertacji [Hig40] pytanie otwarte nazwane później „problemem izomorfizmu". Dane są w nim dwie grupy skończone G, H. Pytanie brzmi: czy izomorfizm pierścieni grupowych: $\mathbb{Z}[G] \simeq \mathbb{Z}[H]$ implikuje izomorfizm grup $G \simeq H$? Daremne próby udzielenia ogólnej odpowiedzi[1] skłoniły część matematyków do analizy przypadków, w których pierścień $\mathbb{Z}$ zastępujemy przez dowolne ciało $\mathbb{K}$. Pomimo pojawienia się wielu rezultatów pozytywnych, uzyskanych dla konkretnych klas grup, ogólna hipoteza okazała się być nieprawdziwa. Celem tej pracy jest przedstawienie dowodu poprawności kontrprzykładu uzyskanego w 1970 roku przez E. Dade, przedstawionego w pracy [Dad70].

W rozdziale wprowadzającym zbieramy potrzebne definicje (produktu półprostego grup, algebry grupowej) oraz podajemy dowody kilku przydatnych dalej prostych obserwacji. Rozdział drugi poświęcony jest konstrukcji zbioru par nieizomorficznych grup, mających stanowić kontrprzykład. Część trzecia zawiera dowód izomorficzności ich algebr grupowych nad dowolnym ciałem. W ostatniej części dyskutujemy problem minimalności opisanego kontrprzykładu.

Podziękowania

Praca ta nie powstałaby bez pomocy kilku pracowników Wydziału MIM, którym chciałbym w tym miejscu podziękować. Dziękuję w pierwszej kolejności mgr Katarzynie Jachim za zwrócenie mojej uwagi na zagadnienie „problemu izomorfizmu", dalej prof. Janowi Oknińskiemu za pomoc merytoryczną i udostępnienie potrzebnych materiałów. Słowa podziękowania za zainteresowanie mnie tematyką teorii reprezentacji grup skończonych kieruję także w kierunku mojego promotora, dr Agnieszki Bojanowskiej - Jackowskiej.

[1] W 2001r. w pracy Hertwecka [Her01] określone zostały dwie nieizomorficzne grupy stanowiące kontrprzykład do ogólnego problemu.

Rozdział 1

Niektóre pojęcia i fakty przygotowawcze

Oryginalna praca E. Dade, zawierająca dowód rozważanego w tej pracy twierdzenia, mieści się na czterech stronach formatu A4. Szczegółowe przedstawienie wszystkich zawartych w niej konstrukcji i rozumowań wymaga nie tylko rozwinięcia pewnych skrótów myślowych czy sprawdzenia odpowiednich rachunków, ale także wprowadzenia i omówienia kilku kluczowych pojęć – zewnętrznych wobec istoty problemu. Będą się one mieściły w paragrafach: produkty półproste grup oraz algebry grupowe. Udowodnimy szereg faktów, które wykorzystywać będziemy w odpowiednich fragmentach dalszych rozdziałów.

1.1. Produkt półprosty grup

Definicja 1 (Zewnętrzny produkt półprosty)**.** *Niech A, B - dowolne grupy, oraz $\phi : B \to Aut(A)$ - homomorfizm. Wówczas na $A \times B$ można określić strukturę grupy $A \rtimes_\phi B$ przyjmując następujące definicje operacji brania elementu neutralnego, brania elementu odwrotnego oraz mnożenia:*

1. $1_{A \rtimes_\phi B} = (1_A, 1_B)$,
2. $(a, b)(x, y) = (a\phi_b(x), by)$,
3. $(a, b)^{-1} = (\phi_{b^{-1}}(b^{-1}), b^{-1})$.

Odnotujmy następujące własności zewnętrznego produktu półprostego:

Uwaga. *Niech $G = A \rtimes_\phi B$. Wówczas:*

1. $A \times \{1_B\} \lhd G$,
2. $G = (A \times \{1_B\})(\{1_A\} \times B) = \{(a, 1_B)(1_A, b) : a \in A, b \in B\}$,
3. $(A \times \{1_B\}) \cap (\{1_A\} \times B) = (1_A, 1_B) = 1_G$.

Dowód. Punkt pierwszy wynika stąd, że $A \times \{1_B\}$ jest jądrem homomorfizmu $p : G \to B$ postaci $p(a, b) = b$. Punkt drugi wynika z bezpośredniego sprawdzenia: dla dowolnych $a \in A, b \in B$ mamy: $(a, 1_B)(1_A, b) = (a\phi_{1_B}(1_A), 1_B) = (a, b)$. Punkt trzeci jest oczywisty.

□

Definicja 2 (Wewnętrzny produkt półprosty)**.** *Niech G - dowolna grupa, $A \lhd G$, $B \leqslant G$, przy czym $G = AB$ oraz $A \cap B = \{1_G\}$. Wówczas G nazywamy wewnętrznym produktem półprostym grup A i B.*

Powyższa definicja zawiera w sobie element niejednoznaczności. Łatwo wskazać dwie nieizomorficzne grupy G, H oraz grupy $A_1 \lhd G, A_2 \lhd H$, $B_1 \leqslant G, B_2 \leqslant H$ takie, że $A_1 \simeq A_2$, $B_1 \simeq B_2$, ale $G \not\simeq H$.[1]

Uwaga. *Niech grupa $G = AB$ będzie wewnętrznym produktem półprostym podgrupy normalnej A oraz podgrupy B. Wówczas $G \simeq A \times_\phi B$, przy czym $\phi : B \to Aut(A)$ jest homomorfizmem postaci*

$$\phi_b(a) = bab^{-1},\ a \in A, b \in B.$$

Dowód. Zauważmy, że w przypadku produktu półprostego $G = AB$ mamy jednoznaczność zapisu elementu $g \in G$ jako iloczynu dwóch elementów[2] $a \in A, b \in B$. Istotnie jeżeli $ab = cd$, gdzie $a, c \in A, b, d \in B$, to $bd^{-1} = c^{-1}a$. Prawa strona równości należy do A, lewa strona do B. Zatem wobec założenia $A \cap B = 1_G$ mamy $b = d, a = c$. Jednoznaczność ta oznacza, że przekształcenie $f : A \times_\phi B \to G$ postaci $f(a, b) = ab$ jest bijekcją. Pozostaje pokazać, że jest to homomorfizm. Dla $a, c \in A$, $b, d \in B$ mamy:

$$f((a,b)(c,d)) = f((a\phi_b(c), bd)) = f(abcb^{-1}, bd) = abcb^{-1}bd = (ab)(cd) = f(a,b)f(c,d).$$

□

Innymi słowy, jeżeli grupa G jest produktem półprostym grupy A i B to oznacza, że istnieje pewien homomorfizm ϕ grupy B w automorfizmy grupy A. Co więcej, w grupie G prawdziwa jest relacja $\phi_b(a) = bab^{-1}$, same zaś mnożenie i odwracanie mają następującą postać:

1. $ab \cdot cd = a\phi_b(c) \cdot bd,\ a, c \in A,\ b, d \in B,$
2. $(a \cdot b)^{-1} = \phi_{b^{-1}}(a^{-1}) \cdot b^{-1}.$

Jeżeli sytuacja będzie tego wymagała, będziemy pisać, że G jest wewnętrznym produktem półprostym A i B względem ϕ.

Przykład. *Grupa podstawowa butelki Kleina zadana jest przez następującą prezentację:*

$$G = \langle\, a, b \,|\, aba^{-1} = b^{-1} \,\rangle.$$

Łatwo widzieć, że $G \simeq \mathbb{Z} \cdot \mathbb{Z}$, gdzie $\phi : \mathbb{Z} \to Aut(\mathbb{Z})$ dane jest wzorem $\phi_a(b) = b^{-1}$.

Na koniec wprowadzenia we własności produktów półprostych udowodnimy przydatny w dalszych rozważaniach lemat:

Lemat 1. *Niech $G = AB$ będzie wewnętrznym produktem półprostym względem ϕ. Niech $\sigma \in Aut(A)$ należy do centralizatora[3] $C_{Aut(A)}(\phi)$. Wówczas istnieje $\overline{\sigma} \in Aut(G)$ będący rozszerzeniem automorfizmu σ na całe G.*

Dowód. Określamy $\overline{\sigma} : G \to G$ następującym wzorem: $\overline{\sigma}(ab) = \sigma(a)b$. Podobnie jak wyżej pokazujemy, że jest to bijekcja. Pozostaje sprawdzić warunek homomorfizmu. Dla $a, c \in A$, $b, d \in B$ mamy zgodnie z założeniami:

$$\overline{\sigma}((ab)(cd)) = \overline{\sigma}(a\phi_b(c)bd) = \sigma(a\phi_b(c))bd = \sigma(a)\phi_b(\sigma(c))bd = (\sigma(a)b)(\sigma(c)d) = \overline{\sigma}(ab)\overline{\sigma}(cd).$$

□

[1] Wystarczy wziąć $G \simeq \mathbb{Z}_4, H \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

[2] Jest to prawdą nawet przy opuszczeniu założenia o normalności podgrupy A w G.

[3] Przypomnijmy, że centralizator elementu $x \in G$, to: $C_G(x) = \{g \in G \,|\, gx = xg\}$.

1.2. Algebry grupowe

Definicja 3 (Algebra grupowa)**.** *Niech $\mathbb{K}$ będzie ciałem, zaś G - grupą. Wówczas przez algebrę grupową $\mathbb{K}[G]$ określamy lewostronną $\mathbb{K}$ - algebrę spełniającą następujące warunki:*

1. *Bazą $\mathbb{K}[G]$ jest następujący zbiór wektorów: $\{x_g : g \in G\}$,*
2. *Działanie dwuliniowe $\mathbb{K}[G] \times \mathbb{K}[G] \to \mathbb{K}[G]$ zadane jest na bazie wzorem: $x_g \cdot x_h = x_{gh}$.*

Algebra grupowa jest zatem zbiorem skończonych sum formalnych postaci:

$$\alpha = \sum_{g \in G} a_g \cdot x_g,\ a_g \in \mathbb{K}.$$

Łatwo sprawdzić, że jest to algebra łączna z jedynką. Identyfikując elementy grupy G z elementami bazowymi algebry grupowej poprzez mnożenie $g \to 1 \cdot x_g$, dostajemy zanurzenie $G \subseteq \mathbb{K}[G]$. Sumy oraz produkty formalne stają się wówczas zwykłymi sumami i produktami. W dalszych rozważaniach będziemy zatem opuszczać kropkę przy mnożeniu $a_g \cdot x_g$, elementy x_g oznaczać będziemy elementami grupy G, zaś jedynkę algebry grupowej utożsamiać będziemy z jedynką grupy G.

Potrzeba nam wspomnieć o relacji pomiędzy $\mathbb{K}[G], \mathbb{K}[H]$, a $\mathbb{K}[G \times H]$. Do jej określenia konieczne są pewne elementarne informacje na temat iloczynów tensorowych. Zawieramy je (bez dowodu) w dwóch poniższych stwierdzeniach:

1. Niech V, W będą przestrzeniami liniowymi nad $\mathbb{K}$. Jeżeli $\{v_i\}_{i \in I}, \{w_j\}_{j \in J}$ są bazami odpowiednio V, W nad $\mathbb{K}$, to $\{v_i \otimes w_j\}_{i \in I,\ j \in J}$ jest bazą $A \otimes B$ nad $\mathbb{K}$,
2. Niech A, B będą algebrami nad $\mathbb{K}$. Wówczas $A \otimes_{\mathbb{K}} B$ jest także $\mathbb{K}$ - algebrą z następującym mnożeniem:
$$(a_1 \otimes b_1)(a_2 \otimes b_2) = (a_1 a_2 \otimes b_1 b_2).$$

Lemat 2.

$$\mathbb{K}[G \times H] \simeq \mathbb{K}[G] \otimes_{\mathbb{K}} \mathbb{K}[H].$$

Dowód. Zacznijmy od oczywistej uwagi:

Uwaga. *Niech E będzie $\mathbb{K}$ - algebrą oraz niech $\tau : G \to U(E)$ będzie homomorfizmem między grupą G a grupą elementów odwracalnych[4] algebry E. Wówczas τ rozszerza się do homomorfizmu $\mathbb{K}$ - algebr $\overline{\tau} : \mathbb{K}[G] \to E$ danego wzorem:*

$$\overline{\tau}\left(\sum a_x x\right) = \sum a_x \tau(x).$$

Przekształcenie $\overline{\tau}$ jest dobrze określone, w sposób oczywisty $\mathbb{K}$ - liniowe. Stąd i z tego, że $\tau(xy) = \tau(x)\tau(y)$ wynika także multiplikatywność $\overline{\tau}$. Z faktu tego będziemy niejednokrotnie korzystać. Sprawdźmy jak przydaje się on do dowodu lematu. Z definicji mnożenia tensorowego w $\mathbb{K}[G] \otimes_{\mathbb{K}} \mathbb{K}[H]$ każdy element bazowy tej algebry jest odwracalny. Przekształcenie $\tau : G \times H \to \mathbb{K}[G] \otimes_{\mathbb{K}} \mathbb{K}[H]$ postaci $\tau(g, h) = g \otimes h$ jest więc niewątpliwie homomorfizmem w grupę elementów odwracalnych. Możemy je zatem liniowo rozszerzyć do homomorfizmu $\mathbb{K}$ - algebr $\overline{\tau} : \mathbb{K}[G \times H] \to \mathbb{K}[G] \otimes_{\mathbb{K}} \mathbb{K}[H]$. Przeprowadza ono bazę jednej przestrzeni na bazę drugiej, jest to więc izomorfizm. □

[4] Algebra traktowana jest tu jako pierścień z 1, a element odwracalny $a \in E$ to taki, dla którego istnieje $b \in E$ spełniający warunek: $ab = 1$.

Do dalszych rozważań konieczne jest ustalenie relacji pomiędzy algebrami grupowymi grupy G i jej podgrupy H (nad danym ciałem). Wprowadźmy dwie dodatkowe definicje:

Definicja 4 (Nośnik)**.** *Niech $\alpha = \sum a_x x \in \mathbb{K}[G]$. Wówczas nośnikiem elementu α, ozn. $Supp(\alpha)$, określamy następujący zbiór: $Supp(\alpha) = \{x \in G \,|\, a_x \neq 0\}$.*

Definicja 5 (Lewy i prawy transwersal[5])**.** *Niech H będzie podgrupą grupy G. Przez lewy transwersal określamy dowolny pełen układ reprezentantów warstw lewostronnych H w G. Analogicznie określamy prawy transwersal.*

Prawdziwy jest następujący fakt:

Lemat 3. *$\mathbb{K}[G]$ jest wolnym prawym $\mathbb{K}[H]$ - modułem, gdzie bazę stanowi lewy transwersal H w G. Podobnie, $\mathbb{K}[G]$ jest wolnym lewym - $\mathbb{K}[H]$ modułem, gdzie bazę stanowi prawy transwersal H w G.*

Dowód. Udowodnimy pierwszą część tezy. Dowód drugiej części jest analogiczny. Niech Y będzie lewym transwersalem. Chcemy pokazać, że:

$$\mathbb{K}[G] = \bigoplus_{i=1}^{[G:H]} y_i \mathbb{K}[H], \quad y_i \in Y.$$

Wykażmy po pierwsze, że elementy y_i rozpinają $\mathbb{K}[G]$. Niech $\alpha \in \mathbb{K}[G]$. Ponieważ $Supp(\alpha)$ jest skończony, zawarty jest w jedynie skończenie wielu lewych warstwach H w G, powiedzmy $y_1H, y_2H, \ldots, y_nH$, gdzie $y_i \in Y, i = 1, 2, 3, \ldots n$. Możemy więc zapisać $\alpha = \alpha_1 + \alpha_2 + \ldots + \alpha_n$, gdzie α_i jest częściową sumą tych $a_x x$, dla których $x \in y_iH$. Skoro $x \in y_iH \Rightarrow y_i^{-1}x \in H$, to pisząc:

$$\alpha = \sum_{i=1}^{n} y_i(y_i^{-1}\alpha_i)$$

dostajemy pierwszą część dowodu, bowiem $y_i^{-1}\alpha_i \in \mathbb{K}[H]$. Aby pokazać, że uzyskana suma jest sumą prostą rozważmy znowu $\alpha = \sum y a_y$, gdzie $y \in Y$, $a_y \in \mathbb{K}[H]$. Niech $y_0 \in Y$. Wówczas $y_0^{-1}\alpha = \sum y_0^{-1} y a_y$. Element $y_0^{-1}y \in H \Leftrightarrow y = y_0$. Zatem przy naturalnej projekcji[6] $\pi_H : \mathbb{K}[G] \to \mathbb{K}[H]$ danej wzorem:

$$\pi_H \left(\sum_{x \in G} a_x x \right) = \sum_{x \in H} a_x x.$$

Zatem $\pi_H(y_0^{-1}\alpha) = \alpha_{y_0}$. Rozkład α zależy więc tylko od postaci π_H, ta zaś jest jednoznaczna. □

Udowodniony fakt ma podstawowe znaczenie w teorii reprezentacji grup. My pokażemy jak można przy jego pomocy dostać związek pomiędzy algebrą grupową $\mathbb{K}[G]$, a algebrą $\mathbb{K}[G/H]$, gdzie H jest podgrupą normalną G. Użyjemy w tym celu także uwagi z dowodu lematu 2. Weźmy naturalny homomorfizm $G \to G/H$. Jest on jednocześnie homomorfizmem grupy G w grupę elementów odwracalnych $\mathbb{K}[G/H]$. Zgodnie ze wspomnianą uwagą, przedłuża się on do $\mathbb{K}$ - homomorfizmu algebr grupowych $\rho_H : \mathbb{K}[G] \to \mathbb{K}[G/H]$. Przyjmując, że $x \in G$ przechodzi na $\overline{x} \in G/H$, homomorfizm ρ_H ma postać:

$$\rho_H \left(\sum a_x x \right) = \sum a_x \overline{x}.$$

[5]Naśladujemy tu terminologię określoną w [Pas77].

[6]Nie jest to homomorfizm algebr. Można pokazać, że jest to przekształcenie $\mathbb{K}[H]$ - liniowe.

Interesuje nas jądro tego przekształcenia. Zacznijmy od trywialnego przypadku: $H = G$. Jądrem ρ_G jest wówczas zbiór:

$$\omega(\mathbb{K}[G]) = \left\{ \sum a_x x \mid \sum a_x = 0 \right\},$$

nazywany ideałem augumentacji algebry $\mathbb{K}[G]$. Przy jego pomocy można opisać jądro w ogólnej sytuacji:

Lemat 4. *Niech $H \triangleleft G$. Wówczas $\omega(\mathbb{K}[H]) \cdot \mathbb{K}[G]$ jest jądrem ρ_H.*

Dowód. Niech X będzie prawym transwersalem H w G. Bierzemy dowolne $\alpha \in \mathbb{K}[G]$. Zgodnie z lematem 3, możemy rozłożyć α na sumę $\sum \alpha_x x$, traktując $\mathbb{K}[G]$ jako lewy $\mathbb{K}[H]$ - moduł. Korzystając z tego, że ρ_H to homomorfizm $\mathbb{K}$ - algebr mamy:

$$\rho_H(\alpha) = \sum \rho_H(\alpha_x)\rho_H(x).$$

Jest jasne, że skoro $\alpha_x \in \mathbb{K}[H]$, to $\rho_H(\alpha_x) \in \mathbb{K}$. Co więcej z definicji zbioru X wiemy, że obrazy $\rho_H(x)$ stanowią bazę $\mathbb{K}[G/H]$. Zatem $\rho_H(\alpha)$ jest kombinacją liniową wektorów niezależnych, zatem $\alpha \in \ker(\rho_H) \Leftrightarrow \rho_H(\alpha_x) = 0, x \in X$. Wiemy, że ρ_H przekształca wszystkie elementy grupy H na jedynkę algebry grupowej $\mathbb{K}[G/H]$. Oznacza to, że w $\rho_H(\alpha_x)$ wszystkie współczynniki stoją przy jedynce. Skoro jednak mamy dostać 0 oznacza to, że $\alpha_x \in \omega(\mathbb{K}[H])$. Przechodząc do ogólnej postaci ρ_H widzimy, że jego jądro ma postać:

$$\ker(\rho_H) = \bigoplus_{x \in X} \omega(\mathbb{K}[H])x = \omega(\mathbb{K}[H]) \cdot \mathbb{K}[G]. \tag{1.1}$$

□

Jest jasne, że ρ_H jest epimorfizmem. Zatem jako wniosek z lematu 3. i twierdzenia o izomorfizmie algebr dostajemy:

$$\mathbb{K}[G]/(\omega(\mathbb{K}[H]) \cdot \mathbb{K}[G]) \simeq \mathbb{K}[G/H]. \tag{1.2}$$

Jesteśmy już prawie gotowi do dowodu kluczowego twierdzenia części wprowadzającej. Wprowadźmy wpierw potrzebne nam definicje:

Definicja 6 (Idempotent)**.** *Element $\alpha \in \mathbb{K}[G]$ nazywamy idempotentem jeżeli $\alpha^2 = \alpha$.*

Definicja 7 (Centrum)**.** *Niech G będzie grupą ($\mathbb{K}[G]$ - algebrą grupową). Centrum grupy (algebry grupowej), oznaczane przez $Z(G)$ ($Z(\mathbb{K}[G])$), to następujący zbiór:*

$$\{g \in G \mid gh = hg, \;\; h \in G\} \;\; \textit{(analogicznie dla algebry grupowej).}$$

Element należący do centrum nazywamy centralnym.

Definicja 8 (Suma podgrupy)**.** *Niech H będzie pogrupą G. Przez sumę H w $\mathbb{K}[G]$, ozn. $\widehat{H}$, rozumiemy element $\sum_{h \in H} h \in \mathbb{K}[G]$.*

Odnotujmy w tym miejscu, że prawdziwa jest następująca równość:

$$\left\{ \alpha \in \mathbb{K}[G] \mid \widehat{H} \cdot \alpha = 0 \right\} = \omega(\mathbb{K}[H]) \cdot \mathbb{K}[G]. \tag{1.3}$$

Sprawdzenie jej prawdziwości jest identyczne z dowodem lematu 4. i formuły (1.1).

Twierdzenie 1. *Jeżeli $H \triangleleft G$ oraz $|H| \neq 0$ w $\mathbb{K}$, wówczas:*

1. $e = \frac{1}{|H|}\widehat{H} \in Z(\mathbb{K}[G])$,
2. *e jest idempotentem w $\mathbb{K}[G]$,*
3. $e\mathbb{K}[G] \simeq \mathbb{K}[G/H]$.

Dowód. Sprawdźmy najpierw, że dla każdego $\alpha \in \mathbb{K}[G]$ mamy $\alpha \cdot e = e \cdot \alpha$. Wystarczy, że pokażemy to dla $e = g,\ g \in G$. Zauważmy, że $g\widehat{H}$ jest sumą wszystkich elementów warstwy gH podgrupy H w G. Podobnie $\widehat{H}g$ jest sumą wszystkich elementów warstwy Hg. Skoro H jest normalna w G, to $gH = Hg$, dla każdego $g \in G$. W szczególności równe są sumy elementów tych warstw w $\mathbb{K}[G]$. Mnożenie przez $\frac{1}{|H|}$ nie wyprowadza nas z $\mathbb{K}[G]$, zatem $e \in Z(\mathbb{K}[H])$.

Do dowodu punktu 2. wystarczy zauważyć, że element $e - 1_G \in \omega(\mathbb{K}[H]) \cdot \mathbb{K}[G]$. Istotnie, $e^2 - e = \frac{1}{|H|}\widehat{H}(e - 1_G)$. Na mocy formuły (1.3) wystarczy sprawdzić, że $e - 1_G \in \ker(\rho_H)$. Mamy:

$$\rho_H(e - 1_G) = \frac{1}{|H|}\sum_{h \in H} \rho_H(h) - \rho_H(1_G) = \frac{1}{|H|} \cdot |H| \cdot 1_{G/H} - 1_{G/H} = 0.$$

Aby pokazać, że $e\mathbb{K}[G] \simeq \mathbb{K}[G/H]$, rozważmy przekształcenie: $f_e : \mathbb{K}[G] \to e\mathbb{K}[G]$, zadane na wektorach bazowych z G wzorem: $f_e(g) = eg$. Jest to, rzecz jasna, epimorfizm $\mathbb{K}$ - algebr. Jego jądrem jest na mocy (1.3) ideał $\omega(\mathbb{K}[H]) \cdot \mathbb{K}[G]$. Korzystając więc z (1.2) oraz z twierdzenia o izomorfizmie otrzymujemy:

$$e\mathbb{K}[G] \simeq \mathbb{K}[G]/(\omega(\mathbb{K}[H]) \cdot \mathbb{K}[G]) \simeq \mathbb{K}[G/H]. \tag{1.4}$$

□

Rozdział 2

Pary nieizomorficznych grup

2.1. Konstrukcja grup

Na początku całej konstrukcji szukamy par liczb pierwszych (p, q) takich, że $q = 1 \, mod \, p^2$. Uzasadnijmy krótko, że istnieje nieskończenie wiele takich par. Weźmy dowolną liczbę pierwszą p i skonstruujmy ciąg arytmetyczny $a_k = (p^2 + 1) + kp^2$, $k \in \mathbb{N}$. Wyraz początkowy oraz różnica tego ciągu są względnie pierwsze, zatem z twierdzenia Dirichleta istnieje w nim nieskończenie wiele liczb pierwszych. Ustalmy pewną taką parę (p, q).

Do konstrukcji potrzebujemy czterech grup; jednej rzędu p, jednej rzędu p^2 i dwóch rzędu q^3. Stosowne definicje przedstawiają się następująco:

$\langle u_1 \rangle \simeq \mathbb{Z}_p$,

$\langle u_2 \rangle \simeq \mathbb{Z}_{p^2}$,

$Q_1 = \langle\, x_1, y_1, z_1 \,|\, x_1^q = y_1^q = z_1^q = 1, [x_1, y_1] = z_1, [x_1, z_1] = 1, [y_1, z_1] = 1 \,\rangle$,

$Q_2 = \langle\, x_2, y_2, z_2 \,|\, x_2^q = z_2^q = 1, y_2^q = z_2, [x_2, y_2] = z_2, [x_2, z_2] = 1, [y_2, z_2] = 1 \,\rangle$.

O ile struktura pierwszych dwóch grup jest zupełnie przejrzysta, o tyle grupy $Q_i, i = 1, 2$ wyglądają na bardziej skomplikowane. Jest jasne, że są one nieprzemienne. Łatwo także zobaczyć, że $\langle y_i, z_i \rangle \triangleleft Q_i$. Istotnie, są to jądra homomorfizmów $Q_i \to \langle x_i \rangle$, które generatory y_i, z_i przeprowadzają na jedynki, zaś x_i przeprowadzają na nie same. Wobec faktu, że $|\langle x_i \rangle|$ są pierwsze, otrzymujemy: $\langle x_i \rangle \cap \langle y_i, z_i \rangle = 1_{Q_i}$. Widzimy więc, że Q_i są produktami półprostymi. Zgodnie z dostępnymi prezentacjami potrafimy dokładnie określić działanie ϕ_i grup $\langle x_i \rangle$ na $\langle y_i, z_i \rangle$:

$$\phi_i(x_i)(y_i) = x_i y_i x_i^{-1} = z_i y_i,$$

$$\phi_i(x_i)(z_i) = x_i z_i x_i^{-1} = z_i.$$

Ostatecznie więc, zgodnie z poczynionymi na początku pracy uwagami na temat produktów półprostych, opis grup Q_i wygląda następująco:

$$Q_1 \simeq \mathbb{Z}_q^2 \rtimes_{\phi_1} \mathbb{Z}_q,$$

$$Q_2 \simeq \mathbb{Z}_{q^2} \rtimes_{\phi_2} \mathbb{Z}_q.$$

Znając strukturę podstawowych cegiełek możemy zabrać się do konstruowania szukanych grup. Sprawdzimy, że mają sens następujące produkty półproste: $Q_j \langle u_i \rangle$, $i, j = 1, 2$. Wyjdźmy od zewnętrznej definicji produktu półprostego. Potrzebujemy w niej jedynie określenia działania grup $\langle u_i \rangle$ na Q_j. Do tego potrzebować będziemy pewnych teorioliczbowych uwag.

Chcemy pokazać, że istnieje liczba naturalna $n \neq 1$, spełniająca następujące kongruencje:

$$n \neq 1 \, mod \, q^2, \quad n^p = 1 \, mod \, q^2.$$

Równoważnie można powiedzieć, że szukamy nietrywialnego elementu grupy $U(\mathbb{Z}_{q^2})$, który ma rząd p. Rząd grupy $U(\mathbb{Z}_{q^2})$ wynosi $q(q-1)$. Wiemy, że $q = 1 \, mod \, p^2$, zatem $p \mid q-1$. Na mocy twierdzenia Cauchy'ego istnieje w tej grupie element rzędu p. Zatem szukane n istnieje. Zauważmy jeszcze, że $n \neq 1 \, mod \, q$. Wiemy, że $q^2 \mid n^p - 1 = (n-1)(n^{p-1} + n^{p-2} + \ldots + 1)$, zatem skoro $n \neq 1 \, mod \, q^2$, to $q \mid n^{p-1} + n^{p-2} + \ldots + 1$. Gdyby $n = 1 \, mod \, q$, dostalibyśmy następującą niedorzeczność:

$$n^{p-1} + n^{p-2} + \ldots + 1 = 1 + 1 + 1 + \ldots + 1 = p \, mod \, q \Rightarrow p = 0 \, mod \, q.$$

Lemat 5. *Niech k będzie ustaloną liczbą całkowitą taką, że $1 \leqslant k < p$. Następujące dwa przekształcenia: $\sigma_j : Q_j \to Q_j$ $j = 1, 2$:*

$$\sigma_j(x_j) = x_j \, , \, \sigma_j(y_j) = y_j^{n^k} \, , \, \sigma_j(z_j) = z_j^{n^k}$$

są automorfizmami rzędu p.

Dowód. Skorzystajmy z lematu 1.1. Niech σ_j' będą obcięciami σ_j do podgrup abelowych $\langle y_j, z_j \rangle$. Potrzeba nam, by były to automorfizmy. Sprawdźmy multiplikatywność:

$$\begin{aligned} \sigma_j((y_j^{n_1} z_j^{m_1})(y_j^{n_2} z_j^{m_2})) &= \sigma(y_j^{n_1+n_2} z_j^{m_1+m_2}) = \\ &= y_j^{n^k(n_1+n_2)} z_j^{n^k(m_1+m_2)} = \\ &= (y_j^{n_1} z_j^{m_1})^{n^k} (y_j^{n_2} z_j^{m_2})^{n^k} = \sigma_j(y_j^{n_1} z_j^{m_1}) \sigma_j(y_j^{n_2} z_j^{m_2}). \end{aligned}$$

Skoro $|\langle y_j, z_j \rangle| = q^2$ to:

$$y_j^{n_1} z_j^{m_1} \in \ker(\sigma_j') \Leftrightarrow n_1 n^k = 0 \, mod \, q^2, \; n_2 n^k = 0 \, mod \, q^2.$$

Korzystamy z tego, że $n^p = 1 \, mod \, q^2 \Rightarrow n \neq 0 \, mod \, q$ i mamy: $q^2 \mid n_1$ oraz $q^2 \mid n_2$. Zatem:

$$y_1^{n_1} z_1^{m_1} \in \ker(\sigma_1') \Leftrightarrow y_1^{n_1} z_1^{m_1} = 1.$$

$$y_2^{n_1} z_2^{m_1} \in \ker(\sigma_2') \Leftrightarrow y_2^{n_1} z_2^{m_1} = \left(z_2^{\frac{n_1}{q^2}} \right)^q = 1.$$

Pozostaje pokazać, że σ_j' są epimorfizmami. Wystarczy, że umiemy dostać za ich pomocą każdy element podgrup $\langle y_j \rangle, \langle z_j \rangle$. Chcąc otrzymać element z_j^m wystarczy rozwiązać kongruencję $xn^k = m \, mod \, q$ i wziąć $\sigma(z_j^x)$. Analogicznie postępujemy dla y_1^m. Chcąc dostać y_2^m rozwiązujemy kongruencję $xn^k = m \, mod \, q^2$. Jeśli $xn^k = Nq^2 + m$, to $\sigma_2(y_2^x) = y_2^{xn^k} = z_2^{Nq} y_2^m = y_2^m$. Wiemy więc, że σ_j' to automorfizmy. Abelowość grup $\langle y_j, z_j \rangle$ gwarantuje nam, że $\sigma_j' \circ \phi_j = \phi_j \circ \sigma_j'$, gdzie ϕ_j to określone wyżej działania $\langle x_j \rangle$ na $\langle y_j, z_j \rangle$. Zgodnie więc z lematem 1.1, σ_j' rozszerzają się do automorfizmów całych Q_j, poprzez

$$\overline{\sigma'}(ab) = \sigma'(a)b, \; a \in \langle y_j, z_j \rangle, b \in \langle x_j \rangle.$$

$\sigma_j(x_j) = x_j \Rightarrow \overline{\sigma_j'} = \sigma_j$. Pokazaliśmy, że σ_j są automorfizmami. Dla ustalonego k zdefiniujmy $f_{jk} = \sigma_j$, oraz $f_{j0} = Id_{Q_j}$. Wobec kongruencji $n^p = 1 \, mod \, q^2$, łatwo widzieć, że $f_{jk_1} \circ f_{jk_2} = f_{jk_3}$, gdzie $k_3 = k_1 + k_2 \, mod \, p$, jak również $(f_1)^p = f_0$. Zatem zbiór $\{f_{jk} \mid 0 \leqslant k < p\}$ wraz ze składaniem przekształceń jest grupą cykliczną rzędu p. Stąd każdy automorfizm σ_j ma rząd p. $\square$

Możemy już zdefiniować działania grup $\langle u_i\rangle$ na Q_j. Niech $u_i^k \in \langle u_i\rangle$, przy czym $k = k' \,mod\, p$. Wówczas określamy następujące przekształcenia: $\sigma_{ij} : \langle u_i\rangle \to Aut(Q_j)$:

$$\sigma_{ij}(u_i^k)(x_j) = x_j \,,\ \sigma_{ij}(u_i^k)(y_j) = y_j^{n^{k'}} \,,\ \sigma_{ij}(u_i^k)(z_j) = z_j^{n^{k'}}.$$

Powyższy lemat gwarantuje nam, że σ_{ij} są dobrze określonymi działaniami grup $\langle u_i\rangle$. Spełniliśmy zatem wszystkie wymogi definicji zewnętrznego produktu półprostego. Ma więc sens rozważanie następujących grup:

$$Q_j \rtimes_{\sigma_{ij}} \langle u_i\rangle,\ \ i,j = 1,2.$$

Niech teraz:

$$\overline{\sigma_{ij}}(u_i^k)(x_j) = x_j = u_i^k x_j u_i^{-k}, \tag{2.1a}$$

$$\overline{\sigma_{ij}}(u_i^k)(y_j) = y_j^{n^{k'}} = u_i^k y_j u_i^{-k}, \tag{2.1b}$$

$$\overline{\sigma_{ij}}(u_i^k)(z_j) = z_j^{n^{k'}} = u_i^k z_j u_i^{-k}. \tag{2.1c}$$

Zgodnie z uwagami na temat produktów półprostych, poczynionymi na początku pracy, dostaliśmy w ten sposób wewnętrzne produkty półproste grup. Mają miejsce następujące izomorfizmy:

$$Q_j \rtimes_{\sigma_{ij}} \langle u_i\rangle \simeq Q_j \rtimes_{\overline{\sigma_{ij}}} \langle u_j\rangle \simeq Q_j\langle u_i\rangle,\ \ i,j = 1,2.$$

Doszliśmy w ten sposób do najważniejszej definicji w tej pracy:

Definicja 9. *Niech p, q - liczby pierwsze spełniające kongruencję: $q = 1 \,mod\, p^2$, oraz niech $Q_j\langle u_i\rangle,\ \ i,j = 1,2$ - grupy określone wyżej. Wówczas definiujemy:*

$$G(p,q) = Q_1\langle u_1\rangle \times Q_2\langle u_2\rangle,$$
$$H(p,q) = Q_1\langle u_2\rangle \times Q_2\langle u_1\rangle.$$

To właśnie grupy $G(p,q), H(p,q)$ są kontrprzykładami do problemu izomorfizmu, w tej odmianie, którą od początku rozważamy. Ich własnościom poświęcamy pozostałą część pracy. Zaczniemy od dowodu, że nie są one izomorficzne.

2.2. $G(p,q) \ncong H(p,q)$

Zakładamy, że p, q są ustalone i dwie rozważane grupy oznaczamy dalej przez G, H. Chcemy policzyć ich komutanty G', H'. Przypomnijmy w postaci uwagi dwie ważne dla nas własności tych podgrup:

Uwaga. *Niech X - grupa. Wówczas:*

1. *Jeżeli $X_1 \lhd X$, to X/X_1 jest abelowa $\Leftrightarrow\ X' \subseteq X_1$,*
2. *Jeżeli $X = X_1 \times X_2$ jest produktem prostym, to $X' = X_1' \times X_2'$.*

Jest jasne, że wystarczy nam policzyć $(Q_j\langle u_i\rangle)'$. Rozważmy homomorfizmy $f_{ij} : Q_j\langle u_i\rangle \to \langle x_j\rangle\langle u_i\rangle$, postaci:

$$f_{ij}(u_i) = u_i,\ \ f_{ij}(x_j) = x_j,\ \ f_{ij}(y_j) = 1, f_{ij}(z_j) = 1.$$

Ich jądrami, a więc podgrupami normalnymi w $Q_j\langle u_i\rangle$ są oczywiście $\langle y_j, z_j\rangle$. Ilorazy: $\langle x_j\rangle\langle u_i\rangle$ – są grupami abelowymi (z 2.1a mamy: $x_j = u_j x_j u_j^{-1}$). Zauważmy, że szukane komutanty są nie tylko zawarte, ale równe $\langle y_j, z_j\rangle$. Istotnie z definicji Q_j: $[x_j, y_j] = z_j \Rightarrow \langle z_j\rangle \subseteq (Q_j\langle u_i\rangle)'$, zaś z 2.1b: $[y_j, u_i] = y_j^{n-1} \Rightarrow \langle y_j\rangle \subseteq (Q_j\langle u_i\rangle)'$.

Komutanty grup G, H mają zatem tę samą postać: $\langle y_1, z_1\rangle \times \langle y_2, z_2\rangle$[1]. Łatwo zobaczyć, że $(G')^q = (H')^q$, tj. podgrupa, złożona z elementów komutantów podniesionych do potęgi q, ma postać $\langle (1, z_2)\rangle$. Poczyniwszy te uwagi wstępne, jesteśmy gotowi do właściwego dowodu.

Dowód nieizomorficzności G, H:

Załóżmy wbrew tezie, że $G \simeq H$. Zatem izomorficzne są też centralizatory $C_G(x) \simeq C_H(x)$, gdzie x jest generatorem grupy cyklicznej $(G')^q = (H')^q$. Tymczasem:

1. $C_G((1, z_2)) = Q_1\langle u_1\rangle \times Q_2$. Istotnie, centralizatorem jedynki jest cała grupa, stąd pierwszy czynnik. Drugi zaś bierze się stąd, że z_2 jest centralny w Q_2, ale na mocy 2.1c nie jest przemienny z u_2.

2. $C_H((1, z_2)) = Q_1\langle u_2\rangle \times Q_2\langle u_1^p\rangle$. Pierwszy czynnik nie budzi wątpliwości, podobnie jak w punkcie 1. Drugi czynnik to $Q_2\langle u_1^p\rangle$, ponieważ po pierwsze: z_2 jest centralny w Q_2, po drugie: z 2.1c obliczamy:

$$u_1^k z_2 u_1^{-k} z_2^{-1} = 1 \Leftrightarrow z_2^{n^k} z_2^{-1} = 1 \Leftrightarrow n^k = 1 \, mod \, q^2 \Leftrightarrow k = p.$$

Te centralizatory nie są jednak grupami izomorficznymi! Spójrzmy na ich p - podgrupy Sylowa. Pierwsza z nich jest izomorficzna z $\langle u_1\rangle \simeq \mathbb{Z}_{p^2}$, a więc jest grupą cykliczną. Druga zaś jest izomorficzna z $\langle u_2\rangle \times \langle u_1^p\rangle \simeq (\mathbb{Z}_p)^2$, a więc nie jest grupą cykliczną. Uzyskana sprzeczność dowodzi, że $G \not\simeq H$.

[1]Zauważmy, że komutant jest w tym przypadku grupą abelową. Pokazuje to, że grupy Dade są rozwiązalne stopnia 2, lub inaczej metabelowe.

Rozdział 3

$\mathbb{K}[G] \simeq \mathbb{K}[H]$

Celem tego rozdziału jest udowodnienie następującego twierdzenia:

Twierdzenie (Dade 1970)**.** *Niech* $\mathbb{K}$ *będzie dowolnym ciałem. Wówczas ma miejsce izomorfizm algebr grupowych:* $\mathbb{K}[G(p,q)] \simeq \mathbb{K}[H(p,q)]$.

Przed rozpoczęciem dowodu warto zwrócić uwagę na delikatność, jaką zawiera w sobie teza. Mamy tu na myśli dowolność rozważanego ciała. Można zadać pytanie: czy w ogóle istnieje choć jedno takie ciało $\mathbb{K}$, że algebra grupowa $\mathbb{K}[A]$ jest izomorficzna z $\mathbb{K}[B]$, gdzie $A \ncong B$? Otóż tak! Weźmy np. ciało algebraicznie domknięte $\mathbb{K}$ charakterystyki 0 i skończoną grupę abelową A. Na mocy tw. Maschke algebra grupowa $\mathbb{K}[A]$ jest półprosta[1]. Co więcej, patrząc na algebrę grupową jak na reprezentację regularną[2] grupy G wiemy, że rozkład na składniki proste jest po prostu rozkładem na reprezentacje nieprzywiedlne. Ilość nieizomorficznych klas reprezentacji nieprzywiedlnych grupy skończonej G równa jest ilości klas sprzężoności w tej grupie.[3] Stąd dostajemy rozkład nie tylko na liniowe podprzestrzenie proste, ale na algebry proste:

$$\mathbb{K}[G] \simeq \underbrace{\mathbb{K} \oplus \mathbb{K} \oplus \ldots \oplus \mathbb{K}}_{|G|}.$$

Biorąc zatem dwie nieizomorficzne skończone grupy abelowe tego samego rzędu, dostaniemy izomorficzne algebry grupowe nad $\mathbb{K}$. Pytanie: dla jakich klas grup i jakich ciał $\mathbb{K}$ izomorfizm algebr grupowych pozwala identyfikować jednoznacznie grupy z danej klasy jest do dziś przedmiotem intensywnych badań i źródłem wielu otwartych problemów. Dotkniemy tej tematyki w następnym rozdziale, zastanawiając się nad minimalnością kontrprzykładu podanego przez Dade. Powyższe twierdzenie dostarcza zaś odpowiedzi jedynie na jedno z najbardziej zasadniczych pytań tej problematyki.

Podobnie jak w rozdziale 2. rozważane grupy oznaczać będziemy przez G, H pamiętając o ustalonej parze liczb pierwszych (p,q), spełniającej odpowiednią kongruencję. Dowód podzielimy na dwie zasadnicze części, pokazując izomorfizm algebr grupowych osobno dla ciał charakterystyki q, osobno zaś dla ciał o charakterystyce różnej od q. Zaczniemy od pokazania pewnych własności tych grup, potrzebnych we właściwym dowodzie:

[1] Można ją przedstawić jako sumę prostą algebr prostych tj. takich, które nie mają właściwych ideałów obustronnych.

[2] Dokładnie rzecz biorąc reprezentacja regularna grupy skończonej G to homomorfizm $\rho : G \to GL_{|G|}(\mathbb{K})$, przeprowadzający element $g \in G$ na macierz ρ_g automorfizmu przestrzeni liniowej $\mathbb{K}^{|G|}$, który wektory bazowe $e_x, x \in G$ przeprowadza na $e_{gx}, x \in G$. Zwykle, gdy nie ma obawy o kolizję oznaczeń, przez reprezentację regularną rozumiemy samą przestrzeń $\mathbb{K}^{|G|}$ wyposażoną w strukturę lewego $\mathbb{K}[G]$ - modułu przez liniowe rozszerzenie ρ. Jest jasne, że ta przestrzeń to po prostu $\mathbb{K}[G]$ traktowana jako lewy moduł nad sobą.

[3] Potrzebne fakty można znaleźć np. w rozdziałach 2. i 3. książki Serre [Ser88].

Lemat 1. $G/\langle u_1^p\rangle \simeq H/\langle u_1^p\rangle$.

Dowód. Rozważamy homomorfizmy $f_1 : G \to G, f_2 : H \to H$, spełniające warunki:

$$f_1|_{Q_1} = Id, \quad f_1(u_1, 1) = (u_1^p, 1), \quad f_1|_{Q_2\langle u_2\rangle} = Id,$$
$$f_2|_{Q_2} = Id, \quad f_2(1, u_1) = (1, u_1^p), \quad f_2|_{Q_1\langle u_2\rangle} = Id.$$

Skoro $\langle u_1\rangle$ jest grupą rzędu p^2, to obydwa te homomorfizmy przeprowadzają na 1 dokładnie te elementy grupy $\langle u_1\rangle$, które mają rząd p. Jest ich oczywiście $p^2 - p$. Zatem $f_i(\langle u_1\rangle) = \langle u_2\rangle$, $i = 1, 2$. Jądra obydwu tych przekształceń są zatem izomorficzne z $\langle u_1^p\rangle$. Obrazy zaś mają jednakową w obydwu przypadkach postać: $Q_1\langle u_2\rangle \times Q_2\langle u_2\rangle$. □

Lemat 2.

$$Q_1\langle u_1\rangle/\langle z_1\rangle \simeq Q_2\langle u_1\rangle/\langle z_2\rangle$$
$$Q_1\langle u_2\rangle/\langle z_1\rangle \simeq Q_2\langle u_2\rangle/\langle z_2\rangle$$

Dowód. Wynika to natychmiast z tego, że $Q_j/\langle z_j\rangle \simeq \mathbb{Z}_q^2,\ j = 1, 2.$ □

3.1. Ciała charakterystyki q

Zauważmy, że grupa $\mathbb{K}^*$ zawiera element rzędu p^2. Istotnie, $\mathbb{K}$ zawiera q - elementowe ciało proste $\mathbb{F}_q$, którego grupa multiplikatywna ma rząd $q-1$. Założenie $q = 1\, mod\, p^2$ pozwala nam stwierdzić, że p^2 jest dzielnikiem $|\mathbb{F}_q^*|$. Grupa $\mathbb{F}_q^*$ jest skończona i cykliczna, a to oznacza już, że musi zawierać element rzędu p^2. Mamy włożenie $\mathbb{F}_q^*$ w $\mathbb{K}^*$, zatem i $\mathbb{K}^*$ zawiera przynajmniej jeden element rzędu p^2. Nazwijmy go ϵ. Spełnia on równość:

$$1 + \epsilon^p + \epsilon^{2p} + \ldots + \epsilon^{(p-1)p} = 0.$$

Jest jasne, że skoro $p \neq q$, to klasa elementu $p \in \mathbb{Z}$ należy do $\mathbb{F}_q^*$, a więc i do $\mathbb{K}^*$. Nie będzie budziło wątpliwości oznaczanie klasy jej odwrotności przez 1/p. Przejdźmy do algebry grupowej $\mathbb{K}[G]$. Rozważmy w niej następujące elementy:

$$e_k = \frac{1}{p}\sum_{j=0}^{p-1}(\epsilon^{pk}u_1^p)^j,\ k = 1, 2, \ldots, p-1.$$

Chcemy pokazać, że $e_r e_k = \delta_{r,k} \cdot e_k$. Inaczej mówiąc, wskazane elementy są ortogonalnymi do siebie idempotentami algebry $\mathbb{K}[G]$. Zauważmy, że przy dowolnym $s \in \{1, 2, \ldots, p-1\}$:

$$(e^{pk}u_1^p)^s e_k = \frac{1}{p}\sum_{j=s}^{p+s-1}(\epsilon^{pk}u_1^p)^j = \frac{1}{p}\sum_{j=0}^{p-1}(\epsilon^{pk}u_1^p)^j = e_k.$$

Podobnie wyliczamy, że dla $r, s \in \{1, 2, \ldots, p-1\}$ mamy $(e^{pr}u_1^p)^s e_k = \epsilon^{p(r-k)s} \cdot e_k$. Zatem:

$$e_r e_k = \frac{1}{p}\sum_{s=0}^{p-1}\epsilon^{p(r-k)s} \cdot e_k = \begin{cases} \frac{1}{p}(\underbrace{1+1+\ldots+1}_{p}) \cdot e_k = e_k, & \text{dla } r = k, \\ \frac{1}{p}\sum\limits_{s=0}^{p-1}\epsilon^{ps} \cdot e_k = 0 \cdot e_k = 0, & \text{dla } r \neq k. \end{cases}$$

Zauważmy dalej, że:

$$\sum_{k=0}^{p-1} e_k = \sum_{j=0}^{p-1} \left(1/p \cdot \sum_{k=0}^{p-1} (\epsilon^{pj})^k \right) u_1^{pj} = 1 + 0u_1^p + 0u_1^{2p} + 0u_1^{(p-1)p} = 1.$$

Wiemy więc, że rozważane elementy tworzą tzw. rozkład ortogonalny jedynki. Łatwo też zauważyć, że skoro u_1^p jest centralny w G, to e_k są centralne w $\mathbb{K}[G]$. Stąd $\mathbb{K}[G]$ rozpada się na następującą sumę prostą pierścieni:

$$\mathbb{K}[G] \simeq \bigoplus_{k=0}^{p-1} e_k \mathbb{K}[G].$$

Istotnie, każdy element $x \in \mathbb{K}[G]$ można zapisać jako $x = 1 \cdot x = \left(\sum\limits_{k=0}^{p-1} e_k \right) x = \sum\limits_{k=0}^{p-1} e_k \cdot x$. Suma zaś jest prosta, bo $e_r e_k = \delta_{r,k} \cdot e_k$.

Lemat 3. *Dla $k \in \{1, 2, \ldots, p-1\}$ mamy $\mathbb{K}$ - izomorfizm:*

$$e_0 \mathbb{K}[G] \simeq e_k \mathbb{K}[G] \simeq \mathbb{K}[G/\langle u_1^p \rangle]. \tag{3.1}$$

Dowód. Dla dowodu izomorfizmu $e_0\mathbb{K}[G] \simeq e_k\mathbb{K}[G]$ zauważmy, że podgrupa postaci $\langle Q_1, Q_2, u_2 \rangle$ jest normalna w G. Istnieje zatem naturalny homomorfizm ilorazowy $\pi : G \to \langle u_1 \rangle$. Określamy homomorfizmy $\lambda_k : G \xrightarrow{\pi} \langle u_1 \rangle \to \mathbb{K}^*$, w następujący sposób: $\lambda_k(u_1) = \epsilon^k$. Rozważamy zaś przekształcenia $\overline{\lambda}_k : \mathbb{K}[G] \to \mathbb{K}[G]$ dane wzorami:

$$\overline{\lambda}_k \left(\sum a_x x \right) = \sum a_x \lambda_k(x) x.$$

Jest jasne, że $\overline{\lambda}_k$ są $\mathbb{K}$ - automorfizmami. Bijektywność nie pozostawia żadnych wątpliwości. Podobnie $\mathbb{K}$ - liniowość. Warunek homomorfizmu wystarczy zatem sprawdzić na elementach grupy G: $\overline{\lambda}_k(xy) = \lambda_k(xy)xy = \lambda_k(x)x\lambda_k(y)y = \overline{\lambda}_k(x)\overline{\lambda}_k(y),\ x, y \in G$. Zauważmy, że:

$$\overline{\lambda}_k(e_0) = \frac{1}{p} \sum_{j=0}^{p-1} \lambda_k(u_1^{pj}) u_1^{pj} = e_k = \frac{1}{p} \sum_{j=0}^{p-1} \epsilon^{pjk} u_1^{pj} = e_k.$$

Stąd $e_0\mathbb{K}[G] \simeq e_k\mathbb{K}[G]$. Aby udowodnić, że: $e_0\mathbb{K}[G] \simeq \mathbb{K}[G/\langle u_1^p \rangle]$ wystarczy zauważyć, że $e_0 = \frac{1}{|\langle u_1^p \rangle|} \widehat{\langle u_1^p \rangle}$ i skorzystać z twierdzenia 1.2.1 i formuły (1.4). □

Wykazaliśmy zatem, że:

$$\mathbb{K}[G] \simeq_{\mathbb{K}} \underbrace{\mathbb{K}[G/\langle u_1^p \rangle] \oplus \mathbb{K}[G/\langle u_1^p \rangle] \oplus \ldots \oplus \mathbb{K}[G/\langle u_1^p \rangle]}_{p}.$$

Całe powyższe rozumowanie, łącznie z tezą lematu 3., jest identyczne także dla grupy H.

$$\mathbb{K}[H] \simeq_{\mathbb{K}} \underbrace{\mathbb{K}[H/\langle u_1^p \rangle] \oplus \mathbb{K}[H/\langle u_1^p \rangle] \oplus \ldots \oplus \mathbb{K}[H/\langle u_1^p \rangle]}_{p}.$$

Wobec lematu 1. $G/\langle u_1^p \rangle \simeq H/\langle u_1^p \rangle$, zatem mamy $\mathbb{K}$ - izomorfizm pierścieni $\mathbb{K}[G] \simeq \mathbb{K}[H]$, a więc izomorfizm algebr grupowych.

3.2. Ciała charakterystyki $\neq$ q

Zgodnie z zauważonymi w rozdziale wprowadzającym związkami pomiędzy algebrami grupowymi a produktami tensorowymi, możemy napisać:

$$\mathbb{K}[G] \simeq \mathbb{K}[Q_1\langle u_1\rangle] \otimes_{\mathbb{K}} \mathbb{K}[Q_2\langle u_2\rangle], \tag{3.2a}$$

$$\mathbb{K}[H] \simeq \mathbb{K}[Q_2\langle u_1\rangle] \otimes_{\mathbb{K}} \mathbb{K}[Q_1\langle u_2\rangle]. \tag{3.2b}$$

Teza będzie udowodniona, jeśli pokażemy następujące izomorfizmy:

$$\mathbb{K}[Q_1\langle u_i\rangle] \simeq \mathbb{K}[Q_2\langle u_i\rangle], \quad i = 1, 2. \tag{3.3}$$

Pokażemy, że w istocie cała trudność dowodu leży w pokazaniu izomorficzności jeszcze skromniejszych struktur. Do tego jednak potrzeba nam skorzystać z założenia o charakterystyce ciała $\mathbb{K}$. Użyjmy twierdzenia 1.2.1. Rolę podgrup normalnych w $Q_j\langle u_i\rangle$, $i, j = 1, 2$, których rzędy nie są zerami w $\mathbb{K}$, odgrywają q - elementowe grupy $\langle z_j\rangle \triangleleft Q_j\langle u_i\rangle$. Elementy $e_j = \frac{1}{|\langle z_j\rangle|}\widehat{\langle z_j\rangle}$ są więc centralnymi idempotentami algebr grupowych $\mathbb{K}[Q_j\langle u_i\rangle]$. Zauważmy, że możemy algebry te rozłożyć na sumy proste pierścieni:

$$\mathbb{K}[Q_j\langle u_i\rangle] \simeq e_j\mathbb{K}[Q_j\langle u_i\rangle] \oplus (1 - e_j)\mathbb{K}[Q_j\langle u_i\rangle].$$

Istotnie, jeżeli $x \in e_j\mathbb{K}[Q_j\langle u_i\rangle] \cap (1 - e_j)\mathbb{K}[Q_j\langle u_i\rangle]$, to $e_jx = (1 - e_j)x = 0 \Rightarrow x = 0$. Korzystając z kolejnej części twierdzenia 1.1 mamy: $e_j\mathbb{K}[Q_j\langle u_i\rangle] \simeq \mathbb{K}[Q_j\langle u_i\rangle/\langle z_j\rangle]$. Na mocy lematu 2: $Q_1\langle u_i\rangle/\langle z_j\rangle \simeq Q_2\langle u_i\rangle/\langle z_j\rangle$. „Za darmo" zatem dostajemy izomorfizmy[4]:

$$e_1\mathbb{K}[Q_1\langle u_i\rangle] \simeq e_2\mathbb{K}[Q_2\langle u_i\rangle].$$

Ostatnia trudność w dowodzie twierdzenia Dade, leżeć będzie zatem w wykazaniu, że:

$$(1 - e_1)\mathbb{K}[Q_1\langle u_i\rangle] \simeq (1 - e_2)\mathbb{K}[Q_2\langle u_i\rangle].$$

Czeka nas sporo zabiegów technicznych, powiedzmy zatem jaki przyświeca nam cel. Chcemy pokazać, że istnieją $\mathbb{K}$ - izomorfizmy pomiędzy $(1-e_j)\mathbb{K}[Q_j\langle u_i\rangle]$, a macierzami $M_{q\times q}(S_j)$, gdzie S_1, S_2 to w tym momencie bliżej nieokreślone pierścienie. Tezę sprowadzimy w ten sposób do wykazania, że $S_1 \simeq S_2$. Dla większej przejrzystości dzielimy pozostałą część dowodu na trzy bloki:

- 3.2.1 Układy idempotentów,
- 3.2.2 $M_{q\times q}(S_j)$,
- 3.2.3 $S_1 \simeq S_2$.

3.2.1. Układy idempotentów

Podobnie jak w paragrafie 3.1 – także i w tym do przeprowadzenia dowodu potrzebować będziemy dwóch dość specyficznych układów idempotentów dających rozkład ortogonalny jedynek pierścieni $(1 - e_j)\mathbb{K}[Q_j\langle u_i\rangle]$ (elementów $1 - e_j$). Będą one jednak bardziej skomplikowane. Rozważmy podgrupy $\langle x_j, z_j\rangle \leqslant Q_j\langle u_i\rangle$. Dla $k = 0, 1, \ldots, q - 1$, kładziemy:

$$f_{jk} = \frac{1}{q} \cdot \widehat{\langle x_j z_j^k\rangle} \in \mathbb{K}[Q_j\langle u_i\rangle].$$

Zapowiadane układy ortogonalnych idempotentów stanowić będą elementy:

$$(1 - e_j)f_{jk} \in (1 - e_j)\mathbb{K}[Q_j\langle u_i\rangle].$$

[4]Są to oczywiście $\mathbb{K}$ - izomorfizmy pierścieni, wynika to z dowodu tw. 1.2.1.

Lemat 4. *Prawdziwe są następujące równości ($k = 0, 1, 2, \ldots q-1$).*

$$y_j^{-k}\left[(1-e_j)f_{j0}\right]y_j^k = (1-e_j)f_{jk}, \tag{3.4a}$$

$$(1-e_j)f_{jk}\cdot(1-e_j)f_{js} = \begin{cases} 0 & dla\ k \neq s, \\ (1-e_j)f_{jk} & dla\ k = s, \end{cases} \tag{3.4b}$$

$$1-e_j = \sum_{k=0}^{q-1}(1-e_j)f_{jk}. \tag{3.4c}$$

Dowód. Formuły (3.4a) wynikają z manipulacji równościami $[x_j, y_j] = z_j$. Korzystając z przemienności elementów y_j oraz z_j:

$$x_jy_jx_j^{-1}y_j^{-1} = z_j \Rightarrow y_j^{-1}x_jy_jx_j^{-1}y_j^{-1} = y_j^{-1}z_j = z_jy_j^{-1} \Rightarrow$$
$$y_j^{-1}x_jy_j = x_jz_j \Rightarrow y_j^{-k}x_jy_j^k = y_j^{-k+1}x_jy_j^{k-1}z_j = \ldots = x_jz_j^k.$$

Analogicznie pokazujemy równości $y_j^{-k}x_j^sy_j^k = x_j^sz_j^{sk}$, $s = 1, 2, \ldots q-1$. Dodając je stronami do jedynek, dostajemy:

$$1 + y_j^{-k}x_jy_j^k + \ldots + y_j^{-k}x_j^{q-1}y_j^k = 1 + x_jz_j^k + \ldots + x_j^{q-1}z_j^{(q-1)k} \Leftrightarrow y_j^{-k}\cdot f_{j0}\cdot y_j^k = f_{jk}.$$

Idempotenty $1-e_j$ są, podobnie jak e_j, centralne w $\mathbb{K}[Q_j\langle u_i\rangle]$. Stąd już wynikają wzory z (3.4a).

Kolejna formuła wynika prosto z (3.4a). Istotnie, korzystamy z tego, że $1-e_j$ są centralnymi idempotentami, więc:

$$(1-e_j)f_{jk}\cdot(1-e_j)f_{js} = (1-e_j)f_k\cdot f_s = (1-e_j)(y_j^{-k}f_{j0}y_j^k)(y_j^{-s}f_{j0}y_j^s) = (1-e_j)y_j^{-s}f_{j,k-s}\cdot f_{j0}y_j^s.$$

Dla $k = s$ wystarczy zauważyć, że $f_{j0} = \frac{1}{|\langle x_j\rangle|}\widehat{\langle x_j\rangle}$ jest idempotentem.[5] Wtedy:

$$f_{jk}^2 = (1-e_j)y_j^{-k}f_{j0}y_j^k = (1-e_j)f_{jk}.$$

Gdy $k - s = m \neq 0$ widzimy, że:

$$f_{j0}\cdot f_{jm} = \frac{1}{q^2}\left(1 + x_j + \cdot + x_j^{q-1}\right)\left(1 + x_jz_j^m + \ldots + x_j^{q-1}z_j^{(q-1)m}\right) =$$
$$= \begin{array}{ccccccc} 1 & + & x_jz_j^m & + & \ldots & + & x_j^{q-1}z_j^{(q-1)m} \\ z_j^{(q-1)m} & + & x_j & + & \ldots & + & x_j^{q-1}z_j^{(q-2)m} \\ z_j^{(q-2)m} & + & x_jz_j^{(q-1)m} & + & \ldots & + & x_j^{q-1}z_j^{(q-3)m} \\ \vdots & & \vdots & & \ddots & & \vdots \\ z_j^m & + & x_jz_j^m & + & \ldots & + & x_j^{q-1} \end{array} =$$
$$= \frac{1}{q^2}\cdot\widehat{\langle z^m\rangle}\cdot\widehat{\langle x_j\rangle} = e_j\cdot\frac{1}{q}\cdot\widehat{\langle x_j\rangle}.$$

Zatem skoro $(1-e_j)e_j = 0$, to dla $k \neq s$ istotnie:

$$(1-e_j)f_{jk}\cdot(1-e_j)f_{js} = (1-e_j)y_j^{-s}f_{j,k-s}\cdot f_{j0}y_j^s = (1-e_j)\cdot e_j\cdot y_j^{-s}1q\cdot\widehat{\langle x_j\rangle}y_j^s = 0.$$

Do dowodu pozostała formuła (3.4*c*). Sprawdzamy ją bezpośrednio:

$$\sum_{k=0}^{q-1}(1-e_j)f_{jk} = (1-e_j)\cdot\frac{1}{q^2}\cdot\sum_{k=0}^{q-1}x_j^k\widehat{\langle z_j^k\rangle} = (1-e_j)\cdot\frac{1}{q}\cdot\left(1 + e_j(\widehat{\langle x_j\rangle} - 1)\right) = (1-e_j).$$

□

[5] Łatwo to sprawdzić: $f_{j0}^2 = q^{-2}\cdot\sum_{k=0}^{q-1}(x_j^k + x_j^{k+1} + \ldots + x_j^{k+q-1}) = q^{-2}\cdot q\cdot(1 + x_j + \ldots + x_j^{q-1}) = f_{j0}$.

3.2.2. $M_{q\times q}(S_j)$

Skonstruowane w 3.2.1 układy idempotentów pozwalają na skorzystanie z faktu, który po krótkim komentarzu uzasadnimy:

Lemat 5. *Niech R będzie pierścieniem z jedynką i niech $1 = r_1 + r_2 + \ldots + r_n$ będzie rozkładem jedynki na sumę ortogonalnych idempotentów R Niech G będzie podgrupą R^*, która działa przez sprzężenia na zbiorze $E = \{r_1, r_2, \ldots, r_n\}$ poprzez tranzytywne permutowanie jego elementów. Wówczas $R \simeq M_{n\times n}(r_1 R r_1)$.*

Przetłumaczmy to na nasze potrzeby. Pierścień R to oczywiście jeden z: $(1-e_j)\mathbb{K}[Q_j\langle u_i\rangle]$. Idempotenty to $\{(1-e_j)f_{jk} \,|\, k = 0, 1, 2, \ldots q-1\}$. Uwagi wymaga dobór grup G. Dla $j = 1$ jest to q - elementowa grupa $(1-e_1)\langle y_1\rangle$. Jej elementy zgodnie z (3.4a) permutują tranzytywnie elementy E. Delikatność pojawia się dla $j = 2$. W tym przypadku rolę G odgrywa q - elementowa grupa $(1-e_2)(\langle y_2\rangle/\langle y_2^q\rangle)$ Skąd to rozróżnienie? Przede wszystkim potrzebujemy, by G miało rząd q, zaś $|(1-e_2)\langle y_2\rangle| = q^2$. Dla $m = 0, 1, \ldots, q^2-1$, klasy $(1-e_2)[y_2^m]$ elementów $(1-e_2)y_2^m$ grupy $(1-e_2)\langle y_2\rangle$, działają na $(1-e_j)f_{jk},\ k = 0, 1, \ldots, q-1$, tak samo jak działają elementy $(1-e_2)y_2^k$, przy czym oczywiście $m = k \,mod\, q$. Na mocy formuły $(3.4a)$ działanie to jest tranzytywne, a zatem spełnione są założenia lematu 5.

Aby przystąpić do dowodu, potrzebujemy poczynić pewne ogólne spostrzeżenie:

Uwaga. *Niech R będzie pierścieniem z 1, w którym istnieje podzbiór $E = \{r_{ij} \,|\, i, j = 1, 2, \ldots, n\}$, spełniający warunki:*

- $r_{ij}r_{ab} = \begin{cases} 0 & dla\ j \neq a, \\ r_{ib} & dla\ j = a. \end{cases}$
- $1 = r_{11} + r_{22} + \ldots + r_{nn}$.

Wówczas $R \simeq M_{n\times n}(r_{11} R r_{11})$.

Dowód. Określamy odwzorowanie $\sigma : R \to M_{n\times n}(r_{11}Rr_{11})$ postaci:

$$\sigma(s) = (r_{1i}sr_{j1})_{i,j=1}^n \in M_{n\times n}(r_{11}Rr_{11}).$$

Jest ono dobrze określone, bo $r_{1i}sr_{j1} = r_{11}(r_{1i}sr_{j1})r_{11} \in r_{11}Rr_{11}$. Jest to bijekcja. Istotnie, dla dowolnego elementu $s \in R$ zachodzi równość:

$$s = 1 \cdot s \cdot 1 = \left(\sum_{i=1}^n r_{ii}\right) s \left(\sum_{j=1}^n r_{jj}\right) = \sum_{i=1}^n \sum_{j=1}^n r_{ii}sr_{jj} = \sum_{i=1}^n \sum_{j=1}^n r_{1i}(r_{i1}sr_{j1})r_{1j},$$

zatem możemy określić przekształcenie odwrotne: $\sigma^{-1} : M_{n\times n}(r_{11}Rr_{11}) \to R$, postaci:

$$\sigma^{-1}((m_{ij})_{i,j=1}^n) = \sum_{i=1}^n \sum_{j=1}^n r_{i1}m_{ij}r_{1j}.$$

Pozostaje sprawdzić, że jest to homomorfizm pierścieni. Zachowywanie dodawania nie budzi wątpliwości. Wykażemy, że σ^{-1} zachowuje mnożenie. Ponieważ mamy już addytywność, wystarczy sprawdzić mnożenie na macierzach bazowych[6] $E_{ij}, E_{kl} \in M_{n\times n}(r_{11}Re_{11})$:

$$\sigma^{-1}(E_{ij}E_{kl}) = \sigma^{-1}(E_{ij})\sigma^{-1}(E_{kl}).$$

[6]Rozumiemy przez to macierze $(E_{ij})_{a,b=1}^n = \begin{cases} 1, & \text{dla } a = i, b = j, \\ 0, & \text{wpp.} \end{cases}$

Mamy:

$$\sigma^{-1}(E_{ij}E_{kl}) = \begin{cases} \sigma^{-1}(E_{il}), & \text{dla } j = k \\ 0, \text{dla } j \neq k \end{cases} = \begin{cases} r_{ij}, & \text{dla} j = k \\ 0, & \text{dla } j \neq k \end{cases},$$

$$\sigma^{-1}(E_{ij})\sigma^{-1}(E_{kl}) = \begin{cases} r_{ij}, & \text{dla} j = k \\ 0, & \text{dla } j \neq k \end{cases}.$$

□

W tej chwili mamy już otwartą drogę do wykazania lematu 5:

Dowód. Określmy więc dla każdego $i = 1, 2, \ldots, n$ element $g_i \in G$, że $g_i^{-1} r_1 g_i = r_i$ i połóżmy dla $i, j = 1, 2, \ldots, n$:

$$r_{ij} := g_i^{-1} r_1 g_j.$$

Elementy te spełniają założenia powyższej uwagi. Istotnie, $r_{ii} = r_i$, więc $\sum_i r_{ii} = 1$. Jeżeli dalej $j \neq a$, to $r_j \neq r_a$, a więc wobec ortogonalności: $r_j r_a = 0$. Zatem dla $j \neq a$:

$$r_{ij} r_{ab} = g_i^{-1} r_1 g_j \cdot g_a^{-1} r_1 g_b = g_i^{-1} g_j r_j \cdot r_a g_a^{-1} g_b = 0.$$

Na koniec, dla $j = a$ mamy:

$$r_{ij} r_{ab} = r_{ij} r_{jb} = g_i^{-1} r_1 g_j g_j^{-1} r_1 g_b = g_i^{-1} r_1 g_b = r_{ib}.$$

Wobec $r_{11} = r_1$, udowodniona wyżej uwaga zapewnia prawdziwość tezy lematu. □

Udowodniliśmy zatem, że dla $i, j = 1, 2$:

$$(1 - e_j)\mathbb{K}[Q_j\langle u_i\rangle] \simeq M_{q\times q}(S_j), \text{ gdzie } S_j = (1 - e_j)f_{j0} \cdot \mathbb{K}[Q_j\langle u_i\rangle] \cdot (1 - e_j)f_{j0}.$$

3.2.3. $S_1 \simeq S_2$

Zauważmy, że podgrupy $H_j := \langle x_j, z_j, u_i\rangle$ grup $Q_j\langle u_i\rangle$ mają w nich indeks q, zaś elementy $1, y_j, y_j^2, \ldots y_j^{q-1}$, tworzą prawy transwersal H_j w $Q_j\langle u_i\rangle$. Na mocy lematu 1.2.3:

$$\mathbb{K}[Q_j\langle u_i\rangle] = \bigoplus_{k=0}^{q-1} \mathbb{K}[Q_j\langle u_i\rangle] y_j^k.$$

Przypomnijmy sobie, zgodnie z formułą (2.1a), że element u_i działa trywialnie na elementach podgrupy $\langle x_j\rangle$. Jest on zatem przemienny z elementem $f_{j0} = \frac{1}{q} \cdot \widehat{\langle x_j\rangle}$. Stąd (pamiętając, że $(1 - e_j)$ to centralne idempotenty):

$$S_j = (1 - e_j)f_{j0} \cdot \mathbb{K}[Q_j\langle u_i\rangle] \cdot (1 - e_j)f_{j0} = \bigoplus_{k=0}^{q-1} \Big(\mathbb{K}[H_j] \cdot (1 - e_j)f_{j0} \cdot y_j^k \cdot (1 - e_j)f_{j0}\Big).$$

Korzystając z (3.4a) mamy jednak:

$$(1 - e_j)f_{j0} \cdot y_j^k \cdot (1 - e_j)f_{j0} = y_j^k \cdot y_j^{-k}[(1 - e_j)f_{j0}]y_j^k \cdot (1 - e_j)f_{j0} = y_j^k \cdot (1 - e_j)f_{jk} \cdot (1 - e_j)f_{j0}.$$

Ostatnie wyrażenie jest jednak równe 0 dla $k \neq 0$, a zatem z całej sumy prostej zostaje nam tylko jeden składnik:

$$S_j = \mathbb{K}[H_j](1 - e_j)f_{j0}.$$

To jest już koniec dowodu, ponieważ $(1 - e_1)f_{10} = (1 - e_2)f_{20}$, zaś grupy H_1 oraz H_2 są w oczywisty sposób izomorficzne.

* * *

W ten sposób zakończyliśmy dowód twierdzenia Dade w przypadku ciał charakterystyki różnej od q. Ostatecznie więc skompletowaliśmy już cały dowód. Warto w tym miejscu wspomnieć, że grupy $G(p,q), H(p,q)$ nie są kontrprzykładami dla ogólnego problemu izomorfizmu[7], innymi słowy $\mathbb{Z}[G(p,q)] \not\cong \mathbb{Z}[H(p,q)]$. Jeszcze przed publikacją omawianego w tej pracy twierdzenia w rozprawie doktorskiej A. Whitcomba [Whi68] pojawia się następujący rezultat:

Twierdzenie (Whitcomb, 1968)**.** *Jeżeli skończone grupy metabelowe G, H są nieizomorficzne, to ich pierścienie grupowe nad* $\mathbb{Z}$ *również.*

Już w rozdziale 2. pokazaliśmy, że komutanty grup Dade są abelowe, stąd nie mogą stanowić kontrprzykładu do problemu izomorfizmu pierścieni grupowych nad $\mathbb{Z}$.

[7]Sam Dade stwierdza to już na początku swojego artykułu [Dad70], przytaczamy niżej użyty przezeń argument.

Rozdział 4

Czy nie ma prostszych kontrprzykładów?

Dowód twierdzenia Dade to zręczna kombinacja metod algebraicznych i „idealnie" dobrane pary grup $G(p,q), H(p,q)$. Fakt uzyskania kontrprzykładu wydaje się nie dostarczać żadnej istotnie ogólnej informacji na temat samego problemu. W większości komentarzy pojawiających się w literaturze panuje dość zgodny pogląd oceniający wynik Dade jako „zaskakująco prosty". Być może to właśnie podejście spowodowało, że już od prawie 40 lat udoskonalanie czy też poszukiwanie innych dróg do zrozumienia problemu izomorfizmu algebr grupowych nad dowolnym ciałem właściwie nie ma miejsca. W tym krótkim rozdziale zamykającym pracę chcielibyśmy wspomnieć o kilku ciekawych wynikach dotyczących izomorfizmów algebr grupowych nad konkretnymi ciałami. Pozwalają one w pewien sposób dostrzec na ile trudno może być poprawić omówione przez nas twierdzenie.

Można zadać sobie pytanie: w jakim sensie uzyskany przez Dade kontrprzykład jest „prosty"? Na pewno zasadniczym kryterium do takich ocen była metabelowość rozważanych grup, a więc 2. stopień rozwiązalności. Już od 1950 roku wiadomo było, że kontrprzykład nie może pochodzić od grup abelowych. Pomimo bowiem uwag poczynionych dla tychże grup na początku rozdziału 3., prawdziwe jest następujące twierdzenie:

Twierdzenie (Perris, Walker (1950))**.** *Jeżeli G, H są skończonymi grupami abelowymi, wówczas* $\mathbb{Q}[G] \simeq \mathbb{Q}[H] \Rightarrow G \simeq H$.

Kryterium „prostoty" nie jest raczej rząd uzyskanych grup. Najmniejsza para (p,q), spełniająca kongruencję $q = 1 \mod p^2$ to $(2,5)$. Grupy $G(2,5), H(2,5)$ mają rząd 125000 (ogólniej, grupa G(p,q) ma rząd p^3q^6).

Można dalej zapytać: skoro dowód jest tak prosty, to gdzie leżała trudność w jego odnalezieniu? Problemem były ciała charakterystyki dzielącej rząd ewentualnego kontrprzykładu i to właśnie stało się główną przyczyną wprowadzenia kongruencji $q = 1 \mod p^2$ w konstrukcję, którą przeprowadzaliśmy. Dlaczego właśnie ciała charakterystyki dzielącej rząd grupy? Za przynajmniej częściowe wyjaśnienie wystarcza następujące twierdzenie, uzyskane przez Passmana na kilka lat przed wynikiem Dade:

Twierdzenie (Passman (1965))**.** *Niech G, H będą grupami skończonymi. Załóżmy, że* $\mathbb{Q}[G] \simeq \mathbb{Q}[H]$. *Wówczas dla wszystkich ciał* $\mathbb{K}$, *których charakterystyka nie dzieli liczby* $|G| = |H|$ *zachodzi izomorfizm* $\mathbb{K}[G] \simeq \mathbb{K}[H]$.

Wreszcie, ostatnie pytanie jakie warto zadać brzmi: czy istnieją kontrprzykłady niższego (niż 125000) rzędu? Nie znamy odpowiedzi na to pytanie. Warto jednak wspomnieć na koniec o kilku interesujących rezultatach dotyczących tej materii.

- grupy abelowe

  Wiemy, że grupy abelowe nie są kontrprzykładem do problemu izomorfizmu, z powodu twierdzenia Perrisa - Walkera. Pozwala nam to odrzucić z rozważań wszystkie grupy rzędu p, gdzie p jest liczbą pierwszą. Przy pomocy komputera można sprawdzić, że jest to ok. 1/10 wszystkich możliwych przypadków.

- p - grupy

  Twierdzenie (Passman (1965)). *Jeżeli dla ustalonego p - pierwszego rozważymy p - grupy G, H, dla których* $|G| = |H| \leqslant p^4$ *oraz ciało* $\mathbb{K}$ *charakterystyki p, to* $\mathbb{K}[G] \simeq \mathbb{K}[H] \Rightarrow G \simeq H$.

  Powyższe twierdzenie zostało w latach 80. i 90. poprawione tak, że dołączono do niego grupy rzędu p^5 (wyniki Kovacsa i Newmana z ok. 1989 r. oraz Salima i Sandberga w 1996 r.). Łatwo widzieć, że wyniki te pozwalają nam wykluczyć z rozważań wszystkie p - grupy przy $p \geqslant 11$, ponieważ dla nich $p^5 \geqslant 125000$. Dodatkowo wiemy (wyniki komputerowe Wursthorna z 1994 i 1997 roku, później zaś dowód Hertwecka i Soriano z 2005), że twierdzenie to jest prawdziwe dla 2 - grup rzędu nie większego niż 2^7.

- grupy rzędu 2p, 4p, 8p – dla p pierwszego, nieparzystego

  Twierdzenie (Sirajul (1975)). *Niech p będzie liczbą pierwszą nieparzystą. Wówczas dowolne dwie nieizomorficzne grupy rzędu 8p mają nieizomorficzne algebry grupowe nad pewnym ciałem algebraicznie domkniętym charakterystyki 2.*

  Twierdzenie to można znaleźć w [Sir75]. Znajdziemy tam również proste wyjaśnienie analogicznego faktu dla grup rzędu 2p i 4p. Jeżeli chodzi o przypadek 4p, można powiedzieć nawet więcej. W 1970 roku Jeyakumar udowodnił w [Jey70] następujące:

  Twierdzenie (Jeyakumar (1970)). *Dla nieizomorficznych grup dihedralnych lub dicyklycznych G, H rzędu 4p, gdzie* $p = q^r$, *q - pierwsze,* $r \in \mathbb{N}$, *istnieje ciało* $\mathbb{K}$ *algebraicznie domknięte charakterystyki 2 takie, że* $\mathbb{K}[G] \not\simeq \mathbb{K}[H]$.

  Najnowsze wyniki pochodzą, jak widać, od grupy zagadnień związanych z p - grupami. Nie jest to przypadek. Do dziś nierozwiązany jest tzw. modularny problem izomorfizmu: czy skończone nieizomorficzne p - grupy G, H mają nieizomorficzne algebry grupowe nad ciałem $\mathbb{Z}_p$? Zagadnienie to jest przedmiotem intensywnych badań prowadzonych współcześnie właściwie na całym świecie. Zaangażowani są w nie także polscy matematycy na czele z dr Czesławem Bagińskim z Białegostoku. Ważną rolę w tych badaniach odgrywają także metody komputerowe (w ramach GAP). Istnieje szereg ogólnej natury rezultatów, które uzyskano w ciągu przeszło 50 lat istnienia modularnego problemu izomorfizmu. Ich pełen przegląd można odnaleźć np. w [Kon05].

Bibliografia

[Dad70] DADE E., *Deux groupes finis distincts ayant la même algèbre de groupe sur tout corps*, Math. Z. 119 (1971), 345 – 348.

[Her01] HERTWECK M., *A counterexample to the isomorphism problem for integral group rings*, Ann. of Math., Volume 154, Number 1 (2001), 115 – 138.

[Hig40] HIGMAN G., *Units in group rings*, Oxford (1940).

[Jey70] JEYAKUMAR V. A, *Group Algebras of Dihedral and Dicyclic Groups Over Modular Fields*, J. London Math. Soc. (1970), 297 – 304.

[Kon05] KONOVALOV A., *On the Modular Isomorphism Problem of Group Algebras*, International Conference 'Groups St. Andrews 2005', dostępny online: http://ukrgap.exponenta.ru/papers/GSTA_05.pdf.

[Pas65a] PASSMAN D.S., *Isomorphic groups and group rings*, Pacific J. Math., 14 (1965), 561 – 583.

[Pas77] PASSMAN D.S., *The Algebraic Structure of Group Rings*, Wiley-Interscience, Nowy Jork (1977).

[Pas65b] PASSMAN D.S., *The group algebras of groups of order p^4 over a modular field*, Michigan Math. J., 12 (1965), 405 – 415.

[PW50] PERRIS S., WALKER G.L., *Abelian Group Algebras of Finite Order*, Trans. Amer. Math. Soc. 68 (1950), 420 – 426.

[Ser88] SERRE J., *Reprezentacje liniowe grup skończonych*, PWN, Warszawa (1988).

[Sir75] SIRAJUL H.M., *On the Isomorphism of Group Algebras of Groups of Order 8Q*, J. London Math. Soc. (1975), 549 – 556.

[Whi68] WHITCOMB A., *The group ring problem*, Chicago (1968).