Uniwersytet w Białymstoku

Wydział Matematyczno-Fizyczny

Instytut Matematyki

dr hab. Ryszard Andruszkiewicz

Wykład monograficzny

Wykład monograficzny
prowadzony dla studentów V roku matematyki
przez dr hab. Ryszarda Andruszkiewicza

Białystok 2012

Spis treści

Wykład 1

Pojęcie pierścienia

1.1 Określenie pierścienia

Definicja 1.1. System algebraiczny $(R, +, \cdot, 0)$ nazywamy *pierścieniem*, jeżeli spełnia on następujące warunki:

A1. $(R, +, 0)$ jest grupą abelową;

A2. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ dla dowolnych $a, b, c \in R$;

A3. $a \cdot (b+c) = a \cdot b + a \cdot c$ i $(b+c) \cdot a = b \cdot a + c \cdot a$ dla dowolnych $a, b, c \in R$.

Definicja 1.2. Grupę $(R, +, 0)$ będziemy nazywali *grupą addytywnę* pierścienia R i oznaczali przez R^+.

Ważnym przykładem pierścienia jest poznany przez nas na algebrze liniowej, pierścień $M_n(K)$ macierzy kwadratowych stopnia $n \in \mathbb{N}$ o współczynnikach z ciała K.

Definicja 1.3. Jeżeli $a \cdot b = b \cdot a$ dla dowolnych $a, b \in R$, to mówimy, że pierścień R jest *przemienny*.

Przykład 1.4. Niech $(A, +, 0)$ będzie dowolna grupą abelową. W zbiorze A określamy mnożenie przyjmując, że

$$a \cdot b = 0 \text{ dla dowolnych } a, b \in A.$$

Aksjomaty **A2** i **A3** są w oczywisty sposób spełnione, a więc system algebraiczny $(A, +, \cdot, 0)$ jest pierścieniem. Nazywamy go *pierścieniem z zerowym mnożeniem na grupie abelowej* A i oznaczamy przez A^0.

Definicja 1.5. Jeżeli istnieje element $1 \in R$ taki, że $1 \cdot a = a \cdot 1 = a$ dla każdego $a \in R$, to element 1 nazywamy *jedynką* i mówimy, że R jest *pierścieniem z jedynką*.

Zauważmy, że $M_n(K)$ jest pierścieniem z jedynką dla dowolnego ciała K. Jeżeli grupa abelowa $(A, +, 0)$ nie jest trywialna, to pierścień A^0 nie posiada jedynki. Rozliczne przykłady przemiennych pierścieni z jedynką zostały

podane na algebrze ogólnej, w tym: ciała, pierścienie liczbowe, $\mathbb{Z}_m$, pierścienie wielomianów skończonej liczby zmiennych o współczynnikach z dowolnego pierścienia przemiennego z jedynką, pierścienie ilorazowe P/I, gdzie I jest ideałem pierścienia przemiennego P z jedynką.

1.2 Własności działań w pierścieniu

Podamy podstawowe własności działań w dowolnym pierścieniu $(R, +\cdot, 0)$.

Stwierdzenie 1.6. *$a \cdot 0 = 0 \cdot a = 0$ dla każdego $a \in R$.*

DOWÓD. Ponieważ $0 = 0 + 0$, więc $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$ na mocy **A3**, skąd z prawa skracania w grupach mamy, że $a \cdot 0 = 0$. Analogicznie $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$, skąd $0 \cdot a = 0$. □

Stwierdzenie 1.7. *$a \cdot (a_1 + a_2 + \ldots + a_n) = a \cdot a_1 + a \cdot a_2 + \ldots + a \cdot a_n$ oraz $(a_1 + a_2 + \ldots + a_n) \cdot a = a_1 \cdot a + a_2 \cdot a + \ldots + a_n \cdot a$ dla dowolnych $a, a_1, \ldots, a_n \in R$ i dla dowolnego naturalnego n.*

DOWÓD. Prosta indukcja w oparciu o **A3**. □

Odejmowanie w pierścieniu R określamy następująco:

$$a - b \stackrel{def}{=} a + (-b) \text{ dla dowolnych } a, b \in R.$$

Stwierdzenie 1.8. *$a \cdot (b - c) = a \cdot b - a \cdot c$ oraz $(b - c) \cdot a = b \cdot a - c \cdot a$ dla dowolnych $a, b, c \in R$.*

DOWÓD. Na mocy **A3** mamy, że $a \cdot (b - c) + a \cdot c = a \cdot ((b + (-c)) + c) = a \cdot (b + ((-c) + c)) = a \cdot b$, skąd mamy pierwszy wzór. Drugi wzór dowodzi się analogicznie. □

Stwierdzenie 1.9. *$(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$ oraz $(-a) \cdot (-b) = a \cdot b$ dla dowolnych $a, b \in R$.*

DOWÓD. Na mocy **A3** mamy, że $a \cdot b + (-a) \cdot b = ((-a) + a) \cdot b = 0 \cdot b = 0$, na mocy stwierdzenia 1.6. Zatem $(-a) \cdot b = -(a \cdot b)$. Analogicznie $a \cdot (-b) = -(a \cdot b)$. Wynika stąd, że $(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = a \cdot b$. □

Dla dowolnego elementu $a \in R$ możemy określić jego naturalną potęgę przy pomocy wzoru:

$$a^n = \underbrace{a \cdot a \cdot \ldots \cdot a}_{n} \text{ dla dowolnego naturalnego } n.$$

Stwierdzenie 1.10. *$a^n \cdot a^m = a^{n+m}$ oraz $(a^n)^m = a^{nm}$ dla dowolnego $a \in R$ i dla dowolnych liczb naturalnych n, m.*

DOWÓD. Zadanie 1 na ćwiczenia. □

Stwierdzenie 1.11. *Jeżeli $a \cdot b = b \cdot a$, to $a^n \cdot b^m = b^m \cdot a^n$ oraz $(a \cdot b)^n = a^n \cdot b^n$ dla dowolnych liczb naturalnych n, m.*

DOWÓD. Zadanie 2 na ćwiczenia. □

Zadanie (3)**.** Dla dowolnego ciała K znaleźć $A, B \in M_2(K)$ takie, że $(A \cdot B)^2 \neq A^2 \cdot B^2$.

Definicja 1.12. Powiemy, że element $a \in R$ jest *nilpotentny*, jeżeli istnieje liczba naturalna n taka, że $a^n = 0$. Pierścień, którego każdy element jest nilpotentny nazywamy *nil-pierścieniem*. Pierścień nie posiadający niezerowych elementów nilpotentnych nazywamy *pierścieniem zredukowanym*.

Zadanie (4)**.** Udowodnić, że pierścień R jest zredukowany wtedy i tylko wtedy, gdy nie posiada elementu niezerowego x takiego, że $x^2 = 0$.

Zadanie (5)**.** Udowodnić, że jeżeli R jest pierścieniem zredukowanym oraz $a, b \in R$ są takie, że $a \cdot b = 0$, to także $b \cdot a = 0$. Czy jest to prawdą w pierścieniu $M_2(K)$?

Zadanie (6)**.** Niech K będzie dowolnym ciałem. Opisać elementy nilpotentne pierścienia $M_2(K)$. Wykazać, że jeżeli $A \in M_2(K)$ jest elementem nilpotentnym, to $A^2 = 0$.

Zadanie (7)**.** Wyznaczyć wszystkie elementy nilpotentne pierścienia reszt modulo 36.

Zadanie (8)**.** Opisać wszystkie liczby naturalne $m > 1$, dla których pierścień reszt modulo m jest zredukowany.

Dla $a \in R$ i liczby całkowitej k możemy określić całkowitą wielokrotność elementu a przez k w ten sposób, że $k \cdot a = \underbrace{a + a + \ldots + a}_{k}$, gdy $k > 0$, $k \cdot a = 0$, dla $k = 0$ oraz $k \cdot a = \underbrace{(-a) + (-a) + \ldots + (-a)}_{|k|}$, gdy $k < 0$.

Stwierdzenie 1.13. *$(-n) \cdot a = n \cdot (-a) = -(n \cdot a)$, $(n+m) \cdot a = n \cdot a + m \cdot a$, $(nm) \cdot a = n \cdot (m \cdot a)$ i $n \cdot (a + b) = n \cdot a + n \cdot b$ dla dowolnych $a, b \in R$ i dla dowolnych liczb całkowitych n, m.*

DOWÓD. Wynika od razu z teorii grup. □

Stwierdzenie 1.14. *$n \cdot (a \cdot b) = (n \cdot a) \cdot b = a \cdot (n \cdot b)$ dla dowolnych $a, b \in R$ i dla każdego całkowitego n.*

DOWÓD. Wynika od razu ze stwierdzenia 1.13 i wcześniejszych własności. □

Przykład 1.15. Udowodnimy, że jeżeli $x^2 = x$ dla każdego elementu x pierścienia R, to pierścień ten jest przemienny. Weźmy dowolne $x, y \in R$. Wtedy $x + y = (x + y)^2$, więc $x + y = (x + y) \cdot (x + y) = x^2 + x \cdot y + y \cdot x + y^2$. Ale $x^2 = x$ i $y^2 = y$, więc stąd $x \cdot y + y \cdot x = 0$. Ponadto dla $a \in R$ mamy, że $a^2 = a$ oraz $(2a)^2 = 2a$, skąd $4a^2 = 2a$, czyli $4a = 2a$, a więc $2a = 0$. Zatem $a + a = 0$, skąd $a = -a$ dla $a \in R$. Zatem $x \cdot y = -y \cdot x = y \cdot x$ i pierścień R jest przemienny.

Definicja 1.16. Powiemy, że pierścień R jest *dziedziną*, jeżeli $R \neq \{0\}$ oraz dla dowolnych niezerowych elementów $a, b \in R$ mamy, że $a \cdot b \neq 0$.

Definicja 1.17. Mówimy, że element a pierścienia R jest *lewostronnym (prawostronnym) dzielnikiem zera*, jeśli istnieje $0 \neq b \in R$ takie, że $a \cdot b = 0$ $(b \cdot a = 0)$.

Zadanie (9)**.** Udowodnić, że każda skończona dziedzina posiada jedynkę.

1.3 Elementy odwracalne

Niech R będzie pierścieniem z jedynką.

Definicja 1.18. Powiemy, że element $a \in R$ jest *odwracalny* w pierścieniu R, jeżeli istnieje $x \in R$ takie, że $a \cdot x = x \cdot a = 1$ (wówczas x nazywamy elementem odwrotnym do elementu a). Zbiór wszystkich elementów odwracalnych pierścienia R będziemy oznaczali przez R^*.

Zadanie (10)**.** Niech R będzie pierścieniem z jedynką i niech $a, b \in R$. Udowodnić, że jeżeli $1 - a \cdot b \in R^*$, to $1 - b \cdot a \in R^*$.

Zadanie (11)**.** Udowodnij, że jeżeli a jest elementem nilpotentnym pierścienia R z jedynką, to $1 - a \in R^*$.

Twierdzenie 1.19. *Dla dowolnego pierścienia R z jedynką $(R^*, \cdot, 1)$ jest grupą.*

DOWÓD. Ponieważ $1 \cdot 1 = 1$, więc $1 \in R^*$. Jeżeli x jest elementem odwrotnym do elementu $a \in R$, to a jest elementem odwrotnym do x, skąd $x \in R^*$. Jeżeli $a, b \in R^*$, to istnieją $x, y \in R$ takie, że $a \cdot x = x \cdot a = 1$ oraz $b \cdot y = y \cdot b = 1$, skąd $(a \cdot b) \cdot (y \cdot x) = a \cdot (b \cdot y) \cdot x = a \cdot 1 \cdot x = a \cdot x = 1$ oraz $(y \cdot x) \cdot (a \cdot b) = y \cdot (x \cdot a) \cdot b = y \cdot 1 \cdot b = y \cdot b = 1$. Zatem $a \cdot b \in R^*$. Ponieważ mnożenie jest łączne nawet w R, więc jest ono także łączne w R^*. □

Definicja 1.20. Grupę $(R^*, \cdot, 1)$ nazywamy *grupą elementów odwracalnych pierścienia R.*

Definicja 1.21. Pierścień z jedynką $R \neq \{0\}$, w którym każdy niezerowy element jest odwracalny nazywamy *pierścieniem z dzieleniem.*

Zadanie (12)**.** Udowodnić, że każda skończona dziedzina jest pierścieniem z dzieleniem.

1.4 Podpierścienie

Definicja 1.22. *Podpierścieniem* pierścienia R nazywamy każdy taki niepusty jego podzbiór S, że

$$s_1 - s_2 \in S \text{ oraz } s_1 \cdot s_2 \in S \text{ dla dowolnych } s_1, s_2 \in S.$$

Oczywiście każdy podpierścień S pierścienia R jest podgrupą grupy R^+, więc $0 \in S$. Wynika stąd także, że S jest pierścieniem ze względu na działania z R ograniczone do S.

Przykład 1.23. Zbiór $\{0\}$ jest podpierścieniem pierścienia R. Nazywamy go *podpierścieniem zerowym*. R jest podpierścieniem pierścienia R (nazywamy go *podpierścieniem niewłaściwym*).

Stwierdzenie 1.24. *Część wspólna dowolnej niepustej rodziny podpierścieni pierścienia R jest podpierścieniem tego pierścienia.*

DOWÓD. Niech $\{S_t\}_{t\in T}$ będzie niepustą rodziną podpierścieni pierścienia R i niech $S = \bigcap_{t\in T} S_t$. Ponieważ dla każdego $t \in T$ jest $0 \in S_t$, więc $0 \in S$. Weźmy dowolne $a, b \in S$. Wtedy $a, b \in S_t$ dla każdego $t \in T$, skąd $a - b, a \cdot b \in S_t$ dla każdego $t \in T$. Zatem $a - b, a \cdot b \in S$. Stąd S jest podpierścieniem pierścienia R. □

Stwierdzenie 1.25. *Dla dowolnego podzbioru X pierścienia R istnieje najmniejszy w sensie inkluzji podpierścień $[X]$ pierścienia R zawierający X.*

DOWÓD. Oznaczmy przez $\mathcal{X}$ rodzinę wszystkich podpierścieni pierścienia R zawierających zbiór X. Rodzina ta jest niepusta, bo np. $R \in \mathcal{X}$. Zatem na mocy stwierdzenia 1.24 część wspólna $[X]$ tej rodziny jest także podpierścieniem pierścienia R zawierającym zbiór X. Stąd $[X] \in \mathcal{X}$ i $[X]$ jest najmniejszym w sensie inkluzji elementem rodziny $\mathcal{X}$. □

Definicja 1.26. Najmniejszy w sensie inkluzji podpierścień pierścienia R zawierający podzbiór X nazywamy *podpierścieniem generowanym przez podzbiór X* i oznaczamy porzez $[X]$. Zamiast $[\{x_1, \ldots, x_n\}]$ będziemy pisali $[x_1, \ldots, x_n]$.

Przykład 1.27. Zauważmy, że $[\emptyset] = \{0\}$, gdyż $\{0\}$ jest najmniejszym podpierścieniem pierścienia R. Można łatwo wykazać, że dla każdego $a \in R$:

$$[a] = \{k_1 a + k_2 a^2 + \ldots + k_n a^n : \ k_1, k_2, \ldots, k_n \in \mathbb{Z}, \ \ n \in \mathbb{N}\}.$$

Definicja 1.28. *Centralizatorem* niepustego podzbioru X pierścienia R nazywamy zbiór

$$C_R(X) = \{r \in R : r \cdot x = x \cdot r \ \text{ dla każdego } x \in X\}.$$

Stwierdzenie 1.29. *Centralizator $C_R(X)$ dowolnego niepustego podzbioru X pierścienia R jest podpierścieniem pierścienia R.*

Dowód. Oczywiście $0 \in C_R(X)$ (dlaczego?). Niech $a, b \in C_R(X)$. Weźmy dowolne $x \in X$. Wtedy $(a-b)\cdot x = a\cdot x - b\cdot x = x\cdot a - x\cdot b = x\cdot(a-b)$, skąd $a-b \in C_R(X)$. Ponadto $(a\cdot b)\cdot x = a\cdot(b\cdot x) = a\cdot(x\cdot b) = (a\cdot x)\cdot b = (x\cdot a)\cdot b = x\cdot(a\cdot b)$, skąd $a\cdot b \in C_R(X)$. □

Definicja 1.30. Centralizator $C_R(R)$ nazywamy *centrum* pierścienia R i oznaczamy symbolem $Z(R)$. Zatem

$$Z(R) = \{a \in R : a\cdot x = x\cdot a \text{ dla kazdego } x \in R\}.$$

Ze stwierdzenia 1.29 wynika od razu następujący

Wniosek 1.31. *Centrum $Z(R)$ pierścienia R jest przemiennym podpierścieniem pierścienia R.*

Wykład 2

Przykłady pierścieni

2.1 Pierścienie macierzy

Niech R będzie dowolnym pierścieniem. Macierzą kwadratową stopnia n nad pierścieniem R nazywamy tablicę postaci

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}, \tag{2.1}$$

w której $a_{ij} \in R$ dla $i, j = 1, 2, \dots, n$.

Macierz (2.1) będziemy też zapisywali w postaci $A = [a_{ij}]_{i,j=1,2,\dots,n}$. Zbiór wszystkich macierzy kwadratowych stopnia n nad pierścieniem R będziemy oznaczali przez $M_n(R)$. Przyjmujemy umowę, że dla macierzy $A \in M_n(R)$ przez $[A]_{ij}$ oznaczamy element stojący w i-tym wierszu i j-tej kolumnie macierzy A. *Macierzą zerową* nazywamy taką macierz $0_n \in M_n(R)$, że $[0_n]_{ij} = 0$ dla $i, j = 1, 2, \dots, n$. W zbiorze $M_n(R)$ wprowadzamy dodawanie przyjmując, że dla dowolnych macierzy $A, B \in M_n(R)$ macierz $A + B$ jest określona następująco:

$$[A + B]_{ij} = [A]_{ij} + [B]_{ij} \text{ dla wszystkich } i, j = 1, 2, \dots, n. \tag{2.2}$$

Ponieważ dodawanie jest określone po współrzędnych, więc jest jasne, że **system algebraiczny** $(M_n(R), +, 0_n)$ **tworzy grupę abelową**, przy czym macierzą przeciwną do macierzy $A \in M_n(R)$ jest macierz $-A$ taka, że $[-A]_{ij} = -[A]_{ij}$ dla $i, j = 1, 2, \dots, n$.

W zbiorze $M_n(R)$ określamy też naturalne mnożenie macierzy przyjmując, że iloczynem macierzy $A, B \in M_n(R)$ jest macierz $A \cdot B$ taka, że

$$[A \cdot B]_{ij} = \sum_{t=1}^{n} [A]_{it} \cdot [B]_{tj} \text{ dla } i, j = 1, \dots, n. \tag{2.3}$$

Zatem aby pomnożyć macierz $A \in M_n(R)$ przez macierz $B \in M_n(R)$ należy pierwszy wiersz macierzy A pomnożyć (skalarnie) przez pierwszą kolumnę macierzy B, następnie należy pomnożyć pierwszy wiersz macierzy A przez drugą kolumnę macierzy B, itd. W ten sposób uzyskamy kolejne wyrazy pierwszego wiersza macierzy $A \cdot B$. Aby otrzymać drugi wiersz macierzy $A \cdot B$ należy pomnożyć drugi wiersz macierzy A przez kolejne kolumny macierzy B. W końcu należy pomnożyć ostatni wiersz macierzy A kolejno przez wszystkie kolumny macierzy B.

Uwaga 2.1. *Mnożenie macierzy kwadratowych nad dowolnym pierścieniem R jest łączne tzn. dla dowolnych macierzy $A, B, C \in M_n(R)$:*

$$(A \cdot B) \cdot C = A \cdot (B \cdot C).$$

DOWÓD. Dla wszystkich $i, j = 1, 2, \ldots, n$ mamy, że $[(A \cdot B) \cdot C]_{ij} = \sum_{t=1}^{n} [A \cdot B]_{it} \cdot [C]_{tj} = \sum_{t=1}^{n} \left(\sum_{l=1}^{n} [A]_{il} \cdot [B]_{lt} \right) \cdot [C]_{tj} = \sum_{t=1}^{n} \sum_{l=1}^{n} ([A]_{il} \cdot [B]_{lt}) \cdot [C]_{tj} = \sum_{t=1}^{n} \sum_{l=1}^{n} [A]_{il} \cdot ([B]_{lt} \cdot [C]_{tj}) = \sum_{l=1}^{n} \sum_{t=1}^{n} [A]_{il} \cdot ([B]_{lt} \cdot [C]_{tj}) = \sum_{l=1}^{n} \left([A]_{il} \cdot \sum_{t=1}^{n} [B]_{lt} \cdot [C]_{tj} \right) = \sum_{l=1}^{n} [A]_{il} \cdot [B \cdot C]_{lj} = [A \cdot (B \cdot C)]_{ij}$. □

Uwaga 2.2. *Mnożenie macierzy kwadratowych nad dowolnym pierścieniem R jest rozdzielne względem dodawania macierzy tzn.*

(i) $A \cdot (B + C) = A \cdot B + A \cdot C$ dla dowolnych $A, B, C \in M_n(R)$ oraz

(ii) $(B + C) \cdot A = B \cdot A + C \cdot A$ dla dowolnych $A, B, C \in M_n(R)$.

DOWÓD. (i). Wystarczy wykazać, że dla wszystkich $i, j = 1, 2, \ldots, n$ mamy, że $[A \cdot (B + C)]_{ij} = [A \cdot B + A \cdot C]_{ij}$. Ale $[A \cdot (B + C)]_{ij} = \sum_{t=1}^{n} [A]_{it} [B + C]_{tj} = \sum_{t=1}^{n} [A]_{it} \cdot ([B]_{tj} + [C]_{tj}) = \sum_{t=1}^{n} ([A]_{it} \cdot [B]_{tj} + [A]_{it} \cdot [C]_{tj}) = \sum_{t=1}^{n} [A]_{it} \cdot [B]_{tj} + \sum_{t=1}^{n} [A]_{it} \cdot [C]_{tj} = [A \cdot B]_{ij} + [A \cdot C]_{ij} = [A \cdot B + A \cdot C]_{ij}$. (ii) można udowodnić podobnie jak (i). □

Podsumowując uzyskane rezultaty możemy powiedzieć, że tak określony system algebraiczny $(M_n(R), +, \cdot, 0_n)$ jest pierścieniem. Nazywamy go **pierścieniem macierzy kwadratowych stopnia n nad pierścieniem R** i oznaczamy przez $M_n(R)$.

Uwaga 2.3. *Jeżeli 1 jest jedynką pierścienia R, to macierz $I_n \in M_n(R)$ taka, że $[I_n]_{ii} = 1$ dla $i = 1, 2, \ldots, n$ oraz $[I_n]_{ij} = 0$ dla wszystkich $i \neq j$, jest jedynką pierścienia $M_n(R)$. Rzeczywiście, niech $A \in M_n(R)$. Wtedy dla wszystkich $i, j = 1, 2, \ldots, n$ mamy, że $[I_n \cdot A]_{ij} = \sum_{t=1}^{n} [I_n]_{it} \cdot [A]_{tj} = [I_n]_{ii} \cdot [A]_{ij} =$*

$1 \cdot [A]_{ij} = [A]_{ij}$ *oraz* $[A \cdot I_n]_{ij} = \sum_{t=1}^{n} [A]_{it} \cdot [I_n]_{tj} = [A]_{ij} \cdot [I_n]_{jj} = [A]_{ij} \cdot 1 = [A]_{ij}$. *Zatem* $I_n \cdot A = A \cdot I_n = A$ *dla każdego* $A \in M_n(R)$.

Uwaga 2.4. *Niech* a *będzie dowolnym elementem pierścienia* R. *Dla* $i, j \in \{1, 2, \ldots, n\}$ *oznaczmy przez* aE_{ij} *taką macierz kwadratową stopnia* n, *która w* i*-tym wierszu i* j*-tej kolumnie ma element* a, *zaś poza tym same zera. Z definicji mnożenia macierzy bez trudu możemy sprawdzić, że dla dowolnych* $a, b \in R$ *oraz dla dowolnych* $i, j, k.l \in \{1, 2, \ldots, n\}$ *zachodzi wzór:*

$$(aE_{ij}) \cdot (bE_{kl}) = \begin{cases} 0_n & \text{dla} \quad j \neq k \\ (ab)E_{il} & \text{dla} \quad j = k \end{cases} . \tag{2.4}$$

Ponadto dla dowolnej macierzy $A \in M_n(R)$ *mamy, że*

$$A = \sum_{t,s=1}^{n} ([A]_{ts} E_{ts}). \tag{2.5}$$

Twierdzenie 2.5. *Dla* $n \geqslant 2$ *pierścień* $M_n(R)$ *jest przemienny wtedy i tylko wtedy, gdy* $a \cdot b = 0$ *dla dowolnych* $a, b \in R$.

DOWÓD. Załóżmy, że pierścień $M_n(R)$ jest przemienny. Weźmy dowolne $a, b \in R$. Wtedy ze wzoru (2.4) mamy, że $(aE_{11}) \cdot (bE_{12}) = (ab)E_{12}$ oraz $(bE_{12}) \cdot (aE_{11}) = 0_n$. Stąd $(ab)E_{12} = 0_n$, czyli $ab = 0$ dla dowolnych $a, b \in R$.

Na odwrót, niech $a \cdot b = 0$ dla dowolnych $a, b \in R$. Zatem ze wzoru (2.3) mamy, że $A \cdot B = 0_n$ dla dowolnych $A, B \in M_n(R)$. Stąd $A \cdot B = B \cdot A$ dla dowolnych $A, B \in M_n(R)$, czyli pierścień $M_n(R)$ jest przemienny. □

Niech X_{ij} dla $i, j = 1, \ldots, n$ będą niepustymi podzbiorami pierścienia R. Symbolem

$$\begin{bmatrix} X_{11} & X_{12} & \ldots & X_{1n} \\ X_{21} & X_{22} & \ldots & X_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ X_{n1} & X_{n2} & \ldots & X_{nn} \end{bmatrix}$$

będziemy oznaczali zbiór wszystkich macierzy $A \in M_n(R)$ takich, że $[A]_{ij} \in X_{ij}$ dla wszystkich $i, j = 1, \ldots, n$.

Zadanie (1)**.** Pokazać, że jeśli S jest podpierścieniem pierścienia R, to $M_n(S)$ jest podpierścieniem pierścienia $M_n(R)$.

Zadanie (2)**.** Niech R będzie pierścieniem, w którym $a \cdot b \neq 0$ dla pewnych $a, b \in R$. Opisać wszystkie podpierścienie pierścienia $M_2(R)$, które są postaci $\begin{bmatrix} X_1 & X_2 \\ X_3 & X_4 \end{bmatrix}$, gdzie $X_1, X_2, X_3, X_4 \in \{\{0\}, R\}$.

Zadanie (3)**.** Niech R będzie dowolnym pierścieniem. Oznaczmy przez $T_n(R)$ zbiór wszystkich macierzy trójkątnych górnych $A \in M_n(R)$, tzn.

$$T_n(R) = \begin{bmatrix} R & R & \dots & R \\ \{0\} & R & \dots & R \\ \vdots & \vdots & \ddots & \vdots \\ \{0\} & \{0\} & \dots & R \end{bmatrix}.$$

Udowodnić, że $T_n(R)$ jest podpierścieniem pierścienia $M_n(R)$.

Zadanie (4)**.** Niech R będzie dowolnym pierścieniem. Oznaczmy przez $J_n(R)$ zbiór wszystkich macierzy $A \in T_n(R)$ takich, że $[A]_{11} = [A]_{22} \dots = [A]_{nn}$, $[A]_{12} = [A]_{23} = \dots = [A]_{n-1,n}, \dots, [A]_{1,n-1} = [A]_{2n}$. Udowodnić, że $J_n(R)$ jest podpierścieniem pierścienia $T_n(R)$.

2.2 Pierścienie szeregów formalnych i pierścienie wielomianów

Niech R będzie dowolnym pierścieniem. Oznaczmy przez $R[[x]]$ zbiór wszystkich nieskończonych ciągów

$$f = (f_0, f_1, f_2, \dots) \tag{2.6}$$

takich, że $f_i \in R$ dla wszystkich $i = 0, 1, \dots$.

Elementy zbioru $R[[x]]$ nazywamy *szeregami formalnymi* zmiennej x o współczynnikach z pierścienia R. Przyjmujemy umowę, że jeśli szereg nazywa się g, to $g = (g_0, g_1, g_2, \dots)$, czyli $g_0, g_1, g_2, \dots$ są jego kolejnymi współczynnikami. Przy tych oznaczeniach dla szeregów $f, g \in R[[x]]$ mamy, że

$$f = g \iff f_i = g_i \text{ dla każdego } i = 0, 1, 2, \dots. \tag{2.7}$$

Szereg $0 = (0, 0, 0, \dots)$ nazywamy *zerowym*, zaś szereg $(f_0, 0, 0, \dots)$ nazywamy *szeregiem stałym*. Jeżeli $f \neq 0$, to istnieje najmniejsze n takie, że $f_n \neq 0$ i wówczas n nazywamy *stopniem szeregu* f i piszemy $st(f) = n$, zaś f_n nazywamy *najmłodszym współczynnikiem* tego szeregu. Ponadto przyjmujemy, że $st(0) = \infty$ oraz dla $n \in \mathbb{N}_0$: $\infty > n$, $\infty + n = \infty + \infty = \infty$.

Sumą szeregów $f, g \in R[[x]]$ nazywamy szereg

$$f + g = (f_0 + g_0, f_1 + g_1, f_2 + g_2, \dots). \tag{2.8}$$

Łatwo zauważyć, że dla dowolnych szeregów $f, g \in R[[x]]$:

$$st(f + g) \geqslant \min\{st(f), st(g)\}. \tag{2.9}$$

Jeżeli zaś $st(f) < st(g)$, to oczywiście $st(f+g) = st(f)$.

Z określenia dodawania szeregów łatwo wynika, że system algebraiczny $(R[[x]], +, 0)$ jest grupą abelową, przy czym *szeregiem przeciwnym* do szeregu f jest szereg $-f = (-f_0, -f_1, -f_2, \ldots)$.

Iloczynem szeregów $f, g \in R[[x]]$ nazywamy szereg

$$f \cdot g = (f_0 g_0, f_0 g_1 + f_1 g_0, f_0 g_2 + f_1 g_1 + f_2 g_0, \ldots). \tag{2.10}$$

Zatem dla każdego $n \in \mathbb{N}_0$:

$$(f \cdot g)_n = \sum_{i=0}^{n} f_i g_{n-i} = \sum_{i+j=n} f_i g_j. \tag{2.11}$$

Jeżeli $f_i = 0$ dla $i = 1, 2, \ldots$, to ze wzoru (2.11) wynika, że

$$(f_0, 0, 0, \ldots) \cdot (g_0, g_1, g_2, \ldots) = (f_0 g_0, f_0 g_1, f_0 g_2, \ldots). \tag{2.12}$$

Jeżeli zaś $f_i = 0$ dla $i = 0, 2, 3, \ldots$, to ze wzoru (2.11) wynika, że

$$(0, f_1, 0, 0, \ldots) \cdot (g_0, g_1, g_2, \ldots) = (0, f_1 g_0, f_1 g_1, f_1 g_2, \ldots). \tag{2.13}$$

Niech teraz $f, g \in R[[x]] \setminus \{0\}$ i $n = st(f)$ oraz $m = st(g)$. Wtedy $(f \cdot g)_k = 0$ dla wszystkich $k < n + m$. Rzeczywiście, $(f \cdot g)_k = \sum_{i+j=k} f_i g_j$ oraz $f_i = 0$ dla $i < n$, zaś dla $i \geqslant n$ jest $j < m$, więc $g_j = 0$. Stąd i z (2.11) mamy, że dla dowolnych szeregów $f, g \in R[[x]]$:

$$st(f \cdot g) \geqslant st(f) + st(g). \tag{2.14}$$

Teraz udowodnimy, że mnożenie szeregów jest rozdzielne względem ich dodawania oraz, że mnożenie szeregów jest łączne. W tym celu weźmy dowolne $f, g, h \in R[[x]]$. Wtedy dla $n \in \mathbb{N}_0$ mamy, że

$$(f \cdot (g+h))_n = \sum_{i+j=n} f_i (g+h)_j = \sum_{i+j=n} f_i (g_j + h_j) = \sum_{i+j=n} (f_i g_j + f_i h_j)$$

$$= \sum_{i+j=n} f_i g_j + \sum_{i+j=n} f_i h_j = (f \cdot g)_n + (f \cdot h)_n = (f \cdot g + f \cdot h)_n,$$

skąd $f \cdot (g+h) = f \cdot g + f \cdot h$. Analogicznie pokazuje się, że $(g+h) \cdot f = g \cdot f + h \cdot f$.

Ponadto $((f \cdot g) \cdot h)_n = \sum_{i+j=n} (f \cdot g)_i h_j = \sum_{i+j=n} \sum_{s+t=i} (f_s g_t) h_j =$ $\sum_{s+t+j=n} (f_s g_t) h_j$ oraz $(f \cdot (g \cdot h))_n = \sum_{s+k=n} f_s (g \cdot h)_k = \sum_{s+k=n} \sum_{t+j=k} f_s (g_t h_j)$ $= \sum_{s+t+j=n} f_s (g_t h_j)$, więc $f \cdot (g \cdot h) = (f \cdot g) \cdot h$. W ten sposób udowodniliśmy następujące

Twierdzenie 2.6. *Dla dowolnego pierścienia R system algebraiczny $(R[[x]], +, \cdot, 0)$ tworzy pierścień.* □

Ten pierścień nazywamy *pierścieniem szeregów formalnych zmiennej x* o współczynnikach z pierścienia R.

Zadanie (5)**.** Udowodnij, że pierścień $R[[x]]$ jest przemienny wtedy i tylko wtedy, gdy pierścień R jest przemienny.

Zadanie (6)**.** Udowodnij, że jeżeli 1 jest jedynką pierścienia R, to $(1, 0, 0, \ldots)$ jest jedynką pierścienia $R[[x]]$.

Zadanie (7)**.** Udowodnij, że jeżeli S jest podpierścieniem pierścienia R, to $S[[x]]$ jest podpierścieniem pierścienia $R[[x]]$.

Definicja 2.7. *Wielomianem zmiennej x o współczynnikach z pierścienia R* nazywamy taki szereg $f \in R[[x]]$, że $0 = f_n = f_{n+1} = f_{n+2} = \ldots$ dla pewnego $n \in \mathbb{N}_0$. Zbiór wszystkich wielomianów $f \in R[[x]]$ oznaczamy przez $R[x]$.

Stwierdzenie 2.8. *Dla dowolnego pierścienia R, $R[x]$ jest podpierścieniem pierścienia $R[[x]]$.*

DOWÓD. Oczywiście $R[x] \neq \emptyset$, bo np. $0 \in R[x]$. Weźmy dowolne $f, g \in R[x]$. Wtedy istnieją $n, m \in \mathbb{N}_0$ takie, że $0 = f_n = f_{n+1} = \ldots$ i $0 = g_m = g_{m+1} = \ldots$. Niech $k = \max\{n, m\}$. Wtedy $0 = f_k = f_{k+1} = \ldots$ i $0 = g_k = g_{k+1} = \ldots$, skąd $0 = (f-g)_k = (f-g)_{k+1} = \ldots$, a więc $f - g \in R[x]$. Weźmy dowolne $s > n+m$ oraz $i, j \in \mathbb{N}_0$ takie, że $i + j = s$. Jeśli $i > n$, to $f_i = 0$, więc $f_i g_j = 0$; jeśli zaś $i \leqslant n$, to $j = s - i \geqslant s - n > n + m - n = m$, więc $g_j = 0$, czyli $f_i g_j = 0$. Stąd na mocy wzoru (2.11), $(f \cdot g)_s = 0$. W konsekwencji $f \cdot g \in R[x]$. □

Otrzymany w ten sposób pierścień $R[x]$ nazywamy *pierścieniem wielomianów zmiennej x o współczynnikach z pierścienia R.*

Zadanie (8)**.** Udowodnij, że jeżeli S jest podpierścieniem pierścienia R, to $S[x]$ jest podpierścieniem pierścienia $R[x]$.

Zadanie (9)**.** Udowodnij, że pierścień $R[x]$ jest przemienny wtedy i tylko wtedy, gdy pierścień R jest przemienny.

2.3 Iloczyn prosty i suma prosta pierścieni

Dla dowolnego niepustego zbioru indeksów T niech $\{R_t\}_{t \in T}$ będzie rodziną pierścieni. Przypomnijmy, że iloczym kartezjański $R = \prod_{t \in T} R_t$ składa się ze wszystkich funkcji $f \colon T \to \bigcup_{t \in T} R_t$ takich, że $f(t) \in R_t$ dla wszystkich $t \in T$, przy czym można utożsamiać f z uogólnionym ciągiem $(x_t)_{t \in T}$, gdzie $x_t = f(t)$ dla $t \in T$. W zbiorze R wprowadzamy dodawanie i mnożenie "po współrzędnych":

$$(x_t)_{t \in T} + (y_t)_{t \in T} = (x_t + y_t)_{t \in T}, \tag{2.15}$$

$$(x_t)_{t\in T}\cdot(y_t)_{t\in T}=(x_t\cdot y_t)_{t\in T}. \tag{2.16}$$

Łatwo wykazać (Zadanie (10) na ćwiczenia), że wówczas $(R,+,\cdot)$ jest pierścieniem. Nazywamy go *iloczynem prostym rodziny pierścieni* $\{R_t\}_{t\in T}$ i oznaczamy przez $\prod_{t\in T}R_t$. Oznaczmy przez $\bigoplus_{t\in T}R_t$ zbiór tych wszystkich $f\in\prod_{t\in T}R_t$, dla których $f(t)\neq 0$ jedynie dla skończenie wielu $t\in T$. Nietrudno jest pokazać (Zadanie 11 na ćwiczenia), że $\bigoplus_{t\in T}R_t$ jest podpierścieniem pierścienia $\prod_{t\in T}R_t$. Nazywamy go *sumą prostą rodziny pierścieni* $\{R_t\}_{t\in T}$ i oznaczamy przez $\bigoplus_{t\in T}R_t$.

Zadanie (12)**.** Udowodnij, że jeżeli $\{R_t\}_{t\in T}$ jest nieskończoną rodziną niezerowych pierścieni, to pierścień $\bigoplus_{t\in T}R_t$ nie posiada jedynki.

Zadanie (13)**.** Udowodnij, że jeżeli 1_t jest jedynką pierścienia R_t dla $t\in T$, to $(1_t)_{t\in T}$ jest jedynką pierścienia $\prod_{t\in T}R_t$ oraz $(\prod_{t\in T}R_t)^*=\prod_{t\in T}R_t^*$.

Zadanie (14)**.** Niech $\{R_t\}_{t\in T}$ będzie niepustą rodziną pierścieni. Udowodnij, że pierścień $\prod_{t\in T}R_t$ jest przemienny wtedy i tylko wtedy, gdy dla każdego $t\in T$ pierścień R_t jest przemienny.

Zadanie (15)**.** Niech $\{R_t\}_{t\in T}$ będzie niepustą rodziną pierścieni. Udowodnij, że pierścień $\bigoplus_{t\in T}R_t$ jest przemienny wtedy i tylko wtedy, gdy dla każdego $t\in T$ pierścień R_t jest przemienny.

Wykład 3

Ideały jednostronne pierścieni

3.1 Iloczyny algebraiczne podgrup w pierścieniu

Definicja 3.1. *Iloczynem algebraicznym podgrup* A, B grupy addytywnej pierścienia R nazywamy podgrupę $A \cdot B$ grupy R^+ generowaną przez wszystkie elementy $a \cdot b$ dla $a \in A$, $b \in B$. Innymi słowy $A \cdot B$ jest najmniejszą w sensie inkluzji podgrupą grupy R^+ zawierającą wszystkie elementy $a \cdot b$ dla $a \in A$, $b \in B$.

Stwierdzenie 3.2. *Dla dowolnych podgrup A, B grupy addytywnej pierścienia R zachodzi wzór:*

$$A \cdot B = \{\sum_{i=1}^{n} a_i b_i : a_1, \ldots, a_n \in A; b_1, \ldots, b_n \in B; n \in \mathbb{N}\}. \tag{3.1}$$

Dowód. Oznaczmy prawą stronę wzoru (3.1) przez C. Wtedy $ab \in C$ dla dowolnych $a \in A$, $b \in B$, skąd $C \neq \emptyset$. Weźmy dowolne $x, y \in C$. Wtedy $x = \sum_{i=1}^{n} a_i b_i$, $y = \sum_{j=1}^{m} c_j d_j$ dla pewnych $a_1, \ldots, a_n, c_1, \ldots, c_m \in A$, $b_1, \ldots, b_n, d_1, \ldots, d_m \in B$. Stąd na mocy stwierdzenia 1.9: $x - y = \sum_{i=1}^{n} a_i b_i + \sum_{j=1}^{m} (-c_j) d_j \in C$, bo $-c_j \in A$ dla $j = 1, \ldots, m$. Zatem C jest podgrupą grupy R^+ zawierającą wszystkie elementy ab dla $a \in A$, $b \in B$.

Niech teraz M będzie dowolną podgrupą grupy R^+ zawierającą wszystkie ab dla $a \in A$, $b \in B$. Weźmy dowolne $n \in \mathbb{N}$ oraz dowolne $a_1, \ldots, a_n \in A$, $b_1, \ldots, b_n \in B$. Wtedy $a_i b_i \in M$ dla $i = 1, \ldots, n$, skąd $\sum_{i=1}^{n} a_i b_i \in M$. Zatem $C \subseteq M$. Oznacza to, że C jest najmniejszą podgrupą grupy R^+ zawierającą wszystkie elementy ab dla $a \in A$, $b \in B$, czyli $C = A \cdot B$. □

Dla dowolnego elementu a pierścienia R przez $\langle a\rangle$ będziemy oznaczali podgrupę grupy R^+ generowaną przez element a. Zatem

$$\langle a\rangle = \{ka : k \in \mathbb{Z}\}. \tag{3.2}$$

Jeżeli A jest podgrupą grupy R^+, to dla $a \in R$ przyjmujemy następujące oznaczenia:

$$aA = \{a \cdot x : x \in A\} \text{ oraz } Aa = \{x \cdot a : x \in A\}. \tag{3.3}$$

Stwierdzenie 3.3. *Dla dowolnych elementów a, b pierścienia R i dla dowolnej podgrupy A grupy R^+ zachodzą następujace wzory:*
(i) $aA = \langle a\rangle \cdot A$,
(ii) $Aa = A \cdot \langle a\rangle$,
(iii) $\langle a\rangle \cdot \langle b\rangle = \langle a \cdot b\rangle$.
W szczególności aA i Aa są podgrupami grupy R^+.

DOWÓD. Z (3.2) i (3.3) wynika od razu, że $aA \subseteq \langle a\rangle \cdot A$. Weźmy dowolne $x \in \langle a\rangle \cdot A$. Wtedy ze stwierdzenia 3.2 i ze wzoru (3.2), $x = \sum_{i=1}^{n} (k_i a)b_i$ dla pewnych $k_1, \ldots, k_n \in \mathbb{Z}$, $b_1, \ldots, b_n \in A$. Zatem ze stwierdzeń 1.7 i 1.14, $x = a \cdot \sum_{i=1}^{n} k_i b_i$. Ale A jest podgrupą grupy R^+, więc $\sum_{i=1}^{n} k_i b_i \in A$, skąd $x \in aA$. Zatem $aA = \langle a\rangle \cdot A$. Analogicznie dowodzimy wzoru *(ii)*.

Z *(i)* oraz ze wzorów (3.2) i (3.3) mamy, że $\langle a\rangle \cdot \langle b\rangle = a\langle b\rangle = \{a(kb) : k \in \mathbb{Z}\}$. Stąd i ze stwierdzenia 1.14 oraz ze wzoru (3.2), $\langle a\rangle \cdot \langle b\rangle = \{k(ab) : k \in \mathbb{Z}\} = \langle ab\rangle$. □

Stwierdzenie 3.4. *Dla dowolnych podgrup A, B, C grupy addytywnej pierścienia R zachodzą następujące wzory:*
(i) $(A \cdot B) \cdot C = A \cdot (B \cdot C)$,
(ii) $A \cdot (B + C) = A \cdot B + A \cdot C$,
(iii) $(B + C) \cdot A = B \cdot A + C \cdot A$.

DOWÓD. Weźmy dowolne $x \in (A \cdot B) \cdot C$. Ze stwierdzenia 3.2, x jest skończoną sumą elementów postaci $y \cdot c$ dla $y \in A \cdot B$, $c \in C$. Ponadto ze stwierdzenia 3.2 każde $y \in A \cdot B$ jest skończoną sumą elementów postaci $a \cdot b$ dla pewnych $a \in A$, $b \in B$. Stąd na mocy stwierdzenia 1.7 x jest skończoną sumą elementów postaci $(a \cdot b) \cdot c$ dla pewnych $a \in A$, $b \in B$, $c \in C$. Ale $(a \cdot b) \cdot c = a \cdot (b \cdot c) \in A \cdot (B \cdot C)$, gdyż $a \in A$ oraz $b \cdot c \in B \cdot C$, więc $x \in A \cdot (B \cdot C)$. Stąd $(A \cdot B) \cdot C \subseteq A \cdot (B \cdot C)$. Przeciwną inkluzję dowodzi się analogicznie. Zatem $(A \cdot B) \cdot C = A \cdot (B \cdot C)$.

Weźmy dowolne $x \in A \cdot (B + C)$. Ze stwierdzenia 3.2 x jest skończoną sumą elementów postaci $a \cdot y$ dla pewnych $a \in A$, $y \in B + C$. Stąd $y = b + c$ dla pewnych $b \in B$, $c \in C$ i $a \cdot y = a \cdot b + a \cdot c \in A \cdot B + A \cdot C$. Zatem $x \in A \cdot B + A \cdot C$ i wobec tego $A \cdot (B + C) \subseteq A \cdot B + A \cdot C$. Ponadto $B \subseteq B + C$ i $C \subseteq B + C$, więc $A \cdot B, A \cdot C \subseteq A \cdot (B + C)$, skąd $A \cdot B + A \cdot C \subseteq A \cdot (B + C)$. W konsekwencji $A \cdot (B + C) = A \cdot B + A \cdot C$. Dowód wzoru *(iii)* jest analogiczny. □

Ze stwiedzenia 3.4 (i) wynika, że iloczyn algebraiczny podgrup jest działaniem łącznym w zbiorze wszystkich podgrup grupy addytywnej pierścienia R. Z tego powodu dla dowolnego $n \in \mathbb{N}$ i dla dowolnych podgrup $A_1, \ldots, A_n$ grupy R^+ wartość iloczynu $A_1 \cdot \ldots \cdot A_n$ nie zależy od sposobu rozstawienia nawiasów. Ponadto ze stwierdzenia 3.2 przez prostą indukcję można wykazać, że podgrupa $A_1 \cdot \ldots \cdot A_n$ składa się ze wszystkich skończonych sum elementów postaci $a_1 \cdot \ldots \cdot a_n$ dla $a_i \in A_i$, $i = 1, \ldots, n$. Jeżeli A jest podgrupą grupy R^+, to zamiast $\underbrace{A \cdot \ldots \cdot A}_{n}$ będziemy pisali A^n. Ponadto ze stwierdzenia 3.4 przez prostą indukcję mamy, że dla dowolnego $n \in \mathbb{N}$ i dla dowolnych podgrup $A, A_1, \ldots, A_n$ grupy R^+ zachodzą wzory:

$$A \cdot (A_1 + \ldots + A_n) = A \cdot A_1 + \ldots + A \cdot A_n, \tag{3.4}$$

$$(A_1 + \ldots + A_n) \cdot A = A_1 \cdot A + \ldots + A_n \cdot A. \tag{3.5}$$

Zadanie (1)**.** Udowodnij, że dla dowolnych podgrup A i B grupy addytywnej pierścienia R i dla dowolnych $a, b \in R$: $\langle a \rangle \cdot A \cdot \langle b \rangle = \{a \cdot x \cdot b : x \in A\}$ oraz $(AB)a = A(Ba)$.

3.2 Ideały lewostronne pierścieni

Definicja 3.5. Niepusty podzbiór $L \subseteq R$ nazywamy *ideałem lewostronnym* pierścienia R, jeżeli:
(1) $l_1 - l_2 \in L$ dla dowolnych $l_1, l_2 \in L$ oraz
(2) $r \cdot l \in L$ dla dowolnych $r \in R$, $l \in L$.
Piszemy wtedy: $L <_l R$.

Z tej definicji wynika od razu, że każdy ideał lewostronny jest podgrupą grupy addytywnej, a nawet jest podpierścieniem pierścienia R. Ponadto $L \subseteq R$ jest ideałem lewostronnym pierścienia R wtedy i tylko wtedy, gdy L jest podgrupą grupy R^+ i $RL \subseteq L$.

Przykład 3.6. Zbiór $\{0\}$ jest ideałem lewostronnym pierścienia R. Nazywamy go *ideałem lewostronnym zerowym*. R jest ideałem lewostronnym pierścienia R. Nazywamy go *ideałem lewostronnym niewłaściwym*.

Przykład 3.7. Dla dowolnego elementu a pierścienia R na mocy stwierdzenia 3.3, Ra jest podgrupą grupy R^+ oraz $R(Ra) = (RR)a \subseteq Ra$. Zatem $Ra <_l R$. Ogólniej: jeśli $L <_l R$, to dla dowolnej podgrupy X grupy R^+, LX jest podgrupą w R^+ oraz $R(LX) = (RL)X \subseteq LX$, a więc $LX <_l R$. W szczególności, jeżeli $L, M <_l R$, to $L \cdot M <_l R$. Jeżeli $L_i <_l R$ dla $i = 1, \ldots, n$, to $R(L_1 \cdot \ldots \cdot L_n) = (R \cdot L_1) \cdot \ldots \cdot L_n \subseteq L_1 \cdot \ldots \cdot L_n$, a więc $L_1 \cdot \ldots \cdot L_n <_l R$.

Przykład 3.8. Dla dowolnego elementu a pierścienia R, $\langle a \rangle + Ra = \{ka + r \cdot a : k \in \mathbb{Z}, r \in R\}$ jest podgrupą grupy R^+ oraz na mocy stwierdzeń 3.4 i 3.3,

$R(\langle a\rangle + Ra) = R\langle a\rangle + R(Ra) = Ra + (RR)a \subseteq Ra \subseteq \langle a\rangle + Ra$. Zatem $\langle a\rangle + Ra$ jest ideałem lewostronnym pierścienia R zawierającym element a. Jeżeli L jest ideałem lewostronnym pierścienia R zawierającym a, to $\langle a\rangle \subseteq L$ i $Ra \subseteq L$, skąd $\langle a\rangle + Ra \subseteq L$. Zatem $\langle a\rangle + Ra$ jest najmniejszym ideałem lewostronnym pierścienia R zawierającym element a. Nazywamy go *ideałem lewostronnym pierścienia R generowanym przez a.*

Przykład 3.9. Niech A będzie dowolną podgrupą grupy addytywnej pierścienia R. Wówczas $A+RA$ jest podgrupą w R^+ oraz $R\cdot(A+RA) = RA+R(RA) = RA + (RR)A \subseteq RA \subseteq A + RA$, a więc $A + RA <_l R$. Ponadto $A \subseteq A + RA$. Jeżeli L jest ideałem lewostronnym pierścienia R takim, że $A \subseteq L$, to $RA \subseteq L$, skąd $A + RA \subseteq L$. Zatem $A + RA$ jest najmniejszym ideałem lewostronnym pierścienia R zawierającym podgrupę A. Nazywamy go *ideałem lewostronnym pierścienia R generowanym przez podgrupę A.*

Przykład 3.10. Uzasadnimy, że dla dowolnego podzbioru X pierścienia R istnieje najmniejszy ideał lewostronny pierścienia R zawierający X. Niech $\langle X\rangle$ oznacza najmniejszą podgrupę grupy R^+ zawierającą podzbiór X. Wtedy $\langle X\rangle + R\langle X\rangle <_l R$ oraz $X \subseteq \langle X\rangle + R\langle X\rangle$. Niech L będzie dowolnym ideałem lewostronnym pierścienia R zawierającym X. Ponieważ L jest podgrupą w R^+, więc $\langle X\rangle \subseteq L$. Zatem z przykładu 3.9 $\langle X\rangle + R\langle X\rangle \subseteq L$. Stąd $\langle X\rangle + R\langle X\rangle$ jest najmniejszym ideałem lewostronnym pierścienia R zawierającym podzbiór X. Nazywamy go *ideałem lewostronnym pierścienia R generowanym przez podzbiór X.*

Przykład 3.11. Część wspólna dowolnej niepustej rodziny $\{L_t\}_{t\in T}$ ideałów lewostronnych pierścienia R jest ideałem lewostronnym pierścienia R. Rzeczywiście, ponieważ ideały lewostronne są podpierścieniami R, więc $L = \bigcap_{t\in T} L_t$ też jest podpierścieniem pierścienia R. Ponadto dla $r \in R$ oraz $l \in L$ mamy, że $l \in L_t$ dla każdego $t \in T$, skąd $r \cdot l \in L_t$ dla każdego $t \in T$. Zatem $r \cdot l \in L$ i L jest ideałem lewostronnym pierścienia R.

Przykład 3.12. Suma algebraiczna skończonej liczby ideałów lewostronnych pierścienia R jest ideałem lewostronnym tego pierścienia. Mianowicie, jeżeli $L_1, L_2, \ldots, L_n$ są ideałami lewostronnymi pierścienia R, to $L_1+L_2+\ldots+L_n = \{l_1 + l_2 + \ldots + l_n : l_i \in L_i \text{ dla } i = 1, 2, \ldots, n\}$ jest ideałem lewostronnym pierścienia R zawierającym wszystkie ideały $L_1, L_2, \ldots, L_n$. Rzeczywiście, dla $a \in L_i$ mamy, że $a = \underbrace{0+\ldots+0}_{i-1}+a+\underbrace{0+\ldots+0}_{n-i}$ dla $i = 1, \ldots, n$, skąd $L_i \subseteq L_1+\ldots+L_n$ dla $i = 1, \ldots, n$. Ponadto ideały lewostronne są podgrupami grupy abelowej R^+, więc ich suma algebraiczna jest też podrupą tej grupy. W końcu dla $r \in R$ oraz $l_i \in L_i$, $i = 1, \ldots, n$ mamy, że $r \cdot (l_1 + \ldots + l_n) = r \cdot l_1 + \ldots + r \cdot l_n \in L_1 + \ldots + L_n$, bo $r \cdot l_i \in L_i$ dla $i = 1, \ldots, n$. Zatem $L_1 + L_2 + \ldots + L_n <_l R$.

Przykład 3.13. Niech X będzie dowolnym niepustym podzbiorem pierścienia R. *Lewostronnym anihilatorem zbioru X w pierścieniu R* nazywamy podzbiór

$l_R(X) = \{r \in R : r \cdot x = 0 \text{ dla każdego } x \in X\}$. Zauważmy, że $0 \in l_R(X)$, bo $0 \cdot r = 0$ nawet dla każdego $r \in R$. Jeśli $a, b \in l_R(X)$, to dla $x \in X$ mamy, że $(a-b) \cdot x = a \cdot x - b \cdot x = 0 - 0 = 0$, skąd $a - b \in l_R(X)$. Niech $r \in R$ oraz $a \in l_R(X)$. Wtedy dla $x \in X$ mamy, że $(r \cdot a) \cdot x = r \cdot (a \cdot x) = r \cdot 0 = 0$, skąd $r \cdot a \in l_R(X)$. Zatem rzeczywiście $l_R(X) <_l R$. Ponadto $l_R(X)X = \{0\}$.

Zadanie (2)**.** Udowodnij, że dla dowolnego $a \in R$ podzbiór $L = \{x - x \cdot a : x \in R\}$ jest ideałem lewostronnym pierścienia R.

Zadanie (3)**.** Niech R będzie pierścieniem z jedynką i niech $L <_l M_2(R)$. Udowodnij, że jeżeli $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in L$, to $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ a & b \end{bmatrix}, \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ c & d \end{bmatrix} \in L$.

Zadanie (4)**.** Udowodnij, że jeżeli L i M są ideałami lewostronnymi pierścienia R, to $\begin{bmatrix} L & M \\ L & M \end{bmatrix} <_l M_2(R)$.

Zadanie (5)**.** Niech K będzie dowolnym ciałem. Opisać wszystkie ideały lewostronne pierścienia macierzy $M_2(K)$.

Zadanie (6)**.** Niech L_t będzie ideałem lewostronnym pierścienia R_t dla każdego $t \in T$. Udowodnij, że wtedy $\prod_{t\in T} L_t <_l \prod_{t\in T} R_t$.

Zadanie (7)**.** Niech R i S będą pierścieniami, z których co najmniej jeden posiada jedynkę. Udowodnij, że wszystkimi ideałami lewostronnymi pierścienia $R \times S$ są jedynie podzbiory postaci $L \times M$, gdzie $L <_l R$ i $M <_l S$.

Zadanie (8)**.** W pierścieniu $2\mathbb{Z} \times 2\mathbb{Z}$ znajdź ideał lewostronny, który nie jest postaci $L \times M$ dla $L, M <_l 2\mathbb{Z}$.

3.3 Ideały prawostronne pierścieni

Definicja 3.14. *Ideałem prawostronnym* pierścienia R nazywamy niepusty podzbiór $P \subseteq R$ taki, że

(1) $p_1 - p_2 \in P$ dla dowolnych $p_1, p_2 \in P$ oraz

(2) $p \cdot r \in P$ dla dowolnych $p \in P$, $r \in R$.

Piszemy wtedy $P <_r R$.

Z tej definicji wynika od razu, że każdy ideał prawostronny jest podgrupą grupy addytywnej, a nawet jest podpierścieniem pierścienia R. Ponadto $P \subseteq R$ jest ideałem prawostronnym pierścienia R wtedy i tylko wtedy, gdy P jest podgrupą grupy R^+ i $PR \subseteq P$.

Uwaga 3.15. *Niech $(R, +, \cdot, 0)$ będzie dowolnym pierścieniem. W zbiorze R wprowadzamy nowe mnożenie $*$ przyjmujac, że*

$$a * b = b \cdot a \text{ dla dowolnych } a, b \in R. \tag{3.6}$$

Łatwo sprawdzić, że $(R, +, *, 0)$ *jest pierścieniem. Nazywamy go* pierścieniem R z odwróconym mnożeniem *i oznaczamy przez* R^{op}. *Wprost z definicji* R^{op} *wynika, że dla dowolnego* $A \subseteq R$*:*

$$A <_r R \iff A <_l R^{op} \text{ oraz } A <_l R \iff A <_r R^{op}.$$

Przykład 3.16. Zbiór $\{0\}$ jest ideałem prawostronnym pierścienia R. Nazywamy go *ideałem prawostronnym zerowym* pierścienia R. R jest ideałem prawostronnym pierścienia R. Nazywamy go *ideałem prawostronnym niewłaściwym pierścienia* R.

Przykład 3.17. Dla dowolnego elementu a pierścienia R na mocy uwagi 3.15 i przykładu 3.7, $aR <_r R$. Ogólniej: jeśli $P <_r R$, to dla dowolnej podgrupy X grupy R^+, $XP <_r R$. W szczególności, jeżeli $P, Q <_r R$, to $P \cdot Q <_r R$. Jeżeli $P_i <_l R$ dla $i = 1, \ldots, n$, to $P_1 \cdot \ldots \cdot P_n <_r R$.

Przykład 3.18. Na mocy uwagi 3.15 i przykładu 3.8, dla dowolnego elementu a pierścienia R, $\langle a \rangle + aR = \{ka + a \cdot r : k \in \mathbb{Z}, r \in R\}$ jest najmniejszym ideałem prawostronnym pierścienia R zawierającym element a. Nazywamy go *ideałem prawostronnym pierścienia* R *generowanym przez* a.

Przykład 3.19. Na mocy uwagi 3.15 i przykładu 3.9, dla dowolnej podgrupy A grupy addytywnej pierścienia R, $A + AR$ jest najmniejszym ideałem prawostronnym pierścienia R zawierającym A. Nazywamy go *ideałem prawostronnym pierścienia* R *generowanym przez podgrupę* A.

Przykład 3.20. Na mocy uwagi 3.15 i przykładu 3.10, dla dowolnego podzbioru X pierścienia R, $\langle X \rangle + \langle X \rangle R$ jest najmniejszym ideałem prawostronnym pierścienia R zawierającym X. Nazywamy go *ideałem prawostronnym pierścienia* R *generowanym przez podzbiór* X.

Przykład 3.21. Na mocy uwagi 3.15 i przykładu 3.11, część wspólna dowolnej niepustej rodziny $\{P_t\}_{t \in T}$ ideałów prawostronnych pierścienia R jest ideałem prawostronnym pierścienia R.

Przykład 3.22. Na mocy uwagi 3.15 i przykładu 3.12, suma algebraiczna skończonej liczby ideałów prawostronnych pierścienia R jest ideałem prawostronnym tego pierścienia.

Przykład 3.23. Niech X będzie niepustym podzbiorem pierścienia R. *Prawostronnym anihilatorem podzbioru* X nazywamy podzbiór: $r_R(X) = \{r \in R : x \cdot r = 0 \text{ dla każdego } x \in X\}$. Na mocy uwagi 3.15 i przykładu 3.13 mamy, że $r_R(X) <_r R$.

Zadanie (9)**.** Udowodnij, że dla dowolnego $a \in R$ podzbiór $P = \{x - a \cdot x : x \in R\}$ jest ideałem prawostronnym pierścienia R.

Zadanie (10)**.** Niech R będzie pierścieniem z jedynką i niech $P <_r M_2(R)$. Udowodnij, że jeżeli $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in P$, to $\begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix}, \begin{bmatrix} 0 & a \\ 0 & c \end{bmatrix}, \begin{bmatrix} 0 & b \\ 0 & d \end{bmatrix}, \begin{bmatrix} b & 0 \\ d & 0 \end{bmatrix} \in P$.

Zadanie (11)**.** Udowodnij, że jeżeli P i Q są ideałami prawostronnymi pierścienia R, to $\begin{bmatrix} P & P \\ Q & Q \end{bmatrix} <_r M_2(R)$.

Zadanie (12)**.** Niech K będzie dowolnym ciałem. Opisać wszystkie ideały prawostronne pierścienia $M_2(K)$.

Zadanie (13)**.** Niech K będzie dowolnym ciałem. Podać przykład ideału lewostronnego (prawostronnego) pierścienia $M_2(K)$, który nie jest ideałem prawostronnym (lewostronnym) tego pierścienia.

Zadanie (14)**.** Niech K będzie dowolnym ciałem. Wykazać, że następujące podzbiory są podpierścieniami pierścienia $M_2(K)$:

(a) $\begin{bmatrix} K & K \\ 0 & 0 \end{bmatrix}$, (b) $\begin{bmatrix} K & K \\ 0 & K \end{bmatrix}$, (c) $\begin{bmatrix} K & 0 \\ K & 0 \end{bmatrix}$.

Które z tych podpierścieni są ideałami lewostronnymi (prawostronnymi) pierścienia $M_2(K)$? Wyznaczyć centrum każdego z tych podpierścieni i opisać wszystkie ich ideały lewostronne i prawostronne.

Uwaga 3.24. *Ideały lewostronne i ideały prawostronne pierścienia R nazywamy* ideałami jednostronnymi pierścienia R.

Zadanie (15)**.** Niech $L <_l R$ i $P <_r R$. Pokazać, że wtedy $[L \cup P] = L+P+LP$.

Zadanie (16)**.** Niech P_t będzie ideałem prawostronnym pierścienia R_t dla każdego $t \in T$. Udowodnij, że wtedy $\prod_{t\in T} P_t <_r \prod_{t\in T} R_t$.

Zadanie (17)**.** Niech R i S będą pierścieniami, z których co najmniej jeden posiada jedynkę. Udowodnij, że wszystkimi ideałami prawostronnymi pierścienia $R \times S$ są jedynie podzbiory postaci $P \times Q$, gdzie $P <_r R$ i $Q <_r S$.

Wykład 4

Ideały pierścieni

4.1 Ideały obustronne pierścieni

Definicja 4.1. *Ideałem obustronnym* pierścienia R nazywamy każdy taki ideał lewostronny, który jest jednocześnie ideałem prawostronnym tego pierścienia. Ideały obustronne będziemy nazywać krótko *ideałami*. Zapis: $I \lhd R$ będzie oznaczał, że I jest ideałem pierścienia R.

Oczywiście $I \subseteq R$ jest ideałem pierścienia R wtedy i tylko wtedy, gdy $I \neq \emptyset$ oraz $i_1 - i_2 \in I$ dla dowolnych $i_1, i_2 \in I$ oraz $r \cdot i, i \cdot r \in I$ dla dowolnych $r \in R$, $i \in I$. Jest to równoważne temu, że I jest podgrupą w R^+ spełniającą warunki: $I \cdot R \subseteq I$ oraz $R \cdot I \subseteq I$.

Z podanych wcześniej informacji o ideałach jednostronnych wynika od razu prawdziwość następujących przykładów.

Przykład 4.2. Zbiór $\{0\}$ jest ideałem pierścienia R. Nazywamy go *ideałem zerowym*. R jest ideałem pierścienia R. Nazywamy go *ideałem niewłaściwym pierścienia* R.

Przykład 4.3. Część wspólna dowolnej niepustej rodziny ideałów pierścienia R jest ideałem tego pierścienia.

Przykład 4.4. Suma algebraiczna skończonej liczby ideałów pierścienia R jest ideałem tego pierścienia.

Przykład 4.5. Iloczyn algebraiczny skończonej liczby ideałów pierścienia R jest ideałem tego pierścienia.

Przykład 4.6. Jeżeli L jest ideałem lewostronnym pierścienia R oraz P jest ideałem prawostronnym tego pierścienia, to $LP \lhd R$. Stąd dla dowolnej podgrupy A w R^+, $LAP \lhd R$. W szczególności dla dowolnego elementu $a \in R$ mamy, że $RaR \lhd R$.

Przykład 4.7. Jeśli $L <_l R$, to $L+LR \lhd R$. Rzeczywiście, na mocy przykładu 3.7, $L+LR <_l R$ oraz ze stwierdzenia 3.4, $(L+LR)\cdot R = LR+(LR)R \subseteq LR+L(RR) \subseteq LR+LR \subseteq L+LR$, więc $L+LR <_r R$ i ostatecznie $L+LR \lhd R$. Jeżeli J jest ideałem pierścienia R zawierającym L, to $LR \subseteq J$, skąd $L+LR \subseteq J$. Zatem $L+LR$ jest najmniejszym ideałem pierścienia R zawierającym ideał lewostronny L.

Przykład 4.8. Jeśli $P <_r R$, to $P+RP \lhd R$. Rzeczywiście, na mocy przykładu 3.19, $P+RP <_r R$ oraz ze stwierdzenia 3.4, $R(P+RP) = RP+R(RP) \subseteq RP+(RR)P \subseteq RP+RP \subseteq P+RP$, więc $P+RP <_l R$ i ostatecznie $P+RP \lhd R$. Jeżeli J jest ideałem pierścienia R zawierającym P, to $RP \subseteq J$, skąd $P+RP \subseteq J$. Zatem $P+RP$ jest najmniejszym ideałem pierścienia R zawierającym ideał prawostronny P.

Przykład 4.9. Niech A będzie podgrupą grupy addytywnej pierścienia R. Wtedy $L = A+RA <_l R$ na mocy przykładu 3.7. Zatem na mocy przykładu 3.19, $L+LR \lhd R$. Ale ze stwierdzenia 3.4, $L+LR = A+RA+AR+RAR$, więc $(A)_R = A+RA+AR+RAR \lhd R$. Jeżeli $J \lhd R$ i $A \subseteq J$, to na mocy przykładu 3.9 $L \subseteq J$, więc z przykladu 3.19, $L+LR \subseteq J$, czyli $(A)_R \subseteq J$. Zatem $(A)_R$ jest najmniejszym ideałem pierścienia R zawierającym podgrupę A.

Przykład 4.10. Niech X będzie podzbiorem pierścienia R. Wówczas $X \subseteq \langle X\rangle$, więc z przykładu 4.9, $(\langle X\rangle)_R$ jest ideałem pierścienia R zawierającym X. Jeżeli $J \lhd R$ i $X \subseteq J$, to $\langle X\rangle \subseteq J$, a więc z przykładu 4.9, $(\langle X\rangle)_R \subseteq J$. Zatem $(\langle X\rangle)_R$ jest najmniejszym ideałem pierścienia R zawierającym podzbiór X. Nazywamy go *ideałem pierścienia R generowanym przez podzbiór X* i oznaczamy symbolem $(X)_R$. Zatem

$$(X)_R = \langle X\rangle + R\langle X\rangle + \langle X\rangle R + R\langle X\rangle R.$$

Zamiast $(\{a_1,\ldots,a_n\})_R$ będziemy pisali $(a_1,\ldots,a_n)_R$. Na mocy stwierdzenia 3.3 dla dowolnego $a \in R$:

$$(a)_R = \langle a\rangle + Ra + aR + RaR.$$

Przykład 4.11. Jeżeli $L <_l R$, to $l_R(L) \lhd R$. Rzeczywiście, na mocy przykładu 3.13, $l_R(L) <_l R$ oraz na mocy stwierdzenia 3.4, $(l_R(L)R)L = l_R(L)(RL) \subseteq l_R(L)L = \{0\}$, więc $l_R(L)R \subseteq l_R(L)$ i wobec tego $l_R(L) <_r R$. Stąd ostatecznie $l_R(L) \lhd R$. Analogicznie pokazuje się, że jeżeli $P <_r R$, to $r_R(P) \lhd R$.

Udowodnimy teraz rezultat bardzo użyteczny w ogólnej teorii pierścieni i nazywany *lematem Andrunakiewicza*.

Twierdzenie 4.12. *Jeżeli $A \lhd B$ i $B \lhd R$, to $(A)_R^3 \subseteq A$.*

DOWÓD. Ponieważ $A \subseteq B$ i $B \lhd R$, więc z przykładu 4.9, $(A)_R \subseteq B$. Stąd $(A)_R^3 \subseteq B(A)_R B$. Ponadto z przykładu 4.9, $(A)_R = A + AR + RA + RAR$, więc na mocy stwierdzenia 3.4, $B(A)_R = BA + BAR + BRA + BRAR$. Ale $B \lhd R$ i $A \lhd B$, więc stąd $B(A)_R \subseteq A + AR + BA + BAR \subseteq A + AR$. Zatem $(A)_R^3 \subseteq (A + AR)B = AB + A(RB) \subseteq A + AB \subseteq A$, bo $AB \subseteq A$ i $RB \subseteq B$. □

Zadanie (1)**.** Niech A będzie podpierścieniem pierścienia R i niech $I \lhd R$. Pokazać, że wtedy $A + I$ jest podpierścieniem pierścienia R.

4.2 Ważne rodzaje ideałów

Definicja 4.13. Mówimy, że ideal I pierścienia R jest *ideałem właściwym*, jeżeli $I \neq R$.

Stwierdzenie 4.14. *Niech I będzie ideałem pierścienia R z jedynką. Wówczas $I = R$ wtedy i tylko wtedy, gdy $1 \in I$.*

DOWÓD. Załóżmy, że $1 \in I$. Wtedy dla dowolnego $a \in R$, $a = a \cdot 1 \in I$, czyli $R \subseteq I$. Ale $I \subseteq R$, więc $I = R$. Implikacja odwrotna jest oczywista. □

Definicja 4.15. Rodzinę $\mathcal{A}$ podzbiorów pierścienia R nazywamy *łańcuchem*, jeżeli dla dowolnych $A, B \in \mathcal{A}$ mamy, że $A \subseteq B$ lub $B \subseteq A$.

Stwierdzenie 4.16. *Suma mnogościowa łańcucha podgrup grupy addytywnej pierścienia R jest podgrupą tej grupy.*

DOWÓD. Niech $\mathcal{A}$ będzie łańcuchem podgrup grupy R^+. Oznaczmy $M = \bigcup_{A \in \mathcal{A}} A$. Wtedy $A \subseteq M$ dla każdego $A \in \mathcal{A}$, skąd $M \neq \emptyset$. Weźmy dowolne $a, b \in M$. Wtedy istnieją $A, B \in \mathcal{A}$ takie, że $a \in A$ i $b \in B$. Ale $\mathcal{A}$ jest łańcuchem, więc $A \subseteq B$ lub $B \subseteq A$. W pierwszym przypadku $a, b \in B$, więc $a - b \in B$, skąd $a - b \in M$. Natomiast w drugim $a, b \in A$, więc $a - b \in A$, skąd $a - b \in M$. Zatem M jest podgrupą grupy R^+. □

Stwierdzenie 4.17. *Suma mnogościowa łańcucha ideałów lewostronnych (prawostronnych) pierścienia R jest ideałem lewostronnym (prawostronnym) tego pierścienia. Ponadto suma mnogościowa łańcucha ideałów pierścienia R jest ideałem pierścienia R.*

DOWÓD. Niech $\mathcal{A}$ będzie łańcuchem ideałów lewostronnych pierścienia R. Wtedy ze stwierdzenia 4.16, $M = \bigcup_{A \in \mathcal{A}} A$ jest podgrupą grupy R^+. Weźmy dowolne $m \in M$ i dowolne $a \in R$. Wtedy istnieje $A \in \mathcal{A}$ takie, że $m \in A$, skąd $a \cdot m \in A$, czyli $a \cdot m \in M$. Zatem $M <_l R$. Wersję prawostronną naszego stwierdzenia dowodzi się analogicznie. Ostatnia cześć stwierdzenia jest konsekwencją jej pierwszej części. □

Definicja 4.18. Mówimy, że ideał I pierścienia R jest *ideałem maksymalnym pierścienia* R, jeżeli $I \neq R$ oraz dla dowolnego ideału J pierścienia R z tego, że $I \subseteq J$ wynika, że $J = I$ lub $J = R$.

Twierdzenie 4.19. *Każdy ideał właściwy I pierścienia R z jedynką jest zawarty w pewnym ideale maksymalnym tego pierścienia.*

DOWÓD. Oznaczmy przez $\mathcal{S}$ rodzinę wszystkich właściwych ideałów pierścienia R zawierających ideał I. Wtedy $I \in \mathcal{S}$, więc $\mathcal{S} \neq \emptyset$. Ponadto rodzina $\mathcal{S}$ jest częściowo uporządkowana przez inkluzję. Niech $\mathcal{A}$ będzie łańcuchem w $\mathcal{S}$ oraz niech $J = \bigcup_{A \in \mathcal{A}} A$. Wtedy ze stwierdzenia 4.17 , J jest ideałem pierścienia R oraz $I \subseteq J$. Jeśli $J = R$, to $1 \in J$, więc istnieje $A \in \mathcal{A}$ takie, że $1 \in A$. Ale wtedy ze stwierdzenia 4.14, $A = R$ i mamy sprzeczność. Zatem $J \neq R$ i ostatecznie $J \in \mathcal{S}$. W ten sposób pokazaliśmy, że w rodzinie $\mathcal{S}$ każdy łańcuch posiada ograniczenie górne. Stąd na mocy lematu Kuratowskiego-Zorna w rodzinie $\mathcal{S}$ istnieje element maksymalny M. Wówczas M jest ideałem właściwym pierścienia R zawierającym ideał I. Niech U będzie ideałem pierścienia R takim, że $M \subseteq U$ oraz $U \neq R$. Wtedy $U \in \mathcal{S}$, więc z maksymalności M w rodzinie $\mathcal{S}$ mamy, że $M = U$. Zatem M jest szukanym ideałem maksymalnym pierścienia R. □

Wniosek 4.20. *Każdy niezerowy pierścień z jedynką posiada ideał maksymalny.*

DOWÓD. Niech R będzie niezerowym pierścieniem z jedynką. Wtedy $\{0\}$ jest ideałem właściwym pierścienia R. Zatem z twierdzenia 4.19 istnieje ideał maksymalny M pierścienia R taki, że $\{0\} \subseteq M$, co kończy dowód wniosku. □

Definicja 4.21. Każdy pierścień R taki, że $R^2 = \{0\}$ nazywamy *pierścieniem z zerowym mnożeniem.*

Zadanie (2)**.** Niech p będzie liczbą pierwszą. Dla $n = 0, 1, 2, \ldots$ oznaczmy $\mathbb{C}_{p^n} = \{z \in \mathbb{C} : z^{p^n} = 1\}$. Wówczas jak wiemy $\mathbb{C}_{p^n}$ jest podgrupą grupy multyplikatywnej ciała liczb zespolonych. Oznaczmy: $\mathbb{C}_{p^\infty} = \bigcup_{n=0}^{\infty} \mathbb{C}_{p^n}$. Udowodnić, że $\mathbb{C}_{p^\infty}$ jest grupą i opisać wszystkie jej podgrupy. Pokazać też, że pierścień $\mathbb{C}^0_{p^\infty}$ nie posiada ideałów maksymalnych.

Definicja 4.22. Mówimy, że ideał I pierścienia R jest *ideałem pierwszym w pierścieniu* R, jeżeli $I \neq R$ oraz dla dowolnych ideałów A, B pierścienia R z tego, że $A \cdot B \subseteq I$ wynika, że $A \subseteq I$ lub $B \subseteq I$.

Twierdzenie 4.23. *Niech M będzie ideałem maksymalnym pierścienia R. Wówczas równoważne są warunki:*

(i) M jest ideałem pierwszym pierścienia R,

(ii) $R^2 \not\subseteq M$.

DOWÓD. Z założenia wynika, że $M \neq R$.

$(i) \Rightarrow (ii)$. Jeżeli $R^2 \subseteq M$, to z pierwszości M jest $R \subseteq M$, skąd $M = R$ i mamy sprzeczność. Zatem $R^2 \not\subseteq M$.

$(ii) \Rightarrow (i)$. Załóżmy, że M nie jest ideałem pierwszym pierścienia R. Wtedy istnieją ideały A, B pierścienia R takie, że $AB \subseteq M$ oraz $A \not\subseteq M$ i $B \not\subseteq M$. Stąd $M \subset M + A$ i $M \subset M + B$. Zatem z maksymalności M mamy, że $M + A = M + B = R$. Ale $R^2 = (M + A)(M + B) = M^2 + MB + AM + AB \subseteq M + M + M + M \subseteq M$, więc $R^2 \subseteq M$ i mamy sprzeczność. Stąd M jest ideałem pierwszym pierścienia R. □

Wniosek 4.24. *W pierścieniu R takim, że $R^2 = R$ każdy ideał maksymalny jest ideałem pierwszym.*

Wniosek 4.25. *W pierścieniu z jedynką każdy ideał maksymalny jest ideałem pierwszym.*

Przykład 4.26. W pierścieniu $\mathbb{Z}^0$ ideały maksymalne są postaci: $p\mathbb{Z}$ dla liczb pierwszych p. Zatem z twierdzenia 4.23 żaden z tych ideałów nie jest ideałem pierwszym pierścienia $\mathbb{Z}^0$.

Zadanie (3)**.** Niech I_1, I_2, I_3 będą ideałami pierścienia R z jedynką takimi, że $R = I_1 + I_2 = I_1 + I_3$. Udowodnić, że wtedy $R = I_1 + I_2 \cap I_3$.

Twierdzenie 4.27. *Niech I będzie właściwym ideałem pierścienia R. Wówczas równoważne są warunki:*

(i) I jest ideałem pierwszym pierścienia R,

(ii) dla dowolnych $a, b \in R$ z tego, że $aRb \subseteq I$ wynika, że $a \in I$ lub $b \in I$.

DOWÓD. $(i) \Rightarrow (ii)$. Załóżmy, że I jest ideałem pierwszym w pierścieniu R i weźmy dowolne $a, b \in R$ takie, że $aRb \subseteq I$. Wtedy $(a)_R Rb = (\langle a \rangle + aR + Ra + RaR)Rb = aRb + aR^2b + RaRb + RaR^2b \subseteq I$. Stąd $(a)_R R(b)_R = (a)_R R(\langle b \rangle + bR + Rb + RbR) = (a)_R Rb + (a)_R RbR + (a)_R R^2b + (a)_R R^2bR \subseteq I$. Zatem $(a)_R R(b)_R \subseteq I$, więc z pierwszości I, $(a)_R \subseteq I$ lub $R(b)_R \subseteq I$. W pierwszym przypadku $a \in I$, zaś w drugim $R \subseteq I$ lub $(b)_R \subseteq I$. Ale $I \neq R$, więc $(b)_R \subseteq I$, skąd $b \in I$.

$(ii) \Rightarrow (i)$. Załóżmy, że ideał I nie jest pierwszy. Wtedy istnieją ideały A i B pierścienia R takie, że $A \cdot B \subseteq I$ oraz $A \not\subseteq I$ i $B \not\subseteq I$. Zatem istnieją $a \in A \setminus I$ oraz $b \in B \setminus I$. Ponadto $aRb \subseteq A \cdot B \subseteq I$, więc $aRb \subseteq I$. Stąd $a \in I$ lub $b \in I$ i mamy sprzeczność. □

Zadanie (4)**.** Udowodnij, że ideał właściwy I pierścienia przemiennego R jest ideałem pierwszym w R wtedy i tylko wtedy, gdy dla dowolnych $a, b \in R$ z tego, że $ab \in I$ wynika, że $a \in I$ lub $b \in I$.

Definicja 4.28. Mówimy, że ideał I pierścienia R jest *ideałem półpierwszym pierścienia R*, jeżeli $I \neq R$ oraz dla dowolnego ideału J pierścienia R z tego, że $J^2 \subseteq I$ wynika, że $J \subseteq I$.

Twierdzenie 4.29. *Niech I będzie właściwym ideałem pierścienia R. Wówczas równoważne są warunki:*

(i) I jest ideałem półpierwszym pierścienia R,

(ii) dla dowolnego $a \in R$ z tego, że $aRa \subseteq I$ wynika, że $a \in I$.

DOWÓD. $(i) \Rightarrow (ii)$. Weźmy dowolne $a \in R$ takie, że $aRa \subseteq I$. Wtedy $(a)_R Ra = (\langle a \rangle + Ra + aR + RaR)Ra = aRa + RaRa + aR^2a + RaR^2a \subseteq I$, skąd $(a)_R R(a)_R = (a)_R R(\langle a \rangle + Ra + aR + RaR) = (a)_R Ra + (a)_R R^2 a + (a)_R RaR + (a)_R R^2 aR \subseteq I$. Zatem $(a)_R R(a)_R \subseteq I$, skąd $[(a)_R^2]^2 \subseteq I$, a więc $(a)_R^2 \subseteq I$. Zatem $(a)_R \subseteq I$ i wobec tego $a \in I$.

$(ii) \Rightarrow (i)$. Weźmy dowolny ideał J pierścienia R taki, że $J^2 \subseteq I$. Wtedy dla dowolnego $a \in J$, $aRa \subseteq J^2$, a więc $aRa \subseteq I$, skąd $a \in I$. Zatem $J \subseteq I$. Stąd I jest ideałem półpierwszym pierścienia R. □

Przykład 4.30. Wprost z definicji każdy ideał pierwszy pierścienia R jest ideałem półpierwszym tego pierścienia. Natomiast ideał $I = \{0\} \times \{0\}$ pierścienia $R = \mathbb{Z} \times \mathbb{Z}$ jest półpierwszy, ale nie jest ideałem pierwszym, bo $I = A \cdot B$ dla $A = \mathbb{Z} \times \{0\}$ i $B = \{0\} \times \mathbb{Z}$.

Przykład 4.31. Część wspólna dowolnej niepustej rodziny ideałów pierwszych (a nawet półpierwszych) pierścienia R jest ideałem półpierwszym tego pierścienia. Rzeczywiście, niech $\{I_t\}_{t \in T}$ będzie rodziną ideałów pierwszych (półpierwszych) pierścienia R. Wtedy na mocy przykładu 4.3, $I = \bigcap_{t \in T} I_t \lhd R$. Ponadto dla $t \in T$ jest $I \subseteq I_t \subset R$, więc $I \neq R$. Weźmy dowolny ideał J pierścienia R taki, że $J^2 \subseteq I$. Wtedy dla każdego $t \in T$: $J^2 \subseteq I_t$, więc $J \subseteq I_t$ z pierwszości (z półpierwszości) I_t. Stąd $J \subseteq \bigcap_{t \in T} I_t$, czyli $J \subseteq I$. Zatem I jest ideałem półpierwszym pierścienia R.

Definicja 4.32. Mówimy, że ciąg (a_n) elementów pierścienia R jest *m-ciągiem*, jeżeli $a_{i+1} \in a_i R a_i$ dla dowolnego $i \in \mathbb{N}$.

Przykład 4.33. Dla dowolnego elementu a pierścienia R, $(a^{3^{n-1}})$ jest m-ciągiem o pierwszym wyrazie równym a, gdyż $a_{i+1} = a^{3^i} = a^{3^{i-1}} a^{3^{i-1}} a^{3^{i-1}} = a_i a_i a_i \in a_i R a_i$ dla $i \in \mathbb{N}$. Zauważmy, że ciąg $(a^{3^{n-1}})$ zawiera wyraz równy 0 wtedy i tylko wtedy, gdy element a jest nilpotentny.

Stwierdzenie 4.34. *Niech (a_n) będzie m-ciągiem w pierścieniu R. Wówczas dla dowolnych liczb naturalnych $k \geqslant l$: $a_k \in (a_l)_R$. W szczególności, jeżeli dla pewnego $I \lhd R$ jest $a_l \in I$, to $a_k \in I$ dla wszystkich $k \geqslant l$.*

DOWÓD. Z przykładu 4.10, $a_l \in (a_l)_R$. Niech $k \geqslant l$ będzie liczbą naturalną, że $a_k \in (a_l)_R$. Wtedy $a_{k+1} \in a_k R a_k \subseteq (a_l)_R R (a_l)_R \subseteq (a_l)_R$, czyli $a_{k+1} \in (a_l)_R$. Zatem przez indukcję $a_k \in (a_l)_R$ dla wszystkich $k \geqslant l$.

Niech $I \lhd R$ i $a_l \in I$. Wtedy z przykładu 4.10, $(a_l)_R \subseteq I$, więc z pierwszej części dowodu $a_k \in I$ dla wszystkich $k \geqslant l$. □

Stwierdzenie 4.35. *Niech I będzie ideałem półpierwszym pierścienia R. Wówczas dla każdego $a \in R \setminus I$ istnieje m-ciąg (a_n) taki, że $a_1 = a$ oraz $a_n \notin I$ dla $n \in \mathbb{N}$.*

DOWÓD. Szukany ciąg skonstruujemy przez indukcję. Ponieważ $I \neq R$, więc $R \setminus I \neq \emptyset$. Weźmy dowolne $a \in R \setminus I$ i niech $a_1 = a$. Wtedy $a_1 \notin I$. Zatem z twierdzenia 4.28, $a_1 R a_1 \not\subseteq I$. Zatem istnieje $a_2 \in a_1 R a_1 \setminus I$. Załóżmy, że zostały już skonstruowane elementy $a_1, \ldots, a_n \in R \setminus I$ takie, że $a_1 = a$ oraz $a_{i+1} \in a_i R a_i$ dla $i = 1, \ldots, n-1$. Wtedy z twierdzenia 4.28 , $a_n R a_n \not\subseteq I$, więc istnieje $a_{n+1} \in a_n R a_n \setminus I$. W ten sposób przez indukcję mamy skonstruowany m-ciąg (a_n) spełniający warunki twierdzenia. □

Stwierdzenie 4.36. *Niech (a_n) będzie m-ciągiem w pierścieniu R i niech $I \lhd R$, przy czym $a_n \notin I$ dla każdego $n \in \mathbb{N}$. Wówczas rodzina $\mathcal{M}$ wszystkich ideałów J pierścienia R zawierających I oraz takich, że $a_n \notin J$ dla wszystkich $n \in \mathbb{N}$ jest niepusta i posiada element maksymalny. Ponadto każdy element maksymalny rodziny $\mathcal{M}$ jest ideałem pierwszym pierścienia R.*

DOWÓD. Na mocy założeń $I \in \mathcal{M}$, więc $\mathcal{M} \neq \emptyset$. Niech $\mathcal{A}$ będzie łańcuchem w $\mathcal{M}$. Wtedy ze stwierdzeniua 4.17, $M = \bigcup_{A \in \mathcal{A}} A$ jest ideałem pierścienia R. Ponadto M zawiera wszystkie ideały z rodziny $\mathcal{A}$, a więc w szczególności $I \subseteq M$. Jeżeli dla pewnego $n \in \mathbb{N}$ jest $a_n \in M$, to dla pewnego $A \in \mathcal{A}$, $a_n \in A$, co prowadzi do sprzeczności. Zatem $a_n \notin M$ dla wszystkich $n \in \mathbb{N}$. Stąd $M \in \mathcal{M}$ i z lematu Kuratowskiego-Zorna w rodzinie $\mathcal{M}$ istnieje element maksymalny.

Niech teraz P będzie dowolnym elementem maksymalnym w rodzinie $\mathcal{M}$. Wtedy w szczególności $P \lhd R$, $I \subseteq P$ oraz $a_n \notin P$ dla każdego $n \in \mathbb{N}$. Stąd $P \neq R$. Niech A i B będą dowolnymi ideałami pierścienia R takimi, że $A \cdot B \subseteq P$. Załóżmy, że $A \not\subseteq P$ i $B \not\subseteq P$. Wtedy $P \subset P + A$ i $P \subset P + B$, więc z maksymalności P w rodzinie $\mathcal{M}$, $P + A, P + B \notin \mathcal{M}$, a zatem istnieją liczby naturalne p i q takie, że $a_p \in P + A$ i $a_q \in P + B$. Ze stwierdzenia 4.34 wynika, że wtedy $a_{p+q} \in (P + A) \cap (P + B)$. Z definicji m-ciągu $a_{p+q+1} \in a_{p+q} R a_{p+q} \subseteq (P + A)(P + B)$. Ale $(P + A)(P + B) = P^2 + PB + AP + AB \subseteq P$, gdyż $AB \subseteq P$. Stąd $a_{p+q+1} \in P$ i mamy sprzeczność. Zatem $A \subseteq P$ lub $B \subseteq P$ i P jest ideałem pierwszym pierścienia R. □

Twierdzenie 4.37. *Każdy ideał półpierwszy I pierścienia R jest częścią wspólną wszystkich ideałów pierwszych pierścienia R zawierających I.*

DOWÓD. Ponieważ $I \neq R$, więc $R \setminus I \neq \emptyset$. Ze stwierdzeń 4.35 i 4.36 dla każdego $a \in R \setminus I$ istnieje ideał pierwszy I_a pierścienia R taki, że $I \subseteq I_a$ oraz $a \notin I_a$. Stąd $I \subseteq \bigcap_{a \in R \setminus I} I_a$. Weźmy dowolne $x \in \bigcap_{a \in R \setminus I} I_a$. Jeśli $x \notin I$, to $x \notin I_x$. Ale $\bigcap_{a \in R \setminus I} I_a \subseteq I_x$, więc mamy sprzeczność. Stąd $x \in I$ i wobec tego $I = \bigcap_{a \in R \setminus I} I_a$. Niech $\mathcal{M}$ będzie rodziną wszystkich ideałów pierwszych pierścienia R zawierających I. Wtedy $\{I_a : a \in R \setminus I\} \subseteq \mathcal{M}$, więc $I \subseteq \bigcap_{M \in \mathcal{M}} M \subseteq \bigcap_{a \in R \setminus I} I_a = I$, skąd $I = \bigcap_{M \in \mathcal{M}} M$. □

Wykład 5

Pierścienie ilorazowe

5.1 Konstrukcja pierścienia ilorazowego

Niech I będzie ideałem pierścienia R. Ponieważ I jest podgrupą grupy addytywnej pierścienia R, więc możemy utworzyć abelową grupę ilorazową R/I. Przypomnijmy, że elementami tej grupy są warstwy, czyli zbiory postaci $a+I = \{a+i : i \in I\}$ dla $a \in R$, przy czym warstwy $a+I$ i $b+I$ są równe wtedy i tylko wtedy, gdy $a-b \in I$. Natomiast sumą warstw $a+I$ oraz $b+I$ jest warstwa $(a+b)+I$, zaś elementem neutralnym dodawania warstw jest warstwa $I = 0+I$. Ponadto warstwą przeciwną do warstwy $a+I$ jest warstwa $(-a)+I$.

W zbiorze warstw R/I wprowadzamy mnożenie przyjmując, że

$$(a+I)\cdot(b+I) = ab+I \text{ dla dowolnych } a,b \in R. \tag{5.1}$$

Zauważmy, że określenie mnożenia nie zależy od wyboru reprezentantów warstw. Rzeczywiście, niech $a, a', b, b' \in R$ będą takie, że $a+I = a'+I$ oraz $b+I = b'+I$. Wówczas $a'-a = i \in I$ oraz $b'-b = j \in I$. Zatem $a' = a+i$, $b' = b+j$ oraz $a'b'-ab = (a+i)(b+j)-ab = ab+aj+ib+ij-ab = (a+i)j+ib \in I$, gdyż $i, j \in I$. Stąd $a'b'+I = ab+I$.

Ponadto dla dowolnych $a, b, c \in R$ mamy, że $[(a+I)\cdot(b+I)]\cdot(c+I) = (ab+I)\cdot(c+I) = (ab)c+I = a(bc)+I = (a+I)\cdot(bc+I) = (a+I)\cdot[(b+I)\cdot(c+I)]$, więc mnożenie warstw jest łączne oraz $(a+I)\cdot[(b+I)+(c+I)] = (a+I)\cdot[(b+c)+I] = a(b+c)+I = (ab+ac)+I = (ab+I)+(ac+I) = (a+I)\cdot(b+I)+(a+I)\cdot(c+I)$, $[(b+I)+(c+I)]\cdot(a+I) = [(b+c)+I]\cdot(a+I) = (b+c)a+I = (ba+ca)+I = (ba+I)+(ca+I) = (b+I)\cdot(a+I)+(c+I)\cdot(a+I)$, czyli mnożenie warstw jest rozdzielne względem dodawania warstw. Stąd mamy, że system algebraiczny $(R/I, +, \cdot, I)$ jest pierścieniem. Nazywamy go *pierścieniem ilorazowym* pierścienia R względem ideału I.

Zadanie (1)**.** Niech I będzie podgrupą grupy addytywnej pierścienia R. Udowodnij, że jeśli I nie jest ideałem pierścienia R, to wzór (5.1) nie jest poprawnie określony, tzn. istnieją $a, b, a', b' \in R$ takie, że $a+I = a'+I$ i $b+I = b'+I$, ale $ab+I \neq a'b'+I$.

Uwaga 5.1. *Jeżeli pierścień R ma jedynkę 1, to $1+I$ jest jedynką pierścienia ilorazowego R/I, gdyż dla każdego $a \in R$ jest $(a+I)\cdot(1+I) = a\cdot 1 + I = a + I = 1\cdot a + I = (1+I)\cdot(a+I)$.*

Uwaga 5.2. *Jeżeli pierścień R jest przemienny, to pierścień ilorazowy R/I też jest przemienny, bo dla dowolnych $a, b \in R$ jest $(b+I)\cdot(a+I) = ba + I = ab + I = (a+I)\cdot(b+I)$.*

5.2 Podpierścienie i ideały w pierścieniach ilorazowych

Uwaga 5.3. *Niech I będzie ideałem pierścienia R. Dla podgrupy A grupy R^+ zawierającej I oznaczmy*

$$A/I = \{a + I : a \in A\}. \tag{5.2}$$

Ponadto dla podgrupy M grupy $(R/I)^+$ oznaczmy

$$M_0 = \{a \in R : a + I \in M\}. \tag{5.3}$$

Ponieważ $0 \in A$, więc $0 + I \in A/I$. Weźmy dowolne $a, b \in A$. Wtedy $(a+I) - (b+I) = (a-b) + I \in A/I$, bo $a - b \in A$. Zatem A/I jest podgrupą grupy $(R/I)^+$.

Dla $i \in I$, $i + I = 0 + I \in M$, więc $i \in M_0$. Stąd $I \subseteq M_0$. Jeżeli $a, b \in M_0$, to $a + I, b + I \in M$, skąd $(a+I) - (b+I) \in M$, czyli $(a-b) + I \in M$. Zatem $a - b \in M_0$. Wobec tego M_0 jest podgrupą grupy R^+ zawierającą I. Ponadto wprost z definicji M_0 mamy, że $M = M_0/I$.

Z definicji A/I mamy od razu, że $A \subseteq (A/I)_0$. Weźmy dowolne $x \in (A/I)_0$. Wtedy $x \in R$ oraz $x + I \in A/I$. Zatem istnieje $a \in A$ takie, że $x + I = a + I$. Stąd $x - a = i$ dla pewnego $i \in I$, a więc $x = a + i \in A$, bo $I \subseteq A$ i A jest podgrupą grupy R^+. Zatem $(A/I)_0 = A$.

Podsumowując nasze rozważania widzimy, że odwzorowania $A \mapsto A/I$ (dla podgrup A grupy R^+ zawierających I) oraz $M \mapsto M_0$ (dla podgrup M grupy $(R/I)^+$) są wzajemnie odwrotne. W konsekwencji tego odwzorowanie $A \mapsto A/I$ jest bijekcją rodziny wszystkich podgrup grupy R^+ zawierających I na rodzinę wszystkich podgrup grupy $(R/I)^+$.

Stwierdzenie 5.4. *Niech I będzie ideałem pierścienia R. Wówczas dla dowolnych podgrup A i B grupy R^+ zawierających I:*

$$A/I \subseteq B/I \iff A \subseteq B.$$

Dowód. Załóżmy, że $A/I \subseteq B/I$ i weźmy dowolne $a \in A$. Wtedy $a+I \in A/I$, a więc $a+I \in B/I$. Zatem istnieje $b \in B$ takie, że $a+I = b+I$. Stąd $a-b = i$ dla pewnego $i \in I$, czyli $a = b+i \in B$, bo $I \subseteq B$ oraz B jest podgrupą grupy R^+. Zatem $A \subseteq B$.

Implikacja odwrotna jest oczywista. □

Stwierdzenie 5.5. *Niech I będzie ideałem pierścienia R. Wówczas odwzorowanie $S \mapsto S/I$ jest bijekcją rodziny wszystkich podpierścieni pierścienia R zawierających I na rodzinę wszystkich podpierścieni pierścienia R/I.*

Dowód. Niech S będzie podpierścieniem pierścienia R zawierającym I. Z uwagi 5.3 S/I jest podgrupą grupy $(R/I)^+$. Weźmy dowolne $a, b \in S$. Wtedy $ab \in S$, więc $(a+I)\cdot(b+I) = ab + I \in S/I$. Stąd S/I jest podpierścieniem pierścienia R/I.

Niech M będzie podpierścieniem pierścienia R/I. Wtedy z uwagi 5.3 M_0 jest podgrupą grupy R^+ zawierającą I. Weźmy dowolne $a, b \in M_0$. Wtedy $a+I, b+I \in M$, więc $(a+I)\cdot(b+I) \in M$, skąd $ab+I \in M$, a więc $ab \in M_0$. Zatem M_0 jest podpierścieniem pierścienia R zawierającym I.

Z tych rozważań i z uwagi 5.3 wynika, że przekształcenia $S \mapsto S/I$ (dla podpierścieni S pierścienia R zawierających I) oraz $M \mapsto M_0$ (dla podpierścieni M pierścienia R/I) są wzajemnie odwrotne. Stąd zaś wynika teza naszego stwierdzenia. □

Stwierdzenie 5.6. *Niech I będzie ideałem pierścienia R. Wówczas odwzorowanie $L \mapsto L/I$ jest bijekcją rodziny wszystkich ideałów lewostronnych pierścienia R zawierających I na rodzinę wszystkich ideałów lewostronnych pierścienia R/I.*

Dowód. Niech L będzie ideałem lewostronnym pierścienia R zawierającym I. Z uwagi 5.3 L/I jest podgrupą grupy $(R/I)^+$. Weźmy dowolne $a \in L$, $r \in R$. Wtedy $ra \in L$, więc $(r+I)\cdot(a+I) = ra + I \in L/I$. Stąd L/I jest ideałem lewostronnym pierścienia R/I.

Niech M będzie ideałem lewostronnym pierścienia R/I. Wtedy z uwagi 5.3 M_0 jest podgrupą grupy R^+ zawierającą I. Weźmy dowolne $a \in M_0$, $r \in R$. Wtedy $a+I \in M$ i $r+I \in R/I$, więc $(r+I)\cdot(a+I) \in M$, skąd $ra+I \in M$, a więc $ra \in M_0$. Zatem M_0 jest ideałem lewostronnym pierścienia R zawierającym I.

Z tych rozważań i z uwagi 5.3 wynika, że przekształcenia $L \mapsto L/I$ (dla ideałów lewostronnych L pierścienia R zawierających I) oraz $M \mapsto M_0$ (dla ideałów lewostronnych M pierścienia R/I) są wzajemnie odwrotne. Stąd zaś wynika teza naszego stwierdzenia. □

Stwierdzenie 5.7. *Niech I będzie ideałem pierścienia R. Wówczas odwzorowanie $P \mapsto P/I$ jest bijekcją rodziny wszystkich ideałów prawostronnych pierścienia R zawierających I na rodzinę wszystkich ideałów prawostronnych pierścienia R/I.*

Dowód. Niech P będzie ideałem prawostronnym pierścienia R zawierającym I. Z uwagi 5.3 P/I jest podgrupą grupy $(R/I)^+$. Weźmy dowolne $a \in P$, $r \in R$. Wtedy $ar \in P$, więc $(a+I)\cdot(r+I) = ar + I \in P/I$. Stąd P/I jest ideałem prawostronnym pierścienia R/I.

Niech M będzie ideałem prawostronnym pierścienia R/I. Wtedy z uwagi 5.3 M_0 jest podgrupą grupy R^+ zawierającą I. Weźmy dowolne $a \in M_0$, $r \in R$.

Wtedy $a+I \in M$ i $r+I \in R/I$, więc $(a+I)\cdot(r+I) \in M$, skąd $ar+I \in M$, a więc $ar \in M_0$. Zatem M_0 jest ideałem prawostronnym pierścienia R zawierającym I.

Z tych rozważań i z uwagi 5.3 wynika, że przekształcenia $P \mapsto P/I$ (dla ideałów prawostronnych P pierścienia R zawierających I) oraz $M \mapsto M_0$ (dla ideałów prawostronnych M pierścienia R/I) są wzajemnie odwrotne. Stąd zaś wynika teza naszego stwierdzenia. □

Stwierdzenie 5.8. *Niech I będzie ideałem pierścienia R. Wówczas odwzorowanie $J \mapsto J/I$ jest bijekcją rodziny wszystkich ideałów pierścienia R zawierających I na rodzinę wszystkich ideałów pierścienia R/I.*

DOWÓD. Niech J będzie ideałem pierścienia R zawierającym I. Z uwagi 5.3 J/I jest podgrupą grupy $(R/I)^+$. Weźmy dowolne $a \in J$, $r \in R$. Wtedy $ra, ar \in J$, więc $(r+I)\cdot(a+I) = ra+I \in J/I$ oraz $(a+I)\cdot(r+I) = ar+I \in J/I$. Stąd J/I jest ideałem pierścienia R/I.

Niech M będzie ideałem pierścienia R/I. Wtedy z uwagi 5.3 M_0 jest podgrupą grupy R^+ zawierającą I. Weźmy dowolne $a \in M_0$, $r \in R$. Wtedy $a+I \in M$ i $r+I \in R/I$, więc $(r+I)\cdot(a+I) \in M$ oraz $(a+I)\cdot(r+I) \in M$, skąd $ra+I \in M$ i $ar+I \in J/I$, a więc $ra, ar \in M_0$. Zatem M_0 jest ideałem pierścienia R zawierającym I.

Z tych rozważań i z uwagi 5.3 wynika, że przekształcenia $J \mapsto J/I$ (dla ideałów J pierścienia R zawierających I) oraz $M \mapsto M_0$ (dla ideałów M pierścienia R/I) są wzajemnie odwrotne. Stąd zaś wynika teza naszego stwierdzenia. □

Zadanie (2)**.** Niech I będzie ideałem pierścienia R. Udowodnij, że dla dowolnych podgrup A i B grupy R^+ zawierających I zachodzą następujące wzory: (a) $A/I \cap B/I = (A \cap B)/I$, (b) $A/I + B/I = (A + B)/I$, (c) $A/I \cdot B/I = (A \cdot B + I)/I$, (d) $(A/I)_{R/I} = (A)_R/I$, (e) $[A/I] = [A]/I$.

5.3 Pierścienie proste, pierwsze i półpierwsze

Definicja 5.9. Powiemy, że pierścień R jest *prosty*, jeżeli $R \neq \{0\}$ oraz jedynymi ideałami pierścienia R są: $\{0\}$ i R.

Zadanie (3)**.** Niech K będzie dowolnym ciałem. Pokazać, że dla dowolnego naturalnego n pierścień $M_n(K)$ jest prosty.

Twierdzenie 5.10. *Pierścień R taki, że $R^2 \neq \{0\}$ jest prosty wtedy i tylko wtedy, gdy $RaR = R$ dla każdego niezerowego elementu $a \in R$.*

DOWÓD. $\Rightarrow$. Załóżmy, że dla każdego niezerowego $a \in R$ jest $RaR = R$. Niech I będzie niezerowym ideałem pierścienia R. Wtedy istnieje $0 \neq a \in I$, więc $RaR = R$. Ale $RaR \subseteq I$, więc $I = R$. Zatem R jest pierścieniem prostym.

$\Leftarrow$. Na odwrót, załóżmy, że R jest pierścieniem prostym. Z przykładu 4.11 $l_R(R) \lhd R$. Jeśli $l_R(R) = R$, to $R^2 = \{0\}$, wbrew założeniu. Zatem z prostoty R wynika, że $l_R(R) = \{0\}$. Analogicznie pokazujemy, że $r_R(R) = \{0\}$. Weźmy dowolne niezerowe $a \in R$. Wtedy $Ra \neq \{0\}$, bo $a \notin r_R(R)$. Zatem $RaR \neq \{0\}$, bo $Ra \not\subseteq l_R(R) = \{0\}$. Ale $RaR \lhd R$ i pierścień R jest prosty, więc $RaR = R$. □

Zadanie (4)**.** Opisać wszystkie pierścienie proste z zerowym mnożeniem.

Zadanie (5)**.** Opisać wszystkie przemienne pierścienie proste.

Twierdzenie 5.11. *Niech I będzie ideałem pierścienia R. Wówczas I jest ideałem maksymalnym pierścienia R wtedy i tylko wtedy, gdy pierścień ilorazowy R/I jest prosty.*

DOWÓD. Załóżmy, że ideał I jest maksymalny. Wtedy $I \neq R$, a więc istnieje $a \in R \setminus I$, skąd $a+I \neq 0+I$ i pierścień ilorazowy R/I jest niezerowy. Niech M będzie dowolnym ideałem pierścienia R/I. Wtedy ze stwierdzenia 5.8 istnieje ideał J pierścienia R taki, że $I \subseteq J$ oraz $M = J/I$. Z maksymalności I jest więc $J = I$ lub $J = R$. Zatem ideał M jest zerowy lub $M = R/I$. Oznacza to, że pierścień R/I jest prosty.

Na odwrót, załóżmy, że pierścień R/I jest prosty. Wtedy R/I jest niezerowy, a więc istnieje $a \in R$ takie, że $a+I \neq 0+I$, skąd $a \notin I$ i wobec tego $I \neq R$. Niech $J \lhd R$ i $I \subseteq J$. Wtedy ze stwierdzenia 5.8 $J/I \lhd R/I$. Ale pierścień R/I jest prosty, więc $J/I = \{0 + I\}$ lub $J/I = R/I$. Zatem ze stwierdzenia 5.4 $J = I$ lub $J = R$. Oznacza to, że ideał I jest maksymalny. □

Definicja 5.12. Powiemy, że pierścień R jest *pierścieniem pierwszym*, jeżeli $R \neq \{0\}$ oraz dla dowolnych ideałów A, B pierścienia R z tego, że $AB = \{0\}$ wynika, że $A = \{0\}$ lub $B = \{0\}$.

Zatem pierścień R jest pierwszy wtedy i tylko wtedy, gdy $\{0\}$ jest ideałem pierwszym w R.

Twierdzenie 5.13. *Niech I będzie ideałem pierścienia R. Wówczas I jest ideałem pierwszym pierścienia R wtedy i tylko wtedy, gdy pierścień ilorazowy R/I jest pierścieniem pierwszym.*

DOWÓD. Załóżmy, że ideał I jest pierwszy. Wtedy $I \neq R$, a więc istnieje $a \in R \setminus I$, skąd $a+I \neq 0+I$ i pierścień ilorazowy R/I jest niezerowy. Weźmy dowolne ideały M i N pierścienia R/I takie, że $M \cdot N = \{0+I\}$. Ze stwierdzenia 5.8 istnieją ideały J i K pierścienia R zawierające I takie, że $M = J/I$ oraz $N = K/I$. Z zadania (2) $M \cdot N = (J \cdot K + I)/I$. Ale $M \cdot N = \{0 + I\}$, więc ze stwierdzenia 5.4 $J \cdot K + I = I$, skąd $J \cdot K \subseteq I$. Zatem z pierwszości I, $J \subseteq I$ lub $K \subseteq I$, czyli $J = I$ lub $K = I$. Stąd $M = \{0+I\}$ lub $N = \{0+I\}$. Zatem pierścień R/I jest pierwszy.

Na odwrót, załóżmy, że pierścień R/I jest pierwszy. Wtedy R/I jest niezerowy, a więc istnieje $a \in R$ takie, że $a + I \neq 0 + I$, skąd $a \notin I$ i wobec tego $I \neq R$. Weźmy dowolne ideały A i B pierścienia R takie, że $A \cdot B \subseteq I$. Wtedy $I \subseteq A + I$, $I \subseteq B + I$ oraz $(A + I) \cdot (B + I) = AB + AI + IB + I^2 \subseteq I$. Ze stwierdzenia 5.8 $M = (A + I)/I \lhd R/I$ i $N = (B + I)/I \lhd R/I$. Ponadto z zadania (2) $M \cdot N = \{0+I\}$. Zatem z pierwszości pierścienia R/I, $M = \{0+I\}$ lub $N = \{0 + I\}$, skąd $A + I = I$ lub $B + I = I$. Zatem $A \subseteq I$ lub $B \subseteq I$ i ideał I jest pierwszy. □

Twierdzenie 5.14. *Dla dowolnego pierścienia $R \neq \{0\}$ równoważne są warunki:*

(i) R jest pierścieniem pierwszym,

(ii) jeżeli $aRb = \{0\}$, to $a = 0$ lub $b = 0$ dla dowolnych $a, b \in R$.

DOWÓD. $(i) \Rightarrow (ii)$. Ponieważ pierścień R jest pierwszy, więc ideał $\{0\}$ jest pierwszy. Weźmy dowolne $a, b \in R$ takie, że $aRb = \{0\}$. Wtedy z twierdzenia 4.27, $a \in \{0\}$ lub $b \in \{0\}$, czyli $a = 0$ lub $b = 0$.

$(ii) \Rightarrow (i)$. Z naszego założenia wynika na mocy twierdzenia 4.27, że ideał $\{0\}$ jest pierwszy, czyli pierścień R jest pierwszy. □

Definicja 5.15. Powiemy, że pierścień R jest *pierścieniem półpierwszym*, jeżeli $R \neq \{0\}$ oraz dla dowolnego ideału A pierścienia R z tego, że $A^2 = \{0\}$ wynika, że $A = \{0\}$.

Zatem pierścień R jest półpierwszy wtedy i tylko wtedy, gdy $\{0\}$ jest ideałem półpierwszym w R.

Twierdzenie 5.16. *Niech I będzie ideałem pierścienia R. Wówczas I jest ideałem półpierwszym pierścienia R wtedy i tylko wtedy, gdy pierścień ilorazowy R/I jest pierścieniem półpierwszym.*

DOWÓD. Załóżmy, że ideał I jest półpierwszy. Wtedy $I \neq R$, a więc istnieje $a \in R \setminus I$, skąd $a + I \neq 0 + I$ i pierścień ilorazowy R/I jest niezerowy. Weźmy dowolny ideał M pierścienia R/I taki, że $M^2 = \{0 + I\}$. Ze stwierdzenia 5.8 istnieje ideał J pierścienia R zawierające I taki, że $M = J/I$. Z zadania (2) $M^2 = (J^2 + I)/I$. Ale $M^2 = \{0 + I\}$, więc ze stwierdzenia 5.4 $J^2 + I = I$, skąd $J^2 \subseteq I$. Zatem z półpierwszości I, $J \subseteq I$, $J = I$. Stąd $M = \{0 + I\}$. Zatem pierścień R/I jest półpierwszy.

Na odwrót, załóżmy, że pierścień R/I jest półpierwszy. Wtedy R/I jest niezerowy, a więc istnieje $a \in R$ takie, że $a+I \neq 0+I$, skąd $a \notin I$ i wobec tego $I \neq R$. Weźmy dowolny ideał A pierścienia R taki, że $A^2 \subseteq I$. Wtedy $I \subseteq A+I$ oraz $(A+I)^2 = A^2+AI+IA+I^2 \subseteq I$. Ze stwierdzenia 5.8 $M = (A+I)/I \lhd R/I$. Ponadto z zadania (2) $M^2 = \{0+I\}$. Zatem z półpierwszości pierścienia R/I, $M = \{0 + I\}$, skąd $A + I = I$. Zatem $A \subseteq I$ i ideał I jest półpierwszy. □

Twierdzenie 5.17. *Dla dowolnego pierścienia $R \neq \{0\}$ równoważne są warunki:*

(i) R jest pierścieniem półpierwszym,

(ii) jeżeli $aRa = \{0\}$, to $a = 0$ dla dowolnego $a \in R$.

DOWÓD. $(i) \Rightarrow (ii)$. Ponieważ pierścień R jest półpierwszy, więc ideał $\{0\}$ jest półpierwszy. Weźmy dowolne $a \in R$ takie, że $aRa = \{0\}$. Wtedy z twierdzenia 4.29, $a \in \{0\}$, czyli $a = 0$.

$(ii) \Rightarrow (i)$. Z naszego założenia wynika na mocy twierdzenia 4.29, że ideał $\{0\}$ jest półpierwszy, czyli pierścień R jest półpierwszy. □

Twierdzenie 5.18. *Pierścień R jest półpierwszy wtedy i tylko wtedy, gdy R posiada ideał pierwszy i część wspólna wszystkich ideałów pierwszych pierścienia R jest ideałem zerowym.*

DOWÓD. Załóżmy, że pierścień R jest półpierwszy. Wtedy ideał zerowy jest półpierwszy, więc z twierdzenia 4.37 w pierścieniu R istnieje ideał pierwszy i $\{0\}$ jest częścią wspólną rodziny wszystkich ideałów pierwszych pierścienia R.

Na odwrót, załóżmy, że pierścień R posiada ideał pierwszy i $\{0\}$ jest częścią wspólną rodziny wszystkich ideałów pierwszych pierścienia R. Wtedy z twierdzenia 4.37 $\{0\}$ jest ideałem półpierwszym pierścienia R, a więc pierścień R jest półpierwszy. □

Twierdzenie 5.19. *Każdy ideał niezerowy pierścienia pierwszego R jest pierścieniem pierwszym.*

DOWÓD. Niech $I \neq \{0\}$ będzie ideałem pierścienia pierwszego R. Weźmy dowolne ideały A i B pierścienia I takie, że $A \cdot B = \{0\}$. Z lematu Andrunakiewicza $(A)_R^3 \subseteq A$ oraz $(B)_R^3 \subseteq B$ oraz $(A)_R, (B)_R \lhd R$. Zatem $(A)_R^3 \cdot (B)_R^3 = \{0\}$, więc z pierwszości pierścienia R, $(A)_R^3 = \{0\}$ lub $(B)_R^3 = \{0\}$. Stąd zaś znowu z pierwszości R wynika, że $(A)_R = \{0\}$ lub $(B)_R = \{0\}$. Zatem $A = \{0\}$ lub $B = \{0\}$ i pierścień I jest pierwszy. □

Twierdzenie 5.20. *Każdy niezerowy ideał pierścienia półpierwszego R jest pierścieniem półpierwszym.*

DOWÓD. Niech $I \neq \{0\}$ będzie ideałem pierścienia półpierwszego R. Weźmy dowolny ideał A pierścienia I taki, że $A^2 = \{0\}$. Z lematu Andrunakiewicza $(A)_R^3 \subseteq A$ oraz $(A)_R \lhd R$. Zatem $(A)_R^6 = \{0\}$, więc z półpierwszości pierścienia R, $(A)_R^3 = \{0\}$. Stąd zaś znowu z półpierwszości R wynika, że $(A)_R = \{0\}$. Zatem $A = \{0\}$ i pierścień I jest półpierwszy. □

Zadanie (6)**.** Udowodnij, że niezerowy pierścień R jest pierwszy wtedy i tylko wtedy, gdy dla dowolnych ideałów lewostronnych (prawostronnych) A i B z tego, że $A \cdot B = \{0\}$ wynika, że $A = \{0\}$ lub $B = \{0\}$.

Zadanie (7)**.** Udowodnij, że niezerowy pierścień R jest półpierwszy wtedy i tylko wtedy, gdy dla dowolnego ideału lewostronnego (prawostronnego) L z tego, że $L^2 = \{0\}$ wynika, że $L = \{0\}$.

Definicja 5.21. Mówimy, że pierścień R jest *nilpotentny*, jeżeli istnieje liczba naturalna n taka, że $R^n = \{0\}$, tzn. $x_1 \cdot x_2 \cdot \ldots \cdot x_n = 0$ dla dowolnych $x_1, x_2, \ldots, x_n \in R$.

Zadanie (8)**.** Udowodnij, że pierścień półpierwszy R nie posiada niezerowych nilpotentnych ideałów jednostronnych.

Zadanie (9)**.** Udowodnij, że dla dowolnego niezerowego ideału lewostronnego (prawostronnego) L pierścienia pierwszego R: $l_R(L) = \{0\}$ ($r_R(L) = \{0\}$).

Zadanie (10)**.** Udowodnij, że dla dowolnego niezerowego ideału lewostronnego L pierścienia półpierwszego R: $l_R(L) \cap L = \{0\}$.

Zadanie (11)**.** Udowodnij, że przemienny pierścień R jest pierwszy wtedy i tylko wtedy, gdy jest on dziedziną.

Zadanie (12)**.** Udowodnij, że przemienny pierścień R jest półpierwszy wtedy i tylko wtedy, gdy jest on zredukowany.

Zadanie (13)**.** Niech K będzie ciałem. W pierścieniu $R = M_2(K)$ rozważmy $A = \begin{bmatrix} K & 0 \\ K & 0 \end{bmatrix}$ oraz $B = \begin{bmatrix} 0 & 0 \\ K & K \end{bmatrix}$. Udowodnij, że R jest pierścieniem pierszym, $A <_l R$, $B <_r R$ oraz $A \cdot B = \{0\}$.

Zadanie (14)**.** Udowodnij, że iloczyn prosty dowolnej niepustej rodziny pierścieni półpierwszych jest pierścieniem półpierwszym.

Wykład 6

Homomorfizmy pierścieni

6.1 Określenie homomorfizmu pierścieni

Definicja 6.1. Niech R i S będą pierścieniami. Przekształcenie $f\colon R \to S$ nazywamy *homomorfizmem pierścieni*, jeżeli dla dowolnych $a, b \in R$:

$$f(a+b) = f(a) + f(b) \text{ i } f(a \cdot b) = f(a) \cdot f(b).$$

Definicja 6.2. Homomorfizm pierścieni, który jest funkcją różnowartościową nazywamy *zanurzeniem pierścieni*. Mówimy, że pierścień R *zanurza się w pierścień* S, jeżeli istnieje zanurzenie pierścienia R w pierścień S.

Definicja 6.3. Homomorfizm pierścieni, który jest funkcją "na", nazywamy *epimorfizmem pierścieni*. Mówimy, że pierścień S jest *obrazem homomorficznym* pierścienia R, jeżeli istnieje epimorfizm pierścienia R na pierścień S.

Przykład 6.4. Niech I będzie ideałem pierścienia R. Rozważmy przekształcenie $\pi\colon R \to R/I$ dane wzorem

$$\pi(a) = a + I \text{ dla } a \in R.$$

Z definicji pierścienia ilorazowego wynika, że π jest "na". Ponadto dla dowolnych $a, b \in R$: $\pi(a+b) = (a+b) + I = (a+I) + (b+I) = \pi(a) + \pi(b)$ oraz $\pi(a \cdot b) = (a \cdot b) + I = (a+I) \cdot (b+I) = \pi(a) \cdot \pi(b)$. Zatem π jest homomorfizmem pierścieni. Nazywamy go *homomorfizmem naturalnym* pierścienia R na pierścień R/I.

Definicja 6.5. Homomorfizm, który jest bijekcją nazywamy *izomorfizmem pierścieni*. Mówimy, że pierścienie R i S są izomorficzne, jeżeli istnieje izomorfizm pierścieni $f\colon R \to S$. Piszemy wtedy $R \cong S$.

Głównym zadaniem teorii pierścieni jest klasyfikowanie rodzin pierścieni ze względu na pewne własności.

6.2 Własności homomorfizmów pierścieni

Stwierdzenie 6.6. *Złożenie homomorfizmów pierścieni jest homomorfizmem pierścieni. Złożenie izomorfizmów pierścieni jest izomorfizmem pierścieni. Przekształcenie odwrotne do izomorfizmu pierścieni jest izomorfizmem pierścieni.*

Dowód. Rzeczywiście, niech $f\colon R \to S$ i $g\colon S \to T$ będą homomorfizmami pierścieni. Wtedy dla dowolnych $a, b \in R$ mamy, że $(g\circ f)(a+b) = g(f(a+b)) = g(f(a)+f(b)) = g(f(a))+g(f(b)) = (g\circ f)(a)+(g\circ f)(b)$ oraz $(g\circ f)(a\cdot b) = g(f(a\cdot b)) = g(f(a)\cdot f(b)) = g(f(a))\cdot g(f(b)) = (g\circ f)(a)\cdot(g\circ f)(b)$. Zatem $g\circ f$ jest homomorfizmem pierścieni. Jeżeli dodatkowo f i g są bijekcjami, to $g\circ f$ też jest bijekcją. Stąd złożenie izomorfizmów pierścieni jest izomorfizmem pierścieni.

Niech f będzie izomorfizmem pierścienia A na pierścień B. Wtedy f jest bijekcją, więc istnieje przekształcenie $f^{-1}\colon B \to A$ odwrotne do f, przy czym dla dowolnych $a \in A$, $b \in B$: $a = f^{-1}(b)$ wtedy i tylko wtedy, gdy $b = f(a)$. Weźmy dowolne $b, c \in B$. Wtedy istnieją $x, y \in A$ takie, że $b = f(x)$ i $c = f(y)$. Stąd $x = f^{-1}(b)$ i $y = f^{-1}(c)$. Ponadto $b + c = f(x) + f(y) = f(x + y)$ i $bc = f(x)f(y) = f(xy)$, więc $x + y = f^{-1}(b + c)$ oraz $xy = f^{-1}(bc)$. Zatem $f^{-1}(b+c) = f^{-1}(b)+f^{-1}(c)$ i $f^{-1}(bc) = f^{-1}(b)f^{-1}(c)$. W konsekwencji bijekcja f^{-1} jest homomorfizmem pierścieni. Zatem f^{-1} jest izomorfizmem pierścieni. □

Stwierdzenie 6.7. *Dla dowolnych pierścieni A, B, C:*
(i) $A \cong A$,
(ii) jeżeli $A \cong B$, to $B \cong A$,
(iii) jeżeli $A \cong B$ i $B \cong C$, to $A \cong C$.

Dowód. (i). Przekształcenie tożsamościowe $f\colon A \to A$ dane wzorem $f(a) = a$ dla $a \in A$ jest bijekcją i jest homomorfizmem pierścieni. Zatem f jest izomorfizmem pierścieni i $A \cong A$. Podpunkty (ii) oraz (iii) wynikają od razu ze stwierdzenia 6.6. □

Stwierdzenie 6.8. *Niech $f\colon R \to S$ będzie homomorfizmem pierścienia R w pierścień S. Wówczas f jest homomorfizmem grupy R^+ w grupę S^+. W szczególości:*
(a) $f(0) = 0$;
(b) $f(-a) = -f(a)$ dla $a \in R$;
(c) $f(a - b) = f(a) - f(b)$ dla $a, b \in R$;
(d) $f(ka) = kf(a)$ dla $k \in \mathbb{Z}$, $a \in R$;
(e) $f(a_1 + a_2 + \ldots + a_n) = f(a_1) + f(a_2) + \ldots + f(a_n)$ dla $a_1, \ldots, a_n \in R$.
Ponadto $f(a_1 \cdot a_2 \cdot \ldots \cdot a_n) = f(a_1) \cdot f(a_2) \cdot \ldots \cdot f(a_n)$ dla $a_1, \ldots, a_n \in R$.

Dowód. Własności $(a) - (e)$ wynikają z teorii grup. Ostatnią część stwierdzenia dowodzi się przez prostą indukcję. □

Definicja 6.9. *Jądrem homomorfizmu* f pierścienia R w pierścień S nazywamy zbiór $Ker(f) = \{a \in R : f(a) = 0\}$. Mówimy, że to jądro jest **trywialne**, jeżeli $Ker(f) = \{0\}$.

Stwierdzenie 6.10. *Niech* $f\colon R \to S$ *będzie homomorfizmem pierścienia* R *w pierścień* S. *Wówczas* $Ker(f) \lhd R$. *Ponadto* f *jest zanurzeniem wtedy i tylko wtedy, gdy jądro* f *jest trywialne.*

DOWÓD. Ze stwierdzenia 6.8 wynika, że $Ker(f)$ jest podgrupą grupy R^+. Niech $i \in Ker(f)$, $a \in R$. Wtedy $f(i) = 0$, skąd $f(a \cdot i) = f(a) \cdot f(i) = f(a) \cdot 0 = 0$ oraz $f(i \cdot a) = f(i) \cdot f(a) = 0 \cdot f(a) = 0$. Zatem $a \cdot i, i \cdot a \in Ker(f)$. Stąd $Ker(f) \lhd R$. Ostatnia część stwierdzenia wynika z teorii grup. □

Stwierdzenie 6.11. *Niech* $f\colon R \to S$ *będzie homomorfizmem pierścienia* R *w pierścień* S. *Wówczas:*

(i) jeżeli A *jest podpierścieniem pierścienia* R, *to* $f(A)$ *jest podpierścieniem pierścienia* S;

(ii) jeżeli B *jest podpierścieniem pierścienia* S, *to* $f^{-1}(B)$ *jest podpierścieniem pierścienia* R *i* $Ker(f) \subseteq f^{-1}(B)$;

(iii) jeżeli $J <_l S$, *to* $f^{-1}(J) <_l R$ *i* $Ker(f) \subseteq f^{-1}(J)$;

(iv) jeżeli $J <_r S$, *to* $f^{-1}(J) <_r R$ *i* $Ker(f) \subseteq f^{-1}(J)$;

(v) jeżeli $J \lhd S$, *to* $f^{-1}(J) \lhd R$ *i* $Ker(f) \subseteq f^{-1}(J)$.

DOWÓD. (i). Z teorii grup wynika, że $f(A)$ jest podgrupą grupy S^+. Niech $x, y \in f(A)$. Wtedy istnieją $a, b \in A$ takie, że $x = f(a)$ i $y = f(b)$. Stąd $a \cdot b \in A$, więc $f(a \cdot b) \in f(A)$. Ale $x \cdot y = f(a) \cdot f(b) = f(a \cdot b)$, więc $x \cdot y \in f(A)$ i $f(A)$ jest podpierścieniem pierścienia S.

(ii). Z teorii grup wynika, że $f^{-1}(B)$ jest podgrupą grupy R^+. Niech $a, b \in f^{-1}(B)$. Wtedy $f(a), f(b) \in B$, skąd $f(a \cdot b) = f(a) \cdot f(b) \in B$, czyli $a \cdot b \in f^{-1}(B)$. Zatem $f^{-1}(B)$ jest podpierścieniem pierścienia R. Ponadto dla $i \in Ker(f)$ jest $f(i) = 0 \in B$, więc $i \in f^{-1}(B)$, czyli $Ker(f) \subseteq f^{-1}(B)$.

(iii). Z (ii) wynika, że $f^{-1}(J)$ jest podpierścieniem pierścienia R zawierającym $Ker(f)$. Ponadto dla $i \in f^{-1}(J)$, $a \in R$ mamy, że $f(ai) = f(a)f(i) \in J$, bo $f(i) \in J$ oraz $J <_l S$. Stąd $ai \in f^{-1}(J)$ i wobec tego $f^{-1}(J) <_l R$.

(iv) pokazujemy podobnie jak (iii). Natomiast (v) wynika z (iii) oraz z (iv). □

Zadanie (1)**.** Niech f będzie homomorfizmem pierścienia R w pierścień S. Udowodnij, że dla dowolnych podgrup A, B grupy R^+ oraz dla dowolnych $a, b \in R$ zachodzą wzory:

(a) $f(A+B) = f(A)+f(B)$, (b) $f(A \cdot B) = f(A) \cdot f(B)$, (c) $f(\langle a \rangle) = \langle f(a) \rangle$, (d) $f([a]) = [f(a)]$,

(e) $f(aA) = f(a)f(A)$, (f) $f(Aa) = f(A)f(a)$, (g) $f(AaB) = f(A)f(a)f(B)$.

Zadanie (2)**.** Niech f będzie homomorfizmem pierścienia R w pierścień S. Udowodnij, że dla dowolnego $n \in \mathbb{N}$ i dla dowolnych podgrup $A_1, \ldots, A_n$ grupy R^+ zachodzą wzory:

(a) $f(A_1 + \ldots + A_n) = f(A_1) + \ldots + f(A_n)$,
(b) $f(A_1 \cdot \ldots \cdot A_n) = f(A_1) \cdot \ldots f(A_n)$.

Stwierdzenie 6.12. *Niech $f\colon R \to S$ będzie homomorfizmem pierścienia R na pierścień S. Wówczas:*
(i) jeżeli $I <_l R$, to $f(I) <_l S$;
(ii) jeżeli $I <_r R$, to $f(I) <_r S$;
(iii) jeżeli $I \lhd R$, to $f(I) \lhd S$.

DOWÓD. Ze stwierdzenia 6.11 wynika, że w każdym przypadku $f(I)$ jest podpierścieniem pierścienia S. Weźmy dowolne $j \in f(I)$ oraz dowolne $b \in S$. Wtedy istnieją $i \in I$ oraz $a \in R$ takie, że $j = f(i)$ oraz $b = f(a)$.

(i). Ponieważ $I <_l R$, więc $ai \in I$, skąd $bj = f(a)f(i) = f(ai) \in f(I)$. Zatem $f(I) <_l S$. (ii) dowodzi się analogicznie jak (i), zaś (iii) wynika z (i) oraz z (ii). □

Stwierdzenie 6.13. *Obraz homomorficzny pierścienia z jedynką jest pierścieniem z jedynką.*

DOWÓD. Niech f będzie homomorfizmem pierścienia R z jedynką e na pierścień S. Wtedy $x = xe = ex$ dla dowolnego $x \in R$. Weźmy dowolne $a \in S$. Wtedy istnieje $x \in R$ takie, że $a = f(x)$. Zatem $af(e) = f(x)f(e) = f(xe) = f(x) = a$ oraz $f(e)a = f(e)f(x) = f(ex) = f(x) = a$. Stąd $f(e)$ jest jedynką pierścienia S. □

Stwierdzenie 6.14. *Obraz homomorficzny pierścienia przemiennego jest pierścieniem przemiennym.*

DOWÓD. Niech f będzie homomorfizmem przemiennego pierścienia R na pierścień S. Weźmy dowolne $a, b \in S$. Wtedy istnieją $x, y \in R$ takie, że $a = f(x)$ i $b = f(y)$. Ponadto z przemienności pierścienia R, $xy = yx$. Zatem $ba = f(y)f(x) = f(yx) = f(xy) = f(x)f(y) = ab$ i pierścień S jest przemienny. □

Stwierdzenie 6.15. *Niech $f\colon R \to S$ będzie homomorfizmem pierścienia R na pierścień S. Wówczas odwzorowanie $B \mapsto f^{-1}(B)$ jest bijekcją rodziny wszystkich podpierścieni (ideałów lewostronnych, ideałów prawostronnych, ideałów) pierścienia S na rodzinę wszystkich podpierścieni (ideałów lewostronnych, ideałów prawostronnych, ideałów) pierścienia R zawierających $Ker(f)$.*

DOWÓD. Niech A będzie podpierścieniem (ideałem lewostronnym, ideałem prawostronnym, ideałem) pierścienia R zawierającym $Ker(f)$. Wtedy na mocy stwierdzeń 6.11 i 6.12 $f(A)$ jest podpierścieniem (ideałem lewostronnym, ideałem prawostronnym, ideałem) pierścienia S. Ponadto $A \subseteq f^{-1}(f(A))$ oraz dla $x \in f^{-1}(f(A))$ mamy, że $f(x) \in f(A)$. Zatem istnieje $a \in A$ takie, że $f(x) = f(a)$. Stąd $f(x - a) = 0$, czyli $x - a \in Ker(f) \subseteq A$, a więc $x \in A$ i ostatecznie $A = f^{-1}(f(A))$. Wynika stąd, że odwzorowanie $B \mapsto f^{-1}(B)$ jest

"na". Weźmy dowolne podpierścienie (ideały lewostronne, ideały prawostronne, ideały) B, C pierścienia S takie, że $f^{-1}(B) = f^{-1}(C)$. Ponieważ odwzorowanie f jest "na", więc $B = f(f^{-1}(B))$ i $C = f(f^{-1}(C))$, skąd $B = C$ i odwzorowanie $B \mapsto f^{-1}(B)$ jest różnowartościowe. □

Wniosek 6.16. *Niech $f\colon R \to S$ będzie izomorfizmem pierścienia R na pierścień S. Wówczas odwzorowanie $B \mapsto f^{-1}(B)$ jest bijekcją rodziny wszystkich podpierścieni (ideałów lewostronnych, ideałów prawostronnych, ideałów) pierścienia S na rodzinę wszystkich podpierścieni (ideałów lewostronnych, ideałów prawostronnych, ideałów) pierścienia R.*

Stwierdzenie 6.17. *Załóżmy, że pierścienie R i S są izomorficzne. Wówczas:*
(i) jeżeli pierścień R jest przemienny, to pierścień S też jest przemienny;
(ii) jeżeli pierścień R ma jedynkę, to pierścień S też ma jedynkę;
(iii) jeżeli pierścień R jest prosty, to pierścień S też jest prosty;
(iv) jeżeli pierścień R jest pierwszy, to pierścień S też jest pierwszy;
(v) jeżeli pierścień R jest półpierwszy, to pierścień S też jest półpierwszy.

DOWÓD. Z założenia istnieje izomorfizm pierścieni $f\colon R \to S$. (i) oraz (ii) wynikają od razu ze stwierdzeń 6.13 i 6.14.

(iii). Ponieważ zbiory R i S są równoliczne oraz $|R| > 1$, więc $|S| > 1$, czyli pierścień S jest niezerowy. Ponadto pierścień R ma dokładnie dwa ideały, więc z wniosku 6.16 pierścień S też posiada dokładnie dwa ideały. Stąd pierścień S jest prosty.

(iv). Podobnie jak w (iii) mamy, że pierścień S jest niezerowy. Weźmy dowolne ideały A i B pierścienia S takie, że $AB = \{0\}$. Wtedy ze stwierdzenia 6.11 i zadania (1) mamy, że $f^{-1}(A), f^{-1}(B) \lhd R$ oraz $f^{-1}(A) \cdot f^{-1}(B) = f^{-1}(AB) = f^{-1}(\{0\}) = \{0\}$. Z pierwszości pierścienia R, $f^{-1}(A) = \{0\}$ lub $f^{-1}(B) = \{0\}$. Zatem $A = \{0\}$ lub $B = \{0\}$ i pierścień S jest pierwszy.

(v). Podobnie jak w (iii) mamy, że pierścień S jest niezerowy. Weźmy dowolny ideał A pierścienia S taki, że $A^2 = \{0\}$. Wtedy ze stwierdzenia 6.11 i zadania (1) mamy, że $f^{-1}(A) \lhd R$ oraz $f^{-1}(A) \cdot f^{-1}(A) = f^{-1}(A^2) = f^{-1}(\{0\}) = \{0\}$. Z półpierwszości pierścienia R, $f^{-1}(A) = \{0\}$. Zatem $A = \{0\}$ i pierścień S jest półpierwszy. □

6.3 Twierdzenia o izomorfizmach

Twierdzenie 6.18 (pierwsze o izomorfizmie)**.** *Niech f będzie homomorfizmem pierścienia R na pierścień S. Wówczas*

$$S \cong R/Ker(f).$$

DOWÓD. Niech $F\colon R/Ker(f) \to S$ będzie dane wzorem $F(r+Ker(f)) = f(r)$ dla $r \in R$. Wtedy z teorii grup wiadomo, że F jest dobrze określoną funkcją, która jest izomorfizmem grup addytywnych. Ponadto dla $a, b \in R$ mamy, że

$F((a+Ker(f))\cdot(b+Ker(f))) = F(ab+Ker(f)) = f(ab) = f(a)f(b) = F(a+Ker(f))\cdot F(b+Ker(f))$, czyli ostatecznie F jest izomorfizmem pierścieni. □

Twierdzenie 6.19 (drugie o izomorfizmie)**.** *Niech A będzie podpierścieniem pierścienia R i niech $I \lhd R$. Wówczas $A + I$ jest podpierścieniem pierścienia R, $A \cap I \lhd A$ oraz*

$$(A + I)/I \cong A/A \cap I.$$

DOWÓD. Z zadania (1) z rozdziału 4, $A + I$ jest podpierścieniem pierścienia R. Weźmy dowolne $a \in A$ oraz $i \in I$. Wtedy $(a + i) - a = i \in I$, skąd $(a + i) + I = a + I$. Zatem $(A + I)/I = \{a + I : a \in A\}$. Wynika stąd, że funkcja $f : A \longrightarrow (A + I)/I$ dana wzorem $f(a) = a + I$ dla $a \in A$ jest "na". Ponadto dla $a, b \in A$ mamy, że $f(a + b) = (a + b) + I = (a + I) + (b + I) = f(a) + f(b)$ oraz $f(a \cdot b) = ab + I = (a + I) \cdot (b + I) = f(a) \cdot f(b)$. Zatem f jest homomorfizmem pierścienia A na pierścień $(A + I)/I$. Stąd z twierdzenia 6.18 wynika, że $(A + I)/I \cong A/Ker(f)$. Ale $x \in Ker(f) \Leftrightarrow (x \in A \wedge x + I = 0 + I) \Leftrightarrow (x \in A \wedge x \in I) \Leftrightarrow x \in A \cap I$. Stąd $Ker(f) = A \cap I$, czyli $A \cap I \lhd A$ i $(A + I)/I \cong A/A \cap I$. □

Twierdzenie 6.20 (trzecie o izomorfizmie)**.** *Niech I, J będą ideałami pierścienia R takimi, że $J \subseteq I$. Wówczas*

$$(R/J)/(I/J) \cong R/I.$$

DOWÓD. Niech $f : R/J \longrightarrow R/I$ będzie przekształceniem danym wzorem $f(a + J) = a + I$ dla $a \in R$. Jeśli $a, b \in R$ są takie, że $a + J = b + J$, to $a - b \in J$. Ale $J \subseteq I$, więc wtedy $a - b \in I$, czyli $a + I = b + I$. Oznacza to, że f jest dobrze określone. Ponadto f jest homomorfizmem pierścienia R/J na pierścień R/I. Zatem z twierdzenia 6.18 mamy, że $R/I \cong (R/J)/Ker(f)$. Niech $a \in R$. Jeśli $a+J \in Ker(f)$, to $a+I = 0+I$, skąd $a \in I$. Jeśli zaś $a \in I$, to $a + I = 0 + I$, skąd $a + J \in Ker(f)$. Zatem $Ker(f) = I/J$ i twierdzenie jest udowodnione. □

Zadanie (3)**.** Niech A będzie dowolnym pierścieniem i niech $R = \begin{bmatrix} A & A \\ 0 & A \end{bmatrix}$ będzie podpierścieniem pierścienia macierzy $M_2(A)$. Skonstruować homomorfizm pierścienia R na pierścień: (a) $A \times A$, (b) A.

Zadanie (4)**.** W pierścieniu macierzy $M_2(\mathbb{R})$ znaleźć podpierścień izomorficzny z ciałem: (a) $\mathbb{R}$, (b) $\mathbb{C}$.

Zadanie (5)**.** Wyznaczyć wszystkie z dokładnością do izomorfizmu pierścienie pierwsze, które są obrazami homomorficznymi pierścienia R z zadania 3 przy założeniu, że A jest ciałem.

Zadanie (6)**.** Czy dla pewnego ciała A podpierścień $S = \begin{bmatrix} A & A \\ 0 & 0 \end{bmatrix}$ pierścienia $M_2(A)$ jest obrazem homomorficznym pierścienia R z zadania 3?

Zadanie (7)**.** Niech A będzie niezerowym pierścieniem z jedynką. Udowodnij, że pierścienie $\begin{bmatrix} A & A \\ 0 & 0 \end{bmatrix}$ i $\begin{bmatrix} 0 & 0 \\ A & A \end{bmatrix}$ są izomorficzne, zaś pierścienie $\begin{bmatrix} A & A \\ 0 & 0 \end{bmatrix}$ i $\begin{bmatrix} 0 & A \\ 0 & A \end{bmatrix}$ nie są izomorficzne.

Zadanie (8)**.** Udowodnij, że dla dowolnego ciała K pierścień $K[x]/(x^2)$ jest izomorficzny z podpierścieniem $A = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} : a, b \in K \right\}$ pierścienia $M_2(K)$.

Wykład 7

Przykłady homomorfizmów

7.1 Dołączanie jedynki do pierścienia

Twierdzenie 7.1. *Niech R będzie pierścieniem, który nie posiada jedynki. Wówczas istnieje pierścień R^1 z jedynką 1 taki, że $R \lhd R^1$, $R + \langle 1 \rangle = R^1$, $R \cap \langle 1 \rangle = \{0\}$ oraz $R^1/R \cong \mathbb{Z}$. Ponadto każdy ideał (ideał lewostronny, ideał prawostronny) pierścienia R jest ideałem (ideałem lewostronnym, ideałem prawostronnym) pierścienia R^1.*

Dowód. W zbiorze $R^1 = R \times \mathbb{Z}$ wprowadzamy dodawanie po współrzędnych:

$$(a,k) + (b,l) = (a+b, k+l) \text{ dla dowolnych } a,b \in R,\ k,l \in \mathbb{Z}$$

oraz mnożenie:

$$(a,k) \cdot (b,l) = (ab + la + kb, kl) \text{ dla dowolnych } a,b \in R,\ k,l \in \mathbb{Z}. \quad (7.1)$$

Udowodnimy najpierw, że $(R^1, +, \cdot, (0,0), (0,1))$ jest pierścieniem z jedynką $(0,1)$. Zauważmy, że $(R^1, +, (0,0))$ jest grupą abelową, gdyż jest to iloczyn prosty grup abelowych R^+ i $\mathbb{Z}^+$.

Weźmy dowolne $x, y, z \in R^1$. Wtedy istnieją $a, b, c \in R$ oraz $k, l, m \in \mathbb{Z}$ takie, że $x = (a,k)$, $y = (b,l)$ i $z = (c,m)$. Ze wzoru (7.1): $(x \cdot y) \cdot z = (ab + la + kb, kl) \cdot (c,m) = ((ab + la + kb)c + m(ab + la + kb) + (kl)c, (kl)m) = ((ab)c + l(ac) + k(bc) + m(ab) + (ml)a + (mk)b + (kl)c, klm)$ oraz $x \cdot (y \cdot z) = (a,k) \cdot (bc + mb + lc, lm) = (a(bc + mb + lc) + (lm)a + k(bc + mb + lc), k(lm)) = (a(bc) + m(ab) + l(ac) + (lm)a + k(bc) + (km)b + (kl)c, klm)$. Zatem z łączności mnożenia w pierścieniu R i własności dodawania i mnożenia liczb całkowitych $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

Ponadto $x \cdot (y + z) = (a,k) \cdot (b + c, l + m) = (a(b + c) + (l + m)a + k(b + c), k(l + m)) = (ab + ac + la + ma + kb + kc, kl + km)$ oraz $x \cdot y + x \cdot z = (ab + la + kb, kl) + (ac + ma + kc, km) = (ab + la + kb + ac + + ma + kc, kl + km)$. Zatem $x \cdot (y + z) = x \cdot y + x \cdot z$. Dalej, $(y + z) \cdot x = (b + c, l + m) \cdot (a,k) = ((b+c)a + k(b+c) + (l+m)a, (l+m)k) = (ba + ca + kb + kc + la + ma, lk + mk)$ oraz

$y\cdot x+z\cdot x=(b,l)\cdot(a,k)+(c,m)\cdot(a,k)=(ba+kb+la,lk)+(ca+kc+ma,mk)=(ba+kb+la+ca+kc+ma,lk+mk)$, skąd $(y+z)\cdot x=y\cdot x+z\cdot x$.

Ze wzoru (7.1) mamy też, że $(0,1)\cdot x=(0\cdot a+k\cdot 0+1\cdot a,1\cdot k)=(a,k)=x$ oraz $x\cdot(0,1)=(a\cdot 0+1\cdot a+k\cdot 0,k\cdot 1)=x$.

Zatem $(R^1,+,\cdot,(0,0),(0,1))$ jest pierścieniem z jedynką $(0,1)$, którą będziemy też oznaczali symbolem 1.

Rozważmy przekształcenie $f\colon R^1\to\mathbb{Z}$ dane wzorem:

$$f((a,k))=k \text{ dla } a\in R, k\in\mathbb{Z}.$$

Dla dowolnych $a,b\in R$, $k,l\in\mathbb{Z}$, $f((a,k)+(b,l))=f((a+b,k+l))=k+l=f((a,k))+f((b,l))$ oraz $f((a,k)\cdot(b,l))=f((ab+la+kb,kl))=kl=f((a,k))\cdot f((b,l))$. Zatem f jest homomorfizmem pierścieni. Ponadto dla $k\in\mathbb{Z}$ mamy, że $k=f((0,k))$, więc f jest epimorfizmem pierścieni. Z definicji f otrzymujemy, że $Ker(f)=\overline{R}$, gdzie $\overline{R}=\{(a,0):a\in R\}$. Stąd na mocy stwierdzenia 6.10 $\overline{R}\lhd R^1$. Ponadto z pierwszego twierdzenia o izomorfizmie $R^1/\overline{R}\cong\mathbb{Z}$. Dla $a\in R$, $k\in\mathbb{Z}$ mamy, że $(a,k)=(a,0)+(0,k)=(a,0)+k(0,1)=(a,0)+k\cdot 1$, skąd $R^1=\overline{R}+\langle 1\rangle$ oraz $\overline{R}\cap\langle 1\rangle=\{(0,0)\}$.

Przekształcenie $a\mapsto(a,0)$ dla $a\in R$ jest różnowartościowe oraz na mocy określeń dodawania i mnożenia w pierścieniu R^1 jest ono homomorfizmem pierścieni. Zatem to odwzorowanie jest zanurzeniem pierścieni. Z tego powodu możemy dokonać utożsamienia:

$$(a,0)\equiv a \text{ dla } a\in R.$$

Przy tym utożsamieniu $R=\overline{R}$ jest ideałem pierścienia R^1, $R^1=R+\langle 1\rangle$, $R\cap\langle 1\rangle=\{0\}$ oraz $R^1/R\cong\mathbb{Z}$.

Niech $I<_l R$. Wtedy I jest podgrupą grupy addytywnej pierścienia R^1. Ponadto dla $i\in I$ oraz $x\in R^1$ istnieją $a\in R$, $k\in\mathbb{Z}$ takie, że $x=a+k\cdot 1$. Zatem $x\cdot i=(a+k\cdot 1)\cdot i=ai+ki\in I$, bo $I<_l R$. Stąd $I<_l R^1$. Analogicznie pokazuje się, że jeśli $I<_r R$, to $I<_r R^1$. W konsekwencji, jeżeli $I\lhd R$, to $I\lhd R^1$. □

7.2 Homomorfizmy na pierścieniach macierzy

Twierdzenie 7.2. *Niech $f\colon R\to S$ będzie homomorfizmem pierścieni. Wówczas $F\colon M_n(R)\to M_n(S)$ dane wzorem $F(A)=[f([A]_{ij})]_{i,j=1,2,\dots,n}$ jest homomorfizmem pierścieni i $Ker(F)=M_n(Ker(f))$. Ponadto F jest epimorfizmem wtedy i tylko wtedy, gdy f jest epimorfizmem.*

Dowód. Weźmy dowolne $A,B\in M_n(R)$. Ze wzoru (2.2) $[A+B]_{ij}=[A]_{ij}+[B]_{ij}$ dla dowolnych $i,j=1,\dots,n$. Zatem $F(A+B)=[f([A]_{ij}+[B]_{ij})]_{i,j=1,\dots,n}=[f([A]_{ij})+f([B]_{ij})]_{i,j=1,\dots,n}=[f([A]_{ij})]_{i,j=1,\dots,n}+[f([B]_{ij})]_{i,j=1,\dots,n}=F(A)+F(B)$.

Ponadto ze wzoru (2.3)

$F(A \cdot B) = \left[f\left(\sum_{t=1}^{n} [A]_{it} \cdot [B]_{tj}\right)\right]_{i,j=1,\ldots,n} = \left[\sum_{t=1}^{n} f([A]_{it}) \cdot f([B]_{tj})\right]_{i,j=1,\ldots,n} = [f([A]_{ij})]_{i,j=1,\ldots,n} \cdot [f([B]_{ij}]_{i,j=1,\ldots,n} = F(A) \cdot F(B)$. Zatem F jest homomorfizmem pierścieni. Pozostała część twierdzenia wynika od razu z definicji odwzorowania F. □

Stwierdzenie 7.3. *Dla dowolnego pierścienia R równoważne są warunki:*
(i) $I = RI = IR = RIR$ dla dowolnego $I \lhd R$,
(ii) $a \in RaR$ dla dowolnego $a \in R$.

DOWÓD. $(i) \Rightarrow (ii)$. Niech $I = (a)_R$. Ponieważ $(a)_R = \langle a \rangle + Ra + aR + RaR$, więc $RI = Ra + RaR$, skąd $RIR = RaR$. Ale $I = RIR$ oraz $a \in I$, więc $a \in RaR$.

$(ii) \Rightarrow (i)$. Oczywiście $RIR \subseteq RI \subseteq I$ oraz $RIR \subseteq IR \subseteq I$. Wystarczy zatem wykazać, że $I \subseteq RIR$. W tym celu weźmy dowolne $a \in I$. Wtedy $a \in RaR \subseteq RIR$, czyli $a \in RIR$. Stąd $I \subseteq RIR$. □

Przykład 7.4. Jeżeli pierścień R posiada jedynkę, to $a \in RaR$ dla każdego $a \in R$. Ponadto z twierdzenia 5.10, jeżeli R jest pierścieniem prostym i $R^2 \neq \{0\}$, to $RaR = R$ dla każdego $0 \neq a \in R$, skąd $a \in RaR$ dla każdego $a \in R$. Mówimy, że pierścień R jest *regularny w sensie von Neumanna*, jeżeli $a \in aRa$ dla każdego $a \in R$. Wówczas $a \in aRaRa \subseteq RaR$ dla każdego $a \in R$.

Twierdzenie 7.5. *Jeżeli $a \in RaR$ dla każdego elementu a pierścienia R, to dla dowolnego $n \in \mathbb{N}$ każdy ideał pierścienia $M_n(R)$ jest postaci $M_n(I)$ dla $I \lhd R$.*

DOWÓD. Niech $J \lhd M_n(R)$. Weźmy dowolne $A \in J$ i dowolne $k, l = 1, \ldots, n$. Niech $a = [A]_{kl}$. Weźmy dowolne $x, y \in R$ oraz dowolne $i, j = 1, \ldots, n$. Wtedy $(xE_{ik}) \cdot A \in J$, więc też $(xE_{ik}) \cdot A \cdot (yE_{lj}) \in J$. Ale $A = \sum_{t,s=1}^{n} ([A]_{ts}E_{ts})$, więc na mocy wzoru (2.4) $(xE_{ik}) \cdot A \cdot (yE_{lj}) = (xay)E_{ij}$. Zatem $(xay)E_{ij} \in J$ dla dowolnych $x, y \in R$ oraz dla dowolnych $i, j \in \{1, 2, \ldots, n\}$. Ponieważ J^+ jest podgrupą grupy addytywnej pierścienia $M_n(R)$, więc stąd $(RaR)E_{ij} \subseteq J$. Ale $a \in RaR$, więc $aE_{ij} \in J$ dla wszystkich $i, j \in \{1, 2, \ldots, n\}$. Niech $I = \{x \in R : xE_{ij} \in J \text{ dla pewnych } i, j = 1, \ldots, n\}$. Wtedy $a \in I$, skąd $I \neq \emptyset$. Weźmy dowolne $x, y \in I$, $r \in R$. Z pierwszej części dowodu $xE_{11}, yE_{11} \in J$, skąd $(x-y)E_{11} = xE_{11} - yE_{11} \in J$, czyli $x - y \in I$. Ponadto $(rE_{11}) \cdot (xE_{11}), (xE_{11}) \cdot (rE_{11}) \in J$, więc na mocy wzoru (2.4), $(rx)E_{11}, (xr)E_{11} \in J$, czyli $rx, xr \in I$. Zatem $I \lhd R$. Ponadto z pierwszej części dowodu i z definicji I, $J = M_n(I)$. □

Twierdzenie 7.6. *Niech $a \in RaR$ dla każdego elementu a pierścienia R. Wówczas dla każdego $n \in \mathbb{N}$ każdy obraz homomorficzny pierścienia $M_n(R)$ jest izomorficzny z pierścieniem postaci $M_n(R/I)$ dla pewnego $I \lhd R$.*

DOWÓD. Załóżmy, że pierścień S jest obrazem homomorficznym pierścienia $M_n(R)$. Wtedy z pierwszego twierdzenia o izomorfizmie $S \cong M_n(R)/Ker(f)$, gdzie f jest homomorfizmem pierścienia $M_n(R)$ na pierścień S. Ale $Ker(f) \lhd M_n(R)$, więc z twierdzenia 7.5, $Ker(f) = M_n(I)$ dla pewnego ideału I pierścienia R. Z przykładu 6.4 wynika, że $\pi\colon R \to R/I$ dane wzorem $\pi(x) = x + I$ jest epimorfizmem pierścieni. Ponadto $Ker(\pi) = I$. Zatem z twierdzenia 7.2, istnieje epimorfizm $\Pi\colon M_n(R) \to M_n(R/I)$ taki, że $Ker(\Pi) = M_n(I) = M_n(Ker(f))$. Stąd i z pierwszego twierdzenia o izomorfizmie $M_n(R/I) \cong M_n(R)/Ker(f)$, a więc $M_n(R/I) \cong S$. □

Z twierdzenia 7.5 i z przykładu 7.4 wynika od razu następujące

Twierdzenie 7.7. *Jeżeli R jest pierścieniem prostym takim, że $R^2 \neq \{0\}$, to dla dowolnego $n \in \mathbb{N}$ pierścień $M_n(R)$ jest prosty.*

Z twierdzenia 7.7 otrzymujemy natychmiast następujący

Wniosek 7.8. *Dla dowolnego ciała K i dla dowolnego naturalnego n pierścień $M_n(K)$ jest prosty.*

Twierdzenie 7.9. *Niech R będzie takim pierścieniem, że dla pewnego $n \in \mathbb{N}$, $n \geqslant 2$, każdy ideał pierścienia $M_n(R)$ jest postaci $M_n(I)$ dla pewnego $I \lhd R$. Wówczas $a \in RaR$ dla każdego $a \in R$.*

DOWÓD. Niech $I \lhd R$. Nietrudno sprawdzić, że

$$J = \begin{bmatrix} I & IR & \dots & IR \\ RI & RIR & \dots & RIR \\ \vdots & \vdots & \ddots & \vdots \\ RI & RIR & \dots & RIR \end{bmatrix}$$

jest ideałem pierścienia $M_n(R)$. Zatem istnieje ideał A pierścienia R taki, że $J = M_n(A)$. Stąd $A = I = RI = IR = RIR$. Zatem na mocy stwierdzenia 7.3, $a \in RaR$ dla każdego $a \in R$. □

Zadanie (1)**.** Niech R będzie pierścieniem takim, że dla pewnego naturalnego $n \geqslant 2$ pierścień $M_n(R)$ jest prosty. Udowodnij, że wówczas pierścień R jest prosty i $R^2 \neq \{0\}$.

Zadanie (2)**.** Dla $n \in \mathbb{N}$ wyznacz wszystkie z dokładnością do izomorfizmu obrazy homomorficzne pierścienia $M_n(\mathbb{Z})$.

Zadanie (3)**.** Niech R będzie dowolnym pierścieniem i $n \in \mathbb{N}$. Udowodnij, że przekształcenie $f\colon M_n(R) \to M_{n+1}(R)$ dane wzorem

$$f\left(\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}\right) = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} & 0 \\ a_{21} & a_{22} & \dots & a_{2n} & 0 \\ \vdots & \vdots & \ddots & \vdots & \\ a_{n1} & a_{n2} & \dots & a_{nn} & 0 \\ 0 & 0 & \dots & 0 & 0 \end{bmatrix}$$

jest zanurzeniem pierścieni.

Zadanie (4)**.** Udowodnij, że dla dowolnego pierścienia R i dla dowolnych $m, n \in \mathbb{N}$: $M_n(M_m(R)) \cong M_{mn}(R)$.

Zadanie (5)**.** Niech K będzie dowolnym ciałem. Pokazać, że dla każdego n pierścienie $M_n(K)$ i $M_{n+1}(K)$ nie są izomorficzne.

7.3 Homomorfizmy na pierścieniach wielomianów

Twierdzenie 7.10. *Niech $f\colon R \to S$ będzie homomorfizmem pierścieni. Wówczas przekształcenie $F\colon R[[x]] \to S[[x]]$ dane wzorem $F((a_0, a_1, \ldots)) = (f(a_0), f(a_1), \ldots)$ jest homomorfizmem pierścieni.*

DOWÓD. Weźmy dowolne szeregi $a, b \in R[[x]]$. Wtedy $a + b = (a_0 + b_0, a_1 + b_1, \ldots)$, więc $F(a + b) = (f(a_0 + b_0), f(a_1 + b_1), \ldots) = (f(a_0) + f(b_0), f(a_1) + f(b_1), \ldots) = (f(a_0), f(a_1), \ldots) + (f(b_0), f(b_1), \ldots) = F(a) + F(b)$. Ponadto $a \cdot b = (c_0, c_1, \ldots)$, gdzie $c_n = \sum_{i=0}^{n} a_i b_{n-i}$ dla $n = 0, 1, \ldots$. Zatem $F(a \cdot b) = (d_0, d_1, \ldots)$, gdzie $d_n = f\left(\sum_{i=0}^{n} a_i b_{n-i}\right) = \sum_{i=0}^{n} f(a_i) \cdot f(b_{n-i})$ dla $n = 0, 1, \ldots$. Ponadto $F(a) \cdot F(b) = (f(a_0), f(a_1), \ldots) \cdot (f(b_0), f(b_1), \ldots) = (e_0, e_1, \ldots)$, gdzie $e_n = \sum_{i=0}^{n} f(a_i) \cdot f(b_{n-i})$ dla $n = 0, 1, \ldots$. Zatem $e_n = d_n$ dla wszystkich $n = 0, 1, \ldots$, skąd $F(a \cdot b) = F(a) \cdot F(b)$. Oznacza to, że F jest homomorfizmem pierścieni. □

Z udowodnionego twierdzenia w prosty sposób wynika następujące

Twierdzenie 7.11. *Niech $f\colon R \to S$ będzie homomorfizmem pierścieni. Wówczas przekształcenie $F\colon R[x] \to S[x]$ dane wzorem $F((a_0, a_1, \ldots)) = (f(a_0), f(a_1), \ldots)$ jest homomorfizmem pierścieni.*

Stwierdzenie 7.12. *Dla dowolnego pierścienia R przekształcenie $f\colon R[[x]] \to R$ dane wzorem $f((a_0, a_1, \ldots)) = a_0$ jest epimorfizmem pierścieni.*

DOWÓD. Weźmy dowolne szeregi $a, b \in R[[x]]$. Wtedy $a + b = (a_0 + b_0, a_1 + b_1, \ldots)$, więc $f(a+b) = a_0 + b_0 = f(a) + f(b)$ oraz $a \cdot b = (a_0 b_0, a_0 b_1 + a_1 b_0, \ldots)$, skąd $f(a \cdot b) = a_0 b_0 = f(a) \cdot f(b)$. Zatem f jest homomorfizmem pierścieni. Ponadto dla dowolnego $a \in R$, $a = f((a, 0, 0, \ldots))$, więc f jest epimorfizmem pierścieni. □

Zupełnie analogicznie można udowodnić następujące

Stwierdzenie 7.13. *Dla dowolnego pierścienia R przekształcenie $f\colon R[x] \to R$ dane wzorem $f((a_0, a_1, \ldots)) = a_0$ jest epimorfizmem pierścieni.*

Zadanie (6)**.** Udowodnij, że dla dowolnego pierścienia R przekształcenie $g\colon R \to R[x]$ dane wzorem $g(a) = (a, 0, 0, \ldots)$ jest zanurzeniem pierścieni.

Z zadania (6) wynika, że podobnie jak w algebrze przemiennej, w pierścieniu $R[x]$ możemy dokonać utożsamienia

$$a \equiv (a, 0, 0, \ldots) \text{ dla } a \in R.$$

Przy tym utożsamieniu pierścień R jest podpierścieniem pierścienia wielomianów $R[x]$.

Zadanie (7)**.** Niech S będzie pierścieniem z jedynką 1 i niech $x = (0, 1, 0, \ldots)$. Udowodnij, że wówczas w pierścieniu $S[[x]]$: $x^n = (0, 0, \ldots, \overset{n}{1}, 0, 0, \ldots)$ dla każdego $n = 0, 1, \ldots$.

Niech S będzie pierścieniem z jedynką 1. Niech $f \in S[x]$ będzie wielomianem stopnia $n \geqslant 1$. Wtedy $f_n \neq 0$ oraz $f_i = 0$ dla każdego $i \geqslant n+1$. Ponadto z zadania (7) i ze wzoru (2.12) mamy, że $(f_k, 0, 0, \ldots) \cdot x^k = (0, \ldots, 0, \overset{k}{f_k}, 0, \ldots)$ dla $k = 1, 2, \ldots$ więc
$f = (f_0, 0, 0, \ldots) + (0, f_1, 0, \ldots) + \ldots + (0, 0, \ldots, f_n, 0, \ldots) \equiv f_0 + f_1 x + {} + f_2 x^2 + \ldots + f_n x^n$. Ponieważ dla wielomianu stałego f jest $f \equiv f_0$, więc dla dowolnego wielomianu $f \in S[x]$ stopnia $n \geqslant 0$ mamy utożsamienie:

$$f \equiv f_0 + f_1 x + f_2 x^2 + \ldots + f_n x^n. \tag{7.2}$$

Otrzymujemy w ten sposób naturalną notację dla wielomianów z pierścienia $S[x]$. Zauważmy, że x należy do centrum pierścienia $S[[x]]$.

Analogicznie szereg $f = (f_0, f_1, \ldots) \in S[[x]]$ można utożsamić z $f_0 + f_1 x + f_2 x^2 + \ldots$.

Zadanie (8)**.** Udowodnij, że dla dowolnego pierścienia S z jedynką element x należy do centrum pierścienia $S[[x]]$.

Jeżeli pierścień R nie posiada jedynki, to sytuacja jest bardziej skomplikowana. Wówczas jak wiemy R jest ideałem pierścienia R^1 posiadającego jedynkę. Stąd $R[x] \lhd R^1[x]$ i dowolny niezerowy wielomian $f \in R[x]$ można jednoznacznie zapisać w postaci $f = f_0 + f_1 x + \ldots + f_n x^n$ dla pewnego $n = 0, 1, \ldots$ i dla pewnych współczynników $f_0, \ldots, f_n \in R$. Należy jednak pamiętać, że w tym przypadku $x \notin R[x]$ oraz $(ax^n) \cdot (bx^m) = (ab)x^{n+m}$ dla dowolnych $a, b \in R$, $n, m = 0, 1, \ldots$. Analogicznie, każdy szereg $f \in R[[x]]$ można jednoznacznie zapisać w postaci $f = f_0 + f_1 x + f_2 x^2 + \ldots$ dla pewnych $f_i \in R$, $i = 0, 1, \ldots$, ale $x \notin R[[x]]$!

7.4 Homomorfizmy związane z iloczynami prostymi

Przykład 7.14. Dla dowolnego niepustego zbioru indeksów T niech $\{R_t\}_{t\in T}$ będzie rodziną pierścieni. Dla dowolnego $s \in T$ rozważmy przekształcenie $\pi_s\colon \prod_{t\in T} R_t \to R_s$ dane wzorem

$$\pi_s((x_t)_{t\in T}) = x_s.$$

Wówczas dla dowolnych $x = (x_t)_{t\in T}, y = (y_t)_{t\in T} \in \prod_{t\in T} R_t$: $\pi_s(x+y) = \pi_s((x_t+y_t)_{t\in T}) = x_s + y_s = \pi_s(x) + \pi_s(y)$ oraz $\pi_s(x\cdot y) = \pi_s((x_t\cdot y_t)_{t\in T}) = x_s \cdot y_s = \pi_s(x)\cdot\pi_s(y)$. Zatem π_s jest homomorfizmem pierścieni. Dla dowolnego $a \in R_s$ mamy, że $a = \pi_s((x_t)_{t\in T})$, gdzie $x_s = a$ oraz $x_t = 0$ dla wszystkich $t \in T \setminus \{s\}$. Stąd π_s jest epimorfizmem pierścieni. Natomiast $Ker\,\pi_s = \prod_{t\in T} I_t$, gdzie $I_s = \{0\}$ oraz $I_t = R_t$ dla wszystkich $t \in T \setminus \{s\}$. Z pierwszego twierdzenia o izomorfizmie wynika stąd, że

$$\prod_{t\in T} R_t / \prod_{t\in T} I_t \cong R_s.$$

Zatem dla każdego $s \in T$ pierścień R_s jest obrazem homomorficznym pierścienia $\prod_{t\in T} R_t$.

Okazuje się, że dla każdego $s \in T$ pierścień R_s zanurza się w pierścień $\prod_{t\in T} R_t$. Łatwo sprawdzić, że przekształcenie $f_s\colon R_s \to \prod_{t\in T} R_t$ dane wzorem

$$f_s(a) = (x_t)_{t\in T} \text{ gdzie } x_s = a \text{ oraz } x_t = 0 \text{ dla } t \in T \setminus \{s\}$$

jest zanurzeniem pierścieni, przy czym $f_s(R_s) \lhd \prod_{t\in T} R_t$.

Wykład 8

Własności pierścieni macierzy

8.1 Centrum pierścienia macierzy

Definicja 8.1. *Obustronnym anihilatorem* niepustego podzbioru X pierścienia R nazywamy zbiór

$$a_R(X) = l_R(X) \cap r_R(X) = \{a \in R : aX = Xa = \{0\}\}. \tag{8.1}$$

Ponieważ $l_R(X)$ i $r_R(X)$ są podpierścieniami pierścienia R, więc $a_R(X)$ jest podpierścieniem pierścienia R. Jeśli zaś $I \lhd R$, to $l_R(I), r_R(I) \lhd R$, więc $a_R(I) \lhd R$. W szczególności $a(R) = a_R(R) \lhd R$ oraz $a(R)R = Ra(R) = \{0\}$, a więc $a(R)^2 = \{0\}$. Ponadto wynika stąd, że $a(R) \subseteq Z(R)$, gdzie $Z(R)$ oznacza centrum pierścienia R.

W pierścieniu macierzy $M_n(R)$ dla podpierścienia $S \subseteq R$ przez SI_n będziemy oznaczali zbiór wszystkich macierzy, które na głównej przekątnej mają ten sam element $s \in S$, zaś na pozostałych miejscach same zera.

Twierdzenie 8.2. *Dla dowolnego pierścienia R i dla dowolnej liczby naturalnej $n \geqslant 2$ mamy, że*

$$Z(M_n(R)) = Z(R)I_n + M_n(a(R)).$$

Dowód. Niech $A \in Z(R)I_n + M_n(a(R))$. Wtedy $A = cI_n + B$ dla pewnego $c \in Z(R)$ oraz dla pewnej macierzy $B \in M_n(a(R))$. Weźmy dowolne $M \in M_n(R)$. Wtedy dla $i, j = 1, 2, \ldots, n$ mamy, że $[B \cdot M]_{ij} = \sum_{t=1}^{n} [B]_{it}[M]_{tj} = 0$, gdyż $[B]_{it}[M]_{tj} = 0$, więc $B \cdot M = 0_n$. Podobnie $M \cdot B = 0_n$, skąd $B \cdot M = M \cdot B$ i $B \in Z(M_n(R))$. Dalej, dla dowolnych $i, j = 1, 2, \ldots, n$ mamy, że $[(cI_n) \cdot M]_{ij} = \sum_{t=1}^{n} [cI_n]_{it}[M]_{tj} = c[M]_{ij}$, gdyż dla $t \neq i$ jest $[cI_n]_{it} = 0$ oraz $[cI_n]_{ii} = c$. Podobnie, $[M \cdot (cI_n)]_{ij} = [M]_{ij}c$. Ale $c \in Z(R)$, więc $[(cI_n) \cdot M]_{ij} = [M \cdot (cI_n)]_{ij}$ dla wszystkich $i, j = 1, 2, \ldots, n$. Zatem $cI_n \in Z(M_n(R))$. Ale $A = (cI_n) + B$, więc też $A \in Z(M_n(R))$.

Na odwrót. Załóżmy, że $A \in Z(M_n(R))$. Weźmy dowolne $x \in R$ oraz dowolne $i, j \in \{1, 2, \ldots, n\}$. Wtedy $(xE_{ij}) \cdot A = A \cdot (xE_{ij})$, skąd $\sum_{t=1}^{n} (x[A]_{jt})E_{it} = \sum_{s=1}^{n} ([A]_{si}x)E_{sj}$, więc $x[A]_{jt} = 0$ dla $t \neq j$, $[A]_{si}x = 0$ dla $s \neq i$, $x[A]_{jj} = [A]_{ii}x$. Wynika stąd, że $[A]_{st} \in a(R)$ dla wszystkich $t \neq s$, $[A]_{tt} \in Z(R)$ dla $t = 1, 2, \ldots, n$ oraz $[A]_{ii} - [A]_{11} \in a(R)$ dla $i = 2, 3, \ldots, n$. Zatem istnieją $a_i \in a(R)$ takie, że $[A]_{ii} = [A]_{11} + a_i$ dla $i = 2, 3, \ldots, n$. Oznaczmy $c = [A]_{11}$. Wtedy uzyskamy, że

$$A = cI_n + \begin{bmatrix} 0 & a_{12} & a_{13} & \ldots & a_{1n} \\ a_{21} & a_2 & a_{23} & \ldots & a_{2n} \\ a_{31} & a_{32} & a_3 & \ldots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \ldots & a_n \end{bmatrix},$$

skąd $A \in Z(R)I_n + M_n(a(R))$. □

Wniosek 8.3. *Jeżeli R jest pierścieniem takim, że $a(R) = \{0\}$, to dla dowolnego $n \geqslant 2$: $Z(M_n(R)) = Z(R)I_n$.*

Wniosek 8.4. *Jeżeli R jest pierścieniem takim, że $a \in RaR$ dla każdego $a \in R$, to dla dowolnego $n \geqslant 2$: $Z(M_n(R)) = Z(R)I_n$. W szczególności, jeśli R jest pierścieniem regularnym w sensie von Neumanna lub R jest idempotentnym pierścieniem prostym lub R posiada jedynkę, to dla dowolnego $n \geqslant 2$: $Z(M_n(R)) = Z(R)I_n$.*

Wniosek 8.5. *Jeżeli R jest przemiennym pierścieniem z jedynką, to dla dowolnego $n \geqslant 2$: $Z(M_n(R)) = RI_n$.*

Zadanie (1)**.** Niech I będzie ideałem pierścienia R i niech $n \geqslant 2$. Udowodnić, że

(a) $l_{M_n(R)}(M_n(I)) = M_n(l_R(I))$,
(b) $r_{M_n(R)}(M_n(I)) = M_n(r_R(I))$,
(c) $a_{M_n(R)}(M_n(I)) = M_n(a_R(I))$.

8.2 Ideały istotne

Definicja 8.6. Niech I będzie ideałem pierścienia R. Mówimy, że I jest *istotny* w R, jeżeli $I \cap J \neq 0$ dla dowolnego niezerowego $J \lhd R$.

Stwierdzenie 8.7. *Dla ideału I pierścienia R takiego, że $a_I(I) = \{0\}$ równoważne są warunki:*

(i) I jest istotny w R,
(ii) $a_R(I) = \{0\}$.

DOWÓD. Załóżmy, że I jest istotny w R i niech $J = a_R(I)$. Wtedy $J \lhd R$. Jeśli $J \neq \{0\}$, to $I \cap J \neq \{0\}$. Ale $I \cap J \subseteq a_I(I)$, więc $a_I(I) \neq \{0\}$ i mamy sprzeczność. Zatem $a_R(I) = \{0\}$.

Na odwrót, załóżmy, że $a_R(I) = \{0\}$. Niech J będzie dowolnym niezerowym ideałem pierścienia R. Zauważmy, że $IJ \subseteq I \cap J$ oraz $JI \subseteq I \cap J$. Ale $a_R(I) = \{0\}$, więc $IJ \neq \{0\}$ lub $JI \neq \{0\}$, skąd $I \cap J \neq \{0\}$. Zatem I jest istotny w R. □

Twierdzenie 8.8. *Dla dowolnego pierścienia R bez jedynki istnieje pierścień $R^\dagger$ posiadający jedynkę 1 i taki, że R jest istotnym ideałem pierścienia $R^\dagger$ oraz $R + \langle 1\rangle = R^\dagger$.*

DOWÓD. Z twierdzenia 7.1 istnieje pierścień R^1 z jedynką 1 i taki, że $R \lhd R^1$ oraz $R + \langle 1\rangle = R^1$. Oznaczmy przez $\mathcal{S}$ rodzinę wszystkich ideałów I pierścienia R^1 takich, że $I \cap R = \{0\}$. Rodzina $\mathcal{S}$ jest niepusta, bo np. $\{0\} \in \mathcal{S}$. Ponadto rodzina $\mathcal{S}$ jest częściowo uporządkowana przez inkluzję. Niech $\mathcal{A}$ będzie łańcuchem w $\mathcal{S}$. Wtedy ze stwierdzenia 4.17, $J = \bigcup_{A\in\mathcal{A}} A \lhd R^1$ oraz $A \subseteq J$ dla każdego $A \in \mathcal{A}$. Jeśli $J \cap R \neq \{0\}$, to istnieje $0 \neq a \in R$ takie, że $a \in J$. Oznacza to, że $a \in A$ dla pewnego $A \in \mathcal{A}$, czyli $A \cap R \neq \{0\}$ wbrew założeniu. Zatem $J \cap R = \{0\}$ i wobec tego $J \in \mathcal{S}$ oraz J jest ograniczeniem górnym łańcucha $\mathcal{A}$. Zatem z lematu Zorna istnieje w rodzinie $\mathcal{S}$ element maksymalny M. Stąd w szczególności $M \lhd R^1$ oraz $M \cap R = \{0\}$. Z drugiego twierdzenia o izomorfizmie $(R + M)/M \cong R/(R \cap M) = R/\{0\}$, skąd $R \cong (R + M)/M$. Ponadto $(R + M)/M \lhd R^1/M$, więc pierścień R możemy utożsamiać z ideałem $(R + M)/M$ pierścienia R^1/M. Ponieważ $R^1 = R + \langle 1\rangle$, więc $R^1/M = (R+M)/R+\langle 1+M\rangle$. Weźmy dowolny niezerowy ideał K pierścienia R^1/M. Wtedy ze stwierdzenia 5.8 istnieje $J \lhd R^1$ taki, że $M \subset J$ oraz $K = J/M$. Stąd z maksymalności M w rodzinie $\mathcal{S}$ wynika, że $J \notin \mathcal{S}$, czyli $J \cap R \neq \{0\}$. Gdyby $J \cap R \subseteq M$, to $J \cap R = (J \cap R) \cap M = J \cap (R \cap M) = J \cap \{0\} = \{0\}$ i otrzymalibyśmy sprzeczność. Zatem $J \cap R \not\subseteq M$, skąd $[(J \cap R) + M]/M \neq \{0 + M\}$ oraz $[(J \cap R) + M]/M \subseteq (R + M)/M \cap J/M = [(R + M)/M] \cap K$. Zatem $(R + M)/M$ jest ideałem istotnym w pierścieniu R^1/M. Wystarczy zatem przyjąć $R^\dagger = R^1/M$. □

Zadanie (2)**.** Niech R będzie pierścieniem takim, że $a(R) = \{0\}$. Udowodnij, że wówczas przy oznaczeniach dowodu twierdzenia 8.8, $M = a_{R^1}(R)$, czyli w tym przypadku $R^\dagger = R^1/a_{R^1}(R)$.

Twierdzenie 8.9. *Niech I będzie ideałem istotnym pierścienia R. Wówczas:*
(i) jeżeli pierścień I jest pierwszy, to pierścień R jest pierwszy,
(ii) jeżeli pierścień I jest półpierwszy, to pierścień R jest półpierwszy,
(iii) jeżeli pierścień I jest zredukowany, to pierścień R jest zredukowany,
(iv) jeżeli pierścień I jest dziedziną, to pierścień R jest dziedziną.

DOWÓD. (i). Ponieważ $I \neq \{0\}$, więc też $R \neq \{0\}$. Weźmy dowolne ideały A i B pierścienia R takie, że $AB = \{0\}$ i załóżmy, że $A \neq \{0\}$ i $B \neq \{0\}$.

Wówczas $A \cap I \neq \{0\}$ i $B \cap I \neq \{0\}$. Ponadto $A \cap I, B \cap I \lhd I$, więc z pierwszości pierścienia I, $(A \cap I)(B \cap I) \neq \{0\}$. Ale $(A \cap I)(B \cap I) \subseteq AB = \{0\}$, więc mamy sprzeczność. Zatem $A = \{0\}$ lub $B = \{0\}$ i pierścień R jest pierwszy.

(ii). Ponieważ $I \neq \{0\}$, więc też $R \neq \{0\}$. Weźmy dowolny ideał A pierścienia R taki, że $A^2 = \{0\}$ i załóżmy, że $A \neq \{0\}$. Wówczas $A \cap I \neq \{0\}$. Ponadto $A \cap I \lhd I$, więc z półpierwszości pierścienia I, $(A \cap I)^2 \neq \{0\}$. Ale $(A \cap I)^2 \subseteq A^2 = \{0\}$, więc mamy sprzeczność. Zatem $A = \{0\}$ i pierścień R jest półpierwszy.

(iii). Weźmy dowolne $a \in R$ takie, że $a^2 = 0$. Wtedy $aIa \subseteq I$ oraz $(aIa)^2 = \{0\}$. Ale pierscień I jest zredukowany, więc $aIa = \{0\}$. Stąd $(aI)^2 = (Ia)^2 = \{0\}$, a ponieważ $aI, Ia \subseteq I$, więc $aI = Ia = \{0\}$. Zatem $a \in a_R(I)$. Ponadto $a_I(I) = \{0\}$, gdyż pierścień I jest zredukowany, więc na mocy stwierdzenia 8.7, $a_R(I) = \{0\}$. Stąd $a = 0$ i pierścień R jest zredukowany.

(iv). Z (iii) wynika, że pierścień R jest zredukowany. Ponadto ze stwierdzenia 8.7, $a_R(I) = \{0\}$. Weźmy dowolne $a, b \in R$ takie, że $ab = 0$. Wtedy $Ia, bI \subseteq I$ oraz $(Ia)(bI) = \{0\}$, skąd $Ia = \{0\}$ lub $bI = \{0\}$. Jeśli $Ia = \{0\}$, to $aI \subseteq I$ oraz $(aI)^2 = \{0\}$, więc $aI = \{0\}$. Zatem $a \in a_R(I) = \{0\}$, czyli $a = 0$. Analogicznie pokazujemy, że jeśli $bI = \{0\}$, to $b = 0$. Zatem R jest dziedziną. □

Z twierdzeń 8.8 i 8.9 wynika od razu następujące

Twierdzenie 8.10. *Niech R będzie pierścieniem bez jedynki i niech $R^\dagger$ będzie pierścieniem z jedynką podanym w twierdzeniu 8.8. Wówczas R jest ideałem istotnym pierścienia $R^\dagger$, $R + \langle 1 \rangle = R^\dagger$ oraz*

(i) jeżeli R jest pierwszy, to $R^\dagger$ jest pierwszy,

(ii) jeżeli R jest półpierwszy, to $R^\dagger$ jest półpierwszy,

(iii) jeżeli R jest zredukowany, to $R^\dagger$ jest zredukowany,

(iv) jeżeli R jest dziedziną, to $R^\dagger$ jest dziedziną,

(v) jeżeli R jest przemienny, to $R^\dagger$ jest przemienny.

8.3 Pierścienie macierzy pierwsze i półpierwsze

Stwierdzenie 8.11. *Dla dowolnych ideałów I i J pierścienia R i dla dowolnego naturalnego n: $M_n(I) \cdot M_n(J) = M_n(IJ)$.*

DOWÓD. Weźmy dowolne $X \in M_n(I) \cdot M_n(J)$. Wtedy X jest skończoną sumą elementów postaci $A \cdot B$ dla $A \in M_n(I)$ oraz $B \in M_n(J)$. Ponieważ $IJ \lhd R$, więc $M_n(IJ) \lhd M_n(R)$. Wystarczy zatem wykazać, że $A \cdot B \in M_n(IJ)$. Ale dla dowolnych $i, j = 1, \ldots, n$, $[A \cdot B]_{ij} = \sum_{t=1}^{n} [A]_{it} \cdot [B]_{tj}$ oraz $[A]_{it} \in I$, $[B]_{tj} \in J$, więc $[A]_{it} \cdot [B]_{tj} \in IJ$, skąd $[A \cdot B]_{ij} \in IJ$. Zatem $A \cdot B \in M_n(IJ)$.

Na odwrót, weźmy dowolne $X \in M_n(IJ)$. Wówczas $[X]_{ij} \in IJ$ dla wszystkich $i, j = 1, \ldots, n$. Ponadto $X = \sum_{i,j=1,\ldots,n} [X]_{ij} E_{ij}$ oraz $M_n(I) \cdot M_n(J) \lhd M_n(R)$, więc wystarczy wykazać, że $aE_{ij} \in M_n(I) \cdot M_n(J)$ dla dowolnego $a \in IJ$ oraz dla dowolnych $i, j = 1, \ldots, n$. Ale a jest skończoną sumą elementów postaci xy dla $x \in I$, $y \in J$, więc bez zmniejszania ogólności możemy zakładać, że $a = xy$. Wtedy $aE_{ij} = (xy)E_{ij} = (xE_{ij}) \cdot (yE_{jj}) \in M_n(I) \cdot M_n(J)$. Stąd $X \in M_n(I) \cdot M_n(J)$. □

Twierdzenie 8.12. *Jeżeli R jest pierścieniem pierwszym, to dla dowolnego naturalnego n pierścień macierzy $M_n(R)$ też jest pierwszy.*

DOWÓD. Ponieważ $R \neq \{0\}$, więc $M_n(R) \neq \{0\}$. Z twierdzenia 8.10 istnieje pierścień pierwszy S z jedynką taki, że $R \lhd S$. Weźmy dowolne ideały A i B pierścienia $M_n(S)$ takie, że $AB = \{0\}$. Z twierdzenia 7.5 istnieją ideały I, J pierścienia S takie, że $A = M_n(I)$ oraz $B = M_n(J)$. Ponadto ze stwierdzenia 8.11 $A \cdot B = M_n(IJ)$. Stąd $IJ = \{0\}$, więc z pierwszości pierścienia S, $I = \{0\}$ lub $J = \{0\}$, czyli $A = \{0\}$ lub $B = \{0\}$. Zatem $M_n(S)$ jest pierścieniem pierwszym. Ale $M_n(R)$ jest niezerowym ideałem pierścienia $M_n(S)$. Zatem z twierdzenia 5.19 pierścień $M_n(R)$ jest pierwszy. □

Twierdzenie 8.13. *Jeżeli R jest pierścieniem półpierwszym, to dla dowolnego naturalnego n pierścień macierzy $M_n(R)$ też jest półpierwszy.*

DOWÓD. Ponieważ $R \neq \{0\}$, więc $M_n(R) \neq \{0\}$. Z twierdzenia 8.10 istnieje pierścień półpierwszy S z jedynką taki, że $R \lhd S$. Weźmy dowolny ideał A pierścienia $M_n(S)$ tak, że $A^2 = \{0\}$. Z twierdzenia 7.5 istnieje ideał I pierścienia S taki, że $A = M_n(I)$. Ponadto ze stwierdzenia 8.11 $A^2 = M_n(I^2)$. Stąd $I^2 = \{0\}$, więc z półpierwszości pierścienia S, $I = \{0\}$, czyli $A = \{0\}$. Zatem $M_n(S)$ jest pierścieniem półpierwszym. Ale $M_n(R)$ jest niezerowym ideałem pierścienia $M_n(S)$. Zatem z twierdzenia 5.20 pierścień $M_n(R)$ jest półpierwszy. □

Stwierdzenie 8.14. *Jeżeli dla pewnego naturalnego n pierścień $M_n(R)$ jest pierwszy, to pierścień R też jest pierwszy.*

DOWÓD. Ponieważ $M_n(R) \neq \{0\}$, więc $R \neq \{0\}$. Weźmy dowolne $I, J \lhd R$ takie, że $IJ = \{0\}$. Wtedy $M_n(I), M_n(J) \lhd M_n(R)$ oraz na mocy stwierdzenia 8.11, $M_n(I) \cdot M_n(J) = M_n(IJ) = \{0\}$. Zatem z pierwszości pierścienia $M_n(R)$, $M_n(I) = \{0\}$ lub $M_n(J) = \{0\}$, czyli $I = \{0\}$ lub $J = \{0\}$. Stąd pierścień R jest pierwszy. □

Stwierdzenie 8.15. *Jeżeli dla pewnego naturalnego n pierścień $M_n(R)$ jest półpierwszy, to pierścień R też jest półpierwszy.*

DOWÓD. Ponieważ $M_n(R) \neq \{0\}$, więc $R \neq \{0\}$. Weźmy dowolne $I \lhd R$ takie, że $I^2 = \{0\}$. Wtedy $M_n(I) \lhd M_n(R)$ oraz na mocy stwierdzenia 8.11, $M_n(I)^2 = M_n(I^2) = \{0\}$. Zatem z półpierwszości pierścienia $M_n(R)$, $M_n(I) = \{0\}$, czyli $I = \{0\}$. Stąd pierścień R jest półpierwszy. □

Zadanie (3)**.** Wyznaczyć wszystkie ideały maksymalne i wszystkie ideały pierwsze pierścienia $M_n(\mathbb{Z})$.

Zadanie (4)**.** Niech R będzie pierścieniem takim, że $a \in RaR$ dla każdego $a \in R$. Udowodnić, że każdy ideał maksymalny pierścienia $M_n(R)$ jest postaci $M_n(I)$ dla pewnego ideału maksymalnego I pierścienia R.

Zadanie (5)**.** Niech R będzie pierścieniem takim, że $a \in RaR$ dla każdego $a \in R$. Udowodnić, że każdy ideał pierwszy pierścienia $M_n(R)$ jest postaci $M_n(I)$ dla pewnego ideału pierwszego I pierścienia R.

Zadanie (6)**.** Udowodnij, że część wspólna skończonej liczby ideałów istotnych pierścienia R jest ideałem istotnym tego pierścienia.

Zadanie (7)**.** Niech I będzie ideałem istotnym pierścienia R. Czy jest prawdą, że dla każdego naturalnego n ideał $M_n(I)$ jest istotny w pierścieniu $M_n(R)$?

Zadanie (8)**.** Udowodnij, że pierścień R jest pierwszy wtedy i tylko wtedy, gdy pierścień $R[x]$ jest pierwszy.

Zadanie (9)**.** Udowodnij, że pierścień R jest półpierwszy wtedy i tylko wtedy, gdy pierścień $R[x]$ jest półpierwszy.

8.4 Macierze odwracalne

Twierdzenie 8.16. *Niech R będzie pierścieniem z jedynką. Niech $a \in R$ będzie elementem nilpotentnym. Wówczas element $1+a$ jest odwracalny w pierścieniu R. Więcej, jeżeli $a^n = 0$, to zachodzi wzór*

$$(1+a)^{-1} = 1 - a + a^2 - a^3 + \ldots + (-a)^{n-1}. \tag{8.2}$$

DOWÓD. Niech $b = -a$. Wtedy $b^n = 0$, skąd z tożsamości $1-b^n = (1-b)\cdot(1+b+b^2+\ldots+b^{n-1}) = (1+b+b^2+\ldots+b^{n-1})\cdot(1-b)$ mamy, że $1 = (1+a)\cdot(1-a+a^2-\ldots+(-a)^{n-1}) = (1-a+a^2-\ldots+(-a)^{n-1})\cdot(1+a)$, skąd mamy wzór (8.2). □

Definicja 8.17. Niech R będzie dowolnym pierścieniem i niech n, k będą liczbami naturalnymi takimi, że $n \geqslant 2$ oraz $k \leqslant n-1$. W pierścieniu $T_n(R)$ macierzy trójkątnych górnych oznaczmy przez $T_n^k(R)$ podzbiór wszystkich macierzy, które mają same zera na k kolejnych przekątnych nad główną przekątną poczynając od głównej przekątnej tzn.

$$T_n^k(R) = \{A \in M_n(R) : [A]_{ij} = 0 \text{ dla wszystkich } i, j \text{ takich, że } j \leqslant i+k-1\}. \tag{8.3}$$

Twierdzenie 8.18. *Dla dowolnego pierścienia R i dla dowolnych liczb naturalnych $n \geqslant 2$ i $k \leqslant n-1$ mamy, że*

$$T_n^k(R) \lhd T_n(R). \tag{8.4}$$

W szczególności $T_n^k(R)$ jest podpierścieniem pierścienia $T_n(R)$.

DOWÓD. Z określenia $T_n^k(R)$ wynika od razu, że $T_n^k(R)$ jest podgrupą grupy addytywnej pierścienia $T_n(R)$. Weźmy dowolne $A \in T_n^k(R)$ oraz dowolne $B \in T_n(R)$. Wtedy $A = \sum_{j>i+k-1} [A]_{ij}E_{ij}$ oraz $B = \sum_{t\geqslant s} [B]_{st}E_{st}$. Zatem $A \cdot B = \sum_{j>i+k-1,\, t\geqslant s} ([A]_{ij} \cdot [B]_{st})(E_{ij} \cdot E_{st})$. Ponadto $E_{ij} \cdot E_{st} = 0_n$, jeśli $j \neq s$ oraz $E_{ij} \cdot E_{st} = E_{it}$, jeśli $j = s$, więc wtedy $t \geqslant s = j > i+k-1$, czyli $t > i+k-1$, skąd wynika, że $A \cdot B \in T_n^k(R)$. Ponadto $B \cdot A = \sum_{j>i+k-1,\, t\geqslant s} ([B]_{st} \cdot [A]_{ij})(E_{st} \cdot E_{ij})$ oraz $E_{st} \cdot E_{ij} = 0_n$, jeśli $t \neq i$ oraz $E_{st} \cdot E_{ij} = E_{sj}$, jeśli $t = i$ i wtedy $j > i+k-1 = t+k-1 \geqslant s+k-1$, więc $j > s+k-1$, skąd $B \cdot A \in T_n^k(R)$. Zatem $T_n^k(R) \lhd T_n(R)$. □

Twierdzenie 8.19. *Dla dowolnego pierścienia R i dla dowolnej liczby naturalnej $n \geqslant 2$:*

$$(T_n^1(R))^n = \{0_n\}.$$

DOWÓD. Wystarczy wykazać, że dla dowolnych $A_1, A_2, \ldots, A_n \in T_n^1(R)$ mamy, że $A_1 \cdot A_2 \cdot \ldots \cdot A_n = \{0_n\}$. Ale $A_1 \cdot A_2 \cdot \ldots \cdot A_n$ jest sumą wszystkich możliwych składników postaci

$$[A_1]_{i_1j_1}[A_2]_{i_2j_2} \ldots [A_n]_{i_nj_n} E_{i_1j_1} \cdot E_{i_2j_2} \cdot \ldots \cdot E_{i_nj_n}, \tag{8.5}$$

gdzie $i_k < j_k$ dla $k = 1, 2, \ldots, n$, więc iloczyn (8.5) może być niezerowy jedynie wówczas, gdy $j_k = i_{k+1}$ dla każdego $k = 1, 2, \ldots, n-1$. Stąd $j_1 \geqslant i_1 + 1$, $j_2 \geqslant i_2 + 1 = j_1 + 1 \geqslant i_1 + 2$, itd. w końcu $j_n \geqslant i_1 + n$, co prowadzi do sprzeczności. Zatem iloczyn (8.5) jest zawsze równy 0_n, czyli $A_1 \cdot A_2 \cdot \ldots \cdot A_n = \{0_n\}$. □

Twierdzenie 8.20. *Niech R będzie pierścieniem z jedynką i niech $n \geqslant 2$ będzie liczbą naturalną. Wówczas dla dowolnej liczby naturalnej $k \leqslant n-1$ zbiór $UT_n^k(R) = I_n + T_n^k(R)$ jest podgrupą normalną grupy elementów odwracalnych pierścienia $T_n(R)$.*

DOWÓD. Oczywiście $I_n \in UT_n^k(R)$. Weźmy dowolne $A \in UT_n^k(R)$. Wtedy istnieje $B \in T_n^k(R)$ takie, że $A = I_n + B$. Ponadto z twierdzenia 8.19, $B^n = 0_n$, więc na mocy twierdzenia 8.16, $A^{-1} = I_n - B + B^2 - \ldots + (-B)^{n-1}$. Ale z twierdzenia 8.18, $-B+B^2-\ldots+(-B)^{n-1} \in T_n^k(R)$, więc $A^{-1} \in UT_n^k(R)$. Niech teraz $X, Y \in UT_n^k(R)$. Wówczas istnieją $B, C \in T_n^k(R)$ takie, że $X = I_n + B$ oraz $Y = I_n + C$, skąd $X \cdot Y = I_n + B + C + B \cdot C$. Ale na mocy twierdzenia

8.18, $B + C + B \cdot C \in T_n^k(R)$, więc $X \cdot Y \in UT_n^k(R)$. Zatem $UT_n^k(R)$ jest podgrupą grupy elementów odwracalnych pierścienia $T_n(R)$.

Weźmy teraz dowolne $X \in UT_n^k(R)$ i dowolne $Y \in (T_n(R))^\star$. Wówczas istnieje $A \in T_n^k(R)$ takie, że $X = I_n + A$. Zatem na mocy twierdzenia 8.18, $Y \cdot X \cdot Y^{-1} = Y \cdot (I_n + A) \cdot Y^{-1} = Y \cdot I_n \cdot Y^{-1} + Y \cdot A \cdot Y^{-1} = I_n + Y \cdot A \cdot Y^{-1} \in UT_n^k(R)$ na mocy twierdzenia 8.18. Zatem $UT_n^k(R)$ jest podgrupą normalną grupy elementów odwracalnych pierścienia $T_n(R)$. □

Twierdzenie 8.21. *Niech R będzie pierścieniem z jedynką i niech $n \geqslant 2$ będzie liczbą naturalną. Wówczas*

$$(T_n(R))^\star = \{A \in T_n(R) : [A]_{ii} \in R^\star \text{ dla } i = 1, 2, \ldots, n\}. \tag{8.6}$$

Dowód. Oznaczmy przez $D(a_1, a_2, \ldots, a_n) = a_1E_{11} + a_2E_{22} + \ldots + a_nE_{nn}$ dla dowolnych $a_1, a_2, \ldots, a_n \in R$. Wtedy $D(a_1, a_2, \ldots, a_n) \cdot D(b_1, b_2, \ldots, b_n) = D(a_1b_1, a_2b_2, \ldots, a_nb_n)$ dla dowolnych $a_1, b_1, \ldots, a_n, b_n \in R$. Wynika stąd, że dla dowolnych $a_1, a_2, \ldots, a_n \in R^\star$ mamy, że $D(a_1, a_2, \ldots, a_n)$ jest elementem odwracalnym pierścienia $T_n(R)$. Niech teraz $A \in T_n(R)$ będzie takie, że $[A]_{ii} = a_i \in R^\star$. Wtedy $A = D(a_1, a_2, \ldots, a_n) \cdot (I_n + B)$ dla pewnego $B \in T_n^1(R)$. Zatem z twierdzenia 8.20 mamy, że $A \in (T_n(R))^\star$. Na odwrót, weźmy dowolne $A \in (T_n(R))^\star$. Wtedy istnieje $B \in T_n(R)$ takie, że $A \cdot B = B \cdot A = I_n$, skąd $[A]_{ii}[B]_{ii} = [B]_{ii}[A]_{ii} = 1$, czyli $[A]_{ii} \in R^\star$ dla $i = 1, 2, \ldots, n$. □

Zadanie (10)**.** Niech R będzie pierścieniem z jedynką i niech $n \geqslant 2$ będzie liczbą naturalną. Wyznaczyć

a) centrum pierścienia $T_n^1(R)$,

b) centrum grupy $UT_n^1(R)$.

Zadanie (11)**.** Niech K będzie ciałem skończonym. Obliczyć rząd grupy $GL_n(K)$ elementów odwracalnych pierścienia $M_n(K)$.

Zadanie (12)**.** Niech p będzie liczbą pierwszą. Wykazać, że $UT_n^1(\mathbb{Z}_p)$ jest p-podgrupą Sylowa grupy $GL_n(\mathbb{Z}_p)$.

Zadanie (13)**.** Niech p będzie liczbą pierwszą. Wykazać, że dla liczb naturalnych $n \leqslant p$ i dla każdego $A \in UT_n^1(\mathbb{Z}_p)$ jest $A^p = I_n$.

Wykład 9

Wewnętrzne sumy proste

9.1 Wewnętrzne sumy proste podgrup

Definicja 9.1. Niech $\{A_t\}_{t\in T}$ będzie rodziną podgrup grupy abelowej $(A, +, 0)$. Najmniejszą w sensie inkluzji podgrupę grupy A zawierającą podzbiór $\bigcup_{t\in T} A_t$ nazywamy *sumą algebraiczną podgrup* rodziny $\{A_t\}_{t\in T}$ i oznaczamy symbolem $\sum_{t\in T} A_t$.

Stwierdzenie 9.2. *Dla dowolnej rodziny $\{A_t\}_{t\in T}$ podgrup grupy abelowej A podgrupa $\sum_{t\in T} A_t$ składa się ze wszystkich możliwych sum postaci $a_1 + \ldots + a_n$, gdzie $a_i \in A_{t_i}$ dla $i = 1, \ldots, n$ oraz $t_1, \ldots, t_n$ są parami różnymi elementami ze zbioru T. W szczególności, jeśli $T = \{1, \ldots, m\}$ dla pewnego $m \in \mathbb{N}$, to $\sum_{t\in T} A_t = A_1 + \ldots + A_m$.*

Dowód. Oznaczmy przez B podzbiór wszystkich możliwych sum postaci $a_1 + \ldots + a_n$, gdzie $a_i \in A_{t_i}$ dla $i = 1, \ldots, n$ oraz $t_1, \ldots, t_n$ są parami różnymi elementami ze zbioru T. Z określenia podgrupy $\sum_{t\in T} A_t$ mamy od razu, że $B \subseteq \sum_{t\in T} A_t$. Ponadto $A_t \subseteq B$ dla dowolnego $t \in T$. Weźmy dowolne $a, b \in B$. Wtedy istnieją skończone podzbiory $T_1 = \{t_1, \ldots, t_p\}$ i $T_2 = \{s_1, \ldots, s_q\}$ zbioru T takie, że $a \in A_{t_1} + \ldots + A_{t_p}$ i $b \in A_{s_1} + \ldots + A_{s_q}$. Niech $T_0 = T_1 \cup T_2$. Wtedy T_0 jest skończonym podzbiorem T oraz $T_0 = \{r_1, \ldots, r_m\}$ dla pewnych parami różnych elementów $r_1, \ldots, r_m \in T$. Stąd $a, b \in A_{r_1} + \ldots + A_{r_m}$, więc $a - b \in A_{r_1} + \ldots + A_{r_m}$. Ale $A_{r_1} + \ldots + A_{r_m} \subseteq B$, więc $a - b \in B$. Zatem B jest podgrupą grupy A zawierającą podzbiór $\bigcup_{t\in T} A_t$. Ale $\sum_{t\in T} A_t$ jest najmniejszą podgrupą grupy A zawierającą $\bigcup_{t\in T} A_t$, więc $\sum_{t\in T} A_t \subseteq B$ i ostatecznie $\sum_{t\in T} A_t = B$. Kończy to dowód naszego stwierdzenia. □

Zadanie (1)**.** Niech A i B będą podgrupami grupy addytywnej pierścienia R.

Udowodnij, że wtedy $A \cdot B = \sum_{a \in A} aB = \sum_{b \in B} Ab$.

Stwierdzenie 9.3. *Niech T będzie zbiorem o co najmniej dwóch elementach i niech $\{A_t\}_{t \in T}$ będzie rodziną podgrup grupy abelowej $(A, +, 0)$. Wówczas następujące warunki są równoważne:*

(i) $A_s \cap \sum_{t \in T \setminus \{s\}} A_t = \{0\}$ dla dowolnego $s \in T$;

(ii) dla dowolnego niezerowego $a \in \sum_{t \in T} A_t$ istnieje dokładnie jeden skończony podzbiór $T_0 = \{t_1, \ldots, t_n\}$ zbioru T i dokładnie jeden zbiór $\{a_1, \ldots, a_n\}$ niezerowych elementów taki, że $a_i \in A_{t_i}$ dla $i = 1, \ldots, n$ oraz $a = a_1 + \ldots + a_n$;

(iii) dla dowolnego skończonego podzbioru n-elementowego $T_0 = \{t_1, \ldots, t_n\}$ zbioru T i dla dowolnych $a_i \in A_{t_i}$, $i = 1, \ldots, n$ z tego, że $a_1 + \ldots + a_n = 0$ wynika $a_1 = \ldots = a_n = 0$.

DOWÓD. $(i) \Rightarrow (ii)$. Istnienie wynika ze stwierdzenia 9.2. Dla udowodnienia jednoznaczności weźmy skończone podzbiory $T_1 = \{t_1, \ldots, t_n\}$ i $T_2 = \{s_1, \ldots, s_m\}$ zbioru T oraz niezerowe elementy $a_i \in A_{t_i}$ dla $i = 1, \ldots, n$ i $b_j \in A_{s_j}$ dla $j = 1, \ldots, m$ takie, że $a_1 + \ldots + a_n = b_1 + \ldots + b_m$. Załóżmy, że $T_1 \not\subseteq T_2$. Bez zmniejszania ogólności rozważań możemy zakładać, że wtedy $t_1 \notin T_2$. Stąd $t_1 \notin \{t_2, \ldots, t_n, s_1, \ldots, s_m\}$, więc na mocy założenia oraz stwierdzenia 9.2, $a_1 \notin A_{t_2} + \ldots + A_{t_n} + A_{s_1} + \ldots + A_{s_m}$. Ale $a_1 = (-a_2) + \ldots + (-a_n) + b_1 + \ldots + b_m \in A_{t_2} + \ldots + A_{t_n} + A_{s_1} + \ldots + A_{s_m}$, więc mamy sprzeczność. Zatem $T_1 \subseteq T_2$. Analogicznie pokazuje się, że $T_2 \subseteq T_1$. Stąd $T_1 = T_2$. Ze względu na przemienność i łączność dodawania w grupie A możemy zakładać, że $t_i = s_i$ dla $i = 1, \ldots, n$. Wtedy dla każdego $i = 1, \ldots, n$: $a_i - b_i \in A_{t_i}$ oraz $a_i - b_i = (b_1 - a_1) + \ldots + (b_{i-1} - a_{i-1}) + (b_{i+1} - a_{i+1}) + \ldots + (b_n - a_n)$, czyli $a_i - b_i \in A_{t_1} + \ldots + A_{t_{i-1}} + A_{t_{i+1}} + \ldots + A_{t_n}$. Z założenia i stwierdzenia 9.2 wynika więc, że $a_i - b_i = 0$, czyli $a_i = b_i$ dla wszystkich $i = 1, \ldots, n$.

$(ii) \Rightarrow (iii)$. Załóżmy, że $a_i \neq 0$ dla pewnego $i = 1, \ldots, n$. Wtedy $n > 1$ oraz istnieje $j \neq i$, $j = 1, \ldots, n$ takie, że $a_j \neq 0$. Ponadto $a_i = (-a_1) + \ldots + (-a_{i-1}) + (-a_{i+1}) + \ldots + (-a_n)$. Wykreślając spośród $-a_1, \ldots, -a_{i-1}, -a_{i+1}, \ldots, -a_n$ wszystkie elementy równe 0 uzyskamy zatem, że istnieje niepusty podzbiór $\{s_1, \ldots, s_m\}$ zbioru $\{t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n\}$ oraz istnieją niezerowe elementy $b_i \in A_{s_i}$ dla $i = 1, \ldots, m$ takie, że $a_i = b_1 + \ldots + b_m$. Ale zbiory $\{t_i\}$ i $\{s_1, \ldots, s_m\}$ są rozłączne, więc mamy sprzeczność z założeniem. Oznacza to, że $a_i = 0$ dla wszystkich $i = 1, \ldots, n$.

$(iii) \Rightarrow (i)$. Niech $a \in A_s \cap \sum_{t \in T \setminus \{s\}} A_t$. Wtedy ze stwierdzenia 9.2 istnieje skończony podzbiór n-elementowy $\{t_1, \ldots, t_n\}$ zbioru $T \setminus \{s\}$ oraz istnieją elementy $a_i \in A_{t_i}$ dla $i = 1, \ldots, n$ takie, że $a = a_1 + \ldots + a_n$. Zatem $(-a) + a_1 + \ldots + a_n = 0$. Ale elementy $s, t_1, \ldots, t_n$ są parami różne, więc na mocy założenia $0 = -a = a_1 = \ldots = a_n$. Stąd $A_s \cap \sum_{t \in T \setminus \{s\}} A_t = \{0\}$ dla dowolnego $s \in T$. □

Definicja 9.4. Mówimy, że podgrupa B grupy abelowej $(A,+,0)$ jest *wewnętrzną sumą prostą* rodziny $\{A_t\}_{t\in T}$ podgrup grupy A i piszemy $B=\bigoplus_{t\in T} A_t$, jeżeli $B=\sum_{t\in T} A_t$ i rodzina $\{A_t\}_{t\in T}$ spełnia którykolwiek z równoważnych warunków stwierdzenia 9.3.

Uwaga 9.5. *Wprost z definicji wewnętrznej sumy prostej wynika, że podgrupa B grupy abelowej $(A,+,0)$ jest wewnętrzną sumą prostą podgrup A_1 i A_2 grupy A wtedy i tylko wtedy, gdy $B=A_1+A_2$ oraz $A_1\cap A_2=\{0\}$. Ponadto na mocy stwierdzenia 9.3 jest to równoważne temu, że każdy element $a\in B$ może być jednoznacznie zapisany w postaci $a=a_1+a_2$ dla pewnych $a_1\in A_1$ i $a_2\in A_2$.*

Uwaga 9.6. *Jeżeli podgrupa B grupy abelowej $(A,+,0)$ jest wewnętrzną sumą prostą podgrup $A_1,\dots,A_n$ grupy A, to będziemy pisali $B=A_1\oplus\ldots\oplus A_n$ lub $B=\bigoplus_{i=1}^{n} A_i$. Podobnie, jeśli podgrupa C grupy A jest wewnętrzną sumą prostą podgrup $B_1,B_2,\dots$ grupy A, to będziemy pisali $C=B_1\oplus B_2\oplus\ldots$ lub $C=\bigoplus_{i=1}^{\infty} B_i$.*

Zadanie (2)**.** Niech $(A,+,0)$ będzie grupą abelową. Udowodnij, że $A_1=\{(a,0):a\in A\}$, $A_2=\{(0,a):a\in A\}$ oraz $A_0=\{(a,a):a\in A\}$ są podgrupami grupy $A\times A$ i $A\times A=A_1\oplus A_2=A_1\oplus A_0=A_2\oplus A_0$.

Stwierdzenie 9.7. *Jeżeli B jest wewnętrzną sumą prostą rodziny $\{B_t\}_{t\in T}$ podgrup grupy abelowej $(A,+,0)$ oraz C jest podgrupą grupy A taką, że $B\cap C=\{0\}$, to $B+C$ jest wewnętrzną sumą prostą podgrup rodziny $\{C\}\cup\{B_t\}_{t\in T}$.*

DOWÓD. Wprost z założenia mamy, że $B+C$ jest sumą algebraiczną podgrup rodziny $\{C\}\cup\{B_t\}_{t\in T}$. Weźmy dowolny skończony podzbiór n-elementowy $T_0=\{t_1,\dots,t_n\}$ $(n=0,1,\dots)$ zbioru T i dowolne $a_i\in A_{t_i}$, $i=1,\dots,n$ oraz dowolne $c\in C$ takie, że $a_1+\ldots+a_n+c=0$. Wtedy $c=-(a_1+\ldots+a_n)$, więc ze stwierdzenia 9.2, $c\in B$. Zatem $c\in B\cap C=\{0\}$, skąd $c=0$ oraz $a_1+\ldots+a_n=0$. Zatem ze stwierdzenia 9.3, $a_1=\ldots=a_n=0$. Na mocy stwierdzenia 9.3, $B+C$ jest wewnętrzną sumą prostą podgrup rodziny $\{C\}\cup\{B_t\}_{t\in T}$. □

Stwierdzenie 9.8. *Załóżmy, że S jest co najmniej dwuelementowym podzbiorem zbioru T. Jeżeli B jest wewnętrzną sumą prostą rodziny $\{B_t\}_{t\in T}$ podgrup grupy abelowej $(A,+,0)$, to $C=\sum_{s\in S} B_s$ jest wewnętrzną sumą prostą podgrup rodziny $\{B_s\}_{s\in S}$. Ponadto dla $S\neq T$, $B=C\oplus D$, gdzie $D=\sum_{t\in T\setminus S} B_t$.*

DOWÓD. Jest prostą konsekwencją stwierdzeń 9.2 i 9.3. □

9.2 Wewnętrzne sumy proste ideałów

Stwierdzenie 9.9. *Suma algebraiczna dowolnej rodziny ideałów lewostronnych (prawostronnych, obustronnych) pierścienia R jest ideałem lewostronnym (prawostronnym, obustronnym) tego pierścienia.*

DOWÓD. Niech $\{A_t\}_{t\in T}$ będzie rodziną ideałów lewostronnych (prawostronnych) pierścienia R. Wówczas dla każdego $t \in T$, A_t jest podgrupą grupy R^+. Zatem $\sum_{t\in T} A_t$ jest podgrupą grupy R^+. Weźmy dowolne $a \in \sum_{t\in T} A_t$ i dowolne $r \in R$. Wówczas ze stwierdzenia 9.2 istnieją parami różne elementy $t_1, \ldots, t_n \in T$ oraz istnieją $a_i \in A_{t_i}$, $i = 1, \ldots, n$ takie, że $a = a_1 + \ldots + a_n$. Stąd $r \cdot a_i \in A_{t_i}$ $(a_i \cdot r \in A_{t_i})$ dla $i = 1, \ldots, n$, a więc $r \cdot a \in A_{t_1} + \ldots + A_{t_n}$ $(a \cdot r \in A_{t_1} + \ldots + A_{t_n})$. Zatem ze stwierdzenia 9.2, $r \cdot a \in \sum_{t\in T} A_t$ $(a \cdot r \in \sum_{t\in T} A_t)$. Stąd $\sum_{t\in T} A_t <_l R$ $(\sum_{t\in T} A_t <_r R)$. Z tych rozważań mamy od razu, że suma algebraiczna ideałów pierścienia R jest ideałem tego pierścienia. □

Definicja 9.10. Mówimy, że ideał lewostronny (prawostronny, obustronny) A pierścienia R jest *wewnętrzną sumą prostą* rodziny $\{A_t\}_{t\in T}$ ideałów lewostronnych (prawostronnych, obustronnych) pierścienia R i piszemy $A = \bigoplus_{t\in T} A_t$, jeżeli $A = \sum_{t\in T} A_t$ i rodzina $\{A_t\}_{t\in T}$ spełnia którykolwiek z równoważnych warunków stwierdzenia 9.3.

Definicja 9.11. Element e pierścienia R nazywamy *idempotentem*, jeżeli $e = e^2$.

Stwierdzenie 9.12. *Niech element e będzie idempotentem pierścienia R. Wówczas $l_R(e) <_l R$ oraz $Re \oplus l_R(e) = R$. Ponadto $r_R(e) <_r R$ i $eR \oplus r_R(e) = R$.*

DOWÓD. Z przykładu 3.13 wynika od razu, że $l_R(e) <_l R$. Weźmy dowolne $a \in R$. Wtedy $a = ae + (a - ae)$. Ponadto $ae \in Re$ oraz $a - ae \in l_R(e)$, bo $(a - ae)e = ae - ae^2 = ae - ae = 0$. Zatem $R = Re + l_R(e)$. Weźmy dowolne $x \in Re \cap l_R(e)$. Wtedy $x = re$ dla pewnego $r \in R$ oraz $0 = xe = (re)e = re^2 = re$, skąd $x = 0$. Zatem $Re \cap l_R(e) = \{0\}$ i ostatecznie $R = Re \oplus l_R(e)$. □

Stwierdzenie 9.13. *Niech A i B będą ideałami lewostronnymi pierścienia R z jedynką 1 takimi, że $R = A \oplus B$. Wówczas istnieją idempotenty $e, f \in R$ takie, że $A = Re$, $B = Rf$, $ef = fe = 0$ i $e + f = 1$.*

DOWÓD. Ponieważ $R = A + B$, więc istnieją $e \in A$ oraz $f \in B$ takie, że $1 = e + f$. Stąd $e = e^2 + ef$, czyli $ef = e - e^2 \in A \cap B = \{0\}$. Zatem $e = e^2$ i $ef = 0$. Analogicznie pokazuje się, że $fe = 0$ i $f = f^2$. Ponieważ $e \in A$ i $A <_l R$, więc $Re \subseteq A$. Weźmy dowolne $a \in A$. Wtedy $a = ae + af$, skąd $af = a - ae \in A \cap B = \{0\}$. Zatem $a = ae \in Re$ i wobec tego $A = Re$. Analogicznie pokazujemy, że $B = Rf$. □

Stwierdzenie 9.14. *Niech I będzie ideałem pierścienia R. Jeżeli pierścień I posiada jedynkę, to istnieje ideał J pierścienia R taki, że $R = I \oplus J$.*

DOWÓD. Niech $e \in I$ będzie jedynką pierścienia I. Wtedy $ae = ea = a$ dla wszystkich $a \in I$. Stąd $I \subseteq Re \subseteq I$, a więc $I = Re$. Ponadto $e = e^2$, więc ze stwierdzenia 9.12, $l_R(e) <_l R$ oraz $I \oplus l_R(e) = R$. Pozostaje zatem pokazać, że $l_R(e) <_r R$. W tym celu weźmy dowolne $x \in l_R(e)$ i dowolne $r \in R$. Wtedy $xe = 0$. Ponadto $I \lhd R$, więc $re \in I$. Ale e jest jedynką pierścienia I, więc $re = e(re)$. Zatem $(xr)e = x(re) = x[e(re)] = (xe)(re) = 0 \cdot re = 0$, skąd $xr \in l_R(e)$. □

Stwierdzenie 9.15. *Niech I, J będą ideałami pierścienia R takimi, że $R = I \oplus J$. Wtedy $IJ = JI = \{0\}$ oraz $R \cong I \times J$.*

DOWÓD. Zauważmy, że $IJ \subseteq I \cap J = \{0\}$, skąd $IJ = \{0\}$. Podobnie $JI = \{0\}$. Ponadto z uwagi 9.5 każdy element $a \in R$ można jednoznacznie zapisać w postaci $a = i + j$ dla pewnych $i \in I$, $j \in J$. Wynika stąd, że odwzorowanie $f\colon I \times J \to R$ dane wzorem $f((i,j)) = i+j$ jest "na". Weźmy dowolne $i_1, i_2 \in I$ oraz dowolne $j_1, j_2 \in J$. Wtedy $f((i_1, j_1) + (i_2, j_2)) = f((i_1 + i_2, j_1 + j_2)) = (i_1 + i_2) + (j_1 + j_2) = (i_1 + j_1) + (i_2 + j_2) = f((i_1, j_1)) + f((i_2, j_2))$ oraz $f((i_1, j_1) \cdot (i_2, j_2)) = f((i_1 i_2, j_1 j_2)) = i_1 i_2 + j_1 j_2$. Ale $f((i_1, j_1)) \cdot f((i_2, j_2)) = (i_1 + j_1) \cdot (i_2 + j_2) = i_1 i_2 + j_1 j_2$, bo $i_1 j_2 = j_1 i_2 = 0$, więc $f((i_1, j_1) \cdot (i_2, j_2)) = f((i_1, j_1)) \cdot f((i_2, j_2))$. Zatem f jest homomorfizmem pierścieni. Niech $(i,j) \in Ker\, f$. Wtedy $i + j = 0$, więc ze stwierdzenia 9.3, $i = j = 0$, skąd $Ker\, f = \{(0,0)\}$ i ostatecznie f jest izomorfizmem pierścieni. □

Zadanie (3)**.** Niech $\{A_t\}_{t \in T}$ będzie rodziną ideałów pierścienia R taką, że $R = \bigoplus_{t \in T} A_t$. Udowodnij, że wówczas

(a) $A_t \cdot A_s = \{0\}$ dla dowolnych $t, s \in T$, $t \neq s$;

(b) dla dowolnego $t \in T$ każdy ideał lewostronny (prawostronny, obustronny) pierścienia A_t jest ideałem lewostronnym (prawostronnym, obustronnym) pierścienia R;

(c) pierścień R jest izomorficzny z zewnętrzną sumą prostą rodziny pierścieni $\{A_t\}_{t \in T}$.

Definicja 9.16. Niech L będzie ideałem lewostronnym (prawostronnym, obustronnym) pierścienia R. Mówimy, że L jest *minimalnym ideałem lewostronnym (prawostronnym, obustronnym)* pierścienia R, jeżeli $L \neq \{0\}$ oraz dla dowolnego niezerowego ideału lewostronnego (prawostronnego, obustronnego) M pierścienia R takiego, że $M \subseteq L$ jest $M = L$.

Stwierdzenie 9.17. *Jeżeli L jest minimalnym ideałem lewostronnym (prawostronnym) pierścienia R, to $L^2 = \{0\}$ lub $L = Re$ ($L = eR$) dla pewnego niezerowego idempotenta $e \in R$.*

Dowód. Załóżmy, że $L^2 \neq \{0\}$. Wtedy istnieje $a \in L$ takie, że $La \neq \{0\}$. Ale $La <_l R$ oraz $La \subseteq L$, więc z minimalności L, $L = La$. Stąd $a \in La$, a więc istnieje $e \in L$ takie, że $a = ea$. Zatem $ea = e^2a$, czyli $e - e^2 \in l_R(a) \cap L$. Ale $l_R(a) <_l R$, więc $l_R(a) \cap L <_l R$. Ponadto $La \neq \{0\}$, więc $l_R(a) \cap L \neq L$. Z minimalności L wynika więc, że $l_R(a) \cap L = \{0\}$, skąd $e = e^2$. Ale $a = ea$ i $a \neq 0$, więc $e \neq 0$. Ponadto $Re \subseteq L$ oraz $0 \neq e = e^2 \in Re$ i $Re <_l R$, więc z minimalności L, $L = Re$.

Rozumowanie dla wersji prawostronnej jest podobne. □

Ponieważ w pierścieniu półpierwszym nie ma niezerowych jednostronnych ideałów nilpotentnych, więc mamy stąd następujący

Wniosek 9.18. *W pierścieniu półpierwszym R każdy minimalny ideał jednostronny jest generowany przez idempotenta.*

Zadanie (4)**.** Niech I będzie ideałem pierścienia półpierwszego R. Udowodnij, że I jest ideałem minimalnym pierścienia R wtedy i tylko wtedy, gdy I jest idempotentnym pierścieniem prostym.

Wykład 10

Pierścienie artinowskie

10.1 Określenie pierścienia artinowskiego

Udowodnimy najpierw bardzo użyteczny lemat zwany też *prawem modularności dla podgrup.*

Lemat 10.1. *Niech A, B, C będą podgrupami grupy abelowej $(G, +, 0)$ takimi, że $A \subseteq C$. Wówczas $(A + B) \cap C = A + (B \cap C)$.*

Dowód. Weźmy dowolne $x \in (A + B) \cap C$. Wtedy $x \in C$ i $x = a + b$ dla pewnych $a \in A$, $b \in B$. Stąd $b = x - a \in C$, gdyż $x \in C$ i $a \in C$, bo $a \in A$ i $A \subseteq C$. Zatem $b \in B \cap C$ i $a \in A$, skąd $x \in A + (B \cap C)$, a więc $(A + B) \cap C \subseteq A + (B \cap C)$.

Ponadto $A \subseteq A + B$ i $A \subseteq C$, więc $A \subseteq (A + B) \cap C$ oraz $B \cap C \subseteq C$ i $B \cap C \subseteq B \subseteq A + B$, skąd $B \cap C \subseteq (A + B) \cap C$. Zatem $A + (B \cap C) \subseteq (A + B) \cap C$ i ostatecznie $(A + B) \cap C = A + (B \cap C)$. □

Twierdzenie 10.2. *Dla dowolnego pierścienia R równoważne są warunki:*

(i) każdy zstępujący ciąg $L_1 \supseteq L_2 \supseteq L_3 \supseteq \ldots$ ideałów lewostronnych pierścienia R stabilizuje się, tzn. istnieje $s \in \mathbb{N}$ takie, że $L_s = L_{s+1} = \ldots$;

(ii) w każdej niepustej rodzinie ideałów lewostronnych pierścienia R istnieje element minimalny.

Dowód. $(i) \Rightarrow (ii)$. Załóżmy, że w pewnej niepustej rodzinie $\mathcal{M}$ ideałów lewostronnych pierścienia R nie istnieje element minimalny. Oznacza to, że dla dowolnego $K \in \mathcal{M}$ istnieje $L \in \mathcal{M}$ takie, że $K \supset L$. Ponieważ rodzina $\mathcal{M}$ jest niepusta, więc istnieje $M_1 \in \mathcal{M}$. Zatem istnieje $M_2 \in \mathcal{M}$ takie, że $M_1 \supset M_2$. Załóżmy, że dla pewnego $n \in \mathbb{N}$ mamy już skonstruowany zstępujący ciąg $M_1 \supset M_2 \supset \ldots \supset M_n$ ideałów lewostronnych z rodziny $\mathcal{M}$. Wtedy istnieje $M_{n+1} \in \mathcal{M}$ takie, że $M_n \supset M_{n+1}$. Stąd przez indukcję mamy zstępujący ciąg $M_1 \supset M_2 \supset M_3 \supset \ldots$ elementów z $\mathcal{M}$, który nie stabilizuje się. Sprzeczność.

$(ii) \Rightarrow (i)$. Niech $L_1 \supseteq L_2 \supseteq \ldots$ będzie dowolnym zstępującym ciągiem ideałów lewostronnych pierścienia R. Wówczas w rodzinie $\mathcal{M} = \{L_1, L_2, \ldots\}$

istnieje element minimalny L_s. Weźmy dowolne naturalne $n \geqslant s$. Wtedy $L_s \supseteq L_n$ i $L_n \in \mathcal{M}$, więc z minimalności L_s, $L_s = L_n$. Zatem ciąg $L_1 \supseteq L_2 \supseteq \ldots$ stabilizuje się. □

Wykorzystując pierścienie z odwróconym mnożeniem i twierdzenie 10.2 otrzymujemy natychmiast następujące

Twierdzenie 10.3. *Dla dowolnego pierścienia R równoważne są warunki:*

(i) każdy zstępujący ciąg $P_1 \supseteq P_2 \supseteq P_3 \supseteq \ldots$ ideałów prawostronnych pierścienia R stabilizuje się, tzn. istnieje $s \in \mathbb{N}$ takie, że $P_s = P_{s+1} = \ldots$;

(ii) w każdej niepustej rodzinie ideałów prawostronnych pierścienia R istnieje element minimalny.

Definicja 10.4. Każdy pierścień R spełniający którykolwiek z równoważnych warunków (i)-(ii) twierdzenia 10.2 nazywamy *lewostronnie artinowskim*, zaś każdy pierścień R spełniający którykolwiek z równoważnych warunków (i)-(ii) twierdzenia 10.3 nazywamy *prawostronnie artinowskim*.

Przykład 10.5. Wykażemy, że podpierścień $R = \begin{bmatrix} \mathbb{R} & \mathbb{R} \\ 0 & \mathbb{Q} \end{bmatrix}$ pierścienia macierzy $M_2(\mathbb{R})$ jest lewostronnie artinowski, ale nie jest prawostronnie artinowski. Wiadomo, że $\mathbb{R}$ jest w naturalny sposób przestrzenią liniową nad ciałem $\mathbb{Q}$ oraz $\dim_{\mathbb{Q}} \mathbb{R} = \infty$. W przestrzeni $\mathbb{R}$ istnieją zatem podprzestrzenie liniowe $V_1 \supset V_2 \supset V_3 \supset \ldots$. Ponadto jeśli V jest podprzestrzenią liniową przestrzeni $\mathbb{R}$, to $\begin{bmatrix} 0 & V \\ 0 & 0 \end{bmatrix}$ jest ideałem prawostronnym pierścienia R. Zatem mamy zstępujący ciąg $\begin{bmatrix} 0 & V_1 \\ 0 & 0 \end{bmatrix} \supset \begin{bmatrix} 0 & V_2 \\ 0 & 0 \end{bmatrix} \supset \begin{bmatrix} 0 & V_3 \\ 0 & 0 \end{bmatrix} \supset \ldots$ ideałów prawostronnych pierścienia R, który się nie stabilizuje. Stąd pierścień R nie jest prawostronnie artinowski. Niech $L <_l R$ i niech $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in L$. Wtedy $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in L$, $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in L$, $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in L$, a więc

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & c \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & c \end{bmatrix} \in L. \tag{10.1}$$

Rozważmy najpierw przypadek gdy L nie zawiera się w ideale lewostronnym $\begin{bmatrix} \mathbb{R} & \mathbb{R} \\ 0 & 0 \end{bmatrix}$. Wtedy ze wzoru (10.1) wynika, że istnieje niezerowe $c \in \mathbb{Q}$ takie, że $\begin{bmatrix} 0 & 0 \\ 0 & c \end{bmatrix}, \begin{bmatrix} 0 & c \\ 0 & 0 \end{bmatrix} \in L$, a stąd otrzymujemy, że $\begin{bmatrix} 0 & \mathbb{R} \\ 0 & \mathbb{Q} \end{bmatrix} \subseteq L$. Zatem $L = \begin{bmatrix} 0 & \mathbb{R} \\ 0 & \mathbb{Q} \end{bmatrix}$ lub istnieje niezerowe $a \in \mathbb{R}$ takie, że $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \in L$. Ale wtedy

$\begin{bmatrix} \mathbb{R} & 0 \\ 0 & 0 \end{bmatrix} \subseteq L$, więc $L = R$. W ten sposób wykazaliśmy, że jeżeli L nie zawiera się w $\begin{bmatrix} \mathbb{R} & \mathbb{R} \\ 0 & 0 \end{bmatrix}$, to $L = R$ lub $L = \begin{bmatrix} 0 & \mathbb{R} \\ 0 & \mathbb{Q} \end{bmatrix}$.

Rozważmy teraz przypadek $L \subseteq \begin{bmatrix} \mathbb{R} & \mathbb{R} \\ 0 & 0 \end{bmatrix}$. Weźmy dowolne $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \in L$. Wtedy dla dowolnego $r \in \mathbb{R}$, $\begin{bmatrix} r & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \in L$, skąd $\begin{bmatrix} ra & rb \\ 0 & 0 \end{bmatrix} \in L$. Wynika stąd, że L jest podprzestrzenią dwuwymiarowej przestrzeni liniowej $\begin{bmatrix} \mathbb{R} & \mathbb{R} \\ 0 & 0 \end{bmatrix}$ nad ciałem $\mathbb{R}$, skąd $\dim_R L \leqslant 2$.

Załóżmy, że pierścień R nie jest lewostronnie artinowski. Wówczas z twierdzenia 10.2 istnieje zstępujący ciąg $L_1 \supset L_2 \supset L_3 \supset \ldots$ ideałów lewostronnych pierścienia R. Jeżeli istnieje $s \in \mathbb{N}$ takie, że $L_s \subseteq \begin{bmatrix} \mathbb{R} & \mathbb{R} \\ 0 & 0 \end{bmatrix}$, to $L_n \subseteq \begin{bmatrix} \mathbb{R} & \mathbb{R} \\ 0 & 0 \end{bmatrix}$ dla wszystkich $n \geqslant s$ i wówczas $2 \geqslant \dim_{\mathbb{R}} L_s > \dim_{\mathbb{R}} L_{s+1} > \ldots$, co prowadzi do sprzeczności. Zatem dla wszystkich $n \in \mathbb{N}$, L_n nie zawiera się w $\begin{bmatrix} \mathbb{R} & \mathbb{R} \\ 0 & 0 \end{bmatrix}$. Z pierwszej części rozumowania wynika zatem, że $L_n = R$ lub $L_n = \begin{bmatrix} 0 & \mathbb{R} \\ 0 & \mathbb{Q} \end{bmatrix}$ dla każdego $n \in \mathbb{N}$. Ale $L_1 \supset L_2 \supset \ldots$, więc mamy sprzeczność. Zatem pierścień R jest lewostronnie artinowski.

Zadanie (1)**.** Udowodnij, że dla dowolnej liczby pierwszej p pierścień $\mathbb{C}^0_{p^\infty}$ jest lewostronnie artinowski.

Zadanie (2)**.** Czy pierścień $\mathbb{Z}$ jest artinowski?

Zadanie (3)**.** Opisać artinowskie dziedziny całkowitości. Opisać dziedziny, które są pierścieniami lewostronnie artinowskimi.

Zadanie (4)**.** Udowodnij, że każdy pierścień skończony jest lewostronnie artinowski.

Twierdzenie 10.6. *Każdy obraz homomorficzny pierścienia lewostronnie artinowskiego jest pierścieniem lewostronnie artinowskim.*

DOWÓD. Niech $f\colon R \to S$ będzie homomorfizmem pierścienia lewostronnie artinowskiego R na pierścień S. Niech $L_1 \supseteq L_2 \supseteq \ldots$ będzie zstępującym ciągiem ideałów lewostronnych pierścienia S. Wtedy ze stwierdzenia 6.15, $f^{-1}(L_1) \supseteq f^{-1}(L_2) \supseteq \ldots$ jest zstępujacym ciągiem ideałów lewostronnych pierścienia R. Zatem z twierdzenia 10.2 istnieje $s \in \mathbb{N}$ takie, że $f^{-1}(L_n) = f^{-1}(L_s)$ dla wszystkich $n \geqslant s$. Ale f jest "na", więc stąd $L_n = L_s$ dla wszystkich $n \geqslant s$ i z twierdzenia 10.2 pierścień S jest lewostronnie artinowski. □

Twierdzenie 10.7. *Niech I będzie ideałem pierścienia R. Jeżeli pierścienie I oraz R/I są lewostronnie artinowskie, to pierścień R też jest lewostronnie artinowski.*

DOWÓD. Niech $L_1 \supseteq L_2 \supseteq L_3 \supseteq \ldots$ będzie zstępującym ciągiem ideałów lewostronnych pierścienia R. Wówczas $L_1 \cap I \supseteq L_2 \cap I \supseteq L_3 \cap I \supseteq \ldots$ jest zstępującym ciągiem ideałów lewostronnych pierścienia I oraz $(L_1 + I)/I \supseteq (L_2+I)/I \supseteq (L_3+I)/I \supseteq \ldots$ jest zstępującym ciągiem ideałów lewostronnych pierścienia R/I. Zatem z twierdzenia 10.2 istnieją $r, s \in \mathbb{N}$ takie, że $L_n \cap I = L_r \cap I$ dla wszystkich $n \geqslant r$ oraz $(L_m + I)/I = (L_s + I)/I$ dla wszystkich $m \geqslant s$. Stąd $L_m + I = L_s + I$ dla wszystkich $m \geqslant s$. Niech $t = r+s$. Wtedy dla wszystkich $n \geqslant t$ mamy, że $L_n \cap I = L_t \cap I$ oraz $L_n + I = L_t + I$. Z lematu 10.1 uzyskujemy, że $L_t = L_t \cap (L_n + I) = L_n + (L_t \cap I)$. Zatem $L_t = L_n + (L_n \cap I) = L_n$ dla wszystkich $n \geqslant t$, czyli ciąg $L_1 \supseteq L_2 \supseteq L_3 \supseteq \ldots$ stabilizuje się i na mocy twierdzenia 10.2 pierścień R jest lewostronnie artinowski. □

Twierdzenie 10.8. *Jeżeli pierścienie $R_1, \ldots, R_n$ ($n \geqslant 2$) są lewostronnie artinowskie, to pierścień $R_1 \times \ldots \times R_n$ też jest lewostronnie artinowski.*

DOWÓD. Indukcja względem n. Załóżmy, że pierścienie R_1 i R_2 są lewostronnie artinowskie. Wtedy z przykładu 7.14, $R_1 \times \{0\} \lhd R_1 \times R_2$, $R_1 \cong R_1 \times \{0\}$ oraz $(R_1 \times R_2)/(R_1 \times \{0\}) \cong R_2$. Zatem z twierdzenia 10.7 pierścień $R_1 \times R_2$ jest lewostronnie artinowski.

Załóżmy, że teza zachodzi dla pewnego naturalnego $n \geqslant 2$. Niech $R_1, \ldots, R_n$, R_{n+1} bedą pierścieniami lewostronnie artinowskimi. Wtedy z założenia indukcyjnego pierścień $R_1 \times \ldots \times R_n$ jest lewostronnie artinowski. Zatem z pierwszej części dowodu pierścień $(R_1 \times \ldots \times R_n) \times R_{n+1}$ też jest lewostronnie artinowski. Ale $R_1 \times \ldots \times R_n \times R_{n+1} \cong (R_1 \times \ldots \times R_n) \times R_{n+1}$, więc pierścień $R_1 \times \ldots \times R_n \times R_{n+1}$ jest lewostronnie artinowski. □

10.2 Półpierwsze pierścienie artinowskie

Lemat 10.9. *Niech $e, f \in R$ będą idempotentami pierścienia R takimi, że $fe = 0$. Wtedy $e + f - ef$ jest idempotentem i $Re + Rf = R(e + f - ef)$ oraz $eR + fR = (e + f - ef)R$.*

DOWÓD. Z przyjętych założeń, $e(e+f-ef) = e^2+ef-e^2f = e+ef-ef = e$, $f(e+f-ef) = fe+f^2-fef = 0+f-0 = f$ oraz $(e+f-ef)e = e^2+fe-efe = e + 0 - 0 = e$, $(e + f - ef)f = ef + f^2 - ef^2 = ef + f - ef = f$. Stąd $e, f \in R(e + f - ef)$ i $e, f \in (e + f - ef)R$, a więc $Re + Rf \subseteq R(e + f - ef)$ i $eR+fR \subseteq (e+f-ef)R$. Ponadto $e, f, ef \in Re+Rf$ i $e, f, ef \in eR+fR$, więc $e+f-ef \in Re+Rf$ i $e+f-ef \in eR+fR$, czyli $R(e+f-ef) \subseteq Re+Rf$ i $(e+f-ef)R \subseteq eR+fR$. Zatem $Re+Rf = R(e+f-ef)$ i $eR+fR = (e+f-ef)R$. W końcu, $(e+f-ef)^2 = (e+f-ef)e+(e+f-ef)f-[(e+f-ef)e]f = e+f-ef$, więc $e + f - ef$ jest idempotentem. □

Twierdzenie 10.10. *Każdy ideał lewostronny (prawostronny) półpierwszego pierścienia R lewostronnie (prawostronnie) artinowskiego jest generowany przez idempotenta.*

DOWÓD. Załóżmy, że tak nie jest. Wówczas rodzina $\mathcal{M}$ wszystkich ideałów lewostronnych (prawostronnych) pierścienia R, które nie są generowane przez idempotenta jest niepusta. Z twierdzenia 10.2 (10.3) istnieje w $\mathcal{M}$ element minimalny L. Ale $\{0\} = R \cdot 0 = 0 \cdot R$ i $0 = 0^2$, więc $L \neq \{0\}$. Z twierdzenia 10.2 (10.3) w rodzinie $\mathcal{L}$ wszystkich niezerowych ideałów lewostronnych (prawostronnych) pierścienia R zawartych w L istnieje element minimalny A. Z wniosku 9.18 istnieje idempotent $e \in L$ taki, że $A = Re$ ($A = eR$). Ponadto ze stwierdzenia 9.12 $A \oplus l_R(e) = R$ ($A \oplus r_R(e) = R$). Ponadto $A \subseteq L$, więc z lematu 10.1, $A \oplus (l_R(e) \cap L) = L$ ($A \oplus (r_R(e) \cap L) = L$). Ale $l_R(e) \cap L <_l R$ ($r_R(e) \cap L <_r R$) i $l_R(e) \cap L \neq \{0\}$ ($r_R(e) \cap L \neq \{0\}$), bo $L \neq Re$ ($L \neq eR$), gdyż L nie jest generowany przez idempotenta oraz $e \neq 0$, więc $l_R(e) \cap L \subset L$ ($r_R(e) \cap L \subset L$). Z minimalności L w rodzinie $\mathcal{M}$ wynika, że $l_R(e) \cap L = Rf$ ($r_R(e) \cap L = fR$) dla pewnego idempotenta f. Lecz $f \in l_R(e)$ ($f \in r_R(e)$), więc $fe = 0$ ($ef = 0$). Zatem z lematu 10.9 $e + f - ef$ ($e + f - fe$) jest idempotentem oraz $L = Re \oplus Rf = R(e + f - ef)$ ($L = eR \oplus fR = (e + f - fe)R$). Sprzeczność. □

Zadanie (5)**.** Udowodnij, że każdy ideał lewostronny półpierwszego pierścienia lewostronnie artinowskiego jest pierścieniem idempotentnym.

Definicja 10.11. Idempotent $e \in R$ pierścienia R nazywamy *centralnym*, jeżeli $e \in Z(R)$, tzn. $ea = ae$ dla dowolnego $a \in R$.

Twierdzenie 10.12. *W pierścieniu zredukowanym każdy idempotent jest centralny.*

DOWÓD. Niech R będzie pierścieniem zredukowanym oraz niech $e^2 = e \in R$. Weźmy dowolne $r \in R$. Wtedy $e(re - ere) = ere - e^2re = ere - ere = 0$, skąd $(re-ere)^2 = re(re-ere)-ere(re-ere) = 0-0 = 0$. Zatem $re-ere = 0$, czyli $re = ere$ dla każdego $r \in R$. Podobnie $(er-ere)e = ere-ere^2 = ere-ere = 0$, skąd $(er - ere)^2 = (er - ere)er - (er - ere)ere = 0 - 0 = 0$, więc $er - ere = 0$, czyli $er = ere$ dla każdego $r \in R$. Zatem $er = ere = re$, czyli $er = re$ dla każdego $r \in R$, a więc $e \in Z(R)$. □

Twierdzenie 10.13. *Każdy ideał półpierwszego pierścienia R lewostronnie (prawostronnie) artinowskiego jest generowany przez centralnego idempotenta.*

DOWÓD. Załóżmy, że pierścień R jest lewostronnie artinowski i niech $I \lhd R$. Wtedy z twierdzenia 10.10 istnieje idempotent $e \in R$ taki, że $I = Re$. Weźmy dowolne $a \in R$. Wtedy $ea \in I$. Zatem $ea = be$ dla pewnego $b \in R$, skąd $eae = be^2 = be = ea$, czyli $ea = eae$. Stąd $e(ea-ae) = e^2a-eae = ea-ea = 0$. Zatem $ea - ae \in I \cap r_R(I)$. Ale $I \cap r_R(I) \lhd R$ i $[I \cap r_R(I)]^2 = \{0\}$, więc z

półpierwszości R, $I \cap r_R(I) = \{0\}$. Stąd $ea - ae = 0$, czyli $ae = ea$ i e jest centralnym idempotentem.

Rozumowanie dla wersji prawostronnej przebiega analogicznie. □

Twierdzenie 10.14. *Każdy półpierwszy pierścień R lewostronnie (prawostronnie) artinowski posiada jedynkę.*

DOWÓD. Z twierdzenia 10.13 istnieje centralny idempotent $e \in R$ taki, że $R = Re$. Weźmy dowolne $a \in R$. Wtedy $a = be$ dla pewnego $b \in R$, skąd $ae = be^2 = be = a$ oraz $ea = ae$, bo $e \in Z(R)$. Zatem $ae = ea = a$ dla każdego $a \in R$, czyli e jest jedynką pierścienia R. □

Zadanie (6)**.** Niech R będzie półpierwszym pierścieniem lewostronnie artinowskim. Udowodnij, że jeżeli $I \lhd R$ oraz $J \lhd I$, to $J \lhd R$.

Twierdzenie 10.15. *Każdy pierwszy pierścień R lewostronnie (prawostronnie) artinowski jest pierścieniem prostym z jedynką.*

DOWÓD. Z założenia wynika, że pierścień R jest półpierwszy. Zatem z twierdzenia 10.14 R ma jedynkę. Niech $I \lhd R$, $I \neq \{0\}$. Wtedy z twierdzenia 10.13 istnieje centralny idempotent $e \in I$ taki, że $I = Re$. Stąd e jest jedynką pierścienia I. Zatem ze stwierdzenia 9.14 istnieje $J \lhd R$ taki, że $I \oplus J = R$. Stąd $IJ = \{0\}$, więc z pierwszości R, $J = \{0\}$ i wobec tego $I = R$. Zatem pierścień R jest prosty. □

Zadanie (7)**.** Udowodnij, że dla dowolnego ciała K i dla dowolnego $n \in \mathbb{N}$ pierścień $M_n(K)$ jest lewostronnie artinowski.

Stwierdzenie 10.16. *Niech I będzie niezerowym ideałem półpierwszego pierścienia R lewostronnie artinowskiego. Jeżeli $L <_l I$, to $L <_l R$. W szczególności I jest półpierwszym pierścieniem lewostronnie artinowskim.*

DOWÓD. Z twierdzenia 5.20 I jest pierścieniem półpierwszym. Natomiast z twierdzenia 10.13 istnieje centralny idempotent $e \in I$ taki, że $I = Re$. Stąd e jest jedynką pierścienia I. Ze stwierdzenia 9.14 istnieje $J \lhd R$ taki, że $I \oplus J = R$. Ponieważ $JI \subseteq I \cap J = \{0\}$, więc $JI = \{0\}$. Weźmy dowolne $r \in R$, $a \in L$. Wtedy istnieją $i \in I$, $j \in J$ takie, że $r = i + j$. Stąd $ja \in JI = \{0\}$, czyli $ra = ia \in L$. Zatem $L <_l R$. Z twierdzenia 10.2 wynika zatem, że pierścien I jest lewostronnie artinowski. □

Twierdzenie 10.17. *Każdy niezerowy ideał półpierwszego pierścienia R lewostronnie (prawostronnie) artinowskiego jest skończoną sumą prostą ideałów pierścienia R, które są pierścieniami prostymi.*

DOWÓD. Załóżmy, że tak nie jest. Wtedy rodzina $\mathcal{M}$ wszystkich niezerowych ideałów pierścienia R, które nie są skończoną sumą prostą ideałów pierścienia R bedących pierścieniami prostymi, jest niepusta. Zatem z twierdzenia 10.2

istnieje w $\mathcal{M}$ element minimalny I. Z założenia I nie jest pierścieniem prostym. Ponadto ze stwierdzenia 10.16 I jest półpierwszym pierścieniem lewostronnie artinowskim. Z twierdzenia 10.2 istnieje pierścień prosty J będący ideałem pierścienia I. Z zadania 6, $J \lhd R$. Z twierdzenia 10.13 ideał J jest generowany przez idempotenta, który jest jedynką pierścienia J. Ze stwierdzenia 9.14 $I = J \oplus K$ dla pewnego $K \lhd I$. Ale z zadania 6, $K \lhd R$. Ponadto $K \neq \{0\}$, bo I nie jest pierścieniem prostym. Stąd $K \subset I$, więc z minimalności I w rodzinie $\mathcal{M}$ mamy, że $K \notin \mathcal{M}$. Zatem $K = I_1 \oplus \ldots \oplus I_s$ dla pewnych niezerowych ideałów $I_1, \ldots, I_s$ pierścienia R, które są pierścieniami prostymi. Stąd $I = J \oplus I_1 \oplus \ldots \oplus I_s$ i mamy sprzeczność. □

Twierdzenie 10.18. *Każdy niezerowy ideał lewostronny półpierwszego pierścienia R lewostronnie artinowskiego jest sumą prostą skończonej liczby minimalnych ideałów lewostronnych pierścienia R.*

DOWÓD. Załóżmy, że tak nie jest. Wtedy rodzina $\mathcal{M}$ wszystkich niezerowych ideałów lewostronnych pierścienia R, które nie są skończoną sumą prostą minimalnych ideałów lewostronnych pierścienia R, jest niepusta. Zatem z twierdzenia 10.2 istnieje w $\mathcal{M}$ element minimalny I. Z założenia I nie jest minimalnym ideałem lewostronnym pierścienia R. Ponadto z twierdzenia 10.10 $I = Re$ dla pewnego idempotenta $e \in R$. Z twierdzenia 10.2 istnieje minimalny ideał lewostronny J pierścienia R zawarty w I. Z twierdzenia 10.10 $J = Rf$ dla pewnego idempotenta $f \in I$. Ze stwierdzenia 9.12 $R = J \oplus K$ dla pewnego $K <_l R$. Zatem z lematu 10.1, $I = J \oplus (I \cap K)$. Ponadto $I \cap K \neq \{0\}$, bo I nie jest minimalny. Stąd $I \cap K \subset I$, więc z minimalności I w rodzinie $\mathcal{M}$ mamy, że $I \cap K \notin \mathcal{M}$. Zatem $I \cap K = I_1 \oplus \ldots \oplus I_s$ dla pewnych minimalnych ideałów lewostronnych $I_1, \ldots, I_s$ pierścienia R. Stąd $I = J \oplus I_1 \oplus \ldots \oplus I_s$ i mamy sprzeczność. □

Twierdzenie 10.19. *Pierścień półpierwszy R jest lewostronnie artinowski wtedy i tylko wtedy, gdy jest skończoną sumą prostą ideałów $I_1, \ldots, I_s$ będących prostymi pierścieniami lewostronnie artinowskimi z jedynką.*

DOWÓD. Załóżmy, że R jest lewostronnie artinowski. Wtedy z twierdzenia 10.17 R jest skończoną sumą prostą ideałów $I_1, \ldots, I_s$ będących pierścieniami prostymi. Ze stwierdzenia 10.16 każdy z pierścieni $I_1, \ldots, I_s$ jest lewostronnie artinowski. Ponadto z twierdzenia 10.14 każde I_k ma jedynkę dla $k = 1, \ldots, s$.

Na odwrót, załóżmy, że pierścień półpierwszy R jest skończoną sumą prostą ideałów $I_1, \ldots, I_s$, z których każdy jest pierścieniem lewostronnie artinowskim. Z zadania 3 z rozdziału 9 wynika zatem, że $R \cong I_1 \times \ldots \times I_s$. Ale z twierdzenia 10.8 pierścień $I_1 \times \ldots \times I_s$ jest lewostronnie artinowski, więc pierścień R też jest lewostronnie artinowski. □

Wykład 11

Struktura artinowskich pierścieni półpierwszych

11.1 Jednostronne ideały artinowskie

Twierdzenie 11.1. *Niech e będzie idempotentem pierścienia półpierwszego R. Wówczas następujące warunki są równoważne:*
(i) Re jest minimalnym ideałem lewostronnym pierścienia R,
(ii) eRe jest pierścieniem z dzieleniem,
(iii) eR jest minimalnym ideałem prawostronnym pierścienia R.

Dowód. $(i) \Rightarrow (ii)$. Z założenia wynika, że $e \neq 0$. Ponadto $e = e^2$, więc $e^2 = e^3$ i $e = e^3 \in eRe$, skąd $eRe \neq \{0\}$ i e jest jedynką pierścienia eRe. Weźmy dowolne $a \in R$ takie, że $eae \neq 0$. Wtedy $eae = e^2ae \in Reae$, więc $Reae \neq \{0\}$. Ale $Reae <_l R$ i $Reae \subseteq Re$, więc z minimalności Re, $Reae = Re$. Istnieje zatem $b \in R$ takie, że $e = e^2 = beae$, czyli $e = e^2 = ebeae = (ebe)(eae)$. Stąd $ebe \neq 0$ i istnieje $x \in R$ taki, że $(exe)(ebe) = e$. Zatem $exe = (exe)e = (exe)[(ebe)(eae)] = [(exe)(ebe)](eae) = e(eae) = eae$, czyli $(eae)(ebe) = (ebe)(eae) = e$, a więc $eae \in (eRe)^*$ i eRe jest pierścieniem z dzieleniem.

$(ii) \Rightarrow (i)$. Z założenia wynika, że $eRe \neq \{0\}$, więc $e \neq 0$. Ale $e = e^2 \in Re$, więc $Re \neq \{0\}$. Weźmy dowolny niezerowy ideał lewostronny L pierścienia R zawarty w Re i wybierzmy $a \in R$ takie, że $0 \neq ae \in L$. Ponieważ pierścień R jest półpierwszy, więc $aeRae \neq \{0\}$. Zatem istnieje $b \in R$ takie, że $aebae \neq 0$, skąd $ebae \neq 0$. Ale eRe jest pierścieniem z dzieleniem, więc istnieje $c \in R$ takie, że $(ece)(ebae) = e$. Stąd $e \in L$ i wobec tego $Re \subseteq L$. Ale $L \subseteq Re$, więc $L = Re$ i wobec tego Re jest minimalnym ideałem lewostronnym pierścienia R.

$(iii) \Rightarrow (ii)$. Z założenia wynika, że $e \neq 0$. Ponadto $e = e^2$, więc $e^2 = e^3$ i $e = e^3 \in eRe$, skąd $eRe \neq \{0\}$ i e jest jedynką pierścienia eRe. Weźmy dowolne $a \in R$ takie, że $eae \neq 0$. Wtedy $eae = eae^2 \in eaeR$, więc $eaeR \neq \{0\}$. Ale $eaeR <_r R$ i $eaeR \subseteq eR$, więc z minimalności eR, $eaeR = eR$.

Istnieje zatem $b \in R$ takie, że $e = e^2 = eaeb$, czyli $e = e^2 = eaebe = (eae)(ebe)$. Stąd $ebe \neq 0$ i istnieje $x \in R$ taki, że $(ebe)(exe) = e$. Zatem $exe = e(exe) = [(eae)(ebe)](exe) = (eae)[(ebe)(exe)] = (eae)e = eae$, czyli $(eae)(ebe) = (ebe)(eae) = e$, a więc $eae \in (eRe)^*$ i eRe jest pierścieniem z dzieleniem.

$(ii) \Rightarrow (iii)$. Z założenia wynika, że $eRe \neq \{0\}$, więc $e \neq 0$. Ale $e = e^2 \in eR$, więc $eR \neq \{0\}$. Weźmy dowolny niezerowy ideał prawostronny P pierścienia R zawarty w eR i wybierzmy $a \in R$ takie, że $0 \neq ea \in P$. Ponieważ pierścień R jest półpierwszy, więc $eaRea \neq \{0\}$. Zatem istnieje $b \in R$ takie, że $eabea \neq 0$, skąd $eabe \neq 0$. Ale eRe jest pierścieniem z dzieleniem, więc istnieje $c \in R$ takie, że $(eabe)(ece) = e$. Stąd $e \in P$ i wobec tego $eR \subseteq P$. Ale $P \subseteq eR$, więc $P = eR$ i wobec tego eR jest minimalnym ideałem prawostronnym pierścienia R. □

Definicja 11.2. Lewostronnym (prawostronnym) *ideałem artinowskim* pierścienia R nazywamy każdy taki ideał lewostrony (prawostronny) $A \subseteq R$, że dowolny zstępujący ciąg $A \supseteq A_1 \supseteq A_2 \supseteq \ldots$ ideałów lewostronnych (prawostronnych) pierścienia R stabilizuje się.

Przykład 11.3. Każdy minimalny ideał lewostronny (prawostronny) pierścienia R jest lewostronnym (prawostronnym) ideałem artinowskim tego pierścienia.

Lemat 11.4. *Jeżeli A i B są lewostronnymi (prawostronnymi) ideałami artinowskimi pierścienia R, to $A + B$ też jest lewostronnym (prawostronym) ideałem artinowskim tego pierścienia.*

DOWÓD. Niech C będzie ideałem lewostronnym (prawostronnym) pierścienia R zawartym w $A+B$. Określamy $C' = \{b \in B : a+b \in C \text{ dla pewnego } a \in A\}$. Wtedy $0 \in C'$, bo $0 \in A$, $0 \in B$ i $0 + 0 = 0 \in C$. Weźmy dowolne $r \in R$, $c_1, c_2 \in C'$. Wtedy $c_1, c_2 \in B$ oraz istnieją $a_1, a_2 \in A$ takie, że $a_1 + c_1 \in C$ i $a_2 + c_2 \in C$. Stąd $(a_1 - a_2) + (c_1 - c_2) = (a_1 + c_1) - (a_2 + c_2) \in C$, a ponieważ $a_1 - a_2 \in A$ i $c_1 - c_2 \in B$,więc $c_1 - c_2 \in C'$. Ponadto $ra_1 \in A$ $(a_1 r \in A)$, $rc_1 \in B$ $(b_1 r \in B)$, $ra_1 + rc_1 = r(a_1 + c_1) \in C$ $(a_1 r + c_1 r = (a_1 + c_1)r \in C)$, więc $rc_1 \in C'$ $(c_1 r \in C')$. Zatem $C' <_l R$ $(C' <_r R)$. Teraz pokażemy, że $C' + A = C + A$. Weźmy dowolne $x \in C'$, $a \in A$. Wtedy $x \in B$ i istnieje $a_1 \in A$ takie, że $x+a_1 \in C$. Ale $x+a = (x+a_1)+(a-a_1)$, więc $x+a \in C+A$. Zatem $C' + A \subseteq C + A$. Weźmy dowolne $y \in C, a \in A$. Wtedy $y \in A + B$, więc istnieją $a_1 \in A$ oraz $b \in B$ takie, że $y = a_1 + b$. Stąd $b \in C'$ oraz $y+a = b+(a_1+a) \in C'+A$. Zatem $C+A \subseteq C'+A$ i ostatecznie $C'+A = C+A$.

Weźmy teraz dowolny zstępujący ciąg $A + B \supseteq C_1 \supseteq C_2 \supseteq \ldots$ ideałów lewostronnych (prawostronnych) pierścienia R. Wtedy $C_1' \supseteq C_2' \supseteq \ldots$ jest zstępującym ciągiem ideałów lewostronnych (prawostronnych) pierścienia R zawartych w B. Zatem istnieje $s \in \mathbb{N}$ takie, że $C_s' = C_n'$ dla wszystkich $n \geqslant s$. Stąd $C_s + A = C_n + A$ dla wszystkich $n \geqslant s$.

Ponadto $C_1 \cap A \supseteq C_2 \cap A \supseteq \ldots$ jest zstępującym ciągiem ideałów lewostronnych (prawostronnych) pierścienia R zawartych w A, więc istnieje $r \in \mathbb{N}$ takie, że $C_r \cap A = C_n \cap A$ dla wszystkich $n \geqslant r$. Niech $t = r+s$. Wtedy dla wszystkich $n \geqslant t$ mamy, że $C_t + A = C_n + A$ i $C_t \cap A = C_n \cap A$. Z lematu 10.1 dla wszystkich $n \geqslant t$: $C_t = C_t \cap (C_t + A) = C_t \cap (C_n + A) = C_n + (C_t \cap A) = C_n + (C_n \cap A) = C_n$. Zatem ciąg $C_1 \supseteq C_2 \supseteq \ldots$ stabilizuje się i $A + B$ jest lewostronnym (prawostronnym) ideałem artinowskim pierścienia R. □

Z lematu 11.4 przez prosta indukcję mamy następujące

Stwierdzenie 11.5. *Suma algebraiczna skończonej liczby lewostronnych (prawostronnych) ideałów artinowskich pierścienia R jest lewostronnym (prawostronnym) ideałem artinowskim tego pierścienia.*

Twierdzenie 11.6. *Dla pierścienia półpierwszego R następujące warunki są równoważne:*

(i) R jest pierścieniem lewostronnie (prawostronnie) artinowskim,

(ii) R jest sumą prostą skończonej liczby minimalnych ideałów lewostronnych (prawostronnych),

(iii) R jest sumą algebraiczną skończonej liczby minimalnych ideałów lewostronnych (prawostronnych).

DOWÓD. Implikacja $(i) \Rightarrow (ii)$ wynika od razu z twierdzenia 10.18. Implikacja $(ii) \Rightarrow (iii)$ jest oczywista. Dla dowodu implikacji $(iii) \Rightarrow (i)$, niech R będzie sumą algebraiczną minimalnych ideałów lewostronnych (prawostronnych) $A_1, \ldots, A_n$. Ponieważ każdy z tych ideałów jest lewostronnie (prawostronnie) artinowski, więc ze stwierdzenia 11.5 R jest lewostronnym (prawostronnym) ideałem artinowskim, a więc z twierdzenia 10.2 (10.3) R jest pierścieniem lewostronnie (prawostronnie) artinowskim. □

Przykład 11.7. Pokażemy, że dla dowolnego pierścienia z dzieleniem D i dla dowolnego $n \in \mathbb{N}$ pierścień macierzy $R = M_n(D)$ jest lewostronnie artinowski. Dla $i = 1, \ldots, n$ E_{ii} jest idempotentem pierścienia R oraz $E_{ii}RE_{ii} = DE_{ii} \cong D$, czyli $E_{ii}RE_{ii}$ jest pierścieniem z dzieleniem. Zatem z twierdzenia 11.1 RE_{ii} jest minimalnym ideałem lewostronnym pierścienia R dla każdego $i = 1, \ldots, n$. Ponadto, jak łatwo zauważyć, $R = (RE_{11}) \oplus \ldots \oplus (RE_{nn})$ i jak wiemy, R jest pierścieniem prostym z jedynką. Zatem R jest pierścieniem pierwszym i z twierdzenia 11.6 pierścień R jest lewostronnie artinowski.

Twierdzenie 11.8. *Dla pierścienia półpierwszego R następujące warunki są równoważne:*

(i) R jest lewostronnie artinowski,

(ii) R ma jedynkę i istnieją idempotenty $e_1, \ldots, e_n \in R$ takie, że $e_1 + \ldots + e_n = 1$, $e_i e_j = 0$ dla wszystkich $i \neq j$ oraz $e_i R e_i$ jest pierścieniem z dzieleniem dla $i = 1, \ldots, n$,

(iii) R jest prawostronnie artinowski.

DOWÓD. $(i) \Rightarrow (ii)$. Z twierdzenia 10.18 istnieją minimalne ideały lewostronne $L_1, \ldots, L_n$ takie, że $R = L_1 \oplus \ldots \oplus L_n$. Ponadto z twierdzenia 10.14 R posiada jedynkę. Zatem istnieją $e_i \in L_i$ dla $i = 1, \ldots, n$ takie, że $1 = e_1 + \ldots + e_n$. Weźmy dowolne $x \in L_i$, $i = 1, \ldots, n$. Wtedy $x = x \cdot 1 = x(e_1 + \ldots + x_n) = xe_1 + \ldots + xe_i + \ldots + xe_n$ oraz $xe_j \in L_j$ dla $j = 1, \ldots, n$. Zatem $0 = xe_1 + \ldots + (xe_i - x) + \ldots + xe_n$ i ze stwierdzenia 9.3, $xe_j = 0$ dla wszystkich $j \neq i$ oraz $x = xe_i$. W szczególności $e_i = e_i^2$ oraz $L_i = Re_i$ dla $i = 1, \ldots, n$. Ponadto mamy stąd, że $e_j e_i = 0$ dla wszystkich $i \neq j$. Z twierdzenia 11.1 wynika, że $e_i R e_i$ jest pierścieniem z dzieleniem dla $i = 1, \ldots, n$.

$(ii) \Rightarrow (i)$. Z twierdzenia 11.1 Re_i jest minimalnym ideałem lewostronnym. Weźmy dowolne $a \in R$. Wtedy $a = a \cdot 1 = a(e_1 + \ldots + e_n) = ae_1 + \ldots + ae_n \in Re_1 + \ldots + Re_n$. Zatem $R = Re_1 + \ldots + Re_n$ i z twierdzenia 11.6 pierścień R jest lewostronnie artinowski.

$(iii) \Rightarrow (ii)$. Z twierdzenia 10.18 istnieją minimalne ideały prawostronne $P_1, \ldots, P_n$ takie, że $R = P_1 \oplus \ldots \oplus P_n$. Ponadto z twierdzenia 10.14 R posiada jedynkę. Zatem istnieją $e_i \in P_i$ dla $i = 1, \ldots, n$ takie, że $1 = e_1 + \ldots + e_n$. Weźmy dowolne $x \in P_i$, $i = 1, \ldots, n$. Wtedy $x = 1 \cdot x = (e_1 + \ldots + x_n)x = e_1 x + \ldots + e_i x + \ldots + e_n x$ oraz $e_j x \in P_j$ dla $j = 1, \ldots, n$. Zatem $0 = e_1 x + \ldots + (e_i x - x) + \ldots + e_n x$ i ze stwierdzenia 9.3 $e_j x = 0$ dla wszystkich $j \neq i$ oraz $x = e_i x$. W szczególności $e_i = e_i^2$ oraz $P_i = e_i R$ dla $i = 1, \ldots, n$. Ponadto mamy stąd, że $e_j e_i = 0$ dla wszystkich $i \neq j$. Z twierdzenia 11.1 wynika, że $e_i R e_i$ jest pierścieniem z dzieleniem dla $i = 1, \ldots, n$.

$(ii) \Rightarrow (iii)$. Z twierdzenia 11.1 $e_i R$ jest minimalnym ideałem prawostronnym. Weźmy dowolne $a \in R$. Wtedy $a = 1 \cdot a = (e_1 + \ldots + e_n)a = e_1 a + \ldots + e_n a \in e_1 R + \ldots + e_n R$. Zatem $R = e_1 R + \ldots + e_n R$ i z twierdzenia 11.6 pierścień R jest prawostronnie artinowski. □

11.2 Twierdzenie Wedderburna-Artina

Lemat 11.9. *Niech R będzie pierścieniem z jedynką posiadającym idempotenty $e_1, \ldots, e_n$ takie, że $e_1 + \ldots + e_n = 1$ oraz $e_i e_j = 0$ dla wszystkich $i \neq j$. Wówczas:*

(i) $R^+ = \bigoplus_{i,j=1}^{n} (e_i R e_j)^+$, *przy czym dla każdego* $a \in R$: $a = \sum_{i,j=1}^{n} e_i a e_j$,

(ii) odwzorowanie $\varphi\colon R \to M_n(R)$ *dane wzorem* $\varphi(a) = [e_i a e_j]_{i,j=1,\ldots,n}$ *jest zanurzeniem pierścieni i* $\varphi(R) = [e_i R e_j]_{i,j=1,\ldots,n}$.

DOWÓD. (i). Weźmy dowolne $a \in R$. Wtedy $a = 1 \cdot a \cdot 1 = (e_1 + \ldots + e_n)a(e_1 + \ldots + e_n) = \sum_{i,j=1}^{n} e_i a e_j$, skąd $R^+ = \sum_{i,j=1}^{n} (e_i R e_j)^+$. Weźmy dowolne $a_{ij} \in R$, $i, j = 1, \ldots, n$ takie, że $\sum_{i,j=1}^{n} e_i a_{ij} e_j = 0$. Ponieważ $e_1, \ldots, e_n$ są idempotentami oraz

$e_ie_j = 0$ dla wszystkich $i \neq j$, więc $0 = e_k\left(\sum_{i,j=1}^{n} e_ia_{ij}e_j\right)e_l = e_k^2a_{kl}e_l^2 = e_ka_{kl}e_l$ dla wszystkich $k, l = 1, \ldots, n$. Zatem ze stwierdzenia 9.3 $R^+ = \bigoplus_{i,j=1}^{n} (e_iRe_j)^+$.

(ii). Weźmy dowolne $a, b \in R$. Wtedy na mocy (i), $a = \sum_{i,j=1}^{n} e_iae_j$ oraz $b = \sum_{i,j=1}^{n} e_ibe_j$. Zatem $a + b = \sum_{i,j=1}^{n} e_i(a+b)e_j$ i wobec tego $\varphi(a+b) = [e_i(a+b)e_j]_{i,j=1,\ldots,n} = [e_iae_j]_{i,j=1,\ldots,n} + [e_ibe_j]_{i,j=1,\ldots,n} = \varphi(a) + \varphi(b)$. Stąd oraz z (i) mamy, że φ jest zanurzeniem grup addytywnych. Ponadto $e_1, \ldots, e_n$ są idempotentami oraz $e_ie_j = 0$ dla wszystkich $i \neq j$, więc na mocy (i) dla dowolnych $i, j = 1, \ldots, n$, $e_ia = \sum_{k=1}^{n} e_iae_k$, $be_j = \sum_{k=1}^{n} e_kbe_j$ oraz $e_iabe_j = \sum_{k=1}^{n} e_iae_kbe_j$. Z (i) mamy, że $ab = \sum_{i,j=1}^{n} e_iabe_j$, więc $\varphi(ab) = [e_iabe_j]_{i,j=1,\ldots,n}$. Stąd $[\varphi(a)\cdot\varphi(b)]_{ij} = \sum_{k=1}^{n} [\varphi(a)]_{ik}[\varphi(b)]_{kj} = \sum_{k=1}^{n} (e_iae_k)(e_kbe_j) = e_iabe_j = [\varphi(ab)]_{ij}$ dla wszystkich $i, j = 1, \ldots, n$. Zatem $\varphi(ab) = \varphi(a)\cdot\varphi(b)$ i φ jest zanurzeniem pierścieni. Wprost z określenia φ otrzymujemy, że $\varphi(R) \subseteq [e_iRe_j]_{i,j=1,\ldots,n}$. Weźmy teraz dowolne $a_{ij} \in R$, $i, j = 1, \ldots, n$ i niech $a = \sum_{i,j=1}^{n} e_ia_{ij}e_j$. Wtedy na mocy (i) oraz stwierdzenia 9.3, $e_ia_{ij}e_j = e_iae_j$ dla wszystkich $i, j = 1, \ldots, n$, skąd $\varphi(a) = [e_ia_{ij}e_j]_{i,j=1,\ldots,n}$. Zatem $\varphi(R) = [e_iRe_j]_{i,j=1,\ldots,n}$. □

Lemat 11.10. *Niech e, f będą idempotentami pierścienia pierwszego R takimi, że Re i Rf są minimalnymi ideałami lewostronnymi . Wówczas istnieją niezerowe $a \in eRf$ i $b \in fRe$ takie, że $ab = e$ i $ba = f$.*

DOWÓD. Z założenia mamy, że $Re \neq \{0\}$ i $Rf \neq \{0\}$, więc $e \neq 0$ i $f \neq 0$. Ale pierścień R jest pierwszy, więc $eRf \neq \{0\}$. Istnieje zatem niezerowe $a \in eRf$. Wtedy $a = ea = af$, więc $Ra \subseteq Rf$ i $a \in Ra$, skąd $Ra \neq \{0\}$ i z minimalności Rf, $Ra = Rf$. Zatem istnieje $x \in R$ takie, że $xa = f$. Stąd $(fxe)a = f$, więc $ba = f$ dla $b = fxe \in fRe$, przy czym $b = fb = be$ oraz $b \neq 0$. Zatem $ab \in eRe$ i $aba = a(ba) = af = a$, skąd $ab \neq 0$ i $(ab)^2 = (aba)b = ab$. Ale z twierdzenia 11.1 eRe jest pierścieniem z dzieleniem i $ab \neq 0$ oraz $ab = (ab)^2$, więc ab jest jedynką pierścienia eRe, czyli $ab = e$. □

Twierdzenie 11.11. *Pierwszy pierścień R jest lewostronnie artinowski wtedy i tylko wtedy, gdy istnieje pierścień D z dzieleniem i $n \in \mathbb{N}$ takie, że $R \cong M_n(D)$.*

DOWÓD. Z przykładu 11.7 wynika, że dla dowolnego pierścienia D z dzieleniem i dla dowolnego $n \in \mathbb{N}$ pierścień $M_n(D)$ jest pierwszy i lewostronnie artinowski.

Na odwrót. Niech R będzie pierwszym pierścieniem lewostronnie artinowskim. Na mocy twierdzenia 11.8 R jest pierścieniem z jedynką i istnieją idempotenty $e_1 = e, \ldots, e_n \in R$ takie, że $e_1 + \ldots + e_n = 1$, $e_i e_j = 0$ dla wszystkich $i \neq j$ oraz $e_i R e_i$ jest pierścieniem z dzieleniem dla $i = 1, \ldots, n$. Z twierdzenia 11.1, Re_i jest minimalnym ideałem lewostronnym dla $i = 1, \ldots, n$. Z lematu 11.10 istnieją zatem $a_i \in eRe_i$ oraz $b_i \in e_i Re$ takie, że $a_i b_i = e$ oraz $b_i a_i = e_i$ dla wszystkich $i = 1, \ldots, n$.

Dla dowolnych $i, j = 1, \ldots, n$ rozważmy przekształcenia $\alpha_{ij} \colon eRe \to e_i R e_j$ oraz $\beta_{ij} \colon e_i R e_j \to eRe$ dane wzorami:

$$\alpha_{ij}(x) = b_i x a_j \text{ oraz } \beta_{ij}(y) = a_i y b_j.$$

Jest jasne, że α i β są homomorfizmami grup addytywnych. Ponadto dla dowolnego $x \in eRe$: $(\beta_{ij} \circ \alpha_{ij})(x) = \beta_{ij}(b_i x a_j) = a_i b_i x a_j b_j = exe = x$ oraz dla dowolnego $y \in e_i R e_j$: $(\alpha_{ij} \circ \beta_{ij})(y) = \alpha_{ij}(a_i y b_j) = b_i a_i y b_j a_j = e_i y e_j = y$. Zatem przekształcenia α_{ij} i β_{ij} są wzajemnie odwrotne i wobec tego α_{ij} jest izomorfizmem grup addytywnych dla dowolnych $i, j = 1, \ldots, n$. W szczególności

$$b_i R a_j = e_i R e_j \text{ dla dowolnych } i, j = 1, \ldots, n. \tag{11.1}$$

Oznaczmy teraz $D = eRe$ i rozważmy odwzorowanie $\gamma \colon M_n(D) \to M_n(R)$ dane wzorem:

$$\gamma([x_{ij}]_{i,j=1,\ldots,n}) = [b_i x_{ij} a_j]_{i,j=1,\ldots,n}. \tag{11.2}$$

Ze wzorów (11.1) i (11.2) wynika, że $\gamma(M_n(D)) = [e_i R e_j]_{i,j=1,\ldots,n}$. Ponadto z własności przekształceń α_{ij} mamy, że przekształcenie γ jest różnowartościowe. Jest jasne, że γ jest homomorfizmem grup addytywnych. Na mocy lematu 11.9 wystarczy zatem wykazać, że $\gamma(A \cdot B) = \gamma(A) \cdot \gamma(B)$ dla dowolnych $A, B \in M_n(D)$. Weźmy dowolne $i, j = 1, \ldots, n$. Wtedy ze wzoru (11.2): $[\gamma(A \cdot B)]_{ij} = b_i [A \cdot B]_{ij} a_j = b_i \left(\sum_{k=1}^{n} [A]_{ik} [B]_{kj} \right) a_j = \sum_{k=1}^{n} b_i [A]_{ik} [B]_{kj} a_j$ oraz $[\gamma(A) \cdot \gamma(B)]_{ij} = \sum_{k=1}^{n} [\gamma(A)]_{ik} [\gamma(B)]_{kj} = \sum_{k=1}^{n} b_i [A]_{ik} a_k b_k [B]_{kj} a_j$. Ale $a_k b_k = e$ oraz $[A]_{ik}, [B]_{kj} \in eRe$, więc $[A]_{ik} a_k b_k [B]_{kj} = [A]_{ik} [B]_{kj}$ dla $k = 1, \ldots, n$, skąd $[\gamma(A) \cdot \gamma(B)]_{ij} = \sum_{k=1}^{n} b_i [A]_{ik} [B]_{kj} a_j$, czyli $[\gamma(A \cdot B)]_{ij} = [\gamma(A) \cdot \gamma(B)]_{ij}$ dla wszystkich $i, j = 1, \ldots, n$. Zatem $\gamma(A \cdot B) = \gamma(A) \cdot \gamma(B)$. □

Twierdzenie 11.12 (Wedderburna-Artina)**.** *Pierścień półpierwszy R jest lewostronnie artinowski wtedy i tylko wtedy, gdy istnieją pierścienie z dzieleniem $D_1, \ldots, D_s$ oraz $n_1, \ldots, n_s \in \mathbb{N}$ takie, że $R \cong M_{n_1}(D_1) \times \ldots \times M_{n_s}(D_s)$.*

DOWÓD. Implikacja $\Leftarrow$ wynika od razu z zadania 14 z rozdziału 5, z twierdzenia 10.8 i z przykładu 11.7.

Dla dowodu implikacji $\Rightarrow$ zauważmy, że na mocy twierdzenia 10.19, istnieją ideały $I_1, \ldots, I_s$ pierścienia R będące prostymi pierścieniami lewostronnie

artinowskimi i takie, że $R = I_1 \oplus \ldots \oplus I_s$. Ponadto z twierdzenia 10.13 pierścień I_k ma jedynkę dla $k = 1, \ldots, s$. Zatem I_k jest pierścieniem pierwszym dla każdego $k = 1, \ldots, s$. Z zadania 3 z rozdziału 9, $R \cong I_1 \times \ldots \times I_s$. Ponadto z twierdzenia 11.11 dla każdego $k = 1, \ldots, s$ istnieją: $n_k \in \mathbb{N}$ oraz pierścień z dzieleniem D_k takie, że $I_k \cong M_{n_k}(D_k)$. Stąd $R \cong M_{n_1}(D_1) \times \ldots \times M_{n_s}(D_s)$. $\square$

Wykład 12

Skończone pierścienie z dzieleniem

12.1 Wielomiany podziału koła

Definicja 12.1. **n-tym wielomianem podziału koła** nazywany unormowany wielomian $F_n \in \mathbb{C}[x]$, najniższego stopnia, którego pierwiastkami są wszystkie zespolone pierwiastki pierwotne stopnia n z jedynki.

Przykład 12.2. Wprost z definicji mamy, że:

$$F_1 = x - 1,\ F_2 = x + 1,\ F_3 = x^2 + x + 1.$$

Dla $n \geqslant 3$:

$$F_n = (x - \omega_1) \cdot (x - \omega_2) \cdot \ldots \cdot (x - \omega_m),$$

gdzie $m = \varphi(n)$, zaś $\omega_1, \omega_2, \ldots, \omega_m$ są pierwiastkami pierwotnymi z jedynki stopnia n, tzn.

$$\omega_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n},$$

dla $k = 0, 1, \ldots, n-1$, $(k, n) = 1$.
W szczególności $st(F_n) = \varphi(n)$.

Fakt 12.3. *Jeżeli ω jest pierwiastkiem pierwotnym z jedynki stopnia $n \geqslant 3$, to $1, \omega, \omega^2, \ldots, \omega^{n-1}$ są wszystkimi pierwiastkami n-tego stopnia z jedynki. Ponadto $\left\{\omega^k : k = 0, 1, \ldots, n-1, (k, n) = 1\right\}$ jest zbiorem wszystkich pierwiastków pierwotnych z jedynki stopnia n.*

Fakt 12.4. *$\omega \in \mathbb{C}$ jest pierwiastkiem pierwotnym z jedynki stopnia $n \geqslant 3 \Leftrightarrow$ [$\omega^n = 1$ oraz $\omega^k \neq 1$ dla $k = 1, 2, \ldots n-1$] (tzn. $o(\omega) = n$ w grupie $\mathbb{C}^*$).*

Fakt 12.5. *Dla każdego $n \in \mathbb{N}$ jeżeli ω jest pierwiastkiem n-tego stopnia z jedynki, to ω jest pierwiastkiem pierwotnym z jedynki stopnia $m \in \mathbb{N}$ dla pewnego m dzielącego n.*

DOWÓD. Rzeczywiście, $\omega = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$ dla pewnego $k = 0, 1, \ldots, n-1$. Niech $d = (k, n)$. Wtedy istnieją $n_1 \in \mathbb{N}$, $k_1 \in \mathbb{N}_0$ względnie pierwsze i takie, że $k = d \cdot k_1$, $n = d \cdot n_1$. Zatem $\omega = \cos\frac{2dk_1\pi}{dn_1} + i\sin\frac{2dk_1\pi}{dn_1} = \cos\frac{2k_1\pi}{n_1} + i\sin\frac{2k_1\pi}{n_1}$, $(k_1, n_1) = 1$, więc ω jest pierwiastkiem pierwotnym z jedynki stopnia n_1 i $n_1|n$. Wystarczy zatem przyjąć $m = n_1$. □

Stwierdzenie 12.6. *Dla dowolnej liczby naturalnej n zachodzi wzór*

$$x^n - 1 = \prod_{\substack{d\in\mathbb{N}\\ d|n}} F_d.$$

DOWÓD. Ponieważ wielomiany F_d są unormowane i mają wszystkie pierwiastki jednokrotne oraz dla $k \neq l$ z faktu 12.4 wielomiany F_k i F_l nie mają wspólnych pierwiastków, więc wielomian $\prod_{d|n} F_d$ też jest unormowany i ma pierwiastki jednokrotne. Wystarczy zatem pokazać, że wielomiany $x^n - 1$ i $\prod_{d|n} F_d$ mają takie same zbiory pierwiastków.

Jeżeli ω jest pierwiastkiem wielomianu $\prod_{d|n} F_d$, to istnieje $d|n$ takie, że $F_d(\omega) = 0$, stąd $\omega^d = 1$ i $n = d \cdot k$ dla pewnego $k \in \mathbb{N}$, więc $(\omega^d)^k = 1$, stąd $\omega^n = 1$, czyli ω jest pierwiastkiem wielomianu $x^n - 1$.

Na odwrót, niech ω będzie pierwiastkiem wielomianu $x^n - 1$. Wtedy $\omega^n = 1$. Stąd z faktu 12.5 istnieje $d|n$ takie, że ω jest pierwiastkiem pierwotnym z jedynki stopnia d, czyli $F_d(\omega) = 0$. Zatem ω jest pierwiastkiem wielomianu $\prod_{d|n} F_d$. □

Wniosek 12.7. *Dla dowolnej liczby naturalnej n zachodzi wzór (Euler):*

$$n = \sum_{d|n} \varphi(d).$$

Stwierdzenie 12.8. *Dla każdego naturalnego n wszystkie współczynniki n-tego wielomianu podziału koła są liczbami całkowitymi, czyli $F_n \in \mathbb{Z}[x]$.*

DOWÓD. Indukcja względem n.

Dla $n = 1$ mamy, że $F_1 = x - 1 \in \mathbb{Z}[x]$.

Niech $n > 1$ będzie taką liczbą naturalną, że $F_k \in \mathbb{Z}[x]$ dla wszystkich liczb naturalnych $k < n$. Pokażemy, że wtedy $F_n \in \mathbb{Z}[x]$ co zakończy dowód. Ze stwierdzenia 12.6 mamy, że

$$x^n - 1 = \prod_{d|n} F_d = F_n \cdot \prod_{\substack{d|n\\ d<n}} F_d.$$

Ponadto z założenia indukcyjnego wielomian $F = \prod_{\substack{d|n\\ d<n}} F_d \in \mathbb{Z}[x]$ oraz F jest unormowany. Zatem

$$x^n - 1 = F_n \cdot F. \tag{12.1}$$

Z twierdzenia o dzieleniu z resztą w $\mathbb{Z}[x]$ mamy, że istnieją wielomiany Q, $R \in \mathbb{Z}[x]$ takie, że

$$x^n - 1 = Q \cdot F + R;\ st(R) < st(F). \tag{12.2}$$

Z (12.1) i (12.2) na podstawie twierdzenia o dzieleniu z resztą w $\mathbb{C}[x]$ mamy: $F_n = Q$, $0 = R$, skąd $F_n \in \mathbb{Z}[x]$. □

Przykład 12.9. Dla dowolnej liczby pierwszej p zachodzi wzór:

$$F_p = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1.$$

Rzeczywiście, ze stwierdzenia 12.6 mamy, że $x^p - 1 = \prod_{d|p} F_d = F_1 \cdot F_p = (x-1) \cdot F_p$, skąd $F_p = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \ldots + x + 1$.

Przykład 12.10. Dla liczb pierwszych p i naturalnych k obliczymy F_{p^k}. Dzielniki p^k: $1, p, p^2, \ldots, p^k$, więc ze stwierdzenia 12.6 mamy, że $x^{p^k} - 1 = F_1 \cdot F_p \cdot \ldots \cdot F_{p^k}$ oraz $x^{p^{k-1}} - 1 = F_1 \cdot F_p \cdot \ldots \cdot F_{p^{k-1}}$, więc $x^{p^k} - 1 = (x^{p^{k-1}} - 1) \cdot F_{p^k}$, skąd $F_{p^k} = \frac{x^{p^k}-1}{x^{p^{k-1}}-1} = F_p(x^{p^{k-1}})$ na mocy poprzedniego przykładu.

Fakt 12.11. *Jeżeli ω jest pierwiastkiem pierwotnym z jedynki stopnia l oraz $p \in \mathbb{Z}$, $(p, l) = 1$, to ω^p jest też pierwiastkiem pierwotnym z jedynki stopnia l.*

Stwierdzenie 12.12. *Jeżeli p jest liczbą pierwszą, zaś n jest liczbą naturalną niepodzielną przez p, to zachodzi wzór:*

$$F_{p \cdot n} = \frac{F_n(x^p)}{F_n}.$$

Dowód. Niech $f = F_{p \cdot n} \cdot F_n$, $g = F_n(x^p)$. Wtedy wielomiany f i g są unormowane i nie mają pierwiastków wielokrotnych, bo $g = (x^p - \omega_1)(x^p - \omega_2) \cdot \ldots \cdot (x^p - \omega_m)$, gdzie $\omega_1, \omega_2, \ldots, \omega_m$ są wszystkimi pierwiastkami pierwotnymi z jedynki stopnia n ($m = \varphi(n)$).

Pozostaje zatem wykazać, że wielomiany f i g mają takie same zbiory pierwiastków.

Niech $\omega \in \mathbb{C}$ będzie pierwiastkiem wielomianu g. Wtedy $\omega^p = \omega_k$ dla pewnego $k \leqslant m$. Zatem $(\omega^p)^n = \omega_k^n = 1$, czyli $\omega^{p \cdot n} = 1$.

Niech l będzie najmniejszą liczbą naturalną taką, że $\omega^l = 1$. Wtedy ω jest pierwiastkiem pierwotnym stopnia l z jedynki, czyli $F_l(\omega) = 0$ oraz $l | pn$.

Jeśli $p | l$, to $l = p \cdot s$ dla pewnego $s \in \mathbb{N}$ oraz $ps | pn$, czyli $s | n$, więc $s \leqslant n$. Ponadto $1 = \omega^l = \omega^{p \cdot s} = (\omega^p)^s = \omega_k^s$. Ponieważ ω_k jest pierwiastkiem pierwotnym z jedynki stopnia n, więc z faktu 12.5 $s = n$, czyli $l = pn$, stąd $F_{pn}(\omega) = 0$.

Jeśli $p \not| l$, to $(p, l) = 1$ oraz $l|p \cdot n$, więc z zasadniczego twierdzenia arytmetyki $l|n$, więc $l \leqslant n$. Ale $(p, l) = 1$, więc z faktu 12.11 ω^p jest pierwiastkiem pierwotnym z jedynki stopnia l.

Ale $\omega^p = \omega_k$ jest pierwiastkiem pierwotnym z jedynki stopnia n, czyli $l = n$. Ponadto $p \not| n$, więc $(p, n) = 1$ i z faktu 12.11 mamy, że ω jest pierwiastkiem pierwotnym z jedynki stopnia n. Stąd $F_n(\omega) = 0$ i $f(\omega) = 0$.

Niech $\omega \in \mathbb{C}$ będzie pierwiastkiem wielomianu f. Wtedy $F_{p\cdot n}(\omega) \cdot F_n(\omega) = 0$. Zatem $F_{p\cdot n}(\omega) = 0$ lub $F_n(\omega) = 0$.

Jeśli $F_{p\cdot n}(\omega) = 0$, to $\omega^{p\cdot n} = 1$ i ω jest pierwiastkiem pierwotnym z jedynki stopnia $p \cdot n$, więc ω^p jest pierwiastkiem pierwotnym z jedynki stopnia n, czyli $F_n(\omega^p) = 0$, więc $g(\omega) = 0$.

Jeśli zaś $F_n(\omega) = 0$, to ω jest pierwiastkiem pierwotnym z jedynki stopnia n i $(n, p) = 1$, więc z faktu 12.11 ω^p jest też pierwiastkiem pierwotnym z jedynki stopnia n, czyli $F_n(\omega^p) = 0$, a więc $g(\omega) = 0$. □

Stwierdzenie 12.13. *Niech p będzie liczbą pierwszą dzielącą liczbę naturalną n. Wtedy $F_{p\cdot n} = F_n(x^p)$.*

DOWÓD. Wystarczy wykazać, że wielomiany $F_{p\cdot n}$ i $F_n(x^p)$ mają takie same zbiory pierwiastków.

Niech $\omega \in \mathbb{C}$ będzie takie, że $F_{p\cdot n}(\omega) = 0$. Wtedy ω jest pierwiastkiem pierwotnym z jedynki stopnia $p \cdot n$. Stąd ω^p jest pierwiastkiem pierwotnym z jedynki stopnia n, czyli $F_n(\omega^p) = 0$.

Na odwrót załóżmy, że $\omega \in \mathbb{C}$ i $F_n(\omega^p) = 0$. Wtedy ω^p jest pierwiastkiem pierwotnym z jedynki stopnia n. Ale $n = p^s \cdot k$ dla pewnych $s, k \in \mathbb{N}$ takich, że $p \not| k$. Ponadto $(\omega^p)^n = 1$, więc $\omega^{p\,\cdot\,n} = 1$. Niech $t = o(\omega)$ w grupie $\mathbb{C}^*$. Wtedy $t|p \cdot n$. Jeśli $p \not| t$, to $(p, t) = 1$, stąd $t|n = p^s \cdot k$, czyli $t|k$. Stąd $\omega^k = 1$, czyli $1 = \omega^{k\cdot p} = (\omega^p)^k$ i $k < n$ (bo $s \geqslant 1$), więc mamy sprzeczność z tym, że $o(\omega^p) = n$. Zatem $p|t$ i $t = p \cdot l$ dla pewnego $l \in \mathbb{N}$. Wtedy $1 = \omega^{p\cdot l} = (\omega^p)^l$, więc ponieważ $o(\omega^p) = n$, to $n|l$. Ale $t = p \cdot l|n$, więc $l|n$, czyli $l = n$. Zatem $t = p \cdot n$, czyli $o(\omega) = p \cdot n$, więc $F_{p\cdot n}(\omega) = 0$. □

Twierdzenie 12.14. *Niech p będzie liczbą pierwszą, która nie dzieli liczby naturalnej m. Wtedy dla każdego naturalnego k:*

$$F_{p^k\cdot m} = \frac{F_m(x^{p^k})}{F_m(x^{p^{k-1}})}.$$

DOWÓD. Indukcja względem k. Dla $k = 1$ teza wynika ze stwierdzenia 12.12. Załóżmy, że teza zachodzi dla pewnego naturalnego k. Wtedy ze stwierdzenia 12.13, $F_{p^{k+1}\cdot m}(x) = F_{p^k\cdot m}(x^p)$. Ponadto z założenia indukcyjnego, $F_{p^k\cdot m}(x^p) = \frac{F_m((x^p)^{p^k})}{F_m((x^p)^{p^{k-1}})} = \frac{F_m(x^{p^{k+1}})}{F_m(x^{p^k})}$, więc $F_{p^{k+1}\cdot m} = \frac{F_m(x^{p^{k+1}})}{F_m(x^{p^k})}$. □

Stwierdzenie 12.15. *Jeżeli $n > 1$ jest liczbą naturalną nieparzystą, to*

$$F_{2n} = F_n(-x).$$

DOWÓD. Ponieważ $n > 1$ i n jest nieparzyste, więc z własności funkcji Eulera $\varphi(n)$ jest liczbą parzystą i wobec tego wielomian $F_n(-x)$ jest unormowany i nie posiada pierwiastków wielokrotnych. Wystarczy zatem pokazać, że wielomiany F_{2n} i $F_n(-x)$ mają ten takie same zbiory pierwiastków. Niech $\omega \in \mathbb{C}$ będzie pierwiastkiem wielomianu F_{2n}. Wtedy ω jest pierwiastkiem pierwotnym z jedynki stopnia $2n$, skąd $\omega^n \neq 1$ oraz $\omega^{2n} = 1$. Zatem $0 = (\omega^n - 1) \cdot (\omega^n + 1)$, więc $\omega^n = -1$, czyli $(-\omega)^n = 1$. Niech $l = o(-\omega)$ w grupie $\mathbb{C}^*$. Wtedy $(-\omega)^l = 1$, więc $\omega^{2l} = (-\omega)^{2l} = 1$, więc $l \geqslant n$. Ale $(-\omega)^n = 1$, więc $l \leqslant n$ i ostatecznie $l = n$ i wobec tego $(-\omega)$ jest pierwiastkiem pierwotnym z jedynki stopnia n. Stąd $F_n(-\omega) = 0$.

Na odwrót, weźmy dowolne $\omega \in \mathbb{C}$ takie, że $F_n(-\omega) = 0$. Wtedy $o(-\omega) = n$ oraz $o(-1) = 2$ w grupie $\mathbb{C}^*$ i liczba n jest nieparzysta, więc $o(\omega) = o(-1) \cdot o(-\omega) = 2n$, czyli ω jest pierwiastkiem pierwotnym z jedynki stopnia $2n$. Zatem $F_{2n}(\omega) = 0$. □

Zadanie (1)**.** Udowodnij, że dla dowolnej liczby naturalnej k i dla dowolnej nieparzystej liczby naturalnej $n > 1$ zachodzi wzór:

$$F_{2^k n} = F_n(-x^{2^k}).$$

Zadanie (2)**.** Udowodnij następujące wzory:

(a) $F_{15} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$,

(b) $F_{21} = x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1$,

(c) $F_{33} = x^{20} - x^{19} + x^{17} - x^{16} + x^{14} - x^{13} + x^{11} - x^{10} + x^9 - x^7 + x^6 - x^4 + x^3 - x + 1$,

(d) $F_{39} = x^{24} - x^{23} + x^{21} - x^{20} + x^{18} - x^{17} + x^{15} - x^{14} + x^{12} - x^{10} + x^9 - x^7 + x^6 - x^4 + x^3 - x + 1$,

(e) $F_{51} = x^{32} - x^{31} + x^{29} - x^{28} + x^{26} - x^{25} + x^{23} - x^{22} + x^{20} - x^{19} + x^{17} - x^{16} + x^{15} - x^{13} + x^{12} - x^{10} + x^9 - x^7 + x^6 - x^4 + x^3 - x + 1$,

(f) $F_{57} = x^{36} - x^{35} + x^{33} - x^{32} + x^{30} - x^{29} + x^{27} - x^{26} + x^{24} - x^{23} + x^{21} - x^{20} + x^{18} - x^{16} + x^{15} - x^{13} + x^{12} - x^{10} + x^9 - x^7 + x^6 - x^4 + x^3 - x + 1$,

(g) $F_{69} = x^{44} - x^{43} + x^{41} - x^{40} + x^{38} - x^{37} + x^{35} - x^{34} + x^{32} - x^{31} + x^{29} - x^{28} + x^{26} - x^{25} + x^{23} - x^{22} + x^{21} - x^{19} + x^{18} - x^{16} + x^{15} - x^{13} + x^{12} - x^{10} + x^9 - x^7 + x^6 - x^4 + x^3 - x + 1$,

(h) $F_{87} = x^{56} - x^{55} + x^{53} - x^{52} + x^{50} - x^{49} + x^{47} - x^{46} + x^{44} - x^{43} + x^{41} - x^{40} + x^{38} - x^{37} + x^{35} - x^{34} + x^{32} - x^{31} + x^{29} - x^{28} + x^{27} - x^{25} + x^{24} - x^{22} + x^{21} - x^{19} + x^{18} - x^{16} + x^{15} - x^{13} + x^{12} - x^{10} + x^9 - x^7 + x^6 - x^4 + x^3 - x + 1$,

(i) $F_{93} = x^{60} - x^{59} + x^{57} - x^{56} + x^{54} - x^{53} + x^{51} - x^{50} + x^{48} - x^{47} + x^{45} - x^{44} + x^{42} - x^{41} + x^{39} - x^{38} + x^{36} - x^{35} + x^{33} - x^{32} + x^{30} - x^{28} + x^{27} - x^{25} + x^{24} - x^{22} + x^{21} - x^{19} + x^{18} - x^{16} + x^{15} - x^{13} + x^{12} - x^{10} + x^9 - x^7 + x^6 - x^4 + x^3 - x + 1$,

(j) $F_{35} = x^{24} - x^{23} + x^{19} - x^{18} + x^{17} - x^{16} + x^{14} - x^{13} + x^{12} - x^{11} + x^{10} - x^8 + x^7 - x^6 + x^5 - x + 1$,

(k) $F_{55} = x^{40} - x^{39} + x^{35} - x^{34} + x^{30} - x^{28} + x^{25} - x^{23} + x^{20} - x^{17} + x^{15} - x^{12} + x^{10} - x^6 + x^5 - x + 1$,

(l) $F_{65} = x^{48} - x^{47} + x^{43} - x^{42} + x^{38} - x^{37} + x^{35} - x^{34} + x^{33} - x^{32} + x^{30} - x^{29} + x^{28} - x^{27} + x^{25} - x^{24} + x^{23} - x^{21} + x^{20} - x^{19} + x^{18} - x^{16} + x^{15} - x^{14} + x^{13} - x^{11} + x^{10} - x^6 + x^5 - x + 1$,

(m) $F_{85} = x^{64} - x^{63} + x^{59} - x^{58} + x^{54} - x^{53} + x^{49} - x^{48} + x^{47} - x^{46} + x^{44} - x^{43} + x^{42} - x^{41} + x^{39} - x^{38} + x^{37} - x^{36} + x^{34} - x^{33} + x^{32} - x^{31} + x^{30} - x^{28} + x^{27} - x^{26} + x^{25} - x^{23} + x^{22} - x^{21} + x^{20} - x^{18} + x^{17} - x^{16} + x^{15} - x^{11} + x^{10} - x^6 + x^5 - x + 1$,

(n) $F_{95} = x^{72} - x^{71} + x^{67} - x^{66} + x^{62} - x^{61} + x^{57} - x^{56} + x^{53} - x^{51} + x^{48} - x^{46} + x^{43} - x^{41} + x^{38} - x^{36} + x^{34} - x^{31} + x^{29} - x^{26} + x^{24} - x^{21} + x^{19} - x^{16} + x^{15} - x^{11} + x^{10} - x^6 + x^5 - x + 1$,

(o) $F_{77} = x^{60} - x^{59} + x^{53} - x^{52} + x^{49} - x^{48} + x^{46} - x^{45} + x^{42} - x^{41} + x^{39} - x^{37} + x^{35} - x^{34} + x^{32} - x^{30} + x^{28} - x^{26} + x^{25} - x^{23} + x^{21} - x^{19} + x^{18} - x^{15} + x^{14} - x^{12} + x^{11} - x^8 + x^7 - x + 1$,

(p) $F_{91} = x^{72} - x^{71} + x^{65} - x^{64} + x^{59} - x^{57} + x^{52} - x^{50} + x^{46} - x^{43} + x^{39} - x^{36} + x^{33} - x^{29} + x^{26} - x^{22} + x^{20} - x^{15} + x^{13} - x^8 + x^7 - x + 1$.

Zadanie (3)**.** Udowodnij, że $F_{105} = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} - x^9 - x^8 - 2x^7 - x^6 - x^5 + x^2 + x + 1$.

Stwierdzenie 12.16. *Jeśli q i $n \geqslant 2$ są liczbami naturalnymi, to*

$$|F_n(q)| > q - 1.$$

W szczególności dla $q > 1$ liczba $F_n(q)$ nie dzieli liczby $q - 1$.

DOWÓD. Ponieważ $n \geqslant 2$, więc 1 nie jest pierwiastkiem pierwotnym z 1 stopnia n, czyli $F_n(1) \neq 0$, a więc $|F_n(1)| > 0 = 1 - 1$ i teza zachodzi dla $q = 1$. Niech dalej $q > 1$. Oznaczmy $m = \varphi(n)$ i niech $\omega_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}, \omega_2, \ldots, \omega_m$ będą wszystkimi pierwiastkami pierwotnymi z 1 stopnia n. Wtedy

$$F_n = (x - \omega_1) \cdot (x - \omega_2) \cdot \ldots \cdot (x - \omega_m),$$

skąd

$$|F_n(q)| = |q - \omega_1| \cdot |q - \omega_2| \cdot \ldots \cdot |q - \omega_m|.$$

Ale z nierówności trójkąta dla $i = 2, \ldots, m$:

$$|q - \omega_i| \geqslant ||q| - |\omega_i|| = |q - 1| = q - 1 \geqslant 1,$$

więc $|F_n(q)| \geqslant |q - \omega_1| \geqslant re(q - \omega_1) = q - \cos\frac{2\pi}{n} > q - 1$, gdyż $\cos\frac{2\pi}{n} < 1$ dla wszystkich $n \geqslant 2$. Zatem $|F_n(q)| > q - 1$. Ponadto ze stwierdzenia 12.8, $F_n(q) \in \mathbb{Z}$, więc $F_n(q)$ nie dzieli liczby $q - 1$. □

Stwierdzenie 12.17. *Dla dowolnych liczb naturalnych d, q, n takich, że $q, n \geqslant 2$, $d|n$ oraz $d < n$ mamy, że*

$$F_n(q) | \tfrac{q^n - 1}{q^d - 1}.$$

DOWÓD. Ze stwierdzenia 12.6, $x^n - 1 = \prod_{l|n} F_l$ oraz $x^d - 1 = \prod_{l|d} F_l$. Zatem $x^n - 1 = F_n \cdot (x^d - 1) \cdot G$, gdzie G jest równe 1, jeśli nie istnieje $l < n$ takie, że $l > d$ oraz G jest iloczynem wszystkich wielomianów F_l dla $d < l < n$ takich, że $l|n$, w przeciwnym przypadku. Stąd $G \in \mathbb{Z}[x]$. Ponadto ze stwierdzenia 12.8, $F_n \in \mathbb{Z}[x]$, więc $F_n(q), G(q), \frac{q^n-1}{q^d-1} \in \mathbb{Z}$ oraz $\frac{q^n-1}{q^d-1} = F_n(q) \cdot G(q)$, czyli $F_n(q) | \frac{q^n-1}{q^d-1}$. □

12.2 Twierdzenie Wedderburna

Twierdzenie 12.18 (Wedderburna)**.** *Każdy skończony pierścień z dzieleniem jest ciałem.*

DOWÓD. Załóżmy, że tak nie jest i niech D będzie nieprzemiennym skończonym pierścieniem z dzieleniem, tzn. $D \neq Z(D)$. Niech $q = |Z(D)|$. Wtedy $q \in \mathbb{N}$ oraz $q > 1$, gdyż $0, 1 \in Z(D)$ i $0 \neq 1$, bo $D \neq \{0\}$. Zauważmy, że $Z(D)$ jest ciałem, gdyż dla dowolnego $a \in Z(D) \setminus \{0\}$ i dla dowolnego $x \in D$, $ax = xa$, skąd $a^{-1}axa^{-1} = a^{-1}xaa^{-1}$, czyli $xa^{-1} = a^{-1}x$, a więc $a^{-1} \in Z(D)$. Ponadto D jest w naturalny sposób przestrzenią liniowa nad ciałem $Z(D)$, gdy przyjmiemy działanie skalara $a \in Z(D)$ na wektor $x \in D$ jako $a \cdot x$. Niech n będzie wymiarem przestrzeni D nad ciałem $Z(D)$. Ponieważ $D \neq Z(D)$ i pierścień D jest skończony, więc $n \in \mathbb{N}$ i $n > 1$ oraz $|D| = q^n$. Ponieważ D jest pierścieniem z dzieleniem, więc $D^\star = D \setminus \{0\}$ jest grupą ze względu na mnożenie. Grupa $D^\star$ działa na zbiór D za pomocą automorfizmów wewnętrznych. Mianowicie dla $g \in D^\star$, $a \in D$ przyjmujemy, że

$$g \circ a = g \cdot a \cdot g^{-1}.$$

Rzeczywiście, $1 \circ a = 1 \cdot a \cdot 1^{-1} = a$ dla $a \in D$ oraz dla $g, h \in D^\star$, $a \in D$ mamy, że $g \circ (h \circ a) = g \cdot (h \circ a) \cdot g^{-1} = g(hah^{-1})g^{-1} = (gh)a(gh)^{-1} = (gh) \circ a$.

Ponieważ dla $a \in D$ jest $a \in Orb(a)$, więc $|Orb(a)| = 1 \Leftrightarrow Orb(a) = \{a\} \Leftrightarrow \forall_{g \in D^\star} g \circ a = a \Leftrightarrow \forall_{g \in D^\star} gag^{-1} = a \Leftrightarrow \forall_{g \in D^\star} ga = ag \Leftrightarrow \forall_{r \in D} ra = ar \Leftrightarrow a \in Z(D)$, czyli

$$\forall_{a \in D} |Orb(a)| = 1 \Leftrightarrow a \in Z(D).$$

Dla $a \in D$, $g \in D^\star$

$$g \in Stab(a) \Leftrightarrow gag^{-1} = a \Leftrightarrow ga = ag \Leftrightarrow g \in C_D(a) \setminus \{0\},$$

przy czym $C_D(a)$ jest podpierścieniem pierścienia D zawierającym $Z(D)$. Zatem $Z_D(a)$ jest podprzestrzenią przestrzeni liniowej D i wobec tego $|C_D(a)| = q^d$ dla pewnej liczby naturalnej $d \leqslant n$. Ponadto $Stab(a) = C_D(a) \setminus \{0\}$, więc $|Stab(a)| = q^d - 1$. Z algebry ogólnej II wiemy, że $Stab(a)$ jest podgrupą grupy D^*, skąd na mocy twierdzenia Lagrange'a, $q^d - 1 | q^n - 1$. Ale $q > 1$, więc z elementarnej teorii liczb, $d|n$. Niech teraz dodatkowo $a \notin Z(D)$. Wtedy $a \neq 0$, więc $a \in Stab(a)$ i $C_D(a) \neq D$, więc $Stab(a) \neq D^*$. Ale $|Stab(a)| = q^d - 1$

i $|D^*| = q^n - 1$, zatem $d < n$. Ze stwierdzenia 12.17 wynika, że $F_n(q)|\frac{q^n-1}{q^d-1}$. Ponadto z algebry ogólnej II, $\frac{q^n-1}{q^d-1} = |Orb(a)|$, czyli $F_n(q)||Orb(a)|$ dla wszystkich $a \in D \setminus Z(D)$. Dalej, ze wzoru orbit D jest sumą skończenie wielu parami rozłącznych orbit, z których dokładnie q jest jednoelementowych, a pozostałe mają liczbę elementów podzielną przez $F_n(q)$. Zatem $q^n = q + lF_n(q)$ dla pewnej liczby całkowitej l, skąd $q^n - 1 = (q-1) + lF_n(q)$. Ponadto ze stwierdzenia 12.17, $F_n(q)|q^n - 1$, więc $F_n(q)|q - 1$ wbrew stwierdzeniu 12.16. □

Wykład 13

Pierścienie zredukowane

13.1 Podstawowe własności pierścieni zredukowanych

Przypomnijmy, że **pierścieniem zredukowanym** nazywamy pierścień nie posiadający niezerowych elementów nilpotentnych.

Lemat 13.1. ***Charakteryzacja pierścieni zredukowanych****. Pierścień R jest zredukowany wtedy i tylko wtedy, gdy nie posiada elementu niezerowego a takiego, że $a^2 = 0$.*

Dowód. $''\Rightarrow''$. Oczywiste. $''\Leftarrow''$. Niech dla dowolnego $0 \neq a \in R$ zachodzi $a^2 \neq 0$. Załóżmy nie wprost, że pierścień R nie jest zredukowany. Wtedy istnieje element $0 \neq b \in R$ taki, że $b^n = 0$ oraz $b^{n-1} \neq 0$ dla pewnego $n = 3, 4, \ldots$. Oznaczmy przez $a = b^{n-1}$. Wtedy $a \neq 0$, skąd $a^2 \neq 0$. Ale $a^2 = (b^{n-1})^2 = b^{2n-2} = b^n \cdot b^{n-2} = 0 \cdot b^{n-2} = 0$, więc mamy sprzeczność. Zatem pierścień R jest zredukowany. □

Uwaga 13.2. *Każda dziedzina jest pierścieniem zredukowanym.*

Następne dwa lematy przedstawiają znane własności elementów pierścieni zredukowanych, które w literaturze nazywane są również "quasi - identycznościami".

Lemat 13.3. *Jeżeli R jest pierścieniem zredukowanym oraz $a_1, a_2 \in R$ są takie, że $a_1 \cdot a_2 = 0$, to także $a_2 \cdot a_1 = 0$.*

Dowód. Ponieważ $(a_2a_1)^2 = (a_2a_1) \cdot (a_2a_1) = a_2 \cdot (a_1a_2) \cdot a_1 = a_2 \cdot 0 \cdot a_1 = 0$, więc z lematu 13.1 mamy, że $a_2a_1 = 0$. □

Lemat 13.4. *Jeżeli R jest pierścieniem zredukowanym oraz $a_1, a_2 \in R$ są takie, że $a_1a_2 = 0$, to $a_1Ra_2 = 0$.*

DOWÓD. Dla dowolnego $b \in R$: $(a_1ba_2)^2 = a_1b(a_2a_1)ba_2 = a_1b \cdot 0 \cdot ba_2 = 0$ na mocy lematu 13.3, więc zgodnie z lematem 13.1 mamy $a_1ba_2 = 0$, bo R jest pierścieniem zredukowanym. Zatem $a_1Ra_2 = 0$. □

Lemat 13.5. *Niech R będzie pierścieniem zredukowanym. Dla każdego $n \in \mathbb{N}$, $n \geqslant 2$ i dla dowolnych $a_1, a_2, \ldots, a_n \in R$ zachodzi:*

$$a_1 \cdot a_2 \cdot \ldots \cdot a_n = 0 \Longrightarrow a_1Ra_2R \cdot \ldots \cdot a_{n-1}Ra_n = 0.$$

DOWÓD. Zastosujemy indukcję względem n. Dla $n = 2$ teza wynika bezpośrednio z lematu 13.4.

Niech dalej $n > 2$ i załóżmy, że teza zachodzi dla liczby $n - 1$. Weźmy dowolne $a_1, \ldots, a_n$ takie, że $a_1 \cdot \ldots \cdot a_n = 0$ oraz dowolne $r_1, \ldots, r_{n-1} \in R$. Ponieważ $(a_1 \cdot \ldots \cdot a_{n-1}) \cdot a_n = 0$. Wtedy z lematu 13.4 mamy, że $(a_1 \cdot \ldots \cdot a_{n-1}) \cdot r_{n-1} \cdot a_n = 0$, czyli $a_1 \cdot \ldots \cdot a_{n-2} \cdot (a_{n-1} \cdot r_{n-1} \cdot a_n) = 0$. Zatem z założenia indukcyjnego $a_1 \cdot r_1 \cdot \ldots \cdot a_{n-2} \cdot r_{n-2} \cdot a_{n-1} \cdot r_{n-1} \cdot a_n = 0$. Stąd i z dowolności wyboru $r_1, \ldots, r_{n-1} \in R$ mamy, że $a_1Ra_2R \cdot \ldots \cdot a_{n-1}Ra_n = 0$ dla dowolnego $n \in \mathbb{N}$. □

Lemat 13.6. *Niech R będzie pierścieniem zredukowanym. Dla każdego $n \in \mathbb{N}$, dla dowolnej permutacji $\sigma \in S_n$ i dla dowolnych $a_1, a_2, \ldots, a_n \in R$ zachodzi:*

$$a_1 \cdot a_2 \cdot \ldots \cdot a_n = 0 \Longrightarrow a_{\sigma(1)} \cdot a_{\sigma(2)} \cdot \ldots \cdot a_{\sigma(n)} = 0$$

DOWÓD. Dla $n = 1$ teza jest oczywista. Dla $n = 2$ teza wynika bezpośrednio z lematu 13.1.

Dla $n = 3$ załóżmy, że $a_1a_2a_3 = 0$. Stąd $a_1 \cdot (a_2a_3) = 0$, więc z lematu 13.3 otrzymujemy, że $a_2a_3a_1 = 0$, czyli dla permutacji $\sigma = (1, 2, 3)$ teza zachodzi. Ponadto z lematu 13.4 mamy, że $a_1a_3 \cdot (a_2a_3) = 0$ i ponownie korzystając z lematu 13.4 otrzymujemy $(a_1a_3a_2) \cdot a_1 \cdot a_3 = 0$. Stąd

$$(a_2a_1a_3)^2 = a_2 \cdot (a_1a_3a_2a_1a_3) = a_2 \cdot 0 = 0,$$

więc $a_2a_1a_3 = 0$, ponieważ pierścień R jest zredukowany. Zatem dla permutacji $\sigma = (1, 2)$ teza zachodzi. Ale permutacje $(1, 2)$ i $(1, 2, 3)$ generują S_3, więc $a_{\sigma(1)} \cdot a_{\sigma(2)} \cdot a_{\sigma(3)} = 0$ dla każdej permutacji $\sigma \in S_3$.

Dla $n > 3$ mamy, że grupa S_n jest generowana przez permutacje $\sigma = (1, 2)$ i $\tau = (1, 2, 3, \ldots, n)$. Wystarczy zatem pokazać, że jeżeli $a_1a_2a_3 \ldots a_n = 0$, to $a_2a_1a_3 \ldots a_n = 0$ oraz $a_2a_3 \ldots a_na_1 = 0$. Z lematu 13.3 mamy od razu, że jeżeli $a_1 \cdot (a_2a_3 \ldots a_n) = 0$, to $(a_2a_3 \ldots a_n) \cdot a_1 = a_2a_3 \ldots a_na_1 = 0$, więc teza zachodzi dla permutacji τ. Podstawmy chwilowo $a = a_3 \cdot \ldots \cdot a_n$. Zatem $a_1a_2a = 0$. Z dowodu dla $n = 3$ mamy więc, że $0 = a_2a_1a = a_2a_1a_3 \cdot \ldots \cdot a_n$, czyli teza zachodzi dla permutacji σ. Zatem teza zachodzi dla dowolnej permutacji z S_n. □

Definicja 13.7. Niech $\mathcal{W}$ będzie pewną własnością pierścieni. Powiemy, że własność $\mathcal{W}$ jest **zamknięta na rozszerzenia**, jeżeli dla dowolnego pierścienia R i dowolnego ideału I pierścienia R z faktu, że I oraz R/I mają własność $\mathcal{W}$ wynika, że R ma własność $\mathcal{W}$.

Wprost z definicji pierścienia zredukowanego mamy następujące

Stwierdzenie 13.8. *Każdy podpierścień, a więc też każdy ideał pierścienia zredukowanego, jest pierścieniem zredukowanym.*

Twierdzenie 13.9. *Niech I będzie dowolnym ideałem pierścienia R. Jeżeli pierścienie I oraz R/I są zredukowane, to R również jest zredukowany.*

Dowód. Niech $r \in R$ będzie takie, że $r^2 = 0$. Wówczas $(r + I)^2 = 0 + I$ w pierścieniu zredukowanym R/I, skąd $r + I = 0 + I$, czyli $r \in I$. Ale I jest pierścieniem zredukowanym, więc $r = 0$. Zatem z lematu 13.1 R jest pierścieniem zredukowanym. □

Przykład 13.10. Obraz homomorficzny pierścienia zredukowanego nie musi być pierścieniem zredukowanym. Rzeczywiście, np. pierścień $\mathbb{Z}_4$ jest obrazem homomorficznym dziedziny $\mathbb{Z}$, ale $\mathbb{Z}_4$ nie jest pierścieniem zredukowanym.

13.2 Twierdzenie Andrunakiewicza - Rjabuhina

Definicja 13.11. Powiemy, że $I \lhd R$ jest **ideałem zredukowanym** wtedy i tylko wtedy, gdy pierścień R/I jest zredukowany.

Przykład 13.12. Jeżeli R jest pierścieniem zredukowanym, to ideał I pierścienia R nie musi być ideałem zredukowanym. Rzeczywiście, rozważmy pierścień liczb całkowitych $\mathbb{Z}$ oraz jego ideał $I = (4)$. Pierścień $\mathbb{Z}$ jest zredukowany, ale $\mathbb{Z}/(4) \cong \mathbb{Z}_4$ nie jest pierścieniem zredukowanym, więc z definicji 13.11 ideał (4) nie jest zredukowany.

Przykład 13.13. Jeżeli I jest ideałem zredukowanym pierścienia R, to R nie musi być pierścieniem zredukowanym. Rzeczywiście, rozważmy niezerowy nil-pierścień R oraz pierścień z dołączoną jedynką R^1. Wtedy $R \lhd R^1$ oraz $R^1/R \cong \mathbb{Z}$. Zatem pierścień R^1/R jest zredukowany, więc z definicji 13.11 R jest ideałem zredukowanym pierścienia R^1. Ale pierścień R^1 nie jest zredukowany.

Uwaga 13.14. *Ideał I pierścienia R jest ideałem zredukowanym w pierścieniu R wtedy i tylko wtedy, gdy dla dowolnego elementu $a \in R$ zachodzi*

$$a^2 \in I \Longrightarrow a \in I.$$

DOWÓD. $''\Rightarrow''$. Weźmy dowolne $a \in R$ takie, że $a^2 \in I$. Wtedy $a^2 + I = (a+I)^2 = I$ i pierścień R/I jest zredukowany, więc $a + I = I$, czyli $a \in I$.
$''\Leftarrow''$. Weźmy dowolne $a \in R$ takie, że $(a+I)^2 = I$. Wtedy $a^2 \in I$, więc $a \in I$, skąd $a + I = I$. Zatem z lematu 13.1 pierścień R/I jest zredukowany, czyli zgodnie z definicją 13.11 ideał I jest zredukowany. □

Uwaga 13.15. *Jeżeli I jest ideałem zredukowanym pierścienia R, to dla dowolnych elementów $a, b \in R$, jeśli $ab \in I$ to $ba \in I$.*

DOWÓD. Wynika bezpośrednio z lematu 13.3 oraz standardowego rachunku na warstwach. □

Uwaga 13.16. *Jeżeli I jest ideałem zredukowanym pierścienia R, to dla dowolnych elementów $x_1, \ldots, x_n \in R$, jeżeli $x_1 \cdot \ldots \cdot x_n \in I$, to*

$$x_{\sigma(1)} \cdot x_{\sigma(2)} \cdot \ldots \cdot x_{\sigma(n)} \in I$$

dla dowolnej permutacji $\sigma \in S_n$.

DOWÓD. Wynika bezpośrednio z lematu 13.6 oraz ze standardowego rachunku na warstwach. □

Uwaga 13.17. *Przecięcie dowolnej niepustej rodziny ideałów zredukowanych jest ideałem zredukowanym.*

DOWÓD. Niech $\{I_t\}_{t\in T}$ będzie rodziną ideałów zredukowanych pierścienia R. Wtedy $J = \bigcap_{t\in T} I_t \lhd R$. Weźmy dowolne $a \in R$ takie, że $a^2 \in J$. Wtedy $a^2 \in I_t$ dla każdego $t \in T$ i z uwagi 13.14, $a \in I_t$ dla każdego $t \in T$, czyli $a \in J$. Zatem z uwagi 13.14 ideał J jest zredukowany. □

Uwaga 13.18. *Suma łańcucha ideałów zredukowanych jest ideałem zredukowanym.*

DOWÓD. Niech $\{I_t\}_{t\in T}$ będzie łańcuchem ideałów zredukowanych pierścienia R. Ze stwierdzenia 4.17 wiemy, że $J = \bigcup_{t\in T} I_t \lhd R$. Weźmy dowolne $a \in R$ takie, że $a^2 \in J$. Wtedy $a^2 \in I_t$ dla pewnego $t \in T$. Wówczas z uwagi 13.14, $a \in I_t$, czyli $a \in J$. Zatem ideał J jest zredukowany. □

Lemat 13.19. *Niech I będzie ideałem zredukowanym pierścienia R. Niech S będzie niepustym podzbiorem R oraz*

$$A = \{r \in R : rs \in I \text{ dla każdego } s \in S\}.$$

Wówczas A jest ideałem zredukowanym pierścienia R.

DOWÓD. Ponieważ $A = \{r \in R : rs \in I \text{ dla dowolnego } s \in S\} = \bigcap_{s\in S}\{r \in R : rs \in I\}$, więc na mocy uwagi 13.17 wystarczy udowodnić, że dla każdego $s \in S$, $A_s = \{r \in R : rs \in I\}$ jest ideałem zredukowanym pierścienia R.

Ponieważ $0 \in A_s$, gdyż $0 \cdot s \in I$, więc $A_s \neq \emptyset$.

Weźmy dowolne $a_1, a_2 \in A_s$. Wtedy $a_1 s \in I$, $a_2 s \in I$, stąd $(a_1 - a_2) \cdot s = a_1 s - a_2 s \in I$, czyli $a_1 - a_2 \in A_s$. Weźmy teraz dowolne $a \in A_s$ oraz $r \in R$. Wtedy $as \in I$, stąd $(ra) \cdot s = r \cdot (as) \in I$, czyli $ra \in A_s$. Ponadto z uwagi 13.15 mamy, że $sa \in I$ oraz $(sa) \cdot r = s \cdot (ar) \in I$. Więc znowu z uwagi 13.15 mamy, że $(ar) \cdot s \in I$, a stąd $ar \in A_s$. Zatem $A_s \lhd R$. Teraz pokażemy, że ideał A_s jest zredukowany. Niech $r \in R$ będzie takie, że $r^2 \in A_s$. Wtedy $r^2 s = r(rs) \in I$. Z uwagi 13.15 zachodzi $(rs)r \in I$. Stąd $rsrs = (rs)^2 \in I$, bo $I \lhd R$. Ale ideał I jest zredukowany, więc z uwagi 13.14 $rs \in I$, czyli $r \in A_s$. Zatem z uwagi 13.14 ideał A_s jest zredukowany. □

Z uwagi 13.15 i z lematu 13.19 wynika od razu następujący lemat:

Lemat 13.20. *Niech I będzie ideałem zredukowanym pierścienia R. Niech S będzie niepustym podzbiorem R oraz*

$$B = \{r \in R : sr \in I \text{ dla każdego } s \in S\}.$$

Wówczas B jest ideałem zredukowanym pierścienia R.

Twierdzenie 13.21. (Andrunakiewicz - Rjabuhin). *Dla dowolnego niezerowego pierścienia R równoważne są warunki:*

(i) R jest zredukowany,

(ii) istnieje niepusta rodzina ideałów $\{I_t\}_{t\in T}$ pierścienia R taka, że $\bigcap_{t\in T} I_t = \{0\}$ oraz R/I_t jest dziedziną dla każdego $t \in T$.

DOWÓD. $(ii) \Rightarrow (i)$. Niech $a \in R$ będzie takie, że $a^2 = 0$. Wtedy $(a + I_t)^2 = I_t$ dla dowolnego $t \in T$. R/I_t jest dziedziną, więc $a + I_t = I_t$, skąd $a \in I_t$ dla dowolnego $t \in T$. Zatem $a \in \bigcap_{t\in T} I_t = \{0\}$, więc $a = 0$. Stąd z lematu 13.1 pierścień R jest zredukowany.

$(i) \Rightarrow (ii)$. Niech R będzie pierścieniem zredukowanym. Wystarczy udowodnić, że dla dowolnego elementu $x \neq 0$ pierścienia R istnieje ideał I_x taki, że R/I_x jest dziedziną oraz $x \notin I_x$, bo wtedy $\bigcap_{x\in R\setminus\{0\}} I_x = \{0\}$.

Rozważmy rodzinę $\mathcal{M}$ wszystkich ideałów zredukowanych pierścienia R, które nie zawierają elementu $0 \neq x \in R$. Wtedy $\mathcal{M} \neq \emptyset$, bo np. $\{0\} \in \mathcal{M}$.

Niech $\mathcal{A}$ będzie łańcuchem w $\mathcal{M}$. Niech $I_0 = \bigcup_{I\in\mathcal{A}} I$. Z uwagi 13.18, I_0 jest ideałem zredukowanym. Ponadto $x \notin I_0$, bo $x \notin I$ dla każdego $I \in \mathcal{A}$. Zatem $I_0 \in \mathcal{M}$ i I_0 jest ograniczeniem górnym łańcucha $\mathcal{A}$. Zatem z lematu

Kuratowskiego - Zorna istnieje w $\mathcal{M}$ element maksymalny I_x. Wtedy I_x jest ideałem zredukowanym pierścienia R oraz $x \notin I_x$.

Pozostaje sprawdzić, że R/I_x jest dziedziną. Załóżmy, że tak nie jest. Wtedy istnieją $a, b \in R \setminus I_x$ takie, że $ab \in I_x$, czyli $a + I_x \neq I_x$, $b + I_x \neq I_x$, ale $ab + I_x = I_x$. Niech $A = \{r \in R : rb \in I_x\}$ i $B = \{r \in R : Ar \subseteq I_x\}$. Z lematów 13.19 i 13.20 mamy, że A i B są ideałami zredukowanymi w pierścieniu R. Z definicji ideału B otrzymujemy, że $AB \subseteq I_x$, bo $Ar \subseteq I_x$ dla dowolnego $r \in B$.

Niech $y \in I_x$. Ponieważ $I_x \lhd R$, więc $yb \in I_x$, stąd $y \in A$, czyli $I_x \subseteq A$. Ponadto $a \in A$, bo $ab \in I_x$ oraz $a \notin I_x$ z założenia, więc $a \in A \setminus I_x$, zatem $I_x \subset A$. Z maksymalności I_x otrzymujemy, że $A \notin \mathcal{M}$, zatem $x \in A$, bo A jest ideałem zredukowanym.

Niech $z \in I_x$. Ponieważ $I_x \lhd R$, więc $Az \subseteq I_x$, stąd $z \in B$, zatem $I_x \subseteq B$. Ponadto $b \in B$, bo $Ab = \{ab : a \in A\} \subseteq I_x$. Z założenia $b \notin I_x$, więc $b \in B \setminus I_x$, skąd $I_x \subset B$. Z maksymalności I_x otrzymujemy, że $B \notin \mathcal{M}$, zatem $x \in B$, bo B jest ideałem zredukowanym.

Zatem $x^2 \in AB \subseteq I_x$, czyli $x^2 \in I_x$ oraz ideał I_x jest zredukowany, w konsekwencji z uwagi 13.14 mamy, że $x \in I_x$, co jest sprzeczne z założeniem. □

Zadanie (1)**.** Niech $P_n = \mathbb{Z}_2$ dla $n = 1, 2, \ldots$ oraz niech $P = \prod_{n=1}^{\infty} P_n$. Udowodnij, że każdy ideał pierścienia P jest ideałem radykalnym. Niech $I = \bigoplus_{n=1}^{\infty} P_n$. Udowodnij, że pierścień $R = P/I$ jest zredukowany i nie posiada ideału, będącego dziedziną.

Wykład 14

Pierścienie Jacobsona

14.1 Podstawowe własności pierścieni Jacobsona

Definicja 14.1. Powiemy, że pierścień R jest **pierścieniem Jacobsona**, jeżeli dla każdego $x \in R$ istnieje liczba naturalna $n = n(x) \geqslant 2$ taka, że $x^n = x$.

Wprost z definicji uzyskujemy następujące

Stwierdzenie 14.2. *Każdy podpierścień i każdy obraz homomorficzny pierścienia Jacobsona jest pierścieniem Jacobsona.*

Stwierdzenie 14.3. *Każdy pierścień Jacobsona jest pierścieniem zredukowanym.*

Dowód. Niech R będzie pierścieniem Jacobsona i niech $x \in R$ będzie takie, że $x^2 = 0$. Wtedy istnieje liczba naturalna $n \geqslant 2$ taka, że $x = x^n$. Stąd $x^n = x^2 \cdot x^{n-2} = 0 \cdot x^{n-2} = 0$, więc $x = 0$ i pierścień R jest zredukowany. □

Stwierdzenie 14.4. *Jeżeli R jest pierścieniem Jacobsona i $x \in R$ oraz $x^n = x$ dla pewnej liczby naturalnej $n \geqslant 2$, to $e = x^{n-1}$ jest centralnym idempotentem w R, $x = e \cdot x$ i $(x) = Re$. Ponadto grupa R^+ jest torsyjna.*

Dowód. Na mocy stwierdzenia 14.3 R jest pierścieniem zredukowanym. Ponadto $(x^{n-1})^2 = x^{2n-2} = x^n \cdot x^{n-2} = x \cdot x^{n-2} = x^{n-1}$, czyli x^{n-1} jest idempotentem w pierścieniu zredukowanym. Zatem $e - x^{n-1} \in Z(R)$. Ponadto $x = e \cdot x$, skąd $(x) \subset Re$. Ale $n \geqslant 2$ i $e = x^{n-1}$, więc $Re \subseteq (x)$ i ostatecznie $(x) = Re$.

Dalej, istnieje liczba naturalna $m \geqslant 2$ taka, że $(2e)^m = 2e$ i $e = e^2$, więc $(2^m - 2)e = 0$, skąd $o(e) \in \mathbb{N}$. Ale $x = e \cdot x$, więc też $o(x) \in \mathbb{N}$ i grupa R^+ jest torsyjna. □

Stwierdzenie 14.5. *Jeżeli dziedzina R jest pierścieniem Jacobsona, to R jest pierścieniem z dzieleniem.*

DOWÓD. Na mocy stwierdzenia 14.4 istnieje niezerowy idempotent $e \in R$. Stąd dla $x \in R$, $e(x - ex) = ex - e^2x = ex - ex = 0$, więc $x = ex$, bo R jest dziedziną. Podobnie, $(x - xe)e = xe - xe^2 = xe - xe = 0$, więc $x = xe$. Zatem e jest jedynką pierścienia R. Weźmy dowolne niezerowe $a \in R$. Wtedy istnieje liczba naturalna $n \geqslant 2$ taka, że $a^n = a$. Ze stwierdzenia 14.4 mamy, że $f = a^{n-1}$ jest idempotentem i $a = fa$. Zatem $f \neq 0$ i z pierwszej części dowodu, $f = e$. Ale $n - 1 \geqslant 1$ i $a^{n-1} = e$, więc $a \in R^*$. Zatem R jest pierścieniem z dzieleniem. □

Stwierdzenie 14.6. *Suma prosta pierścieni Jacobsona jest pierścieniem Jacobsona.*

DOWÓD. Niech $\{R_t\}_{t\in T}$ będzie niepustą rodziną pierścieni Jacobsona i niech $R = \bigoplus_{t\in T} R_t$. Weźmy dowolne $x \in R$. Wtedy istnieje niepusty skończony podzbiór $S \subseteq T$ oraz istnieją $x_s \in R_s$ dla $s \in S$ takie, że $x = \Sigma_{s\in S} x_s$. Stąd dla każdego $n \in \mathbb{N}$ jest $x^n = \Sigma_{s\in S} x_s^n$ oraz na mocy stwierdzenia 14.4 dla każdego $s \in S$ istnieje liczba naturalna n_s taka, że $x_s^{n_s} = e_s$ jest idempotentem oraz $e_s x_s = x_s$. Stąd dla $n = \Pi_{s\in S} n_s$ mamy, że $x^{n+1} = x$ i R jest pierścieniem Jacobsona. □

Stwierdzenie 14.7. *Niezerowy pierścień skończony R jest pierścieniem Jacobsona wtedy i tylko wtedy, gdy R jest skończoną sumą prostą pewnych ciał skończonych. W szczególności każdy skończony pierścień Jacobsona jest przemienny.*

DOWÓD. Niech R będzie niezerowym skończonym pierścieniem Jacobsona. Ze stwierdzenia 14.3 i z twierdzenia Wedderburna-Artina R jest skończoną sumą prostą pierścieni postaci $M_n(D)$, gdzie D jest skończonym pierścieniem z dzieleniem. Ale R jest zredukowany, więc $n = 1$. Ponadto z twierdzenia Wedderburna D jest ciałem. Zatem R jest skonczoną sumą prostą pewnych ciał skończonych. Stąd R jest przemienny.

Na odwrót, wobec stwierdzenia 15.6, wystarczy wykazać, że każde ciało skończone K jest pierścieniem Jacobsona. Ale jeśli $n = |K|$, to dla każdego niezerowego $a \in K$ mamy $a^{n-1} = 1$, skąd $a^n = a$. Wobec tego $x^n = x$ dla każdego $x \in K$ i K jest pierścieniem Jacobsona. □

Przypomnijmy, że jeśli grupa addytywna pierścienia R jest torsyjna, to dla każdej liczby pierwszej p, $R_p = \{x \in R : p^n x = 0 \text{ dla pewnego } n \in \mathbb{N}\}$ jest ideałem w R oraz $R = \bigoplus_{p\in\mathbb{P}} R_p$. Ponadto, jeśli grupa addytywna pierścienia zredukowanego S jest p-grupą dla pewnej liczby pierwszej p, to $pS = \{0\}$. Rzeczywiście, weźmy dowolne $x \in S$. Wtedy istnieje $n \in \mathbb{N}$ takie, że $p^n x = 0$, skąd $(px)^n = 0$. Ale S jest pierścieniem zredukowanym, więc w konsekwencji $px = 0$ i $pS = \{0\}$. Wobec tego, jeśli grupa addytywna pierścienia zredukowanego R jest torsyjna, to $pR_p = \{0\}$ dla każdej liczby pierwszej p. Jeśli R jest pierścieniem Jacobsona, to ze stwierdzenia 14.3 R jest zredukowany i na mocy

stwierdzenia 14.4 grupa R^+ jest torsyjna. Wobec tego dla każdej liczby pierwszej p, R_p jest pierścieniem Jacobsona takim, że $pR_p = \{0\}$ oraz $R = \bigoplus_{p\in\mathbb{P}} R_p$. Na odwrót, załóżmy, że dla każdej liczby pierwszej p, R_p jest pierścieniem Jacobsona takim, że $pR_p = \{0\}$. Wtedy na mocy stwierdzenia 14.6, $R = \bigoplus_{p\in\mathbb{P}} R_p$ też jest pierścieniem Jacobsona. W ten sposób udowodniliśmy następujące

Stwierdzenie 14.8. *Pierścień R jest pierścieniem Jacobsona wtedy i tylko wtedy, gdy R jest sumą prostą rodziny $\{R_p\}_{p\in\mathbb{P}}$ pierścieni Jacobsona takich, że $pR_p = \{0\}$ dla każdego $p \in \mathbb{P}$.*

Problem klasyfikacji pierścieni Jacobsona sprowadza się zatem do problemu klasyfikacji pierścieni Jacobsona, których grupa addytywna jest elementarną p-grupą abelową.

Stwierdzenie 14.9. *Niech p będzie liczbą pierwszą i niech R będzie pierścieniem takim, że $pR = \{0\}$. Wówczas R jest pierścieniem Jacobsona wtedy i tylko wtedy, gdy dla każdego $x \in R$ istnieje $n \in \mathbb{N}$ takie, że $x^{p^n} = x$.*

Dowód. $\Rightarrow$. Weźmy dowolne $x \in R$. Jeśli $x = 0$, to wystarczy wziąć $n = 1$. Niech dalej $x \neq 0$. Istnieje $m \in \mathbb{N}$ takie, że $x^m = x$ oraz $px = 0$, więc pierścień $[x]$ jest skończony i przemienny. Ponadto jest to niezerowy pierścień Jacobsona, więc ze stwierdzenia 14.7, $[x]$ jest skończoną sumą prostą ciał skończonych, z których każde ma charakterystykę p. Oznaczmy te ciała przez $K_1, \ldots, K_s$ i niech $|K_i| = p^{n_i}$ dla $i = 1, \ldots, s$. Dalej, $x = x_1 + \ldots + x_s$, dla pewnych $x_i \in K_i$, $i = 1, \ldots, s$ oraz dla dowolnego $k \in \mathbb{N}$ jest $x^k = x_1^k + \ldots + x_s^k$. Niech $n = n_1 \cdot \ldots \cdot n_s$ i weźmy dowolne $i = 1, \ldots, s$. Jeśli $x_i \neq 0$, to w ciele K_i, $x_i^{p^{n_i}-1} = 1$, skąd $x_i^{p^n-1} = 1$, a więc $x_i^{p^n} = x_i$. Jeśli zaś $x_i = 0$, to też $x_i^{p^n} = x_i$. Zatem $x^{p^n} = x$.

Implikacja odwrotna jest oczywista. □

Uwaga 14.10. *Jeśli R jest pierścieniem takim, że $pR = \{0\}$ dla pewnej liczby pierwszej p, to w naturalny sposób R jest przestrzenią liniową nad ciałem $\mathbb{Z}_p$, mianowicie dla $a \in \mathbb{Z}_p$ i $\alpha \in R$ przyjmuje się, że $a \circ \alpha = a \cdot \alpha$, gdzie $a \cdot \alpha$ jest całkowitą wielokrotnością elementu α przez liczbę całkowitą a. Na grupie abelowej $\mathbb{Z}_p^+ \times R^+$ można wprowadzić mnożenie przy pomocy wzoru:*

$$(a_1, r_1) \cdot (a_2, r_2) = (a_1 \cdot a_2, a_1 \cdot r_2 + a_2 \cdot r_1 + r_1 r_2).$$

Proste sprawdzenie pokazuje, że otrzymujemy w ten sposób pierścień z jedynką $(1, 0)$, który będziemy oznaczali przez R^1. Jest jasne, że $pR^1 = \{0\}$, $\{0\} \times R \lhd R^1$ i $R^1/(\{0\} \times R) \cong \mathbb{Z}_p$ oraz $R \cong \{0\} \times R$. Dowodzi się to wszystko podobnie jak dla przypadku dołączania jedynki do pierścienia przy pomocy pierścienia $\mathbb{Z}$. Zauważmy, że jeśli dodatkowo, R jest pierścieniem Jacobsona, to na mocy stwierdzenia 14.9, dla każdego $x \in R$ istnieje $n \in \mathbb{N}$ takie, że $x^{p^n} = x$. Wtedy dla dowolnego $a \in \mathbb{Z}_p$ jest $a^{p^n} = a$, więc ze wzoru Newtona i tego, że $pR^1 = \{0\}$ oraz tego, że $(a, 0) \cdot (0, x) = (0, x) \cdot (a, 0)$ otrzymamy,

że $(a,x)^{p^n} = (a^{p^n}, x^{p^n}) = (a,x)$. *Wobec tego* R^1 *jest pierścieniem Jacobsona! W ten sposób wykazaliśmy, że każdy pierścień Jacobsona, którego grupa addytywna jest elementarną abelową p-grupą jest ideałem w pierścieniu Jacobsona z jedynką, którego grupa addytywna jest elementarną p-grupą abelową. Zatem klasyfikacja pierścieni Jacobsona sprowadza się do opisu pierścieni Jacobsona z jedynką, których grupa addytywna jest elementarną p-grupą abelową!*

14.2 Pierścienie endomorfizmów grup abelowych i ich własności

Niech $(A,+)$ będzie dowolną grupą abelową. Oznaczmy przez $End(A)$ rodzinę wszystkich endomorfizmów grupy A. $End(A)$ jest grupą abelową ze względu na naturalne dodawanie przekształceń, tzn. dla dowolnych $f,g \in End(A)$ i dla dowolnego $a \in A$:

$$(f+g)(a) = f(a) + g(a).$$

W zbiorze $End(A)$ można też wprowadzić mnożenie, jako składanie przekształceń, tzn. dla dowolnych $f,g \in End(A)$ i dla dowolnego $a \in A$:

$$(fg)(a) = f(g(a)).$$

Proste sprawdzenie pokazuje, że $(End(A),+,\cdot)$ jest pierścieniem z jedynką id_A, gdzie $id_A(x) = x$ dla każdego $x \in A$. Otrzymany w ten sposób pierścień nazywamy **pierścieniem endomorfizmów grupy abelowej** A i oznaczamy przez $End(A)$.

Niech teraz R będzie dowolnym pierścieniem i $a \in R$. Oznaczmy przez l_a i przez r_a przekształcenia R w R dane wzorami:

$$l_a(x) = ax \quad \text{oraz} \quad r_a(x) = xa \quad \text{dla dowolnych } a \in R.$$

Zauważmy, że dla dowolnych $a,x,y \in R$: $l_a(x+y) = a(x+y) = ax + ay = l_a(x) + l_a(y)$ oraz $r_a(x+y) = (x+y)a = xa + ya = r_a(x) + r_a(y)$, więc

$$l_a, r_a \in End(R^+) \text{ dla dowolnego } a \in R.$$

Ponadto, dla dowolnych $a,x \in R$: $(l_a r_a)(x) = l_a(r_a(x)) = l_a(xa) = axa$ oraz $(r_a l_a)(x) = r_a(l_a(x)) = r_a(ax) = axa$, więc

$$l_a r_a = r_a l_a \text{ dla każdego } a \in R.$$

Stąd dla każdego $a \in R$ przekształcenie $ad(a) = l_a - r_a \in End(R^+)$ oraz $ad(a)l_a = l_a ad(a)$ i $ad(a)r_a = r_a ad(a)$. Ponadto

$$ad(a)(x) = ax - xa \text{ dla każdego } x \in R.$$

Ponadto, z uzyskanych zależności i ze wzoru dwumianowego Newtona wynika, że dla dowolnego $n \in \mathbb{N}$:

$$(ad(a)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k l_a^{n-k} r_a^k.$$

Zauważmy, że przekształcenie $\varphi\colon R \to End(R^+)$ dane wzorem $\varphi(a) = l_a$ dla $a \in R$ jest homomorfizmem pierścieni. Rzeczywiście, dla dowolnych $a, b, x \in R$: $\varphi(a+b)(x) = l_{a+b}(x) = (a+b)x = ax + bx = l_a(x) + l_b(x) = (l_a + l_b)(x)$, skąd $\varphi(a+b) = \varphi(a) + \varphi(b)$ oraz $\varphi(ab)(x) = l_{ab}(x) = abx$ i $(\varphi(a)\varphi(b))(x) = \varphi(a)(\varphi(b)(x)) = l_a(l_b(x)) = l_a(bx) = abx$, skąd $\varphi(ab) = \varphi(a)\varphi(b)$. Ponadto $Ker\varphi = \{a \in R : aR = \{0\}\}$, skąd wynika w szczególności, że jeśli pierścień R jest zredukowany, to φ jest zanurzeniem pierścieni.

Jeśli istnieje liczba pierwsza p taka, że $pR = \{0\}$, to $pEnd(R^+) = \{0\}$. Rzeczywiście, dla dowolnych $f \in End(R^+)$, $x \in R$ mamy, że $(pf)(x) = f(px) = f(0) = 0$, skąd $pf = 0$. Wobec tego dla dowolnego $a \in R$ i dla dowolnego $n \in \mathbb{N}$ zachodzi wówczas wzór:

$$(ad(a))^{p^n} = l_a^{p^n} - r_a^{p^n}.$$

Jeśli dodatkowo $a^{p^n} = a$ dla pewnego $n \in \mathbb{N}$, to z powyższego wzoru wynika, że $ad(a)^{p^n} = ad(a)$.

Twierdzenie 14.11. (lemat Hersteina). *Niech D będzie pierścieniem z dzieleniem takim, że $pD = \{0\}$ dla pewnej liczby pierwszej p. Jeśli $a \in D \setminus Z(D)$ i $a^k = 1$ dla pewnego naturalnego k, to istnieje $x \in D^*$ takie, że $xax^{-1} = a^i \neq a$ dla pewnego naturalnego i.*

DOWÓD. Z założeń wynika, że $a \neq 0$ i $a \neq 1$, więc $k \geqslant 2$ oraz pierścień $K = [a]$ jest skończony i przemienny. Ale K jest podpierścieniem pierścienia z dzieleniem D, więc K jest dziedziną. Wobec tego K jest ciałem skończonym i $pK = \{0\}$. Wobec tego grupa K^* jest cykliczna i istnieje $m \in \mathbb{N}$ takie, że $|K| = p^m$. Wówczas $b^{p^m} = b$ dla każdego $b \in K$, więc w szczególności $a^{p^m} = a$. Stąd i z rozważań o endomorfizmach grupy R^+ przedstawionych przed sformułowaniem naszego twierdzenia otrzymujemy, że $(ad(a))^{p^m} = ad(a)$. Ponadto w pierścieniu wielomianów $K[t]$ mamy, że $t^{p^m} - t = t \cdot \prod_{b \in K^*} (t - b)$, gdyż wielomian $t^{p^m} - t$ ma stopień równy p^m i każdy element ciała p^m-elementowego K jest jego pierwiastkiem. Ponieważ D jest pierścieniem zredukowanym, więc odworowanie $\varphi\colon D \to End(D^+)$ dane wzorem $\varphi(y) = l_y$ dla $y \in D$ jest zanurzeniem pierścieni i wobec tego $\varphi(K)$ jest ciałem izomorficznym z K. Zatem w pierścieniu $D[t]$ zachodzi wzór $t^{p^m} - t = t \cdot \prod_{b \in K^*} (t - l_b)$. Ale $ad(a)$ jest przemienne z każdym l_b dla $b \in K$ oraz $(ad(a))^{p^m} = ad(a)$, więc otrzymujemy zależność:

$$0 = ad(a) \prod_{b \in K^*} (ad(a) - l_b).$$

Ponadto $ad(a) \neq 0$, bo $a \neq Z(D)$ i podpierścień $[ad(a), l_b : b \in K]$ pierścienia $End(D^+)$ jest przemienny, więc z powyższego wzoru wynika, że istnieje $b \in K^*$ takie, że odwzorowanie $ad(a) - l_b$ nie jest różnowartościowe. Zatem $Ker(ad(a) - l_b) \neq \{0\}$ i istnieje $x \in D^*$ takie, że $0 = (ad(a) - l_b)(x) = ax - xa - bx$. Stąd zaś uzyskujemy, że $xax^{-1} = a - b \neq a$, bo $b \neq 0$. Ale w grupie D^*, $o(xax^{-1}) = o(a) \in \mathbb{N}$, więc w skończonej grupie cyklicznej K^*, $o(a) = o(a - b)$. Zatem w tej grupie podgrupy $< a >$ i $< a - b >$ mają ten sam rząd i wobec tego $a - b \in < a >$. Zatem istnieje liczba naturalna i taka, że $a - b = a^i$, skąd $xax^{-1} = a^i \neq a$. □

Twierdzenie 14.12. (uogólnione twierdzenie Wedderburna). *Jeżeli D jest pierścieniem z dzieleniem i grupa D^* jest torsyjna, to D jest ciałem. W szczególności każdy pierścień z dzieleniem będący pierścieniem Jacobsona jest przemienny.*

DOWÓD. Załóżmy, że przy tych założeniach pierścień D nie jest ciałem, tzn. nie jest przemienny. Istnieje wówczas $a \in D \setminus Z(D)$. Ponadto ze stwierdzenia 14.4 grupa D^+ jest torsyjna, więc istnieje liczba pierwsza p taka, że $pD = \{0\}$. Zatem z lematu Hersteina istnieje $x \in D^*$ takie, że $xax^{-1} = a^i \neq a$ dla pewnego $i \in \mathbb{N}$. Stąd $xa^sx^{-1} = a^{is}$ dla każdego $s \in \mathbb{N}$. Dalej, przez prostą indukcję uzyskujemy, że $x^ka^sx^{-k} = a^{si^k}$ dla dowolnych $k, s \in \mathbb{N}$, a więc $x^ka^s = a^{si^k}x^k$. Ale $o(x), o(a) \in \mathbb{N}$, więc zbiór $A = \{a^tx^s : t \in \{1, \ldots, o(a)\}, s \in \{1, \ldots, o(x)\}\}$ jest skończoną podgrupą grupy D^* zawierającą a i x. Ale $ax \neq xa$, więc grupa A nie jest abelowa.

Ponieważ grupa D^* jest torsyjna, więc D jest pierścieniem Jacobsona. Oznaczmy przez T zbiór wszystkich elementów postaci $\sum_{g \in A} k_g g$, gdzie $k_g \in \mathbb{Z}$. Ponieważ $pD = \{0\}$, więc zbiór T jest skończony. Ponadto T jest podpierścieniem D. Zatem T jest skończonym pierścieniem Jacobsona i ze stwierdzenia 14.7 T jest przemienny. Ale $a, x \in T$ i $ax \neq xa$, więc mamy sprzeczność. □

Twierdzenie 14.13. *Każdy pierścień Jacobsona jest przemienny.*

DOWÓD. Niech R będzie pierścieniem Jacobsona. Jeśli $R = \{0\}$, to R jest przemienny. Niech dalej $R \neq \{0\}$. Wobec stwierdzenia 14.8 wystarczy wykazać nasze twierdzenie w przypadku, gdy $pR = \{0\}$ dla pewnej liczby pierwszej p. Ale R jest pierścieniem zredukowanym, więc z twierdzenia Andrunakiewicza-Rjabuhina istnieje niepusta rodzina $\{I_t\}_{t \in T}$ ideałów pierścienia R taka, że $\bigcap_{t \in T} I_t = \{0\}$ oraz R/I_t jest dziedziną dla każdego $t \in T$. Wobec tego dla każdego $t \in T$ dziedzina R/I_t jest pierścieniem Jacobsona, a więc na mocy stwierdzenia 14.5, R/I_t jest pierścieniem z dzieleniem. Ponadto $p(R/I_t) = \{0\}$, więc z twierdzenia 14.12 pierścień R/I_t jest przemienny. Weźmy dowolne $a, b \in R$. Wtedy dla każdego $t \in T$ mamy, że $(a + I_t)(b + I_t) = (b + I_t)(a + I_t)$, więc $ab - ba \in I_t$. Zatem $ab - ba \in \bigcap_{t \in T} I_t = \{0\}$, więc $ab - ba = 0$, czyli $ab = ba$ i pierścień R jest przemienny. □

Stwierdzenie 14.14. *Klasa pierścieni Jacobsona jest zamknięta na rozszerzenia, tzn. jeśli $I \lhd R$ i R/I oraz I są pierścieniami Jacobsona, to R jest pierścieniem Jacobsona.*

Dowód. Weźmy dowolne niezerowe $a \in R$. Ponieważ R/I jest pierścieniem Jacobsona, więc istnieje liczba naturalna $m \geqslant 2$ taka, że $a + I = (a + I)^m$, skąd $b = a^m - a \in I$. Ale I też jest pierścieniem Jacobsona, więc istnieje liczba naturalna $n \geqslant 2$ taka, że $b = b^n$. Zatem $(a^m - a)^n = a^m - a$. Stąd $[a] = \langle a \rangle + \ldots + \langle a^{mn-1} \rangle$. Ponadto ze stwierdzenia 14.4 grupy I^+ i $(R/I)^+$ są torsyjne, więc grupa R^+ jest torsyjna i stąd pierścień $[a]$ jest skończony. Ponadto ze stwierdzenia 14.3 pierścienie R/I oraz I są zredukowane, więc pierścień R też jest zredukowany. Wobec tego $[a]$ jest skończonym przemiennym pierścieniem zredukowanym. Zatem z twierdzenia Wedderburna-Artina $[a]$ jest skończoną sumą prostą ciał skończonych i z twierdzenia 14.7 $[a]$ jest pierścieniem Jacobsona. Zatem istnieje liczba naturalna $k \geqslant 2$ taka, że $a = a^k$. Ponadto, $0 = 0^2$, więc R jest pierścieniem Jacobsona. □

Wykład 15

Pierścienie regularne w sensie von Neumanna

15.1 Podstawowe własności pierścieni regularnych w sensie von Neumanna

Definicja 15.1. Powiemy, że pierścień R jest **regularny w sensie von Neumanna**, jeżeli dla dowolnego $a \in R$ istnieje $x \in R$ takie, że $a = axa$.

Twierdzenie 15.2. *Dla dowolnego pierścienia R równoważne są warunki:*
(i) R jest pierścieniem regularnym w sensie von Neumanna,
(ii) $M_2(R)$ jest pierścieniem regularnym w sensie von Neumanna.

Dowód. $(ii) \Rightarrow (i)$. Weźmy dowolne $a \in R$. Wtedy istnieją $x, y, z, t \in R$ takie, że $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} x & y \\ z & t \end{bmatrix} \cdot \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$. Stąd $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} axa & 0 \\ 0 & 0 \end{bmatrix}$, a więc $a = axa$ i pierścień R jest regularnym w sensie von Neumanna.

$(i) \Rightarrow (ii)$. Weźmy dowolne $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(R)$. Wtedy istnieje $x \in R$ takie, że $c = cxc$, więc dla $X = \begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix}$ mamy, że $A_1 = A - AXA = \begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix}$ dla pewnych $a_1, b_1, d_1 \in R$. Dalej, istnieją $r, s \in R$ takie, że $a_1 = a_1 r a_1$ i $d_1 = d_1 s d_1$. Niech $Y = \begin{bmatrix} r & 0 \\ 0 & s \end{bmatrix}$. Wtedy $A_2 = A_1 - A_1 Y A_1 = \begin{bmatrix} 0 & b_2 \\ 0 & 0 \end{bmatrix}$ dla pewnego $b_2 \in R$. Istnieje więc $u \in R$ takie, że $b_2 = b_2 u b_2$. Niech $Z = \begin{bmatrix} 0 & 0 \\ u & 0 \end{bmatrix}$. Wtedy $A_2 = A_2 Z A_2$. Stąd $A_1 - A_1 Y A_1 = (A_1 - A_1 Y A_1) Z (A_1 - A_1 Y A_1)$, czyli $A_1 = A_1 T A_1$ dla pewnego $T \in M_2(R)$. Zatem $A - AXA = (A - AXA)T(A - AXA)$, skąd $A = ASA$ dla $S = X + T - AX - XAT + XATAX \in M_2(R)$. Zatem pierścień $M_2(R)$ jest regularny w sensie von Neumanna. $\square$

Stwierdzenie 15.3. *Klasa pierścieni regularnych w sensie von Neumanna jest zamknięta na rozszerzenia, tzn. jeśli $I \lhd R$ i pierścienie I oraz R/I są regularne w sensie von Neumanna, to pierścień R też jest regularny w sensie von Neumanna.*

DOWÓD. Weźmy dowolne $a \in R$. Wtedy istnieje $y \in R$ takie, że $a+I = (a+I)(y+I)(a+I)$, skąd $i = a-aya \in I$. Zatem istnieje $j \in I$ takie, że $i = iji$. Stąd $a-aya = (a-aya)j(a-aya)$, więc $a = axa$ dla $x = y+j-jay-yaj+yajay$ i pierścień R jest regularny w sensie von Neumanna. □

Stwierdzenie 15.4. *Każdy ideał i każdy obraz homomorficzny pierścienia regularnego w sensie von Neumanna jest pierścieniem regularnym w sensie von Neumanna.*

DOWÓD. Niech R będzie pierścieniem regularnym w sensie von Neumanna i niech $I \lhd R$. Weźmy dowolne $a \in I$. Wtedy istnieje $x \in R$ takie, że $a = axa$. Stąd $a = a(xax)a$. Ale $a \in I$, więc $xax \in I$. Zatem pierścień I jest regularny w sensie von Neumanna.

Niech $f\colon R \to S$ będzie homomorfizmem pierścienia R na pierścień S. Weźmy dowolne $a \in S$. Wtedy istnieje $b \in R$ takie, że $a = f(b)$. Stąd istnieje $x \in R$ takie, że $b = bxb$. Zatem $a = f(bxb) = f(b)f(x)f(b) = af(x)a$ i pierścień S jest regularny w sensie von Neumanna. □

Stwierdzenie 15.5. *Każdy pierścień regularny w sensie von Neumanna jest pierścieniem półpierwszym.*

DOWÓD. Niech R będzie pierścieniem regularnym w sensie von Neumanna. Weźmy dowolne $a \in R$ takie, że $aRa = \{0\}$. Wtedy $a = axa$ dla pewnego $x \in R$, więc $a \in aRa$, skąd $a = 0$ i pierścień R jest półpierwszy. □

Przykład 15.6. Zauważmy, że każdy pierścień D z dzieleniem jest regularny w sensie von Neumanna, bo $0 = 0 \cdot 0 \cdot 0$ oraz dla niezerowego $a \in D$ istnieje $b \in D$ takie, że $ab = 1$, skąd $a = aba$. W szczególności każde ciało jest pierścieniem regularnym w sensie von Neumanna.

Na mocy twierdzenia 15.2 mamy stąd, że dla dowolnego pierścienia D z dzieleniem, pierścień macierzy $M_2(D)$ jest regularny w sensie von Neumanna.

Przykład 15.7. Zauważmy, że ideał jednostronny pierścienia regularnego w sensie von Neumanna nie musi być pierścieniem regularnym w sensie von Neumanna. Mianowicie, niech D będzie dowolnym pierścieniem z dzieleniem. Wtedy $R = M_2(D)$ jest pierścieniem regularnym w sensie von Neumanna na mocy przykładu 15.6. Ponadto $L = \begin{bmatrix} D & 0 \\ D & 0 \end{bmatrix} <_l R$ i $I = \begin{bmatrix} 0 & 0 \\ D & 0 \end{bmatrix} \lhd L$, przy czym $I^2 = \{0_2\}$ oraz $I \neq \{0_2\}$. Gdyby pierścień L był regularny w sensie von Neumanna, to na mocy stwierdzenia 15.4 pierścień I byłby regularny w sensie von Neumanna, co przeczy stwierdzeniu 15.5. Zatem pierścień L nie jest regularny

w sensie von Neumanna. Podobnie można pokazać, że $P = \begin{bmatrix} D & D \\ 0 & 0 \end{bmatrix} <_r R$ i P nie jest pierścieniem regularnym w sensie von Neumanna.

Stwierdzenie 15.8. *Jeżeli $\{R_t\}_{t\in T}$ jest niepustą rodziną pierścieni regularnych w sensie von Neumanna, to pierścienie $\prod_{t\in T} R_t$ i $\bigoplus_{t\in T} R_t$ też są regularne w sensie von Neumanna.*

DOWÓD. Weźmy dowolne $a = (a_t)_{t\in T} \in \prod_{t\in T} R_t$. Wtedy dla każdego $t \in T$ istnieje $x_t \in R_t$ takie, że $a_t = a_t x_t a_t$. Niech $x = (x_t)_{t\in T}$. Wtedy $x \in \prod_{t\in T} R_t$ oraz $a = axa$, więc pierścień $\prod_{t\in T} R_t$ jest regularny w sensie von Neumanna. Ponadto $\bigoplus_{t\in T} R_t \lhd \prod_{t\in T} R_t$, więc ze stwierdzenia 15.4 pierścień $\bigoplus_{t\in T} R_t$ jest regularny w sensie von Neumanna. □

Stwierdzenie 15.9. *Jeżeli dziedzina R jest regularna w sensie von Neumanna, to R jest pierścieniem z dzieleniem.*

DOWÓD. Weźmy dowolne niezerowe $a \in R$. Wtedy istnieje $x \in R$ takie, że $a = axa$. Stąd $ax = axax$, więc $e = ax$ jest idempotentem i $a = ea$, skąd $e \neq 0$. Dla dowolnego $b \in R$ mamy, że $e(b - eb) = eb - e^2b = eb - eb = 0$, więc $b - eb = 0$, gdyż R jest dziedziną i $e \neq 0$. Stąd $b = eb$ dla każdego $b \in R$. Ponadto $(b - be)e = be - be^2 = be - be = 0$, więc $b - be = 0$ i w konsekwencji e jest jedynką pierścienia R. Jeżeli $f \in R$ jest idempotentem, to $0 = f(e - f)$, skąd $f = 0$ lub $f = e$. Zatem e jest jedynym niezerowym idempotentem pierścienia R. Weźmy dowolne niezerowe $c \in R$. Wtedy istnieje $y \in R$ takie, że $c = cyc$, skąd $cy = cycy$ i $cy \neq 0$. Zatem cy jest niezerowym idempotentem w R, skąd $cy = e$. Ponadto, $yc = ycyc$, więc yc jest niezerowym idempotentem w R i stąd $yc = e$. Zatem $cy = yc = e$ i R jest pierścieniem z dzieleniem. □

Stwierdzenie 15.10. *Jeżeli pierścień R jest regularny w sensie von Neumanna, to dla każdego $a \in R$ istnieje idempotent $e \in R$ taki, że $Ra = Re$.*

DOWÓD. Weźmy dowolne $a \in R$. Wtedy istnieje $x \in R$ takie, że $a = axa$, skąd $xa = xaxa$. Zatem $e = xa$ jest idempotentem i $a = ae \in Re$. Wobec tego $Ra \subseteq Re$. Ale $e \in Ra$, więc $Re \subseteq Ra$ i ostatecznie $Ra = Re$. □

Lemat 15.11. *Jeżeli pierścień R jest regularny w sensie von Neumanna, to dla dowolnych $a, b \in R$ istnieje idempotent $e \in R$ taki, że $Ra + Rb = Re$.*

DOWÓD. Ze stwierdzenia 15.10 wynika, że istnieją idempotenty $e, f \in R$ takie, że $Ra = Re$ i $Rb = Rf$. Zatem $Ra + Rb = Re + Rf$. Ponadto $e - ef \in Re + Rf$ oraz $e = (e - ef) + f \in R(e - ef) + Rf$, więc $Re + Rf = R(e - ef) + Rf$ i $Ra + Rb = R(e - ef) + Rf$. Ze stwierdzenia 15.10 istnieje idempotent $g \in R(e - ef)$ taki, że $Rg = R(e - ef)$. Ale $(e - ef)f = ef - ef^2 = ef - ef = 0$, więc też $gf = 0$ i $Ra + Rb = Rg + Rf$. Ponadto, $g + f - fg \in Rg + Rf$ i $f = f(f + g - fg)$ oraz $g = g(g + f - fg)$, więc $Ra + Rb = R(g + f - fg)$. Stąd i ze stwierdzenia 15.10 istnieje idempotent $u \in R$ taki, że $Ra + Rb = Ru$. □

Ze stwierdzenia 15.10 i z lematu 15.11 przez prostą indukcję uzyskujemy następujące

Stwierdzenie 15.12. *Jeżeli pierścień R jest regularny w sensie von Neumanna, to dla dowolnego $n \in \mathbb{N}$ i dla dowolnych $a_1, a_2, \ldots, a_n \in R$ istnieje idempotent $e \in R$ taki, że $Ra_1 + Ra_2 + \ldots + Ra_n = Re$.*

Twierdzenie 15.13. *Dla dowolnego pierścienia R następujące warunki są równoważne:*

(i) R jest regularny w sensie von Neumanna,

(ii) dla każdego $a \in R$ istnieje idempotent $e \in R$ taki, że $Ra + \langle a \rangle = Re$, tzn. każdy lewostronny ideał główny pierścienia R jest generowany przez idempotenta,

(iii) dla każdego $a \in R$ istnieje idempotent $e \in R$ taki, że $aR + \langle a \rangle = eR$, tzn. każdy prawostronny ideał główny pierścienia R jest generowany przez idempotenta.

DOWÓD. $(i) \Rightarrow (ii)$. Wynika od razu ze stwierdzenia 15.10.

$(ii) \Rightarrow (i)$. Weźmy dowolne $a \in R$. Wtedy istnieje idempotent $e \in R$ taki, że $Ra + \langle a \rangle = Re$. Ale $e = e^2$, więc $e \in Re$ oraz $e = e^3 \in ReRe$, skąd $Re \subseteq ReRe \subseteq Re$, czyli $Re = (Re)^2$. Wobec tego $Ra \subseteq Ra + \langle a \rangle = (Ra + \langle a \rangle)^2 = RaRa + Ra^2 + aRa + \langle a^2 \rangle \subseteq Ra$, skąd $Ra = Ra + \langle a \rangle$ i $a \in Ra$ oraz $Ra = Re$. Zatem istnieją $x, r \in R$ takie, że $a = re$ i $e = xa$. Stąd $ae = re^2 = re = a$, czyli $a = ae = axa$, a więc $a = axa$ i pierścień R jest regularny w sensie von Neumanna.

Analogicznie dowodzi się równoważności warunków (i) oraz (iii). □

Przykład 15.14. Niech V będzie niezerową przestrzenią liniową nad ciałem K. Oznaczmy przez R pierścień wszystkich przekształceń K-liniowych przestrzeni V w siebie. Udowodnimy, że pierścień R jest regularny w sensie von Neumanna. Weźmy dowolne $f \in R$. Jeśli $f = 0$, to $f = f \circ f \circ f$. Niech dalej $f \neq 0$. Wtedy $Ker f$ jest właściwą podprzestrzenią przestrzeni V i istnieje podprzestrzeń $U \subseteq V$ taka, że $Ker f \oplus U = V$. Stąd $g\colon U \to f(V)$ dane wzorem $g(\alpha) = f(\alpha)$ dla $\alpha \in U$ jest izomorfizmem liniowym. Istnieje zatem przekształcenie liniowe $h\colon f(V) \to U$ odwrotne do g. Ponadto $f(V)$ jest podprzestrzenią w V, więc istnieje podprzestrzeń $W \subseteq V$ taka, że $f(V) \oplus W = V$. Przekształcenie $\pi\colon V \to f(V)$ dane wzorem $\pi(\alpha + \beta) = \alpha$ dla dowolnych $\alpha \in f(V)$, $\beta \in W$ jest K-liniowe. Zatem przekształcenie $\varphi = h \circ \pi \in R$. Pokażemy, że $f = f \circ \varphi \circ f$. W tym celu wystarczy wykazać, że $f(\alpha) = (f \circ \varphi \circ f)(\alpha)$ dla dowolnego $\alpha \in U$. A to z kolei jest równoważne temu, że $\gamma = f(\varphi(\gamma))$ dla dowolnego $\gamma \in f(V)$. Ale dla $\gamma \in f(V)$ mamy, że $\varphi(\gamma) = h(\pi(\gamma)) = h(\gamma)$, więc $f(\varphi(\gamma)) = f(h(\gamma)) = g(h(\gamma)) = \gamma$, bo h jest funkcją odwrotną do g. Zatem rzeczywiście $f = f \circ \varphi \circ f$ i pierścień R jest regularny w sensie von Neumanna.

Przykład 15.15. Każdy pierścień Jacobsona R jest pierścieniem regularnym w sensie von Neumanna, bo dla każdego $a \in R$ istnieje liczba naturalna $n \geqslant 2$ taka, że $a = a^n$. Stąd $a = a^{n^2}$ i $n^2 \geqslant 4$ oraz $a = axa$ dla $x = a^{n^2-2}$. □

Stwierdzenie 15.16. *Dla dowolnego pierścienia R i dla dowolnych $m, n \in \mathbb{N}$ pierścienie macierzy $M_m(M_n(R))$ i $M_{mn}(R)$ są izomorficzne.*

DOWÓD. Elementy pierścienia $M_m(M_n(R))$ są $m \times m$ macierzami o wyrazach z pierścienia $M_n(R)$, czyli są to macierze postaci $A = [A_{ij}]_{i,j=1,2,\ldots,m}$, gdzie $A_{ij} \in M_n(R)$ dla wszystkich $i, j = 1, 2, \ldots, m$. Zatem A jest macierzą blokową złożoną z m^2 macierzy kwadratowych stopnia n. Oznaczmy przez $\varphi(A)$ macierz powstającą z A przez usunięcie nawiasów we wszystkich jej blokach A_{ij}. Oczywiście $\varphi(A) \in M_{mn}(R)$ i otrzymujemy w ten sposób naturalne przekształcenie $\varphi\colon M_m(M_n(R)) \to M_{mn}(R)$. Jest jasne, że φ jest bijekcją, a nawet φ jest izomorfizmem grup addytywnych pierścieni $M_m(M_n(R))$ i $M_{mn}(R)$. Pozostaje zatem do wykazania, że $\varphi(A \cdot B) = \varphi(A) \cdot \varphi(B)$ dla dowolnych $A, B \in M_m(M_n(R))$.

Przypomnijmy, że jeśli $s \in \mathbb{N}$, P jest pierścieniem i $C \in M_s(P)$, to przez $C[i, j]$ oznaczamy wyraz stojący w i-tym wierszu i j-tej kolumnie macierzy C dla dowolnych $i, j \in \{1, 2, \ldots, s\}$ i wówczas macierz C można jednoznacznie zapisać w postaci $C = \sum_{,j=1}^{s} C[i, j]E_{ij}$, przy czym dla $c \in C$, cE_{ij} jest $s \times s$ - macierzą, która w i-tym wierszu i j-tej kolumnie ma element c, a poza tym same zera. Wobec tego dowolną macierz $A = [A_{ij}]_{i,j=1,2,\ldots,m} \in M_m(M_n(R))$ można jednoznacznie zapisać w postaci $A = \sum_{i,j=1}^{m}(\sum_{k,l=1}^{n}(A_{ij}[k, l]E_{kl}))E_{ij} = \sum_{i,j=1}^{m}\sum_{k,l=1}^{n}((A_{ij}[k, l]E_{kl})E_{ij})$. Ponieważ φ jest izomorfizmem grup addytywnych, więc z naszych rozważań otrzymujemy, że pozostaje wykazać, że dla dowolnych $a, b \in R$, $i_1, i_2, j_1, j_2 \in \{1, 2, \ldots, m\}$, $k_1, k_2, l_1, l_2 \in \{1, 2, \ldots, n\}$ zachodzi:

$$\varphi(((aE_{k_1l_1})E_{i_1j_1}) \cdot ((bE_{k_2l_2})E_{i_2j_2})) = \varphi((aE_{k_1l_1})E_{i_1j_1}) \cdot \varphi((bE_{k_2l_2})E_{i_2j_2}).$$

Wprost z określenia φ otrzymujemy dla $a \in R$, $i, j \in \{1, 2, \ldots, m\}$, $k, l \in \{1, 2, \ldots, n\}$:

$$\varphi((aE_{kl})E_{ij}) = aE_{(i-1)n+k,(j-1)n+l}.$$

Możliwe są teraz tylko dwa przypadki: 1. $j_1 \neq i_2$ oraz 2. $j_1 = i_2$.

W przypadku 1, $(j_1 - 1)n + l_1 \neq (i_2 - 1)n + k_2$, więc $((aE_{k_1l_1})E_{i_1j_1}) \cdot ((bE_{k_2l_2})E_{i_2j_2}) = 0$ oraz $\varphi((aE_{k_1l_1})E_{i_1j_1}) \cdot \varphi((bE_{k_2l_2})E_{i_2j_2}) = 0$, a zatem dowodzony wzór zachodzi.

W przypadku 2, $((aE_{k_1l_1})E_{i_1j_1}) \cdot ((bE_{k_2l_2})E_{i_2j_2}) = ((aE_{k_1l_1}) \cdot (bE_{k_2l_2}))E_{i_1j_2}$ i teraz mamy znawu dwa przypadki: (a) $l_1 \neq k_2$ oraz (b) $l_1 = k_2$. W przypadku (a), $(aE_{k_1l_1}) \cdot (bE_{k_2l_2}) = 0$ oraz $(j_1 - 1)n + l_1 \neq (i_2 - 1)n + k_2$, więc $\varphi((aE_{k_1l_1})E_{i_1j_1}) \cdot \varphi((bE_{k_2l_2})E_{i_2j_2}) = 0$, a zatem dowodzony wzór zachodzi. Natomiast w przypadku (b), $(aE_{k_1l_1}) \cdot (bE_{k_2l_2}) = (ab)E_{k_1l_2}$, skąd $((aE_{k_1l_1})E_{i_1j_1}) \cdot ((bE_{k_2l_2})E_{i_2j_2}) = ((ab)E_{k_1l_2})E_{i_1j_2}$, czyli $\varphi(((aE_{k_1l_1})E_{i_1j_1}) \cdot ((bE_{k_2l_2})E_{i_2j_2})) = (ab)E_{(i_1-1)n+k_1,(j_2-1)n+l_2}$ oraz $(j_1-1)n+l_1 = (i_2-1)n+k_2$, więc $\varphi((aE_{k_1l_1})E_{i_1j_1}) \cdot \varphi((bE_{k_2l_2})E_{i_2j_2}) = (aE_{(i_1-1)n+k_1,(j_1-1)n+l_1}) \cdot (bE_{(i_2-1)n+k_2,(j_2-1)n+l_2}) =$

$(ab)E_{(i_1-1)n+k_1,(j_2-1)n+l_2}$, a zatem nasz wzór też jest prawdziwy w tym przypadku. □

Twierdzenie 15.17. *Jeżeli R jest pierścieniem regularnym w sensie von Neumanna, to dla każdej liczby naturalnej n pierścień macierzy $M_n(R)$ też jest regularny w sensie von Neumanna.*

Dowód. Z twierdzenia 15.2 wynika, że pierścień $M_2(R)$ jest regularny w sensie von Neumanna. Załóżmy, że dla pewnego $m \in \mathbb{N}$ pierścień $M_{2^m}(R)$ jest regularny w sensie von Neumanna. Wtedy z twierdzenia 15.2 pierścień $M_2(M_{2^m}(R))$ jest regularny w sensie von Neumanna. Zatem ze stwierdzenia 15.15 pierścień $M_{2^{m+1}}(R)$ jest regularny w sensie von Neumanna. Wobec tego przez indukcję mamy, że dla dowolnego $s \in \mathbb{N}$ pierścień $M_{2^s}(R)$ jest regularny w sensie von Neumanna. Weźmy dowolną liczbę naturalną n. Wtedy istnieje liczba naturalna s taka, że $2^s > n$. Weźmy dowolne $A \in M_n(R)$. Z regularności pierścienia $M_{2^s}(R)$ wynika istnienie macierzy $X \in M_n(R)$, $Y \in M_{n\times(2^s-n)}(R)$, $Z \in M_{(2^s-n)\times n}(R)$, $U \in M_{(2^s-n)\times(2^s-n)}(R)$ takich, że $\begin{bmatrix} A & 0_{n\times(2^s-n)} \\ 0_{(2^s-n)\times n} & 0_{(2^s-n)\times(2^s-n)} \end{bmatrix} = \begin{bmatrix} A & 0_{n\times(2^s-n)} \\ 0_{(2^s-n)\times n} & 0_{(2^s-n)\times(2^s-n)} \end{bmatrix} \cdot \begin{bmatrix} X & Y \\ Z & U \end{bmatrix} \cdot \begin{bmatrix} A & 0_{n\times(2^s-n)} \\ 0_{(2^s-n)\times n} & 0_{(2^s-n)\times(2^s-n)} \end{bmatrix}$, skąd $\begin{bmatrix} A & 0_{n\times(2^s-n)} \\ 0_{(2^s-n)\times n} & 0_{(2^s-n)\times(2^s-n)} \end{bmatrix} = \begin{bmatrix} AXA & 0_{n\times(2^s-n)} \\ 0_{(2^s-n)\times n} & 0_{(2^s-n)\times(2^s-n)} \end{bmatrix}$, czyli $A = AXA$ i pierścień $M_n(R)$ jest regularny w sensie von Neumanna. □

15.2 Pierścienie silnie regularne

Stwierdzenie 15.18. *Dla dowolnego pierścienia R następujące warunki są równoważne:*

(i) R jest zredukowany i regularny w sensie von Neumanna,
(ii) $a \in a^2R$ dla dowolnego $a \in R$,
(iii) $a \in Ra^2$ dla dowolnego $a \in R$.

Dowód. $(i) \Rightarrow (ii)$. Weźmy dowolne $a \in R$. Wtedy istnieje $x \in R$ takie, że $a = axa$. Stąd $(a - a^2x)a = a^2 - a(axa) = a^2 - a^2 = 0$, więc $(a - a^2x)^2 = 0$. Ale pierścień R jest zredukowany, więc $a - a^2x = 0$, skąd $a = a^2x$ i $a \in a^2R$.

$(ii) \Rightarrow (i)$. Weźmy dowolne $a \in R$ takie, że $a^2 = 0$. Wtedy istnieje $y \in R$ takie, że $a = a^2y$. Stąd $a = 0$ i pierścień R jest zredukowany. Niech $a \in R$. Wtedy istnieje $x \in R$ taki, że $a = a^2x$. Stąd $a(a - axa) = a^2 - (a^2x)a = a^2 - a^2 = 0$, więc $(a - axa)^2 = 0$. Ale pierścień R jest zredukowany, więc $a - axa = 0$ i $a = axa$, a zatem pierścień R jest regularny w sensie von Neumanna.

Analogicznie dowodzi się równoważności warunków (i) oraz (iii). □

Definicja 15.19. Zredukowane pierścienie regularne w sensie von Neumanna nazywamy **pierścieniami silnie regularnymi**.

Stwierdzenie 15.20. *Każdy obraz homomorficzny pierścienia silnie regularnego jest pierścieniem silnie regularnym.*

Dowód. Niech $f\colon R \to S$ będzie homomorfizmem pierścienia silnie regularnego R na pierścień S. Weźmy dowolne $a \in S$. Wtedy istnieje $a_1 \in R$ takie, że $f(a_1) = a$. Ale R jest silnie regularny, więc na mocy stwierdzenia 15.18 istnieje $b_1 \in R$ takie, że $a_1 = a_1^2 b_1$. Stąd $a = a^2 f(b_1)$ i na mocy stwierdzenia 15.18 pierścień S jest silnie regularny. □

Stwierdzenie 15.21. *Klasa pierścieni silnie regularnych jest zamknięta na rozszerzenia.*

Dowód. Niech $I \lhd R$ i niech I oraz R/I będą pierścieniami silnie regularnymi. Wtedy I i R/I są pierścieniami zredukowanymi, więc na mocy stwierdzenia 13.9 pierścień R jest zredukowany. Ponadto I i R/I są pierścieniami regularnymi w sensie von Neumanna, więc ze stwierdzenia 15.3 pierścień R jest regularny w sensie von Neumanna. Zatem pierścień R jest silnie regularny. □

Stwierdzenie 15.22. *Jeżeli R jest pierścieniem silnie regularnym, to każdy jego ideał jednostronny jest pierścieniem silnie regularnym. W szczególności każdy ideał pierścienia silnie regularnego jest pierścieniem silnie regularnym.*

Dowód. Niech $L <_l R$, gdzie R jest pierścieniem silnie regularnym. Weźmy dowolne $a \in L$. Wtedy na mocy stwierdzenia 15.18 istnieje $x \in R$ takie, że $a = xa^2$, skąd $a = xxa^2a = (x^2a)a^2$ i $x^2a \in L$, bo $L <_l R$. Zatem ze stwierdzenia 15.18 pierścień L jest silnie regularny. Podobnie pokazuje się, że jeżeli $P <_r R$, to P jest pierścieniem silnie regularnym. □

Stwierdzenie 15.23. *Pierścień silnie regularny R jest pierścieniem pierwszym wtedy i tylko wtedy, gdy R jest pierścieniem z dzieleniem.*

Dowód. Oczywiście każdy pierścień z dzieleniem jest zredukowany i pierwszy oraz jest regularny w sensie von Neumanna, a więc jest pierścieniem silnie regularnym.

Na odwrót, niech R będzie silnie regularnym pierścieniem pierwszym. Wtedy R jest zredukowanym pierścieniem pierwszym, wiec ze stwierdzenia 13.11 R jest dziedziną. Stąd i ze stwierdzenia 15.9 R jest pierścieniem z dzieleniem. □

Stwierdzenie 15.24. *Każdy ideał jednostronny pierścienia silnie regularnego R jest ideałem pierścienia R.*

Dowód. Niech $L <_l R$ i weźmy dowolne $a \in L$ i dowolne $r \in R$. Ze stwierdzenia 15.10 istnieje idempotent $e \in Ra$ taki, że $Ra = Re$. Ale pierścień R jest zredukowany, więc $e \in Z(R)$. Ponadto $a = ye$ dla pewnego $y \in R$, więc $ar = (ye)r = y(er) = (yr)e \in Ra \subseteq L$. Stąd $L \lhd R$.

Analogicznie pokazuje się, że jeśli $P <_r R$, to $P \lhd R$. □

Twierdzenie 15.25. *Pierścień zredukowany R jest silnie regularny wtedy i tylko wtedy, gdy każdy jego obraz pierwszy jest pierścieniem z dzieleniem.*

Dowód. Załóżmy, że pierścień R jest silnie regularny i niech S będzie jego obrazem homomorficznym i niech S będzie pierścieniem pierwszym. Wtedy na mocy stwierdzenia 15.20 S jest pierścieniem silnie regularnym. Zatem ze stwierdzenia 15.23 S jest pierścieniem z dzieleniem.

Na odwrót, załóżmy, że R jest pierścieniem zredukowanym i każdy pierwszy obraz R jest pierścieniem z dzieleniem. Niech I będzie ideałem półpierwszym pierścienia R. Wtedy na mocy twierdzenia 4.37 I jest częścią wspólną niepustej rodziny $\mathcal{A}$ wszystkich ideałów pierwszych pierścienia R zawierających I. Weźmy dowolne $r \in R$ takie, że $r^2 \in I$. Wtedy dla każdego $A \in \mathcal{A}$ jest $r^2 \in A$, skąd $(r + A)^2 = 0$ w pierścieniu R/A, który jest z dzieleniem. Zatem $r \in A$ dla każdego $A \in \mathcal{A}$, skąd $r \in I$. W ten sposob pokazaliśmy, że pierścień R/I jest zredukowany.

Załóżmy, że istnieje $a \in R$ takie, że $a \notin aRa$. Niech $\mathcal{R}$ będzie rodziną takich ideałów półpierwszych I pierścienia R, że $a \notin aRa + I$. Ponieważ pierścień R jest zredukowany i $a \notin aRa$, więc $\{0\} \in \mathcal{R}$. Zatem rodzina $\mathcal{R}$ jest niepusta. Niech $\{I_s\}_{s\in S}$ będzie łańcuchem ideałów z rodziny $\mathcal{R}$. Oczywiście $a \notin aRa + \bigcup_{s\in S} I_s$. Zauważmy też, że jeśli dla pewnego $r \in R$, $r^2 \in \bigcup_{s\in S} I_s$, to $r^2 \in I_s$ dla pewnego $s \in S$. Jednakże, jak wykazaliśmy wcześniej R/I_s jest pierścieniem zredukowanym, więc $r \in I_s$. To dowodzi, że $\bigcup_{s\in S} I_s \in \mathcal{R}$. Stosując lemat Zorna możemy więc znaleźć w $\mathcal{R}$ ideał maksymalny Q. Zauważmy, że Q nie może być ideałem pierwszym, gdyż wówczas z założenia R/Q byłby pierścieniem z dzieleniem i mielibyśmy, że $a \in aRa + Q$. Istnieją więc ideały A, B pierścienia R takie, że $Q \subset A$, $Q \subset B$ oraz $AB \subseteq Q$. Niech $K = \{r \in R : rB \subseteq Q\}$ oraz $L = \{r \in R : Kr \subseteq Q\}$. Oczywiście K i L są ideałami w R oraz $A \subseteq K$ i $B \subseteq L$. Zauważmy, że $(K \cap L)^2 \subseteq KL \subseteq Q$. Z półpierwszości ideału Q wynika więc, że $K \cap L \subseteq Q$. Zauważmy również, że jeśli I jest takim ideałem R, że $I^2 \subseteq L$, to $KIKI \subseteq KI^2 \subseteq KL \subseteq Q$. Z półpierwszości Q wynika więc, że $KI \subseteq Q$. Z definicji ideału L otrzymujemy, że $I \subseteq L$, co dowodzi, że L jest ideałem półpierwszym. Podobnie wykazujemy, że K jest ideałem półpierwszym. Z maksymalności Q wynika, że $a \in aRa + K$ oraz $a \in aRa + L$. Zatem $a - axa \in K$ oraz $a - aya \in L$ dla pewnych $x, y \in R$. Wówczas $a - a(x + y - xay)a = a - axa - (a - axa)ya \in K$, a także $a - a(x + y - xay)a = a - aya - ax(a - aya) \in L$. Stąd więc $a \in aRa + (K \cap L) \subseteq aRa + Q$. Uzyskana sprzeczność kończy dowód. □