WYBRANE ZAGADNIENIA INFORMATYKI TECHNICZNEJ

Podstawy matematyczne

pod redakcją naukową Zenona A. Sosnowskiego

Politechnika Białostocka

WYBRANE ZAGADNIENIA INFORMATYKI TECHNICZNEJ

Podstawy matematyczne

Pod redakcją naukową Zenona A. Sosnowskiego

Politechnika Białostocka

OFICYNA WYDAWNICZA POLITECHNIKI BIAŁOSTOCKIEJ
BIAŁYSTOK 2022

Recenzenci:
dr hab. Ryszard Andruszkiewicz, prof. UwB
dr hab. inż. Waldemar Hołubowski, prof. PŚ
dr Małgorzata Jastrzębska, UPH
dr hab. Jerzy Matczuk, prof. UW
dr Karol Pryszczepko, UwB
dr inż. Witold Tomaszewski, PŚ

Redaktor naukowy dyscypliny informatyka techniczna i telekomunikacja:
prof. dr hab. Jarosław Stepaniuk

Korekta językowa:
Agnieszka Polecka

Skład, opracowanie graficzne:
Kamil Zabielski

Okładka:
Marcin Dominów
Zdjęcie na okładce: squarefrog
https://pixabay.com/pl/illustrations/matryca-zasłona-tekstura-komputer-5470930/

ISBN: 978-83-67185-17-2
ISBN: 978-83-67185-18-9 (eBook)
DOI: 10.24427/978-83-67185-18-9

Druk: PPH Remigraf sp. z o.o.

Oficyna Wydawnicza Politechniki Białostockiej
ul. Wiejska 45C, 15-351 Białystok
e-mail: oficyna.wydawnicza@pb.edu.pl
www.pb.edu.pl

Spis treści

Wstęp 5

1 ALGEBRY GRUPOWE W TEORII KODÓW 7
Czesław Bagiński, Kamil Zabielski
Wprowadzenie 7
1.1 Wprowadzenie do algebr grupowych 9
1.2 Kody i ich realizacja z pomocą algebr grupowych 21
Podsumowanie 35
Bibliografia 36

2 O ADDYTYWNYCH GRUPACH (ŁĄCZNYCH) PIERŚCIENI PRZEMIENNYCH 37
Mateusz Woronowicz
Wprowadzenie 37
2.1 Oznaczenia 38
2.2 Wiadomości wstępne 40
2.3 Klasyfikacja torsyjnych *CR*-, *ACR*- i *AR*-grup 45
2.4 Klasyfikacja beztorsyjnych całkowicie rozkładalnych *CR*-grup 47
2.5 Beztorsyjne $(A)CR$-grupy rangi dwa 48
2.6 O strukturze mieszanych $(A)CR$-grup 52
2.7 *E*-grupy i *CRM*-grupy jako szczególne przypadki *CR*-grup 59
Podsumowanie 64
Bibliografia 64

3 PROBABILISTYCZNE I ALGEBRAICZNE ASPEKTY ZAOKRĄGLANIA LICZB 67
Ryszard Mazurek
Wprowadzenie 67
3.1 Probabilistyczne aspekty zaokrąglania liczb 68
3.2 Algebraiczne aspekty zaokrąglania liczb 81
3.2.1 Grupoid zdefiniowany przy pomocy zaokrąglania do setek . . . 81
3.2.2 Grupoid zdefiniowany przy pomocy zaokrąglania do części całkowitej 90
Podsumowanie 92
Bibliografia 92

4 O WŁASNOŚCIACH PIERŚCIENI Z GRADACJAMI WZGLĘDEM PÓŁGRUP 93
Marek Kępczyk
Wprowadzenie 93
4.1 Pierścienie β-radykalne 96
4.2 Pierścienie T-nilpotentne 99
4.3 Półkratowe sumy pierścieni 103
4.4 Półgrupowe sumy pierścieni 108
4.5 S-sumy pierścieni 115
Podsumowanie 118
Bibliografia 119

Wstęp

Algebra abstrakcyjna jest ważnym narzędziem współczesnej informatyki. Podstawowe dzisiaj techniki kryptograficzne opierają się na abstrakcyjnych konstrukcjach algebraicznych z wykorzystaniem pojęcia ciała skończonego, grupy, czy pierścienia.

Niniejsza monografia jest zbiorem czterech prac naukowych przedstawiających osiągnięcia badawcze z obszaru algebry. Poszczególne rozdziały dotyczą zagadnień związanych z wykorzystaniem ideałów pierścieni grupowych do generowania kodów korekcyjnych, wpływie struktury addytywnej na strukturę pierścienia łącznego, zagadnienia dotyczące zaokrąglania liczb oraz przegląd obecnego stanu wiedzy o pierścieniach z różnego typu gradacjami.

W rozdziale pierwszym ALGEBRY GRUPOWE W TEORII KODÓW Czesław Bagiński i Kamil Zabielski opisują wykorzystanie ideałów pierścieni grupowych do konstrukcji kodów korekcyjnych. Okazuje się, że owe abstrakcyjne konstrukcje mogą być źródłem zarówno nowych kodów, jak również źródłem nowych algorytmów odkodowywania kodów znanych wcześniej. W niektórych przypadkach w obliczeniach Autorzy wykorzystali system GAP - rozbudowany pakiet do obliczeń symbolicznych stworzonych na potrzeby algebry abstrakcyjnej, zwłaszcza teorii grup.

Mateusz Woronowicz w rozdziale drugim O ADDYTYWNYCH GRUPACH (ŁĄCZNYCH) PIERŚCIENI PRZEMIENNYCH przedstawia stan obecnej wiedzy o wpływie struktury addytywnej na strukturę pierścienia łącznego. Zostały w nim dokładnie omówione zarówno klasyczne, jak i najnowsze wyniki z tego zakresu. Zgodnie z intencją Autora, praca ma charakter przeglądowy, co czyni ją użyteczną w kontekście potencjalnych zastosowań w informatyce.

W rozdziale trzecim PROBABILISTYCZNE I ALGEBRAICZNE ASPEKTY ZAOKRĄGLANIA LICZB, autorstwa Ryszarda Mazurka, przedstawiono zagadnienia dotyczące zaokrąglania liczb, które mogą być rozwiązywane za pomocą narzędzi informatycznych i matematycznych oraz stanowić punkt wyjścia do badania bardziej skomplikowanych (pod względem rachunkowym) modyfikacji tych zagadnień. W szczególności zaprezentowano algorytmy, dzięki którym wyznaczono zbiory potęg poszczególnych elementów grupoidu złożonego z reszt z dzielenia przez l00, oraz wyznaczono wszystkie cykliczne podgrupoidy tego grupoidu będące półgrupami.

Rozdział czwarty Marka Kępczyka O WŁASNOŚCIACH PIERŚCIENI Z GRADACJAMI WZGLĘDEM PÓŁGRUP jest poświęcony przedstawieniu obecnego stanu wiedzy o pierścieniach z różnego typu gradacjami. Skupiono się głównie na pierścieniach, których własności są zbliżone do pierścieni nilpotentnych. Autor przedstawia szereg ciekawych wyników związanych z pierścieniami z tożsamością wielomianową.

Zespół autorski niniejszej monografii ma nadzieję, że treści w niej zawarte zainteresują potencjalnych czytelników.

Białystok, kwiecień 2022 Zenon A. Sosnowski

Rozdział 1

ALGEBRY GRUPOWE W TEORII KODÓW

Czesław Bagiński, Kamil Zabielski*

Streszczenie Rozwój teorii kodowania i teorii informacji jest pokłosiem realnej potrzeby usprawnienia komunikacji między urządzeniami technicznymi. Wzrost znaczenia informacji oraz rosnące zapotrzebowanie optymalizacji stosunku ilości przesyłanych informacji do zdolności korekcji i detekcji błędów jest nie do zignorowania. Odpowiedzią na te rosnące potrzeby jest algebraiczna teoria kodowania. Autorzy w pracy przedstawiają formalną konstrukcję kodów z wykorzystaniem języka teorii algebr grupowych, w szczególności z wykorzystaniem ideałów tych algebr. W pracy autorzy prezentują podstawy formalne, przedstawiają konstrukcję kodu Golay'a oraz kodu Reeda-Mullera, ostatecznie ilustrując w przykładach rachunki z wykorzystaniem systemu `GAP`.

Słowa kluczowe: algebry grupowe, teoria kodowania, kody, gap

Wprowadzenie

Teoria kodowania narodziła się wraz z teorią informacji w latach 50-tych XX w. z potrzeby usprawnienia komunikacji między urządzeniami technicznymi oraz między człowiekiem a urządzeniem. Kody używane do tego celu stały się swego rodzaju językiem zrozumiałym dla komunikujących się stron. Wraz z rewolucją technologiczną oraz wyjątkowo szybkim rozwojem znaczenia informacji i jej przekazu, w odpowiedzi na gwałtownie rosnące zapotrzebowanie, sięgnięto do niezawodnego narzędzia, jakim jest matematyka. W efekcie powstała algebraiczna teoria kodowania, która z jednej strony uporządkowała dotychczasowe pomysły efektywnie działających kodów, z drugiej, dzięki abstrakcyjnym konstrukcjom, od dawna znanym w algebrze, stała się źródłem nowych kodów, których własności coraz lepiej spełniają wymagające oczekiwania. Jednym z tych wymagań, wynikającym z zawodności urządzeń przekazujących, jak również różnorodności warunków przekazu, jest potrzeba rozpoznawania błędów powstałych w przekazie i ich poprawiania przez odbiorcę, bez konieczności ponownego jej wysyłania, ponieważ bardzo często po-

* Wydział Informatyki, Politechnika Białostocka, Wiejska 45A, 15-351 Białystok, c.baginski@pb.edu.pl

DOI 10.24427/978-83-67185-18-9_1

wtórzenie przekazu nie jest po prostu możliwe. Spełnienie tych warunków wiąże się z wymuszeniem nadmiarowości przekazywanych informacji, co przy jej ogromie może oznaczać spowolnienie kodowania, jego przesyłu, procesu dekodowania i wreszcie reakcji na otrzymane wiadomości. W stopniu zadowalającym te warunki spełniają dobrze skonstruowane kody liniowe, znane od końca lat pięćdziesiątych dwudziestego wieku. Kody liniowe to w istocie konkretne podprzestrzenie przestrzeni liniowej $W = \mathbb{F}^n$, której wektory, przedstawione w standardowej bazie przestrzeni W, są wzajemnie jednoznacznie przyporządkowane jednostkom informacji, a ich postać pozwala na taki ich przesył między nadawcą i odbiorcą, że nawet w przypadku wystąpienia zakłóceń powodujących zniekształcenie przesyłanych informacji, odbiorca z dużym prawdopodobieństwem może precyzyjnie ją odtworzyć. Podstawowy, matematyczny opis własności kodów nie wymaga szczególnie głębokiej wiedzy matematycznej. Jest oparty na standardowym kursie algebry liniowej, kombinatoryki i rachunku prawdopodobieństwa. W końcu lat sześćdziesiątych odkryto, że niektórym z kodów liniowych można nadać bogatszą strukturę algebraiczną - ideałów algebr grupowych. Teoria algebr grupowych jest dalece zaawansowanym obszarem badań algebry abstrakcyjnej, wciąż intensywnie rozwijanym i coraz częściej dostarczającym interesujących przykładów zastosowań w teorii kodowania, zwłaszcza, że owa bogatsza struktura pozwala czasem na stworzenie szybszych algorytmów kodujących i dekodujących wiadomości.

Celem tego artykułu jest pokazanie na kilku przykładach jak można reprezentować kody w postaci ideałów algebry grupowej. Do zrozumienia materiału wystarczy podstawowy kurs algebry abstrakcyjnej, wykładany zwykle na drugim roku studiów matematycznych. W pierwszym rozdziale wprowadzimy podstawowe fakty z teorii algebr grupowych, a w drugim przedstawimy kilka wybranych kodów i przedstawimy je w języku teorii algebr. W niektórych przypadkach w obliczeniach posłużymy się systemem `GAP` - rozbudowanym pakietem do obliczeń symbolicznych stworzonych na potrzeby algebry abstrakcyjnej, zwłaszcza teorii grup. Współcześnie informatyka dostarcza całe mnóstwo systemów wspomagających obliczenia symboliczne oraz wnioskowanie matematyczne. Systemy algebry komputerowej (ang. Computer Algebra System) są powszechnie wykorzystywane jako wsparcie dowodu formalnego, poprzez ułatwienie wyszukiwania pewnych wzorców, jak również bywają podstawą dowodu. Na szczególną uwagę zasługuje właśnie `GAP` (p. GAP (2021)), ze względu na to, że jest żywo rozbudowywanym oprogramowaniem open source z zakresu obliczeniowej teorii grup i tylko nieznacznie odstaje od silnych komercyjnych programów z tego zakresu, jakimi są `CAYLEY` i `MAGMA`.

Nie wchodząc zbytnio w szczegóły techniczne, warto nadmienić, że `GAP` poza rdzennymi implementacjami standardowych obiektów algebraicznych, pozwala na proste i szerokie rozszerzanie bazowych funkcjonalności przez zastosowanie mechanizmu paczek. Na szczególną uwagę zasługują te, które są zaakceptowane; to znaczy takie, których kod źródłowy społeczność uważa za stabilny, a prezentowane wyniki za godne zaufania. Do badania kodów korekcyjnych, warto przyjrzeć się paczce

GUAVA, zaakceptowanej w lutym 2003 r. Wedderga, natomiast, jest to paczka, która okazuje się szczególnie przydatna przy badaniu półprostych algebr grupowych nad ciałami skończonymi z wykorzystaniem algorytmu rozkładu Weddeburna Broche i del Río (2007), Olteanu i del Río (2009), zaakceptowana w styczniu 2008 r.

1.1 Wprowadzenie do algebr grupowych

Wszystkie algebry i przestrzenie rozważane w tej pracy, są nad ciałami skończonymi. Na ogół są to ciała charakterystyki 2 lub ciała proste $\mathbb{Z}_p$, gdzie p jest liczbą pierwszą. Podstawy teorii ciał skończonych można znaleźć np. w Kobliz (2006). Tu przytoczymy jedynie następujące twierdzenie.

Twierdzenie 1.1. Niech p będzie liczbą pierwszą i $\mathbb{F}_q$ niech będzie ciałem o $q = p^k$ ($k \in \mathbb{N}$) elementach. Wówczas:

(a) Dla dowolnego $\alpha \in \mathbb{F}$ $f_q(\alpha) = 0$, gdzie $f_q(x) = x^q - x \in \mathbb{F}_q$, innymi słowy

$$f_q(x) = x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha).$$

(b) Wielomian $f_q(x)$ rozkłada się nad ciałem $\mathbb{F}_p = \mathbb{Z}_p$ na iloczyn wszystkich wielomianów nierozkładalnych nad $\mathbb{F}_p$, których stopnie są dzielnikami liczby k.

(c) Multyplikatywna grupa ciała $\mathbb{F}_q$ jest cykliczna, tzn. istnieje element $\omega \in \mathbb{F}_q$, taki że

$$\mathbb{F}_q^* = \mathbb{F}_q = \left\{ \omega, \omega^2, \omega^3, \ldots, \omega^{q-1} = 1 \right\}.$$

Niech G będzie grupą skończoną z operacją o multyplikatywnym zapisie i $\mathbb{F}$ ciałem skończonym. Symbolem $\mathbb{F}[G]$ oznaczymy zbiór wszystkich formalnych kombinacji liniowych postaci:

$$\sum_{g \in G} a_g g, \quad a_g \in \mathbb{F}. \tag{1.1.1}$$

Zakładamy przy tym, że jeśli $\alpha = \sum_{g \in G} a_g g$ oraz $\beta = \sum_{g \in G} b_g g$, to $\alpha = \beta$ wtedy i tylko wtedy, gdy zachodzą równości $a_g = b_g$ dla wszystkich $g \in G$. W zbiorze $\mathbb{F}[G]$ definiujemy dodawanie elementów przyjmując, że dla określonych wyżej α i β dane jest:

$$\alpha + \beta = \sum_{g \in G} a_g g + \sum_{g \in G} b_g g \stackrel{\text{def.}}{=} \sum_{g \in G} (a_g + b_g) g. \tag{1.1.2}$$

Wprowadzamy również operację mnożenia elementów zbioru $\mathbb{F}[G]$ przez elementy z ciała $\mathbb{F}$; mianowicie, jeśli $a \in \mathbb{F}$ i $\alpha \in \mathbb{F}[G]$ to

$$a\alpha = a \cdot \sum_{g \in G} a_g g \stackrel{\text{def.}}{=} \sum_{g \in G} (a a_g) g = \alpha a. \tag{1.1.3}$$

.

Te dwie operacje (1.1.2) (1.1.3) wprowadzają w zbiorze $\mathbb{F}[G]$ strukturę przestrzeni liniowej nad ciałem $\mathbb{F}$. Standardową bazą tej przestrzeni jest zbiór elementów grupy G. Do struktury przestrzeni liniowej dodajemy jeszcze strukturę pierścienia, wprowadzając mnożenie elementów tego zbioru (które, jak łatwo pokazać, jest rozdzielne względem dodawania (1.1.2) zdefiniowanego wyżej):

$$\alpha \cdot \beta = \left(\sum_{g \in G} a_g g \right) \cdot \left(\sum_{g \in G} b_g g \right) \stackrel{\text{def.}}{=} \sum_{g \in G} \left(\sum_{xy=g} a_x b_y \right) g. \tag{1.1.4}$$

Wszystkie te działania wprowadzają w $\mathbb{F}[G]$ strukturę algebry, którą nazywamy algebrą grupową grupy G nad ciałem $\mathbb{F}$. Element neutralny mnożenia w ciele $\mathbb{F}$, czyli po prostu jedynka tego ciała, i element neutralny grupy G zwykle oznacza się symbolem 1. Symbol ten ma, zatem, dwa znaczenia. W algebrze $\mathbb{F}[G]$ rozumiany jest jako skalar; w grupie jako element standardowej bazy tej algebry. Jeśli jednak przyjmiemy utożsamienie jedynki z ciała z jedynką w grupie, nie będzie to prowadzić do nieporozumień.

Struktura algebry grupowej jest silnie zależna od tego, czy $\operatorname{char}\mathbb{F}$ i $|G|$ są względnie pierwsze. Zajmiemy się najpierw przypadkiem, gdy $\operatorname{char}\mathbb{F} > 0$ nie dzieli rzędu grupy G.

Twierdzenie 1.2. Niech $\mathbb{F}$ będzie ciałem charakterystyki $p > 0$ i G grupą, której rząd nie jest podzielny przez p. Wówczas istnieją liczby naturalne $n_1, n_2, \ldots, n_k$ oraz ciała $\mathbb{F}_1$, $\mathbb{F}_2$, ..., $\mathbb{F}_k$, będące rozszerzeniami ciała $\mathbb{F}$, takie że

$$\mathbb{F}[G] \cong M_{n_1}(\mathbb{F}_1) \oplus M_{n_2}(\mathbb{F}_2) \oplus \ldots \oplus M_{n_k}(\mathbb{F}_k), \tag{1.1.5}$$

gdzie $M_{n_i}(\mathbb{F}_i)$ jest algebrą macierzy kwadratowych nad ciałem $\mathbb{F}_i$, $i = 1, 2, \ldots, k$. Ponadto

$$|G| = \dim_{\mathbb{F}} \mathbb{F}[G] = n_1^2 \dim_{\mathbb{F}} \mathbb{F}_1 + n_2^2 \dim_{\mathbb{F}} \mathbb{F}_2 + \cdots + n_k^2 \dim_{\mathbb{F}} \mathbb{F}_k.$$

Do uzyskania rozkładu opisanego powyższym twierdzeniem należy wyznaczyć układ centralnych prymitywnych idempotentów tej algebry. Wcześniej, jeszcze jedno pojęcie; powiemy, że element a algebry $\mathscr{A}$ anihiluje podzbiór B tej algebry, jeśli dla dowolnego $b \in B$ zachodzi równość $ab = ba = 0$. Anihilatorem podzbioru B nazywamy zbiór wszystkich elementów algebry anihilujących wszystkie elementy zbioru B:

$$Ann_{\mathscr{A}}(B) = \{a \in \mathscr{A} : \forall_{(b \in B)}\, ab = ba = 0\}$$

.

Definicja 1.1. Centralnym prymitywnym idempotentem algebry A nazywamy element **e**, taki, że:

(i) $\mathbf{e}^2 = \mathbf{e}$;
(ii) $\mathbf{e}\alpha = \alpha\mathbf{e}$, dla dowolnego $\alpha \in A$;
(iii) nie istnieją $\mathbf{e}_1,\ \mathbf{e}_2$ spełniające warunki (i) i (ii), takie, że $\mathbf{e}_1 + \mathbf{e}_2 = \mathbf{e}$.

Centralność zapewnia (ii), a prymitywność (iii).

Twierdzenie 1.3. Niech $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_k\}$ będzie zbiorem wszystkich centralnych prymitywnych idempotentów algebry $\mathbb{F}[G]$. Wówczas:

(i) $\mathbf{e}_1 + \mathbf{e}_2 + \cdots + \mathbf{e}_k = 1$.
(ii) Każda składowa sumy prostej (1.1.5) ma postać $\mathbf{e}_i\mathbb{F}[G]$, tzn. jest ideałem głównym generowanym przez $\mathbf{e}_i$. Ponadto, każda taka składowa jest ideałem minimalnym.
(iii) Każdy ideał algebry $\mathbb{F}[G]$ jest sumą prostą ideałów minimalnych; dokładniej, jeśli I jest ideałem, to $I = \mathbf{e}\mathbb{F}[G]$, gdzie $\mathbf{e} = \mathbf{e}_{i_1} + \mathbf{e}_{i_2} + \cdots + \mathbf{e}_{i_m}$, $1 \leqslant i_1 < i_2 < \ldots < i_m \leqslant k$, w szczególności liczba wszystkich ideałów jest równa 2^k. Ponadto, jeśli $I = \mathbf{e}\mathbb{F}[G]$ jest ideałem, to $\mathrm{Ann}_{\mathbb{F}[G]}(I) = (1-\mathbf{e})\mathbb{F}[G]$.
(iv) Jeżeli każdy element grupy G ma rząd dzielący $|\mathbb{F}| - 1$, to wszystkie ciała $\mathbb{F}_i$ ze sformułowania tw. 1.1.5 są izomorficzne z $\mathbb{F}$. Ponadto, liczba k jest równa liczbie klas elementów sprzężonych grupy G.
(v) Jeśli G jest grupą abelową, to $\mathbb{F}[G]$ jest sumą prostą ciał $\mathbb{F}_i$, a przy założeniach podpunktu (iv):

$$\mathbb{F}[G] \cong \underbrace{\mathbb{F} \oplus \ldots \oplus \mathbb{F}}_{|G|}.$$

Przykład 1.1. Niech $G = \langle g : g^3 = e\rangle = \{g, g^2, g^3 = 1\}$ będzie grupą cykliczną rzędu 3. Wówczas:

$$\mathbb{F}[G] = \{a + bg + cg^2 : a, b, c \in \mathbb{F}\}$$

jest przestrzenią trójwymiarową nad $\mathbb{F}$ z mnożeniem określonym wzorem:

$$\begin{aligned}&(ae + bg + cg^2)(a'e + b'g + c'g^2) = \\ &= (aa' + bc' + cb')e + (ab' + ba' + cc')g + (ac' + bb' + ca')g^2.\end{aligned}$$

Wewnętrzna struktura algebry, oprócz tego, że w oczywisty sposób zależy od G, jest zależna od ciała $\mathbb{F}$. Dla rozważanej grupy rzędu 3, jeżeli ciało $\mathbb{F}$ ma charakterystykę różną od 3, ale nie ma w niej pierwiastka trzeciego stopnia z 1, różnego od 1, to dla elementów:

$$\mathbf{e} = \frac{1}{3} + \frac{1}{3}g + \frac{1}{3}g^2 = \frac{1+g+g^2}{3} \ \text{ i } \ \mathbf{f} = 1 - \mathbf{e}$$

spełnione są warunki:

$$\mathbf{e}^2 = \mathbf{e},\ \ \mathbf{f}^2 = \mathbf{f},\ \ \mathbf{ef} = \mathbf{fe} = 0,\ \ \mathbf{e} + \mathbf{f} = 1.$$

Jeśli teraz $\alpha = a + bg + cg^2$ jest dowolnym elementem algebry $\mathbb{F}[G]$, to można go zapisać w postaci:

$$\alpha = \alpha \cdot 1 = \alpha(\mathbf{e} + \mathbf{f}) = \alpha\mathbf{e} + \alpha\mathbf{f} = \alpha_1 + \alpha_2$$

gdzie

$$\alpha_1 = (a+b+c)\mathbf{e}, \;\; \alpha_2 = ((a-c)+(b-c)g)\mathbf{f}$$

i oczywiście $\alpha_1 \cdot \alpha_2 = 0$. To pozwala patrzeć na $\mathbb{F}[G]$ jak na zbiór par postaci (α_1, α_2), przy czym elementy stojące na pierwszym miejscu można traktować jak elementy ciała $\mathbb{F}$, a elementy stojące na drugim, jak elementy ciała $\mathbb{F}(\omega)$, gdzie ω jest pierwiastkiem trzeciego stopnia z 1. Algebra rozkłada się zatem na sumę prostą dwóch ciał:

$$\mathbb{F}[G] \cong \mathbb{F} \oplus \mathbb{F}(\omega).$$

Zauważmy, że ta algebra ma dokładnie dwa ideały właściwe. Jeśli $\mathbb{F} = GF(p)$ jest ciałem p-elementowym, takim, że $3 \nmid p-1$, to $\dim_{\mathbb{F}}\mathbb{F}(\omega) = 2$.

Niech teraz $\mathbb{F}$ będzie ciałem zawierającym element $\omega \neq 1$ taki, że $\omega^3 = 1$. Niech ponadto:

$$\mathbf{e}_1 = \frac{1+g+g^2}{3}, \;\; \mathbf{e}_2 = \frac{1+\omega g+\omega^2 g^2}{3}, \;\; \mathbf{e}_3 = \frac{1+\omega^2 g+\omega g^2}{3}.$$

Wówczas łatwo sprawdzić, że:

(a) $1 + \omega + \omega^2 = 0$,
(b) $\mathbf{e}_1$, $\mathbf{e}_2$ i $\mathbf{e}_3$ są liniowo niezależne i spełniają zależności:

$$\mathbf{e}_i^2 = \mathbf{e}_i, \;\; \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3 = 1, \;\; e_i e_j = 0 \;\text{ dla } i \neq j.$$

(c) $\mathbf{e}_i\mathbb{F}[G] \cong \mathbb{F}$ dla $i = 1,2,3$.

Rozważmy teraz przypadek bardziej ogólny.

Przykład 1.2. Niech $G = \langle g : g^r = e\rangle = \{g, g^2, \ldots, g^{r-1}, g^r = 1\}$ będzie grupą cykliczną rzędu r i $\mathbb{F}$ ciałem, którego charakterystyka nie dzieli rzędu grupy. Wówczas:

$$\mathbb{F}[G] = \{a_0 + a_1 g + a_2 g^2 + \ldots a_{r-1} g^{r-1} : \; a_0, a_1, a_2, \ldots, a_{r-1} \in \mathbb{F}\}$$

z naturalnym dodawaniem tych wyrażeń i mnożeniem przez elementy z ciała $\mathbb{F}$ jest przestrzenią r-wymiarową nad $\mathbb{F}$. Z algebraicznego punktu widzenia ciekawszą jest struktura pierścienia (a zatem i algebry), którą uzyskujemy definiując w $\mathbb{F}[G]$ operację mnożenia. Mówiąc poglądowo, jest ono takie, jak mnożenie wielomianów zmiennej g, z uwzględnieniem równości $g^r = 1$, co pozwala na redukcję wykładników dla g do zbioru reszt modulo r, $\mathbb{Z}_r$.

Mnożenie, zgodnie z definicją, jest więc określone wzorem

$$(a_0e + a_1g + a_2g^2 + \cdots + a_{r-1}g^{r-1})(b_0e + b_1g + b_2g^2 + \cdots + b_{r-1}g^{r-1}) =$$
$$= \left(\sum_{i+j\equiv 0} a_ib_j\right) + \left(\sum_{i+j\equiv 1} a_ib_j\right) g + \left(\sum_{i+j\equiv 2} a_ib_j\right) g^2 + \cdots + \left(\sum_{i+j\equiv -1} a_ib_j\right) g^{r-1} =$$
$$= \sum_{k=0}^{r-1} \left(\sum_{i+j\equiv k} \right) g^k,$$

gdzie przystawanie pod znakiem sumy, jest brane modulo r. Struktura ideałów tego pierścienia jest zależna od charakterystyki p ciała $\mathbb{F}$ i zależności między p i r. Przypadek $p = r$ jest algebraicznie bardziej skomplikowany. Zajmiemy się zatem przypadkiem $p \neq r$. Jeśli ciało $\mathbb{F}$ nie zawiera pierwiastków stopnia r z jedynki, to stopień rozszerzenia ciała $|\mathbb{F}(\omega) : \mathbb{F}|$ jest dzielnikiem liczby $r-1$. Załóżmy najpierw, że ten stopień jest równy $r-1$, wówczas dla elementów:

$$\mathbf{e} = \frac{1 + g + g^2 + \cdots + g^{r-1}}{r}, \quad \mathbf{f} = 1 - \mathbf{e}, \tag{1.1.6}$$

spełnione są dwa warunki:

$$\mathbf{e}^2 = \mathbf{e}, \quad \mathbf{f}^2 = \mathbf{f}, \quad \mathbf{ef} = \mathbf{fe} = 0, \quad \mathbf{e} + \mathbf{f} = 1. \tag{1.1.7}$$

Ideały główne algebry, generowane przez te elementy, są jedynymi niezerowymi ideałami właściwymi, a ponadto

$$\mathbb{F}[G] = \mathbf{e}\mathbb{F}[G] \oplus \mathbf{f}\mathbb{F}[G],$$

przy czym ideał $\mathbf{e}\mathbb{F}[G]$ jest izomorficzny z ciałem $\mathbb{F}$, natomiast ideał $\mathbf{f}\mathbb{F}[G]$ jest izomorficzny z ciałem $\mathbb{F}(\omega)$, gdzie ω jest pierwiastkiem pierwotnym stopnia r nad ciałem $\mathbb{F}$.

Załóżmy teraz drugi skrajny przypadek, innymi słowy załóżmy, że ciało $\mathbb{F}$ zawiera pierwiastek stopnia r z 1, czyli $|\mathbb{F}(\omega) : \mathbb{F}| = 1$. Jeśli ciało jest skończone, to ma to miejsce wtedy i tylko wtedy, gdy r jest dzielnikiem rzędu multyplikatywnej grupy ciała $\mathbb{F}$, tzn. gdy $r \mid (|\mathbb{F}| - 1)$. Oznaczmy, jak wyżej, ten pierwiastek przez ω. Niech dalej:

$$\begin{aligned}
\mathbf{e}_0 &= \tfrac{1+g+g^2+\cdots+g^{r-1}}{r}, \\
\mathbf{e}_1 &= \tfrac{1+\omega g+\omega^2 g^2+\cdots+\omega^{r-1} g^{r-1}}{r}, \\
\mathbf{e}_2 &= \tfrac{1+\omega^2 g+\omega^4 g^2+\cdots+\omega^{2(r-1)} g^{r-1}}{r}, \\
\cdots &= \cdots\cdots\cdots\cdots\cdots\cdots, \\
\mathbf{e}_{r-1} &= \tfrac{1+\omega^{r-1} g+\omega^{2(r-1)} g^2+\cdots+\omega^{(r-1)^2} g^{r-1}}{r}.
\end{aligned} \tag{1.1.8}$$

Wówczas

$$\mathbf{e}_0+\mathbf{e}_1+\mathbf{e}_2+\cdots+\mathbf{e}_{r-1}=1,\ \mathbf{e}_i\mathbf{e}_j=\mathbf{e}_j\mathbf{e}_i=0\ \text{ dla }\ i\neq j,\ \mathbf{e}_i^2=\mathbf{e}_i,\ 0\leqslant i,j\leqslant r-1. \tag{1.1.9}$$

Wynika stąd, że

$$\mathbb{F}[G]=\mathbf{e}_0\mathbb{F}[G]\oplus\mathbf{e}_1\mathbb{F}[G]\oplus\ldots\oplus\mathbf{e}_{r-1}\mathbb{F}[G],$$

przy czym wszystkie ideały $\mathbf{e}_i\mathbb{F}[G]$ są jednowymiarowymi podprzestrzeniami przestrzeni $\mathbb{F}[G]$, które jako algebry są izomorficzne z ciałem $\mathbb{F}$.

Przypadek, gdy $1<|\mathbb{F}(\omega):\mathbb{F}|=k<r$ wymaga delikatniejszej analizy algebraicznej.

Niech $k=r-1$. Nie wdając się w szczegóły, rozważmy grupę Galois rozszerzenia $Gal(\mathbb{F}(\omega)/\mathbb{F})$. Jej rząd jest równy stopniowi rozszerzenia $|\mathbb{F}(\omega):\mathbb{F}|$. Działanie tej grupy na $\mathbb{F}(\omega)$ można w naturalny sposób rozszerzyć na działanie na algebrze $\mathbb{F}(\omega)[G]$. Bezpośrednio sprawdza się, że automorfizmy zachowują zbiór $\{\mathbf{e}_1,\ \mathbf{e}_2,\ \ldots,\ \mathbf{e}_{r-1}\}$. Bez zmniejszenia ogólności można przyjąć, że orbitami tego działania są zbiory $\{\mathbf{e}_1,\mathbf{e}_2,\ldots,\mathbf{e}_k\},\{\mathbf{e}_{k+1},\mathbf{e}_{k+2},\ldots,\mathbf{e}_{2k}\},\ldots,\{\mathbf{e}_{(l-1)k+1},\mathbf{e}_{(l-1)k+2},\ldots,\mathbf{e}_{lk}\}$. Niech

$$\begin{aligned}\mathbf{f}_1&=\mathbf{e}_1+\mathbf{e}_2+\cdots+\mathbf{e}_k,\\ \mathbf{f}_2&=\mathbf{e}_{k+1}+\mathbf{e}_{k+2}+\cdots+\mathbf{e}_{2k},\\ \cdots&=\cdots,\\ \mathbf{f}_l&=\mathbf{e}_{(l-1)k+1}+\mathbf{e}_{(l-1)k+2}+\cdots+\mathbf{e}_{lk}.\end{aligned}$$

Wówczas dla każdego i, $1\leqslant i\leqslant l$, $\mathbf{f}_i\in\mathbb{F}[G]$ oraz

$$\mathbf{f}_i^2=\mathbf{f}_i,\ \mathbf{f}_i\mathbf{f}_j=0\ \text{ dla }\ i\neq j,\ \sum_{i=1}^{l}\mathbf{f}_i=1-\mathbf{e}_0. \tag{1.1.10}$$

Ponadto dla dowolnego i, $\mathbf{f}_i\mathbb{F}[G]\cong\mathbb{F}(\omega)$. Zatem

$$\mathbb{F}[G]\cong\mathbb{F}\oplus\underbrace{\mathbb{F}(\omega)\oplus\cdots\oplus\mathbb{F}(\omega)}_{l}. \tag{1.1.11}$$

Dla ilustracji wcześniejszych, ogólnych rozważań rozpatrzmy przypadek, gdzie $r=5$ i $\mathbb{F}=\mathbb{Z}_p$, gdzie $p\in\{11,13,19\}$. Niech najpierw $\mathbb{F}=\mathbb{Z}_{11}$ i $\omega=3$. Wtedy

$$\omega^1=3,\ \omega^2=9,\ \omega^3=5,\ \omega^4=4,\omega^5=1,$$

a wobec tego, że $r^{-1}=5^{-1}=9$:

$$\begin{aligned}
\mathbf{e}_0 &= \tfrac{1+g+g^2+g^3+g^4}{5} &&= 9(1+g+g^2+g^3+g^4) &&= 9+9g+9g^2+9g^3+9g^4,\\
\mathbf{e}_1 &= \tfrac{1+3g+9g^2+5g^3+4g^4}{5} &&= 9(1+3g+9g^2+5g^3+4g^4) &&= 9+5g+4g^2+g^3+3g^4,\\
\mathbf{e}_2 &= \tfrac{1+9g+4g^2+3g^3+5g^4}{5} &&= 9(1+9g+4g^2+3g^3+5g^4) &&= 9+4g+3g^2+5g^3+g^4,\\
\mathbf{e}_3 &= \tfrac{1+5g+3g^2+4g^3+9g^4}{5} &&= 9(1+5g+3g^2+4g^3+9g^4) &&= 9+g+5g^2+3g^3+4g^4,\\
\mathbf{e}_4 &= \tfrac{1+4g+5g^2+9g^3+3g^4}{5} &&= 9(1+4g+5g^2+9g^3+3g^4) &&= 9+3g+g^2+4g^3+5g^4,
\end{aligned}$$

co oznacza, że dla $i = 0,1,2,3,4$ mamy $\mathbf{e}_i\mathbb{F}[G] \cong \mathbb{F}$, czyli $\mathbb{F}[G] \cong \mathbb{F}\oplus\mathbb{F}\oplus\mathbb{F}\oplus\mathbb{F}\oplus\mathbb{F}$.

Niech teraz $\mathbb{F} = \mathbb{Z}_{13}$. Najmniejszym ciałem charakterystyki 13 zawierającym pierwiastek stopnia 5 z 1 jest ciało o 13^4 elementach ($13^4 \equiv 1 \pmod 5$ i dla $k < 4$, $13^k \not\equiv 1 \pmod 5$), więc w algebrze $\mathbb{F}[G]$ mamy sytuację opisaną wzorami (1.1.6) i (1.1.7). Zatem:

$$\mathbb{F}[G] \cong \mathbb{F}\oplus\mathbb{F}(\omega).$$

Rozważmy na koniec przypadek $\mathbb{F} = \mathbb{Z}_{19}$. Ponieważ $19^2 \equiv 1 \pmod 5$, więc $|\mathbb{F}(\omega) : \mathbb{F}| = 2$, a jedyny nietożsamościowy automorfizm rozszerzenia $\mathbb{F}(\omega)/\mathbb{F}$ jest indukowany przez przyporządkowanie $\omega \to \omega^{-1}$. Orbitami działania na elementach $\mathbf{e}_i$ (patrz (1.1.8) są $\{\mathbf{e}_1,\mathbf{e}_4\}$ oraz $\{\mathbf{e}_2,\mathbf{e}_3\}$. Stąd

$$\begin{aligned}
\mathbf{f}_1 &= \mathbf{e}_1+\mathbf{e}_4 = \tfrac{2+(\omega+\omega^4)(g+g^4)+(\omega^2+\omega^3)(g^2+g^3)}{5},\\
\mathbf{f}_2 &= \mathbf{e}_2+\mathbf{e}_3 = \tfrac{2+(\omega^2+\omega^3)(g+g^4)+(\omega+\omega^4)(g^2+g^3)}{5}.
\end{aligned}$$

Jednakże $1+\omega+\omega^2+\omega^3+\omega^4 = 0$, zatem dla $t = \omega+\omega^4$ mamy $t^2+t-1 = 0$, a ponieważ nad ciałem $\mathbb{Z}_{19}$ mamy $t^2+t-1 = (t-4)(t+5)$, możemy przyjąć, że $t = \omega+\omega^4 = 4$ i w konsekwencji $\omega^2+\omega^3 = t^2-2 = 14$. Ostatecznie zatem

$$\begin{aligned}
\mathbf{f}_1 &= \mathbf{e}_1+\mathbf{e}_4 = \tfrac{2+4(g+g^4)+14(g^2+g^3)}{5} = 8-3g-g^2-g^3-3g^4,\\
\mathbf{f}_2 &= \mathbf{e}_2+\mathbf{e}_3 = \tfrac{2+14(g+g^4)+4(g^2+g^3)}{5} = 8-g-3g^2-3g^3-g^4,
\end{aligned}$$

$\mathbf{f}_1\mathbb{F}[G] \cong \mathbf{f}_2\mathbb{F}[G] \cong \mathbb{F}(\omega)$ i $\mathbb{F}[G] \cong \mathbb{F}\oplus\mathbb{F}(\omega)\oplus\mathbb{F}(\omega)$.

Bazując na powyższym przykładzie można analogicznie rozważyć przypadek, gdy G jest grupą cykliczną rzędu będącego potęgą liczby pierwszej r. W następstwie, korzystając z zasadniczego twierdzenia o strukturze dowolnej grupy abelowej oraz tego, że

$$\mathbb{F}[G\times H] = \mathbb{F}[G]\otimes_{\mathbb{F}}\mathbb{F}[H],$$

można uzyskać strukturalny rozkład algebry $\mathbb{F}[G]$ na sumę prostą ciał, będących rozszerzeniami ciała $\mathbb{F}$ o stosowne pierwiastki z 1.

Przykład 1.3. Na koniec tej części zademonstrujemy na przykładzie wynik obliczeń wykonanych w GAP-ie dla grupy cyklicznej rzędu 17 i ciała 2-elementowego.

```
gap> G := CyclicGroup(17);
<pc group of size 17 with 1 generators>
gap> F := GF(2);
gap> FG := GroupRing(F, G);
<algebra-with-one over GF(2), with 1 generators>
gap> FGe :=
   ↪ PrimitiveCentralIdempotentsByCharacterTable(FG)
   ↪ ;;
(Z(2)^0)*<identity> of ...+(Z(2)^0)*f1+(Z(2)^0)*f1^2+(
   ↪ Z(2)^0)*f1^3+(Z(2)^0)*f1^4+(Z(2)^0)*f1^5+(Z(2)
   ↪ ^0)*f1^6+(Z(2)^0)*f1^7+(Z(2)^0)*f1^8+(Z(2)^0)*f1
   ↪ ^9+(Z(2)^0)*f1^10+(Z(2)^0)*f1^11+(Z(2)^0)*f1
   ↪ ^12+(Z(2)^0)*f1^13+(Z(2)^0)*f1^14+(Z(2)^0)*f1
   ↪ ^15+(Z(2)^0)*f1^16
(Z(2)^0)*f1+(Z(2)^0)*f1^2+(Z(2)^0)*f1^4+(Z(2)^0)*f1
   ↪ ^8+(Z(2)^0)*f1^9+(Z(2)^0)*f1^13+(Z(2)^0)*f1^15+(
   ↪ Z(2)^0)*f1^16
(Z(2)^0)*f1^3+(Z(2)^0)*f1^5+(Z(2)^0)*f1^6+(Z(2)^0)*f1
   ↪ ^7+(Z(2)^0)*f1^10+(Z(2)^0)*f1^11+(Z(2)^0)*f1
   ↪ ^12+(Z(2)^0)*f1^14
```

W przetłumaczeniu na bardziej przejrzystą postać idempotenty wyznaczone przez GAP są następujące:

$$\begin{aligned}
\mathbf{e}_0 &= 1+x+x^2+x^3+\ldots+x^{16},\\
\mathbf{e}_1 &= x+x^2+x^4+x^8+x^9+x^{13}+x^{15}+x^{16},\\
\mathbf{e}_2 &= x^3+x^5+x^6+x^7+x^{10}+x^{11}+x^{12}+x^{14},
\end{aligned}$$

Podany rozkład algebry jest szczególnym przypadkiem sytuacji ogólnej.

Przykład 1.4. Niech G będzie grupą dihedralną rzędu $2r$, gdzie r jest liczbą pierwszą:

$$G = \langle x,y |\ x^r = 1,\ y^2 = 1,\ yxy = x^{-1}\rangle. \tag{1.1.12}$$

Załóżmy, że $p \nmid 2r$, gdzie $p = \mathrm{char}\mathbb{F}$. Niech także $|\mathbb{F}(\omega) : \mathbb{F}| = k$. Niech najpierw $k = r-1$. Wówczas idempotenty algebry $\mathbb{F}[\langle x\rangle]$ opisane wzorami (1.1.6) są przemienne z y i tym samym algebra $\mathbb{F}[G]$ rozpada się na sumę prostą

$$\mathbb{F}[G] = \mathbf{e}_0\mathbb{F}[G] \oplus \mathbf{e}_1\mathbb{F}[G].$$

Pierwsza składowa ma wymiar dwa, bo jest rozpięta nad $\mathbb{F}$ na zbiorze $\{\mathbf{e}_0,\ \mathbf{e}_0 y\}$ i rozpada się na sumę prostą jednowymiarowych składowych.

$$\mathbf{e}_0\mathbb{F}[G] = \mathbf{f}_{00}\mathbb{F}[G] \oplus \mathbf{f}_{01}\mathbb{F}[G],$$

gdzie $\mathbf{f}_{00} = \mathbf{e}_0 \cdot \frac{1+y}{2}$ i $\mathbf{f}_{01} = \mathbf{e}_0 \cdot \frac{1-y}{2}$.

Druga składowa zawiera $\frac{r-1}{2}$-wymiarowe centrum rozpięte na zbiorze $\{\mathbf{e}_1 \cdot \frac{x^i+x^{-i}}{2} : i = 1,2,\ldots,\frac{r-1}{2}\}$ i można dowieść, że jest ono izomorficzne z ciałem $\mathbb{F}(\omega+\omega^{-1})$, którego stopień rozszerzenia nad $\mathbb{F}$ jest równy $\frac{r-1}{2}$. Z tego faktu, na podstawie twierdzenia 1.2, wynika, że

$$\mathbf{e}_1\mathbb{F}[G] \cong M_2\left(\mathbb{F}\left(\omega+\omega^{-1}\right)\right).$$

Załóżmy teraz, że $k = 1$. Wówczas idempotenty zdefiniowane wzorami (1.1.8) nie są centralnymi idempotentami w $\mathbb{F}[G]$, ale są nimi elementy:

$$\mathbf{f}_1 = \mathbf{e}_1 + \mathbf{e}_{r-1},\ \mathbf{f}_2 = \mathbf{e}_2 + \mathbf{e}_{r-2},\ldots,\ \mathbf{f}_{(r-1)/2} = \mathbf{e}_{(r-1)/2} + \mathbf{e}_{(r+1)/2}.$$

Ponadto, każda z podalgebr $\mathbf{f}_i\mathbb{F}[G]$ jest izomorficzna z algebrą macierzy $M_2(\mathbb{F})$. Mamy zatem:

$$\mathbb{F}[G] \cong \mathbb{F} \oplus \mathbb{F} \oplus \underbrace{M_2(\mathbb{F}) \oplus \ldots \oplus M_2(\mathbb{F})}_{(r-1)/2}.$$

Przykład 1.5. Niech $G = A_4$ będzie grupą permutacji parzystych stopnia 4. Można ją opisać w następujący sposób:

$$G = \langle x_1, x_2, y |\ x_1^2 = x_2^2 = 1,\ x_1x_2 = x_2x_1,\ y^3 = 1,\ yx_1y^{-1} = x_2,\ yx_2y^{-1} = x_1x_2\rangle.$$

Załóżmy najpierw, że ciało $\mathbb{F}$ zawiera pierwiastek pierwotny ω trzeciego stopnia z 1. Wtedy elementy:

$$\begin{aligned}
\mathbf{e}_0 &= \tfrac{(1+x_1+x_2+x_1x_2)(1+y+y^2)}{12},\\
\mathbf{e}_1 &= \tfrac{(1+x_1+x_2+x_1x_2)(1+\omega y+\omega^2y^2)}{12},\\
\mathbf{e}_2 &= \tfrac{(1+x_1+x_2+x_1x_2)(1+\omega^2 y+\omega y^2)}{12},
\end{aligned}$$

wyznaczają trzy jednowymiarowe składowe z rozkładu $\mathbb{F}[G]$, a zatem składowe izomorficzne z ciałem $\mathbb{F}$. Grupa A_4 ma dokładnie 4 klasy elementów sprzężonych, zatem oprócz wymienionych jest jeszcze jedna składowa, której wymiar na $\mathbb{F}$ wynosi 9. Na podstawie twierdzenia 1.2, jest to zatem składowa izomorficzna z $M_3(\mathbb{F})$. Idempotent, który tę składową generuje, może być wyznaczony ze wzoru

$$\mathbf{f} = 1 - (\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3).$$

Jeżeli ciało $\mathbb{F}$ nie zawiera pierwiastka trzeciego stopnia z 1, to algebra $\mathbb{F}[G]$ rozkłada się na sumę trzech składowych, które są wyznaczone przez idempotenty:

$$\mathbf{e}_0, \mathbf{e}_1 + \mathbf{e}_2 = \frac{(1+x_1+x_2+x_1x_2)\left(2-y-y^2\right)}{12}, \mathbf{f}.$$

Przykład 1.6. Na koniec zilustrujemy przypadek, gdy char$\mathbb{F}=2$ i G jest grupą nieparzystego rzędu. Najmniejszą nieabelową grupą rzędu nieparzystego jest grupa rzędu 21 postaci:

$$G=\langle x,y|\ x^7=1,\ y^3=1,\ y^{-1}xy=x^2\rangle. \tag{1.1.13}$$

Załóżmy najpierw, że ciało $\mathbb{F}$ zawiera pierwiastki z jedynki stopni 3 i 7. Najmniejszym takim ciałem jest $GF(2^6)$, którego jedynymi podciałami są $\mathbb{Z}_2$, $GF(2^2)$ i $GF(2^3)$. Algebra grupowa $\mathbb{F}[G]$ rozkłada się na sumę prostą pięciu ideałów minimalnych, z czego trzy są izomorficzne z ciałem $\mathbb{F}$. Ponieważ suma wymiarów składowych jest równa 21, a pozostałe składowe nie są przemienne, więc stanowią sumę dwóch egzemplarzy algebry $M_3(\mathbb{F})$. Można sprawdzić, że idempotentami wyznaczającymi te składowe są:

$$\begin{aligned}
\mathbf{e}_1 &= (1+y+y^2)(1+x+x^2+x^3+x^4+x^5+x^6),\\
\mathbf{e}_2 &= (1+\omega y+\omega^2 y^2)(1+x+x^2+x^3+x^4+x^5+x^6),\\
\mathbf{e}_3 &= (1+\omega^2 y+\omega y^2)(1+x+x^2+x^3+x^4+x^5+x^6),\\
\mathbf{e}_4 &= 1+x+x^2+x^4,\\
\mathbf{e}_5 &= 1+x^3+x^5+x^6,
\end{aligned}$$

gdzie ω jest pierwiastkiem trzeciego stopnia z 1. Zauważmy dalej, że elementy $\mathbf{e}_1$, $\mathbf{e}_4$ i $\mathbf{e}_5$ niezależnie od tego, jakim ciałem jest $\mathbb{F}$, są idempotentami algebry $\mathbb{F}[G]$. To oznacza, że oprócz sytuacji opisanej wyżej mamy taką, gdy ciało $\mathbb{F}$ nie zawiera pierwiastka trzeciego stopnia z 1 i wtedy idempotenty

$$\mathbf{e}_1, \mathbf{e}_2+\mathbf{e}_3,\ \mathbf{e}_4,\ \mathbf{e}_5$$

wyznaczają cztery składowe sumy prostej, którymi są kolejno $\mathbb{F}$, $\mathbb{F}(\omega)$, a dwa ostatnie są izomorficzne z $M_3(\mathbb{F})$. Potwierdzają to rachunki wykonane w GAP.

```
gap> G := OneSmallGroup( 21, IsAbelian, false );;;
gap> F := GF(2);;
gap> FG := GroupRing(F, G);;
gap> FGe :=
   ↪ PrimitiveCentralIdempotentsByCharacterTable(FG);
(Z(2)^0)*<identity> of ...+(Z(2)^0)*f1+(Z(2)^0)*f2+(Z
   ↪ (2)^0)*f1^2+(Z(2)^0)*f1*f2+(Z(2)^0)*f2^2+(Z(2)
   ↪ ^0)*f1^2*f2+(Z(2)^0)*f1*f2^2+(Z(2)^0)*f2^3+(Z(2)
   ↪ ^0)*f1^2*f2^2+(Z(2)^0)*f1*f2^3+(Z(2)^0)*f2^4+(Z
   ↪ (2)^0)*f1^2*f2^3+(Z(2)^0)*f1*f2^4+(Z(2)^0)*f2
   ↪ ^5+(Z(2)^0)*f1^2*f2^4+(Z(2)^0)*f1*f2^5+(Z(2)^0)*
   ↪ f2^6+(Z(2)^0)*f1^2*f2^5+(Z(2)^0)*f1*f2^6+(Z(2)
   ↪ ^0)*f1^2*f2^6
(Z(2)^0)*f1+(Z(2)^0)*f1^2+(Z(2)^0)*f1*f2+(Z(2)^0)*f1
   ↪ ^2*f2+(Z(2)^0)*f1*f2^2+(Z(2)^0)*f1^2*f2^2+(Z(2)
   ↪ ^0)*f1*f2^3+(Z(2)^0)*f1^2*f2^3+(Z(2)^0)*f1*f2
```

```
    ↪ ^4+(Z(2)^0)*f1^2*f2^4+(Z(2)^0)*f1*f2^5+(Z(2)^0)*
    ↪ f1^2*f2^5+(Z(2)^0)*f1*f2^6+(Z(2)^0)*f1^2*f2^6
(Z(2)^0)*<identity> of ...+(Z(2)^0)*f2^3+(Z(2)^0)*f2
    ↪ ^5+(Z(2)^0)*f2^6
(Z(2)^0)*<identity> of ...+(Z(2)^0)*f2+(Z(2)^0)*f2^2+(
    ↪ Z(2)^0)*f2^4
```

Kolejne idempotenty wskazane w powyższej tabeli są następujące:

$$\begin{aligned}
\mathbf{e}_0 &= (1+y+y^2)(1+x+x^2+x^3+x^4+x^5+x^6) = \mathbf{f}_1,\\
\mathbf{e}_2+\mathbf{e}_3 &= (y+y^2)(1+x+x^2+x^3+x^4+x^5+x^6) \quad = \mathbf{f}_2,\\
\mathbf{e}_4 &= 1+x^3+x^5+x^6 \quad = \mathbf{f}_3,\\
\mathbf{e}_5 &= 1+x+x^2+x^4 \quad = \mathbf{f}_4.
\end{aligned}$$

Wśród wszystkich ideałów algebry grupowej $\mathbb{F}[G]$, na szczególną uwagę zasługuje ideał augmentacyjny, który będziemy oznaczać symbolem $A(\mathbb{F}[G])$. Ideał augmentacyjny $A(\mathbb{F}[G])$ jest jądrem homomorfizmu $\phi : \mathbb{F}[G] \to \mathbb{F}$:

$$\phi(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g.$$

Zauważamy, że jeśli tylko $\alpha = \sum_{g\in G} a_g g$ oraz $\phi(\alpha) = 0$, to:

$$\phi(\alpha) = \sum_{g\in G} a_g = 0,$$

$$\alpha = \sum_{g\in G} a_g g - \sum_{g\in G} a_g = \sum_{g\in G} a_g (g-1).$$

Z powyższego, wszystkie elementy postaci $g-1$ należą do $\ker\phi$, a zatem ideał augmentacyjny algebry grupowej generowany jest przez wszystkie elementy postaci $g-1$, gdzie $g \in G$:

$$A(\mathbb{F}[G]) = \langle g-1 :\ g\in G\rangle = \sum_{g\in G}(g-1)\mathbb{F}[G] = \{\sum_{g\in G} a_g g \in \mathbb{F}[G] :\ \sum_{g\in G} a_g = 0\}.$$

Zauważmy jeszcze, że algebra ilorazowa $\mathbb{F}[G]/A(\mathbb{F}[G])$ jest izomorficzna z ciałem $\mathbb{F}$.

W przypadku, gdy char$\mathbb{F}$ nie dzieli $|G|$, ideał augmentacyjny, jak każdy ideał algebry $\mathbb{F}[G]$, jest generowany przez idempotent tej algebry. Niech zatem:

$$\mathbf{e}_0 = \frac{\sum_{g\in G} g}{|G|}.$$

Wówczas, jak wiemy, $\mathbf{e}_0\mathbb{F}[G] \cong \mathbb{F}$. Ponadto, dla dowolnego $g \in G$ mamy

$$\mathbf{e}_0 (g-1) = 0,$$

co oznacza, że

$$\mathbb{F}[G] = e_0\mathbb{F}[G] \oplus A(\mathbb{F}[G]),$$

a stąd

$$A(\mathbb{F}[G]) = (1-e_0)\mathbb{F}[G].$$

Jeśli $G = \langle x : \ x^n = e \rangle$ jest grupą cykliczną rzędu n, to:

$$A(\mathbb{F}[G]) = (x-1)\mathbb{F}[G], \tag{1.1.14}$$

tzn. jest ideałem głównym generowanym przez element $x-1$, bowiem każdy element $g \in G$ ma postać x^i, $i = 0, 1, \ldots, n-1$, a zatem

$$(g-1)\mathbb{F}[G] = (x^i-1)\mathbb{F}[G] = (x-1)(x^{i-1}+\ldots+x+1)\mathbb{F}[G] \subseteq (x-1)\mathbb{F}[G].$$

Stąd

$$A(\mathbb{F}[G]) = \sum_{g\in G} (g-1)\mathbb{F}[G] \subseteq (x-1)\mathbb{F}[G].$$

Równość (1.1.14) domyka inkluzja w stronę przeciwną, która wydaje się oczywista.

Jeżeli charakterystyka ciała $\mathbb{F}$ jest równa p, zaś G jest skończoną p-grupą, tzn. $|G| = p^k$, dla pewnej liczby całkowitej k, to $\mathscr{A} = A(\mathbb{F}[G])$ jest ideałem największym algebry $\mathbb{F}[G]$, tzn. każdy ideał tej algebry jest zawarty w jej ideale augmentacyjnym. Ponadto ideał ten jest nilpotentny, tzn. istnieje liczba naturalna m, taka że iloczyn dowolnych m elementów ideału augmentacyjnego jest równy zero. Ten fakt z jednej strony oznacza ogromną różnorodność ideałów zawartych w $\mathscr{A}$ i tym samym duży rezerwuar kodów, z drugiej jednak, skomplikowana struktura tego ideału wymusza dużą pracochłonność opisu tych kodów/ideałów. By nieco przybliżyć tę strukturę rozważmy dwa przypadki grup abelowych, w pewnym sensie skrajnych z punktu widzenia ich struktury. Niech najpierw $G = \langle x : \ x^{p^n} = 1 \rangle$ będzie grupą cykliczną rzędu p^n. Wówczas, oprócz standardowej bazy algebry $\mathbb{F}[G]$, złożonej z elementów grupy G mamy bazę złożoną z potęg elementu $(x-1)$:

$$1,\ (x-1),\ (x-1)^2,\ \ldots,\ (x-1)^{p^n-1}.$$

Zaletą tej bazy jest to, że jej kolejne elementy generują wszystkie ideały. Są one potęgami ideału augmentacyjnego:

$$\mathbb{F}[G] \supset (x-1)\mathbb{F}[G] \supset (x-1)^2\mathbb{F}[G] \supset \ldots \supset (x-1)^{p^n-1}\mathbb{F}[G] \supset \{0\},$$

przy czym ilorazy dwóch kolejnych są jednowymiarowe.

Inną, bardziej skomplikowaną sytuację mamy w przypadku elementarnej abelowej p-grupy. Niech zatem G będzie taką grupą, tzn.

$$G = \langle x_1, x_2, \ldots, x_k : \ x_i^p = e, \ x_i x_j = x_j x_i, \ i, j \in \{1, 2, \ldots, k\} \rangle.$$

Dla dowolnych $\alpha, \beta \in \mathbb{F}[G]$ zachodzi równość

$$\alpha\beta - 1 = (\alpha - 1)(\beta - 1) + (\alpha - 1) + (\beta - 1), \tag{1.1.15}$$

a każdy element grupy G ma postać $g = x_1^{m_1} x_2^{m_2} \ldots x_k^{m_k}$, $0 \leq m_j < p$. Zatem wielokrotnie korzystając z tej tożsamości, dowolny element ideału $\mathscr{A}$ możemy przedstawić w postaci kombinacji liniowej elementów:

$$(x_1 - 1)^{m_1} (x_2 - 1)^{m_2} \ldots (x_k - 1)^{m_k}, \ \ 0 \leq m_j < p. \tag{1.1.16}$$

Wynika stąd w szczególności, że dla dowolnego $\alpha \in \mathscr{A}$ mamy $\alpha^p = 0$, co oznacza między innymi, że 0 jest jedynym idempotentem w $\mathscr{A}$. Łatwą indukcją można również dowieść, że ideał $\mathscr{A}^m$ jest rozpięty na elementach postaci (1.1.16), dla których zachodzi nierówność $m_1 + m_2 + \ldots + m_k \geq m$. Przy maksymalnych wartościach wszystkich m_j (równych $p-1$) dostajemy element $(x_1 - 1)^{p-1}(x_2 - 1)^{p-1} \ldots (x_k - 1)^{p-1} = \sum_{x \in G} x$. Oznacza to po pierwsze, że $\mathscr{A}^{m(p-1)}$ jest rozpięty na tym elemencie, czyli ma wymiar 1, a po drugie, wobec faktu iż ten element anihiluje $\mathscr{A}$, dostajemy równość

$$\mathscr{A}^{m(p-1)+1} = 0.$$

Można także dowieść, że anihilatorem ideału $\mathscr{A}^j$ jest ideał $\mathscr{A}^i$, gdzie $i = m(p-1) + 1 - j$. Wyczerpujący opis najważniejszych własności ideału $\mathscr{A}$ można znaleźć w monografiach Passman (1977) i Sehgal (1978).

1.2 Kody i ich realizacja z pomocą algebr grupowych

Dla celów tworzenia kodów będziemy interpretować zbiór $\mathbb{F}_q$, z zachowaniem własności przedstawionych w powyższym rozdziale, jako alfabet, którego symbole posłużą do zapisania dowolnej informacji. Jednostkami informacji są ciągi elementów ciała $\mathbb{F}_q$, o ustalonej długości $m \in \mathbb{N}$. Zbiór wszystkich jednostek informacji można więc utożsamiać z przestrzenią liniową $\mathbb{F}_q^m$. Do kodowania informacji posłuży przestrzeń $\mathbb{F}_q^n$, gdzie $n > m$. Dowolna podprzestrzeń $\mathscr{C}$ wymiaru m tej przestrzeni nazywamy kodem długości n. Elementy podprzestrzeni $\mathscr{C}$ nazywamy słowami kodowymi. Macierz różnowartościowego przekształcenia liniowego $\psi : \mathbb{F}_q^m \to C$ z przestrzeni informacji $\mathbb{F}_q^m$ na kod $\mathscr{C} \subseteq \mathbb{F}_q^n$ nazywamy macierzą generującą.

Niech $\mathscr{C} \subset \mathbb{F}_q^n$ będzie kodem. Kod $\mathscr{C}$ nazwiemy liniowym, jeśli, jak wyżej, możemy przedstawić go w postaci podprzestrzeni liniowej $\mathbb{F}_q^m \subseteq \mathbb{F}_q^n$.

Niech $C_0, C_1 \in \mathscr{C}$ będą słowami kodowymi. Odległością Hamminga między słowami kodowymi C_0 i C_1 nazwiemy liczbę współrzędnych, na których C_0 różni się od C_1 i oznaczać będziemy przez $\mathrm{d}(C_0, C_1)$. Łatwo wykazać, że odległość Hamminga jest metryką na $\mathscr{C}$.

Wagą Hamminga słowa kodowego C nazwiemy liczbę niezerowych współrzędnych w tym słowie i oznaczać będziemy przez $\mathrm{wt}(C)$. Formalnie, wagę Hamminga słowa kodowego definiować można również jako odległość Hamminga tego słowa od wektora zerowego. W dalszej części pracy pisać będziemy skrótowo – odległość oraz waga.

Odległością minimalną $\mathrm{d}(\mathscr{C})$ kodu $\mathscr{C}$ nazwiemy minimalną odległość Hamminga między dwoma różnymi słowami kodowymi lub równoważnie, minimalną wagę niezerowego słowa kodowego.

Twierdzenie 1.4. Niech dany będzie liniowy kod $\mathscr{C}$; niech $\mathrm{d}(\mathscr{C}) = d$, wtedy:

(i) Liniowy kod $\mathscr{C}$ może wykrywać $d-1$ błędów.
(ii) Liniowy kod $\mathscr{C}$ może korygować κ błędów, gdzie κ dane jest wzorem

$$\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Kod liniowy $\mathscr{C}$ długości n, wymiaru k oraz średnicy d nazywany jest (n,k,d)-kodem.

Szczególnym przypadkiem kodów liniowych są kody cykliczne. Powiemy, że liniowy kod $\mathscr{C}$ jest kodem cyklicznym jeśli dla dowolnego słowa kodowego $C_0 = (c_1, c_2, \ldots, c_{n-1}, c_n)$, słowo $C_1 = (c_n, c_1, \ldots, c_{n-2}, c_{n-1})$ także jest słowem kodowym. Innymi słowy, jeśli $G = C_n = \langle g \mid g^n = 1 \rangle$ jest grupą cykliczną rzędu n, której działanie na $\mathbb{F}_q^n$ jest realizowane przez operację mnożenia przez macierz

$$M_g = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix},$$

to kod $\mathscr{C}$ jest cykliczny, jeśli z faktu, że $v \in \mathscr{C}$ jest słowem kodowym, wynika, że $gv \in \mathscr{C}$ również jest słowem kodowym:

$$v \in \mathscr{C} \implies gv \in \mathscr{C}.$$

W poniższych przykładach podamy realizacje wybranych kodów cyklicznych w postaci ideałów algebr grupowych.

Przykład 1.7. Jednym z najmniej skomplikowanych kodów cyklicznych jest kod binarny długości n i wymiaru $n-1$, którego słowa kodowe zawierają cyfrę kontroli parzystości (powiedzmy, że jest to pierwsza współrzędna słowa kodowego). Niech $n>1$ będzie ustaloną liczbą nieparzystą i $\mathbb{F}=GF(2)=\mathbb{Z}_2$. Nasz kod można określić w następujący sposób:

$$\mathscr{C}=\left\{(c_0,c_1,\ldots,c_{n-1})\in\mathbb{F}^n:\ \sum_{i=0}^{n-1}c_i=0\right\}.$$

Zgodnie z obserwacjami poczynionymi w końcu poprzedniego rozdziału, ideał augmentacyjny algebry $\mathbb{F}[G]$ składa się ze wszystkich elementów postaci: $a_0+a_1x+a_2x^2+\ldots+a_{n-1}x^{n-1}$, takich że $a_0+a_1+a_2+\ldots+a_{n-1}=0$. Jeśli zatem $\varphi\colon\mathbb{F}[G]\to\mathbb{F}^n$ jest wzajemnie jednoznacznym odwzorowaniem określonym wzorem:

$$\varphi\left(\sum_{i=0}^{n-1}a_ix^i\right)=(a_0,a_1,\ldots,a_n),$$

to $\varphi(A(\mathbb{F}[G]))=\mathscr{C}$.

Ideał augmentacyjny algebry grupowej grupy cyklicznej generowanej przez element x jest ideałem głównym generowanym przez element $x-1$. Jego anihilatorem jest ideał generowany przez element

$$\varepsilon=1+x+x^2+\ldots+x^{n-1},$$

a zatem może służyć do algebraicznego testowania, czy dany element algebry grupowej należy do $\mathbb{A}(\mathbb{F}[G])$ (czy jest słowem kodowym):

$$\alpha\in A(G)\Leftrightarrow\alpha\cdot\varepsilon=0.$$

Zamieńmy teraz rolami elementy ε i $(x-1)$: niech kodem będzie ideał generowany przez ε, a $x-1$ posłuży nam do algebraicznego testowania, jaki element jest słowem kodowym. Bezpośrednio z postaci ε wynika, że jest to przestrzeń jednowymiarowa, której elementami są 0 i ε, co przy innym zapisie odpowiada kodowi powtórzeniowemu oznaczanemu symbolem $(n,2,n)$, czyli kodowi

$$\mathscr{C}=\{(\underbrace{0,0,\ldots,0}_{n}),\ (\underbrace{1,1,\ldots,1}_{n})\}.$$

Pójdźmy dalej, niech H będzie podgrupą grupy G rzędu k, $n=km$, generowaną przez element $y=x^m$ i niech

$$\eta=1+y+y^2+\ldots+y^{k-1}=\sum_{h\in H}h.$$

Niech ponadto T będzie zbiorem reprezentantów warstw grupy G względem H. Wówczas zbiór

$$I = \{\eta t \mid t \in T\}$$

jest bazą ideału $\eta\mathbb{F}[G]$ jako przestrzeni liniowej nad $\mathbb{F}$. Łatwo dostrzec, że wszystkie elementy ideału I są postaci

$$\alpha = \sum_{t\in T} a_t t\eta,$$

co oznacza, że gdyby zapisać je w standardowej bazie G nad $\mathbb{F}$, to wszystkie współczynniki przy elementach postaci th, dla ustalonego $t \in T$ i dowolnego $h \in H$ byłyby takie same, a kod jest algebro-grupową realizacją kodu powtórzeniowego, zdefiniowanego następująco:

Niech $W = \mathbb{F}^k$ i $V = \mathbb{F}^{km} = W^m$, wówczas przez (k,m)-powtórzeniowy kod rozumiemy podprzestrzeń, której elementami są ciągi

$$(\underbrace{w,w,\ldots,w}_{m}) \text{ , gdzie } w \in W.$$

Dla ilustracji ostatniego stwierdzenia rozważmy przykład grupy G rzędu $n = 9$ i podgrupy H rzędu $k = 3$ ($k = 3 = m$). Niech przy tym $T = 1,x,x^2$. Jeśli $\alpha = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + a_6x^6 + a_7x^7 + a_8x^8 \in \mathbb{F}G$ jest dowolnym elementem algebry (który odpowiada wektorowi $(a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8) \in \mathbb{F}^9$), to wobec równości

$$\begin{aligned}
\eta = x^3\eta = x^6\eta &= 1 + x^3 + x^6 \leftrightarrow (1,0,0,1,0,0,1,0,0)\\
x\eta = x^4\eta = x^7\eta &= x + x^4 + x^7 \leftrightarrow (0,1,0,0,1,0,0,1,0)\\
x^2 = x^5\eta = x^8\eta &= x^2 + x^5 + x^8 \leftrightarrow (0,0,1,0,0,1,0,0,1)
\end{aligned}$$

otrzymujemy postać dowolnego elementu ideału $\eta\mathbb{F}[G]$

$$\eta\alpha = (a_0 + a_3 + a_6)\eta + (a_1 + a_4 + a_7)x\eta + (a_2 + a_5 + a_8)x^2\eta,$$

który przy podstawieniu $b_0 = a_0 + a_3 + a_6$, $b_1 = a_1 + a_4 + a_7$, $b_2 = a_2 + a_5 + a_8$ odpowiada wektorowi $(b_0,b_1,b_2,b_0,b_1,b_2,b_0,b_1,b_2)$, ten zaś możemy zapisać w postaci (w,w,w) dla $w = (b_0,b_1,b_2) \in \mathbb{F}^3$.

Powyższe rozumowanie można przenieść na ogólny przypadek, gdy $\mathbb{F}$ jest dowolnym ciałem skończonym, G jest dowolną grupą skończoną, zaś H – jej podgrupą normalną. Wtedy przyjmujemy, że $\eta = \sum_{h\in H} h$ i gdy charakterystyka ciała nie dzieli $|G|$ możemy η zastąpić idempotentem $\mathbf{e} = \frac{\eta}{|H|}$. To pozwala na uzyskanie łatwego kryterium rozpoznawania słów kodowych: $\alpha \in \mathbb{F}[G]$ jest słowem kodowym wtedy i tylko wtedy $\alpha(1-\mathbf{e}) = 0$.

W następnych przykładach, odnosząc się czasem do przykładów omówionych w poprzednim rozdziale, przedstawimy kody zrealizowane w tam wskazanych algebrach grupowych z pomocą programu GAP. Na potrzeby skrócenia pracy, część kodu, która w sposób naturalny powtarza się między kolejnymi przykładami zastąpiono `[...]`.

Przykład 1.8. Zaczniemy od algebry grupowej grupy cyklicznej rzędu 17 opisanej w przykładzie 1.3. W poniższych przykładach konstruujemy algebrę grupową, a następnie z kolejnych centralnych prymitywnych idempotentów oraz ich sum, tworzymy lewostronne ideały w tej algebrze, na podstawie których generujemy kolejne kody.

```
gap> G := CyclicGroup(17);; S := AsSet(G);;
gap> F := GF(2);;;
gap> FG := GroupRing(F, G);
<algebra-with-one over GF(2), with 1 generators>
gap>
```

```
gap> I := LeftIdealByGenerators(FG,[FGe[1]]);;
gap> V := VectorSpace(F,CodeByLeftIdeal(F,G,S,I));;
gap> B := Basis(V);;
gap> C1 := GeneratorMatCode(B,F);
a linear [17,1,17]8 code defined by generator matrix
   ↪ over GF(2)
gap>
```

```
gap> I := LeftIdealByGenerators(FG,[FGe[2]]);;
[...]
gap> C2 := GeneratorMatCode(B,F);
a linear [17,8,1..6]3..7 code defined by generator
   ↪ matrix over GF(2)
gap>
```

Zauważamy, że kod $\mathscr{C}_1$ jest kodem powtórzeniowym, natomiast kod $\mathscr{C}_2$ jest kodem cyklicznym; kod wygenerowany przez ostatni z idempotentów - $\mathscr{C}_3$ jest kodem tożsamym z $\mathscr{C}_2$.

Kody powstałe jako ideał generowany przez sumę idempotentów, to znaczy – kod $\mathscr{C}_{12}$ dany jest jako suma idempotentów $\mathbf{e}_1, \mathbf{e}_2$ dane są jak niżej.

```
gap> I := LeftIdealByGenerators(FG,[FGe[1] + FGe[2]])
   ↪ ;;
[...]
gap> C12 := GeneratorMatCode(B,F);
a linear [17,9,1..5]3..4 code defined by generator
   ↪ matrix over GF(2)
gap>
```

```
gap> I := LeftIdealByGenerators(FG,[FGe[1] + FGe[3]])
   ↪ ;;
[...]
gap> C13 := GeneratorMatCode(B,F);
a linear [17,9,1..5]3..4 code defined by generator
   ↪ matrix over GF(2)
gap>
```

```
gap> I := LeftIdealByGenerators(FG,[FGe[2] + FGe[3]])
   ↪ ;;
[...]
gap> C23 := GeneratorMatCode(B,F);
a linear [17,16,1..2]1 code defined by generator
   ↪ matrix over GF(2)
gap>
```

Wagi oraz wymiary powyższych kodów to odpowiednio

```
gap> List([C1, C2, C3, C12, C13, C23], MinimumWeight);
[ 17, 6, 6, 5, 5, 2 ]
gap>
```

```
gap> List([C1, C2, C3, C12, C13, C23], Dimension);
[ 1, 8, 8, 9, 9, 16 ]
gap>
```

Niech $\mathscr{C}$ będzie dowolnym kodem cyklicznym długości n nad ciałem $\mathbb{F}$. Bezpośrednio z definicji wynika, że jako przestrzeń liniowa, $\mathscr{C}$ jest G-modułem, gdzie $G = \langle x : x^n = e \rangle$, co oznacza, że jest określone naturalne mnożenie elementów z $\mathscr{C}$ przez elementy z algebry grupowej $\mathbb{F}[G]$, jak swego rodzaju uogólnione skalary. Jeżeli $\mathrm{char}\,\mathbb{F}$ nie dzieli rzędu grupy, to $\mathbb{F}[G]$ jest algebrą półprostą (patrz [1.2,1.3]), co z kolei oznacza, że każdy G-moduł jest sumą prostą podmodułów prostych, te zaś są izomorficzne z minimalnymi ideałami algebry $\mathbb{F}[G]$, jako modułami nad $\mathbb{F}[G]$. Podsumowując, każdy kod cykliczny można zrealizować jako sumę prostą kodów, z których każdy jest izomorficzny (jako G-moduł) z ideałem minimalnym algebry $\mathbb{F}[G]$.

Przykład 1.9. Pokażemy teraz konstrukcję kodu na podstawie przykładu 1.6. Skonstruujmy algebrę grupową nad ciałem charakterystyki dwa oraz jedyną nieabelową grupą rzędu 21, a następnie weźmy układ centralnych prymitywnych idempotentów tej algebry (patrz przykład 1.6).

Kolejno, utworzymy kody $\mathscr{C}_1, \mathscr{C}_2, \mathscr{C}_3, \mathscr{C}_4$, które odpowiadają lewostronnym ideałom w tej algebrze generowanym przez idempotenty $\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_3, \mathbf{f}_4$.

```
gap> I := LeftIdealByGenerators(FG,[FGe[1]]);;
gap> V := VectorSpace(F,CodeByLeftIdeal(F,G,S,I));;
gap> B := Basis(V);;
gap> C1 := GeneratorMatCode(B,F);
a linear [21,1,21]10 code defined by generator matrix
   ↪ over GF(2)
gap>
```

```
gap> I := LeftIdealByGenerators(FG,[FGe[3]]);;
gap> V := VectorSpace(F,CodeByLeftIdeal(F,G,S,I));;
gap> B := Basis(V);;
gap> C3 := GeneratorMatCode(B,F);
a linear [21,9,1..4]4..10 code defined by generator
   ↪ matrix over GF(2)
gap>
```

Kody $\mathscr{C}_2, \mathscr{C}_4$, które utworzone zostały z idempotentów $\mathbf{f}_2, \mathbf{f}_4$, są równoważne kodom $\mathscr{C}_1, \mathscr{C}_3$ odpowiednio.

```
gap> IsEquivalent(C1, C2);
true
gap> IsEquivalent(C3, C4);
true
gap> IsEquivalent(C1, C3);
false
gap>
```

Zatem wystarczy tylko podać opis kodów $\mathscr{C}_1$ i $\mathscr{C}_3$. W szczególności, minimalne wagi Hamminga dla obu kodów przedstawiają się następująco:

```
gap> MinimumWeight(C1);
14
gap> MinimumWeight(C3);
4
gap>
```

Następny przykład jest ilustracją realizacji kodu niecyklicznego za pomocą algebry grupowej elementarnej grupy abelowej rzędu 8 nad ciałem $\mathbb{F}_8$ (Wolfmann (1991)). Mamy tu do czynienia z sytuacją, gdy charakterystyka ciała dzieli rząd grupy. Jak wiemy, struktura tych algebr jest opisana w znacznie mniej wyczerpującym stopniu.

Przykład 1.10. Rozważmy rozszerzony kod Golay'a, binarny kod o wymiarze 12, korygujący trzy lub mniej błędów, którym posługiwała się między innymi sonda kosmiczna Voyager, w latach osiemdziesiątych XX w. Za jego pomocą kodowała między innymi zdjęcia przesyłane z kosmosu.

Niech

$$B = \begin{bmatrix} 1&1&0&1&1&1&0&0&0&1&0&1 \\ 1&0&1&1&1&0&0&0&1&0&1&1 \\ 0&1&1&1&0&0&0&1&0&1&1&1 \\ 1&1&1&0&0&0&1&0&1&1&0&1 \\ 1&1&0&0&0&1&0&1&1&0&1&1 \\ 1&0&0&0&1&0&1&1&0&1&1&1 \\ 0&0&0&1&0&1&1&0&1&1&1&1 \\ 0&0&1&0&1&1&0&1&1&1&0&1 \\ 0&1&0&1&1&0&1&1&1&0&0&1 \\ 1&0&1&1&0&1&1&1&0&0&0&1 \\ 0&1&1&0&1&1&1&0&0&0&1&1 \\ 1&1&1&1&1&1&1&1&1&1&1&0 \end{bmatrix}$$

będzie macierzą nad ciałem $\mathbb{F}_2$ i niech $M = [I;B]$ będzie 12×24-macierzą nad tym ciałem, gdzie I jest macierzą jednostkową stopnia 12. Macierz M jest macierzą generującą tego kodu, tzn. przestrzeń informacji W jest 12-wymiarową przestrzenią nad ciałem $\mathbb{F}_2$, a słowa kodowe stanowią podprzestrzeń przestrzeni 24-wymiarowej, które otrzymujemy mnożąc wektory przestrzeni W przez macierz M. Ten kod oznaczymy symbolem $\mathscr{C}_{24}$. W literaturze określa się go również jako kod Golay'a $(24,12,8)$ Wolfmann (1991).

Kod Golay'a ma następujące własności:

1. Kod $\mathscr{C}_{24}$ ma długość 24 wymiar 12 i średnicę 8;
2. Macierzą sprawdzającą kodu jest $[I;B]^T$;
3. Kod $\mathscr{C}_{24}$ koryguje co najwyżej 3 błędy.

Niech $\mathbb{F}_8$ będzie ciałem 8-elementowym. Niech α będzie generatorem multyplikatywnej grupy tego ciała, tzn. $\alpha \neq 1$ i $\alpha^7 = 1$. Stąd:

$$1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6 = 0,$$

a ponieważ

$$1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6 = \left(1 + \alpha + \alpha^3\right)\left(1 + \alpha^2 + \alpha^3\right),$$

więc możemy przyjąć, że $1 + \alpha + \alpha^3 = 0$, tzn. $\alpha^3 = 1 + \alpha$. Pozostałymi pierwiastkami wielomianu $f(x) = 1 + x + x^3 \in \mathbb{F}_2[x]$ są α^2 i α^4.
Istotnie $f(\alpha^2) = (1 + \alpha + \alpha^3)^2 = 0$ i $f(\alpha^4) = (1 + \alpha + \alpha^3)^4 = 0$. Elementy α^3, α^5 i α^6 są pierwiastkami wielomianu $g(x) = 1 + x^2 + x^3 \in \mathbb{F}_2[x]$. Niech teraz G będzie addytywną grupą ciała $\mathbb{F}_8$. Ze względu na dwoistość ról elementów, wprowadzimy dla elementów grupy addytywnej oznaczenia zgodnie z następującym przyporządkowaniem. Dla $\beta \in \mathbb{F}_8$ przez X^β oznaczymy ten sam element β, ale jako element

bazy przestrzeni $\mathbb{F}_8[G]$. Przy czym, addytywne działanie w $\mathbb{F}_8$ zostanie zastąpione działaniem multyplikatywnym zgodnie ze wzorem:

$$X^{\beta}X^{\gamma} = X^{\beta+\gamma}.$$

W szczególności zatem, elementy $X^0 = 1, X^{\alpha}, X^{\alpha^2}, X^{\alpha^4}$ tworzą podgrupę rzędu 4 w grupie G. Rzeczywiście, skoro $1+\alpha = \alpha^3$, więc $\alpha+\alpha^2 = \alpha^4$ i tym samym

$$X^{\alpha}X^{\alpha^2} = X^{\alpha+\alpha^2} = X^{\alpha^4},$$

skąd już łatwo wyprowadzić pozostałe zależności.

Niech teraz

$$y = 1 + X\left(1 + \alpha X^{\alpha} + \alpha^2 X^{\alpha^2} + \alpha^4 X^{\alpha^4}\right).$$

Lemat 1.1. Ideał I algebry $\mathbb{F}_8[G]$ generowany przez element y spełnia następujące warunki:
(i) $I^2 = 0$;
(ii) $\dim_{\mathbb{F}_8} I = 4$.

Dowód. (i) Ponieważ algebra jest przemienna, więc wystarczy zauważyć, że $y^2 = 0$. Istotnie, w ciele $\mathbb{Z}_2$ mamy $1+1=0$, zatem $X^2 = X^{1+1} = X^0 = 1$ i dalej

$$\begin{aligned} y^2 &= (1+X(1+\alpha X^{\alpha}+\alpha^2 X^{\alpha^2}+\alpha^4 X^{\alpha^4}))^2 &&= \\ &= 1^2 + X^2(1^2+\alpha^2 X^{2\alpha}+\alpha^4 X^{2\alpha^2}+\alpha X^{2\alpha^4}) &&= \\ &= \alpha^2+\alpha^4+\alpha = \alpha(1+\alpha+\alpha^3) &&= 0. \end{aligned}$$

(ii) Dowód tej części jest dość kłopotliwy, dlatego wskażemy tylko jego zarys. Korzystając z tego, że grupa G, w zapisie formalnym z wykorzystaniem notacji X^{β}, jest generowana przez elementy $X, X^{\alpha}, X^{\alpha^2}$. Zatem element y można zapisać w postaci

$$\begin{aligned} y &= 1+X+\alpha X^{\alpha+1}+\alpha^2 X^{\alpha^2+1}+\alpha^4 X^{\alpha^4+1} &&= \\ &= 1+X+\alpha X^{\alpha^3}+\alpha^4 X^{\alpha^5}+\alpha^2 X^{\alpha^6} &&= \\ &= (X+1)+\alpha(X\cdot X^{\alpha}+1)+\alpha^4(X\cdot X^{\alpha}\cdot X^{\alpha^2}+1)+\alpha^2(X\cdot X^{\alpha^2}+1). \end{aligned}$$

Następnie korzystając z tożsamości 1.1.15, która dla algebry nad ciałem 2–elementowym przyjmuje postać

$$ab+1 = (a+1)(b+1)+(a+1)+(b+1)$$

oraz jej iteracji

$$\begin{aligned} abc+1 = {} & (a+1)(b+1)(c+1)+(a+1)(b+1)+(a+1)(c+1)+(b+1)(c+1)+ \\ & +(a+1)+(b+1)+(c+1) \end{aligned}$$

dostajemy postać

$$\begin{aligned} y = {} & \alpha^4(X+1)(X^{\alpha}+1)(X^{\alpha^2}+1)+ \\ & + \alpha^2(X+1)(X^{\alpha}+1)+\alpha(X+1)(X^{\alpha^1}+1)+\alpha^4(X^{\alpha}+1)(X^{\alpha^2}+1)+ \\ & + (X+1)+\alpha^2(X^{\alpha}+1)+\alpha(X^{\alpha^2}+1). \end{aligned} \tag{1.2.1}$$

Ideał augmentacyjny $A = A(\mathbb{F}_8[G])$ algebry $\mathbb{F}_8[G]$, który, jak wiadomo, jest jej największym ideałem, jest podprzestrzenią rozpiętą nad $\mathbb{F}_8$ na elementach:

$$\begin{gathered} X+1,\ X^{\alpha}+1,\ X^{\alpha^2}+1, \\ (X+1)(X^{\alpha}+1),\ (X+1)(X^{\alpha^2}+1),\ (X^{\alpha}+1)(X^{\alpha^2}+1), \\ (X+1)(X^{\alpha}+1)(X^{\alpha^2}+1), \end{gathered} \tag{1.2.2}$$

przy czym A^2 jest podprzestrzenią rozpiętą na elementach z drugiego i trzeciego wiersza ostatniej listy (ma więc wymiar 4), natomiast A^3 jest jednowymiarową przestrzenią rozpiętą na elemencie z ostatniego wiersza.

Łatwo teraz zauważyć, że ideał generowany przez y jest rozpięty na elementach:

$$\begin{aligned} & y, \\ & \alpha^2(X+1)(X^{\alpha}+1)+\alpha(X+1)(X^{\alpha^2}+1), \\ & (X+1)(X^{\alpha}+1)+\alpha(X^{\alpha}+1)(X^{\alpha^2}+1), \\ & (X+1)(X^{\alpha^2}+1)+\alpha^2(X^{\alpha}+1)(X^{\alpha^2}+1), \\ & \alpha^4(X+1)(X^{\alpha}+1)(X^{\alpha^2}+1). \end{aligned}$$

Element y jest jedynym elementem, który nie należy do A^2, zatem jest on liniowo niezależny od pozostałych. Ponadto,

$$y(X+1)+\alpha^2 y(X^{\alpha}+1)+\alpha y(X^{\alpha^2}+1) = \alpha^2(X+1)(X^{\alpha}+1)(X^{\alpha^2}+1),$$

co oznacza, że cztery pozostałe elementy są liniowo zależne. Jednocześnie, nietrudno zauważyć, że jeśli pominiemy jeden z nich, drugi, trzeci lub czwarty, pozostałe trzy są liniowo niezależne. To kończy dowód lematu.

Dowód poniższego lematu w części wynika z poprzedniego, w części zaś jest nieskomplikowaną obserwacją, którą możemy przeprowadzić na bazie poprzedniego dowodu.

Lemat 1.2. Anihilatorem ideału I jest ideał I; innymi słowy $I^2 = 0$ oraz dla dowolnego $r \in \mathbb{R}_8[G] - I$ zachodzi nierówność $r \cdot y \neq 0$.

Ciało $\mathbb{F}_8$ jest przestrzenią liniową wymiaru 3 nad ciałem $\mathbb{F}_2 = \{0, 1\}$. Rozważmy bazę tej przestrzeni złożonej z elementów:

$$u_1 = \alpha^3,\ u_2 = \alpha^6,\ u_3 = \alpha^5.$$

Każdy element ciała odpowiada zatem trójwyrazowemu binarnemu ciągowi współczynników kombinacji liniowej dającej dany element:

$$\begin{array}{ll}
0 & \leftrightarrow (0,0,0);\\
1 = u_1 + u_2 + u_3 & \leftrightarrow (1,1,1);\\
\alpha = u_2 + u_3 & \leftrightarrow (0,1,1);\\
\alpha^2 = u_1 + u_3 & \leftrightarrow (1,0,1);\\
\alpha^3 = u_1 & \leftrightarrow (1,0,0);\\
\alpha^4 = u_1 + u_2 & \leftrightarrow (1,1,0);\\
\alpha^5 = u_3 & \leftrightarrow (0,0,1);\\
\alpha^6 = u_2 & \leftrightarrow (0,1,0).
\end{array}$$

Oto kilka przykładowych obliczeń:

$$1 = \alpha^7 = \alpha^4\alpha^3 = \alpha^3\alpha(1+\alpha) = \alpha^3(\alpha+\alpha^2) = \alpha^3(1+\alpha^3+\alpha^2) = \alpha^3+\alpha^6+\alpha^5$$
$$\alpha = 1+\alpha^3 = (\alpha^3+\alpha^6+\alpha^5)+\alpha^3 = \alpha^6+\alpha^5$$

Rozważmy elementy:

$$\begin{aligned}
x_1 &= y = 1+X(1+\alpha X^{\alpha}+\alpha^2 X^{\alpha^2}+\alpha^4 X^{\alpha^4}) = 1+X+\alpha X^{\alpha^3}+\alpha^2 X^{\alpha^6}+\alpha^4 X^{\alpha^5} =\\
&= 1+X+\alpha X^{\alpha^3}+\alpha^4 X^{\alpha^5}+\alpha^2 X^{\alpha^6},\\
x_2 &= X^{\alpha} y = X^{\alpha}+X^{\alpha+1}+\alpha X^{\alpha+\alpha^3}+\alpha^2 X^{\alpha+\alpha^6}+\alpha^4 X^{\alpha+\alpha^5} =\\
&= X^{\alpha}+X^{\alpha^3}+\alpha X+\alpha^2 X^{\alpha^5}+\alpha^4 X^{\alpha^6}\\
&= \alpha X+X^{\alpha}+X^{\alpha^3}+\alpha^2 X^{\alpha^5}+\alpha^4 X^{\alpha^6},\\
x_3 &= X^{\alpha^2} y = X^{\alpha^2}+X^{\alpha^2+1}+\alpha X^{\alpha^2+\alpha^3}+\alpha^2 X^{\alpha^2+\alpha^6}+\alpha^4 X^{\alpha^2+\alpha^5} =\\
&= X^{\alpha^2}+X^{\alpha^6}+\alpha X^{\alpha^5}+\alpha^2 X+\alpha^4 X^{\alpha^3}\\
&= \alpha^2 X+X^{\alpha^2}+\alpha^4 X^{\alpha^3}+\alpha X^{\alpha^5}+X^{\alpha^6},\\
x_4 &= X^{\alpha^4} y = X^{\alpha^4}+X^{\alpha^4+1}+\alpha X^{\alpha^4+\alpha^3}+\alpha^2 X^{\alpha^4+\alpha^6}+\alpha^4 X^{\alpha^4+\alpha^5} =\\
&= \alpha^4 X+\alpha^2 X^{\alpha^3}+X^{\alpha^4}+X^{\alpha^5}+\alpha X^{\alpha^6}.
\end{aligned}$$

Tworzą one bazę ideału I jako przestrzeni liniowej nad ciałem $\mathbb{F}_8$. Ze względu na to, że $\mathbb{F}_8$ jest przestrzenią liniową nad $\mathbb{F} = \mathbb{Z}_2$, można ideał I traktować, jako 12-wymiarową podprzestrzeń algebry $\mathbb{F}[G]$. Nie jest to jednak ideał tej algebry, zatem poza algebraiczną prezentacją oraz możliwością algebraicznego testowania, czy dany element reprezentuje słowo kodowe, nie daje dodatkowych korzyści w postaci alternatywnych algorytmów dekodowania.

W nieco ogólniejszym ujęciu wygląda to następująco: rozważmy podprzestrzeń algebry $\mathbb{F}_8[G]$ z ustaloną bazą $\{v_1, v_2, \ldots, v_k\}$ nad ciałem $\mathbb{F}_8$. Binarnym przekształceniem ze względu na bazę $\{u_1, u_2, u_3\}$ ciała $\mathbb{F}_8$ nad ciałem $\mathbb{F}_2$ nazywamy funkcję, która każdej kombinacji liniowej $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k$ przyporządkowuje ciąg binarny powstały z ciągu $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ przez zastąpienie wyrazów α_i ciągami binarnych współczynników (a_{i1}, a_{i2}, a_{i3}) i opuszczeniu nawiasów, gdzie
$\alpha_i = a_{i1}u_1 + a_{i2}u_2 + a_{i3}u_3$.

Twierdzenie 1.5. Binarny obraz ideału I w przestrzeni $\mathbb{F}_2^{24}$, ze względu na bazę $\{u_1, u_2, u_3\}$ jest $(24, 12, 8)$-kodem Golay'a.

Przykład 1.11. Innym przykładem kodów, które mogą być zrealizowane w języku algebr grupowych jest rodzina kodów Reeda-Mullera zaproponowana przez Mullera w 1954 r. Istnieje wiele sposobów ich opisu, patrz np. Hoffman i in. (1991). Tu przedstawimy standardową definicję opartą na pojęciu funkcji boolowskiej. Jeśli X jest dowolnym ustalonym zbiorem, to przez funkcję boolowską określoną na X rozumiemy dowolną funkcję $f\colon X \to \mathbb{Z}_2$. Każda funkcja boolowska może być utożsamiana z funkcją charakterystyczną podzbioru $A = \{x \in X : \ f(x) = 1\}$.

Niech

$$X_m = \{(a_1, a_2, \ldots, a_m) : \ a_i \in \{0,1\}\} = \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2}_{m}$$

będzie zbiorem wszystkich ciągów binarnych długości m. Jest jasne, że $|X_m| = 2^m$. Rozważmy zbiór wszystkich funkcji boolowskich określonych na zbiorze X_m. Ma on 2^{2^m} elementów i można go w naturalny sposób traktować, jako algebrę nad ciałem $\mathbb{F} = \mathbb{Z}_2$

$$\mathbb{A}_m = \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2}_{2^m}.$$

z naturalnymi operacjami dodawania i mnożenia oraz mnożenia przez skalary. Przestawimy konstrukcję kodów Reeda-Mullera jako podprzestrzeni tej przestrzeni. Niech $T_1,\ T_2,\ \ldots, T_m$ będą przemiennymi zmiennymi. Aby wskazać te podprzestrzenie wprowadźmy najpierw przyporządkowanie

$$\begin{aligned}
T_0 &\leftrightarrow (1,1,1,1,1,1,1,1,\ldots,1,1,1,1) = t_0\\
T_1 &\leftrightarrow (0,1,0,1,0,1,0,1,\ldots,0,1,0,1) = t_1\\
T_2 &\leftrightarrow (0,0,1,1,0,0,1,1,\ldots,0,0,1,1) = t_2\\
&\ldots\ldots\ldots\ldots\\
T_{m-1} &\leftrightarrow (\underbrace{0,0,\ldots,0}_{2^{m-2}},\underbrace{1,1,\ldots,1}_{2^{m-2}},\underbrace{0,0,\ldots,0}_{2^{m-2}},\underbrace{1,1,\ldots,1}_{2^{m-2}}) = t_{m-1}\\
T_m &\leftrightarrow (\underbrace{0,0,\ldots,0}_{2^{m-1}},\underbrace{1,1,\ldots,1}_{2^{m-1}}) = t_m
\end{aligned}$$

Zauważmy, że powyższe przyporządkowanie w naturalny sposób przedłuża się do epimorfizmu algebry wielomianów $\mathbb{Z}_2[T_0, T_1, \ldots, T_{m-1}]$ na $\mathbb{A}$. Jądrem tego odwzorowania jest ideał generowany przez wielomiany $T_i^2 = T_i$, $i = 0, 1, \ldots, m-1$. Ponadto, nietrudno dowieść, że nasz epimorfizm działa wzajemnie jednoznacznie na podprzestrzeni rozpiętej na zbiorze wszystkich jednomianów postaci

$$T_1^{\varepsilon_1} T_2^{\varepsilon_2} \ldots T_m^{\varepsilon_m}, \;\; \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m \in \{0, 1\}.$$

Przez stopień takiego jednomianu rozumiemy $\sum_{1 \leq i \leq m} \varepsilon_i$, a przez stopień ich kombinacji liniowej – największą z wartości stopni jednomianów, które wchodzą do kombinacji z niezerowym współczynnikiem.

Kodem Reeda-Mullera $RM(r,m)$ nazywamy podprzestrzeń przestrzeni $\mathbb{A}_m$, która jest obrazem podprzestrzeni rozpiętej na wszystkich jednomianach stopnia $\leq r$.

Twierdzenie 1.6. Kod Reeda-Mullera $\mathscr{C} = RM(r,m)$ ma następujące własności:

(i) Długość kodu $\mathscr{C}$ jest równa 2^m.
(ii) Wymiar kodu jest równy $dim_{\mathbb{F}} \mathscr{C} = 1 + \binom{m}{1} + \binom{m}{2} + \ldots + \binom{m}{r}$.
(iii) Średnica kodu jest równa 2^{m-r}, wykrywa $2^{m-r} - 1$ błędów i koryguje $2^{m-r-1} - 1$ z nich.
(iv) Macierz generująca kodu $\mathscr{C}$ jest równa $[I;B]$, gdzie

$$B = [t_0; t_1; \ldots; t_m; t_1 t_2; \ldots; t_{m-1} t_m; \ldots]^T,$$

czyli jest macierzą, której kolejne wiersze odpowiadają jednomianom stopnia $\leq r$ uporządkowanym leksykograficznie.

Przejdźmy teraz do demonstracji tego kodu jako ideału algebry grupowej. Niech G będzie elementarną grupą abelową rzędu 2^m, tzn.

$$G = \langle x_1, x_2, \ldots, x_m : \; x_i^2 = e, \; x_i x_j = x_j x_i, \; i, j = 1, 2, \ldots, m \rangle$$

i $\mathbb{F} = \mathbb{Z}_2$. Niech dalej, $\mathscr{A}$ będzie ideałem augmentacyjnym algebry $\mathbb{F}[G]$ oraz dla dowolnego podzbioru Y grupy G przez $\overline{Y}$ będziemy rozumieć element algebry $\mathbb{F}[G]$ postaci $\sum_{y \in Y} y$. Z opisu własności ideału $\mathscr{A}$ podanego na końcu rozdziału 1.1 wynika, że

$$\mathscr{A}^m = \mathrm{lin}((x_1 + 1)(x_2 + 1) \ldots (x_m + 1)) \;\; \text{i} \;\; \mathscr{A}^{m+1} = 0.$$

Zauważmy, że jeśli $\{x_{i_1}, x_{i_2}, \ldots, x_{i_k}\}$ jest k-elementowym podzbiorem zbioru $\{x_1, x_2, \ldots, x_m\}$, to

$$(x_{i_1} + 1)(x_{i_2} + 1) \ldots (x_{i_k} + 1) = \overline{\langle x_{i_1}, x_{i_2}, \ldots, x_{i_k} \rangle}.$$

Wynika z tego, że ideał $\mathscr{A}^j$, $j = 1, 2, \ldots, m$ jest rozpięty, jako przestrzeń liniowa, na elementach postaci $\overline{\langle Y \rangle}$, gdzie Y przebiega wszystkie podzbiory zbioru $\{x_1, x_2, \ldots, x_m\}$,

których moc jest nie mniejsza niż j. Liczba takich podzbiorów jest równa

$$\binom{m}{j}+\binom{m}{j+1}+\ldots+\binom{m}{m}=\binom{m}{0}+\binom{m}{1}+\ldots+\binom{m}{m-j},$$

co oznacza, że $\mathscr{A}^j$ ma wymiar taki, jak kod Reeda-Mullera $RM(m-j,m)$. Dowodzi się, że w standardowej bazie algebry $\mathbb{F}[G]$ ideał A^j zachowuje wszystkie cechy tego kodu. Jednocześnie A^j jako ideał algebry $\mathbb{F}[G]$ ma dodatkowe zalety, które pozwalają na zaproponowanie algorytmu dekodowania. Na podstawie Landrock i Manz (1992) zilustrujemy to w przypadku, gdy $m=5, j=4$. Takich parametrów użyto w kodzie Reeda-Mullera, wykorzystanego do przekazu zdjęć wykonanych w ramach misji statku kosmicznego Mariner w 1969 r.

Niech

$$G=\langle x_1,x_2,x_3,x_4,x_5:\ x_i^2=e,\ x_ix_j=x_jx_i,\ i,j\in\{1,2,3,4,5\}\rangle.$$

Wówczas

Ideał $\mathscr{A}^i$	generatory $\mathscr{A}^i$ modulo $\mathscr{A}^{i+1}$	$\dim\mathscr{A}^i/\mathscr{A}^{i+1}$
$\mathscr{A}^0=\mathbb{F}[G]$	1	$\binom{5}{0}=1$
$\mathscr{A}$	$(x_1+1),\ (x_2+1),\ (x_3+1),\ (x_4+1),\ (x_5+1)$	$\binom{5}{1}=5$
$\mathscr{A}^2$	$(x_i+1)(x_j+1),\ \ i<j,\ \ i,j\in\{1,2,3,4,5\}$	$\binom{5}{2}=10$
$\mathscr{A}^3$	$(x_i+1)(x_j+1)(x_k+1),\ \ i<j<k,\ \ i,j,k\in\{1,2,3,4,5\}$	$\binom{5}{3}=10$
$\mathscr{A}^4$	$(x_i+1)(x_j+1)(x_k+1)(x_l+1),\ \ i<j<k<l,\ \ i,j,k,l\in\{1,2,3,4,5\}$	$\binom{5}{4}=5$
$\mathscr{A}^5$	$(x_1+1)(x_2+1)(x_3+1)(x_4+1)(x_5+1)$	$\binom{5}{5}=1$

Podane parametry oznaczają, że kodem $RM(4,5)$ jest ideał $\mathscr{A}^4$. Jako przestrzeń liniowa jest on rozpięty na elementach z ostatnich dwóch wierszy powyższej tabeli, a więc ma wymiar 6 i tym samym, liczba słów kodowych jest równa $2^6=64$.

Ostatni element jest równy $\eta=\sum_{x\in G}x$, a zatem jego waga Hamminga $\mathrm{wt}(\eta)=32$. Waga Hamminga pozostałych elementów jest równa 16. Dokładniej, jeśli G_i, $i=1,2,3,4,5$ jest podgrupą grupy G generowaną przez elementy x_j, gdzie $i\neq j$, to bazą kodu jest układ:

$$\begin{aligned}
\gamma_0&=\textstyle\sum_{x\in G}x=(x_1+1)(x_2+1)(x_3+1)(x_4+1)(x_5+1),\\
\gamma_1&=\textstyle\sum_{x\in G_1}x=(x_2+1)(x_3+1)(x_4+1)(x_5+1),\\
\gamma_2&=\textstyle\sum_{x\in G_2}x=(x_1+1)(x_3+1)(x_4+1)(x_5+1),\\
\gamma_3&=\textstyle\sum_{x\in G_3}x=(x_1+1)(x_2+1)(x_4+1)(x_5+1),\\
\gamma_4&=\textstyle\sum_{x\in G_4}x=(x_1+1)(x_2+1)(x_3+1)(x_5+1),\\
\gamma_5&=\textstyle\sum_{x\in G_5}x=(x_1+1)(x_2+1)(x_3+1)(x_4+1).
\end{aligned}$$

Dla sprawdzenia, czy dany element α algebry reprezentuje słowo kodowe, wystarczy sprawdzić, czy jest anihilowane przez elementy postaci $(x_i+1)(x_j+1)$, $i<j$. Jeśli α reprezentuje słowo kodowe, tzn.

$$\alpha = a_0\gamma_0 + a_1\gamma_1 + a_2\gamma_2 + a_3\gamma_3 + a_4\gamma_4 + a_5\gamma_6,$$

to dla $i = 1,2,3,4,5$, zachodzi równość $\alpha\cdot(x_i+1) = a_i\gamma_0$, co automatycznie wyznacza skalary a_1,a_2,a_3,a_4. To z kolei pozwala wyznaczyć a_0.

Załóżmy teraz, że w wyniku transmisji danych, po wysłaniu słowa reprezentowanego przez element α otrzymano słowo reprezentowane przez β. Z własności kodu wiadomo, że koryguje błędy, jeśli ich liczba nie przekracza liczby 7. Jeśli więc słowo β różni się od α na nie więcej niż 7 pozycjach, to $\alpha = \beta+\varepsilon$, gdzie ε ma wagę Hamminga nieprzekraczającą tej liczby. To oznacza, że każde ze słów reprezentowanych przez $\varepsilon\cdot(x_i+1)$ ma wagę Hamminga nie przekraczającą liczby 14. Dla wyznaczenia wysłanego słowa α na podstawie β i przedstawienia go w postaci kombinacji liniowej elementów γ_i, $i = 0,1,2,3,4,5$ wystarczy zauważyć, że

$$\begin{aligned}\beta(x_i+1) &= (\alpha+\varepsilon)(x_i+1)\\ &= \alpha(x_i+1)+\varepsilon(x_i+1)\\ &= a_i\gamma_0+\varepsilon(x_i+1).\end{aligned}$$

Wobec tego, że $\mathrm{wt}(\gamma_0) = 32$ i $\mathrm{wt}(\varepsilon(x_i+1)) \leqslant 14$, $a_i = 0$ wtedy i tylko wtedy, gdy $\mathrm{wt}(\beta(x_i+1)) \leqslant 14$. Ta obserwacja pozwala wyznaczyć współczynniki a_1,a_2,a_3,a_4. Do wyznaczenia a_0 wystarczy zauważyć, że $a_0 = 0$ wtedy i tylko wtedy, gdy waga Hamminga elementu $a_1\gamma_1+a_2\gamma_2+a_3\gamma_3+a_4\gamma_4+a_5\gamma_5+\beta$ nie przekracza 7.

Podsumowanie

Czytelnika zainteresowanego tym obszarem badawczym odsyłamy do dwóch publikacji przeglądowych, a mianowicie Milies (2019) oraz Guerreiro (2016). Obie cytują po kilkadziesiąt artykułów, w większości opublikowanych po roku 2000. Liczne, szczegółowe wyniki przywoływane w tych pracach, odnoszą się do przypadku, gdy charakterystyka ciała nie dzieli rzędu grupy, te zaś są albo abelowe, albo bliskie abelowym. Algebraiczny opis rozważanych kodów jest oparty na dobrze znanej strukturze półprostych algebr grupowych. Tymczasem, jak widzieliśmy w przykładach kodów Golay'a i Reeda-Müllera, bardzo obiecujące wyniki uzyskano wcześniej dla algebr modularnych, tzn. takich, gdy charakterystyka ciała dzieli rząd grupy, a nawet dla p-grup. Struktura algebr grupowych p-grup nad ciałami charakterystyki p jest bardzo skomplikowana i daleko do uzyskania jej zadowalającego opisu, co może

być elementem zniechęcającym do poszukiwań w tych obszarach. Jednakże, wiele wiadomo dla bardzo konkretnych klas grup, które nie były badane pod kątem ich przydatności dla teorii kodowania. Dotyczy to w szczególności p-grup abelowych lub p-grup, które są w jakimś sensie bliskie abelowym. Na szczególną uwagę zasługuje zbadanie własności ideałów generowanych przez elementy centralne w algebrach grupowych 2-grup bliskim grupom dihedralnym (patrz Bagiński i Konovalov (2004) i Bagiński i Kurdics (2014)).

Bibliografia

Bagiński, C., i Kurdics, J. (2014, January). On the center of the modular group algebra of a finite p-group. Journal of Algebra and Its Applications, 13(04), 1350127. doi: 10.1142/s0219498813501272

Bagiński, C., i Konovalov, A. (2004, July). On 2-groups of almost maximal class. Publicationes Mathematicae, 65.

Broche, O., i del Río, A. (2007). Wedderburn decomposition of finite group algebras. Finite Fields and Their Applications, 13(1), 71-79. doi: 10.1016/j.ffa.2005.08.002

Gap – groups, algorithms, and programming, version 4.11.1 [Computer software manual]. (2021).

Guerreiro, M. (2016, May). Group algebras and coding theory. São Paulo Journal of Mathematical Sciences, 10(2), 346–371. doi: 10.1007/s40863-016-0040-x

Hoffman, D. G., Wal, Leonard, D. A., Lidner, C. C., Phelps, K. T. i Rodger, C. A. (1991). Coding theory: The essentials. USA: Marcel Dekker, Inc.

Kobliz, N. (2006). Wykład z teorii liczb i kryptografii. Warszawa: WNT.

Landrock, P., i Manz, O. (1992, September). Classical codes as ideals in group algebras. Des. Codes Cryptography, 2(3), 273–285. doi: 10.1007/BF00141972

Milies, C. (2019, April). Group algebras and coding theory: a short survey. Revista Integración, 37, 153-166. doi: 10.18273/revint.v37n1-2019008

Olteanu, G., i del Río, A. (2009, May). An algorithm to compute the wedderburn decomposition of semisimple group algebras implemented in the gap package wedderga. J. Symb. Comput., 44(5), 507–516. doi: 10.1016/j.jsc.2007.07.019

Passman, D. S. (1977). The algebraic structure of group rings [Book]. Wiley New York.

Sehgal, S. K. (1978). Topics in group rings (50). Marcel Dekker Incorporated.

Wolfmann, J. (1991, May). A new construction of the binary golay code (24, 12, 8) using a group algebra over a finite field. Discrete Math., 31(3), 337–338. doi: 10.1016/0012-365X(80)90147-8

Rozdział 2

O ADDYTYWNYCH GRUPACH (ŁĄCZNYCH) PIERŚCIENI PRZEMIENNYCH

Mateusz Woronowicz*

Streszczenie Jednymi z ważnych zagadnień algebraicznych znajdujących praktyczne zastosowanie w naukach informatycznych są przemienność oraz łączność pierścieni konstruowanych na grupach abelowych. Wykorzystywane są one, między innymi, w kryptografii oraz algorytmach związanych z segmentacją i rozpoznawaniem obrazów cyfrowych. Niniejszy rozdział stanowi przegląd aktualnej wiedzy dotyczącej struktury $(A)CR$-grup, czyli grup abelowych, na których każde (łączne) mnożenie pierścieniowe jest przemienne. Stanowi ona teoretyczny fundament, na którym można budować struktury algebraiczne potrzebne do konstrukcji algorytmów. W szczególności, niniejsze opracowanie zawiera: klasyfikacje torsyjnych $(A)CR$-grup oraz beztorsyjnych całkowicie rozkładalnych CR-grup, opis wszystkich beztorsyjnych CR-grup rangi dwa pozwalający sklasyfikować beztorsyjne grupy abelowe rangi dwa, na których istnieje struktura nieprzemiennego i jednocześnie niełącznego pierścienia, opis wszystkich beztorsyjnych ACR-grup rangi dwa, klasyfikację beztorsyjnych ACR-grupy rangi dwa niebędących CR-grupami wraz z konstrukcją $2^{\aleph_0}$ nieizomorficznych grup posiadających tę własność w każdym z dwóch możliwych przypadków związanych ze zbiorem typów takiej grupy oraz częściowy opis struktury mieszanych $(A)CR$-grup.

Słowa kluczowe: grupy addytywne pierścieni, pierścień przemienny, pierścień łączny, pierścień nieprzemienny, pierścień niełączny, typ.

Wprowadzenie

Teoria pierścieni posiada szerokie spektrum zastosowań w naukach informatycznych. Przejawia się ono, między innymi, w kryptografii oraz rozpoznawaniu obrazów (zob. Lidl i Harald (1994)). Szczególnym przypadkiem zastosowania teorii pierścieni w informatyce są algorytmy związane z segmentacją obrazów cyfrowych (zob. Garcés, Torres, Pereira i Rodríguez (2014)). Opierają się one na arytmetyce

* Wydział Informatyki, Politechnika Białostocka, Wiejska 45A, 15-351 Białystok, m.woronowicz@pb.edu.pl

DOI 10.24427/978-83-67185-18-9_2

pierścieni $\mathbb{Z}_n$ reszt modulo n. Klasycznymi przykładami zastosowań tych pierścieni są algorytmy dodawania liczb n-bitowych (zob. Cormen, Leiserson i Rivest (1990); Karatsuba (1995); Knuth (1997); K. Woronowicz (2015)). Arytmetyka modularna znajduje zastosowanie także w licznych językach programowania i kalkulatorach. Ważnymi własnościami wielu mnożeń pierścieniowych stosowanych w informatyce są więc przemienność oraz łączność. W tym kontekście pojawia się naturalne pytanie o strukturę grup abelowych, które mogą być grupami addytywnymi wyłącznie pierścieni o tych własnościach. W niniejszym rozdziale zostaną zaprezentowane najważniejsze wyniki z tego zakresu - zarówno klasyczne, jak i najnowsze. W szczególności omówiona zostanie struktura $(A)CR$-grup, czyli grup abelowych, na których każde (łączne) mnożenie pierścieniowe jest przemienne. Pojęcia te zostały wprowadzone w pracy Feigelstock (2000). Jej autor zamieścił tam wiele interesujących rezultatów – opisał on, między innymi, strukturę torsyjnych $(A)CR$-grup, wykazując jednocześnie równoważność warunków CR i ACR dla torsyjnych grup abelowych, częściowo scharakteryzował mieszane CR-grupy, podał przykład beztorsyjnej ACR-grupy, która nie jest CR-grupą oraz zauważył, że każdy pierścień, którego grupa addytywna jest torsyjną $(A)CR$-grupą jest łączny (zob. (Feigelstock, 2000, Theorems 5 & 10, Example, Corollary 4)). Ta ostatnia obserwacja przyczyniła się niedawno do wprowadzenia i częściowego zbadania pojęcia AR-grupy, czyli takiej grupy abelowej, która może być grupą addytywną jedynie pierścieni łącznych (zob. Andruszkiewicz i Woronowicz (2017); Najafizadeh i Woronowicz (2017); M. Woronowicz (2020)). Zagadnienia badane w cytowanym artykule Feigelstocka poruszane były także w znacznie wcześniejszych pracach Beaumont i Wisner (1959); Jackett (1979); Schultz (1973) oraz w nowych i stosunkowo nowych pracach Aghdam (2006); Aghdam i Najafizadeh (2008); Andruszkiewicz i Woronowicz (2017); Najafizadeh i Woronowicz (2017); M. Woronowicz (2020).

Zasadniczym celem niniejszego rozdziału jest przegląd aktualnego stanu wiedzy z zakresu grup addytywnych (łącznych) pierścieni przemiennych w kontekście potencjalnych zastosowań w naukach informatycznych. Wyniki składające się na ten rozdział pochodzą z cytowanych wyżej prac. Niektóre z nich są prezentowane z nowymi dowodami. Uwaga ta dotyczy w szczególności dowodu twierdzenia klasyfikacyjnego dla beztorsyjnych całkowicie rozkładalnych CR-grup, wykorzystującego zdecydowanie bardziej elementarne techniki niż dowód znany dotychczas (por. Twierdzenie 2.4 i (Feigelstock, 2000, Theorem 8)). Szczegółowe informacje na temat historii badań $(A)CR$-grup dostępne są w M. Woronowicz (2019).

2.1 Oznaczenia

Wszystkie grupy występujące w niniejszej pracy są abelowe. Stosujemy tradycyjny dla nich zapis addytywny. Ze względu na fakt rozważania grup abelowych w kon-

tekście grup addytywnych pierścieni, przemienność grup będzie za każdym razem podkreślana w sformułowaniach twierdzeń.

Dla dowolnej grupy abelowej A, symbole $\mathbb{P}(A)$, $T(A)$ i $\mathscr{D}(A)$ oznaczają odpowiednio zbiór tych wszystkich liczb pierwszych p, dla których p-komponent A_p grupy A jest nietrywialny, oraz część torsyjną i podzielną otoczkę grupy A. Grupa $\mathscr{D}(A)$ i jej własności omówione są w (Fuchs, 1970, §24). Ranga i ranga beztorsyjna grupy A oznaczane są odpowiednio przez $r(A)$ i $r_0(A)$. Najmniejszą liczbę naturalną m taką, że $mA = \{0\}$ nazywamy wykładnikiem grupy A i oznaczamy przez $\exp(A)$. Jeśli taka liczba m nie istnieje, to przyjmujemy, że $\exp(A) = \infty$. Zbiór wszystkich elementów a grupy A, które dla ustalonej liczby naturalnej n spełniają warunek $na = 0$ oznaczamy symbolem $A[n]$. Jeżeli p jest liczbą pierwszą, to zbiór $\bigcap_{n=1}^{\infty} p^n A$ będziemy zapisywać jako $p^\infty A$. Symbole $h_p^A(a)$ i $o(a)$ oznaczają odpowiednio p-wysokość elementu a w grupie A oraz jego rząd. Podgrupę grupy A generowaną przez zbiór X zawarty w A oznaczamy przez $\langle X \rangle$. Jeżeli X jest podzbiorem beztorsyjnej grupy abelowej A, zaś a jest elementem tej grupy, to symbole $\langle X \rangle_*$ i $\mathfrak{t}(a)$ oznaczają odpowiednio czystą podgrupę grupy A generowaną przez X oraz typ elementu a. Chcąc podkreślić, że typ elementu a jest rozważany w grupie A będziemy pisali $\mathfrak{t}_A(a)$ zamiast $\mathfrak{t}(a)$. Zbiór typów wszystkich niezerowych elementów grupy A oznaczamy przez $\mathscr{T}[A]$. Pojęcie typu elementu grupy zostało szczegółowo omówione w (Fuchs, 1973, §85). Symbolem $\mathfrak{R}(A)$ oznaczamy rdzeń beztorsyjnej grupy abelowej A, tzn. zbiór wszystkich liczb wymiernych q, dla których $qA \subseteq A$. Jest on unitarnym podpierścieniem w ciele liczb wymiernych (zob. Stratton (n.d.)). Jeżeli grupa abelowa A jest sumą prostą grup A_i, przy czym i przebiega pewien niepusty zbiór I, to dla dowolnego elementu j zbioru I symbolem $\overline{A}_j$ oznaczamy zbiór tych wszystkich elementów a grupy A, których nośnik $\operatorname{supp}(a)$ zawiera się w zbiorze $\{j\}$. Na każdej grupie abelowej A można w trywialny sposób określić strukturę pierścienia definiując mnożenie: $a \cdot b = 0$ dla wszystkich $a, b \in A$. Taki pierścień nazywamy pierścieniem z zerowym mnożeniem i oznaczamy symbolem A^0. Jeśli jest to jedyny (łączny) pierścień możliwy do określenia grupie A, to mówimy, że A jest $\mathrm{nil}_{(a)}$-grupą. Wiedza dotycząca zależności między tymi pojęciami dla grup torsyjnych, mieszanych i beztorsyjnych uwzględniająca wyniki najnowszych badań z tego zakresu dostępna jest w M. Woronowicz (2019, 2020). Symbolem $\square A$ oznaczamy podgrupę kwadratową grupy abelowej A generowaną przez kwadraty wszystkich możliwych pierścieni o grupie addytywnej A (zob. Aghdam (1987); Andruszkiewicz i Woronowicz (2016a, 2016b); Najafizadeh (2015); M. Woronowicz (2019). W szczególności grupa A jest nil-grupą wtedy i tylko wtedy, gdy $\square A = \{0\}$. Pierścień endomorfizmów grupy abelowej A oznaczamy przez $\mathrm{E}(A)$. Grupę addytywną i obustronny anihilator pierścienia R oznaczamy odpowiednio przez R^+ oraz $\mathfrak{a}(R)$. W drodze wyjątku, grupę addytywną pierścienia $\mathrm{E}(A)$ oznaczamy tradycyjnie przez $\mathrm{End}(A)$.

Symbole $\mathbb{P}(R)$, R_p, $T(R)$ i $p^\infty R$ odnoszą się do grupy addytywnej pierścienia R w sposób wyjaśniony w poprzednim akapicie. Jeżeli X jest podzbiorem w R, to $\langle X \rangle$ i $[X]$ oznaczają odpowiednio podgrupę grupy R^+ generowaną przez X oraz podpier-

ścień pierścienia R generowany przez X. Fakt, że niepusty podzbiór I pierścienia R jest obustronnym ideałem w R zapisujemy symbolicznie jako $I \lhd R$. Rozważając dowolny pierścień R nie zakładamy ani jego łączności, ani przemienności, ani też unitarności. Przyjmujemy jedynie, że mnożenie pierścienia R jest obustronnie rozdzielne względem dodawania. Przez podpierścień pierścienia R rozumiemy podzbiór w R, który jest podgrupą w R^+ i jest zamknięty ze względu na mnożenie pierścienia R. W szczególności, jeśli S jest podpierścieniem unitarnego pierścienia R, to nie zakładamy, że jedynka pierścienia R należy do S. Grupę elementów odwracalnych unitarnego pierścienia R oznaczamy przez R^*. Jeśli R jest dziedziną całkowitości, to $\Pi(R)$ oznacza zbiór wszystkich liczb pierwszych p takich, że $R \neq pR$.

Symbole $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{P}$, $\mathbb{N}$ i $\mathbb{N}_0$ oznaczają odpowiednio ciało liczb wymiernych, pierścień liczb całkowitych oraz zbiory wszystkich liczb: pierwszych, naturalnych (rozumianych jako dodatnie liczby całkowite) i całkowitych nieujemnych. Ponadto dla dowolnej liczby pierwszej p oraz dowolnej liczby naturalnej n, symbole $Z(p^\infty)$, $Z(n)$ i $\mathbb{Z}_n$ oznaczają kolejno: p-grupę quasicykliczną, grupę cykliczną rzędu n oraz pierścień reszt modulo n, którego mnożenie oznaczane jest przez $\odot_n$. Najmniejszą wspólną wielokrotność ustalonych liczb całkowitych k i l oznaczamy przez $\mathrm{NWW}(k,l)$.

Wszystkie pozostałe oznaczenia są zgodne z notacją stosowaną w klasycznej dwutomowej monografii Fuchs (1970, 1973) poświęconej grupom abelowym lub zostaną wprowadzone i wyjaśnione w dalszej części tej pracy.

2.2 Wiadomości wstępne

W rozważaniu struktury pierścienia na grupie abelowej, która nie jest beztorsyjna wielokrotne zastosowanie będzie miała następująca, dobrze znana:

Uwaga 2.1. W dowolnym pierścieniu $(R,+,\cdot,0)$:

(i) $R_p \lhd R$ dla dowolnej liczby pierwszej p;
(ii) $T(R) \lhd R$;
(iii) $T(R) = \bigoplus_{p\in\mathbb{P}(R)} R_p$;
(iv) $R_p \cdot R_q = \{0\}$ dla dowolnych różnych liczb pierwszych p i q.

Jednym z ważnych narzędzi używanych do konstruowania mnożeń pierścieniowych na grupach abelowych jest produkt tensorowy takich grup (zob. (Fuchs, 1970, §59) i por. np. z Feigelstock (2000)). Fundamentalny związek struktury pierścienia na dowolnej grupie abelowej A z produktem tensorowym grup abelowych ilustruje poniższe, znane

Twierdzenie 2.1. Niech A będzie grupą abelową. Wówczas:

(i) $\mathrm{Mult}(A) \cong \mathrm{Hom}(A \otimes A, A)$;

(ii) $\mathrm{Mult}(A) \cong \mathrm{Hom}\big(A, \mathrm{End}(A)\big)$.

Dowód. Zob. (Fuchs, 1973, Theorem 118.1).

Podamy teraz szereg technicznych lematów, które znacznie ułatwią przeprowadzenie dowodów zasadniczych rezultatów dotyczących struktury $(A)CR$-grup.

Lemat 2.1. Niech A i B będą grupami abelowymi takimi, że $A = T(A)$, $\exp(A_p) < \infty$, $B = pB$ oraz $B_p = \{0\}$ dla wszystkich $p \in \mathbb{P}(A)$. Jeżeli R jest pierścieniem o grupie addytywnej $A \oplus B$, to $R = R_1 \times R_2$ dla pewnych pierścieni R_1 i R_2 odpowiednio o grupach addytywnych A i B.

Dowód. Rozważmy dowolny pierścień $R = (A \oplus B, *)$ i oznaczmy $G = A \oplus \{0\}$ oraz $H = \{0\} \oplus B$. Wtedy $G * H = H * G = \{0\}$, gdyż $G = T(G)$ i $H = pH$ dla każdego $p \in \mathbb{P}(G)$. Rozważmy dowolne $g_1, g_2 \in G$ i $h_1, h_2 \in H$. Wtedy $g_1 * g_2 = g_3 + h$ dla pewnych $g_3 \in G$, $h \in H$. Niech $m = \mathrm{NWW}\big(o(g_1), o(g_2), o(g_3)\big)$. Wówczas $0 = m(g_1 * g_2) = m(g_3 + h) = mh$, skąd $h \in T(H)$. Weźmy dowolne $p \in \mathbb{P}$. Jeżeli $p \mid o(h)$, to $p \mid m$, więc z określenia liczby m wynika, że $p \in \mathbb{P}(G)$. Ale $H_p = \{0\}$ dla każdego $p \in \mathbb{P}(G)$, więc $h = 0$. Zatem $G * G \subseteq G$. Dalej, $h_1 * h_2 = g + h_3$ dla pewnych $g \in G$, $h_3 \in H$. Niech P będzie skończonym podzbiorem w $\mathbb{P}(G)$ takim, że $g \in \bigoplus_{p \in P} G_p$. Wtedy dla $n = \prod_{p \in P} \exp(G_p)$ otrzymujemy, że $n\big(\bigoplus_{p \in P} G_p\big) = \{0\}$. Ponadto $H = pH$ dla każdego $p \in \mathbb{P}(G)$, więc $h_1 = nh_1'$, $h_2 = nh_2'$ i $h_3 = n^2 h_3'$ dla pewnych $h_1', h_2', h_3' \in H$. Zatem $n^2(h_1' * h_2') = g + n^2 h_3'$, skąd $g = n^2\big((h_1' * h_2') - h_3'\big) \in \in n^2(G \oplus H)$. Ale $\big(n^2(G \oplus H)\big)_p = \{0\}$ dla każdego $p \in P$, więc $g = 0$. Wobec tego $h_1 * h_2 \in H$. Stąd $H * H \subseteq H$. W ten sposób pokazaliśmy, że $G, H \lhd R$ i $R = G \oplus H$. Niech $R_1 = (A, \circledast)$ oraz $R_2 = (B, \star)$ będą pierścieniami z mnożeniami w naturalny sposób indukowanymi odpowiednio z podpierścieni G i H pierścienia R. Wtedy $R = R_1 \times R_2$.

Lemat 2.2. Niech $G = A \oplus H$, gdzie A i H są takimi grupami abelowymi, że $A_p \neq \neq \{0\}$, $H_p = \{0\}$ oraz $\dim_{\mathbb{Z}_p} H/pH > 1$ dla pewnego $p \in \mathbb{P}$. Istnieją wówczas łączny pierścień $R = (G, *)$ oraz $x, y \in H$ takie, że $(0,y)^2 = (0,x) * (0,y) = (0,0)$ oraz $(0,y) * \\ *(0,x) = (a,0)$ i $(0,x)^2 = (b,0)$ dla pewnych $a, b \in A \setminus \{0\}$.

Dowód. Rozważmy diagram:

$$G \xrightarrow{\pi_1} H \xrightarrow{\pi_2} H/pH \xrightarrow{\varphi} \bigoplus_{i \in I} \mathbb{Z}_p^+,$$

gdzie π_1 jest naturalnym rzutowaniem grupy G na grupę H, π_2 jest epimorfizmem kanonicznym, zaś φ jest izomorfizmem. Niech $f = \varphi \circ \pi_2 \circ \pi_1$. Z przyjętych założeń wynika istnienie takiego $x \in H \setminus pH$, że $\big|\operatorname{supp} \varphi(x + pH)\big| \geq 2$. Weźmy dowolne $i_1, i_2 \in \operatorname{supp} \varphi(x + pH)$ takie, że $i_1 \neq i_2$. Niech $\varepsilon = (\varepsilon_i)_{i \in I}$ będzie elementem grupy $\bigoplus_{i \in I} \mathbb{Z}_p^+$ takim, że:

$$\varepsilon_i = \begin{cases} 1 \text{ , dla } i = i_1 \\ 0 \text{ , dla } i \neq i_1 \end{cases}.$$

Niech ponadto $c = \varepsilon \cdot \varphi(x+pH)$, przy czym $\cdot$ oznacza mnożenie pierścienia $\prod_{i\in I}\mathbb{Z}_p$. Wówczas $\varphi^{-1}(c) = y + pH$ dla pewnego $y \in H \setminus pH$. Dla $t = 1,2$, epimorfizmy $\mu_t \colon \bigoplus_{i\in I}\mathbb{Z}_p^+ \to \mathbb{Z}_p^+$ definiujemy w sposób następujący:

$$\mu_1\left((k_i)_{i\in I}\right) = k_{i_1}, \quad \mu_2\left((k_i)_{i\in I}\right) = k_{i_2}.$$

Wtedy:

$$\mu_1\Big(f\big((0,y)\big)\Big) \odot_p \mu_2\Big(f\big((0,y)\big)\Big) = 0,\ \mu_1\Big(f\big((0,x)\big)\Big) \odot_p \mu_2\Big(f\big((0,y)\big)\Big) = 0,$$

$$\mu_1\Big(f\big((0,y)\big)\Big) \odot_p \mu_2\Big(f\big((0,x)\big)\Big) \neq 0,\ \mu_1\Big(f\big((0,x)\big)\Big) \odot_p \mu_2\Big(f\big((0,x)\big)\Big) \neq 0.$$

Bezpośrednio z przyjętych założeń wynika istnienie zanurzenia $\iota \colon \mathbb{Z}_p^+ \to A$. Rozważmy odwzorowanie $* \colon G \times G \to G$ dane wzorem:

$$g_1 * g_2 = \left(\iota\Big(\mu_1\big(f(g_1)\big) \odot_p \mu_2\big(f(g_2)\big)\Big), 0\right)$$

dla wszystkich $g_1, g_2 \in G$. Ponieważ przekształcenia ι, μ_1, μ_2 i f są homomorfizmami grup oraz $\odot_p$ jest mnożeniem pierścieniowym, to $R = (G, *)$ jest pierścieniem. Ponadto $f(A) = \{0\}$, więc $A \subseteq \mathfrak{a}(R)$. Stąd oraz na mocy inkluzji $R^2 \subseteq A$ otrzymujemy, że $(G*G)*G = G*(G*G) = \{0\}$. Wobec tego pierścień R jest łączny. Ostatecznie otrzymujemy więc, że $(0,y)^2 = (0,x)*(0,y) = (0,0)$ oraz $(0,y)*(0,x) = (a,0)$ i $(0,x)^2 = (b,0)$ dla pewnych $a, b \in A \setminus \{0\}$.

Lemat 2.3. Niech p będzie liczbą pierwszą, zaś n liczbą naturalną. Niech ponadto H będzie nil_a-grupą taką, że $H_p = \{0\}$. Jeżeli R jest łącznym pierścieniem o grupie addytywnej $Z(p^n) \oplus H$, to $R^2 \subseteq Z(p^n) \oplus \{0\}$. W szczególności, jeśli $n = 1$ oraz $R^2 \neq \neq \{0\}$, to $R^2 = Z(p) \oplus \{0\}$.

Dowód. Niech $I = Z(p^n) \oplus \{0\}$ i niech $B = \{0\} \oplus H$. Ponieważ $B_p = \{0\}$, to $I = \neq R_p \lhd R$. Załóżmy nie wprost, że $B^2 \nsubseteq I$. Wtedy $(R/I)^2 \neq \{0+I\}$. Ale $(R/I)^+ \cong H$, więc H nie jest nil_a-grupą, sprzeczność. Zatem $R^2 \subseteq Z(p^n) \oplus \{0\}$. Jeśli więc $n = 1$ i $R^2 \neq \{0\}$, to R^2 jest nietrywialną podgrupą w $Z(p) \oplus \{0\}$, skąd $R^2 = Z(p) \oplus \{0\}$.

Lemat 2.4. Niech H będzie nil_a-grupą taką, że $H_p = \{0\}$ oraz $H = \langle h_0 \rangle + pH$ dla pewnych $p \in \mathbb{P}$ i $h_0 \in H$. Jeżeli R jest łącznym pierścieniem o grupie addytywnej $Z(p) \oplus H$ i $R^2 \neq \{0\}$, to $R \cong \mathbb{Z}_p \times H^0$ lub $R = \big\langle (0,h_0) \big\rangle + \mathfrak{a}(R)$, przy czym $o\big((0,h_0)^2\big) = p$ i $R^3 = \{0\}$.

Dowód. Niech $I = Z(p) \oplus \{0\}$ i niech $B = \{0\} \oplus H$. Wtedy $I = R_p$, więc $I \lhd R$. Ponadto $R^2 = I$ na mocy Lematu 2.3. Weźmy dowolne $a \in I \setminus \{0\}$. Wówczas $o(a) = \neq p$, skąd $\langle a \rangle = I$. Mamy do rozważenia dwa przypadki:

(i). $a^2 \neq 0$. Wtedy $I \cong \mathbb{Z}_p$. Zatem pierścień I posiada jedynkę. Istnieje więc ideał J pierścienia R taki, że $R = I \oplus J$ (por. (Gardner i Wiegandt, 2004, Szendrei's Theorem 1.2.5)). Stąd $H \cong (R/I)^+ \cong J^+$. Ponadto H jest nil_a-grupą, więc $J^2 = \{0\}$. Zatem $R \cong \mathbb{Z}_p \times H^0$.

(ii). $a^2 = 0$. Wtedy $R^4 = I^2 = \langle a^2 \rangle = \{0\}$. Załóżmy nie wprost, że $R^3 \neq \{0\}$. Ponieważ $R^2 \lhd R$, to $R^3 \subseteq R^2$. Ale R^3 jest podpierścieniem w R, $R^2 = I$ oraz $|I| = p$, więc $R^3 = R^2$. Stąd $R^3 = R^2 \cdot R = R^3 \cdot R = R^4 = \{0\}$, sprzeczność. Zatem $R^3 = \{0\}$. Weźmy dowolne $b \in B$. Wtedy $ab \in I$, więc istnieje $k \in \mathbb{Z}$ takie, że $ab = ka$. Stąd $(ab)b = (ka)b = k(ab) = k(ka) = k^2a$. Ale $R^3 = \{0\}$, więc $k^2a = 0$. Zatem $p \mid k^2$, skąd $p \mid k$. Wobec tego $ka = 0$, czyli $ab = 0$. Stąd $aB = \{0\}$. Podobnie pokazuje się, że $Ba = \{0\}$. Ponadto $a^2 = 0$, więc $a \in \mathfrak{a}(R)$. Dalej, $(pB)R = p(BR) \subseteq pR^2 = pI = \{0\}$, skąd $(pB)R = \{0\}$. Analogicznie $R(pB) = \{0\}$. Zatem $pB \subseteq \mathfrak{a}(R)$. Ponadto $H = \langle h_0 \rangle + pH$ dla pewnego $h_0 \in H$, więc $R = \big\langle (0,h_0) \big\rangle + \mathfrak{a}(R)$. Ale $R^2 \neq \{0\}$, więc $(0,h_0)^2 \neq 0$. Stąd oraz na mocy równości $R^2 = I$ otrzymujemy, że $o\big((0,h_0)^2\big) = p$.

Lemat 2.5. Niech A, B i C będą beztorsyjnymi grupami abelowymi i niech G będzie czystą podgrupą w A.

(1.) Jeżeli a_1 i a_2 są zależnymi elementami w A, to $\mathfrak{t}(a_1) = \mathfrak{t}(a_2)$.
(2.) $\mathfrak{t}(a) \cdot \mathfrak{t}(b) \geq \mathfrak{t}(a)$ dla wszystkich $a, b \in A$.
(3.) Jeżeli $R = (A, \star)$ jest pierścieniem, to $\mathfrak{t}(a \star b) \geq \mathfrak{t}(a) \cdot \mathfrak{t}(b)$ dla wszystkich $a, b \in A$.
(4.) Jeżeli $R = (A, \star)$ jest pierścieniem, to $\mathfrak{t}(a \star b) \geq \mathfrak{t}(a) \vee \mathfrak{t}(b)$ dla wszystkich $a, b \in A$.
(5.) Jeżeli A i B są podgrupami w $\mathbb{Q}^+$, to $\mathfrak{t}(A \cdot B) = \mathfrak{t}(A) \cdot \mathfrak{t}(B)$.

Dowód. Własność (1.) udowodniona jest w (Fuchs, 1973, p. 108-109). Dowód własności (2.) wynika wprost z (Feigelstock, 1983, Consequence 1.3.2). Własność (3.) jest bezpośrednią konsekwencją równości $(p^n x) \star y = p^n (x \star y) = x \star (p^n y)$, które są prawdziwe dla wszystkich $x, y \in A$, $p \in \mathbb{P}$ i $n \in \mathbb{N}$, oraz określenia iloczynu typów (zob. (Fuchs, 1973, p. 110)). Własność (4.) wynika wprost z (3.) i (2.). Pozostało udowodnić własność (5.). Jeżeli $A = \{0\}$ lub $B = \{0\}$, to teza jest oczywista. Niech dalej $A \neq \{0\}$ i $B \neq \{0\}$. Wtedy bez utraty ogólności możemy przyjąć, że $1 \in A \cap B$ (zob. (M. Woronowicz, 2016, Remark 4.2)). Wówczas $h_p^{A \cdot B}(1) = h_p^A(1) + h_p^B(1)$ (jeśli którakolwiek p-wysokość jest nieskończona, to przyjmujemy, że ich suma jest nieskończona). Stąd $\mathfrak{t}_{A \cdot B}(1) = \mathfrak{t}_A(1) \cdot \mathfrak{t}_B(1)$. Ponadto $\mathfrak{t}(A \cdot B) = \mathfrak{t}_{A \cdot B}(1)$, $\mathfrak{t}(A) = \mathfrak{t}_A(1)$ i $\mathfrak{t}(B) = \mathfrak{t}_B(1)$ (por. (Fuchs, 1973, p. 109)), więc $\mathfrak{t}(A \cdot B) = \mathfrak{t}(A) \cdot \mathfrak{t}(B)$.

Lemat 2.6. Niech A i B będą nietrywialnymi podgrupami grupy $\mathbb{Q}^+$. Wówczas następujące warunki są równoważne:

(i) B jest obrazem homomorficznym grupy A;
(ii) $B = q \cdot A$ dla pewnego $q \in \mathbb{Q} \setminus \{0\}$;
(iii) $mA = nB$ dla pewnych $m, n \in \mathbb{N}$;
(iv) $B \cong A$.

Dowód. Załóżmy, że istnieje homomorfizm f grupy A na grupę B. Weźmy dowolne $b \in B \setminus \{0\}$. Istnieje wówczas $a \in A \setminus \{0\}$ takie, że $b = f(a)$. Ponieważ $\langle a \rangle \cap \langle b \rangle \neq \neq \{0\}$, to istnieje $q \in \mathbb{Q} \setminus \{0\}$ takie, że $b = q \cdot a$. Rozważmy dowolne $x \in A$. Wtedy $x = \frac{k}{n} \cdot a$ dla pewnych $k \in \mathbb{Z}$ i $n \in \mathbb{N}$. Zatem $nf(x) = f(nx) = f(ka) = kf(a) = = kb = k(q \cdot a)$, skąd $f(x) = q \cdot \left(\frac{k}{n} \cdot a\right) = q \cdot x$. Wobec tego $B = f(A) = q \cdot A$. W ten sposób wykazaliśmy implikację $(i) \Rightarrow (ii)$. Implikacje $(ii) \Rightarrow (iii)$, $(iii) \Rightarrow (iv)$ oraz $(iv) \Rightarrow (i)$ są trywialne.

Bezpośrednią konsekwencją (Fuchs, 1973, Proposition 85.4), Lematu 2.6 oraz punktu (5.) Lematu 2.5 jest następujący

Wniosek 2.1. Dla dowolnych podgrup A, B, C grupy $\mathbb{Q}^+$ następujące warunki są równoważne:

(i) $n(A \cdot C) \subseteq B$ dla pewnego $n \in \mathbb{N}$;
(ii) $\mathfrak{t}(A) \cdot \mathfrak{t}(C) \leq \mathfrak{t}(B)$.

W poniższej definicji zamieszczamy zwięzłe zestawienie głównych pojęć związanych z tematyką niniejszego rozdziału.

Definicja 2.1. Grupę abelową A nazywamy CR-grupą, gdy każdy pierścień o grupie addytywnej A jest przemienny. Jeżeli A spełnia warunek CR ograniczony do klasy pierścieni łącznych, to mówimy, że A jest ACR-grupą. W przypadku, gdy A może być grupą addytywną jedynie pierścieni łącznych, to A nazywamy AR-grupą.

Bezpośrednią konsekwencją powyższej definicji jest następująca

Uwaga 2.2. Każda CR-grupa jest ACR-grupą.

Okazuje się, że zachodzi także zdecydowanie mniej oczywista zależność.

Twierdzenie 2.2. Każda CR-grupa jest AR-grupą.

Dowód. Rozważmy dowolną CR-grupę A. Weźmy dowolne $* \in \mathrm{Mult}(A)$ oraz $a \in A$. Bezpośrednie sprawdzenie pokazuje, że mnożenie $x_1 \circledast x_2 = x_1 * (a * x_2)$ określone dla wszystkich $x_1, x_2 \in A$, wprowadza na A strukturę pierścienia. Rozważmy dowolne $x, y \in A$. Ponieważ A jest CR-grupą, to $x \circledast y = y \circledast x$, czyli $x * (a * y) = y * (a * x)$. Ale również mnożenie $*$ jest przemienne, skąd $x * (a * y) = (a * x) * y = (x * a) * y$. Ponadto elementy x, y oraz a zostały wybrane w sposób dowolny, więc pierścień $(A, *)$ jest łączny. Zatem A jest AR-grupą.

Jeżeli G jest grupą abelową postaci $G = A \oplus B$ i R jest pierścieniem o grupie addytywnej A, to $S = R \times B^0$ jest pierścieniem o grupie addytywnej izomorficznej z grupą G. Stąd otrzymujemy natychmiast następujące:

Stwierdzenie 2.1. Składnik prosty $(A)CR$-grupy (AR-grupy) jest $(A)CR$-grupą (AR-grupą).

Poniższe stwierdzenie charakteryzuje rozkładalne *ACR*-grupy.

Stwierdzenie 2.2. Niech $\{G_i\colon i\in I\}$, gdzie $I\neq\emptyset$, będzie rodziną grup abelowych. Jeżeli $\bigoplus_{i\in I}G_i$ jest *ACR*-grupą, to $\mathrm{Hom}(G_i\otimes G_j,G_k)=\{0\}$ dla wszystkich parami różnych $i,j,k\in I$.

Dowód. Załóżmy, że dla pewnych parami różnych $i,j,k\in I$ istnieje niezerowy homomorfizm $f\colon G_i\otimes G_j\to G_k$. Niech ϕ_k będzie naturalną injekcją grupy G_k w grupę G i niech π_t będzie naturalnym rzutowaniem grupy G na grupę G_t dla $t\in i,j$. Wówczas $(G,*)$, gdzie $g_1*g_2=\phi_k\Big(f\big(\pi_i(g_1)\otimes\pi_j(g_2)\big)\Big)$, jest pierścieniem takim, że $G*(G*G)=(G*G)*G=\{0\}$. W szczególności wynika stąd, że pierścień $(G,*)$ jest łączny. Ponieważ $f\neq 0$, odwzorowania π_i oraz π_j są surjektywne i ϕ_k jest injekcją, to istnieją $a,b\in G$ takie, że $a*b\neq 0$. Elementy $x=(x_s)_{s\in I}$ oraz $y=(y_s)_{s\in I}$ definiujemy następująco:

$$x_s=\begin{cases}\pi_i(a)\text{ , gdy }s=i\\ 0_s\quad\text{ , gdy }s\neq i\end{cases}\text{ oraz }y_s=\begin{cases}\pi_j(b)\text{ , gdy }s=j\\ 0_s\quad\text{ , gdy }s\neq j\end{cases}.$$

Wówczas $x,y\in G$, $x*y=a*b\neq 0$ oraz $y*x=0$. Zatem łączny pierścień $(G,*)$ nie jest przemienny, skąd wynika, że G nie jest *ACR*-grupą.

2.3 Klasyfikacja torsyjnych *CR*-, *ACR*- i *AR*-grup

Poniższy lemat okaże się pomocny przy klasyfikacji torsyjnych *CR*-, *ACR*- i *AR*-grup przeprowadzonej w Twierdzeniu 2.3.

Lemat 2.7. Niech R będzie łącznym pierścieniem o grupie addytywnej A i niech M będzie lewostronnym R-modułem.

(i) Jeżeli $R^2\circ M\neq\{0\}$, to $A\oplus M$ nie jest *AR*-grupą.
(ii) Jeżeli $R\circ M\neq\{0\}$, to $A\oplus M$ nie jest *ACR*-grupą.

Dowód. Niech $G=A\oplus M$. Mnożenie pierścienia R oznaczmy standardową kropką.

(i). Rozważmy funkcję $*\colon G\times G\to G$ daną wzorem:

$$(a_1,m_1)*(a_2,m_2)=(0,a_1\circ m_2),$$

dla wszystkich $a_1,a_2\in A$ i $m_1,m_2\in M$. Bezpośrednie sprawdzenie pokazuje, że $S=(G,*)$ jest pierścieniem. Ponieważ $R^2\circ M\neq\{0\}$, to istnieją $r_1,r_2\in R$ oraz $m\in M$ takie, że $(r_1\cdot r_2)\circ m\neq 0$. Stąd $(r_1,0)*\big((r_2,0)*(0,m)\big)=(r_1,0)*(0,r_2\circ m)=\big(0,r_1\circ(r_2\circ m)\big)=\big(0,(r_1r_2)\circ m\big)\neq(0,0)$. Ale $\big((r_1,0)*(r_2,0)\big)*(0,m)=(0,0)*(0,m)=(0,0)$, więc pierścień jest niełączny. Zatem G nie jest *AR*-grupą.

(ii). Niech $\star\colon G\times G\to G$ będzie funkcją określoną za pomocą wzoru:

$$(a_1,m_1)\star(a_2,m_2)=(a_1\cdot a_2,a_1\circ m_2),$$

dla wszystkich $a_1,a_2\in A$ i $m_1,m_2\in M$. Na mocy standardowego sprawdzenia otrzymujemy wówczas, że $P=(G,\star)$ jest pierścieniem. Dla dowolnych $a_1,a_2,a_3\in A$ oraz $m_1,m_2,m_3\in M$ zachodzi $\big((a_1,m_1)\star(a_2,m_2)\big)\star(a_3,m_3)=(a_1\cdot a_2,a_1\circ m_2)\star$ $\star(a_3,m_3)=\big((a_1\cdot a_2)\cdot a_3,(a_1\cdot a_2)\circ m_3\big)=\big(a_1\cdot(a_2\cdot a_3),a_1\circ(a_2\circ m_3)\big)=(a_1,m_1)\star$ $\star(a_2\cdot a_3,a_2\circ m_3)=(a_1,m_1)\star\big((a_2,m_2)\star(a_3,m_3)\big)$, więc pierścień P jest łączny. Ponieważ $R\circ M\neq\{0\}$, to $r\circ m\neq 0$ dla pewnych $r\in R$ i $m\in M$. Stąd $(r,0)\star(0,m)=$ $=(0,r\circ m)\neq(0,0)$ oraz $(0,m)\star(r,0)=(0,0)$ i w konsekwencji łączny pierścień P nie jest przemienny. Zatem G nie jest ACR-grupą.

Wniosek 2.2. Dla wszystkich $m,n\in\mathbb{N}$ oraz dowolnej nietrywialnej grupy abelowej G ani $Z(p^m)\oplus Z(p^n)$, ani $\mathbb{Z}^+\oplus G$ nie jest AR-grupą. Grupy te nie są również ACR-grupami.

Twierdzenie 2.3. Dla dowolnej torsyjnej grupy abelowej G następujące warunki są równoważne:

(i) G jest CR-grupą;
(ii) G jest AR-grupą;
(iii) G jest ACR-grupą;
(iv) $G=\bigoplus_{p\in\mathbb{P}(G)}\Big(Z(p^{n_p})\oplus\big(\bigoplus_{i\in I_p}Z(p^\infty)\big)\Big)$, gdzie $n_p\in\mathbb{N}_0$ oraz I_p jest pewnym zbiorem dla każdego $p\in\mathbb{P}(G)$.

Dowód. Z Uwagi 2.1 wynika, że wystarczy udowodnić twierdzenie dla p-grup. Rozważmy więc dowolne $p\in\mathbb{P}$ oraz dowolną p-grupę abelową G. Jeżeli $G=\{0\}$, to równoważność warunków $(i)-(iv)$ jest oczywista. Niech dalej $G\neq\{0\}$.

Implikacje $(i)\Rightarrow(ii)$ oraz $(i)\Rightarrow(iii)$ są bezpośrednimi konsekwencjami odpowiednio Twierdzenia 2.2 i Uwagi 2.2.

Aby udowodnić implikacje $(ii)\Rightarrow(iv)$ oraz $(iii)\Rightarrow(iv)$ załóżmy, że nietrywialna p-grupa G nie jest postaci $Z(p^n)\oplus D$, gdzie n jest pewną nieujemną liczbą całkowitą, zaś D jest pewną podzielną p-grupą. Z (Fuchs, 1970, Corollary 27.3) wynika wówczas istnienie takich $m,s\in\mathbb{N}$, że grupa $Z(p^m)\oplus Z(p^s)$ jest składnikiem prostym w G. Zatem G nie jest ani AR-grupą, ani ACR-grupą na mocy Wniosku 2.2 i Stwierdzenia 2.1.

Przypuśćmy, że $G=Z(p^n)\oplus D$, gdzie n jest pewną nieujemną liczbą całkowitą, zaś D jest pewną podzielną p-grupą. Rozważmy dowolny pierścień R taki, że $R^+=G$. Ponieważ $D=p^nD$ i D jest nil-grupą, to $\{0\}\oplus D\subseteq\mathfrak{a}(R)$. Stąd, dla $A=Z(p^n)\oplus\{0\}$ otrzymujemy, że $R^2=A^2$. Ponadto $A\cong\mathbb{Z}^+_{p^n}$ i każde mnożenie pierścieniowe $*$ określone na grupie $\mathbb{Z}^+_{p^n}$ jest zdeterminowane przez wartość $1*1$, więc pierścień R jest łączny i przemienny. Wobec tego warunek (iv) implikuje każdy spośród warunków $(i)-(iii)$.

2.4 Klasyfikacja beztorsyjnych całkowicie rozkładalnych *CR*-grup

Ponieważ każda beztorsyjna grupa abelowa rangi jeden zanurza się w grupę $\mathbb{Q}^+$, to poniższe twierdzenie klasyfikuje beztorsyjne całkowicie rozkładalne *CR*-grupy.

Twierdzenie 2.4. Niech $\{G_i\colon i\in I\}$, gdzie $I\neq\emptyset$, będzie rodziną nietrywialnych podgrup grupy $\mathbb{Q}^+$ i niech $G=\bigoplus_{i\in I}G_i$. Wówczas następujące warunki są równoważne:

(i) G jest *CR*-grupą;
(ii) $n(G_i\cdot G_j)\not\subseteq G_k$ dla wszystkich $n\in\mathbb{N}$ oraz $i,j,k\in I$ takich, że $i\neq j$;
(iii) $\mathfrak{t}(G_i)\cdot\mathfrak{t}(G_j)\not\leq\mathfrak{t}(G_k)$ dla wszystkich $i,j,k\in I$ takich, że $i\neq j$.

Dowód. Równoważność warunków (ii) oraz (iii) jest bezpośrednią konsekwencją Wniosku 2.1. Udowodnimy równoważność warunków (i) oraz (ii). Załóżmy najpierw, że $n(G_i\cdot G_j)\subseteq G_k$ dla pewnych $n\in\mathbb{N}$ oraz $i,j,k\in I$ takich, że $i\neq j$. Mamy do rozważenia dwa przypadki:

(I). $i\neq j$ oraz $k=i$. Wówczas $(G_i\oplus G_j,*)$, gdzie $(a_1,c_1)*(a_2,c_2)=\big(n(a_1\cdot\cdot c_2),0\big)$, jest pierścieniem, w którym dla dowolnych niezerowych $a\in G_i$ oraz $c\in G_j$ jest $(a,0)*(0,c)=\big(n(a\cdot c),0\big)\neq(0,0)$ i $(0,c)*(a,0)=(0,0)$. Zatem $G_i\oplus G_j$ nie jest *CR*-grupą. Ponadto grupa G ma składnik prosty izomorficzny z $G_i\oplus G_j$, więc ze Stwierdzenia 2.1 wynika, że G nie jest *CR*-grupą.

(II). Elementy i,j,k są parami różne. Analogicznie jak w punkcie (I) uzasadnia się, że $(G_i\oplus G_j\oplus G_k,\star)$, gdzie $(a_1,b_1,c_1)\star(a_2,b_2,c_2)=\big(0,0,n(a_1\cdot b_2)\big)$ jest nieprzemiennym pierścieniem i w związku z tym G nie jest *CR*-grupą.

Na odwrót. Przypuśćmy teraz, że $n(G_i\cdot G_j)\not\subseteq G_k$, dla wszystkich $n\in\mathbb{N}$ oraz $i,j,k\in I$ takich, że $i\neq j$. Rozważmy dowolne $*\in\mathrm{Mult}(G)$. Niech $S=(G,*)$. Jeżeli $G*G=\{0\}$, to oczywiście pierścień S jest przemienny. Niech dalej $G*G\neq\{0\}$. Istnieją wówczas $a,c\in G$ oraz $i,j\in I$ takie, że $\pi_i(a)*\pi_j(c)\neq 0$, gdzie π_t jest naturalną projekcją grupy G na podgrupę $\overline{G_t}$ dla $t=i,j$. Z (Fuchs, 1973, Theorem 119.1) wynika istnienie pierścienia $R=\big(\mathscr{D}(G),\circledast\big)$ takiego, że S jest podpierścieniem w R. Weźmy dowolne $k\in\operatorname{supp}\big(\pi_i(a)*\pi_j(c)\big)$. Niech φ_t będzie naturalnym zanurzeniem grupy $\mathbb{Q}^+$ w grupę $\mathscr{D}(G)$ takim, że $\varphi_t(\mathbb{Q}^+)$ jest t-tym składnikiem prostym Q_t w $\mathscr{D}(G)$ dla $t=i,j$. Niech ponadto ψ_k będzie naturalnym rzutowaniem grupy $\mathscr{D}(G)$ na jej k-ty składnik prosty $Q_k\cong\mathbb{Q}^+$, niech $\phi\colon Q_k\to\mathbb{Q}^+$ będzie naturalnym izomorfizmem i niech $\vartheta=\phi\circ\psi_k$. Dla wszystkich $q_1,q_2\in\mathbb{Q}^+$ definiujemy $q_1\odot q_2=\vartheta\big(\varphi_i(q_1)\circledast\varphi_j(q_2)\big)$. Ponieważ ϑ, φ_i, φ_j są addytywnymi homomorfizmami oraz $\circledast$ jest niezerowym mnożeniem pierścieniowym, to mnożenie $\odot$ wprowadza na grupie $\mathbb{Q}^+$ strukturę pierścienia z niezerowym mnożeniem. Z (M. Woronowicz, 2016, Remark 4.2) wynika więc istnienie takiego $q\in\mathbb{Q}\setminus\{0\}$, że $q_1\odot q_2=q_1\cdot q\cdot q_2$ dla wszystkich $q_1,q_2\in\mathbb{Q}^+$. Zatem dla wszystkich $x\in G_i$ i $y\in G_j$ otrzymujemy, że:

$$q\cdot x\cdot y=x\odot y=\vartheta\big(\varphi_i(x)*\varphi_j(y)\big)\in G_k, \tag{2.4.1}$$

skąd $q(G_i \cdot G_j) \subseteq G_k$. Istnieje więc $n \in \mathbb{N}$ takie, że $n(G_i \cdot G_j) \subseteq G_k$, co wobec przyjętego założenia oznacza równość $j = i$. Z (2.4.1) oraz określenia funkcji ϑ wynika więc, że:

$$\psi_k\big(\varphi_i(g_1) * \varphi_i(g_2)\big) = \phi^{-1}(g_1 \cdot q \cdot g_2)$$

dla wszystkich $g_1, g_2 \in G_i$. Zatem:

$$\psi_k\big(\varphi_i(g_1) * \varphi_i(g_2)\big) = \psi_k\big(\varphi_i(g_2) * \varphi_i(g_1)\big) \tag{2.4.2}$$

dla wszystkich $g_1, g_2 \in G_i$. Ponadto uzyskana wcześniej równość $j = i$ implikuje, iż mnożenie $*$ jest całkowicie zdeterminowane przez wartości $\psi_k\big(\varphi_i(g_1) * \varphi_i(g_2)\big) \neq 0$, gdzie $i,k \in I$ i $g_1, g_2 \in G_i$, więc pierścień S jest przemienny. Wobec tego G jest CR-grupą.

2.5 Beztorsyjne $(A)CR$-grupy rangi dwa

Uwaga 2.3. Jeżeli A nie jest CR-grupą, to istnieje $\circ \in \mathrm{Mult}(A)$ takie, że $a_1 \circ a_2 \neq \neq a_2 \circ a_1$ dla pewnych $a_1, a_2 \in A$. Zatem $(A, \cdot)$, gdzie $a \cdot b = a \circ b - b \circ a$ dla wszystkich $a, b \in A$, jest pierścieniem z niezerowym mnożeniem, który jest antyprzemienny.

Twierdzenie 2.5. Każda beztorsyjna nierozkładalna grupa abelowa rangi dwa jest CR-grupą.

Dowód. Rozważmy dowolną beztorsyjną nierozkładalną grupę abelową A rangi dwa. Jeśli $\square A = \{0\}$, to teza jest oczywista. Niech dalej $\square A \neq \{0\}$. Załóżmy nie wprost, że A nie jest CR-grupą. Z Uwagi 2.3 wynika wówczas istnienie takiego antyprzemiennego pierścienia $R = (A, \cdot)$, że $R^2 \neq \{0\}$. Istnieją więc $a, b \in A$ takie, że $a^2 = b^2 = 0$, $ba = -ab$ i $ab \neq 0$. Załóżmy nie wprost, że elementy a i b są zależne. Wówczas $b = qa$ dla pewnego $q \in \mathbb{Q}$. Stąd $ab = qa^2 = 0$, sprzeczność. Wobec tego elementy a i b są niezależne. Ponadto $r(A) = 2$, więc istnieją $n \in \mathbb{N}$ oraz $k, l \in \mathbb{Z}$ takie, że $n(ab) = ka + lb$, przy czym $k^2 + l^2 > 0$. Ze względu na antyprzemienność pierścienia R, bez utraty ogólności możemy przyjąć, że $l \neq 0$. Wtedy, po obustronnym lewostronnym pomnożeniu ostatniej równości przez a, otrzymujemy, że $(na)(ab) = l(ab)$. Niech $\alpha = na$ i niech $\beta = ab$. Wówczas $\alpha\beta = l\beta$. Aby wykazać niezależność elementów α i β rozważmy dowolne $K, L \in \mathbb{Z}$ oraz załóżmy, że $K\alpha + L\beta = 0$. Wtedy $Kna + L(ab) = 0$, więc $Kn^2a + Ln(ab) = 0$. Stąd oraz na mocy uzasadnionej wcześniej równości $n(ab) = ka + lb$ otrzymujemy, że $(Kn^2 + Lk)a + Llb = 0$. Ale elementy a i b są niezależne oraz $l \neq 0$ i $n \in \mathbb{N}$, więc $L = K = 0$. Zatem elementy α i β są niezależne. Weźmy dowolne $x \in A$. Wtedy $sx = h\alpha + t\beta$ dla pewnych $s \in \mathbb{N}$ i $h, t \in \mathbb{Z}$. Zatem $s(\alpha x) = t(\alpha\beta) = (tl)\beta = l(t\beta) = l(sx - h\alpha)$, czyli $s(lx - \alpha x) = = (lh)\alpha$. Stąd $lx - \alpha x \in \langle\alpha\rangle_*$. Ponadto $s(\alpha x) = (tl)\beta$, więc $\alpha x \in \langle\beta\rangle_*$. Wobec tego $lx = (lx - \alpha x) + \alpha x \in \langle\alpha\rangle_* + \langle\beta\rangle_*$. Stąd oraz na mocy dowolności wyboru elementu x

i niezależności elementów α oraz β otrzymujemy, że $lA \subseteq \langle\alpha\rangle_* \oplus \langle\beta\rangle_* \subseteq A$. Ponadto $\mathfrak{t}(\alpha) \leq \mathfrak{t}(\beta)$ na mocy definicji elementów α i β oraz punktów (1.) i (4.) Lematu 2.5. Zatem (Arnold, 1982, Theorem 2.3) implikuje rozkładalność grupy A, sprzeczność.

Lemat 2.8. Niech $\{A_i\colon i \in I\}$, gdzie $|I| \geq 2$, będzie rodziną nietrywialnych podgrup grupy $\mathbb{Q}^+$ i niech $A = \bigoplus_{i\in I} A_i$. Jeżeli istnieją $i, j \in I$ takie, że $i \neq j$ oraz $\mathfrak{t}(A_i)\cdot\mathfrak{t}(A_j) = \mathfrak{t}(A_i)$, to A nie jest AR-grupą.

Dowód. Z (Fuchs, 1973, Propositions 85.3 & 85.4) wynika, że warunek $\mathfrak{t}(A_i)\cdot\mathfrak{t}(A_j) = \mathfrak{t}(A_i)$ równoważny jest warunkowi $\mathrm{Hom}\,(A_i \otimes A_j, A_i) \neq \{0\}$. Istnieją więc $a \in A_i$, $b \in A_j$ oraz homomorfizm $f\colon A_i \otimes A_j \to A_i$ takie, że $f(a\otimes b) \neq 0$. Dla $s \in \{i, j\}$ niech π_s będzie naturalną projekcją grupy A na grupę A_s i niech ι_s będzie naturalnym zanurzeniem grupy A_s w grupę A. Ponadto definiujemy $F = \iota_i \circ f$, $\alpha = \iota_i(a)$ oraz $\beta = \iota_j(b)$. Bezpośrednie sprawdzenie pokazuje, że funkcja $*\colon A \times A \to A$ dana wzorem:

$$x * y = F\big(\pi_i(x) \otimes \pi_j(y)\big)$$

dla wszystkich $x, y \in A$, wprowadza na grupie A strukturę pierścienia, w którym $\alpha * *\beta \neq 0$ i $\beta * \beta = 0$. Niech $c = \pi_i(\alpha * \beta)$. Wtedy $c \in A_i \setminus \{0\}$, więc $c = \frac{k}{n}a$ dla pewnych $k \in \mathbb{Z}\setminus\{0\}$ i $n \in \mathbb{N}$. Jeżeli $f(c\otimes b) = 0$, to $kf(a\otimes b) = f\big((ka)\otimes b\big) = f\big((nc)\otimes b\big) = nf(c\otimes b) = 0$, co jest niemożliwe, gdyż $k \neq 0$, $f(a\otimes b) \neq 0$ i $T(A_i) = \{0\}$. Stąd $f(c\otimes b) \neq 0$. Wobec tego $(\alpha * \beta) * \beta \neq 0$. Ale $\alpha * (\beta * \beta) = 0$, więc pierścień $(A, *)$ nie jest łączny. Zatem A nie jest AR-grupą.

Możemy teraz podać opis CR-grup rangi dwa. Udowodnimy mianowicie następujące

Twierdzenie 2.6. Niech A będzie beztorsyjną grupą abelową rangi dwa. Wówczas następujące warunki są równoważne:

(i) A nie jest AR-grupą;
(ii) A nie jest CR-grupą;
(iii) $A = A_1 \oplus A_2$, przy czym $A_1 \neq \{0\}$, $A_2 \neq \{0\}$ oraz $\mathfrak{t}(A_i)\cdot\mathfrak{t}(A_j) = \mathfrak{t}(A_i)$ dla pewnych $i, j \in \{1, 2\}$ takich, że $i \neq j$;
(iv) $A \cong B \oplus C$, gdzie B i C są takimi nietrywialnymi podgrupami w $\mathbb{Q}^+$, że $n(B\cdot C) \subseteq \subseteq C$ dla pewnego $n \in \mathbb{N}$;
(v) A jest grupą addytywną pewnego niełącznego i jednocześnie nieprzemiennego pierścienia.

Dowód. Implikacja $(i) \Rightarrow (ii)$ jest bezpośrednią konsekwencją Twierdzenia 2.2. Jeżeli A nie jest CR-grupą, to z Twierdzenia 2.5 wynika, że grupa A jest rozkładalna. Istnieją więc nietrywialne podgrupy A_1 i A_2 grupy A takie, że $A = A_1 \oplus A_2$. W szczególności wynika stąd, że $r(A_1) = r(A_2) = 1$. Stąd oraz na mocy Twierdzenia 2.4 i punktu (2.) Lematu 2.5 otrzymujemy, że $\mathfrak{t}(A_i)\cdot\mathfrak{t}(A_j) = \mathfrak{t}(A_i)$ dla pewnych $i, j \in \{1, 2\}$ takich, że $i \neq j$. Kończy to dowód implikacji $(ii) \Rightarrow (iii)$. Równoważność warunków (iii)

oraz (iv) wynika natychmiast z Wniosku 2.1 i znanego faktu, że każda beztorsyjna grupa abelowa rangi jeden zanurza się w $\mathbb{Q}^+$. Jeśli więc zachodzi warunek dany w (iv), to spełnione są założenia Lematu 2.8. Niech $*$ oznacza niełączne mnożenie pierścieniowe skonstruowane w jego dowodzie. Zachowując pozostałe oznaczenia zastosowane we wspomnianym dowodzie otrzymujemy wówczas, że $\alpha * \beta \neq 0$ i $\beta * \alpha = 0$. Zatem niełączny pierścień $(A,*)$ jest jednocześnie nieprzemienny. W ten sposób wykazaliśmy implikację $(iv) \Rightarrow (v)$. Implikacja $(v) \Rightarrow (i)$ jest oczywista.

Wniosek 2.3. Warunki *CR* i *AR* są równoważne dla beztorsyjnych grup abelowych rangi dwa.

Następne twierdzenie opisuje beztorsyjne *ACR*-grupy rangi dwa.

Twierdzenie 2.7. Niech A będzie beztorsyjną grupą abelową rangi dwa. Wówczas następujące warunki są równoważne:

(i) A nie jest *ACR*-grupą;
(ii) $A = A_1 \oplus A_2$, gdzie A_1 i A_2 są nietrywialnymi podgrupami grupy A spełniającymi warunki $\mathfrak{t}(A_i)^2 = \mathfrak{t}(A_i)$ oraz $\mathfrak{t}(A_i) \cdot \mathfrak{t}(A_j) = \mathfrak{t}(A_j)$ dla pewnych $i, j \in \{1,2\}$ takich, że $i \neq j$;
(iii) $A \cong B \oplus C$ dla pewnych nietrywialnych podgrup B i C grupy $\mathbb{Q}^+$ takich, że $\square B \neq \neq \{0\}$ oraz $n(B \cdot C) \subseteq C$ dla pewnego $n \in \mathbb{N}$;
(iv) istnieją dwa niezależne elementy $x, y \in A$, łączny pierścień $R = (A, \cdot)$ oraz nietrywialny homomorfizm $f\colon A \to \big(\mathfrak{N}(A)\big)^+$ takie, że $x \cdot y = f(x)y$ lub $x \cdot y = f(y)x$.

Dowód. $(i) \Rightarrow (ii)$. Warunek (i) implikuje, że A nie jest *CR* grupą, więc z Twierdzenia 2.6 i (M. Woronowicz, 2016, Remark 4.2) wynika, że bez utraty ogólności możemy przyjąć, iż $A = A_1 \oplus A_2$ dla pewnych podgrup A_1 i A_2 grupy $\mathbb{Q}^+$ zawierających liczbę 1. Niech $x = (1,0)$ i niech $y = (0,1)$. Wtedy $\{x,y\}$ jest maksymalnym podzbiorem niezależnym w A. Dalej, wprost z przyjętego założenia wynika istnienie łącznego pierścienia R o grupie addytywnej A, który nie jest przemienny. Niech $\star$ oznacza mnożenie pierścienia R. Z dowodu (Beaumont i Wisner, 1959, Lemma 2) wynika, że mamy do rozważenia następujące przypadki:

1. $x \star x = ax$, $x \star y = ay$, $y \star x = 0$ i $y \star y = 0$, gdzie $a \in \mathbb{Q} \setminus \{0\}$. Odpowiednio na mocy punktów (1.), (3.) i (2.) Lematu 2.5 otrzymujemy wówczas, że $\mathfrak{t}_A(x) = \mathfrak{t}_A(ax) = = \mathfrak{t}_A(x \star x) \geq \mathfrak{t}_A(x)^2 \geq \mathfrak{t}_A(x)$, czyli $\mathfrak{t}_A(x)^2 = \mathfrak{t}_A(x)$. Powołując się ponownie na ten sam zestaw punktów Lematu 2.5 uzyskujemy, że $\mathfrak{t}_A(y) = \mathfrak{t}_A(ay) = \mathfrak{t}_A(x \star y) \geq \geq \mathfrak{t}_A(x) \cdot \mathfrak{t}_A(y) \geq \mathfrak{t}_A(y)$. Zatem $\mathfrak{t}_A(x) \cdot \mathfrak{t}_A(y) = \mathfrak{t}_A(y)$. Ponadto $\langle x \rangle_* \cong A_1$ i $\langle y \rangle_* \cong A_2$, więc $\mathfrak{t}(A_1)^2 = \mathfrak{t}(A_1)$ oraz $\mathfrak{t}(A_1) \cdot \mathfrak{t}(A_2) = \mathfrak{t}(A_2)$.
2. $x \star x = 0$, $x \star y = 0$, $y \star x = bx$ i $y \star y = by$, gdzie $b \in \mathbb{Q} \setminus \{0\}$. Rozumując analogicznie jak w punkcie 1. otrzymujemy stąd, że $\mathfrak{t}(A_2)^2 = \mathfrak{t}(A_2)$ oraz $\mathfrak{t}(A_2) \cdot \mathfrak{t}(A_1) = \mathfrak{t}(A_1)$.

3. $x\star x = ax$, $x\star y = ay$, $y\star x = bx$ i $y\star y = by$, gdzie $a,b \in \mathbb{Q}\setminus\{0\}$. Stosując te same techniki jak w przypadku 1. uzyskujemy wówczas, że $\mathfrak{t}_A(x)^2 = \mathfrak{t}_A(x)$, $\mathfrak{t}_A(x)\cdot \mathfrak{t}_A(y) = \mathfrak{t}_A(y)$, $\mathfrak{t}_A(y)\cdot\mathfrak{t}_A(x) = \mathfrak{t}_A(x)$ i $\mathfrak{t}_A(y)^2 = \mathfrak{t}_A(y)$. Ale $\mathfrak{t}_A(x)\cdot\mathfrak{t}_A(y) = \mathfrak{t}_A(y)\cdot\mathfrak{t}_A(x)$, więc $\mathfrak{t}_A(y) = \mathfrak{t}_A(x)$. Ponadto $\langle x\rangle_* \cong A_1$ i $\langle y\rangle_* \cong A_2$, skąd $\mathfrak{t}(A_1)^2 = \mathfrak{t}(A_1)$ oraz $\mathfrak{t}(A_1)\cdot\mathfrak{t}(A_2) = \mathfrak{t}(A_2)$.
4. $x\star x = ax$, $x\star y = bx$, $y\star x = ay$ i $y\star y = by$, gdzie $a,b \in \mathbb{Q}\setminus\{0\}$. Wtedy, analogicznie jak w punkcie 3. pokazuje się, że $\mathfrak{t}(A_1)^2 = \mathfrak{t}(A_1)$ oraz $\mathfrak{t}(A_1)\cdot\mathfrak{t}(A_2) = \mathfrak{t}(A_2)$.

$(ii) \Rightarrow (i)$. Bez utraty ogólności możemy przyjąć, że A_1 i A_2 są podgrupami w $\mathbb{Q}^+$ zawierającymi liczbę 1 takimi, że $\mathfrak{t}(A_1)^2 = \mathfrak{t}(A_1)$ oraz $\mathfrak{t}(A_1)\cdot\mathfrak{t}(A_2) = \mathfrak{t}(A_2)$. Z Wniosku 2.1 wynika wówczas istnienie takich $n_1, n_2 \in \mathbb{N}$, że $n_1(A_1\cdot A_1) \subseteq A_1$ oraz $n_2(A_1\cdot A_2) \subseteq A_2$. Niech $n = \mathrm{NWW}(n_1,n_2)$. Wtedy $n \in A_1 \cap A_2$ oraz $n(A_1\cdot A_1) \subseteq A_1$ i $n(A_1\cdot A_2) \subseteq A_2$. Rozważmy funkcję $\circledast\colon A\times A \to A$ daną wzorem:

$$(a_1,a_2)\circledast(b_1,b_2) = (a_1\cdot n\cdot b_1, a_1\cdot n\cdot b_2)$$

dla wszystkich $a_1,b_1 \in A_1$ i $a_2,b_2 \in A_2$. Bezpośrednie sprawdzenie pokazuje, że $\circledast \in \mathrm{Mult}(A)$. Niech $S = (A,\circledast)$. Wtedy dla dowolnych $a_1,b_1,c_1 \in A_1$ i $a_2,b_2,c_2 \in A_2$, $\big((a_1,a_2)\circledast(b_1,b_2)\big)\circledast(c_1,c_2) = \big(n^2\cdot a_1\cdot b_1\cdot c_1, n^2\cdot a_1\cdot b_1\cdot c_2\big) = (a_1,a_2)\circledast\big((b_1,b_2)\circledast (c_1,c_2)\big)$. Zatem pierścień S jest łączny. Ale $(1,0)\circledast(0,1) = (0,n) \neq (0,0)$ oraz $(0,1)\circledast(1,0) = (0,0)$, więc pierścień S nie jest przemienny. Wobec tego A nie jest ACR-grupą.

W ten sposób udowodniliśmy równoważność warunków (i) oraz (ii). Równoważność warunków (ii) oraz (iii) jest bezpośrednią konsekwencją Wniosku 2.1, (M. Woronowicz, 2016, Theorem 4.8) i możliwości zanurzenia każdej beztorsyjnej grupy abelowej rangi jeden w $\mathbb{Q}^+$. Natomiast równoważność warunków (i) oraz (iv) wynika wprost z (Beaumont i Wisner, 1959, Theorem 2).

Bezpośrednią konsekwencją Twierdzeń 2.6 i 2.7 jest następujące

Twierdzenie 2.8. Beztorsyjna grupa abelowa A rangi dwa jest ACR-grupą niebędącą CR-grupą wtedy i tylko wtedy, gdy $A = A_1 \oplus A_2$ dla pewnych nietrywialnych podgrup A_1 i A_2 grupy A takich, że zachodzi dokładnie jeden z dwóch następujących przypadków:

(i) $\mathfrak{t}(A_i)^2 = \mathfrak{t}(A_i)$, $\mathfrak{t}(A_j)^2 > \mathfrak{t}(A_j)$, $\mathfrak{t}(A_i)\cdot\mathfrak{t}(A_j) = \mathfrak{t}(A_i)$ dla pewnych $i,j \in \{1,2\}$;
(ii) $\mathfrak{t}(A_i)^2 > \mathfrak{t}(A_i)$, $\mathfrak{t}(A_j)^2 > \mathfrak{t}(A_j)$ oraz $\mathfrak{t}(A_i)\cdot\mathfrak{t}(A_j) = \mathfrak{t}(A_i)$ dla pewnych $i,j \in \{1,2\}$ takich, że $i \neq j$.

Uwaga 2.4. Z punktu (2.) Lematu 2.5 wynika ponadto, że jeśli grupa A spełnia warunek (i) powyższego twierdzenia, to $\mathfrak{t}(A_i) > \mathfrak{t}(A_j)$.

Wniosek 2.4. Istnieje $2^{\aleph_0}$ nieizomorficznych ACR-grup rangi dwa niebędących CR-grupami spełniających warunek (i) Twierdzenia 2.8 oraz $2^{\aleph_0}$ nieizomorficznych ACR-grup rangi dwa niebędących CR-grupami spełniających warunek (ii) tego twierdzenia.

Dowód. Niech $\{P_1, P_2, P_3\}$ będzie trójelementowym podziałem zbioru $\mathbb{P}$ takim, że $|P_i| = \aleph_0$ dla każdego $i \in \{1,2,3\}$ i niech P_0 będzie dowolnym podzbiorem zbioru P_3. Ponadto definiujemy:

$$B = \left\langle \frac{1}{p} : p \in P_0 \cup P_1 \right\rangle, \quad B_1 = \left\langle \frac{1}{q} : q \in P_2 \right\rangle, \quad C = \left[\frac{1}{p} : p \in P_0 \cup P_1 \right]^+,$$

$$C_1 = B_1 + C, \quad A = B \oplus C, \quad A_1 = B \oplus C_1.$$

Wtedy $\mathfrak{t}(B)^2 > \mathfrak{t}(B)$, $\mathfrak{t}(C)^2 = \mathfrak{t}(C)$, $\mathfrak{t}(C) > \mathfrak{t}(B)$, $\mathfrak{t}(C) \cdot \mathfrak{t}(B) = \mathfrak{t}(C)$ oraz $\mathfrak{t}(C_1)^2 > \mathfrak{t}(C_1)$ i $\mathfrak{t}(B) \cdot \mathfrak{t}(C_1) = \mathfrak{t}(C_1)$, więc z Twierdzenia 2.8 wynika, że A i A_1 są ACR-grupami niebędącymi CR-grupami.

Ponieważ $|P_3| = \aleph_0$, to P_3 zawiera dokładnie $2^{\aleph_0}$ niepustych podzbiorów różnych od P_0. Niech $P_0^\dagger$ będzie dowolnym takim podzbiorem i niech:

$$B^\dagger = \left\langle \frac{1}{p} : p \in P_0^\dagger \cup P_1 \right\rangle, \quad C^\dagger = \left[\frac{1}{p} : p \in P_0^\dagger \cup P_1 \right]^+, \quad C_1^\dagger = B_1 + C^\dagger,$$

$$A^\dagger = B^\dagger \oplus C^\dagger, \quad A_1^\dagger = B^\dagger \oplus C_1^\dagger.$$

Z poprzedniej części dowodu wynika, że $A^\dagger$ i $A_1^\dagger$ są ACR-grupami niebędącymi CR-grupami. Ponieważ $P_0^\dagger \neq P_0$ i $P_1 \cap P_3 = \emptyset$, to $C^\dagger \ncong C$ i $C_1^\dagger \ncong C_1$. Na mocy (Fuchs, 1973, Proposition 86.1) otrzymujemy więc, że $A^\dagger \ncong A$ oraz $A_1^\dagger \ncong A_1$.

Uwaga 2.5. Twierdzenie 2.6 opisuje w szczególności wszystkie beztorsyjne grupy abelowe rangi dwa, na których istnieje struktura niełącznego i jednocześnie nieprzemiennego pierścienia. Wniosek 2.4 implikuje więc istnienie $2^{\aleph_0}$ nieizomorficznych grup mających tę własność.

2.6 O strukturze mieszanych $(A)CR$-grup

Lemat 2.9. Jeżeli G jest mieszną $(A)CR$-grupą i $p \in \mathbb{P}(G)$, to G_p jest $(A)CR$-grupą.

Dowód. Załóżmy, że G_p nie jest $(A)CR$-grupą. Z (Fuchs, 1970, Theorem 24.5 & Corollary 27.3) i Twierdzenia 2.3 wynika wówczas istnienie takich $m,n \in \mathbb{N}$, że $Z(p^m) \oplus Z(p^n)$ jest składnikiem prostym w G. Stąd oraz na mocy Wniosku 2.2, Stwierdzenia 2.1 i Uwagi 2.2 otrzymujemy, że G nie jest $(A)CR$-grupą.

Twierdzenie 2.9. Niech G będzie mieszaną ACR-grupą i niech $p \in \mathbb{P}(G)$. Wówczas G_p jest składnikiem prostym w G. Jeżeli H jest uzupełnieniem prostym podgrupy G_p w grupie G, to $\dim_{\mathbb{Z}_p} H/pH \leq 1$. W szczególności $H = pH$, gdy grupa G_p nie jest ani podzielna, ani zredukowana. Ponadto, jeśli grupa G_p nie jest cykliczna, to $r_0(H) = 1$.

Dowód. Niech D będzie największą podzielną podgrupą w G_p. Z (Fuchs, 1970, Theorem 24.5) wynika wówczas, że $G = D \oplus B$ dla pewnej podgrupy B grupy G. Zatem $G_p = D \oplus B_p$ oraz grupa B_p jest zredukowana. Stąd oraz na mocy Lematu 2.9 i Twierdzenia 2.3 otrzymujemy, że $\exp(B_p) < \infty$. Ponadto B_p jest czystą podgrupą w B, więc B_p jest składnikiem prostym w B na mocy (Fuchs, 1970, Theorem 27.5). Wobec tego G_p jest składnikiem prostym w G. Z Twierdzenia 2.3 wynika, że mamy do rozważenia trzy przypadki:

(i). $G_p = Z(p^n)$, gdzie $n \in \mathbb{N}$. Jeżeli $\dim_{\mathbb{Z}_p} H/pH > 1$, to Lemat 2.2 implikuje istnienie łącznego pierścienia o grupie addytywnej G, który nie jest przemienny, sprzeczność. Zatem $\dim_{\mathbb{Z}_p} H/pH \leq 1$.

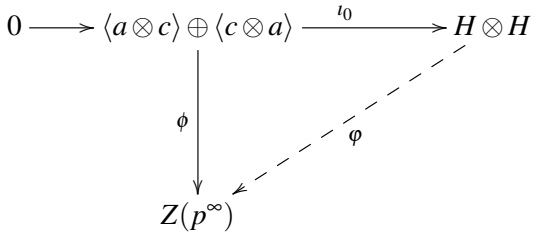
(ii). G_p jest grupą podzielną. Wtedy $\dim_{\mathbb{Z}_p} H/pH \leq 1$ na mocy argumentacji identycznej jak w punkcie (i).

(iii). $G_p = Z(p^n) \oplus D$, gdzie $n \in \mathbb{N}$ oraz D jest nietrywialną podzielną p-grupą. Wtedy grupa G ma składnik prosty izomorficzny z grupą $C = \mathbb{Z}^+_{p^n} \oplus Z(p^\infty) \oplus H$. Stwierdzenie 2.1 implikuje, że C jest ACR-grupą. Załóżmy nie wprost, że $H \neq pH$. Niech $\pi\colon H \to \mathbb{Z}^+_p$ będzie epimorfizmem, zaś $\iota\colon \mathbb{Z}^+_p \to \mathbb{Z}^+_{p^n}$ oraz $\iota\colon \mathbb{Z}^+_{p^n} \to Z(p^\infty)$ – naturalnymi zanurzeniami. Niech ponadto $f = \iota \circ \pi$. Bezpośrednie sprawdzenie pokazuje, że funkcja $*\colon C \times C \to C$ dana za pomocą wzoru:

$$(k_1, d_1, h_1) * (k_2, d_2, h_2) = \Big(0, \iota\big(k_1 \odot_{p^n} f(h_2)\big), 0\Big)$$

dla wszystkich $k_1, k_2 \in \mathbb{Z}^+_{p^n}$, $d_1, d_2 \in D$ i $h_1, h_2 \in H$, wprowadza na grupie C strukturę pierścienia. Ponadto $(C * C) * C = C * (C * C) = \{0\}$, więc pierścień $(C, *)$ jest łączny. Z określenia funkcji f wynika istnienie takiego $h \in H$, że $f(h) \neq 0$. Stąd $(1,0,0) * (0,0,h) = \Big(0, \iota\big(1 \odot_{p^n} f(h)\big), 0\Big) \neq (0,0,0)$. Ale $(0,0,h) * (1,0,0) = (0,0,0)$, więc pierścień $(C, *)$ nie jest przemienny. Zatem C nie jest ACR-grupą, sprzeczność. Wobec tego $H = pH$.

Jeżeli grupa G_p nie jest cykliczna, to zachodzi przypadek (ii) lub (iii). W obu tych przypadkach $E = Z(p^\infty) \oplus H$ jest składnikiem prostym w G. Załóżmy nie wprost, że $r_0(H) > 1$. Istnieją wówczas $a, c \in H \setminus T(H)$ takie, że $\langle a \rangle + \langle c \rangle = \langle a \rangle \oplus \langle c \rangle$. Stąd oraz na mocy (Feigelstock, 1974, Theorem 2) i podstawowych własności produktu tensorowego grup abelowych otrzymujemy, że $\langle a \otimes c \rangle \oplus \langle c \otimes a \rangle$ jest wolną podgrupą grupy $H \otimes H$. Weźmy dowolne $d \in Z(p^\infty) \setminus \{0\}$. Wówczas $\langle d \rangle = Z(p^s)$ dla pewnego $s \in \mathbb{N}$. Ponieważ $\langle a \otimes c \rangle / p^s \langle a \otimes c \rangle \cong Z(p^s)$, to istnieje epimorfizm $\psi\colon \langle a \otimes c \rangle \to Z(p^s)$ taki, że $\psi(a \otimes c) = d$. Niech $\vartheta\colon \langle a \otimes c \rangle \oplus \langle c \otimes a \rangle \to \langle a \otimes c \rangle$ będzie naturalnym rzutowaniem i niech $\phi = \psi \circ \vartheta$. Wtedy $\phi \in \operatorname{Hom}\big(\langle a \otimes c \rangle \oplus \langle c \otimes a \rangle, Z(p^\infty)\big)$ oraz $\phi(a \otimes c) = d$ i $\phi(c \otimes a) = 0$. Niech ι_0 będzie restrykcją odwzorowania identycznościowego na $H \otimes H$ do podgrupy $\langle a \otimes c \rangle \oplus \langle c \otimes a \rangle$. Z injektywności grupy $Z(p^\infty)$ (zob. (Fuchs, 1970, Theorem 24.5)) wynika wówczas istnienie takiego homomorfizmu $\varphi\colon H \otimes H \to Z(p^\infty)$, że $\phi = \varphi \circ \iota_0$. Opisaną sytuację ilustruje poniższy diagram:



Bezpośrednie sprawdzenie pokazuje, że funkcja $\star\colon E\times E\to E$ dana wzorem:

$$(d_1,h_1)\star(d_2,h_2)=\big(\varphi(h_1\otimes h_2),0\big)$$

dla wszystkich $d_1,d_2\in Z(p^\infty)$ i $h_1,h_2\in H$, wprowadza na grupie E strukturę pierścienia, w którym $(0,a)\star(0,c)=(d,0)$ i $(0,c)\star(0,a)=(0,0)$. Ale $(E\star E)\star E=\{0\}$ oraz $E\star(E\star E)=\{0\}$. Zatem $(E,\star)$ jest pierścieniem łącznym, który nie jest przemienny. Wobec tego E nie jest *ACR*-grupą. Stąd oraz na mocy Stwierdzenia 2.1, również G nie jest *ACR*-grupą, sprzeczność.

Następne twierdzenie charakteryzuje mieszane *CR*-grupy i jest wynikiem komplementarnym względem Twierdzenia 2.9. W celu uproszczenia zapisów, w jego dowodzie stosowana będzie notacja związana z zewnętrznymi sumami prostymi.

Twierdzenie 2.10. Niech G będzie mieszaną *CR*-grupą i niech $p\in\mathbb{P}(G)$. Wówczas $G=G_p\oplus H$ dla pewnej p-podzielnej podgrupy H grupy G. Jeżeli grupa G_p nie jest cykliczna, to $r_0(H)=1$.

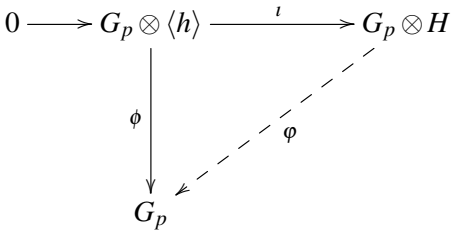
Dowód. Analogicznie jak w dowodzie Twierdzenia 2.9 uzasadnia się, że $G=G_p\oplus H$ dla pewnej podgrupy H grupy G. Z Uwagi 2.2 wynika, że G jest *ACR*-grupą, więc Twierdzenie 2.9 implikuje równość $r_0(H)=1$ warunkowaną brakiem cykliczności grupy G_p oraz nierówność $\dim_{\mathbb{Z}_p}H/pH\leq 1$. Załóżmy nie wprost, że $\dim_{\mathbb{Z}_p}H/pH=$ $=1$. Powołując się ponownie na Twierdzenie 2.9 otrzymujemy wówczas, że grupa G_p jest zredukowana albo podzielna.

Jeżeli zachodzi pierwszy przypadek, to ze Stwierdzenia 2.1 i Twierdzenia 2.3 wynika, że bez utraty ogólności możemy przyjąć, iż $G_p=\mathbb{Z}^+_{p^n}$ dla pewnego $n\in\mathbb{N}$. Wtedy $p^{n-1}G_p\cong\mathbb{Z}^+_p$, więc warunek $\dim_{\mathbb{Z}_p}H/pH=1$ implikuje istnienie epimorfizmu $f\colon H\to p^{n-1}G_p$. Bezpośrednie sprawdzenie pokazuje, że odwzorowanie $*\colon G\times G\to G$ dane wzorem:

$$(g_1,h_1)*(g_2,h_2)=\big(g_1\odot_{p^n}f(h_2),0\big),$$

gdzie $g_1,g_2\in G_p$, $h_1,h_2\in H$, wprowadza na grupie G strukturę pierścienia. Ponieważ f jest epimorfizmem, to istnieje $h\in H$ takie, że $f(h)=p^{n-1}$. Stąd $(1,0)*(0,h)=$ $=\big(p^{n-1},0\big)\neq(0,0)$ oraz $(0,h)*(1,0)=(0,0)$. Zatem $(1,0)*(0,h)\neq(0,h)*(1,0)$, skąd wynika, że G nie jest *CR*-grupą, sprzeczność. Zatem zachodzi drugi przypadek,

czyli grupa G_p jest nietrywialną podzielną p-grupą. Weźmy dowolne $h \in H \setminus pH$. Wtedy $o(h) = \infty$, więc $\langle h \rangle \cong \mathbb{Z}^+$ i w konsekwencji istnieje izmorfizm $\phi\colon G_p \otimes \langle h \rangle \to$ $\to G_p$ (por. (Fuchs, 1970, p. 255, (G))). Niech $\iota\colon G_p \otimes \langle h \rangle \to G_p \otimes H$ będzie naturalną injekcją. Ponieważ grupa G_p jest injektywna (por. (Fuchs, 1970, Theorem 24.5)), to istnieje homomorfizm $\varphi\colon G_p \otimes H \to G_p$ spełniający warunek $\phi = \varphi \circ \iota$. Opisaną sytuację przedstawia diagram:



Standardowe sprawdzenie uzasadnia, że funkcja $\star\colon G \times G \to G$ określona za pomocą wzoru:

$$(g_1, h_1) \star (g_2, h_2) = \big(\varphi(g_1 \otimes h_2), 0\big),$$

dla wszystkich $g_1, g_2 \in G_p$ oraz $h_1, h_2 \in H$, wprowadza na grupie G strukturę pierścienia. Oznaczmy ten pierścień przez R i weźmy dowolne $g \in G_p \setminus \{0\}$. Wtedy $(0,h) \star (g,0) = \big(\varphi(0 \otimes 0), 0\big) = (0,0)$ oraz $(g,0) \star (0,h) = \big(\varphi(g \otimes h), 0\big) \neq (0,0)$, gdyż $\varphi(g \otimes h) = \varphi\big(\iota(g \otimes h)\big) = \phi(g \otimes h)$, $\ker(\phi) = \{0\}$ i $g \otimes h \neq 0$ (por. (Fuchs, 1970, p. 255, (G))). Zatem pierścień R nie jest przemienny, skąd wynika, że G nie jest *CR*-grupą, sprzeczność. Wobec tego $\dim_{\mathbb{Z}_p} H/pH = 0$, czyli $H = pH$.

Następny rezultat będzie pomocny we wskazaniu przykładu mieszanej *ACR*-grupy niebędącej *CR*-grupą (zob. Przykład 2.1).

Stwierdzenie 2.3. Niech H będzie nil_a-grupą taką, że $H_p = \{0\}$ dla pewnej liczby pierwszej p. Jeżeli istnieje $h_0 \in H$ takie, że $H = \langle h_0 \rangle + pH$, to $A = Z(p) \oplus H$ jest *ACR*-grupą.

Dowód. Niech $\xi = (0, h_0)$. Rozważmy dowolny łączny pierścień R o grupie addytywnej A. Z Lematu 2.4 wynika, że jeśli $R^2 \neq \{0\}$ i $R \ncong \mathbb{Z}_p \times H^0$, to $R = \langle \xi \rangle + \mathfrak{a}(R)$, przy czym $o\left(\xi^2\right) = p$. Weźmy dowolne $a, b \in R$. Wtedy $a = k\xi + x$ oraz $b = l\xi + y$ dla pewnych $k, l \in \mathbb{Z}$ i $x, y \in \mathfrak{a}(R)$. Stąd $ab = (kl)\xi^2 = ba$. Zatem pierścień R jest przemienny w każdym z możliwych przypadków. Wobec tego A jest *ACR*-grupą.

Przykład 2.1. Niech H będzie nietrywialną nil-podgrupą grupy $\mathbb{Q}^+$. Wtedy $H \neq pH$ dla pewnego $p \in \mathbb{P}$. Z (Arnold, 1982, Theorem 1.4) wynika więc, że H spełnia założenia Stwierdzenia 2.3. Zatem $A = Z(p) \oplus H$ jest *ACR*-grupą. Jednak A nie jest *CR*-grupą na mocy Twierdzenia 2.10. W szczególności wynika stąd, że A nie jest *AR*-grupą.

Na mocy Twierdzenia 2.3, Przykładu 2.1 i Wniosku 2.4 otrzymujemy następujący

Wniosek 2.5. Warunki *CR* i *ACR* są równoważne wyłącznie w klasie torsyjnych grup abelowych.

Ponieważ warunek $H \neq pH$ implikuje istnienie epimorfizmu $f\colon H \to Z(p)$, to fakt, że grupa A z Przykładu 2.1 nie jest *CR*-grupą można uzasadnić również w oparciu o następujące

Stwierdzenie 2.4. Niech A i H będą grupami abelowymi. Jeżeli A nie jest nil-grupą oraz A jest obrazem homomorficznym grupy H, to $A \oplus H$ nie jest *CR*-grupą.

Dowód. Niech $f\colon H \to A$ będzie epimorfizmem i niech $R = (A, \cdot)$ będzie dowolnym pierścieniem takim, że $R^2 \neq \{0\}$. Bezpośrednie sprawdzenie pokazuje, że odwzorowanie $*\colon (A \oplus H) \times (A \oplus H) \to (A \oplus H)$ dane wzorem:

$$(a_1, h_1) * (a_2, h_2) = \big(a_1 \cdot f(h_2), 0\big),$$

dla wszystkich $a_1, a_2 \in A$ i $h_1, h_2 \in H$, wprowadza na grupie $A \oplus H$ strukturę pierścienia. Ponieważ $R^2 \neq \{0\}$, to istnieją $a, b \in A$ takie, że $a \cdot b \neq 0$. Weźmy dowolne $h \in f^{-1}\big(\{b\}\big)$. Wtedy $(a,0) * (0,h) \neq (0,0)$ oraz $(0,h) * (a,0) = (0,0)$, więc $A \oplus H$ nie jest *CR*-grupą.

Okazuje się, że twierdzenie odwrotne do Twierdzenia 2.2 nie jest prawdziwe, tj. istnieją *AR* grupy niebędące *CR*-grupami (zob. Przykład 2.2). Aby się o tym przekonać udowodnimy najpierw następujące

Twierdzenie 2.11. Jeżeli C jest nietrywialną torsyjną *AR*-grupą oraz A beztorsyjną nil-grupą taką, że $A = pA$ dla każdego $p \in \mathbb{P}(C)$, to $G = C \oplus A$ jest *AR*-grupą.

Dowód. Niech D będzie największą podzielną podgrupą grupy C i niech K będzie zredukowanym składnikiem prostym w C komplementarnym względem D. Wówczas $G = K \oplus D \oplus A$ oraz Twierdzenia 2.1 i 2.3 wraz z podstawowymi własnościami produktu tensorowego grup abelowych i grupy homomorfizmów addytywnych implikują, że $G \otimes G \cong K \oplus (A \otimes A)$ oraz $\mathrm{Mult}(G) \cong \mathrm{Mult}(K) \oplus \mathrm{Hom}\big((K \oplus \oplus A) \otimes (K \oplus A), D\big)$ (por. (Fuchs, 1970, p. 255: (I), (D) & (H)) oraz (Fuchs, 1970, Theorems 43.1 & 43.2); w szczególności $\mathrm{Hom}(A \otimes A, K) = \{0\}$, gdyż grupa $A \otimes A$ jest p-podzielna oraz grupa K_p jest p-zredukowana dla każdego $p \in \mathbb{P}(K)$). Ponadto z Twierdzenia 2.3 wynika, że K jest *CR*-grupą, więc jeśli $* \in \mathrm{Mult}(G)$, to istnieją łączne i przemienne mnożenie pierścieniowe $\diamond\colon K \times K \to K$ oraz homomorfizm $\xi\colon (K \oplus A) \otimes (K \oplus A) \to D$ takie, że:

$$(k_1, d_1, a_1) * (k_2, d_2, a_2) = \Big(k_1 \diamond k_2, \xi\big((k_1, a_1) \otimes (k_2, a_2)\big), 0\Big),$$

dla wszystkich $k_1,k_2 \in K$, $d_1,d_2 \in D$ oraz $a_1,a_2 \in A$ (w celu ujednolicenia zapisu grupę C traktujemy jak zewnętrzną sumę prostą grup K i D). Dla dowolnych $k_1,k_2,k_3 \in K$ oraz $a_1,a_2,a_3 \in A$ otrzymujemy, że $\xi\big((k_1 \diamond k_2,0)\otimes(k_3,a_3)\big) = \xi\big((k_1\diamond \diamond k_2,0)\otimes(k_3,0)\big)$. Ponadto istnieje taki składnik prosty H grupy K, że $k_1,k_2,k_3 \in H$ oraz $H \cong \mathbb{Z}_m^+$ dla pewnego $m \in \mathbb{N}$. Niech h będzie generatorem grupy cyklicznej H. Dla $i = 1,2,3$ istnieje wówczas $l_i \in \mathbb{Z}$ takie, że $k_i = l_i h$. Stąd $\xi\big((k_1 \diamond k_2,0)\otimes \otimes(k_3,0)\big) = (l_1l_2l_3)\xi\big((h\diamond h,0)\otimes(h,0)\big)$. Z określenia grupy H, Twierdzenia 2.3 i Uwagi 2.1 wynika, że $h\diamond h \in H$, skąd $h\diamond h = lh$ dla pewnego $l \in \mathbb{Z}$. Zatem $\xi\big((k_1\diamond k_2,0)\otimes(k_3,a_3)\big) = (ll_1l_2l_3)\xi\big((h,0)\otimes(h,0)\big)$. Analogicznie, $\xi\big((k_1,a_1)\otimes(k_2\diamond \diamond k_3,0)\big) = (ll_1l_2l_3)\xi\big((h,0)\otimes(h,0)\big)$. Wobec tego pierścień $(G,*)$ jest łączny. Zatem G jest AR-grupą.

Przykład 2.2. Niech $A = \left\langle \frac{1}{p} : p \in \mathbb{P} \right\rangle + \left[\frac{1}{2}\right]^+$, niech $H = A \oplus A$ i niech $G = Z(2^\infty)\oplus \oplus H$. Wtedy H jest beztorsyjną grupą abelową rangi dwa. Ponadto, z (M. Woronowicz, 2016, Remark 4.5 & Theorem 4.8) i (Andruszkiewicz i Woronowicz, 2016a, Proposition 2.10) wynika, że H jest 2-podzielną nil-grupą. Stąd oraz na mocy Twierdzeń 2.10 i 2.11 otrzymujemy, że G jest AR-grupą niebędącą CR-grupą. W szczególności G nie jest ACR-grupą.

Bezpośrednią konsekwencją Twierdzenia 2.2 oraz Przykładu 2.2 jest następujące

Twierdzenie 2.12. Klasa CR-grup jest właściwą podklasą klasy AR-grup.

Ponadto z Przykładów 2.2 i 2.1 wynika natychmiast poniższy

Wniosek 2.6. Istnieją mieszane AR-grupy niebędące ACR-grupami oraz istnieją mieszane ACR-grupy niebędące AR-grupami.

Stwierdzenie 2.5. Jeżeli C jest nietrywialną torsyjną CR-grupą oraz A jest podgrupą grupy $\mathbb{Q}^+$ taką, że $A = pA$ dla każdego $p \in \mathbb{P}(C)$, to $G = C \oplus A$ jest CR-grupą.

Dowód. Niech D będzie największą podzielną podgrupą grupy C i niech K będzie zredukowanym składnikiem prostym w C komplementarnym względem D. Załóżmy najpierw, że A jest nil-grupą. Zachowując wszystkie oznaczenia z dowodu Twierdzenia 2.11 otrzymujemy, że $\xi\big((k_1,a_1)\otimes(k_2,a_2)\big) = \xi\big((k_1,0)\otimes(k_2,0)\big) + \xi\big((0,a_1)\otimes \otimes(0,a_2)\big)$. Ponieważ $a_1,a_2 \in \mathbb{Q}$, to $(0,a_1)\otimes(0,a_2) = (0,a_2)\otimes(0,a_1)$. Ponadto istnieje taki składnik prosty H grupy K, że $k_1,k_2 \in H$ i $H \cong \mathbb{Z}_m$ dla pewnego $m \in \mathbb{N}$. Istnieją więc $h \in H$ oraz $l_1,l_2 \in \mathbb{Z}$ takie, że $H = \langle h\rangle$ oraz $k_1 = l_1h$ i $k_2 = l_2h$. Stąd $\xi\big((k_1,0)\otimes(k_2,0)\big) = (l_1l_2)\xi\big((h,0)\otimes(h,0)\big) = (l_2l_1)\xi\big((h,0)\otimes(h,0)\big) = \xi\big((k_1,0)\otimes \otimes(k_2,0)\big)$. Zatem pierścień $(G,*)$, gdzie $*$ jest mnożeniem opisanym w dowodzie Twierdzenia 2.11, jest przemienny. Wobec tego G jest CR-grupą.

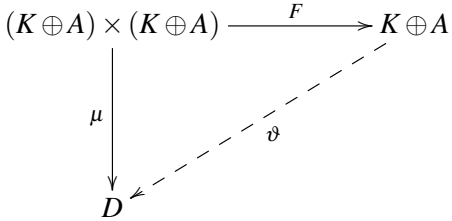
Przypuśćmy teraz, że A nie jest nil-grupą. Bez utraty ogólności możemy przyjąć, że $1 \in A$ (por. (M. Woronowicz, 2016, Remark 4.2)). Mamy do rozważenia trzy przypadki:

(i) $C = K$. Wtedy teza jest bezpośrednią konsekwencją Lematu 2.1 oraz (M. Woronowicz, 2016, Remark 4.2).

(ii). $C = K \oplus D$, gdzie $K \neq \{0\}$ i $D \neq \{0\}$. Wówczas Twierdzenia 2.3 i (M. Woronowicz, 2016, Theorem 4.8) wraz (Fuchs, 1973, Proposition 85.3) i (Fuchs, 1973, Theorem 85.1) oraz podstawowymi własnościami produktu tensorowego grup abelowych i grupy homomorfizmów addytywnych implikują, że $\mathrm{Mult}(G) \cong \mathrm{Mult}(K) \oplus \oplus \mathrm{Hom}(K \oplus A, D) \oplus \mathrm{Mult}(A)$ ($\mathrm{Hom}(A,K) = \{0\}$, gdyż $A = pA$ oraz grupa K_p jest p-zredukowana dla każdego $p \in \mathbb{P}(K)$). W szczególności istnieje izomorfizm $f\colon (K \oplus \oplus A) \otimes (K \oplus A) \to K \oplus A$, więc $\mathrm{Hom}(K \oplus A, D) \cong \mathrm{Hom}\big((K \oplus A) \otimes (K \oplus A), D\big)$. Ponadto ze Stwierdzenia 2.1 wynika, że K jest CR-grupą. Stąd oraz na mocy (M. Woronowicz, 2016, Remark 4.2) otrzymujemy, że jeśli $* \in \mathrm{Mult}(G)$, to istnieją łączne i przemienne mnożenie pierścieniowe $\diamond\colon K \times K \to K$, dwuliniowa funkcja $\mu\colon (K \oplus A) \times (K \oplus A) \to D$ oraz $c_4 \in A$ takie, że:

$$(k_1, d_1, a_1) * (k_2, d_2, a_2) = \Big(k_1 \diamond k_2, \mu\big((k_1, a_1), (k_2, a_2)\big), a_1 \cdot c_4 \cdot a_2\Big),$$

dla wszystkich $k_1, k_2 \in K$, $d_1, d_2 \in D$ i $a_1, a_2 \in A$ (w celu zachowania przejrzystości zapisu, grupę C traktujemy jak zewnętrzną sumę prostą grup K i D). Ponadto istnieje określone jednoznacznie $\varphi \in \mathrm{Hom}\big((K \oplus A) \otimes (K \oplus A), D\big)$ takie, że $\mu = \varphi \circ e$, gdzie $e\colon (K \oplus A) \times (K \oplus A) \to (K \oplus A) \otimes (K \oplus A)$ jest funkcją tensorową (por. (Fuchs, 1970, Theorem 59.1)). Stąd, dla $F = f \circ e$ i $\vartheta = \varphi \circ f^{-1}$ otrzymujemy, że $\mu = \vartheta \circ F$. Opisaną sytuację ilustruje poniższy diagram:



W szczególności wynika stąd, że $F \in \mathrm{Mult}(K \oplus A)$. Powołując się na Twierdzenie 2.3, Lemat 2.1 oraz (M. Woronowicz, 2016, Remark 4.2) uzyskujemy, iż istnieją przemienne mnożenie pierścieniowe $\star\colon K \times K \to K$ oraz $c_3 \in A$ takie, że:

$$F\big((k_1, a_1), (k_2, a_2)\big) = (k_1 \star k_2, a_1 \cdot c_3 \cdot a_2),$$

dla wszystkich $k_1, k_2 \in K$ oraz $a_1, a_2 \in A$. Stąd, dla dowolnych $k_1, k_2 \in K$, $d_1, d_2 \in D$ i $a_1, a_2 \in A$ otrzymujemy:

$$(k_1, d_1, a_1) * (k_2, d_2, a_2) = \big(k_1 \diamond k_2, \vartheta(k_1 \star k_2, a_1 \cdot c_3 \cdot a_2), a_1 \cdot c_4 \cdot a_2\big).$$

Przemienność mnożenia $*$ wynika więc z przemienności mnożeń $\diamond$, $\star$ oraz $\cdot$. Zatem każdy pierścień $(G, *)$ jest przemienny, skąd wynika, że G jest CR-grupą.

(iii). $C = D$. Wtedy dowód przebiega analogicznie jak rozumowanie przedstawione w punkcie (ii).

Uwaga 2.6. Z Przykładu 2.1 i Stwierdzenia 2.5 wynika, że każdy spośród przypadków (i) – (iii) analizowanych w dowodzie Twierdzenia 2.9 jest realizowany przez pewną mieszaną *ACR*-grupę.

Uwaga 2.7. Jeżeli A jest mieszaną *ACR*-grupą taką, że $\mathbb{P}(A) = \{p\}$ i grupa A_p nie jest cykliczna, to z Twierdzeń 2.9 i 2.3 wynika, że $A = Z(p^n) \oplus D \oplus H$ albo $A = D \oplus H$, gdzie $n \in \mathbb{N}$, D jest nietrywialną podzielną p-grupą, zaś H jest beztorsyjną grupą abelową rangi jeden. Ponadto, jeżeli zachodzi pierwsza ewentualność, to $H = pH$ na mocy Twierdzenia 2.9. Zatem wszystkie mieszane *ACR*-grupy A takie, że $\mathbb{P}(A) = \{p\}$ i grupa A_p nie jest ani podzielna, ani zredukowana są opisane w Stwierdzeniu 2.5. W szczególności są one *CR*-grupami.

2.7 *E*-grupy i *CRM*-grupy jako szczególne przypadki *CR*-grup

Definicja 2.2. Grupę abelową A nazywamy *CRM*-grupą, jeśli istnieje przemienny i łączny pierścień $R = (A, \circ)$ taki, że każde mnożenie pierścieniowe $*$ na A, różne od $\circ$, jest stowarzyszone z pewnym elementem c grupy A w taki sposób, że dla wszystkich $a, b \in A$ zachodzi $a * b = a \circ c \circ b$.

Uwaga 2.8. Z dowodu (Schultz, 1973, Lemma 8) wynika, że każda grupa abelowa będąca grupą addytywną przemiennego unitarnego pierścienia R spełniającego warunek $R \cong \mathrm{E}(R^+)$ jest *CRM*-grupą. Pierścienie R o takich własnościach określa się mianem E-pierścieni, zaś ich grupy addytywne nazywa się E-grupami (zob. (Schultz, 1973, p. 65, Definition)). Pojęcie E-pierścienia zostało wprowadzone w związku z Problemem 45 postawionym przez L. Fuchsa w Fuchs (1958). Badania takich pierścieni były kontynuowane m. in. w pracach Dugas, Mader i Vinsonhaler (1987); Göbel, Herden i Shelah (2011). E-pierścienie mają zastosowanie, między innymi w topologii algebraicznej (zob. (Göbel i in., 2011, Introduction)).

Ponieważ dla każdej nietrywialnej nil-grupy A zachodzi $A^0 \ncong \mathrm{E}(A)$, to istnieją *CRM*-grupy niebędące E-grupami.

Bezpośrednią konsekwencją obserwacji poczynionych w Uwadze 2.8 jest następujący

Wniosek 2.7. Klasa E-grup jest właściwą podklasą klasy *CRM*-grup.

Dwa następne lematy będą pomocne w klasyfikacji torsyjnych *CRM*-grup.

Lemat 2.10. Niech A i B będą grupami abelowymi takimi, że $A = T(A)$, $\exp(A_p) < \infty$, $B = pB$ oraz $B_p = \{0\}$ dla każdego $p \in \mathbb{P}(A)$. Jeżeli $\left|\mathbb{P}(A)\right| = \infty$, to $G = A \oplus B$ nie jest *CRM*-grupą.

Dowód. Wystarczy wykazać, że nie istnieje łączny pierścień $P = (G, \circ)$ taki, że dla każdego $* \in \mathrm{Mult}(G) \setminus \{\circ\}$ istnieje takie $c \in G$, że dla wszystkich $a, b \in G$ zachodzi $a * b = a \circ c \circ b$. Załóżmy nie wprost, że taki pierścień istnieje. Z Lematu 2.1 wynika, że $P = R \times H$ dla pewnych pierścieni R i H takich, że $R^+ = A$ oraz $H^+ = B$. Dla każdego pierścienia U o grupie addytywnej A definiujemy $\mathbb{P}^0_U = \big\{p \in \mathbb{P}(A) \colon U^2_p = \{0\}\big\}$ i $\mathbb{P}^1_U = \mathbb{P}(A) \setminus \mathbb{P}^0_U$.

Przypuśćmy najpierw, że $\big|\mathbb{P}^1_R\big| = \infty$. Niech $*$ oznacza mnożenie pierścienia $S \times H$, gdzie S jest pierścieniem takim, że $S^+ = A$, $\mathbb{P}^1_S \subsetneq \mathbb{P}^1_R$, $\big|\mathbb{P}^1_S\big| = \infty$ oraz $*_{|A_p \times A_p} = \circ_{|A_p \times A_p}$ dla każdego $p \in \mathbb{P}^1_S$. Niech ponadto $c_1 = \pi(c)$, gdzie π jest naturalną projekcją grupy G na grupę A. Wtedy $* \neq \circ$ oraz warunek $a * b = a \circ c \circ b$ implikuje, że $\big|\operatorname{supp}(c_1)\big| = \infty$, sprzeczność.

Załóżmy teraz, że $\big|\mathbb{P}^1_R\big| < \infty$. Wtedy $\mathbb{P}^0_R \neq \emptyset$, bo $\big|\mathbb{P}(A)\big| = \infty$. Weźmy dowolne $p \in \mathbb{P}^0_R$. Ponieważ grupa A_p jest zredukowana, to z (Feigelstock, 1983, Theorem 2.1.1) wynika istnienie takiego pierścienia N, że $N^+ = A$ i $p \in \mathbb{P}^1_N$. Niech teraz $*$ oznacza mnożenie pierścienia $N \times H$. Istnieją wówczas $x, y \in G$ takie, że p-ta współrzędna elementu $x * y$ jest niezerowa. Ale $x * y = x \circ c \circ y$ oraz $p \in \mathbb{P}^0_R$, więc p-ta współrzędna elementu $x * y$ jest zerowa, sprzeczność.

Lemat 2.11. Niech p będzie liczbą pierwszą, niech n będzie liczbą naturalną i niech D będzie nietrywialną podzielną p-grupą. Wtedy $A = \mathbb{Z}^+_{p^n} \oplus D$ nie jest *CRM*-grupą.

Dowód. Ponieważ $\{0\} \oplus D$ anihiluje dowolny pierścień o grupie addytywnej A, to każde mnożenie pierścieniowe $*$ określone na grupie A jest całkowicie zdeterminowane przez wartość $(1,0) * (1,0)$. Ponadto z (Andruszkiewicz i Woronowicz, 2016a, Lemma 2.1) wynika, że $\Box A \cong \bigoplus_{i \in I} \mathbb{Z}^+_{p^n}$, przy czym $|I| = 1 + \dim_{\mathbb{Z}_p} D[p]$. Jeśli więc A jest *CRM*-grupą, to istnieje łączny pierścień $R = (A, \circ)$ taki, że $(1,0) \circ (1,0) = (k,x)$ dla pewnych $k \in \mathbb{Z}^+_{p^n}$ i $x \in \bigoplus_{i \in J} Z(p^n) \subseteq D$, przy czym $|J| = |I| - 1$, oraz dla każdego $* \in \mathrm{Mult}(A) \setminus \{\circ\}$ istnieje $c \in A$ takie, że dla wszystkich $a, b \in A$ zachodzi $a * b = a \circ c \circ b$. Oczywiście każde takie c jest postaci $c = (c_1, c_2)$, gdzie $c_1 \in \mathbb{Z}_{p^n}$ i $c_2 \in D$, oraz $(0, c_2)$ i $(0, x)$ należą do anihilatora dowolnego pierścienia o grupie addytywnej A.

Symbolem $*$ oznaczmy najpierw mnożenie pierścienia $\mathbb{Z}_{p^n} \times D^0$. Ponieważ $|I| \geq 2$, to $R \neq \mathbb{Z}_{p^n} \times D^0$. Zatem $(1,0) = (1,0) * (1,0) = (1,0) \circ (c_1, c_2) \circ (1,0) = (1,0) \circ (c_1, 0) \circ (1,0) = c_1\big((1,0) \circ (1,0) \circ (1,0)\big) = c_1\big((k,x) \circ (1,0)\big) = c_1\big((k,0) \circ (1,0)\big) = c_1 k\big((1,0) \circ (1,0)\big) = c_1 k(k,x)$, skąd $c_1 k^2 \equiv 1 \pmod{p^n}$ oraz $(c_1 k)x = 0$. Wobec tego $c_1, k \in \mathbb{Z}^*_{p^n}$ i $o(x) \mid c_1 k$. Stąd $p \nmid o(x)$. Ale x jest elementem p-grupy D, więc $o(x) = 1$ i w konsekwencji $x = 0$.

Niech $\iota \colon \mathbb{Z}^+_{p^n} \to D$ będzie dowolnym monomorfizmem i niech $* \colon A \times A \to A$ oznacza teraz funkcję daną wzorem:

$$(k_1, d_1) * (k_2, d_2) = \big(0, \iota(k_1 \odot_{p^n} k_2)\big)$$

dla wszystkich $k_1, k_2 \in \mathbb{Z}^+_{p^n}$ i $d_1, d_2 \in D$. Wtedy $* \in \mathrm{Mult}(A)$ oraz $(A*A)*A = A*$ $*(A*A) = \{0\}$. Ponadto $\mathbb{Z}_{p^n} \times D^0$ jest pierścieniem o grupie addytywnej A, więc $R \neq (A,*)$. Stąd oraz na mocy uzasadnionej wcześniej równości $x = 0$ i rachunków analogicznych jak w poprzednim akapicie otrzymujemy, że dla $d = \iota(1)$ zachodzi i $(0,d) = (1,0)*(1,0) = (1,0) \circ (c_1,c_2) \circ (1,0) = c_1 k^2 (1,0)$. Ale $d \neq 0$, sprzeczność. Ostatecznie uzyskujemy więc, że A nie jest *CRM*-grupą.

Możemy teraz udowodnić twierdzenie klasyfikacyjne dla torsyjnych *CRM*-grup.

Twierdzenie 2.13. Torsyjna grupa abelowa A jest *CRM*-grupą wtedy i tylko wtedy, gdy $A = Z(m) \oplus D$, gdzie D jest torsyjną grupą podzielną taką, że $D_p = \{0\}$ dla każdego dzielnika pierwszego p liczby naturalnej m.

Dowód. Załóżmy, że A jest *CRM*-grupą. Jeżeli $A = \{0\}$, to wystarczy przyjąć $m = 1$ i $D = \{0\}$. Niech dalej $A \neq \{0\}$. Weźmy dowolne $p \in \mathbb{P}(A)$. Niech $D_{(p)}$ będzie największą podzielną podgrupą w A_p. Wtedy $A_p = D_{(p)} \oplus B$ dla pewnej zredukowanej podgrupy B grupy A_p. Jeżeli grupa B nie jest cykliczna, to z (Fuchs, 1970, Corollary 27.3) wynika, że $Z(p^n) \oplus Z(p^r)$ jest składnikiem prostym w A_p dla pewnych $n, r \in \mathbb{N}$. Stąd oraz na mocy Wniosku 2.2 i Twierdzenia 2.3 otrzymujemy, że A_p nie jest *AR*-grupą. Powołując się teraz na Stwierdzenie 2.1 uzyskujemy więc, że A nie jest *AR*-grupą. Zatem A nie jest *CRM*-grupą, sprzeczność. Wobec tego $B = Z(p^s)$ dla pewnego $s \in \mathbb{N}_0$. Z Lematu 2.11 wynika więc, że $D_{(p)} = \{0\}$ albo $s = 0$. Dalej, niech $P_1 = \{p \in \mathbb{P}(A) \colon A_p = Z(p^{n_p}) \text{ dla pewnego } n_p \in \mathbb{N}\}$ i niech $P_2 = \mathbb{P}(A) \setminus P_1$. Wtedy $A = \left(\bigoplus_{p \in P_1} Z(p^{n_p})\right) \oplus D$, gdzie $D = \bigoplus_{p \in P_2} A_p$ jest grupą podzielną. Stąd oraz na mocy Lematu 2.10 uzyskujemy, że $|P_1| < \infty$. Zatem $A = Z(m) \oplus D$, przy czym $m = \prod_{p \in P_1} p^{n_p}$ oraz $D_p = \{0\}$ dla każdej liczby pierwszej p dzielącej m.

Na odwrót. Jeżeli $m = 1$, to grupa A jest podzielna. Wówczas A jest nil-grupą na mocy (Feigelstock, 1983, Theorem 2.1.1), skąd wynika, że A jest *CRM*-grupą. Załóżmy teraz, że $m > 1$. Rozważmy dowolny pierścień R o grupie addytywnej A. Z Uwagi 2.1 i (Feigelstock, 1983, Theorem 2.1.1) wynika wtedy, że $R \cong S \times D^0$, gdzie S jest pewnym pierścieniem o grupie addytywnej $\mathbb{Z}^+_m$. Niech $*$ oznacza mnożenie pierścienia S i niech $c = 1*1$. Wtedy $c \in \mathbb{Z}^+_m$ oraz dla dowolnych $k, l \in \mathbb{Z}^+_m$ otrzymujemy, że $k*l = (kl)(1*1) = (kl)c = (k \odot_m l) \odot_m c = k \odot_m c \odot_m l$. Zatem $S^+ \oplus D$ jest *CRM*-grupą, przy czym rolę mnożenia $\circ$ z Definicji 2.2 odgrywa mnożenie pierścienia $\mathbb{Z}_m \times D^0$. Ponadto $A \cong S^+ \oplus D$, więc A jest *CRM*-grupą.

Bezpośrednią konsekwencją Twierdzeń 2.3 i 2.13 jest następujący

Wniosek 2.8. Torsyjne *CRM*-grupy tworzą właściwą podklasę w klasie torsyjnych *CR*-grup.

Uwaga 2.9. Z (Fuchs, 1973, p. 216, Example 4), (M. Woronowicz, 2016, Theorem 4.8), Wniosku 2.7 i faktu, że każda nil-grupa jest *CRM*-grupą wynika, że każda beztorsyjna grupa abelowa rangi jeden jest *CRM*-grupą. Ponieważ każda beztorsyjna

grupa abelowa rangi jeden zanurza się w $\mathbb{Q}^+$, to opis podgrup grupy $\mathbb{Q}^+$, które nie są nil-grupami przeprowadzony w (M. Woronowicz (2016)) pozwala uzyskać ten rezultat w przejrzysty i bardzo elementarny sposób. Istotnie, z (M. Woronowicz, 2016, Remark 4.2) wynika, że wystarczy rozważyć sytuację, w której A jest podgrupą grupy $\mathbb{Q}^+$ zawierającą liczbę 1. Jeżeli A nie jest nil-grupą, to z (M. Woronowicz, 2016, Theorem 4.8) wynika, że bez utraty ogólności możemy przyjąć, że $A = \left\langle \frac{1}{n} \right\rangle + S^+$ dla pewnego $n \in \mathbb{N}$ i pewnego unitarnego podpierścienia S ciała $\mathbb{Q}$. Wtedy $(A, *)$, gdzie $x * y = x \cdot n \cdot y$ dla wszystkich $x, y \in A$, jest łącznym pierścieniem przemiennym. Rozważmy dowolne $\circledast \in \mathrm{Mult}(A)$ takie, że $\circledast \neq *$. Z (M. Woronowicz, 2016, Remark 4.2) wynika wówczas istnienie takiego $a \in A$, że $x \circledast y = x \cdot a \cdot y$ dla wszystkich $x, y \in A$. Bezpośrednie sprawdzenie pokazuje, że dla $c = \frac{1}{n} \circledast \frac{1}{n}$ oraz wszystkich $x, y \in A$ zachodzi $x \circledast y = x * c * y$. Ponadto $c \in A$, więc rolę mnożenia $\circ$ opisanego w Definicji 2.2 spełnia $*$. Ostatecznie otrzymujemy więc, że A jest *CRM*-grupą.

Przykład 2.3. Oznaczmy $A_1 = \left[\frac{1}{2}\right]^+$, $A_2 = \left[\frac{1}{3}\right]^+$ oraz $A = A_1 \oplus A_2$. Niech $\circ$ oznacza mnożenie pierścienia $\left[\frac{1}{2}\right] \times \left[\frac{1}{3}\right]$, niech $* \in \mathrm{Mult}(A)$ i niech $R = (A, *)$. Niech ponadto $x = (1,0)$, $y = (0,1)$ oraz $z = x + y$. Wtedy $\mathfrak{t}(x) = \mathfrak{t}(A_1)$, $\mathfrak{t}(y) = \mathfrak{t}(A_2)$ i $\mathfrak{t}(z) = \mathfrak{t}(\mathbb{Z}^+)$, skąd $\mathfrak{t}(z) < \mathfrak{t}(x)$, $\mathfrak{t}(z) < \mathfrak{t}(y)$ i $\mathfrak{t}(x) \neq \mathfrak{t}(y)$. Zatem $\left|\mathscr{T}[A]\right| \geq 3$. Ponadto $\square A \neq \{0\}$, więc z (Feigelstock, 1983, Theorem 2.1.7) wynika, że $\left|\mathscr{T}[A]\right| = 3$. Stąd oraz na mocy (Aghdam, 2006, Theorem 2) istnieją $a, b \in \mathbb{Q}$ takie, że $x * x = ax$, $x * y = y * x = 0$ i $y * y = by$. Zatem istnieją takie pierścienie R_1 i R_2, że $R_1^+ = A_1$, $R_2^+ = A_2$ oraz $R = R_1 \times R_2$. Ponadto A_1 i A_2 są *CRM*-grupami na mocy Uwagi 2.9. Istnieją więc $c_1 \in A_1$ oraz $c_2 \in A_2$ takie, że dla wszystkich $a_1, b_1 \in A_1$ oraz $a_2, b_2 \in A_2$ zachodzi $(a_1, a_2) * (b_1, b_2) = (a_1 \cdot c_1 \cdot b_1, a_2 \cdot c_2 \cdot b_2) = (a_1, a_2) \circ (c_1, c_2) \circ (b_1, b_2)$. Zatem A jest *CRM*-grupą.

Następne rezultaty wiążą się z własnościami pierścieni filialnych i ich grup addytywnych badanych od lat 80-tych XX wieku, między innymi przez G. Ehrlich, E. R. Puczyłowskiego, R. R. Andruszkiewicza, K. Pryszczepko i M. Woronowicza (zob. np. Andruszkiewicz (2003); Andruszkiewicz, Mączyński i Pryszczepko (2016); Andruszkiewicz i Puczyłowski (1988); Andruszkiewicz i Woronowicz (2014); Ehrlich (1983/1984); M. Woronowicz (2019)). Przypomnijmy więc, że łączny pierścień R nazywamy filialnym, gdy każdy ideał dowolnego ideału pierścienia R jest ideałem w R.

Twierdzenie 2.14. Każda filialna dziedzina całkowitości R charakterystyki zero taka, że $\Pi(R) \neq \emptyset$ jest E-pierścieniem. W szczególności, R^+ jest *CRM*-grupą.

Dowód. Rozważmy dowolne $f \in \mathrm{E}(R^+)$, $p \in \Pi(R)$, $x \in R$ i $n \in \mathbb{N}$. Z (Andruszkiewicz, 2003, Theorem 3.1) wynika wówczas, że $x = k_n 1 + p^n x_n$ dla pewnych $k_n \in \mathbb{Z}$ oraz $x_n \in R$. Niech $a = f(1)$. Wtedy $f(x) = k_n a + p^n f(x_n)$ oraz $ax = k_n a + p^n a x_n$, skąd $f(x) - ax \in p^n R$. Ponadto n było wybrane dowolnie, więc $f(x) - ax \in p^\infty R$. Ale $p^\infty R = \{0\}$ na mocy (Andruszkiewicz, 2003, Propositions 3.4 & 3.6), skąd $f(x) = ax$.

Wobec tego funkcja φ przyporządkowująca dowolnemu elementowi $y \in R$ endomorfizm l_y grupy R^+ dany wzorem $l_y(r) = yr$ dla każdego $r \in R^+$, jest surjektywna. Standardowe sprawdzenie pokazuje, że jest ona również zanurzeniem pierścieni. Zatem $R \cong \mathrm{E}(R^+)$. Wobec tego R jest E-pierścieniem, skąd R^+ jest E-grupą. Na mocy Wniosku 2.7 otrzymujemy więc, że R^+ jest CRM-grupą.

Uwaga 2.10. Zauważmy, że fakt, iż grupa addytywna filialnej dziedziny całkowitości R charakterystyki zero takiej, że $\Pi(R) \neq \emptyset$ jest CRM-grupą można uzasadnić odwołując się również do (Andruszkiewicz, 2003, Theorem 3.1, Propositions 3.4 & 3.6). Istotnie, niech $A = R^+$ i niech standardowa kropka oznacza mnożenie pierścienia R. Weźmy dowolne $p \in \Pi(R)$, $n \in \mathbb{N}$ oraz $a, b \in A$. Z (Andruszkiewicz, 2003, Theorem 3.1) przez prostą indukcję wynika, że $A = \langle 1 \rangle + p^s A$ dla każdego $s \in \mathbb{N}$. Stąd $a = k_n 1 + p^n a_n$ oraz $b = l_n 1 + p^n b_n$ dla pewnych $k_n, l_n \in \mathbb{Z}$ i $a_n, b_n \in A$. Zatem $a \cdot b = (k_n l_n)1 + p^n\big(k_n b_n + l_n a_n + p^n(a_n \cdot b_n)\big)$. Rozważmy dowolne $* \in \mathrm{Mult}(A)$. Wtedy $a * b = (k_n l_n)(1 * 1) + p^n\big(k_n(1 * b_n) + l_n(a_n * 1) + p^n(a_n * b_n)\big)$. Niech $c = 1 * 1$ i niech $c_n = k_n(1 * b_n) + l_n(a_n * 1) + p^n(a_n * b_n)$. Wówczas $a * b = (k_n l_n)c + p^n c_n$ oraz $a \cdot c \cdot b = (a \cdot b) \cdot c = (k_n l_n)c + p^n\big(k_n(b_n \cdot c) + l_n(a_n \cdot c) + p^n(a_n \cdot b_n \cdot c)\big)$. Zatem $a * b - a \cdot c \cdot b \in p^n A$. Stąd oraz na mocy dowolności wyboru liczby naturalnej n, otrzymujemy, że $a * b - a \cdot c \cdot b \in p^\infty A$. Wobec tego $a * b = a \cdot c \cdot b$ na mocy (Andruszkiewicz, 2003, Propositions 3.4 & 3.6). Ponadto $c \in A$, więc A jest CRM-grupą.

Wniosek 2.9. Niech $A = \bigoplus_{p \in P} Z(p^{n_p})$, gdzie P jest niepustym podzbiorem w $\mathbb{P}$ oraz $n_p \in \mathbb{N}$ dla każdego $p \in P$, i niech R będzie filialną dziedziną całkowitości charakterystyki zero taką, że $\Pi(R) \neq \emptyset$ i $\Pi(R) \cap P = \emptyset$. Niech ponadto $B = R^+$ albo $B = \mathbb{Q}^+$. Wówczas $G = A \oplus B$ jest CR-grupą. Ponadto G jest CRM-grupą wtedy i tylko wtedy, gdy $|P| < \infty$.

Dowód. Rozważmy dowolny pierścień $S = (G, *)$. Z Lematu 2.1 wynika wówczas istnienie pierścieni S_1 oraz S_2 takich, że $S_1^+ = A$, $S_2^+ = B$ oraz $S = S_1 \times S_2$. Pierścień S_1 jest przemienny na mocy Twierdzenia 2.3. Przemienność pierścienia S_2 jest natomiast konsekwencją Twierdzenia 2.14, gdy $B = R^+$, albo (M. Woronowicz, 2016, Remark 4.2), gdy $B = \mathbb{Q}^+$. Zatem pierścień S jest przemienny, skąd wynika, że G jest CR-grupą. Jeżeli $|P| = \infty$, to A nie jest CRM-grupą na mocy Lematu 2.10. Jeśli natomiast $|P| < \infty$, to istnieje $m \in \mathbb{N}$ takie, że $A = Z(m)$. Zatem A jest CRM-grupą i bez utraty ogólności możemy przyjąć, że $A = \mathbb{Z}_m^+$. Ponadto B jest CRM-grupą – dla $B = R^+$ fakt ten wynika z Twierdzenia 2.14, zaś dla $B = \mathbb{Q}^+$ jest on konsekwencją Uwagi 2.9. Jeżeli $B = R^+$, to definiujemy $U = R$. Jeśli natomiast $B = \mathbb{Q}^+$, to określamy $U = \mathbb{Q}$. Niech $\circ$ oznacza mnożenie pierścienia $\mathbb{Z}_m \times U$, zaś standardowa kropka – mnożenie pierścienia U. Z Uwagi 2.10 i (M. Woronowicz, 2016, Remark 4.2) wynika wówczas istnienie takich $c_1 \in A$ i $c_2 \in B$, że dla wszystkich $a_1, a_2 \in A$ oraz $b_1, b_2 \in B$ zachodzi $(a_1, b_1) * (a_2, b_2) = (a_1 \odot_m c_1 \odot_m a_2, b_1 \cdot c_2 \cdot b_2) =$ $= (a_1, b_1) \circ (c_1, c_2) \circ (a_2, b_2)$. Zatem G jest CRM-grupą.

Podsumowanie

Kończąc rozważania na temat struktury $(A)CR$-grup podsumujemy krótko stan obecnej wiedzy na ich temat. Znana jest pełna klasyfikacja torsyjnych *CR*-grup, będąca jednocześnie klasyfikacją torsyjnych *ACR*-grup i *AR*-grup (zob. Twierdzenie 2.3). W świetle Twierdzenia (Fuchs, 1973, Theorem 85.1), sklasyfikowane z dokładnością do izomorfizmu są także beztorsyjne całkowicie rozkładalne *CR*-grupy (zob. Twierdzenie 2.4). Istnieją również dosyć szczegółowe opisy beztorsyjnych *CR*- i *ACR*--grup rangi dwa pozwalające sklasyfikować z dokładnością do izomorfizmu wszystkie beztorsyjne grupy abelowe rangi dwa, które nie są *CR*-grupami oraz wszystkie beztorsyjne grupy abelowe rangi dwa, które nie są *ACR*-grupami (zob. Twierdzenia 2.6 oraz 2.7 i por. (Fuchs, 1973, Theorem 85.1)). Dwa ostatnie wyniki bezpośrednio przyczyniły się do podania pełnej klasyfikacji beztorsyjnych *ACR*-grup rangi dwa niebędących *CR*-grupami (zob. Twierdzenie 2.8 i por. (Fuchs, 1973, Theorem 85.1)). Ważnymi przykładami beztorsyjnych *CR*-grup są grupy addytywne filialnych dziedzin całkowitości charakterystyki zero (zob. Twierdzenie 2.14 i por. Andruszkiewicz (2003) oraz M. Woronowicz (2019)). Wyniki dotyczące mieszanych $(A)CR$-grup mają charakter cząstkowy. Niemniej, Twierdzenia 2.9 i 2.10 opisujące ich strukturę są na tyle precyzyjne, że wraz z dodatkowymi, często bardzo technicznymi rezultatami zamieszczonymi w tym rozdziale, pozwalają konstruować mieszane $(A)CR$-grupy (zob. Uwaga 2.6 i Wniosek 2.9). Znane są także niemal wszystkie zależności między warunkami *CR*, *ACR* oraz *AR* rozważanymi w klasach torsyjnych, beztorsyjnych i mieszanych grup abelowych (zob. Uwaga 2.2, Twierdzenie 2.12 oraz Wnioski 2.3, 2.5 i 2.6).

Bibliografia

Aghdam, A. M. (1987). Square subgroup of an abelian group. Acta. Sci. Math., 51, 343–348.

Aghdam, A. M. (2006). Rings on indecomposable torsion free groups of rank two. Int. Math. Forum, 1, 141–146.

Aghdam, A. M., i Najafizadeh, A. (2008). On torsion free rings with indecomposable additive group of rank two. SEA Bull. Math., 32, 199–208.

Andruszkiewicz, R. R. (2003). The classification of integral domains in which the relation of being an ideal is transitive. Comm. Algebra., 31, 2067–2093.

Andruszkiewicz, R. R., Mączyński, M. i Pryszczepko, K. (2016). Imbedding a filial ring with identity. Comm. Algebra, 44, 2067–2074.

Andruszkiewicz, R. R., i Puczyłowski, E. R. (1988). On filial rings. Portugal. Math., 45, 139–149.

Andruszkiewicz, R. R., i Woronowicz, M. (2014). On ti-groups. W: A. Gomolińska

i inni. (red.), Recent results in pure and applied mathematics, podlasie 2014 Bialystok University of Technology Publishing Office, 33–41.
Andruszkiewicz, R. R., i Woronowicz, M. (2016a). Some new results for the square subgroup of an abelian group. Comm. Algebra, 44, 2351–2361.
Andruszkiewicz, R. R., i Woronowicz, M. (2016b). A torsion-free abelian group exists whose the quotient group modulo the square subgroup is not a nil-group. Bull. Aust. Math. Soc., 94, 449–456.
Andruszkiewicz, R. R., i Woronowicz, M. (2017). On additive groups of associative and commutative rings. Quaest. Math., 40, 527–537.
Arnold, D. M. (1982). Finite rank torsion free abelian groups and rings. Berlin, Heidelberg, New York,: Springer-Verlag.
Beaumont, R. A., i Wisner, R. J. (1959). Rings with additive group which is a torsion-free group of rank two. Acta. Sci. Math. Szeged, 20, 105–116.
Cormen, T. H., Leiserson, C. E. i Rivest, R. L. (1990). Introduction to algorithms. Cambridge (Massachusetts), London: MIT Press and McGraw-Hill.
Dugas, M., Mader, A. i Vinsonhaler, C. (1987). Large e-rings exist. J. Algebra, 108, 88–101.
Ehrlich, G. (1983/1984). Filial rings. Portugal. Math., 42, 185–194.
Feigelstock, S. (1974). On the tensor product of exact sequences of modules over a dedekind ring. Archiv der Math., 25, 598–601.
Feigelstock, S. (1983). Additive groups of rings. vol. 1. Boston: Pitman Advanced Publishing Program.
Feigelstock, S. (2000). Additive groups of commutative rings. Quest. Math., 23, 241–245.
Fuchs, L. (1958). Abelian groups. Budapest: Publ. House Hungar. Acad. Sci.
Fuchs, L. (1970). Infinite abelian groups. vol. 1. New York, London: Academic Press.
Fuchs, L. (1973). Infinite abelian groups. vol. 2. New York, London: Academic Press.
Garcés, Y., Torres, E., Pereira, O. i Rodríguez, R. (2014). Application of the ring theory in the segmentation of digital image. IJSCMC, 3.
Gardner, B. J., i Wiegandt, R. (2004). Radical theory of rings. New York, Basel: Marcel Dekker, INC.
Göbel, R., Herden, D. i Shelah, S. (2011). Absolute e-rings. Adv. Math., 226, 235–253.
Jackett, D. R. (1979). The type set of torsion free abelian group of rank two. J. Austral. Math. Soc. (Series A), 27, 507–510.
Karatsuba, A. (1995). The complexity of computations. Proceedings of the Steklov Institute of Mathematics, 211, 169-183.
Knuth, D. E. (1997). The art of computer programming, vol. 2. Reading, Massachusetts: Addison-Wesley.
Lidl, R., i Harald, N. (1994). Introduction to finite fields and their applications. New

York: Cambridge University Press.
Najafizadeh, A. (2015). On the square submodule of a mixed module. Gen. Math. Notes, 27, 1-8.
Najafizadeh, A., i Woronowicz, M. (2017). A note on additive groups of some specific torsion-free rings of rank three and mixed associative rings. Discuss. Math. Gen. Algebra Appl., 37, 223–232.
Schultz, P. (1973). The endomorphism ring of the additive group of a ring. J. Austral. Math. Soc., 15, 60–69.
Stratton, A. E. (n.d.). Type sets of torsion free rings of finite rank. Comment. Math. Univ. St. Pauli.
Woronowicz, K. (2015). Algorithm of adding the m-bite numbers. AiCSR, 12, 95–108.
Woronowicz, M. (2016). A note on additive groups of some specific associative rings. Ann. Math. Sil., 30, 219–229.
Woronowicz, M. (2019). Grupy addytywne pierścieni łącznych. Unpublished doctoral dissertation, Uniwersytet Warszawski, Wydział Matematyki, Informatyki i Mechaniki.
Woronowicz, M. (2020). A note on feigelstock's conjecture on the equivalence of the notions of nil and associative nil groups in the context of additive groups of rings of finite rank. Bull. Belg. Math. Soc. Simon Stevin, 27, 509–519.

Rozdział 3

PROBABILISTYCZNE I ALGEBRAICZNE ASPEKTY ZAOKRĄGLANIA LICZB

Ryszard Mazurek*

Streszczenie Niniejszy rozdział jest poświęcony probabilistycznym i algebraicznym zagadnieniom związanym z zaokrąglaniem liczb rzeczywistych. Dla każdej liczby rzeczywistej a, która może być zapisana w układzie dziesiętnym z dwoma miejscami po przecinku wyznaczono częstość, z jaką dla stu kolejnych liczb naturalnych x zaokrąglenia iloczynów ax do najbliższej liczby całkowitej są zaokrągleniami w dół. Ponadto zbadano dwa grupoidy zdefiniowane z wykorzystaniem, odpowiednio, zaokrągleń liczb naturalnych do setek i zaokrągleń liczb rzeczywistych do części całkowitej. W każdym z tych grupoidów wyznaczono wszystkie podgrupoidy cykliczne będące półgrupami.

Słowa kluczowe: zaokrąglenie liczby rzeczywistej, grupoid, półgrupa

Wprowadzenie

Z zaokrągleniami liczb często mamy do czynienia w życiu codziennym (na przykład gdy wyliczona kwota podatku VAT wynosi 1234,5678 zł i trzeba ją zaokrąglić do pełnych groszy, albo gdy mówimy, że spotkanie trwało około 30 minut, a w rzeczywistości trwało 27 minut i 42 sekundy). Konieczność zaokrąglania liczb często pojawia się również przy pomiarach lub wyliczeniach wielkości fizycznych w nauce i technice.

W niniejszym rozdziale rozważane są trzy rodzaje zaokrągleń liczb rzeczywistych nieujemnych: zaokrąglanie do najbliższej liczby całkowitej (tzn. zaokrąglanie względem cyfry jedności), zaokrąglanie względem cyfry setek i zaokrąglanie do części całkowitej (nazywane także obcinaniem, gdyż polega ono na „obcięciu" cyfr po przecinku w zapisie dziesiętnym liczby). W pierwszej części rozdziału badane są pewne probabilistyczne aspekty zaokrąglania do najbliższej liczby całkowitej. W części tej, dla każdej liczby rzeczywistej nieujemnej a, która może być zapisana w układzie dziesiętnym z dwoma miejscami po przecinku, wyznaczono prawdopodobieństwo

* Wydział Informatyki, Politechnika Białostocka, Wiejska 45A, 15-351 Białystok, r.mazurek@pb.edu.pl

DOI 10.24427/978-83-67185-18-9_3

wylosowania ze zbioru $\{1,2,\ldots,100\}$ takiej liczby x, że zaokrąglenie iloczynu ax do najbliższej liczby całkowitej jest zaokrągleniem w dół. W drugiej części rozdziału zbadano dwa grupoidy zdefiniowane z wykorzystaniem, odpowiednio, zaokrągleń liczb naturalnych względem cyfry setek i zaokrągleń liczb rzeczywistych do części całkowitej. W każdym z tych grupoidów wyznaczono wszystkie podgrupoidy cykliczne, które są półgrupami.

3.1 Probabilistyczne aspekty zaokrąglania liczb

W tej części rozdziału rozważymy prawdopodobieństwa zdarzeń związanych z zaokrąglaniem liczb rzeczywistych do najbliższej liczby całkowitej. Punktem wyjścia jest następujący przykład.

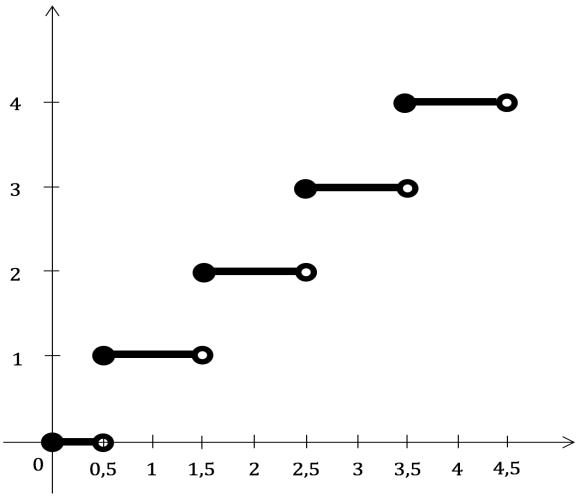
Przykład 3.1.1. Bank oferuje roczną lokatę, na którą klienci banku mogą wpłacać w pełnych złotych dowolną kwotę nieprzekraczającą 1000 zł. Lokata jest oprocentowana roczną stopą procentową 5% z roczną kapitalizacją odsetek. Po roku bank wypłaca klientom należną kwotę zaokrągloną do pełnych złotych. Zakładając, że rozkład wpłacanych kwot jest jednostajny, należy rozstrzygnąć, co jest bardziej prawdopodobne dla losowej wpłaty: to że należna kwota będzie zaokrąglona w dół, czy że będzie zaokrąglona w górę.

Oznaczmy przez x kwotę (w złotych), którą klient lokuje w banku. Dopuszczalne jest lokowanie kwot tylko w pełnych złotych, więc x jest liczbą naturalną nie większą niż 1000. Ponieważ lokata jest oprocentowana roczną stopą procentową 5% z kapitalizacją roczną, więc stan lokaty po roku wynosi $1,05x$ zł i jest to kwota należna klientowi. Jednak zgodnie z przedstawionymi zasadami, bank wypłaca klientowi nie kwotę $1,05x$ zł, lecz jej zaokrąglenie do pełnych złotych.

Zasada zaokrąglania kwot do pełnych złotych jest dobrze znana (stosuje się ją np. w prawie podatkowym): końcówki kwot wynoszące mniej niż 50 groszy pomija się, a końcówki kwot wynoszące 50 i więcej groszy podwyższa się do pełnych złotych, przy czym przez końcówkę kwoty rozumiemy nadwyżkę kwoty ponad liczbę pełnych złotych, które się w tej kwocie mieszczą. Aby rozwiązanie rozważanego problemu przedstawić w sposób zwarty, wprowadzimy funkcję opisującą proces zaokrąglania liczby rzeczywistej nieujemnej r do najbliższej liczby całkowitej, odpowiadający rozważanemu w naszym przykładzie zaokrąglaniu do pełnych złotych. Oznaczmy przez t końcówkę liczby r, tzn. $r = [r] + t$, gdzie $[r]$ jest częścią całkowitą liczby r, a t jest liczbą z przedziału $[0,1)$. Wówczas zaokrągleniem liczby r jest liczba $(r)_0$ zdefiniowana następująco:

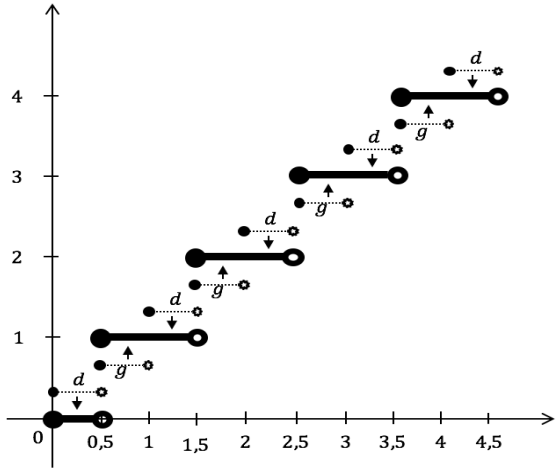
$$(r)_0 = \begin{cases} [r], & \text{jeśli } t < 0,5, \\ [r]+1, & \text{jeśli } t \geq 0,5. \end{cases} \tag{3.1.1}$$

Początkowy fragment wykresu funkcji $(r)_0$ jest przedstawiony na rysunku 3.1.



Rysunek 3.1: Wykres funkcji $(r)_0$

W pierwszym z przypadków wyróżnionych w definicji (3.1.1), tzn. gdy $t < 0,5$, mówimy, że liczba r jest zaokrąglana w dół, a w drugim (gdy $t \geq 0,5$) – że liczba r jest zaokrąglana w górę. Na przykład, zaokrąglenia liczb $2,4$ i $1,9$ są takie same i wynoszą 2, ale dla liczby $2,4$ jest to zaokrąglenie w dół, a dla liczby $1,9$ – w górę. Ponieważ w rozważanym przykładzie interesuje nas nie wartość zaokrąglenia, lecz to, czy ta wartość jest wynikiem zaokrąglenia w dół, czy w górę, więc na wykresie funkcji zaokrąglania $(r)_0$ (przedstawionym na rysunku 3.1) dodatkowo wyodrębniamy przypadki zaokrągleń w dół (oznaczone przez d) i w górę (oznaczone przez g), otrzymując rysunek 3.2.



Rysunek 3.2: Wykres funkcji $(r)_0$ z podziałem na zaokrąglenia w dół (d) i w górę (g)

Rozważmy dla przykładu lokaty w wysokości kolejno od 1 zł do 40 zł (przy efektywnej stopie rocznej 5%). W tabeli 3.1 pokazano, dla których z nich należne kwoty są zaokrąglane w dół, a dla których w górę.

Lokowana kwota x	Należna kwota $1{,}05 \cdot x$	Rodzaj zaokrąglenia
1	1,05	d
2	2,10	d
3	3,15	d
4	4,20	d
5	5,25	d
6	6,30	d
7	7,35	d
8	8,40	d
9	9,45	d
10	10,50	g
11	11,55	g
12	12,60	g
13	13,65	g
14	14,70	g
15	15,75	g
16	16,80	g
17	17,85	g
18	18,90	g
19	19,95	g
20	21,00	d

Lokowana kwota x	Należna kwota $1{,}05 \cdot x$	Rodzaj zaokrąglenia
21	22,05	d
22	33,10	d
23	24,15	d
24	25,20	d
25	26,25	d
26	27,30	d
27	28,35	d
28	29,40	d
29	30,45	d
30	31,50	g
31	32,55	g
32	33,60	g
33	34,65	g
34	35,70	g
35	36,75	g
36	37,80	g
37	38,85	g
38	39,90	g
39	40,95	g
40	42,00	d

Tabela 3.1: Rodzaje zaokrągleń dla lokat w wysokości od 1 zł do 40 zł przy rocznej stopie procentowej 5%

Jak pokazuje tabela 3.1, dla lokowanych kwot w wysokości (w złotych) od 1 do 20 otrzymujemy taki sam ciąg rodzajów zaokrągleń

$$d,d,d,d,d,d,d,d,d,g,g,g,g,g,g,g,g,g,g,d, \tag{3.1.2}$$

jak dla lokowanych kwot w wysokości od 21 do 40. Sugeruje to, że ciąg rodzajów zaokrągleń (w dół lub w górę) jest okresowy, o okresie długości 20. I rzeczywiście tak jest, gdyż dla dowolnej lokowanej kwoty x zł otrzymujemy równość

$$1{,}05(x+20) = 1{,}05x+21,$$

a więc rodzaj zaokrąglenia dla lokowanych kwot $x+20$ zł i x zł jest taki sam.

Jesteśmy już gotowi, aby udzielić odpowiedzi na pytanie z przykładu 3.1.1. Kwoty możliwych wpłat (w złotych), czyli zbiór liczb $\{1,2,\ldots,1000\}$ dzielimy na 50 rozłącznych podzbiorów 20-elementowych w ten sposób, że pierwszy podzbiór zawiera

wpłaty w wysokości od 1 do 20, drugi - od 21 do 40, trzeci - od 41 do 60, itd. Ponieważ ciąg rodzajów zaokrągleń dla kolejnych kwot z danego podzbioru jest taki sam jak dla kwot od 1 do 20, czyli jest ciągiem (3.1.2), w którym jest tyle samo zaokrągleń w dół co w górę, więc jeśli wysokości lokowanych kwot (w pełnych złotych) są jednakowo prawdopodobne, to dla losowej lokowanej kwoty jest tak samo prawdopodobne, że kwota należna (po roku trwania lokaty) będzie zaokrąglona w dół, jak i w górę.

Rozważmy lokatę bankową podobną do tej z przykładu 3.1.1, lecz z nieco niższą stopą procentową. Również w tym przypadku będziemy zakładać, że rozkład lokowanych kwot jest jednostajny.

Przykład 3.1.2. Bank oferuje roczną lokatę, na którą klienci banku mogą wpłacać dowolną kwotę w pełnych złotych nieprzekraczającą 1000 zł. Lokata jest oprocentowana roczną stopą procentową 4% z kapitalizacją roczną. Po roku bank wypłaca klientowi należną kwotę zaokrągloną do pełnych złotych. Co jest bardziej prawdopodobne dla losowej wpłaty: zaokrąglenie należnej kwoty w górę, czy w dół?

Poszukując odpowiedzi na powyższe pytanie, tym razem rozpoczniemy od wyznaczenia liczby naturalnej n takiej, że dla każdej liczby naturalnej x zaokrąglenie kwoty $x+n$ zł jest tego samego rodzaju jak kwoty x zł. Ponieważ

$$1,04(x+n) = 1,04x+1,04n,$$

więc aby zaokrąglenia kwot $x+n$ zł i x zł były tego samego rodzaju, wystarczy aby liczba $1,04n$ była naturalna. Zatem szukamy liczby naturalnej n takiej, że

$$1,04n = m \text{ dla pewnej liczby naturalnej } m. \tag{3.1.3}$$

Równanie (3.1.3) jest równoważne równaniu

$$104n - 100m = 0,$$

które chcemy rozwiązać w liczbach naturalnych. W tym celu skorzystamy z przytoczonego niżej znanego twierdzenia o rozwiązaniach równania diofantycznego pierwszego stopnia z dwiema niewiadomymi.

Twierdzenie 3.1.3. (Sierpiński, 1987, Twierdzenie 12) Jeżeli para liczb całkowitych (x_0, y_0) jest rozwiązaniem równania $ax+by=c$, gdzie a,b,c są danymi liczbami całkowitymi, to wszystkie rozwiązania tego równania w liczbach całkowitych x,y są zawarte we wzorach:

$$x = x_0 + \frac{b}{NWD(a;b)}t;\ y = y_0 - \frac{a}{NWD(a;b)}t,$$

gdzie t jest dowolną liczbą całkowitą.

Z twierdzenia 3.1.3 wynika, że najmniejszą „dobrą” wartością n jest

$$n = \frac{100}{NWD(104;100)} = \frac{100}{4} = 25.$$

Zatem ciąg rodzajów zaokrągleń kwot rozważanych w przykładzie 3.1.2 jest okresowy, o okresie długości 25. Aby zobaczyć, który z rodzajów zaokrągleń przeważa w pełnych okresach, wystarczy wyznaczyć rodzaje zaokrągleń dla lokat w wysokości (w złotych) od 1 do 25. Rodzaje zaokrągleń dla tych kwot są przedstawione w tabeli 3.2.

Lokowana kwota x	Należna kwota $1{,}04 \cdot x$	Rodzaj zaokrąglenia
1	1,04	d
2	2,08	d
3	3,12	d
4	4,16	d
5	5,20	d
6	6,24	d
7	7,28	d
8	8,32	d
9	9,36	d
10	10,40	d
11	11,44	d
12	12,48	d
13	13,52	g

Lokowana kwota x	Należna kwota $1{,}04 \cdot x$	Rodzaj zaokrąglenia
14	14,56	g
15	15,60	g
16	16,64	g
17	17,68	g
18	18,72	g
19	19,76	g
20	20,80	g
21	21,84	g
22	22,88	g
23	23,92	g
24	24,96	g
25	26,00	d

Tabela 3.2: Rodzaje zaokrągleń dla lokat w wysokości od 1 zł do 25 zł przy rocznej stopie procentowej 4%

Jak widzimy w tabeli 3.2, dla wpłat w wysokości (w złotych) od 1 do 25, należne kwoty są w trzynastu przypadkach zaokrąglane w dół, a w dwunastu - w górę.

Aby odpowiedzieć na pytanie sformułowane w przykładzie 3.1.2, przy założeniu, że każda z możliwych kwot wpłaty jest tak samo prawdopodobna, postąpimy analogicznie jak w przykładzie 3.1.1. Ponieważ możliwych kwot wpłaty jest 1000 i długość okresu rodzajów zaokrągleń jest równa 25, a ponadto 25 dzieli 1000, więc, podobnie jak w przykładzie 3.1.1, możemy zbiór możliwych wartości wpłat rozbić na sumę rozłączną 25-elementowych podzbiorów w taki sposób, że w każdym podzbiorze rodzaje zaokrągleń są takie same jak dla kwot od 1 zł do 25 zł. Zatem dla kwot z każdego z tych podzbiorów mamy 13 zaokrągleń w dół i 12 zaokrągleń w górę. Wynika stąd, że dla losowej lokaty bardziej prawdopodobne jest zaokrąglenie należnej kwoty w dół – wynosi ono $\frac{13}{25} = 0,52$.

Dotychczasowe rozważania skłaniają do sformułowania następującego ogólniejszego problemu:

Problem 3.1.4. Dana jest liczba rzeczywista nieujemna a, która w zapisie dziesiętnym może być przedstawiona z dwoma miejscami po przecinku (np. $a = 3,00$ lub $a = 3,10$, lub $a = 3,12$). Dla liczb całkowitych nieujemnych x rozważamy zaokrąglenia iloczynów ax do najbliższej liczby całkowitej (według zasady przedstawionej w przykładzie 3.1.1). Co jest bardziej prawdopodobne dla losowo wybranej liczby x: zaokrąglenie liczby ax w dół, czy w górę?

Szczególne przypadki tego problemu rozważaliśmy w przykładzie 3.1.1 (dla $a = 1,05$) i w przykładzie 3.1.2 (dla $a = 1,04$) dla liczb naturalnych x nieprzekraczających 1000. Wyjaśnijmy, dlaczego w problemie 3.1.4 dopuszczamy wartość $x = 0$. Otóż, jak się niebawem okaże, w rozwiązaniu tego problemu ważne będą nie wartości x, lecz reszty z dzielenia tych wartości przez 100, a te zaczynają się od 0, a nie od 1.

Aby rozwiązać problem 3.1.4, zauważmy najpierw, że ponieważ x jest liczbą całkowitą nieujemną, więc wystarczy ograniczyć się do liczb a z przedziału $[0,1)$. Rzeczywiście, a można zapisać jako $a = k + r$, gdzie k jest nieujemną liczbą całkowitą i r jest liczbą rzeczywistą z przedziału $[0,1)$, a wtedy $ax = (k+r)x = kx + rx$. Ponieważ kx jest liczbą całkowitą nieujemną, więc rodzaj zaokrąglenia liczb ax i rx jest taki sam. Zatem bez straty ogólności rozważań możemy zakładać, że a należy do przedziału $[0,1)$, a ponieważ w zapisie dziesiętnym liczby a dopuszczamy tylko dwa miejsca po przecinku, więc a jest jedną z liczb ze 100-elementowego zbioru

$$S = \{0,00; 0,01; 0,02; ...; 0,97; 0,98; 0,99\}. \tag{3.1.4}$$

Kolejną upraszczającą obserwacją jest spostrzeżenie, że przy danym czynniku a rodzaj zaokrąglenia (w dół lub w górę) jest dla liczb x i $x + 100$ taki sam, gdyż $a(x + 100) = ax + 100a$ i $100a$ jest liczbą całkowitą nieujemną (ponieważ liczba a może być w zapisie dziesiętnym przedstawiona z dwoma miejscami po przecinku). Zatem aby rozstrzygnąć, który rodzaj zaokrąglenia (w dół, czy w górę) jest dla danej liczby a bardziej prawdopodobny, wystarczy dla tej liczby wyznaczyć ciąg rodzajów zaokrągleń (d lub g) iloczynów ax dla wartości x od 0 do 99 (lub jakichkolwiek stu kolejnych liczb naturalnych x).

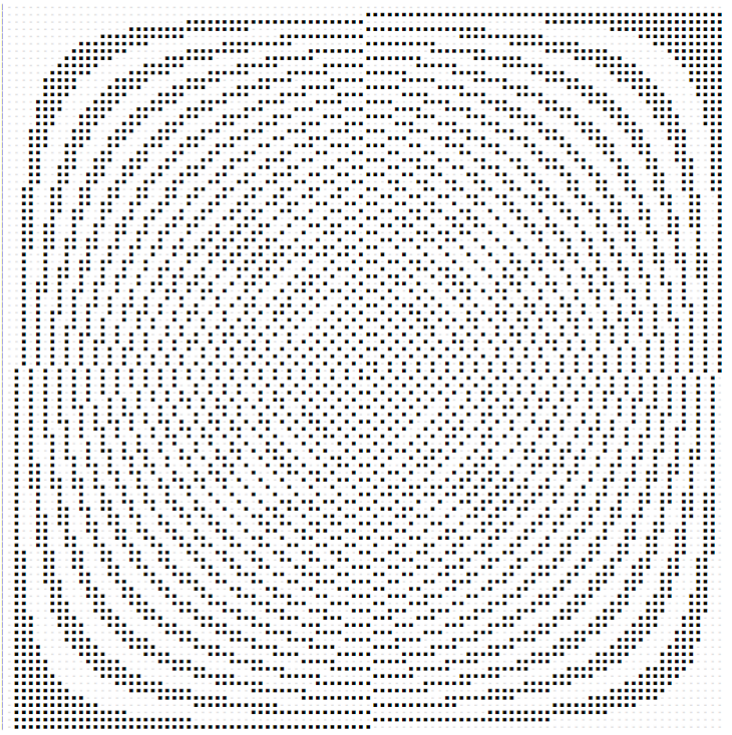
Na rysunku 3.3 przedstawiono w formie graficznej rodzaje zaokrągleń iloczynów ax do najbliższej liczby całkowitej dla wszystkich par (a,x), gdzie

$$a \in \{0,00; 0,01; \ldots; 0,99\} \text{ i } x \in \{0,1,\ldots,99\}.$$

Na rysunku tym widzimy tablicę o wymiarach 100×100, której wiersze (od góry w dół) odpowiadają kolejnym wartościom a, czyli kolejno liczbom

$$0,00; 0,01; 0,02; \ldots; 0,98; 0,99,$$

natomiast kolumny (od lewej strony do prawej) odpowiadają kolejnym wartościom x, czyli kolejno liczbom $0,1,\ldots,99$. Jeżeli liczba ax jest zaokrąglana w górę, to na pozycji (a,x) znajduje się czarny kwadracik, a jeśli w dół, to biały. Rysunek 3.3 jest wynikiem prostego programu komputerowego.



Rysunek 3.3: Graficzne przedstawienie rodzajów zaokrągleń iloczynów ax dla par (a,x), gdzie $0 \leq a \leq 0{,}99$ i $0 \leq x \leq 99$

Rozważmy dowolną liczbę a ze zbioru S opisanego w (3.1.4). Policzymy, ile jest takich liczb $x \in \{0,1,\ldots,99\}$, że iloczyn ax jest zaokrąglany w dół. Oczywiście liczba ax jest zaokrąglana w dół wtedy i tylko wtedy, gdy w zapisie dziesiętnym tej liczby pierwsza cyfra po przecinku jest mniejsza niż 5, czyli gdy przedostatnia cyfra liczby całkowitej nieujemnej $100ax$ jest mniejsza od 5, a więc gdy reszta z dzielenia liczby $100ax$ przez 100 jest mniejsza lub równa 49. Zapisując iloczyn $100ax$ w postaci Ax, gdzie $A = 100a$ jest liczbą całkowitą nieujemną, stwierdzamy zatem, że dla iloczynów ax liczba zaokrągleń w dół jest równa liczbie takich $x \in \{0,1,2,\ldots,99\}$, że reszta z dzielenia liczby Ax przez 100 jest mniejsza niż 50. Aby zbadać, ile jest takich liczb x, skorzystamy z następującego znanego twierdzenia o rozwiązaniach kongruencji pierwszego stopnia.

Twierdzenie 3.1.5. (Narkiewicz, 1997, Twierdzenie 1.22) Niech m będzie liczbą naturalną i niech a,b będą liczbami całkowitymi takimi, że a nie dzieli się przez m. Wówczas kongruencja

$$ax \equiv b \ (mod\ m) \tag{3.1.5}$$

ma rozwiązanie wtedy i tylko wtedy, gdy b dzieli się przez $NWD(a;m)$. Gdy warunek ten jest spełniony, to kongruencja (3.1.5) ma $NWD(a;m)$ różnych rozwiązań w zbiorze $\{0,1,2,\ldots,n-1\}$ i wszystkie one przystają do siebie $(mod\ \frac{m}{NWD(a;m)})$.

Policzymy, ile jest liczb $x \in \{0,1,2,\ldots,99\}$ takich, że $Ax \equiv b \ (mod\ 100)$ i $0 \leq b \leq 49$, gdzie $a \in \{0,00;0,01;\ldots;0,99\}$ i $A = 100a$. Jeżeli $a \neq 0$, to z twierdzenia 3.1.5 wynika, że ta kongruencja ma rozwiązanie wtedy i tylko wtedy, gdy $b = k \cdot NWD(A;100)$ dla pewnej liczby całkowitej k spełniającej warunek $0 \leq k \cdot NWD(A;100) \leq 49$, a więc takich liczb b jest $[\frac{49}{NWD(A;100}\,)] + 1$. Zgodnie z twierdzeniem 3.1.5, dla każdej takiej liczby b kongruencja $Ax \equiv b \ (mod\ 100)$ ma $NWD(A;100)$ rozwiązań w zbiorze $\{0,1,\ldots,99\}$. Wynika stąd, że dla $a \neq 0$ liczba przypadków, gdy iloczyn ax jest zaokrąglany w dół, wynosi

$$\left(\left[\frac{49}{NWD(A;100)}\right]+1\right)\cdot NWD(A;100), \tag{3.1.6}$$

gdzie $A = 100a$. Jeżeli $a = 0$, to liczba zaokrągleń w dół jest równa 100 i taką samą wartość otrzymujemy ze wzoru (3.1.6) zastosowanego do liczby $a = 0$. Udowodniliśmy więc następujące stwierdzenie.

Stwierdzenie 3.1.6. Dla liczby nieujemnej a, która w zapisie dziesiętnym może być przedstawiona z dwoma miejscami po przecinku, dla dowolnego ciągu stu kolejnych liczb całkowitych nieujemnych x, wśród zaokrągleń liczb ax do najbliższej liczby całkowitej jest dokładnie

$$\left(\left[\frac{49}{NWD(100a;100)}\right]+1\right)\cdot NWD(100a;100) \tag{3.1.7}$$

zaokrągleń w dół, a więc prawdopodobieństwo zaokrąglenia liczby ax w dół jest równe

$$\frac{([\frac{49}{NWD(100a;100)}]+1)\cdot NWD(100a;100)}{100}. \tag{3.1.8}$$

Wróćmy do przykładu 3.1.1. Rozważaliśmy w nim lokatę w kwocie (w pełnych złotych) od 1 zł do 1000 zł, oprocentowaną roczną stopą procentową 5%, z której po roku jest wypłacana należna kwota zaokrąglona do pełnych złotych. W przykładzie tym pytaliśmy, co jest bardziej prawdopodobne: zaokrąglenie należnej kwoty w górę, czy w dół? Załóżmy, że kwoty możliwych wpłat są jednakowo prawdopodobne. Kwoty te dzielimy na 10 grup po 100 elementów: wpłaty w kwocie (w złotych) od 1 do 100, od 101 do 200, od 201 do 300, itd. Zgodnie ze stwierdzeniem

3.1.6, w każdej z tych 100-elementowych grup liczba zaokrągleń w dół jest równa

$$\left(\left[\frac{49}{NWD(100\cdot 1,05;100)}\right]+1\right)\cdot NWD(1,05\cdot 100;100)=$$

$$=\left(\left[\frac{49}{NWD(105;100)}\right]+1\right)\cdot NWD(105;100)=$$

$$=\left(\left[\frac{49}{5}\right]+1\right)\cdot 5=(9+1)\cdot 5=50,$$

a więc prawdopodobieństwo, że wypłacana kwota będzie zaokrąglona w dół wynosi

$$\frac{50\cdot 10}{100\cdot 10}=0,5.$$

Zatem w przykładzie 3.1.1, tak jak już wcześniej stwierdziliśmy, zaokrąglenia w dół są tak samo prawdopodobne, jak zaokrąglenia w górę.

Zastosujmy stwierdzenie 3.1.6, aby jeszcze raz (ale inną metodą niż poprzednio) wyliczyć prawdopodobieństwo zaokrąglenia w dół w przykładzie 3.1.2. W tym celu w stwierdzeniu 3.1.6 przyjmujemy $a=1,04$ i otrzymujemy wartość tego prawdopodobieństwa:

$$\frac{([\frac{49}{NWD(104;100)}]+1)\cdot NWD(104;100)}{100}=\frac{([\frac{49}{4}]+1)\cdot 4}{100}=\frac{(12+1)\cdot 4}{100}=\frac{13}{25}=0,52.$$

Zatem w przypadku lokaty rozważanej w przykładzie 3.1.2, bardziej prawdopodobne jest zaokrąglenie wypłaty w dół, niż w górę.

Wracamy do problemu 3.1.4. Z definicji części całkowitej wynika, że

$$\left[\frac{s}{t}\right]+1>\frac{s}{t}\text{ dla dowolnych liczb rzeczywistych } s,t \text{ takich, że } t\neq 0. \qquad (3.1.9)$$

Zakładając, że liczba t jest dodatnia, po pomnożeniu nierówności (3.1.9) obustronnie przez t, otrzymujemy nierówność

$$\left(\left[\frac{s}{t}\right]+1\right)t>s. \qquad (3.1.10)$$

W szczególności, jeśli a jest liczbą nieujemną taką jak w stwierdzeniu 3.1.6, to

$$\left(\left[\frac{49}{NWD(100a;100)}\right]+1\right)\cdot NWD(100a;100)>49,$$

a więc na mocy stwierdzenia 3.1.6, wśród dowolnych stu kolejnych liczb całkowitych nieujemnych x jest co najmniej 50 takich, dla których liczba ax jest zaokrąglana w dół. Zatem nigdy liczba zaokrągleń w górę nie będzie większa niż liczba zaokrągleń w dół.

Zastanówmy się jeszcze, jaka może być liczba zaokrągleń w dół iloczynów ax, gdy rozważamy sto kolejnych liczb całkowitych nieujemnych x? Jak widzieliśmy

w przykładach 3.1.1 i 3.1.2, możliwe są wartości 50 i 52, ale czy oprócz nich możliwe są inne? Aby odpowiedzieć na to pytanie, wystarczy wyznaczyć wartości iloczynu (3.1.7) dla wszystkich możliwych wartości $NWD(100a;100)$. Wyniki rachunków przedstawione są w tabeli 3.3 (w której jest również zawarta odpowiedź na pytanie z problemu 3.1.4). Jak widzimy z tej tabeli, liczba zaokrągleń w dół może przyjąć tylko cztery wartości: 50, 52, 60 i 100, przy czym liczba zaokrągleń w dół jest większa niż 50 wtedy i tylko wtedy, gdy liczba $NWD(100a;100)$ jest podzielna przez 4, czyli gdy liczba $100a$ dzieli się przez 4.

$NWD(100a,100)$	1	2	4	5	10	20	25	50	100
Liczba zaokrągleń w dół	50	50	52	50	50	60	50	50	100
Prawdopodobieństwo zaokrąglenia w dół	0,5	0,5	0,52	0,5	0,5	0,6	0,5	0,5	1

Tabela 3.3: Liczby i prawdopodobieństwa zaokrągleń w dół w zależności od $NWD(100a;100)$

W przykładzie 3.1.2 rozważaliśmy lokatę bankową, na którą klient może wpłacić w pełnych złotych kwotę $x \leq 1000$, a po roku bank wypłaca mu kwotę $1,04x$ zł zaokrągloną do pełnych złotych. Stwierdziliśmy już, że przy wpłatach w wysokości kolejno od 1 zł do 1000 zł, kwota $1,04x$ zł będzie częściej zaokrąglana w dół, niż w górę. Może to sugerować, że fikcyjny bank z przykładu 3.1.2 „zarabia" na takim sposobie zaokrąglania należnych kwot wypłat. Sprawdźmy, czy rzeczywiście tak jest.

Dla konkretnej wpłaty x zł różnica między należną kwotą a jej zaokrągleniem jest równa $1,04x-(1,04x)_0$. Policzymy, jaka jest całkowita różnica między należnymi kwotami a ich zaokrągleniami, przy założeniu, że każda z kwot od 1 zł do 1000 zł pojawia się jednokrotnie jako wpłata, tzn. obliczymy sumę

$$\sum_{x=1}^{1000}(1,04x-(1,04x)_0).$$

W świetle wcześniejszych rozważań jest oczywiste, że

$$\sum_{x=1}^{1000}(1,04x-(1,04x)_0)=10\sum_{x=1}^{100}(1,04x-(1,04x)_0)$$

i dlatego wystarczy obliczyć sumę

$$\sum_{x=1}^{100}(1,04x-(1,04x)_0).$$

Postawimy sobie zadanie ogólniejsze.

Problem 3.1.7. Dana jest liczba rzeczywista nieujemna a, która w zapisie dziesiętnym może być przedstawiona z dwoma miejscami po przecinku. Obliczyć sumę

$$S_{100}(a) = \sum_{x=1}^{100} (ax - (ax)_0).$$

Oczywiście dla dowolnej liczby naturalnej m mamy równość

$$S_{100}(a+m) = S_{100}(a).$$

Zatem, aby wyznaczyć wszystkie możliwe wartości sumy $S_{100}(a)$, wystarczy je wyznaczyć dla $a < 1$. W tabeli 3.4 podane są te wartości, wyliczone w arkuszu kalkulacyjnym Excel (z wykorzystaniem formuły matematycznej ZAOKR z parametrem „liczba_cyfr" równym 0).

a	$S_{100}(a)$	a	$S_{100}(a)$	a	$S_{100}(a)$	a	$S_{100}(a)$
0,00	0	0,25	−12,5	0,50	−25	0,75	−12,5
0,01	−0,5	0,26	−1	0,51	−0,5	0,76	0
0,02	−1	0,27	−0,5	0,52	0	0,77	−0,5
0,03	−0,5	0,28	0	0,53	−0,5	0,78	−1
0,04	0	0,29	−0,5	0,54	−1	0,79	−0,5
0,05	−2,5	0,30	−5	0,55	−2,5	0,80	0
0,06	−1	0,31	−0,5	0,56	0	0,81	−0,5
0,07	−0,5	0,32	0	0,57	−0,5	0,82	−1
0,08	0	0,33	−0,5	0,58	−1	0,83	−0,5
0,09	−0,5	0,34	−1	0,59	−0,5	0,84	0
0,10	−5	0,35	−2,5	0,60	0	0,85	−2,5
0,11	−0,5	0,36	0	0,61	−0,5	0,86	−1
0,12	0	0,37	−0,5	0,62	−1	0,87	−0,5
0,13	−0,5	0,38	−1	0,63	−0,5	0,88	0
0,14	−1	0,39	−0,5	0,64	0	0,89	−0,5
0,15	−2,5	0,40	0	0,65	−2,5	0,90	−5
0,16	0	0,41	−0,5	0,66	−1	0,91	−0,5
0,17	−0,5	0,42	−1	0,67	−0,5	0,92	0
0,18	−1	0,43	−0,5	0,68	0	0,93	−0,5
0,19	−0,5	0,44	0	0,69	−0,5	0,94	−1
0,20	0	0,45	−2,5	0,70	−5	0,95	−2,5
0,21	−0,5	0,46	−1	0,71	−0,5	0,96	0
0,22	−1	0,47	−0,5	0,72	0	0,97	−0,5
0,23	−0,5	0,48	0	0,73	−0,5	0,98	−1
0,24	0	0,49	−0,5	0,74	−1	0,99	−0,5

Tabela 3.4: Wartości $S_{100}(a)$ w zależności od a

W przykładzie 3.1.2 rozważyliśmy lokatę roczną oprocentowaną efektywną stopą roczną 4% i stwierdziliśmy, że przy jednostajnym rozkładzie wpłat i zaokrąglaniu

wypłat do pełnych złotych, wypłaty będą częściej zaokrąglane w dół, niż w górę, a więc bank częściej będzie wypłacać kwoty niższe niż wynikające z oprocentowania. Mogłoby się wydawać, że taki sposób zaokrąglania wypłat przyniesie bankowi korzyść (przy założeniu jednostajnego rozkładu wpłat). Tak jednak nie jest, gdyż jak widzimy w tabeli 3.4, suma $S_{100}(0,04)$ jest równa zero. Warto przy okazji zauważyć, że dla żadnego a suma $S_{100}(a)$ nie jest dodatnia.

Pokażemy, jak wartość $S_{100}(a)$ może być obliczona bez sumowania kolejnych stu składników. W tym celu skorzystamy z następującej obserwacji.

Lemat 3.1.8. Niech $\mathbb{U}$ bedzie zbiorem liczb postaci $\frac{k}{2}$, gdzie k jest liczbą naturalną nieparzystą, tzn. $\mathbb{U} = \{\frac{1}{2}, \frac{3}{2}, \frac{5}{2}, \ldots\}$. Dla każdej liczby naturalnej n i każdej liczby rzeczywistej r takiej, że $0 \leq r \leq n$ mamy równość

$$(n-r)_0 = \begin{cases} n-(r)_0, & \text{jeśli } r \notin \mathbb{U}, \\ n-(r)_0+1, & \text{jeśli } r \in \mathbb{U}. \end{cases} \tag{3.1.11}$$

Dowód. Jeśli r jest liczbą całkowitą, to $r \notin \mathbb{U}$ i oczywiście $(n-r)_0 = n-r = n-(r)_0$. Załóżmy więc, że liczba r nie jest całkowita i oznaczmy $t = r - [r]$. Ponieważ $r \leq n$ i liczba r nie jest całkowita, więc $[r]+1 \leq n$ i dlatego $n-[r]-1 \geq 0$. Ponadto

$$n-r = n-([r]+t) = (n-[r]-1)+(1-t). \tag{3.1.12}$$

Musi zachodzić jeden z poniższych trzech przypadków:

1) $t < 0,5$. Wówczas $r \notin \mathbb{U}$ i $(r)_0 = [r]$. Ponadto $1-t > 0,5$, więc korzystając z (3.1.12), otrzymujemy $(n-r)_0 = (n-[r]-1)+1 = n-[r] = n-(r)_0$.

2) $t = 0,5$. Wówczas $r \in \mathbb{U}$ i $(r)_0 = [r]+1$. Ponadto $1-t = 0,5$, więc z (3.1.12) otrzymujemy $(n-r)_0 = (n-[r]-1)+1 = n-[r] = n-(r)_0+1$.

3) $t > 0,5$. Wówczas $r \notin \mathbb{U}$ i $(r)_0 = [r]+1$. Ponadto $1-t < 0,5$, więc korzystając z (3.1.12), otrzymujemy $(n-r)_0 = n-[r]-1 = n-([r]+1) = n-(r)_0$.

W każdym z możliwych przypadków otrzymaliśmy wartość $(n-r)_0$ zgodną z (3.1.11), a więc dowód jest zakończony. □

Przypomnijmy, że dla liczby nieujemnej a, która może być zapisana z dwoma miejscami po przecinku, chcemy obliczyć sumę $S_{100}(a) = \sum_{x=1}^{100}(ax-(ax)_0)$. Oczywiście $S_{100}(0) = 0$. Aby obliczyć sumę $S_{100}(a)$ dla $a \neq 0$, zaczynamy od wyznaczenia najmniejszej liczby naturalnej n takiej, że an jest liczbą naturalną. Używając analogicznej argumentacji jak w przykładzie 3.1.2 stwierdzamy, że poszukiwaną liczbą jest

$$n = \frac{100}{NWD(A;100)}, \text{ gdzie } A = 100a.$$

Teraz rozważmy dowolną liczbę naturalną x taką, że $x < \frac{n}{2}$. Zauważmy, że $ax \notin \mathbb{U}$. Rzeczywiście, jeśli $ax \in \mathbb{U}$, to $a \cdot 2x$ jest liczbą naturalną i z wyboru liczby n wynika,

że $2x \geq n$, czyli $x \geq \frac{n}{2}$, sprzeczność. Dalej, dla każdego $x < \frac{n}{2}$ mamy $\frac{n}{2} < n-x \leq n-1$, więc w sumie

$$S_n(a) = \sum_{x=0}^{n} (ax - (ax)_0)$$

możemy składnik odpowiadający liczbie $x < \frac{n}{2}$ połączyć w parę ze składnikiem odpowiadającym liczbie $n-x$, przy czym $\frac{n}{2} < n-x \leq n-1$. Ponieważ, jak już wcześniej zauważyliśmy, $ax \notin \mathbb{U}$, więc z lematu 3.1.8 wynika, że

$$(a(n-x))_0 = (an-ax)_0 = an - (ax)_0,$$

a więc suma składników odpowiadających liczbom x i $n-x$ jest równa

$$\Big(ax - (ax)_0\Big) + \Big(a(n-x) - (a(n-x))_0\Big) = ax - (ax)_0 + an - ax - (an - (ax)_0) = 0.$$

Oprócz już rozważonych składników, w sumie $S_n(a)$ występuje jeszcze składnik odpowiadający liczbie $x = n$, który oczywiście jest równy 0 (gdyż wtedy $ax = an$ jest liczbą naturalną), oraz ewentualnie składnik odpowiadający liczbie $x = \frac{n}{2}$. Jest jasne, że ten ostatni składnik pojawi się wtedy i tylko wtedy, gdy n jest liczbą parzystą. Podsumowując, jeśli n jest liczbą nieparzystą, to $S_n(a) = 0$, a jeśli liczba n jest parzysta, to $S_n(a) = a \cdot \frac{n}{2} - (a \cdot \frac{n}{2})_0$. Pozostaje wyznaczyć wartość $a \cdot \frac{n}{2} - (a \cdot \frac{n}{2})_0$ dla parzystego n. Z wyboru liczby n wynika, że liczba an jest nieparzysta, więc liczba $a \cdot \frac{n}{2} = \frac{an}{2}$ ma w zapisie dziesiętnym cyfrę 5 na pierwszym miejscu po przecinku. Zatem liczba ta jest zaokrąglana w górę i dlatego dla $x = \frac{n}{2}$ (gdy n jest parzyste) mamy

$$a \cdot \frac{n}{2} - (a \cdot \frac{n}{2})_0 = -0,5,$$

a więc gdy n jest parzyste, to $S_n(a) = -0,5$.

Ponieważ $n = \frac{100}{NWD(100a;100)}$ i $S_{100}(a) = \frac{100}{n} \cdot S_n(a)$, więc otrzymujemy równość

$$S_{100}(a) = NWD(100a;100) \cdot S_n(a).$$

Ponadto $n = \frac{100}{NWD(100a;100)}$ jest liczbą parzystą wtedy i tylko wtedy, gdy liczba $NWD(100a;100)$ nie dzieli się przez 4, czyli gdy 4 nie dzieli liczby $100a$. Zatem udowodniliśmy następujące stwierdzenie, rozwiązujące problem 3.1.7.

Stwierdzenie 3.1.9. Jeżeli a jest liczbą rzeczywistą nieujemną, która w zapisie dziesiętnym może być przedstawiona z dwoma miejscami po przecinku, to

$$S_{100}(a) = \begin{cases} -NWD(100a;100) \cdot 0,5, & \text{jeśli 4 nie dzieli } 100a, \\ 0, & \text{jeśli 4 dzieli } 100a. \end{cases}$$

3.2 Algebraiczne aspekty zaokrąglania liczb

W tej części rozdziału rozważymy dwa grupoidy zdefiniowane przy pomocy zaokrąglania liczb, odpowiednio do setek i do części całkowitej. W każdym z tych grupoidów wyznaczymy wszystkie podgrupoidy cykliczne będące półgrupami.

Przypomnijmy, że grupoidem nazywamy zbiór W z określonym w nim działaniem dwuargumentowym $\diamond$. Podgrupoidem grupoidu $(W,\diamond)$ nazywamy podzbiór V zbioru W taki, że V z działaniem $\diamond$ ograniczonym do elementów zbioru V jest grupoidem. Podgrupoidem grupoidu $(W,\diamond)$ generowanym przez podzbiór $Z \subseteq W$ nazywamy najmniejszy (ze względu na relację inkluzji) podgrupoid grupoidu $(W,\diamond)$ zawierający Z; podgrupoid ten oznaczamy symbolem $\langle Z\rangle$ (jest on przekrojem wszystkich podgrupoidów zawierających Z). Podgrupoidem cyklicznym nazywamy podgrupoid $\langle x\rangle$ generowany przez pojedynczy element $x \in W$.

Niech $\mathbb{N}$ oznacza zbiór liczb naturalnych. Dla elementu x grupoidu $(W,\diamond)$ i liczby $n \in \mathbb{N}$ definiujemy indukcyjnie element $x^{(n)} \in W$ następująco:

$$x^{(1)} = x,\ x^{(n)} = x^{(n-1)} \diamond x \text{ dla } n > 1.$$

Zatem

$$x^{(1)} = x,\ x^{(2)} = x \diamond x,\ x^{(3)} = (x \diamond x) \diamond x,\ x^{(4)} = ((x \diamond x) \diamond x) \diamond x, \text{ itd.}$$

Element $x^{(n)}$ będziemy nazywać n-tą potęgą elementu x, a zbiór wszystkich potęg elementu x będziemy oznaczać przez $P(x)$, tzn. $P(x) = \{x^{(n)} : n \in \mathbb{N}\}$.

Niech $(W,\diamond)$ będzie grupoidem. Mówimy, że działanie $\diamond$ jest łączne w niepustym podzbiorze Z zbioru W, jeśli $(a \diamond b) \diamond c = a \diamond (b \diamond c)$ dla dowolnych elementów $a,b,c \in Z$. Jeżeli działanie $\diamond$ jest łączne w zbiorze W, to grupoid $(W,\diamond)$ nazywamy półgrupą.

3.2.1 Grupoid zdefiniowany przy pomocy zaokrąglania do setek

Zaokrąglenie liczby całkowitej nieujemnej x (zapisanej w układzie dziesiętnym) do setek polega na zastąpieniu jej cyfr jedności i dziesiątek zerami, a ponadto dodaniu 100 do tak otrzymanej liczby, jeśli cyfra dziesiątek przed wyzerowaniem była większa lub równa 5. Otrzymane w ten sposób zaokrąglenie liczby x będziemy oznaczać symbolem $(x)_{-2}$ (indeks -2 w tym symbolu jest liczbą, której należy użyć w Excelu jako wartość parametru „liczba_cyfr" w formule matematycznej ZAOKR, aby otrzymać zaokrąglenie do setek). Zauważmy, że jeśli $[x]_{100}$ jest resztą z dzielenia liczby x przez 100, to

$$(x)_{-2} = \begin{cases} x - [x]_{100}, & \text{jeśli } [x]_{100} < 50, \\ x - [x]_{100} + 100, & \text{jeśli } [x]_{100} \geq 50. \end{cases} \tag{3.2.1}$$

Pokażemy, że zaokrąglanie do setek zachowuje nierówności, tzn. ma następującą własność.

Stwierdzenie 3.2.1. Niech x i y będą nieujemnymi liczbami całkowitymi. Jeżeli $x \leq y$, to $(x)_{-2} \leq (y)_{-2}$.

Dowód. Niech $k = [x]_{100}$ i $l = [y]_{100}$. Wtedy $x = 100m+k$ i $y = 100n+l$ dla pewnych nieujemnych liczb całkowitych m,n. Ponieważ $x \leq y$, więc

$$100m \leq x \leq y < 100(n+1)$$

i dlatego $m < n+1$, tzn. $m \leq n$. Jeżeli $m \leq n-1$, to

$$(x)_{-2} < 100(m+1) \leq 100n \leq (y)_{-2},$$

a więc spełniona jest nierówność, którą dowodzimy.

Pozostał do rozpatrzenia przypadek, gdy $m = n$. Wtedy $k \leq l$ i musi zachodzić jeden z poniższych trzech przypadków:

1) $k \leq l < 50$. Wówczas $(x)_{-2} = 100m = 100n = (y)_{-2}$.
2) $k < 50 \leq l$. Wówczas $(x)_{-2} = 100m = 100n < 100(n+1) = (y)_{-2}$.
3) $50 \leq k \leq l$. Wówczas $(x)_{-2} = 100(m+1) = 100(n+1) = (y)_{-2}$.

W każdym z tych przypadków otrzymaliśmy nierówność $(x)_{-2} \leq (y)_{-2}$, więc dowód jest zakończony. □

Niech $T = \{0,1,\ldots,99\}$ i $x,y \in T$. Wtedy iloczyn xy jest liczbą całkowitą nieujemną nieprzekraczającą liczby $99^2 = 9801$. Zatem zaokrąglenie iloczynu xy do setek nie przekracza liczby 9800, a więc po podzieleniu tego zaokrąglenia przez 100 jako wynik otrzymujemy liczbę ze zbioru T, którą będziemy oznaczać przez $x \circ y$. Wynika stąd, że zbiór T jest grupoidem z działaniem

$$x \circ y = \frac{(xy)_{-2}}{100}. \tag{3.2.2}$$

Łącząc (3.2.2) z (3.2.1) otrzymujemy następującą definicję działania $\circ$ w zbiorze T, odwołującą się do reszt z dzielenia przez 100:

$$x \circ y = \begin{cases} \frac{xy-[xy]_{100}}{100}, & \text{jeśli } [xy]_{100} < 50, \\ \frac{xy-[xy]_{100}}{100} + 1, & \text{jeśli } [xy]_{100} \geq 50. \end{cases} \tag{3.2.3}$$

Oczywiście działanie $\circ$ jest przemienne. Pokażemy, że nie ma ono elementu neutralnego. Przypuśćmy, że $e \in T$ jest elementem neutralnym. Wtedy $51 \circ e = 51$, a więc musi być $51e \geq 5050$, skąd wynikają nierówności

$$e \geq \frac{5050}{51} = 99\frac{1}{51} > 99.$$

Zatem $e \notin T$, tzn. otrzymaliśmy sprzeczność.

Zauważmy, że działanie $\circ$ zachowuje nierówności, tzn. $\circ$ ma następującą własność.

Wniosek 3.2.2. Jeżeli $x, y, z \in T$ i $x \leq y$, to $x \circ z \leq y \circ z$.

Dowód. Ponieważ $x \leq y$ i $z \geq 0$, więc $xz \leq yz$ i dlatego na mocy stwierdzenia 3.2.1 zachodzi nierówność $(xz)_{-2} \leq (yz)_{-2}$. Stąd i z (3.2.2) wynika, że

$$x \circ z = \frac{(xz)_{-2}}{100} \leq \frac{(yz)_{-2}}{100} = y \circ z,$$

co kończy dowód. □

Pokażemy, że dla każdego $x \in T$ ciąg kolejnych potęg elementu x jest nierosnący.

Stwierdzenie 3.2.3. Jeżeli $m, n \in \mathbb{N}$ i $m \leq n$, to $x^{(m)} \geq x^{(n)}$ dla każdego $x \in T$.

Dowód. Niech $x \in T$. Wystarczy udowodnić, że $x^{(n)} \geq x^{(n+1)}$ dla każdego $n \in \mathbb{N}$. Zastosujemy metodę indukcji matematycznej. Ponieważ $x < 100$, więc $x^2 \leq 100x$ i ze stwierdzenia 3.2.1 wynika, że $(x^2)_{-2} \leq (100x)_{-2} = 100x$. Zatem

$$x^{(2)} = x \circ x = \frac{(x^2)_{-2}}{100} \leq \frac{100x}{100} = x = x^{(1)}.$$

Udowodniliśmy już, że $x^{(1)} \geq x^{(2)}$. Stąd i z wniosku 3.2.2 otrzymujemy

$$x^{(2)} = x^{(1)} \circ x \geq x^{(2)} \circ x = x^{(3)}.$$

Kontynując w ten sposób, stwierdzamy że

$$x^{(1)} \geq x^{(2)} \geq x^{(3)} \geq \ldots,$$

skąd wynika dowodzona własność. □

Odnotujmy jeszcze jedną zależność między potęgami $x^{(1)} = x$ i $x^{(2)}$ elementu $x \in T$, z której skorzystamy w dalszej części rozdziału.

Stwierdzenie 3.2.4. Jeżeli $x \in T \setminus \{0\}$, to $x^{(2)} < x$.

Dowód. Niech s będzie resztą z dzielenia x^2 przez 100. Jeżeli $s < 50$, to $x \circ x = \frac{x^2 - s}{100} \leq \frac{x^2}{100}$. W przeciwnym przypadku $s \geq 50$ i wówczas $x \circ x = \frac{x^2 - s}{100} + 1 \leq \frac{x^2 + 50}{100}$. Zatem w każdym przypadku mamy $x^{(2)} = x \circ x \leq \frac{x^2+50}{100}$ i dlatego wystarczy pokazać, że

$$\frac{x^2 + 50}{100} < x \text{ (tzn. } x^2 - 100x + 50 < 0) \text{ dla każdej liczby naturalnej } x \leq 99. \quad (3.2.4)$$

Ponieważ $1 \leq x \leq 99$, więc $-49 \leq x-50 \leq 49$ i dlatego $(x-50)^2 \leq 49^2$. Zatem $x^2 - 100x = (x-50)^2 - 50^2 \leq 49^2 - 50^2 = (49-50)(49+50) = -99 < -50$, czyli jest spełniony warunek (3.2.4). □

Ze stwierdzenia 3.2.3 wynika, że dla każdego $x \in T$ istnieje liczba naturalna k taka, że $x^{(k)} = x^{(k+1)}$. Najmniejszą liczbę k o tej własności oznaczmy przez $\ell(x)$. Bezpośrednią konsekwencją stwierdzenia 3.2.3 jest nierówność $\ell(x) \leq x+1$.

Przypomnijmy, że dla $x \in T$ symbol $P(x)$ oznacza zbiór potęg elementu x, czyli $P(x) = \{x^{(n)} : n \in \mathbb{N}\}$. Jest jasne, że zbiór $P(x)$ ma $\ell(x)$ elementów. Z definicji liczby $\ell(x)$ wynika, że elementami zbioru $P(x)$ są kolejne potęgi liczby x, do potęgi $x^{(\ell(x))}$ włącznie, tzn. kolejne wyrazy ciągu potęg $(x^{(n)})$ dla wykładników od $n = 1$ do $n = \ell(x)$. Poniżej przedstawiono algorytm wyznaczający ten ciąg potęg.

Algorytm 3.1 $findPowers(x)$ - algorytm wyznaczania ciągu potęg $(x^{(n)})$

INPUT: x - liczba ze zbioru T
OUTPUT: $powers_x$ - kolejne potęgi liczby x

1: $powers_x \leftarrow \emptyset$
2: $previous \leftarrow -1$
3: $current \leftarrow x$
4: **while** $previous \neq current$ **do**
5: $\quad powers_x \leftarrow powers_x \cup \{current\}$
6: $\quad previous \leftarrow current$
7: $\quad current \leftarrow current \circ x$
8: **end while**
9: **return** $powers_x$

Kolejny algorytm korzysta z algorytmu 3.1, aby wyznaczyć ciągi potęg $(x^{(n)})$ dla kolejnych liczb $x \in T$ i $n = 1, 2, \ldots, \ell(x)$.

Algorytm 3.2 Algorytm wyznaczania ciągów potęg $(x^{(n)})$

OUTPUT: c - ciągi $(x^{(n)})$

1: $c \leftarrow \emptyset$
2: **for** $x \leftarrow 0$ **to** 99 **do**
3: $\quad c \leftarrow c \cup findPowers(x)$
4: **end for**
5: **return** c

W tabelach 3.5 i 3.6 przedstawiono wartości $\ell(x)$ i kolejne wartości $x^{(n)}$ dla wszystkich $x \in T = \{0, 1, 2, \ldots, 99\}$ i $n \leq \ell(x)$, otrzymane jako wynik działania algorytmu 3.2.

x	$\ell(x)$	ciąg $(x^{(n)})$
0	1	0
1	2	1,0
2	2	2,0
3	2	3,0
4	2	4,0
5	2	5,0
6	2	6,0
7	2	7,0
8	3	8,1,0
9	3	9,1,0
10	3	10,1,0
11	3	11,1,0
12	3	12,1,0
13	3	13,2,0
14	3	14,2,0
15	3	15,2,0
16	3	16,3,0
17	4	17,3,1,0
18	4	18,3,1,0
19	4	19,4,1,0
20	4	20,4,1,0
21	4	21,4,1,0
22	4	22,5,1,0
23	4	23,5,1,0
24	4	24,6,1,0
25	5	25,6,2,1,0
26	5	26,7,2,1,0
27	5	27,7,2,1,0
28	5	28,8,2,1,0
29	5	29,8,2,1,0
30	5	30,9,3,1,0
31	5	31,10,3,1,0
32	5	32,10,3,1,0
33	5	33,11,4,1,0
34	5	34,12,4,1,0
35	5	35,12,4,1,0
36	6	36,13,5,2,1,0
37	6	37,14,5,2,1,0
38	6	38,14,5,2,1,0
39	6	39,15,6,2,1,0

x	$\ell(x)$	ciąg $(x^{(n)})$
40	6	40,16,6,2,1,0
41	6	41,17,7,3,1,0
42	6	42,18,8,3,1,0
43	6	43,18,8,3,1,0
44	7	44,19,8,4,2,1,0
45	7	45,20,9,4,2,1,0
46	7	46,21,10,5,2,1,0
47	7	47,22,10,5,2,1,0
48	7	48,23,11,5,2,1,0
49	7	49,24,12,6,3,1,0
50	7	50,25,13,7,4,2,1
51	7	51,26,13,7,4,2,1
52	7	52,27,14,7,4,2,1
53	7	53,28,15,8,4,2,1
54	8	54,29,16,9,5,3,2,1
55	8	55,30,17,9,5,3,2,1
56	8	56,31,17,10,6,3,2,1
57	8	57,32,18,10,6,3,2,1
58	8	58,34,20,12,7,4,2,1
59	8	59,35,21,12,7,4,2,1
60	9	60,36,22,13,8,5,3,2,1
61	9	61,37,23,14,9,5,3,2,1
62	9	62,38,24,15,9,6,4,2,1
63	10	63,40,25,16,10,6,4,3,2,1
64	10	64,41,26,17,11,7,4,3,2,1
65	10	65,42,27,18,12,8,5,3,2,1
66	11	66,44,29,19,13,9,6,4,3,2,1
67	11	67,45,30,20,13,9,6,4,3,2,1
68	11	68,46,31,21,14,10,7,5,3,2,1
69	12	69,48,33,23,16,11,8,6,4,3,2,1
70	12	70,49,34,24,17,12,8,6,4,3,2,1
71	12	71,50,36,26,18,13,9,6,4,3,2,1
72	13	72,52,37,27,19,14,10,7,5,4,3,2,1
73	13	73,53,39,28,20,15,11,8,6,4,3,2,1
74	14	74,55,41,30,22,16,12,9,7,5,4,3,2,1
75	14	75,56,42,32,24,18,14,11,8,6,5,4,3,2
76	14	76,58,44,33,25,19,14,11,8,6,5,4,3,2
77	14	77,59,45,35,27,21,16,12,9,7,5,4,3,2
78	15	78,61,48,37,29,23,18,14,11,9,7,5,4,3,2
79	16	79,62,49,39,31,24,19,15,12,9,7,6,5,4,3,2

Tabela 3.5: Wartości $\ell(x)$ i ciągi $(x^{(n)})$ dla $x \leq 79$ i $n \leq \ell(x)$

W tabeli 3.6 dla liczb $k > m$ symbol $k \searrow m$ oznacza malejący ciąg liczb naturalnych, zmniejszających się o 1, rozpoczynający się od k i kończący na m, tzn. ciąg

$$k, k-1, k-2, \ldots, m+1, m.$$

x	$\ell(x)$	ciąg $(x^{(n)})$
80	17	80,64,51,41,33,26,21,17,14,11,9,7 ↘ 2
81	17	81,66,53,43,35,28,23,19,15,12,10,8,6 ↘ 2
82	18	82,67,55,45,37,30,25,21,17,14,11,9,7 ↘ 2
83	19	83,69,57,47,39,32,27,22,18,15,12,10,8 ↘ 2
84	19	84,71,60,50,42,35,29,24,20,17,14,12,10,8 ↘ 3
85	21	85,72,61,52,44,37,31,26,22,19,16,14,12,10 ↘ 3
86	22	86,74,64,55,47,40,34,29,25,22,19,16,14,12,8 ↘ 3
87	24	87,76,66,57,50,44,38,33,29,25,22,19,17,15,13,11 ↘ 3
88	24	88,77,68,60,53,47,41,36,32,28,25,22,19,17,15,13,11 ↘ 3
89	26	89,79,70,62,55,49,44,39,35,31,28,25,22,20,18,16,14,12 ↘ 4
90	28	90,81,73,66,59,53,48,43,39,35,32,29,26,23,21,19,17,15 ↘ 5
91	30	91,83,76,69,63,57,52,47,43,39,35,32,29,26,24,22,20,18,16 ↘ 5
92	32	92,85,78,72,66,61,56,52,48,44,40,37,34,31,29,27,25,23,21,19,17 ↘ 6
93	35	93,86,80,74,69,64,60,56,52,48,45,42,39,36,33,31,29,27,25,23,21 ↘ 7
94	39	94,88,83,78,73,69,65,61,57,54,51,48,45,42,39,37,35,33,31,29,27,25 ↘ 8
95	43	95,90,86,82,78,74,70,67,64,61,58,55,52,49,47,45,43,41,39,37,35,33,31,29 ↘ 10
96	48	96,92,88,84,81,78,75,72,69,66,63,60,58,56,54,52,50,48,46,44,42,40,38,36 ↘ 12
97	56	97,94,91,88,85,82,80,78,76,74,72,70,68,66,64,62,60,58,56,54,52,50 ↘ 16
98	62	98,96,94,92,90,88,86,84,82,80,78,76,74 ↘ 25
99	50	99 ↘ 50

Tabela 3.6: Wartości $\ell(x)$ i ciągi $(x^{(n)})$ dla $80 \leq x \leq 99$ i $n \leq \ell(x)$

Przypomnijmy, że podgrupoid V grupoidu $(T, \circ)$ nazywamy cyklicznym, jeżeli jest on generowany przez pojedynczy element grupoidu T, tzn. $V = \langle x \rangle$ dla pewnego $x \in T$. W tej części rozdziału wyznaczymy wszystkie cykliczne podgrupoidy grupoidu T, które są półgrupami. W wykonaniu tego zadania pomocne będzie następujące twierdzenie.

Twierdzenie 3.2.5. Niech zbiór W z działaniem $\diamond$ będzie grupoidem. Dla dowolnego elementu $x \in W$ następujące warunki są równoważne:

(1) $\langle x \rangle$ z działaniem $\diamond$ jest półgrupą.
(2) $P(x)$ z działaniem $\diamond$ jest półgrupą.
(3) Działanie $\diamond$ jest łączne w zbiorze $P(x)$.
(4) $x^{(m)} \diamond x^{(n)} = x^{(m+n)}$ dla dowolnych liczb $m, n \in \mathbb{N}$.

Jeżeli jest spełniony którykolwiek z powyższych (równoważnych) warunków, to $\langle x \rangle = P(x)$.

Dowód. (1) $\Rightarrow$ (3): Ta implikacja jest oczywista.

(3) $\Rightarrow$ (4): Załóżmy, że działanie $\diamond$ jest łączne w zbiorze $P(x)$. Pokażemy, że wtedy spełniony jest warunek (4). W tym celu zastosujemy metodę indukcji ze względu na n. Ponieważ dla dowolnego $m \in \mathbb{N}$ mamy $x^{(m)} \diamond x^{(1)} = x^{(m)} \diamond x = x^{(m+1)}$, więc dla

$n = 1$ warunek (4) jest spełniony. Załóżmy, że jest on spełniony dla danej liczby n i dowolnej liczby m. Stąd i z założenia o łączności działania $\diamond$, otrzymujemy dla dowolnej liczby m, że

$$x^{(m)} \diamond x^{(n+1)} = x^{(m)} \diamond (x^{(n)} \diamond x) = (x^{(m)} \diamond x^{(n)}) \diamond x = x^{(m+n)} \diamond x = x^{((m+n)+1)} = x^{(m+(n+1))}.$$

Zatem warunek (4) jest spełniony również dla $n+1$.

(4) $\Rightarrow$ (2): Załóżmy, że jest spełniony warunek (4). Aby pokazać, że spełniony jest warunek (2), wystarczy pokazać, że działanie $\diamond$ jest łączne w zbiorze $P(x)$. W tym celu rozważmy dowolne elementy $a, b, c \in P(x)$. Wówczas $a = x^{(p)}, b = x^{(q)}, c = x^{(r)}$ dla pewnych $p, q, r \in \mathbb{N}$. Korzystając z (4), otrzymujemy równości

$$(a \diamond b) \diamond c = (x^{(p)} \diamond x^{(q)}) \diamond x^{(r)} = x^{(p+q)} \diamond x^{(r)} = x^{((p+q)+r)} = x^{(p+(q+r))} =$$

$$= x^{(p)} \diamond x^{(q+r)} = x^{(p)} \diamond (x^{(q)} \diamond x^{(r)}) = a \diamond (b \diamond c),$$

a więc warunek (2) jest spełniony.

(2) $\Rightarrow$ (1): Załóżmy, że spełniony jest warunek (2). Wtedy $P(x)$ jest podgrupoidem grupoidu W, a ponieważ $x = x^{(1)} \in P(x)$, więc otrzymujemy zawieranie $\langle x \rangle \subseteq P(x)$. Ponieważ odwrotne zawieranie jest oczywiste, więc zachodzi równość $\langle x \rangle = P(x)$, a zatem na mocy (2) zbiór $\langle x \rangle$ jest półgrupą.

Prawdziwość ostatniej części twierdzenia została pokazana w dowodzie implikacji (2) $\Rightarrow$ (1). $\square$

Ponieważ działanie $\circ$ jest przemienne, więc z twierdzenia 3.2.5 otrzymujemy następujący wniosek.

Wniosek 3.2.6. Dla dowolnego elementu $x \in T$ następujące warunki są równoważne.

(1) $\langle x \rangle$ z działaniem $\circ$ jest półgrupą.
(2) Działanie $\circ$ jest łączne w zbiorze $P(x)$.
(3) $x^{(m)} \circ x^{(n)} = x^{(m+n)}$ dla dowolnych liczb $m, n \in \mathbb{N}$ takich, że $m \leq n \leq \ell(x)$.

Aby sprawdzić dla danej liczby $x \in T$, czy podgrupoid $\langle x \rangle$ jest półgrupą (równoważnie, czy działanie $\circ$ jest łączne w zbiorze $\langle x \rangle$), można zastosować poniższy algorytm, korzystający z wniosku 3.2.6 (algorytm sprawdza, czy spełniony jest warunek (3) z tego wniosku).

Algorytm 3.3 *checkAssociativity*(x) - algorytm sprawdzania łączności działania $\circ$ w zbiorze $\langle x \rangle$

INPUT: $powers_x$ - ciąg potęg $(x^{(n)})$ liczby $x \in T$
OUTPUT: Wynik sprawdzenia łączności działania $\circ$ w zbiorze $\langle x \rangle$

```
1: ℓ ← length(powers_x)
2: for m ← 1 to ℓ do
3:     for n ← m to ℓ do
4:         left ← powers_x[m] ∘ powers_x[n]
5:         if m+n > ℓ then
6:             right ← powers_x[ℓ]
7:         else
8:             right ← powers_x[m+n]
9:             if left ≠ right then
10:                return false; m, n
11:            end if
12:        end if
13:    end for
14: end for
15: return true
```

Aby wyznaczyć wszystkie liczby $x \in T$, dla których działanie $\circ$ w zbiorze $\langle x \rangle$ jest łączne, zastosowano poniższy algorytm 3.4.

Algorytm 3.4 Algorytm sprawdzania łączności działania $\circ$ w zbiorze $\langle x \rangle$ dla wszystkich $x \in T$

OUTPUT: *results* - Wynik sprawdzenia łączności działania $\circ$ w zbiorze $\langle x \rangle$ dla kolejnych liczb $x \in T$

```
1: results ← ∅
2: for x ← 0 to 99 do
3:     powers_x ← findPowers(x)
4:     result ← checkAssociativity(powers_x)
5:     results ← results ∪ {result}
6: end for
7: return results
```

W wyniku działania algorytmu 3.4 stwierdzono, że działanie $\circ$ jest łączne w zbiorze $\langle x\rangle$ (tzn. $\langle x\rangle$ jest półgrupą) tylko i wyłącznie dla następujących trzydziestu dziewięciu wartości x:

$$0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,$$
$$21,22,23,24,28,29,30,31,32,33,34,35,36,37,38,39,44,45,$$

tzn. dla wszystkich nieujemnych liczb całkowitych x mniejszych od 46, z wyjątkiem następujących siedmiu liczb:

$$25,26,27,40,41,42,43.$$

Zatem w zbiorze $\{0,1,\ldots,99\}$ jest 61 liczb x takich, że działanie $\circ$ nie jest łączne w podgrupoidzie cyklicznym $\langle x\rangle$. W tabeli 3.7 dla każdej z tych sześćdziesięciu jeden liczb x podano najmniejszą w porządku leksykograficznym parę uporządkowaną (m,n) taką, że $x^{(m)}\circ x^{(n)} \neq x^{(m+n)}$.

x	(m,n)
25	(2,2)
26	(2,2)
27	(2,2)
40	(2,2)
41	(2,4)
42	(2,4)
43	(2,4)
46	(2,2)
47	(3,4)
48	(2,3)
49	(2,5)
50	(2,2)

x	(m,n)
51	(2,3)
52	(2,7)
53	(2,7)
54	(2,2)
55	(2,8)
56	(2,3)
57	(2,8)
58	(2,8)
59	(2,8)
60	(2,9)
61	(2,9)
62	(2,2)

x	(m,n)
63	(2,6)
64	(2,5)
65	(2,3)
66	(2,4)
67	(2,3)
68	(2,5)
69	(2,6)
70	(2,12)
71	(2,2)
72	(2,11)
73	(2,3)
74	(2,3)

x	(m,n)
75	(2,2)
76	(2,2)
77	(2,14)
78	(2,15)
79	(2,2)
80	(2,7)
81	(2,2)
82	(2,6)
83	(2,2)
84	(2,3)
85	(2,5)
86	(2,4)

x	(m,n)
87	(2,2)
88	(2,2)
89	(2,5)
90	(2,10)
91	(2,9)
92	(2,9)
93	(2,5)
94	(2,2)
95	(2,2)
96	(2,2)
97	(2,3)
98	(2,7)
99	(2,25)

Tabela 3.7: Liczby $x \in T$, dla których działanie $\circ$ nie jest łączne w zbiorze $\langle x\rangle$ wraz z najmniejszą (w porządku leksykograficznym) parą (m,n) taką, że $x^{(m)}\circ x^{(n)} \neq x^{(m+n)}$

Zauważmy, że już na podstawie tabel 3.5 i 3.6 można było stwierdzić, że dla każdej liczby $x \geq 50$ podgrupoid generowany przez x nie jest półgrupą. Otóż zgodnie z twierdzeniem 3.2.5, jeżeli dla elementu $x \in T$ podgrupoid $\langle x\rangle$ jest półgrupą, to zbiór $P(x)$ jest zamknięty ze względu na działanie $\circ$, co na mocy poniższego wniosku implikuje, że $x^{(\ell(x))} = 0$. Zatem warunkiem koniecznym, aby podmonoid $\langle x\rangle$ był półgrupą jest równość $x^{(\ell(x))} = 0$, a jak widzimy z tabel 3.5 i 3.6, równość ta nie zachodzi dla żadnej liczby $x \geq 50$.

Wniosek 3.2.7. Jeżeli $x \in T$ i zbiór $P(x)$ jest zamknięty ze względu na działanie $\circ$, to $x^{(\ell(x))} = 0$.

Dowód. Załóżmy, że zbiór $P(x)$ jest zamknięty ze względu na działanie $\circ$ i $x^{(\ell(x))} \neq 0$. Wówczas $x^{(\ell(x))} \circ x^{(\ell(x))} = x^{(k)}$ dla pewnego $k \in \mathbb{N}$ i ze stwierdzenia 3.2.4 otrzymujemy

$$x^{(k)} = x^{(\ell(x))} \circ x^{(\ell(x))} < x^{(\ell(x))},$$

co jest niemożliwe, gdyż $x^{(\ell(x))}$ jest najmniejszym elementem zbioru $P(x)$. □

3.2.2 Grupoid zdefiniowany przy pomocy zaokrąglania do części całkowitej

W tej części rozdziału rozważymy grupoid zdefiniowany przy pomocy zaokrąglania liczb rzeczywistych nieujemnych do części całkowitej, tzn. zaokrąglania w dół do najbliższej liczby całkowitej. Takie zaokrąglanie polega na zastąpieniu liczby nieujemnej x jej częścią całkowitą $[x]$. Jest ono również nazywane obcinaniem, gdyż polega na „obcięciu" cyfr po przecinku w zapisie dziesiętnym zaokrąglanej liczby. W arkuszu kalkulacyjnym Excel zaokrąglenie liczby do jej części całkowitej można wyznaczyć przy pomocy formuły matematycznej ZAOKR.DO.CAŁK.

Niech $\mathbb{R}_+$ oznacza zbiór nieujemnych liczb rzeczywistych. Oczywiście zbiór $\mathbb{R}_+$ jest grupoidem z działaniem

$$x \circledast y = [xy].$$

Jest jasne, że jeśli iloczyn xy jest liczbą całkowitą (w szczególności, jeśli x i y są liczbami całkowitymi), to $x \circledast y = xy$.

Wyznaczymy wszystkie liczby $x \in \mathbb{R}_+$ takie, że podgrupoid $\langle x \rangle$ grupoidu $(\mathbb{R}_+, \circledast)$ jest półgrupą.

Twierdzenie 3.2.8. Niech $x \in \mathbb{R}_+$. Podgrupoid $\langle x \rangle$ jest półgrupą wtedy i tylko wtedy, gdy x jest liczbą całkowitą lub $x < \sqrt{2}$.

Dowód. Załóżmy, że $\langle x \rangle$ jest półgrupą. Wtedy spełniony jest warunek (4) z twierdzenia 3.2.5 i dlatego

$$x^{(3)} \circledast x^{(3)} = x^{(6)} = x^{(4)} \circledast x^{(2)} = x^{(2)} \circledast x^{(2)} \circledast x^{(2)}, \tag{3.2.5}$$

a ponieważ $x^{(3)}$ i $x^{(2)}$ są liczbami całkowitymi, więc z (3.2.5) wynika następująca równość iloczynów liczb całkowitych nieujemnych:

$$x^{(3)} \cdot x^{(3)} = x^{(2)} \cdot x^{(2)} \cdot x^{(2)}. \tag{3.2.6}$$

Korzystając z jednoznaczności rozkładu liczb naturalnych na iloczyn potęg liczb pierwszych, można łatwo wywnioskować z (3.2.6), że $x^{(2)} = k^2$ i $x^{(3)} = k^3$ dla pewnej

nieujemnej liczby całkowitej k (wynika to także z (Sierpiński, 1964, str. 29, Corollary 1)). Metodą indukcji matematycznej udowodnimy, że

$$x^{(n)} = k^n \text{ dla każdej liczby naturalnej } n \geq 2. \tag{3.2.7}$$

Wiemy już, że równość w (3.2.7) zachodzi dla $n = 2$ i $n = 3$. Załóżmy więc, że $n \geq 4$ i równość w warunku (3.2.7) zachodzi dla liczby $n-2$. Ponieważ $x^{(2)}$ i $x^{(n-2)}$ są liczbami całkowitymi, więc korzystając z twierdzenia 3.2.5 otrzymujemy równości

$$x^{(n)} = x^{(2)} \circledast x^{(n-2)} = x^{(2)} \cdot x^{(n-2)} = k^2 \cdot k^{n-2} = k^n.$$

Zatem równość w (3.2.7) zachodzi dla liczby n, skąd wynika prawdziwość (3.2.7).

Zauważmy, że

$$[x] = k. \tag{3.2.8}$$

Rzeczywiście, ponieważ $x^{(2)} = k^2$, czyli $[x^2] = k^2$, więc

$$k^2 \leq x^2 < k^2 + 1 \leq k^2 + 2k + 1 = (k+1)^2$$

i dlatego $k \leq x < k+1$, skąd wynika (3.2.8).

Na mocy (3.2.8) mamy równość $x = k + r$, gdzie $0 \leq r < 1$. Pokażemy, że $k \in \{0, 1\}$ lub $r = 0$. Ponieważ

$$x^{(2)}x = k^2 x = k^2(k+r) = k^3 + k^2 r,$$

więc

$$k^3 = x^{(3)} = x^{(2)} \circledast x = [x^{(2)}x] = [k^3 + k^2 r] = k^3 + [k^2 r]$$

i dlatego $[k^2 r] = 0$, skąd wynika, że $k^2 r < 1$. Analogicznie można pokazać, że

$$k^n r < 1 \text{ dla każdej liczby naturalnej } n.$$

Zatem $r = 0$ lub $k \in \{0, 1\}$.

Jeśli $r = 0$, to $x = k$ jest liczbą całkowitą. Pozostaje do rozważenia przypadek, gdy $r \neq 0$. Wtedy $k = 0$ lub $k = 1$. Jeśli $k = 0$, to oczywiście $x = k + r = r < \sqrt{2}$. Załóżmy, że $k = 1$. Wtedy $[x^2] = x^{(2)} = k^2 = 1^2 = 1$. Zatem $x^2 < 2$ i dlatego $x < \sqrt{2}$.

Udowodniliśmy, że jeśli $\langle x \rangle$ jest półgrupą, to x jest liczbą całkowitą lub $x < \sqrt{2}$. Na mocy twierdzenia 3.2.5, aby udowodnić implikację odwrotną, wystarczy pokazać, że jeśli x jest liczbą całkowitą lub $x < \sqrt{2}$, to zbiór $P(x)$ z działaniem $\circledast$ jest półgrupą.

Jeżeli liczba x jest całkowita, to $x^{(n)} = x^n$ dla każdego $n \in \mathbb{N}$. Zatem w tym przypadku $P(x) = \{x^n : n \in \mathbb{N}\}$ i działanie $\circledast$ ograniczone do zbioru $P(x)$ jest zwykłym mnożeniem, a więc $P(x)$ z działaniem $\circledast$ jest półgrupą.

Pozostał do rozważenia przypadek, gdy $x < \sqrt{2}$. Jeżeli $x < 1$, to $x^{(n)} = 0$ dla każdego $n \geq 2$, więc $P(x) = \{x, 0\}$ jest półgrupą z działaniem $\circledast$. Jeśli $1 \leq x < \sqrt{2}$, to

$x^{(n)} = 1$ dla każdego $n \geq 2$, więc $P(x) = \{x, 1\}$ i oczywiście $P(x)$ z działaniem $\circledast$ jest półgrupą. □

Twierdzenie 3.2.8 może sugerować, że zbiór

$$V = \{x \in \mathbb{R}_+ : x < \sqrt{2}\}$$

z działaniem $\circledast$ jest półgrupą. To jednak nie jest prawdą, gdyż, na przykład, liczby $\frac{9}{10}, 1, \frac{12}{10}$ należą do V,

$$\frac{9}{10} \circledast \left(\frac{12}{10} \circledast 1\right) = \frac{9}{10} \circledast 1 = 0$$

oraz

$$\left(\frac{9}{10} \circledast \frac{12}{10}\right) \circledast 1 = 1 \circledast 1 = 1.$$

Zatem działanie $\circledast$ nie jest łączne w zbiorze V.

Podsumowanie

W rozdziale przedstawiono wybrane zagadnienia dotyczące zaokrąglania liczb, które mogą być rozwiązywane za pomocą narzędzi informatycznych i matematycznych. Pokazano związki między zaokrągleniami liczb a rachunkiem prawdopodobieństwa, algebrą i elementarną teorią liczb. Materiał przedstawiony w rozdziale może być punktem wyjścia do badania bardziej skomplikowanych (pod względem rachunkowym) modyfikacji tych zagadnień.

Bibliografia

Narkiewicz, W. (1997). Teoria liczb. Państwowe Wydawnictwo Naukowe, Warszawa.

Sierpiński, W. (1964). Elementary theory of numbers. Państwowe Wydawnictwo Naukowe, Warszawa.

Sierpiński, W. (1987). Wstęp do teorii liczb. Wydawnictwa Szkolne i Pedagogiczne, Warszawa.

Rozdział 4

O WŁASNOŚCIACH PIERŚCIENI Z GRADACJAMI WZGLĘDEM PÓŁGRUP

Marek Kępczyk*

Streszczenie Naszym głównym celem jest zebranie, uporządkowanie oraz uzupełnienie znanych wyników dotyczących pierścieni z różnego typu S-gradacjami, gdzie S jest półgrupą. Skupimy się głównie na klasach pierścieni, które są bezpośrednimi uogólnieniami klasy pierścieni nilpotentnych. Przedstawimy własności pierścieni T-nilpotentnych oraz radykalnych w sensie radykału pierwszego, tzw. pierścieni β-radykalnych. Na tej podstawie wykażemy, że są to klasy zamknięte na gradacje względem skończonych 2-grup. Analogiczny fakt udowodniony był wcześniej dla klasy PI-pierścieni. Podamy opisy wszystkich półgrup S, dla których klasa PI-pierścieni jest zamknięta względem coraz ogólniejszych typów S-gradacji. Przedstawimy też trudności, które stoją na przeszkodzie do uzyskania analogicznych charakteryzacji dla obydwu pozostałych klas pierścieni.

Słowa kluczowe: półgrupy, kraty, pierścienie z gradacją, radykały

Wprowadzenie

W zrozumieniu zagadnień poruszanych w tym rozdziale monografii wystarczy znajomość podstawowych faktów z Teorii Pierścieni Nieprzemiennych, które można znaleźć na przykład w Lam (1991).

Historycznie bardzo ważna motywacja do badań i wyników, które przedstawimy, dotyczących pierścieni, pochodzi z teorii grup. Mianowicie w latach 50. ubiegłego wieku zajmowano się intensywnie grupami, które są iloczynami dwóch podgrup właściwych. Niech G będzie grupą A, B jej podgrupami. Załóżmy, że dla każdego $g \in G$ istnieją takie $a \in A$ oraz $b \in B$, że $g = ab$. Zapisujemy to krótko $G = A \cdot B$. Ito (1955) pokazał, że jeżeli A i B są grupami abelowymi, to G jest grupą metaabelową. Kegel oraz Wielandt (1958, 1961) pokazali, że jeżeli A i B są skończonymi grupami nilpotentnymi, to G jest grupą rozwiązalną.

* Wydział Informatyki, Politechnika Białostocka, Wiejska 45A, 15-351 Białystok, m.kepczyk@pb.edu.pl

DOI 10.24427/978-83-67185-18-9_4

Kegel przeniósł powyższą tematykę na grunt teorii pierścieni w następujący sposób. Niech R będzie pierścieniem łącznym oraz R_1, R_2 jego podpierścieniami. Załóżmy, że dla każdego $r \in R$ istnieją takie $r_1 \in R_1$ oraz $r_2 \in R_2$, że $r = r_1 + r_2$. Zapisujemy to krótko $R = R_1 + R_2$. Kegel również wykazał w Kegel (1962/63), że jeżeli R_1 oraz R_2 są nilpotentne (tzn. spełniają tożsamości postaci $x_1x_2\cdots x_m = 0$), to R również. W Bahturin i Giambruno (1994) udowodniono, że jeżeli R_1 oraz R_2 są przemienne, to R spełnia tożsamość $[x_1, x_2][x_3, x_4] = 0$, gdzie $[a, b] = ab - ba$. W Kępczyk i Puczyłowski (2001) pokazano, że jeżeli R_1 oraz R_2 są nil-pierścieniami ograniczonego indeksu (tzn. spełniają tożsamość postaci $x^n = 0$), to R jest pierścieniem nil ograniczonego indeksu. Okazało się (Ferrero i Puczyłowski (1989)), że sławny w teorii pierścieni, ciągle otwarty Problem Koethe ma pozytywne rozwiązanie wtedy i tylko wtedy, gdy prawdziwa jest następująca implikacja: jeżeli R_1 jest pierścieniem nilpotentnym R_2 jest nil-pierścieniem, to R jest nil-pierścieniem (tzn. dla każdego $x \in R$ istnieje liczba naturalna n taka, że $x^n = 0$).

Wyniki te dały początek wielu badań koncentrujących się głównie na dwóch obszarach. Wiele prac dotyczyło po pierwsze pierścieni, które są sumami dwóch podpierścieni w kontekście radykałów (np. Ferrero i Puczyłowski (1989); Kępczyk i Puczyłowski (1996)) oraz po drugie tożsamości wielomianowych (np. Beidar i Mikhalev (1995), Felzenszwalb, Giambruno i Leal (2003), Kępczyk (2015), Kępczyk (2016)). Beidar i Mikhalev, zainspirowani wynikami częściowymi, postawili w Beidar i Mikhalev (1995) następujący problem. Przypuśćmy, że R_1 oraz R_2 spełniają tożsamości wielomianowe (krótko, są *PI*- pierścieniami), czy wtedy również R jest *PI*- pierścieniem? Całościową pozytywną odpowiedź podano w Kępczyk (2017). Przeniesienie wspomnianych wyników do ogólniejszego przypadku większej liczby podpierścieni ograniczyło się, jak do tej pory wedle naszej wiedzy, do następującego stwierdzenia, które ze względu na pewne tematyczne podobieństwo do niektórych wyników z rozdziałów 4.4 oraz 4.5, dla kompletności przedstawimy z dowodem:

Stwierdzenie 4.0.1. (Kępczyk, 2020, Stwierdzenie 4.3) Niech R_1, R_2, R_3 będą podpierścieniami pierścienia R takimi, że $R = R_1 + R_2 + R_3$. Jeżeli R_1, R_2 oraz R_3 są podpierścieniami z zerowym mnożeniem, to R jest pierścieniem nilpotentnym.

Dowód. Rozważmy następujący prawostronny ideał $P = R_1 + R_1R$ pierścienia R. Na podstawie modularności kraty podgrup addytywnych pierścienia R dostajemy $P = R_1 + (R_2 + R_3) \cap P$. Oczywiście $R_1 <_r P$, bo $R_1P = \{0\}$. Standardowy fakt dotyczący pierścieni nilpotentnych mówiący, że jednostronny ideał nilpotentny generuje dwustronny ideał nilpotentny, implikuje że ideał $H \lhd P$ generowany przez R_1 jest nilpotentny. Ponadto $P = H + (R_2 + R_3) \cap P$. Pokażemy, że $((R_2 + R_3) \cap P)^5 = \{0\}$.

Niech $a_i = b_i + c_i \in (R_2 + R_3) \cap P$, gdzie $b_i \in R_2$, $c_i \in R_3$ oraz $a_i \in P$ dla $i = 1, 2, 3, 4, 5$. Ponieważ $R_1P = \{0\}$, więc:

$$rb_i = -rc_i \text{ dla dowolnego } r \in R_1. \tag{4.0.1}$$

Ponadto $R_2^2 = R_3^2 = \{0\}$, więc $a_1a_2a_3a_4a_5 = b_1c_2b_3c_4b_5 + c_1b_2c_3b_4c_5$. Zauważmy, że $c_2b_3 = t + x + y$, gdzie $t \in R_1$, $x \in R_2$ oraz $y \in R_3$. Na podstawie (4.0.1) mamy $tc_4 = -tb_4$, więc $b_1c_2b_3c_4b_5 = b_1(t+x+y)c_4b_5 = b_1tc_4b_5 = -b_1tb_4b_5 \in b_1tR_2^2 = = \{0\}$. Podobnie pokazujemy, że $c_1b_2c_3b_4c_5 = 0$. Wobec tego $a_1a_2a_3a_4a_5 = 0$ i stąd $((R_2 + R_3) \cap P)^5 = \{0\}$.

Ponieważ $((R_2 + R_3) \cap P)^5 = \{0\}$ oraz $P/H = (((R_2 + R_3) \cap P) + H)/H$, P jest nilpotentny. Dodatkowo ideał $J \lhd R$ generowany przez P jest nilpotentny. Ponadto $R/J = (R_2 + J)/J + (R_3 + J)/J$. Teraz do R/J wystarczy zastosować twierdzenie Kegela (z Kegel (1962/63)), z którego wynika, że R/J jest pierścieniem nilpotentnym. W konsekwencji R jest również nilpotentny, co kończy dowód. □

Wyjaśnienie braku innych podobnych rezultatów wynika z twierdzenia Bokutia z Bokut (1976), który wykazał, że dowolną algebrę nad ciałem można włożyć w algebrę prostą, która jest sumą trzech podalgebr nilpotentnych indeksu nilpotentności trzy. Zatem algebra tego typu może mieć właściwie dowolnie zadane własności, co pokazuje, że przypadki sum dwóch i więcej niż dwóch podpierścieni są zdecydowanie odmienne. Ponadto w tej ogólniejszej sytuacji nie można spodziewać się żadnych prawidłowości bez dodatkowych założeń dotyczących mnożenia.

Niektóre ważne konstrukcje w teorii pierścieni opierają się na sumach ich podgrup addytywnych ze ściśle określonymi warunkami dotyczącymi mnożenia. Są to pierścienie z różnego typu gradacjami. W pracy zajmiemy się przedstawieniem wyników odnoszących się do zagadnień opisanych wyżej (dla dwóch podpierścieni) dla szeregu coraz ogólniejszych rodzajów gradacji. Dokładniej, zajmiemy się sumami półkratowymi, S- gradacjami oraz S-sumami pierścieni, gdzie S jest półgrupą. Skoncentrujemy się na przedstawieniu, uporządkowaniu i rozwinięciu wyników z Janeski i Weissglass (1973); Kelarev (1993); Kelarev i McConnell (1995); Teply, Turman i Quesada (1980); Weissglass (1973), głównie w odniesieniu do klas pierścieni β radykalnych, T-nilpotentnych oraz PI-pierścieni. Własności, potrzebne fakty i nowe wyniki dotyczące klasy β-radykalnych i pierścieni T-nilpotentnych zaprezentujemy w dwóch pierwszych rozdziałach. W trzecim rozdziale przedstawimy wyniki związane z sumami półkratowymi, głównie w odniesieniu do znanych klas radykalnych. W kolejnych dwóch rozdziałach zajmiemy się sumami półgrupowymi oraz S-sumami, odpowiednio. Główne rezultaty tam przedstawione dotyczyć będą klasy PI-pierścieni. W przypadku pozostałych klas, wyniki jakie uzyskaliśmy, doprowadzają do kilku otwartych problemów, które przedstawimy. Większość znanych wyników, których będziemy potrzebować dla kompletności oraz wygody czytelnika, przedstawimy z dowodami.

Wszystkie pierścienie rozważane w pracy są pierścieniami łącznymi. Oznaczając przez I ideał, ideał lewostronny lub ideał prawostronny pierścienia A, piszemy $I \lhd A$, $I <_l$ lub $I <_r A$, odpowiednio. Przez $\mathbb{N}$ oznaczamy zbiór liczb naturalnych. Niech R będzie pierścieniem oraz $S \subseteq R$. Wtedy $r_R(S) = \{x \in R \,|\, Sx = \{0\}\}$ oraz $l_R(S) = \{x \in \in R \,|\, xS = \{0\}\}$.

Niech A będzie pierścieniem. Przez A^n, gdzie n jest liczbą naturalną, oznaczamy podpierścień pierścienia A generowany przez produkty postaci $x_1x_2\cdots x_n$ elementów z A. Pierścień A nazywa się nilpotentnym jeżeli $A^n = 0$ dla pewnego $n \geq 1$. Klasę wszystkich pierścieni nilpotentnych oznaczamy przez $\mathscr{N}$. Powiemy, że pierścień A jest lokalnie nilpotentny, jeżeli każdy jego skończony podzbiór generuje podpierścień nilpotentny w A. Klasę wszystkich pierścieni lokalnie nilpotentnych oznaczamy przez $\mathscr{L}$. Jeżeli ideał I jest złożony z elementów nilpotentnych nazywamy go nil ideałem. Nil radykałem pierścienia A nazywamy sumę wszystkich nil ideałów pierścienia A i oznaczamy przez $\mathscr{K}(A)$. Klasę wszystkich nil-pierścieni oznaczamy przez $\mathscr{K}$. Wiadomo, że $\mathscr{N} \subsetneq \mathscr{L} \subsetneq \mathscr{K}$.

4.1 Pierścienie β-radykalne

Rozpoczniemy ten paragraf przedstawiając definicję radykału pierwszego β. Posłużymy się konstrukcją Baera. Oznaczmy przez $W(A)$ sumę nilpotentnych ideałów pierścienia A. Możemy zdefiniować teraz następujący łańcuch ideałów $W_\alpha(A)$ pierścienia A dla dowolnej liczby porządkowej α:

(1) $W_0(A) = 0$.
(2) Załóżmy, że $\alpha > 0$ i $W_\gamma(A)$ określone zostało dla $\gamma < \alpha$. Wtedy:

   (a) $W_\alpha(A) = \bigcup_{\gamma<\alpha} W_\gamma(A)$, jeżeli α jest liczbą graniczną.
   (b) $W_\alpha(A)$ jest takim ideałem A, że $W_\alpha(A)/W_{\alpha-1}(A) = W(A/W_{\alpha-1}(A))$, jeżeli α nie jest liczbą graniczną.

Radykał pierwszy pierścienia A określamy następująco:

$$\beta(A) = \bigcup_{\alpha\geq 0} W_\alpha(A). \tag{4.1.1}$$

Przez β oznaczamy klasę wszystkich pierścieni A takich, że $\beta(A) = A$. Klasę β nazywamy radykałem pierwszym lub β-radykałem. Pierścień $A \in \beta$ nazywamy pierścieniem β-radykalnym, natomiast $A/\beta(A)$ pierścieniem półpierwszym. Powiemy, że pierścień R jest sumą podprostą pierścieni R_t, gdzie $t \in T$ wtedy i tylko wtedy, gdy R zawiera takie ideały I_t, że $\bigcap I_t = \{0\}$ oraz $R_t \simeq R/I_t$. Wiadomo, że każdy pierścień półpierwszy jest sumą podprostą pierścieni pierwszych. Zatem $A \notin \beta$ wtedy i tylko wtedy, gdy istnieje właściwy ideał I pierścienia A taki, że A/I jest pierścieniem pierwszym.

Łatwo pokazać, że β-radykał jest dziedziczny na podpierścienie, tzn. dowolny podpierścień pierścienia β-radykalnego jest również β-radykalny. Ponadto radykał β jest prawostronnie silny tzn., jeżeli $I <_r R$ i $I \in \beta$, to $I + RI \in \beta$, czyli $I \subseteq \beta(R)$.

Niech R będzie pierścieniem, T dowolnym zbiorem indeksów takim, że $I_t \lhd R$ oraz $I_t \in \beta$, gdzie $t \in T$. Wtedy oczywiście $\sum_{t\in T} I_t \in \beta$.

Zauważmy, że dla liczby porządkowej α, to $a \in W_\alpha(A)$ wtedy i tylko wtedy, gdy aA jest nilpotentny modulo $W_\gamma(A)$ dla pewnego $\gamma < \alpha$. Pokażemy, że jeżeli $I \lhd A$, to $W_\alpha(I) \subseteq W_\alpha(A)$. Oczywiście $W_0(I) = W_0(A)$. Załóżmy, że $i \in W_\alpha(I)$, $\alpha > 0$ oraz $W_\beta(I) \subseteq W_\beta(A)$ dla dowolnego $\beta < \alpha$. Stąd $(iA)^{2n} = (iAiA)^n \subseteq (iI)^n \subseteq W_\gamma(I) \subseteq \subseteq W_\gamma(A)$ dla pewnej liczby naturalnej n i liczby porządkowej $\gamma < \alpha$. Zatem nasza teza wynika na podstawie indukcji pozaskończonej.

Teraz wykażemy, że jeżeli $I <_r A$ i $I \subseteq W_\alpha(A)$, to $I = W_\alpha(I)$. Jeszcze raz zastosujemy indukcję względem liczby porządkowej α. Dla $\alpha = 0$ teza jest oczywista. Załóżmy, że $\alpha > 0$ i teza zachodzi dla dowolnego $\gamma < \alpha$. Wystarczy teraz pokazać, że $I \subseteq W_\alpha(I)$. Weźmy $i \in I$. Ponieważ $i \in W_\alpha(A)$, otrzymujemy $(iI)^n \subseteq W_\gamma(A)$ dla pewnej liczby naturalnej n i liczby porządkowej $\gamma < \alpha$. Wykorzystując założenie indukcyjne dostajemy $(iI)^n = W_\gamma((iI)^n)$. Ale $(iI)^n \lhd iI$, więc $W_\gamma((iI)^n) \subseteq W_\gamma(iI)$. Zatem $(iI)^n \subseteq W_\gamma(iI)$.

Udowodniliśmy następujący

Lemat 4.1. (por.(Chebotar, Lee i Puczyłowski, 2010, Stwierdzenie 1) Niech A będzie pierścieniem oraz α będzie liczbą porządkową.

(1) Jeżeli $I \lhd A$, to $W_\alpha(I) \subseteq W_\alpha(A)$.
(2) Jeżeli $I <_r A$ oraz $I \subseteq W_\alpha(A)$, to $I = W_\alpha(I)$.

Przyjmijmy w dalszych rozważaniach tego rozdziału następującą konwencję: piszemy $A^0 \subseteq W_\alpha(A)$ wtedy i tylko wtedy, gdy A jest nilpotentny modulo $W_\gamma(A)$ dla pewnej liczby porządkowej $\gamma < \alpha$.

Lemat 4.2. (Kępczyk, 2020, Lemat 2.2.) Jeżeli A jest pierścieniem oraz $A^n \subseteq W_\alpha(A)$ dla pewnej liczby naturalnej n i liczby porządkowej α, to $(bA)^{n-1} \subseteq W_\alpha(bA)$ dla każdego $b \in A$.

Dowód. Niech $b \in A$ oraz załóżmy, że $n = 1$. W konsekwencji $A = W_\alpha(A)$, więc bA jest nilpotentny modulo $W_\gamma(A)$ dla pewnej liczby porządkowej $\gamma < \alpha$. Zatem $(bA)^k \subseteq W_\gamma(A)$ dla pewnego $k \in \mathbb{N}$. Stąd na mocy Lematu 4.1 mamy, że $(bA)^k = = W_\gamma((bA)^k) \subseteq W_\gamma(bA)$ i wobec tego $(bA)^{n-1} = (bA)^0 \subseteq W_\alpha(bA)$.

Załóżmy teraz, że $n > 1$, czyli $2(n-1) \geq n$. Zatem $(bA)^{n-1} \subseteq (A^2)^{n-1} \subseteq A^n \subseteq \subseteq W_\alpha(A)$. Stąd na mocy Lematu 4.1 mamy, że $(bA)^{n-1} = W_\alpha((bA)^{n-1}) \subseteq W_\alpha(bA)$. □

Przykład 4.1. Niech F będzie ciałem, $F[x]$ pierścieniem wielomianów zmiennej x nad F oraz (x^i) ideałem w $F[x]$ generowanym przez x^i, gdzie $i \in \mathbb{N}$. Połóżmy $R_i = = xF[x]/(x^i)$. Rozważmy następującą sumę prostą pierścieni R_i:

$$R = \bigoplus_{i\in\mathbb{N}} R_i. \tag{4.1.2}$$

Zauważmy, że $W(R) = R$, ale R nie jest pierścieniem nilpotentnym, czyli $\mathscr{N} \subsetneq \beta$.

Daje się również wykazać, że $\beta \subsetneq \mathscr{L}$. W dalszej części tego rozdziału będziemy wykorzystywać specjalnie dobrany porządek częściowy.

Przypomnimy teraz definicję porządku częściowego i kilka potrzebnych dalej pojęć z nim związanych.

Definicja 4.1. Porządkiem częściowym zbioru X nazywamy relację $\preceq$, która jest zwrotna, antysymetryczna i przechodnia, tzn.

1. $\forall_{x\in X}\ x \preceq x$,
2. $\forall_{x,y\in X}\ (x \preceq y \wedge y \preceq x) \Longrightarrow (x = y)$,
3. $\forall_{x,yz\in X}\ (x \preceq y \wedge y \preceq z) \Longrightarrow (x \preceq y)$.

Porządek częściowy $\preceq$ zbioru X nazywamy liniowym, jeżeli spełnia następujący warunek:

$$\forall_{x,y\in X}\ (x \preceq y) \vee (y \preceq x).$$

Podzbiór Y zbioru X uporządkowanego przez pewien porządek częściowy $\leqslant$ nazywamy łańcuchem jeżeli Y jest uporządkowany liniowo przez $\leqslant$. Podzbiór $Z \subseteq X$, w którym żadne dwa elementy nie są porównywalne nazywamy antyłańcuchem.

Definicja 4.2. Element $x \in X$ nazywamy elementem maksymalnym w zbiorze $(X, \leqslant)$ wtedy i tylko wtedy, gdy dla dowolnego $y \in X$, $y \leqslant x$ lub zbiór $\{x, y\}$ jest antyłańcuchem w X.

Zauważmy, że jeżeli $A \in \beta$, to istnieje taka liczba naturalna $n > 1$ i liczba porządkowa α, że $A^n \subseteq W_\alpha(A)$. Zbiór par (α, n), gdzie α jest liczbą porządkową oraz n jest liczbą naturalną, można uporządkować liniowo w następujący sposób:

$$(\gamma, m) \preceq (\alpha, n) \iff \gamma \leq \alpha \vee (\alpha = \gamma \wedge m \leq n).$$

Jeżeli $(\gamma, m) \preceq (\alpha, n)$ oraz $(\gamma, m) \neq (\alpha, n)$ piszemy $(\gamma, m) \prec (\alpha, n)$. Zatem dla dowolnego $A \in \beta$ istnieje minimalna para (α, n) taka, że $A^n \subseteq W_\alpha(A)$. Tak dobraną parę (α, n) będziemy nazywać β-indeksem pierścienia A.

Jesteśmy przygotowani, żeby przedstawić przydatny później wynik, którego dowód w Kępczyk (2020) zawiera lukę. Podamy teraz pełny dowód tego twierdzenia.

Twierdzenie 4.1. (por.(Kępczyk, 2020, Stwierdzenie 2.4)) Niech R_1 będzie podpierścieniem, a R_2 będzie podgrupą grupy addytywnej pierścienia R oraz $R = R_1 + R_2$. Jeżeli $R_1 \in \beta$ oraz $R_2^2 \subseteq R_1$, to $R \in \beta$.

Dowód. Zauważmy, że dowolny obraz homomorficzny pierścienia R spełnia założenia twierdzenia. Jeżeli zatem $R \neq 0$ oraz $R \notin \beta$, możemy założyć, że R jest pierścieniem pierwszym.

Rozważmy:

$$T = R_2 + R_2^3 + R_2^5 + \cdots .$$

Ponieważ $T^2 \subseteq R_1$ możemy dodatkowo założyć, że $T = R_2$. Dalej dowód przeprowadzimy przez indukcję względem β-indeksu $i = (\alpha, n)$ pierścienia R_1. Dla $i = (0,1)$ mamy $R_1 = 0$, co prowadzi do sprzeczności, gdyż wtedy $R = R_2$ i $R_2^2 = 0$. Zatem załóżmy, że $(0,1) \prec (\alpha, n)$ i teza naszego twierdzenia zachodzi dla każdego $(\gamma, m) \prec (\alpha, n)$. Stosując Lemat 4.2, dla dowolnego $b \in R_2^2$, bR_1 ma β-indeks $j \prec (\alpha, n)$. Rozważmy $bR = bR_1 + bR_2$. Ponieważ $(bR_2)^2 \subseteq bR_2^4 \subseteq bR_1$, stosując założenie indukcyjne dostajemy $bR \in \beta$. Zatem $bR \subseteq \beta(R) = 0$, skąd $bR = 0$. Ponieważ R jest pierścieniem pierwszym, to $b = 0$. Zatem $R_2^2 = 0$. Niech $l_{R_2}(R_2) = \{x \in R_2 \,|\, xR_2 = 0\}$. Możemy zastosować teraz (Kępczyk i Puczyłowski, 1996, Twierdzenie 1), z którego wynika, że $l_{R_2}(R_2) \subseteq \beta(R)$. Zatem $R_2 = l_{R_2}(R_2) \subseteq \beta(R) = 0$, więc $R = R_1 \in \beta$, co daje sprzeczność i kończy dowód. □

4.2 Pierścienie T-nilpotentne

W rozdziale tym zajmiemy się kolejnym uogólnieniem nilpotentności.

Definicja 4.3. Powiemy, że pierścień R jest lewostronnie T-nilpotentny wtedy i tylko wtedy, gdy dowolny niezerowy obraz homomorficzny pierścienia R ma niezerowy lewostronny anihilator.

Pierścienie prawostronnie T-nilpotentne definiuje się analogicznie. Łatwo pokazać, że nie są to pojęcia symetryczne, tzn. można wskazać przykłady pierścieni T–nilpotentnych z lewej strony, które nie są T-nilpotentne z prawej. Oczywiście każdy pierścień nilpotentny jest prawostronnie i lewostronnie T-nilpotentny. W dalszych rozważaniach skupimy się na pierścieniach lewostronnie T-nilpotentnych, ale przedstawiane dalej wyniki odnoszące się do tej klasy mają swoją oczywistą dualną prawostronną wersję.

Z pojęciem T-nilpotentności ściśle wiąże się pojęcie hiperanihilatora. Niech A będzie pierścieniem. Powiemy, że $l(A)$ jest lewostronnym hiperanihilatorem pierścienia A wtedy i tylko wtedy, gdy $l(A) = \bigcup_{\alpha \geq 0} l_\alpha(A)$, gdzie:

$$l_0(A) = 0,$$

oraz dla liczby porządkowej $\alpha \geq 1$,

$$l_\alpha(A) = \Big\{ x \in A \,|\, xA \subseteq \bigcup_{\beta < \alpha} l_\beta(A) \Big\}. \tag{4.2.1}$$

Łatwo można pokazać, że pierścień A jest lewostronnie T-nilpotentny wtedy i tylko wtedy, gdy $l(A) = A$. Dodatkowo wykorzystując powyższą definicję hiperanihilatora $l(A)$ i konstrukcję (4.1.1) radykału $\beta(A)$, otrzymujemy stąd, że je-

żeli $l(A) = A$, to $\beta(A) = A$. Istotnie, $l_1(A) = l_A(A) \lhd A$, czyli $l_1(A)^2 = 0$, więc $l_1(A) \subseteq\subseteq W_1(A)$. Analogicznie, stosując dowód indukcyjny, można pokazać, że $l_\alpha(A) \subseteq W_\alpha(A)$ dla dowolnej liczbny porządkowej α. Oczywiście $l_\alpha(A) \lhd A$ dla dowolnego α. Stąd $l(A) \subseteq \beta(A)$ i ponieważ $A = l(A)$, więc $\beta(A) = A$.

Rozważmy następujący warunek:

(p) Dla dowolnego ciągu $(a_1, a_2, \ldots)$ istnieje taki podciąg $(a_{i_1}, a_{i_2}, \ldots)$, że iloczyn $a_{i_1} a_{i_2} \cdot \cdots \cdot a_{i_n} = 0$ dla pewnej liczby naturalnej n. (4.2.2)

Pokażemy, wykorzystując wyniki z Gardner (1992), że (p) jest warunkiem równoważnym z lewostronną T- nilpotentnością. Potrzebować będziemy pewnych modyfikacji dwóch znanych faktów dotyczących skończonych pokryć grup i pierścieni (por. (Lanski, 1990, Lemat)) oraz (Lanski, 1990, Twierdzenie), których dowody przedstawimy dla kompletności. Ideę dowodu pierwszego z nich zaczerpnęliśmy z (Neumann, 1954, Lemat (4.1)).

Lemat 4.3. (por. (Neumann, 1954, Lemat (4.1)) Niech grupa G będzie sumą mnogościową skończonej liczby warstw względem podgrup $C_1, C_2, \ldots, C_n$:

$$G = \bigcup_{i=1}^{n} C_i g_i. \tag{4.2.3}$$

Wtedy pewna podgrupa C_i ma skończony indeks w G. Ponadto, jeżli $C_1, \ldots, C_k$ są wszystkimi podgrupami skończonego indeksu w grupie G wśród podgrup $C_1, \ldots, C_n$, to $G = \bigcup_{i=1}^{k} C_i g_i$.

Dowód. Przeprowadzimy dowód ze względu na liczbę r różnych elementów w zbiorze $C = \{C_1, C_2, \ldots, C_n\}$. Jeżeli $r = 1$ teza jest oczywista. Załóżmy, że $r > 1$ i teza zachodzi, gdy liczba różnych podgrup w pokryciu (4.2.3) jest mniejsza niż r. Możemy tak przenumerować elementy zbioru C, że $C_n = C_{n-1} = \cdots = C_{l+1}$ i w zbiorze $\{C_1, C_2, \ldots, C_l\}$ podgrupa C_n nie występuje. Rozważmy:

$$H = \bigcup_{i=l+1}^{n} C_n g_i. \tag{4.2.4}$$

Jeżli $H = G$, to C_n jest podgrupą skończonego indeksu w grupie G i teza zachodzi. Załóżmy, że dla pewnego $h \in G$ mamy, że $h \notin H$. Wtedy $C_n h \cap C_n g_i = \emptyset$ dla każdego $i = l+1, \ldots, n$. Zatem ze wzoru (4.2.3),

$$C_n h \subseteq \bigcup_{i=1}^{l} C_i g_i. \tag{4.2.5}$$

Stąd dla każdego $j = l+1,\ldots,n$ mamy, że $C_n g_j \subseteq \bigcup_{i=1}^{l} C_i g_i h^{-1} g_j$. Wobec tego:

$$G = \bigcup_{i=1}^{l} C_i g_i \cup \bigcup_{j=l+1}^{n} \bigcup_{i=1}^{l} C_i g_i h^{-1} g_j$$

i na mocy założenia indukcyjnego dla pewnego $i = 1,\ldots,l$ podgrupa C_i ma skończony indeks w grupie G.

Niech teraz $C_1,\ldots,C_k$ będą wszystkimi wśród podgrup $C_1,\ldots,C_n$ podgrupami skończonego indeksu w grupie G. Wtedy $D = C_1 \cap \ldots \cap C_k$ też jest podgrupą skończonego indeksu w grupie G. Załóżmy, że $G \neq \bigcup_{i=1}^{k} C_i g_i$. Wtedy istnieje $h \in G$ takie, że $h \notin \bigcup_{i=1}^{k} C_i g_i$. Ponadto D jest podgrupą skończonego indeksu w grupie C_i dla każdego $i = 1,\ldots,k$, więc istnieją $x_1,\ldots,x_t \in G$, gdzie $t \in \mathbb{N}$, takie, że $\bigcup_{i=1}^{k} C_i g_i = \bigcup_{j=1}^{t} D x_j$. Stąd $Dh \cap Dx_j = \emptyset$ dla każdego $j = 1,\ldots,t$, więc ze wzoru (4.2.3), $Dh \subseteq \bigcup_{i=k+1}^{n} C_i g_i$, skąd $Dx_j \subseteq \bigcup_{i=k+1}^{n} C_i g_i h^{-1} x_j$. To oznacza, że grupa G jest skończoną sumą pewnych warstw względem podgrup $C_{l+1},\ldots,C_n$, z których każda ma nieskończony indeks w grupie G. Ale to przeczy pierwszej części naszego lematu. Wobec tego $G = \bigcup_{i=1}^{k} C_i g_i$. □

Ponieważ ideały (ideały lewostronne lub prawostronne) dowolnego pierścienia są podgrupami jego grupy addytywnej, to Lemat 4.3 oraz powyższy wniosek można zastosować również w przypadku ideałów pierścieni. Dokładniej, jeżeli pierścień R jest skończoną sumą mnogościową ideałów, to przecięcie tych ideałów jest podgrupą skończonego indeksu w grupie $(R,+)$.

Lemat 4.4. (por. (Lanski, 1990, Twierdzenie) Niech R będzie nil-pierścieniem oraz $B_1,\ldots,B_n$ jego niepustymi podzbiorami takimi, że $B_i \neq \{0\}$ dla każdego $i = 1,\ldots,n$. Jeżeli $R = \bigcup_{i=1}^{n} r_R(B_i)$, to $l_R(R) \neq \{0\}$.

Dowód. Na podstawie Lematu 4.2.5 możemy bez zmniejszania ogólności zakładać, że każda z podgrup $r_R(B_i)$ ma skończony indeks w grupie $(R,+)$. Stąd $D = \bigcap_{i=1}^{n} r_R(B_i)$ też ma skończony indeks w grupie $(R,+)$. Ponadto $D <_r R$, bo $r_R(B_i) <_r R$ dla każdego $i = 1,\ldots,n$. Zatem grupa $(R/D,+)$ jest skończona i w konsekwencji tego pierścień $End(R/I,+)$ jej endomorfizmów jest skończony. Weźmy dowolne

$a, x \in R$ i niech $(x+D)F(a) = xa+D$. Standardowe sprawdzenie pokazuje, że $F(a)$ jest dobrze określoną funkcją ze zbioru R/D w siebie, a nawet $F(a) \in End(R/D,+)$. Ponadto F jest homomorfizmem pierścienia R w pierścień $End(R/D,+)$ o jądrze $I = KerF = \{a \in R \mid xa \in D \text{ dla każdego } x \in R\}$. Stąd $RI \subseteq D$ oraz pierścień R/I jest skończony. Dodatkowo R/I jest nil-pierścieniem, więc $(R/I)^m = 0$ dla pewnego $m \in \mathbb{N}$, czyli $R^m \subseteq I$ i w konsekwencji $R^{m+1} \subseteq D$. W szczególności $B_1R^{m+1} = 0$. Istnieje zatem najmniejsza liczba naturalna k taka, że $B_1R^k = 0$. Jeżli $k = 1$, to $\{0\} \neq B_1 \subseteq l_R(R)$, skąd $l_R(R) \neq \{0\}$, a jeżeli $k > 1$, to $\{0\} \neq B_1R^{k-1} \subseteq l_R(R)$, więc też $l_R(R) \neq \{0\}$. □

Przedstawimy teraz zapowiadaną wcześniej charakteryzację pierścieni lewostronnie T-nilpotentnych.

Twierdzenie 4.2.1. **(**Gardner, 1992, Twierdzenie 1) Pierścień R jest lewostronnie T-nilpotentny wtedy i tylko wtedy, gdy elementy pierścienia R spełniają warunek (p).

Dowód. Niech S będzie dowolnym niezerowym obrazem homomorficznym pierścienia R spełniającego warunek (p). Wówczas warunek (p) jest spełniony w S. Oczywiście S jest nil-pierścieniem. Przypuśćmy, że $l_S(S) = 0$. Wtedy na mocy Lematu 4.4 dla dowolnego $n \in \mathbb{N}$ i dla dowolnych niezerowych $x_1, \ldots, x_n \in S$ mamy, że $S \neq \bigcup_{i=1}^{n} r_S(\{x_i\})$. Niech a_1 będzie dowolnym niezerowym elementem pierścienia S. Ponieważ $S \neq r_S(\{a_1\})$, więc istnieje $a_2 \in S$ takie, że $a_1a_2 \neq 0$. Przypuśćmy, że dla pewnej liczby naturalnej $n \geq 2$ skonstruowaliśmy już niezerowe elementy $a_1, a_2, \ldots, a_n$ pierścienia S takie, że dla każdego $k \leq n$ i dla dowolnych liczb naturalnych $i_1 < i_2 < \ldots < i_k \leq n$ mamy, że $a_{i_1}a_{i_2}\ldots a_{i_k} \neq 0$. Wtedy zbiór X wszystkich takich iloczynów $a_{i_1}a_{i_2}\ldots a_{i_k}$ jest skończony, więc na mocy Lematu 4.4 mamy, że $S \neq \bigcup_{x \in X} r_S(\{x\})$. Zatem istnieje $a_{n+1} \in S$ takie, że $xa_{n+1} \neq 0$ dla każdego $x \in X$. Stąd dla dowolnej liczby naturalnej $k \leq n+1$ i dla dowolnych liczb naturalnych $i_1 < i_2 < \ldots < i_k \leq n+1$ mamy, że $a_{i_1}a_{i_2}\ldots a_{i_k} \neq 0$. Wobec tego przez indukcję mamy skonstruowany ciąg $(a_1, a_2, a_3, \ldots)$ elementów pierścienia S, który nie spełnia warunku (p), co prowadzi do sprzeczności. Wobec tego $l_S(S) \neq 0$ i z dowolności S wynika, że pierścień R jest lewostronnie T- nilpotentny.

Na odwrót. Załóżmy, że pierścień R jest lewostronnie T-nilpotentny i niech $(a_1, a_2, \ldots)$ będzie dowolnym ciągiem jego elementów. Przypuśćmy, że każdy element zbioru $A = \{a_1, a_1a_2, a_1a_2a_3, \ldots\}$ jest niezerowy. Ponieważ $R = l(R) = l_\alpha(R)$ dla pewnej liczby porządkowej α, więc istnieje najmniejsza liczba porządkowa $\beta \leq \alpha$ taka, że $a = a_1a_2\ldots a_n \in l_\beta(R)$ dla pewnego $n \in \mathbb{N}$. Oczywiście liczba β nie jest graniczna, więc $aR \subseteq l_{\beta-1}(R)$, skąd $aa_{n+1} \in l_{\beta-1}(R)$, co przeczy minimalności β. Wobec tego nie każdy element zbioru A jest niezerowy, a to oznacza, że $a_1a_2\ldots a_m = 0$ dla pewnego $m \in \mathbb{N}$, skąd w szczególności ciąg $(a_1, a_2, \ldots)$ spełnia warunek (p). □

Wykażemy, że analogiczna teza, jak dla β radykału w Twierdzeniu 4.1, zachodzi dla klasy pierścieni T-nilpotentnych.

Twierdzenie 4.2.2. Niech R_1 będzie podpierścieniem, a R_2 będzie podgrupą grupy addytywnej pierścienia R oraz $R = R_1 + R_2$. Jeżeli R_1 jest pierścieniem lewostronnie T-nilpotentnym oraz $R_2^2 \subseteq R_1$, to R jest pierścieniem lewostronnie T-nilpotentnym.

Dowód. Jeżli $R_1 = \{0\}$, to teza jest oczywista, bo wtedy $R = R_2$ i $R_2^2 = \{0\}$. Niech dalej $R_1 \neq \{0\}$. Rozważmy $P = R_1 + R_1R$. Oczywiście $P <_r R$ i $P = R_1 + R_1R_2$. Ponadto z modularności kraty podgrup grupy $(R,+)$ mamy, że $P = R_1 + (R_2 \cap P)$. Zatem $R = P + R_2$. Przypuśćmy, że $R_1 \not\subseteq l(P)$. Wtedy $l(P) \neq P$ i pierścień $\overline{P} = P/l(P)$ ma zerowy lewostronny anihilator. Ale $\overline{R_1} = (R_1 + l(P))/l(P) \neq 0$ i $\overline{P} = \overline{R_1} + \overline{R_1}\,\overline{R_2}$ dla $\overline{R_2} = (R_2 + \mathbb{1}(P))/l(P)$ oraz lewostronny anihilator L pierścienia $\overline{R_1}$ jest niezerowy, gdyż $\overline{R_1}$ jest niezerowym obrazem homomorficznym lewostronie T-nilpotentnego pierścienia R_1, więc stąd $L\overline{P} = \{0\}$, co prowadzi do sprzeczności. Wobec tego $R_1 \subseteq l(P)$. Dalej, $(P \cap R_2)P = (P \cap R_2)R_1 + (P \cap R_2)^2$ i $(P \cap R_2)R_1 \subseteq l(P)$, gdyż $R_1 \subseteq l(P) \lhd P$ oraz $(P \cap R_2)^2 \subseteq R_2^2 \subseteq R_1 \subseteq l(P)$, więc $(P \cap R_2)P \subseteq l(P)$, skąd $P \cap R_2 \subseteq l(P)$. Ale $P = R_1 + (P \cap R_2)$, więc $P \subseteq l(P)$, czyli $P = l(P)$.

Ponieważ $R = P + R_2$, więc $R_2P \subseteq P + R_2$, skąd $R_2PR_2 \subseteq PR_2 + R_2^2$. Ale $P <_r R$ i $R_2^2 \subseteq P$, więc mamy stąd:

$$R_2PR_2 \subseteq P. \tag{4.2.6}$$

Weźmy dowolny ciąg (a_n) elementów pierścienia R. Wtedy $a_n = x_n + y_n$, gdzie $x_n \in P$ oraz $y_n \in R_2$ dla każdego $n \in \mathbb{N}$. Weźmy dowolne $k \in \mathbb{N}$. Z dowodu Twierdzenia 4.2.1 wynika, że istnieje $m = m(k) \in \mathbb{N}$ takie, że $x_{k+1} \cdot x_{k+2} \cdot \ldots \cdot x_{k+m} = 0$. Zauważmy, że $a_k \cdot a_{k+1} \cdot \ldots \cdot a_{k+m} = x_k \cdot a_{k+1} \cdot \ldots \cdot a_{k+m} + y_k \cdot x_{k+1} \cdot \ldots \cdot x_{k+m} + x$, gdzie x jest skończoną sumą elementów postaci $y_k \cdot \ldots \cdot y \cdot \ldots$, gdzie $y \in R_2$, więc ponieważ $R_2^2 \subseteq \subseteq P <_r R$, to na mocy (4.2.6) $x \in P$ oraz $x_k \cdot a_{k+1} \cdot \ldots \cdot a_{k+m} \in P$ i $y_k \cdot x_{k+1} \cdot \ldots \cdot x_{k+m} = 0$. Wobec tego $c_k = a_k \cdot a_{k+1} \cdot \ldots \cdot a_{k+m} \in P$. Z dowolności k możemy skonstruować zatem ciąg (c_k) elementów pierścienia P i na mocy dowodu Twierdzenia 3.4 oraz konstrukcji c_k otrzymujemy stąd, że $a_1 \cdot a_2 \cdot \ldots \cdot a_n = 0$ dla pewnego $n \in \mathbb{N}$. Wobec tego na mocy Twierdzenia 4.2.1 pierścień R jest lewostronnie T-nilpotentny. □

4.3 Półkratowe sumy pierścieni

Przypomnijmy, że półgrupą nazywamy zbiór $(S,\cdot)$ dwuargumentowym multyplikatywnym działaniem łącznym $\cdot$. Element $x \in S$ taki, że $x^2 = x$ nazywamy idempotentem półgrupy $(S,\cdot)$. Natomiast półgrupę, której wszystkie elementy są idempotentami nazywamy pasem.

Definicja 4.4. Półkratą nazywamy dowolny pas przemienny.

Niech S będzie półgrupą. Przypomnijmy, że pierścień A jest pierścieniem z S–gradacją jeżeli $A = \oplus_{s \in S} A_s$ oraz $A_sA_t \subseteq A_{st}$ dla dowolnych $s, t \in S$. Ponadto dla każdego

$t \in S$, A_t jest podgrupą grupy $(A,+)$. W naszych dalszych rozważaniach zaprezentujemy ogólniejsze podejście. Niech R_s będzie podgrupą addytywną pierścienia R dla dowolnego $s \in S$. Sumę $\sum_{s\in S} R_s$ definiujemy następująco:

$$\sum_{s\in S} R_s = \{x_{s_1} + \ldots + x_{s_n} \mid x_{s_i} \in R_{s_i}, n \in \mathbb{N}\}.$$

Definicja 4.3.1. Pierścień R jest sumą półkratową podgrup addytywnych R_s pierścienia R względem półkraty S, gdzie $s \in S$ wtedy i tylko wtedy, gdy $R = \sum_{s\in S} R_s$ oraz $R_s R_t \subseteq R_{st}$ dla dowolnych $s, t \in S$.

Niech P będzie półkratą. Możemy w P określić następującą relację podzielności:

$$\forall_{x,y\in P}\, y \,|\, x \Leftrightarrow \exists_{z\in P}\, x = yz.$$

Powiemy, że element α jest zerem w P, jeżeli $\forall_{x\in P} x\alpha = \alpha$.

Pokażemy teraz, że każdy pierścień, który jest sumę półkratową można przedstawić w postaci innej sumy półkratowej dwóch podpierścieni, z których jeden jest ideałem. Niech P będzie taką półkratą, że $|P| > 1$. Weźmy niezerowy element $\alpha \in P$. Niech $Q_\alpha = \{\beta \in P : \beta \mid \alpha\}$. Oczywiście $\beta\gamma \in Q_\alpha$ implikuje $\beta \in Q_\alpha$, $\gamma \in Q_\alpha$. Z drugiej strony, jeżeli $\beta \in Q_\alpha$ oraz $\gamma \in Q_\alpha$, to istnieją $\delta, \omega \in P$ takie, że $\beta\delta = \alpha$ i $\gamma\omega = \alpha$. Stąd $(\beta\delta)(\gamma\omega) = (\beta\gamma)(\delta\omega) = \alpha^2 = \alpha$. Zatem $\beta\gamma \in Q_\alpha$. To pokazuje, że Q_α oraz $Q = P \setminus Q_\alpha$ są podpółkratami P oraz $P = Q_\alpha \cup Q$. Dodatkowo Q jest ideałem w P. Możemy również zakładać, że $\{Q_\alpha, Q\}$ jest półkratą z działaniami $Q_\alpha^2 = Q_\alpha$, $Q^2 = Q$ oraz $Q_\alpha Q = QQ_\alpha = Q$. Dowiedliśmy zatem następujący

Lemat 4.5. (por. (Janeski i Weissglass, 1973, Lemat 3)) Niech R będzie sumą półkratową $R = \sum_{\alpha\in P} R_\alpha$, gdzie $|P| > 1$. Wtedy istnieją takie rozłączne podpółkraty A i B półkraty P, że $P = A \cup B$. Ponadto:

1. $R_A = \sum_{\alpha\in A} R_\alpha$ jest sumą półkratową oraz $R_{\alpha_0} \lhd R_A$ dla pewnego $\alpha_0 \in A$.
2. $R_B = \sum_{\alpha\in A} R_\alpha$ jest sumą półkratową oraz $R_B \lhd R$.
3. $R = R_A + R_B$ jest sumą półkratową, gdzie $A^2 = A$, $B^2 = B$ oraz $AB = BA = B$.

Żeby sformułować kolejne wyniki w tym rozdziale potrzebujemy ogólnego pojęcia klasy radykalnej.

Definicja 4.3.2. Powiemy, że klasa pierścieni $\mathscr{T}$ jest klasą radykalną wtedy i tylko wtedy, gdy spełnia następujące warunki:

1. $\mathscr{T}$ jest zamknięta na obrazy homomorficzne, tzn. jeżeli $R \in \mathscr{T}$, to dla dowolnego $I \lhd R$, $R/I \in \mathscr{T}$,
2. $\mathscr{T}$ jest zamknięta na rozszerzenia, tzn. jeżeli $I \lhd R$, $I \in \mathscr{T}$ oraz $R/I \in \mathscr{T}$, to $R \in \mathscr{T}$.
3. $\mathscr{T}$ jest zamknięta na sumy ideałów, tzn. jeżeli $I_t \in \mathscr{T}$ dla dowolnego zbioru T, to $\sum_{t\in T} I_t \in \mathscr{T}$.

Klasę radykalną $\mathscr{T}$ nazywamy radykałem, natomiast $R \in \mathscr{T}$ pierścieniem $\mathscr{T}$-radykalnym. Największy $\mathscr{T}$-radykalny ideał pierścienia R nazywamy radykałem R i oznaczamy przez $\mathscr{T}(R)$. Jeżeli $\mathscr{T}(R) = 0$ pierścień R nazywamy $\mathscr{T}$-półprostym. Przykładami radykałów są klasy $\beta, \mathscr{L}, \mathscr{K}$.

Udowodnimy teraz następujące:

Stwierdzenie 4.3.3. Niech $R = \sum_{\alpha \in P} R_\alpha$ będzie sumą półkratową względem skończonej półkraty P oraz $\mathscr{T}$ jest dowolnym radykałem. Jeżeli dla dowolnego α, $R_\alpha \in \mathscr{T}$, to $R \in \mathscr{T}$.

Dowód. Zastosujemy indukcję względem $|P|$. W przypadku $|P| = 1$ teza jest oczywista. Załóżmy, że $|P| = s > 1$ i teza zachodzi dla każdej półkraty Ω, dla której $|\Omega| < s$. Z Lematu 4.5, $R = R_A + R_B$ oraz $R_B \lhd R$, gdzie R_A, R_B są sumami półkaratowymi względem półkrat A oraz B, odpowiednio. Dodatkowo A i B są rozłącznymi niezerowymi podpółkratami takimi, że $P = A \cup B$. Ponieważ $|A|, |B| < |P|$, z założenia indukcyjnego dostajemy $R_A, R_B \in \mathscr{T}$. Zatem ponieważ $R/R_B = (R_A + R_B)/R_B \approx$ $\approx R_A/R_A \cap R_B$, R/R_B jest obrazem homomorficznym pierścienia R_A. Stąd $R/R_B \in \mathscr{T}$, co w konsekwencji daje $R \in \mathscr{T}$ i kończy dowód. □

Oczywiście powyższe stwierdzenie ma zastosowanie, gdy $\mathscr{T} = \beta, \mathscr{L}, \mathscr{K}$. Łatwo również zauważyć, że Stwierdzenie 4.3.3 ma zastosowanie dla każdej klasy pierścieni $\mathscr{T}$, która jest zamknięta na obrazy homomorficzne i rozszerzenia. W szczególności zachodzi więc również dla $\mathscr{T} = \mathscr{N}$ oraz klasy pierścieni lewostronnie (prawostronnie) T-nilpotentnych.

Problem 4.3.4. Czy założenie o skończoności P w Stwierdzeniu 4.3.3 można pominąć?

Zauważmy, że nie jest to możliwe dla $\mathscr{T} = \mathscr{N}$. Niech P będzie dowolną nieskończoną półkratą oraz $M = \{e_1, e_2, \ldots\}$ dowolnym nieskończonym zbiorem jej idempotentów. Połóżmy, jak w Przykładzie 4.1, $R_{e_i} = xF[x]/(x^i)$, gdzie $e_i \in M$ oraz $R_s = 0$ dla pozostałych elementów α z P. Rozważmy sumę półkratową $R = \sum_{\alpha \in P} R_\alpha$. Oczywiście $R \notin \mathscr{N}$.

W przypadku klasy $\mathscr{L}$ odpowiedź jest pozytywna nawet gdy założymy, że P jest dowolnym pasem. Zachodzi bowiem następujące

Twierdzenie 4.3.5. (Kelarev i McConnell, 1995, Twierdzenie 2.2) Następujące warunki są równoważne:

1. dla dowolnej S-sumy $R = \sum_{\alpha \in S} R_\alpha$, jeżeli wszystkie podpierścienie spośród R_α są lokalnie nilpotentne, to pierścień R jest lokalnie nilpotentny,
2. S jest pasem.

Żeby odpowiedzieć na pytanie 4.3.4 w przypadku klasy nil-pierścieni $\mathscr{K}$ potrzebujemy pewnych przygotowań. Niech $R = \sum_{\alpha \in P} R_\alpha$ będzie sumą półkratową oraz $r \in R$.

Nośnikiem $\mathrm{Supp}_P(r)$ elementu r nazywamy następujący zbiór:

$$\mathrm{Supp}_P(r) = \left\{ \alpha \in P \,|\, r = \sum_{\alpha \in P} r_\alpha, r_\alpha \neq 0 \right\}.$$

W każdej półkracie P można w następujący sposób określić porządek częściowy:

$$\alpha \leqslant \beta \iff \alpha = \alpha\beta.$$

Oczywiście relacja $\leqslant$ jest zwrotna i antysymetryczna. Załóżmy, że $x \leqslant y$ oraz $y \leqslant z$ dla pewnych $x, y, z \in P$. Stąd $x = xy = x(yz) = (xy)z = xz$. Zatem $x \leqslant z$, co pokazuje, że $\leqslant$ jest relacją przechodnią w P. Porządek $\leqslant$ nazywa się naturalnym porządkiem półkraty P.

Przykład 4.3.6. Niech $(2^X, \cap)$ będzie półkratą wszystkich podzbiorów 2^X ustalonego zbioru X. Jeżeli $A, B \in 2^X$, to $A \leqslant B \iff A = A \cap B \iff A \subseteq B$.

Przedstawimy teraz pewne proste własności naturalnego porządku półkraty P:

a) $\forall_{a,b \in P}\ (ab \leqslant a \wedge ab \leqslant b)$,
b) $\forall_{a,b,c \in P}\ (ab \leqslant c) \Rightarrow (a \leqslant c \wedge b \leqslant c)$,
c) $\forall_{a,b,c \in P}\ (a \leqslant b) \Rightarrow (ac \leqslant bc)$.

Niech $a, b, c \in P$. Oczywiście $ab = (ab)a = (ab)b$. Stąd $ab \leqslant b$ oraz $ab \leqslant b$, co daje $a)$. Własność b) wynika wprost z $a)$. Jeżeli $a \leqslant b$, to $a = ab$. Stąd $ac = acb = ac^2b = = acbc$, co implikuje $ac \leqslant bc$.

Podamy teraz zapowiadaną odpowiedź na pytanie 4.3.4 w przypadku klasy nil-pierścieni $\mathscr{K}$.

Stwierdzenie 4.3.7. Niech R będzie sumą półkratową $R = \sum_{\alpha \in P} R_\alpha$. Jeżeli $R_\alpha \in \mathscr{K}$ dla każdego $\alpha \in P$, to $R \in \mathscr{K}$.

Dowód. Załóżmy, że R nie jest nil-pierścieniem. Wybierzmy element $x \in R$, który ma następujące własności:

1. x nie jest nilpotentny,
2. podpółkrata $\Omega = \langle \mathrm{Supp}_P(x) \rangle$ generowana przez $\mathrm{Supp}_P(x)$ w P jest minimalna.

Niech α_0 będzie elementem maksymalnym w $\mathrm{Supp}_P(x)$ względem porządku naturalnego $\leqslant$ półkraty P. Ponadto $x = a + b$, gdzie $a \in R_{\alpha_0}$ oraz $b \in \sum_{\alpha \in \mathrm{Supp}_P(x) \setminus \{\alpha_0\}} R_\alpha$. Na podstawie własności a) oraz b) łatwo zauważyć, że α_0 jest także elementem maksymalnym w Ω. Niech n będzie taką liczbą naturalną, że $a^n = 0$. Zatem $\alpha_0 \notin \mathrm{Supp}_P(x^n)$. Niech Ω' będzie podpółkratą w P generowaną przez $\mathrm{Supp}_P(x^n)$. Oczywiście $\alpha_0 \notin \Omega'$. Stąd $\Omega' \subsetneq \Omega$. Ponieważ x^n nie jest elementem nilpotentnym otrzymujemy sprzeczność z minimalnością podpółgrupy Ω. Uzyskana sprzeczność kończy dowód. □

W świetle przedstawionych wyników możemy sformułować następujący

Problem 4.3.8. Niech $R = \sum_{\alpha \in S} R_\alpha$ będzie sumą półkratową. Czy jeżeli $R_\alpha \in \beta$ dla każdego $\alpha \in S$, to $R \in \beta$?

Odpowiedź jest pozytywna w przypadku, gdy naturalny porządek $\leqslant$ półkraty P jest dodatkowo artinowski i wąski.

Definicja 4.3.9. Niech $(S, \leqslant)$ będzie zbiorem uporządkowanym.

1. $(S, \leqslant)$ jest artinowski wtedy i tylko wtedy, gdy każdy ściśle malejący ciąg elementów jest skończony.
2. $(S, \leqslant)$ jest wąski wtedy i tylko wtedy, gdy każdy antyłańcuch w S jest skończony.

Stwierdzenie 4.3.10. Niech $R = \sum_{\alpha \in S} R_\alpha$ będzie taką sumą półkratową, że naturalny porządek $(P, \leqslant)$ jest artinowski i wąski. Ponadto $\mathscr{T}$ dowolnym radykałem. Wtedy, jeżeli $R_\alpha \in \mathscr{T}$ dla każdego $\alpha \in S$, to $R \in \mathscr{T}$.

Dowód. Oczywiście możemy założyć, że $|P| > 1$. Stosując Lemat 4.5 otrzymujemy, że $R = R_A + R_B$, gdzie A oraz B są rozłącznymi podpółkratami P. Ponadto $R_B \lhd R$, $A^2 = A$ oraz $R_\alpha \lhd R_A$ dla pewnego różnego od zera $\alpha \in A$. Jeżeli B zawiera taki element β, że zbiór $\{\alpha, \beta\}$ jest antyłańcuchem, to pierścień R_B można analogicznie rozłożyć na sumę dwóch podpierścieni. Stąd $R = R_A + R_C + R_D$, gdzie R_A, R_B oraz R_D są podpierścieniami R. Ponadto $B^2 = B$ oraz $R_D \lhd R$. Opisaną konstrukcję można kontynuować względem R_D jeżeli w B istnieje element δ, że $\{\alpha, \beta, \delta\}$ tworzą antyłańcuch.

Ponieważ każdy antyłańcuch w P jest skończony, to istnieje takie $n \in \mathbb{N}$, że $R = R_{A_1} + R_{A_2} + \cdots + R_{A_n} + R_S$, gdzie R_{A_i} jest podpierścieniem R oraz $A_i^2 = A_i$ dla dowolnego $i \in \{1, 2, \ldots, n\}$. Ponadto $S \lhd P$ oraz $R_{\alpha_n} \lhd R_S$. Pierścień R_S można analogicznie rozłożyć na sumę dwóch podpierścieni względem elementu $s_1 \in S$ takiego, że $s_1 < \alpha_n$. Wtedy $R_S = R_{S_1} + R_{S_2}$. Ponieważ porządek $(P, \leqslant)$ jest artinowski, tę konstrukcję również można powtarzać skończoną liczbę razy, odpowiednio definiując kolejne elementy łańcucha $s_m < s_{m-1} < \ldots < s_1$ dla pewnego $m \in \mathbb{N}$. Zatem $R = R_{A_1} + R_{A_2} + \cdots + R_{A_n} + R_{S_1} + R_{S_2} + \cdots + R_{S_m}$. Stąd $I = R_{\alpha_1} + R_{\alpha_2} + \cdots + R_{\alpha_n} + + R_{s_1} + R_{s_2} + \cdots + R_{s_m}$ jest ideałem pierścienia R. Stosując Stwierdzenie 4.3.3 dostajemy, że $\beta(I) = I$. Zatem $I \subseteq \beta(R)$. W szczególności $R_{\alpha_1} \subseteq \beta(R)$. Ponieważ α_1 jest elementem różnym od zera wybranym dowolnie, więc otrzymujemy, że $R_\alpha \subseteq \beta(R)$ dla dowolnego różnego od zera $\alpha \in P$. Zatem $\beta(R) = R$, co należało dowieść. □

Powiemy, że radykał $\mathscr{T}$ jest dziedziczny (na ideały) jeżeli dowolny ideał pierścienia $\mathscr{T}$-radykalnego jest $\mathscr{T}$-radykalny. Przykładami radykałów dziedzicznych są β, $\mathscr{L}$ oraz $\mathscr{K}$. Zakończymy ten rozdział wykazując, że dla dowolnego radykału dziedzicznego $\mathscr{T}$ klasa $\mathscr{T}$-półprosta jest zamknięta na sumy półkratowe.

Twierdzenie 4.3.11. (por. (Teply i in., 1980, Twierdzenie 1)) Niech $R = \sum_{\alpha \in P} R_\alpha$ będzie sumą półkratową podpierścieni oraz $\mathscr{T}$ dziedzicznym radykałem. Jeżeli dla dowolnego $\alpha \in P$, R_α jest pierścieniem $\mathscr{T}$-półprostym, to R jest również $\mathscr{T}$-półprosty.

Dowód. Załóżmy nie wprost, że $I \in \mathscr{T}$ jest różnym od zera ideałem pierścienia R. Niech $0 \neq x \in I$ oraz X będzie zbiorem elementów maksymalnych w $\mathrm{Supp}_P(x)$. Ponadto $P' = \{\alpha \in P \,|\, \alpha \leqslant \beta \text{ dla } \beta \in X\}$. Oczywiście P' jest podpółkratą, $G = \sum_{\alpha \in P'} R_\alpha$ jest ideałem w R oraz $x \in G$. Rozważmy $H = G \cap I$. Ponieważ $\mathscr{T}$ jest dziedziczny, $0 \neq H \in \mathscr{T}$.

Niech γ będzie pewnym ustalonym elementem ze zbioru X. Zauważmy, że każdy element y z G ma postać $y = a_y + b_y$, gdzie $a_y \in R_\gamma$ oraz $b_y \in \sum_{\alpha \in P' \setminus \{\gamma\}} R_\alpha$. Rozważmy następujący zbiór $G' = \{(a_y, y) | \, y \in G\}$. Oczywiście G' jest zamknięty na dodawanie. Ponieważ γ jest elementem maksymalnym w P', zbiór G' jest zamknięty również na mnożenie, co implikuje, że jest podpierścieniem w $R_\gamma \oplus G$. Łatwo zauważyć, że G' jest izomorficzny z G. Analogicznie możemy zdefiniować ideał H' pierścienia G' izomorficzny z H. Mamy więc $H' \lhd G'$ oraz $H' \in \mathscr{T}$. Niech $\phi : G \to R_\gamma$ będzie rzutowaniem G' na R_γ. Łatwo pokazać, że odwzorowanie ϕ jest zamknięte na dodawanie. Ponieważ γ jest elementem maksymalnym w P', to odwzorowanie ϕ jest również zamknięte na mnożenie, czyli jest homomorfizmem. Ponieważ $H' \in \mathscr{T}$ i $(a_x, x) \in H'$, to $0 \neq \phi(H') \in \mathscr{T}$. Ale $\phi(H') \lhd R_\gamma$, co daje sprzeczność, gdyż R_γ jest $\mathscr{T}$-półprosty. □

Dowód powyższego twierdzenia oparliśmy na dowodzie (Teply i in., 1980, Twierdzenia 1) sformułowanego analogicznie, ale przy silniejszym założeniu dotyczącym sumy półkratowej $R = \sum_{\alpha \in P} R_\alpha$. Rozważa się tam sumę półkratową (supplementary semilattice sum) spełniającą dodatkowo następujący warunek: $R_\alpha \cap \sum_{\alpha \in P \setminus \{\alpha\}} R_\alpha = \{0\}$ dla dowolnego $\alpha \in P$.

4.4 Półgrupowe sumy pierścieni

Rozpocznijmy od definicji tytułowego pojęcia.

Definicja 4.4.1. Pierścień R jest sumą półgrupową podgup addytywnych R_s pierścienia R względem półgrupy S, gdzie $s \in S$ wtedy i tylko wtedy, gdy $R = \sum_{s \in S} R_s$ oraz $R_s R_t \subseteq R_{st}$ dla dowolnych $s, t \in S$.

Oczywiście każdy pierścień z S–gradacją jest sumą półgrupową.

Przykład 4.4.2. Przedstawimy zaprezentowaną w Puczyłowski (1999) modyfikację ciekawego i ważnego przykładu algebry nad ciałem z Salwa (1996), która jest sumą półgrupową. Niech W będzie półgrupą wolną wyznaczoną przez symbole $\bar{x} = x_\alpha$ oraz $\bar{y} = y_\beta$, gdzie α i β są dodatnimi liczbami rzeczywistymi takimi, że $\frac{\alpha}{\beta}$ jest liczbą niewymierną. Rozważmy ideał I półgrupy W generowany przez zbiór $M = \{w \in M : |\beta \deg_{\bar{y}}(w) - \alpha \deg_{\bar{x}}(w)| \geq \alpha + \beta\}$ oraz algebrę ściągniętą $R = F_0[M/I]$ nad ciałem F. Zauważmy, że jeżeli $w \in W \setminus I$ oraz $w\bar{x} \in I$, to istnieją $u', u \in M$ takie, że $w = u'u$ oraz $ux \in M$. Oczywiście $u \notin M$.

Zatem $\beta \deg_{\bar{y}}(u) - \alpha \deg_{\bar{x}}(u) < \alpha + \beta$ oraz $\beta \deg_{\bar{y}}(u) - \alpha \deg_{\bar{x}}(u) - \alpha = \beta \deg_{\bar{y}}(u\bar{x}) + + (-\alpha) \deg_{\bar{x}}(u\bar{x}) < \beta < \alpha + \beta$. Stąd, ponieważ $u\bar{x} \in M$, mamy więc $\beta \deg_{\bar{y}}(u\bar{x}) + + (-\alpha) \deg_{\bar{x}}(u\bar{x}) \leq -\alpha - \beta$. Zatem $\beta \deg_{\bar{y}}(u) - \alpha \deg_{\bar{x}}(u) \leq -\beta$. Symetrycznie, jeżeli $w\bar{y} \in I$, to istnieją v', $v \in M$ takie, że $w = v'v$ oraz $\beta \deg_{\bar{y}}(v) - \alpha \deg_{\bar{x}}(v) \geq \alpha$.

Załóżmy, że jednocześnie $w\bar{x} \in I$ oraz $w\bar{y} \in I$. W konsekwencji $u = tv$ lub $v = tu$ dla pewnego $t \in W$. Jeżeli $v = tu$, to $\alpha \leq \beta \deg_{\bar{y}}(tu) - \alpha \deg_{\bar{x}}(tu) = \beta(\deg_{\bar{y}}(t) + + \deg_{\bar{y}}(u)) + (-\alpha)(\deg_{\bar{x}}(t) + \deg_{\bar{x}}(u)) \leq \beta \deg_{\bar{y}}(t) - \alpha \deg_{\bar{x}}(t) - \beta$. Stąd $\alpha + \beta \leq \leq \beta \deg_{\bar{y}}(t) - \alpha \deg_{\bar{x}}(t)$, co implikuje $w \in I$ i daje sprzeczność. Analogicznie $\beta \deg_{\bar{y}}(t) - \alpha \deg_{\bar{x}}(t) \leq -\alpha - \beta$ jeżeli $u = tv$. Stąd jeszcze raz $w \in I$ prowadzi do sprzeczności. Zatem obraz homomorficzny z elementu $\bar{x} + \bar{y}$ w algebrze $R = F_0[M/I]$ jest prawostronnie regularny. W szczególności z nie jest nilpotentny, co pociąga, że R nie jest nil.

Niech $M_1 = \{w \in M : \beta \deg_{\bar{y}}(w) - \alpha \deg_{\bar{x}}(w) < 0\}$ oraz niech $M_2 = \{w \in M : \beta \deg_{\bar{y}}(w) - \alpha \deg_{\bar{x}}(w) > 0\}$. Zauważmy, że $M = M_1 \cup M_2$. W konsekwencji $R = R_1 + R_2$ jest sumą dwóch podpierścieni $R_1 = F_0[M_1 \cup I/I]$ oraz $R_2 = F_0[M_2 \cup I/I]$. Łatwo pokazać, że $R_1 = W(R_1)$ oraz $R_2 = W(R_2)$. Zatem R jest przykładem pierścienia będącego sumą dwóch podpierścieni β-radykalnych, który nie jest nil. W Salwa (1996) pokazano dodatkowo, że R jest pierścieniem prymitywnym.

Połóżmy $R_w = Fs$ dla $w \in W \setminus I$ oraz $R_w = 0$ dla $w \in I$. Wynika stąd, że R jest sumą półgrupową względem W, której wszystkie podpierścienie spośród R_w są równe zero.

W dowodzie następnego twierdzenia wykorzystywać będziemy opis struktury pewnych półgrup prostych. Następujący przykład półgrupy macierzowej wykorzystywany jest w tym opisie. Oznaczmy przez $M_{xy}(G)$ zbiór macierzy o elementach z danej grupy G o indeksach z dwóch (niekoniecznie skończonych) zbiorów X oraz Y. Niech e_{xy} będzie macierzą, w której na miejscu xy stoi 1, a poza tym same zera.

Definicja 4.4.3. Niech dana będzie grupa G, dwa niepuste zbiory X, Y oraz macierz $A \in M_{xy}(G)$. Półgrupą macierzową Reesa nazywamy zbiór $G \times X \times$ Y z następującym działaniem:

$$(g_1, x_1, y_1) \cdot (g_2, x_2, y_2) = (g_1 a_{y_1 x_2} g_2, x_1, y_2). \tag{4.4.1}$$

Półgrupę tę oznacza się standardowo przez $\mathscr{M}(G; X, Y; A)$.

Zauważmy, że jeżeli (g, x, y) utożsamimy z macierzą ge_{xy}, to iloczyn (4.4.1) odpowiada macierzy $BAC = g_1 e_{x_1 y_1} A g_2 e_{x_2 y_2} = g_1 a_{y_1 x_2} g_2 e_{x_1 y_2}$.

Przez S^0 oznaczamy półgrupę z dołączonym zerem. W półgrupie $\mathscr{M}^0(G^0; X, Y; A)$ utożsamia się wszystkie elementy postaci $(0, x, y)$.

Niech S będzie półgrupą z zerem. Powiemy, że S jest 0-prosta jeżeli jedynymi jej ideałami są $\{0\}$ i S. Półgrupę S nazwiemy kompletnie 0-prostą jeżeli S posiada zarówno lewostronny jak i prawostronny ideał 0-minimalny.

Wielokrotnie wykorzystywać będziemy dalej następujący znany wynik L. N. Shevrina:

Twierdzenie 4.4.4. Załóżmy, że torsyjna półgrupa S zawiera skończenie wiele elementów idempotentnych, każdy obraz homomorficzny S, który jest nil jest nilpotentny oraz każda podgrupa S jest skończona. Wtedy S posiada skończony łańcuch ideałów:

$$\emptyset = S_0 \subseteq S_1 \subseteq \ldots \subseteq S_n = S \tag{4.4.2}$$

taki, że dla dowolnego $1 \leq i \leq n-1$, S_{i+1}/S_i jest nilpotentny albo skończony.

Dowód. Niech $H \neq S$ będzie ideałem w S i załóżmy, że dla półgrupy H można skonstruować skończony łańcuch postaci (4.4.2). Zachodzi teraz jeden z dwóch następujących przypadków:

1. Półgrupa $Q = S/H$ posiada nil ideał.

Wtedy niech H_1/H będzie maksymalnym nil ideałem w S/H. Z założenia H_1/H jest nilpotentny.

2. Półgrupa $Q = S/H$ nie posiada nil ideałów.

Ponieważ Q jest półgrupą torsyjną, każdy ideał właściwy w Q zawiera idempotent. Niech J będzie ideałem minimalnym w Q. Na podstawie (Clifford i Preston, 1961, Twierdzenia 2.29), J jest 0-prosty lub prosty. Rozumowanie w obu przypadkach jest analogiczne. Załóżmy zatem, że J jest półgrupą 0-prostą. Ponieważ J jest półgrupą torsyjną z (Clifford i Preston, 1961, Corollary 2.56) dostajemy, że J jest kompletnie 0-prosty. Stąd i z (Clifford i Preston, 1961, Twierdzenia 3.5), $J = \mathscr{M}^0(G^0;X,Y;A)$ dla pewnej grupy G^0 oraz macierzy A. Rozważmy odwzorowanie $\phi : G \to \mathscr{M}^0(G^0;X,Y;A)$ dane wzorem $\phi(g) = (gh^{-1},x,y)$, gdzie $h \in G$ jest elementem grupy G, który stoi na głównej przekątnej macierzy A dla pewnego $x \in X$ oraz $y \in Y$. Łatwo sprawdzić, że ϕ jest izomorfizmem grupy G. Zatem J zawiera podgrupę izomorficzną z G. Z założenia G jest grupą skończoną. Ponieważ J zawiera skończenie wiele idempotentów, zbiory X i Y muszą być skończone. Zatem J jest skończonym ideałem w Q. W konsekwencji $J = H_1/H$ dla pewnego ideału H_1 półgrupy S.

Zatem w obu przypadkach istnieje ideał w S, którego półgrupa ilorazowa względem H jest nilpotentna albo skończona. Każde zastosowanie metody opisanej w 2. wymaga dołączenia kolejnego idempotenta z S. Ponieważ z założenia idempotentów w S jest skończenie wiele, konstrukcja ta może być wykonana skończenie wiele razy. Oczywiście wydłużenia łańcucha (4.4.2) metodą opisaną w 1. nie można wykonać dwa razy pod rząd. Zatem S posiada skończony łańcuch (4.4.2), co kończy dowód. □

Powiemy, że półgrupa S jest nil ograniczonego indeksu jeżeli istnieje taka liczba naturalna m, że dla każdego $s \in S$, $s^m = 0$.

Uwaga 4.4.5. Zauważmy, że analogiczną tezę jak w Twierdzeniu 4.4.4 otrzymujemy, gdy zamiast nilpotentności założymy, że każdy obraz homomorficzny S, który jest nil jest nil ograniczonego indeksu. Wtedy S posiada skończony łańcuch (4.4.2) taki,

że dla dowolnego $1 \leq i \leq n-1$, iloraz S_{i+1}/S_i jest nil ograniczonego indeksu albo skończony.

Definicja 4.4.6. Powiemy dla półgrupy S, że klasa pierścieni $\mathscr{M}$ jest S-zamknięta wtedy i tylko wtedy, gdy do $\mathscr{M}$ należą wszystkie sumy półgrupowe $R = \sum_{s\in S} R_s$ takie, że jeżeli każdy podpierścień spośród R_s dla $s \in S$ należy do $\mathscr{M}$, to $R \in \mathscr{M}$.

Lemat 4.6. Klasa pierścieni $\mathscr{M}$, która jest zamknięta na sumy jednostronnych ideałów, obrazy homomorficzne, podpierścienie oraz zawierająca klasę wszystkich pierścieni z zerowym mnożeniem, jest G-zamknięta dla dowolnej grupy skończonej G.

Dowód. Niech $G = \{e = g_1, g_2, \ldots, g_n\}$ oraz e jej elementem neutralnym. Rozważmy sumę grupową $R = \sum_{s\in G} R_s$ względem grupy G oraz załóżmy, że $R_e \in \mathscr{M}$. Niech T będzie następującym pierścieniem macierzowym:

$$T = \begin{pmatrix} R_e & R_{g_1g_2^{-1}} & \cdots & R_{g_1g_n^{-1}} \\ R_{g_2g_1^{-1}} & R_e & \cdots & R_{g_2g_n^{-1}} \\ \vdots & \vdots & & \vdots \\ R_{g_ng_1^{-1}} & R_{g_ng_2^{-1}} & \cdots & R_e \end{pmatrix}.$$

Ponieważ T jest sumą lewostronnych ideałów z $\mathscr{M}$ postaci:

$$L_i = \begin{pmatrix} 0 \cdots R_{g_1g_i^{-1}} \cdots 0 \\ 0 \cdots R_{g_2g_i^{-1}} \cdots 0 \\ \vdots \quad\quad \vdots \quad\quad \vdots \\ 0 \cdots R_{g_ng_i^{-1}} \cdots 0 \end{pmatrix},$$

więc $T \in \mathscr{M}$. Niech $a = \sum_{g\in G} a_g$, gdzie $a_g \in R_g$ dla dowolnego $g \in G$. Zdefiniujmy następująco element pierścienia T:

$$a_T = \begin{pmatrix} a_e & a_{g_1g_2^{-1}} & \cdots & a_{g_1g_n^{-1}} \\ a_{g_2g_1^{-1}} & a_e & \cdots & a_{g_2g_n^{-1}} \\ \vdots & \vdots & & \vdots \\ a_{g_ng_1^{-1}} & a_{g_ng_2^{-1}} & \cdots & a_e \end{pmatrix}. \tag{4.4.3}$$

Łatwo sprawdzić, że zbiór M wszystkich elementów pierścienia T uzyskanych w ten sposób tworzy podpierścień w T. Zdefiniujmy odwzorowanie $\phi : M \to R$ następująco: jeżeli a_T jest postaci (4.4.3), to $\phi(a_T) = a_e + a_{g_2g_1^{-1}} + \ldots + a_{g_ng_1^{-1}}$. Można pokazać, że ϕ jest homomorfizmem, którego obrazem jest R. Ponieważ $M \subseteq T$ jest podpierścieniem T, więc $M \in \mathscr{M}$. Skąd $R \in \mathscr{M}$. □

Powyższy lemat można uogólnić w następujący sposób:

Lemat 4.7. (por. (Kelarev, 1993, Lemat 5.)) Niech $\mathscr{M}$ będzie klasą pierścieni zamkniętą na grupy skończone, na sumy jednostronnych ideałów oraz rozszerzenia. Ponadto niech $\mathscr{M}$ zawiera klasę pierścieni z zerowym mnożeniem. Wtedy klasa $\mathscr{M}$ jest S-zamknięta dla dowolnej półgrupy skończonej S.

Dowód. Stosując rozumowanie indukcyjne względem liczby elementów S oraz fakt, że $\mathscr{M}$ jest zamknięta na rozszerzenia, wystarczy wykazać tezę przy założeniu, że S jest półgrupą prostą lub 0-prostą. Jeżeli $S^2 = 0$, to $R^2 = 0$. Zatem $R \in \mathscr{M}$.

Wystarczy bez straty ogólności założyć, że S jest półgrupą 0-prostą. Stąd, analogicznie jak w dowodzie Twierdzenia 4.4.4, $S = \mathscr{M}^0(G^0; X, Y; A)$ dla pewnej grupy G^0. Kolumny półgrupy macierzowej $\mathscr{M}^0(G^0; X, Y; A)$ są prawostronnymi ideałami S. Wynika stąd, że R jest sumą prawostronnych ideałów, które są sumami półgrupowymi o mniejszej liczbie elementów niż S. Z założenia indukcyjnego R jest sumą lewostronnych ideałów z $\mathscr{M}$. Stąd $R \in \mathscr{M}$, co kończy dowód. □

Przykładami klas $\mathscr{M}$ spełniających założenia powyższych dwóch lematów są klasa pierścieni lewostronnie (prawostronnie) T-nilpotentnych, β-radykalnych oraz PI-pierścieni.

Skoncentrujemy się teraz na klasie PI-pierścieni. Przedstawimy jedną z wielu równoważnych definicji tej klasy. Rozważmy pierścień wielomianów $\mathbb{Z}[x_1, x_2, \ldots]$ od nieprzemiennych zmiennych o współczynnikach z pierścienia liczb całkowitych $\mathbb{Z}$. Powiemy, że wielomian $f \in \mathbb{Z}[x_1, x_2, \ldots]$ jest unormowany, jeżeli przynajmniej jeden współczynnik jednomianu najwyższego stopnia z nośnika f jest równy 1.

Definicja 4.4.7. Pierścień A jest PI-pierścieniem wtedy i tylko wtedy, gdy istnieje wielomian $f \in \mathbb{Z}[x_1, x_2, \ldots]$ taki, że dla dowolnego homomorfizmu ϕ, gdzie $\phi : \mathbb{Z}[x_1, x_2, \ldots] \to A$ oraz $\phi(f) = 0$. Powiemy wtedy, że $f = 0$ jest tożsamością wielomianową na A lub że A spełnia f. Stopień wielomianu f nazywa się stopniem tożsamości wielomianowej $f = 0$.

Wiadomo, że jeżeli pierścień A spełnia tożsamość wielomianową stopnia d, to spełnia również tożsamość wieloliniową:

$$g = x_1 \cdots x_d + \sum_{id \neq \pi \in S_k} \alpha_\pi x_{\pi(1)} \cdots x_{\pi(d)} = 0, \tag{4.4.4}$$

gdzie S_d grupą permutacji zbioru $\{1, 2, \ldots, d\}$ oraz $\alpha_\pi \in \mathbb{Z}$.

Bardzo ważną informację o klasie PI-pierścieni podaje następujące

Twierdzenie 4.4.8. **(**Kępczyk i Puczyłowski, 2001, Twierdzenie 3) Przypuśćmy, że $\mathfrak{F}$ jest homomorficznie zamkniętą klasą pierścieni, która dodatkowo jest zamknięta na potęgi proste. Jeżeli dowolny niezerowy pierścień z $\mathfrak{F}$ zawiera niezerowy jednostronny PI ideał, to $\mathfrak{F}$ składa się z PI pierścieni.

Stąd dostajemy następujący

Wniosek 4.4.9. Niech pierścień $R = R_1 + R_2$ będzie sumą dwóch *PI*-podpierścieni R_1 oraz R_2. Jeżeli R_1 jest jednostronnym ideałem pierścienia R, to R jest *PI*-pierścieniem.

Oznaczmy klasę wszystkich *PI*-pierścieni przez $\mathscr{P}$.

Następujące przykłady pochodzące z Kelarev (1993), których pewne modyfikacje teraz przedstawimy, zawężają klasę półgrup S, dla których klasa $\mathscr{P}$ jest S-zamknięta.

Przykład 4.4.10. Niech G będzie dowolną grupą nieskończoną. Pokażemy, że klasa $\mathscr{P}$ nie jest G-zamknięta. W G istnieje nieskończony ciąg elementów $g_1, g_2, \ldots g_n, \ldots$ taki, że dla dowolnych liczb naturalnych $m \leq n$, $g_m g_{m+1} \cdots g_n \neq e$. Rzeczywiście, niech $g_1 \neq e$. Załóżmy, że wyznaczono elementy $g_1, g_2, \ldots, g_n$ tego ciągu dla $n > 1$. Rozważmy zbiór $C = \{(g_m g_{m+1} \cdots g_n)^{-1} \,|\, m \leq n\} \cup \{e\}$. Wystarczy teraz za g_{n+1} przyjąć dowolny element ze zbioru $G \setminus C$. Rozważmy F-algebrę B generowaną przez elementy $a_1, a_2, \ldots a_n, \ldots$ z następującymi relacjami: $a_i a_j = 0$ dla dowolnych liczb naturalnych i oraz j takich, że $j \neq i+1$. Możemy zdefiniować następującą podalgebrę z gradacją $A = \oplus_{g \in G} A_g$ algebry B. Niech $A_g = 0$ dla $g \in G \setminus C$ oraz A_g będzie podprzestrzenią liniową algebry B generowaną przez iloczyny $a_m a_{m+1} \cdots a_n$, dla których $g_m g_{m+1} \cdots g_n = g$. Oczywiście wszystkie podalgebry wśród A_g są algebrami z zerowym mnożeniem. Łatwo zauważyć, że A nie spełnia jednak tożsamości wieloliniowej (4.4.4) dla żadnego stopnia d. Zatem A nie jest *PI*-algebrą.

Przykład 4.4.11. Niech S będzie dowolną nil półgrupą. Pokażemy, że jeżeli klasa *PI*-pierścieni jest S-zamknięta, to S jest półgrupą nilpotentną. Załóżmy, że S nie jest nilpotentna. Zatem dla każdego $n \in \mathbb{N}$ istnieje niepusty podzbiór półgrupy S postaci $M_n = \{s_{in} \,|\, s_{1n} s_{2n} \cdots s_{nn} \neq 0\}$. Rozważmy F-algebrę A generowaną przez różne elementy a_{ij} gdzie $i, j \in \mathbb{N}$. Dodatkowo niech generatory A spełniają następujące relacje: $a_{im} a_{jn} = 0$ jeżeli tylko $m \neq n$ lub $j \neq i+1$. Przez A_s oznaczmy podprzestrzeń liniową A generowaną przez iloczyny $a_{kn} a_{(k+1)n} \cdots a_{mn}$, gdzie $k \leq m \leq n$, takie, że $s_{kn} s_{(k+1)n} \cdots s_{mn} = s$. Oczywiście $A = \oplus_{s \in S} A_s$ jest algebrą z S-gradacją. Zauważmy, że jeżeli dla pewnego $s \in S$, A_s jest podalgebrą, to $A_s^2 \subseteq A_s \cap A_{s^2}$. Ale S jest nil, więc $s \neq s^2$. Stad $A_s^2 = 0$. Jednakże dla dowolnego $d \in \mathbb{N}$, elementy $a_{1d}, a_{2d}, \ldots, a_{dd}$ nie spełniają tożsamości wieloliniowej (4.4.4). Zatem A nie jest *PI*-algebrą. Otrzymana sprzeczność pokazuje, że nil półgrupa S musi być nilpotentna w tym przypadku.

Przykład 4.4.12. Zauważmy, że klasa $\mathscr{P}$ nie jest S-zamknięta w przypadku półgrup S zawierających nieskończenie wiele idempotentów $I = \{e_1, e_2, \ldots\}$. Niech $R_{e_i} = F_i$, gdzie F_i jest pierścieniem macierzy wymiaru $i \times i$ nad ustalonym ciałem F dla $i \in \mathbb{N}$ oraz $R_s = 0$ dla każdego $s \in S \setminus I$. Oczywiście pierścień $R = \oplus_{s \in S} R_s$ nie jest *PI*-pierścieniem.

Następny przykład dotyczy także klas pierścieni, którymi zajmowaliśmy się wcześniej. Oznaczmy przez $\mathscr{TN}$ klasę pierścieni lewostronnie T-nilpotentnych.

Przykład 4.4.13. Rozważmy F-algebrę wolną $A = F[x_1, x_2, \ldots, x_n]$ o współczynnikach z ciała F od nieprzemiennych zmiennych $X = \{x_1, x_2, \ldots, x_n\}$, gdzie $n > 1$. Podalgebra XA algebry A posiada naturalną gradację względem stopnia jednomianów z XA. Niech S będzie dowolną półgrupą, która nie jest torsyjna oraz a jej niecyklicznym elementem. Niech P_{a^n} będzie podgrupą grupy addytywnej XA generowaną przez jednomiany stopnia n. W przypadku, gdy $t \in S \setminus \{a, a^2, \ldots\}$ połóżmy $P_t = 0$. Oczywiście $XA = \oplus_{s \in S} P_s$ jest algebrą z gradacją względem S, wszystkie podalgebry spośród P_s są pierścieniami z zerowym mnożeniem oraz $XA \notin \mathscr{P} \cup \beta \cup \mathscr{T}\mathscr{N}$.

Jesteśmy przygotowani do podania głównego wyniku w tym rozdziale, który jest uogólnieniem (Kelarev, 1993, Twierdzenie 1).

Twierdzenie 4.4.14. Klasa $\mathscr{P}$ jest S-zamknięta wtedy i tylko wtedy, gdy półgrupa S posiada skończony łańcuch ideałów:

$$\emptyset = S_0 \subseteq S_1 \subseteq \ldots \subseteq S_n = S \tag{4.4.5}$$

taki, że dla dowolnego $1 \leq i \leq n-1$, każdy iloraz S_{i+1}/S_i jest nilpotentny albo skończony.

Dowód. Załóżmy, że klasa $\mathscr{P}$ jest S-zamknięta. Pokażemy, że S posiada skończony łańcuch (4.4.5). Przykład 4.4.10 pokazuje, że S nie zawiera grup skończonych. Z Przykładów 4.4.12 oraz 4.4.13 dostajemy, że półgrupa S jest torsyjna oraz zawiera skończoną liczbę idempotentów. Z założenia oraz Przykładu 4.4.11 wynika, że każdy obraz homomorficzny S, który jest nil jest nilpotentny. Stosując Twierdzenia 4.4.4 dostajemy tezę.

Załóżmy, że S posiada skończony łańcuch (4.4.6) oraz $R = \sum_{s \in S} R_s$ jest sumą półgrupową taką, że wszystkie podpierścienie spośród podgrup addytywnych R_s pierścienia R są z $\mathscr{P}$. Niech $I_i = \sum_{s \in S_i} R_s$ dla $1 < i \leq n$. Oczywiście $I_i \lhd R$ oraz $I_i = \sum_{s \in S_i} R_s$. Zauważmy, że $I_{i+1}/I_i = \sum_{s \in S_{i+1}/S_i} P_s$, gdzie podpierścienie spośród P_s dla $s \in S_{i+1}/S_i$ są izomorficzne z odpowiednimi podpierścieniami R_s dla $s \neq 0$ oraz $P_0 = 0$, zatem są PI- pierścieniami. Z założenia iloraz S_{i+1}/S_i jest skończony lub nilpotentny. Na podstawie Lematu 4.7, I_{i+1}/I_i jest PI-pierścieniem, gdy S_{i+1}/S_i jest skończona. W przypadku, gdy S_{i+1}/S_i jest nilpotentna, I_{i+1}/I_i jest również PI-pierścieniem. Zatem dla każdego $i \in \{1, 2, \ldots, n\}$, $I_{i+1}/I_i \in \mathscr{P}$, co implikuje (po n krokach), że $R \in \mathscr{P}$. □

Implikację (i) $\Rightarrow$ (ii) powyższego twierdzenia możemy rozszerzyć na klasę β oraz $\mathscr{T}\mathscr{N}$.

Stwierdzenie 4.4.15. Niech półgrupa S posiada skończony łańcuch ideałów:

$$\emptyset = S_0 \subseteq S_1 \subseteq \ldots \subseteq S_n = S \tag{4.4.6}$$

taki, że dla dowolnego $1 \leq i \leq n-1$, każdy iloraz S_{i+1}/S_i jest nilpotentny albo skończony. Wtedy klasa $\mathscr{U}$, gdzie $\mathscr{U} = \beta$ lub $\mathscr{U} = \mathscr{T}\mathscr{N}$ jest S-zamknięta.

Dowód. Załóżmy, że półgrupa S spełnia założenia powyższego stwierdzenia oraz $R = \sum_{s\in S} R_s$ jest sumą półgrupową taką, że wszystkie podpierścienie spośród podgrup addytywnych R_s pierścienia R są z $\mathscr{U}$. Niech $i \in \{1,2,\ldots,n\}$. Istnieją takie ideały $I_i, I_{i+1} \lhd R$, wyznaczone przez półgrupy S_i, S_{i+1} z łańcucha (4.4.6), że I_{i+1}/I_i. Ponieważ S_{i+1}/S_i jest nilpotentny albo skończony, więc na mocy Lematów 4.6 oraz 4.7, $I_{i+1}/I_i \in \mathscr{U}$. Ponieważ klasa $\mathscr{U}$ jest zamknięta na rozszerzenia, więc $I_{i+1} \in \mathscr{U}$. W konsekwencji $I_n = R \in \mathscr{U}$, co należało udowodnić. □

Pojawia się naturalne pytanie:

Problem 4.4.16. Czy implikację w Stwierdzeniu 4.4.15 można odwrócić?

4.5 S-sumy pierścieni

Zakończymy przedstawieniem następującego uogólnienia pojęcia sumy półgrupowej:

Definicja 4.5.1. Powiemy, że pierścień $R = \sum_{\alpha\in S} R_\alpha$ jest S-sumą, gdzie R_s są podgrupami grupy abelowej R oraz S jest dowolną półgrupą wtedy i tylko wtedy, gdy $R_s R_t \subseteq \sum_{q\in\langle st\rangle} R_q$, gdzie $\langle st\rangle$ oznacza podpółgrupę w S generowaną przez st.

Oczywiście każdy pierścień, który jest sumą półgrupową jest S-sumą.

Naszym celem jest uogólnienie Twierdzenia 4.4.5 na przypadek S-sum. Potrzebować będziemy następującego twierdzenia:

Twierdzenie 4.5.2. (Kępczyk, 2021, Twierdzenie 4) Niech R_1 będzie PI-podpierścieniem pierścienia R oraz R_2 podgrupą grupy addytywnej R taką, że $R = R_1 + R_2$ oraz R_2 spełnia tożsamość wielomianową. Wtedy:

1. jeżeli $R_2^t \subseteq R_1$ dla pewnej liczby całkowitej t, to R jest PI-pierścieniem;
2. jeżeli $(R_1R_2)^k \subseteq R_1$ dla pewnej liczby całkowitej k, to R jest PI-pierścieniem.

Potrzebować też będziemy następujących lematów:

Lemat 4.8. Niech G będzie skończoną 2-grupą oraz $R = \sum_{s\in G} R_s$ G-sumą. Jeżeli $R_e \in \mathscr{U}$, gdzie $\mathscr{U} = \mathscr{P}$ lub $\mathscr{U} = \beta$ lub $\mathscr{U} = \mathscr{TN}$, to $R \in \mathscr{U}$.

Dowód. Każda skończona 2-grupa posiada ciąg centralny o ilorazach rzędu dwa. Ponadto jeżeli N jest dzielnikiem normalnym grupy G, to $R = \sum_{gN\in G/N} R_{gN}$ G/N-sumą, której składnikiem początkowym jest R_N. Zatem jeżeli $R_N \in \mathscr{U}$ oraz G/N jest grupą rzędu dwa, to na podstawie Twierdzeń 4.5.2, 4.1 oraz 4.2.2, $R \in \mathscr{U}$. Wykorzystując rozumowanie indukcyjne względem rzędu grupy G otrzymujemy tezę. □

Lemat 4.9. Niech S będzie skończoną półgrupą oraz $R = \sum_{s\in S} R_s$ jest S-sumą, jedynymi podgrupami S są 2-grupy. Jeżeli wszystkie podpierścienie spośród R_s są PI-pierścieniami, to R jest PI-pierścieniem.

Dowód. Teza wynika z Lematów 4.7 oraz 4.8. □

Lemat 4.10. Dla dowolnej grupy torsyjnej G, która nie jest 2-grupą, istnieje G-suma $R = \sum_{s\in G} R_s$ taka, że wszystkie podpierścienie spośród R_s są pierścieniami z zerowym mnożeniem, ale $R \notin \mathscr{P} \cup \beta \cup \mathscr{T}\mathscr{N}$.

Dowód. Niech $A = XB[X]$ będzie pierścieniem wielomianów przemiennych zmiennych ze zbioru $X = \{x, y, z\}$ o współczynnikach z pierścienia B bez wyrazów stałych. Załóżmy, że $B \notin \mathscr{P} \cup \beta \cup \mathscr{T}$. Niech I będzie ideałem A generowanym przez x^3, y^3, xy, xz oraz yz. Rozważmy pierścień $R = A/I$. Niech $R_g = (zB[z] + xB + y^2B + I)/I$, $R_{g^2} = (x^2B + yB + I)/I$ oraz $R_s = 0$ dla dowolnego $s \in G \setminus \{g, g^2\}$. Zauważmy, że $R_g R_{g^2} = R_{g^2} R_g = 0$. Ponadto, ponieważ $g, g^2 \in \langle g \rangle$, więc $R_g^2 = (zB[z] + x^2B + I)/I \subseteq \sum_{s\in\langle g\rangle} R_s$ oraz $R_{g^2}^2 = (y^2B + I)/I \subseteq \sum_{s\in\langle g\rangle} R_s$. Stąd R jest G-sumą, wszystkie podpierścienie spośród R_s są pierścieniami z zerowym mnożeniem oraz $R \notin \mathscr{P} \cup \beta \cup \mathscr{T}\mathscr{N}$. □

Twierdzenie 4.5.3. (por. (Kępczyk, 2020, Twierdzenie 5.3)) Następujące warunki są równoważne:

(i) dla dowolnej S-sumy $R = \sum_{s\in S} R_s$, jeżeli wszystkie podpierścienie spośród R_s są PI-pierścieniami, to R jest PI-pierścieniem;
(ii) S^0 posiada skończony łańcuch ideałów taki, że:

$$0 = S_0 \subseteq S_1 \subseteq \ldots \subseteq S_n = S^0,$$

gdzie każdy S_i/S_{i-1} jest nilpotentny lub skończony dla $i = 1, \ldots, n$ oraz każda podgrupa S jest 2-grupą.

Dowód. (i) $\Rightarrow$ (ii). Podobnie jak w dowodzie Twierdzenia 4.4.14, wykorzystując Przykłady 5.9 - 5.12 oraz Twierdzenie 4.4.4 dostajemy, że S posiada skończony łańcuch (4.4.2). Ponadto na podstawie Lematu 4.10, każda podgrupa S jest 2-grupą.

(ii) $\Rightarrow$ (i). Wystarczy zastosować Lemat 4.9 oraz rozumowanie indukcyjne względem długości łańcucha (4.4.2) analogiczne jak w dowodzie Twierdzenia 4.4.14. □

Problem 4.5.4. Czy klasę PI-pierścieni w Twierdzeniu 4.10 można zastąpić klasą β lub $\mathscr{T}\mathscr{N}$?

Przedstawione w pracy Kelarev i McConnell (1995) wyniki, które stanowią główną motywację dla tematyki tego rozdziału, dotyczą S-sum pierścieni przy ogólniejszej definicji tego pojęcia. Nazwiemy te sumy, dla odróżnienia, S_∞-sumami pierścieni. Zasadnicza różnica wyraża się w definicji sumy $\sum_{\alpha\in S} R_\alpha$, w której do tej pory dopuszczaliśmy jedynie skończone liczby składników. Rozważmy teraz następujący przypadek:

$$\sum_{s\in S} R_s = \{x_s + x_t + \ldots \mid x_s \in R_s, x_t \in R_t, \ldots\}. \tag{4.5.1}$$

Definicja 4.5.5. Powiemy, że pierścień $R = \sum_{\alpha \in S} R_\alpha$ z sumą (4.5.1), jest S_∞-sumą względem półgrupy S wtedy i tylko wtedy, gdy $R_s R_t \subseteq \sum_{q \in \langle st \rangle} R_q$, gdzie $\langle st \rangle$ oznacza podpółgrupę w S generowaną przez st.

Oczywiście każdy pierścień, który jest S-sumą półgrupową jest S_∞-sumą półgrupową, ale nie na odwrót. Wystarczy rozważyć pierścień wielomianów $F[x]$ oraz pierścień szeregów formalnych $F\{x\}$ zmiennej x nad dowolnym ciałem F. Są to pierścienie z naturalnymi gradacjami względem półgrupy $\mathbb{N}$. Różnicę między pojęciami S-sum dobrze widać także, gdy rozważymy pierścień $R = \oplus_{s \in S} R_s$ oraz $R = \prod_{s \in S} R_s$, gdzie S jest nieskończoną półgrupą z zerowym mnożeniem oraz R_α są dla $s \in S$ podgrupami grupy abelowej R.

Zaważmy, że w przypadku S_∞-sum zachodzi analogiczne do 4.5.3 twierdzenie.

Twierdzenie 4.5.6. **(**Kępczyk, 2020, Twierdzenie 5.3) Następujące warunki są równoważne:

(i) dla dowolnej S_∞-sumy $R = \sum_{s \in S} R_s$, jeżeli wszystkie podpierścienie spośród R_s są PI-pierścieniami, to R jest PI-pierścieniem;
(ii) S^0 posiada skończony łańcuch ideałów taki, że:

$$0 = S_0 \subseteq S_1 \subseteq \ldots \subseteq S_n = S^0,$$

gdzie każdy S_i/S_{i-1} jest nilpotentny lub skończony dla $i = 1, \ldots, n$ oraz każda podgrupa S jest 2-grupą.

Zaprezentujemy, w kilku następujących lematach, wyniki dotyczące klas $\mathscr{T}\mathscr{N}$ oraz β, których nie udało się nam uzyskać w przypadku S-sum, a które zachodzą dla S_∞-sum pierścieni.

Lemat 4.11. Jeżeli półgrupa S ma nieskończenie wiele idempotentów, to istnieje S_∞-suma $R = \sum_{s \in S} R_s$ taka, że wszystkie podpierścienie spośród R_s są nilpotentne, ale R nie jest nil-pierścieniem.

Dowód. Niech $\{e_1, e_2, \ldots\}$ będzie dowolnym nieskończonym zbiorem idempotentów półgrupy S. Połóżmy $R_{e_i} = xF[x]/(x^i)$. Niech $R_s = 0$ dla pozostałych elementów s z S. Oczywiście $R = \prod_{s \in S} R_s$ jest S_∞-sumą, która nie jest nil. □

Lemat 4.12. Jeżeli nil półgrupa S, która nie jest półgrupą nil ograniczonego indeksu, to istnieje S_∞-suma $R = \sum_{s \in S} R_s$ taka, że wszystkie podpierścienie spośród R_s są nilpotentne, ale R nie jest nil-pierścieniem.

Dowód. Z założenia istnieje w S ciąg elementów $s_1, s_2, \ldots$ taki, że $\langle s_i \rangle$ są półgrupami nilpotentnymi o coraz większym stopniu nilpotentności dla kolejnych $i \in \mathbb{N}$. Ponadto $\langle s_i \rangle \cap \langle s_j \rangle = 0$ dla $i \neq j$. Bez straty ogólności możemy założyć, że dla każdej liczby naturalnej i, $\langle s_i \rangle$ jest półgrupą nilpotentną o stopniu nilpotentności równym $i+1$. Niech dla dowolnego $i \in \mathbb{N}$, $R_{s_i^m} = (xF[x]/(x^{i+1}))^m$, gdzie $1 \leq$

$m < i+1$. Przyjmijmy $R_s = 0$ dla pozostałych elementów $s \in S$. Łatwo zauważyć, że $R = \prod_{i\in\mathbb{N}} xF[x]/(x^{i+1}) = \sum_{s\in S} R_s$ jest S_∞-sumą. Oczywiście R nie jest nilpierścieniem. □

Lemat 4.13. Jeżeli G jest nieskończoną grupą torsyjną, to istnieje G_∞-suma $R = \sum_{s\in G} R_s$ taka, że wszystkie podpierścienie spośród $R_s \in \mathscr{U}$, gdzie $\mathscr{U} = \beta$ lub $\mathscr{U} = \mathscr{T}\mathscr{N}$, ale $R \notin \mathscr{U}$.

Dowód. Niech:

$$R_e = \bigoplus_{i\in\mathbb{N}} xF[x]/(x^i),$$

gdzie e jest elementem neutralnym grupy G. Połóżmy $R_{g_i} = xF[x]/(x^i)$ dla $e \neq e_i \in G$ oraz $R_g = 0$ dla pozostałych elementów g z G. Łatwo zauważyć, że $R = \prod_{g\in G} R_g$ jest G_∞-sumą, która nie jest nil. □

Powyższe fakty prowadzą do następującego stwierdzenia:

Stwierdzenie 4.5.7. Niech dla pewnej półgrupy S, $R = \sum_{s\in S} R_s$ będzie S_∞-sumą taką, że jeżeli wszystkie podpierścienie spośród $R_s \in \mathscr{U}$, gdzie $\mathscr{U} = \beta$ lub $\mathscr{U} = \mathscr{T}\mathscr{N}$, to $R \in \mathscr{U}$. Wtedy S^0 posiada skończony łańcuch ideałów taki, że:

$$0 = S_0 \subseteq S_1 \subseteq \ldots \subseteq S_n = S^0,$$

gdzie każdy iloraz S_i/S_{i-1} jest nil ograniczonego indeksu lub jest skończony dla $i = 1,\ldots,n$ oraz każda podgrupa S jest 2-grupą.

Dowód. Załóżmy, że $\mathscr{U} = \mathscr{T}\mathscr{N}$ lub $\mathscr{U} = \beta$. Wykorzystując Przykład 4.4.13 oraz Lematy 4.10 oraz 4.13 dostajemy, że dowolna podgrupa w S jest skończoną 2-grupą. Z Lematu 4.11 S ma skończenie wiele idempotentów. Stosując Lemat 4.12 otrzymujemy dodatkowo, że każdy nil obraz homomorficzny S jest nil ograniczonego indeksu. Teza wynika teraz z Twierdzenia 4.4.4, Uwagi 4.4.5 oraz Lematu 4.8. □

Nasuwa się pytanie, czy można odwrócić implikację w Stwierdzeniu 4.5.7. Wobec Lematu 4.7 sprowadza się ono do następującej kwestii:

Problem 4.5.8. Niech dla pewnej półgrupy S, $R = \sum_{s\in S} R_s$ będzie S_∞-sumą taką, że wszystkie podpierścienie spośród $R_s \in \mathscr{U}$, gdzie $\mathscr{U} = \beta$ lub $\mathscr{U} = \mathscr{T}\mathscr{N}$. Czy jeżeli S jest nil półgrupą ograniczonego indeksu, to $R \in \mathscr{U}$?

Podsumowanie

Przedstawiliśmy własności kilku klas pierścieni, które są bezpośrednimi uogólnieniami klasy pierścieni nilpotentnych ze szczególnym uwzględnieniem pierścieni

T-nilpotentnych oraz pierścieni radykalnych w sensie radykału pierwszego. Bezpośrednią motywacją do zajęcia się tymi klasami był znany wynik Kegela mówiący, że pierścienie, które są sumami dwóch podpierścieni nilpotentnych są nilpotentne. Poszukiwanie uogólnienia tego rezultatu, gdzie zamiast dwóch rozważa się dowolną skończoną liczbę podpierścieni o własnościach bliskich nilpotentności, doprowadziło do zajęcia się pierścieniami z różnego typu S-gradacjami, gdzie S jest półgrupą. W pracy zaprezentowaliśmy aktualny stan wiedzy związany z tego rodzaju sumami podpierścieni. Na tej podstawie przedstawiliśmy także nowe wyniki oraz szereg pytań, które stanowić mogą materiał do dalszych badań.

Bibliografia

Bahturin, Y., i Giambruno, A. (1994). Identities of sums of commutative subalgebras. Rend. Mat. Palermo, 43, 250–258.

Beidar, K., i Mikhalev, A. (1995). Generalized polynomial identities and rings which are sums of two subrings. Algebra and Logic, 34, 3–11.

Bokut, L. (1976). Imbeddings into simple associative algebra. Algebra i Logika, 15, 117–147.

Chebotar, M., Lee, P. i Puczyłowski, E. (2010). A note on termination of the Baer construction of the prime radical. Arch. Math. (Basel), 95 no. 4, 325–332.

Clifford, A., i Preston, G. (1961). The algebraic theory of semigroups, Vol. I. Math. Surveys No. 7, Amer. Math. Soc. Providence.

Felzenszwalb, B., Giambruno, A. i Leal, G. (2003). On rings which are sums of two *PI*-subrings: a combinatorial approach. Pacific J. Math., 209 no. 1, 17–30.

Ferrero, M., i Puczyłowski, E. (1989). On rings which are sums of two subrings. Arch. Math., 53, 4–10.

Gardner, B. J. (1992). Some nil ring properties related to T-nilpotence. Bull. Austral. Math. Soc., 46, 519–523.

Janeski, J., i Weissglass, J. (1973). Regularity of semilattice sums of rings. Proc. Amer. Math. Soc., 39, 479–482.

Kępczyk, M. (2015). Note on algebras which are sums of two *PI* subalgebras. J. Algebra Appl., 14 no 10., 1550149, 10 pp.

Kępczyk, M. (2016). A note on algebras which are sums of two subalgebras. Canad. Math. Bull., 59 no. 2, 340–345.

Kępczyk, M. (2017). A ring which is a sum of two PI subrings is always a PI ring. Israel J. Math., 221 no. 1, 481–487.

Kępczyk, M. (2020). Rings which are sums of PI subrings. J. Algebra Appl., 19 no. 8, 2050157, 12 pp.

Kępczyk, M. (2021). Note on rings which are sums of a subring and an additive subgroup. Appl. Algebra Engrg. Comm. Comput., 32 no. 3, 359–364.

Kępczyk, M., i Puczyłowski, E. (1996). On radicals of rings which are sums of two subrings. Arch. Math., 66, 8–12.
Kępczyk, M., i Puczyłowski, E. (2001). Rings which are sums of two subrings satisfying polynomial identities. Comm. Algebra, 29, 2059–2065.
Kegel, O. (1962/63). Zur Nilpotenz gewisser assoziativer Ringe. Math. Ann., 149, 258–260.
Kelarev, A. (1993). On semigroup graded PI-algebras. Semigroup Forum, 47, 294–298.
Kelarev, A., i McConnell, N. (1995). Two version of graded rings. Publ. Math. Debrecen, 47, 219–227.
Lam, T. (1991). A first course in noncommutative rings (131). New York: Springer-Verlag, BerlinHeidelberg-New York.
Lanski, C. (1990). Can a semi-prime ring be a finite union of right annihilators? Canad. Math. Bull. Vol., 33 no. 1, 126–128.
Neumann, B. (1954). Groups covered by permutable subsets. J. Lond. Math. Soc., 29, 236–248.
Puczyłowski, E. (1999). Some results and questions on nil rings. Mat. Contemp., 16, 265–280.
Salwa, A. (1996). Rings that are sums of two locally nilpotent subrings. Comm. Algebra, 24 no. 12, 3921–3931.
Teply, M., Turman, E. i Quesada, A. (1980). On semisimple semigroup rings. Proc. Amer. Math. Soc., 79, 157–163.
Weissglass, J. (1973). Semigroup rings and semilattice sums of rings. Proc. Amer. Math. Soc., 3, 471–478.


Politechnika
Białostocka