Uniwersytet Warszawski
Wydział Matematyki, Informatyki i Mechaniki

Karol Pryszczepko

Przemienne pierścienie filialne

rozprawa doktorska

Promotor
dr hab. Ryszard Andruszkiewicz
Wydział Matematyki i Informatyki
UwB

Wrzesień 2014

Oświadczenie autora rozprawy:
oświadczam, że niniejsza rozprawa została napisana przeze mnie samodzielnie.

.....	.....
data	*podpis autora rozprawy*

Oświadczenie promotora rozprawy:
niniejsza rozprawa jest gotowa do oceny przez recenzentów.

.....	.....
data	*podpis promotora rozprawy*

Streszczenie

W rozprawie rozważane są tylko pierścienie łączne, zwane dalej pierścieniami. Dobrze wiadomo, że w klasie pierścieni relacja bycia ideałem nie jest przechodnia. Celem rozprawy jest rozważenie szeregu zagadnień związanych z pierścieniami w których ta relacja zachodzi. Pierścienie te dalej będziemy nazywali filialnymi. Motywacją do naszych badań były prace między innymi: Kruse, Andrijanowa, Puczyłowskiego.

W pierwszym rozdziale rozprawy przypominamy i uzupełniamy potrzebne dalej wiadomości o grupach, pierścieniach i klasach radykalnych.

W drugim rozdziale przedstawiamy wyniki dotyczące filialnych pierścieni β-radykalnych. W szczególności uzupełniamy pewne luki w klasyfikacji H-pierścieni (tj. pierścieni, w których każdy podpierścień jest ideałem) podanej przez Kruse i Andrijanowa, poprzez podanie pełnej klasyfikacji pierścieni z prawie zerowym mnożeniem ograniczonego wykładnika.

W rozdziale trzecim podajemy pełną klasyfikację przemiennych, filialnych pierścieni zredukowanych dowodząc, że są to pewne podpierścienie produktu ciał liczb p-adycznych. Niezbędne przy tym okazuje się udowodnione przez nas twierdzenie, zgodnie z którym, każdy przemienny, filialny pierścień zredukowany jest ideałem w pewnym przemiennym, filialnym, zredukowanym pierścieniu z jedynką.

W rozdziale czwartym przedstawiamy konstrukcję i własności ważnych przykładów pierścieni filialnych, tj. pierścieni Kruse i Andrijanowa. Podajemy tam również klasyfikacje pewnych ich rozszerzeń, które odegrają kluczową rolę w opisie filialnych, przemiennych pierścieni noetherowskich.

Rozdział piąty zawiera wyniki dotyczące pierścieni filialnych o nietorsyjnym nil-radykale.

W kolejnych dwóch rozdziałach przedstawiamy pełną klasyfikację przemiennych, torsyjnych pierścieni filialnych i przemiennych filialnych pierścieni noetherowskich.

Ostatni, ósmy rozdział poświęcony jest problemowi dołączania jedynki do pierścienia filialnego. Dowodzimy tam, że nie każdy pierścień filialny jest ideałem w filialnym pierścieniu z jedynką, konstruując minimalny przykład takiego pierścienia. Jest odpowiedź na pytanie postawione, przez autora, na konferencji „Radicals of rings and related topics" w Warszawie w 2009 roku.

SŁOWA KLUCZOWE: ideał, H-pierścień, pierścień filialny, pierścień z prawie zerowym mnożeniem, nil-radykał, pierścień silnie regularny

KLASYFIKACJA TEMATYCZNA PRACY: 13B02, 13C05, 16D25, 16N40

Abstract

In this work we consider only associative rings which we call simply rings. It is well known that the relation of being an ideal is not transitive in the class of all associative rings. The aim of the dissertation is to consider a number of issues connected with the rings in which the transitive property does hold. These rings will be called filial. Our research is motivated, inter alia, by the papers of Kruse, Andrijanow and Puczyłowski.

In the first chapter of dissertation, we recall and extend necessary informations about groups, rings and radical classes.

In the second chapter of the thesis we present our results on filial β-radical rings. In particular we fulfill the gaps in the classification of H-rings (i.e. rings in which each subring is an ideal), given by Kruse and Andrijanow. Namely we give the classification of almost null rings with the bounded exponent of additive group.

In the third chapter we give a full classification of commutative reduced filial rings by proving that they are some specific subrings of product of p-adic integers. It turned out that to show this it is necessary to use our theorem saying that every reduced filial ring is an ideal in a reduced filial ring with an identity.

In the fourth chapter we present the construction and properties of important examples of filial rings i.e. Kruse and Andrijanow rings. Additionally we give some classification theorems for extensions of these ring, which play a central role in the description of the commutative filial noetherian rings.

In the fifth chapter we collect our results concerning filial rings with non-torsion nil radical.

In the next two chapters we present a full classification of commutative torsion filial rings and commutative noetherian filial rings.

The last, eight chapter is devoted to a problem of adjoining an identity to a filial ring. In this section we prove that not every filial ring is an ideal in filial ring with an identity, by constructing a minimal example. This is the answer to the question posed by the author at the conference „Radicals of rings and related topics" in Warsaw, Poland in 2009.

KEYWORDS: ideal, H-ring, filial ring, almost null ring, nil radical, strongly regular ring

2010 MATHEMATIC SUBJECT CLASSIFICATION: 13B02, 13C05, 16D25, 16N40

Spis treści

Wstęp

Rozprawa dotyczy teorii ideałów pierścieni łącznych. Jej głównym celem jest rozważenie szeregu zagadnień związanych z następującym ogólnym pytaniem

Które pierścienie posiadają własność „przechodniości bycia ideałem"? Innymi słowy, dla jakich pierścieni R ideał ideału pierścienia R jest ideałem pierścienia R?

Problem ten został sformułowany przez F. Szásza w monografii [47] w roku 1974 (Problem 9). To naturalne pytanie związane było z pewnymi ogólnymi zagadnieniami dotyczącymi teorii radykałów (por. [48]). Analogiczna własność badana była również dla innych ważnych struktur algebraicznych. Na przykład, w teori grup intensywnie badane są tak zwane t-grupy, tj. grupy w której każda subnormalna podgrupa jest normalna (por. [19, 40]). Warto wspomnieć, że pewne wyniki dotyczące tego zagadnienia uzyskano również dla struktur niełącznych, np. algebr Liego (por. [50]).

Pierścienie, w których relacja bycia ideałem jest przechodnia badała jako pierwsza G. Ehrlich w [21] i nazwała je **filialnymi**. Silną motywacją do badania pierścieni filialnych jest to, że stanowią one bardzo naturalne uogólnienie tak zwanych H-pierścieni, czyli łącznych pierścieni, w których każdy podpierścień jest ideałem. Klasa ta była wnikliwie badana przez wielu autorów, spośród których najważniejsze rezultaty otrzymali L. Rédei [43], V. I. Andrijanow [2, 3] i R. L. Kruse [35, 36]. Dzięki wysiłkom tych autorów i użyciu niezwykle skomplikowanych technik, udało się sprowadzić problem klasyfikacji H-pierścieni do opisu nil-H-p-pierścieni, gdzie p jest liczbą pierwszą. W opisie tej ostatniej klasy występuje kilkanaście typów pierścieni opisanych przez skomplikowane relacje na generatorach z użyciem wielu parametrów. Nie rozstrzygnięto jednak problemu izomorfizmu takich pierścieni z różnych klas, a nawet z tej samej klasy w zależności od użytych parametrów.

W tym kontekście powstaje naturalne pytanie o zastosowanie przemiennych pierścieni filialnych w teorii pierścieni łącznych. Przypomnijmy, że podpierścień A pierścienia R jest n-osiągalny, jeżeli dla pewnych podpierścieni $A = A_0, A_1, \cdots, A_n = R$ pierścienia R, A_i jest ideałem w A_{i+1} dla $i = 0, 1, \ldots, i-1$, zaś podpierścień A jest dokładnie n-osiągalny jeśli dodatkowo A nie jest $n-1$ osiągalny w R. Problem konstrukcji podpierścieni dokładnie n-osiągalnych w danym pierścieniu odgrywa fundamentalną rolę w teorii radykałów, a mianowicie przy badaniu stabilizacji tak zwanych łańcuchów Kurosza (por. [20] i [5, 7, 11]). W pracy [7] udowodniono, że jeśli dziedzina całkowitości R nie jest filialna, to można w niej znaleźć podpierścienie dokładnie n-osiągalne dla dowolnego naturalnego n. Wykorzystując ten fakt można konstruować łańcuchy Kurosza (w klasie pierścieni łącznych, niekoniecznie przemiennych) stabilizujące się na dowolnym skończonym kroku (por. [20], [7]). Wspomniane badania, zapoczątkowane

przez pionierską pracę [20] i kontynuowane w [7] należą do najbardziej wartościowych i cenionych w teorii radykałów. Użycie pierścieni filialnych i ich własności pozwoliło na rozwiązanie problemów związanych z omawianą tematyką. Jak do tej pory nie udało się osiągnąć podobnej sztuki przy użyciu pierścieni nieprzemiennych.

W roku 1988 A. D. Sands w [45] badał filialność różnych typów pierścieni. Co ciekawe, w przeciwieństwie do Ehrlich, zajmował się on także jednostronną filialnością tzn. relacją przechodniości bycia ideałem lewostronnym. Niemal równolegle G. Tzinntzis w [49] użył pierścieni filialnych w badaniach nad pierścieniami idempotentnymi. Różne aspekty tej problematyki podjął także S. Veldsman w [51]. Badanie lewostronnej filialności pierścieni i algebr było kontynuowane przez M. Filipowicz i E. R. Puczyłowskiego w pracach [23, 24, 25]. Uzyskali oni tam wiele cennych i nowych rezultatów oraz wyodrębnili bardzo ważną podklasę pierścieni filialnych jaką tworzą pierścienie silnie regularne. Wynikiem ich wysiłków jest niemal kompletna klasyfikacja lewostronnie filialnych algebr nad ciałami.

Bezpośrednią kontynuacją pracy Ehrlich, był artykuł [6] R. R. Andruszkiewicza i Puczyłowskiego z roku 1988, w którym autorzy podawali dalsze przykłady, własności i charakteryzacje pierścieni filialnych. W 2003 roku Andruszkiewicz w [8] podał kompletną klasyfikację filialnych dziedzin całkowitości, dowodząc że są one pewnymi, konkretnie określonymi, podpierścieniami produktu ciał liczb p-adycznych. Następnym naturalnym krokiem w poszukiwaniu opisu przemiennych pierścieni filialnych było zbadanie przemiennych pierścieni zredukowanych. Tematyce tej poświęcona jest praca [10], która podaje warunki konieczne i dostateczne na to aby przemienny beztorsyjny pierścień zredukowany był filialny.

Celem niniejszej rozprawy doktorskiej jest kontynuacja badań przemiennych pierścieni filialnych. W szczególności formułujemy i dowodzimy twierdzenie klasyfikacyjne dla przemiennych, zredukowanych pierścieni filialnych. To twierdzenie okazuje się być analogiczne do twierdzenia opisującego filialne dziedziny całkowitości charakterystyki zero (por. Theorem 8.8., [8]), jednak warto podkreślić, że nie jest to automatyczne uogólnienie znanego już wyniku, i w dowodzie wymaga użycia zupełnie innych metod. Ponadto w pracy tej podajemy, wraz z uzasadnieniem pełną klasyfikację przemiennych noetherowskich pierścieni filialnych. Niezbędne przy tym okazuje się głębokie zbadanie struktury pewnych klas H-pierścieni (por. [35, 2]). Omawiane wyniki uzyskujemy wykorzystując różnorodne metody współczesnej algebry np. teorię radykałów, teorię rozszerzeń pierścieni.

Rozdział pierwszy ma charakter wprowadzający, przedstawiamy w nim najważniejsze definicje i fakty dotyczące teorii grup, teorii liczb i teorii pierścieni, które będą wykorzystywane w dalszej części pracy. Na szczególna uwagę zasługuje przedstawiony tu ogólny schemat badania własności pierścieni przy użyciu różnorodnych klas radykalnych (por. paragraf 1.3.2).

Rozdział drugi dotyczy filialnych pierścieni radykalnych w sensie Baera. Od dawna wiadomo (por. [4], Stwierdzenie 3.2.9), że są one nil-H-pierścieni. Bardzo ważną podklasę w rodzinie nil-H-pierścieni stanowią pierścienie z prawie zerowym mnożeniem ([35], Definition 2.1). Zostały one odkryte przez Kruse i niezależnie przez Andrijanowa. Znaleźli oni pewne charakteryzacje tych pierścieni, które jednak są bardzo dalekie od opisu z dokładnością do izomorfizmu. W tym rozdziale dowodzimy szeregu

twierdzeń klasyfikujących pierścienie z prawie zerowym mnożeniem. Jest to istotne rozwinięcie i uzupełnienie wyników uzyskanych przez Kruse i Andrijanowa. Podajemy, między innym, kompletną klasyfikację pierścieni z prawie zerowym mnożeniem ograniczonego wykładnika oraz konstruujemy wiele przykładów takich pierścieni. Dowodzimy ponadto, że pierścienie z prawie zerowym mnożeniem są to dokładnie podpierścienie pewnych uniwersalnych pierścieni (por. Wniosek 2.49).

Rozdział trzeci zawiera kompletną klasyfikację przemiennych filialnych pierścieni zredukowanych. Jest to istotne i nietrywialne rozwinięcie idei zapoczątkowanych w pracy Andruszkiewicza [8]. Warto tutaj podkreślić, że uzyskane tam wyniki dla filialnych dziedzin, nie przenoszą się automatycznie na pierścienie zredukowane. W tym rozdziale dowodzimy również, że każdy przemienny filialny pierścień zredukowany jest ideałem w pewnym przemiennym filialnym pierścieniu zredukowanym z jedynką. Jest to kluczowy wynik, wykorzystywany w dowodzie twierdzenia klasyfikacyjnego. W rozdziale tym konstruujemy również przykład $\mathbb{S}$-półprostego, przemiennego, zredukowanego, pierścienia filialnego z jedynką, który nie zawiera ideału będącego dziedziną.

Rozdział czwarty dotyczy ogólnych własności pierścieni filialnych. Przedstawiamy w nim, niektóre ich charakteryzacje i przykłady oraz pewne zaawansowane konstrukcje. Najistotniejsze, z punktu widzenia klasyfikacji pierścieni filialnych, są tu konstrukcje pierścieni Andrijanowa oraz (uogólnionych) pierścieni Krusego. Konstrukcje te opierają się o pewne nietrywialne, ogólne przykłady rozszerzeń pierścieni. Udowodnione w tym rozdziale fakty pozwolą nam, między innymi, sklasyfikować noetherowskie pierścienie filialne.

Rozdział piąty dotyczy przemiennych pierścieni filialnych o nietorsyjnym nil-radykale. Wykazujemy w nim, że takie pierścienie to dokładnie rozszerzenia pierścieni postaci $A \oplus B$, gdzie A jest przemiennym, filialnym nil-pierścieniem, natomiast B jest przemiennym pierścieniem silnie regularnym, przez pierścień $m\mathbb{Z}$ dla pewnej liczby całkowitej m. Dalej badamy pewne własności takich rozszerzeń.

Rozdział szósty i siódmy zawierają, odpowiednio, twierdzenie klasyfikujące torsyjne przemienne pierścienie filialne i twierdzenia klasyfikujące przemienne noetherowskie pierścienie filialne.

W ostatnim, ósmym rozdziale dyskutujemy problem dołączania jedynki do pierścienia filialnego. Konstruujemy minimalny (ze względu na moc) przykład pierścienia filialnego, który nie zanurza się jako ideał w żaden pierścień filialny z jedynką. Jest to odpowiedź na pytanie postawione na konferencji „Radicals of rings and related topics" w Warszawie w 2009, (por. [51]).

Wiele z prezentowanych w tej pracy wyników zostało już opublikowanych (por. [12, 13, 14, 15, 17]) i referowanych na międzynarodowych konferencjach.

Podziękowania Pragnę podziękować promotorowi doktorowi habilitowanemu Ryszardowi Andruszkiewiczowi za cierpliwość, wyrozumiałość, poświęcony czas i liczne dyskusje.

Rozdział 1

Preliminaria

Oznaczenia używane w tej pracy nie odbiegają od powszechnie przyjętych. Dla kompletności podamy najważniejsze z nich.

Przez $\mathbb{Z}$ i $\mathbb{Q}$ oznaczamy odpowiednio pierścień liczb całkowitych i ciało liczb wymiernych. Dodatnie liczby całkowite nazywamy liczbami naturalnymi, zbiór wszystkich liczb naturalnych oznaczamy przez $\mathbb{N}$, ponadto przez $\mathbb{N}_0$ oznaczamy zbiór wszystkich nieujemnych liczb całkowitych i symbolem $\mathbb{P}$ oznaczamy zbiór wszystkich liczb pierwszych oraz dla $p \in \mathbb{P}$ symbolem $\mathbb{Z}_p$ oznaczamy ciało p-elementowe, przy czym $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$. Największy wspólny dzielnik liczb całkowitych a, b oznaczamy przez $NWD(a, b)$.

Pierwszy rozdział pracy ma charakter wprowadzający. Zawiera on niezbędne definicje i fakty dotyczące teorii grup i pierścieni oraz teorii liczb, które będą wykorzystywane w dalszej części pracy.

1.1 Teoria grup

Dla podzbioru A grupy G przez $\langle A \rangle$ oznaczamy podgrupę grupy G generowaną przez A. Jeżeli H jest podgrupą grupy G, to piszemy $H \leq G$. Pisząc, że H jest p-grupą zawsze zakładamy, że p jest liczbą pierwszą. Dla dowolnej grupy abelowej G oznaczamy $G_p = \{x \in G \ : \ p^n x = 0 \text{ dla pewnego } n \in \mathbb{N}\}$ dla $p \in \mathbb{P}$ oraz $\mathbb{T}(G) = \{x \in G \ : \ o(x) \in \mathbb{N}\}$, gdzie $o(x)$ oznacza rząd elementu x. Jest jasne, że jeżeli grupa G jest torsyjna, to $G = \bigoplus_{p \in \mathbb{P}} G_p$.

Lemat 1.1. *Niech a będzie takim elementem grupy abelowej A, że $o(a)$ jest liczbą bezkwadratową. Wówczas $\langle ka \rangle = \langle k^2 a \rangle$ dla dowolnego $k \in \mathbb{Z}$.*

Dowód. Ponieważ $(k^2, o(a)) = (k, o(a))$, więc $\frac{o(a)}{(k^2, o(a))} = \frac{o(a)}{(k, o(a))}$, czyli $o(k^2 a) = o(ka)$. Ale $k^2 a \in \langle ka \rangle$, więc $\langle ka \rangle = \langle k^2 a \rangle$. □

Stwierdzenie 1.2. *Niech x będzie elementem rzędu p w p-grupie $\langle a \rangle$. Wówczas dla dowolnej grupy abelowej B i dla $A = \langle a \rangle \oplus B$ mamy*

$$o(a) = max\{o(v) \ : \ v \in A_p \ i \ x \in \langle v \rangle\}.$$

Dowód. Załóżmy, że istnieje $v_0 \in A_p$ takie, że $x \in \langle v_0 \rangle$ i $o(v_0) = p^t > p^r = o(a)$. Ponieważ $o(x) = p$, więc $x = Up^{t-1}v_0$ dla pewnego $U \in \mathbb{Z}$, $p \nmid U$. Ale $v_0 = ka + b$ dla pewnych $k \in \mathbb{Z}$ oraz $b \in B$. Wobec tego $p^{t-1}v_0 \in B$, więc $x \in B$, sprzeczność. Zatem $o(a) = max\{o(v) : v \in A_p \text{ i } x \in \langle v \rangle\}$. □

Niech a będzie elementem grupy abelowej A i niech $p \in \mathbb{P}$. Mówimy, że element a ma **p-wysokość** α, jeśli $\alpha = max\{\beta \in \mathbb{N}_0 : p^\beta x = a \text{ dla pewnego } x \in A\}$.

Lemat 1.3. *Niech A będzie grupą abelową i niech $x \in A$ będzie elementem rzędu p, skończonej p-wysokości. Wówczas istnieją podgrupy B, C w A takie, że $x \in B$, B jest cykliczna oraz $A = B \oplus C$.*

Dowód. Wniosek 27.2 z [28]. □

Lemat 1.4. *Niech A będzie grupą abelową i niech $b \in A$ oraz $C \leq A$ będą takie, że $A = \langle b \rangle \oplus C$ i dla każdego $U \in \mathbb{Z}$ z tego, że $Ub = 0$ wynika $UC = 0$. Wówczas $A = \langle b - c \rangle \oplus C$ dla dowolnego $c \in C$.*

Dowód. Weźmy dowolne $a \in A$. Wtedy $a = kb + x$ dla pewnych $k \in \mathbb{Z}$ i $x \in C$. Zatem $a = k(b - c) + (x + kc) \in \langle b - c \rangle + C$. Stąd $A = \langle b - c \rangle + C$. Weźmy dowolne $U \in \mathbb{Z}$ takie, że $U(b - c) \in C$. Wtedy $Ub \in C \cap \langle b \rangle = 0$, czyli $Ub = 0$. Wobec tego $Uc = 0$ i $U(b - c) = 0$. Zatem $\langle b - c \rangle \cap C = 0$ i $A = \langle b - c \rangle \oplus C$. □

Twierdzenie 1.5 (Prüfer, Baer, [41])**.** *Grupa abelowa ma skończony wykładnik wtedy i tylko wtedy, gdy jest izomorficzna z sumą prostą skończonych grup cyklicznych, których rzędy są ograniczone przez pewną liczbę naturalną.*

Twierdzenie 1.6 (Walker)**.** *Niech F, F', G, H będą takimi grupami abelowymi, że $F \oplus G \cong F' \oplus H$. Jeżeli $F \cong F'$ i grupa F jest skończenie generowana, to $G \cong H$.*

Dowód. Wniosek 8 z [52]. □

Definicja 1.7. Niech $p \in \mathbb{P}$. Grupę

$$\mathbb{Z}_{p^\infty} = \langle x_1, x_2, \ldots : px_1 = 0, px_{i+1} = x_i, \text{ dla dowolnego } i \in \mathbb{N} \rangle,$$

nazywamy **quasicykliczną p-grupą**.

Kolejny lemat nie wymaga dowodu.

Lemat 1.8. *Niech $p \in \mathbb{P}$ i niech A będzie grupą abelową nieskończonego rzędu zawierającą taki ciąg elementów $x_1, x_2, \ldots$, że $o(x_1) = p$ oraz $x_n = px_{n+1}$, dla wszystkich $n \in \mathbb{N}$. Wówczas podgrupa $\langle x_1, x_2, x_3, \ldots \rangle$ grupy A jest izomorficzna z grupą $\mathbb{Z}_{p^\infty}$.*

Przypomnijmy, że grupę abelową G nazywamy **grupą podzielną**, jeżeli dla dowolnych $n \in \mathbb{N}$ i $a \in G$ równanie $nx = a$ ma rozwiązanie w G.

Twierdzenie 1.9. *Podgrupa podzielna grupy abelowej wydziela się w niej jako składnik prosty.*

Dowód. Twierdzenie 21.2 z [28]. □

Twierdzenie 1.10 (Twierdzenie klasyfikacyjne dla grup podzielnych)**.** *Każda podzielna grupa abelowa rozkłada się na sumę prostą podgrup izomorficznych z grupą addytywną ciała $\mathbb{Q}$ lub z grupami $\mathbb{Z}_{p^\infty}$, niewykluczone, że dla różnych $p \in \mathbb{P}$.*

Dowód. Stwierdzenie 4.1.5 z [44]. □

Niech $A, B \leq G$. Mówimy, że B jest **minimalną podzielną podgrupą zawierającą** A, jeżeli B jest grupą podzielną nie zawierającą właściwej podzielnej podgrupy zawierającej A.

Twierdzenie 1.11 (Kulikov)**.** *Niech A będzie podgrupą podzielnej grupy D. Wtedy w D istnieje minimalna podgrupa podzielna zawierająca grupę A. Każde dwie minimalne podgrupy podzielne zawierające A są izomorficzne nad A.*

Dowód. Twierdzenie 24.4 z [28]. □

Podzielnym nakryciem grupy abelowej A nazywamy taką grupę podzielną $E(A)$, w której A jest istotną podgrupą.

Twierdzenie 1.12. *Każda grupa abelowa A ma podzielne nakrycie $E(A)$, które jest wyznaczone z dokładnością do izomorfizmu nad A.*

Dowód. Stwierdzenie 4.3.5 z [44]. □

Dla dowolnej grupy abelowej A przez $D(A)$ oznaczamy największą podzielną podgrupę grupy A. Jeśli $D(A) = 0$, to mówimy, że A jest **grupą zredukowaną**.

1.1.1 Prawie podzielne grupy abelowe

Mówimy, że grupa abelowa A jest **prawie podzielna**, jeżeli $kA = k^2A$ dla każdego $k \in \mathbb{Z}$.

Uwaga 1.13. Dla dowolnej grupy abelowej A następujące warunki są równoważne:

(i) grupa A jest prawie podzielna,

(ii) $kA = k^2A$ dla każdego $k \in \mathbb{N}$,

(iii) $pA = p^2A$ dla każdego $p \in \mathbb{P}$.

W szczególności p-grupa abelowa A jest prawie podzielna wtedy i tylko wtedy, gdy $pA = p^2A$. Oczywiście każda abelowa grupa podzielna jest prawie podzielna. Łatwo też zauważyć, że każda beztorsyjna grupa prawie podzielna jest podzielna.

Uwaga 1.14. Proste sprawdzenie pokazuje, że klasa wszystkich grup prawie podzielnych jest zamknięta na obrazy homomorficzne i sumy proste, lecz nie jest zamknięta na rozszerzenia, bo na przykład dla $p \in \mathbb{P}$ grupa cykliczna rzędu p^2 nie jest prawie podzielna, a jest rozszerzeniem grupy cyklicznej rzędu p przez grupę cykliczną rzędu p.

Dowody następnych dwóch lematów są natychmiastowe.

Lemat 1.15. *Grupa abelowa A jest prawie podzielna wtedy i tylko wtedy, gdy grupy $A/\mathbb{T}(A)$ i $\mathbb{T}(A)$ są prawie podzielne.*

Lemat 1.16. *Zredukowana abelowa grupa torsyjna A jest prawie podzielna, wtedy i tylko wtedy, gdy $pA_p = 0$ dla każdego $p \in \mathbb{P}$.*

Następne stwierdzenie daje pewną charakteryzację grup prawie podzielnych.

Stwierdzenie 1.17. *Dla dowolnej grupy abelowej A następujące warunki są równoważne:*

(i) grupa A jest prawie podzielna,

(ii) istnieją grupa podzielna D i grupa zredukowana B takie, że $A \cong D \oplus B$ oraz grupa $B/\mathbb{T}(B)$ jest podzielna i $pB_p = 0$ dla każdego $p \in \mathbb{P}$.

Dowód. $(i) \Rightarrow (ii)$. Istnieje zredukowana podgrupa $B \leq A$ taka, że $A = D(A) \oplus B$. Stąd grupa B jest prawie podzielna. Z Uwagi 1.13 i Lematu 1.15 wynika, że grupa $B/\mathbb{T}(B)$ jest podzielna. Ponadto na mocy Lematu 1.15, grupa $\mathbb{T}(B)$ jest prawie podzielna i zredukowana, więc na podstawie Lematu 1.16, $pB_p = 0$ dla każdego $p \in \mathbb{P}$.

$(i) \Leftarrow (ii)$. Z Lematu 1.16 wynika, że grupa $\mathbb{T}(B)$ jest prawie podzielna. Zatem na mocy Lematu 1.15, grupa B jest prawie podzielna. Wobec tego z Uwagi 1.14 wynika, że grupa A jest prawie podzielna. □

Struktura abelowych grup prawie podzielnych jest bardzo skomplikowana, o czym świadczy następujący przykład.

Przykład 1.18. Niech Π będzie nieskończonym podzbiorem zbioru $\mathbb{P}$ i niech X będzie nieskończonym podzbiorem Π. Niech $G = \prod_{p\in\Pi} C_p$, gdzie $C_p = \langle c_p \rangle$ jest grupą p-elementową dla każdego $p \in \Pi$. Niech $\mathbb{1}_X = (a_p)_{p\in\Pi} \in G$ będzie takie, że $a_p = \begin{cases} 0 & \text{jeżeli } p \notin X \\ c_p & \text{jeżeli } p \in X, \end{cases}$ Niech $A(X) = \{a \in G \,:\, na \in \langle \mathbb{1}_X \rangle \text{ dla pewnego } n \in \mathbb{N}\}$. Wtedy $A(X) \leq G$, $\mathbb{T}(G) = \bigoplus_{p\in\Pi} C_p \subseteq A(X)$. Ponadto grupa $G/\mathbb{T}(G)$ jest beztorsyjna i podzielna, jest więc przestrzenią liniową nad ciałem $\mathbb{Q}$. Ponieważ $|X| = \infty$, więc $\mathbb{1}_X + \mathbb{T}(G) \neq 0 + \mathbb{T}(G)$ i stąd $lin_{\mathbb{Q}}(\mathbb{1}_X + \mathbb{T}(G)) \cong \mathbb{Q}$ oraz $lin_{\mathbb{Q}}(\mathbb{1}_X + \mathbb{T}(G)) = A(X)/\mathbb{T}(G)$. Zatem z Lematu 1.15 wynika, że grupa $A(X)$ jest prawie podzielna.

Niech teraz Y będzie takim nieskończonym podzbiorem Π, że $X \setminus Y$ lub $Y \setminus X$ jest zbiorem nieskończonym. Pokażemy, że wówczas $A(X) \ncong A(Y)$, gdzie $A(Y)$ jest grupą skonstruowaną w sposób analogiczny jak $A(X)$. Bez zmniejszania ogólności możemy założyć, że $|Y \setminus X| = \infty$. Załóżmy, że $f\colon A(X) \to A(Y)$ jest izomorfizmem grup. Wtedy $f(\mathbb{T}(A(X))) = \mathbb{T}(A(Y))$, czyli $f(\mathbb{T}(G)) = \mathbb{T}(G)$. Ponadto, dla każdego $p \in Y \setminus X$, $\mathbb{1}_X \in pA(X)$, więc $f(\mathbb{1}_X) \in pA(Y)$. Dalej, istnieją $n \in \mathbb{N}$, $k \in \mathbb{Z}$ takie, że $nf(\mathbb{1}_X) = k\mathbb{1}_Y$. Zatem dla każdego $p \in Y \setminus X$, $k\mathbb{1}_Y \in pA(Y)$, skąd po uwzględnieniu p-tych współrzędnych, $p \mid k$. Ale $|Y \setminus X| = \infty$, więc $k = 0$ i w konsekwencji $n\mathbb{1}_X = 0$, sprzeczność.

Oczywiście istnieją parami rozłączne i nieskończone podzbiory $X_1, X_2, \ldots$ zbioru Π takie, że $\Pi = \bigcup_{i\in\mathbb{N}} X_i$. Dla niepustego podzbioru $I \subseteq \mathbb{N}$, niech $X_I = \bigcup_{i\in I} X_i$. Odnotujmy, że jeśli $I \neq J$ dla pewnych dwóch podzbiorów w $\mathbb{N}$, to jeden ze zbiorów $X_I \setminus X_J$ lub $X_J \setminus X_I$ jest nieskończony. Stąd grupy $A(X_I)$ dla $\emptyset \neq I \subseteq \mathbb{N}$ są parami nieizomorficzne i jest ich $2^{\aleph_0}$.

Wobec tego, istnieje co najmniej $2^{\aleph_0}$ nieizomorficznych rozszerzeń grupy $\bigoplus_{p\in\Pi} C_p$ przez grupę addytywną ciała $\mathbb{Q}$.

1.2 Teoria liczb

Prosty dowód następnego, technicznego lematu, wynika bezpośrednio z Twierdzenia Dirichleta o postępie arytmetycznym, jednak my podamy jego elementarny dowód.

Lemat 1.19. *Niech p będzie liczbą pierwszą i niech a, b będą liczbami całkowitymi, z których co najmniej jedna nie jest podzielna przez p. Wówczas istnieją względnie pierwsze liczby całkowite x i y takie, że $x \equiv a \pmod p$ i $y \equiv b \pmod p$.*

Dowód. Bez zmniejszenia ogólności możemy założyć, że $a, b \in \mathbb{Z}_p$ oraz $a \neq 0$. Jeśli $b = 0$, to wystarczy przyjąć $x = a + p$ i $y = p$, gdyż p nie dzieli a. Niech dalej $b \neq 0$. Ponieważ grupa multiplikatywna ciała $\mathbb{Z}_p$ jest cykliczna, więc istnieje $c \in \mathbb{Z}_p \setminus \{0\}$ takie, że $a \equiv c^k \pmod p$ i $b \equiv c^l \pmod p$ dla pewnych $k, l \in \mathbb{N}$. Stąd p nie dzieli c. Niech $x = c^k + (c+1)p$ i $y = c^l$. Wtedy $x \equiv a \pmod p$ i $y \equiv b \pmod p$. Gdyby liczby x i y nie były względnie pierwsze, to dla pewnej liczby pierwszej q mielibyśmy, że $q \mid c^l$ i $q \mid c^k + (c+1)p$. Stąd $q \mid c$, a więc $q < p$. Zatem $q \mid (c+1)p$, skąd $q \mid c+1$. Ale $q|c$, więc $q|(c+1) - c$, czyli $q \mid 1$ i mamy sprzeczność. □

Stwierdzenie 1.20. *Niech p będzie nieparzystą liczbą pierwszą i niech $A, F, V_1, V_2 \in \mathbb{Z}$ będą takie, że $p \nmid F^2 - 4A$. Wtedy*

$$\{X^2 + FXY + AY^2 + V_1X + V_2Y \ : \ X, Y \in \mathbb{Z}_p\} = \mathbb{Z}_p.$$

Dowód. Udowodnimy najpierw, że $\{X^2 + FXY + AY^2 \ : \ X, Y \in \mathbb{Z}_p\} = \mathbb{Z}_p$. Ponieważ $p > 2$, więc $\frac{1}{2} \in \mathbb{Z}_p$ oraz dla dowolnych $X, Y \in \mathbb{Z}_p$ mamy

$$X^2 + FXY + AY^2 = \left(X + \frac{F}{2}Y\right)^2 - (F^2 - 4A)\left(\frac{Y}{2}\right)^2,$$

wobec tego wystarczy pokazać, że $\{U^2 - \Delta V^2 \ : \ U, V \in \mathbb{Z}_p\} = \mathbb{Z}_p$ dla $\Delta = F^2 - 4A$. Weźmy dowolne $c \in \mathbb{Z}_p$ i rozważmy zbiory $A = \{U^2 - c \ : \ U \in \mathbb{Z}_p\}$ i $B = \{\Delta V^2 \ : \ V \in \mathbb{Z}_p\}$. Ponieważ zbiór $\{W^2 \ : \ W \in \mathbb{Z}_p\} = \{0^2, 1^2, \ldots, (\frac{p-1}{2})^2\}$ ma dokładnie $\frac{p+1}{2} > \frac{p}{2}$ elementów oraz $p \nmid \Delta$, więc zbiory A i B mają dokładnie po $\frac{p+1}{2}$ elementów. Zatem te zbiory nie mogą być rozłączne jako podzbiory zbioru $\mathbb{Z}_p$. Istnieją więc $U, V \in \mathbb{Z}_p$ takie, że $U^2 - c = \Delta V^2$, skąd $c = U^2 - \Delta V^2$.

Przejdźmy teraz do przypadku ogólnego, gdy V_1 i V_2 są dowolnymi liczbami całkowitymi. Ponieważ $p \nmid F^2 - 4A$, więc istnieją $a, b \in \mathbb{Z}$ takie, że $2a + Fb \equiv V_1 \pmod p$ i $Fa + 2Ab \equiv V_2 \pmod p$. Stąd dla dowolnych $X, Y \in \mathbb{Z}$ zachodzi $X^2 + FXY + AY^2 +$

$V_1X + V_2Y \equiv (X+a)^2 + F(X+a)(Y+b) + A(Y+b)^2 - (a^2 + Fab + Ab^2) \pmod{p}$. Wobec tego z pierwszej części dowodu mamy, że $\{X^2 + FXY + AY^2 + V_1X + V_2Y \ : \ X, Y \in \mathbb{Z}_p\} = \mathbb{Z}_p$. □

Przedstawimy teraz, ważną w dalszej części pracy, konstrukcję bezatomowej algebry Boole'a podzbiorów zbioru $\mathbb{N}$.

Przykład 1.21. Niech p będzie dowolną liczbą pierwszą. Niech $A_{i,k} = \{p^i t + k : t \in \mathbb{N}\}$ dla $i \in \mathbb{N}_0$ i $k \in \{0, 1, \ldots, p^i - 1\}$ i niech

$$\mathfrak{D}_p = \left\{ \bigcup_{j=1}^{n} X_j \ : \ n \in \mathbb{N} \text{ oraz } X_j = A_{i,k}, \text{ gdzie } i \in \mathbb{N}_0, \ k \in \{0, 1, \ldots, p^i - 1\} \right\}.$$

Łatwo jest sprawdzić, że dla $i_1 \leq i_2$ mamy

$$A_{i_1,k_1} \cap A_{i_2,k_2} = \begin{cases} A_{i_2,k_2} & \text{jeżeli } k_1 \equiv k_2 \pmod{p^{i_1}} \\ \emptyset & \text{jeżeli } k_1 \not\equiv k_2 \pmod{p^{i_1}}. \end{cases}$$

Każdy element $\mathfrak{D}_p$ może być zapisany jako rozłączna suma zbiorów $A_{i,k}$. Stąd dla dowolnych $X, Y \in \mathfrak{D}_p$, $X \cap Y \in \mathfrak{D}_p$. Ponadto $A'_{i,k} = \mathbb{N} \setminus A_{i,k} = \bigcup_{j \in \{0,1,\ldots,p^i-1\}, j \neq k} A_{i,j} \in \mathfrak{D}_p$ i ostatecznie $\mathfrak{D}_p$ jest algebrą Boole'a podzbiorów zbioru $\mathbb{N}$. Oczywiście dla każdego $A_{i,k}$ i dowolnego $j > i$ mamy $A_{i,k} \supsetneq A_{j,k}$, skąd wynika, że algebra $\mathfrak{D}_p$ jest bezatomowa.

Zauważmy, że dla różnych $p, q \in \mathbb{P}$, $\mathfrak{D}_p \neq \mathfrak{D}_q$. Rzeczywiście, gdyby tak nie było, to $\{pt \ : \ t \in \mathbb{N}\} \in \mathfrak{D}_q$, skąd $\{q^i s + k \ : \ s \in \mathbb{N}\} \subseteq \{pt \ : \ t \in \mathbb{N}\}$ dla pewnych $i \in \mathbb{N}_0$ i $k \in \{0, 1, \ldots, q^i - 1\}$. Zatem $2q^i + k, q^i + k \in \{pt \ : \ t \in \mathbb{N}\}$, więc $2q^i + k \equiv q^i + k \pmod{p}$, skąd $p \mid q^i$, sprzeczność.

1.3 Teoria pierścieni

Wszystkie rozważane w pracy pierścienie są łączne, ale nie muszą posiadać jedynki. Podzbiór S pierścienia R jest **podpierścieniem**, jeżeli jest on pierścieniem ze względu na te same działania dwuargumentowe co pierścień R. Dla dowolnego podzbioru X pierścienia R przez $[X]$ oznaczamy najmniejszy podpierścień w R zawierający X, przy czym jeśli $X = \{a_1, \ldots, a_n\}$, to zamiast $[\{a_1, \ldots, a_n\}]$ piszemy $[a_1, \ldots, a_n]$.

Podpierścień I pierścienia R nazywamy **ideałem** (**ideałem lewostronnym**), jeżeli $ri, ir \in I$ dla dowolnych $r \in R$, $i \in I$ ($ri \in I$ dla dowolnych $r \in R$, $i \in I$). Dla oznaczenia, że I jest ideałem (ideałem lewostronnym) pierścienia R piszemy $I \lhd R$ ($I <_l R$). **Ideał prawostronny** I pierścienia R definiujemy analogicznie i piszemy $I <_r R$. Najmniejszy ideał pierścienia R zawierający jego podzbiór X oznaczamy symbolem X_R, przy czym jeśli $X = \{a_1, \ldots, a_n\}$, to zamiast $\{a_1, \ldots, a_n\}_R$ piszemy $(a_1, \ldots, a_n)_R$ lub krótko $(a_1, \ldots, a_n)$. Ponadto, dla dowolnego $a \in R$ określamy $Ra = \{ra \ : \ r \in R\}$, przy czym jest jasne, że $Ra <_l R$. Ideał (ideał lewostronny, ideał prawostronny) I pierścienia R nazywamy **ideałem istotnym**, jeżeli $I \cap J \neq 0$ dla dowolnego ideału J pierścienia R. **Centrum pierścienia** R oznaczamy przez $Z(R)$.

Grupę addytywną pierścienia R oznaczmy przez R^+ i dla $a \in R$ rząd elementu a w grupie R^+ oznaczamy przez $o(a)$, przy czym $\mathbb{T}(R) = \mathbb{T}(R^+)$ i $\mathbb{T}(R) \lhd R$. Jeżeli R jest pierścieniem takim, że R^+ jest p-grupą (jest grupą torsyjną, jest grupą prawie podzielną), to mówimy krótko, że R jest **p-pierścieniem** (**pierścieniem torsyjnym**, **pierścieniem prawie podzielnym**, odpowiednio). Jeżeli R jest pierścieniem torsyjnym i p jest liczbą pierwszą, to używamy oznaczenia $R_p = \{a \in R : p^k a = 0 \text{ dla pewnego } k \in \mathbb{N}\}$ i wówczas $R_p \lhd R$ oraz $R = \bigoplus_{p\in\mathbb{P}} R_p$. Ponadto, $R(p^n) = \{a \in R : p^n a = 0\} \lhd R$ dla $n \in \mathbb{N}$. Mówimy, że element a pierścienia R jest **nilpotentny**, jeżeli $a^t = 0$ dla pewnej liczby naturalnej t, jeżeli zaś $a^2 = a$, to taki element a nazywamy **idempotentem**. Jeżeli pierścień R nie posiada niezerowych elementów nilpotentnych, to mówimy, że jest on **zredukowany**.

Jeśli X jest niepustym podzbiorem pierścienia R, to zbiory $l_R(X) = \{a \in R : aX = 0\}$ i $a_R(X) = \{a \in R : aX = Xa = 0\}$ nazywamy odpowiednio **lewostronnym anihilatorem** i **obustronnym anihilatorem** zbioru X w pierścieniu R. Łatwo sprawdzić, że $l_R(X) <_l R$ oraz $a_R(X)$ jest podpierścieniem pierścienia R.

Dla liczby naturalnej n, przez $\mathbb{Z}_n$ oznaczamy pierścień o elementach $0, 1, \ldots, n-1$ z naturalnymi działaniami modulo n. Dla dowolnej grupy abelowej $(M, +)$ przez M^0 oznaczamy pierścień z zerowym mnożeniem, którego grupą addytywną jest $(M, +)$.

Mówimy, że pierścień R jest **sumą podprostą** pierścieni $\{A_i\}_{i\in I}$, jeżeli R zawiera rodzinę ideałów $\{B_i\}_{i\in I}$ taką, że $\bigcap_{i\in I} B_i = 0$ oraz $R/B_i \cong A_i$ dla każdego $i \in I$.

Następne twierdzenie jest uogólnieniem znanego Twierdzenia Köthe-Dicksona o podnoszeniu idempotentów i będzie przez nas często stosowane.

Twierdzenie 1.22. *Niech I będzie nil-ideałem pierścienia R i niech $m \in \mathbb{N}$ będzie takie, że dla każdego $i \in I$ istnieje dokładnie jedno $j \in I$ takie, że $i = mj$. Jeżeli $a^2 - ma \in I$ dla pewnego $a \in R$, to istnieje $b \in a + I$ takie, że $b^2 = mb$.*

Dowód. Dla $f \in a + I$ niech $f' = f^2 - mf$. Wtedy $f' \in I$ oraz $ff' = f'f$. Wybierzmy f takie, że f' ma najmniejszy stopień nilpotentności s. Z założeń istnieje $g \in I$ stopnia nilpotentności s takie, że $f' = m^2 g$ oraz $ag = ga$. Niech $h = a - 2ag + mg$. Wtedy $h \in a + I$ oraz $h' = h^2 - mh = 4a^2g^2 - 3m^2g^2 - 4mag^2$. Jeśli $s > 1$, to $(h')^{s-1} = 0$, co przeczy minimalności s. Zatem $s = 1$ i $f^2 - mf = 0$. □

W pracy będziemy niejednokrotnie wykorzystywali następujący, dobrze znany, rezultat.

Stwierdzenie 1.23. *Niech I będzie ideałem pierścienia R takim, że $a_I(I) = 0$. Wówczas I jest ideałem istotnym w R wtedy i tylko wtedy, gdy $a_R(I) = 0$.*

Dowód. Lemat 1.1 z [9]. □

Dla dowolnego pierścienia R zbiór $End(R^+)$ wszystkich endomorfizmów grupy R^+ jest pierścieniem ze względu na naturalne dodawanie i składanie funkcji. Niech $End(R_R) = \{f \in End(R^+) : f(xy) = f(x)y \text{ dla wszystkich } x, y \in R\}$. Jest jasne, że $End(R_R)$ jest podpierścieniem pierścienia $End(R^+)$. Dowód następnego stwierdzenia jest natychmiastowy.

Stwierdzenie 1.24. *Jeżeli I jest ideałem istotnym pierścienia R takim, że $l_I(I) = 0$, to przekształcenie $f\colon R \to End(I_I)$ dane wzorem $f(a) = l_a$, gdzie $l_a(x) = ax$ dla $x \in I$, jest zanurzeniem pierścieni.*

Centroidem pierścienia R nazywamy zbiór $C(R) = \{f \in End(R^+) : f(xy) = xf(y) = f(x)y$ dla dowolnych $x, y \in R\}$. Proste sprawdzenie pokazuje, że dla dowolnego pierścienia R centroid $C(R)$ jest podpierścieniem pierścienia $End(R^+)$.

Uwaga 1.25. Niech C będzie przemiennym pierścieniem i niech A będzie C-algebrą. Na grupie $C^+ \times A^+$ określmy mnożenie wzorem

$$(c_1, a_1)(c_2, a_2) = (c_1c_2, c_1a_2 + c_2a_1 + a_1a_2)$$

dla dowolnych $c_1, c_2 \in C$, $a_1, a_2 \in A$. W ten sposób otrzymujemy nową C-algebrę, którą oznaczamy przez $C \boxplus A$. Zamiast (c, a) piszemy krótko $c + a$. Przy takim utożsamieniu, $C \subseteq Z(C \boxplus A)$, $A \lhd C \boxplus A$ oraz $(C \boxplus A)/A \cong C$. Jest jasne, że jeśli algebra A jest przemienna, to algebra $C \boxplus A$ również jest przemienna. Jeśli pierścień C posiada jedynkę 1, to zakładamy, że A jest unitarnym C-modułem i wówczas $(1, 0)$ jest jedynką algebry $C \boxplus A$. Ponadto, jeśli algebra A ma jedynkę, to $C \boxplus A \cong C \oplus A$. Odnotujmy, że każdy pierścień jest w naturalny sposób $\mathbb{Z}$-algebrą.

1.3.1 Definicja i podstawowe charakteryzacje pierścieni filialnych

Definicja 1.26. Powiemy, że pierścień R jest **filialny** (**lewostronnie filialny**), jeżeli dla dowolnych podpierścieni A, B pierścienia R z tego, że $A \lhd B$ i $B \lhd R$ ($A <_l B$ i $B <_l R$) wynika, że $A \lhd R$ ($A <_l R$).

Problem opisu pierścieni filialnych został postawiony przez F. Szásza w monografii [47]. Klasa pierścieni filialnych była badana przez wielu autorów. Systematyczne badania przemiennych pierścieni filialnych rozpoczęła Ehrlich w [21]. Znalazła ona, między innymi, następującą ważną charakteryzację przemiennych pierścieni filialnych, którą będziemy często wykorzystywali bez jej przywoływania.

Stwierdzenie 1.27 ([21], Theorem 4)**.** *Przemienny pierścień R jest filialny wtedy i tylko wtedy, gdy $\langle a\rangle + Ra = \langle a\rangle + \langle a^2\rangle + Ra^2$ dla każdego $a \in R$.*

Jej badania zainspirowały Andruszkiewicza i Puczyłowskiego do napisania dwóch ważnych prac. W pierwszej z nich [6] udowodnili oni, między innymi, następujące fakty:

Stwierdzenie 1.28 ([6], Proposition 2)**.** *Torsyjny pierścień R jest filialny wtedy i tylko wtedy, gdy R_p jest pierścieniem filialnym dla każdego $p \in \mathbb{P}$.*

Twierdzenie 1.29 ([6], Theorem 1)**.** *Pierścień R jest filialny wtedy i tylko wtedy, gdy $(a) = \langle a\rangle + (a)^2$ dla każdego $a \in R$.*

Druga praca [8], napisana przez Andruszkiewicza, zawiera kompletną klasyfikację filialnych dziedzin całkowitości. Część obserwacji tam przedstawionych będziemy wykorzystywali, dlatego teraz je przypomnimy.

Stwierdzenie 1.30 ([8], Proposition 2.5)**.** *Każde przemienna filialna dziedzina jest ideałem w filialnej dziedzinie całkowitości.*

Twierdzenie 1.31 ([8], Theorem 3.1)**.** *Dziedzina całkowitości R charakterystyki zero jest pierścieniem filialnym wtedy i tylko wtedy, gdy spełnione są następujące warunki:*

(i) $R = \langle 1 \rangle + pR$ *dla każdego* $p \in \mathbb{P}$.

(ii) dla każdego niezerowego $a \in R$*, istnieją* $n \in \mathbb{N}$ *i element odwracalny* $u \in R$ *takie, że* $a = mu$.

Twierdzenie 1.32 ([8], Theorem 3.3)**.** *Niech R będzie filialną dziedziną całkowitości charakterystyki zero. Wówczas:*

(i) dla każdego $m \in \mathbb{N}$, $R = \langle 1 \rangle + mR$,

(ii) dla każdego $I \lhd R$*, istnieje* $n \in \mathbb{N}_0$ *takie, że* $I = mR$.

W szczególności, każda filialna dziedzina całkowitości charakterystyki zero jest dziedziną ideałów głównych.

Dla filialnej dziedziny całkowitości R charakterystyki zero, niech:

$$\Pi(R) = \{p \in \mathbb{P} \ : \ p \cdot 1 \text{ jest nieodwracalne w } R\}. \tag{1.1}$$

Dla dowolnego podzbioru $X \subseteq \mathbb{N}$, niech $S(X)$ będzie najmniejszym multiplikatywnym podzbiorem w $\mathbb{N}$ zawierającym X.

Stwierdzenie 1.33 ([8], Proposition 3.4)**.** *Niech R będzie filialną dziedziną całkowitości charakterystyki zero. Wówczas dla dowolnych* $s \in S(\Pi(R))$, $m \in \mathbb{Z}$, *elementu odwracalnego* $u \in R$, $s \mid mu$ *w* R *wtedy i tylko wtedy, gdy* $s \mid m$ *w* $\mathbb{Z}$.

1.3.2 Pojęcie radykału

Definicja 1.34. Powiemy, że klasa pierścieni $\mathbb{M}$ jest **klasą radykalną**, jeżeli spełnia następujące warunki:

(i) klasa $\mathbb{M}$ jest homomorficznie zamknięta, tzn. jeśli R' jest obrazem homomorficznym pierścienia $R \in \mathbb{M}$, to $R' \in \mathbb{M}$,

(ii) klasa $\mathbb{M}$ jest zamknięta na rozszerzenia, tzn. jeśli $I \lhd R$ oraz $I \in \mathbb{M}$ i $R/I \in \mathbb{M}$, to $R \in \mathbb{M}$,

(iii) klasa $\mathbb{M}$ jest zamknięta na sumy algebraiczne ideałów, tzn. dla dowolnych ideałów R_t pierściena R, jeśli $R_t \in \mathbb{M}$, to $\sum R_t \in \mathbb{M}$.

Jeżeli $\mathbb{M}$ jest klasą radykalną, to mówimy krótko, że $\mathbb{M}$ jest radykałem. Jeżeli R jest pierścieniem z klasy radykalnej $\mathbb{M}$, to mówimy, że pierścień R jest $\mathbb{M}$-radykalny. Z definicji radykału wynika, że dla dowolnego pierścienia R i dowolnego radykału $\mathbb{M}$, R zawiera największy $\mathbb{M}$-radykalny ideał, mianowicie $\sum\{I \lhd R \ : \ I \in \mathbb{M}\}$, który oznaczamy przez $\mathbb{M}(R)$. Jeżeli $\mathbb{M}(R) = 0$, to mówimy, że pierścień R jest $\mathbb{M}$-półprosty. Łatwo możemy zauważyć, że pierścień $R/\mathbb{M}(R)$ jest $\mathbb{M}$-półprosty dla dowolnego pierścienia R. Wobec tego każdy pierścień jest rozszerzeniem pierścienia $\mathbb{M}$-radykalnego przez pierścień $\mathbb{M}$-półprosty.

Radykały odgrywają istotną rolę w badaniu różnych klas pierścieni. Zazwyczaj badania takie przebiegają zgodnie z następującym schematem

Schemat badania ustalonej klasy pierścieni $\mathcal{K}$ przy pomocy radykału $\mathbb{M}$:

* PROBLEM 1. Badamy pierścienie $\mathbb{M}$-radykalne z klasy $\mathcal{K}$,

* PROBLEM 2. Badamy pierścienie $\mathbb{M}$-półproste z klasy $\mathcal{K}$,

* PROBLEM 3. Badamy rozszerzenia pierścieni $\mathbb{M}$-radykalnych z klasy $\mathcal{K}$ przez pierścienie $\mathbb{M}$-półproste z klasy $\mathcal{K}$.

Często odpowiedni wybór radykału $\mathbb{M}$ dla klasy $\mathcal{K}$ pozwala stosunkowo prosto rozwiązać pierwsze dwa problemy z powyższej listy. Natomiast PROBLEM 3 jest bardziej skomplikowany ze względu na słabo rozwiniętą teorię rozszerzeń pierścieni i wymaga niejednokrotnie zaawansowanych badań. W tej pracy będziemy badać pierścienie filialne według powyższego schematu. W związku z tym przejdziemy teraz do krótkiego omówienia radykałów, które odgrywają dużą rolę w opisie pierścieni filialnych.

1. **Radykał Baer'a β.** Niech dla dowolnego pierścienia R, $W(R)$ oznacza sumę algebraiczną wszystkich nilpotentnych ideałów w R. Dla liczb porządkowych $\alpha \geq 0$ zdefiniujmy łańcuch ideałów $\{W_\alpha(R)\}$ pierścienia R następująco:

- $W_0(R) = 0$,

- Przypuśćmy, że $\alpha > 0$ i, że ideały $W_\gamma(R)$ są dobrze zdefiniowane dla $\gamma < \alpha$. Wówczas:

(i) jeżeli α jest graniczną liczbą porządkową, to $W_\alpha(R) = \bigcup_{\gamma<\alpha} W_\gamma(R)$,

(ii) jeżeli zaś α nie jest graniczną liczbą porządkową, to $W_\alpha(R)$ definiujemy jako ideał R zawierający $W_{\alpha-1}(R)$ i taki, że $W_\alpha(R)/W_{\alpha-1}(R) = W(R/W_{\alpha-1}(R))$.

Dobrze wiadomo, że zdefiniowany wyżej łańcuch ideałów stabilizuje się na pewnej liczbie porządkowej α i wówczas ideał $W_\alpha(R)$ nazywamy radykałem Baer'a i oznaczamy przez $\beta(R)$. Ponadto wiadomo, że pierścień R jest β-radykalny wtedy i tylko wtedy, gdy w każdym jego niezerowym obrazie homomorficznym istnieje pewien niezerowy ideał I taki, że $I^2 = 0$. Radykał Baer'a stanowi silne narzędzie do badania pierścieni filialnych. Już w doktoracie [4], udowodniono następujące ważny rezultat

Twierdzenie 1.35 ([4], Stwierdzenie 3.2.9)**.** *Dowolny β-radykalny pierścień R jest filialny wtedy i tylko wtedy, gdy każdy podpierścień pierścienia R jest jego ideałem.*

Wykorzystując własności radykału Baer'a, Filipowicz i Puczyłowski opisali lewostronnie filialne algebry nad ciałami (por. Twierdzenie 3.10 z [22]).

2. **Nil-radykał $\mathcal{N}$ (Köethe).** Pierścień, którego każdy element jest nilpotentny nazywamy **nil-pierścieniem**. Klasa $\mathcal{N}$ wszystkich nil-pierścieni jest klasą radykalną i dobrze wiadomo, że dla pierścienia przemiennego R, $\mathcal{N}(R) = \beta(R)$ oraz $\mathcal{N}(R)$ jest zbiorem wszystkich elementów nilpotentnych pierścienia R i $R/\mathcal{N}(R)$ jest pierścieniem zredukowanym. W kolejnych dwóch rozdziałach skupimy się na przemiennych nil-pierścieniach filialnych i przemiennych filialnych pierścieniach zredukowanych. Okazuje się że dla pierścieni z tych dwóch klas jesteśmy w stanie udowodnić pewne twierdzenia klasyfikacyjne. Dalsza część naszych badań będzie dotyczyła problemu opisu rozszerzeń przemiennych nil-pierścieni przez przemienne filialne pierścienie nil-półproste.

3. **Radykał podidempotentny $\mathcal{I}$.** Powiemy, że pierścień R jest **podidempotentny** jeżeli $I^2 = I$ dla każdego $I \lhd R$. Wykorzystując Lemat Andrunakiewicza (por. Lemma 1.2.7 w [31]), łatwo jest pokazać, że każdy pierścień podidempotentny jest filialny. Klasa $\mathcal{I}$ wszystkich pierścieni podidempotentnych stanowi radykał, którego opis nie został jeszcze znaleziony. W pracy [6] udowodniono następujące stwierdzenie.

Stwierdzenie 1.36 ([6], Proposition 3)**.** *Każde rozszerzenie pierścienia $\mathcal{I}$-radykalnego przez pierścień filialny jest pierścieniem filialnym.*

Powyższy rezultat pozwolił zredukować problem opisu pierścieni filialnych do opisu $\mathcal{I}$-półprostych pierścieni filialnych (modulo problem rozszerzeń).

4. **Radykał silnie regularny $\mathbb{S}$.** Powiemy, że pierścień R jest **silnie regularny**, jeżeli $a \in Ra^2$ dla każdego $a \in R$. Klasa $\mathbb{S}$ wszystkich pierścieni silnie regularnych jest radykałem. Jest jasne, że $\mathbb{S} \subseteq \mathcal{I}$ oraz $\mathbb{S}(R) = \mathcal{I}(R)$ dla przemiennego pierścienia R. Znaczenie radykału $\mathbb{S}$ do badania pierścieni filialnych zostało odkryte przez Filipowicz i Puczyłowskiego. Udowodnili oni, mianowicie bardzo ważne i często przez nas wykorzystywane rezultaty.

Twierdzenie 1.37 ([23], Theorem 3.4)**.** *Dla dowolnego pierścienia R następujące warunki są równoważne:*

(i) pierścień R jest zredukowany i lewostronnie filialny,

(ii) pierścień R zawiera ideał $I \in \mathbb{S}$ taki, że R/I jest przemiennym zredukowanym pierścieniem filialnym,

(iii) $R/\mathbb{S}(R)$ jest przemiennym zredukowanym pierścieniem filialnym.

Twierdzenie 1.38 ([23], Theorem 4.1)**.** *Jeżeli zredukowany lewostronnie filialny pierścień R jest algebrą nad ciałem F, to $R \in \mathbb{S}$.*

5. **Radykał prawie silnie regularny $\mathbb{S}_a$.** Pierścień R nazywamy **prawie silnie regularnym**, jeżeli dla każdego $a \in R$ istnieje $n \in \mathbb{N}$ takie, że $na \in Ra^2$. Klasa $\mathbb{S}_a$ wszystkich pierścieni prawie silnie regularnych stanowi radykał. Znaczenie tej klasy radykalnej do badania przemiennych pierścieni filialnych zostało odkryte przez Andruszkiewicza i M. Sobolewską w [10] (por. Stwierdzenie 3.3).

6. **Radykał p-podzielny $\mathcal{T}_p$.** Niech p będzie liczbą pierwszą. Pierścień R taki, że $R = pR$ nazywamy **p-podzielnym**. Klasa wszystkich pierścieni p-podzielnych jest radykałem. Jej znaczenie do opisu przemiennych pierścieni filialnych zostało po raz pierwszy zauważone w pracach [10] i [12].

7. **Radykał torsyjny $\mathbb{T}$.** Klasa $\mathbb{T}$ wszystkich pierścieni torsyjnych jest radykałem. Jest to bardzo użyteczny radykał przy badaniu przemiennych pierścieni filialnych. Dla tej klasy udaje się rozwiązać PROBLEM 1 (por. Rozdział 6).

Dodatkowe informacje na temat klas radykalnych i ich własności, wykorzystywane w tej pracy bez szczególnych odwołań, można znaleźć w monografii [31].

Rozdział 2

Filialne pierścienie β-radykalne

2.1 Fundamentalne własności H-pierścieni

Pierścień, w którym każdy podpierścień jest ideałem, nazywamy **H-pierścieniem**. Badaniem H-pierścieni zajmowało się wielu autorów, spośród których warto wyróżnić Andrijanowa ([2, 3]), Kruse ([35, 36]), Rédeia ([42, 43]) oraz Freidmana ([29]). Poniższa uwaga grupuje pewne, dobrze znane, własności H-pierścieni, które będą wykorzystywane w dalszej części pracy.

Uwaga 2.1. 1. Dowolny H-pierścień jest filialny.

2. Pierścień R jest H-pierścieniem wtedy i tylko wtedy, gdy $[a] \lhd R$ dla każdego $a \in R$.

3. Dowolny podpierścień i obraz homomorficzny H-pierścienia jest H-pierścieniem.

4. (por. [36]) Torsyjny pierścień R jest H-pierścieniem wtedy i tylko wtedy, gdy R_p jest H-pierścieniem dla dowolnej liczby pierwszej p.

5. Dowolny H-pierścień jest β-radykalny wtedy i tylko wtedy, gdy jest nil-pierścieniem.

W nawiązaniu do schematu badania klasy pierścieni filialnych, warto zaznaczyć, że przy opisie H-pierścieni podstawową rolę odgrywa nil-radykał równoważny radykałowi Baer'a na mocy punktu 5. ostatniej uwagi. Najbardziej czytelne w tej tematyce jest rozwiązanie PROBLEMU 2. Mianowicie zachodzi następujące twierdzenie.

Twierdzenie 2.2 (Freidman)**.** *Wszystkimi z dokładnością do izomorfizmu niezerowymi zredukowanymi H-pierścieniami są:*

(i) $n\mathbb{Z}$ *dla* $n \in \mathbb{N}$,

(ii) $\mathbb{Z}_m$ *dla bezkwadratowej liczby naturalnej* m,

(iii) $n\mathbb{Z} \oplus \mathbb{Z}_m$ *gdzie* $m, n \in \mathbb{N}$, m *jest liczbą bezkwadratową i* $m \mid n$.

Bardziej skomplikowany jest PROBLEM 3, którego rozwiązanie należy przypisać Kruse (por. Stwierdzenia 3.8 i 3.9 w [35]). Otrzymał on bardzo złożony opis oparty na kilkunastu lematach, który niestety jest jeszcze daleki do opisu z dokładnością do izomorfizmu. W Rozdziałach 4 i 5 rozwijamy metody Krusego do opisu pewnych pierścieni filialnych.

Z naszego punktu widzenia, wobec Twierdzenia 1.35, najistotniejsze jest rozwiązanie PROBLEMU 1. Bardzo ważną podklasę w rodzinie nil-H-pierścieni stanowią pierścienie z prawie zerowym mnożeniem. Zostały one odkryte przez Kruse i niezależnie przez Andrijanowa.

Definicja 2.3 ([35], Definition 2.1)**.** Mówimy, że pierścień R jest **z prawie zerowym mnożeniem**, jeżeli spełnione są następujące warunki:

(i) $a^3 = 0$ dla dowolnego $a \in R$,

(ii) dla dowolnego $a \in R$ istnieje bezkwadratowa liczba naturalna M taka, że $Ma^2 = 0$,

(iii) $ab \in \langle a^2 \rangle \cap \langle b^2 \rangle$ dla dowolnych $a, b \in R$.

Kruse i Andrijanow znaleźli pewne charakteryzacje pierścieni z prawie zerowym mnożeniem, które jednak są bardzo dalekie od opisu z dokładnością do izomorfizmu (por. Twierdzenia 2.16, 2.17). W następnym paragrafie przedstawimy nasze rozważania dotyczące tego zagadnienia, które jednak nie wyczerpują całego tematu. Następny rezultat, uzyskany przez Kruse, daje redukcję opisu nil-H-pierścieni do opisu torsyjnych nil-H-pierścieni (modulo opis pierścieni z prawie zerowym mnożeniem).

Stwierdzenie 2.4 ([35], Proposition 2.6)**.** *Nietorsyjny nil-pierścień jest H-pierścieniem wtedy i tylko wtedy, gdy jest pierścieniem z prawie zerowym mnożeniem.*

Wobec Uwagi 2.1 punkt 4., omawiany problem redukuje się do opisu nil-H-p-pierścieni. Okazuje się jednak, że można go dalej zredukować do p-pierścieni ograniczonego wykładnika dzięki następującemu wynikowi Kruse.

Stwierdzenie 2.5 ([35], Proposition 2.5)**.** *Nil-p-pierścień nieograniczonego wykładnika jest H-pierścieniem wtedy i tylko wtedy, gdy jest pierścieniem z prawie zerowym mnożeniem.*

Opisowi nil-H-p-pierścieni ograniczonego wykładnika jest poświęcona cała rozprawa doktorska [36]. Niezależnie podobną klasyfikację (też w terminach generatorów i relacji) uzyskał Andrijanow w pracy [3]. Warto tu jednak nadmienić, że ich klasyfikacje zawierają istotne luki, między innymi, brakuje opisów z dokładnością do izomorfizmu i redukcji zbyt dużej liczby parametrów. Zwracają na to uwagę również V. G. Antipkin i V. P. Elizarov w [18], (strona 461). Odnotujmy jeszcze, że Andrijanow wymienia szesnaście klas nil-H-p-pierścieni, z których pierwsza jest klasą p-pierścieni z prawie zerowym mnożeniem. Co do pozostałych klas, Andrijanow pisze, że wszystkie wymienione klasy są różne w tym sensie, że dla dowolnych dwóch klas R_i oraz R_j jeżeli $i \neq j$,

to istnieje pierścień P, który należy do klasy R_i lecz nie jest izomorficzny z żadnym pierścieniem z klasy R_j.

Przedstawimy teraz dwa fakty bezpośrednio związane z pracami [42, 43]. Rezultaty te są dobrze znane, jednak ich dowody, podane przez Rédeia są skomplikowane. Dlatego, dla kompletności przedstawimy, własne, prostsze dowody tych faktów.

Lemat 2.6. *Jeżeli a jest nilpotentnym elementem H-pierścienia R i istnieje bezkwadratowa liczba naturalna M taka, że $Ma^2 = 0$, to $a^3 = 0$.*

Dowód. Jeżeli $a^2 = 0$, to $a^3 = 0$. Niech dalej $a^2 \neq 0$. Wtedy z założenia $o(a^2) = N$ w grupie R^+ jest liczbą naturalną bezkwadratową. Ponadto $a^3 \in [a^2] \lhd R$, więc istnieją $n \in \mathbb{N}$ oraz $k_1, \ldots, k_n \in \mathbb{Z}$ takie, że $a^3 = k_1a^2 + k_2a^4 + \ldots + k_na^{2n}$. Stąd $k_1a^2 = xa^2$ dla pewnego $x \in [a]$. Przez indukcję otrzymujemy, że $k_1^m a^2 = x^m a^2$ dla dowolnego $m \in \mathbb{N}$. Ale R jest nil-pierścieniem, więc $k_1^m a^2 = 0$ dla pewnego $m \in \mathbb{N}$. Zatem $N \mid k_1^m$. Ale N jest liczbą bezkwadratową, więc $N \mid k_1$ i wobec tego $k_1a^2 = 0$ oraz $a^3 = k_2a^4 + \ldots + k_na^{2n} \in [a]a^3$. Zatem $a^3 = 0$. □

Twierdzenie 2.7. *Niech a będzie nilpotentnym elementem H-pierścienia R. Jeżeli a ma nieskończony rząd w grupie R^+, to $a^3 = 0$ i istnieje liczba naturalna bezkwadratowa M taka, że $Ma^2 = 0$.*

Dowód. Załóżmy, że $o(a^2) = \infty$. Pokażemy, że $\langle a \rangle \cap \langle a^2 \rangle = 0$. Załóżmy, że dla pewnych $k, l \in \mathbb{Z}$, $ka = la^2$. Stąd $k^2a = l^2a^3$ i przez prostą indukcję $k^n a = l^n a^{n+1}$ dla dowolnej liczby naturalnej n. Ale a jest elementem nilpotentnym, więc $k^n a = 0$ dla pewnego $n \in \mathbb{N}$, skąd $k = 0$ i w konsekwencji $\langle a \rangle \cap \langle a^2 \rangle = 0$. Dalej $[a^2] \lhd R$, więc $a^3 \in [a^2]$. Istnieją zatem $k_1, k_2, \ldots, k_s \in \mathbb{Z}$ takie, że $a^3 = k_1a^2 + k_2a^4 + \cdots + k_sa^{2s}$. Stąd $k_1a^2 = ba^2$ dla pewnego $b \in [a]$. Zatem przez prostą indukcję $k_1^n a^2 = b^n a^2$ dla dowolnego naturalnego n i w konsekwencji $k_1^n a^2 = 0$ dla pewnego $n \in \mathbb{N}$. Ale $o(a^2) = \infty$, więc $k_1 = 0$ oraz $a^3 \in [a]a^3$, więc $a^3 = 0$. Zatem $[a]^+ = \langle a \rangle^+ \oplus \langle a^2 \rangle^+$. Ponadto $[2a]^+ = \langle 2a \rangle^+ \oplus \langle 4a^2 \rangle^+ \lhd [a]$, więc $2a^2 = a(2a) = U \cdot 2a + V \cdot 4a^2$, skąd $2 = 4V$, sprzeczność. Wobec tego $o(a^2) < \infty$.

Przypuśćmy, że $o(a^2) = p^2m$ dla pewnej liczby pierwszej p oraz liczby naturalnej m. Ponieważ $(pma)^2 = 0$, więc $\langle pma \rangle = [pma] \lhd R$. Zatem $a(pma) = U(pma)$ dla pewnego $U \in \mathbb{Z}$. Stąd $0 = p(pma^2) = p(Upma) = (p^2Um)a$, ale $o(a) = \infty$, więc $U = 0$ i $pma^2 = 0$, sprzeczność z określeniem $o(a^2)$.

Wobec tego, na mocy Lematu 2.6, mamy tezę. □

Niejednokrotnie będziemy wykorzystywali następujący, udowodniony przez Kruse, lemat.

Lemat 2.8 ([35], Lemma 2.7)**.** *Jeżeli R jest nil-H-p-pierścieniem, to dla dowolnego $a \in R$, $a^3 \in \langle a^2 \rangle$ i w szczególności $[a] = \langle a \rangle + \langle a^2 \rangle$.*

2.2 Pierścienie z prawie zerowym mnożeniem

Odnotujmy, że każdy pierścień R z prawie zerowym mnożeniem jest H-pierścieniem oraz $R^3 = 0$. Dowód następnego stwierdzenia jest standardowy.

Stwierdzenie 2.9. *Niech R będzie pierścieniem torsyjnym. Wówczas R jest z prawie zerowym mnożeniem wtedy i tylko wtedy, gdy R_p jest z prawie zerowym mnożeniem dla każdego $p \in \mathbb{P}$.*

Zaczniemy od przedstawienia kilku faktów dających podstawowe własności pierścieni z prawie zerowym mnożeniem.

Uwaga 2.10. Jeżeli R jest pierścieniem z prawie zerowym mnożeniem, to $a(R) = \{a \in R : a^2 = 0\}$. Rzeczywiście, jeśli $a \in R$ i $a^2 = 0$, to z warunku (iii) Definicji 2.3, $ab = 0$ oraz $ba = 0$ dla dowolnego $b \in R$, czyli $aR = Ra = 0$ i $a \in a(R)$.

Lemat 2.11. *Niech I, J będą ideałami pierścienia R takimi, że I jest pierścieniem z prawie zerowym mnożeniem oraz $J^2 = IJ = JI = 0$. Wówczas $I+J$ jest pierścieniem z prawie zerowym mnożeniem.*

Dowód. Dowodu wymaga jedynie punkt (iii) Definicji 2.3. Niech $a, i \in I$, $b, j \in J$, wówczas $(a + b)(i + j) = ai$. Ale pierścień I jest z prawie zerowym mnożeniem, więc istnieje $K \in \mathbb{Z}$ takie, że $ai = Ka^2$. Ponieważ $(a + b)^2 = a^2$, więc $(a + b)(i + j) = ai = Ka^2 = K(a+b)^2 \in \langle (a+b)^2 \rangle$. Analogicznie uzasadnia się, że $(i+j)(a+b) \in (a+b)^2\rangle$. □

Stwierdzenie 2.12. *Jeżeli nil-H-pierścień R spełnia którykolwiek z poniższych warunków:*

(i) R jest p-pierścieniem oraz $ab \in \langle a^2 \rangle \cap \langle b^2 \rangle$ dla dowolnych $a, b \in R$,

(ii) $pR = 0$ dla pewnego $p \in \mathbb{P}$,

(iii) R jest pierścieniem prawie podzielnym,

to R jest pierścieniem z prawie zerowym mnożeniem.

Dowód. (i). Niech $a \in R$. Pokażemy, że $pa^2 = 0$. Jeśli $a^2 = 0$, to $pa^2 = 0$. Niech więc $a^2 \neq 0$ i $m \in \mathbb{N}$ będzie takie, że $p^m a^2 = 0$ oraz $p^{m-1}a^2 \neq 0$. Wtedy $(p^{m-1}a)^2 = 0$, ale $0 \neq (p^{m-1}a)a \in \langle (p^{m-1}a)^2 \rangle = 0$. Sprzeczność. Zatem $m = 1$. Ponieważ R jest H-pierścieniem, więc teza ostatecznie wynika z Lematu 2.6.

(ii). Wynika z Twierdzenia 3.3. z pracy [25].

(iii). Jeżeli grupa R^+ zawiera element nieskończonego rzędu, to teza wynika ze Stwierdzenia 2.4. Załóżmy więc, że R^+ jest grupą torsyjną. Na mocy Stwierdzenia 2.9 wystarczy wykazać, że R_p jest pierścieniem z prawie zerowym mnożeniem dla każdego $p \in \mathbb{P}$. Jeżeli R_p^+ jest grupą o skończonym wykładniku, to $p^s R_p = 0$ dla pewnego $s \in \mathbb{N}$, ale z założenia $p^s R_p = pR_p$, więc $pR_p = 0$ i na mocy punktu (ii), R_p jest pierścieniem z prawie zerowym mnożeniem. W przypadku, gdy grupa R_p^+ nie ma skończonego wykładnika, teza wynika ze Stwierdzenia 2.5. □

Następne stwierdzenie jest dobrze znane, jednak my podamy jego nowy dowód.

Stwierdzenie 2.13. *Dowolny nil-H-p-pierścień R jest nilpotentny.*

Dowód. Jeżeli grupa addytywna R^+ nie jest ograniczonego wykładnika, to ze Stwierdzenia 2.5, R jest pierścieniem z prawie zerowym mnożeniem, więc $R^3 = 0$.

Załóżmy dalej, że $p^k R = 0$ dla pewnego $k \in \mathbb{N}$. Udowodnimy, że wówczas $R^{3k} = 0$. Zauważmy, że R/pR jest nil-H-pierścieniem takim, że $p(R/pR) = 0$. Na mocy Stwierdzenia 2.12 punkt (ii), $(R/pR)^3 = 0$, skąd $R^3 \subseteq pR$. Stąd $R^{3k} \subseteq (pR)^k \subseteq p^k R = 0$. □

Zauważmy, że jeżeli H-pierścień R spełnia którykolwiek z warunków: lewostronna noetherowskość, prawostronna noetherowskość, obustronna noetherowskość, ACC na podpierścienie, to pierścień R spełnia każdy z tych warunków; wobec tego w dalszej części pracy będziemy taki pierścień nazywać krótko noetherowskim.

Lemat 2.14. *Dla dowolnego nil-H-pierścienia R następujące warunki są równoważne:*

(i) pierścień R jest noetherowski,

(ii) grupa R^+ jest skończenie generowana,

(iii) pierścień R jest skończenie generowany.

W szczególności każdy noetherowski nil-H-pierścień jest nilpotentny.

Dowód. $(i) \Rightarrow (ii)$. Załóżmy najpierw, że pierścień R nie jest torsyjny. Wówczas ze Stwierdzenia 2.4 wynika, że R jest pierścieniem z prawie zerowym mnożeniem. Stąd $R^3 = 0$ i pierścienie R/R^2 oraz R^2 są noetherowskimi pierścieniami z zerowym mnożeniem. Wobec tego grupy $(R/R^2)^+$ oraz $(R^2)^+$ są skończenie generowane. Zatem grupa R^+ jest skończenie generowana. Jeżeli zaś, pierścień R jest torsyjny, to $R = \bigoplus_{p\in\Pi} R_p$ dla pewnego skończonego podzbioru $\Pi \subseteq \mathbb{P}$ i na podstawie Stwierdzenia 2.13, $R^n = 0$ dla pewnego $n \in \mathbb{N}$. Wobec tego pierścienie z zerowym mnożeniem R^i/R^{i+1} dla $i = 1, 2, \ldots, n-1$ są noetherowskie. Stąd grupy grupy addytywne tych pierścieni są skończenie generowane, a więc grupa R^+ jest skończenie generowana.

Implikacja $(ii) \Rightarrow (iii)$ jest oczywista.

$(iii) \Rightarrow (i)$. Niech $R = [a_1, a_2, \ldots, a_n]$ dla pewnych $a_1, a_2, \ldots, a_n \in R$. Wówczas $R = [a_1] + [a_2] + \cdots + [a_n]$. Ponadto z Twierdzenia 2.7 i z Lematu 2.8 wynika, że $[a_i] = \langle a_i \rangle + \langle a_i^2 \rangle$ dla $i = 1, 2, \ldots, n$. Stąd, $R = \langle a_1 \rangle + \langle a_1^2 \rangle + \langle a_2 \rangle + \langle a_2^2 \rangle + \cdots + \langle a_n \rangle + \langle a_n^2 \rangle$ i grupa R^+ jest skończenie generowana, więc pierścień R jest noetherowski.

□

Poniżej zaprezentujemy przykład nil-H-pierścienia, który nie jest z prawie zerowym mnożeniem. Przykład ten można wydedukować z prac Andrianowa, jednak my przedstawimy jego kompletną konstrukcję wraz z dowodem.

Stwierdzenie 2.15. *Niech N będzie pierścieniem z prawie zerowym mnożeniem takim, że $p^m N = 0$ dla pewnej liczby naturalnej m. Niech $R = [a] \oplus N$, gdzie $o(a) = p^n$ dla pewnej liczby naturalnej $n > m$ oraz $a^2 = p^m a$. Wówczas R jest H-pierścieniem i dodatkowo, R jest pierścieniem z prawie zerowym mnożeniem wtedy i tylko wtedy, gdy $N^2 = 0$ oraz $n = m + 1$.*

Dowód. Zauważmy, że $[a]$ jest nil-pierścieniem, gdyż $a^3 = p^m a^2 = p^{2m}a$ oraz $p^n a = 0$. Z przyjętych założeń wynika, że $[a] \cong p^m\mathbb{Z}_{p^{n+m}}$ oraz $N^3 = 0$. Zatem R jest nil-pierścieniem takim, że $p^n R = 0$. Niech $r \in R$. Wówczas istnieją $k \in \mathbb{Z}$ oraz $x \in N$ takie, że $r = (ka, x)$. Dla $y \in N$ mamy $yx = Ux^2$ dla pewnego $U \in \mathbb{Z}$, więc $(0, y)r = (0, Ux^2) = U(0, x^2) = Ur^2 + (-U)kp^m r \in [r]$. Ponadto $[a] = \langle a \rangle$ i $(a, 0)r = (ka^2, 0) = (kp^m a, 0) = p^m r \in [r]$. Analogicznie można pokazać, że $r(0, y) \in [r]$ oraz $r(a, 0) \in [r]$. Zatem $[r] \lhd R$ i R jest H-pierścieniem.

Załóżmy, że R jest pierścieniem z prawie zerowym mnożeniem. Wówczas $[a]$ jest też pierścieniem z prawie zerowym mnożeniem jako podpierścień w R i wówczas $0 = pa^2 = p^{m+1}a$, skąd $p^n \mid p^{m+1}$. Ale $m < n$, więc $n = m + 1$. Jeżeli $N^2 \neq 0$, to istnieje $x_0 \in N$ taki, że $x_0^2 \neq 0$. Ponieważ $(0, x_0)(a, x_0) = (0, x_0^2)$ oraz $(a, x_0)^2 = (a^2, x_0^2) = (p^m a, x_0^2)$, więc jeśli R jest pierścieniem z prawie zerowym mnożeniem, to istnieje $V \in \mathbb{Z}$ takie, że $(0, x_0^2) = V(p^m a, x_0^2)$. Stąd $Vp^m a = 0$ i $Vx_0^2 = x_0^2$. Ale $o(a) = p^n > p^m$, więc $p \mid V$. Ponieważ $px_0^2 = 0$, więc $Vx_0^2 = 0$ i $x_0^2 = 0$, sprzeczność.

Jeżeli zaś $N^2 = 0$ i $[a]$ jest pierścieniem z prawie zerowym mnożeniem, to $N \subseteq a(R)$ i R jest pierścieniem z prawie zerowym mnożeniem na mocy Lematu 2.11. □

Dla dowolnego pierścienia R i dowolnej liczby pierwszej p niech

$$R[p] = \{a \in R \ : \ pa^2 = 0\}.$$

Poniższe dwa twierdzenia zostały udowodnione niezależnie przez Kruse i Andrijanowa, przy użyciu nietrywialnych metod wykorzystujących twierdzenie Chevalley'a por. [32, strony 143-144]:

Twierdzenie 2.16 ([35], Proposition 2.10)**.** *Niech S będzie pierścieniem takim, że $S = S[p]$ dla pewnej liczby pierwszej p. Wówczas S jest pierścieniem z prawie zerowym mnożeniem wtedy i tylko wtedy, gdy spełniony jest jeden z następujących warunków:*

(1) $S^2 = 0$,

(2) istnieje $x \in S$ *taki, że* $x^2 \neq 0$, $px, x^2 \in a(S)$, *oraz* $S = \langle x \rangle + a(S)$,

(3) istnieją $x, y \in S$ *takie, że* $S = \langle x, y \rangle + a(S)$, $x^2 \neq 0$, $y^2 \neq 0$, $px, py, x^2, y^2 \in a(S)$, $y^2 = Ax^2$, $xy = F_1 x^2$, $yx = F_2 x^2$ *dla takich* $A, F_1, F_2 \in \mathbb{Z}$, *że kongruencja*

$$X^2 + (F_1 + F_2)X + A \equiv 0 \pmod{p} \tag{2.1}$$

nie ma rozwiązania.

Ponadto, jeżeli S jest pierścieniem z prawie zerowym mnożeniem, to $S/a(S)$ jest $\mathbb{Z}_p$-algebrą oraz $\dim_{\mathbb{Z}_p} S/a(S) \leq 2$, przy czym $\dim_{\mathbb{Z}_p} S/a(S) = k - 1$ wtedy i tylko wtedy, gdy S spełnia warunek (k).

Twierdzenie 2.17 ([35], Proposition 2.10)**.** *Pierścień R jest z prawie zerowym mnożeniem wtedy i tylko wtedy, gdy $R = \sum_{p \in \mathbb{P}} R[p]$, gdzie dla dowolnych różnych $p, q \in \mathbb{P}$, $R[p] \cdot R[q] = 0$, $R[p] \lhd R$ i $R[p]$ spełnia jeden z warunków (1), (2), (3) Twierdzenia 2.16.*

Uwaga 2.18. Niech S będzie pierścieniem z prawie zerowym mnożeniem takim, że $S = S[p]$ dla pewnej liczby pierwszej p. Zauważmy, że:

(i) jeżeli $\dim_{\mathbb{Z}_p} S/a(S) = 1$, to dla dowolnego $x \in S \setminus a(S)$, $S = \langle x \rangle + a(S)$. W szczególności, jeśli $o(x) = n \in \mathbb{N}$, to $nx^2 = 0$, więc $p \mid n$ i $n = p^\alpha m$ dla pewnych $\alpha, m \in \mathbb{N}$ takich, że $p \nmid m$. Zatem $o(mx) = p^\alpha$, $mx \notin a(S)$ i $S = \langle mx \rangle + a(S)$.

(ii) jeżeli $\dim_{\mathbb{Z}_p} S/a(S) = 2$ oraz $S = \langle x, y \rangle + a(S)$ dla pewnych $x, y \in S$, to istnieją $A, F_1, F_2 \in \mathbb{Z}$ takie, że spełniony jest warunek (3) Twierdzenia 2.16. Rzeczywiście, w tym przypadku warstwy $x + a(S)$, $y + a(S)$ są liniowo niezależne nad $\mathbb{Z}_p$, bo generują dwuwymiarową przestrzeń liniową $S/a(S)$. Ponadto $x^2 \neq 0$, $y^2 \neq 0$ oraz $px, py, x^2, y^2 \in a(S)$. Ponieważ $|S^2| = p$ oraz $x^2 \neq 0$, więc $S^2 = \langle x^2 \rangle$. Istnieją zatem $F_1, F_2, A \in \mathbb{Z}$ takie, że $y^2 = Ax^2$, $xy = F_1x^2$, $yx = F_2x^2$. Weźmy dowolne $T \in \mathbb{Z}$. Ponieważ warstwy $x + a(S)$, $y + a(S)$ są liniowo niezależne, więc $T[x + a(S)] + [y + a(S)] \neq a(S)$, skąd $Tx + y \notin a(S)$. Na mocy Uwagi 2.10, $(Tx + y)^2 \neq 0$, więc:

$$T^2x^2 + Txy + Tyx + y^2 = T^2x^2 + TF_1x^2 + TF_2x^2 + Ax^2 =$$

$$(T^2 + T(F_1 + F_2) + A)x^2 \neq 0.$$

Zatem kongruencja (2.1) nie ma rozwiązania.

Podobne rozumowanie jak w punkcie (i) w przypadku gdy $o(x) \in \mathbb{N}$ ($o(y) \in \mathbb{N}$) pozwala zakładać, że $o(x) = p^\alpha$ ($o(y) = p^\alpha$) dla pewnego $\alpha \in \mathbb{N}$.

Pierwszy opis nil-H-p-pierścieni generowanych przez jeden element pochodzi od Rédeia [42]. Inne spojrzenie na ten problem przedstawili Freidman w krótkiej notce [30] i Kruse w swoim doktoracie [36]. W żadnej z tych prac nie podano jednak klasyfikacji tych pierścieni z dokładnością do izomorfizmu. Następne twierdzenie uzupełnia tę lukę.

Twierdzenie 2.19. *Wszystkimi, z dokładnością do izomorfizmu, niezerowymi nil-H-p-pierścieniami generowanymi przez jeden element są:*

(i) $p^m\mathbb{Z}_{p^{m+n}}$ *dla pewnych* $m, n \in \mathbb{N}$, $m \leq n$,

(ii) $x\mathbb{Z}_p[x]/(x^3)$,

(iii) $x\mathbb{Z}_{p^m}[x]/(px^2, x^3)$, $m \in \mathbb{N}$, $m \geq 2$,

(iv) $x\mathbb{Z}_{p^{m+n}}[x]/(px^2 - p^m x, x^3 - p^{2m-2}x)$ *dla pewnych* $m, n \in \mathbb{N}$, $m \geq 2$.

Dowód. Niech R będzie niezerowym nil-H-p-pierścieniem generowanym przez element y. Załóżmy najpierw, że $y^2 \in \langle y \rangle$. Wtedy $y^2 = Ky$ dla pewnego $K \in \mathbb{N}$. Ale $o(y) = p^n$ dla pewnego $n \in \mathbb{N}$, zatem gdyby $p \nmid K$, to $y \in Ry$ i ponieważ R jest nil-pierścieniem, więc $y = 0$, wbrew założeniu, że $R \neq 0$. Zatem $p \mid K$ i istnieją $Q, m \in \mathbb{N}$ takie, że $p \nmid Q$ oraz $y^2 = Qp^m y$. Ponadto istnieje $t \in \mathbb{Z}$ takie, że $p^n \mid 1 - tQ$. Zatem dla $x = ty$ mamy $[y] = [x]$ oraz $x^2 = t^2y^2 = t^2Qp^m y = p^m x$, czyli $x^2 = p^m x$. Stąd $R^+ = \langle x \rangle$ i przekształcenie $f\colon R \to p^m\mathbb{Z}_{p^{m+n}}$ dane wzorem $f(kx) = p^m k$ dla $k \in \mathbb{Z}_{p^n}$

jest izomorfizmem pierścieni. Zauważmy jeszcze, że jeśli $m > n$, to $x^2 = 0$ i wtedy $R \cong p^n\mathbb{Z}_{p^{2n}}$. Wobec tego jeśli $R = [y]$ i $y^2 \in \langle y\rangle$, to pierścień R jest taki jak w punkcie (i).

Teraz załóżmy, że $y^2 \notin \langle y\rangle$. Na mocy Lematu 2.8, dla każdego $a \in R$ mamy $a^3 \in \langle a^2\rangle$ oraz $[a] = \langle a\rangle + \langle a^2\rangle$. Ale $py^2 = y \cdot py \in [py]$, więc istnieją $U, V \in \mathbb{Z}$ takie, że $py^2 = Upy + Vp^2y^2$. Stąd $p(1 - Vp)y^2 = Upy$. Ponieważ $o(y) = p^s$ dla pewnego $s \in \mathbb{N}$, więc $py^2 \in \langle py\rangle$. Istnieją zatem $m, Q \in \mathbb{N}$ takie, że $p \nmid Q$ oraz $py^2 = Qp^my$. Ponadto istnieje $t \in \mathbb{Z}$ takie, że $p^s \mid 1 - tQ$. Zatem dla $x = ty$ mamy, że $[y] = [x]$, $x^2 \notin \langle x\rangle$ oraz $px^2 = pt^2y^2 = t^2Qp^my = p^mx$, czyli $px^2 = p^mx$. Załóżmy, że $s \leq m$. Wtedy $px^2 = 0$. Ale $x^3 = tx^2$ dla pewnego $t \in \mathbb{Z}$, przy czym jeśli $p \nmid t$, to $x^2 \in Rx^2$, co implikuje $x^2 = 0$, skąd $x^2 \in \langle x\rangle$, wbrew założeniu. Zatem $p \mid t$ i wobec tego $x^3 = 0$. Ponadto R^+ jest sumą prostą swoich podgrup cyklicznych $\langle x\rangle$ i $\langle x^2\rangle$. Zatem każdy element z pierścienia R można jednoznacznie zapisać w postaci $kx + lx^2$ dla pewnych $k \in \mathbb{Z}_{p^s}$ oraz $l \in \mathbb{Z}_p$. Wynika stąd, że przekształcenie $g\colon R \to x\mathbb{Z}_{p^s}[x]/(px^2, x^3)$ dane wzorem $g(kx + lx^2) = k\overline{x} + l\overline{x}^2$, gdzie $\overline{x} = x + (px^2, x^3)$, jest izomorfizmem pierścieni. Zatem w tym przypadku pierścień R jest taki jak w punkcie (ii) jeżeli $s = 1$ lub taki jak w punkcie (iii) jeżeli $s > 1$.

Pozostaje do rozpatrzenia przypadek, gdy $s > m$. Wtedy $px^2 = p^mx \neq 0$. Zauważmy, że wówczas $m > 1$. Rzeczywiście, gdyby $m = 1$, to $px^2 = px$, skąd przez indukcję $px^k = px$ dla każdego $k = 1, 2, \ldots$. Ale element x jest nilpotentny, więc stąd $px = 0$, czyli $1 = s > m$ i mamy sprzeczność. Zatem $m > 1$. Ponadto $x^3 \in \langle x^2\rangle$, więc $x^3 = Tx^2$ dla pewnego $T \in \mathbb{N}$. Gdyby $p \nmid T$, to $x^2 \in Rx^2$, skąd $x^2 = 0$ i mamy sprzeczność. Zatem $p \mid T$ i istnieją $K, t \in \mathbb{N}$ takie, że $x^3 = Kp^tx^2$ oraz $p \nmid K$. Stąd $x^3 = Kp^{t-1}(px^2) = Kp^{t-1}p^mx$, czyli $x^3 = Kp^{m+t-1}x$ oraz $x^4 = Kp^{2m+t-2}x$. Niech $a = x^2 - p^{m-1}x$. Wtedy $p^{m-1}x^3 = p^{m-2}x \cdot px^2 = p^{m-2}x \cdot p^mx = p^{2m-2}x^2 = p^{2m-3}(px^2) = p^{2m-3} \cdot p^mx = p^{3m-3}x$ oraz $a^2 = x^4 - p^{m-1}x^3 - p^{m-1}x^3 + p^{2m-2}x^2 = Kp^{2m+t-2}x - Kp^{2m+t-2}x - p^{3m-3}x + p^{3m-3}x = 0$, więc $\langle a\rangle = [a] \lhd R$. Stąd $xa \in \langle a\rangle$. Ale $xa = x^3 - p^{m-1}x^2 = x^3 - p^{m-2}(px^2) = x^3 - p^{m-2}(p^mx) = x^3 - p^{2m-2}x$, więc istnieje $U \in \mathbb{N}$ takie, że $x^3 - p^{2m-2}x = U(x^2 - p^{m-1}x)$. Ponadto $x^3 \in \langle x\rangle$, więc jeśli $p \nmid U$, to stąd $x^2 \in \langle x\rangle$, co prowadzi do sprzeczności. Zatem $p \mid U$. Ale $p(x^2 - p^{m-1}x) = px^2 - p^mx = 0$, więc stąd $x^3 - p^{2m-2}x = 0$, czyli $x^3 = p^{2m-2}x$. Dalej, $\langle x\rangle \cap \langle x^2\rangle = \langle px^2\rangle = \langle p^mx\rangle$ i $R = [x] = \langle x\rangle + \langle x^2\rangle$, więc każdy element pierścienia R można jednoznacznie zapisać w postaci $kx + lx^2$ dla pewnych $k \in \mathbb{Z}_{p^s}$ oraz $l \in \mathbb{Z}_p$. Ponadto $n = s - m \in \mathbb{N}$, bo $s > m$ i $s = m + n$. Wynika stąd, że przekształcenie $h\colon R \to x\mathbb{Z}_{p^{m+n}}/(px^2 - p^mx, x^3 - p^{2m-2}x)$ dane wzorem $h(kx + lx^2) = kX + lX^2$, gdzie $X = x + (px^2 - p^mx, x^3 - p^{2m-2}x)$, jest izomorfizmem pierścieni. Zatem w tym przypadku pierścień R jest taki jak w punkcie (iv).

Pierścienie R z punktu (i) są izomorficzne z podpierścieniami H-pierścieni postaci $\mathbb{Z}_{p^r}$, a więc są H-pierścieniami. Niech $m_1, m_2, n_1, n_2 \in \mathbb{N}$ będą takie, że $m_1 \leq n_1$ i $m_2 \leq n_2$ oraz $R_1 \cong R_2$ dla $R_1 = p^{m_1}\mathbb{Z}_{p^{m_1+n_1}}$ i $R_2 = p^{m_2}\mathbb{Z}_{p^{m_2+n_2}}$. Wtedy $|R_1| = |R_2|$, skąd $p^{n_1} = p^{n_2}$, a więc $n_1 = n_2$. Ponadto $R_1^2 \cong R_2^2$, skąd $|R_1^2| = |R_2^2|$, a więc $p^{n_1-m_1} = p^{n_2-m_2}$, czyli $n_1 - m_1 = n_2 - m_2$, skąd $m_1 = m_2$. To pokazuje, że pierścienie z klasy (i) są parami nieizomorficzne. Żaden z takich pierścieni nie może być izomorficzny z pierścieniem z punktu (ii) lub (iii), gdyż grupa R^+ jest cykliczna, zaś grupy addytywne pierścieni z punktów (ii), (iii) nie są cykliczne.

Przyjrzyjmy się teraz bliżej pierścienieniom z klasy (iv). Pokażemy, że pierścień $R = x\mathbb{Z}_{p^{m+n}}[x]/(px^2 - p^m x, x^3 - p^{2m-2}x)$ jest nil-H-pierścieniem o dokładnie p^{n+m+1}-elementach. Oznaczmy $I = (px^2 - p^m x, x^3 - p^{2m-2}x)$ i niech $X = x + I$. Pokażemy najpierw, że każdy element pierścienia R można jednoznacznie zapisać w postaci $kX + lX^2$ dla pewnych $k \in \mathbb{Z}_{p^{m+n}}$ oraz $l \in \mathbb{Z}_p$. Ponieważ $x^3 - p^{2m-2}x \in I$, więc każdy element należący do R ma postać $sX + tX^2$ dla pewnych $s, t \in \mathbb{Z}_{p^{m+n}}$. Ale $t = qp + r$ dla pewnych $q, r \in \mathbb{Z}$, $0 \leq r < p$ oraz $pX^2 = p^m X$, więc $sX + tX^2 = (s + qp^m)X + rX^2$. Pozostaje zatem wykazać, że jeżeli $k \in \mathbb{Z}_{p^{m+n}}$ oraz $l \in \mathbb{Z}_p$ i $kx + lx^2 \in I$, to $k = 0$ i $l = 0$. Ale dla pewnych wielomianów $f, g \in \mathbb{Z}_{p^{m+n}}[x]$ zachodzi $kx + lx^2 = f \cdot (px^2 - p^m x) + g \cdot (x^3 - p^{2m-2}x)$, więc $kx + lx^2 = x(x - p^{m-1})[pf + g \cdot (x + p^{m-1})]$. Stąd $k + lx = (x - p^{m-1})[pf + g \cdot (x + p^{m-1})]$ oraz $p^{m+n} \mid k + lp^{m-1}$. Ale $m \geq 2$, więc $p \mid k$. Przy naturalnym homomorfizmie pierścienia $\mathbb{Z}_{p^{m+n}}[x]$ na pierścień $\mathbb{Z}_p[x]$ uzyskamy stąd, że $lx = x^2 G$ dla pewnego $G \in \mathbb{Z}_p[x]$. Wobec tego $l = 0$ oraz $k = (x - p^{m-1})[pf + g \cdot (x + p^{m-1})]$, skąd $k = 0$. W ten sposób wykazaliśmy jednoznaczność zapisu elementów pierścienia R w postaci $kX + lX^2$ dla pewnych $k \in \mathbb{Z}_{p^{m+n}}$ oraz $l \in \mathbb{Z}_p$. Wynika stąd od razu, że $|R| = p^{m+n+1}$. Ponadto $p^{m+n}R = 0$, więc grupa R^+ nie jest cykliczna. Zatem w szczególności, żaden z pierścieni z punktu (i) nie może być izomorficzny z pierścieniem z punktu (iv).

Dalej, $X^3 = p^{2m-2}X$, skąd przez indukcję $X^k = p^{(k-1)(m-1)}X$ dla $k = 3, 4, \ldots$. Ale $p^{m+n}X = 0$ i $m \geq 2$, więc $X^{n+m+1} = 0$ i wobec tego $R^{n+m-1} = 0$. Zauważmy, że $pX^2 = p^m X$ oraz $R = [X]$. W celu wykazania, że R jest H-pierścieniem wystarczy zatem pokazać, że dla dowolnych $k \in \mathbb{Z}_{p^{m+n}}$ oraz $l \in \mathbb{Z}_p$ zachodzi $X \cdot (kX + lX^2) \in [kX + lX^2]$. Jeśli $p \mid k$, to $k = pt$ dla pewnego $t \in \mathbb{Z}$ oraz $X \cdot (kX + lX^2) = tpX^2 + lX^3 = tp^m X + lp^{2m-2}X = (kp^{m-1} + lp^{2m-2})X$ oraz $p^{m-1}(kX + lX^2) = p^{m-1}kX + lp^{m-2}(pX^2) = p^{m-1}kX + lp^{m-2}p^m X = (kp^{m-1} + lp^{2m-2})X$, skąd $X \cdot (kX + lX^2) \in [kX + lX^2]$. Dalej załóżmy, że $p \nmid k$. Wówczas $X \cdot (kX + lX^2) = kX^2 + lX^3 = kX^2 + lp^{2m-2}X = lp^{2m-2}X + kX^2$. Ponadto $(kX + lX^2)^2 = k^2X^2 + 2klX^3 + l^2X^4 = k^2X^2 + 2klp^{2m-2}X + l^2p^{3m-3}X$ oraz istnieje $C \in \mathbb{Z}_{p^{m+n}}$ takie, że $Ck = 1$. Stąd $C(kX + lX^2)^2 = (2lp^{2m-2} + Cl^2p^{3m-3})X + kX^2$ oraz $lCp^{2m-2}(kX + lX^2) = klCp^{2m-2}X + Cl^2p^{2m-3}(pX^2) = lp^{2m-2}X + Cl^2p^{3m-3}X$, więc $C(kX + X^2)^2 - lC(kX + lX^2) = lp^{2m-2}X + kX^2$, czyli też $X \cdot (kX + lX^2) \in [kX + lX^2]$. Zauważmy jeszcze, że $\langle p^m X \rangle \lhd R$ oraz $pX^2 = p^m X$. Wynika stąd, że $pR^2 = \langle p^m X \rangle$ i ponieważ $o(X) = p^{m+n}$, więc $|pR^2| = p^n$. Stąd R nie jest pierścieniem z prawie zerowym mnożeniem, gdyż $n > 1$

Pierścienie z punktów (ii) i (iii) spełniają warunek (ii) Stwierdzenia 2.16, więc są one pierścieniami z prawie zerowym mnożeniem, zaś pierścienie z punktu (iv) nie są z prawie zerowym mnożeniem, więc żaden pierścień z punktów (ii) lub (iii) nie jest izomorficzny z żadnym pierścieniem z punktu (iv). Dodatkowo grupy addytywne pierścieni z punktów (ii) i (iii) są izomorficzne odpowiednio z grupami $\mathbb{Z}_p^+ \times \mathbb{Z}_p^+$ oraz $\mathbb{Z}_{p^m}^+ \times \mathbb{Z}_p^+$ $(m = 2, 3, \ldots)$. Wobec tego pierścienie: $x\mathbb{Z}_p[x]/(x^3)$, $x\mathbb{Z}_{p^m}[x]/(px^2, x^3)$ $(m = 2, 3, \ldots)$ są parami nieizomorficzne.

Pozostało do pokazania, że pierścienie z klasy (iv) są parami nieizomorficzne. Weźmy dowolne $m_1, m_2, n_1, n_2 \in \mathbb{N}$ takie, że $m_1, m_2 \geq 2$ oraz $R_1 \cong R_2$ dla $R_1 = x\mathbb{Z}_{p^{m_1+n_1}}[x]/(px^2 - p^{m_1}x, x^3 - p^{2m_1-2}x)$ i $R_2 = x\mathbb{Z}_{p^{m_2+n_2}}[x]/(px^2 - p^{m_2}x, x^3 - p^{2m_2-2}x)$. Wtedy $|R_1| = |R_2|$, więc na mocy wcześniejszych rozważań , $p^{m_1+n_1+1} = p^{m_2+n_2+1}$, skąd $m_1 + n_1 = m_2 + n_2$. Ponadto $pR_1^2 \cong pR_2^2$, więc $|pR_1^2| = |pR_2^2|$ i ponownie wykorzystując

poprzednie obliczenia, $p^{n_1} = p^{n_2}$, więc $n_1 = n_2$ i ostatecznie $m_1 = m_2$ i $n_1 = n_2$. □

Lemat 2.20. *Niech S będzie pierścieniem opisanym w Twierdzeniu 2.16 w punkcie (2) lub (3). Jeżeli podgrupa $\langle x^2 \rangle$ jest istotna w grupie $a(S)^+$, to pierścień S nie rozkłada się na sumę prostą swoich dwóch niezerowych ideałów.*

Dowód. Załóżmy, że istnieją niezerowe ideały I, J pierścienia S takie, że $I \oplus J = S$. Wtedy $I^2 \oplus J^2 = S^2 = \langle x^2 \rangle$. Ponieważ $o(x^2) = p$, więc $I^2 = 0$ lub $J^2 = 0$. Załóżmy, że $J^2 = 0$. Na mocy Uwagi 2.10, $J \subseteq a(S)$. Ponieważ $J \neq 0$ oraz podgrupa $\langle x^2 \rangle^+$ jest istotna w grupie $a(S)^+$, więc $J \cap \langle x^2 \rangle \neq 0$. Ale $I^2 = \langle x^2 \rangle$, więc $I \cap J \neq 0$, sprzeczność. □

Łatwo jest zauważyć, że każdy pierścień spełniający warunek *(1)* lub *(2)* Twierdzenia 2.16 jest przemienny. Kwestia przemienności pierścieni spełniających warunek *(3)* tego stwierdzenia jest bardziej skomplikowana i zostanie dokładniej przedstawiona w kolejnych stwierdzeniach.

Uwaga 2.21. Pokażemy, że pierścień $S = \langle x, y \rangle + a(S)$ opisany w Twierdzeniu 2.16 punkt *(3)* dla $p = 2$ jest nieprzemienny i można dla niego tak wybrać elementy $x, y \in R$ by spełniały relacje:

$$y^2 = xy = x^2,\ yx = 0. \tag{2.2}$$

Rzeczywiście, gdy $xy = yx$, to $F_1 \equiv F_2 \pmod 2$ i kongruencja (2.1) przybiera postać $X^2 + A \equiv 0 \pmod 2$, ma więc rozwiązanie, co prowadzi do sprzeczności. Załóżmy zatem, że $F_1 \not\equiv F_2 \pmod 2$. Wówczas elementy x, y spełniają jeden z warunków:

(*i*) $y^2 = x^2$, $xy = x^2$, $yx = 0$,

(*ii*) $y^2 = x^2$, $xy = 0$, $yx = x^2$.

Zauważmy, że w przypadku (*ii*) zmieniając miejscami elementy x z y w punkcie (*ii*), uzyskujemy punkt (*i*).

Liczba parametrów występujących w opisie pierścieni z Twierdzenia 2.16 punkt *(3)* może zostać istotnie zredukowana, co pokazują następne stwierdzenia.

Stwierdzenie 2.22. *Niech $p > 2$ i niech μ będzie ustaloną niereszą kwadratową modulo p. Pierścień S spełniający warunek (3) Twierdzenia 2.16 jest przemienny wtedy i tylko wtedy, gdy istnieją $x_0, y_0 \in S$ takie, że $S = \langle x_0, y_0 \rangle + a(S)$, $x_0^2 \neq 0$, $y_0^2 \neq 0$, $px_0, py_0, x_0^2, y_0^2 \in a(S)$, $y_0^2 = -\mu x_0^2$, $x_0 y_0 = y_0 x_0 = 0$.*

Dowód. Załóżmy, że pierścień S jest przemienny. Wówczas $F_1 \equiv F_2 \pmod p$. Oznaczmy $F = F_1$. Załóżmy, że $F \not\equiv 0 \pmod p$. Niech $x_1 = x$ oraz $y_1 = Fx - y$. Wówczas $S = \langle x_1, y_1 \rangle + a(S)$ i na podstawie Uwagi 2.18 punkt (ii), $y_1^2 = Bx_1^2$ dla pewnego $B \in \mathbb{Z}$. Ponadto $x_1 y_1 = y_1 x_1 = (Fx - y)x = Fx^2 - yx = Fx^2 - Fx^2 = 0$. Zatem zgodnie z Uwagą 2.18 punkt (ii), kongruencja $X^2 + B \equiv 0 \pmod p$ nie ma rozwiązania. Ale $p > 2$, więc $\left(\frac{-B}{p}\right) = -1$. Zatem istnieje $K \in \mathbb{Z}$ taki, że $(-B)K^2 \equiv \mu \pmod p$. Przyjmując $x_0 = x_1$, $y_0 = Ky_1$ dostajemy $S = \langle x_0, y_0 \rangle + a(S)$, $x_0 y_0 = y_0 x_0 = 0$ oraz $y_0^2 = -\mu x_0^2$.

Implikacja w drugą stronę jest oczywista. □

Stwierdzenie 2.23. *Pierścień S spełniający warunek (3) Twierdzenia 2.16 dla $p > 2$ jest nieprzemienny wtedy i tylko wtedy, gdy istnieją $x_1, y_1 \in S$ takie, że $S = \langle x_1, y_1\rangle + a(S)$, $x_1^2 \neq 0$, $y_1^2 \neq 0$, $px_1, py_1, x_1^2, y_1^2 \in a(S)$, $y_1^2 = Bx_1^2$, $x_1y_1 = -x_1^2$, $y_1x_1 = x_1^2$ dla pewnego $B \in \mathbb{Z}$ takiego, że $\left(\frac{-B}{p}\right) = -1$.*

Dowód. Załóżmy, że S jest pierścieniem nieprzemiennym. Wtedy $F_1 \not\equiv F_2 \pmod p$. Istnieją zatem $\alpha, \beta \in \mathbb{Z}$ takie, że $\alpha(F_1 - F_2) \equiv F_1 + F_2 \pmod p$ i $\beta(F_2 - F_1) \equiv 2 \pmod p$. Wówczas $p \nmid \beta$, bo $p > 2$ oraz $\alpha + \beta F_1 \equiv -1 \pmod p$, $\alpha + \beta F_2 \equiv 1 \pmod p$. Niech $x_1 = x$, $y_1 = \alpha x + \beta y$. Wtedy $S = \langle x_1, y_1\rangle + a(S)$, gdyż $\begin{vmatrix} 1 & 0 \\ \alpha & \beta \end{vmatrix} \equiv \beta \not\equiv 0 \pmod p$. Na mocy Uwagi 2.18 punkt (ii), istnieje $B \in \mathbb{Z}$ takie, że $y_1^2 = Bx_1^2$. Policzmy:

$$x_1y_1 = x(\alpha x + \beta y) = \alpha x^2 + \beta xy = (\alpha + \beta F_1)x^2 = -x^2 = -x_1^2,$$

$$y_1x_1 = (\alpha x + \beta y)x = \alpha x^2 + \beta yx = (\alpha + \beta F_2)x^2 = x^2 = x_1^2.$$

Zatem na mocy Uwagi 2.18 punkt (ii), kongruencja $X^2 + B \equiv 0 \pmod p$ nie ma rozwiązania, skąd, wobec $p > 2$ otrzymujemy $-B$ jest niereszą kwadratową modulo p.

Ponieważ $p > 2$, więc implikacja odwrotna jest oczywista. □

Uwaga 2.24. Okazuje się, że w odróżnieniu od Stwierdzenia 2.22, w przypadku nieprzemiennym, dla różnych niereszt kwadratowych modulo p otrzymujemy nieizomorficzne pierścienie. Niech S_1 będzie pierścieniem, w którym istnieją elementy x_1, y_1 takie, że $S_1 = \langle x_1, y_1\rangle + a(S_1)$, $x_1^2 \neq 0$, $y_1^2 \neq 0$, $px_1, py_1, x_1^2, y_1^2 \in a(S_1)$, $y_1^2 = Ax_1^2$, $x_1y_1 = -Fx_1^2$, $y_1x_1 = Fx_1^2$ dla pewnych $A, F \in \mathbb{Z}$ takich, że $\left(\frac{-A}{p}\right) = -1$ i $p \nmid F$. Niech S_2 będzie pierścieniem, w którym istnieją elementy X_1, Y_1 takie, że $S_2 = \langle X_1, Y_1\rangle + a(S_2)$, $X_1^2 \neq 0$, $Y_1^2 \neq 0$, $pX_1, pY_1, X_1^2, Y_1^2 \in a(S_2)$, $Y_1^2 = BX_1^2$, $X_1Y_1 = -FX_1^2$, $Y_1X_1 = FX_1^2$ dla pewnego $B \in \mathbb{Z}$ takiego, że $\left(\frac{-B}{p}\right) = -1$.

Pokażemy, że jeśli $S_1 \cong S_2$, to $A \equiv B \pmod p$. Załóżmy, że $f\colon S_1 \to S_2$ jest izomorfizmem pierścieni. Wówczas $f(x_1) = aX_1 + bY_1 + n_1$, $f(y_1) = cX_1 + dY_1 + n_2$, dla pewnych $n_1, n_2 \in a(S_2)$ oraz $a, b, c, d \in \mathbb{Z}$ takich, że $\begin{vmatrix} a & b \\ c & d \end{vmatrix} \equiv ad - bc \not\equiv 0 \pmod p$. Wówczas

$$\begin{cases} -F(aX_1 + bY_1 + n_1)^2 &= (aX_1 + bY_1 + n_1)(cX_1 + dY_1 + n_2) \\ F(aX_1 + bY_1 + n_1)^2 &= (cX_1 + dY_1 + n_2)(aX_1 + bY_1 + n_1) \\ A(aX_1 + bY_1 + n_1)^2 &= (cX_1 + dY_1 + n_2)^2 \end{cases}$$

Stąd

$$\begin{cases} -F(a^2 + Bb^2) &\equiv ac - Fad + Fbc + bdB &\pmod p \\ F(a^2 + Bb^2) &\equiv ac - Fbc + Fad + bdB &\pmod p \\ A(a^2 + Bb^2) &\equiv c^2 + Bd^2 &\pmod p \end{cases} \tag{2.3}$$

Dodając do siebie dwie pierwsze kongruencje i dzieląc przez 2 otrzymujemy $ac + bdB \equiv 0 \pmod p$. Ponieważ jednocześnie $p \nmid F$, więc z pierwszej kongruencji ostatniego układu:

$$a^2 + b^2B \equiv ad - bc \pmod p. \tag{2.4}$$

Z powyższych rozważań i tożsamości:

$$(a^2 + b^2B)(c^2 + d^2B) = (ac + bdB)^2 + B(ad - bc)^2$$

wynika, że

$$(ad - bc)(c^2 + d^2B) \equiv B(ad - bc)^2 \pmod{p}.$$

Ale $p \nmid ad - bc$, więc $c^2 + d^2B \equiv B(ad - bc) \pmod{p}$. Ponadto, z ostatniej kongruencji układu (2.3), $A(a^2 + Bb^2) \equiv B(ad - bc) \pmod{p}$. Z kongruencji (2.4), $A(ad - bc) \equiv B(ad - bc) \pmod{p}$ i ponieważ $p \nmid ad - bc$, więc ostatecznie $A \equiv B \pmod{p}$.

Z Twierdzenia 2.19 i jego dowodu oraz ze Stwierdzenia 2.15 uzyskujemy następujące

Stwierdzenie 2.25. *Wszystkimi, z dokładnością do izomorfizmu, niezerowymi p-pierścieniami z prawie zerowym mnożeniem generowanymi przez jeden element są:*

(i) $p^m\mathbb{Z}_{p^{m+n}}$, $m, n \in \mathbb{N}$, *gdzie* $n = m$ *lub* $n = m + 1$,

(ii) $x\mathbb{Z}_p[x]/(x^3)$,

(iii) $x\mathbb{Z}_{p^m}[x]/(px^2, x^3)$, $m \in \mathbb{N}$, $m \geq 2$.

2.3 Pierścienie z prawie zerowym mnożeniem o grupie addytywnej ograniczonego wykładnika

2.3.1 Przypadek $\dim_{\mathbb{Z}_p} R/a(R) = 1$

Przykład 2.26. Niech s będzie dowolną bezkwadratową liczbą naturalną i niech M będzie dowolną grupą abelową posiadającą element α rzędu s. Niech $\langle x\rangle$ będzie grupą cykliczną nieskończoną lub rzędu $n \in \mathbb{N}$, gdzie $s \mid n$. W grupie abelowej $R^+ = \langle x\rangle \times M$ wprowadzamy mnożenie przyjmując, że dla dowolnych $k_1, k_2 \in \mathbb{Z}$, $m_1, m_2 \in M$ mamy

$$(k_1x, m_1) \cdot (k_2x, m_2) = (0, (k_1k_2)\alpha). \tag{2.5}$$

Ponieważ $s \mid n$, więc mnożenie zadane w ten sposób jest dobrze określone i rozdzielne względem dodawania. Ponadto jest ono przemienne oraz $(ab)c = a(bc) = 0$ dla dowolnych $a, b, c \in R$. Wobec tego otrzymujemy przemienny pierścień R taki, że $R^3 = 0$.

Weźmy dowolne $a = (k_1x, m_1) \in R$. Wówczas $a^2 = (0, k_1^2\alpha)$. Ponieważ $o(\alpha) = s$ jest liczbą bezkwadratową, więc na mocy Lematu 1.1, $\langle a^2\rangle = \langle(0, k_1\alpha)\rangle$. Ponadto, dla dowolnego $b = (k_2x, m_2) \in R$, $ab = (0, k_1k_2\alpha) = k_2(0, k_1\alpha) \in \langle a^2\rangle$. To pokazuje, że otrzymany pierścień jest z prawie zerowym mnożeniem. Będziemy go oznaczali przez $\langle x\rangle \times_\alpha M$. Odnotujmy też, że $a(\langle x\rangle \times_\alpha M) = \langle sx\rangle \times M$.

Lemat 2.27. *Niech s będzie dowolną bezkwadratową liczbą naturalną i niech M_1, M_2 będą izomorficznymi grupami abelowymi. Niech $\langle x_1\rangle$, $\langle x_2\rangle$ będą izomorficznymi grupami cyklicznymi nieskończonymi lub rzędu n, gdzie $s \mid n$. Jeżeli $\alpha \in M_1$, $\beta \in M_2$ są elementami rzędu s dla których istnieje izomorfizm $f\colon M_1 \to M_2$ taki, że $f(\alpha) = \beta$, to pierścienie $\langle x_1\rangle \times_\alpha M_1$ oraz $\langle x_2\rangle \times_\beta M_2$ są izomorficzne.*

Dowód. Niech odwzorowanie $F\colon \langle x_1\rangle \times_\alpha M_1 \to \langle x_2\rangle \times_\beta M_2$ będzie dane wzorem

$$F((kx_1, m)) = (kx_2, f(m)) \text{ dla dowolnych } k \in \mathbb{Z},\ m \in M_1.$$

Łatwo sprawdzić, że F jest izomorfizmem grup addytywnych. Ponadto dla dowolnych $k_1, k_2 \in \mathbb{Z}$, $m_1, m_2 \in M_1$, $F((k_1x_1, m_1)(k_2m_1, m_2)) = F((0, k_1k_2\alpha)) = (0, k_1k_2f(m)) = (0, k_1k_2\beta)$ oraz $F((k_1x_1, m_1))F((k_2x_1, m_2)) = (k_1x_2, f(m_1))(k_2x_2, f(m_2)) = (0, k_1k_2\beta)$, co pokazuje, że F jest izomorfizmem pierścieni. □

Ponieważ każda nietrywialna podgrupa grupy quasicyklicznej posiada dokładnie jedną podgrupę rzędu p, więc z poprzedniego lematu otrzymujemy następujący wniosek.

Wniosek 2.28. *Jeżeli $\langle x\rangle$ jest grupą cykliczną nieskończoną lub rzędu n, gdzie $p \mid n$ i M jest podgrupą quasicyklicznej p-grupy, to dla dowolnych elementów $\alpha, \beta \in M$ rzędu p, pierścienie $\langle x\rangle \times_\alpha M$ oraz $\langle x\rangle \times_\beta M$ są izomorficzne.*

Stwierdzenie 2.29. *Jeżeli R jest p-pierścieniem z prawie zerowym mnożeniem ograniczonego wykładnika takim, że $R^2 \neq 0$, to $R = S \oplus I$, gdzie $I^2 = 0$ i S jest skończonym pierścieniem z prawie zerowym mnożeniem, nierozkładalnym na sumę prostą dwóch swoich niezerowych ideałów. Ponadto pierścień S spełnia te same warunki Twierdzenia 2.16, które spełnia pierścień R.*

Dowód. Na podstawie Twierdzenia 2.16, $R = \langle x\rangle + a(R)$ gdzie x spełnia warunek *(2)* Twierdzenia 2.16 lub $R = \langle x, y\rangle + a(R)$ gdzie x, y spełniają warunek *(3)* Twierdzenia 2.16. Oba przypadki będziemy rozważali równocześnie. Oznaczmy przez C podgrupę $\langle x\rangle$ (odpowiednio $\langle x, y\rangle$). Na mocy Twierdzenia 1.5, istnieje skończona podgrupa $A \leq a(R)$ taka, że $px, x^2 \in A$ (odpowiednio $px, py, x^2 \in A$) oraz $a(R)^+ = A \oplus B$ dla pewnej podgrupy $B \leq a(R)$. Wtedy $R = (C + A) + B$. Ponieważ $R^2 \subseteq \langle x^2\rangle \subseteq A$, więc $C + A$ jest podpierścieniem R. Pokażemy, że $(C + A) \cap B = 0$. Jeżeli $c + a = b$ dla pewnych $a \in A$, $b \in B$ i $c \in C$, to $c \in a(R)$. Ponadto $c = kx$ dla pewnego $k \in \mathbb{Z}$ (odpowiednio $c = kx + ly$ dla pewnych $k, l \in \mathbb{Z}$), więc z Uwagi 2.18 wynika, że $p \mid k$ (odpowiednio $p \mid k$ i $p \mid l$), skąd $c \in A$ i $c + a = b \in A \cap B = 0$. Zatem $R = (C + A) \oplus B$.

Dalej, pierścień $C + A$ jest skończony. Stąd $C + A = S_1 \oplus S_2 \oplus \cdots \oplus S_k$ dla pewnych skończonych podpierścieni $S_1, S_2, \ldots, S_k$ pierścienia $C + A$, z których każdy jest nierozkładalny na sumę prostą swoich niezerowych ideałów. Ale, $|(C + A)^2| = p$, więc bez tracenia ogólności możemy założyć, że $|S_1^2| = p$ i $S_t^2 = 0$ dla $t \in \{2, 3, \ldots, k\}$. Przyjmując $S = S_1$ i $I = S_2 \oplus \cdots \oplus S_k \oplus B$ mamy, że $R = S \oplus I$, gdzie $I \subseteq a(R)$. Ponadto, ponieważ $x^2 \neq 0$, (odpowiednio $x^2 \neq 0$ i $y^2 \neq 0$), więc $x = x_1 + i$ dla pewnych $0 \neq x_1 \in S$, $i \in I$ (odpowiednio $x = x_1 + i$ i $y = y_1 + j$ dla pewnych niezerowych $x_1, y_1 \in S$ oraz $i, j \in I$). Wówczas $S = \langle x_1\rangle + a(S)$ (odpowiednio $S = \langle x_1, y_1\rangle + a(S)$) oraz x_1 spełnia ten sam warunek *(2)* Twierdzenia 2.16 co x (x_1 i y_1 spełniają ten sam warunek *(3)* Twierdzenia 2.16 co x i y). □

Lemat 2.30. *Niech dla $i = 1, 2$, T_i będzie jednym z pierścieni:*

(i) $p^m\mathbb{Z}_{p^{2m+1}}$, $p \in \mathbb{P}$, $m \in \mathbb{N}$,

(ii) $\mathbb{Z}_{p^m} \times_{p^{n-1}} \mathbb{Z}_{p^n}$, $p \in \mathbb{P}$, $m, n \in \mathbb{N}$,

natomiast C_i będzie dowolnym pierścieniem z zerowym mnożeniem. Wówczas $T_1 \oplus C_1 \cong T_2 \oplus C_2$ wtedy i tylko wtedy, gdy $T_1 = T_2$ i $C_1 \cong C_2$.

Dowód. Niech dla $i = 1, 2$, $R_i = T_i \oplus C_i$ oraz $R_1 \cong R_2$. Zauważmy, że jeśli T_1 jest p-pierścieniem, a T_2 jest q-pierścieniem, to $p = q$, gdyż $|R_1^2| = p$ i $|R_2^2| = q$.

Załóżmy najpierw, że $T_1 = p^{m_1}\mathbb{Z}_{p^{2m_1+1}}$ i $T_2 = p^{m_2}\mathbb{Z}_{p^{2m_2+1}}$ dla pewnych $p \in \mathbb{P}$, $m_1, m_2 \in \mathbb{N}$. Ponieważ $|R_1^2| = |R_2^2| = p$ oraz $R_1^2 \subseteq p^{m_1}\mathbb{Z}_{p^{2m_1+1}}$, $R_2^2 \subseteq p^{m_2}\mathbb{Z}_{p^{2m_2+1}}$, więc ze Stwierdzenia 1.2 wynika, że $p^{m_1+1} = \max\{o(v) \ : \ v \in (R_1)_p, \ R_1^2 \subseteq \langle v \rangle\}$, $p^{m_2+1} = \max\{o(v) \ : \ v \in (R_2)_p, \ R_2^2 \subseteq \langle v \rangle\}$. Zatem $m_1 = m_2$, skąd $T_1 = T_2$ i na podstawie Twierdzenia 1.6, $C_1 \cong C_2$.

Teraz załóżmy, że $T_1 = \mathbb{Z}_{p^{m_1}} \times_{p^{n_1-1}} \mathbb{Z}_{p^{n_1}}$, $T_2 = \mathbb{Z}_{p^{m_2}} \times_{p^{n_2-1}} \mathbb{Z}_{p^{n_2}}$ dla pewnych $n_1, n_2, m_1, m_2 \in \mathbb{N}$. Ponieważ $|R_1^2| = |R_2^2| = p$ oraz $R_1^2 \subseteq \mathbb{Z}_{p^{n_1}}$, $R_2^2 \subseteq \mathbb{Z}_{p^{n_2}}$, więc ze Stwierdzenia 1.2 wynika, że $p^{n_1} = \max\{o(v) \ : \ v \in R_1, \ R_1^2 \subseteq \langle v \rangle\}$, $p^{n_2} = \max\{o(v) \ : \ v \in R_2, \ R_2^2 \subseteq \langle v \rangle\}$. Zatem $n_1 = n_2$. Dalej, bez tracenia ogólności załóżmy, że $m_1 < m_2$. Wówczas $(R_1(p^{m_1}))^2 \neq 0$, ale $(R_2(p^{m_1}))^2 = 0$, sprzeczność. Zatem $m_1 = m_2$. Stąd $T_1 = T_2$ i na mocy Twierdzenia 1.6, $C_1 \cong C_2$.

W końcu załóżmy, że $T_1 = p^{m_1}\mathbb{Z}_{p^{2m_1+1}}$, $T_2 = (\mathbb{Z}_{p^{m_2}} \times_{p^{n_2-1}} \mathbb{Z}_{p^{n_2}})$ dla pewnych $m_1, n_2, m_2 \in \mathbb{N}$. Ponieważ $|R_1^2| = |R_2^2| = p$ oraz $R_1^2 \subseteq p^{m_1}\mathbb{Z}_{p^{2m_1+1}}$, $R_2^2 \subseteq \mathbb{Z}_{p^{n_2}}$, więc ze Stwierdzenia 1.2 wynika, że $p^{m_1+1} = \max\{o(v) \ : \ v \in (R_1)_p, \ R_1^2 \subseteq \langle v \rangle\}$, $p^{n_2} = \max\{o(v) \ : \ v \in (R_2)_p, \ R_2^2 \subseteq \langle v \rangle\}$. Zatem $m_1 + 1 = n_2$. Jeżeli $m_2 < m_1 + 1$, to $(R_1(p^{m_2}))^2 = 0$, ale $(R_2(p^{m_2}))^2 \neq 0$, sprzeczność. Jeżeli zaś $m_2 > m_1 + 1$, to $(R_1(p^{m_1+1}))^2 \neq 0$, ale $(R_2(p^{m_1+1}))^2 = 0$, sprzeczność. Stąd $m_2 = m_1 + 1$. Zauważmy, że w pierścieniu R_1 istnieje element $y = p^{m_1}$ taki, że $y^2 = p^{m_1}y \neq 0$. Zatem istnieje $z \in R_2 = (\mathbb{Z}_{p^{m_1+1}} \times_{p^{m_1}} \mathbb{Z}_{p^{m_1+1}}) \oplus C_2$ takie, że $z^2 = p^{m_1}z \neq 0$. Wówczas $z = (U, V) + a$ dla pewnych $U, V \in \mathbb{Z}_{p^{m_1+1}}$, $a \in C_2$ i $z^2 = (0, U^2p^{m_1})$, $p^{m_1}z = (p^{m_1}U, p^{m_1}V) + p^{m_1}a$. Stąd $p^{m_1}U = 0$ i w konsekwencji $p \mid U$, ale wówczas $z^2 = (0, U^2p^{m_1}) = 0$, sprzeczność.

Implikacja przeciwna jest oczywista. □

Twierdzenie 2.31. *Wszystkimi, z dokładnością do izomorfizmu, p-pierścieniami R z prawie zerowym mnożeniem o ograniczonym wykładniku grupy R^+ i takimi, że* $\dim_{\mathbb{Z}_p} R/a(R) = 1$ *są pierścienie postaci $R = T \oplus C$, gdzie T jest jednym z pierścieni*

(i) $p^m\mathbb{Z}_{p^{2m+1}}$, $m \in \mathbb{N}$,

(ii) $\mathbb{Z}_{p^m} \times_{p^{n-1}} \mathbb{Z}_{p^n}$, $m, n \in \mathbb{N}$,

natomiast C jest p-pierścieniem z zerowym mnożeniem ograniczonego wykładnika grupy addytywnej.

Ponadto pierścienie wymienione w punktach (i) , (ii) są nierozkładalne na sumę prostą swoich dwóch niezerowych ideałów.

Dowód. Na mocy Przykładu 2.26, Stwierdzenia 2.25 oraz Lematu 2.11, każdy pierścień $R = T \oplus C$, gdzie T oraz C są takie jak w sformułowaniu twierdzenia, jest pierścieniem z prawie zerowym mnożeniem dla którego $\dim_{\mathbb{Z}_p} R/a(R) = 1$.

Na odwrót, Stwierdzenie 2.29 pozwala ograniczyć się do przypadku, w którym R jest nierozkładalny na sumę prostą swoich niezerowych ideałów. Z Uwagi 2.18 wynika, że $R = \langle r \rangle + a(R)$ dla każdego $r \in R$ takiego, że $r^2 \neq 0$.

Jeśli grupa R^+ jest cykliczna, to na podstawie Stwierdzenia 2.25, $R \cong p^m \mathbb{Z}_{p^{2m+1}}$ dla pewnej liczby naturalnej m.

Załóżmy dalej, że grupa R^+ nie jest cykliczna. Ponieważ $|R^2| = p$, więc na mocy Lematu 1.3, istnieją $b \in R$ oraz $C \leq R^+$ takie, że $R^2 \subseteq \langle b \rangle$ i $R^+ = \langle b \rangle \oplus C$, przy czym $C \neq 0$. Na podstawie Twierdzenia 1.5, $C = \bigoplus_{i \in I} \langle c_i \rangle$ dla pewnych $c_i \in C$. Weźmy dowolne $j \in I$. Jeśli $c_j^2 = 0$, to $A = \langle c_j \rangle \lhd R$ oraz $J = \langle b \rangle + \bigoplus_{i \in I \setminus \{j\}} \langle c_i \rangle \lhd R$, przy czym $R = A \oplus J$, co przeczy nierozkładalności R na sumę prostą dwóch niezerowych ideałów. Zatem $c_j^2 \neq 0$ dla wszystkich $j \in I$. Załóżmy, że $|I| > 1$. Niech $c = c_{i_0}$ będzie elementem maksymalnego rzędu spośród elementów $\{c_i \mid i \in I\}$. Istnieje $i \in I \setminus \{i_0\}$, przy czym $c_i^2 \neq 0$. Ale $\dim_{\mathbb{Z}_p} R/a(R) = 1$, więc istnieje $k \in \mathbb{Z}$ takie, że $c - kc_i \in a(R)$, czyli $(c - kc_i)^2 = 0$. Ponadto z Lematu 1.4, otrzymujemy $\langle c \rangle \oplus \langle c_i \rangle = \langle c - kc_i \rangle \oplus \langle c_i \rangle$, więc $C = \langle c - kc_i \rangle \oplus \langle c_i \rangle \oplus \bigoplus_{j \in I \setminus \{i_0, i\}} \langle c_j \rangle$. Stąd, podobnie jak wcześniej, uzyskujemy sprzeczność z nierozkładalnością R na sumę prostą dwóch niezerowych ideałów. Wobec tego $|I| = 1$ i $R^+ = \langle b \rangle \oplus \langle c \rangle$. Jeśli $b^2 = 0$, to na mocy Przykładu 2.26 i Wniosku 2.28 uzyskujemy, że $R \cong \mathbb{Z}_{p^m} \times_{p^{n-1}} \mathbb{Z}_{p^n}$ dla pewnych $m, n \in \mathbb{N}$.

Niech dalej $b^2 \neq 0$. Ponieważ $\dim_{\mathbb{Z}_p} R/a(R) = 1$, więc istnieją $l, t \in \mathbb{Z}$ takie, że $b - lc, c - tb \in a(R)$. Jeśli $o(b) \leq o(c)$, to z Lematu 1.4 wynika, że $R^+ = \langle b \rangle \oplus \langle c - tb \rangle$, przy czym $\langle b \rangle$ i $\langle c - tb \rangle$ są podpierścieniami (a więc też ideałami) pierścienia R, otrzymujemy sprzeczność z nierozkładalnością R na sumę prostą dwóch niezerowych ideałów. Wobec tego $o(b) > o(c)$ i Lematu 1.4, $R^+ = \langle b - lc \rangle \oplus \langle c \rangle$. Ale $o(b) = p^n$ i $o(c) = p^m$ dla pewnych $m, n \in \mathbb{N}$, $n > m$ i $R^2 \subseteq \langle b \rangle$ oraz $|R^2| = p$, więc $R^2 = p^{n-1}\langle b \rangle = p^{n-1}\langle b - lc \rangle$. Stąd na mocy Przykładu 2.26 i Wniosku 2.28 mamy, $R \cong \mathbb{Z}_{p^m} \times_{p^{n-1}} \mathbb{Z}_{p^n}$.

Problem izomorfizmu dla pierścieni opisanych w twierdzeniu rozstrzyga Lemat 2.30.

Pozostało do wykazania, że żaden z pierścieni opisanych w punktach $(i), (ii)$ nie rozkłada się na sumę prostą swoich dwóch niezerowych ideałów. Załóżmy, że R jest pierścieniem z jednej z klas $(i), (ii)$ oraz $R = A \oplus B$ dla pewnych swoich niezerowych ideałów A i B. Ponieważ $|R^2| = p$ oraz $R^2 = A^2 \oplus B^2$, więc bez tracenia ogólności możemy przyjąć, że $A^2 \neq 0$ oraz $B^2 = 0$. Ale A, jako podpierścień pierścienia R, jest pierścieniem z prawie zerowym mnożeniem o ograniczonym wykładniku grupy A^+ takim, że $\dim_{\mathbb{Z}_p} A/a(A) = 1$, więc z udowodnionej już części twierdzenia, $A \cong T \oplus C$, gdzie T oraz C są takie jak w sformułowaniu twierdzenia. Stąd $R \cong T \oplus (C \oplus B)$, co na mocy jednoznaczności przedstawienia pierścienia R w postaci podanej w twierdzeniu daje $R = T$ oraz $0 = C \oplus B$. Sprzeczność z tym, że $B \neq 0$. □

2.3.2 Przypadek $\dim_{\mathbb{Z}_p} R/a(R) = 2$

Przykład 2.32. Niech p będzie dowolną liczbą pierwszą i niech $F_1, F_2, A \in \mathbb{Z}$ będą takie, że kongruencja

$$X^2 + (F_1 + F_2)X + A \equiv 0 \pmod{p} \tag{2.6}$$

nie nie ma rozwiązania. Niech $U \in \mathbb{Z}_p \setminus \{0\}$. Niech $m, n \in \mathbb{N}$, przy czym $n > 1$. Niech ponadto $R^+ = \mathbb{Z}_{p^m}^+ \times \mathbb{Z}_{p^n}^+$ lub $R^+ = \mathbb{Z}^+ \times \mathbb{Z}_{p^n}^+$. W grupie R^+ określamy mnożenie przy

pomocy wzoru:

$$(k_1, l_1) \cdot (k_2, l_2) = (0, U \cdot (k_1 l_2 F_2 + l_1 k_2 F_1 + A k_1 k_2 + l_1 l_2) \cdot p^{n-1}). \tag{2.7}$$

Łatwo sprawdzić, że tak zdefiniowane mnożenie jest dobrze określone i rozdzielne względem dodawania oraz $(ab)c = a(bc) = 0$ dla dowolnych $a, b, c \in R$. Otrzymujemy w ten sposób pierścień R, który będziemy oznaczali odpowiednio symbolami:

$$(\mathbb{Z}_{p^m} \times_{Up^{n-1}} \mathbb{Z}_{p^n})_{F_1,F_2,A} \quad \text{lub} \quad (\mathbb{Z} \times_{Up^{n-1}} \mathbb{Z}_{p^n})_{F_1,F_2,A}.$$

Ponadto, ponieważ kongruencja (2.6) nie ma rozwiązania, więc $\langle (k,l)^2 \rangle = \langle (0, p^{n-1}) \rangle$ o ile $p \nmid k$ lub $p \nmid l$ oraz $(k,l)^2 = (0,0)$ jeśli $p \mid k$ i $p \mid l$.

Niech $y = (1,0)$, $x = (0,1)$. Wtedy $R^+ = \langle y \rangle \oplus \langle x \rangle$, $x^2 = U \cdot p^{n-1} x$, $y^2 = Ax^2$, $xy = F_1 x^2$, $yx = F_2 x^2$, $o(x^2) = p$ oraz $x^2, px, py \in a(R)$. Zatem na podstawie Twierdzenia 2.16 punkt *(3)*, R jest pierścieniem z prawie zerowym mnożeniem. Ponadto $a(R) = \langle py \rangle \oplus \langle px \rangle$, $(R/a(R))^+ \cong \mathbb{Z}_p^+ \times \mathbb{Z}_p^+$.

Zauważmy, że istnieje $V \in \mathbb{Z}$ takie, że $UV \equiv 1 \pmod{p}$. Niech $F_1' = UF_1$, $F_2' = UF_2$, $A' = U^2 A$. Łatwo zauważyć, że kongruencja

$$X^2 + (F_1' + F_2')X + A' \equiv 0 \pmod{p},$$

nie ma rozwiązania. Ponadto, przekształcenie $f\colon (\mathbb{Z}_{p^m} \times_{p^{n-1}} \mathbb{Z}_{p^n})_{F_1',F_2',A'} \to (\mathbb{Z}_{p^m} \times_{Up^{n-1}} \mathbb{Z}_{p^n})_{F_1,F_2,A}$ dane wzorem $f((k,l)) = (k, Vl)$ jest izomorfizmem pierścieni. Podobnie przekształcenie $g\colon (\mathbb{Z} \times_{p^{n-1}} \mathbb{Z}_{p^n})_{F_1',F_2',A'} \to (\mathbb{Z} \times_{Up^{n-1}} \mathbb{Z}_{p^n})_{F_1,F_2,A}$ dane wzorem $g((k,l)) = (k, Vl)$ jest izomorfizmem pierścieni. Widzimy zatem, że bez zmniejszania ogólności możemy dalej przyjąć $U = 1$.

Zauważmy jeszcze, że jeśli liczba całkowita W nie jest podzielna przez p, to istnieje $V \in \mathbb{Z}$ takie, że $WV \equiv 1 \pmod{p}$ i kongruencja $X^2 + (WF_1 + WF_2)X + W^2 A \equiv 0 \pmod{p}$ nie ma rozwiązania oraz przekształcenie $f\colon (\mathbb{Z}_{p^m} \times_{p^{n-1}} \mathbb{Z}_{p^n})_{F_1,F_2,A} \to (\mathbb{Z}_{p^m} \times_{p^{n-1}} \mathbb{Z}_{p^n})_{WF_1,WF_2,W^2A}$ dane wzorem $f((k,l)) = (Vk, l)$ jest izomorfizmem pierścieni.

Twierdzenie 2.33. *Niech $p \in \mathbb{P}$ i niech $R = (\mathbb{Z}_{p^m} \times_{p^{n-1}} \mathbb{Z}_{p^n})_{F_1,F_2,A}$, gdzie m, n, F_1, F_2, A są takie jak w Przykładzie 2.32. Wówczas:*

(i) jeżeli $p > 2$ i pierścień R jest przemienny, to $F_1 \equiv F_2 \pmod{p}$ oraz

$$R \cong (\mathbb{Z}_{p^m} \times_{p^{n-1}} \mathbb{Z}_{p^n})_{0,0,A-F_1^2},$$

(ii) jeżeli $p = 2$, to pierścień R jest nieprzemienny oraz

$$R \cong (\mathbb{Z}_{2^m} \times_{2^{n-1}} \mathbb{Z}_{2^n})_{0,1,1} \cong (\mathbb{Z}_{2^m} \times_{2^{n-1}} \mathbb{Z}_{2^n})_{1,0,1},$$

(iii) jeżeli $p > 2$ i pierścień R jest nieprzemienny, to $F_1 \not\equiv F_2 \pmod{p}$ oraz

$$R \cong (\mathbb{Z}_{p^m} \times_{p^{n-1}} \mathbb{Z}_{p^n})_{-1,1,[4A-(F_1+F_2)^2]V^2},$$

gdzie $V \in \mathbb{Z}$ jest takie, że $V(F_1 - F_2) \equiv 1 \pmod{p}$.

Dowód. W punkcie (i) skonstruujemy izomorfizm pierścieni

$$f\colon (\mathbb{Z}_{p^m} \times_{p^{n-1}} \mathbb{Z}_{p^n})_{0,0,A-F_1^2} \to (\mathbb{Z}_{p^m} \times_{p^{n-1}} \mathbb{Z}_{p^n})_{F_1,1F,A}.$$

Jeśli $m \geq n$, to wystarczy f określić wzorem $f((k,l)) = (k, (l - F_1 k) \cdot 1)$. Natomiast w przypadku, gdy $m < n$ wystarczy f zadać wzorem $f(k,l) = ((k - F_1 U l) \cdot 1, AUl)$, gdzie U jest taką liczbą całkowitą, że $(A - F_1^2)U \equiv 1 \pmod{p}$.

W punkcie (ii) skonstruujemy izomorfizm pierścieni:

$$f\colon (\mathbb{Z}_{2^m} \times_{2^{n-1}} \mathbb{Z}_{2^n})_{1,0,1} \to (\mathbb{Z}_{2^m} \times_{2^{n-1}} \mathbb{Z}_{2^n})_{0,1,1}.$$

Jeśli $m \geq n$, to wystarczy f zadać wzorem $f((k,l)) = (k, (k + l) \cdot 1)$, a jeśli $m < n$, to wystarczy f określić wzorem $f((k,l)) = ((k + l) \cdot 1, l)$.

Rozważmy teraz punkt (iii). Z założeń wynika, że kongruencja $Y^2 + 4A - (F_1 + F_2)^2 \equiv 0 \pmod{p}$ nie ma rozwiązania. Ponadto, ponieważ $p \nmid F_1 - F_2$, więc istnieją $\alpha, \beta \in \mathbb{Z}$ takie, że $\alpha(F_1 - F_2) \equiv F_1 + F_2 \pmod{p}$ oraz $\beta(F_1 - F_2) \equiv -2 \pmod{p}$. Stąd

$$\alpha + \beta F_1 \equiv -1 \pmod{p} \text{ oraz } \alpha + \beta F_2 \equiv 1 \pmod{p}. \tag{2.8}$$

Niech

$$B = \alpha^2 + \alpha\beta(F_1 + F_2) + \beta^2 A. \tag{2.9}$$

Wówczas

$$B(F_1 - F_2)^2 \equiv 4A - (F_1 + F_2)^2 \pmod{p}, \tag{2.10}$$

skąd

$$B \equiv [4A - (F_1 + F_2)^2]V^2 \pmod{p}.$$

Zatem kongruencja $X^2 + B \equiv 0 \pmod{p}$ nie posiada rozwiązania. W szczególności $p \nmid B$ i istnieje $D \in \mathbb{Z}$ takie, że $BD \equiv 1 \pmod{p}$. Ponadto $p \nmid \beta$, bo $p > 2$.

Jeżeli $m \geq n$, to wykorzystując kongruencje (2.8), (2.10) i równość (2.9) oraz naturalne uproszczenia uzyskamy, że przekształcenie $f\colon (\mathbb{Z}_{p^m} \times_{p^{n-1}} \mathbb{Z}_{p^n})_{-1,1,B} \to (\mathbb{Z}_{p^m} \times_{p^{n-1}} \mathbb{Z}_{p^n})_{F_1,F_2,A}$ dane wzorem $f((k,l)) = (\beta k, (\alpha k + l) \cdot 1)$ jest izomorfizmem pierścieni.

Jeżeli zaś $m < n$, to wykorzystując kongruencje (2.8), (2.10) i równość (2.9) uzyskujemy po uproszczeniach, że przekształcenie $f\colon (\mathbb{Z}_{p^m} \times_{p^{n-1}} \mathbb{Z}_{p^n})_{-1,1,B} \to (\mathbb{Z}_{p^m} \times_{p^{n-1}} \mathbb{Z}_{p^n})_{F_1,F_2,A}$ dane wzorem $f((k,l)) = ((l\alpha\beta D + k\beta) \cdot 1, \beta^2 AD \cdot l)$ jest izomorfizmem pierścieni. □

Przykład 2.34. Niech p, U, F_1, F_2, A będą takie jak w Przykładzie 2.32. Niech $m, n, s \in \mathbb{N}$. Niech ponadto $R^+ = \mathbb{Z}_{p^m} \times \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^s}$ lub $R^+ = \mathbb{Z} \times \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^s}$ lub $R^+ = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_{p^s}$. W grupie R^+ wprowadzamy mnożenie za pomocą wzoru

$$(k_1, l_1, t_1) \cdot (k_2, l_2, t_2) = (0, 0, U(k_1 l_2 F_2 + l_1 k_2 F_1 + A k_1 k_2 + l_1 l_2) \cdot p^{s-1}) \tag{2.11}$$

Łatwo sprawdzić, że tak zdefiniowane mnożenie jest dobrze określone i rozdzielne względem dodawania oraz $(ab)c = a(bc) = 0$ dla dowolnych $a, b, c \in R$. Otrzymujemy w ten sposób pierścień R. Ponadto, ponieważ kongruencja (2.6) nie ma rozwiązania, więc $(k,l,t)^2 = (0,0,0)$ wtedy i tylko wtedy gdy $p \mid k$ i $p \mid l$. Dodatkowo, $(k,l,t)^2 = \langle (0,0,p^{s-1}) \rangle$ o ile $p \nmid k$ lub $p \nmid l$.

Niech $y = (1,0,0)$, $x = (0,1,0)$, $z = (0,0,1)$. Wówczas $x^2 = Up^{s-1}z$, $y^2 = Ax^2$, $xy = F_1x^2$, $yx = F_2x^2$, $a(R) = \langle py\rangle \oplus \langle px\rangle \oplus \langle z\rangle$, $R = \langle x,y\rangle + a(R)$, $(R/a(R))^+ \cong \mathbb{Z}_p^+ \times \mathbb{Z}_p^+$, więc na podstawie Twierdzenia 2.16, pierścień R jest z prawie zerowym mnożeniem, który dalej będziemy oznaczać odpowiednio przez

$$(\mathbb{Z}_{p^m} \times \mathbb{Z}_{p^n})_{F_1,F_2,A} \times_{Up^{s-1}} \mathbb{Z}_{p^s},$$

$$(\mathbb{Z} \times \mathbb{Z}_{p^n})_{F_1,F_2,A} \times_{Up^{s-1}} \mathbb{Z}_{p^s},$$

$$(\mathbb{Z} \times \mathbb{Z})_{F_1,F_2,A} \times_{Up^{s-1}} \mathbb{Z}_{p^s}.$$

Ponadto, przekształcenie

$$f\colon (\mathbb{Z}_{p^m} \times \mathbb{Z}_{p^n})_{F_1,F_2,A} \times_{p^{s-1}} \mathbb{Z}_{p^s} \to (\mathbb{Z}_{p^m} \times \mathbb{Z}_{p^n})_{F_1,F_2,A} \times_{Up^{s-1}} \mathbb{Z}_{p^s}$$

dane wzorem $f((k,l,t)) = (k,l,Ut)$ jest izomorfizmem pierścieni. Podobnie można skonstruować izomorfizm dla pierścieni w pozostałych dwóch przypadkach. Widzimy zatem, że bez zmniejszania ogólności możemy dalej przyjąć $U = 1$.

Zauważmy jeszcze, że jeśli liczba całkowita W nie jest podzielna przez p, to kongruencja $X^2+(WF_1+WF_2)X+W^2A \equiv 0 \pmod p$ nie ma rozwiązania oraz przekształcenia

$$f\colon (\mathbb{Z}_{p^m} \times \mathbb{Z}_{p^n})_{F_1,F_2,A} \times_{p^{s-1}} \mathbb{Z}_{p^s} \to (\mathbb{Z}_{p^m} \times \mathbb{Z}_{p^n})_{WF_1,WF_2,W^2A} \times_{p^{s-1}} \mathbb{Z}_{p^s},$$

$$g\colon (\mathbb{Z} \times \mathbb{Z}_{p^n})_{F_1,F_2,A} \times_{p^{s-1}} \mathbb{Z}_{p^s} \to (\mathbb{Z} \times \mathbb{Z}_{p^n})_{WF_1,WF_2,W^2A} \times_{p^{s-1}} \mathbb{Z}_{p^s}$$

dane wzorami $f((k,l,t)) = (k,Wl,W^2t)$, $g((k,l,t)) = (k,Wl,W^2t)$, są izomorfizmami pierścieni.

Twierdzenie 2.35. *Niech $p \in \mathbb{P}$ i niech $R = (\mathbb{Z}_{p^m} \times \mathbb{Z}_{p^n})_{F_1,F_2,A} \times_{p^{s-1}} \mathbb{Z}_{p^s}$, gdzie m,n,s,F_1,F_2,A są takie jak w Przykładzie 2.34. Wówczas:*

(i) jeżeli $p > 2$ i pierścień R jest przemienny, to $F_1 \equiv F_2 \pmod p$ oraz

$$R \cong (\mathbb{Z}_{p^m} \times \mathbb{Z}_{p^n})_{0,0,A-F_1^2} \times_{p^{s-1}} \mathbb{Z}_{p^s},$$

(ii) jeżeli $p = 2$, to pierścień R jest nieprzemienny oraz

$$R \cong (\mathbb{Z}_{2^m} \times \mathbb{Z}_{2^n})_{0,1,1} \times_{2^{s-1}} \mathbb{Z}_{2^s} \cong (\mathbb{Z}_{2^m} \times \mathbb{Z}_{2^n})_{1,0,1} \times_{2^{s-1}} \mathbb{Z}_{2^s},$$

(iii) jeżeli $p > 2$ i pierścień R jest nieprzemienny, to $F_1 \not\equiv F_2 \pmod p$ oraz

$$R \cong (\mathbb{Z}_{p^m} \times \mathbb{Z}_{p^n})_{-1,1,[4A-(F_1+F_2)^2]V^2} \times_{p^{s-1}} \mathbb{Z}_{p^s},$$

gdzie $V \in \mathbb{Z}$ jest takie, że $V(F_1 - F_2) \equiv 1 \pmod p$.

Dowód. W punkcie (i) konstruujemy izomorfizm pierścieni

$$F\colon (\mathbb{Z}_{p^m} \times \mathbb{Z}_{p^n})_{0,0,A-F_1^2} \times_{p^{s-1}} \mathbb{Z}_{p^s} \to (\mathbb{Z}_{p^m} \times \mathbb{Z}_{p^n})_{F_1,F_1,A} \times_{p^{s-1}} \mathbb{Z}_{p^s}.$$

Jeżeli $m \geq n$, to wystarczy F określić wzorem $F((k,l,t)) = (k,(l-F_1k)\cdot 1,t)$, a jeżeli $m < n$, to wystarczy przyjąć $F((k,l,t)) = ((k-F_1Ul)\cdot 1, AU\cdot l, AUt)$, gdzie U jest taką liczbą całkowitą, że $(A-F_1^2)U \equiv 1 \pmod p$.

W punkcie (ii) skonstruujemy izomorfizm pierścieni

$$F\colon (\mathbb{Z}_{2^m}\times\mathbb{Z}_{2^n})_{1,0,1}\times_{2^{s-1}}\mathbb{Z}_{2^s} \to (\mathbb{Z}_{2^m}\times\mathbb{Z}_{2^n})_{0,1,1}\times_{2^{s-1}}\mathbb{Z}_{2^s}.$$

Jeśli $m \geq n$, to wystarczy F zadać wzorem $F((k,l,t)) = (k,(k+l)\cdot 1,t)$, a jeśli $m < n$, to wystarczy F określić wzorem $F((k,l,t)) = ((k+l)\cdot 1, l, t)$.

W punkcie (iii) skonstruujemy izomorfizm pierścieni

$$F\colon (\mathbb{Z}_{p^m}\times\mathbb{Z}_{p^n})_{-1,1,[4A-(F_1+F_2)^2]V^2}\times_{p^{s-1}}\mathbb{Z}_{p^s} \to (\mathbb{Z}_{p^m}\times\mathbb{Z}_{p^n})_{F_1,F_2,A}\times_{p^{s-1}}\mathbb{Z}_{p^s}.$$

Jeśli $m \geq n$, to wystarczy F zadać wzorem $F((k,l,t)) = (\beta k,(\alpha k+l)\cdot 1,t)$, a jeżeli $m < n$, to wystarczy F zadać wzorem $F((k,l,t)) = ((l\alpha\beta D + k\beta)\cdot 1, \beta^2 AD\cdot l, \beta^2 AD\cdot t)$, gdzie α,β,D są takie jak w dowodzie Stwierdzenia 2.33 punkt (iii). □

Lemat 2.36. *Dla każdej nieparzystej liczby $p \in \mathbb{P}$ niech μ_p będzie ustaloną niereszta kwadratową modulo p. Niech dla $i = 1,2$, T_i będzie jednym z pierścieni:*

(i) $(\mathbb{Z}_{p^m}\times_{p^{n-1}}\mathbb{Z}_{p^n})_{0,0,-\mu_p}$, *gdzie* $p \in \mathbb{P}$, $p > 2$, $m,n \in \mathbb{N}$, $n > 1$,

(ii) $(\mathbb{Z}_{p^m}\times_{p^{n-1}}\mathbb{Z}_{p^n})_{-1,1,-V^2\mu_p}$, *gdzie* $p \in \mathbb{P}$, $p > 2$, $m,n \in \mathbb{N}$, $n > 1$, $V = 1,2,...,(p-1)/2$,

(iii) $(\mathbb{Z}_{2^m}\times_{2^{n-1}}\mathbb{Z}_{2^n})_{1,0,1}$, *gdzie* $p \in \mathbb{P}$, $m,n \in \mathbb{N}$, $n > 1$,

(iv) $(\mathbb{Z}_{p^m}\times\mathbb{Z}_{p^n})_{0,0,-\mu_p}\times_{p^{s-1}}\mathbb{Z}_{p^s}$, *gdzie* $p \in \mathbb{P}$, $p > 2$, $m,n,s \in \mathbb{N}$, $m \leq n$,

(v) $(\mathbb{Z}_{p^m}\times\mathbb{Z}_{p^n})_{-1,1,-V^2\mu_p}\times_{p^{s-1}}\mathbb{Z}_{p^s}$, *gdzie* $p \in \mathbb{P}$, $p > 2$, $m,n,s \in \mathbb{N}$, $m \leq n$, $V = 1,2,...,(p-1)/2$,

(vi) $(\mathbb{Z}_{2^m}\times\mathbb{Z}_{2^n})_{1,0,1}\times_{2^{s-1}}\mathbb{Z}_{2^s}$, *gdzie* $p \in \mathbb{P}$, $m,n,s \in \mathbb{N}$, $m \leq n$,

natomiast C_i będzie dowolnym pierścieniem z zerowym mnożeniem. Wówczas $T_1\oplus C_1 \cong T_2\oplus C_2$ wtedy i tylko wtedy, gdy $T_1 \cong T_2$ i $C_1 \cong C_2$.

Dowód. Niech dla $i = 1,2$, $R_i = T_i \oplus C_i$ oraz $R_1 \cong R_2$. Zauważmy, że jeśli T_1 jest p-pierścieniem, a T_2 jest q-pierścieniem, to $p = q$, gdyż $|R_1^2| = p$ i $|R_2^2| = q$.

Załóżmy najpierw, że T_1, T_2 są z pierścieniami z tej samej klasy (i), (ii) lub (iii) i $T_1^+ = \mathbb{Z}_{p^{m_1}}^+\times\mathbb{Z}_{p^{n_1}}^+$, $T_2^+ = \mathbb{Z}_{p^{m_2}}^+\times\mathbb{Z}_{p^{n_2}}^+$. Bez tracenia ogólności przyjmijmy, że $R_1^2 \subseteq \mathbb{Z}_{p^{n_1}}^+$ i $R_2^2 \subseteq \mathbb{Z}_{p^{n_2}}^+$. Wtedy ze Stwierdzenia 1.2 wynika, że $p^{n_1} = \max\{o(v) : v \in (R_1)_p,\ R_1^2 \subseteq \langle v\rangle\}$, $p^{n_2} = \max\{o(v) : v \in (R_2)_p,\ R_2^2 \subseteq \langle v\rangle\}$, skąd $n_1 = n_2$. Jeżeli zaś $m_1 \neq m_2$, to bez tracenia ogólności możemy założyć, że $m_1 < m_2$. Wówczas $\dim_{\mathbb{Z}_p}(R_1(p^{m_1})/a(R_1(p^{m_1})) \geq 1 + \dim_{\mathbb{Z}_p}(R_2(p^{m_1})/a(R_2(p^{m_1}))$, sprzeczność. Zatem $m_1 = m_2$ i od razu $T_1 = T_2$ jeśli T_i jest z klasy (i) lub (iii). Jeżeli natomiast T_i jest z klasy (ii), to $T_1 = (\mathbb{Z}_{p^m}\times_{p^{n-1}}\mathbb{Z}_{p^n})_{-1,1,-V_1^2\mu_p}$, $T_2 = (\mathbb{Z}_{p^m}\times_{p^{n-1}}\mathbb{Z}_{p^n})_{-1,1,-V_2^2\mu_p}$ dla pewnych $V_1,V_2 \in \{1,2,\ldots,(p-1)/2\}$ i wówczas na mocy Uwagi 2.24, $V_1 = V_2$, skąd $T_1 = T_2$. Z Twierdzenia 1.6 otrzymujemy, że $C_1 \cong C_2$. Jeżeli zaś T_1, T_2 są pierścieniami

z różnych klas spośród (i), (ii) lub (iii), to oczywiście $R_1 \ncong R_2$, gdyż w klasie (i) są tylko przemienne pierścienie R takie, że $|R^2| = p$ przy $p > 2$, w klasie (ii) są tylko nieprzemienne pierścienie R takie, że $|R^2| = p$ przy $p > 2$, zaś w klasie (iii) znajdują się tylko pierścienie R takie, że $|R^2| = 2$.

Załóżmy teraz, że T_1 jest pierścieniem z klasy (i), (ii) lub (iii), zaś T_2 jest pierścieniem z klasy (iv), (v) lub (vi). Wówczas $T_1^+ = \mathbb{Z}_{p^{m_1}}^+ \times \mathbb{Z}_{p^{n_1}}^+$, $T_2^+ = \mathbb{Z}_{p^{m_2}}^+ \times \mathbb{Z}_{p^{n_2}}^+ \times \mathbb{Z}_{p^s}^+$. Ponadto istnieją $x \in \mathbb{Z}_{p^s}$, $x^2 = 0$, $o(x) = p^s$, $C' \leq R_2^+$ takie, że $R_2^2 \subseteq \langle x \rangle$ oraz $R_2^+ = \langle x \rangle \oplus C'$. Zatem istnieją $b \in R_1$ i $C \leq R_1^+$ takie, że $R^+ = \langle b \rangle \oplus C$, $R_1^2 \subseteq \langle b \rangle$, $o(b) = p^s$ i $b^2 = 0$. Na podstawie Stwierdzenia 1.2, $o(b) = p^{n_1}$. Ponadto $b = (pK \cdot 1, pL \cdot 1) + a$ dla pewnych $K, L \in \mathbb{Z}$ oraz $a \in C$. Ale $\langle (0, p^{n_1-1} \cdot 1) \rangle = R_1^2$, więc istnieje $U \in \mathbb{Z}$ takie, że $(0, p^{n_1-1} \cdot 1) = Up^{n_1-1}b$. Wówczas $Up^{n_1-1}b = (0,0) + Up^{n_1-1}a$, skąd $p^{n_1-1} \cdot 1 = 0$ w pierścieniu $\mathbb{Z}_{p^{n_1}}$, sprzeczność.

W końcu, niech T_1, T_2 będą pierścieniami z tej samej klasy (iv), (v) lub (vi) i $T_1^+ = \mathbb{Z}_{p^{m_1}} \times \mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{s_1}}$, $T_2^+ = \mathbb{Z}_{p^{m_2}} \times \mathbb{Z}_{p^{n_2}} \times \mathbb{Z}_{p^{s_2}}$. Bez tracenia ogólności możemy założyć, że $R_1^2 \subseteq \mathbb{Z}_{p^{s_1}}$ i $R_2^2 \subseteq \mathbb{Z}_{p^{s_2}}$, $m_1 \leq n_1$ i $m_2 \leq n_2$. Wtedy na mocy Stwierdzenia 1.2, $p^{s_1} = \max\{o(v) \ : \ v \in (R_1)_p,\ R_1^2 \subseteq \langle v \rangle\}$, $p^{s_2} = \max\{o(v) \ : \ v \in (R_2)_p,\ R_2^2 \subseteq \langle v \rangle\}$, skąd $s_1 = s_2$. Jeżeli $n_1 \neq n_2$, to bez tracenia ogólności możemy przyjąć, że $n_1 < n_2$. Wtedy $\dim_{\mathbb{Z}_p}(R_1(p^{n_1})/a(R_1(p^{n_1})) = 2$, natomiast $\dim_{\mathbb{Z}_p}(R_2(p^{n_1})/a(R_2(p^{n_1})) \leq 1$, sprzeczność. Stąd $n_1 = n_2$.

Jeżeli $m_1 \neq m_2$, to bez tracenia ogólności możemy założyć, że $m_1 < m_2$. Wówczas $\dim_{\mathbb{Z}_p}(R_1(p^{m_1})/a(R_1(p^{m_1})) \geq 1 + \dim_{\mathbb{Z}_p}(R_2(p^{m_1})/a(R_2(p^{m_1}))$, sprzeczność. Zatem $m_1 = m_2$. Jeśli T_i jest z klasy (iv) lub (vi) to natychmiast $T_1 = T_2$. Natomiast jeśli T_i jest z klasy (v), to $T_1 = T_2$ na mocy Uwagi 2.24. Na podstawie Twierdzenia 1.6, $C_1 \cong C_2$.

Jeżeli zaś T_1, T_2 są pierścieniami z różnych klas spośród (iv), (v) lub (vi), to ponownie $R_1 \ncong R_2$, gdyż w klasie (iv) są tylko przemienne pierścienie R takie, że $|R^2| = p$ dla $p > 2$, w klasie (v) są tylko nieprzemienne pierścienie R takie, że $|R^2| = p$ przy $p > 2$, zaś w klasie (vi) znajdują się tylko pierścienie R takie, że $|R^2| = 2$.

□

Twierdzenie 2.37. *Niech $p \in \mathbb{P}$ i jeśli $p > 2$ niech μ_p będzie ustaloną niereszta kwadratową modulo p. Wszystkimi z dokładnością do izomorfizmu p-pierścieniami R z prawie zerowym mnożeniem o ograniczonym wykładniku grupy R^+ i takimi, że $\dim_{\mathbb{Z}_p} R/a(R) = 2$ są pierścienie postaci $R = T \oplus C$, gdzie T jest jednym z pierścieni:*

(i) $(\mathbb{Z}_{p^m} \times_{p^{n-1}} \mathbb{Z}_{p^n})_{0,0,-\mu_p}$, *dla* $p > 2$, $m, n \in \mathbb{N}$, $n > 1$,

(ii) $(\mathbb{Z}_{p^m} \times_{p^{n-1}} \mathbb{Z}_{p^n})_{-1,1,-V^2\mu_p}$, *dla* $p > 2$, $m, n \in \mathbb{N}$, $n > 1$, $V = 1, 2, ..., (p-1)/2$,

(iii) $(\mathbb{Z}_{2^m} \times_{2^{n-1}} \mathbb{Z}_{2^n})_{1,0,1}$, *dla* $m, n \in \mathbb{N}$, $n > 1$,

(iv) $(\mathbb{Z}_{p^m} \times \mathbb{Z}_{p^n})_{0,0,-\mu_p} \times_{p^{s-1}} \mathbb{Z}_{p^s}$, *dla* $p > 2$, $m, n, s \in \mathbb{N}$, $m \leq n$,

(v) $(\mathbb{Z}_{p^m} \times \mathbb{Z}_{p^n})_{-1,1,-V^2\mu_p} \times_{p^{s-1}} \mathbb{Z}_{p^s}$, *dla* $p > 2$, $m, n, s \in \mathbb{N}$, $m \leq n$, $V = 1, 2, ..., (p-1)/2$,

(vi) $(\mathbb{Z}_{2^m} \times \mathbb{Z}_{2^n})_{1,0,1} \times_{2^{s-1}} \mathbb{Z}_{2^s}$, *dla* $m, n, s \in \mathbb{N}$, $m \leq n$.

natomiast C jest p-pierścieniem z zerowym mnożeniem ograniczonego wykładnika grupy addytywnej.

Ponadto, pierścienie z punktów $(i) - (vi)$ są nierozkładalne na sumę prostą swoich dwóch niezerowych ideałów.

Dowód. Na mocy Przykładów 2.32 i 2.34 oraz Lematu 2.11, każdy pierścień $R = T \oplus C$, gdzie T oraz C są takie jak w sformułowaniu twierdzenia, jest pierścieniem z prawie zerowym mnożeniem dla którego $\dim_{\mathbb{Z}_p} R/a(R) = 2$.

Stwierdzenie 2.29 pozwala ograniczyć się do przypadku, w którym R jest nierozkładalny na sumę prostą dwóch swoich niezerowych ideałów.

Ponieważ $|R^2| = p$, więc na podstawie Lematu 1.3, istnieją $b \in R$ oraz $C \leq R^+$ takie, że $R^2 \subseteq \langle b \rangle$ i $R^+ = \langle b \rangle \oplus C$, przy czym $C \neq 0$, gdyż $\dim_{\mathbb{Z}_p} R/a(R) = 2$. Na mocy Twierdzenia 1.5, $C = \bigoplus_{i \in I} \langle c_i \rangle$ dla pewnych $c_i \in C$. Weźmy dowolne $j \in I$. Jeśli $c_j^2 = 0$, to $\langle c_j \rangle \lhd R$ oraz $J = \langle b \rangle + \bigoplus_{i \in I \setminus \{j\}} \langle c_i \rangle \lhd R$, przy czym $R = \langle c_j \rangle \oplus J$, co przeczy nierozkładalności R na sumę prostą dwóch niezerowych ideałów. Zatem $c_j^2 \neq 0$ dla wszystkich $j \in I$. Niech $i, j \in I$, $i \neq j$. Załóżmy, że warstwy $c_i + a(R)$, $c_j + a(R)$ są liniowo zależne. Ponieważ, jak pokazaliśmy $c_i, c_j \notin a(R)$, więc można zakładać, że $o(c_j) \geq o(c_i)$ i $c_j - kc_i \in a(R)$ dla pewnego $k \in \mathbb{Z}$. Zgodnie z Lematem 1.4, $\langle c_i \rangle \oplus \langle c_j \rangle = \langle c_i \rangle \oplus \langle c_j - kc_i \rangle$, więc $\langle c_j - kc_i \rangle$ oraz $T = \langle b \rangle \oplus \bigoplus_{t \in I \setminus \{j\}} \langle c_t \rangle$ są podpierścieniami w R oraz $T \cap \langle c_j - kc_i \rangle = 0$, co przeczy nierozkładalności R na sumę prostą swoich dwóch niezerowych ideałów. Stąd dla dowolnych różnych $i, j \in I$ warstwy $c_i + a(R)$ oraz $c_j + a(R)$ są liniowo niezależne nad $\mathbb{Z}_p$.

Niech $c = c_{i_0}$ będzie elementem maksymalnego rzędu spośród elementów $\{c_i \mid i \in I\}$. Załóżmy, że $|I| > 2$. Wtedy istnieją różne $i, j \in I \setminus \{i_0\}$. Ponieważ $\dim_{\mathbb{Z}_p} R/a(R) = 2$ i każde dwie spośród warstw $c + a(R)$, $c_i + a(R)$, $c_j + a(R)$ są liniowo niezależne nad $\mathbb{Z}_p$, więc $c - kc_i - lc_j \in a(R)$ dla pewnych $k, l \in \mathbb{Z}$. Ponadto na mocy Lematu 1.4, $\langle c \rangle \oplus \langle c_i \rangle \oplus \langle c_j \rangle = \langle c - kc_i - lc_j \rangle \oplus \langle c_i \rangle \oplus \langle c_j \rangle$, skąd $I = \langle c - kc_i - c_j \rangle$ oraz $J = \langle b \rangle \oplus \langle c_i \rangle \oplus \langle c_j \rangle \oplus \bigoplus_{t \in I \setminus \{i_0, i\}} \langle c_t \rangle$ są niezerowymi ideałami pierścienia R takimi, że $R = I \oplus J$. Przeczy to nierozkładalności R na sumę prostą swoich dwóch niezerowych ideałów. Stąd $|I| \leq 2$.

Załóżmy, że $|I| = 1$. Wówczas $R^+ = \langle b \rangle \oplus \langle c \rangle$. Ponieważ $\dim_{\mathbb{Z}_p} R/a(R) = 2$, więc $b^2 \neq 0$. Ponieważ $\langle b \rangle$ jest pierścieniem z prawie zerowym mnożeniem, więc z Twierdzenia 2.31, Przykładu 2.32 oraz Stwierdzenia 2.33 wynika, że R jest izomorficzny z pierścieniem z punktu (i), (ii) lub (iii).

Niech dalej $|I| = 2$. Wówczas $R^+ = \langle b \rangle \oplus \langle c \rangle \oplus \langle d \rangle$ dla pewnego $d \in C$, przy czym $o(d) \leq o(c)$.

Jeśli $b^2 = 0$, to z Twierdzenia 2.31, Przykładu 2.34 i Stwierdzenia 2.35 wynika, że pierścień R jest izomorficzny z pierścieniem z punktu (iv), (v) lub (vi).

Niech dalej $b^2 \neq 0$. Wtedy ze Twierdzenia 2.31 wynika, że $o(b) = p^n$ dla pewnego $n \in \mathbb{Z}$, $n > 1$. Ponieważ $\dim_{\mathbb{Z}_p} R/a(R) = 2$ oraz $b, c, d \notin a(R)$ i jak wykazaliśmy warstwy $c + a(R)$ i $d + a(R)$ są liniowo niezależne, więc $b - kc - ld \in a(R)$ dla pewnych $k, l \in \mathbb{Z}$, przy czym $p \nmid k$ lub $p \nmid l$.

Załóżmy, że $p \mid k$. Wtedy $p \nmid l$ i $d - Vb \in a(R)$ dla pewnego $V \in \mathbb{Z}$ oraz $b - ld \in a(R)$. Jeśli $o(b) \leq o(d)$, to na mocy Lematu 1.4, $\langle b \rangle \oplus \langle d \rangle = \langle b \rangle \oplus \langle d - Vb \rangle$ i pierścień R jest sumą prostą dwóch swoich niezerowych ideałów $\langle d - Vb \rangle$ i $\langle b \rangle \oplus \langle c \rangle$, co prowadzi do

sprzeczności. Jeśli zaś $o(b) > o(d)$, to z Lematu 1.4 wynika, że $\langle b\rangle \oplus \langle d\rangle = \langle b - ld\rangle \oplus \langle d\rangle$. Zatem $R^+ = \langle b - ld\rangle \oplus \langle c\rangle \oplus \langle d\rangle$, przy czym $(b-ld)^2 = 0$ i $R^2 = p^{n-1}\langle b\rangle = p^{n-1}\langle b - ld\rangle$. Zatem z Twierdzenia 2.31, Przykładu 2.34 i Stwierdzenia 2.35 wynika, że pierścień R jest izomorficzny z pierścieniem z punktu (iv), (v) lub (vi).

Niech teraz $p \nmid k$. Wówczas $c - Ub - Wd \in a(R)$ dla pewnych $U, W \in \mathbb{Z}$. Jeśli $o(b) \leq o(c)$, to z Lematu 1.4 wynika, że $R^+ = \langle b\rangle \oplus \langle c - Ub - Wd\rangle \oplus \langle d\rangle$. Zatem R jest suma prostą swoich dwóch niezerowych ideałów $\langle b\rangle \oplus \langle d\rangle$ i $\langle c - Ub - Wd\rangle$, wbrew założeniu. Stąd $o(b) > o(c)$ i na podstawie Lematu 1.4, $R^+ = \langle b - kc - ld\rangle \oplus \langle c\rangle \oplus \langle d\rangle$. Kładąc $b_1 = b - kc - ld$ mamy $R^+ = \langle b_1\rangle \oplus \langle c\rangle \oplus \langle d\rangle$. Stąd $R^2 = p^{n-1}\langle b\rangle = p^{n-1}\langle b_1\rangle$ przy czym $b_1^2 = 0$. Zatem z Twierdzenia 2.31, Przykładu 2.34 i Stwierdzenia 2.35 wynika, że pierścień R jest izomorficzny z pierścieniem z punktu (iv), (v) lub (vi).

Problem izomorfizmu między pierścieniami opisanymi w twierdzeniu rozstrzyga Lemat 2.36.

Pozostało do wykazania, że każdy pierścień R z klasy $(i) - (vi)$ nie rozkłada się na sumę prostą swoich dwóch niezerowych ideałów. Załóżmy, że R jest dowolnym pierścieniem z jednej z klas $(i) - (vi)$ i że $R = A \oplus B$ dla pewnych niezerowych ideałów $A, B \lhd R$. Podobnie jak w dowodzie Stwierdzenia 2.31 można założyć, że $A^2 \neq 0$ oraz $B^2 = 0$. Stąd $B \subseteq a(R)$ i $\dim_{\mathbb{Z}_p} A/a(A) = 2$. Zatem, z udowodnionej już części twierdzenia, $A = T \oplus C$, gdzie T oraz C są takie jak w sformułowaniu twierdzenia. Stąd $R \cong T \oplus (C \oplus B)$, co na mocy jednoznaczności przedstawienia pierścienia R w postaci podanej w twierdzeniu daje $R = T$ i $0 \cong C \oplus B$. Sprzeczność z tym, że $B \neq 0$.

□

Z Twierdzeń 2.31 oraz 2.37 wynika następujący

Wniosek 2.38. *Niech $p \in \mathbb{P}$ i jeśli $p > 2$ niech μ_p będzie ustaloną niereszą kwadratową modulo p. Wszystkimi, z dokładnością do izomorfizmu, przemiennymi pierścieniami R z prawie zerowym mnożeniem takimi, że $pR = 0$, $R^2 \neq 0$ są pierścienie postaci:*

(i) $(\mathbb{Z}_p \times_1 \mathbb{Z}_p) \oplus C$,

(ii) $\big((\mathbb{Z}_p \times \mathbb{Z}_p)_{0,0,-\mu_p} \times_1 \mathbb{Z}_p\big) \oplus C$, *dla* $p > 2$,

gdzie C jest p-pierścieniem z zerowym mnożeniem takim, że $pC = 0$.

2.4 Pierścienie z prawie zerowym mnożeniem o podzielnym anihilatorze

Opis pierścieni z prawie zerowym mnożeniem, których grupa addytywna jest nieograniczonego wykładnika jest skomplikowany i wymaga dalszych, zaawansowanych badań. Poniższe stwierdzenie i przykład pokazują jak złożony może być problem opisu takich pierścieni. Okazuje się jednak, że istnieje prosty opis w przypadku, gdy omawiane pierścienie mają podzielny anihilator.

Stwierdzenie 2.39. *Niech p będzie dowolną liczbą pierwszą i niech M_1, M_2 będą abelowymi p-grupami. Niech $\alpha \in M_1$, $\beta \in M_2$ będą takie, że $o(\alpha) = o(\beta) = p$. Wówczas, następujące warunki są równoważne:*

(i) $\mathbb{Z}_p \times_\alpha M_1 \cong \mathbb{Z}_p \times_\beta M_2$,

(ii) istnieje izomorfizm grup $f\colon M_1 \to M_2$ *taki, że* $f(\alpha) = \beta$.

Dowód. $(i) \Rightarrow (ii)$. Niech $F\colon \mathbb{Z}_p \times_\alpha M_1 \to \mathbb{Z}_p \times_\beta M_2$ będzie izomorfizmem pierścieni. Wówczas $F((\mathbb{Z}_p \times_\alpha M_1)^2) = (\mathbb{Z}_p \times_\beta M_2)^2$, więc $F(\{0\} \times \langle\alpha\rangle) = \{0\} \times \langle\beta\rangle$. Stąd $F((0,\alpha)) = k(0,\beta)$ dla pewnego niezerowego $k \in \mathbb{Z}_p$. Ponadto $F(a(\mathbb{Z}_p \times_\alpha M_1)) = a(\mathbb{Z}_p \times_\beta M_2)$, więc $F(\{0\} \times M_1) = \{0\} \times M_2$. Istnieje zatem bijekcja $g\colon M_1 \to M_2$ taka, że $F((0,m)) = (0, g(m))$ dla każdego $m \in M_1$. Stąd g jest izomorfizmem grup $g(\alpha) = k\beta$. Oczywiście, istnieje $l \in \mathbb{Z}_p$ takie, że $kl \equiv 1 \pmod p$. Ale M_2 jest p-grupą, więc funkcja $h\colon M_2 \to M_2$ dana wzorem $h(x) = lx$ jest izomorfizmem grup. Wystarczy zatem położyć $f = h \circ g$.

$(ii) \Rightarrow (i)$. Określmy funkcję $F\colon \mathbb{Z}_p \times_\alpha M_1 \to \mathbb{Z}_p \times_\beta M_2$ formułą

$$F((k,m)) = (k, f(m)) \text{ for any } k \in \mathbb{Z}_p,\ m \in M_1.$$

Łatwo jest sprawdzić, że F jest izomorfizmem grup. Ponadto dla dowolnych $k_1, k_2 \in \mathbb{Z}_p$, $m_1, m_2 \in M_1$ mamy $F((k_1,m_1)(k_2,m_2)) = F((0,(k_1k_2)\alpha)) = (0, k_1k_2f(m)) = (0,(k_1k_2)\beta)$ oraz $F((k_1,m_1))F((k_2,m_2)) = (k_1, f(m_1))(k_2, f(m_2)) = (0,(k_1k_2)\beta)$. To pokazuje, że F jest izomorfizmem pierścieni. □

Przykład 2.40. Dla $p \in \mathbb{P}$ niech $M = \bigoplus_{t=1}^{\infty} \mathbb{Z}_{p^t}$. Niech ponadto $\varepsilon_i = (0,0,\dots,\underbrace{1}_{i},0,\dots) \in M$ dla $i = 1,2,\dots$. Pokażemy, że pierścienie $R_i = \mathbb{Z}_p \times_{p^{i-1}\varepsilon_i} M$ dla $i = 1,2,\dots$ są parami nieizomorficzne. Zauważmy, że dla dowolnych liczb naturalnych $i > j$ mamy $p^{j-1}\varepsilon_j \notin p^{i-1}M$. Stąd, nie istnieje automorfizm f grupy M taki, że $f(p^{i-1}\varepsilon_i) = p^{j-1}\varepsilon_j$. Ze Stwierdzenia 2.39 pierścienie R_i oraz R_j nie są izomorficzne.

Twierdzenie 2.41. *Niech* R *będzie (przemiennym) pierścieniem z prawie zerowym mnożeniem. Istnieje (przemienny) prawie podzielny pierścień* S *z prawie zerowym mnożeniem taki, że* R *jest ideałem istotnym w* S *oraz* $a(S)^+$ *jest grupą podzielną.*

Dowód. Niech $A = a(R)$. Istnieje wówczas grupa podzielna $(B,+)$ taka, że A^+ jest istotną podgrupą w B. Oznaczymy przez B pierścień z zerowym mnożeniem o grupie addytywnej B. Na podstawie Lematu 2.11, pierścień $R \oplus B$ jest z prawie zerowym mnożeniem i jest on przemienny, jeśli pierścień R jest przemienny. Ponadto $I = \{(x,x) : x \in A\} \lhd R \oplus B$ i $I \subseteq a(R \oplus B)$. Niech $S = (R \oplus B)/I$. Wtedy $(R+I)/I \cong R/(R \cap I) \cong R$ oraz $(R+I)/I \lhd S$. Można więc utożsamiać R z $(R+I)/I$. Ponadto S jest pierścieniem z prawie zerowym mnożeniem jako obraz homomorficzny pierścienia z prawie zerowym mnożeniem $R \oplus B$.

Niech $J \lhd R \oplus B$ taki, że $I \subsetneq J$. Wtedy istnieje $(a,b) \in J \setminus I$. Jeżeli $a \notin a(R)$, to istnieje $x \in R$ takie, że $xa \neq 0$ lub $ax \neq 0$. Wtedy $(x,0)(a,b) = (xa,0) \notin I$ lub $(a,b)(x,0) = (ax,0) \notin I$, skąd $(xa,0) + I \in (R+I)/I \cap J/I$ lub $(ax,0) + I \in (R+I)/I \cap J/I$. Jeżeli zaś $a \in a(R)$, to $(a,a) \in I$ oraz $(a,b) = (a,0) + (0,b-a)$, więc $(a,b) + I = (0,b-a) + I$ przy czym $(0,b-a) \in J \setminus I$. Stąd $b - a \neq 0$, więc $\langle b-a\rangle \cap a(R) \neq 0$ z istotności A^+ w B^+. Zatem $0 \neq k(b-a) \in a(R)$ dla pewnego $k \in \mathbb{Z}$. Stąd $(0,k(b-a)) \in J \setminus I$ oraz $(0,k(b-a)) + I = (-k(b-a),0) + I \in (R+I)/I \cap J/I$. Zatem $(R+I)/I$ jest ideałem istotnym w S.

Zauważmy, że $(0,b)+I \in a(S)$ dla każdego $b \in B$. Jeśli $(r,b)+I \in a(S)$ dla pewnych $r \in R, b \in B$, to dla każdego $y \in R$ mamy $[(r,b)+I]\cdot[(y,0)+I] = (0,0)+I$. Stąd $(ry,0) \in I$, więc $ry = 0$. Dlatego $rR = 0$ i podobnie $Rr = 0$. Zatem $r \in a(R) = A$, więc $(r,b)+I = [(r,r)+(0,b-r)]+I = (0,b-r)+I$. Stąd $a(S) = \{(0,b)+I \,:\, b \in B\}$. Ponadto przekształcenie $b \mapsto (0,b)+I$ jest izomorfizmem pierścienia B na pierścień $a(S)$. Zatem grupa $a(S)^+$ jest podzielna.

Weźmy dowolne $s \in S$ i dowolne $p \in \mathbb{P}$. Istnieje wówczas liczba bezkwadratowa M taka, że $Ms^2 = 0$. Stąd $(Ms)^2 = 0$ i wprost z definicji pierścienia z prawie zerowym mnożeniem, $Ms \in a(S)$. Ponieważ $(p^2, M) \mid p$, więc istnieją $k, l \in \mathbb{Z}$ takie, że $p = kM + lp^2$. Zatem $ps = k(Ms) + p^2(ls)$ i z podzielności grupy $a(S)^+$, $ps \in p^2S$. Zatem $pS = p^2S$. □

Lemat 2.42. *Niech R będzie pierścieniem z prawie zerowym mnożeniem o podzielnym anihilatorze. Wówczas $R = \mathbb{T}(R) \oplus C$, gdzie C jest takim ideałem pierścienia R, że $C^2 = 0$ oraz grupa C^+ jest podzielna.*

Dowód. Ponieważ grupa $a(R)^+$ jest podzielna, więc $a(R)^+ = \mathbb{T}(a(R))^+ \oplus C^+$ dla pewnej beztorsyjnej podgrupy $C^+ \leq a(R)^+$. Podgrupy $\mathbb{T}(a(R))^+$ oraz C^+ są podzielne jako składniki proste podgrupy podzielnej i oczywiście $\mathbb{T}(R) \cap C = 0$. Pokażemy, że $R = \mathbb{T}(R) + C$. Weźmy dowolne $a \in R$. Ponieważ R jest pierścieniem z prawie zerowym mnożeniem, więc istnieje liczba bezkwadratowa $m \in \mathbb{N}$ taka, że $ma^2 = 0$. Stąd $(ma)^2 = 0$ i $ma \in a(R)$. Zatem $ma = t+c$, gdzie $t \in \mathbb{T}(a(R))$, $c \in C$. Ponadto $c = mc_1$, $t = mt_1$ dla pewnych $c_1 \in C$, $t_1 \in \mathbb{T}(a(R))$. Zatem $m(a - t_1 - c_1) = 0$. Stąd $a - t_1 - c_1 \in \mathbb{T}(R)$ i $a = (a - t_1 - c_1) + t_1 + c_1 \in \mathbb{T}(R) + C$. □

Przykład 2.43. Niech p, F_1, F_2, A, U będą takie jak w Przykładzie 2.32 i niech $R^+ = \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{p^\infty}$. Na grupie R^+ określmy mnożenie wzorem

$$(k_1,l_1,t_1)(k_2,l_2,t_2) = (0, U(k_1l_2F_2 + l_1k_2F_1 + k_1k_2A + l_1l_2)\cdot x_1). \tag{2.12}$$

Podobnie jak w Przykładzie 2.34 dowodzi się, że R z tak określonym mnożeniem jest pierścieniem z prawie zerowym mnożeniem. Będziemy go oznaczali przez $(\mathbb{Z}_p \times \mathbb{Z}_p)_{F_1,F_2,A} \times_{Ux_1} \mathbb{Z}_{p^\infty}$. Ponadto, funkcja $f\colon (\mathbb{Z}_p \times \mathbb{Z}_p)_{F_1,F_2,A} \times_{x_1} \mathbb{Z}_{p^\infty} \to (\mathbb{Z}_p \times \mathbb{Z}_p)_{F_1,F_2,A} \times_{Ux_1} \mathbb{Z}_{p^\infty}$ dana wzorem $f(k,l,t) = (k,l,Ut)$ jest izomorfizmem pierścieni.

Twierdzenie 2.44. *Niech $p \in \mathbb{P}$ i jeśli $p > 2$ niech μ_p będzie ustaloną nieresztą kwadratową modulo p. Niech $R = (\mathbb{Z}_p \times \mathbb{Z}_p)_{F_1,F_2,A} \times_{x_1} \mathbb{Z}_{p^\infty}$, gdzie F_1, F_2, A są takie jak w Przykładzie 2.32. Wówczas:*

(i) jeżeli $p > 2$ i pierścień R jest przemienny, to $F_1 \equiv F_2 \pmod p$ oraz

$$R \cong (\mathbb{Z}_p \times \mathbb{Z}_p)_{0,0,A-F_1^2} \times_{x_1} \mathbb{Z}_{p^\infty},$$

(ii) jeżeli $p = 2$, to pierścień R jest nieprzemienny oraz

$$R \cong (\mathbb{Z}_2 \times \mathbb{Z}_2)_{1,0,1} \times_{x_1} \mathbb{Z}_{2^\infty} \cong (\mathbb{Z}_2 \times \mathbb{Z}_2)_{0,1,1} \times_{x_1} \mathbb{Z}_{p^\infty},$$

(iii) jeżeli $p > 2$ i pierścień R jest nieprzemienny, to $F_1 \not\equiv F_2 \pmod p$ oraz

$$R \cong (\mathbb{Z}_p \times \mathbb{Z}_p)_{-1,1,[4A-(F_1+F_2)^2]V^2} \times_{x_1} \mathbb{Z}_{p^\infty},$$

gdzie $V \in \mathbb{Z}$ jest takie, że $V(F_1 - F_2) \equiv 1 \pmod p$.

Dowód. W punkcie (i) przekształcenie $F\colon (\mathbb{Z}_p \times \mathbb{Z}_p)_{0,0,A-F_1^2} \times_{x_1} \mathbb{Z}_{p^\infty} \to R$ określone wzorem wzorem $F((k,l,t)) = (k, (l - Fk) \cdot 1, t)$ jest izomorfizmem pierścieni.

W punkcie (ii) przekształcenie $F\colon (\mathbb{Z}_2 \times \mathbb{Z}_2)_{1,0,1} \times_{x_1} \mathbb{Z}_{2^\infty} \to (\mathbb{Z}_2 \times \mathbb{Z}_2)_{0,1,1} \times_{x_1} \mathbb{Z}_{2^\infty}$ zadane wzorem $F((k,l,t)) = (k, (k + l) \cdot 1, t)$ jest izomorfizmem pierścieni.

W punkcie (iii) przekształcenie $F\colon (\mathbb{Z}_p \times \mathbb{Z}_p)_{-1,1,[4A-(F_1+F_2)^2]V^2} \times_{x_1} \mathbb{Z}_{p^\infty} \to R$ określone wzorem $F((k,l,t)) = (\beta k, (\alpha k + l) \cdot 1, t)$, gdzie α i β są takie jak w dowodzie Stwierdzenia 2.33 punkt (iii), jest izomorfizmem pierścieni.

□

Uwaga 2.45. Niech p będzie liczbą pierwszą i niech R będzie p-pierścieniem z prawie zerowym mnożeniem takim, że $a(R)^+$ jest grupą podzielną i $R^2 \neq 0$. Na podstawie Twierdzenia 2.16, istnieje $x \in R$ (lub istnieją $x, y \in R$) taki, że $x^2 \neq 0$ oraz $R = \langle x \rangle + a(R)$ (x, y spełniają warunek (3) Twierdzenia 2.16). Wówczas $px \in a(R)$ i $px = px_1$ dla pewnego $x_1 \in a(R)$. Stąd $p(x - x_1) = 0$, i $x - x_1 \notin a(R)$. Zatem na mocy Uwagi 2.18, $R = \langle x - x_1 \rangle + a(R)$ i bez tracenia ogólności możemy zakładać, że $o(x) = p$, (podobne rozważania pokazują, że możemy również przyjąć $o(x) = o(y) = p$). Ponieważ $o(x^2) = p$, więc istnieje podgrupa $M \leq a(R)$, $M \cong \mathbb{Z}_{p^\infty}$ taka, że $x^2 \in M$ oraz $a(R)^+ = M \oplus N$ dla pewnej podzielnej podgrupy $N \leq a(R)$. Stąd N oraz $\langle x \rangle + M$, ($\langle x, y \rangle + M$) są podpierścieniami H-pierścienia R, więc $N \lhd R$ oraz $\langle x \rangle + M \lhd R$, ($\langle x, y \rangle + M \lhd R$). Ponadto $R = (\langle x \rangle + M) + N$, ($R = (\langle x, y \rangle + M) + N$). Niech $k \in \mathbb{Z}$, $m \in M$, $n \in N$ będą takie, że $kx + m = n$. Wtedy $kx = n - m \in a(R)$, więc $p \mid k$, skąd $kx = 0$ i $m = n \in M \cap N = 0$. Stąd, $R = (\langle x \rangle + M) \oplus N^0$ (podobne argumenty pokazują, że $R = (\langle x, y \rangle + M) \oplus N^0$.

Wykorzystując Przykłady 2.26 i Wniosek 2.28 (Przykład 2.43) łatwo jest sprawdzić, że $\langle x \rangle + M \cong \mathbb{Z}_p \times_{x_1} \mathbb{Z}_{p^\infty}$ (oraz $\langle x, y \rangle + M \cong (\mathbb{Z}_p \times \mathbb{Z}_p)_{F_1,F_2,A} \times_{x_1} \mathbb{Z}_{p^\infty}$, gdzie $F_1, F_2, A \in \mathbb{Z}$ są takie, że kongruencja (2.6) nie ma rozwiązania).

Następne twierdzenie klasyfikuje wszystkie pierścienie z prawie zerowym mnożeniem o podzielnym anihilatorze.

Twierdzenie 2.46. *Niech dla każdej nieparzystej liczby pierwszej p, μ_p będzie ustaloną nieresztą kwadratową modulo p. Wszystkimi, z dokładnością do izomorfizmu, pierścieniami z prawie zerowym mnożeniem o podzielnym anihilatorze są pierścienie postaci:*

$$\bigoplus_{p \in \Pi} R_{(p)} \oplus C, \tag{2.13}$$

gdzie $\Pi \subseteq \mathbb{P}$ oraz $R_{(p)}$ jest jednym z następujących pierścieni:

(i) $\mathbb{Z}_p \times_{x_1} \mathbb{Z}_{p^\infty}$,

(ii) $(\mathbb{Z}_p \times \mathbb{Z}_p)_{0,0,-\mu_p} \times_{x_1} \mathbb{Z}_{p^\infty}$, *dla $p > 2$,*

(iii) $(\mathbb{Z}_p \times \mathbb{Z}_p)_{-1,1,-V^2\mu_p} \times_{x_1} \mathbb{Z}_{p^\infty}$, *dla* $p > 2$, $V = 1, 2, ..., \frac{p-1}{2}$,

(iv) $(\mathbb{Z}_2 \times \mathbb{Z}_2)_{1,0,1} \times_{x_1} \mathbb{Z}_{2^\infty}$,

natomiast C jest dowolnym pierścieniem z zerowym mnożeniem o podzielnej grupie addytywnej. Ponadto każdy z pierścieni $(i) - (iv)$ jest nierozkładalny na sumę prostą swoich dwóch niezerowych ideałów.

Dowód. Niech R będzie pierścieniem z prawie zerowym mnożeniem o podzielnym anihilatorze. Na mocy Lematu 2.42, $R = \mathbb{T}(R) \oplus C_1$ dla pewnego $C_1 \lhd R$ takiego, że $C_1^2 = 0$ oraz grupa C_1^+ jest podzielna. Stąd $a(R) = a(\mathbb{T}(R)) \oplus C_1$, więc $a(\mathbb{T}(R))^+$ jest grupą podzielną. Dalej, $\mathbb{T}(R) = \bigoplus_{p\in\mathbb{P}} \mathbb{T}(R)_p$, więc $\mathbb{T}(R)_p^+$ jest grupą podzielną dla każdego $p \in \mathbb{P}$. Niech $\Pi = \{p \in \mathbb{P} \ : \ \mathbb{T}(R)_p^2 \neq 0\}$. Jeśli $\Pi = \emptyset$, to $R^2 = 0$ i grupa R^+ jest podzielna. W przeciwnym przypadku ustalmy $p \in \Pi$. Z Uwagi 2.45 oraz Twierdzenia 2.44 wynika, że $\mathbb{T}(R)_p \cong R_{(p)} \oplus N_p$ gdzie $R_{(p)}$ jest jednym z pierścieni z punktów $(i)-(iv)$, a N_p jest p-pierścieniem z zerowym mnożeniem o podzielnej grupie addytywnej. Wobec tego wystarczy przyjąć $C = (\bigoplus_{p\in\Pi} N_p) \oplus C_1$. Ponadto na mocy Lematu 2.20, każdy z pierścieni z punktów $(i)-(iv)$ jest nierozkładalny na sumę prostą swoich dwóch niezerowych ideałów.

Niech $\Pi, \Pi' \subseteq \mathbb{P}$. Załóżmy, że $R \cong \bigoplus_{p\in\Pi} R_{(p)} \oplus C$ i $R' \cong \bigoplus_{p\in\Pi'} R'_{(p)} \oplus C'$, gdzie $R_{(p)}$ dla $p \in \Pi$ oraz $R'_{(p)}$ dla $p \in \Pi'$ są pierścieniami z punktów $(i) - (iv)$, natomiast C i C' są dowolnymi pierścieniami z zerowym mnożeniem o podzielnej grupie addytywnej. Załóżmy, że $R \cong R'$. Wówczas

$$\mathbb{T}(R) \cong \mathbb{T}(R'),\ R/\mathbb{T}(R) \cong R'/\mathbb{T}(R'),\ R_p \cong R'_p \text{ dla każdego } p \in \mathbb{P}. \tag{2.14}$$

Zauważmy, że $\Pi = \{p \in \mathbb{P} \ : \ (R_p)^2 \neq 0\}$ oraz $\Pi' = \{p \in \mathbb{P} \ : \ (R'_p)^2 \neq 0\}$, skąd $\Pi = \Pi'$. Ustalmy dowolne $p \in \Pi$. Wtedy $R_p \cong R_{(p)} \oplus C_p$ i $R'_p \cong R'_{(p)} \oplus C'_p$, więc na mocy (2.14), $R_{(p)} \oplus C_p \cong R'_{(p)} \oplus C'_p$. Zatem $\dim_{\mathbb{Z}_p}(R_{(p)} \oplus C_p)/a(R_{(p)} \oplus C_p) = \dim_{\mathbb{Z}_p}(R'_{(p)} \oplus C'_p)/a(R'_{(p)} \oplus C'_p)$, skąd $\dim_{\mathbb{Z}_p}(R_{(p)})/a(R_{(p)}) = \dim_{\mathbb{Z}_p}(R'_{(p)})/a(R'_{(p)})$. Wobec tego, jeśli $\dim_{\mathbb{Z}_p}(R_{(p)})/a(R_{(p)}) = 1$, to $R_{(p)} = R'_{(p)} = \mathbb{Z}_p \times_{x_1} \mathbb{Z}_{p^\infty}$ oraz ze Stwierdzenia 4.2.2 z [44], $C_p \cong C'_p$. Niech dalej $\dim_{\mathbb{Z}_p}(R_{(p)})/a(R_{(p)}) = 2$. Jeżeli $p = 2$, to $R_{(p)} = R'_{(p)} = (\mathbb{Z}_2 \times \mathbb{Z}_2)_{1,0,1} \times_{x_1} \mathbb{Z}_{2^\infty}$ i ze Stwierdzenia 4.2.2 z [44], $C_p \cong C'_p$. Niech dalej $p > 2$. Jeśli $R_{(p)}$ jest przemienny, to $R_{(p)} = R'_{(p)} = (\mathbb{Z}_p \times \mathbb{Z}_p)_{0,0,-\mu_p} \times_{x_1} \mathbb{Z}_{p^\infty}$ i ze Stwierdzenia 4.2.2 z [44], $C_p \cong C'_p$. Jeżeli zaś $R_{(p)}$ nie jest przemienny, to $R_{(p)} = (\mathbb{Z}_p \times \mathbb{Z}_p)_{-1,1,-V^2\mu_p} \times_{x_1} \mathbb{Z}_{p^\infty}$ i $R'_{(p)} = (\mathbb{Z}_p \times \mathbb{Z}_p)_{-1,1,-V'^2\mu_p} \times_{x_1} \mathbb{Z}_{p^\infty}$ dla pewnych $V, V' \in \{1, 2, ..., \frac{p-1}{2}\}$. Wtedy na podstawie Uwagi 2.24, $V = V'$, więc $R_{(p)} = R'_{(p)}$ i ze Stwierdzenia 4.2.2 z [44], $C_p \cong C'_p$. Ponadto dla dowolnego $p \in \mathbb{P} \setminus \Pi$, na mocy (2.14), $C_p \cong C'_p$. Wobec tego, $C_p \cong C'_p$ dla dowolnego $p \in \mathbb{P}$, skąd $\mathbb{T}(C) \cong \mathbb{T}(C')$. Ponieważ $C/\mathbb{T}(C) \cong R/\mathbb{T}(R)$ i $C'/\mathbb{T}(C') \cong R'/\mathbb{T}(R')$, więc z (2.14), $C/\mathbb{T}(C) \cong C'/\mathbb{T}(C')$. Ale z podzielności C i C', $C \cong C/\mathbb{T}(C) \times \mathbb{T}(C)$ i $C' \cong C'/\mathbb{T}(C') \times \mathbb{T}(C')$, więc $C \cong C'$. □

Z udowodnionego właśnie twierdzenia wynika od razu następujący wniosek, klasyfikujący wszystkie przemienne pierścienie z prawie zerowym mnożeniem o podzielnym anihilatorze.

Wniosek 2.47. *Wszystkimi, z dokładnością do izomorfizmu, przemiennymi pierścieniami z prawie zerowym mnożeniem o podzielnym anihilatorze są pierścienie postaci* $\bigoplus_{p\in\Pi} R_{(p)} \oplus C$*, gdzie* C *jest dowolnym pierścieniem z zerowym mnożeniem o podzielnej grupie addytywnej,* $\Pi \subseteq \mathbb{P}$ *oraz pierścienie* $R_{(p)}$ *dla każdego* $p \in \mathbb{P}$ *są takie jak w punktach* $(i) - (ii)$ *Twierdzenia 2.46 .*

Z powyższego wniosku oraz Twierdzenia 2.41 wynika kolejny wniosek, klasyfikujący wszystkie przemienne pierścienie z prawie zerowym mnożeniem.

Wniosek 2.48. *Pierścień* R *jest przemiennym pierścieniem z prawie zerowym mnożeniem wtedy i tylko wtedy, gdy jest izomorficzny z podpierścieniem pierścienia* $\bigoplus_{p\in\Pi} R_{(p)} \oplus C$*, gdzie* C *jest dowolnym pierścieniem z zerowym mnożeniem o podzielnej grupie addytywnej,* $\Pi \subseteq \mathbb{P}$ *oraz pierścienie* $R_{(p)}$ *dla każdego* $p \in \mathbb{P}$ *są takie jak w punktach* $(i) - (ii)$ *Twierdzenia 2.46 .*

Z Twierdzeń 2.41 oraz 2.46 wynika od razu następujący wniosek, który klasyfikuje wszystkie pierścienie z prawie zerowym mnożeniem.

Wniosek 2.49. *Pierścień* R *jest z prawie zerowym mnożeniem wtedy i tylko wtedy, gdy jest izomorficzny z podpierścieniem pierścienia* $\bigoplus_{p\in\mathbb{P}} R_{(p)} \oplus C$*, gdzie pierścienie* C *oraz* $R_{(p)}$ *dla każdego* $p \in \mathbb{P}$ *są takie jak w Twierdzeniu 2.46.*

Rozdział 3

Przemienne, filialne pierścienie zredukowane

3.1 Podstawowe własności CRF-pierścieni

Dla liczby pierwszej p, przez $\mathcal{Z}_p$ będziemy oznaczać pierścień p-adycznych liczb całkowitych, natomiast przez $\mathcal{Q}_p$ jego ciało ułamków. Dobrze wiadomo, że dla każdej liczby pierwszej p, pierścień $\mathcal{Z}_p$ spełnia warunki (i) oraz (ii) Twierdzenia 1.31, i wobec tego jest on lokalną, filialną dziedziną całkowitości charakterystyki zero. Dla dowolnego niepustego podzbioru $\Pi \subseteq \mathbb{P}$, niech $\mathcal{Z}_\Pi = \prod_{p\in\Pi} \mathcal{Z}_p$ i $\mathcal{Q}_\Pi = \prod_{p\in\Pi} \mathcal{Q}_p$. Grupę elementów odwracalnych pierścienia R będziemy oznaczali przez R^*.

Jak już wspominaliśmy, kompletną klasyfikację przemiennych, filialnych dziedzin uzyskano w [8]. Zauważono tam, że każda przemienna, filialna dziedzina jest ideałem pewnej filialnej dziedziny całkowitości (por. Stwierdzenie 1.30). Ponadto udowodniono, że każda przemienna dziedzina dodatniej charakterystyki jest filialna wtedy i tylko wtedy, gdy jest ciałem (Corollary 2.6, [8]). Powyższe spostrzeżenia redukują problem opisu filialnych dziedzin do opisu filialnych dziedzin całkowitości charakterystyki zero nie będących ciałami, i ich ideałów.

W rozważaniach przeprowadzonych w [8] istotną rolę odegrał, określony dla dziedzin całkowitości R, zbiór $\Pi(R)$ zdefiniowany wzorem (1.1). Udowodniono tam następujące twierdzenie klasyfikacyjne.

Twierdzenie 3.1. *Niech Π będzie ustalonym, niepustym podzbiorem w $\mathbb{P}$. Pierścień R jest filialną dziedziną całkowitości charakterystyki zero taką, że $\Pi(R) = \Pi$ wtedy i tylko wtedy, gdy R jest izomorficzny z pewnym podpierścieniem pierścienia $\mathcal{Q}_\Pi = \prod_{p\in\Pi} \mathcal{Q}_p$ postaci $K \cap \mathcal{Z}_\Pi$, gdzie $\mathcal{Z}_\Pi = \prod_{p\in\Pi} \mathcal{Z}_p$, K jest podciałem w $\mathcal{Q}_\Pi$ takim, że dla każdego $a \in K$, $a = (a_p)_{p\in\Pi}$ mamy $a_p \in \mathcal{Z}_p$ dla prawie wszystkich $p \in \Pi$.*

Z Twierdzenia Andrunakiewicza-Ryabukhina (por. [34]) wynika, że każdy pierścień zredukowany jest sumą podprostą dziedzin. Mogłoby się więc wydawać, że z klasyfikacji filialnych dziedzin całkowitości powinny łatwo wynikać twierdzenia strukturalne dla przemiennych, zredukowanych pierścieni filialnych. Przykład pierścienia $\mathbb{Z}\oplus\mathbb{Z}$ pokazuje jednak, że już suma prosta filialnych dziedzin całkowitości nie musi być pierścieniem

filialnym, a nawet, że suma podprosta skończonych ciał prostych nie musi być pierścieniem filialnym. Uzyskane rezultaty o filialnych dziedzinach całkowitości nie mają więc bezpośredniego przeniesienia na ich podproste sumy.

Z Twierdzenia 1.37 wynika, że każdy zredukowany pierścień filialny jest rozszerzeniem pewnego pierścienia silnie regularnego przez przemienny, filialny, $\mathbb{S}$-półprosty pierścień zredukowany. Dlatego w tym rozdziale zbadamy przemienne, zredukowane i $\mathbb{S}$-półproste pierścienie filialne. Innymi słowy, spróbujemy rozwiązać PROBLEM 2 dla przemiennych, zredukowanych pierścieni filialnych i radykału $\mathbb{S}$.

Systematyczne badanie przemiennych, zredukowanych pierścieni filialnych rozpoczęto w [10]. Zgodnie z wprowadzoną tam notacją przemienny, zredukowany pierścień filialny nazywamy CRF**-pierścieniem**. Uogólniono tam również definicję zbioru $\Pi(R)$ na przemienne pierścienie beztorsyjne R, przyjmując

$$\Pi(R) = \{p \in \mathbb{P} \ : \ pR \neq R\}.$$

We wspomnianej pracy, autorzy używając własności klas radykalnych $\mathbb{S}_a$ oraz $\mathcal{T}_p$ uzyskali szereg rezultatów związanych z filialnością. W szczególności udowodnili oni następujące fakty:

Stwierdzenie 3.2 ([10], Remark 1, Theorem 3, Proposition 2)**.** *Niech R będzie przemiennym, beztorsyjnym pierścieniem zredukowanym. Wówczas dla każdej liczby pierwszej p mamy:*

(i) $p \in \Pi(R)$ wtedy tylko wtedy, gdy $\mathcal{T}_p(R) \neq R$,

(ii) pierścień $R/\mathcal{T}_p(R)$ jest beztorsyjny,

(iii) jeżeli R jest pierścieniem filialnym, to pierścień $R/\mathcal{T}_p(R)$ jest zredukowany.

Stwierdzenie 3.3 ([10], Proposition 3)**.** *Przemienny, beztorsyjny pierścień zredukowany R jest filialny wtedy i tylko wtedy, gdy $R \in \mathbb{S}_a$ oraz $Rc + \langle c\rangle = pRc + \langle c\rangle$ dla dowolnych $c \in R$, $p \in \mathbb{P}$.*

Stwierdzenie 3.3 jest interesującym odpowiednikiem Twierdzenia 1.31. W dalszej części pracy wynik ten jeszcze bardziej wzmocnimy (por. Stwierdzenie 3.12).

Następne twierdzenie odgrywa bardzo ważną rolę w klasyfikacji CRF-pierścieni. Zostało ono po raz pierwszy sformułowane i udowodnione (w nieco innej formie) w pracy [10]. Zaprezentujemy teraz nowy dowód tego rezultatu.

Twierdzenie 3.4 ([10], Theorem 4)**.** *Niech A i B będą przemiennymi, zredukowanymi beztorsyjnymi pierścieniami filialnymi takimi, że $pA \neq A$ i $pB \neq B$ dla pewnej liczby pierwszej p. Wówczas pierścień $A \oplus B$ nie jest filialny.*

Dowód. Z przyjętych założeń wynika, że istnieją $a \in A \setminus pA$ i $b \in B \setminus pB$. Zgodnie ze Stwierdzenia 3.3 istnieją $k, l \in \mathbb{N}$ takie, że $ka \in Aa^2$ i $lb \in Bb^2$. Stąd $n = k \cdot l \in \mathbb{N}$ i $na = a_0a^2$ oraz $nb = b_0b^2$ dla pewnych $a_0 \in A$ i $b_0 \in B$. Dalej, istnieją ,$\alpha \in \mathbb{N}_0$, $m \in \mathbb{N}$ takie, że $p \nmid m$ i $n = p^\alpha m$. Załóżmy, że pierścień $A \oplus B$ jest filialny. Wtedy istnieją $x \in A$, $y \in B$ oraz $U, V \in \mathbb{Z}$ takie, że $(a_0a, 0) \cdot (p^{\alpha+1}ma, p^{\alpha+1}mb) = (x, y) \cdot$

$(p^{2\alpha+2}m^2a^2, p^{2\alpha+2}m^2b^2)+U(p^{2\alpha+2}m^2a^2, p^{2\alpha+2}m^2b^2)+V(p^{\alpha+1}ma, p^{\alpha+1}mb)$. Ale $(a_0a, 0)\cdot (p^{\alpha+1}ma, p^{\alpha+1}mb) = (p^{2\alpha+1}m^2a, 0)$, więc $p^{2\alpha+1}m^2a = p^{2\alpha+2}m^2xa^2 + Up^{2\alpha+2}m^2a^2 + Vp^{\alpha+1}ma$, oraz $0 = p^{2\alpha+2}m^2yb^2 + Up^{2\alpha+2}m^2b^2 + Vp^{\alpha+1}mb$. Z beztorsyjności pierścienia $A \oplus B$ oraz z drugiej równości otrzymujemy, $Vb \in p^{\alpha+1}B$. Ponieważ $b \notin pB$, więc z beztorsyjności pierścienia B, $V = p^{\alpha+1}W$ dla pewnego $W \in \mathbb{Z}$. Wobec tego z pierwszej równości oraz z beztorsyjności pierścienia A uzyskamy, że $m^2a \in pA$. Ale $p \nmid m$, więc $a \in pA$, sprzeczność. □

Bezpośrednią konsekwencją powyższego twierdzenia i dziedziczności radykału $\mathcal{T}_p$ jest następujące stwierdzenie.

Stwierdzenie 3.5 ([10], Theorem 5)**.** *Każdy niezerowy, beztorsyjny CRF-pierścień R taki, że $\mathcal{T}_p(R) = 0$ dla pewnej liczby pierwszej p, jest dziedziną.* □

Ze Stwierdzeń 3.2 i 3.5 wynika

Stwierdzenie 3.6 ([10], Theorem 6)**.** *Niech R będzie niezerowym, beztorsyjnym CRF-pierścieniem. Wówczas dla każdego $p \in \Pi(R)$, pierścień $R/\mathcal{T}_p(R)$ jest dziedziną.*

Przedstawimy teraz dalsze własności radykału $\mathcal{T}_p$.

Lemat 3.7. *Dla pierścienia zredukowanego R, $\mathcal{T}_p(R) = \bigcap_{n=1}^{\infty} p^nR$.*

Dowód. Inkluzja $\mathcal{T}_p(R) \subseteq \bigcap_{n=1}^{\infty} p^nR$ jest oczywista, ponieważ $\mathcal{T}_p(R) = \bigcap_{n=1}^{\infty} p^n\mathcal{T}_p(R)$. Niech teraz $a \in \bigcap_{n=1}^{\infty} p^nR$. Wtedy $a = pr$ dla pewnego $r \in pR$. Jednocześnie jeśli $s \in pR$ i $a = ps$, to $p(r - s) = 0$ i $r = pr_1$, $s = ps_1$ dla pewnych $r_1, s_1 \in R$. Stąd $p^2(r_1 - s_1) = 0$, a więc $(p(r_1 - s_1))^2 = 0$. Zatem $p(r_1 - s_1) = 0$, gdyż pierścień R jest zredukowany. Dlatego $pr_1 = ps_1$, skąd $r = s$. Dla $n \in \mathbb{N}$, $a = p^{n+1}b$ dla pewnego $b \in R$, więc $a = p(p^nb)$, skąd $r = p^nb \in p^nR$. Zatem $r \in \bigcap_{n=1}^{\infty} p^nR$, skąd $p(\bigcap_{n=1}^{\infty} p^nR) = \bigcap_{n=1}^{\infty} p^nR$, więc $\bigcap_{n=1}^{\infty} p^nR \subseteq \mathcal{T}_p(R)$ i ostatecznie $\mathcal{T}_p(R) = \bigcap_{n=1}^{\infty} p^nR$. □

Uwaga 3.8. Lemat 3.7 nie jest prawdziwy w klasie wszystkich pierścieni. Rzeczywiście, niech p będzie ustaloną liczbą pierwszą i niech A^0 będzie pierścieniem z zerowym mnożeniem, którego grupą addytywną jest $A = \bigoplus_{i=1}^{\infty}\langle a_i\rangle$, gdzie $o(a_i) = p^i$ dla każdego $i \in \mathbb{N}$. Niech $B = \langle p^{i-1}a_i - a_1 \ : \ i \in \mathbb{N}\rangle$. Wtedy A jest zredukowaną p-grupą i $pB = 0$. Zauważmy, że $D(A/B) = C/B$ dla pewnej p-podgrupy $C \leq A$. Wówczas $p(C/B) = C/B$, skąd $C = pC + B$ i $pC = p(pC)$. Wobec tego grupa pC jest podzielna. Ale grupa A jest zredukowana, więc $pC = 0$, skąd $C = B$ oraz $D(A/B) = 0$. Zatem grupa A/B jest zredukowaną p-grupą i $\mathcal{T}_p(A/B) = 0$. Pokażemy, że $a_1 \notin B$. Jeżeli $a_1 = \sum_{i=1}^{n} k_i(p^{i-1}a_i - a_1)$ dla pewnych liczb całkowitych $k_1, k_2, \ldots, k_n$, to $(1 + \sum_{i=1}^{n} k_i)a_1 = \sum_{i=1}^{n} k_ip^{i-1}a_i \in \langle a_1\rangle \cap (\bigoplus_{i=2}^{\infty}\langle a_i\rangle) = 0$. Skąd $o(a_i) \mid k_ip^{i-1}$ dla każdego $i \geq 2$. Ale $o(a_i) = p^i$, więc $p \mid k_i$ dla każdego $i \geq 2$ i w konsekwencji $p \nmid 1 + \sum_{i=1}^{n} k_i$, sprzeczność z tym, że $(1 + \sum_{i=1}^{n} k_i)a_1 = 0$. Zatem $0 \neq a_1 + B \in \bigcap_{n=1}^{\infty} p^n(A/B)$.

Lemat 3.9. *Niech R będzie niezerowym $\mathbb{S}$-półprostym CRF-pierścieniem. Wówczas:*

(i) $\Pi(R) \neq \emptyset$,

(ii) *jeśli* $p_1, \ldots, p_s, p \in \Pi(R)$ *oraz* $\bigcap_{i=1}^{s} \mathcal{T}_{p_i}(R) \subseteq \mathcal{T}_p(R)$, *to* $\mathcal{T}_{p_i}(R) = \mathcal{T}_p(R)$ *dla pewnego* $i \in \{1, \ldots, s\}$,

(iii) *dla każdego* $\emptyset \neq \Pi \subseteq \Pi(R)$ *oraz* $A = \bigcap_{p \in \Pi} \mathcal{T}_p(R)$, R/A *jest pierścieniem beztorsyjnym i* $mA = A$ *dla każdego* $m \in S(\Pi)$,

(iv) $\bigcap_{p \in \Pi(R)} \mathcal{T}_p(R) = 0$.

Dowód. (i). Przypuśćmy, że $\Pi(R) = \emptyset$. Wtedy $pR = R$ dla każdego $p \in \mathbb{P}$. Z Lematu 1 z [10], R jest pierścieniem beztorsyjnym. Stąd R jest $\mathbb{Q}$-algebrą. Na mocy Twierdzenia 1.38, $R \in \mathbb{S}$, ale $\mathbb{S}(R) = 0$, skąd $R = 0$, sprzeczność.

(ii). Z założeń wynika, że $\mathcal{T}_{p_1}(R) \cdot \cdots \cdot \mathcal{T}_{p_s}(R) \subseteq \mathcal{T}_p(R)$. Stąd, i na mocy Twierdzenia 6 z [10], istnieje $i \in \{1, \ldots, s\}$ takie, że $\mathcal{T}_{p_i}(R) \subseteq \mathcal{T}_p(R)$. Jeżeli $\mathcal{T}_{p_i}(R) \neq \mathcal{T}_p(R)$, to $0 \neq \mathcal{T}_p(R)/\mathcal{T}_{p_i}(R) \lhd R/\mathcal{T}_{p_i}(R)$ i z Twierdzenia 5 z [10], $R/\mathcal{T}_{p_i}(R)$ jest dziedziną. Zgodnie z Lematem 5 z [10], istnieje $m \in \mathbb{N}$ takie, że $mR \subseteq \mathcal{T}_p(R)$. Sprzeczność z beztorsyjnością pierścienia $R/\mathcal{T}_p(R)$.

(iii). Niech $r \in R$, $n \in \mathbb{N}$ będą takie, że $n(r + A) = A$. Wtedy $nr \in A$ i $nr \in \mathcal{T}_p(R)$ dla każdego $p \in \Pi$. Na mocy Twierdzenia 3 z [10], $r \in \mathcal{T}_p(R)$ dla każdego $p \in \Pi$, skąd $r \in A$.

Weźmy dowolne $q \in \Pi$ i $a \in A$. Ponieważ $a \in \mathcal{T}_q(R)$, więc istnieje $x \in \mathcal{T}_q(R)$ taki, że $a = qx$. Ponadto pierścień R/A jest beztorsyjny, skąd $x \in A$. Stąd $A \subseteq qA$ i $A = qA$. Zatem $mA = A$ dla każdego $m \in S(\Pi)$.

(iv). Niech $B = \bigcap_{p \in \Pi(R)} \mathcal{T}_p(R)$. Ponieważ $B \lhd R$, więc B jest CRF-pierścieniem. Z $\mathbb{S}$-półprostoty R wynika, że $\mathbb{S}(B) = 0$. Dla $p \in \Pi(R)$, $pB = B$ na mocy *(iii)*. Natomiast dla każdego $p \in \mathbb{P} \setminus \Pi(R)$, zachodzi równość $pR = R$ z której wynika, że dla każdego $a \in B$ istnieje $x \in R$ taki, że $a = px$. Ponownie na mocy *(iii)*, $x \in B$, skąd wynika już równość $pB = B$. Wobec tego $pB = B$ dla każdego $p \in \mathbb{P}$ i B jest $\mathbb{Q}$-algebrą. Z Twierdzenia 1.38 wynika, że $B \in \mathbb{S}$, skąd $B = 0$. □

3.2 Dołączanie jedynki do CRF-pierścieni

Następny lemat jest znany i ma standardowy dowód.

Lemat 3.10. *Niech* p *będzie dowolną liczba pierwszą i niech* R *będzie dowolnym pierścieniem. Wówczas:*

(i) *jeżeli* R *jest pierścieniem zredukowanym, to* $R_p = \{x \in R : px = 0\}$,

(ii) *jeżeli* $R \in \mathbb{S}$, *to* $R = pR \oplus R_p$.

Lemat 3.11. *Niech* R *będzie* CRF*-pierścieniem takim, że* $R \neq \mathbb{S}(R)$. *Wówczas:*

(i) $R_p = \mathbb{S}(R)_p$ *i* $pR_p = 0$ *dla każdej liczby pierwszej* p,

(ii) $R/\mathbb{S}(R)$ *jest beztorsyjnym* CRF*-pierścieniem takim, że* $\Pi(R/\mathbb{S}(R)) \neq \emptyset$,

(iii) $R \in \mathbb{S}_a$,

(iv) $R = pR \oplus R_p$ *dla każdego* $p \in \mathbb{P} \setminus \Pi(R/\mathbb{S}(R))$,

(v) *dla każdego* $p \in \Pi(R/\mathbb{S}(R))$ *istnieje* $a \in R \setminus (pR + \mathbb{S}(R))$ *takie, że* $a^2 - ma \in \mathcal{T}_p(R)$ *dla pewnego* $m \in S(\Pi(R/(R)))$, $(\langle a \rangle + pR) \cap R_p = 0$, $R = (\langle a \rangle + p^n R) + R_p$ *dla każdego* $n \in \mathbb{N}$. *Ponadto:*

(a) *jeśli* $p \mid m$, *to* $aR_p = 0$ *i* $R = (\langle a \rangle + p^n R) \oplus R_p$ *dla każdego* $n \in \mathbb{N}$, *przy czym* $\langle a \rangle + p^n R \lhd R$,

(b) *jeśli* $p \nmid m$, *to* $R = (\langle a \rangle + p^n R + aR_p) \oplus l_R(a)$ *i* $\langle a \rangle + p^n R + aR_p \lhd R$, *przy czym* $ax = mx$ *dla każdego* $x \in aR_p$ *i* $n \in \mathbb{N}$.

Dowód. Ponieważ pierścień R jest zredukowany, więc na podstawie Lematu 3.10, $pR_p = 0$ dla każdej liczby pierwszej p. Ale $R_p \lhd R$, więc pierścień R_p jest filialny i zredukowany jako ideał pierścienia R. Z Twierdzenia 1.38 wynika, że $R_p \in \mathbb{S}$ i wobec tego $R_p = \mathbb{S}(R)_p$. Kończy to dowód (i).
Pierścień $R/\mathbb{S}(R)$ jest przemienny i filialny jako obraz homomorficzny pierścienia R. Ponadto $\mathbb{T}(R) = \bigoplus_{p\in\mathbb{P}} \mathbb{T}(R)_p = \bigoplus_{p\in\mathbb{P}} R_p$, więc $\mathbb{T}(R) \subseteq \mathbb{S}(R)$. Niech $r \in R$ będzie taki, że $nr \in \mathbb{S}(R)$ dla pewnego $n \in \mathbb{N}$. Wtedy istnieje $b \in \mathbb{S}(R)$ takie, że $nr = (nr)^2 b$, skąd $n(r - nr^2 b) = 0$. Zatem $r - nr^2 b \in \mathbb{T}(R) \subseteq \mathbb{S}(R)$ oraz $b \in \mathbb{S}(R)$, skąd $r \in \mathbb{S}(R)$ i pierścień $R/\mathbb{S}(R)$ jest beztorsyjny. Weźmy $x \in R$ taki, że $x^2 \in \mathbb{S}(R)$. Wtedy istnieje $y \in \mathbb{S}(R)$ taki, że $x^2 = x^4 y$, skąd $(x - x^3 y)^2 = 0$ i ponieważ pierścień R jest zredukowany, więc $x - x^3 y = 0$. Zatem $x = x^3 y \in \mathbb{S}(R)$. Stąd pierścień $R/\mathbb{S}(R)$ jest zredukowany. Załóżmy, że $\Pi(R/\mathbb{S}(R)) = \emptyset$. Wtedy dla każdego $p \in \mathbb{P}$, $p(R/\mathbb{S}(R)) = R/\mathbb{S}(R)$, skąd z beztorsyjności $R/\mathbb{S}(R)$ wynika, że $R/\mathbb{S}(R)$ jest $\mathbb{Q}$-algebrą. Ale $R/\mathbb{S}(R)$ jest pierścieniem filialnym, więc z Twierdzenia 1.38 mamy $R/\mathbb{S}(R) \in \mathbb{S}$, skąd $R/\mathbb{S}(R) = 0$, czyli $R = \mathbb{S}(R)$, sprzeczność. Zatem $\Pi(R/\mathbb{S}(R)) \neq \emptyset$. Kończy to dowód (ii).
Na podstawie Stwierdzenia 3.3 mamy $R/\mathbb{S}(R) \in \mathbb{S}_a$. Ponieważ $\mathbb{S}(R) \in \mathbb{S}_a$ i $\mathbb{S}_a$ jest klasą radykalną, więc $R \in \mathbb{S}_a$. To pokazuje prawdziwość (iii).
Jeżeli $p \in \mathbb{P} \setminus \Pi(R/\mathbb{S}(R))$, to $R/\mathbb{S}(R) = p(R/\mathbb{S}(R))$, skąd $R = pR + \mathbb{S}(R)$. Na podstawie Lematu 3.10, $\mathbb{S}(R) = p\mathbb{S}(R) + \mathbb{S}(R)_p = p\mathbb{S}(R) + R_p$, więc $R = pR + R_p$. Ponadto pierścień R jest zredukowany, więc $pR \cap R_p = 0$. Zatem $R = pR \oplus R_p$. Kończy to dowód (iv).
Dla $p \in \mathbb{P}$, na podstawie Lematu 3.10, $\mathbb{S}(R) = p\mathbb{S}(R) \oplus \mathbb{S}(R)_p$, skąd $p\mathbb{S}(R) = p^2\mathbb{S}(R)$, więc $p\mathbb{S}(R) \subseteq \mathcal{T}_p(R)$ i $\mathcal{T}_p(\mathbb{S}(R)) = p\mathbb{S}(R)$. Dla $p \in \Pi(R/\mathbb{S}(R))$ z Twierdzenia 6 z [10], $(R/\mathbb{S}(R))/\mathcal{T}_p(R/\mathbb{S}(R))$ jest przemienną filialną dziedziną charakterystyki zero nie będącą ciałem. Ponadto $(\mathcal{T}_p(R) + \mathbb{S}(R))/\mathbb{S}(R) \subseteq \mathcal{T}_p(R/\mathbb{S}(R))$ oraz istnieje $I \lhd R$ taki, że $\mathcal{T}_p(R/\mathbb{S}(R)) = I/\mathbb{S}(R)$. Wtedy $p(I/\mathbb{S}(R)) = I/\mathbb{S}(R)$, więc $I = pI + \mathbb{S}(R)$, skąd $I = pI + \mathbb{S}(R)_p$, bo $\mathbb{S}(R) = p\mathbb{S}(R) + \mathbb{S}(R)_p = \mathcal{T}_p(\mathbb{S}(R)) + \mathbb{S}(R)_p$. Zatem $pI = p^2 I$, więc $pI \subseteq \mathcal{T}_p(R)$ i $I \subseteq \mathcal{T}_p(R) + \mathbb{S}(R)$. Stąd ostatecznie $\mathcal{T}_p(R/\mathbb{S}(R)) = (\mathcal{T}_p(R) + \mathbb{S}(R))/\mathbb{S}(R) = (\mathcal{T}_p(R) + R_p)/\mathbb{S}(R)$. Zatem $R/(\mathcal{T}_p(R) \oplus R_p)$ jest przemienną filialną dziedziną charakterystyki zero nie będącą ciałem i ze Stwierdzenia 1.30 oraz Twierdzeń 1.32 i 3.1 wynika, że istnieje $m \in S(\Pi(R/\mathbb{S}(R)))$, a nawet $m \in S(\Pi(R/(\mathcal{T}_p(R) \oplus R_p))$ oraz istnieje filialna dziedzina całkowitości D charakterystyki zero taka, że $m \in S(\Pi(D))$ i $R/(\mathcal{T}_p(R) \oplus R_p) \cong mD$. Istnieje zatem $a \in R \setminus (\mathcal{T}_p(R) \oplus R_p)$ takie, że $ar - mr \in \mathcal{T}_p(R) \oplus R_p$ dla każdego $r \in R$. Zatem

$a^2 - ma = x_0 + s_0$ dla pewnych $x_0 \in \mathcal{T}_p(R)$, $s_0 \in R_p$. Stąd istnieje $e = e^2 \in R_p$, takie, że $s_0 = es_0$. Zatem $(a-ae)^2 - m(a-ae) = (a^2 - ma) - 2a^2e + a^2e^2 + mae = x_0 + s_0 - 2a^2 + a^2e + mae = x_0 + s_0 - mae - x_0e - s_0e + mae = x_0$, bo $s_0 = s_0e$ i $x_0e = 0$. Bez zmniejszania ogólności możemy więc zakładać, że $a^2 - ma \in \mathcal{T}_p(R)$. Z filialności pierścienia D mamy $R = \langle a \rangle + pR + \mathcal{T}_p(R) + R_p = \langle a \rangle + pR + R_p$. Stąd jeśli $a \in pR + R_p$, to $R = pR + R_p$, więc $pR = p^2R$, czyli $pR \subseteq \mathcal{T}_p(R)$, a zatem $a \in \mathcal{T}_p(R) + R_p$, sprzeczność. Stąd $a \notin pR + R_p$. Ponadto $R = \langle a \rangle + mR + \mathcal{T}_p(R) + R_p = \langle a \rangle + aR + \mathcal{T}_p(R) + R_p$. Dalej $pR \cap R_p = 0$ z beztorsyjności R i jeśli $K \in \mathbb{Z}$, $r \in R$ są takie, że $Ka + pr \in R_p$ i $p \nmid K$, to stąd $a \in pR + R_p$, sprzeczność. Zatem $p \mid K$, skąd $Ka + pr \in pR \cap R_p = 0$. Zatem $(\langle a \rangle + pR) \cap R_p = 0$. Przez prostą indukcję $R = \langle a \rangle + p^nR + R_p$ dla każdego $n \in \mathbb{N}$.
Niech $p \mid m$. Wtedy $a^2 \in pR + \mathcal{T}_p(R) \subseteq pR$, więc dla $x \in R_p$, $a^2x = 0$, skąd $(ax)^2 = 0$ i $ax = 0$ ponieważ R jest zredukowany. Stąd $aR_p = 0$ i $\langle a \rangle + p^nR \lhd R$ oraz $R = (\langle a \rangle + p^nR) \oplus R_p$.
Niech teraz $p \nmid m$. Wtedy $R_p = mR_p$ i dla $x \in R_p$, $mx = (mx - ax) + ax$, przy czym $a(mx - ax) = (ma - a^2)x = -x_0x = 0$, bo $x_0 \in \mathcal{T}_p(R) \subseteq pR$ i $x \in R_p$ oraz $a(ax) = a^2x = (ma + x_0)x = m(ax)$. Stąd $R_p = aR_p \oplus l_{R_p}(a)$. Zatem $R = (\langle a \rangle + p^nR + aR_p) + l_{R_p}(a)$. Jeśli $K \in \mathbb{Z}$, $r \in R$, $x \in R_p$ są takie, że $Ka + p^nr + ax \in (pR + aR_p) \cap l_{R_p}(a) \subseteq (pR + aR_p) \cap R_p \subseteq (pR \cap R_p) + (aR_p) \cap R_p = aR_p$, to $Ka + p^nr + ax \in aR_p \cap l_{R_p}(a) = 0$. Stąd $(\langle a \rangle + p^nR + aR_p) \cap l_{R_p}(a) = 0$ i $(\langle a \rangle + p^nR + aR_p)l_{R_p}(a) = 0$, więc $\langle a \rangle + p^nR + aR_p \lhd R$ i $R = (\langle a \rangle + p^nR + aR_p) \oplus l_{R_p}(a)$, co kończy dowód (v). □

Sformułujemy teraz anonsowane wcześniej uogólnienie Stwierdzenia 3.3.

Stwierdzenie 3.12. *Dla przemiennego zredukowanego pierścienia R z jedynką następujące warunki są równoważne:*

(i) pierścień R jest filialny,

(ii) $R \in \mathbb{S}_a$ i $R = \langle 1 \rangle + pR + \mathbb{S}(R)_p$ dla dowolnej liczby pierwszej p.

Dowód. $(i) \Rightarrow (ii)$. Jeżeli $R = \mathbb{S}(R)$, to $R \in \mathbb{S}_a$, gdyż $\mathbb{S} \subseteq \mathbb{S}_a$. Jeżeli zaś $R \neq \mathbb{S}(R)$, to ze Stwierdzenia 3.11 otrzymujemy, że $R \in \mathbb{S}_a$. Weźmy dowolne $p \in \mathbb{P}$. Wtedy $pR = R(p \cdot 1)$ i z filialności pierścienia R, $R(p \cdot 1) = R(p \cdot 1)^2 + p \cdot \langle 1 \rangle$. Wobec tego dla $a \in R$ istnieją $b \in R$, $k \in \mathbb{Z}$ takie, że $pa = p^2b + pk \cdot 1$, skąd $p(a - (pb + k \cdot 1)) = 0$. Zatem $a - (pb + k \cdot 1) \in R_p$. Ale $R_p \lhd R$, skąd R_p jest zredukowanym pierścieniem filialnym takim, że $pR_p = 0$. Zatem na mocy Twierdzenia 1.38 mamy, że $R_p \in \mathbb{S}$. Dalej, $a - (pb + k \cdot 1) \in \mathbb{S}(R) = p\mathbb{S}(R) + \mathbb{S}(R)_p$. Wobec tego $a \in \langle 1 \rangle + pR + \mathbb{S}(R)_p$ i stąd $R = \langle 1 \rangle + pR + \mathbb{S}(R)_p$.

$(ii) \Rightarrow (i)$. Jeżeli $k, l \in \mathbb{Z}$ są takie, że $R = kR + \langle 1 \rangle + \mathbb{S}(R) = lR + \langle 1 \rangle + \mathbb{S}(R)$, to $R = (kl)R + \langle 1 \rangle + \mathbb{S}(R)$. Ale $\mathbb{S}(R) = p\mathbb{S}(R) + \mathbb{S}(R)_p$ dla dowolnego $p \in \mathbb{P}$, skąd $R = pR + \langle 1 \rangle + \mathbb{S}(R)$ i dalej $R = mR + \langle 1 \rangle + \mathbb{S}(R)$ dla każdego $m \in \mathbb{N}$. Weźmy dowolne $a \in R$. Ponieważ $R \in \mathbb{S}_a$, więc istnieją $m \in \mathbb{Z}$ oraz $b \in R$ takie, że $ma = a^2b$. Zatem $Ra = \langle 1 \rangle \cdot a + (ma)R + a\mathbb{S}(R) \subseteq \langle a \rangle + Ra^2 + a\mathbb{S}(R)$. Ale dla $x \in \mathbb{S}(R)$, $ax \in \mathbb{S}(R)$, więc $ax \in (ax)^2\mathbb{S}(R) \subseteq a^2\mathbb{S}(R)$, skąd $Ra \subseteq \langle a \rangle + Ra^2$. Wobec tego $Ra = \langle a \rangle + Ra^2$ i pierścień R jest filialny. □

Z Twierdzenia 1 z [27] wynika od razu, następujące ważne twierdzenie.

Twierdzenie 3.13. *Centroid silnie regularnego pierścienia jest przemiennym pierścieniem silnie regularnym z jedynką.*

Stwierdzenie 3.14. *Jeżeli R jest CRF-pierścieniem, to $\mathbb{T}(C(R))$ jest pierścieniem silnie regularnym.*

Dowód. Jeżeli $R \in \mathbb{S}$, to tezę otrzymujemy bezpośrednio z Twierdzenia 3.13. Niech dalej $R \neq \mathbb{S}(R)$. Z założeń wynika, że $C(R)$ jest pierścieniem zredukowanym, więc $\mathbb{T}(C(R)) = \bigoplus_{p\in\mathbb{P}}(C(R))_p$ i $pC(R)_p = 0$ dla każdego $p \in \mathbb{P}$. Pozostaje zatem wykazać, że dla każdej liczby pierwszej p pierścień $C(R)_p$ jest silnie regularny.
Jeśli $p \in \mathbb{P} \setminus \Pi(R/\mathbb{S}(R))$, to z Lematu 3.11 wynika, że $R = pR \oplus R_p$. Stąd $C(R)_p \cong C(R_p)$. Ale z Twierdzenia 1.38 wynika, że $R_p \in \mathbb{S}$. Ponadto na podstawie Twierdzenia 3.13, $C(R_p) \in \mathbb{S}$ i w konsekwencji $C(R)_p \in \mathbb{S}$.
Niech teraz $p \in \Pi(R/\mathbb{S}(R))$. Wtedy, zgodnie z Lematem 3.11, istnieją $a \in R \setminus (pR + \mathbb{S}(R))$ oraz $m \in S(\Pi(R/\mathbb{S}(R)))$ takie, że $a^2 - ma \in \mathcal{T}_p(R)$ i $R = (\langle a\rangle + pR) \oplus R_p$, przy czym $R_p \in \mathbb{S}$ oraz $R_p = \mathbb{S}(R)_p$.
Niech $p \mid m$. Wtedy z Lematu 3.11 wynika, że $aR_p = 0$ oraz $\langle a\rangle + pR \lhd R$ i $R = (\langle a\rangle + pR) \oplus R_p$. Ponadto $a^2 \in pR$. Niech $f \in C(R)_p$. Wtedy $pf = 0$, więc $0 = pf(R) = f(pR)$, skąd $0 = f(a^2) = af(a)$, więc $0 = f(af(a)) = f(a)f(a) = [f(a)]^2$. Ale pierścień R jest zredukowany, więc $f(a) = 0$. Wobec tego $C(R)_p \cong C(R_p)$ i, zgodnie z Twierdzeniem 3.13, istnieje $h \in C(R)_p$ takie, że $f = f^2h$.
Niech dalej $p \nmid m$. Wtedy, na podstawie Lematu 3.11, mamy $\langle a\rangle + pR + aR_p \lhd R$, $R = (\langle a\rangle + pR + aR_p) \oplus l_{R_p}(a)$ i $ax = mx$ dla każdego $x \in aR_p$. Niech $f \in C(R)_p$. Wtedy $0 = pf(R) = f(pR)$. Ale $a^2 - ma \in \mathcal{T}_p(R) \subseteq pR$, więc $0 = f(a^2 - ma) = f(a^2) - f(ma)$, skąd $af(a) = mf(a)$. Ale $pf(a) = 0$, więc $f(a) \in R_p$ i $p \nmid m$, skąd istnieje $l \in \mathbb{Z}$ takie, że $ml \equiv 1 \pmod p$ i dlatego $f(a) = laf(a)$. Dalej $(la)^2 - (la) = l^2a^2 - la = l^2(ma + x_0) - la$ dla pewnego $x_0 \in \mathcal{T}_p(R)$, więc $(la)^2 - (la) = l(lma) + l^2x_0 - la$. Ponadto $ml = 1 + pK$ dla pewnego $K \in \mathbb{Z}$, więc $(la)^2 - (la) = la + lpKa + l^2x_0 - la \in pR$. Ponadto $\langle a\rangle + pR = \langle la\rangle + pR$ i $aR_p = (la)R_p$ oraz $l_{R_p}(a) = l_{R_p}(la)$. Zatem dla $a_1 = la$ mamy $\langle a_1\rangle + pR + a_1R_p \lhd R$ i $R = (\langle a_1\rangle + pR + a_1R_p) \oplus l_{R_p}(a_1)$ oraz $a_1^2 - a_1 \in pR$. Stąd $0 = f(a_1^2 - a_1) = f(a_1^2) - f(a_1) = a_1f(a_1) - f(a_1)$. Zatem

$$f(a_1) = a_1f(a_1). \tag{3.1}$$

Dla $x \in R_p$, $a_1(a_1x) = a_1x$, gdyż $a_1^2 - a_1 \in pR$. Stąd $f(r) = f(a_1)r$ dla każdego $r \in \langle a_1\rangle + pR + a_1R_p$. Niech $h = f|_{l_{R_p}(a_1)}$. Wtedy $h \in C(l_{R_p}(a_1))$, więc na podstawie Twierdzenia 3.13, istnieje $h_1 \in C(l_{R_p}(a_1))$ takie, że $h = h^2h_1$. Ponadto $f(a_1) \in R_p \in \mathbb{S}$, więc istnieje $s_0 \in R_p$ takie, że $f(a_1) = [f(a_1)]^2s_0$. Ze wzoru (3.1) wynika, że $f^2(a_1) = [f(a_1)]^2$. Przekształcenie $g\colon \langle a_1\rangle + pR + a_1R_p \to \langle a_1\rangle + pR + a_1R_p$ dane wzorem $g(r) = s_0r$ jest homomorfizmem lewostronnych $(\langle a_1\rangle + pR + a_1R_p)$-modułów. Stąd $F\colon R \to R$ dane wzorem $F(r_1 + r_2) = g(r_1) + h_1(r_2)$ dla $r_1 \in \langle a_1\rangle + pR + a_1R_p$, $r_2 \in l_{R_p}(a_1)$ jest homomorfizmem lewostronnych R-modułów. Ponadto dla $r_1 \in \langle a_1\rangle + pR + a_1R_p$,

$r_2 \in l_{R_p}(a_1)$ mamy, że

$$\begin{aligned}(f^2F - f)(r_1 + r_2) &= f^2(g(r_1) + h_1(r_2)) - f(r_1) - f(r_2)\\ &= f(f(g(r_1)) + f(h_1(r_2))) - f(r_1) - f(r_2)\\ &= f(f(s_0r_1) + h(h_1(r_2))) - f(r_1) - f(r_2)\\ &= f(f(s_0r_1)) + f(h(h_1(r_2))) - f(r_1) - f(r_2)\\ &= f(s_0f(r_1)) + (h^2h_1)(r_2) - f(r_1) - f(r_2)\\ &= s_0f(f(a_1)r_1) + h(r_2) - f(r_1) - h(r_2)\\ &= s_0f^2(a_1)r_1 - f(r_1) = s_0[f(a_1)]^2r_1 - f(a_1)r_1\\ &= f(a_1)r_1 - f(a_1)r_1 = 0.\end{aligned}$$

Zatem $f^2F = f$ i $pF = 0$. Stąd pierścień $C(R)_p$ jest silnie regularny. □

Zauważmy najpierw, że zgodnie z Lematem 1 z [10], każdy przemienny, zredukowany i $\mathbb{S}$-półprosty pierścień filialny jest beztorsyjny. Poniższy fakt jest analogiczny do Stwierdzenia 1.30 i jest uogólnieniem Twierdzenia 2.1 z [12].

Twierdzenie 3.15. *Każdy niezerowy CRF-pierścień jest ideałem istotnym w pewnym CRF-pierścieniu z jedynką.*

Dowód. Niech $R \neq 0$ będzie CRF-pierścieniem. Wówczas $End(R_R) = C(R)$ i $C(R)$ jest przemiennym pierścieniem zredukowanym z jedynką id_R. Ze Stwierdzenia 1.8, przekształcenie $\varphi\colon R \to C(R)$ dane wzorem $\varphi(a) = l_a$ jest zanurzeniem pierścieni. Ponadto $\overline{R} = \varphi(R) \lhd C(R)$ i lewostronny anihilator pierścienia $\overline{R}$ w $C(R)$ jest zerowy. Stąd, i na mocy Stwierdzenia 1.23, $\overline{R}$ jest ideałem istotnym w każdym podpierścieniu $C(R)$ zawierającym $\overline{R}$. Jeżeli $R \in \mathbb{S}$, to Twierdzenie 3.13 implikuje, że pierścień $C(R)$ jest silnie regularny. Niech dalej $R \neq \mathbb{S}(R)$ i niech

$$S = \{f \in C(R) \ : \ nf \in \overline{R} + \langle id_R\rangle \text{ dla pewnego } n \in \mathbb{N}\}.$$

Oczywiście S jest podpierścieniem w $C(R)$ zawierającym $\mathbb{T}(C(R))$. Na mocy Stwierdzenia 3.14, $\mathbb{T}(C(R)) \in \mathbb{S}$. Ponadto $\overline{R} + \langle id_R\rangle \subseteq S$.
Ze Stwierdzenia 3.11 wynika, że $\overline{R} \in \mathbb{S}_a$. Ponadto $(\overline{R} + \langle id_R\rangle)/\overline{R} \in \mathbb{S}_a$ jako obraz homomorficzny, pierścienia $\mathbb{Z}$. Stąd $\overline{R} + \langle id_R\rangle \in \mathbb{S}_a$ oraz z definicji S, $S \in \mathbb{S}_a$.
Zgodnie ze Stwierdzeniem 3.12 wystarczy pokazać, że $S = \langle id_R\rangle + pS + \mathbb{S}(R)_p$ dla każdego $p \in \mathbb{P}$. Jeżeli $p \in \mathbb{P} \setminus \Pi(R/\mathbb{S}(R))$, to z Lematu 3.11 wynika, że $R = pR \oplus R_p$, skąd $pR = p^2R$, więc $pR \subseteq \mathcal{T}_p(R)$. Ale pierścień R jest zredukowany, więc dla każdego $x \in pR$ istnieje dokładnie jedno $y \in pR$ takie, że $x = py$. Odwzorowanie $h\colon pR \to pR$ dane wzorem $h(x) = y$ jest homomorfizmem lewostronnych R-modułów oraz $id_{pR} = ph$. Dalej $C(R) = C(pR) \oplus C(R_p)$, więc każde $f \in S$ jest postaci $f = f_1 + f_2$, gdzie $f_1 \in C(pR)$ oraz $f_2 \in C(R_p)$. Zatem $f = (f_1 + 0) + (0 + f_2)$ i $0 + f_2 \in \mathbb{S}(S)_p$, zaś $f_1 = f_1 \cdot id_{pR} = p(f_1h) \in pS$, więc $S = \langle id_R\rangle + pS + \mathbb{S}(S)_p$.
Niech dalej $p \in \Pi(R/\mathbb{S}(R))$. Zgodnie z Lematem 3.11, istnieją $a \in R \setminus (pR + \mathbb{S}(R))$ oraz $m \in S(\Pi(R/\mathbb{S}(R)))$ takie, że $a^2 - ma \in \mathcal{T}_p(R)$ oraz dla każdego $r \in R$, $ar - mr \in \mathcal{T}_p(R) \oplus R_p$. Ponadto $R = (\langle a\rangle_p R) \oplus R_p$. Dla dowolnych $r \in R$, $n \in \mathbb{N}$ istnieje więc dokładnie jedna para $(x_{n,r}, s_r) \in \mathcal{T}_p(R) \oplus R_p$ taka, że $ar - mr = p^n x_{n,r} + s_r$. Zatem $s\colon R \to R_p$ dane wzorem $s(r) = s_r$ jest homomorfizmem lewostronnych R-modułów

oraz dla każdego $n \in \mathbb{N}$ przekształcenie $f_n \colon R \to \mathcal{T}_p(R)$ dane wzorem $f_n(r) = x_{n,r}$ też jest homomorfizmem lewostronnych R-modułów. Stąd, oraz z definicji f_n i s mamy

$$p^n f_n = l_a - m \cdot id_R - s. \tag{3.2}$$

Ale $ps = 0$, więc $s \in \mathbb{S}(S)_p$, czyli $s \in S$ i oczywiście $f_n \in S$ dla każdej liczby naturalnej n. Dalej, dla $n \in \mathbb{N}$ i $r \in R$ mamy $ar - mr = p^n x_{n,r} + s_r$, więc $a(pr) - m(pr) = p^{n+1} x_{n,r} + 0$, skąd $f_{n+1}(pr) = x_{n,r} = f_n(r)$, czyli $pf_{n+1}(r) = f_n(r)$ i wobec tego

$$f_n = pf_{n+1} \text{ dla każdego } n \in \mathbb{N}. \tag{3.3}$$

Stąd

$$\langle f_1, f_2, \ldots\rangle = p\langle f_1, f_2, \ldots\rangle \subseteq pS. \tag{3.4}$$

Z (3.2) mamy, że $l_a \in pS + \langle id_R\rangle + \mathbb{S}(S)_p$. Ponadto $R = \langle a\rangle + pR + R_p$, więc $\overline{R} = \langle l_a\rangle + p\overline{R} + \overline{R}_p$. Ale $\overline{R}_p \subseteq \mathbb{S}(S)_p$, więc

$$\overline{R} + \langle id_R\rangle + \overline{R}_p = \langle id_R\rangle + pS + \mathbb{S}(S)_p. \tag{3.5}$$

Weźmy dowolne $f \in S$. Z definicji S istnieje najmniejsze $n_0 \in \mathbb{N}$ takie, że $n_0 f \in \langle id_R\rangle + \overline{R} + \langle f_1, f_2, \ldots\rangle + \mathbb{S}(S)_p$.
Załóżmy, że $p \mid n_0$. Wtedy istnieje $m_0 \in \mathbb{N}$ takie, że $n_0 = pm_0$ oraz $p(m_0 f) \in \overline{R} + \langle id_R\rangle + \langle f_1, f_2, \ldots\rangle + \mathbb{S}(S)_p$. Ale $\overline{R} = \langle l_a\rangle + p\overline{R} + \overline{R}_p \subseteq \langle l_a\rangle + p\overline{R} + \mathbb{S}(S)_p$, więc $p(m_0 f) \in p\overline{R} + \langle l_a\rangle + \langle id_R\rangle + \langle f_1, f_2 \ldots\rangle + \mathbb{S}(S)_p$. To implikuje istnienie $r \in R$, $k, l \in \mathbb{Z}$, $x \in \langle f_1, f_2 \ldots\rangle$, $e \in \mathbb{S}(S)_p$ takich, że $p(m_0 f) = pl_r + kl_a + l \cdot id_R + x + e$. Z (3.2) oraz (3.4) mamy, odpowiednio, $l_a = pf_1 + m \cdot id_R + s$ oraz $x = py$ dla pewnego $y \in \langle f_1, f_2 \ldots\rangle$. W konsekwencji $p(m_0 f) = pl_r + kpf_1 + km \cdot id_R + l \cdot id_R + py + s'$, gdzie $s' = ks + e \in \mathbb{S}(S)_p$. Stąd

$$pg = t \cdot id_R + s', \tag{3.6}$$

gdzie $g = m_0 f - l_r - kf_1 - y$ oraz $t = km + l$. Jeśli $p \nmid t$, to istnieją $u, v \in \mathbb{Z}$ takie, że $pu + tv = 1$. Zatem dla dowolnego $b \in R$

$$b = pnb + tvb = pnb + (vpg - vs')b$$

$$= pnb + pvg(b) - vs'b \in pR \oplus R_p.$$

Stąd $R = pR \oplus R_p$, a więc $a \in pR + \mathbb{S}(R)$, sprzeczność. Zatem $t = pt'$ dla pewnego $t' \in \mathbb{Z}$. Wobec (3.6) mamy $p(g - t' \cdot id_R) \in \mathbb{S}(S)_p$, więc $p^2(g - t' \cdot id_R) = 0$, stąd $[p(g - t' \cdot id_R)]^2 = 0$ i wobec tego $p(g - t' \cdot id_R) = 0$. Zatem ze Stwierdzenia 3.14, $g - t' \cdot id_R \in \mathbb{S}(S)_p$, czyli $m_0 f - l_r - kf_1 - y - t' \cdot id_R \in \mathbb{S}(S)_p$, a więc $m_0 f \in \langle id_R\rangle + \overline{R} + \langle f_1, f_2, \ldots,\rangle + \mathbb{S}(S)_p$, co przeczy minimalności n_0.
Wobec tego $p \nmid n_0$ i istnieją $u, v \in \mathbb{Z}$ takie, że $pu + vn_0 = 1$. Stąd oraz z (3.4), (3.5) mamy, że $f = p(uf) + v(n_0 f) \in \langle id_R\rangle + pS + \mathbb{S}(S)_p$. Zatem $S = \langle id_R\rangle + pS + \mathbb{S}(S)_p$. $\square$

3.3 Twierdzenia klasyfikacyjne dla CRF-pierścieni

Stwierdzenie 3.16. *Klasa CRF-pierścieni to dokładnie rodzina wszystkich rozszerzeń przemiennych pierścieni silnie regularnych przez $\mathbb{S}$-półproste CRF-pierścienie.*

Dowód. Przypuśćmy, że przemienny silnie regularny pierścień I jest ideałem pierścienia R i R/I jest $\mathbb{S}$-półprostym CRF-pierścieniem. Na podstawie Twierdzenia 1.37, pierścień R jest zredukowany i lewostronnie filialny. Weźmy dowolne $a \in R$, $i, j \in I$. Wtedy $(ai - ia)j = a(ij) - i(aj) = aji - aji = 0$. Oczywiście $ai - ia \in I$ oraz $(ai-ia)^2 = 0$. Zatem $ai = ia$, gdyż pierścień R jest zredukowany. Niech teraz $a, b \in R$. $i \in I$. Wówczas $(ab-ba)i = a(bi) - b(ai) = bia - bia = 0$. Ponieważ pierścień R/I jest przemienny, więc $ab - ba \in I$. Stąd $(ab - ba)^2 = 0$, i ostatecznie $ab = ba$, czyli R jest CRF-pierścieniem.

Implikacja w drugą stronę jest natychmiastową konsekwencją Twierdzenia 1.37. □

Warto w tym miejscu odnotować, że natura rozszerzeń omawianych w poprzednim stwierdzeniu wydaje się być skomplikowana. Pokazuje to następujący przykład.

Przykład 3.17. Niech Π będzie nieskończonym podzbiorem w $\mathbb{P}$ i niech D będzie ustalonym, właściwym podpierścieniem ciała $\mathbb{Q}$, $1 \in D$. Udowodnimy, że istnieje co najmniej $2^{\aleph_0}$ nieizomorficznych, istotnych rozszerzeń pierścienia $S = \bigoplus_{p\in\Pi} \mathbb{Z}_p$ przez D.
Niech $A = \prod_{p\in\Pi} \mathbb{Z}_p$. Ponieważ $a_A(S) = 0$, więc S jest ideałem istotnym w każdym podpierścieniu T pierścienia A zawierającym S. Podobnie jak w Przykładzie 1.18 dla nieskończonego podzbioru $X \subseteq \Pi$, niech $\mathbb{1}_X = (a_p)_{p\in\Pi} \in A$ będzie takie, że $a_p = \begin{cases} 0 & \text{jeżeli } p \notin X \\ 1 & \text{jeżeli } p \in X, \end{cases}$ i niech $A(X) = \{a \in A \,:\, na \in \langle \mathbb{1}_X \rangle \text{ dla pewnego } n \in \mathbb{N}\}$. Wtedy $A(X) \lhd A$, $\mathbb{T}(A) = S$. Ponadto grupa A^+/S jest beztorsyjna i podzielna, jest więc przestrzenią liniową nad ciałem $\mathbb{Q}$. Ponieważ $|X| = \infty$, więc $\mathbb{1}_X + S \neq 0 + S$ i stąd $lin_{\mathbb{Q}}(\mathbb{1}_X + S) \cong \mathbb{Q}^+$ oraz $lin_{\mathbb{Q}}(\mathbb{1}_X + S) = A(X)^+/S$. Z definicji $\mathbb{1}_X$ i nieskończoności zbioru X wynika, że $\mathbb{1}_X + S$ jest jedynką pierścienia $A(X)/S$. Ale $A(X)^+/S \cong \mathbb{Q}^+$, więc $A(X)/S \cong \mathbb{Q}$. Ponadto $S, A(X)/S \in \mathbb{S}$, więc $A(X) \in \mathbb{S}$. Dalej, istnieje podpierścień $R(X) \subseteq A(X)$ zawierający S i taki, że $\mathbb{1}_X \in R(X)$ i $R(X)/S \cong D$. Jeżeli Y jest nieskończonym podzbiorem w Π takim, że $|Y \setminus X| = \infty$, to $\mathbb{1}_Y \notin R(X)$, bo inaczej $n\mathbb{1}_Y = k\mathbb{1}_X$ dla pewnych $n \in \mathbb{N}$, $k \in \mathbb{Z}$, co prowadzi do sprzeczności z tym, że $|Y \setminus X| = \infty$. Ale $\mathbb{1}_Y \in R(Y)$, więc $R(X) \ncong R(Y)$ na mocy pierwszej części rozważań. Powtarzając zatem rozumowanie przedstawione w Przykładzie 1.18 otrzymujemy, że istnieje co najmniej $2^{\aleph_0}$ nieizomorficznych, istotnych rozszerzeń pierścienia $\bigoplus_{p\in\Pi} \mathbb{Z}_p$ przez D.

Lemat 3.18. *Niech $\emptyset \neq \Pi \subseteq \mathbb{P}$. Wówczas każdy podpierścień A pierścienia $\mathcal{Z}_\Pi$ jest $\mathbb{S}$-półprosty.*

Dowód. Przypuśćmy, że istnieje $0 \neq a = (a_p)_{p\in\Pi} \in \mathbb{S}(A)$. Wtedy $a_q \neq 0$ dla pewnego $q \in \Pi$. Stąd $qa \in \mathbb{S}(A)$ i istnieje $b \in \mathbb{S}(A)$ takie, że $qa = b(qa)^2$. Ale $b = (b_p)_{p\in\Pi}$, więc $qa_q = b_q q^2 a_q^2$. Skąd $1 = q(b_q a_q)$. Sprzeczność, gdyż $q \in \Pi(\mathcal{Z}_q)$. □

Lemat 3.19. *Niech $\emptyset \neq \Pi \subseteq \mathbb{P}$ i niech A będzie filialnym podpierścieniem pierścienia $\mathcal{Z}_\Pi$ z tą samą jedynką. Wówczas nie istnieje nietrywialne zanurzenia pierścienia A w pierścień $\mathcal{Z}_\Pi$. W szczególności, jeśli B jest filialnym podpierścieniem pierścienia $\mathcal{Z}_\Pi$ z tą sama jedynką i $B \cong A$, to $B = A$.*

Dowód. Przypuśćmy, że istnieje zanurzenie $f\colon A \to \mathcal{Z}_\Pi$ takie, że $a \neq f(a)$ dla pewnego $a \in A$ i $f(1) = 1$. Niech $a = (a_p)_{p\in\Pi}$, $f(a) = (b_p)_{p\in\Pi}$. Wówczas istnieje $q \in \Pi$ takie, że $a_q \neq b_q$. Stąd istnieją $\alpha \in \mathbb{N}_0$ i $u \in \mathcal{Z}_q^*$ takie, że $a_q - b_q = q^\alpha u$. Zgodnie z Wnioskiem 1 z [10] istnieją $c \in A$ i $k \in \mathbb{Z}$ takie, że $a = q^{\alpha+1}c + k \cdot 1$, więc $f(a) = q^{\alpha+1}f(c) + k \cdot 1$. Wtedy $a - f(a) = q^{\alpha+1}(c - f(c))$. Skąd $q^\alpha u = q^{\alpha+1}d$ dla pewnego $d \in \mathcal{Z}_q$. Zatem $q \in \mathcal{Z}_q^*$, sprzeczność. □

Twierdzenie 3.20. *Niech Π będzie dowolnym niepustym podzbiorem w $\mathbb{P}$. Wówczas pierścień R jest $\mathbb{S}$-półprostym CRF-pierścieniem z jedynką takim, że $\Pi(R) = \Pi$ wtedy i tylko wtedy, gdy R jest izomorficzny z podpierścieniem pierścienia $\mathcal{Q}_\Pi$ postaci $K \cap \mathcal{Z}_\Pi$ gdzie K jest jednoznacznie wyznaczonym, silnie regularnym podpierścieniem w $\mathcal{Q}_\Pi$ z tą sama jedynką i takim, że dla każdego $a \in K$, $a = (a_p)_{p\in\Pi}$, $a_p \in \mathcal{Z}_p$ dla prawie wszystkich $p \in \Pi$.*

Dowód. Niech R będzie $\mathbb{S}$-półprostym CRF-pierścieniem z jedynką takim, że $\Pi(R) = \Pi$. Z Lematu 3.9, punkt *(iv)* wiemy, że odwzorowanie $\varphi\colon R \to \prod_{q\in\Pi} R/\mathcal{T}_q(R)$ dane wzorem $\varphi(a) = (a + \mathcal{T}_q(R))_{q\in\Pi}$ dla $a \in R$ jest zanurzeniem pierścieni. Zgodnie z Twierdzeniem 6 z [10], $R/\mathcal{T}_p(R)$ jest filialną dziedziną całkowitości i $p \in R/\mathcal{T}_p(R)$ dla każdego $p \in \Pi$. Na podstawie Twierdzeń 6 i 7 z [10], dla każdego $p \in \Pi$ istnieje zanurzenie pierścieni $f_p\colon R/\mathcal{T}_p(R) \to \mathcal{Z}_p$ takie, że $f_p(1 + \mathcal{T}_p(R)) = (1, 1, \dots)$. Stąd, istnieje zanurzenie pierścieni $\Phi\colon R \to \mathcal{Z}_\Pi$ takie, że $\Phi(1) = (1, 1, \dots)$. Oznaczmy $A = \Phi(R)$.
Niech $K = \{\frac{1}{n}a \mid a \in A, n \in S(\Pi)\}$. Oczywiście K jest podpierścieniem w $\mathcal{Q}_\Pi$ i $A \subseteq K$. Weźmy dowolne $a \in A$. Z Twierdzenia 2 z [10], istnieją $m \in S(\Pi)$, $b \in A$ takie, że $ma = a^2b$. Stąd $a = a^2(\frac{1}{m}b) \in a^2K$ co pokazuje, że $\frac{1}{n}a = (\frac{1}{n}a)^2(\frac{n}{m}b)$ dla każdego $n \in S(\Pi)$, więc $K \in \mathbb{S}$.
Pokażemy, że $K \cap \mathcal{Z}_\Pi \subseteq A$. Weźmy dowolne niezerowe $r \in K \cap \mathcal{Z}_\Pi$. Wtedy istnieją $n \in S(\Pi)$ oraz $a = (a_p)_{p\in\Pi} \in A$ takie, że $r = \frac{1}{n}a$. Stąd $\frac{1}{n}a \in \mathcal{Z}_\Pi$. Z filialności A dostajemy, że $A = nA + \langle 1\rangle$. Zatem $a = nb + k \cdot 1$ dla pewnych $k \in \mathbb{Z}$ i $b = (b_p)_{p\in\Pi} \in A$. Oczywiście $r = b + \frac{k}{n} \cdot 1 \in \mathcal{Z}_\Pi$ i $b \in \mathcal{Z}_\Pi$, skąd $\frac{k}{n} \cdot 1 \in \mathcal{Z}_\Pi$ i dla każdego $p \in \Pi$, $\frac{k}{n} \in \mathcal{Z}_p$. Ponieważ $n \in S(\Pi)$, więc istnieją różne liczby pierwsze $p_1, p_2, \dots, p_s$ i nieujemne liczby całkowite $l_1, l_2, \dots, l_s$ takie, że $n = p_1^{l_1}p_2^{l_2}\cdots p_s^{l_s}$. Stąd $p_i^{l_i} \mid k$ w pierścieniu $\mathcal{Z}_{p_i}$ dla każdego $i = 1, 2, \dots, s$. Ze Stwierdzenia 1.33 otrzymujemy, że $p_i^{l_i} \mid k$ w pierścieniu $\mathbb{Z}$ dla każdego $i = 1, 2, \dots, s$. Zatem $n \mid k$ w $\mathbb{Z}$ i $\frac{k}{n} \cdot 1 \in A$, więc $r \in A$ i ostatecznie $A = K \cap \mathcal{Z}_\Pi$.
Z definicji K i $\mathcal{Z}_\Pi$ wynika, że dla każdego $a \in K$, $a = (a_p)_{p\in\Pi}$ mamy $a_p \in \mathcal{Z}_p$ dla prawie wszystkich $p \in \Pi$.

Na odwrót, niech K będzie silnie regularnym podpierścieniem pierścienia $\mathcal{Q}_\Pi$ z tą samą jedynką i takim, że dla każdego $a \in K$, $a = (a_p)_{p\in\Pi}$, $a_p \in \mathcal{Z}_p$ dla prawie wszystkich $p \in \Pi$ i niech $A = K \cap \mathcal{Z}_\Pi$. Wówczas $(1, 1, \dots) \in A$ i na mocy Lematu 3.18, pierścień A jest $\mathbb{S}$-półprosty. Oczywiście A jest przemiennym zredukowanym pierścieniem beztorsyjnym takim, że $\Pi(\mathcal{Z}_\Pi) = \Pi$.

Niech p będzie dowolną liczbą pierwszą. Jeśli $p \notin \Pi(A)$, to $p \cdot 1 \in A^* \subseteq \mathcal{Z}_\Pi^*$ i $p \notin \Pi(\mathcal{Z}_\Pi) = \Pi$. Jeśli $p \notin \Pi$, to $p \cdot 1 \in \mathcal{Z}_\Pi^*$. Ale $p \cdot 1 \in K$, gdyż $1 \in K$. Ponadto $K \in \mathbb{S}$, więc $p \cdot 1 = (p \cdot 1)^2 b$ dla pewnego $b \in K$. Stąd $1 = (p \cdot 1)b$, więc $p \cdot 1 \in K^*$. Dlatego $b \in K \cap \mathcal{Z}_\Pi$, skąd $p \cdot 1 \in A^*$ i $p \notin \Pi(A)$. Zatem $\Pi(A) = \Pi$.
Teraz pokażemy, że $A = pA + \langle 1 \rangle$ dla dowolnej liczby pierwszej p. Jest to oczywiste dla $p \notin \Pi(A)$. Niech więc $p \in \Pi(A)$. Weźmy dowolne $a = (a_q)_{q \in \Pi} \in A$. Z filialności $\mathcal{Z}_p$ istnieją $k \in \mathbb{Z}$ i $b_p \in \mathcal{Z}_p$ takie, że $a_p = pb_p + k$. Stąd $b_p = \frac{a_p - k}{p} \in \mathcal{Z}_p$. Ponadto dla $q \in \Pi \setminus \{p\}$, $b_q = \frac{a_q - k}{p} \in \mathcal{Z}_q$, gdyż $\frac{1}{p} \in \mathcal{Z}_q$. Niech $b = (\frac{a_q - k}{p})_{q \in \Pi}$. Wówczas $b \in \mathcal{Z}_\Pi$ oraz $a = pb + k \cdot 1$. Pozostało wykazać, że $b \in K$. Jest jasne, że $a, 1 \in K$, więc $a - k \cdot 1 \in K$. Ale pierścień K jest silnie regularny, więc $p \cdot 1 = (p \cdot 1)^2 c$ dla pewnego $c \in K$. Stąd $1 = (p \cdot 1)c$ co pokazuje, że $p \cdot 1 \in K^*$. Ale $(p \cdot 1)b = a - k \cdot 1$ i $b = (a - k \cdot 1)c \in K$. Dlatego $A = pA + \langle 1 \rangle$ dla każdego $p \in \mathbb{P}$.
Weźmy dowolne niezerowe $a = (a_p)_{p \in X} \in A$. Ponieważ $a \in K$, więc $a_p \in \mathcal{Z}_p$ dla prawie wszystkich $p \in \Pi$. Ponadto $K \in \mathbb{S}$, więc istnieje $b = (b_p)_{p \in \Pi} \in K$ takie, że $a = a^2 b$. Istnieje więc tylko skończona ilość liczb pierwszych $q_1, q_2, \ldots, q_l$ takich, że $b_{q_i} \in \mathcal{Q}_{q_i} \setminus \mathcal{Z}_{q_i}$ dla $i = 1, 2, \ldots, l$. Stąd, dla każdego $i = 1, 2 \ldots, l$ istnieje $n_i \in \mathbb{N}$ takie, że $n_i q_i \in \mathcal{Z}_{q_i}$. Kładąc $n = n_1 n_2 \cdots n_l$ mamy $nb \in \mathcal{Z}_\Pi$ oraz $nb \in K$. Stąd $nb \in A$, więc $A \in \mathbb{S}_a$. Na podstawie Wniosku 1 z [10] wynika, że pierścień A jest filialny.
Niech L będzie silnie regularnym podpierścieniem w $\mathcal{Q}_\Pi$ z tą samą jedynką i takim, że dla $a \in L$, $a = (a_p)_{p \in \Pi}$ mamy $a_p \in \mathcal{Z}_p$ dla prawie wszystkich $p \in \Pi$ i niech $K \cap \mathcal{Z}_\Pi \cong L \cap \mathcal{Z}_\Pi$. Z pierwszej części dowodu i z Lematu 3.19 otrzymujemy, że $K \cap \mathcal{Z}_\Pi = L \cap \mathcal{Z}_\Pi$. Weźmy dowolne $a = (a_p)_{p \in X} \in K$. Ponieważ $a_p \in \mathcal{Z}_p$ dla prawie wszystkich $p \in \Pi$, więc istnieje $n \in S(\Pi)$ takie, że $na \in \mathcal{Z}_\Pi$. Dlatego $na \in K \cap \mathcal{Z}_\Pi$, skąd $na \in L \cap \mathcal{Z}_\Pi$. Więc $na \in L$ i $a \in L$, gdyż $L \in \mathbb{S}$. Stąd $K \subseteq L$. Podobnie pokazuje się, że $L \subseteq K$, skąd $K = L$. □

Definicja 3.21. Niech K będzie podpierścieniem pierścienia $\mathcal{Q}_\Pi$ z tą samą jedynką i niech $a \in K$. Przez $supp(a)$ oznaczamy zbiór $\{p \in \Pi : a_p \neq 0\}$ i niech

$$\mathcal{B}_K = \{supp(a) : a \in K\}. \tag{3.7}$$

Standardowe sprawdzenie pokazuje, że $\mathcal{B}_K$ jest algebrą Boole'a zbiorów. Dla dowolnego podzbioru $Y \subseteq \Pi$, niech $\mathbb{1}_Y = (a_p)_{p \in \Pi} \in \mathcal{Z}_\Pi$ będzie określone formułą

$$a_p = \begin{cases} 0 & \text{jeżeli } p \notin Y \\ 1 & \text{jeżeli } p \in Y. \end{cases} \tag{3.8}$$

Dowód następnego lematu jest natychmiastowy.

Lemat 3.22. *Niech Π będzie dowolnym niepustym podzbiorem w $\mathbb{P}$ i niech K będzie podpierścieniem w $\mathcal{Q}_\Pi$ z tą samą jedynką. Wówczas K jest pierścieniem silnie regularnym wtedy i tylko wtedy, gdy dla każdego $a \in K$ istnieje $b \in K$ takie, że $ab = \mathbb{1}_{supp(a)}$. W szczególności, jeśli K jest pierścieniem silnie regularnym, to $\mathbb{1}_Y \in K$ dla każdego $Y \in \mathcal{B}_K$.*

Lemat 3.23. *Niech Π będzie dowolnym niepustym podzbiorem w $\mathbb{P}$ i niech K będzie silnie regularnym podpierścieniem w $\mathcal{Q}_\Pi$ z tą samą jedynką takim, że dla każdego $a \in K$, $a = (a_p)_{p \in \Pi}$, mamy $a_p \in \mathcal{Z}_p$ dla prawie wszystkich $p \in \Pi$. Niech $S = K \cap \mathcal{Z}_\Pi$. Wówczas:*

(i) każdy ideał J pierścienia K jest postaci $J = \{\frac{1}{n}i : i \in J \cap S, n \in \mathbb{N}\}$,

(ii) jeżeli pierścień S jest noetherowski, to pierścień K też jest noetherowski,

(iii) pierścień S zawiera niezerowy ideał, który jest dziedziną wtedy i tylko wtedy, gdy pierścień K zawiera niezerowy ideał, który jest dziedziną.

Dowód. (i) Z dowodu Twierdzenia 3.20 mamy $K = \{\frac{1}{n}a : a \in S, n \in \mathbb{N}\}$. Zauważmy, że $J \lhd K$ implikuje $J \cap S \lhd S$. Pokażemy, że $J = \{\frac{1}{n}i : i \in J \cap S, n \in \mathbb{N}\}$. Rzeczywiście $\frac{1}{n}i = (\frac{1}{n} \cdot 1)i \in J$ dla $i \in J \cap S$. Jeżeli $j \in J$, to istnieje $n \in \mathbb{N}$ takie, że $n \cdot j \in S$ i wtedy oczywiście $j = \frac{1}{n}(nj)$.

Punkty (ii), (iii) wynikają bezpośrednio z (i). □

Teraz przedstawimy przykład CRF-pierścienia, który nie posiada ideału będącego dziedziną.

Twierdzenie 3.24. *Niech Π będzie dowolnym niepustym podzbiorem w $\mathbb{P}$. Wówczas R jest $\mathbb{S}$-półprostym CRF-pierścieniem z jedynką nieposiadającym ideału będącego dziedziną i takim, że $\Pi(R) = \Pi$ wtedy i tylko wtedy, gdy R jest izomorficzny z podpierścieniem pierścienia $\mathcal{Q}_\Pi$ postaci $K \cap \mathcal{Z}_\Pi$, gdzie K jest jednoznacznie wyznaczonym, silnie regularnym podpierścieniem w $\mathcal{Q}_\Pi$ z tą samą jedynką i takim, że dla każdego $a \in K$, $a = (a_p)_{p\in\Pi}$, mamy $a_p \in \mathcal{Z}_p$ dla prawie wszystkich $p \in \Pi$ oraz algebra Boole'a $\mathcal{B}_K$ jest bezatomowa.*

Dowód. Niech R będzie $\mathbb{S}$-półprostym CRF-pierścieniem z jedynką, który nie posiada ideał będącego dziedziną i takim, że $\Pi(R) = \Pi$. Na podstawie Twierdzenia 3.20, R jest izomorficzny z podpierścieniem pierścienia $\mathcal{Q}_\Pi$ postaci $K \cap \mathcal{Z}_\Pi$, gdzie K jest jednoznacznie wyznaczonym, silnie regularnym podpierścieniem w $\mathcal{Q}_\Pi$ z tą samą jedynką i takim, że dla każdego $a \in K$, $a = (a_p)_{p\in\Pi}$, mamy $a_p \in \mathcal{Z}_p$ dla prawie wszystkich $p \in \Pi$. Lemat 3.23 implikuje, że pierścień K nie posiada ideału, który jest dziedziną. Weźmy dowolny niepusty $Y \in \mathcal{B}_K$. Zgodnie z Lematem 3.22, $a = \mathbb{1}_Y \in K$. Ale $I = Ka$ nie jest dziedziną, więc istnieją niezerowe $c, d \in I$ takie, że $cd = 0$. Oczywiście $\emptyset \neq supp(c) \subseteq Y$ oraz $\emptyset \neq supp(d) \subseteq Y$. Ponadto $supp(c) \cap supp(d) = \emptyset$ ponieważ $cd = 0$. Stąd $supp(c) \subsetneq Y$ lub $supp(d) \subsetneq Y$ i algebra $\mathcal{B}_K$ jest bezatomowa.

Na odwrót, na mocy Lematu 3.23 wystarczy udowodnić, że pierścień K nie posiada ideału, który jest dziedziną. Niech $\{0\} \neq I \lhd K$. Weźmy dowolne niezerowe $a \in I$. Algebra $\mathcal{B}_K$ jest bezatomowa, więc istnieje $Y \in \mathcal{B}_K$ takie, że $\emptyset \neq Y \subsetneq supp(a)$. Na podstawie Lematu 3.22, $\mathbb{1}_Y, \mathbb{1}_{supp(a)\setminus Y} \in K$ i $a\mathbb{1}_Y, a\mathbb{1}_{supp(a)\setminus Y}$ są niezerowymi elementami z I. Zatem I nie jest dziedziną. □

Z Twierdzeń 3.15, 3.24 łatwo wynika następujące twierdzenie.

Twierdzenie 3.25. *R jest $\mathbb{S}$-półprostym CRF-pierścieniem, który nie posiada ideału będącego dziedziną wtedy i tylko wtedy, gdy R jest izomorficzny z pewnym istotnym ideałem pierścienia $K \cap \mathcal{Z}_\Pi$, gdzie K jest jednoznacznie wyznaczonym, silnie regularnym podpierścieniem w $\mathcal{Q}_\Pi$ z tą samą jedynką i takim, że dla każdego $a \in K$, $a = (a_p)_{p\in\Pi}$, mamy $a_p \in \mathcal{Z}_p$ dla prawie wszystkich $p \in \Pi$ oraz algebra Boole'a $\mathcal{B}_K$ jest bezatomowa.*

Przykład 3.26. Niech $\Pi = \{p_1, p_2, \dots\}$ będzie dowolnym nieskończonym podzbiorem w $\mathbb{P}$ i niech $\mathfrak{D}$ będzie dowolną bezatomową algebrą Boole'a podzbiorów zbioru Π. Algebra taka została skonstruowana w Przykładzie 1.21. W pierścieniu $\mathcal{Q}_\Pi$ definiujemy podpierścień

$$K = [a\mathbb{1}_Y : Y \in \mathfrak{D}, 0 \neq a \in \mathbb{Q}]. \tag{3.9}$$

Łatwo jest sprawdzić, że

$$K = \langle a\mathbb{1}_Y : Y \in \mathfrak{D}, 0 \neq a \in \mathbb{Q}\rangle. \tag{3.10}$$

Stąd, dowolne niezerowe $d \in K$ może być zapisane w postaci

$$d = a_1\mathbb{1}_{Y_1} + a_2\mathbb{1}_{Y_2} + \cdots + a_k\mathbb{1}_{Y_k}, \tag{3.11}$$

gdzie $0 \neq a_i \in \mathbb{Q}$, $\emptyset \neq Y_i \in \mathfrak{D}$ dla każdego $i \in \{1, 2, \dots, k\}$ i $Y_i \cap Y_j = \emptyset$ dla $i \neq j$, $supp(d) = Y_1 \cup Y_2 \cup \cdots \cup Y_k$. Pokażemy, że pierścień K jest silnie regularny. Niech d będzie postaci (3.11). Połóżmy $d' = a_1^{-1}\mathbb{1}_{Y_1} + a_2^{-1}\mathbb{1}_{Y_2} + \cdots + a_k^{-1}\mathbb{1}_{Y_k}$. Oczywiście $d' \in K$ i ponadto $d \cdot d' = \mathbb{1}_{supp(d)} \in K$. Na podstawie Lematu 3.22, K jest silnie regularnym podpierścieniem w $\mathcal{Q}_\Pi$. Oczywiście $K \cap \mathcal{Z}_\Pi \neq \{0\}$. Jest łatwo sprawdzić, że $\mathcal{B}_K$ jest bezatomowa, więc z Twierdzenia 3.24 wynika, że $K \cap \mathcal{Z}_\Pi$ jest niezerowym $\mathbb{S}$-półprostym CRF-pierścieniem, bez niezerowych ideałów, które są dziedzinami. Dodatkowo odnotujmy, że $\Pi(K \cap \mathcal{Z}_\Pi) = \Pi$.

Rozdział 4

Przykłady i własności pierścieni filialnych

W tym rozdziale przedstawimy fundamentalne przykłady i konstrukcje pierścieni filialnych, które będą miały zastosowanie w klasyfikacji noetherowskich, przemiennych pierścieni filialnych.

4.1 Użyteczne własności pierścieni filialnych

Lemat 4.1. *Niech I będzie pierścieniem filialnym, którego każdy ideał jest ideałem pierścienia R oraz $R/I \in \mathcal{I}$. Wówczas pierścień R jest filialny.*

Dowód. Niech $A \lhd B$ oraz $B \lhd R$. Wtedy $(A+I)/I \lhd (B+I)/I \lhd R/I$, skąd $(A+I)/I \lhd R/I$, gdyż każdy podidempotentny pierścień jest filialny. Ponadto $(A+I)/I = (A^2+I)/I$, skąd $A + I = A^2 + I$. Przecinając obie strony z A otrzymujemy z modularności kraty podgrup w R^+, $A = A^2 + (I \cap A)$. Ponieważ $I \cap A \lhd I \cap B \lhd I$, więc z założenia $I \cap A \lhd R$. Ponadto $RA \subseteq RA^2 + R(I \cap A) \subseteq BA + (I \cap A) \subseteq A$. Dowód $AR \subseteq A$ jest analogiczny. □

Stwierdzenie 4.2. *Niech A, B będą przemiennymi p-pierścieniami takimi, że $1 \in A$ oraz $\mathcal{N}(A) \neq 0$ i $\mathcal{N}(B) \neq 0$. Wówczas pierścień $A \oplus B$ nie jest filialny.*

Dowód. Załóżmy, że pierścień $A \oplus B$ jest filialny. Wówczas na podstawie Twierdzenia 1.35, $\mathcal{N}(A) \oplus \mathcal{N}(B)$ jest H-pierścieniem. Istnieją niezerowe $a \in A$, $b \in B$ takie, że $pa = a^2 = 0$ oraz $pb = b^2 = 0$. Zatem $\langle (a,b) \rangle \lhd \mathcal{N}(A) \oplus \mathcal{N}(B) \lhd A \oplus B$. Z filialności pierścienia $A \oplus B$, $\langle (a,b) \rangle \lhd A \oplus B$. Wobec tego $(a,0) = (a,b) \cdot (1,0) \in \langle (a,b) \rangle$. Stąd $(a,0) = k \cdot (a,b)$ dla pewnego $k \in \mathbb{Z}$, więc $a = ka$, $0 = kb$, co daje sprzeczność. □

Lemat 4.3. *Niech A, B będą przemiennymi pierścieniami filialnymi takimi, że dla dowolnych $a \in A$, $b \in B$ zachodzi*

$$(a,0) \in (A \oplus B)(a^2, b^2) + \langle (a^2, b^2) \rangle + \langle (a,b) \rangle \tag{4.1}$$

Wówczas pierścień $A \oplus B$ jest filialny.

Dowód. Niech $a \in A$, $b \in B$. Wówczas $S = (A \oplus B)(a^2, b^2) + \langle (a^2, b^2) \rangle + \langle (a, b) \rangle$ jest podpierścieniem w $A \oplus B$. Z (4.1) uzyskujemy, że $(a^2, 0) \in S$, $(0, b) = (a, b) - (a, 0) \in S$, $(0, b^2) \in S$. Ponadto z filialności pierścieni A i B, $Aa \subseteq Aa^2 + \langle a^2 \rangle + \langle a \rangle$ i $Bb \subseteq Bb^2 + \langle b^2 \rangle + \langle b \rangle$. Zatem $(A \oplus B)(a, b) \subseteq S$ i pierścień $A \oplus B$ jest filialny. □

Przypomnijmy, że dla beztorsyjnego CRF-pierścienia R, $\Pi(R) = \{p \in \mathbb{P} \ : \ pR \neq R\}$. W dalszych badaniach istotną rolę odegra następujące uogólnienie zbioru $\Pi(R)$ dla filialnego pierścienia przemiennego R o torsyjnym nil-radykale. Mianowicie

$$\Pi(R) = \{p \in \mathbb{P} \ : \ \mathcal{N}(R)_p \neq 0\} \cup \Pi((R/\mathcal{N}(R))/\mathbb{S}(R/\mathcal{N}(R))). \tag{4.2}$$

Poprawność tej definicji wynika z Lematu 1 z [10] oraz Lematu 3.10. Następne twierdzenie jest uogólnieniem Wniosku 3 z pracy [10].

Twierdzenie 4.4. *Niech $\{A_i\}_{i \in T}$ będzie dowolną niepustą rodziną przemiennych pierścieni filialnych takich, że $\mathcal{N}(A_i) \subseteq \mathbb{T}(A_i)$ dla każdego $i \in T$ oraz $\Pi(A_i) \cap \Pi(A_j) = \emptyset$ dla dowolnych $i, j \in T$, $i \neq j$. Wówczas pierścień $\bigoplus_{i \in T} A_i$ jest filialny.*

Dowód. Niech A, B będą dowolnymi przemiennymi pierścieniami filialnymi takimi, że $\mathcal{N}(A) \subseteq \mathbb{T}(A)$, $\mathcal{N}(B) \subseteq \mathbb{T}(B)$ oraz $\Pi(A) \cap \Pi(B) = \emptyset$. Wtedy $\mathbb{S}(A/\mathcal{N}(A)) = I/\mathcal{N}(A)$ i $\mathbb{S}(B/\mathcal{N}(B)) = J/\mathcal{N}(B)$ dla pewnych $I \lhd A$, $J \lhd B$. Z Twierdzenia o izomorfizmie wynika, że $\Pi(A) = \Pi(\mathcal{N}(A)) \cup \Pi(A/I)$ oraz $\Pi(B) = \Pi(\mathcal{N}(B)) \cup \Pi(B/J)$. Niech $a \in A$, $b \in B$. Ponieważ pierścień A/I jest przemienny, filialny i $\mathbb{S}$-półprosty, więc zgodnie z Lematem 3.11, istnieją $m \in S(\Pi(A/I))$ oraz $a_1 \in A$ takie, że $ma - a^2 a_1 \in I$. Dalej, pierścień $I/\mathcal{N}(A) \in \mathbb{S}$, więc istnieje $i \in I$ takie, że $ma - a^2 a_1 - (ma - a^2 a_1)^2 i = x \in \mathcal{N}(A)$ dla pewnego $x \in \mathcal{N}(A)$. Ale $\mathcal{N}(A) \subseteq \mathbb{T}(A)$, więc istnieje $k \in S(\Pi(\mathcal{N}(A)))$ takie, że $kx = 0$, skąd $mka = a^2 a_2$ dla pewnego $a_2 \in A$. W ten sposób pokazaliśmy, że istnieje $M \in S(\Pi(A))$ takie, że $Ma = a^2 a_2$ dla pewnego $a_2 \in A$. Analogicznie, istnieje $N \in S(\Pi(B))$ takie, że $Nb = b^2 b_2$ dla pewnego $b_2 \in B$. Z przyjętych założeń wynika, że $NWD(M, N) = 1$, więc istnieją $U, V \in \mathbb{Z}$ takie, że $MU + NV = 1$, więc

$$(Ua_2, -Vb_2)(a^2, b^2) + VN(a, b) = (Ua_2 a^2 + VNa, V(Nb - b^2 b_2))$$

$$= (UMa + VNa, 0) = ((UM + VN)a, 0) = (a, 0).$$

Zatem zgodnie z Lematem 4.3, pierścień $A \oplus B$ jest filialny.
Niech T' będzie niepustym, skończonym podzbiorem zbioru T. Z własności klas radykalnych i definicji zbioru Π wynika, że $\Pi(\bigoplus_{i \in T'} A_i) = \bigcup_{i \in T'} \Pi(A_i)$. Stąd i z pierwszej części dowodu przez indukcję uzyskujemy, że pierścień $\bigoplus_{i \in T'} A_i$ jest filialny dla każdego niepustego skończonego podzbioru T' zbioru T.
Weźmy dowolne $a, b \in R = \bigoplus_{i \in T} A_i$. Wtedy istnieje skończony, niepusty podzbiór T' zbioru T taki, że $a, b \in R' = \bigoplus_{i \in T'} A_i$. Z filialności R' otrzymujemy $ab \in R'a^2 + \langle a^2 \rangle + \langle a \rangle \subseteq Ra^2 + \langle a^2 \rangle + \langle a \rangle$, co kończy dowód filialności pierścienia R.

□

Bezpośrednio z powyższego twierdzenia wynika następujący wniosek.

Wniosek 4.5. *Niech D będzie filialną dziedziną całkowitości charakterystyki zero, która nie jest ciałem, i niech N będzie niezerowym nil-H-q-pierścieniem, $q \in \mathbb{P}$. Niech $R = mD \oplus N$, gdzie $m \in \mathbb{N}$. Jeżeli $q \notin \Pi(D)$, to R jest pierścieniem filialnym.*

Stwierdzenie 4.6. *Niech S będzie pierścieniem takim, że $S = S_1 + S_2 + \cdots + S_k$ dla pewnych swoich filialnych podpierścieni $S_1, S_2, \ldots, S_k$. Jeżeli istnieją liczby naturalne $n_1, n_2, \ldots, n_k$ takie, że $NWD(n_1, n_2, \ldots, n_k) = 1$ i dla dowolnych $a \in S$, $i \in \{1, 2, \ldots, k\}$ istnieją $t_1, \ldots, t_k \in \mathbb{N}$ takie, że $n_i^{t_i} a \in S_i$, to pierścień S jest filialny.*

Dowód. Niech $a, b \in S$. Z założeń wynika, że istnieje $t \in \mathbb{N}$ takie, że $n_i^t a \in S_i$ oraz $n_i^t b \in S_i$ dla każdego $i \in \{1, 2, \ldots, k\}$. Zatem na podstawie Twierdzenia 1.29 wynika, że $n_i^{2t}(ab), n_i^{2t}(ba) \in (n_i^t a)_{S_i}^2 + \langle n_i^t a \rangle \subseteq (a)_S^2 + \langle a \rangle$. Ponieważ $NWD(n_1, n_2, \ldots, n_k) = 1$, więc istnieją $r_1, r_2, \ldots, r_k \in \mathbb{Z}$ takie, że $n_1^{2t} r_1 + n_2^{2t} r_2 + \cdots + n_k^{2t} r_k = 1$. Wówczas $ab = \sum_{i=1}^k r_i (n_i^{2t} ab) \in (a)_S^2 + \langle a \rangle$ i podobnie $ba \in (a)_S^2 + \langle a \rangle$. Stąd ostatecznie S jest pierścieniem filialnym na mocy Twierdzenia 1.29. □

Lemat 4.7. *Niech D będzie filialną dziedziną całkowitości charakterystyki zero, która nie jest ciałem, i niech N będzie nil-H-q-pierścieniem, gdzie $q \in \mathbb{P}$, $q \in \Pi(D)$. Niech ponadto $m \in \mathbb{N}$, $t \in \mathbb{N}_0$, $q \nmid m$. Wówczas pierścień $mq^t D \oplus N$ jest filialny wtedy i tylko wtedy, gdy pierścień $q^t D \oplus N$ jest filialny.*

Dowód. Niech $S = q^t D \oplus N$ i $R = mq^t D \oplus N$. Wtedy $R \lhd S$, więc jeżeli S jest pierścieniem filialnym, to również R jest pierścieniem filialnym.

Załóżmy, że pierścień R jest filialny i niech $a \in S$. Wówczas istnieje $t_1 \in \mathbb{N}$ takie, że $q^{t_1} a \in q^t D \oplus \{0\}$ oraz $m^t a \in R$. Ale $S = R + (q^t D \times \{0\})$, więc ze Stwierdzenia 4.6, pierścień S jest filialny. □

Twierdzenie 4.8. *Niech D będzie filialną dziedziną całkowitości charakterystyki zero, która nie jest ciałem, niech $m \in \mathbb{N}$ i niech N będzie niezerowym przemiennym nil-q-pierścieniem, przy czym $q \in \Pi(D)$. Wówczas dla pierścienia $R = mD \oplus N$ następujące warunki są równoważne:*

(i) pierścień R jest filialny,

(ii) N jest pierścieniem z prawie zerowym mnożeniem takim, że $q^\alpha N = 0$ dla pewnego $\alpha \in \mathbb{N}$ oraz $q^\alpha \mid m$.

Dowód. $(i) \Rightarrow (ii)$. Zaczniemy od wykazania, że $q \mid m$. Niech $x \in N \setminus \{0\}$ będzie taki, że $x^2 = 0$, $qx = 0$ i niech $a = (mq, x)$. Z filialności pierścienia R wynika, że $(m, 0)a \in Ra^2 + \langle a^2 \rangle + \langle a \rangle$. Istnieją więc $d \in D$, $U, W \in \mathbb{Z}$ takie, że $(m^2 q, 0) = (m^3 q^2 d, 0) + W(m^2 q^2, 0) + U(mq, x)$. Stąd $Ux = 0$ i w konsekwencji $q \mid U$ oraz $U = qV$ dla pewnego $V \in \mathbb{Z}$. Ponadto $m^2 q = m^3 q^2 d + W m^2 q^2 + V m q^2$, skąd $m = m^2 q d + W m q + V q$. Zatem $q \mid m$ w D. Ale $q \in \Pi(D)$, więc na mocy Stwierdzenia 1.33, $q \mid m$ w $\mathbb{Z}$. Stąd $m = q^\alpha m_1$ dla pewnych $\alpha \in \mathbb{N}$, $m_1 \in \mathbb{Z}$, $q \nmid m_1$. Na podstawie Lematu 4.7, pierścień $S = q^\alpha D \oplus N$ jest filialny. Pierścień N jest filialny jako ideał pierścienia filialnego S. Ponadto na mocy Stwierdzenia 1.35, N jest H-pierścieniem. Udowodnimy, że N jest pierścieniem z prawie zerowym mnożeniem. Zgodnie ze Stwierdzeniem 2.12 punkt (i)

wystarczy pokazać, że $xy \in \langle y^2 \rangle$ dla dowolnych $x, y \in N$. Ustalmy liczbę naturalną $r \geq \alpha$ taką, że $q^r y = 0$. Z filialności S wynika, że

$$S(q^r, y) \subseteq S(q^{2r}, y^2) + \langle (q^{2r}, y^2) \rangle + \langle (q^r, y) \rangle,$$

skąd

$$(0, xy) = (q^\alpha d, x_1)(q^{2r}, y^2) + U(q^{2r}, y^2) + V(q^r, y),$$

dla pewnych $d \in D$, $x_1 \in N$, $U, V \in \mathbb{Z}$. Wówczas $0 = q^{\alpha+2r}d + Uq^{2r} + Vq^r$ i Stwierdzenia 1.33 wynika, że $q^r \mid V$. Ponadto $xy = x_1 y^2 + Uy^2 + Vy$, skąd $xy = x_1 y^2 + Uy^2$, ponieważ $Vy = 0$. Skoro N jest H-q-pierścieniem, więc zgodnie z Lematem 2.8, $x_1 y^2 \in \langle y^2 \rangle$ i w konsekwencji $xy \in \langle y^2 \rangle$. Zatem N jest pierścieniem z prawie zerowym mnożeniem.

Pozostało do wykazania, że $q^\alpha N = 0$. Udowodnimy najpierw, że $q^\alpha a(N) = 0$. Załóżmy, że tak nie jest. Istnieje wówczas $x \in N$, taki, że $x^2 = 0$ i $q^\alpha x \neq 0$. Z filialności S otrzymujemy

$$S(q^{\alpha+1}, x) \subseteq S(q^{2\alpha+2}, 0) + \langle (q^{2\alpha+2}, 0) \rangle + \langle (q^{\alpha+1}, x) \rangle,$$

skąd wynika, że

$$(q^{2\alpha+1}, 0) = (q^{3\alpha+2}d, 0) + U(q^{2\alpha+2}, 0) + V(q^{\alpha+1}, x),$$

dla pewnych $d \in D$, $U, V \in \mathbb{Z}$. Zatem $0 = Vx$ i ponieważ $q^\alpha x \neq 0$, więc $q^{\alpha+1} \mid V$. Dalej, z równości $q^{2\alpha+1} = q^{3\alpha+2}d + Uq^{2\alpha+2} + Vq^{\alpha+1}$, podzielności $q^{\alpha+1} \mid V$ i ze Stwierdzenia 1.33 otrzymujemy $q^{2\alpha+2} \mid q^{2\alpha+1}$ w $\mathbb{Z}$, sprzeczność. Zatem $q^\alpha a(N) = 0$ i ponieważ $qN \subseteq a(N)$, więc $q^{\alpha+1}N = 0$.
Załóżmy, że $q^\alpha N \neq 0$. Wówczas istnieje $x \in N$, $x^2 \neq 0$, $q^\alpha x \neq 0$ i $q^{\alpha+1}x = 0$. Z filialności S otrzymujemy

$$S(q^\alpha, x) \subseteq S(q^{2\alpha}, x^2) + \langle (q^{2\alpha}, x^2) \rangle + \langle (q^\alpha, x) \rangle.$$

Ponieważ $Nx^2 = 0$, więc istnieją $d \in D$, $U, V \in \mathbb{Z}$ takie, że

$$(0, x^2) = (q^{3\alpha}d, 0) + U(q^{2\alpha}, x^2) + V(q^\alpha, x).$$

Zatem $0 = q^{3\alpha}d + Uq^{2\alpha} + Vq^\alpha$ co wobec Stwierdzenia 1.33 oznacza, że $q^\alpha \mid V$ w $\mathbb{Z}$. Zatem $V = V_1 q^\alpha$ dla pewnego $V_1 \in \mathbb{Z}$. Wówczas $0 = q^\alpha d + U + V_1$ i ponownie ze Stwierdzenia 1.33, $q^\alpha \mid U + V_1$ w $\mathbb{Z}$. Dalej, $x^2 = Ux^2 + Vx$, więc jeśli $q \mid U$, to $Ux^2 = 0$, $q \mid V_1$ i $x^2 = Vx$, skąd $x^2 = 0$, sprzeczność. Zatem $q \nmid U$ i $(1 - U)x^2 = Vx$. Jeśli $q \mid 1 - U$, to $Vx = 0$ i $q \mid V_1$. Ale $q \mid U + V_1$, więc $q \mid U$, sprzeczność. Wobec tego $q \nmid 1 - U$ i $x^2 = q^\alpha W x$ dla pewnego $W \in \mathbb{Z}$, $q \nmid W$. Niech $T \in \mathbb{Z}$ będzie takie, że $TW \equiv 1 \pmod{q}$. Dla $y = Tx$ mamy, że $o(y) = o(x) = q^{\alpha+1}$ i $y^2 = q^\alpha y$. Z filialności pierścienia S wynika, że

$$S(q^\alpha, y) \subseteq S(q^{2\alpha}, y^2) + \langle (q^{2\alpha}, y^2) \rangle + \langle (q^\alpha, y) \rangle,$$

skąd otrzymujemy

$$(0, y^2) = (q^{3\alpha}d, 0) + U(q^{2\alpha}, y^2) + V(q^\alpha, y),$$

dla pewnych $d \in D$, $U, V \in \mathbb{Z}$. Zatem $0 = q^{3\alpha}d + Uq^{2\alpha} + Vq^{\alpha}$, więc $V = q^{\alpha}V_1$ dla pewnego $V_1 \in \mathbb{Z}$ oraz $y^2 = Uy^2 + Vy$. Stąd $0 = q^{\alpha}d + U + V_1$ oraz $q^{\alpha}y = Uq^{\alpha}y + q^{\alpha}V_1 y$. Dalej, $q^{\alpha}(1 - U - V_1)y = 0$, więc $q \mid 1 - (U + V_1)$. Ale $q^{\alpha} \mid U + V_1$ na mocy Stwierdzenia 1.33, więc $q \mid 1$, sprzeczność. Zatem ostatecznie $q^{\alpha}N = 0$.

$(ii) \Rightarrow (i)$ Wobec Lematu 4.7 wystarczy wykazać filialność pierścienia $q^{\alpha}D \oplus N$. W tym celu weźmy dowolne $a \in D$ oraz $x \in N$. Wystarczy pokazać, że

$$(q^{\alpha}D \oplus N)(q^{\alpha}a, x) \subseteq (q^{\alpha}D \oplus N)(q^{2\alpha}a^2, x^2) + \langle (q^{2\alpha}a^2, x^2) \rangle + \langle (q^{\alpha}a, x) \rangle.$$

Pierścień N jest z prawie zerowym mnożeniem, więc $Nx^2 = 0$, czyli wystarczy pokazać, że

$$(q^{2\alpha}aD) \oplus Nx \subseteq (q^{3\alpha}a^2D) \oplus \{0\} + \langle (q^{2\alpha}a^2, x^2) \rangle + \langle (q^{\alpha}a, x) \rangle.$$

Sprowadza się to do pokazania dwóch inkluzji

$$\{0\} \oplus Nx \subseteq (q^{3\alpha}a^2D) \oplus \{0\} + \langle (q^{2\alpha}a^2, x^2) \rangle + \langle (q^{\alpha}a, x) \rangle \tag{4.3}$$

oraz

$$(q^{2\alpha}aD) \oplus \{0\} \subseteq (q^{3\alpha}a^2D) \oplus \{0\} + \langle (q^{2\alpha}a^2, x^2) \rangle + \langle (q^{\alpha}a, x) \rangle. \tag{4.4}$$

Dla $a = 0$ obie inkluzje są oczywiste, gdyż $Nx \subseteq \langle x^2 \rangle$. Niech więc dalej $a \neq 0$.

Dla dowodu inkluzji (4.3), niech $y \in N$. Ponieważ $Nx \subseteq \langle x^2 \rangle$, więc istnieje $k \in \mathbb{Z}$ takie, że $yx = kx^2$. Z filialności D wynika, że $D = q^{\alpha}aD + \langle 1 \rangle$, skąd otrzymujemy, że $ka \in q^{\alpha}aD + \langle 1 \rangle$. Niech $b \in D$ oraz $l \in \mathbb{Z}$ będą takie, że $0 = q^{\alpha}ab + ka + l$. Ponieważ $q^{\alpha}x = 0$ oraz $0 = q^{3\alpha}a^2b + kq^{2\alpha}a^2 + q^{2\alpha}al$, więc

$$(0, yx) = (q^{3\alpha}a^2b, 0) + k(q^{2\alpha}a^2, x^2) + q^{\alpha}l(q^{\alpha}a, x).$$

Dla dowodu inkluzji (4.4), niech $c \in D$ będzie dowolne. Z filialności D wynika, że $c \in q^{\alpha}aD + \langle 1 \rangle$. Istnieją więc $d \in D$ oraz $k \in \mathbb{Z}$ takie, że $c = q^{\alpha}ad + k$. Ponieważ $q^{\alpha}x = 0$ oraz $q^{2\alpha}ac = q^{3\alpha}a^2d + q^{2\alpha}ak$, więc

$$(q^{2\alpha}ac, 0) = (q^{3\alpha}a^2d, 0) + 0 \cdot (q^{2\alpha}a^2, x^2) + q^{\alpha}k(q^{\alpha}a, x),$$

co kończy dowód.

□

Twierdzenie 4.9. *Niech D będzie filialną dziedziną całkowitości charakterystyki zero, która nie jest ciałem, niech $m \in \mathbb{N}$ i niech N będzie niezerowym przemiennym nil-pierścieniem torsyjnym takim, że $\Pi(N) \subseteq \Pi(D)$. Wówczas dla pierścienia $R = mD \oplus N$ następujące warunki są równoważne:*

(i) pierścień R jest filialny,

(ii) N jest pierścieniem z prawie zerowym mnożeniem takim, że $mN = 0$.

Dowód. $(i) \Rightarrow (ii)$. Weźmy dowolne $p \in \Pi(N)$. Wtedy $N_p \neq 0$ i N_p jest ideałowym składnikiem prostym pierścienia N. Wobec tego pierścień $mD \oplus N_p$ jest filialny jako obraz homomorficzny pierścienia filialnego R. Zatem z Twierdzenia 4.8, pierścień N_p

jest z prawie zerowym mnożeniem i $mN_p = 0$. Stąd $mN = 0$ i na mocy Stwierdzenia 2.9, pierścień N jest z prawie zerowym mnożeniem.

$(ii) \Rightarrow (i)$. Z założeń wynika, że dla każdego $p \in \Pi(N)$ pierścień N_p jest z prawie zerowym mnożeniem i istnieje $\alpha_p \in \mathbb{N}$ spełniające warunki $p^{\alpha_p} N_p = 0$ i $p^{\alpha_p} \mid m$. Wobec tego zbiór $\Pi(N)$ jest skończony i z Twierdzenia 4.8 dla każdego $p \in \Pi(N)$ pierścień $S_p = mD \oplus N_p$ jest filialny i może być traktowany jako podpierścień pierścienia R oraz $R = \sum_{p \in \Pi(N)} S_p$. Oznaczmy $n = \prod_{p \in \Pi(N)} p^{\alpha_p}$ oraz $n_p = \frac{n}{p^{\alpha_p}}$ dla $p \in \Pi(N)$. Wtedy $NWD(\{n_p \mid p \in \Pi(N)\}) = 1$ oraz $n_p R \subseteq S_p$ dla każdego $p \in \Pi(N)$. Zatem na mocy Stwierdzenia 4.6 pierścień R jest filialny. □

Twierdzenie 4.10. *Niech R będzie pierścieniem β-radykalnym i niech m będzie liczbą naturalną. Wówczas następujące warunki są równoważne:*

(i) pierścień $m(\mathbb{Z} \boxplus R) + R$ jest filialny,

(ii) R jest pierścieniem z prawie zerowym mnożeniem takim, że $mR = m^2R$ oraz pierścień mR jest prawie podzielny.

Dowód. Oznaczmy $S = m(\mathbb{Z} \boxplus R) + R$. Wówczas $\beta(S) = R$.

$(i) \Rightarrow (ii)$. Pierścień R jest filialny jako ideał pierścienia filialnego S. Z Twierdzenia 1.35 wynika, że R jest nil-H-pierścieniem. Weźmy dowolne $k \in \mathbb{Z}$. Z filialności pierścienia S i tego, że $km \cdot 1 \in Z(S)$ wynika, że

$$km \cdot S = (km)^2 \cdot S + km \cdot \langle 1 \rangle.$$

Zatem dla dowolnego $a \in R$ istnieje $x \in R$ oraz istnieją $l_1, l_2 \in \mathbb{Z}$ takie, że

$$kma = (km)^2(l_1 \cdot 1 + x) + kml_2 \cdot 1,$$

skąd otrzymujemy $((km)^2 l_1 + kml_2) \cdot 1 = kma - (km)^2 x \in R \cap \langle 1 \rangle = 0$. Zatem $kma = k^2m^2x \in k^2(m^2R)$. Stąd $k(mR) = k^2(m^2R)$ dla każdego $k \in \mathbb{Z}$, więc w szczególności $mR = m^2R$ i $k(mR) = k^2(mR)$ dla każdego $k \in \mathbb{Z}$.

Teraz pokażemy, że pierścień R jest z prawie zerowym mnożeniem. Jeśli pierścień R nie jest torsyjny, to na podstawie Stwierdzenia 2.4, jest on pierścieniem z prawie zerowym mnożeniem. Niech dalej pierścień R będzie torsyjny. Zgodnie ze Stwierdzeniem 2.9 wystarczy wykazać, że pierścień R_p jest z prawie zerowym mnożeniem dla każdego $p \in \mathbb{P}$. Jeżeli $p \nmid m$, to $kR_p = k^2R_p$ dla każdego $k \in \mathbb{Z}$, więc na mocy Stwierdzenia 2.12 punkt (iii), pierścień R_p jest z prawie zerowym mnożeniem. Niech dalej $p \mid m$. Jeżeli R_p jest pierścieniem nieograniczonego wykładnika, to ze Stwierdzenia 2.5, R_p jest z prawie zerowym mnożeniem. Niech dalej R_p będzie pierścieniem ograniczonego wykładnika. Wówczas $mR_p = m^2R_p$ i $p \mid m$, więc $mR_p = 0$, skąd $(mR) \cap R_p = 0$. Weźmy dowolne $x, y \in R_p$. Wówczas z Lematu 2.8 wynika, że $\langle x^2 \rangle \lhd R$ i ponadto $mR \lhd R$. Wobec tego

$$\langle x^2 \rangle + \langle m \cdot 1 + x \rangle + mR \lhd \langle x \rangle + \langle x^2 \rangle + \langle m \cdot 1 \rangle + mR \lhd S.$$

Zatem z filialności S, $\langle x^2 \rangle + \langle m \cdot 1 + x \rangle + mR \lhd S$ i $xy = (m \cdot 1 + x)y = Kx^2 + mr + L(m \cdot 1 + x)$ dla pewnych $K, L \in \mathbb{Z}$ i $r \in R$. Stąd $Lm = 0$, czyli $L = 0$ i $xy - Kx^2 \in (mR) \cap R_p = 0$,

więc $xy \in \langle x^2 \rangle$. Analogicznie $xy \in \langle y^2 \rangle$ co wobec Stwierdzenia 2.12 punkt (i) oznacza, że R_p jest pierścieniem z prawie zerowym mnożeniem.

$(ii) \Rightarrow (i)$. Pierścień R jest z prawie zerowym mnożeniem, więc $R^3 = 0$ oraz $aR = Ra = \langle a^2 \rangle$ dla dowolnego $a \in R$. Należy wykazać, że $(\alpha)_S \subseteq (\alpha)_S^2 + \langle \alpha \rangle$ dla dowolnego $\alpha \in S$. Ale $\alpha = km \cdot 1 + a$ dla pewnych $a \in R$ oraz $k \in \mathbb{Z}$, więc ponieważ $km \cdot 1 \in Z(S)$, $(km)^3 \cdot 1 = (km)^3 \cdot 1 + a^3 = \alpha((km)^2 \cdot 1 - kma + a^2) \in (\alpha)_S$. Stąd $(km)^3 R \subseteq (\alpha)_S$. Ponadto $kmR = (km)^2 R$, więc $kmR \subseteq (\alpha)_S$. Ale $aR = Ra = \langle a^2 \rangle$ i $(\alpha)_S = R\alpha R + R\alpha + \alpha R + \langle \alpha \rangle = R(km \cdot 1 + a)R + R(km \cdot 1 + a) + (km \cdot 1 + a)R + \langle \alpha \rangle$, więc ponieważ $RaR \subseteq R^3 = 0$, to

$$(\alpha)_S = kmR + \langle a^2 \rangle + \langle \alpha \rangle. \tag{4.5}$$

Dalej, $a^2 = \alpha^2 - kma - km\alpha$, dlatego $a^2 \in (\alpha)_S^2 + kmR + \langle \alpha \rangle$. Ponadto $\alpha^2 = (km)^2 \cdot 1 + (a^2 + 2kma)$, więc na mocy (4.5) i tego, że $kmR = (km)^2 R$, $(\alpha^2)_S = (km)^2 R + \langle (a^2 + 2kma)^2 \rangle + \langle \alpha^2 \rangle = kmR + \langle \alpha^2 \rangle$. Zatem $kmR \subseteq (\alpha)_S^2$. Ponadto $a^2 = \alpha^2 - kma - km\alpha$, więc $a^2 \in (\alpha)_S^2 + \langle \alpha \rangle$, i wobec (4.5), $(\alpha)_S \subseteq (\alpha)_S^2 + \langle \alpha \rangle$. □

Podstawiając $m = 1$ w powyższym twierdzeniu uzyskujemy następujący wniosek, którego inny dowód był przedstawiony w pracy [14] (por. Theorem 4.2).

Wniosek 4.11. *Niech R będzie pierścieniem β-radykalnym. Wówczas następujące warunki są równoważne:*

(i) pierścień $\mathbb{Z} \boxplus R$ jest filialny,

(ii) R jest prawie podzielnym pierścieniem z prawie zerowym mnożeniem.

4.2 Pierścienie Andrijanowa

Niech $N \neq 0$ będzie prawie podzielnym pierścieniem torsyjnym z prawie zerowym mnożeniem i niech D będzie filialną dziedziną całkowitości charakterystyki zero, która nie jest ciałem i taką, że dla każdego $x \in N$, $o(x) \in S(\Pi(D))$. Weźmy dowolne $x \in N$. Wtedy $D = \langle 1 \rangle + o(x)D$ i dla dowolnego $d \in D$ zapisanego w postaci $d = k \cdot 1 + o(x)d_1$ dla pewnych $k \in \mathbb{Z}$, $d_1 \in D$ kładziemy $d \circ x = kx$. Wówczas działanie $\circ$ jest dobrze określone na mocy Stwierdzenia 1.33. Bezpośrednie rachunki pokazują, że N jest unitarną D-algebrą przy działaniu zewnętrznym $\circ$. Ponadto łatwo zauważyć, że jeśli N jest unitarną D-algebrą przy działaniu zewnętrznym $*$, to $* = \circ$.

Stwierdzenie 4.12. *Niech D będzie filialną dziedziną całkowitości charakterystyki zero, która nie jest ciałem. Niech $p \in \Pi(D)$, $m \in S(\Pi(D))$ i niech N będzie nil-H-p-pierścieniem. Jeżeli $p \nmid m$ i pierścień $m(D \boxplus N)$ jest filialny, to $pN = p^2N$. W szczególności N jest pierścieniem z prawie zerowym mnożeniem.*

Dowód. Oczywiście $m(D \boxplus N) = m(D \boxplus N) + N$. Niech $x \in N$. Wtedy z filialności pierścienia $m(D \boxplus N)$ oraz tego, że $mp \cdot 1 \in Z(D \boxplus N)$ mamy $(mp)x = (md + y)(mp \cdot 1)^2 + U(mp \cdot 1)$ dla pewnych $y \in N$, $d \in D$, $U \in \mathbb{Z}$. Stąd $mpx = m^2p^2y$ i $m^3p^2d = -Ump$. Ale $p \nmid m$, więc z pierwszej równości otrzymujemy, że $px = p^2my$. Zatem $pN \subseteq p^2N$, skąd $pN = p^2N$ i N jest pierścieniem prawie podzielnym. Stąd na podstawie Stwierdzenia 2.12 punkt (iii) uzyskujemy, że N jest pierścieniem z prawie zerowym mnożeniem. □

Definicja 4.13. Niech $N \neq 0$ będzie prawie podzielnym pierścieniem torsyjnym z prawie zerowym mnożeniem i niech D będzie filialną dziedziną całkowitości charakterystyki zero, która nie jest ciałem i taką, że dla każdego $x \in N$, $o(x) \in S(\Pi(D))$. Wtedy pierścień $D \boxplus N$ będziemy nazywali **pierścieniem Andrijanowa**.

Uwaga 4.14. Dla dowolnego pierścienia Andrijanowa $A = D \boxplus N$ mamy $\Pi(A) = \Pi(N) \cup \Pi(D) = \Pi(D)$.

Twierdzenie 4.15. *Dowolny pierścień Andrijanowa $D \boxplus N$ jest filialny.*

Dowód. Niech $R = D \boxplus N$. Jest jasne, że R jest pierścieniem z jedynką, $D \subseteq Z(R)$, $\beta(R) = N \neq 0$ i $R/\beta(R) \cong D$, $R^+ = D^+ \oplus N^+$, $N^3 = 0$, $Na = aN = \langle a^2 \rangle$ i $Da = \langle a \rangle$ dla wszystkich $a \in N$ oraz $lN = l^2N$ dla $l \in \mathbb{N}$. Pokażemy, że $(\alpha)_R \subseteq (\alpha)_R^2 + \langle \alpha \rangle$ dla każdego $\alpha \in R$. Zauważmy, że zachodzi to dla $\alpha \in N$, gdyż wówczas $(\alpha)_R = D\alpha + \langle \alpha^2 \rangle = \langle \alpha \rangle + \langle \alpha^2 \rangle \subseteq (\alpha)_R^2 + \langle \alpha \rangle$. Niech dalej $\alpha \notin N$. Wówczas $\alpha = d + a$ dla pewnych $0 \neq d \in D$ oraz $a \in N$. Skoro D jest filialną dziedziną całkowitości charakterystyki zero, więc na mocy Twierdzenia 1.31, istnieją $k \in S(\Pi(D))$ oraz $u \in D^*$ takie, że $d = ku$. Ale $uN = N$ i wobec tego $dN = kN$. Zatem $d^2N = k^2N = kN = dN$. Dalej, $d^2 - a^2 = \alpha(d - a) \in (\alpha)_R$ oraz $Na^2 = 0$, więc $d^2N \subseteq (\alpha)_R$, skąd $kN \subseteq (\alpha)_R$. Wobec tego

$$(\alpha)_R = D\alpha + \langle a^2 \rangle + kN. \tag{4.6}$$

Dalej, $\alpha^2 = d^2 + (2da + a^2)$, więc po podstawieniu w miejsce α elementu α^2 uzyskamy ze wzoru (4.6), $(\alpha^2)_R = D\alpha^2 + \langle (2da + a^2)^2 \rangle + k^2N$. Ponieważ $k^2N = kN$ oraz $dN = kN$, więc $(\alpha^2)_R = D\alpha^2 + kN$. Dalej, $\alpha^2 = d^2 + 2da + a^2$ i $da \in kN$, więc $(\alpha^2)_R = D(d^2 + a^2) + kN$. Wystarczy zatem wykazać, że $D\alpha \subseteq D(d^2 + a^2) + kN + \langle \alpha \rangle$ oraz $a^2 \in D(d^2 + a^2) + kN + \langle \alpha \rangle$. Ponieważ $D = \langle 1 \rangle + o(a)D$, więc dla dowodu pierwszej inkluzji wystarczy pokazać, że $(o(a)D)\alpha \subseteq D(d^2+a^2)+kN+\langle \alpha \rangle$. Z filialności D mamy, że $D = dD + \langle 1 \rangle$, skąd $o(a)D = o(a)dD + o(a)\langle 1 \rangle$. Zatem $(o(a)D)\alpha = o(a)(d + a)D\alpha + o(a)\langle \alpha \rangle \subseteq (\alpha^2)_R + \langle \alpha \rangle$. Zostało więc do pokazania jeszcze to, że $a^2 \in D(d^2 + a^2) + kN + \langle \alpha \rangle$. Z filialności D istnieją $s_1 \in \mathbb{Z}$ oraz $d_2 \in D$ takie, że $u^{-1} = s_1 \cdot 1 + o(a)d_2$, przy czym $NWD(s_1, o(a)) = 1$, bo $o(a) \in S(\Pi(D))$. Istnieje zatem $l \in \mathbb{Z}$ takie, że $o(a)|ls_1 - 1$. Stąd $(lu^{-1})(d^2 + a^2) + kla - kl(d + a) = lu^{-1}kud + l(u^{-1}a^2) - kld = l(s_1a^2) = a^2$. Tym samym udowodniliśmy filialność pierścienia R. □

Stwierdzenie 4.16. *Niech $R_i = D_i \boxplus N_i$ dla $i = 1, 2$ będą pierścieniami Andrijanowa. Wówczas następujące warunki są równoważne:*

(i) $R_1 \cong R_2$,

(ii) $D_1 \cong D_2$ *i* $N_1 \cong N_2$.

Dowód. $(i) \Rightarrow (ii)$. Niech $f\colon D_1 \boxplus N_1 \to D_2 \boxplus N_2$ będzie izomorfizmem pierścieni. Wówczas $f(\beta(D_1 \boxplus N_1)) = \beta(D_2 \boxplus N_2)$, skąd $f(N_1) = N_2$ i $N_1 \cong N_2$. Dalej, $(D_1 \boxplus N_1)/N_1 \cong (D_2 \boxplus N_2)/N_2$, a więc $D_1 \cong D_2$.

$(ii) \Rightarrow (i)$. Niech $g\colon D_1 \to D_2$ oraz $h\colon N_1 \to N_2$ będą izomorfizmami pierścieni. Wówczas standardowe sprawdzenie, w oparciu o definicję działania $\circ$, pokazuje, że odwzorowanie $F\colon D_1 \boxplus N_1 \to D_2 \boxplus N_2$ dane wzorem $F(d+a) = g(d)+h(a)$ dla $d \in D_1$, $a \in N_1$, jest izomorfizmem pierścieni. □

Twierdzenie 4.17. *Niech $D \boxplus N$ będzie pierścieniem Andrijanowa i niech M będzie niezerowym, przemiennym, torsyjnym nil-pierścieniem takim, że $\Pi(M) \subseteq \Pi(D) \setminus \Pi(N)$. Wówczas dla dowolnego $m \in \mathbb{N}$ i dla pierścienia $R = (mD \boxplus N) \oplus M$ równoważne są warunki:*

(i) pierścień R jest filialny,

(ii) M jest pierścieniem z prawie zerowym mnożeniem takim, że $mM = 0$.

Dowód. $(i) \Rightarrow (ii)$. Ponieważ $(mD \boxplus N)/N \cong mD$, więc pierścień $mD \oplus M$ jest obrazem homomorficznym filialnego pierścienia R. Zatem pierścień $mD \oplus M$ jest filialny i z Twierdzenia 4.9, M jest pierścieniem z prawie zerowym mnożeniem takim, że $mM = 0$.

$(ii) \Rightarrow (i)$. Na mocy Twierdzenia 4.9, pierścień $mD \oplus M$ jest filialny. Weźmy dowolne $a, b \in R$. Wówczas istnieje niepusty, skończony podzbiór Π zbioru $\Pi(N)$ taki, że $a, b \in S = (mD \oplus M) + mD \boxplus N_0$, gdzie $N_0 = \bigoplus_{p \in \Pi} N_p$. Wtedy z Twierdzenia 4.15, pierścień $D \boxplus N_0$ jest filialny. Ale $mD \boxplus N_0 \lhd D \boxplus N_0$, więc pierścień $mD \boxplus N_0$ jest filialny. Ponadto, dla każdego $p \in \Pi(M)$ istnieje $\alpha_p \in \mathbb{N}$ takie, że $p^{\alpha_p} \mid m$ oraz $p^{\alpha_p} M_p = 0$. Niech $n = \prod_{p \in \Pi} p$ i $s = \prod_{p \in \Pi(M)} p^{\alpha_p}$. Ponieważ $\Pi(M) \subseteq \Pi(D) \setminus \Pi(N)$, więc liczby n i s są względnie pierwsze. Dalej, $mD \oplus M$, $mD \boxplus N_0$ i S są podpierścieniami pierścienia R. Zatem na mocy Stwierdzenia 4.6, pierścień S jest filialny. Wobec tego $ab, ba \in (a)_S^2 + \langle a \rangle \subseteq (a)_R^2 + \langle a \rangle$ i pierścień R jest filialny. □

4.3 Pierścienie Krusego

Przedstawimy teraz skomplikowane konstrukcje rozszerzeń pewnych torsyjnych pierścieni z prawie zerowym mnożeniem przez przemienne filialne dziedziny charakterystyki zero nie będące ciałami. Prezentowane rozszerzenia nie są sprowadzalne do klasycznych konstrukcji algebraicznych, takich jak sumy proste, czy różnorodne dołączanie jedynki. Pozwoli to nam budować nowe, nietrywialne przykłady pierścieni filialnych. Jednocześnie prezentowana teoria pokazuje harmonijny związek filialnych dziedzin całkowitości z pierścieniami z prawie zerowym mnożeniem. Pierwsze tego typu rozszerzenia (jedynie przez podpierścienie pierścienia $\mathbb{Z}$) rozważał Kruse (por. [35]) przy opisie H-pierścieni. Z tego powodu nazwaliśmy konstruowane w tym paragrafie pierścienie jego nazwiskiem. Uzasadnienie filialności takich pierścieni jest jednak bardziej skomplikowane niż dowody Krusego przeprowadzane w podobnych rozszerzeniach dla H-pierścieni.

Przykład 4.18. Niech D będzie filialną dziedziną całkowitości charakterystyki zero taką, że $\Pi(D) \neq \emptyset$ i niech $m \in S(\Pi(D))$, $m > 1$. Niech Π_1 i Π_2 będą dowolnymi rozłącznymi podzbiorami w zbiorze wszystkich dzielników pierwszych liczby m, przy czym $\Pi_0 = \Pi_1 \cup \Pi_2 \neq \emptyset$. Dla każdego $p \in \Pi_0$ niech N_p będzie p-pierścieniem z prawie zerowym mnożeniem, przy czym istnieje $0 \neq x_p \in N_p$ taki, że $0 = x_p^2 = p x_p$. Niech dla każdego $p \in \Pi_1$, $N_p^2 = 0$ i $mN_p = 0$. Ponadto, niech dla każdego $p \in \Pi_2$ liczby całkowite U_{0p}, U_{1p}, U_{2p} będą tak dobrane, by $p \nmid U_{0p}$ oraz by kongruencja

$$1 + (2U_{2p} - U_{1p})X + U_{0p}X^2 \equiv 0 \pmod{p} \tag{4.7}$$

nie miała rozwiązania. Z podstawowych własności kongruencji kwadratowych wynika, że dla dowolnej liczby pierwszej p istnieją liczby całkowite U_{0p}, U_{1p}, U_{2p}, dla których powyższa kongruencja nie ma rozwiązania.

Będziemy zakładali, że dla każdego $p \in \Pi_2$ istnieje $y_p \in N_p$ takie, że $py_p \in a(N_p)$, $0 \neq y_p^2 = U_{0p}x_p$, $my_p = U_{1p}x_p$ oraz $N_p = \langle y_p \rangle + a(N_p)$ i $ma(N_p) = 0$. Klasyfikacja takich pierścieni N_p została przedstawiona w Twierdzeniu 2.31. Zauważmy, że $m^2(\bigoplus_{p\in\Pi_0} N_p) = 0$. Z filialności D, $D = \langle 1 \rangle + mD$, skąd $mD = m\langle 1 \rangle + m^2D$. W grupie addytywnej $mD^+ \times \bigoplus_{p\in\Pi_0} N_p^+$ wprowadzamy mnożenie

$$\left(\alpha, \sum_{p\in\Pi_1} z_p + \sum_{p\in\Pi_2} (K_p y_p + z_p)\right) \cdot \left(\beta, \sum_{p\in\Pi_1} z'_p + \sum_{p\in\Pi_2} (K'_p y_p + z'_p)\right) =$$

$$\left(\alpha\beta, (k_1k_2) \sum_{p\in\Pi_1} x_p + \sum_{p\in\Pi_2} (k_1k_2 + k_1U_{2p}K'_p + k_2U_{2p}K_p + K_pK'_pU_{0p})x_p\right), \tag{4.8}$$

gdzie $z_p, z'_p \in a(N_p)$ dla $p \in \Pi_0$, $\alpha = k_1m + m^2d_1$, $\beta = k_2m + m^2d_2$ dla pewnych $k_1, k_2 \in \mathbb{Z}$, $d_1, d_2 \in D$ oraz $K_p, K'_p \in \mathbb{Z}$.

Udowodnimy, że tak zdefiniowane mnożenie zadaje na grupie $mD^+ \times \bigoplus_{p\in\Pi_0} N_p^+$ strukturę pierścienia łącznego. Jeśli $k_1, k_2 \in \mathbb{Z}$, $d_1, d_2 \in D$ są takie, że

$$k_1m + m^2d_1 = k_2m + m^2d_2, \tag{4.9}$$

to $m^2 \mid (k_2m - k_1m)$ w D. Ale $m \in S(\Pi(D))$, więc na mocy Stwierdzenia 1.33, $m \mid k_2 - k_1$ w $\mathbb{Z}$. Zatem $k_2 - k_1 = Qm$ dla pewnego $Q \in \mathbb{Z}$ i $k_1m + m^2d_1 = k_1m + Qm^2 + m^2d_2$, skąd $d_1 = Q + d_2$. W ten sposób udowodniliśmy, że dla dowolnych $k_1, k_2 \in \mathbb{Z}$, $d_1, d_2 \in D$, równość (4.9) zachodzi wtedy i tylko wtedy, gdy

$$\exists Q \in \mathbb{Z} \ : \ k_2 = k_1 + mQ \text{ oraz } d_2 = d_1 - Q. \tag{4.10}$$

Dla $p \in \Pi_2$, $N_p = \{Ky_p + x \ : \ K \in \mathbb{Z}, x \in a(N_p)\}$. Niech $K_1, K_2 \in \mathbb{Z}$, $x_1, x_2 \in a(N_p)$ będą takie, że

$$K_1y_p + x_1 = K_2y_p + x_2. \tag{4.11}$$

Wtedy $(K_1 - K_2)y_p \in a(N_p)$ i $py_p \in a(N_p)$ oraz $y_p \notin a(N_p)$, więc $K_1 - K_2 = Kp$ dla pewnego $K \in \mathbb{Z}$. Stąd $K_2 = K_1 - pK$ i $K_1y_p + x_1 = K_1y_p - pKy_p + x_2$, więc $x_2 = x_1 + K(py_p)$. Wobec tego dla dowolnych $K_1, K_2 \in \mathbb{Z}$, $x_1, x_2 \in a(N_p)$, równość (4.11) zachodzi wtedy i tylko wtedy, gdy

$$\exists K \in \mathbb{Z} \ : \ K_2 = K_1 - pK \text{ i } x_2 = x_1 + K(py_p). \tag{4.12}$$

Każdy element grupy $\bigoplus_{p\in\Pi_0} N_p$ można jednoznacznie zapisać w postaci $x_1 + x_2$, gdzie $x_1 \in \bigoplus_{p\in\Pi_1} N_p$ i $x_2 \in \bigoplus_{p\in\Pi_2} N_p$. Dalej, x_2 można jednoznacznie zapisać w postaci sumy elementów z N_p dla $p \in \Pi_2$, a każdy z tych elementów dla $p \in \Pi_2$ jest postaci $K_py_p + z_p$, gdzie $K_p \in \mathbb{Z}$ i $z_p \in a(N_p)$. Stąd każdy element $x \in \bigoplus_{p\in\Pi_0} N_p$ jest postaci

$$x = \sum_{p\in\Pi_1} z_p + \sum_{p\in\Pi_2} (K_py_p + z_p), \tag{4.13}$$

gdzie każde $K_p \in \mathbb{Z}$, oraz każde $z_p \in a(N_p)$, przy czym wybór elementu $\sum_{p\in\Pi_1} z_p$ jest jednoznaczny, a postać każdego $K_p y_p + z_p$ jest ograniczona warunkiem (4.12).

Zauważmy, że mnożenie na pierwszej współrzędnej jest takie jak w pierścieniu mD, więc pozostaje do sprawdzenia jedynie dobra określoność mnożenia na drugiej współrzędnej. Niech $k_1, k_1', k_2, k_2' \in \mathbb{Z}$, $d_1, d_1', d_2, d_2' \in D$ będą takie, że $k_1 m + m^2 d_1 = k_1' m + m^2 d_1'$, $k_2 m + m^2 d_2 = k_2' m + m^2 d_2'$ oraz niech $K_p, K_p', L_p, L_p' \in \mathbb{Z}$, $z_p, z_p', u_p, u_p' \in a(N_p)$ dla $p \in \Pi_2$ będą takie, że $K_p y_p + z_p = L_p y_p + u_p$, $K_p' y_p + z_p' = L_p' y_p + u_p'$. Wtedy na mocy (4.10) $k_1' \equiv k_1 \pmod m$ i $k_2' \equiv k_2 \pmod m$. Ale $p \mid m$, czyli $k_1' \equiv k_1 \pmod p$ i $k_2' \equiv k_2 \pmod p$ dla każdego $p \in \Pi_0$. Zatem $k_1' k_2' \equiv k_1 k_2 \pmod p$ i $(k_1' k_2')x_p = (k_1 k_2)x_p$ dla każdego $p \in \Pi_0$, skąd $(k_1' k_2')(\sum_{p\in\Pi_0} x_p) = (k_1 k_2)(\sum_{p\in\Pi_0} x_p)$. Ponadto z (4.12) dla każdego $p \in \Pi_2$, $L_p \equiv K_p \pmod p$ i $L_p' \equiv K_p' \pmod p$, więc

$$k_1 U_{2p} K_p' + k_2 U_{2p} K_p + K_p K_p' U_{0p} \equiv k_1' U_{2p} L_p' + k_2' U_{2p} L_p + L_p L_p' U_{0p} \pmod p,$$

dla każdego $p \in \Pi_1$. Powyższe rozważania pokazują, że badane mnożenie jest dobrze określone. Ponadto, wprost z definicji wynika, że jest też ono przemienne, a standardowe sprawdzenie pokazuje, że to mnożenie jest rozdzielne względem dodawania.

Udowodnimy, że badane mnożenie jest łączne. Weźmy dowolne $k_1, k_2, k_3 \in \mathbb{Z}$, $d_1, d_2, d_3 \in D$, $K_p, K_p', K_p'' \in \mathbb{Z}$ dla $p \in \Pi_2$ oraz $z_p, z_p', z_p'' \in a(N_p)$ dla $p \in \Pi_0$ i niech

$$a = \left(k_1 m + m^2 d_1, \sum_{p\in\Pi_1} z_p + \sum_{p\in\Pi_2} (K_p y_p + z_p)\right),$$

$$b = \left(k_2 m + m^2 d_2, \sum_{p\in\Pi_1} z_p' + \sum_{p\in\Pi_2} (K_p' y_p + z_p')\right),$$

$$c = \left(k_3 m + m^2 d_3, \sum_{p\in\Pi_1} z_p'' + \sum_{p\in\Pi_2} (K_p'' y_p + z_p'')\right).$$

Wtedy $ab = (0 \cdot m + m^2 d, (k_1 k_2) \sum_{p\in\Pi_2} x_p + \sum_{p\in\Pi_2} (k_1 U_{2p} K_p' + k_2 U_{2p} K_p + K_p K_p' U_{0p}) x_p)$, dla pewnego $d \in D$, więc $(ab)c = ((k_1 m + m^2 d_1)(k_2 m + m^2 d_2)(k_3 m + m^2 d_3), 0)$ i podobnie $a(bc) = ((k_1 m + m^2 d_1)(k_2 m + m^2 d_2)(k_3 m + m^2 d_3), 0)$, więc $(ab)c = a(bc)$ i mnożenie jest łączne. Otrzymany w ten sposób pierścień będziemy nazywali **pierścieniem Krusego**.

Odnotujmy dodatkowo, że ze wzoru (4.8) dla dowolnych $x, y \in \bigoplus_{p\in\Pi_0} N_p$, $(0, x)(0, y) = (0, xy)$ i stąd $\bigoplus_{p\in\Pi_0} N_p \cong \{(0, x) : x \in \bigoplus_{p\in\Pi_0} N_p\}$. Można więc dokonać utożsamienia $(0, x) \equiv x$ dla $x \in \bigoplus_{p\in\Pi_0} N_p$. Ze wzoru (4.8) otrzymujemy, że przekształcenie $f\colon R \to mD$ dane wzorem $f((d, x)) = d$ dla $d \in mD$, $x \in \bigoplus_{p\in\Pi_0} N_p$ jest homomorfizmem pierścienia R na pierścień mD i $Ker\, f = \bigoplus_{p\in\Pi_0} N_p$. Zatem

$$\bigoplus_{p\in\Pi_0} N_p \lhd R \text{ oraz } R/\bigoplus_{p\in\Pi_0} N_p \cong mD.$$

Dalej ze wzoru (4.8) mamy też, że dla $a, b \in m^2 D$ jest $(a, 0)(b, 0) = (ab, 0)$, skąd $\{(a, 0) : a \in m^2 D\} \cong m^2 D$. Ponadto $\{(a, x) : a \in m^2 D, x \in \bigoplus_{p\in\Pi_0} N_p\} \cong$

$m^2D \times \bigoplus_{p\in\Pi_0} N_p$. Oczywiście $\mathcal{N}(R) = \mathbb{T}(R) = \bigoplus_{p\in\Pi_0} N_p$. Oznaczmy $v = (m, 0)$, $x_0 = \sum_{p\in\Pi_0} x_p$. Wówczas ze wzoru (4.8)

$$v^2 = mv + x_0 \text{ oraz } vx_0 = mx_0 = x_0^2 = 0. \tag{4.14}$$

Twierdzenie 4.19. *Dowolny pierścień Krusego jest filialny.*

Dowód. Niech R będzie pierścieniem Krusego i niech będą zachowane wszystkie oznaczenia użyte w Przykładzie 4.18. Ze wzoru (4.8), $vy_p = U_{2p}x_p$ dla każdego $p \in \Pi_2$. Niech $n = \prod_{p\in\Pi_0} p$ i $n_p = \frac{n}{p}$ dla $p \in \Pi_0$. Wówczas na mocy założeń istnieje $t \in \mathbb{N}$ takie, że dla każdego $p \in \Pi_0$ i dla $m_p = n_p^t$ jest $m_p(\bigoplus_{q\in\Pi_0\setminus\{p\}} N_q) = 0$ oraz $m_pN_p = N_p$. Ponadto wtedy $NWD(\{m_p \ : \ p \in \Pi_0\}) = 1$. Na mocy Stwierdzenia 4.6, wystarczy wykazać, że dla każdego $p \in \Pi_0$ pierścień m_pR jest filialny. Zauważamy, że dla każdego $p \in \Pi_0$

$$m_pR = \{(m_pmd, x) \ : \ d \in D, x \in N_p\}. \tag{4.15}$$

Z filialności pierścienia D, $D = \langle 1\rangle + m_pD$, więc $mD = m\langle 1\rangle + mm_pD$. Stąd $R = \langle v\rangle + m_pR + \bigoplus_{q\in\Pi_0\setminus\{p\}} N_q$. Dalej, $m_p(\bigoplus_{q\in\Pi_0\setminus\{p\}} N_q) = 0$, więc $(m_pR)\cdot(\bigoplus_{q\in\Pi_0\setminus\{p\}} N_q) = 0$. Weźmy dowolne $p \in \Pi_0$ i niech $a \in (m_pD) \times a(N_p)$. Wtedy $a = (m_pmk + m_pm^2d, x)$ dla pewnych $k \in \mathbb{Z}$, $d \in D$, $x \in a(N_p)$. Pokażemy, że dla każdego $b \in m_pR$, $ba \in (m_pR)a^2 + \langle a^2\rangle + \langle a\rangle$. Ze wzoru (4.8), $va - ma = (0, km_px_p)$. Jeżeli $p \mid k$, to $va = ma$ oraz $b = m_pk'v + (m_pm^2d', x')$ dla pewnych $k' \in \mathbb{Z}$, $d' \in D$, $x' \in N_p$, więc $ba = m_pk'ma + (m_pm^2d', x')a$ oraz na mocy wzoru (4.8) $(m_pm^2d', x')a = (m_pm^2d', 0)a = (m_pm^2d'(m_pmk + m_pm^2d), 0)$. Z filialności m_pmD istnieją $d_1 \in D$ oraz $U, V \in \mathbb{Z}$ takie, że $m_pm^2d'(m_pmk + m_pm^2d) = m_pmd_1(m_pmk + m_pm^2d)^2 + U(m_pmk + m_pm^2d)^2 + V(m_pmk + m_pm^2d)$. Zatem $(m_pm^2d', x')a = (m_pmd_1, 0)a^2 + Ua^2 + Va - V(0, x')$. Jeżeli $m_pmk + m_pm^2d = 0$, to stąd $ba \in (m_pR)a^2 + \langle a^2\rangle + \langle a\rangle$. W przeciwnym przypadku $m_pm^2d' = m_pmd_1(m_pmk + m_pm^2d) + U(m_pmk + m_pm^2d) + V$, więc $m \mid V$ w D i na mocy Stwierdzenia 1.33, $m \mid V$ w $\mathbb{Z}$. Stąd $V(0, x) = 0$ i wobec tego, również w tym przypadku, $ba \in (m_pR)a^2 + \langle a^2\rangle + \langle a\rangle$. Niech teraz $p \nmid k$. Ponieważ $p \mid m$, więc $k + md \neq 0$. Zatem z filialności D, $D = \langle 1\rangle + m(k + md)D$. Dalej, $p \nmid m_p$ i $p \nmid k$, więc istnieje $U \in \mathbb{Z}$ takie, że $Uk^2m_p^3 \equiv 1 \pmod p$ i istnieją $V \in \mathbb{Z}$, $d_1 \in D$ takie, że $-U(k + md) = V + m(k + md)d_1$. Zatem $md_1(k + md) + U(k + md) + V = 0$, skąd po pomnożeniu obu stron ostatniej równości przez m_p^2m

$$(m_pmd_1)(km_pm + m_pm^2d) + Um_p(km_pm + m_pm^2d) + Vm_p^2m = 0. \tag{4.16}$$

Ponadto, $a^2 = ((km_pm + m_pm^2d)^2, k^2m_p^2x_p)$ i $mx = 0$, więc $(m_pmd_1, 0)a^2 + Um_pa^2 + Vm_p^2ma = ((m_pmd_1)(km_pm + m_pm^2d)^2 + Um_p(km_pm + m_pm^2d)^2 + Vm_p^2m(km_pm + m_pm^2d), Um_p^3k^2x_p)$ i stąd wobec (4.16) i tego, że $Uk^2m_p^2 \equiv 1 \pmod p$, $(m_pmd_1, 0)a^2 + Um_pa^2 + Vm_p^2ma = (0, x_p)$. Zatem

$$(0, x_p) \in (m_pR)a^2 + \langle a^2\rangle + \langle a\rangle. \tag{4.17}$$

Weźmy dowolne $b \in m_pR$. Wtedy $b = (m_pmd', x')$ dla pewnych $d' \in D$, $x' \in N_p$. Ponadto $ba = (m_pmd', 0)a = ((m_pmd')(km_pm + m_pm^2d), Lx_p)$ dla pewnego $L \in \mathbb{Z}$. Stąd i z (4.17) pozostaje sprawdzić, że

$$(m_pmd'(km_pm + m_pm^2d), 0) \in (m_pR)a^2 + \langle a^2\rangle + \langle a\rangle. \tag{4.18}$$

Ale $D = \langle 1\rangle + m_p m(k+md)D$, więc istnieje $d_1 \in D$ takie, że $d' = W + m_p m(k+md)d_1$ dla pewnego $W \in \mathbb{Z}$. Stąd $(m_p m d')(km_p m + m_p m^2 d) = W m_p m(km_p m + m_p m^2 d) + (m_p m d_1)(km_p m + m_p m^2 d)^2$ i wobec tego $(m_p m d'(km_p m + m_p m^2 d), 0) = (m_p m d_1, 0)a^2 + W m_p m a$. Zatem

$$(m_p R)a \subseteq (m_p R)a^2 + \langle a^2\rangle + \langle a\rangle \text{ dla każdego } a \in (m_p m D) \times a(N_p). \tag{4.19}$$

Jeśli $p \in \Pi_1$, to $N_p = a(N_p)$ i w tym przypadku filialność pierścienia $m_p R$ dla $p \in \Pi_1$ wynika bezpośrednio z (4.19). Pozostaje zatem uzasadnić, że dla $p \in \Pi_2$ pierścień $m_p R$ jest również filialny, co wobec (4.19) sprowadza się do wykazania, że dla każdego całkowitego K niepodzielnego przez $p \in \Pi_2$ i dla dowolnych $k \in \mathbb{Z}$, $d \in D$, $z \in a(N_p)$ oraz dla $a = (km_p m + m_p m^2 d, Ky_p + z)$ mamy

$$(m_p R)a \subseteq (m_p R)a^2 + \langle a^2\rangle + \langle a\rangle. \tag{4.20}$$

Ze wzoru (4.8) wynika, że przekształcenie $\varphi\colon (pm_p m D) \times N_p \to R$ dane wzorem $\varphi((pm_p m d, x)) = (pm_p m d, x)$ dla $d \in D$, $x \in N_p$ jest zanurzeniem pierścieni. Ponadto $\varphi((pm_p m D) \times N_p) \lhd R$. Zgodnie z Twierdzeniem 4.8, pierścień $(pm_p m D) \times N_p$ jest filialny, gdyż $(pm)N_p = 0$ i N_p jest pierścieniem z prawie zerowym mnożeniem. Z filialności D, $D = \langle 1\rangle + pm_p m D$, więc $m_p m D = m_p m\langle 1\rangle + pm_p^2 m^2 D$, skąd $m_p m D = m_p m\langle 1\rangle + pm_p m D$. Wobec tego

$$m_p R = \langle m_p v\rangle + (pm_p m D) \times N_p. \tag{4.21}$$

Ze wzoru (4.8) wynika, że dla każdego $d' \in pm_p m D$ mamy

$$(m_p v)(d', 0) = m_p m(d', 0). \tag{4.22}$$

Dalej, $(m_p v)^2 = m_p^2 v^2 = m_p^2(mv + \sum_{q\in\Pi_0} x_q) = m_p m(m_p v) + m_p^2 x_p$, czyli

$$(m_p v)^2 = m_p m(m_p v) + m_p^2 x_p. \tag{4.23}$$

Załóżmy, że $p \mid k$. Wtedy $a \in (pm_p m D) \times N_p$. Jeśli $b \in (pm_p m D) \times N_p$, to z filialności pierścienia $(pm_p m D) \times N_p$, $ba = ca^2 + Ua^2 + Va$ dla pewnych $U, V \in \mathbb{Z}$ i $c \in (pm_p m D) \times N_p$, czyli $ba \in (m_p R)a^2 + \langle a^2\rangle + \langle a\rangle$. Zatem dla k podzielnego przez p pozostaje wykazać, zgodnie z (4.21), że $(m_p v)a \in (m_p R)a^2 + \langle a^2\rangle + \langle a\rangle$. Ale ze wzoru (4.8), $(m_p v)a - (m_p m)a \in \langle (0, x_0)\rangle$, więc pozostaje wykazać, że $(0, x_0) \in (m_p R)a^2 + \langle a^2\rangle + \langle a\rangle$. Ze wzoru (4.8) $a^2 = ((km_p, +m_p m^2 d)^2, K^2 U_{0p} x_p)$. Jeśli $k + md = 0$, to $a^2 = (0, K^2 U_{0p} x_p)$, a ponieważ $p \nmid K$ i $p \nmid U_{0p}$, więc $(0, x_0) \in \langle a^2\rangle$. Niech dalej $k + md \neq 0$. Wtedy z filialności D, $D = \langle 1\rangle + m(k+md)D$. Ponadto istnieje $U \in \mathbb{Z}$ takie, że $UK^2 U_{0p} m_p \equiv 1 \pmod p$ i istnieją $V \in \mathbb{Z}$, $d_1 \in D$ takie, że $-U(k + md) = V + m(k + md)d_1$. Zatem $md_1(k + md) + U(k + md) + V = 0$, skąd po pomnożeniu przez $m_p^2 m$

$$(m_p m d_1)(km_p m + m_p m^2 d) + U m_p(km_p m + m_p m^2 d) + V m_p^2 m = 0.$$

Stąd $(m_p m d_1)a^2 + U m_p a^2 + V m_p^2 m a = ((m_p m d_1)(km_p m + m_p m^2 d)^2, 0) + (U m_p(km_p m + m_p m^2 d)^2, x_p) + (V m_p^2 m(km_p m + m_p m^2 d), 0) = (0, x_0)$, co kończy rozważania w przypadku, gdy $p \mid k$.

Niech teraz $p \nmid k$. Wtedy $a = (km_pm + pm_pmr, Ky_p + z)$, gdzie $r = \frac{m}{p}d \in D$. Dalej, ze wzoru (4.8), $(pm_pmr, 0)a = (pm_pmr(km_pm + pm_pmr), 0)$ i $km_pma = (km_pm(km_pm + pm_pmr), kKm_pmy_p)$, więc $km_pma + (pm_pmr, 0)a = ((km_pm + pm_pmr)^2, kKm_pmy_p)$. Ale $my_p = U_{1p}x_p$, więc $km_pma + (pm_pmr, 0)a = ((km_pm + pm_pmr)^2, kKm_pU_{1p}x_p)$. Ze wzoru (4.8), $(m_pmr, 0)(pa) = (m_pmr \cdot p(km_pm + pm_pmr), 0)$, więc

$$km_pma + (m_pmr, 0)(pa) = ((km_pm + pm_pmr)^2, kKm_pU_{1p}x_p) \tag{4.24}$$

Ponadto, ze wzoru (4.8) mamy

$$a^2 = ((km_pm + pm_pmr)^2, (k^2m_p^2 + 2km_pKU_{2p} + K^2U_{0p})x_p). \tag{4.25}$$

Ze wzorów (4.24) i (4.25) otrzymujemy

$$a^2 - [km_pma + (m_pmr, 0)(pa)] = (0, (k^2m_p^2 + 2km_pKU_{2p} + K^2U_{0p} - kKm_pU_{1p})x_p).$$

Ale z udowodnionego kroku dla k podzielnych przez p mamy

$$(m_pmr, 0)(pa) \in (m_pR)(pa)^2 + \langle (pa)^2 \rangle + \langle pa \rangle,$$

stąd

$$(0, (k^2m_p^2 + 2km_pKU_{2p} + K^2U_{0p} - kKm_pU_{1p})x_p) \in (m_pR)a^2 + \langle a^2 \rangle + \langle a \rangle. \tag{4.26}$$

Ale $p \nmid k$ i $p \nmid m_p$ więc istnieje $L \in \mathbb{Z}$ takie, że $K \equiv Lm_pk \pmod{p}$. Stąd

$$\begin{aligned}
&(k^2m_p^2 + 2km_pKU_{2p} + K^2U_{0p} - kKm_pU_{1p})x_p \\
&= (k^2m_p^2 + 2k^2Lm_p^2U_{2p} + L^2m_p^2k^2U_{0p} - k^2m_p^2LU_{1p})x_p \\
&= [k^2m_p^2(1 + 2LU_{2p} + L^2U_{0p} - LU_{1p})]x_p \\
&= k^2m_p^2(1 + (2U_{2p} - U_{1p})L + U_{0p}L^2)x_p.
\end{aligned}$$

i dalej, z warunku (4.7) mamy

$$(0, x_p) \in (m_pR)a^2 + \langle a^2 \rangle + \langle a \rangle. \tag{4.27}$$

Ponieważ $(m_pv)a - m_pma \in \langle (0, x_p) \rangle$, więc z (4.27)

$$(m_pv)a - m_pma \in (m_pR)a^2 + \langle a^2 \rangle + \langle a \rangle. \tag{4.28}$$

Ponadto dla $y \in N_p$, $(0, y)a \in \langle (0, x_p) \rangle$, więc z (4.27)

$$(\{0\} \times N_p)a \subseteq (m_pR)a^2 + \langle a^2 \rangle + \langle a \rangle. \tag{4.29}$$

Dla $d_1 \in D$, $(pm_pmd_1, 0)a = (m_pmd_1, 0)(pa) \in (m_pR)(pa)^2 + \langle (pa)^2 \rangle + \langle pa \rangle$ na mocy udowodnionego kroku dla k podzielnych przez p, co razem z (4.29) daje

$$((pm_pmD) \times N_p)a \subseteq (m_pR)a^2 + \langle a^2 \rangle + \langle a \rangle.$$

Stąd i z (4.21) mamy ostatecznie, że $(m_pR)a \subseteq (m_pR)a^2 + \langle a^2 \rangle + \langle a \rangle$. □

Stwierdzenie 4.20. *Jeżeli R jest pierścieniem Krusego, to dla każdego $p \in \Pi_0$, $\mathcal{N}(R)_p$ nie wydziela się w R jako ideałowy składnik prosty.*

Dowód. Załóżmy, że dla pewnego $p \in \Pi_0$ istnieje $I \lhd R$ taki, że $N_p \oplus I = R$, gdzie $N_p = \mathcal{N}(R)_p$. Wtedy $\mathbb{T}(R) = N_p \oplus \mathbb{T}(I)$, ale $\mathbb{T}(R) = \bigoplus_{q\in\Pi_0} N_q$, więc $\mathbb{T}(I) = \bigoplus_{q\in\Pi_0\setminus\{p\}} N_q$. Dalej, $v = y_0 + i_0$ dla pewnych $y_0 \in N_p$, $i_0 \in I$. Ale $o(v) = \infty$, więc również $o(i_0) = \infty$. Stąd $v^2 = y_0^2 + i_0^2$ i $v^2 = mv + x_0 = my_0 + mi_0 + \sum_{q\in\Pi_0} x_q = (my_0 + x_p) + (mi_0 + \sum_{q\in\Pi_0\setminus\{p\}} x_q)$. Zatem $y_0^2 = my_0 + x_p$ oraz $i_0^2 = mi_0 + \sum_{q\in\Pi_0\setminus\{p\}} x_q$. Jeżeli $y_0 \in a(N_p)$, to $y_0^2 = my_0 = 0$, skąd $x_p = 0$, sprzeczność. Zatem $y_0 \notin a(N_p)$ i stąd $p \in \Pi_2$, a więc istnieją $K \in \mathbb{Z}$ oraz $z_0 \in a(N_p)$ takie, że $p \nmid K$ oraz $y_0 = Ky_p + z_0$. Stąd $y_0^2 = K^2y_p^2 = K^2U_{0p}x_p$ i $my_0 = K(my_p) = KU_{1p}x_p$. Wobec tego $K^2U_{0p}x_p = KU_{1p}x_p + x_p$, czyli

$$K^2U_{0p} - KU_{1p} - 1 \equiv 0 \pmod{p}. \tag{4.30}$$

Ponadto $vy_p = y_0y_p$, więc $U_{2p}x_p = Ky_p^2 = KU_{0p}x_p$. Stąd

$$U_{2p} \equiv KU_{0p} \pmod{p}. \tag{4.31}$$

Z (4.30) i (4.31) wynika, że $K^2U_{0p} + K(U_{1p} - 2U_{2p}) + 1 \equiv K^2U_{0p} + K^2U_{0p} - 1 - 2K^2U_{0p} + 1 \equiv 0 \pmod{p}$, co przeczy warunkowi (4.7). □

Stwierdzenie 4.21. *Jeżeli dla pierścienia Krusego R i każdego $p \in \Pi_0$ pierścień $\mathcal{N}(R)_p$ jest nierozkładalny na sumę prostą swoich dwóch niezerowych ideałów, to R również nie rozkłada się na sumę prostą swoich dwóch niezerowych ideałów.*

Dowód. Załóżmy, że przy założeniach stwierdzenia i stosowanych w tym paragrafie oznaczeniach, pierścień R jest sumą prostą dwóch swoich niezerowych ideałów I, J. Wtedy $\mathcal{N}(R) = \mathcal{N}(I) \oplus \mathcal{N}(J)$, skąd $R/\mathcal{N}(R) \cong I/\mathcal{N}(I) \oplus J/\mathcal{N}(J)$. Ale $R/\mathcal{N}(R) \cong mD$, więc bez zmniejszania ogólności możemy zakładać, że $J = \mathcal{N}(J)$. Stąd $J \subseteq \mathbb{T}(R)$ i zbiór $\Pi = \{p \in \Pi_0 \,:\, J_p \neq 0\}$ jest niepusty oraz $J = \bigoplus_{p\in\Pi} J_p$. Ponadto dla każdego $p \in \Pi$ zachodzi $N_p = I_p \oplus J_p$, co wobec nierozkładalności N_p na sumę dwóch niezerowych ideałów oznacza, że $I_p = 0$, czyli $J_p = N_p$ i $J = \bigoplus_{p\in\Pi} N_p$. Zatem $R = I \oplus (\bigoplus_{p\in\Pi} N_p)$, co przeczy Stwierdzeniu 4.20. □

Stwierdzenie 4.22. *Jeżeli R jest pierścieniem Krusego, to*

$$[v] + \bigoplus_{p\in\Pi_0} N_p = \langle v\rangle + \bigoplus_{p\in\Pi_0} N_p, \tag{4.32}$$

oraz $[v] + \bigoplus_{p\in\Pi_0} N_p$ jest H-pierścieniem.

Dowód. Zastosujemy oznaczenia wprowadzone w dowodzie Twierdzenia 4.19. Na mocy (4.14), $A = \langle v\rangle + \bigoplus_{p\in\Pi_0} N_p = [v] + \bigoplus_{p\in\Pi_0} N_p$ i A jest podpierścieniem pierścienia R.

Pokażemy najpierw, że dla każdego $p \in \Pi_0$ i dla dowolnych $a, b \in m_pA$ zachodzi $ab \in [b]$. Zauważmy, że $m_pA = \langle m_pv\rangle + N_p$. Stąd $b = km_pv + x$ dla pewnych $k \in \mathbb{Z}$, $x \in N_p$. Możliwe są tylko dwa przypadki: (1) $x \in a(N_p)$ i (2) $x^2 \neq 0$.

W przypadku (1), $vx = mx = 0$, więc $vb = km_pv^2 = km_pmv + km_px_p$. Jeżeli $p \mid k$, to $vb = km_pmv = mb \in [b]$. Ponadto wtedy dla $y \in N_p$ mamy $yb = 0$. Ale

$a \in \langle m_p v\rangle + N_p$, więc wówczas $ab \in [b]$. Niech teraz $p \nmid k$. Wtedy $b^2 = k^2 m_p^2 v^2 = k^2 m_p^2 mv + k^2 m_p^2 x_p = k m_p mb + k^2 m_p^2 x_p$, skąd $k^2 m_p^2 x_p \in [b]$, a więc $x_p \in [b]$. Zatem $vb = mb + k m_p x_p \in [b]$ oraz $yb = 0$ dla $y \in N_p$, więc także $ab \in [b]$.

W przypadku (2), $p \in \Pi_2$ i $N_p = \langle y_p\rangle + a(N_p)$, więc $x = Ky_p + z$ dla pewnych $K \in \mathbb{Z}$, $p \nmid K$, $z \in a(N_p)$. Załóżmy, że $p \mid k$. Wtedy $b^2 = k^2 m_p^2 mv + K^2 U_{0p} x_p$ oraz $k m_p mb = k^2 m_p^2 mv$, skąd $K^2 U_{0p} x_p \in [b]$, a zatem $x_p \in [b]$. Ponadto, $mb = k m_p mv + K U_{1p} x_p$, więc $k m_p mv \in [b]$. Dalej, $vb = k m_p mv + K U_{2p} x_p$, skąd $vb \in [b]$. Dla $y \in N_p$ mamy $yb = yx \in \langle x_p\rangle \subseteq [b]$. Wobec tego $ab \in [b]$. W końcu, niech $p \nmid k$. Wtedy $b^2 - k m_p mb = k^2 m_p^2 mv + k^2 m_p^2 x_p + 2kK m_p v y_p + K^2 y_p^2 - k^2 m_p^2 mv - k m_p K(m y_p) = (k^2 m_p^2 + 2k^2 m_p^2 L U_{2p} + L^2 m_p^2 k^2 U_{0p} - k^2 m_p^2 L U_{1p}) x_p$, skąd na mocy (4.7), $x_p \in [b]$. Dalej, na mocy (4.8), $vx - mx \in \langle x_p\rangle$, wobec tego $vb - mb = k m_p x_p + (vx - mx) \in \langle x_p\rangle \subseteq [b]$, więc $vb \in [b]$ oraz dla $y \in N_p$, $yb \in \langle x_p\rangle \subseteq [b]$. Zatem $ab \in [b]$.

Niech teraz $a, b \in A$ będą dowolne. Istnieją wówczas $k_p \in \mathbb{Z}$, $p \in \Pi_0$ takie, że $\sum_{p\in\Pi_0} k_p m_p = 1$, więc $a = \sum_{p\in\Pi_0} k_p (m_p a)$ i $b = \sum_{p\in\Pi_0} k_p (m_p b)$. Zatem z pierwszej części dowodu $ab = \sum_{p,q\in\Pi_0} (k_p k_q)((m_p a)(m_q b)) \in \sum_{q\in\Pi_0} [m_q b] \subseteq [b]$. Stąd $[b] \lhd A$ i A jest H-pierścieniem. □

Twierdzenie 4.23. *Niech R będzie pierścieniem Krusego opisanym w Przykładzie 4.18 i niech M będzie niezerowym, przemiennym i torsyjnym nil-pierścieniem takim, że $\Pi(M) \subseteq \Pi(D) \setminus \Pi_0$. Wówczas dla pierścienia $S = R \oplus M$ równoważne są warunki:*

(i) pierścień S jest filialny,

(ii) M jest pierścieniem z prawie zerowym mnożeniem takim, że $mM = 0$.

Dowód. $(i) \Rightarrow (ii)$. Ponieważ $R/\mathcal{N}(R) \cong mD$, więc pierścień $mD \oplus M$ jest filialny jako obraz homomorficzny pierścienia filialnego S. Na podstawie Twierdzenia 4.9, M jest pierścieniem z prawie zerowym mnożeniem takim, że $mM = 0$.

$(ii) \Rightarrow (i)$. Na mocy założeń dla każdego $p \in \Pi(M)$ istnieje $\alpha_p \in \mathbb{N}$ takie, że $p^{\alpha_p} \mid m$ i $p^{\alpha_p} M_p = 0$. Niech $n = \prod_{p\in\Pi(M)} p^{\alpha_p}$ i $s = \prod_{p\in\Pi_0} p$. Wtedy $s^\alpha N = 0$ dla pewnego $\alpha \in \mathbb{N}$. Ponieważ $\Pi(M) \subseteq \Pi(D) \setminus \Pi_0$, więc $NWD(n, s) = 1$. Ponadto $nM = 0$ i $s^\alpha N = 0$, więc $s^\alpha R \cong s^\alpha mD$. Zatem na mocy Twierdzenia 4.9, pierścień $s^\alpha R \oplus M$ jest filialny. Ale pierścień R też jest filialny oraz R i $s^\alpha R \oplus M$ są podpierścieniami pierścienia S, przy czym $S = R + (s^\alpha R \oplus M)$, więc na mocy Stwierdzenia 4.6, pierścień S jest filialny. □

Przykład 4.24. Niech R będzie pierścieniem Krusego. Zachowujemy wszystkie oznaczenia stosowane w dowodzie Twierdzenia 4.19. Niech M będzie torsyjnym, niezerowym, przemiennym prawie podzielnym pierścieniem z prawie zerowym mnożeniem takim, że $o(x) \in S(\Pi(D))$ oraz $NWD(o(x), m) = 1$ dla każdego $x \in M$.

Niech s będzie liczbą naturalną względnie pierwszą z liczbą m. Wtedy $s\mathcal{N}(R) = \mathcal{N}(R)$, na mocy naszych założeń. Z filialności D, $D = \langle 1\rangle + sD$, czyli $mD = m\langle 1\rangle + msD$, skąd $R = \langle v\rangle + sR + \mathcal{N}(R)$, a więc $R = \langle v\rangle + sR$, bo $s\mathcal{N}(R) = \mathcal{N}(R)$. Niech dodatkowo $x \in M$ będzie takie, że $o(x) | s$. Wykażemy, że dla dowolnych $k_1, k_2 \in \mathbb{Z}$, $r_1, r_2 \in R$

$$k_1 v + s r_1 = k_2 v + s r_2 \Longrightarrow (k_1 m)x = (k_2 m)x. \tag{4.33}$$

Rzeczywiście, przechodząc do pierścienia ilorazowego $R/\mathcal{N}(R) \cong mD$ uzyskamy, że $k_1m + smd_1 = k_2m + smd_2$ dla pewnych $d_1, d_2 \in D$. Stąd $s|k_1 - k_2$. Ale $o(x)|s$, więc $o(x)|k_1 - k_2$ w pierścieniu D i na mocy Stwierdzenia 1.33, $o(x)|k_1 - k_2$ w pierścieniu $\mathbb{Z}$. Wobec tego $(k_1 - k_2)x = 0$, skąd $(k_1m)x = (k_2m)x$.

Możemy teraz zdefiniować działanie zewnętrzne $\circ\colon R \times M \to M$ w następujący sposób: jeśli $x \in M$ oraz $a \in R$ i s jest liczbą naturalną względnie pierwszą z liczbą m taką, że $o(x)|s$ oraz $a = kv + sr$ dla pewnych $k \in \mathbb{Z}$, $r \in R$, to $a \circ x = (km)x$. Własność (4.33) gwarantuje nam poprawną określoność $\circ$. Natomiast standardowe sprawdzenie pokazuje, że działanie zewnętrzne $\circ$ zadaje na M strukturę R-algebry.

Pokażemy, że pierścień $S = R \boxplus M$ jest filialny. Najpierw zauważmy, że $m^2R \cong m^3D$, bo na mocy Przykładu 4.18, $m^2\mathcal{N}(R) = 0$, $m^2R \cap \mathcal{N}(R) = 0$ i $\varphi\colon mD \to R/\mathcal{N}(R)$ jest izomorfizmem pierścieni takim, że $\varphi(m) = v + \mathcal{N}(R)$. Stąd i ze zgodności działań zewnętrznych wynika, że $\Phi\colon m^3D \boxplus M \to m^2R \boxplus M$ dane wzorem $\Phi(m^3d, x) = (\varphi(m^3d), x)$, dla $d \in D$, $x \in M$ jest izomorfizmem pierścieni. Ponadto $m^2M = M$, więc $m^2S \cong m^3D \boxplus M$. Ale pierścień $D \boxplus M$ jest filialny na mocy Twierdzenia 4.15 i ponieważ $m^3D \boxplus M \lhd D \boxplus M$, więc $m^2R \boxplus M$ jest pierścieniem filialnym jako ideał pierścienia filialnego. Zatem m^2S jest pierścieniem filialnym.

Niech M' będzie skończoną sumą prostą pewnych p-komponent pierścienia M. Wtedy istnieje $n \in \mathbb{N}$ takie, że $NWD(n, m) = 1$ oraz dla każdego $x \in M'$, istnieje $t \in \mathbb{N}$ takie, że $n^tx = 0$. Niech $S' = R \boxplus M'$. Wtedy $m^2S' \lhd m^2S$, więc m^2S' jest pierścieniem filialnym. Ponadto $S' = m^2S' + R$ i wobec tego na podstawie Stwierdzenia 4.6 pierścień S' jest filialny. Weźmy dowolne $a, b \in S$. Wtedy istnieje pierścień M' będący skończoną sumą prostą pewnych p-komponent pierścienia M taki, że $a, b \in S' = R \boxplus M'$. Zatem z filialności S', $ab \in S'a^2 + \langle a^2\rangle + \langle a\rangle \subseteq Sa^2 + \langle a^2\rangle + \langle a\rangle$, co kończy dowód filialności pierścienia S.

Tak skonstruowany pierścień S będziemy nazywali **uogólnionym pierścieniem Krusego**.

Stwierdzenie 4.25. *Jeżeli $S = R \boxplus M$ jest uogólnionym pierścieniem Krusego, to dla każdej liczby pierwszej p takiej, że $S_p \neq 0$, S_p nie wydziela się w S jako ideałowy składnik prosty.*

Dowód. Zachowujemy wszystkie oznaczenia z Przykładu 4.24. Istnieje niepusty zbiór Π_3 liczb pierwszych taki, że $M = \bigoplus_{p\in\Pi_3} M_p$ oraz $M_p \neq 0$ dla $p \in \Pi_3$. Stąd dla $p \in \mathbb{P}$ mamy $S_p \neq 0$ wtedy i tylko wtedy, gdy $p \in \Pi_0 \cup \Pi_3$. Załóżmy, że dla pewnego $p \in \Pi_0 \cup \Pi_3$ istnieje $I \lhd S$ taki, że $I \oplus S_p = S$.

Rozważmy najpierw przypadek, gdy $p \in \Pi_3$. Wtedy $S_p = M_p$. Dla każdego $q \in \Pi_3 \setminus \{p\}$, $(M_p)_q \oplus I_q = S_q$, więc $I_q = M_q$, skąd $\bigoplus_{q\in\Pi_3\setminus\{p\}} M_q \subseteq I$. Ponadto dla każdego $q \in \Pi_0$, $(M_p)_q \oplus I_q = S_q$, więc $I_q = N_q$, skąd $N = \bigoplus_{q\in\Pi_0} N_q \subseteq I$. Ale $S/M \cong R$ i $R/N \cong mD$, więc stąd $I/J \cong mD$ dla $J = N \oplus (\bigoplus_{q\in\Pi\setminus\{p\}} M_q)$. Wobec tego $mD \oplus M_p \cong I/J \oplus M_p$. Ale pierścień $I/J \oplus M_p$ jest obrazem homomorficznym filialnego pierścienia S, więc pierścień $mD \oplus M_p$ jest filialny, co przeczy Twierdzeniu 4.8, bo $p \nmid m$.

Niech dalej $p \in \Pi_0$. Wtedy $S_p = N_p$. Dla każdego $q \in \Pi_3$, $(N_p)_q \oplus I_q = S_q$, więc $I_q = M_q$, skąd $M \subseteq I$. Wobec tego $(N_p + M)/M \oplus I/M = S/M$. Ponadto $S/M \cong R$ oraz $(N_p + M)/M \cong N_p$, więc otrzymujemy sprzeczność ze Stwierdzeniem 4.20. $\square$

Twierdzenie 4.26. *Niech $R \boxplus M$ będzie uogólnionym pierścieniem Krusego opisanym w Przykładzie 4.24 i niech M_0 będzie niezerowym, przemiennym i torsyjnym nil-pierścieniem takim, że $\Pi(M) \subseteq \Pi(D) \setminus (\Pi_0 \cup \Pi(M))$. Wówczas dla pierścienia $T = (R \boxplus M) \oplus M_0$ równoważne są warunki:*

(i) pierścień T jest filialny,

(ii) M_0 jest pierścieniem z prawie zerowym mnożeniem takim, że $mM_0 = 0$.

Dowód. $(i) \Rightarrow (ii)$. Ponieważ $(R \boxplus M)/\mathcal{N}(R \boxplus M) \cong mD$, więc pierścień $mD \oplus M_0$ jest obrazem homomorficznym filialnego pierścienia T. Stąd pierścień $mD \oplus M_0$ jest filialny i na mocy Twierdzenia 4.9, M_0 jest pierścieniem z prawie zerowym mnożeniem takim, że $mM_0 = 0$.

$(ii) \Rightarrow (i)$. Weźmy dowolne $a, b \in T$. Wtedy istnieje niepusty, skończony podzbiór Π zbioru $\Pi(M)$ taki, że $a, b \in S = (R \boxplus X) \oplus M_0$, gdzie $X = \bigoplus_{p \in \Pi} M_p$. Z Przykładu 4.24 wiemy, że pierścień $R \boxplus X$ jest filialny. Na mocy założeń, dla każdego $p \in \Pi(M_0)$ istnieje $\alpha_p \in \mathbb{N}$ takie, że $p^{\alpha_p} \mid m$ i $p^{\alpha_p}(M_0)_p = 0$. Niech $n = \prod_{p \in \Pi(M_0)} p^{\alpha_p}$ i $s = \prod_{p \in \Pi_0 \cup \Pi} p$. Wtedy $s^\alpha(N + X) = 0$ dla pewnego $\alpha \in \mathbb{N}$. Ponieważ $\Pi(M_0) \subseteq \Pi(D) \setminus (\Pi_0 \cup \Pi(M))$, więc $NWD(n, s) = 1$. Ponadto $nM_0 = 0$ i $s^\alpha(N + X) = 0$, więc $s^\alpha(R \boxplus X) \cong s^\alpha mD$. Zatem na podstawie Twierdzenia 4.9 pierścień $s^\alpha(R \boxplus X) \oplus M_0$ jest filialny. Ale pierścień $R \boxplus X$ też jest filialny oraz $R \boxplus X$ i $s^\alpha(R \boxplus X) \oplus M_0$ są podpierścieniami pierścienia S, przy czym $S = (R \boxplus X) + [(s^\alpha(R \boxplus X) \oplus M)]$, więc na mocy Stwierdzenia 4.6, pierścień S jest filialny. Stąd $ab \in Sa^2 + \langle a^2 \rangle + \langle a \rangle \subseteq Ta^2 + \langle a \rangle + \langle a \rangle$ i pierścień T jest filialny. $\square$

4.4 Klasyfikacja pewnych rozszerzeń za pomocą pierścieni Krusego i pierścieni Andrijanowa

W całym paragrafie R jest przemiennym pierścieniem filialnym takim, że $N = \mathcal{N}(R) \neq 0$, przy czym grupa N^+ ma ograniczony wykładnik oraz istnieje filialna dziedzina całkowitości D charakterystyki zero nie będąca ciałem i istnieje $m \in S(\Pi(D))$ takie, że $R/N \cong mD$. Wobec tego istnieje skończony, niepusty zbiór $\Pi_0 \subseteq \mathbb{P}$ taki, że $N = \bigoplus_{p \in \Pi_0} N_p$ oraz $N_p \neq 0$ dla każdego $p \in \Pi_0$. Niech $\Pi_1 = \{p \in \Pi_0 \ : \ p \mid m\}$ i $\Pi_2 = \{p \in \Pi_0 \ : \ p \nmid m\}$. Wtedy $\Pi_0 = \Pi_1 \cup \Pi_2$. Załóżmy też, że $\Pi_0 \subseteq \Pi(D)$ i N_p nie wydziela się jako ideałowy składnik prosty w R dla żadnego $p \in \Pi_1$.

Z przyjętych założeń wynika, że pierścień R jest $\mathbb{S}$-półprosty i istnieje $t \in \mathbb{N} \setminus \{1\}$ takie, że $p^t N_p = 0$ oraz N_p jest przemiennym nil-H-p-pierścieniem dla każdego $p \in \Pi_0$. Ponadto zachodzi następujący lemat.

Lemat 4.27. *Istnieje $v \in R$ takie, że $o(v + N) = \infty$ w grupie $(R/N)^+$, $v^2 = mv + x_0$ dla pewnego $x_0 \in N$, $vr - mr \in N$ dla każdego $r \in R$ oraz $\langle v \rangle + Rv + N = R$ i $\langle v \rangle + mR + N = R$.*

Uwaga 4.28. Oczywiście $x_0 = \sum_{p \in \Pi_0} x_p$, gdzie $x_p \in N_p$ dla $p \in \Pi_0$ i na mocy Twierdzenia 1.22 można zakładać, że $x_p = 0$ dla każdego $p \in \Pi_2$.

Lemat 4.29. *Dla każdego $p \in \Pi_2$, N_p nie wydziela się w R jako ideałowy składnik prosty.*

Dowód. Załóżmy, że dla pewnego $p \in \Pi_2$ istnieje $A \lhd R$ takie, że $R = A \oplus N_p$. Wtedy $N = \mathcal{N}(A) \oplus N_p$ i $R/N \cong mD$, więc $A/\mathcal{N}(A) \cong mD$. Dalej, pierścień $A/\mathcal{N}(A) \oplus N_p$ jest filialny jako obraz homomorficzny filialnego pierścienia R oraz $A/\mathcal{N}(A) \oplus N_p \cong mD \oplus N_p$. Na podstawie Twierdzenia 4.8, $p \mid m$ i mamy sprzeczność. □

Lemat 4.30. *Dla każdego $p \in \Pi_0$ mamy:*

(i) $(\langle v \rangle + p^t R) \cap N_p = 0$,

(ii) $\langle v \rangle \cap p^t R = p^t \langle v \rangle$,

(iii) $\langle v \rangle + p^t R + N_p = R$.

Dowód. (i). Pokażemy najpierw, że $p^t R \cap N_p = 0$. Weźmy $r \in R$ i $x \in N_p$ takie, że $p^t r = x$. Wtedy $p^t(r + N) = 0 + N$, więc $r \in N$, bo $R/N \cong mD$. Ale $p^t x = 0$, więc $p^{2t} r = 0$, skąd $r \in N_p$. Zatem $p^t r = 0$ i $p^t R \cap N_p = 0$. Weźmy teraz dowolne $k \in \mathbb{Z}$, $r \in R$ takie, że $kv + p^t r \in N_p$. Wówczas w pierścieniu $mD \cong R/N$ mamy $km + p^t r_0 = 0$ dla pewnego $r_0 \in mD$. Zatem w pierścieniu D mamy $p^t m \mid km$, więc zgodnie ze Stwierdzeniem 1.33, $p^t m \mid km$ w $\mathbb{Z}$ i stąd $p^t \mid k$. Wobec tego $kv + p^t r \in p^t R \cap N = 0$. Zatem $(\langle v \rangle + p^t R) \cap N_p = 0$.

(ii). Weźmy dowolne $l \in \mathbb{Z}$ i $a \in R$ takie, że $lv = p^t a$. Wtedy w pierścieniu $mD \cong R/N$ mamy $lm = p^t mb$ dla pewnego $b \in D$. Zatem na podstawie Stwierdzenia 1.33, $p^t m | lm$ w $\mathbb{Z}$, skąd $l = p^t K$ dla pewnego $K \in \mathbb{Z}$ oraz $lv \in p^t \langle v \rangle$. Wobec tego $\langle v \rangle \cap p^t R \subseteq p^t \langle v \rangle$ i inkluzja przeciwna jest oczywista, więc $\langle v \rangle \cap p^t R = p^t \langle v \rangle$.

(iii). Ponieważ $\bigoplus_{q \in \Pi_0 \setminus \{p\}} N_q \subseteq p^t R$ oraz $\langle 1 \rangle + p^t D = D$, więc $m\langle 1 \rangle + p^t mD = mD$. Stąd $\langle v \rangle + p^t R + N = R$, czyli $\langle v \rangle + p^t R + N_p = R$. □

Lemat 4.31. *Dla każdego $p \in \Pi_2$ mamy:*

(i) $\langle v \rangle + p^t R$ *jest podpierścieniem w* R,

(ii) $vr = mr$ *dla każdego* $r \in N_p$,

(iii) $pN_p = 0$ *i* N_p *jest pierścieniem z prawie zerowym mnożeniem.*

Dowód. (i). Ponieważ $x_p = 0$, więc $x_0 \in p^t R$. Ale $v^2 = mv + x_0$ i $p^t R \lhd R$, więc $\langle v \rangle + p^t R$ jest podpierścieniem w R.

(ii). Weźmy dowolne $x \in N_p$. Ponieważ $x_p = 0$, więc $x_0 x = 0$, czyli $(v^2 - mx)x = 0$. Stąd $v^2 x = mvx$ dla $x \in N_p$. Niech $X = \{x \in N_p : vx = 0\}$ i $Y = \{x \in N_p : vx = mx\}$. Wtedy $X, Y \lhd R$. Ponadto $p \nmid m$, więc $X \cap Y = 0$. Dla $x \in N_p$ mamy $mx = (mx - vx) + vx$, $mx - vx \in X$ oraz $vx \in Y$, bo $mvx = v^2 x$. Ale $p \nmid m$, więc $mN_p = N_p$ i wobec tego $N_p = X \oplus Y$. Z Lematu 4.30 wynika, że $R^+ = (\langle v \rangle + p^t R + Y) \oplus X$, a ponieważ $\langle v \rangle + p^t R + Y)X = 0$ i $\langle v \rangle + p^t R$ jest podpierścieniem w R, więc $\langle v \rangle + p^t R + Y \lhd R$. Wobec tego $R = (\langle v \rangle + p^t R + Y) \oplus X$. Dalej, pierścień $[(\langle v \rangle + p^t R + Y)/\mathcal{N}(\langle v \rangle + p^t R + Y)] \oplus X$ jest filialny jako obraz homomorficzny pierścienia

filialnego R oraz $(\langle v\rangle+p^tR+Y)/\mathcal{N}(\langle v\rangle+p^tR+Y)\cong mD$, tym samym pierścień $mD\oplus X$ jest filialny. Ponadto $p\in\Pi(D)$, więc jeśli $X\neq 0$, to na mocy Twierdzenia 4.8, $p\mid m$, co prowadzi do sprzeczności. Zatem $X=0$ i wobec tego $vx=mx$ dla wszystkich $x\in N_p$.

(iii). Z punktu (ii), $N_ppv=mpN_p=pN_p$, bo $p\nmid m$. Ponadto z filialności R wynika, że $Rpv\subseteq Rp^2v^2+\langle p^2v^2\rangle+\langle pv\rangle$. Ale

$$\langle p^2v^2\rangle+\langle pv\rangle=\langle p^2mv+p^2x_0\rangle+\langle pv\rangle=\langle pv\rangle+\langle p^2x_0\rangle\subseteq p\langle v\rangle+p^tR,$$

więc $pN_p\subseteq(\langle v\rangle+p^tR)+p^2v^2R$. Stąd i z Lematu 4.30 wynika, że $pN_p\subseteq(\langle v\rangle+p^tR)+p^2N_p$. Ale $p^2N_p\subseteq pN_p$ i $N_p\cap(\langle v\rangle+p^tR)=0$, więc z modularności kraty podgrup w R^+ mamy $pN_p\subseteq p^2N_p$, skąd $pN_p=p^2N_p$. Ponadto $p^tN_p=0$, więc stąd $pN_p=0$. Dalej, N_p jest nil-H-pierścieniem, więc ze Stwierdzenia 2.12 punkt (ii), wynika, że N_p jest pierścieniem z prawie zerowym mnożeniem. □

Twierdzenie 4.32. *Niech D będzie filialną dziedziną całkowitości charakterystyki zero nie będącą ciałem i niech $m\in S(\Pi(D))$. Niech $N\neq 0$ będzie przemiennym pierścieniem z prawie zerowym mnożeniem ograniczonego wykładnika takim, że $\Pi(N)\subseteq\Pi(D)$ i $p\nmid m$ dla każdego $p\in\Pi(N)$. Niech R będzie pierścieniem przemiennym. Wówczas pierścień R jest filialnym rozszerzeniem pierścienia N przez mD wtedy i tylko wtedy, gdy $R\cong m(D\boxplus N)$ i $D\boxplus N$ jest przemiennym pierścieniem Andrijanowa.*

Dowód. Załóżmy, że $D\boxplus N$ jest przemiennym pierścieniem Andrijanowa i $R\cong m(D\boxplus N)$. Wtedy na podstawie Twierdzenia 4.15, pierścień $D\boxplus N$ jest filialny. Dalej, pierścień $m(D\boxplus N)$ jest filialny jako ideał pierścienia $D\boxplus N$. Ponadto $p\nmid m$ dla każdego $p\in\Pi(N)$, więc $mN=N$ i $m(D\boxplus N)=mD\boxplus N$. Zatem R jest filialnym rozszerzeniem pierścienia N przez mD.

Na odwrót, z przyjętych założeń i z Uwagi 4.28, wynika, że $x_0=0$, czyli $v^2=mv$. Ponadto, na mocy Lematu 4.31, $vx=mx$ dla każdego $x\in N$ i $D\boxplus N$ jest przemiennym pierścieniem Andrijanowa. Na podstawie Lematu 4.30 przez prostą indukcję uzyskujemy, że $R=\langle v\rangle+\left(\prod_{p\in\Pi_0}p^t\right)R+N$. Weźmy dowolne $x\in\left(\langle v\rangle+\left(\prod_{p\in\Pi_0}p^t\right)R\right)\cap N$ i dowolne ustalone $p\in\Pi_0$. Niech $m_p=\prod_{q\in\Pi_0\setminus\{p\}}q$. Skoro $m_px\in N_p\cap(\langle v\rangle+p^tR)$, więc na mocy Lematu 4.30, $m_px=0$ dla każdego $p\in\Pi_0$. Ponadto $NWD(\{m_p : p\in\Pi_0\})=1$, więc $x=0$. Wobec tego $\left(\langle v\rangle+\left(\prod_{p\in\Pi_0}p^t\right)R\right)\cap N=0$ i $R^+=\left(\langle v\rangle+\left(\prod_{p\in\Pi_0}p^t\right)R\right)^+\oplus N^+$. Ponadto $\langle v\rangle+\left(\prod_{p\in\Pi_0}p^t\right)R$ jest podpierścieniem w R izomorficznym z mD. Wobec tego $R\cong mD\boxplus N=m(D\boxplus N)$, bo $p\nmid m$ dla każdego $p\in\Pi_0$. □

Dalej będziemy zakładali, że $\Pi_1\neq\emptyset$ i wobec tego $m>1$.

Lemat 4.33. *Dla każdego $p\in\Pi_1$ pierścień N_p jest z prawie zerowym mnożeniem.*

Dowód. Ponieważ $p^tR\oplus N_p\lhd R$, więc pierścień $p^tR\oplus N_p$ jest filialny i wobec tego pierścień $[p^tR/(\mathcal{N}(p^tR))]\oplus N_p$ jest filialny. Ponadto $R/N\cong mD$, więc $(p^tR+N)/N\cong p^tmD$, skąd $p^tR/(N\cap p^tR)\cong p^tmD$. Stąd pierścień $p^tmD\oplus N_p$ jest filialny. Ale $p\in\Pi(D)$, więc na podstawie Twierdzenia 4.8 pierścień N_p jest z prawie zerowym mnożeniem. □

Lemat 4.34. *Jeżeli $p \in \Pi_1$, to dla każdego $x \in N_p$, $vx - mx \in \langle x^2 \rangle$. W szczególności, jeśli $x \in a(N_p)$, to $vx = mx$.*

Dowód. Weźmy dowolne $x \in N_p$ i niech $a = p^t v + x$. Wtedy $va = p^t v^2 + vx = p^t(mv + x_0) + vx = p^t mv + p^t \sum_{q \in \Pi_1 \setminus \{p\}} x_q + vx$. Ponadto $a^2 = p^{2t}v^2 + 2p^t vx + x^2 = p^{2t}v^2 + x^2$, bo $p^t N_p = 0$. Stąd $a^2 = p^{2t}mv + p^{2t}x_0 + x^2 = p^{2t}mv + p^{2t}\sum_{q \in \Pi_1 \setminus \{p\}} x_q + x^2$. Z filialności pierścienia R, $va \in Ra^2 + \langle a^2 \rangle + \langle a \rangle$. Stąd istnieją $r \in R$, $K, L \in \mathbb{Z}$ takie, że

$$p^t mv + p^t \sum_{q \in \Pi_1 \setminus \{p\}} x_q + vx = r(p^{2t}mv + p^{2t} \sum_{q \in \Pi_1 \setminus \{p\}} x_q + x^2)$$

$$+K(p^{2t}mv + p^{2t} \sum_{q \in \Pi_1 \setminus \{p\}} x_q + x^2) + L(p^t v + x).$$

Stąd w pierścieniu $mD \cong R/N$ mamy $p^t m^2 = mdp^{2t}m^2 + Kp^{2t}m^2 + Lp^t m$, dla pewnego $d \in D$. Po skróceniu przez $p^t m$, $m = m^2 dp^t + Kp^t m + L$. Stąd $p^t \mid L - m$ w pierścieniu D i na mocy Stwierdzenia 1.33, $p^t \mid L - m$ w $\mathbb{Z}$. Zatem $vx - Kx^2 - mx \in p^t R \cap N_p$. Ale na podstawie Lematu 4.30, $p^t R \cap N_p = 0$, więc ostatecznie $vx = mx + Kx^2$, czyli $vx - mx \in \langle x^2 \rangle$.

Dla $x \in a(N_p)$, $x^2 = 0$, więc teza drugiej części Lematu jest oczywista. □

Lemat 4.35. *Dla $p \in \Pi_1$ mamy $x_p^2 = 0$, $vx_p = mx_p$. Ponadto $vx_0 = mx_0$ oraz $x_0^2 = 0$.*

Dowód. Na mocy Lematu 4.34, $vx_p = mx_p + Kx_p^2$ dla pewnego $K \in \mathbb{Z}$. Ale $x_p^3 = 0$ na podstawie Lematu 4.33, więc Lemat 4.34 implikuje, że $vx_p^2 = mx_p^2$. Stąd

$$v^2 x_p = v(mx_p + Kx_p^2) = mvx_p + Kmx_p^2 = m(mx_p + Kx_p^2) + Kmx_p^2 = m^2 x_p,$$

bo $p \mid m$ i $px_p^2 = 0$ na mocy Lematu 4.33. Zatem $v^2 x_p = m^2 x_p$. Ponadto

$$v^2 x_p = (mv + x_0)x_p = mvx_p + x_p^2 = m^2 x_p + Kmx_p^2 + x_p^2 = m^2 x_p + x_p^2,$$

skąd $x_p^2 = 0$ oraz $vx_p = mx_p$. Ale $x_0 = \sum_{p \in \Pi_1} x_p$, więc $vx_0 = mx_0$ oraz $x_0^2 = 0$. □

Lemat 4.36. *W pierścieniu R zachodzą następujące zależności:*

(i) $[v] = \langle v \rangle + \langle x_0 \rangle$ *oraz* $[v]N = vN$,

(ii) $v^2 x = m^2 x = mvx$ *dla dowolnego* $x \in N$,

(iii) $v^k x = m^k x$ *dla dowolnych* $x \in N, k \in \{2, 3, \dots\}$.

Dowód. (i). Na podstawie Lematów 4.35, 4.34, mamy $v(v^2 - mv) = m(v^2 - mv)$, czyli $v^3 = 2mv^2 - m^2 v$ i wobec tego $[v] = \langle v \rangle + \langle v^2 \rangle = \langle v \rangle + \langle mv + x_0 \rangle = \langle v \rangle + \langle x_0 \rangle$, czyli $[v] = \langle v \rangle + \langle x_0 \rangle$. Ponieważ N jest pierścieniem z prawie zerowym mnożeniem i $x_0^2 = 0$, więc $Nx_0 = 0$. Stąd $[v]N = vN$, co kończy dowód (i).

(ii). Weźmy dowolne $p \in \Pi_1$ i dowolne $x \in N_p$. Zauważmy, że $v^2 x = (mv + x_0)x = mvx$, bo $x_0 x = 0$. Ponadto na mocy Lematu 4.34, $vx = mx + Kx^2$ dla pewnego $K \in \mathbb{Z}$. Ponieważ $p \mid m$, więc $mvx = m^2 x$, czyli $v^2 x = m^2 x$. Stąd, na podstawie Lematu 4.31 (ii) mamy $v^2 x = m^2 x = mvx$ dla każdego $x \in N$, co kończy dowód (ii).

Punkt (iii) wynika przez prostą indukcję z (ii). □

Lemat 4.37. *Dla każdego $p \in \Pi_1$, mamy:*

(i) $v^t N_p = 0$ *oraz* $[v] + p^t R \lhd R$,

(ii) $vN_p \subseteq \langle x_p \rangle$, $px_p = 0$ *oraz* $x_p \neq 0$.

Dowód. (i). Ponieważ $p \mid m$, więc na mocy Lematu 4.36 (iii), $v^t N_p = 0$. Na podstawie Lematu 4.30, mamy, że $[v] + p^t R + vN_p \lhd R$. Ponadto

$$[v] + p^t R \lhd [v] + p^t R + v^{t-1} N_p \lhd [v] + p^t R + v^{t-2} N_p \lhd \cdots \lhd [v] + p^t R + vN_p \lhd R.$$

Z filialności R, $[v] + p^t R \lhd R$, co kończy dowód (i).

(ii). Na mocy udowodnionego punktu i Lematu 4.36 (i) mamy

$$vN_p \subseteq [v] + p^t R = \langle v \rangle + \langle x_0 \rangle + p^t R \subseteq \langle v \rangle + \langle x_p \rangle + p^t R,$$

więc $vN_p \subseteq \langle x_p \rangle + (\langle v \rangle + p^t R)$. Weźmy dowolne $x \in N_p$. Wtedy $vx = kx_p + a$ dla pewnych $k \in \mathbb{Z}$, $a \in \langle v \rangle + p^t R$. Stąd $vx - kx_p \in N_p \cap (\langle v \rangle + p^t R) = 0$, na mocy Lematu 4.30 i $vN_p \subseteq \langle x_p \rangle$.

Załóżmy, że $px_p \neq 0$. Wtedy istnieje $u \in \mathbb{N}$ takie, że $p^u x_p \neq 0$ oraz $p^{u+1} x_p = 0$. Weźmy $a = p^u v + p^u x_p$. Wtedy

$$a^2 = p^{2u} v^2 = p^{2u}(mv + x_0) = p^{2u} mv + p^{2u} \sum_{q \in \Pi_1 \setminus \{p\}} x_q.$$

Ponadto $va = v(p^u v + p^u x_p) = p^u v^2 + p^u v x_p$ oraz na mocy Lematów 4.34 i 4.35, $vx_p = mx_p$, więc $va = p^u v^2 + p^u m x_p$. Ale $p \mid m$ i $p^{u+1} x_p = 0$, więc

$$va = p^u v^2 = p^u(mv + x_0) = p^u mv + p^u x_p + p^u \sum_{q \in \Pi_1 \setminus \{p\}} x_q.$$

Z filialności R mamy, że $va \in Ra^2 + \langle a^2 \rangle + \langle a \rangle$. Zatem dla pewnych $r \in R$, $K, L \in \mathbb{Z}$ mamy

$$p^u mv + p^u x_p + p^u \sum_{q \in \Pi_1 \setminus \{p\}} x_q = r[p^{2u} mv + p^{2u} \sum_{q \in \Pi_1 \setminus \{p\}} x_q]$$

$$+K(p^{2u} mv + p^{2u} \sum_{q \in \Pi_1 \setminus \{p\}} x_q) + L(p^u v + p^u x_p).$$

Przechodząc do pierścienia $mD \cong R/N$ mamy

$$p^u m^2 = \overline{r} p^{2u} m^2 + K p^{2u} m^2 + L p^u m,$$

dla pewnego $\overline{r} \in mD$, więc w pierścieniu D, mamy $p^u m^2 \mid L p^u m$, skąd $m \mid L$ i na mocy Stwierdzenia 1.33, $m \mid L$ w pierścieniu $\mathbb{Z}$. Ale $p \mid m$, więc $p \mid L$ i wobec tego $L p^u x_p = 0$. Zatem mamy $p^u x_p \in p^{u+1} Rv + \langle v \rangle + \langle x_0 - x_p \rangle$ i na mocy Lematu 4.30 mamy

$$p^u x_p \in \langle v \rangle + p^{u+1}(\langle v \rangle + p^t R + N_p)v + \langle x_0 - x_p \rangle.$$

Ale z Lematu 4.37 (ii), $vN_p \subseteq \langle x_p \rangle$. Ponadto $p^{u+1}x_p = 0$, więc stąd $p^u x_p \in \langle v \rangle + \langle x_0 - x_p \rangle + p^t R$. Ponadto $\langle x_0 - x_p \rangle \subseteq p^t R$, więc $p^u x_p \in (\langle v \rangle + p^t R) \cap N_p$. Zatem na mocy Lematu 4.30, $p^u x_p = 0$, sprzeczność.

Załóżmy, że $x_p = 0$. Z (ii) $vN_p \subseteq \langle x_p \rangle$, więc $vN_p = 0$. Ponadto, na podstawie Lematu 4.30, $\langle v \rangle + p^t R + N_p = R$ oraz $p^t N_p = 0$, więc $\langle v \rangle + p^t R \lhd R$, bo $v^2 = mv + \sum_{q \in \Pi \setminus \{p\}} x_q \in \langle v \rangle + p^t R$. Ale na mocy Lematu 4.30, $(\langle v \rangle + p^t R) \cap N_p = 0$, więc N_p wydziela się w R jako ideałowy składnik prosty, sprzeczność. □

Lemat 4.38. *Dla dowolnego $p \in \Pi_1$ mamy:*

(i) $va(N_p) = ma(N_p) = 0$,

(ii) $pmN_p = 0$, *w szczególności* $m^2 \left(\sum_{p \in \Pi_1} N_p \right) = 0$.

Dowód. (i). Na mocy Lematu 4.34, $va(N_p) = ma(N_p)$. Ponadto z 4.37 (ii), $va(N_p) \subseteq \langle x_p \rangle$ i $px_p = 0$. Załóżmy, że $ma(N_p) \neq 0$. Wtedy $va(N_p) = \langle x_p \rangle$. Zatem istnieje $y_0 \in a(N_p)$ takie, że $vy_0 = my_0 = x_p$. Niech $\hat{v} = v - y_0$. Wtedy $\hat{v} + N = v + N$, $\hat{v}r - mr \in N$ dla każdego $r \in R$, $\langle \hat{v} \rangle + R\hat{v} + N = R$, $\langle \hat{v} \rangle + mR + N = R$ oraz $\hat{v}^2 - m\hat{v} = v^2 - 2vy_0 + y_0^2 - mv + my_0 = (v^2 - mv) - 2x_p + 0 + x_p = x_0 - x_p = \sum_{q \in \Pi_1 \setminus \{p\}} x_q$, co przeczy Lematowi 4.37, w którym v zastąpimy przez $\hat{v}$. Zatem $va(N_p) = ma(N_p) = 0$.

(ii). Na podstawie Lematu 4.33, N_p jest pierścieniem z prawie zerowym mnożeniem, więc $pN_p \subseteq a(N_p)$. Wobec tego z (i), $pmN_p = 0$ i stąd w szczególności $m^2 \left(\sum_{p \in \Pi_1} N_p \right) = 0$. □

Lemat 4.39. *Dla każdego $p \in \Pi_1$ i dowolnego $y \in N_p$, $my, y^2, vy \in \langle x_p \rangle$. Ponadto:*

(i) jeżeli $vy \neq 0$, to $y^2 \neq 0$,

(ii) jeżeli $x_p \notin [y]$, to $my = 0$ oraz $y \in a(R)$,

(iii) jeżeli $y^2 \notin \langle y \rangle$ i $x_p \in [y]$, to $my = 0$.

Dowód. (i) Niech $y \in N_p$ i załóżmy najpierw, że $vy = x_p$. Na mocy Lematów 4.37, 4.38, $y \notin a(N_p)$, a więc $y^2 \neq 0$, w szczególności $o(y^2) = p$. Zauważamy, że

$$(v-y)^2 - m(v-y) = (v^2 - mv) - 2x_p + y^2 + my = x_0 - 2x_p + y^2 + my =$$

$$\sum_{q \in \Pi \setminus \{p\}} x_q + x_p - 2x_p + y^2 + my = \sum_{q \in \Pi \setminus \{p\}} x_q + (-x_p + y^2 + my).$$

Z Lematu 4.37 (ii) mamy, że $(v-y)N_p \subseteq \langle -x_p + y^2 + my \rangle$. Ponadto $(v-y)y = x_p - y^2$, więc $x_p - y^2 = L(-x_p + y^2 + my)$ dla pewnego $L \in \mathbb{Z}$. Ponadto na podstawie Lematu 4.34, istnieje $K \in \mathbb{Z}$ takie, że $vy = my + Ky^2$, więc $x_p = my + Ky^2$ i $my = x_p - Ky^2$. Wobec tego $x_p - y^2 = L(-x_p + y^2 + x_p - Ky^2)$, czyli $x_p - y^2 = L(1-K)y^2$, więc $x_p = [1 + L(1-K)]y^2$. Ale z Lematu 4.37, $o(x_p) = p$ oraz jak wiemy $o(y^2) = p$, więc stąd $y^2 \in \langle x_p \rangle$. W końcu $my = x_p - Ky^2 \in \langle x_p \rangle$.

Weźmy teraz dowolne $y \in N_p$ takie, że $vy \neq 0$. Na mocy Lematu 4.37 (ii), istnieje $H \in \mathbb{Z}$, takie, że $p \nmid H$ oraz $vy = Hx_p$. Istnieje także $T \in \mathbb{Z}$ takie, że $HT \equiv 1$

(mod $o(y)$) i stąd $v(Ty) = x_p$. Niech $y_0 = Ty$. Wtedy $vy_0 = x_p$ i $y = Hy_0$. Z pierwszej części dowodu, $y_0^2 \neq 0$, $y_0^2, my_0 \in \langle x_p \rangle$, więc też $y^2 \neq 0$ oraz $vy, y^2, my \in \langle x_p \rangle$.

(ii). Ponieważ $o(x_p) = p$, więc $[y] \cap \langle x_p \rangle = 0$. Ponadto $[y] \lhd R$, więc $vy \in [y]$. Ale na podstawie Lematu 4.37 (ii), $vy \in \langle x_p \rangle$, więc $vy \in [y] \cap \langle x_p \rangle = 0$, stąd $vy = 0$. Dalej, $(v-y)^2 - m(v-y) = (v^2 - my) + y^2 + my = \sum_{q \in \Pi \setminus \{p\}} x_q + x_p + y^2 + my$, więc na mocy Lematu 4.37 (ii), mamy, że $(v-y)N_p \subseteq \langle x_p + y^2 + my \rangle$. Ale $(v-y)y = -y^2$, więc istnieje $U \in \mathbb{Z}$ takie, że $-y^2 = U(x_p + y^2 + my)$. Ponadto na podstawie Lematu 4.34, istnieje $K \in \mathbb{Z}$ takie, że $vy = my + Ky^2$ i $vy = 0$, więc $my = -Ky^2$ oraz $-y^2 = U(x_p + (1-K)y^2)$, skąd $-Ux_p = [1 + U(1-K)]y^2$. Jeśli $U \not\equiv 0 \pmod{p}$, to $x_p \in \langle y^2 \rangle$ wbrew założeniu. Zatem $U \equiv 0 \pmod{p}$ i $y^2 = 0$. Stąd $my = -Ky^2 = 0$. Ponadto na mocy Lematu 4.30, $R = \langle v \rangle + p^t R + N$, więc $y \in a(R)$.

(iii). Załóżmy na początek, że $vy \neq 0$. Z dowodu punktu (a) wynika, że $my, y^2 \in \langle x_p \rangle$. Załóżmy, że $my \neq 0$. Na podstawie Lematu 4.38 (ii), $o(my) = p$. Ale $my \in \langle x_p \rangle$ i $o(x_p) = p$, więc $x_p = Vmy$ dla pewnego $V \in \mathbb{Z}$. Ponadto $y^2 = Ux_p$ dla pewnego $U \in \mathbb{Z}$, więc $y^2 = UVmy \in \langle y \rangle$, sprzeczność. Zatem $my = 0$.

Niech dalej $vy = 0$ (i oczywiście $y^2 \notin \langle y \rangle$ i $x_p \in [y]$). Na mocy Lematu 4.34, $vy = my + Ky^2$ dla pewnego $K \in \mathbb{Z}$, skąd $my + Ky^2 = 0$. Jeśli $p \nmid K$, to $y^2 = Lmy \in \langle y \rangle$ dla pewnego $L \in \mathbb{Z}$, sprzeczność. Zatem $p \mid K$, skąd $my = 0$, bo $py^2 = 0$. Dalej $(v-y)^2 - m(v-y) = (v^2 - mv) + y^2 = x_0 + y^2 = \sum_{q \in \Pi_1 \setminus \{p\}} x_q + (x_p + y^2)$, więc $(v-y)N_p \subseteq \langle x_p + y^2 \rangle$ na mocy Lematu 4.37. Ale $(v-y)y = -y^2$, więc istnieje $U \in \mathbb{Z}$ takie, że $-y^2 = U(x_p + y^2)$, skąd $Ux_p = -(1+U)y^2$. Jeśli $U \equiv -1 \pmod{p}$, to $x_p = 0$, sprzeczność. Zatem $p \nmid 1 + U$, skąd $y^2 \in \langle x_p \rangle$.

Weźmy dowolne $y \in N_p$. Pokażemy, że $my, y^2, vy \in \langle x_p \rangle$. Jeżeli $y^2 = 0$, to $y \in a(N_p)$ oraz na mocy Lematów 4.34, 4.38 (i), $vy = my = 0$, czyli $my, y^2, vy \in \langle x_p \rangle$. Niech dalej $y^2 \neq 0$. Jeżeli $y^2 \notin \langle y \rangle$, to $y^2, my, vy \in \langle x_p \rangle$ na mocy części (iii) dowodu. Niech więc dalej $0 \neq y^2 \in \langle y \rangle$. Jeśli $vy \neq 0$, to z części (i) dowodu, $y^2, my, vy \in \langle x_p \rangle$. Niech zatem dalej $0 \neq y^2 \in \langle y \rangle$ oraz $vy = 0$. Jeżeli teraz dodatkowo $x_p \notin [y]$, to z części (b) dowodu, $y^2, my, vy \in \langle x_p \rangle$. Pozostaje zatem do rozpatrzenia przypadek $0 \neq y^2 \in \langle y \rangle$, $vy = 0$ oraz $x_p \in [y]$. Na podstawie Lematu 4.34, $vy = my + Ky^2$ dla pewnego $K \in \mathbb{Z}$ i na mocy Lematu 4.37 (ii), $vy \in \langle x_p \rangle$, więc wystarczy wykazać, że $y^2 \in \langle x_p \rangle$. Ale $y^2 \neq 0$ i $py^2 = 0$, więc $o(y^2) = p$. Grupa $\langle y \rangle$ jest cykliczną p-grupą, więc ma dokładnie jedną podgrupę rzędu p, którą jest $\langle y^2 \rangle$. Ale $0 \neq [y] \cap \langle x_p \rangle = \langle y \rangle \cap \langle x_p \rangle$, więc ponieważ $o(x_p) = p$, to $\langle x_p \rangle \subseteq \langle y \rangle$ oraz $|\langle x_p \rangle| = p$. Stąd $\langle x_p \rangle = \langle y^2 \rangle$ i $y^2 \in \langle x_p \rangle$. □

Lemat 4.40. *Jeżeli $p \in \Pi_1$ i $N_p^2 \neq 0$, to istnieje $y_p \in N_p$ takie, że $N_p = \langle y_p \rangle + a(N_p)$, $vy = U_{2p}x_p$, $y_p^2 = U_{0p}x_p$, $my_p = U_{1p}x_p$ dla pewnych $U_{0p}, U_{1p}, U_{2p} \in \mathbb{Z}$ takich, że $p \nmid U_{0p}$ oraz kongruencja*

$$1 + (2U_{2p} - U_{1p})x + U_{0p}x^2 \equiv 0 \pmod{p} \tag{4.34}$$

nie ma rozwiązania.

Dowód. Z założenia wynika, że istnieje $y_p \in N_p$ takie, że $y_p^2 \neq 0$. Na podstawie Lematu 4.39, istnieją $U_{0p}, U_{1p}, U_{2p} \in \mathbb{Z}$ takie, że $y_p^2 = U_{0p}x_p$, $my_p = U_{1p}x_p$, $vy_p = U_{2p}x_p$, przy czym $p \nmid U_{0p}$. Ponadto na mocy Lematu 4.34, istnieje $V \in \mathbb{Z}$ takie, że $vy_p = my_p + Vy_p^2$.

Dla $X \in \mathbb{Z}$ mamy, że

$$\begin{aligned}(v + Xy_p)^2 - m(v + Xy_p) &= (v^2 - mv) + 2Xvy_p + X^2y_p^2 - X(my_p) \\ &= x_0 + 2XU_{2p}x_p + X^2U_{0p}x_p - XU_{1p}x_p \\ &= \textstyle\sum_{q\in\Pi_1\setminus\{p\}} x_q + (1 + (2U_{2p} - U_{1p})X + X^2U_{0p})x_p.\end{aligned}$$

Na mocy Lematu 4.37 (ii), $(1 + 2XU_{2p} - XU_{1p} + X^2U_{0p})x_p \neq 0$. Zatem kongruencja (4.34) nie ma rozwiązania.

Niech $p = 2$. Wobec Twierdzenia 2.16 oraz przemienności pierścienia R otrzymujemy, że $N_2 = \langle y_2\rangle + a(N_2)$.

Niech więc dalej $p > 2$. Wykażemy, że $N_p \subseteq \langle y_p\rangle + a(N_p)$, co zakończy dowód. Załóżmy, że tak nie jest. Wtedy istnieje $y_1 \in N_p$ taki, że $y_1 \notin \langle y_p\rangle + a(N_p)$. W szególności $y_1 \notin a(N_p)$, a więc $y_1^2 \neq 0$. Ponadto $py_1^2 = 0$, $py_p^2 = 0$, więc $py_1, py_p \in a(N_p)$. Zatem warstwy $y_p + a(N_p)$, $y_1 + a(N_p)$ są liniowo niezależne nad $\mathbb{Z}_p$. Na podstawie Twierdzenia 2.16 i przemienności pierścienia R istnieją $A, F \in \mathbb{Z}$ takie, że $y_1^2 = Ay_p^2$, $y_py_1 = Fy_p^2$ oraz dla dowolnego $K \in \mathbb{Z}$, $p \nmid K^2 + 2FK + A$. Na mocy Twierdzenia 1.20, dla dowolnych $V_1, V_2 \in \mathbb{Z}$ mamy

$$\{[Y^2 + 2FXY + AX^2 + V_1X + V_2Y]_p \ : \ X, Y \in \mathbb{Z}_p\} = \mathbb{Z}_p. \tag{4.35}$$

Ale z pierwszej części dowodu i Lematu 4.39 mamy $my_1 = H_1x_p$, $y_1^2 = U_{0p}Ax_p$, $vy_1 = H_2x_p$ dla pewnych $H_1, H_2 \in \mathbb{Z}$, więc dla dowolnych $X, Y \in \mathbb{Z}$ mamy, że

$$(v + Xy_p + Yy_1)^2 - m(v + Xy_p + Yy_1)$$

$$= (v^2 - mv) + X^2y_p^2 + Y^2y_1^2 + 2Xvy_p + 2Yvy_1 + 2XYy_py_1 - X(my_p) - Y(my_1)$$

$$= x_0 + X^2U_{0p}x_p + Y^2U_{0p}Ax_p + 2XU_{2p}x_p + 2YH_2x_p + 2XYFU_{0p}x_p - XU_{1p}x_p - YH_2x_p$$

$$= \sum_{q\in\Pi_1\setminus\{p\}} x_q + (1 + X^2U_{0p} + Y^2U_{0p}A + 2XU_{2p} + 2YH_2 + 2XYFU_{0p} - XU_{1p} - YH_2)x_p.$$

Na podstawie Lematu 4.37 (ii), $(1+X^2U_{0p}+Y^2U_{0p}A+2XU_{2p}+2YH_2+2XYFU_{0p}-XU_{1p} - YH_2)x_p \neq 0$ dla dowolnych $X, Y \in \mathbb{Z}$, co przeczy (4.35). Wobec tego $N_p = \langle y_p\rangle + a(N_p)$.

□

Twierdzenie 4.41. *Niech D będzie filialną dziedziną całkowitości charakterystyki zero nie będącą ciałem i niech $m \in S(\Pi(D))$. Niech $N \neq 0$ będzie przemiennym pierścieniem z prawie zerowym mnożeniem ograniczonego wykładnika takim, że $\Pi(N) \subseteq \Pi(D)$. Niech $\Pi_1 = \{p \in \Pi(N) \ : \ p \mid m\}$ i $\Pi_2 = \{p \in \Pi(N) \ : \ p \nmid m\}$. Niech pierścień przemienny R będzie takim rozszerzeniem pierścienia N przez pierścień mD, że N_p nie wydziela się w R jako ideałowy składnik prosty dla wszystkich $p \in \Pi_1$. Wówczas:*

(i) Jeżeli $\Pi_2 = \emptyset$, to pierścień R jest filialny wtedy i tylko wtedy, gdy R jest pierścieniem Krusego,

(ii) Jeżeli $\Pi_1 \neq \emptyset$ i $\Pi_2 \neq \emptyset$, to pierścień R jest filialny wtedy i tylko wtedy, gdy R jest uogólnionym pierścieniem Krusego.

Dowód. Załóżmy, że R jest pierścieniem Krusego lub uogólnionym pierścieniem Krusego. Wówczas na podstawie Twierdzenia 4.19 i Przykładu 4.24 pierścień R jest filialny.

Na odwrót, załóżmy, że $\Pi_2 = \emptyset$. Wtedy $\Pi_1 = \Pi_0$. Wykorzystując Lematu 4.30 i prostą indukcję, otrzymujemy $R = \langle v \rangle + \left(\prod_{p\in\Pi_0} p^t\right) R + N$. Stosując to samo rozumowanie co w dowodzie Stwierdzenia 4.32 uzyskujemy, że $R^+ = \left(\langle v\rangle + \left(\prod_{p\in\Pi_0} p^t\right) R\right)^+ \oplus N^+$. Stąd $\left(\langle v\rangle + \left(\prod_{p\in\Pi_0} p^t\right) R\right)^+ \cong (mD)^+$. Na podstawie rozważań tego rozdziału i Przykładu 4.18 mamy, że R jest pierścieniem Krusego.

Niech teraz $\Pi_1 \neq \emptyset$ i $\Pi_2 \neq \emptyset$. Stosując to samo rozumowanie co w dowodzie Stwierdzenia 4.32 uzyskujemy, że $R^+ = \left(\langle v\rangle + \left(\prod_{p\in\Pi_2} p^t\right) R\right)^+ \oplus \bigoplus_{p\in\Pi_2} N_p^+$. Ponadto $x_0 \in \left(\prod_{p\in\Pi_2} p^t\right) R$, więc $\langle v\rangle + \left(\prod_{p\in\Pi_2} p^t\right) R$ jest podpierścieniem w R, który na mocy pierwszej części dowodu jest pierścieniem Krusego. Wobec tego z udowodnionych lematów i na mocy Przykładu 4.24, R jest uogólnionym pierścieniem Krusego. □

Twierdzenie 4.42. *Niech D będzie filialną dziedziną całkowitości charakterystyki zero nie będącą ciałem i niech $m \in S(\Pi(D))$. Niech A będzie przemiennym pierścieniem filialnym takim, że $\mathcal{N}(A) = N$ i $A/N \cong mD$, przy czym $N \neq 0$ jest pierścieniem z prawie zerowym mnożeniem ograniczonego wykładnika takim, że $\Pi_0 = \Pi(N) \subseteq \Pi(D)$. Niech $\Pi_1 = \{p \in \Pi(N) \ : \ p \mid m\}$ i $\Pi_2 = \{p \in \Pi(N) \ : \ p \nmid m\}$. Niech zbiór Π_3 tych wszystkich $p \in \Pi(N)$, dla których N_p wydziela się w A jako ideałowy składnik prosty będzie niepusty. Wówczas istnieje $S \lhd A$ taki, że $(\bigoplus_{p\in\Pi_3} N_p) \oplus S = A$ oraz pierścień $\bigoplus_{p\in\Pi_3} N_p$ jest z prawie zerowym mnożeniem i $m(\bigoplus_{p\in\Pi_3} N_p) = 0$. Ponadto wówczas $\mathcal{N}(S) = \bigoplus_{p\in\Pi_0\setminus\Pi_3} N_p$, $S/\mathcal{N}(S) \cong mD$ oraz:*

(i) jeżeli $\Pi_3 = \Pi_0$, to $S \cong mD$,

(ii) jeżeli $\Pi_3 = \Pi_1$ i $\Pi_2 \neq \emptyset$, to $S \cong (mD) \boxplus (\bigoplus_{p\in\Pi_2} N_p)$ i $D \boxplus (\bigoplus_{p\in\Pi_2} N_p)$ jest przemiennym pierścieniem Andrijanowa,

(iii) jeżeli $\Pi_3 \neq \Pi_1$ i $\Pi_2 = \emptyset$, to S jest pierścieniem Krusego,

(iv) jeżeli $\Pi_3 \neq \Pi_1$ i $\Pi_2 \neq \emptyset$, to S jest uogólnionym pierścieniem Krusego.

Dowód. Najpierw przez indukcję wykażemy, że jeśli Π jest niepustym podzbiorem zbioru Π_3, to $(\bigoplus_{p\in\Pi} N_p) \oplus S_\Pi = A$ dla pewnego $S_\Pi \lhd A$. Jest to oczywiste dla $|\Pi| = 1$. Niech $|\Pi| > 1$ i załóżmy, że teza zachodzi dla wszystkich niepustych podzbiorów zbioru Π_3 mocy mniejszej niż $|\Pi|$. Wybierzmy dowolne $p \in \Pi$. Wtedy istnieją $I, J \lhd A$ takie, że $N_p \oplus I = A$ oraz $(\bigoplus_{q\in\Pi\setminus\{p\}} N_q) \oplus J = A$. Z pierwszej równości wynika, że $I_q = A_q = N_q$ dla każdego $q \in \Pi \setminus \{p\}$. Zatem $\bigoplus_{q\in\Pi\setminus\{p\}} N_q \subseteq I$ i z prawa modularności dla podgrup grupy A^+ otrzymujemy $(\bigoplus_{q\in\Pi\setminus\{p\}} N_q) \oplus (I \cap J) = I$. Wobec tego $(\bigoplus_{q\in\Pi} N_q) \oplus (I \cap J) = A$ i wystarczy przyjąć $S_\Pi = I \cap J$. W ten sposób wykazaliśmy, że $(\bigoplus_{p\in\Pi_3} N_p) \oplus S = A$ dla pewnego $S \lhd A$. Ale $A/\mathbb{T}(A) \cong mD$, więc stąd $S/\mathbb{T}(S) \cong mD$. Zatem pierścień $mD \oplus (\bigoplus_{q\in\Pi} N_q)$ jest obrazem homomorficznym filialnego pierścienia A. Wobec tego pierścień $mD \oplus (\bigoplus_{q\in\Pi} N_q)$ jest filialny i na podstawie Twierdzenia 4.9, pierścień $\bigoplus_{p\in\Pi_3} N_p$ jest z prawie zerowym mnożeniem i $m(\bigoplus_{p\in\Pi_3} N_p) = 0$.

Zauważmy, że $\mathbb{T}(A) = \mathcal{N}(A) = \bigoplus_{p\in\Pi_0\setminus\Pi_3} N_p$. Ponadto, gdyby dla pewnego $p \in \Pi_0 \setminus \Pi_3$ istniał $J \lhd S$ taki, że $S = N_p \oplus J$, to $J \lhd A$ oraz $N_p \oplus (\bigoplus_{q\in\Pi_3} N_q) \oplus J = S$, co przeczy definicji Π_3. Wobec tego $\Pi(S) = \Pi_0 \setminus \Pi_3$ i dla każdego $p \in \Pi(S)$, $N_p = \mathcal{N}(S)_p$ nie wydziela się jako ideałowy składnik prosty w pierścieniu S.

Jeśli $\Pi_3 = \Pi_0$, to $T(S) = 0$, więc $S \cong mD$. Niech teraz $\Pi_3 = \Pi_1$ i $\Pi_2 \neq \emptyset$. Wtedy $\Pi(S) = \Pi_2$, więc na mocy Twierdzenia 4.32, $S \cong (mD)\boxplus(\bigoplus_{p\in\Pi_2} N_p)$ i $D\boxplus(\bigoplus_{p\in\Pi_2} N_p)$ jest przemiennym pierścieniem Andrijanowa.

Załóżmy, że $\Pi_3 \neq \Pi_1$ i $\Pi_2 = \emptyset$. Wtedy $\Pi(S) = \Pi_1 \setminus \Pi_3 \neq \emptyset$, więc na mocy Twierdzenia 4.41, S jest pierścieniem Krusego. W końcu, niech $\Pi_3 \neq \Pi_1$ i $\Pi_2 \neq \emptyset$. Wtedy $\Pi(S) = (\Pi_1 \setminus \Pi_3) \cup \Pi_2$, więc na podstawie Twierdzenia 4.41, S jest uogólnionym pierścieniem Krusego. □

Rozdział 5

Przemienne pierścienie filialne o nietorsyjnym nil-radykale

W tym rozdziale omówimy i przedstawimy pewne fakty związane z pierścieniami filialnymi, które posiadają niezerowy, nilpotentny element nieskończonego rzędu.

5.1 Klasyfikacja przemiennych pierścieni R takich, że pierścień $\mathbb{Z}^0 \oplus R$ jest filialny

Twierdzenie 5.1. *Dla przemiennego pierścienia R równoważne są warunki:*

(i) pierścień $\mathbb{Z}^0 \oplus R$ jest filialny,

(ii) $Ra = \langle a^2 \rangle + Ra^2$ dla każdego $a \in R$.

Dowód. $(i) \Rightarrow (ii)$. Dla $a \in R$ oraz $\alpha = (1, a) \in \mathbb{Z}^0 \oplus R$ mamy, że $\alpha^2 = (0, a^2)$ oraz $(\mathbb{Z}^0 \oplus R)\alpha^2 = \{0\} \oplus Ra^2$, skąd $\langle \alpha \rangle + \langle \alpha^2 \rangle + (\mathbb{Z}^0 \oplus R)\alpha^2 = \langle (1, a) \rangle + (\{0\} \oplus (\langle a^2 \rangle + Ra^2))$. Stąd i z filialności pierścienia $\mathbb{Z}^0 \oplus R$ dla dowolnego $b \in R$ istnieją $k, l \in \mathbb{Z}$ oraz $x \in R$ takie, że $(0, b) \cdot \alpha = k \cdot (1, a) + (0, la^2 + xa^2)$. Zatem $(0, ba) = (k, ka + la^2 + xa^2)$, skąd $k = 0$ i $ba = la^2 + xa^2$. Wobec tego $Ra \subseteq \langle a^2 \rangle + Ra^2$ i ostatecznie $Ra = \langle a^2 \rangle + Ra^2$.

$(ii) \Rightarrow (i)$. Weźmy dowolne $\alpha \in \mathbb{Z}^0 \oplus R$. Wtedy istnieją $k \in \mathbb{Z}$ i $a \in R$ takie, że $\alpha = (k, a)$. Stąd $\alpha^2 = (0, a^2)$ oraz $\langle \alpha \rangle + \langle \alpha^2 \rangle + (\mathbb{Z}^0 \oplus R)\alpha^2 = \langle \alpha \rangle + (\{0\} \oplus (\langle a^2 \rangle + Ra^2)) = \langle \alpha \rangle + (\{0\} \oplus Ra) = \langle \alpha \rangle + (\mathbb{Z}^0 \oplus R)\alpha$, więc pierścień $\mathbb{Z}^0 \oplus R$ jest filialny. □ □

Wniosek 5.2. *Jeżeli $R \neq 0$ jest zredukowanym przemiennym pierścieniem takim, że pierścień $\mathbb{Z}^0 \oplus R$ jest filialny, to R jest pierścieniem silnie regularnym (w szczególności R posiada niezerowego idempotenta).*

Dowód. Weźmy $0 \neq a \in R$. Na mocy Twierdzenia 5.1, $Ra^3 = \langle a^6 \rangle + Ra^6$. Zatem istnieje $b \in R$ takie, że $a^4 = ba^5$. Stąd $a^3(a - ba^2) = 0$, więc $(a - ba^2)^4 = 0$. Ale R jest zredukowany, więc $a = ba^2$ i w konsekwencji $R \in \mathbb{S}$. □

Opiszemy teraz dokładniej przemienne pierścienie R spełniające warunek

$$Ra = \langle a^2 \rangle + Ra^2 \text{ dla każdego } a \in R. \tag{5.1}$$

Lemat 5.3. *Jeżeli przemienny nil-pierścień R spełnia warunek (5.1), to R jest pierścieniem z prawie zerowym mnożeniem.*

Dowód. Załóżmy, że istnieje $a \in R$ takie, że $a^3 \neq 0$. Wtedy $a^{s+3} = 0$ oraz $a^{s+2} \neq 0$ dla pewnego $s \in \mathbb{N}$. Ale $Ra^{s+1} \subseteq \langle a^{2s+2} \rangle + Ra^{2s+2} = 0$, bo $2s+2 \geq s+3$, więc $Ra^{s+1} = 0$, skąd $0 = aa^{s+1} = a^{s+2}$, sprzeczność. Wobec tego $a^3 = 0$ dla każdego $a \in R$.

Weźmy dowolne $a \in R$. Wtedy $a^3 = 0$ i z warunku (5.1), $Ra^2 = \langle a^4 \rangle + Ra^4 = 0$. Stąd $Ra = \langle a^2 \rangle$, a więc R jest H-pierścieniem. Na mocy Twierdzenia 2.7, $o(a^2) < \infty$ dla każdego $a \in R$.

Załóżmy, że istnieje $a \in R$ takie, że $o(a^2)$ dzieli się przez kwadrat liczby pierwszej p. Niech $o(a^2) = p^2 n$ dla pewnego $n \in \mathbb{N}$. Wtedy $pna^2 \neq 0$ oraz $(pna)^2 = 0$ i $R(pna) = \langle (pna)^2 \rangle$, więc $Rpna = 0$, skąd $apna = 0$, czyli $pna^2 = 0$, sprzeczność.

□

Uwaga 5.4. Z Lematu 5.3 wynika, że przemienny nil-pierścień R jest pierścieniem z prawie zerowym mnożeniem wtedy i tylko wtedy, gdy $Ra = \langle a^2 \rangle$ dla każdego $a \in R$. Ponadto, jeżeli przemienny pierścień R z jedynką spełnia warunek (5.1), to R jest silnie regularny. Rzeczywiście, jeśli $1 \in R$, to $\langle a^2 \rangle \subseteq Ra^2$ oraz $Ra = Ra^2$, skąd $a \in Ra^2$ dla każdego $a \in R$.

Uwaga 5.5. Każdy pierścień silnie regularny i każdy pierścień z prawie zerowym mnożeniem spełnia warunek (5.1). Niech R będzie pierścieniem przemiennym takim, że $R = P \oplus N$, gdzie $P \in \mathbb{S}$ oraz N jest pierścieniem z prawie zerowym mnożeniem. Weźmy dowolne $a = (s, x) \in R$, $b = (r, y) \in R$. Istnieje wówczas $s_1 \in S$ takie, że $s = s^2 s_1$ i istnieje $k \in \mathbb{Z}$ takie, że $yx = kx^2$. Zatem $ba = (s^2 s_1 r, kx^2)$, $a^2 = (s^2, x^2)$, więc $ba - ka^2 = (s^2 s_1 r - ks^2, 0) = (s^2 s_1 r - ks^3 s_1, 0) = (s_1 r - kss_1, 0)a^2$. Stąd $ba \in \langle a^2 \rangle + Ra^2$ i pierścień R spełnia warunek (5.1). W szczególności pierścień R jest filialny.

Lemat 5.6. *Jeżeli pierścień przemienny R spełnia warunek (5.1), to każdy ideał I pierścienia R też spełnia (5.1).*

Dowód. Weźmy dowolne $a \in I$. Wtedy $Ra^2 = \langle a^4 \rangle + Ra^4 \subseteq Ia^3$ oraz $Ia \subseteq \langle a^2 \rangle + Ra^2$, więc $Ia \subseteq \langle a^2 \rangle + Ia^3 \subseteq \langle a^2 \rangle + Ia^2 \subseteq Ia$. Zatem $Ia = \langle a^2 \rangle + Ia^2$, czyli I spełnia warunek (5.1). □

Twierdzenie 5.7. *Dla przemiennego pierścienia R równoważne są warunki:*

(i) pierścień $\mathbb{Z}^0 \oplus R$ jest filialny,

(ii) pierścień R spełnia warunek (5.1),

(iii) $R = \mathbb{S}(R) \oplus \mathcal{N}(R)$ i $\mathcal{N}(R)$ jest pierścieniem z prawie zerowym mnożeniem.

Dowód. $(i) \Rightarrow (ii)$. Wynika bezpośrednio z Twierdzenia 5.1

$(ii) \Rightarrow (iii)$. Ponieważ $\mathcal{N}(R) \lhd R$, więc na mocy Lematu 5.6, pierścień $\mathcal{N}(R)$ spełnia warunek (5.1). Na podstawie Lematu 5.3, $\mathcal{N}(R)$ jest pierścieniem z prawie zerowym mnożeniem. Oczywiście $\mathbb{S}(R) \cap \mathcal{N}(R) = 0$. Ponadto pierścień $R/\mathcal{N}(R)$ też spełnia warunek (5.1) i jest zredukowany, a więc na mocy Twierdzenia 5.1 i Wniosku

5.2 pierścień $R/\mathcal{N}(R)$ jest silnie regularny. Weźmy dowolne $a \in R$. Wtedy istnieje $b \in R$ takie, że $a - a^2b \in \mathcal{N}(R)$ i $ab + \mathcal{N}(R)$ jest idempotentem w pierścieniu $R/\mathcal{N}(R)$. Zatem zgodnie z Twierdzeniem 1.22, istnieje idempotent $e = ab + x$, gdzie $x \in \mathcal{N}(R)$. Wobec tego $a - ae \in \mathcal{N}(R)$, a więc $a \in Re + \mathcal{N}(R)$. Ale $Re \lhd R$, więc z Lematu 5.6, Re spełnia warunek (5.1) i e jest jedynką w Re. Z Uwagi 5.4 otrzymujemy, że $Re \in \mathbb{S}$, czyli $Re \subseteq \mathbb{S}(R)$. Stąd $a \in \mathbb{S}(R) + \mathcal{N}(R)$, więc ostatecznie $R = \mathbb{S}(R) \oplus \mathcal{N}(R)$.

$(iii) \Rightarrow (i)$. Wynika z Uwagi 5.5 i Twierdzenia 5.1. □

5.2 Charakteryzacje przemiennych pierścieni filialnych o nietorsyjnym nil-radykale

Stwierdzenie 5.8. *Jeżeli N jest przemiennym, nietorsyjnym, filialnym nil-pierścieniem, to:*

(i) N jest pierścieniem z prawie zerowym mnożeniem,

(ii) istnieje $y \in N$ taki, że $o(y) = \infty$ i $y^2 = 0$.

Dowód. (i). Na mocy założeń pierścień N jest β-radykalny. Zatem na podstawie Twierdzenia 1.35, R jest H-pierścieniem. Wobec tego na mocy Stwierdzenia 2.4, R jest pierścieniem z prawie zerowym mnożeniem.

(ii). Istnieje $x \in N$ taki, że $o(x) = \infty$. Zatem na mocy punktu (i) oraz Twierdzenia 2.7 istnieje $U \in \mathbb{N}$ takie, że $Ux^2 = 0$. Stąd $(Ux)^2 = 0$ i wystarczy przyjąć $y = Ux$. □

Twierdzenie 5.9. *Niech R będzie przemiennym pierścieniem filialnym takim, że pierścień $\mathcal{N}(R)$ nie jest torsyjny i $R/\mathcal{N}(R) \in \mathbb{S}$. Wtedy $R = \mathcal{N}(R) \oplus \mathbb{S}(R)$.*

Dowód. Z założeń wynika, że $\mathcal{N}(R)$ jest pierścieniem filialnym, więc ze Stwierdzenia 5.8 wynika, że $\mathcal{N}(R)$ jest pierścieniem z prawie zerowym mnożeniem.

Niech $e = e^2 \in R$ i niech $i \in \mathcal{N}(R)$ będzie takie, że $o(i) = \infty$ oraz $i^2 = 0$. Załóżmy, że $ei = i$. Wtedy $o(e) = \infty$. Ponadto $R/\mathcal{N}(R) \in \mathbb{S}$, więc istnieje $r \in R$ takie, że $2e + \mathcal{N}(R) = (2e + \mathcal{N}(R)))^2(r + \mathcal{N}(R))$. Zatem $2e - 4er \in \mathcal{N}(R)$. Ale $i^2 = 0$ i $\mathcal{N}(R)$ jest z prawie zerowym mnożeniem, więc $i \in a(\mathcal{N}(R))$. Stąd $0 = (2e - 4er)i = 2ei - 4rei = 2i - 4ri$. Ponadto $\langle i \rangle = [i] \lhd R$, więc istnieje $l \in \mathbb{Z}$ takie, że $ri = li$. Zatem $0 = 2i - 4li = (2 - 4l)i$. Ale $o(i) = \infty$, więc $2 - 4l = 0$, sprzeczność. Wobec tego $ei \neq i$. Dalej, $ei = Ki$ dla pewnego $K \in \mathbb{Z}$, skąd $Ki = e^2i = e(ei) = e(Ki) = K(ei) = K^2i$, a więc $K = K^2$. Ponadto $K \neq 1$, więc $K = 0$ i $ei = 0$.

Niech teraz $j \in \mathcal{N}(R)$, $o(j) = \infty$. Wtedy na podstawie Twierdzenia 2.7 istnieje $U \in \mathbb{N}$ takie, że $Uj^2 = 0$, więc $(Uj)^2 = 0$ i $o(Uj) = \infty$ i z pierwszej części dowodu $e(Uj) = 0$, czyli $U(ej) = 0$. Ponadto $[j] = \langle j \rangle + \langle j^2 \rangle$ i $[j] \lhd R$, więc $ej = V_1j + V_2j^2$ dla pewnych $V_1, V_2 \in \mathbb{Z}$. Stąd $0 = U(ej) = UV_1j + UV_2j^2 = UV_1j$, skąd $UV_1j = 0$, skąd $V_1 = 0$. Wobec tego $ej = V_2j^2$. Ale $j^3 = 0$, więc stąd $ej^2 = 0$. Zatem $ej = e^2j = e(ej) = e(V_2j^2) = V_2(ej^2) = 0$. W ten sposób wykazaliśmy, że $ej = 0$ dla każdego $j \in \mathcal{N}(R)$ takiego, że $o(j) = \infty$.

Weźmy dowolne $x \in \mathcal{N}(R)$ takie, że $o(x) < \infty$. Z założenia istnieje $i_0 \in \mathcal{N}(R)$ takie, że $o(i_0) = \infty$. Wtedy $o(i_0 + x) = \infty$ i z pierwszej części dowodu $ei_0 = 0$ oraz

$e(i_0 + x) = 0$, skąd $ex = 0$. W ten sposób wykazaliśmy, że $e\mathcal{N}(R) = 0$ dla każdego idempotenta $e \in R$.

Weźmy dowolne $a \in R$. Wtedy z silnej regularności pierścienia $R/\mathcal{N}(R)$ istnieje $r \in R$ takie, że $a - a^2r \in \mathcal{N}(R)$ oraz $ar + \mathcal{N}(R)$ jest idempotentem w $R/\mathcal{N}(R)$. Zgodnie z Twierdzeniem 1.22, istnieje $e = e^2 \in R$ takie, że $ar - e \in \mathcal{N}(R)$. Stąd $a - ae \in \mathcal{N}(R)$ i $a \in Re + \mathcal{N}(R)$. Weźmy dowolne $b \in R$ takie, że $be \in \mathcal{N}(R)$. Wtedy $0 = (be)e = be^2 = be$, skąd $\mathcal{N}(R) \cap Re = 0$. Dlatego $Re \cong (Re + \mathcal{N}(R))/\mathcal{N}(R) \lhd R/\mathcal{N}(R)$ i $R/\mathcal{N}(R) \in \mathbb{S}$, więc $Re \in \mathbb{S}$. Zatem $Re \subseteq \mathbb{S}(R)$ i $a \in \mathbb{S}(R) + \mathcal{N}(R)$. Stąd $R = \mathcal{N}(R) + \mathbb{S}(R)$. Ale $\mathcal{N}(R) \cap \mathbb{S}(R) = 0$, więc $R = \mathbb{S}(R) \oplus \mathcal{N}(R)$. □

Lemat 5.10. *Niech R będzie przemiennym pierścieniem filialnym o nietorsyjnym nilradykale. Jeżeli $R \neq \mathbb{S}(R) \oplus \mathcal{N}(R)$, to $R/(\mathbb{S}(R) \oplus \mathcal{N}(R))$ jest przemiennym, beztorsyjnym, zredukowanym i $\mathbb{S}$-półprostym pierścieniem filialnym. Ponadto $ay \neq 0$ dla dowolnego $a \in R \setminus (\mathbb{S}(R) \oplus \mathcal{N}(R))$ i dowolnego $y \in R$ takiego, że $y^2 = 0$, $o(y) = \infty$.*

Dowód. Niech $N = \mathcal{N}(R)$. Z filialności pierścienia R i Stwierdzenia 5.8 wynika, że N jest pierścieniem z prawie zerowym mnożeniem i istnieje $y \in N$ taki, że $y^2 = 0$ oraz $o(y) = \infty$.

Pierścień $R/(\mathbb{S}(R) \oplus N)$ jest przemienny i filialny jako obraz homomorficzny pierścienia R. Istnieje $T \lhd R$ takie, że $N \subseteq T$ i $T/N = \mathbb{S}(R/N)$. Oczywiście $T/N \in \mathbb{S}$ oraz $\mathbb{S}(T) \cap N = 0$. Ponadto na mocy Twierdzenia 5.9, $T = \mathbb{S}(T) \oplus N$. Dalej, $\mathbb{S}(T) \subseteq R$ i $(\mathbb{S}(R)+N)/N \cong \mathbb{S}(R)/(N \cap \mathbb{S}(R)) \in \mathbb{S}$. Zatem $(\mathbb{S}(R)+N)/N \subseteq \mathbb{S}(R/N) = T/N$, skąd $\mathbb{S}(R) \subseteq \mathbb{S}(T)$. Zatem $T = \mathbb{S}(R) \oplus N$. Ponadto pierścień R/N jest zredukowany i filialny, więc pierścień $(R/N)/(\mathbb{S}(R/N))$ jest zredukowany i $\mathbb{S}$-półprosty. Jest on również beztorsyjny na mocy Lematu 1 z [10]. Dalej

$$(R/N)/(\mathbb{S}(R/N)) = (R/N)/((\mathbb{S}(R) \oplus N)/N) \cong R/(\mathbb{S}(R) \oplus N),$$

więc $R/(\mathbb{S}(R) \oplus N)$ jest przemiennym, beztorsyjnym, zredukowanym i $\mathbb{S}$-półprostym pierścieniem filialnym.

Weźmy teraz dowolne $a \in R \setminus (\mathbb{S}(R) \oplus \mathcal{N}(R))$ i dowolne $y \in R$ takie, że $y^2 = 0$, $o(y) = \infty$. Pokażemy, że $Ra \cap \langle y \rangle \neq 0$. Załóżmy, że $Ra \cap \langle y \rangle = 0$. Wtedy $Ra \oplus \langle y \rangle \lhd R$, ponieważ $Ra \oplus \langle y \rangle \lhd Ra + N \lhd R$ oraz $y \in a(N)$, gdyż pierścień N jest z prawie zerowym mnożeniem. Zatem pierścień $Ra \oplus \langle y \rangle$ jest filialny. Ale $\langle y \rangle \cong \mathbb{Z}^0$, więc na podstawie Twierdzenia 5.1, pierścień Ra spełnia warunek (5.1). Ponadto $a^2 \notin \mathbb{S}(R) \oplus N$ i $a^2 \in Ra$, więc $\mathcal{N}(Ra) \neq Ra$. Zatem na mocy Twierdzenia 5.7, $\mathbb{S}(Ra) \neq 0$ i $Ra = \mathbb{S}(Ra) \oplus \mathcal{N}(Ra)$. Ale pierścień N jest z prawie zerowym mnożeniem, więc $[\mathcal{N}(Ra)]^3 = 0$, skąd $(a^2)^3 \in \mathbb{S}(Ra)$. Zatem $a^6 \in \mathbb{S}(R) \oplus N$, skąd $a \in \mathbb{S}(R) \oplus N$, sprzeczność. Wobec tego $Ra \cap \langle y \rangle \neq 0$.

Przypuśćmy, że $ay = 0$. Ponieważ $a^2 \in R \setminus (\mathbb{S}(R) \oplus N)$, więc z pierwszej części dowodu $Ra^2 \cap \langle y \rangle \neq 0$. Zatem $ra^2 = Uy \neq 0$ dla pewnych $r \in R$, $U \in \mathbb{Z}$. Ale $y^2 = 0$, więc $(ra^2)^2 = 0$ i $(ra)^4 = 0$. Zatem $ra = x \in N$ i $xa = Uy$. Ale $ay = 0$, więc $xa^2 = 0$. Ponadto z filialności i $\mathbb{S}$-półprostoty pierścienia $R/(\mathbb{S}(R) \oplus N)$ wynika, że istnieją $n \in \mathbb{N}$, $b \in R$ oraz $i \in \mathbb{S}(R) \oplus N$ takie, że $na = a^2b + i$. Zatem $0 \neq nUy = x(na) = xa^2b + xi = xi$. Ale $i = s + m$ dla pewnych $s \in \mathbb{S}(R)$, $m \in N$, więc $xi = xm \in \langle x^2 \rangle \subseteq \mathbb{T}(N)$ i wobec tego $0 \neq nUy \in \mathbb{T}(N)$, co przeczy temu, że $o(y) = \infty$. □

Twierdzenie 5.11. *Niech R będzie przemiennym pierścieniem filialnym o nietorsyjnym nil-radykale i niech $R \neq \mathbb{S}(R) \oplus \mathcal{N}(R)$. Wówczas istnieją $m \in \mathbb{N}$, $v \in R \setminus (\mathcal{N}(R) \oplus \mathbb{S}(R))$ takie, że $v^2 - mv \in \mathcal{N}(R)$, $va = ma$ dla każdego $a \in \mathbb{S}(R)v$ oraz $\mathbb{S}(R) = \mathbb{S}(R)v \oplus l_{\mathbb{S}(R)}(v)$. Ponadto pierścień $\langle v \rangle + \mathcal{N}(R)$ jest filialny, $(\langle v \rangle + \mathcal{N}(R))/\mathcal{N}(R) \cong m\mathbb{Z}$ i $(\langle v \rangle + \mathcal{N}(R)) \cap \mathbb{S}(R)v = 0$ oraz*

$$R = (\langle v \rangle + \mathcal{N}(R) + \mathbb{S}(R)v) \oplus l_{\mathbb{S}(R)}(v). \tag{5.2}$$

W szczególności $R/(\mathcal{N}(R) \oplus \mathbb{S}(R)) \cong m\mathbb{Z}$.

Dowód. Oznaczmy $N = \mathcal{N}(R)$, $S = \mathbb{S}(R)$. Na podstawie Stwierdzenia 5.8, N jest pierścieniem z prawie zerowym mnożeniem i istnieje $y \in N$ takie, że $o(y) = \infty$ i $y^2 = 0$. Stąd $(S \oplus N)y = 0$ oraz $\langle y \rangle = [y] \lhd N$, więc $\langle y \rangle \lhd R$ i $Ry \subseteq \langle y \rangle$. Weźmy dowolne $a \in R \setminus (S \oplus N)$. Z Lematu 5.10 wynika, że $ay \neq 0$. Zatem istnieje $m \in \mathbb{N}$ takie, że $Ry = m\langle y \rangle$. Stąd $vy = my$ dla pewnego $v \in R$. Zatem $v \notin S \oplus N$, bo $(S \oplus N)y = 0$ i $o(y) = \infty$.

Weźmy dowolne $r \in R$. Wtedy istnieje $U \in \mathbb{Z}$ takie, że $ry = Umy$, czyli $ry = Uvy$. Stąd $r - Uv \in l_R(y)$ i na podstawie Lematu 5.10, $l_R(y) \subseteq S \oplus N$. Zatem $l_R(y) = S \oplus N$ oraz $R = \langle v \rangle + S \oplus N$, przy czym $\langle v \rangle \cap (S \oplus N) = 0$, bo na mocy Lematu 5.10 pierścień $R/(S \oplus N)$ jest beztorsyjny i $v \notin S \oplus N$. Ale $vy = my$, więc $v^2 y = mvy$, skąd $v^2 - mv \in l_R(y) = S \oplus N$. Zatem $R/(S \oplus N) \cong m\mathbb{Z}$.

Dalej, $v^2 = mv + s_0 + x_0$, gdzie $s_0 \in S$, $x_0 \in N$ oraz $R^+ = \langle v \rangle^+ \oplus S^+ \oplus N^+$. Ponieważ pierścień S jest silnie regularny, więc istnieje $e = e^2 \in Ss_0$ takie, że $s_0 = s_0 e$. Stąd i z tego, że $v^2 = mv + s_0 + x_0$ mamy $v^2 e = mve + s_0$. Zatem $ve \in S$ oraz $(v - ve)^2 - m(v - ve) = v^2 - 2v^2 e + v^2 e^2 - mv + mve = (v^2 - mv) - 2v^2 e + v^2 e + mve = s_0 + x_0 - v^2 e + mve = x_0 \in N$. Wobec tego można zastąpić v przez $v - ve$ i dla nowego v będzie $v^2 - mv = x_0 \in N$ oraz $vy = my$.

Ponadto $o(v + N) = \infty$, więc $(\langle v \rangle + N)/N \cong m\mathbb{Z}$. Stąd $\mathbb{S}((\langle v \rangle + N)/N) = 0$ i wobec tego $(\mathbb{S}(\langle v \rangle + N) + N)/N = 0$. Zatem $\mathbb{S}(\langle v \rangle + N) \subseteq N$, skąd $\mathbb{S}(\langle v \rangle + N) = 0$ oraz $(\langle v \rangle + N) \cap S = 0$ i w szczególności $(\langle v \rangle + N) \cap Sv = 0$.

Weźmy dowolne $a, b \in \langle v \rangle + N$. Wtedy z filialności pierścienia R i tego, że $R = \langle v \rangle + S + N$ istnieją $U_1, U_2, k \in \mathbb{Z}$, $s \in S$, $x \in N$, dla których $ba = U_1 a + U_2 a^2 + (kv + s + x)a^2$. Stąd $sa^2 \in S \cap (\langle v \rangle + N) = 0$, więc $ba = U_1 a + U_2 a^2 + (kv + x)a^2$ i pierścień $\langle v \rangle + N$ jest filialny.

Niech $s \in S$, wtedy $vs \in S$ i pierścień S jest silnie regularny. Istnieje zatem $r \in S$ takie, że $vs = (vs)^2 r$, skąd $v(s - vs^2 r) = 0$. Stąd $s - vs^2 r \in l_S(v)$, czyli $s \in Sv + l_S(v)$. Wobec tego $S = Sv + l_S(v)$. Weźmy dowolne $s \in S$ takie, że $sv \in l_S(v)$. Wtedy $sv^2 = 0$, skąd $(sv)^2 = 0$ i ponieważ pierścień S jest zredukowany, więc $sv = 0$. Zatem $Sv \cap l_S(v) = 0$ i $S = Sv \oplus l_S(v)$. Wobec tego $R^+ = ((\langle v \rangle + N)^+ \oplus (Sv)^+) \oplus l_S(v)^+$ i $((\langle v \rangle + N) + Sv) \cdot l_S(v) = 0$. Zatem $(\langle v \rangle + N) + Sv \lhd R$, $l_S(v) \lhd R$, co dowodzi wzoru (5.2).

Weźmy dowolne $a \in Sv$. Wtedy $a = vs$ dla pewnego $s \in S$. Zatem $va = v^2 s = (mv + x_0)s = m(vs) + x_0 s$. Ale $x_0 s \in S \cap N = 0$, więc $x_0 s = 0$ i $va = ma$. □

Definicja 5.12. Przemienny pierścień filialny R o nietorsyjnym nil-radykale i taki, że $R/\mathcal{N}(R) \cong m\mathbb{Z}$ dla pewnego $m \in \mathbb{N}$, będziemy nazywali B**-pierścieniem**.

Przykład 5.13. Niech R będzie B-pierścieniem i $R/\mathcal{N}(R) \cong m\mathbb{Z}$ dla pewnego $m \in \mathbb{N}$. Niech S i T będą przemiennymi pierścieniami silnie regularnymi. Na mocy Lematu 5.11 istnieje $v \in R$ takie, że $R^+ = \langle v \rangle \oplus \mathcal{N}(R)$, $o(v) = \infty$ oraz $v^2 - mv \in \mathcal{N}(R)$ i pierścień $\mathcal{N}(R)$ jest z prawie zerowym mnożeniem oraz nie jest torsyjny. Standardowe sprawdzenie pokazuje, że S jest R-algebrą przy działaniu zewnętrznym $\circ$ zdefiniowanym w następujący sposób: dla $k \in \mathbb{Z}$, $x \in \mathcal{N}(R)$ i $a \in S$ przyjmujemy $(kv+x) \circ a = (km)a$. Na podstawie Stwierdzenia 1.36 pierścień $R \boxplus S$ jest filialny. Wobec tego, jeszcze raz ze Stwierdzenia 1.36, pierścień $A = (R \boxplus S) \oplus T$ też jest filialny i jest przemienny oraz ma nietorsyjny nil-radykał. Ponadto, $\mathcal{N}(A) = \mathcal{N}(R)$, $\mathbb{S}(A) = S \oplus T$, $A/\mathbb{S}(A) \cong R$ i $A^+ = \langle v \rangle \oplus \mathcal{N}(A) \oplus \mathbb{S}(A)$.

Na podstawie Twierdzenia 5.11 i Przykładu 5.13 otrzymujemy od razu następujące twierdzenie klasyfikacyjne dla przemiennych pierścieni filialnych o nietorsyjnym nil-radykale wyrażone w języku pierścieni silnie regularnych i B-pierścieni.

Twierdzenie 5.14. *Dla przemiennego pierścienia R równoważne są warunki:*

(i) R jest pierścieniem filialnym o nietorsyjnym nil-radykale oraz $R \neq \mathbb{S}(R) \oplus \mathcal{N}(R)$,

(ii) istnieje B-pierścień A oraz istnieją przemienne pierścienie silnie regularne S i T takie $R \cong (A \boxplus S) \oplus T$.

5.3 Klasyfikacje pewnych klas B-pierścieni

W całym tym paragrafie będziemy zakładali, że R jest B-pierścieniem, $N = \mathcal{N}(R)$ i $R/N \cong m\mathbb{Z}$ dla pewnego $m \in \mathbb{N}$. Na podstawie Stwierdzenia 5.8, N jest przemiennym pierścieniem z prawie zerowym mnożeniem i istnieje $y \in N$ takie, że $y^2 = 0$ oraz $o(y) = \infty$. Ponadto na mocy Twierdzenia 5.11 i jego dowodu, istnieje $v \in R \setminus N$ takie, że $x_0 = v^2 - mv \in N(R)$, $R^+ = \langle v \rangle \oplus N(R)$ i $vy = my$.

Lemat 5.15. *Dla każdego $x \in N$ mamy, że $vx - mx \in \langle x^2 \rangle$. Jeżeli $x \in N$ i $V \in \mathbb{Z}$ oraz $vx = mx + Vx^2$, to*

$$(v-x)^2 - m(v-x) = x_0 - mx + (1-2V)x^2. \tag{5.3}$$

W szczególności dla każdego $x \in a(N)$ mamy $vx = mx$ oraz:

$$(v-x)^2 - m(v-x) = x_0 - mx. \tag{5.4}$$

Dowód. Weźmy dowolne $x \in N$. Ponieważ N jest pierścieniem z prawie zerowym mnożeniem, więc $(y + x^2)^2 = 0$. Z filialności pierścienia R, $v(y + x^2) = W(y + x^2)$ dla pewnego $W \in \mathbb{Z}$. Ale $v(y + x^2) = vy + vx^2 = my + vx^2$, więc $my + vx^2 = Wy + Wx^2$, skąd $(m - W)y \in \mathbb{T}(N)$, a zatem $m = W$ i $vx^2 = mx^2$.

Jeżeli $o(x) = \infty$, to $[x] = \langle x \rangle + \langle x^2 \rangle \lhd R$ i istnieją $U, V \in \mathbb{Z}$ takie, że $vx = Ux + Vx^2$. Ale $vx^2 = mx^2$, więc $v^2x = Uvx + mVx^2 = U^2x + (UV + mV)x^2$ i $v^2x = (mv + x_0)x = mvx + x_0x = mUx + mVx^2 + x_0x$, skąd $(mU - U^2)x = UVx^2 - xx_0 \in \mathbb{T}(N)$. Dlatego $mU = U^2$, skąd $U = m$ lub $U = 0$. Jeżeli $U = 0$, to $vx = Vx^2$, skąd $vx^2 = Vx^3 = 0$,

więc $mx^2 = 0$. Zatem $(mx)^2 = 0$ i na podstawie Lematu 5.10, $v(mx) \neq 0$. Ale $v(mx) = m(Vx^2) = V(mx^2) = 0$, więc mamy sprzeczność. Zatem $m = U$ i wobec tego $vx = mx + Vx^2$, skąd $vx - mx \in \langle x^2 \rangle$.

Niech teraz $o(x) < \infty$. Wtedy $o(y+x) = \infty$, więc $v(y+x) = m(y+x) + V(y+x)^2$ dla pewnego $V \in \mathbb{Z}$. Ale $v(y+x) = vy + vx = my + vx$ oraz $(y+x)^2 = x^2$, więc z $my + vx = my + mx + Vx^2$ wynika, że $vx = mx + Vx^2$, skąd $vx - mx \in \langle x^2 \rangle$. Wtedy $(v-x)y = vy = my$ oraz $(v-x)^2 - m(v-x) = v^2 - 2vx + x^2 - mv + mx = (v^2 - mv) + x^2 - 2(mx + Vx^2) + mx = x_0 + x^2 - mx - 2Vx^2 = x_0 - mx + (1-2V)x^2$. □

Lemat 5.16. *Elementy x_0 oraz v można wybrać tak, że $x_0^2 = 0$.*

Dowód. Załóżmy, że $x_0^2 \neq 0$. Wtedy istnieje bezkwadratowa liczba naturalna s taka, że $o(x_0^2) = s$. Stąd $(sx_0)^2 = 0$. Ponadto na podstawie Lematu 5.15, $vx_0 = mx_0 + Vx_0^2$ dla pewnego $V \in \mathbb{Z}$. Ponieważ $v^2 = mv + x_0$, więc $v^2x_0 = mvx_0 + x_0^2$. Zatem $Vmx_0^2 = x_0^2$, skąd $(1 - Vm)x_0^2 = 0$. Wobec tego $[(1 - Vm)x_0]^2 = 0$. Dalej, dla $x = Vx_0$ z tego, że $vx_0 = mx_0 + Vx_0^2$ otrzymujemy $vx = mx + x^2$. Zatem na mocy wzoru (5.4), $(v-x)^2 - m(v-x) = x_0 - mx - x^2$. Ale $x^2 \in a(N)$ i $x_0 - mx = (1 - Vm)x_0 \in a(N)$, więc $[x_0 - mx - x^2]^2 = 0$. Wobec tego za v wystarczy przyjąć $v - x$ i za x_0 przyjąć $x_0 - mx - x^2$.

□

Lemat 5.17. *Elementy x_0 oraz v można wybrać tak, że $x_0^2 = 0$ oraz $mx_0 = 0$.*

Dowód. Na mocy Lematu 5.16 możemy przyjąć, że $x_0^2 = 0$. Wówczas $vx_0 = mx_0$. Ale $v^2 = mv + x_0$, więc dla $x \in N$, $xx_0 = 0$, skąd $v^2x = mvx$ dla każdego $x \in N$. W szczególności $v^2N = mvN$. Ale $R = \langle v \rangle + N$, więc $\langle v \rangle + Rv = \langle v \rangle + \langle v^2 \rangle + Nv = \langle v \rangle + \langle x_0 \rangle + Nv$, czyli

$$\langle v \rangle + Rv = \langle v \rangle + \langle x_0 \rangle + Nv. \tag{5.5}$$

Stąd

$$\langle v^2 \rangle + Rv^2 = \langle v^2 \rangle + \langle mx_0 \rangle + Nv^2, \tag{5.6}$$

czyli

$$\langle v^2 \rangle + Rv^2 = \langle v^2 \rangle + \langle mx_0 \rangle + mvN. \tag{5.7}$$

Zatem $\langle v \rangle + \langle v^2 \rangle + Rv^2 = \langle v \rangle + \langle x_0 \rangle + mvN$. Ale z filialności pierścienia R, $\langle v \rangle + Rv = \langle v \rangle + \langle v^2 \rangle + Rv^2$, więc $\langle v \rangle + \langle x_0 \rangle + mvN = \langle v \rangle + \langle x_0 \rangle + vN$. Ponadto $o(v + N) = \infty$ w grupie $(R/N)^+$, więc

$$\langle x_0 \rangle + vN = \langle x_0 \rangle + mvN. \tag{5.8}$$

Po pomnożeniu obu stron równości (5.7) przez v^2 otrzymujemy $\langle v^4 \rangle + Rv^4 = \langle v^4 \rangle + \langle m^3x_0 \rangle + m^3vN$, gdyż $v^2x_0 = mvx_0 = m^2x_0$ i $mv^3N = mv(v^2N) = mv(mvN) = m^2v^2N = m^3vN$. Ale $v^4 = (mv + x_0)^2 = m^2v^2 + 2mvx_0 = m^2v^2 + 2m^2x_0$, więc stąd

$$\langle v^2 \rangle + \langle v^4 \rangle + Rv^4 = \langle v^2 \rangle + \langle 2m^2x_0 \rangle + \langle m^3x_0 \rangle + m^3vN \tag{5.9}$$

Z filialności pierścienia R oraz z (5.6), (5.7) i (5.9) uzyskujemy, że $\langle v^2 \rangle + \langle mx_0 \rangle + mvN = \langle v^2 \rangle + \langle 2m^2x_0 \rangle + \langle m^3x_0 \rangle + m^3vN$, ale $o(v^2 + N) = \infty$ w grupie $(R/N)^+$ i dlatego $\langle mx_0 \rangle + mvN = \langle 2m^2x_0 \rangle + \langle m^3x_0 \rangle + m^3vN$. Zatem istnieją $U \in \mathbb{Z}$ oraz $x \in N$ takie, że

$mx_0 = Um^2x_0 + m^3vx$. Ale $x_0 \in a(N)$, więc stąd $m^3(vx) \in a(N)$, czyli $[m^3(vx)]^2 = 0$. Zatem $m^6(vx)^2 = 0$. Ale $o((vx)^2) = 1$ lub $o((vx)^2)$ jest liczbą bezkwadratową, więc $m(vx)^2 = 0$, czyli $m(vx) = x_1 \in a(N)$. Wobec tego $Um^2x_0 + m^3vx = m^2(Ux_0 + mvx) = m^2(Ux_0 + x_1) = m^2x_2$, gdzie $x_2 = Ux_0 + x_1 \in a(N)$ oraz $m(x_0 - mx_2) = 0$. Przyjmując w Lemacie 5.15, $x = x_2$ dostajemy, że $(v - x_2)^2 - m(v - x_2)^2 = x_0 - mx_2$. Powyższe rozważania pokazują, że wystarczy przyjąć $x_0 - mx_2$ za x_0 i $v - x_2$ za v. □

Niech dalej elementy x_0 oraz v będą wybrane tak, że $x_0^2 = mx_0 = 0$.

Lemat 5.18. *Dla dowolnych $k \in \mathbb{N}$, $x \in N$ mamy:*

(i) jeśli $V \in \mathbb{Z}$ i $vx = mx + Vx^2$, to $mVx^2 = 0$,

(ii) $v^2x = m^2x = mvx$,

(iii) $m^2N = mvN = m^2vN = m^3N$,

(iv) $k(m^2N) = k^2(m^2N)$.

Dowód. Na mocy Lematu 5.15, $vx = mx + Vx^2$ dla pewnego $V \in \mathbb{Z}$ oraz $vx^2 = mx^2$. Zatem $v^2x = v(mx + Vx^2) = mvx + Vmx^2$ oraz $v^2 = mv + x_0$ i $x_0 \in a(N)$, więc $v^2x = mvx$, skąd $Vmx^2 = 0$, co dowodzi (i). Dalej, $v^2x = m(mx + Vx^2) = m^2x + mVx^2 = m^2x$, co dowodzi (ii).

(iii). Mnożąc obie strony równości (5.8) przez m z uwzględnieniem tego, że $mx_0 = 0$ i wykorzystując punkt (ii) uzyskujemy tezę.

(iv). Mnożąc stronami równość (5.5) przez k dostajemy $\langle kv\rangle + R(kv) = \langle kv\rangle + \langle kx_0\rangle + kvN$. Ponadto $(kv)^2 = k^2v^2 = k^2(mv + x_0) = k^2mv + k^2x_0 = km(kv) + k^2x_0$, więc $k^2v^3 = m(kv)^2$ oraz $\langle kv\rangle + \langle k^2v^2\rangle = \langle kv\rangle + \langle k^2x_0\rangle$. Zatem $\langle kv\rangle + \langle k^2v^2\rangle + R(k^2v^2) = \langle kv\rangle + \langle k^2x_0\rangle + \langle k^2v^3\rangle + k^2v^2N = \langle kv\rangle + \langle k^2x_0\rangle + k^2mvN$. Z filialności pierścienia R, mamy $\langle kv\rangle + \langle kx_0\rangle + kvN = \langle kv\rangle + \langle k^2x_0\rangle + k^2mvN$. Ale $o(kv + N) = \infty$ w grupie $(R/N)^+$, więc stąd

$$\langle kx_0\rangle + kvN = \langle k^2x_0\rangle + k^2mvN. \tag{5.10}$$

Mnożąc ostatnią równość przez m i uwzględniając $mx_0 = 0$ mamy $k(mvN) = k^2(m^2vN)$. Stąd i z punktu (iii) mamy tezę.

□

Stwierdzenie 5.19. *Wszystkimi, z dokładnością do izomorfizmu, B-pierścieniami R takimi, że $R/\mathcal{N}(R) \cong \mathbb{Z}$ są pierścienie $\mathbb{Z} \boxplus N$, gdzie N jest przemiennym, nietorsyjnym prawie podzielnym pierścieniem z prawie zerowym mnożeniem.*

Dowód. Implikacja $\Leftarrow$ wynika bezpośrednio z Wniosku 4.11. Na odwrót, ponieważ $m = 1$, więc na podstawie Lematu 5.17, $v = v^2$. Dalej, z Lematu 5.18 otrzymujemy, że $N = vN$. Ponieważ $R = \langle v\rangle + N$, więc v jest jedynką pierścienia R. Ale $R^+ = \langle v\rangle \oplus N$, więc otrzymujemy stąd, że $R \cong \mathbb{Z} \boxplus N$. □

Rozdział 6

Przemienne torsyjne pierścienie filialne

6.1 Użyteczne lematy związane z idempotentami w pierścieniach filialnych

Lemat 6.1. *Niech R będzie przemiennym pierścieniem filialnym posiadającym nil-ideał I, który jest p-pierścieniem. Wówczas dla każdego idempotenta $e \in R$, $eI = 0$ lub $ei = i$ dla każdego $i \in I$.*

Dowód. Załóżmy, że tak nie jest. Wówczas eI oraz $J = \{ei - i \,:\, i \in I\}$ są niezerowymi ideałami pierścienia R zawartymi w I takimi, że $eI \cap J = 0$. Ponieważ I jest nil-p-pierścieniem, więc istnieją niezerowe $a \in eI$ oraz $b \in J$ takie, że $a^2 = b^2 = 0$ i $pa = pb = 0$. Stąd $ab = 0$, $\langle a\rangle \cap \langle b\rangle = 0$ i wobec tego $\langle a+b\rangle = [a+b]$. Ale z Twierdzenia 1.35 wynika, że I jest H-pierścieniem, więc z filialności pierścienia R, $\langle a+b\rangle \lhd R$. Zatem $e(a+b) = k(a+b)$ dla pewnego $k \in \mathbb{Z}$. Ponadto $e(a+b) = ea + eb = a + 0 = a$, więc $a = ka + kb$. Stąd $kb \in \langle a\rangle \cap \langle b\rangle = 0$, więc $kb = 0$ i w konsekwencji $p \mid k$ i $ka = 0$, więc $a = 0$, sprzeczność. □

Lemat 6.2. *Niech R będzie przemiennym pierścieniem filialnym takim, że $\mathcal{N}(R)$ jest niezerowym p-pierścieniem oraz $R/\mathcal{N}(R) \in \mathbb{S}$. Wówczas dla każdego idempotenta $e \in R$, pierścień Re jest silnie regularny wtedy i tylko wtedy, gdy $e\mathcal{N}(R) = 0$.*

Dowód. $\Rightarrow$. Z założenia $Re \subseteq \mathbb{S}(R)$. Stąd $e\mathcal{N}(R) \subseteq \mathbb{S}(R) \cap \mathcal{N}(R) = 0$, więc $e\mathcal{N}(R) = 0$.

$\Leftarrow$. Z założenia $\mathcal{N}(R) \subseteq l_R(e)$. Ale $R = Re \oplus l_R(e)$, więc $Re \cong (Re + \mathcal{N}(R))/\mathcal{N}(R) \lhd R/\mathcal{N}(R)$. Ponadto $R/\mathcal{N}(R) \in \mathbb{S}$ oraz radykał $\mathbb{S}$ jest dziedziczny, więc $Re \in \mathbb{S}$. □

Lemat 6.3. *Niech R będzie przemiennym pierścieniem filialnym takim, że $\mathcal{N}(R)$ jest niezerowym p-pierścieniem oraz $R/\mathcal{N}(R) \in \mathbb{S}$. Jeżeli $\mathbb{S}(R) + \mathcal{N}(R) \neq R$, to istnieje idempotent $e \in R$ taki, że $\mathcal{N}(R) \subseteq eR$ oraz $R = eR \oplus l_R(e)$, przy czym $l_R(e) \in \mathbb{S}$.*

Dowód. Z założenia istnieje $x \in R \setminus (\mathbb{S}(R) + \mathcal{N}(R))$. Z silnej regularności pierścienia $R/\mathcal{N}(R)$ istnieje $y \in R$ takie, że $x - x^2y \in \mathcal{N}(R)$ oraz $yx + \mathcal{N}(R)$ jest idempotentem w $R/\mathcal{N}(R)$. Ale $\mathcal{N}(R)$ jest nil-pierścieniem, więc na podstawie Twierdzenia 1.22 istnieje

idempotent $e \in R$ taki, że $yx - e \in \mathcal{N}(R)$. Zatem $x - ex = (x - x^2y) + x(xy - e) \in \mathcal{N}(R)$, skąd $x \in eR + \mathcal{N}(R)$. Ale $x \notin \mathbb{S}(R) + \mathcal{N}(R)$, więc $e \notin \mathbb{S}(R)$. Zatem $Re \notin \mathbb{S}$ i na mocy Lematu 6.2, $e\mathcal{N}(R) \neq 0$. Wobec tego na podstawie Lematu 6.1, $ei = i$ dla każdego $i \in \mathcal{N}(R)$. Zatem $\mathcal{N}(R) \subseteq eR$, skąd $\mathcal{N}(eR) = \mathcal{N}(R)$. Ponadto $R = eR \oplus l_R(e)$ i $R/\mathcal{N}(R) \in \mathbb{S}$, więc $l_R(e) \in \mathbb{S}$. □

Lemat 6.4. *Niech R będzie przemiennym pierścieniem filialnym takim, że $\mathcal{N}(R)$ jest niezerowym p-pierścieniem oraz $R/\mathcal{N}(R) \in \mathbb{S}$. Jeśli $e\mathcal{N}(R) = 0$ dla każdego idempotenta $e \in R$, to $R = \mathbb{S}(R) \oplus \mathcal{N}(R)$.*

Dowód. Załóżmy, że $R \neq \mathbb{S}(R) \oplus \mathcal{N}(R)$. Wtedy zgodnie z Lematem 6.3, istnieje $e = e^2 \in R$ taki, że $\mathcal{N}(R) \subseteq eR$. Weźmy dowolne $i \in \mathcal{N}(R)$. Wówczas $i = ex$ dla pewnego $x \in R$. Stąd $0 = ei = e^2x = ex = i$. Zatem $\mathcal{N}(R) = 0$ i mamy sprzeczność. □

Lemat 6.5. *Niech R będzie przemiennym p-pierścieniem filialnym, takim, że grupa $\mathcal{N}(R)^+$ nie ma ograniczonego wykładnika. Wówczas $R = \mathbb{S}(R) \oplus \mathcal{N}(R)$.*

Dowód. Weźmy dowolne $e = e^2 \in R$. Jeśli $e\mathcal{N}(R) \neq 0$, to $\mathcal{N}(R) = \mathcal{N}(R)e$ na podstawie Lematu 6.1. Ale $p^n e = 0$ dla pewnego naturalnego n, więc $p^n\mathcal{N}(R) = 0$, sprzeczność. Zatem $e\mathcal{N}(R) = 0$ i na mocy Lematu 6.4, $R = \mathbb{S}(R) \oplus \mathcal{N}(R)$. □

Lemat 6.6. *Niech R będzie przemiennym, filialnym pierścieniem z jedynką takim, że $\mathcal{N}(R)$ jest niezerowym p-pierścieniem oraz $R/\mathcal{N}(R) \in \mathbb{S}$. Wówczas $R = \langle 1 \rangle + \mathbb{S}(R) + \mathcal{N}(R)$.*

Dowód. Na podstawie Twierdzenia 1.35, $\mathcal{N}(R)$ jest H-pierścieniem, więc ze Stwierdzenia 2.13 wynika, że pierścień $\mathcal{N}(R)$ jest nilpotentny. Zatem istnieje niezerowe $i_0 \in l_{\mathcal{N}(R)}(\mathcal{N}(R))$. Wówczas $\langle i_0 \rangle \lhd \mathcal{N}(R)$, więc $\langle i_0 \rangle \lhd R$. Weźmy dowolne $r \in R$. Wtedy istnieje całkowite k takie, że $ri_0 = ki_0$, skąd $r - k \cdot 1 \in l_R(i_0)$. Zatem $R = \langle 1 \rangle + l_R(i_0)$. Ponadto $\mathbb{S}(R) \cap \mathcal{N}(R) = 0$, więc $\mathbb{S}(R) \subseteq l_R(i_0)$, skąd $\mathbb{S}(l_R(i_0)) = \mathbb{S}(R)$. Z określenia i_0, $\mathcal{N}(R) \subseteq l_R(i_0)$, więc $\mathcal{N}(l_R(i_0)) = \mathcal{N}(R)$. Weźmy dowolne $e = e^2 \in l_R(i_0)$. Wtedy $ei_0 = 0$ oraz $i_0 \neq 0$, więc na mocy Lematu 6.1, $e\mathcal{N}(R) = 0$. Zatem stosując Lemat 6.4 do pierścienia $l_R(i_0)$ otrzymujemy, że $l_R(i_0) = \mathbb{S}(R) + \mathcal{N}(R)$. Wobec tego $R = \langle 1 \rangle + \mathbb{S}(R) + \mathcal{N}(R)$. □

Lemat 6.7. *Niech R będzie filialnym p-pierścieniem z jedynką. Wówczas $\beta(R) = \beta(R)(p) + p \cdot \langle 1 \rangle$. W szczególności grupa $p\beta(R)^+$ jest cykliczna oraz $y^2 \in (\beta(R)(p))^2 + \langle y \rangle$ dla każdego $y \in \beta(R)$.*

Dowód. Ponieważ R^+ jest p-grupą, więc istnieje $n \in \mathbb{N}$ takie, że $o(1) = p^n$ w R^+. Stąd $p^n R = 0$ i $pR \subseteq \beta(R)$. Z filialności pierścienia R i Twierdzenia 1.35 mamy, że $\beta(R)$ jest H-pierścieniem. Ale $\langle p \cdot 1 \rangle = [p \cdot 1] \lhd \beta(R)$, więc $\langle p \cdot 1 \rangle \lhd R$, czyli $pR \subseteq p\langle 1 \rangle$. W szczególności $p\beta(R) \subseteq p\langle 1 \rangle$ i $p\beta(R)^+$ jest grupą cykliczną.

Jeżeli $p\beta(R) = 0$, to $\beta(R) \subseteq \beta(R)(p)$ i $\beta(R) = \beta(R)(p) + p\langle 1 \rangle$. Niech dalej $p\beta(R) \neq 0$. Weźmy dowolne $i \in \beta(R)$. Istnieje wówczas $k \in \mathbb{Z}$ takie, że $pi = k(p \cdot 1)$.

Jeśli $p \nmid k$, to istnieje $l \in \mathbb{Z}$ takie, że $lk \equiv 1 \pmod{p^n}$, więc $p \cdot 1 = lpi$. Zatem $p\beta(R) \subseteq pi\beta(R)$ i przez indukcję $p\beta(R) \subseteq pi^m\beta(R)$ dla każdego naturalnego m. Ale $\beta(R)$ jest nil-pierścieniem, skąd $p\beta(R) = 0$, sprzeczność.

Wobec tego $p \mid k$ i istnieje $k' \in \mathbb{Z}$ takie, że $k = pk'$. Wtedy $p(i - (pk') \cdot 1) = 0$, $i - (pk') \cdot 1 \in \beta(R)(p)$, skąd $i = (i - (pk') \cdot 1) + pk' \cdot 1 \in \beta(R)(p) + p \cdot \langle 1 \rangle$. Zatem $\beta(R) = \beta(R)(p) + p \cdot \langle 1 \rangle$.

Weźmy dowolne $y \in \beta(R)$. Wtedy z pierwszej części dowodu, istnieją $j \in \beta(R)(p)$ oraz $K \in \mathbb{Z}$ takie, że $y = j + Kp \cdot 1$. Stąd $y^2 = j^2 + K^2p^2 \cdot 1 = j^2 + Kp \cdot y \in (\beta(R)(p))^2 + \langle y \rangle$. □

6.2 K_0-pierścienie

Przykład 6.8. Niech $n \in \mathbb{N}$, $p \in \mathbb{P}$ i niech N będzie przemiennym pierścieniem z prawie zerowym mnożeniem takim, że $pN = 0$ przy czym jeśli $n = 1$, to $N \neq 0$. Wtedy N jest $\mathbb{Z}_{p^n}$-algebrą przy naturalnym działaniu zewnętrznym

$$k \circ a = ka \text{ dla } k \in \mathbb{Z}_{p^n}, a \in N.$$

Jest jasne, że $S = \mathbb{Z}_{p^n} \boxplus N$ jest pierścieniem przemiennym. Ponadto $\mathcal{N}(S) = p\langle 1 \rangle + N \neq 0$ oraz $S/\mathcal{N}(S) \cong \mathbb{Z}_p$. Na podstawie Wniosku 4.11, pierścień $\mathbb{Z} \boxplus N$ jest filialny. Standardowe sprawdzenie pokazuje, że przekształcenie $f\colon \mathbb{Z} \boxplus N \to S$ dane wzorem $f((k, x)) = (k \cdot 1, x)$ dla $k \in \mathbb{Z}$, $x \in N$ jest homomorfizmem pierścienia $\mathbb{Z} \boxplus N$ na pierścień S. Zatem S jest pierścieniem filialnym.

Zauważmy, że przekształcenie $f\colon \mathbb{Z}_{p^n} \boxplus N \to \mathbb{Z}_p \boxplus N$ dane wzorem $f((k, a)) = (k \cdot 1, a)$ jest epimorfizmem pierścieni o jądrze $\langle p(1, 0) \rangle$. Zatem

$$(\mathbb{Z}_{p^n} \boxplus N)/\langle p(1, 0) \rangle \cong \mathbb{Z}_p \boxplus N. \tag{6.1}$$

Załóżmy, że $m \in \mathbb{N}$ oraz M jest przemiennym pierścieniem z prawie zerowym mnożeniem takim, że $pM = 0$. Wykażemy, że $\mathbb{Z}_{p^n} \boxplus N \cong \mathbb{Z}_{p^m} \boxplus M$, wtedy i tylko wtedy, gdy $n = m$ oraz $N \cong M$. Załóżmy najpierw, że $\mathbb{Z}_{p^n} \boxplus N \cong \mathbb{Z}_{p^m} \boxplus M$. Wtedy $o((1, 0))$ w grupie $\mathbb{Z}_{p^n} \boxplus N^+$ jest równy $o((1, 0))$ w grupie $\mathbb{Z}_{p^m} \boxplus M^+$, skąd $m = n$. Załóżmy, że $n = m = 1$. Wówczas $\mathcal{N}(\mathbb{Z}_p \boxplus N) \cong \mathcal{N}(\mathbb{Z}_p \boxplus M)$ skąd $M \cong N$. Jeśli zaś $n \geq 2$, to z formuły (6.1) i tego, że $(\mathbb{Z}_{p^n} \boxplus N)/\langle p(1, 0) \rangle \cong (\mathbb{Z}_{p^m} \boxplus M)/\langle p(1, 0) \rangle$ wynika, że $\mathbb{Z}_p \boxplus N \cong \mathbb{Z}_p \boxplus M$, a więc także $N \cong M$.

Na odwrót, jeżeli $g\colon N \to M$ jest izomorfizmem pierścieni i $n = m$, to łatwo wykazać, że przekształcenie $G\colon \mathbb{Z}_{p^n} \boxplus N \to \mathbb{Z}_{p^m} \boxplus M$ dane wzorem $G((k, a)) = (k, g(a))$ jest izomorfizmem pierścieni.

Definicja 6.9. Będziemy mówili, że pierścień R jest **K_0-pierścieniem**, jeżeli R jest przemiennym, filialnym pierścieniem z jedynką takim, że $\mathcal{N}(R) \neq 0$ oraz $R/\mathcal{N}(R)$ jest ciałem.

Lemat 6.10. *Każdy K_0 pierścień R jest $\mathbb{S}$-półprosty.*

Dowód. Załóżmy, że $\mathbb{S}(R) \neq 0$. Wówczas mamy, że $\mathcal{N}(R) \cap \mathbb{S}(R) = 0$ oraz $(\mathcal{N}(R) \oplus \mathbb{S}(R))/\mathcal{N}(R)$ jest niezerowym ideałem w ciele $R/\mathcal{N}(R)$. Stąd mamy $\mathcal{N}(R) \oplus \mathbb{S}(R) = R$. Ale R ma jedynkę, więc $\mathcal{N}(R)$ też ma jedynkę, co przeczy temu, że $\mathcal{N}(R) \neq 0$. □

Następujące Twierdzenie daje pewną charakteryzację K_0-pierścieni.

Twierdzenie 6.11. *Dla dowolnego pierścienia R następujące warunki są równoważne:*

(i) R jest K_0-pierścieniem,

(ii) istnieje przemienny pierścień N z prawie zerowym mnożeniem, $N \lhd R$ taki, że $pN = 0$ dla pewnego $p \in \mathbb{P}$ oraz $R = \langle 1 \rangle + N$, $o(1) = p^m$ w grupie R^+ i jeśli $m = 1$, to $N \neq 0$.

Dowód. $(i) \Rightarrow (ii)$. Z założenia wynika, że istnieje $0 \neq x \in \mathcal{N}(R)$ taki, że $x^2 = 0$. Na mocy Twierdzenia 1.35, $\mathcal{N}(R)$ jest H-pierścieniem i $[x] = \langle x \rangle$. Stąd $\langle x \rangle \lhd \mathcal{N}(R)$, ale $\mathcal{N}(R) \lhd R$, więc z filialności R mamy, że $\langle x \rangle \lhd R$. Weźmy dowolne $a \in R$. Wtedy istnieje $k \in \mathbb{Z}$ takie, że $ax = kx$, skąd $(a - k \cdot 1)x = 0$, czyli $a - k \cdot 1 \in l_R(x)$. Zatem

$$R = \langle 1 \rangle + l_R(x). \tag{6.2}$$

Teraz pokażemy, że $l_R(x) \subseteq \mathcal{N}(R)$. Załóżmy, że tak nie jest. Wtedy istnieje $y \in l_R(x) \setminus \mathcal{N}(R)$. Ponieważ $R/\mathcal{N}(R)$ jest ciałem, więc istnieje $z \in R$ takie, że $1 - zy = b \in \mathcal{N}(R)$. Stąd $x = bx$. Ale $\mathcal{N}(R)$ jest nil-pierścieniem, więc $x = 0$, sprzeczność. Zatem $l_R(x) \subseteq \mathcal{N}(R)$ i wobec (6.2),

$$R = \langle 1 \rangle + \mathcal{N}(R). \tag{6.3}$$

Stąd $R/\mathcal{N}(R) \cong \langle 1 \rangle / (\langle 1 \rangle \cap \mathcal{N}(R))$. Ale $R/\mathcal{N}(R)$ jest ciałem, więc istnieje liczba pierwsza p taka, że $(\langle 1 \rangle / \langle 1 \rangle \cap \mathcal{N}(R)) \cong \mathbb{Z}_p$. Stąd $R/\mathcal{N}(R) \cong \mathbb{Z}_p$. Ponadto $p \cdot 1 \in \mathcal{N}(R)$, więc istnieje najmniejsze $m \in \mathbb{N}$ takie, że $(p \cdot 1)^m = 0$. Wtedy $o(1) = p^m$ w grupie R^+ oraz $p^m R = 0$ i R jest p-pierścieniem.

Z Lematu 6.7, Stwierdzenia 2.12 punkt (ii) i wzoru (6.3) wynika, że wystarczy przyjąć $N = \mathcal{N}(R)(p)$.

$(ii) \Rightarrow (i)$. Na podstawie Przykładu 6.8, $\mathbb{Z}_{p^m} \boxplus N$ jest przemiennym pierścieniem filialnym. Zauważmy, że $f \colon \mathbb{Z}_{p^m} \boxplus N \to R$ dane wzorem $f((k, a)) = k \cdot 1 + a$ jest epimorfizmem pierścieni. Zatem pierścień R jest filialny. Ponadto $\mathcal{N}(R) = p\langle 1 \rangle + N \neq 0$ i $R/\mathcal{N}(R) \cong \mathbb{Z}_p$. □

Przykład 6.12. Niech $C = \mathbb{Z}_p \times_1 \mathbb{Z}_p$. Wówczas C jest $\mathbb{Z}_p$-algebrą z bazą $\{x, x^2\}$, gdzie $x^3 = 0$. Niech $m \geq 2$ będzie dowolną liczbą naturalną i $t_0 \in \mathbb{Z}_p \setminus \{0\}$. Niech P będzie $\mathbb{Z}_{p^m}$-algebrą generowaną przez elementy $1, x$ i relacje $px = 0, x^2 = t_0 p^{m-1} \cdot 1$ (dalej element $t_0 p^{m-1} \cdot 1$ będziemy oznaczali krótko przez $t_0 p^{m-1}$). Wówczas pierścień P jest skończony oraz

$$P \cong \mathbb{Z}_{p^m}[X]/(pX, X^2 - t_0 p^{m-1}).$$

Ponadto każdy element z P można jednoznacznie zapisać w postaci $k + lx$, gdzie $k \in \mathbb{Z}_{p^m}$, $l \in \mathbb{Z}_p$. Zauważamy dalej, że

$$P \cong (\mathbb{Z}_{p^m} \boxplus C)/\langle (-p^{m-1} t_0, x^2) \rangle$$

Na mocy Przykładu 6.8, pierścień $\mathbb{Z}_{p^m} \boxplus C$ jest filialny, i w konsekwencji pierścień P jest też filialny jako jego obraz homomorficzny.

Niech B będzie niezerową $\mathbb{Z}_p$-algebrą taką, że $B^2 = 0$. Wówczas B jest P-algebrą przy działaniu zewnętrznym

$$(k + lx) \circ b = kb \text{ dla } k \in \mathbb{Z}_{p^m}, l \in \mathbb{Z}_p, b \in B.$$

Można pokazać, że

$$P \boxplus B \cong ((\mathbb{Z}_{p^m} \boxplus C) \oplus B)/\langle((-p^{m-1}t_0, x^2), 0)\rangle.$$

Na mocy Twierdzenia 6.11 pierścień $P \boxplus B$ jest K_0-pierścieniem. Ponadto każdy element z $P \boxplus B$ można jednoznacznie zapisać w postaci $k + lx + b$, gdzie $k \in \mathbb{Z}_{p^m}$, $l \in \mathbb{Z}_p$, $b \in B$.

Niech C' będzie $\mathbb{Z}_p$-algebrą z bazą $\{y, y^2\}$, gdzie $y^3 = 0$ i niech $m' \geq 2$ będzie dowolną liczbą naturalną, $s_0 \in \mathbb{Z}_p \setminus \{0\}$. Niech P' będzie $\mathbb{Z}_{p^{m'}}$-algebrą generowaną przez elementy $1, y$ i relacje $py = 0, y^2 = s_0 p^{m'-1} \cdot 1$. Niech B' będzie $\mathbb{Z}_p$-algebrą taką, że $B'^2 = 0$. Załóżmy, że $f\colon P \boxplus B \to P' \boxplus B'$ jest izomorfizmem pierścieni. Wtedy $f(1) = 1$, skąd $m = m'$. Dalej, $f(x) = k + ly + b$ dla pewnych $k \in \mathbb{Z}_{p^m}$, $l \in \mathbb{Z}$, $b \in B'$. Ponieważ $px = 0$, więc $p \cdot f(x) = 0$ i wobec tego $pk = 0$. Zatem $k = k_0 p^{m-1}$ dla pewnego $k_0 \in \mathbb{Z}_p$ oraz

$$f(x) = k_0 p^{m-1} \cdot 1 + ly + b.$$

Ponadto $(f(x))^2 = f(x^2) = f(t_0 p^{m-1} \cdot 1) = t_0 p^{m-1} f(1) = t_0 p^{m-1} \cdot 1$, więc

$$(k_0 p^{m-1} \cdot 1 + ly + b)^2 = t_0 p^{m-1} \cdot 1.$$

Zatem $l^2 y^2 = t_0 p^{m-1} \cdot 1$, czyli $l^2 s_0 p^{m-1} \cdot 1 = t_0 p^{m-1} \cdot 1$, skąd $l^2 s_0 \equiv t_0 \pmod{p}$. Zauważmy, że $(P \boxplus B)(p) = [x] \oplus B$, oraz $(P' \boxplus B')(p) = [y] \oplus B'$. Zatem $f([x] \oplus B) = [y] \oplus B'$. Dalej, $a([x] \oplus B) = \langle x^2 \rangle \oplus B$ oraz $a([y] \oplus B') = \langle y^2 \rangle \oplus B'$, więc $\langle x^2 \rangle \oplus B \cong \langle y^2 \rangle \oplus B'$. Stąd $\dim_{\mathbb{Z}_p} B' = \dim_{\mathbb{Z}_p} B$ i wobec tego $B \cong B'$.

Na odwrót, niech $m = m'$ i $l^2 s_0 \equiv t_0 \pmod{p}$ dla pewnego $l \in \mathbb{Z}_p \setminus \{0\}$ i niech $g\colon B \to B'$ będzie izomorfizmem pierścieni. Określamy $f\colon P \boxplus B \to P' \boxplus B'$ wzorem

$$f(k_1 + k_2 x + b) = k_1 + lk_2 y + g(b).$$

Jest jasne, że f jest izomorfizmem grup addytywnych. Proste sprawdzenie pokazuje, że f jest homomorfizmem pierścieni. Zatem $P \boxplus B \cong P' \boxplus B'$.

Z powyższych rozważań wynika, że dla ustalonych $m \geq 2$ i B oraz $p > 2$ istnieją dokładnie dwa z dokładnością do izomorfizmu takie pierścienie $P \boxplus B$. Jeden z nich otrzymujemy dla $t_0 = 1$ natomiast drugi dla dowolnej niereszty kwadratowej t_0 modulo p.

Przykład 6.13. Niech p będzie nieparzystą liczbą pierwszą i niech $C = (\mathbb{Z}_p \times \mathbb{Z}_p)_{0,0,\alpha} \times_1 \mathbb{Z}_p$ będzie skończoną $\mathbb{Z}_p$-algebrą z bazą $\{x, x^2, y\}$ gdzie $xy = yx = 0, x^3 = 0, y^2 = \alpha x^2$ oraz $-\alpha$ jest niereszą kwadratową modulo p. Niech $m \geq 2$, $t_0 \in \mathbb{Z}_p \setminus \{0\}$ i niech P będzie $\mathbb{Z}_{p^m}$-algebrą generowaną przez elementy $1, x, y$ takie, że $xy = yx = px = py = 0, x^2 = t_0 p^{m-1} \cdot 1, y^2 = \alpha x^2$. Wówczas

$$P \cong \mathbb{Z}_{p^m}[X, Y]/(XY, pX, pY, X^2 - t_0 p^{m-1}, Y^2 - \alpha X^2).$$

Zauważamy, że każdy element z P możemy jednoznacznie zapisać w postaci $k \cdot 1 + l_1 x + l_2 y$, gdzie $k \in \mathbb{Z}_{p^m}$, $l_1, l_2 \in \mathbb{Z}_p$. Ponadto

$$P \cong (\mathbb{Z}_{p^m} \boxplus C)/\langle(-p^{m-1}t_0, x^2)\rangle.$$

Na podstawie Przykładu 6.8 pierścień P jest filialny.

Niech C' będzie $\mathbb{Z}_p$-algebrą z bazą $\{x_1, y_1, x_1^2\}$, gdzie $x_1y_1 = y_1x_1 = 0, x_1^3 = 0, y_1^2 = \beta x_1^2$ dla pewnej niereszty kwadratowej $-\beta$ modulo p. Niech $s_0 \in \mathbb{Z}_p \setminus \{0\}$ i niech P' będzie $\mathbb{Z}_{p^{m'}}$-algebrą generowaną przez elementy $1, x_1, y_1$ takie, że $x_1y_1 = y_1x_1 = px_1 = py_1 = 0, x_1^2 = s_0p^{m-1} \cdot 1, y_1^2 = \beta x_1^2$.

Wówczas istnieje niezerowe $\gamma \in \mathbb{Z}_p$ takie, że $\beta = \gamma^2\alpha$, gdyż $-\alpha$ i $-\beta$ są nieresztami kwadratowymi. Z teori liczb wiadomo, że $\{u^2 + v^2\Delta \,:\, u, v \in \mathbb{Z}_p\} = \mathbb{Z}_p$ dla dowolnego niezerowego $\Delta \in \mathbb{Z}_p$. Istnieją zatem $l_1, k_1 \in \mathbb{Z}_p$ takie, że $t_0 \equiv s_0(l_1^2 + k_1^2\gamma^2\alpha) \pmod p$. Ponadto istnieje $\gamma' \in \mathbb{Z}_p$ takie, że $\gamma \cdot \gamma' \equiv 1 \pmod p$. Niech dalej $l_2 = -\alpha\gamma k_1$, $k_2 = \gamma' l_1$. Określmy funkcję $f\colon P \to P'$ wzorem

$$f(U \cdot 1 + Vx + Wy) = U \cdot 1 + (Vl_1 + Wl_2)x_1 + (Vk_1 + Wk_2)y_1, \tag{6.4}$$

gdzie $U \in \mathbb{Z}_{p^m}$, $V, W \in \mathbb{Z}_p$. Można sprawdzić, że tak określona funkcja jest izomorfizmem pierścieni.

Niech B będzie $\mathbb{Z}_p$-algebrą taką, że $B^2 = 0$. Wówczas B jest P-algebrą przy działaniu zewnętrznym

$$(k + l_1x + l_2y) \circ b = kb \text{ dla } k \in \mathbb{Z}_{p^m}, l_1, l_2 \in \mathbb{Z}_p, b \in B.$$

Można pokazać, że

$$P \boxplus B \cong ((\mathbb{Z}_{p^m} \boxplus C) \oplus B)/\langle((-p^{m-1}t_0, x^2), 0)\rangle.$$

Na mocy Twierdzenia 6.11 pierścień $P \boxplus B$ jest K_0-pierścieniem. Ponadto każdy element z $P \boxplus B$ można jednoznacznie zapisać w postaci $k + l_1x + l_2y + b$, gdzie $k \in \mathbb{Z}_{p^m}$, $l_1, l_2 \in \mathbb{Z}_p$, $b \in B$.

Niech B' będzie $\mathbb{Z}_p$-algebrą z zerowym mnożeniem. Załóżmy, że $f\colon P \boxplus B \to P' \boxplus B'$ jest izomorfizmem pierścieni. Wtedy $f(1) = 1$, skąd $m = m'$. Zauważmy, że $(P \boxplus B)(p) = [x, y] \oplus B$, oraz $(P' \boxplus B')(p) = [x_1, y_1] \oplus B'$. Zatem $f([x, y] \oplus B) = [x_1, y_1] \oplus B'$. Dalej, $a([x, y] \oplus B) = \langle x^2\rangle \oplus B$ oraz $a([x_1, y_1] \oplus B') = \langle x_1^2\rangle \oplus B'$, więc $\langle x^2\rangle \oplus B \cong \langle x_1^2\rangle \oplus B'$. Stąd $\dim_{\mathbb{Z}_p} B' = \dim_{\mathbb{Z}_p} B$ i wobec tego $B \cong B'$.

Na odwrót, niech $m = m'$ i niech $g\colon B \to B'$ będzie izomorfizmem pierścieni. Określamy $F\colon P \boxplus B \to P' \boxplus B'$ wzorem

$$F(r + b) = f(r) + g(b) \text{ dla } r \in P,\ b \in B,$$

gdzie f jest jak we wzorze (6.4). Łatwo sprawdzić, że f jest izomorfizmem pierścieni. Zatem $P \boxplus B \cong P' \boxplus B'$.

Z powyższych rozważań wynika, że dla ustalonych $m \geq 2$ i B istnieje dokładnie jeden, z dokładnością do izomorfizmu, pierścień $P \boxplus B$. Otrzymujemy go biorąc np. $t_0 = 1$.

Twierdzenie 6.14. *Wszystkimi z dokładnością do izomorfizmu K_0-pierścieniami są pierścienie opisane w przykładach 6.8, 6.12, 6.13.*

Dowód. Niech R będzie K_0-pierścieniem. Wtedy na podstawie Twierdzenia 6.11, istnieje przemienny pierścień N z prawie zerowym mnożeniem, $N \lhd R$ taki, że $pN = 0$ dla pewnego $p \in \mathbb{P}$ oraz $R = \langle 1 \rangle + N$, $o(1) = p^m$ w grupie R^+ i jeśli $m = 1$, to $N \neq 0$. Ponieważ $o(1) = p^m$ i $pN = 0$, więc $\langle 1 \rangle \cap N = 0$ lub $\langle 1 \rangle \cap N = \langle p^{m-1} \cdot 1 \rangle \neq 0$ i $m \geq 2$. Jeśli $\langle 1 \rangle \cap N = 0$, to $R \cong \mathbb{Z}_{p^m} \boxplus N$, czyli R jest taki jak w Przykładzie 6.8.

Niech dalej $\langle 1 \rangle \cap N = \langle p^{m-1} \cdot 1 \rangle$. Na podstawie Wniosku 2.38 mamy, że $N = B \oplus C$, gdzie $B^2 = 0$, $pB = 0$ oraz $C = 0$ lub $C \cong \mathbb{Z}_p \times_1 \mathbb{Z}_p$ lub $C \cong (\mathbb{Z} \times \mathbb{Z})_{0,0,A} \times_1 \mathbb{Z}$ dla pewnej niereszty kwadratowej $-A$ modulo p. Skąd $p^{m-1} \cdot 1 = b_0 + c_0$ dla pewnych $b_0 \in B$, $c_0 \in C$.

Załóżmy najpierw, że $b_0 \neq 0$. Wtedy $B = \langle b_0 \rangle \oplus B_1$ dla pewnej podgrupy B_1 w B^+. Oznaczmy $N_0 = B_1 \oplus C$. Udowodnimy, że wówczas $R^+ = \langle 1 \rangle^+ \oplus N_0^+$. Jeżeli $\langle 1 \rangle \cap N_0 \neq 0$, to $b_0 + c_0 \in B_1 \oplus C$, stąd $b_0 \in B_1$, więc $b_0 \in B_1 \cap \langle b_0 \rangle = 0$, sprzeczność. Zatem $\langle 1 \rangle \cap N_0 = 0$. Ponadto $b_0 = p^{m-1} \cdot 1 - c_0 \in \langle 1 \rangle + N_0$, więc $R^+ = \langle 1 \rangle^+ \oplus N_0^+$. Zatem $R \cong \mathbb{Z}_{p^m} \boxplus N_0$, czyli R jest taki jak w Przykładzie 6.8.

Teraz załóżmy, że $b_0 = 0$, tzn. $p^{m-1} \cdot 1 \in C$. Zatem $C \neq 0$, więc C jest $\mathbb{Z}_p$-algebrą z bazą $\{x, x^2\}$, gdzie $x^3 = 0$ lub z bazą $\{x, y, x^2\}$, gdzie $xy = yx = x^3 = 0$, $y^2 = \alpha x^2$ dla pewnej niereszty kwadratowej $\alpha \in \mathbb{Z}_p$. W obu przypadkach $a(C) = \langle x^2 \rangle$ i $p^{m-1} \cdot 1 \in a(C)$, więc istnieje $t_0 \in \mathbb{Z}_p \setminus \{0\}$ takie, że $x^2 = t_0 p^{m-1} \cdot 1$. Dalej, $R = (\langle 1 \rangle + C) + B$. Ponadto $(\langle 1 \rangle + C) \cap B = 0$. Rzeczywiście, weźmy $c \in C$, $b \in B$, $k \in \mathbb{Z}$ takie, że $k \cdot 1 + c = b$. Wtedy $k \cdot 1 \in \langle 1 \rangle \cap N \subseteq C$, więc $b - c \in C$, stąd $b \in B \cap C$, więc $b = 0$ oraz $(\langle 1 \rangle + C) \cap B = 0$. Zatem $R = (\langle 1 \rangle + C) \oplus B$. Niech $P = \langle 1 \rangle + C$. Jeżeli bazą C jest $\{x, x^2\}$, to $R \cong P \boxplus B$ i R jest jak Przykładzie 6.12. Jeśli zaś bazą C jest $\{x, y, x^2\}$, to $R \cong P \boxplus B$ i R jest jak w Przykładzie 6.13.

Na odwrót, jeśli pierścień R jest izomorficzny z pierścieniem opisanym w Przykładach 6.8, 6.12, 6.13, to R jest K_0-pierścieniem. Załóżmy, że pewien pierścień R opisany w Przykładzie 6.12 jest izomorficzny z pierścieniem R_1 opisanym w Przykładzie 6.13. Niech $f \colon R \to R_1$ będzie izomorfizmem pierścieni. Wówczas $f(1) = 1$, więc $p^m = p_1^{m_1}$, skąd $p = p_1$ i $m = m_1$. Ponadto $R(p) = B \oplus C$ i $R_1(p) = B_1 \oplus C_1$, więc $f(B \oplus C) = B_1 \oplus C_1$. Zatem $f(a(B \oplus C)) = a(B_1 \oplus C_1)$, więc $f(B \oplus a(C)) = B_1 \oplus a(C_1)$. Wobec tego $C/a(C) \cong C_1/a(C_1)$. Ale $\dim_{\mathbb{Z}_p} C/a(C) = 1$ i $\dim_{\mathbb{Z}_p} C_1/a(C_1) = 2$, więc mamy sprzeczność.

Pozostaje jeszcze wykazać, że dowolny pierścień $R \cong \mathbb{Z}_{p^m} \boxplus N$ opisany w Przykładzie 6.8 nie jest izomorficzny z żadnym z pierścieni opisanych w Przykładach 6.12, 6.13. Załóżmy, że tak nie jest. Wówczas $R^+ = \langle 1 \rangle^+ \oplus N^+$ oraz $R = \langle 1 \rangle + (B \oplus C)$, gdzie $m \geq 2$ i B jest taki, że $B^2 = 0$ oraz C jest $\mathbb{Z}_p$-algebrą z bazą $\{x, x^2\}$, gdzie $x^3 = 0$ lub z bazą $\{x, y, x^2\}$, gdzie $xy = yx = x^3 = 0$, $y^2 = \alpha x^2$ dla pewnej niereszty kwadratowej $\alpha \in \mathbb{Z}_p$. Stąd $|R| \geq p^{m+1}$, gdyż C nie zawiera się w $\langle 1 \rangle$ i wobec tego $N \neq 0$. Ponadto $N \subseteq R(p) = C \oplus B$. Ale $\langle 1 \rangle \oplus N = R$, więc z prawa modularności dla podgrup w R^+ mamy $(\langle 1 \rangle \cap (C \oplus B)) \oplus N = C \oplus B$, czyli $\langle p^{m-1} \cdot 1 \rangle \oplus N = C \oplus B$. Ponadto $\langle p^{m-1} \cdot 1 \rangle = C^2 = a(C)$, więc $C^2 \oplus N = C \oplus B$. Ponownie z modularności kraty podgrup R^+ otrzymujemy $C^2 \oplus (N \cap C) = C$, przy czym $N \cap C \lhd C$. Sprzeczność, gdyż na podstawie Twierdzeń 2.31 oraz 2.37, C nie rozkłada się na sumę prostą swoich dwóch niezerowych ideałów. $\square$

6.3 Twierdzenie klasyfikacyjne dla torsyjnych pierścieni filialnych

Uwaga 6.15. Niech C będzie K_0-p-pierścieniem i niech S będzie przemiennym p-pierścieniem silnie regularnym. Pokażemy, że strukturę unitarnej C-algebry na pierścieniu S można zadać na dokładnie jeden sposób. Mianowicie, na podstawie Twierdzenia 6.11, $C = \langle 1\rangle + \mathcal{N}(C)$ oraz $p\cdot 1 \in \mathcal{N}(C)$. Stąd dla $k \in \mathbb{Z}$ mamy $k\cdot 1 \in \mathcal{N}(C) \iff p \mid k$. Dlatego działanie zewnętrzne dane wzorem

$$(k \cdot 1 + x) \circ s = ks, \quad \text{dla } k \in \mathbb{Z}, x \in \mathcal{N}(C), s \in S$$

jest dobrze określone. Proste sprawdzenie pokazuje, że przy tym działaniu S jest unitarną C-algebrą.

Załóżmy, że S jest unitarną C-algebrą przy działaniu zewnętrznym $*$. Wtedy dla dowolnych $k \in \mathbb{Z}, x \in \mathcal{N}(C), s \in S$, $(k \cdot 1 + x) * s = ks + x * s$. Ale $x^n = 0$ dla pewnego $n \in \mathbb{N}$, skąd $(x*s)^n = 0$ i wobec tego $x*s = 0$, bo pierścień S jest zredukowany. Zatem $* = \circ$.

Ponieważ, $S \lhd C \boxplus S$ oraz $(C \boxplus S)/S \cong C$, więc na mocy Lematu 6.10, $\mathbb{S}(C \boxplus S) = S$.

Twierdzenie 6.16. *Pierścień R jest przemiennym torsyjnym pierścieniem filialnym wtedy i tylko wtedy, gdy $R = \bigoplus_{p\in\mathbb{P}} R_p$ oraz każde R_p jest jednym z poniższych pierścieni:*

(i) $S \oplus N$, gdzie N jest przemiennym nil-H-p-pierścieniem oraz S jest przemiennym p-pierścieniem silnie regularnym,

(ii) $(C \boxplus S) \oplus S_1$, gdzie S i S_1 są przemiennymi p-pierścieniami silnie regularnymi i p-pierścień C jest K_0-pierścieniem.

Dowód. Każdy pierścień torsyjny R można zapisać w postaci $R = \bigoplus_{p\in\mathbb{P}} R_p$, przy czym każdy ze składników tej sumy jest wyznaczony jednoznacznie. Ze Stwierdzenia 1.28 otrzymujemy, że R jest filialny wtedy i tylko wtedy, gdy R_p jest filialny dla każdego $p \in \mathbb{P}$. Wobec tego wystarczy udowodnić nasze twierdzenie w przypadku, gdy R jest przemiennym p-pierścieniem.

Załóżmy, że pierścień R jest filialny. Wówczas z Twierdzenia 1.35 wynika, że $\mathcal{N}(R)$ jest H-p-pierścieniem. Ponadto p-pierścień $R/\mathcal{N}(R)$ jest filialny i zredukowany. Zatem na mocy Twierdzenia 1.38 otrzymujemy, że $R/\mathcal{N}(R) \in \mathbb{S}$. Jeśli zatem $R = \mathcal{N}(R)$ lub $\mathcal{N}(R) = 0$, to R jest taki jak w punkcie (i).

Niech dalej $0 \neq \mathcal{N}(R) \neq R$. Jeśli grupa $\mathcal{N}(R)^+$ nie jest ograniczonego wykładnika, to z Lematu 6.5 otrzymujemy, że $R = \mathbb{S}(R) \oplus \mathcal{N}(R)$.

Załóżmy więc, że grupa $\mathcal{N}(R)^+$ jest ograniczonego wykładnika. Wtedy ponieważ, $p(R/\mathcal{N}(R)) = 0$, więc $p^m R = 0$, dla pewnego $m \in \mathbb{N}$. Załóżmy, że $R \neq \mathbb{S}(R) \oplus \mathcal{N}(R)$. Wtedy na podstawie Lematu 6.3, istnieje idempotent $e \in R \setminus (\mathbb{S}(R) + \mathcal{N}(R))$ taki, że $\mathcal{N}(R) \subseteq eR$ oraz $R = eR \oplus l_R(e)$, przy czym $l_R(e) \in \mathbb{S}$. Stąd eR jest przemiennym filialnym pierścieniem z jedynką e oraz $\mathcal{N}(eR) = \mathcal{N}(R)$ i $p^m(eR) = 0$. Ponadto $(eR)/\mathcal{N}(R) \in \mathbb{S}$. Na mocy Lematu 6.6, $eR = \langle e\rangle + \mathbb{S}(eR) + \mathcal{N}(R)$. Oznaczmy $C = \langle e\rangle + \mathcal{N}(R)$ i $N = (\mathcal{N}(R))(p)$. Wtedy, na podstawie Lematu 6.7, $\mathcal{N}(R) = N + p\langle e\rangle$

i $C = \langle e \rangle + N$. Zgodnie z Twierdzeniem 6.11, C jest K_0-pierścieniem. Na mocy Lematu 6.10, $C \cap \mathbb{S}(eR) = 0$. Zatem eR jest sumą prostą podpierścieni C i $\mathbb{S}(eR)$. Ponadto dla $k \in \mathbb{Z}$ oraz $x \in N$, $s \in \mathbb{S}(eR)$ mamy, że $(ke+x)\cdot s = (ke)s$, więc $\mathbb{S}(eR)$ jest w naturalny sposób C-algebrą. Wobec tego $eR \cong C \boxplus \mathbb{S}(eR)$ i ostatecznie $R \cong (C \boxplus \mathbb{S}(eR)) \oplus l_R(e)$.

Na odwrót. Jeżeli $R \cong S \oplus N$, gdzie N jest nil-H-p-pierścieniem oraz S p-pierścieniem silnie regularnym, to ze Stwierdzenia 1.36 wynika, że R jest filialny.

Niech teraz $R \cong (C \boxplus S) \oplus S_1$, gdzie S i S_1 są p-pierścieniami silnie regularnymi i p-pierścień C jest K_0-pierścieniem. Ponieważ R jest rozszerzeniem pierścienia $C \boxplus S$ przez S_1 więc ze Stwierdzenia 1.36 wystarczy wykazać, że pierścień $C \boxplus S$ jest filialny. Ale $C \boxplus S$ jest rozszerzeniem silnie regularnego pierścienia S przez pierścień filialny C, więc ze Stwierdzenia 1.36 wynika, że pierścień $C \boxplus S$ jest filialny. □

Uwaga 6.17. Nietrudno jest zauważyć, że pierścienie S i N występujące w punkcie (i) Twierdzenia 6.16 są wyznaczone jednoznacznie z dokładnością do izomorfizmu przez pierścień $A = S \oplus N$, gdyż $S = \mathbb{S}(A)$ oraz $N = \mathcal{N}(A)$. Ponadto, $A/\mathbb{S}(A)$ jest nil-pierścieniem, zaś jeżeli T jest pierścieniem z punktu (ii) Twierdzenia 6.16, to $T/\mathbb{S}(T)$ jest niezerowym pierścieniem z jedynką jako K_0-pierścień. Wobec tego $A \ncong T$.

Niestety w przypadku pierścieni C, S_1 i S_2 występujących w punkcie (ii) Twierdzenia 6.16 kwestia jednoznaczności nie jest sprawą prostą. Mianowicie, jeśli np. pierścień S_1 ma jedynkę, to $C \boxplus S_1 \cong C \oplus S_1$ i wtedy $(C \boxplus S_1) \oplus S_2 \cong C \oplus (S_1 \oplus S_2) = A$. W tym przypadku jedynie pierścienie $N = \mathcal{N}(A)$ i $S_1 \oplus S_2 = \mathbb{S}(A)$ są jednoznacznie wyznaczone z dokładnością do izomorfizmu przez pierścień A.

Z Twierdzenia 6.16 otrzymujemy natychmiast następujący wniosek.

Wniosek 6.18. *Pierścień R jest przemiennym torsyjnym pierścieniem filialnym z jedynką wtedy i tylko wtedy, gdy $R = \bigoplus_{p\in\Pi} R_p$, gdzie Π jest skończonym podzbiorem w $\mathbb{P}$ oraz każde R_p jest jednym z poniższych pierścieni:*

(i) przemiennym p-pierścieniem silnie regularnym z jedynką,

(ii) $(C \boxplus S) \oplus S_1$, gdzie S i S_1 są przemiennymi p-pierścieniami silnie regularnymi, przy czym S_1 jest pierścieniem z jedynką i p-pierścień C jest K_0-pierścieniem.

Rozdział 7

Przemienne noetherowskie pierścienie filialne

7.1 Klasyfikacja noetherowskich CRF-pierścieni

Twierdzenie 7.1. *Dla dowolnego pierścienia R z jedynką następujące warunki są równoważne:*

(i) R jest noetherowskim $\mathbb{S}$-półprostym CRF-pierścieniem,

(ii) $R \cong \bigoplus_{i=1}^{n} D_i$, gdzie D_i jest filialną dziedziną całkowitości charakterystyki zero, która nie jest ciałem dla każdego $i \in \{1, 2, \ldots, n\}$ oraz $\Pi(D_i) \cap \Pi(D_j) = \emptyset$ dla $i \neq j$.

Dowód. $(i) \Rightarrow (ii)$. Na podstawie Twierdzenia 3.20, istnieje niepusty podzbiór $\Pi \subseteq \mathbb{P}$ i silnie regularny podpierścień K w $\mathcal{Q}_\Pi$ z tą samą jedynką taki, że dla każdego $a \in K$, $a = (a_p)_{p\in\Pi}$ mamy $a_p \in \mathcal{Z}_p$ dla prawie wszystkich $p \in \Pi$ oraz $R \cong K \cap \mathcal{Z}_\Pi$. Lemat 3.23 implikuje, że K jest pierścieniem noetherowskim. Z Lematu 3.22 otrzymujemy, że $\mathcal{B}_K$ jest artinowską algebrą Boole'a.

Istnieją zatem parami rozłączne atomy $\Pi_1, ..., \Pi_k \in \mathcal{B}_K$ takie, że $\Pi = \Pi_1 \cup \Pi_2 \cup \cdots \cup \Pi_k$. Standardowe rozumowanie i Lemat 3.22 pokazują, że $\mathbb{1}_{\Pi_1}, \mathbb{1}_{\Pi_2}, \ldots, \mathbb{1}_{\Pi_k} \in K$ są parami ortogonalnymi idempotentami i $1 = \mathbb{1}_{\Pi_1} + \mathbb{1}_{\Pi_2} + \cdots + \mathbb{1}_{\Pi_k}$. Ponieważ Π_i jest atomem, więc $\mathbb{1}_{\Pi_i}K$ jest dziedziną całkowitości. Ale $\mathbb{1}_{\Pi_i}K$ jest ideałem w pierścieniu silnie regularnym K, skąd $\mathbb{1}_{\Pi_i}K \in \mathbb{S}$. Zatem $\mathbb{1}_{\Pi_i}K$ jest ciałem. To pokazuje, że $K = \bigoplus_{i=1}^{k} \mathbb{1}_{\Pi_i}K$ i w konsekwencji $R \cong \bigoplus_{i=1}^{k}[(\mathbb{1}_{\Pi_i}K) \cap \mathcal{Z}_{\Pi_i}]$. Ponadto z Twierdzenia 3.1 wynika, że $D_i = (\mathbb{1}_{\Pi_i}K) \cap \mathcal{Z}_{\Pi_i}$ jest filialną dziedziną całkowitości charakterystyki zero oraz $\Pi(D_i) = \Pi_i$ dla $i \in \{1, 2, \ldots, k\}$.

$(ii) \Rightarrow (i)$. Z Twierdzenia 4.4 wynika, że R jest $\mathbb{S}$-półprostym CRF-pierścieniem. Na podstawie Twierdzenia 1.32, D_i jest dziedziną ideałów głównych, a więc i pierścieniem noetherowskim. Stąd pierścień R jest noetherowski.

□

W powyższym Twierdzeniu istotną rolę odgrywał fakt, że pierścień R posiadał jedynkę. Teraz pokażemy w jaki sposób opuścić to założenie.

Twierdzenie 7.2. *Dla dowolnego pierścienia R następujące warunki są równoważne:*

(i) R jest noetherowskim $\mathbb{S}$-półprostym CRF-pierścieniem,

(ii) $R \cong \bigoplus_{i=1}^{n} m_i D_i$, gdzie D_i jest filialną dziedziną całkowitości charakterystyki zero, która nie jest ciałem, $m_i \in \mathbb{N}$ dla każdego $i \in \{1, 2, \ldots, n\}$ oraz $\Pi(D_i) \cap \Pi(D_j) = \emptyset$ dla $i \neq j$.

Dowód. $(i) \Rightarrow (ii)$. Twierdzenie 3.15 pokazuje, że istnieje beztorsyjny CRF-pierścień S z jedynką taki, że R jest w nim istotnym ideałem. Ponieważ pierścień R jest noetherowski, więc $End(R_R)$ jest noetherowskim R-modułem. Ale z dowodu Twierdzenia 3.15, S jest R-podmodułem w $End(R_R)$, więc S jest noetherowskim R-modułem. Zatem S jest pierścieniem noetherowskim. Na podstawie Twierdzenia 7.1, $S \cong \bigoplus_{i=1}^{n} D_i$, gdzie D_i jest filialną dziedziną całkowitości charakterystyki zero, ale nie ciałem dla każdego $i \in \{1, 2, \ldots, n\}$ i $\Pi(D_i) \cap \Pi(D_j) = \emptyset$ dla $i \neq j$. Ponieważ R jest ideałem istotnym w S, więc $R \cong \bigoplus_{i=1}^{n} J_i$, gdzie J_i jest niezerowym ideałem w D_i. Z Twierdzenia 1.32 otrzymujemy, że $J_i \cong m_i D_i$, $m_i \in \mathbb{N}$ dla każdego $i \in \{1, 2, \ldots, n\}$. Ostatecznie $R \cong \bigoplus_{i=1}^{n} m_i D_i$.

$(ii) \Rightarrow (i)$. Z Twierdzenia 1.32 wynika, że D_i jest pierścieniem noetherowskim dla każdego $i \in \{1, 2, \ldots, n\}$. Z filialności D_i wynika, że $m_i D_i$ jest pierścieniem noetherowskim dla dowolnego $i \in \{1, 2, \ldots, n\}$. W konsekwencji R jest pierścieniem noetherowskim. Ponadto z Twierdzenia 4.4 wynika, że R jest $\mathbb{S}$-półprostym CRF-pierścieniem. □

Dalej przyjrzymy się strukturze dowolnych noetherowskich CRF-pierścieni. Jeżeli R jest noetherowskim CRF-pierścieniem takim, że $0 \neq \mathbb{S}(R)$, to $\mathbb{S}(R)$ jest pierścieniem noetherowskim z jedynką. Zatem $\mathbb{S}(R)$ wydziela się jako ideałowy składnik prosty z R i $R = \mathbb{S}(R) \oplus T$ dla pewnego $T \lhd R$. Ponieważ T spełnia wszystkie założenia Twierdzenia 7.2, więc jego struktura jest opisana i wystarczy zbadać pierścień $\mathbb{S}(R)$. Ale standardowe obliczenia pokazują, że każdy silnie regularny, noetherowski, CRF-pierścień jest skończoną sumą prostą ciał.

Z powyższych rozważań i Twierdzenia 7.2 natychmiast wynika następujące twierdzenie.

Twierdzenie 7.3. *Dla dowolnego pierścienia R następujące warunki są równoważne:*

(i) R jest noetherowskim CRF-pierścieniem,

(ii) $R \cong S \oplus \big(\bigoplus_{i=1}^{n} m_i D_i \big)$, gdzie D_i jest filialną dziedziną całkowitości charakterystyki zero, ale nie ciałem, $m_i \in \mathbb{N}$ dla każdego $i \in \{1, 2, \ldots, n\}$ i $\Pi(D_i) \cap \Pi(D_t) = \emptyset$ dla $i \neq t$ oraz S jest skończoną sumą prostą ciał.

Udowodnimy teraz analog Twierdzenia 7.3 dla skończenie generowanych $\mathbb{S}$-półprostych CRF-pierścieni. Wynik ten jest uprecyzyjnieniem Twierdzenia 2.4 z [13].

Twierdzenie 7.4. *Dla dowolnego pierścienia R następujące warunki są równoważne:*

(i) R jest skończenie generowanym CRF-pierścieniem,

(ii) $R \cong S \oplus mD$, *gdzie* $D = [\frac{1}{s}]$ *dla pewnych* $s, m \in \mathbb{N}$ *oraz* S *jest skończoną sumą prostą ciał skończonych.*

Dowód. $(i) \Rightarrow (ii)$. Ponieważ pierścień R jest noetherowski, więc na podstawie Twierdzenia 7.3, $R \cong \left(\bigoplus_{j=1}^{k} F_j\right) \oplus \left(\bigoplus_{i=1}^{n} m_i D_i\right)$, gdzie D_i jest filialną dziedziną całkowitości charakterystyki zero, ale nie ciałem, $m_i \in \mathbb{N}$ dla każdego $i \in \{1, 2, \ldots, n\}$ i $\Pi(D_i) \cap \Pi(D_t) = \emptyset$ dla $i \neq t$ oraz pierścień F_j jest ciałem dla każdego $j \in \{1, 2, \ldots, k\}$. Ponadto $m_i D_i$ jest obrazem homomorficznym pierścienia R. Stąd $m_i D_i$ jest skończenie generowany jako pierścień. Ale z filialności D_i, $D_i = m_i D_i + \langle 1 \rangle$, skąd D_i też jest pierścieniem skończenie generowanym. Z Twierdzenia 5.1 z [8] otrzymujemy, że D_i jest skończenie generowanym podpierścieniem $\mathbb{Q}$. Zatem $\mathbb{N} \setminus \Pi(D_i)$ jest zbiorem skończonym i pownieważ $\Pi(D_i) \cap \Pi(D_t) = \emptyset$ dla $i \neq t$, więc $n = 1$. Ponadto $D_1 = [\frac{1}{s}]$ dla pewnego $s \in \mathbb{N}$.

Każde ciało F_j jest także obrazem homomorficznym pierścienia R, skąd F_j jest pierścieniem skończenie generowanym i w konsekwencji, skończonym.

$(ii) \Rightarrow (i)$. Istnieje $k \in \mathbb{N}$ takie, że $NWD(k, s) = 1$ i $mD = k[\frac{1}{s}]$ (gdzie $k = \frac{m}{NWD(m,s)}$). Pokażemy, że $mD = [\frac{k}{s}]$. Oczywiście $[\frac{k}{s}] \subseteq k[\frac{1}{s}]$. Niech $a \in [\frac{1}{s}]$. Wtedy istnieją $l \in \mathbb{Z}$ oraz $t \in \mathbb{N}$ takie, że $a = \frac{l}{s^t}$. Ale $NWD(k, s) = 1$, więc istnieją $u, v \in \mathbb{Z}$ takie, że $k^{t-1}u + s^{t-1}v = 1$. Dalej $ka = (\frac{k}{s})^t lu + \frac{k}{s} lv \in [\frac{k}{s}]$ i w konsekwencji mD jest pierścieniem skończenie generowanym. Jest też jasne, że każde ciało F_j jest skończenie generowane. Stąd R jest pierścieniem skończenie generowanym. Ponadto mD jest CRF-pierścieniem i ze Stwierdzenia 1.36 wynika, że pierścień R jest filialny. □

7.2 Torsyjne noetherowskie pierścienie filialne

Następne twierdzenie wynika z Twierdzeń 2.31 oraz 2.37 i w pełni klasyfikuje noetherowskie, torsyjne pierścienie z prawie zerowym mnożeniem.

Twierdzenie 7.5. *Wszystkimi z dokładnością do izomorfizmu noetherowskimi, torsyjnymi pierścieniami z prawie zerowym mnożeniem są pierścienie postaci* $\bigoplus_{p \in \Pi} R_{(p)} \oplus C$, *gdzie* Π *jest skończonym podzbiorem w* $\mathbb{P}$, *dla każdego* $p \in \Pi$, $R_{(p)}$ *jest pierścieniem opisanym w punktach* $(i) - (ii)$ *Twierdzenia 2.31 lub pierścieniem opisanym w punktach* $(i) - (vi)$ *Twierdzenia 2.37, natomiast* C *jest skończonym pierścieniem z zerowym mnożeniem.*

Dobrze wiadomo, że wszystkimi z dokładnością do izomorfizmu niezerowymi, przemiennymi, noetherowskimi, silnie regularnymi, p-pierścieniami są skończone sumy proste ciał charakterystyki p. Z Lematu 2.14 wynika, że noetherowski nil-H-p-pierścień jest skończony. Ponadto z Twierdzenia 6.14 i Przykładów 6.8, 6.12, 6.13 wynika, że K_0-pierścień jest noetherowski wtedy i tylko wtedy, gdy jest skończony. Stąd, z Twierdzenia 6.16 i z Uwagi 6.17 mamy następujący wniosek.

Wniosek 7.6. *Wszystkimi z dokładnością do izomorfizmu przemiennymi torsyjnymi, noetherowskimi, pierścieniami filialnymi są pierścienie postaci* $\bigoplus_{p \in \Pi} R_p$, *gdzie* Π *jest skończonym podzbiorem zbioru liczb pierwszych oraz każde* R_p *jest jednym z poniższych pierścieni:*

(i) $S \oplus N$, *gdzie* N *jest skończonym przemiennym nil-H-p-pierścieniem oraz* S *jest skończoną sumą prostą ciał charakterystyki* p,

(ii) $C \oplus S$, *gdzie* S *jest skończoną sumą prostą ciał charakterystyki* p *i* p*-pierścień* C *jest skończonym* K_0*-pierścieniem.*

Dobrze wiadomo, że każde ciało, które jest skończenie generowane jako pierścień, jest skończone, i każdy skończenie generowany pierścień przemienny jest noetherowski. Stąd, i z Wniosku 7.6, otrzymujemy następujący wniosek.

Wniosek 7.7. *Wszystkimi, z dokładnością do izomorfizmu, torsyjnymi, skończenie generowanymi przemiennymi pierścieniami filialnymi są pierścienie postaci* $\bigoplus_{p\in\Pi} R_p$, *gdzie* Π *jest skończonym podzbiorem zbioru liczb pierwszych oraz każde* R_p *jest jednym z poniższych pierścieni:*

(i) $S \oplus N$, *gdzie* N *jest skończonym przemiennym nil-H-p-pierścieniem oraz* S *jest skończoną suma prostą ciał skończonych charakterystyki* p,

(ii) $C \oplus S$, *gdzie* S *jest skończoną sumą prostą ciał skończonych charakterystyki* p *i* p*-pierścień* C *jest skończonym* K_0*-pierścieniem.*

W szczególności każdy taki pierścień jest skończony.

7.3 Noetherowskie filialne pierścienie o nietorsyjnym nil-radykale

Z opisu podgrup grupy $\mathbb{Z}_{p^\infty}$, Twierdzenia 2.46 i Lematu 2.14 wynika następujące twierdzenie, klasyfikujące w pewien sposób, wszystkie noetherowskie pierścienie z prawie zerowym mnożeniem.

Wniosek 7.8. *Dla każdej nieparzystej liczby pierwszej* p *niech* μ_p *będzie ustaloną nieresztą kwadratową modulo* p. R *jest noetherowskim pierścieniem z prawie zerowym mnożeniem wtedy i tylko wtedy, gdy* R *zanurza się w pierścień postaci*

$$\bigoplus_{p\in\Pi} R_{(p)} \oplus C, \tag{7.1}$$

gdzie Π *jest skończonym podzbiorem w* $\mathbb{P}$ *oraz* $R_{(p)}$ *jest jednym z następujących pierścieni:*

(i) $\mathbb{Z}_p \times_{p^{s-1}} \mathbb{Z}_{p^s}$, $s \in \mathbb{N}$,

(ii) $(\mathbb{Z}_p \times \mathbb{Z}_p)_{0,0,-\mu_p} \times_{p^{s-1}} \mathbb{Z}_{p^s}$, *dla* $p > 2$, $s \in \mathbb{N}$,

(iii) $(\mathbb{Z}_p \times \mathbb{Z}_p)_{-1,1,-V^2\mu_p} \times_{p^{s-1}} \mathbb{Z}_{p^s}$, *dla* $p > 2$, $s \in \mathbb{N}$, $V \in \{1, 2, ..., (p-1)/2\}$,

(iv) $(\mathbb{Z}_2 \times \mathbb{Z}_2)_{1,0,1} \times_{p^{s-1}} \mathbb{Z}_{2^s}$, $s \in \mathbb{N}$,

natomiast C jest dowolnym pierścieniem z zerowym mnożeniem o skończenie generowanej grupie addytywnej.

Dalej zbadamy przemienne pierścienie filialne R takie, że $0 \neq \mathcal{N}(R) \neq R$.

Twierdzenie 7.9. *Dla przemiennego pierścienia R o nietorsyjnym nil-radykale, następujące warunki są równoważne:*

(i) R jest filialnym pierścieniem noetherowskim,

(ii) $R = \mathbb{S}(R) \oplus \mathcal{N}(R)$, gdzie $\mathbb{S}(R)$ jest skończoną sumą prostą ciał i $\mathcal{N}(R)$ jest pierścieniem z prawie zerowym mnożeniem takim, że grupa $\mathcal{N}(R)^+$ jest skończenie generowana.

Dowód. $(i) \Rightarrow (ii)$. Załóżmy, że $R \neq \mathbb{S}(R) \oplus \mathcal{N}(R)$. Wówczas na mocy Twierdzenia 5.14 istnieje noetherowski, przemienny B-pierścień R. Wtedy $\mathcal{N}(R)$ jest nil-H-pierścieniem noetherowskim, więc z Lematu 2.14 wynika, że grupa $\mathcal{N}(R)^+$ jest skończenie generowana. Ponadto ta grupa nie jest torsyjna i na podstawie Lematu 5.18, $m^2\mathcal{N}(R)^+$ jest grupą prawie podzielną. Wobec tego $m^2\mathcal{N}(R)^+$ jest skończenie generowaną, nietorsyjną grupą prawie podzielną. Ale wtedy na mocy Uwagi 1.13 i Lematu 1.15, $m^2\mathcal{N}(R)^+/\mathbb{T}(m^2\mathcal{N}(R))$ jest niezerową grupą podzielną i ta grupa jest skończenie generowana, co prowadzi do sprzeczności. Zatem $R = \mathbb{S}(R) \oplus \mathcal{N}(R)$. Ponadto $\mathbb{S}(R)$ i $\mathcal{N}(R)$ są przemiennymi pierścieniami noetherowskimi i na mocy Stwierdzenia 5.8 pierścień $\mathcal{N}(R)$ jest z prawie zerowym mnożeniem. Stąd pierścienie z zerowym mnożeniem $\mathcal{N}(R)^2$ i $\mathcal{N}(R)/\mathcal{N}(R)^2$ też są noetherowskie. Wobec tego grupa $\mathcal{N}(R)^+$ jest skończenie generowana. Ponadto pierścień $\mathbb{S}(R)$ jest silnie regularny, więc zgodnie z Twierdzeniem 7.3 jest on skończoną sumą prostą ciał.

$(ii) \Rightarrow (i)$. Wynika bezpośrednio ze Stwierdzenia 1.36. □

7.4 Noetherowskie filialne pierścienie o torsyjnym, niezerowym nil-radykale

Poniżej prezentujemy kluczowe twierdzenie tego rozdziału.

Twierdzenie 7.10. *Przemienny pierścień R o torsyjnym nil-radykale jest filialny i noetherowski wtedy i tylko wtedy, gdy R jest postaci $R = S \oplus \bigoplus_{i=1}^{s}(T_i \oplus M_i)$, gdzie S jest skończoną sumą prostą ciał, M_i jest pierścieniem z prawie zerowym mnożeniem takim, że $\Pi(M_i) \cap \Pi(\mathcal{N}(T_i)) = \emptyset$ i każde T_i jest jednym z poniższych pierścieni:*

(i) skończonym K_0-pierścieniem,

(ii) skończonym i nilpotentnym H-p-pierścieniem,

(iii) m_iD_i, gdzie D_i jest filialną dziedziną całkowitości charakterystyki zero, która nie jest ciałem, $m_i \in S(\Pi(D_i))$ oraz $m_iM_i = 0$,

(iv) m_iR_i, gdzie R_i jest noetherowskim przemiennym pierścieniem Andrijanowa, $m_i \in S(\Pi(R_i))$ oraz $m_iM_i = 0$,

(v) noetherowskim pierścieniem Krusego lub noetherowskim uogólnionym pierścieniem Krusego takim, że $T_i/\mathcal{N}(T_i) \cong m_iD_i$, gdzie D_i jest filialną dziedziną całkowitości charakterystyki zero, która nie jest ciałem, $m_i \in S(\Pi(D_i))$ oraz $m_iM_i = 0$,

przy czym $\Pi(T_i) \cap \Pi(T_j) = \emptyset$ dla wszystkich $i \neq j$.

Dowód. Niech R będzie przemiennym pierścieniem o torsyjnym nil-radykale. Jeżeli $\mathcal{N}(R) = 0$, to teza wynika z Twierdzenia 7.3. Niech dalej $\mathcal{N}(R) \neq 0$ i załóżmy dodatkowo, że pierścień R jest noetherowski. Wówczas $\mathbb{S}(R)$ jest skończoną sumą prostą ciał i $R = \mathbb{S}(R) \oplus J$, gdzie J jest przemiennym, noetherowskim, $\mathbb{S}$-półprostym pierścieniem takim, że $0 \neq \mathcal{N}(J) \subseteq \mathbb{T}(J)$. Jeżeli $J = \mathbb{T}(J)$, to teza wynika z Wniosku 7.6.

Dalej będziemy zakładali, że $\mathbb{T}(J) \neq J$ i pierścień R jest filialny. Oczywiście $\mathbb{T}(J)$ jest przemiennym, noetherowskim, $\mathbb{S}$-półprostym, filialnym pierścieniem torsyjnym. Zatem na podstawie Wniosku 7.6, $\mathbb{T}(J) = \bigoplus_{p\in\Pi} \mathbb{T}(J)_p$, gdzie Π jest skończonym podzbiorem zbioru liczb pierwszych oraz $\mathbb{T}(J)_p$ jest nil-H-pierścieniem lub $\mathbb{T}(J)_p$ jest skończonym K_0-pierścieniem dla każdego $p \in \Pi$. Niech $\Pi_0 = \{p \in \Pi : \mathbb{T}(J)_p$ jest K_0 pierścieniem$\}$. Ponieważ każdy K_0-pierścień ma jedynkę i zbiór Π_0 jest skończony, więc

$$J = \left(\bigoplus_{p\in\Pi_0} \mathbb{T}(J)_p\right) \oplus A \text{ dla pewnego } A \lhd J. \tag{7.2}$$

Pierścień A jest oczywiście filialny i noetherowski jako ideał w R. Jest on również $\mathbb{S}$-półprosty jako ideał w J. Ponieważ $\mathcal{N}(J) \subseteq \mathbb{T}(J)$, więc z określenia zbioru Π_0, $\mathbb{T}(A) = \bigoplus_{p\in\Pi\setminus\Pi_0} \mathbb{T}(J)_p \subseteq \mathcal{N}(A)$ oraz $\mathcal{N}(A) \subseteq \mathbb{T}(A)$, skąd $\mathcal{N}(A) = \mathbb{T}(A)$. Ponadto $\mathbb{T}(A) \neq A$, gdyż $\mathbb{T}(J) \neq J$ i A nie posiada ideału będącego K_0-pierścieniem. Jeżeli $\mathbb{T}(A) = 0$, to na mocy Twierdzenia 7.2, $A \cong \bigoplus_{i=1}^{n} m_iD_i$, gdzie D_i jest filialną dziedziną całkowitości charakterystyki zero, która nie jest ciałem, $m_i \in S(\Pi(D_i))$ dla każdego $i \in \{1, 2, \ldots, n\}$ i $\Pi(D_i) \cap \Pi(D_j) = \emptyset$ dla $i \neq j$.

Wobec tego możemy dalej zakładać, że $\mathcal{N}(A) = \mathbb{T}(A) \neq 0$. Z naszych rozważań wynika, że istnieje skończony niepusty podzbiór $\Delta \subseteq \mathbb{P}$ taki, że $\mathbb{T}(A) = \bigoplus_{p\in\Delta} \mathbb{T}(A)_p$, gdzie $\mathbb{T}(A)_p$ jest niezerowym, noetherowskim nil-H-p-pierścieniem dla każdego $p \in \Delta$. Na podstawie Lematu 2.14, pierścień $\mathbb{T}(A)_p$ jest skończony i nilpotentny dla każdego $p \in \Delta$.

Niech $B = A/\mathbb{T}(A)$. Wówczas B jest niezerowym, beztorsyjnym, noetherowskim CRF-pierścieniem. Pokażemy, że $\mathbb{S}(B) = 0$. Załóżmy, że $\mathbb{S}(B) \neq 0$. Wtedy $\mathbb{S}(B) = I/\mathbb{T}(A) \neq 0$ dla pewnego $I \lhd A$. Oczywiście, istnieje $m \in \mathbb{N}$ takie, że $m\mathbb{T}(A) = 0$. Ponadto $I/\mathbb{T}(A)$ jest pierścieniem beztorsyjnym i silnie regularnym, więc $m(I/\mathbb{T}(A)) = I/(\mathbb{T}(A))$. Stąd $mI + \mathbb{T}(A) = I$. Jeżeli $mi \in \mathbb{T}(A)$ dla pewnego $i \in I$, to $m(mi) = 0$, skąd $i \in \mathbb{T}(A)$ i $mi = 0$. Zatem $mI \oplus \mathbb{T}(A) = I$ i $mI \cong I/\mathbb{T}(A)$. Ponieważ radykał $\mathbb{S}$ jest dziedziczny i $I/\mathbb{T}(A) \in \mathbb{S}$, więc $mI \subseteq \mathbb{S}(A)$, skąd $I = \mathbb{T}(A)$, co przeczy temu, że $I/\mathbb{T}(A) \neq 0$.

Niech $\Pi_1 = \Delta \setminus \Pi(B)$ i niech $n = \prod_{p\in\Pi_1} p$. Wtedy $nB = B$ i istnieje $t \in \mathbb{N}$ takie, że $n^t\left(\bigoplus_{p\in\Pi_1} \mathbb{T}(A)_p\right) = 0$. Stąd $A = n^tA + \mathbb{T}(A)$. Ale $n^t\mathbb{T}(A)_q = \mathbb{T}(A)_q$ dla $q \in \Delta \setminus \Pi_1$ oraz $\mathbb{T}(A) = \bigoplus_{p\in\Delta} \mathbb{T}(A)_p$, więc $A = n^tA + \bigoplus_{p\in\Pi_1} \mathbb{T}(A)_p$. Jeżeli $n^ta \in \bigoplus_{p\in\Pi_1} \mathbb{T}(A)_p$ dla pewnego $a \in A$, to istnieje $m \in S(\Pi_1)$ takie, że $mn^ta = 0$,

skąd $a \in \bigoplus_{p\in\Pi_1} \mathbb{T}(A)_p$, gdyż $n \in S(\Pi_1)$. Ale $n^t \left(\bigoplus_{p\in\Pi_1} \mathbb{T}(A)_p\right) = 0$, więc $n^t a = 0$ i w konsekwencji $n^t A \cap \bigoplus_{p\in\Pi_1} \mathbb{T}(A)_p = 0$. Stąd

$$A = n^t A \oplus \bigoplus_{p\in\Pi_1} \mathbb{T}(A)_p, \tag{7.3}$$

więc $n^t A/\mathbb{T}(n^t A) \cong B$ oraz $\Pi(n^t A) = \Pi(\mathbb{T}(n^t A)) \cup \Pi(B)$. Wobec tego ze wzoru (7.3) i z definicji Π_1, $\Pi(n^t A) = \Pi(B)$ oraz

$$\Pi_1 \cap \Pi(n^t A) = \emptyset. \tag{7.4}$$

Z Twierdzenia 7.2 wynika, że $B \cong \bigoplus_{i=1}^s m_i D_i$, gdzie D_i jest filialną dziedziną całkowitości charakterystyki zero, która nie jest ciałem, $m_i \in S(\Pi(D_i))$ dla każdego $i \in \{1, 2, \ldots, s\}$ i $\Pi(D_i) \cap \Pi(D_j) = \emptyset$ dla wszystkich $i \neq j$. Zatem istnieją ideały $A_1, A_2, \ldots, A_s$ pierścienia $n^t A$ takie, że $\mathbb{T}(n^t A) \subseteq A_i$ oraz $A_i/\mathbb{T}(n^t A) \cong m_i D_i$ dla każdego $i \in \{1, 2, \ldots, s\}$ oraz

$$B = \bigoplus_{i=1}^{s} A_i/\mathbb{T}(n^t A). \tag{7.5}$$

Oznaczmy $\Delta_0 = \Pi(\mathbb{T}(n^t A))$. Ponieważ $\Pi(B) = \bigcup_{i=1}^s \Pi(D_i) = \bigcup_{i=1}^s \Pi(A_i/\mathbb{T}(n^t A))$ oraz $\Delta_0 \subseteq \Pi(B)$, więc $\Delta_0 = \bigcup_{i=1}^s [\Delta_0 \cap \Pi(A_i/\mathbb{T}(n^t A))]$.

Teraz udowodnimy, że jeżeli $\Delta_0 \cap \Pi(A_i/\mathbb{T}(n^t A)) = \emptyset$ dla pewnego $i \in \{1, 2, \ldots, s\}$, to $\mathbb{T}(n^t A)$ wydziela się jako ideałowy składnik prosty w A_i i $A_i = \mathbb{T}(n^t A) \oplus C_i$, gdzie $C_i \cong m_i D_i$. Niech $m = \prod_{p\in\Delta_0} p$. Wówczas $m^s \mathbb{T}(n^t A) = 0$ dla pewnego $s \in \mathbb{N}$ oraz $m(A_i/\mathbb{T}(n^t A)) = A_i/\mathbb{T}(n^t A)$, skąd $m^s A_i + \mathbb{T}(n^t A) = A_i$. Załóżmy, że $m^s a \in \mathbb{T}(n^t A)$. Wtedy $r(m^s a) = 0$ dla pewnego $r \in S(\Delta_0)$. Stąd $rm^s \in S(\Delta_0)$ i w konsekwencji $a \in \bigoplus_{p\in\Delta_0} \mathbb{T}(n^t A)_p = \mathbb{T}(n^t A)$. Ale $m^s \mathbb{T}(n^t A) = 0$, wiec $m^s a = 0$, skąd $m^s A_i \cap \mathbb{T}(n^t A) = 0$ i ostatecznie $m^s A_i \oplus \mathbb{T}(n^t A) = A_i$.

Niech $\Omega = \{i \in \{1, 2, \ldots, s\} \ : \ \Delta \cap \Pi(A_i/\mathbb{T}(n^t A)) = \emptyset\}$. Ponieważ $n^t A = \sum_{i=1}^s A_i$, więc

$$n^t A = \sum_{i\in\{1,2,\ldots,s\}\setminus\Omega} A_i + \sum_{i\in\Omega} C_i. \tag{7.6}$$

Jeżeli $c \in C_i \cap C_j$ dla pewnych różnych $i, j \in \Omega$, to $c + \mathbb{T}(A) \in (A_i/\mathbb{T}(n^t A)) \cap (A_j/\mathbb{T}(n^t A))$ i ze wzoru (7.5) mamy $c = 0$. Stąd $\sum_{i\in\Omega} C_i = \bigoplus_{i\in\Omega} C_i$.

Niech $a \in \sum_{i\in\{1,2,\ldots,s\}\setminus\Omega} A_i$, $c_i \in C_i$ dla $i \in \Omega$ będą takie, że $a + \sum_{i\in\Omega} c_i = 0$. Wówczas w pierścieniu ilorazowym $n^t A/\mathbb{T}(n^t A)$ mamy $\overline{a} + \sum_{i\in\Omega} \overline{c}_i = \overline{0}$, skąd $\overline{c_i} = \overline{0}$ dla każdego $i \in \Omega$ i w konsekwencji $\overline{a} = \overline{0}$. Stąd $c_i \in C_i \cap \mathbb{T}(n^t A) = 0$ dla każdego $i \in \Omega$, więc $a = 0$. Zatem $\sum_{i\in\{1,2,\ldots,s\}\setminus\Omega} A_i \cap \bigoplus_{i\in\Omega} C_i = 0$ i

$$n^t A = \left(\sum_{i\in\{1,2,\ldots,s\}\setminus\Omega} A_i\right) \oplus \left(\bigoplus_{i\in\Omega} C_i\right).$$

Niech $\Gamma = \{1, 2, \ldots, s\} \setminus \Omega$. Oczywiście $\mathbb{T}(n^t A) = \mathbb{T}(\sum_{i\in\Gamma} A_i)$ i $\Delta = \bigcup_{i\in\Gamma} [\Delta \cap \Pi(A_i/\mathbb{T}(n^t A))]$. Niech $\Delta_j = \Delta \setminus \Pi(A_j/\mathbb{T}(n^t A))$ i $L_j = \prod_{p\in\Delta_j} p$ dla $j \in \Gamma$. Istnieje

liczba naturalna k taka, że $L_j^k \cdot \left(\bigoplus_{p\in\Delta_j} \mathbb{T}(n^tA)_p\right) = 0$ oraz $L_j^k \left(\bigoplus_{p\in\Delta\setminus\Delta_j} \mathbb{T}(n^tA)_p\right) = \bigoplus_{p\in\Delta\setminus\Delta_j} \mathbb{T}(n^tA)_p$, skąd $A_j = L_j^kA_j \oplus \left(\bigoplus_{p\in\Delta_j} \mathbb{T}(n^tA)_p\right)$. Dalej

$$m_jD_j \cong A_j/\mathbb{T}(A_j) =$$

$$= \left(L_j^kA_j \oplus \left(\bigoplus_{p\in\Delta_j} \mathbb{T}(n^tA)_p\right)\right) / \left(\left(\bigoplus_{p\in\Delta\setminus\Delta_j} \mathbb{T}(n^tA)_p\right) \oplus \left(\bigoplus_{p\in\Delta_j} \mathbb{T}(n^tA)_p\right)\right) \cong$$

$$L_j^kA_j / \left(\bigoplus_{p\in\Delta\setminus\Delta_j} \mathbb{T}(n^tA)_p\right) = L_j^kA_j/\mathcal{N}(L_j^kA_j).$$

Odnotujmy, że $\Delta \cap \Pi(A_j/\mathbb{T}(n^tA)) = \Delta \setminus \Delta_j$. Pokażemy, że $\sum_{j\in\Gamma} A_j = \bigoplus_{j\in\Gamma} L_j^kA_j$. Oczywiście $\mathbb{T}(n^tA) \subseteq \sum_{j\in\Gamma} L_j^kA_j$, gdyż $\Delta = \bigcup_{j\in\Gamma}[\Delta \setminus \Delta_j]$ oraz $\bigoplus_{p\in\Delta\setminus\Delta_j} \mathbb{T}(n^tA)_p \subseteq L_j^kA_j$. Ale $\sum_{j\in\Gamma} A_j = \sum_{j\in\Gamma} L_j^kA_j + \mathbb{T}(A)$, więc $\sum_{j\in\Gamma} A_j = \sum_{j\in\Gamma} L_j^kA_j$. Niech $a_j \in L_j^kA_j$ dla $j \in \Gamma$ będą takie, że $\sum_{j\in\Gamma} a_j = 0$. Wówczas w pierścieniu ilorazowym $A/\mathbb{T}(A)$, $\sum_{j\in\Gamma} \overline{a}_j = \overline{0}$. Zatem $a_j \in L_j^kA_j \cap \mathbb{T}(A)$, skąd $a_j \in \bigoplus_{p\in\Delta\setminus\Delta_j} \mathbb{T}(n^tA)_p$ dla każdego $j \in \Gamma$. Ale zbiory $\Delta \setminus \Delta_j$ są parami rozłączne, więc $a_j = 0$ dla każdego $j \in \Gamma$, gdyż $a_j \in \mathbb{T}(n^tA)$. Zatem

$$\sum_{j\in\Gamma} A_j = \bigoplus_{j\in\Gamma} L_j^kA_j. \tag{7.7}$$

I ostatecznie

$$R = \mathbb{S}(R) \oplus \left(\bigoplus_{p\in\Pi_0} \mathbb{T}(J)_p\right) \oplus \left(\bigoplus_{p\in\Pi_1} \mathbb{T}(A)_p\right) \oplus \left(\bigoplus_{i\in\Omega} C_i\right) \oplus \left(\bigoplus_{j\in\Gamma} L_j^kA_j\right).$$

i dla każdego $j \in \Gamma$, $L_j^kA_j$ jest przemiennym, filialnym, $\mathbb{S}$-półprostym pierścieniem noetherowskim takim, że $0 \neq \mathbb{T}(L_j^kA_j) = \mathcal{N}(L_j^kA_j) \neq L_j^kA_j$, $m_jD_j \cong L_j^kA_j/\mathcal{N}(L_j^kA_j)$ oraz $\Pi(\mathbb{T}(L_j^kA_j)) \subseteq \Pi(D_j)$. Jeśli dla każdego $p \in \Pi(\mathbb{T}(L_j^kA_j))$, $(\mathbb{T}(L_j^kA_j))_p$ nie wydziela się jako ideałowy składnik prosty pierścienia $L_j^kA_j$, to na mocy Twierdzeń 4.32 i 4.41, $L_j^kA_j \cong m_jR_j$ dla pewnego przemiennego noetherowskiego pierścienia Andrijanowa R_j lub $L_j^kA_j$ jest noetherowskim pierścieniem Krusego lub noetherowskim uogólnionym pierścieniem Krusego.

Niech zatem, $(\mathbb{T}(L_j^kA_j))_p$ wydziela się jako ideałowy składnik prosty pierścienia $L_j^kA_j$ dla pewnego $p \in \Pi(\mathbb{T}(L_j^kA_j))$. Z Twierdzenia 4.8 wynika, że $p \mid m_j$. Zatem na podstawie Twierdzenia 4.42, pierścień $L_j^kA_j$ jest taki jak w punktach $(iii) - (v)$.

Ponadto $R/(\mathbb{S}(R) \oplus \mathcal{N}(R)) \cong \bigoplus_{i\in\Omega\cup\Gamma} D_i$ i pierścień $R/(\mathbb{S}(R) \oplus \mathcal{N}(R))$ jest filialny oraz $\Omega \cap \Gamma = \emptyset$, więc na mocy Twierdzenia 3.4, $\Pi(D_i) \cap \Pi(D_j) = \emptyset$. dla różnych $i, j \in \Omega \cup \Gamma$. Stąd i z przeprowadzonego rozumowania wynika, że $\Pi(T_i) \cap \Pi(T_j) = \emptyset$ dla wszystkich $i \neq j$.

Na odwrót. Filialność pierścienia $T_i \oplus M_i$, dla T_i takiego jak w punkcie (i) lub (ii) wynika z Twierdzenia 4.4, dla T_i takiego jak w punkcie (iii) wynika z Twierdzenia 4.9, dla T_i takiego jak w punkcie (iv) wynika z Twierdzenia 4.17, dla T_i takiego jak

w punkcie (v) wynika z Twierdzeń 4.23, 4.26. Filialność pierścienia $\bigoplus_{i=1}^{s}(T_i \oplus M_i)$ wynika z Twierdzenia 4.4. Natomiast filialność pierścienia R wynika ze Stwierdzenia 1.36. Noetherowskość pierścienia R wynika bezpośrednio z założeń i faktu, że skończona suma prosta przemiennych pierścieni noetherowskich jest pierścieniem noetherowskim. □

Rozdział 8

Dołączanie jedynki do torsyjnego pierścienia filialnego

Lemat 8.1. *Jeżeli nil-H-p-pierścień I jest ideałem w pewnym filialnym p-pierścieniu z jedynką, to:*

(i) grupa pI^+ jest cykliczna,

(ii) jeżeli $I(p)^2 \neq 0$, to $y^2 \in I(p)^2 + \langle y \rangle$ dla każdego $y \in I$.

Dowód. (i). Niech R będzie filialnym p-pierścieniem z jedynką takim, że $I \lhd R$.

Wówczas $B = \beta(R)$ jest pierścieniem filialnym jako ideał pierścienia R. Na podstawie Twierdzenia 1.35, $\beta(R)$ jest H-pierścieniem. Ponadto, ze Stwierdzenia 2.13 wynika, że pierścień I jest nilpotentny, więc $I \subseteq \beta(R)$. Zatem na mocy Lematu 6.7, grupa pI^+ jest cykliczna.

(ii). Oczywiście $B(p)^2 \neq 0$, gdyż $I \subseteq B$. Ze Stwierdzenia 2.12 punkt (ii) wynika, że $B(p)$ jest p-pierścieniem z prawie zerowym mnożeniem, więc $|B(p)^2| = p$. Ponieważ $0 \neq I(p)^2 \subseteq B(p)^2$, więc $I(p)^2 = B(p)^2$. Niech $y \in I$. Na mocy Lematu 6.7, $y^2 \in B(p)^2 + \langle y \rangle$, więc $y^2 \in I(p)^2 + \langle y \rangle$. □

Stwierdzenie 8.2. *Jeżeli filialny p-pierścień R spełnia którykolwiek z warunków:*

(i) grupa R^+ jest cykliczna,

(ii) $pR = 0$,

to R jest ideałem w pewnym filialnym p-pierścieniu z jedynką.

Dowód. (i). Niech $R^+ = \langle a \rangle$ dla pewnego $a \in R$. Wówczas $o(a) = p^s$ i $a^2 = p^r a$ dla pewnych $s \in \mathbb{N}$, $r \in \mathbb{N}_0$. Wtedy $\langle a \rangle \cong p^r\mathbb{Z}_{p^{r+s}}$, ale $p^r\mathbb{Z}_{p^{r+s}} \lhd \mathbb{Z}_{p^{r+s}}$, więc R jest ideałem w p-pierścieniu z jedynką.

(ii). Ponieważ R jest algebrą nad $\mathbb{Z}_p$, to na mocy Uwagi 1.25, $\mathbb{Z}_p \boxplus R$ jest p-pierścieniem z jedynką, w którym R jest ideałem i takim, że $(\mathbb{Z}_p \boxplus R)/R \cong \mathbb{Z}_p$. Z Lematu 4.1 wynika, że pierścień $\mathbb{Z}_p \boxplus R$ jest filialny. □

Ze Stwierdzenia 8.2 otrzymujemy natychmiast następujący wniosek.

Wniosek 8.3. *Filialny p-pierścień R taki, że $|R| \leq p^2$ jest ideałem w pewnym filialnym p-pierścieniu z jedynką.*

Stwierdzenie 8.4. *Dowolny pierścień z prawie zerowym mnożeniem R jest ideałem w pewnym filialnym pierścieniu z jedynką.*

Dowód. Z Twierdzenia 2.41 wynika, że $R \lhd S$, gdzie S jest pierścieniem z prawie zerowym mnożeniem takim, że $pS = p^2S$ dla dowolnej liczby pierwszej p. Na podstawie Wniosku 4.11, $\mathbb{Z} \boxplus S$ jest pierścieniem filialnym, w którym R jest ideałem. □

Uwaga 8.5. Z Lematu 8.1, punkt (i) wynika, że pierścień $\mathbb{Z}^0_{p^2} \oplus \mathbb{Z}^0_{p^2}$ nie jest ideałem w żadnym filialnym p-pierścieniu z jedynką, ale jest on ideałem w pewnym pierścieniu filialnym z jedynką na mocy Stwierdzenia 8.4.

Stwierdzenie 8.6. *Każdy filialny p-pierścień R generowany przez jeden element jest ideałem w pewnym filialnym, przemiennym p-pierścieniu z jedynką.*

Dowód. Bez tracenia ogólności można zakładać, że pierścień R nie ma jedynki. Niech $R = [a]$ dla pewnego $a \in R$. Ponieważ R jest pierścieniem przemiennym, więc z przyjętych założeń oraz Wniosku 7.7 wynika, że $R \cong S \oplus N$ gdzie N jest niezerowym skończonym przemiennym nil-H-p-pierścieniem oraz S jest skończoną sumą prostą ciał skończonych charakterystyki p. Na mocy Twierdzenia 4.1 wystarczy pokazać, że N jest ideałem w pewnym filialnym, przemiennym p-pierścieniu z jedynką. Z Twierdzenia 2.19 wynika, że N jest izomorficzny z jednym z poniższych pierścieni:

(i) $p^m\mathbb{Z}_{p^{m+n}}$ dla pewnych $m, n \in \mathbb{Z}$, $m \leq n$,

(ii) $\mathbb{Z}_{p^m} \times_1 \mathbb{Z}_p$ dla pewnego $m \in \mathbb{N}$,

(iii) $x\mathbb{Z}_{p^{m+n}}[x]/(px^2 - p^m x, x^3 - p^{2m-2}x)$ dla pewnych $m, n \in \mathbb{N}$, $m \geq 2$.

W przypadku (i), $N \lhd \mathbb{Z}_{p^{m+n}}$.

W przypadku (ii), jeśli $m = 1$, to $N \cong x\mathbb{Z}_p[x]/(x^3) \lhd \mathbb{Z}_p[x]/(x^3)$. Jeżeli, zaś $m > 1$, to niech $S = \mathbb{Z}_{p^{2m-1}} \boxplus y\mathbb{Z}_p[y]/(y^3)$. Pierścień S jest filialny na mocy Przykładu 6.8. Można sprawdzić, że odwzorowanie $\varphi\colon \mathbb{Z}_p \times_1 \mathbb{Z} \to S$ dane wzorem $\varphi((\alpha.\beta)) = \alpha p^{m-1} + \beta p^{2m-2} + \alpha\overline{y} + \beta\overline{y^2}$, $(\varphi((1,0)) = p^{m-1} + \overline{y})$, jest monomorfizmem. Ponadto $Im\varphi \subseteq \mathcal{N}(S)$, więc $Im\varphi \lhd S$.

W przypadku (iii) niech $T = \mathbb{Z}_{p^{2m+n-1}} \boxplus y\mathbb{Z}_p[y]/(y^3)$. Pierścień T jest filialny na mocy Przykładu 6.8 i odwzorowanie $\psi\colon x\mathbb{Z}_{p^{m+n}}[x]/(px^2 - p^m x, x^3 - p^{2m-2}x) \to T$ dane wzorem $\psi(\overline{x}) = p^{m-1} + \overline{y}$ jest monomorfizmem. □

Przez R^{op} będziemy rozumieć pierścień R z odwróconym mnożeniem. Ponadto odnotujmy, że dowolny pierścień R jest filialny wtedy i tylko wtedy, gdy pierścień R^{op} jest filialny.

Twierdzenie 8.7. *Dowolny filialny pierścień (przemienny) R taki, że $|R| = 8$ jest ideałem w pewnym filialnym 2-pierścieniu (przemiennym) z jedynką.*

Dowód. Bez tracenia ogólności można zakładać, że pierścień R nie ma jedynki.

Jeżeli grupa R^+ jest cykliczna lub $2R = 0$, to teza wynika ze Stwierdzenia 8.2. Niech więc dalej $R^+ \cong \mathbb{Z}_4^+ \times \mathbb{Z}_2^+$. Istnieją wówczas $x_1, x_2 \in R$ takie, że $R^+ = \langle x_1 \rangle \oplus \langle x_2 \rangle$, gdzie $o(x_1) = 4$, $o(x_2) = 2$.

Jeżeli R nie jest nil-pierścieniem, ale jest przemienny, to na podstawie Wniosku 7.7, $R \cong S \oplus N$, gdzie S jest sumą prostą ciał charakterystyki 2 oraz N jest nil-pierścieniem takim, że $|N| \leq 4$. Zgodnie ze Stwierdzeniem 8.2, istnieje filialny 2-pierścień N_1 z jedynką taki, że $N \lhd N_1$. Wówczas $R \lhd S \oplus N_1$ i $S \oplus N_1$ jest filialny na mocy Lematu 4.1.

Jeżeli zaś R nie jest nil-pierścieniem i nie jest przemienny, to z Twierdzenia 3 z [18], wynika, że $R \cong \begin{pmatrix} \mathbb{Z}_4 & 2\mathbb{Z}_4 \\ 0 & 0 \end{pmatrix}$ lub $R \cong \begin{pmatrix} \mathbb{Z}_4 & 0 \\ 2\mathbb{Z}_4 & 0 \end{pmatrix}$. W pierwszym przypadku

$$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 0 & 0 \end{pmatrix} \right\} \lhd \begin{pmatrix} 2\mathbb{Z}_4 & 2\mathbb{Z}_4 \\ 0 & 0 \end{pmatrix} \lhd \begin{pmatrix} \mathbb{Z}_4 & 2\mathbb{Z}_4 \\ 0 & 0 \end{pmatrix},$$

ale $\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 0 & 0 \end{pmatrix} \right\}$ nie jest ideałem w $\begin{pmatrix} \mathbb{Z}_4 & 2\mathbb{Z}_4 \\ 0 & 0 \end{pmatrix}$, więc R nie jest pierścieniem filialnym. Podobnie można pokazać, że $\begin{pmatrix} \mathbb{Z}_4 & 0 \\ 2\mathbb{Z}_4 & 0 \end{pmatrix}$ też nie jest pierścieniem filialnym.

Załóżmy, że R jest nil-pierścieniem.

Jeżeli $x_1^2 \notin \langle x_1 \rangle$, to $x_1^2 = kx_1 + lx_2$ dla pewnych $k, l \in \mathbb{Z}$ oraz $|\langle x_1 \rangle + \langle x_1^2 \rangle| = 8$, skąd $R = \langle x_1 \rangle + \langle x_1^2 \rangle$. Stąd R jest torsyjnym 2-pierścieniem generowanym przez jeden element, więc teza wynika ze Stwierdzenia 8.6.

Załóżmy teraz, że $x_1^2 \in \langle x_1 \rangle$. Istnieje wówczas $t \in \mathbb{Z}$ takie, że $x_1^2 = tx_1$. Jeżeli $2 \nmid t$, to $x_1 \in Rx_1$ i ponieważ R jest nil-pierścieniem, więc $x_1 = 0$, sprzeczność. Zatem $2 \mid t$ i $x_1^2 \in \langle 2x_1 \rangle$. Stąd $[x_1] = \langle x_1 \rangle$ i ponieważ R jest H-pierścieniem, więc $\langle x_1 \rangle \lhd R$. Dalej $2R^2 = 0$ i $R(2) = \langle 2x_1 \rangle + \langle x_2 \rangle$, więc $x_1x_2, x_2x_1 \in \langle 2x_1 \rangle$. Oczywiście $x_2^2 \in R(2)$, więc istnieją liczby całkowite k, l takie, że $x_2^2 = k(2x_1) + lx_2$. Wówczas $x_2^3 = 2kx_1x_2 + lx_2^2 = l(2kx_1 + lx_2)$ i dla dowolnego $m \in \mathbb{N}$, $x_2^m = 2L_mx_1 + l^{m-1}x_2$ dla pewnego $L_m \in \mathbb{Z}$. Ponieważ R jest nil-pierścieniem, więc $x_2^m = 0$ dla pewnego $m \in \mathbb{Z}$, skąd $l^{m-1}x_2 = 0$. Zatem $2 \mid l$ i $x_2^2 = 2kx_1$.

Podsumowując powyższe rozważania widzimy, że $x_1^2 = 2ax_1$, $x_1x_2 = 2bx_1$, $x_2x_1 = 2cx_1$, $x_2^2 = 2dx_1$ dla pewnych $a, b, c, d \in \mathbb{Z}_2$.

Jeżeli $a = b = c = d = 0$, to $R \cong [(4,0),(0,2)] \lhd \mathbb{Z}_{16} \boxplus 2\mathbb{Z}_4$. Izomorfizm $f\colon R \to [(4,0),(0,2)]$ zadany jest na generatorach $f(x_1) = (4,0)$, $f(x_2) = (0,2)$. Ponadto pierścień $\mathbb{Z}_{16} \boxplus 2\mathbb{Z}_4$ jest filialny na mocy Przykładu 6.8.

Jeżeli $d = 0$, to $x_2^2 = 0$ i $[x_2] = \langle x_2 \rangle \lhd R$, więc $x_1x_2, x_2x_1 \in \langle x_2 \rangle \cap \langle 2x_1 \rangle = 0$. Zatem $R = [x_1] \oplus \langle x_2 \rangle^0$. Ale, $[x_1]$ jest pierścieniem z prawie zerowym mnożeniem, którego grupa addytywna jest cykliczna, więc ze Stwierdzenia 2.25, $[x_1] \cong 2\mathbb{Z}_8$. Stąd $R \cong 2\mathbb{Z}_8 \oplus 2\mathbb{Z}_4 \lhd \mathbb{Z}_8 \boxplus 2\mathbb{Z}_4$ i pierścień $\mathbb{Z}_8 \boxplus 2\mathbb{Z}_4$ jest filialny na mocy Przykładu 6.8.

Pozostały zatem do rozpatrzenia następujące przypadki:

1. $x_2^2 = 2x_1$, $x_1^2 = 0$, $x_1x_2 = 0$, $x_2x_1 = 0$,

2. $x_2^2 = 2x_1$, $x_1^2 = 0$, $x_1x_2 = 0$, $x_2x_1 = 2x_1$,

3. $x_2^2 = 2x_1$, $x_1^2 = 0$, $x_1x_2 = 2x_1$, $x_2x_1 = 0$,

4. $x_2^2 = 2x_1$, $x_1^2 = 0$, $x_1x_2 = 2x_1$, $x_2x_1 = 2x_1$,

5. $x_2^2 = 2x_1$, $x_1^2 = 2x_1$, $x_1x_2 = 0$, $x_2x_1 = 0$,

6. $x_2^2 = 2x_1$, $x_1^2 = 2x_1$, $x_1x_2 = 0$, $x_2x_1 = 2x_1$,

7. $x_2^2 = 2x_1$, $x_1^2 = 2x_1$, $x_1x_2 = 2x_1$, $x_2x_1 = 0$,

8. $x_2^2 = 2x_1$, $x_1^2 = 2x_1$, $x_1x_2 = 2x_1$, $x_2x_1 = 2x_1$,

Ad.1. Niech $T = (\mathbb{Z}_{16} \boxplus y\mathbb{Z}_p[y]/(y^3))/(8 \cdot 1 - \overline{y^2})$. Pierścień $\mathbb{Z}_{16} \boxplus y\mathbb{Z}_p[y]/(y^3)$ jest filialny na mocy Przykładu 6.8, więc T jako jego obraz homomorficzny jest też pierścieniem filialnym. Ponadto przekształcenie $\varphi\colon R \to T$ zadane na generatorach $\varphi(x_1) = 4 \cdot \overline{1}$, $\varphi(x_2) = \overline{\overline{y}}$ jest monomorfizmem pierścieni takim, że $Im\varphi \subseteq \mathcal{N}(T)$, więc $Im\varphi \lhd \mathcal{N}(T)$.

Ad.2. Niech $S = [x, y]$, gdzie $o(x) = o(y) = 2$, $x^2 = y^2 = yx$, $xy = 0$. Wówczas S jest pierścieniem z prawie zerowym mnożeniem na mocy Twierdzenia 2.16 punkt (3). Niech $T = (\mathbb{Z}_8 \boxplus S)/I$, gdzie $I = (2x - 4 \cdot 1)$. Pierścień $\mathbb{Z}_8 \boxplus S$ jest filialny na mocy Przykładu 6.8, więc T jako jego obraz homomorficzny jest też pierścieniem filialnym. Przekształcenie $\varphi\colon R \to T$ zadane na generatorach $\varphi(x_1) = 2 \cdot \overline{1} + \overline{y}$, $\varphi(x_2) = \overline{x} + \overline{y}$ jest monomorfizmem pierścieni takim, że $Im\varphi \subseteq \mathcal{N}(T)$, więc $Im\varphi \lhd \mathcal{N}(T)$.

Ad.3. Pierścień R^{op} jest izomorficzny z pierścieniem z punktu 2. Zatem R^{op} jest ideałem w pewnym 2-pierścieniu filialnym z jedynką P, więc R jest ideałem w filialnym 2-pierścieniu z jedynką P^{op}.

Ad.4. Kładąc $x = x_1 + x_2$ oraz $y = x_2$ otrzymujemy: $x^2 = 2x$, $y^2 = 2x$, $xy = 0$, $yx = 0$. Zatem pierścienie z przypadków 4. oraz 5. są izomorficzne.

Ad.5. Niech $S = x\mathbb{Z}_2[x]/(x^3)$. Wówczas S jest pierścieniem z prawie zerowym mnożeniem na mocy Twierdzenia 2.16, punkt (2). Pierścień $\mathbb{Z}_8 \boxplus S$ jest filialny na mocy Przykładu 6.8, więc $T = (\mathbb{Z}_8 \boxplus S)/I$, gdzie $I = (4 \cdot 1 - \overline{x^2})$ jako jego obraz homomorficzny, jest też pierścieniem filialnym. Przekształcenie $\varphi\colon R \to T$ zadane na generatorach $\varphi(x_1) = 2 \cdot \overline{1}$, $\varphi(x_2) = \overline{x}$ jest monomorfizmem pierścieni takim, że $Im\varphi \subseteq \mathcal{N}(T)$, więc $Im\varphi \lhd \mathcal{N}(T)$.

Ad.6. Niech $S = [x, y]$, gdzie $o(x) = o(y) = 2$, $x^2 = y^2 = yx$, $xy = 0$. Wówczas S jest pierścieniem z prawie zerowym mnożeniem na mocy Stwierdzenia 2.16. Niech $T = (\mathbb{Z}_{16} \boxplus S)/I$, gdzie $I = (8 \cdot 1 - x^2)$. Pierścień $\mathbb{Z}_{16} \boxplus S$ jest filialny na mocy Przykładu 6.8, więc T jako jego obraz homomorficzny jest też pierścieniem filialnym. Przekształcenie $\varphi\colon R \to T$ zadane na generatorach $\varphi(x_1) = 4 \cdot \overline{1} + \overline{x}$, $\varphi(x_2) = \overline{y}$ jest monomorfizmem pierścieni takim, że $Im\varphi \subseteq \mathcal{N}(T)$, więc $Im\varphi \lhd \mathcal{N}(T)$.

Ad.7. Pierścień R^{op} jest izomorficzny z pierścieniem z punktu 6. Zatem R^{op} jest ideałem w pewnym 2-pierścieniu filialnym z jedynką P, więc R jest ideałem w filialnym 2-pierścieniu z jedynką P^{op}.

Ad.8. Kładąc $x = x_1 + x_2$ oraz $y = x_2$ otrzymujemy: $x^2 = 0$, $y^2 = 2x$, $xy = 0$, $yx = 0$. Zatem pierścienie z przypadków 8. oraz 1. są izomorficzne. □

Lemat 8.8. *Jeżeli nil-H-p-pierścień I, który nie jest pierścieniem z prawie zerowym mnożeniem jest ideałem w pewnym filialnym pierścieniu z jedynką, to jest on ideałem w pewnym filialnym p-pierścieniu z jedynką.*

Dowód. Niech R będzie filialnym pierścieniem z jedynką takim, że $I \lhd R$. Bez tracenia ogólności można zakładać, że I jest ideałem istotnym w R. Wówczas $\beta(R)$ jest pierścieniem filialnym jako ideał pierścienia R. Na podstawie Twierdzenia 1.35, $\beta(R)$ jest H-pierścieniem. Na mocy Stwierdzenia 2.13, pierścień I jest nilpotentny. Jeżeli w grupie $\beta(R)^+$ istnieje element nieskończonego rzędu, to ze Stwierdzenia 2.4 wynika, że $\beta(R)$ jest pierścieniem z prawie zerowym mnożeniem i wobec tego I jest pierścieniem z prawie zerowym mnożeniem jako podpierścień w $\beta(R)$, sprzeczność. Zatem grupa $\beta(R)^+$ jest torsyjna. Ponieważ I jest ideałem istotnym w R, więc $\beta(R)^+$ jest p-grupą. Ponownie, ze Stwierdzenia 2.5 wynika, że grupa $\beta(R)^+$ jest ograniczonego wykładnika. Stąd, istnieje $n \in \mathbb{N}$ takie, że $p^n\beta(R)^+ = 0$. Ponadto, $\beta(R)$ jest ideałem istotnym w R, bo $I \subseteq \beta(R)$ oraz I jest istotny w R.

Jeżeli $p \cdot 1 \notin \beta(R)$, to $p^m \cdot 1 \notin \beta(R)$ dla dowolnego $m \in \mathbb{N}$, gdyż $p \cdot 1 \in Z(R)$. W szczególności $p^m R \neq 0$ dla każdego naturalnego m. Z istotności $\beta(R)$ w R mamy $p^{n+1}R \cap \beta(R) \neq 0$. Stąd $p^{n+1}r \in \beta(R) \setminus \{0\}$ dla pewnego $r \in R$. Zatem $(p(r)_R)^{n+1} \subseteq \beta(R)$, skąd $((p(r)_R + \beta(R))/\beta(R))^{n+1} = 0$, więc $p(r)_R \subseteq \beta(R)$. Wobec tego $0 = p^n(p(r)_R) = p^{n+1}(r)_R$, skąd $p^{n+1}r = 0$, sprzeczność. Wobec tego $p \cdot 1 \in \beta(R)$ i istnieje $s \in \mathbb{N}$ takie, że $(p \cdot 1)^s = 0$. Wtedy $p^s R = 0$ i R jest p-pierścieniem. □

Twierdzenie 8.9. *Każdy filialny (przemienny) pierścień R taki, że $|R| < 16$ jest ideałem w pewnym filialnym (przemiennym) pierścieniu z jedynką. Ponadto istnieje przemienny filialny pierścień szesnastoelementowy, który nie jest ideałem w żadnym filialnym pierścieniu z jedynką.*

Dowód. Dowód pierwszej części Twierdzenia wynika ze Stwierdzenia 1.28, Wniosku 8.3 oraz Twierdzenia 8.7.

Na grupie $I^+ = \langle x_1\rangle \oplus \langle x_2\rangle \oplus \langle x_3\rangle$, $o(x_1) = 4$, $o(x_2) = o(x_3) = 2$ określmy mnożenie za pomocą relacji $x_1^2 = x_2$, $x_1x_3 = x_3x_1 = x_3^2 = 2x_1$, $x_2I = Ix_2 = 0$. Łatwo jest sprawdzić, że $(xy)z = x(yz) = 0$ dla dowolnych $x, y, z \in I$ więc wyżej określone mnożenie jest łączne i zadaje na I strukturę pierścienia.

Ponieważ $2x_1 = x_1x_3 \notin \langle x_1^2\rangle = \langle x_2\rangle$, więc I nie jest pierścieniem z prawie zerowym mnożeniem.

Pokażemy, że I jest H-pierścieniem. Niech $i \in I$. Wtedy istnieją $a, b, c \in \mathbb{Z}$ takie, że $i = ax_1 + bx_2 + cx_3$. Stąd $i^2 = a^2x_1^2 + c^2x_3^2 + 2acx_1x_3 = a^2x_2 + 2c^2x_1 + 2ac(2x_1) = ax_2 + 2cx_1$. Ponieważ $[i] = \langle i\ \rangle + \langle i^2\rangle$, $x_1i = ax_2 + 2cx_1 \in [i]$, $x_2i = 0 \in [i]$ oraz $x_3i = 2ax_1 + 2cx_1 = X(ax_1 + bx_2 + cx_3) + Y(ax_2 + 2cx_1)$, gdzie jeśli $a = 0$, to $X = 0$, $Y = 1$, jeśli $c = 0$, to $X = 2$, $Y = 0$, jeśli $a = \pm 1$ i $c = 1$, to $X = Y = 0$ i ostatecznie jeśli $a = 2$ i $c = 1$, to $X = 0$, $Y = 1$. Powyższe rozważania pokazują, że $[i] \lhd I$, więc I jest H-pierścieniem.

Ponieważ $I(2)^2 = \langle 2x_1\rangle$ oraz $x_1^2 = x_2$, więc $x_1^2 \notin I(2)^2 + \langle x_1\rangle$. Zatem na podstawie Lematu 8.1, I nie jest ideałem w żadnym filialnym 2-pierścieniu z jedynką. Ponadto na mocy Lematu 8.8, I nie jest ideałem w żadnym filialnym pierścieniu z jedynką. □

Bibliografia

[1] S. A. Amitsur, *A general theory of radicals II, Radicals in rings and bicategories*, Amer. J. Math. **76** (1954), 100–125.

[2] V. I. Andrijanow, *Mixed Hamiltonian nilrings*, (Russian) Ural. Gos. Univ. Mat. Zap. **5**(3) (1966), 15–30.

[3] V. I. Andrijanow, *Periodic Hamiltonian rings*, Mat. Sb. (N.S.) **74**(116) (1967), 241–261; translation in Mat. Sbornik **74**(116) No. 2 (1967), 225-241.

[4] R. R. Andruszkiewicz, *Podpierścienie osiągalne w pierścieniach łącznych*, rozprawa doktorska, MIMUW, (1990).

[5] R. R. Andruszkiewicz, E. R. Puczyłowski *Kurosh's chains of associative rings*, Glasg. Math. J. 32 (1990), no. 01, 67–69.

[6] R. R. Andruszkiewicz, E. R. Puczyłowski, *On filial rings*, Portugal. Math. **45** (1988), 139–149.

[7] R. R. Andruszkiewicz, E. R. Puczyłowski *Accessible subrings and Kurosh's chains of associative rings*, Algebra Colloq. 4 (1997), no. 1, 79-88.

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

[9] R.R. Andruszkiewicz, *Essential cover and closure*, Serdica Math. J. **30** (2004), 505—512.

[10] R.R. Andruszkiewicz, M. Sobolewska, *Commutative reduced filial rings*, Algebra and Discrete Math. **3** (2007), 18–26.

[11] R.R. Andruszkiewicz, M. Sobolewska, *Accessible subrings and Kurosh's chains of associative rings*, J. Aust. Math. Soc. **95** (2013), no. 2, 145–157.

[12] R. R. Andruszkiewicz, K. Pryszczepko *A classification of commutative reduced filial rings*, Comm. Algebra. **37** (2009), 3820–3826.

[13] R .R. Andruszkiewicz, K. Pryszczepko *On commutative reduced filial rings*, Bull. Aust. Math. Soc. **81** (2010), 310–316.

[14] R. R. Andruszkiewicz, K. Pryszczepko *The classification of commutative noetherian, filial rings with identity*, Comm. Algebra. **40** (2012), 1690–1703.

[15] R. R. Andruszkiewicz, K. Pryszczepko *The classification of commutative torsion filial rings*, J. Aust. Math. Soc. **95** (2013), no. 3, 289–296.

[16] R. Andruszkiewicz, K. Pryszczepko *On the non-torsion almost null rings* Recent Results in Pure and Applied Mathematics, Białystok Technical University Publishing Office, 2014.

[17] R. R. Andruszkiewicz, K. Pryszczepko *Adjoining an identity to a filial ring*, NYJM **20** (2014), 695–710.

[18] V. G. Antipkin, V. P. Elizarov *Rings of order p^3*, Sib. Mat. Zhurnal. **23**(4) (1982), 9–18.

[19] A. Ballester-Bolinches, R. Esteban-Romero, M. Asaad, *Products of finite groups*, de Gruyter Expositions in Mathematics, 53. Walter de Gruyter GmbH & Co. KG, Berlin, (2010).

[20] K. I. Beidar, *A chain of Kurosh may have an arbitrary finite length*, Czechoslovak Math. J. 32(107) (1982), no. 3, 418–422.

[21] G. Ehrlich, *Filial rings*, Portugal. Math. **42** (1983/1984), 185–194.

[22] M. Filipowicz, *Struktura i własności wyróżnionych typów algebr filialnych*, rozprawa doktorska, MIMUW, (2009).

[23] M. Filipowicz, E. R. Puczyłowski, *Left filial rings* Algebra Colloq. **11**(3) (2004), 335–344.

[24] M. Filipowicz, E. R. Puczyłowski, *On filial and left filial rings*, Publ. Math. Debrecen. **66**(3-4) (2005), 257–267.

[25] M. Filipowicz, E. R. Puczyłowski *The Structure of left filial algebras over a field*, Taiwanese J. Math. **13**(3) (2009), pp. 1017-1029.

[26] L. Fuchs, I. Halparin, *On the imbedding of a regular ring in a regular ring with identity*, Fund. Math. **54** (1964), 285-290.

[27] N. Funayama *Imbedding a regular ring with identity* Nagoya Math. J. **27**(1) (1966), 61-64.

[28] L. Fuchs *Infinite abelian groups, volume 1*, Academic Press, London 1970.

[29] P. A. Freidman, *Rings with idealizer condition II*, Ucen. Zap. Ural'sk. Gos. Univ. **2** (1959), 35-48 (Russian).

[30] P. A. Freidman, *Letter to the editors*, Mat. Sb. **52** (94) (1960), 915-916 (Russian).

[31] B. J. Gardner, R. Wiegandt, *Radical theory of rings*, Marcel Dekker, New York 2004.

[32] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed. New York: Springer-Verlag, 1990.

[33] I. Kaplansky, *Modules over Dedekind rings and valuation rings.*, Trans. Amer. Math. Soc. **72** (1952), 327–340.

[34] A. Klein, *A simple proof of a theorem on reduced rings*, Canad. Math. Bull. **23**(4) (1980), 495–496.

[35] R. L. Kruse, *Rings in which all subrings are ideals*, Canad. J. Math., **20** (1968), 862-871.

[36] R. L. Kruse, *Rings with periodic additive group in which all subrings are ideals*, Dissertation, California Institute of Technology, (1964).

[37] R. L. Kruse, D. T. Prince *Nilpotent rings*, Gordon and Breach, Science Publishers, (1969).

[38] A. G. Kurosh, *Radicals of rings and algebras*, Colloq. Math. Soc. János Bolyai, **5** (1971), 297–314. Russian original: Mat Sb. **33(75)** (1953), 13–26.

[39] T. Y. Lam, *A first course in noncommutative rings*, Grad. Texts in Math., 131. Springer-Verlag, New York, 2001.

[40] J. C. Lennox, S. S. Stonehewer *Subnormal Subgroups of Groups*, Clarendor Press, Oxford 1981.

[41] H. Prüfer, *Unendliche abelsche Gruppen von Elementen endlicher Ordnung*, Dissertation, Berlin, 1921.

[42] L. Rédei, *Vollidealringe im weiteren Sinn. I*, Acta Math. Acad. Sci. Hungar. **3** (1952), 243–268.

[43] L. Rédei, *Die Vollidealringe*, Monatsh. Math. **56** (1952), 89–95.

[44] D. J. S. Robinson, *A Course in the Theory of Groups*, Springer-Verlag New York Inc. (1996).

[45] A. D. Sands, *On ideals in over-rings*, Publ. Math. Debrecen **35** (1988), 273–279.

[46] L. Shao-Xue *On algebras in which every subalgebra is an ideal*, Chinese Math. Acta, **5** (1964), pp. 571–577.

[47] F. Szász, *Radical of rings*, Akademiami Kiado, Budapest 1981.

[48] F. Szász, R. Wiegandt *On the dualization of subdirect embeddings* Acta Math. Acad. Sci. Hung., **20** (1969), 289–302.

[49] G. Tzinntzis *An almost subidempotent radical property*, Acta Math. Hung., **49**(1-2) (1987), 173–184.

[50] V. R. Varea, *On lie algebras in which the relation of being an ideal is transitive*, Comm. Algebra. **13**(5) (1985), 1135–1150.

[51] S. Veldsman, *Extensions and ideals of rings*, Publ. Math. Debrecen **38** (1991), 297–309.

[52] E. A. Walker *Cancellation in direct sums of groups*, Proc. Amer. Math. Soc. **7** (1956), 898–902.

[53] http://aragorn.pb.bialystok.pl/∼piotrgr/BanachCenter/meeting.html