ROCZNIKI POLSKIEGO TOWARZYSTWA MATEMATYCZNEGO
Seria II: WIADOMOŚCI MATEMATYCZNE XXVIII (1990)

wmptm 1897

Ministerstwo Nauki i Szkolnictwa Wyższego

JAN KREMPA i ZBIGNIEW MARCINIAK (Warszawa)

Pierścienie grupowe*

Każda grupa nosi w sobie zalążek pierścienia łącznego z jedynką. Aby go opisać dla danej grupy G, należy najpierw wybrać współczynniki; niech to będą np. liczby zespolone. Nasz pierścień będzie się więc składał ze wszystkich skończonych sum formalnych postaci

$$a = a(g_1)g_1 + \ldots + a(g_n)g_n,$$

gdzie g_i są elementami grupy G, a $a(g_i)$ są liczbami zespolonymi. Napisy te dodajemy *po współrzędnych*:

$$\sum_g a(g)g + \sum_g b(g)g = \sum_g \big(a(g)+b(g)\big)g.$$

Mnożenie odbywa się w sposób równie naturalny: otwieramy nawiasy, a jednomiany $a(g)g$, $b(h)h$ mnożymy według wzoru

$$\big(a(g)g\big)\cdot\big(b(h)h\big) = \big(a(g)\,b(h)\big)(gh).$$

Tak otrzymany pierścień nazywamy *pierścieniem grupowym* grupy G o współczynnikach z ciała $\boldsymbol{C}$ i oznaczamy przez $\boldsymbol{C}[G]$ lub $\boldsymbol{C}G$.

Elementy pierścienia $\boldsymbol{C}[G]$ można również interpretować jako funkcje $a\colon G \to \boldsymbol{C}$ o skończonych nośnikach $\{g|\ a(g) \neq 0\}$. Zgodnie z przyjętymi definicjami, należy je dodawać „po wartościach", natomiast mnożyć – używając znanej z analizy operacji splotu

$$(a\cdot b)(g) = \sum_{h\in G} a(gh^{-1})\,b(h).$$

Z tego powodu algebry grupowe nad $\boldsymbol{C}$ odgrywają ważną rolę w analizie harmonicznej.

Oto dwa najprostsze przykłady pierścieni grupowych. Niech

$$C_2 = \langle t|\ t^2 = 1\rangle = \{1, t\}$$

---

* Odczyt wygłoszony w 1986 roku na Konwersatorium w Instytucie Matematyki Uniwersytetu Warszawskiego.

oznacza grupę cykliczną rzędu 2. Mamy wówczas

$$C[C_2] = \{a+bt \mid a, b \in C\} \cong C \oplus C$$

z mnożeniem

$$(a+bt)(c+dt) = (ac+bd)+(ad+bc)t.$$

Dla grupy cyklicznej nieskończonej $C_\infty = \langle t \rangle$ otrzymujemy

$$C[C_\infty] = \{\sum_{i=n}^{m} a_i t^i \mid a_i \in C,\ n, m \in Z\}.$$

Elementy tego pierścienia mnożymy dokładnie tak, jak się mnoży wielomiany. Otrzymaliśmy zatem pierścień wielomianów Laurenta

$$C[t, t^{-1}].$$

Łatwo zauważyć, że pierścień grupowy jest przemienny tylko wtedy, gdy grupa G, od której zaczynaliśmy, jest przemienna.

Zamiast liczb zespolonych możemy użyć liczb rzeczywistych, wymiernych, ciała reszt modulo p lub ogólniej, dowolnego pierścienia przemiennego z jedynką. Jak się okaże dalej, szczególnie pożyteczne jest rozważanie pierścienia grupowego $Z[G]$ o współczynnikach całkowitych.

Co zyskujemy zamieniając grupę na jej pierścień grupowy? Dysponując pierścieniem, możemy podjąć próbę kopiowania metod algebry liniowej. Naśladując definicję przestrzeni liniowej, możemy rozważyć grupę abelową V wraz z mnożeniem przez skalary należące do dowolnego pierścienia R. Tak otrzymujemy *R-moduły*. Na przykład, dla $R = C[C_2]$ możemy w grupie abelowej C wprowadzić mnożenie przez skalary wzorem

$$(a+bt)z = (a+b)z$$

albo wzorem

$$(a+bt)z = (a-b)z.$$

Otrzymane $C[C_2]$-moduły oznaczmy odpowiednio przez V i W.

Niektóre twierdzenia o przestrzeniach liniowych dają się uogólnić do twierdzeń o R-modułach. Na przykład znane stwierdzenie: *każda skończenie generowana przestrzeń liniowa nad ciałem K jest postaci* $K \oplus \ldots \oplus K$ ma następujący odpowiednik dla pierścienia $C[C_2]$: *każdy skończenie generowany* $C[C_2]$*-moduł jest postaci* $V \oplus \ldots \oplus V \oplus W \oplus \ldots \oplus W$. Tutaj V, W są modułami zdefiniowanymi w poprzednim akapicie. Jest to bardzo szczególny przypadek twierdzenia Maschke [17], [18], które pozwala klasyfikować CG-moduły dla dowolnej grupy skończonej G.

Dla pierścienia grupowego $C[C_\infty]$ grupy cyklicznej nieskończonej również potrafimy opisać jego moduły. Zauważyliśmy wcześniej, że $C[C_\infty] = C[t, t^{-1}]$, czyli jest to przemienna dziedzina ideałów głównych. Skończenie generowane moduły takich pierścieni są dobrze znane [6].

Problem opisu CG-modułów dla dowolnej grupy nieskończonej G jest trudny i wciąż daleki od rozwiązania.

Dlaczego usiłujemy zbadać moduły nad pierścieniami grupowymi? Odpowiedzią niech będzie opis kilku sytuacji, w których pojawiają się one w sposób naturalny.

(A) Rozważmy parę izometrii płaszczyzny euklidesowej:

$$S, T\colon \boldsymbol{R}^2 \to \boldsymbol{R}^2,$$

$$S(x, y) = (x, y+1), \quad T(x, y) = (x+1, -y).$$

Niech Γ będzie grupą izometrii płaszczyzny, generowaną przez S i T. Grupa Γ jest przykładem grupy *krystalograficznej*. W szczególności działa ona na płaszczyźnie, dając butelkę Kleina jako przestrzeń orbit. Podgrupa translacji $\Gamma_0 = \langle S, T^2\rangle$, izomorficzna z $\boldsymbol{Z} \oplus \boldsymbol{Z}$, jest podgrupą o indeksie dwa w Γ. Grupa Γ działa na Γ_0 przez automorfizmy wewnętrzne. Działanie to faktoryzuje się do działania grupy $C_2 = \Gamma/\Gamma_0$. Jego przedłużenie liniowe zadaje na Γ_0 strukturę $\boldsymbol{Z}[C_2]$-modułu. Moduł ten zawiera istotne informacje o strukturze grupy Γ. Łatwo się przekonać, że jest on izomorficzny z $V_{\boldsymbol{Z}} \oplus W_{\boldsymbol{Z}}$, gdzie $V_{\boldsymbol{Z}}, W_{\boldsymbol{Z}}$ są „$\boldsymbol{Z}$-wersjami" modułów V, W zdefiniowanych wcześniej dla pierścienia $\boldsymbol{C}[C_2]$.

Ogólniej, jeśli grupa G ma abelowy dzielnik normalny A, to A można traktować jak $\boldsymbol{Z}[G/A]$-moduł. Studiowanie własności tych modułów oraz ich związku ze strukturą grupy G zapoczątkował P. Hall. Używając tej metody, matematycy brytyjscy uzyskali w latach siedemdziesiątych istotne informacje o strukturze grup policyklicznych [25]. Wśród nich znajdują się wszystkie grupy krystalograficzne [12].

(B) Załóżmy, że grupa G działa liniowo na n-wymiarowej przestrzeni liniowej V nad ciałem K, tzn. mamy dany homomorfizm grup (reprezentację)

$$\varrho\colon G \to GL_n(K).$$

Wtedy V możemy wyposażyć w strukturę $K[G]$-modułu, określając mnożenie przez skalary wzorem

$$\Big(\sum a(g)\,g\Big)\cdot v = \sum a(g)\,\varrho(g)\,v \in V.$$

E. Noether pierwsza zauważyła, że potraktowanie reprezentacji jak $K[G]$-modułów dostarcza nowych technik do ich badania. Są one szczególnie skuteczne w przypadku, gdy G jest grupą skończoną, a K jest ciałem o dodatniej charakterystyce [11].

(C) Jak dla każdego pierścienia, tak i dla $R = K[G]$ możemy badać ciągi dokładne R-modułów oraz ich niedokładność po zastosowaniu różnych funktorów. Droga ta prowadzi do działu algebry homologicznej, zwanego *teorią (ko)homologii grup* o współczynnikach w $K[G]$-modułach. Jest to jeden ze sposobów zdobywania informacji o grupie G oraz o pewnych przestrzeniach topologicznych z nią związanych [4], [7].

(D) Jeśli $K \subseteq L$ jest rozszerzeniem Galois ciał, to dla grupy K-automorfizmów $G = \mathrm{Gal}(L/K)$ grupa addytywna L oraz grupa multyplikatywna $L^* = L - \{0\}$ stają się $\boldsymbol{Z}[G]$-modułami. W szczególności można zastosować technikę przykładu (C) do tych modułów, aby uzyskać informacje o samym rozszerzeniu. Przykładem twierdzenia tego rodzaju jest tzw. *90 Twierdzenie Hilberta* [4].

(E) Jeśli grupa G działa na przestrzeni topologicznej X poprzez homeomorfizmy, to grupy łańcuchów (singularnych, komórkowych, ...) stają się w naturalny sposób $\boldsymbol{Z}G$-modułami. Ponadto działanie grupy G jest przemienne z operatorami brzegu; w konsekwencji grupy homologii $H_*(X)$ przestrzeni X są także $\boldsymbol{Z}G$-modułami. Badanie tych modułów jest źródłem informacji o działaniu grupy G na X. W ten sposób można na przykład udowodnić, że grupa skończona nie może działać w sposób wolny na przestrzeni $\boldsymbol{R}^n$ [5].

Z powyższych przykładów wynika, że badanie modułów nad pierścieniami grupowymi jest ważnym zadaniem. Jednakże pierścienie grupowe manifestują się w zastosowaniach nie tylko poprzez swe moduły.

Rozważmy kompleks komórkowy X wraz z homotopijnie mu równoważnym podkompleksem A. Kiedy próbujemy w kontrolowany sposób „zgniatać" X na A, komórka po komórce, pojawia się tzw. *torsja Whiteheada* — element grupy abelowej $\mathrm{Wh}(G)$, gdzie $G = \pi_1(X)$ [10]. Grupa $\mathrm{Wh}(G)$ może być opisana w terminach pierścienia $\boldsymbol{Z}G$ jak następuje: niech (dla $n \geqslant 1$) $GL_n(\boldsymbol{Z}G)$ oznacza grupę macierzy odwracalnych stopnia n, o współczynnikach z pierścienia $\boldsymbol{Z}G$. Mamy zanurzenia

$$GL_n(\boldsymbol{Z}G) \to GL_{n+1}(\boldsymbol{Z}G)$$

dane przez

$$A \mapsto \begin{bmatrix} A & 0 \\ 0 & 1 \end{bmatrix}.$$

Niech $GL(\boldsymbol{Z}G) = \bigcup_n GL_n(\boldsymbol{Z}G)$. Aby otrzymać $\mathrm{Wh}(G)$, należy podzielić grupę $GL(\boldsymbol{Z}G)$ najpierw przez jej komutant, a następnie przez obraz grupy $\pm G \subseteq GL_1(\boldsymbol{Z}G) \subseteq GL(\boldsymbol{Z}G)$.

Zrozumienie grupy $\mathrm{Wh}(G)$ ma kluczowe znaczenie dla rozwiązania wielu problemów topologii rozmaitości. My zacznijmy skromnie: od $GL_1(\boldsymbol{Z}G)$. Z definicji, $GL_1(\boldsymbol{Z}G)$ składa się z elementów odwracalnych, albo krócej, jedności pierścienia $\boldsymbol{Z}G$. Oczywiście są wśród nich elementy postaci $\pm g$ dla $g \in G$. Te jedności nazywamy *trywialnymi*.

Czy istnieją jakieś inne jedności w $\boldsymbol{Z}G$? Odpowiedź jest z reguły twierdząca. A oto sposób na uzyskanie przykładów.

Przypuśćmy, że nasza grupa G ma podgrupę cykliczną $H = \langle h \rangle$ rzędu n, która nie jest dzielnikiem normalnym w G. Istnieje zatem element $g \in G$ taki, że

$gHg^{-1} \neq H$. Rozważmy element

$$n = (1-h)g(1+h+\ldots+h^{n-1}) \in ZG.$$

Z założenia o elemencie g wynika, że po otwarciu nawiasów nie wszystko się poskraca, tzn. $n \neq 0$. Z drugiej strony

$$n^2 = (1-h)g(1+\ldots+h^{n-1})\,(1-h)g(1+\ldots+h^{n-1}) = 0,$$

bo $(1+h+\ldots+h^{n-1})\,(1-h) = 1-h^n = 0$. Elementy $u = 1+n$, $v = 1-n \in ZG$ spełniają warunek $uv = vu = 1$, są więc nietrywialnymi jednościami w ZG.

Żeby stwierdzić, że pewien element $a \in ZG$ jest jednością, należy znaleźć element $b \in ZG$ taki, że $ab = 1$ oraz $ba = 1$. Czy nie wystarczy połowa sprawdzenia, tj. czy z $ab = 1$ nie wynika czasem, że $ba = 1$?

Zauważmy, że pytanie to ma sens w dowolnym pierścieniu. Odpowiedź jest oczywiście twierdząca w pierścieniach przemiennych. Pierścień macierzy $M_n(K)$ stopnia $n \geqslant 2$, o współczynnikach z ustalonego ciała K nie jest przemienny, ale odpowiedź dla niego jest także twierdząca: jeśli $ab = 1$, to $\det(a) \neq 0$, a więc a ma też lewą odwrotność. Z drugiej strony łatwo jest podać przykład negatywny w pierścieniu endomorfizmów dowolnej nieskończenie wymiarowej przestrzeni liniowej. Np. jeśli L, R oznaczają odpowiednio przesunięcia w lewo i prawo przestrzeni Hilberta l^2, to mamy $LR = \mathrm{id}$, ale $RL \neq \mathrm{id}$.

Jaka jest odpowiedź dla pierścieni grupowych? Problem ten postawił G. Higman w 1940 roku w swojej pracy doktorskiej, pisanej pod kierunkiem Whiteheada. Przypuśćmy, że $ab = 1$ dla pewnych elementów $a, b \in ZG$. Interesuje nas $e = ba$. Mamy

$$e^2 = (ba)\,(ba) = b(ab)a = ba = e.$$

Elementy e pierścienia R, spełniające warunek: $e^2 = e$, nazywamy *idempotentami*. Oczywiście 0 i 1 są idempotentami w dowolnym pierścieniu. Są to tzw. *idempotenty trywialne*. Idempotenty są bardzo ważne, gdyż np. pozwalają rozkładać pierścień na sumę prostą: jeśli mamy $e = e^2 \in R$, to uzyskujemy rozkład

$$R = Re \oplus R(1-e)$$

pierścienia R na sumę prostą jego (lewostronnych) ideałów.

Zajmiemy się zbadaniem idempotentów w CG. Skąd je brać? Jeśli G ma podgrupę skończoną H, to element

$$e = (1/|H|)\Big(\sum_{h \in H} h\Big) \in CG$$

jest, jak łatwo sprawdzić, idempotentem. Ponadto, jeśli $e \in CG$ jest idempotentem, a element $u \in CG$ jest odwracalny, to sprzężenie $ueu^{-1} \in CG$ jest znów idempotentem.

Aby znaleźć właściwe narzędzie do badania idempotentów, przyjrzyjmy się pierścieniowi macierzy $M_n(C)$. Każda macierz idempotentna $E = E^2 \in M_n(C)$

jest sprzężona z macierzą postaci

$$\begin{bmatrix} 1 & 0 & 0 \\ & \ddots & \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix},$$

a zatem klasę sprzężoności E opisuje w pełni jedna liczba: jej ślad $\mathrm{Tr}(E)$.

Jeśli mamy do czynienia z grupą skończoną G rzędu n, to reprezentacja regularna daje zanurzenie pierścieni

$$\varrho\colon CG \to M_n(C);$$

jak łatwo wykazać, zachodzi wówczas wzór

$$\mathrm{Tr}\,\varrho(a) = a(1)|G| \quad \text{dla } a = \sum a(g)g.$$

Aby zbadać idempotent $e \in CG$, trzeba więc zająć się liczbą $e(1)|G|$.

Jeśli grupa G jest nieskończona, to powyższy napis nie ma sensu, więc musimy zadowolić się liczbą $\mathrm{tr}(e) = e(1)$. Następująca lista to spis oczywistych własności funkcji tr: $CG \to C$, $\mathrm{tr}\,(a) = a(1)$.

(i) tr jest C-liniowa,

(ii) $\mathrm{tr}\,(ab) = \mathrm{tr}\,(ba)$.

Niech $*\colon CG \to CG$ będzie dane wzorem

$$\Big(\sum a(g)g\Big)^* = \sum \overline{a(g)}\,g^{-1}.$$

Wtedy $\mathrm{tr}\,(aa^*) = \sum |a(g)|^2$. Wobec tego

(iii) $\mathrm{tr}\,(aa^*) = 0$ pociąga $a = 0$.

Okazuje się, że te własności wystarczają, by rozwiązać problem Higmana. Oto główne twierdzenie.

TWIERDZENIE (Kaplansky, Zaleskiĭ). *Jeśli $e \in CG$ jest idempotentem, to*

(a) $\mathrm{tr}\,(e)$ *jest liczbą wymierną,*

(b) $0 \leqslant \mathrm{tr}\,(e) \leqslant 1$,

(c) $\mathrm{tr}\,(e) = 0 \Rightarrow e = 0$, $\mathrm{tr}\,(e) = 1 \Rightarrow e = 1$.

Przytoczymy szkic dowodu części (b) i (c). Jedyny znany dziś sposób udowodnienia tego twierdzenia używa analizy matematycznej w sposób następujący:

Pierścień CG można wyposażyć w iloczyn hermitowski:

$$\langle a, b\rangle = \sum_g a(g)\overline{b(g)}.$$

Po uzupełnieniu otrzymamy przestrzeń Hilberta H, zawierającą CG jako pod-

zbiór gęsty. Dla każdego $a \in CG$ mnożenie przez a z lewej strony zadaje operator ograniczony $L_a \in B(H)$. Niech A będzie domknięciem zbioru $\{L_a \mid a \in CG\}$ w normie operatorowej. Funkcjonał tr: $CG \to C$ można bez trudu przedłużyć na A z zachowaniem własności (i)–(iii). Jeśli e jest idempotentem w CG, to w algebrze A jest już dość miejsca na to, by sprzęgnąć L_e z projekcją:

$$L_e \sim P, \quad P = PP^*.$$

Wtedy

$$\operatorname{tr}(e) = \operatorname{tr}(L_e) = \operatorname{tr}(P) = \operatorname{tr}(PP^*) \geqslant 0.$$

Ponadto jeśli $\operatorname{tr}(e) = 0$, to $\operatorname{tr}(PP^*) = 0$, a zatem $P = 0$ i $e = 0$. Jeśli natomiast $\operatorname{tr}(e) = 1$, to $\operatorname{tr}(f) = 0$, gdzie $f = 1 - e$ jest nowym idempotentem. Stąd $f = 0$, a więc $e = 1$. Szczegóły dowodu można znaleźć w książce [23].

Nie znamy czysto algebraicznego dowodu części (b) i (c) twierdzenia. Natomiast dowód części (a) używa wyłącznie argumentów z teorii liczb. Zauważmy jednak, że wszystkie części twierdzenia są oczywiste, gdy grupa G jest skończona. Istotnie, wtedy

$$\operatorname{tr}(e) = \dim((CG)e)/|G|$$

jest liczbą wymierną, która znika dokładnie wtedy, gdy $e = 0$. Sprawa jest równie prosta dla grup nieskończonych, jeśli tylko rozważany idempotent może być sprzężony z elementem leżącym w pierścieniu grupowym pewnej skończonej podgrupy. Do niedawna wszystkie znane idempotenty dopuszczały takie sprzężenia. Co więcej, panowało wśród specjalistów przekonanie, że takie sprzężenie jest zapewne zawsze możliwe: cóż bowiem mógłby oznaczać licznik i mianownik ułamka $\operatorname{tr}(e)$? Dopiero w 1982 roku udało się [13] wskazać idempotent, który nie jest sprzężony z żadnym elementem pochodzącym od podgrupy skończonej. Stawia to twierdzenie Kaplanskiego–Zaleskiego w nowym świetle.

Możemy teraz łatwo rozwiązać problem Higmana. Niech $a, b \in ZG$ będą elementami spełniającymi warunek $ab = 1$. Zauważyliśmy już, że $e = ba$ jest idempotentem. Ponadto

$$\operatorname{tr}(e) = \operatorname{tr}(ba) = \operatorname{tr}(ab) = 1.$$

Stąd $ba = 1$. Ten sam dowód działa dla pierścieni grupowych o współczynnikach z dowolnego ciała o charakterystyce zero. Natomiast dla ciał o charakterystykach dodatnich pytanie Higmana pozostaje otwarte.

Pytanie podobne do problemu Higmana pojawiło się w 1954 roku w pracy Cockcrofta [9]. Próbował on udowodnić słynną hipotezę Whiteheada, która mówi, że podkompleks dwuwymiarowego, asferycznego CW-kompleksu jest też asferyczny. Jeśli L jest kontrprzykładem i jego grupa podstawowa G jest wolna, to łatwy argument topologiczny pokazuje, że

$$\pi_2(L) \neq 0 \quad \text{oraz} \quad \pi_2(L) \oplus ZG^n = ZG^n$$

dla pewnej liczby n. Ostatnia równość jest równoważna istnieniu macierzy $X, Y \in M_n(ZG)$ spełniających równości: $XY = I$, $YX \neq I$. Cockcroft udowodnił, że to się nie może zdarzyć, gdy G jest grupą wolną, i pytał, czy inne pierścienie grupowe mają podobną własność.

Wzorując się na już rozstrzygniętym przypadku $n = 1$, tworzymy macierz idempotentną $E = YX \in M_n(ZG)$. Dla dowolnego pierścienia współczynników k macierz spełniająca warunek $E = E^2 \in M_n(kG)$ daje rozkład modułu wolnego $(k[G])^n$ na sumę prostą jego podmodułów $P = \text{im } E$, $Q = \text{im } (I - E)$. Moduły, które są składnikami prostymi modułów wolnych, są znane jako moduły *projektywne*. Są one podstawowymi cegiełkami w algebrze homologicznej [4].

Co wiemy o kG-modułach projektywnych? Zajmijmy się najpierw przypadkiem współczynników wymiernych: $k = Q$. Oczywiście każdy QG-moduł wolny jest projektywny. Widzieliśmy też wcześniej, że jeśli grupa G ma podgrupę skończoną, to pierścień QG ma nietrywialny element idempotentny e, a więc ma też moduł projektywny QGe, który nie jest wolny. Jeśli grupa G jest beztorsyjna, to nie mamy oczywistych kandydatów na QG-moduły projektywne, które nie są wolne. W 1976 roku Quillen i Suslin udowodnili niezależnie hipotezę Serre'a, która w szczególności mówi, że każdy moduł projektywny nad pierścieniem wielomianów $Q[x_1, \ldots, x_n]$ jest wolny. Wykorzystując ten wynik nietrudno jest [20] otrzymać podobny wynik dla QG, gdy G jest skończenie generowaną, wolną grupą abelową. Niezależnie można udowodnić podobne twierdzenie dla grupy wolnej nieabelowej.

W roku 1980 Lewin [21] oraz Artamonow [1] podali pierwsze przykłady QG-modułów projektywnych, które nie są wolne, dla pewnych grup beztorsyjnych G. Ich przykłady P spełniają warunek

$$P \oplus QG = QG \oplus QG,$$

a więc są *stabilnie wolne*.

Lewin podał też przykład ZG-modułu projektywnego, który nie jest wolny. W jego przykładzie G jest grupą krystalograficzną Γ z przykładu (A).

ZG-moduły projektywne są szczególnie interesujące ze względu na ich zastosowania w topologii: za ich pomocą można np. mierzyć przeszkodę do tego, by dla danego CW-kompleksu istniał równoważny mu homotopijnie CW-kompleks skończony [29]. To i podobne zastosowania zapoczątkowały rozwój *algebraicznej K-teorii*. W teorii tej moduły stabilnie wolne grają rolę obiektów trywialnych. Obecnie nie jest znany ani jeden przykład grupy beztorsyjnej G takiej, by pewien ZG-moduł (lub nawet QG-moduł) był projektywny, lecz nie stabilnie wolny. Farrell i Hsiang [15] udowodnili w 1977 roku, że znalezienie takiego przykładu nie jest możliwe wśród grup krystalograficznych.

Jak zauważyliśmy wcześniej, moduł projektywny może powstać, gdy mamy w pierścieniu element idempotentny. Jednakże słynna hipoteza Kaplanskiego mówi, że pierścień grupowy grupy beztorsyjnej nie ma idempotentów różnych

od 0 i 1. Jest to zresztą część jeszcze ogólniejszej hipotezy: *jeśli grupa G jest beztorsyjna i K jest ciałem, to pierścień K[G] nie ma dzielników zera*, tj. takich elementów $a, b \neq 0$ że $ab = 0$. (Przypomnijmy, że $e^2 = e$ pociąga $e(1-e) = 0$). Jak dotąd, udało się tę hipotezę udowodnić jedynie dla pewnych specjalnych klas grup [14].

Istnieją przypadki, dla których dowód hipotezy o dzielnikach zera jest bardzo prosty. Rozważmy np. pierścień $K[C_\infty] = K[t, t^{-1}]$. Pierścień ten nie ma dzielników zera, gdyż iloczyn elementów

$$a = a_n t^n + (\textit{wyrazy niższych stopni}),$$

$$b = b_m t^m + (\textit{wyrazy niższych stopni})$$

jest postaci

$$ab = a_n b_m t^{n+m} + (\textit{wyrazy niższych stopni}),$$

a więc $ab \neq 0$. Skorzystaliśmy tu z tego, że grupę C_∞ można uporządkować w sposób zgodny z działaniem grupowym [23]. Podany wyżej argument daje się bez trudu przenieść na dowolne grupy uporządkowane.

Można pójść jeszcze dalej tą drogą: powiemy, że grupa G ma *własność u.p.* (*unique product*), jeśli dla każdej pary jej niepustych, skończonych podzbiorów A, B pośród iloczynów ab, $a \in A$, $b \in B$, istnieje element $a_0 b_0$, który zapisuje się tak tylko na jeden sposób. Jest oczywiste, że C_∞ ma własność u.p. oraz że ta własność wystarcza do dowodu hipotezy o dzielnikach zera.

Własność u.p. została odkryta przez Higmana w jego rozprawie doktorskiej [24]. Niestety, praca ta nie została nigdy opublikowana w całości i własność u.p. została zapomniana. Odkryto ją ponownie w latach sześćdziesiątych.

W 1980 roku Strojnowski [27] udowodnił, że własność u.p. pociąga tzw. *własność t.u.p.* (*two unique product property*), która brzmi: dla każdej pary niepustych, skończonych podzbiorów A, B grupy G spełniających $|A| + |B| > 2$ istnieją wśród iloczynów ab co najmniej *dwa*: $a_0 b_0$, $a_1 b_1$, zapisujące się w tej formie jednoznacznie. Ta nowa własność, także znana od dawna, implikuje dodatkowo, że w pierścieniu $K[G]$ wszystkie jedności są trywialne, tj. postaci rg, gdzie $g \in G$ i $r \in K^*$. Istotnie, jeśli $a, b \in K[G]$ i $ab = 1$, to kładziemy

$$A = \{g|\ a(g) \neq 0\}, \qquad B = \{g|\ b(g) \neq 0\}.$$

Jeśli a i b nie są jednomianami, to $|A| + |B| > 2$ i dwa elementy w nośniku ab nie mogą się skrócić, wbrew założeniu: $ab = 1$.

Nie jest łatwo sprawdzać własność u.p. dla konkretnych grup. Jak dotąd, znany jest zaledwie jeden przykład grupy beztorsyjnej, która nie ma własności u.p. Został on podany przez Ripsa i Segeva w 1985 roku (preprint). Na przykład nie wiadomo, które beztorsyjne grupy krystalograficzne spełniają warunek u.p.

Całkiem konkretnie, nie wiadomo, czy grupa

$$G = \langle x, y |\ x^{-1} y^2 x = y^{-2},\ y^{-1} x^2 y = x^{-2} \rangle$$

ma własność u.p.([1]) W szczególności nie wiemy, czy pierścień ZG ma nietrywialne jedności, choć od dawna wiemy, że nie ma on dzielników zera [23].

Pierścień grupowy $K[G]$ został zbudowany z dwóch składników: grupy G oraz pierścienia K. Czy składniki te dadzą się odczytać z pierścienia $K[G]$? Oczywisty izomorfizm

$$K[G \times H] = (K[G])[H]$$

wykazuje, że odpowiedź na tak ogólne pytanie jest negatywna.

Jeśli ustalimy grupę, to możemy pytać, czy pierścień K da się wyznaczyć z pierścienia $K[G]$, tj. czy z izomorfizmu

$$K[G] \approx L[G]$$

wynika izomorfizm $K \approx L$. Szczególnie interesujący jest przypadek, gdy G jest nieskończoną grupą cykliczną C_∞. W języku geometrii algebraicznej odpowiada on pytaniu, czy

$$V \times T \approx W \times T$$

implikuje izomorfizm $V \approx W$ dla zbiorów afinicznych V, W i jednowymiarowego torusa T. Wiadomo, że $K[C_\infty] \approx L[C_\infty]$ implikuje $K \approx L$, jeżeli K jest *dziedziną Dedekinda* [27], [30]. W geometrii algebraicznej odpowiada to przypadkowi, gdy V jest krzywą nieosobliwą. W przypadku pierścienia odpowiadającego powierzchniom algebraicznym, nawet nieosobliwym, odpowiedź może już być negatywna [18], [30].

Zapytajmy teraz, czy można odtworzyć grupę przy ustalonych współczynnikach. Dokładniej, załóżmy że K-algebry $K[G]$ i $K[H]$ są izomorficzne. Czy $G \approx H$?

Izomorfizm $K[G] \approx K[H]$ przenosi grupę G na podgrupę w grupie elementów odwracalnych pierścienia $K[H]$. Jeśli choć jedna z grup G, H, np. H, ma własność u.p., to mamy

$$GL_1(K[H]) = K^* \times H$$

i stąd łatwo wynika, że $G \approx H$. W ogólnym przypadku grupa $GL_1(K[H])$ jest znacznie większa od $K^* \times H$.

Ograniczmy się teraz do grup skończonych. Odpowiedź zależeć będzie od wyboru współczynników K. Np. jeśli K jest ciałem liczb zespolonych, a G, H są skończonymi grupami abelowymi tego samego rzędu, to z twierdzenia Maschke wynika, że $CG \approx CH$. Odpowiedź jest tu więc negatywna. Ogólnie, jeśli K jest ciałem, to grupa G nie da się na ogół odczytać z $K[G]$. Co więcej, mamy

([1]) Dodane w korekcie: D. S. Promislow wykazał w pracy *A simple example of a torsion-free nonunique product group*, Bull. London Math. Soc. 20 (4) (1988), 302–304, że grupa G nie ma własności u.p.!

następujące twierdzenie Dade'a udowodnione w 1971 roku [23]: istnieją nieizomorficzne grupy metaabelowe G_1, G_2 rzędu 125 000 takie, że dla *każdego* ciała K mamy izomorfizm $K[G_1] \approx K[G_2]$. Grupa G jest *metaabelowa*, jeśli ma abelowy dzielnik normalny A taki, że grupa G/A jest też abelowa.

Aby jeszcze bardziej usztywnić sytuację, załóżmy, że grupy są skończone i K jest pierścieniem liczb całkowitych $\mathbf{Z}$. Wtedy $\mathbf{Z}G \approx \mathbf{Z}H$ pociąga $G \approx H$ w następujących przypadkach:

(a) Grupy G, H są abelowe (łatwe ćwiczenie [26]).

(b) Grupy G, H są metaabelowe (praca doktorska Whitcomba z 1967 roku [26]).

(c) Grupy G, H są nilpotentne (wynik Roggenkampa i Scotta z 1984 roku, preprint).

Ogólnie nic więcej na ten temat w chwili, gdy piszemy ten tekst, nie wiadomo – nawet dla skończonych grup rozwiązalnych. Badania trwają.

Warto wiedzieć również, że pierścienie grupowe mają zastosowania pozamatematyczne. Między innymi spotyka się je w elektrotechnice, jako pierścienie *liczb strukturalnych* [2].

Ciekawe i użyteczne są także uogólnienia pierścieni grupowych. Wśród nich najważniejsze to *pierścienie z gradacją* [22] i *pierścienie półgrupowe* [16], [8], ale to już zupełnie inne historie.

Bibliografia

[1] В. А. Артамонов, *Проективные несвободные модули над групповыми кольцами разрешимых групп*, Мат. Сборник 116 (158), Но. 2 (10) (1981), 234–244.

[2] S. Bellert, H. Woźniakowski, *Analiza i synteza układów elektrycznych metodą liczb strukturalnych*, Warszawa 1968.

[3] А. А. Бовди, *Групповые кольца*, Ужг. Гос. Унив., Ужгород 1974.

[4] S. Balcerzyk, *Wstęp do algebry homologicznej*, Biblioteka Matematyczna 34, PWN, 1972.

[5] G. E. Bredon, *Introduction to Compact Transformation Groups*, Academic Press, 1972.

[6] J. Browkin, *Teoria cial*, Biblioteka Matematyczna 49, PWN, 1977.

[7] K. Brown, *Cohomology of Groups*, Springer, N. Y., 1982.

[8] A. H. Clifford, G. B. Preston, *The algebraic theory of semigroups*, Providence 1961 (jest też przekład rosyjski).

[9] W. H. Cockcroft, *On two dimensional aspherical complexes*, Proc. London Math. Soc. (3) 4 (1954), 375–384.

[10] M. Cohen, *A Course in Simple Homotopy Theory*, Springer, 1973.

[11] C. W. Curtis, I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Interscience, N. Y., 1962.

[12] D. Farkas, *Cristallographic groups and their mathematics*, Rocky Mntn. Journal 11 (1981), No. 4, 511–551.

[13] –, Z. Marciniak, *Idempotents in Group Rings – a Surprise*, Journal of Algebra 81, No. 1 (1983), 266.

[14] –, R. Snider, *K_0 and noetherian group rings*, J. Algebra 42 (1976), 192–198.

[15] F. T. Farrell, W. C. Hsiang, *The Topological Euclidean Space Form Problem*, Inv. Math. 45 (1978), 181–192.
[16] R. Gilmer, *Commutative semigroup rings*, Chicago Lecture Notes in Math., Chicago 1984.
[17] M. I. Kargapołow, J. I. Mierzliakow, *Podstawy teorii grup*, PWN, 1976.
[18] A. I. Kostrykin, *Wstęp do algebry*, PWN, 1984.
[19] J. Krempa, *Isomorphic group rings with nonisomorphic coefficient rings*, Proc. AMS 83 (1981), No. 3.
[20] T. Y. Lam, *Serre's Conjecture*, Springer, Berlin 1978.
[21] J. Lewin, *Projective modules over group algebras of torsion-free groups*, Michigan Math. J. 29 (1982), 59–64.
[22] C. Nastasescu, F. van Oystaeyen, *Graded and filtered rings and modules*, Springer, Lecture Notes in Math. 758, Berlin 1979.
[23] D. S. Passman, *The algebraic structure of group rings*, Interscience, 1977.
[24] R. Sandling, *Graham Higman's Thesis "Units in Group Rings"*, Springer Lecture Notes in Math. 882.
[25] D. Segal, *Polycyclic Groups*, Camb. Univ. Press, 1983.
[26] S. K. Sehgal, *Topics in Group Rings*, M. Dekker, 1978.
[27] A. Strojnowski, *A note on u.p. groups*, Comm. in Algebra 8 (3) (1980), 231–234.
[28] M. Van den Berg, *Group rings over Dedekind rings*, Preprint, 86–03, Uniwersytet w Antwerpii.
[29] C. T. C. Wall, *Finiteness conditions for CW-complexes*, Ann. Math. 81 (1965), 56–69.
[30] K. Yoshida, *On the coefficient ring of a torus extension*, Osaka J. Math. 17 (1980), 769–782.
[31] Л. Е. Залесский, А. В. Михалев, *Групповые кольца*, 5–118 w: *Итоги Науки и Техники*, ВИНИТИ 1973.