Wykład 10
Homomorfizmy i ideały

1 Pojęcie ideału pierścienia

Definicja 10.1. *Ideałem pierścienia* P nazywamy niepusty podzbiór $I \subseteq P$ taki, że

$$\text{(I) } \forall_{i,j\in I}\ i-j \in I \text{ oraz (II) } \forall_{i\in I}\forall_{a\in P}\ a\cdot i \in I.$$

Napis: $I \lhd P$, oznacza, że I jest ideałem pierścienia P.

Przykład 10.2. W dowolnym pierścieniu P zbiór $\{0\}$ jest ideałem (nazywamy go *ideałem zerowym*), gdyż $0-0=0\in\{0\}$ i $a\cdot 0=0\in\{0\}$ dla każdego $a\in P$. Ponadto cały pierścień P jest ideałem P (nazywamy go *ideałem niewłaściwym*). Ideały $I\neq P$ nazywamy *ideałami właściwymi*.

Stwierdzenie 10.3. *Dla ideału I pierścienia P równoważne są warunki:*
(i) $I=P$,
(ii) $1\in I$,
(iii) pewien element odwracalny pierścienia P należy do I.
W szczególności I jest ideałem właściwym w P wtedy i tylko wtedy, gdy $1\notin I$.

Dowód. Implikacje $(i)\Rightarrow(ii)$ i $(ii)\Rightarrow(iii)$ są oczywiste. Dla dowodu implikacji $(iii)\Rightarrow(i)$ załóżmy, że dla pewnego $u\in P^*$ jest $u\in I$. Wówczas $1=u^{-1}\cdot u\in I$ na mocy (II). Wobec tego dla dowolnego $a\in P$ na mocy (II) mamy, że $a=a\cdot 1\in I$, skąd $I=P$. □

Stwierdzenie 10.4. *Każde ciało K ma dokładnie dwa ideały: $\{0\}$ i K.*

Dowód. Ponieważ K jest ciałem, więc $|K|>1$, skąd $\{0\}$ i K są różnymi ideałami K. Niech I będzie niezerowym ideałem K. Wtedy istnieje niezerowe $i\in I$, skąd $1=i^{-1}\cdot i\in I$. Zatem ze Stwierdzenia 10.3, $I=K$. □

Uwaga 10.5. Niech I będzie ideałem pierścienia P. Wtedy na mocy (I), $I\leq P^+$. W szczególności $0\in I$. Ponadto jeśli $i_1,\ldots,i_n\in I$ oraz $a_1,\ldots,a_n\in P$, to $a_1\cdot i_1,\ldots,a_n\cdot i_n\in I$, skąd $a_1\cdot i_1+\ldots+a_n\cdot i_n\in I$. Zauważmy też, że chociaż $\mathbb{Z}\leq\mathbb{Q}^+$, to jednak na mocy Stwierdzenia 10.4, $\mathbb{Z}$ nie jest ideałem pierścienia $\mathbb{Q}$.

Twierdzenie 10.6. *Część wspólna dowolnej niepustej rodziny $\{I_t\}_{t\in T}$ ideałów pierścienia P jest ideałem pierścienia P.*

Dowód. Niech $I=\bigcap_{t\in T}I_t$. Wtedy $0\in I_t$ dla $t\in T$, więc $0\in I$. Dla $i,j\in I$ mamy, że $i,j\in I_t$ dla każdego $t\in T$, więc $i-j\in I_t$ dla $t\in T$, skąd $i-j\in I$. Ponadto dla

$a \in P$, $i \in I$ mamy, że $i \in I_t$ dla $t \in T$, więc $ai \in I_t$ dla każdego $t \in T$, skąd $ai \in I$. Zatem $I \lhd P$. $\square$

Uwaga 10.7. Z Twierdzenia 10.6 wynika, że dla dowolnego podzbioru X pierścienia P istnieje najmniejszy w sensie inkluzji ideał pierścienia P zawierający zbiór X. Nazywamy go *ideałem generowanym* przez zbiór X i oznaczamy przez (X). Natomiast X nazywamy *zbiorem generatorów* ideału (X). Np. $(\emptyset) = \{0\}$. Jeśli zbiór X jest skończony oraz $X = \{a_1, \ldots, a_n\}$, to zamiast $(\{a_1, \ldots, a_n\})$ piszemy $(a_1, \ldots, a_n)$. Jeżeli istnieje $a \in P$ takie, że $I = (a)$, to mówimy, że *ideał I jest główny.* Jeżeli istnieją $a_1, \ldots, a_n \in P$ takie, że $I = (a_1, \ldots, a_n)$, to mówimy, że *ideał I jest skończenie generowany.*

Twierdzenie 10.8. *Dla dowolnych elementów $a_1, \ldots, a_n$ pierścienia P zachodzi wzór:*

$$(a_1, \ldots, a_n) = \{x_1a_1 + \ldots + x_na_n : x_1, \ldots, x_n \in P\}.$$

W szczególności $(a) = \{xa \ : \ x \in P\}$ dla każdego $a \in P$.

Dowód. Oznaczmy $J = \{x_1a_1 + \ldots + x_na_n : x_1, \ldots, x_n \in P\}$. Wtedy $a_k = 0 \cdot a_1 + \ldots + 1 \cdot a_k + \ldots + 0 \cdot a_n \in J$ dla $k = 1, \ldots, n$. Zatem $\{a_1, \ldots, a_n\} \subseteq J$. Niech $i, j \in J$, $a \in P$. Wtedy istnieją $x_1, \ldots, x_n, y_1, \ldots, y_n \in P$ takie, że $i = x_1a_1 + \ldots + x_na_n$ oraz $j = y_1a_1 + \ldots + y_na_n$, więc $i - j = (x_1 - y_1)a_1 + \ldots + (x_n - y_n)a_n \in J$, $ai = (ax_1)a_1 + \ldots + (ax_n)a_n \in J$. Zatem $J \lhd P$ oraz $\{a_1, \ldots, a_n\} \subseteq J$. Niech A będzie dowolnym ideałem pierścienia P zawierającym zbiór $\{a_1, \ldots, a_n\}$. Wtedy z Uwagi 10.5 mamy, że $x_1a_1 + \ldots + x_na_n \in A$ dla dowolnych $x_1, \ldots, x_n \in P$. Zatem $J \subseteq A$, czyli J jest najmniejszym ideałem pierścienia P zawierającym zbiór $\{a_1, \ldots, a_n\}$. Zatem $J = (a_1, \ldots, a_n)$. $\square$

Przykład 10.9. Z teorii grup wiemy, że wszystkimi podgrupami grupy $\mathbb{Z}^+$ są zbiory wielokrotności ustalonych nieujemnych liczb całkowitych. Na mocy Twierdzenia 10.8 mamy więc stąd, że każdy ideał pierścienia $\mathbb{Z}$ jest główny i wszystkimi ideałami tego pierścienia są ideały postaci (k) dla $k = 0, 1, 2, \ldots$.

Podobnie jest w pierścieniu $\mathbb{Z}_m$, gdyż każda niezerowa podgrupa grupy addytywnej tego pierścienia składa się z całkowitych wielokrotności ustalonych dzielników naturalnych liczby m. Wynika stąd, że wszystkie ideały pierścienia $\mathbb{Z}_m$ są postaci: (d), gdzie $d = 0$ lub $d < m$ jest naturalnym dzielnikiem liczby m. W szczególności każdy ideał pierścienia $\mathbb{Z}_m$ jest główny i ten pierścień posiada tyle ideałów, ile dzielników naturalnych ma liczba m.

Twierdzenie 10.10. *Jeżeli $I_1, \ldots, I_n$ są ideałami pierścienia P, to $I_1 + \ldots + I_n \lhd P$.*

Dowód. Z teorii grup mamy

$$I_1 + \ldots + I_n = \{i_1 + \ldots + i_n : i_k \in I_k \ \text{ dla } \ k = 1, \ldots, n\}$$

jest podgrupą grupy P^+ zawierającą $I_1 \cup \ldots \cup I_n$. Niech $a \in P$, $i \in I_1 + \ldots + I_n$. Wtedy istnieją $i_k \in I_k$ dla $k = 1, \ldots, n$ takie, że $i = i_1 + \ldots + i_n$, skąd $ai = ai_1 + \ldots + ai_n \in I_1 + \ldots + I_n$, bo $ai_k \in I_k$ dla $k = 1, \ldots, n$. $\square$

Twierdzenie 10.11. *Niech I, J będą ideałami pierścienia P. Wówczas zbiór*

$$I \cdot J = \left\{ \sum_{k=1}^{n} i_k j_k \ : \ i_k \in I, j_k \in J \text{ dla } k = 1, \ldots, n; \ n \in \mathbb{N} \right\}$$

jest ideałem pierścienia P oraz $I \cdot J \subseteq I \cap J$.

Dowód. Ponieważ $0 \in I$ oraz $0 \in J$, więc $0 = 0 \cdot 0 \in I \cdot J$ ($n = 1$, $i_1 = 0$, $j_1 = 0$). Weźmy dowolne $c \in P$ oraz dowolne $x, y \in I \cdot J$. Wtedy istnieją $n, m \in \mathbb{N}$ oraz $i_1, \ldots, i_n, a_1, \ldots, a_m \in I$, $j_1, \ldots, j_n, b_1, \ldots, b_m \in J$ takie, że $x = i_1 j_1 + \ldots + i_n j_n$ i $y = a_1 b_1 + \ldots + a_m b_m$. Zatem $x - y = i_1 j_1 + \ldots + i_n j_n + (-a_1) b_1 + \ldots + (-a_m) b_m \in I \cdot J$ oraz $c \cdot x = (ci_1) j_1 + \ldots + (ci_n) j_n \in I \cdot J$, bo $-a_t \in I$ dla wszystkich $t = 1, \ldots, m$ i $ci_k \in I$ dla wszystkich $k = 1, \ldots, n$. Stąd $I \cdot J \lhd P$. Ponadto $i_k j_k \in I$ oraz $i_k j_k \in J$, więc $i_k j_k \in I \cap J$ dla wszystkich $k = 1, \ldots, n$, skąd $x \in I \cdot J$ i $I \cdot J \subseteq I \cap J$. $\square$

Stwierdzenie 10.12. Niech A i B będą dowolnymi pierścieniami. Wówczas K jest ideałem pierścienia $A \times B$ wtedy i tylko wtedy, gdy $K = I \times J$, gdzie $I \lhd A$ i $J \lhd B$.

Dowód. Niech $I \lhd A$, $J \lhd B$ i $K = I \times J$. Ponieważ $I, J \neq \emptyset$, więc $K \neq \emptyset$. Weźmy dowolne $x \in A \times B$ i dowolne $i, j \in K$. Wtedy istnieją $i_1, i_2 \in I$, $j_1, j_2 \in J$ oraz $a \in A$, $b \in B$ takie, że $x = (a, b)$, $i = (i_1, j_1)$, $j = (i_2, j_2)$. Stąd $i_1 - i_2 \in I$, $j_1 - j_2 \in J$ oraz $i - j = (i_1 - i_2, j_1 - j_2)$, więc $i - j \in K$. Ponadto $x \cdot i = (a \cdot i_1, b \cdot j_1) \in K$, bo $a \cdot i_1 \in I$ oraz $b \cdot j_1 \in J$. Zatem $K \lhd A \times B$.

Na odwrót, niech $K \lhd A \times B$. Oznaczmy: $I = \{a \in A \ : \ (a, 0) \in K\}$, $J = \{b \in B \ : \ (0, b) \in B\}$. Wtedy dla dowolnego $(a, b) \in I \times J$ mamy, że $(a, b) = (a, 0) + (0, b) \in K$, skąd $I \times J \subseteq K$. Ponadto, jeśli $(x, y) \in K$, to $(1, 0) \cdot (x, y) \in K$ i $(0, 1) \cdot (x, y) \in K$, skąd $(x, 0) \in K$ i $(0, y) \in K$. Zatem $x \in I$, $y \in J$ i $(x, y) \in I \times J$. Wobec tego $K = I \times J$. Pozostaje jeszcze do wykazania, że $I \lhd A$ i $J \lhd B$. Ale $(0, 0) \in K$, więc $0 \in I$ i $0 \in J$, skąd zbiory I, J są niepuste. Weźmy dowolne $i_1, i_2 \in I$, $j_1, j_2 \in J$ i dowolne $a \in A$, $b \in B$. Wtedy $(i_1, 0), (i_2, 0) \in K$ i $(0, j_1), (0, j_2) \in K$, więc $(i_1 - i_2, 0) = (i_1, 0) - (i_2, 0) \in K$ i $(0, j_1 - j_2) = (0, j_1) - (0, j_2) \in K$, co oznacza, że $i_1 - i_2 \in I$ i $j_1 - j_2 \in J$. Ponadto $(a \cdot i_1, 0) = (a, 0) \cdot (i_1, 0) \in K$ i $(0, b \cdot j_1) = (0, b) \cdot (0, j_1) \in K$, co oznacza, że $a \cdot i_1 \in I$ oraz $b \cdot j_1 \in J$. Wobec tego $I \lhd A$ i $J \lhd B$. $\square$

Zagadka 1. Niech P będzie dowolnym podpierścieniem ciała $\mathbb{Q}$ i niech $I \lhd P$. Udowodnij, że istnieje $n \in \mathbb{N}_0$ takie, że $I = (n)$.

Zagadka 2. Udowodnij, że dla dowolnych elementów a i b pierścienia P zachodzi wzór:

$$(a) \cdot (b) = (ab).$$

Zagadka 3. Udowodnij, że dla dowolnych elementów $a_1, a_2, \ldots, a_n$ pierścienia P zachodzi wzór:

$$(a_1, a_2, \ldots, a_n) = (a_1) + (a_2) + \ldots + (a_n).$$

Zagadka 4. Udowodnij, że jeśli pierścień P posiada dokładnie dwa ideały, to P jest ciałem.

2 Konstrukcja pierścienia ilorazowego

Niech I będzie ideałem pierścienia P. Wówczas I jest podgrupą grupy abelowej P^+, więc można zbudować grupę ilorazową $P/I = \{a + I : a \in P\}$. Ponadto:

$$a + I = \{a + i : i \in I\} \text{ dla } a \in P,$$

$$a + I = b + I \Leftrightarrow a - b \in I \text{ dla } a, b \in P,$$

$$(a + I) + (b + I) = (a + b) + I \text{ dla } a, b \in P,$$

$$(P/I, +, I) \text{ tworzy grupę abelową.}$$

W P/I można też określić naturalne mnożenie:

$$(a + I) \cdot (b + I) = ab + I \text{ dla } a, b \in P.$$

Sprawdzimy, czy takie mnożenie warstw nie zależy od wyboru reprezentantów. W tym celu weźmy dowolne $a_1, a_2, b_1, b_2 \in P$ takie, że $a_1 + I = a_2 + I$ oraz $b_1 + I = b_2 + I$. Wtedy $i = a_1 - a_2 \in I$ oraz $j = b_1 - b_2 \in I$, więc $a_1 = a_2 + i$, $b_1 = b_2 + j$, skąd $a_1b_1 - a_2b_2 = (a_2+i)(b_2+j) - a_2b_2 = a_2j + ib_2 + ij \in I$, gdyż $I \lhd P$. Zatem $a_1b_1 + I = a_2b_2 + I$ i mnożenie warstw jest dobrze określone.

Dla $a, b \in P$ mamy, że $(b + I) \cdot (a + I) = ba + I = ab + I = (a + I) \cdot (b + I)$, więc mnożenie warstw jest przemienne.

Dla $a, b, c \in P$ mamy, że $(a + I) \cdot [(b + I) \cdot (c + I)] = (a + I) \cdot (bc + I) = a(bc) + I = (ab)c + I = (ab + I) \cdot (c + I) = [(a + I) \cdot (b + I)] \cdot (c + I)$, więc mnożenie warstw jest łączne. Ponadto $(a + I) \cdot [(b + I) + (c + I)] = (a + I) \cdot [(b + c) + I] = a(b + c) + I = (ab + ac) + I = (ab + I) + (ac + I) = (a + I) \cdot (b + I) + (a + I) \cdot (c + I)$, więc mnożenie warstw jest rozdzielne względem dodawania warstw. W końcu, $(a + I) \cdot (1 + I) = a \cdot 1 + I = a + I$ dla $a \in P$, więc system algebraiczny $(P/I, +, \cdot, I, 1 + I)$ jest pierścieniem. Nazywamy go *pierścieniem ilorazowym względem ideału* I.

3 Ideały: pierwsze i maksymalne

Definicja 10.13. Ideał I pierścienia P nazywamy
(i) *ideałem pierwszym* pierścienia P, jeżeli

$$I \neq P \text{ oraz } \forall_{a,b \in P}[ab \in I \Rightarrow (a \in I \text{ lub } b \in I)];$$

(ii) *ideałem maksymalnym* pierścienia P, jeżeli

$$I \neq P \text{ oraz } \forall_{J \lhd P}[I \subseteq J \Rightarrow (I = J \text{ lub } J = P)].$$

Twierdzenie 10.14. *Niech I będzie ideałem pierścienia P. Wówczas równoważne są warunki:*

(i) I jest ideałem pierwszym pierścienia P;

(ii) pierścień ilorazowy P/I jest dziedzią całkowitości.

Dowód. $(i) \Rightarrow (ii)$. Z założenia $I \neq P$, więc $1 \notin I$, czyli $1 + I \neq 0 + I$. Zatem pierścień P/I jest niezerowy. Niech $a, b \in P$ będą takie, że $(a + I) \cdot (b + I) = I$. Wtedy $ab + I = 0 + I$, więc $ab \in I$. Zatem z pierwszości I wynika, że $a \in I$ lub $b \in I$, czyli $a + I = 0 + I = I$ lub $b + I = 0 + I = I$. Zatem P/I jest dziedziną całkowitości.

$(ii) \Rightarrow (i)$. Z założenia $1 + I \neq 0 + I$, skąd $1 \notin I$, więc $I \neq P$. Weźmy dowolne $a, b \in P$ takie, że $ab \in I$. Wtedy $ab + I = 0 + I$, skąd $(a + I) \cdot (b + I) = I$. Ale P/I jest dziedziną całkowitości, więc $a + I = I = 0 + I$ lub $b + I = I = 0 + I$, czyli $a \in I$ lub $b \in I$. Zatem I jest ideałem pierwszym pierścienia P. □

Twierdzenie 10.15. *Niech I będzie ideałem pierścienia P. Wówczas równoważne są warunki:*

(i) I jest ideałem maksymalnym pierścienia P,

(ii) pierścień ilorazowy P/I jest ciałem.

Dowód. $(i) \Rightarrow (ii)$. Z założenia $I \neq P$, więc $1 \notin I$, skąd $1 + I \neq 0 + I = I$. Weźmy dowolne $a \in P$ takie, że $a + I \neq 0 + I$. Wtedy $a \notin I$. Zatem $I \subset I + (a)$, więc z Twierdzenia 10.10 i z maksymalności I wynika, że $I + (a) = P$. Stąd $1 = i + xa$ dla pewnych $i \in I$ oraz $x \in P$. Zatem $1 - xa = i \in I$, więc $1 + I = xa + I = (x + I) \cdot (a + I)$, czyli $a + I$ jest elementem odwracalnym pierścienia P/I. Zatem P/I jest ciałem.

$(ii) \Rightarrow (i)$. Z założenia $1 + I \neq 0 + I$, skąd $1 \notin I$, więc $I \neq P$. Niech $J \lhd P$ oraz $I \subset J$. Wystarczy wykazać, że $J = P$. Ale istnieje $a \in J \setminus I$, więc $a + I \neq 0 + I$. Zatem istnieje $x \in P$ taki, że $(a + I) \cdot (x + I) = 1 + I$, czyli $ax + I = 1 + I$. Zatem $i = ax - 1 \in I$. Stąd $1 = ax - i \in J$, bo $ax \in J$, $i \in I \subset J$. Zatem $1 \in J$, skąd $J = P$. □

Ponieważ każde ciało jest dziedziną całkowitości, więc z Twierdzeń 10.14 i 10.15 mamy od razu następujący

Wniosek 10.16. *Każdy ideał maksymalny pierścienia P jest ideałem pierwszym pierścienia P.* □

Uwaga 10.17. Implikacja odwrotna nie jest prawdziwa, bo np. $\{0\}$ jest ideałem pierwszym pierścienia $\mathbb{Z}$, ale $\{0\} \subset (2) \subset \mathbb{Z}$, więc $\{0\}$ nie jest ideałem maksymalnym pierścienia $\mathbb{Z}$.

4 Homomorfizmy pierścieni

Definicja 10.18. Niech A, B będą pierścieniami. Przekształcenie $f\colon A \to B$ spełniające warunki:
(I) $f(1) = 1$,
(II) $\forall_{a,b\in A}\ f(a+b) = f(a) + f(b)$,
(III) $\forall_{a,b\in A}\ f(ab) = f(a)f(b)$
nazywamy *homomorfizmem* pierścienia A w pierścień B. Natomiast zbiór

$$Ker(f) = \{x \in A : f(x) = 0\}$$

nazywamy *jądrem homomorfizmu* f. Jeżeli dodatkowo f jest różnowartościowe, to mówimy, że f jest *zanurzeniem pierścienia A w pierścień B*. Jeżeli zaś homomorfizm f jest bijekcją, to mówimy, że f jest *izomorfizmem pierścieni.*

Definicja 10.19. Powiemy, że pierścień B jest *obrazem homomorficznym* pierścienia A, jeżeli istnieje homomorfizm $f\colon A \to B$ pierścienia A na pierścień B.

Definicja 10.20. Powiemy, że pierścień A *zanurza się w pierścień* B, jeśli istnieje zanurzenie $f\colon A \to B$.

Definicja 10.21. Powiemy, że pierścienie A i B są *izomorficzne* i piszemy, $A \cong B$, jeżeli istnieje izomorfizm $f\colon A \to B$.

Definicja 10.22. *Automorfizmem pierścienia A* nazywamy każdy izomorfizm $f\colon A \to A$.

Uwaga 10.23. Zauważmy, że jeśli f jest homomorfizmem pierścienia A w pierścień B, to f jest homomorfizmem grupy A^+ w grupę B^+. Ponadto, jeśli h jest homomorfizmem grupy A^+ w grupę B^+, to h jest homomorfizmem pierścienia A w pierścień B wtedy i tylko wtedy, gdy $h(1) = 1$ i $h(ab) = h(a)h(b)$ dla dowolnych $a, b \in A$.

Stwierdzenie 10.24. *Złożenie homomorfizmów pierścieni jest homomorfizmem pierścieni, tzn. jeżeli $f\colon A \to B$ i $g\colon B \to C$ są homomorfizmami pierścieni, to $g \circ f\colon A \to C$ też jest homomorfizmem pierścieni. W szczególności złożenie izomorfizmów pierścieni jest izomorfizmem pierścieni.*

Dowód. Rzeczywiście, na mocy Uwagi 10.23 i Stwierdzenia 5.15 dla dowolnych $a, b \in A$: $(g \circ f)(a+b) = (g \circ f)(a) + (g \circ f)(b)$. Ponadto $(g \circ f)(1) = g(f(1)) = g(1) = 1$ oraz dla dowolnych $a, b \in A$: $(g \circ f)(ab) = g(f(ab)) = g(f(a)f(b)) = (g \circ f)(a) \cdot (g \circ f)(b)$. □

Stwierdzenie 10.25. *Jeżeli $f\colon A \to B$ jest izomorfizmem pierścieni, to $f^{-1}\colon B \to A$ też jest izomorfizmem pierścieni.*

Dowód. Ze Stwierdzenia 5.16 i z Uwagi 10.23 wynika, że f^{-1} jest bijekcją i f^{-1} jest izomorfizmem grupy B^+ na grupę A^+. Ponadto $f(1) = 1$, więc $f^{-1}(1) = 1$. Weźmy

dowolne $y_1, y_2 \in B$. Wtedy istnieją $x_1, x_2 \in A$ takie, że $y_1 = f(x_1)$ i $y_2 = f(x_2)$, więc $y_1y_2 = f(x_1)f(x_2) = f(x_1x_2)$, skąd $f^{-1}(y_1y_2) = x_1x_2 = f^{-1}(y_1)f^{-1}(y_2)$. $\square$

Ze stwierdzeń 10.24 i 10.25 oraz z tego, że przekształcenie tożsamościowe pierścienia A na pierścień A jest jego automorfizmem wynika od razu następujące

Stwierdzenie 10.26. *Dla dowolnych pierścieni A, B, C:*
a) $A \cong A$,
b) jeśli $A \cong B$, to $B \cong A$,
c) jeśli $A \cong B$ i $B \cong C$, to $A \cong C$. $\square$

Stwierdzenie 10.27. *Niech $f\colon A \to B$ będzie homomorfizmem pierścienia A w pierścień B. Wówczas:*
(i) $f(0) = 0$, $f(-a) = -f(a)$ i $f(ka) = kf(a)$ dla $a \in A$ i $k \in \mathbb{Z}$;
(ii) $f(a_1 + a_2 + \ldots + a_n) = f(a_1) + f(a_2) + \ldots + f(a_n)$ dla dowolnych $a_1, a_2, \ldots, a_n \in A$;
(iii) $f(a_1a_2 \ldots a_n) = f(a_1)f(a_2) \ldots f(a_n)$ dla dowolnych $a_1, a_2, \ldots, a_n \in A$;
(iv) $f(a^n) = [f(a)]^n$ dla dowolnych $a \in A$ i $n \in \mathbb{N}$;
(v) $Ker(f) \lhd A$;
(vi) jeżeli P jest podpierścieniem A, to $f(P)$ jest podpierścieniem B;
(vii) jeżeli S jest podpierścieniem B, to $f^{-1}(S)$ jest podpierścieniem A;
(viii) f jest zanurzeniem $\iff Ker(f) = \{0\}$.

Dowód. (i), (ii) oraz $(viii)$ wynikają od razu ze Stwierdzenia 5.18 i z Uwagi 10.23. Wzór (iii) zachodzi dla $n = 2$. Jeśli zaś ten wzór zachodzi dla $n-1$, gdzie $n \in \{3, 4, \ldots\}$, to dla $a_1, a_2, \ldots, a_n \in A$ mamy: $a_1a_2 \ldots a_n = (a_1a_2 \ldots a_{n-1})a_n$, więc stąd i na mocy założenia indukcyjnego, $f(a_1a_2 \ldots a_n) = f(a_1a_2 \ldots a_{n-1})f(a_n) = f(a_1)f(a_2) \ldots f(a_n)$, co kończy dowód (iii). Podstawiając w (iii), $a = a_1 = a_2 = \ldots = a_n$ uzyskujemy od razu wzór (iv). Ze Stwierdzenia 5.18 i z Uwagi 10.23 mamy, że $Ker(f) \leq A^+$. Ponadto dla $i \in Ker(f)$, $a \in A$ jest $f(i) = 0$, więc $f(ai) = f(a)f(i) = f(a) \cdot 0 = 0$, skąd $ai \in Ker(f)$ i $Ker(f) \lhd A$, co kończy dowód (v).

(vi). Ponieważ $P \leq A^+$, więc z Uwagi 10.23 i ze Stwierdzenia 5.18, $f(P) \leq B^+$. Ale $1 = f(1) \in f(P)$ oraz dla $x, y \in f(P)$ istnieją $a, b \in P$ takie, że $x = f(a)$, $y = f(b)$, więc $xy = f(a)f(b) = f(ab) \in f(P)$, bo $ab \in P$. Zatem $f(P)$ jest podpierścieniem pierścienia B.

(vii). Ponieważ $S \leq B^+$, wic z Uwagi 10.23 i ze Stwierdzenia 5.18, $f^{-1}(S) \leq A^+$. Dalej, $f(1) = 1 \in S$, więc $1 \in f^{-1}(S)$. Ponadto dla $a, b \in f^{-1}(S)$ mamy, że $f(a), f(b) \in S$, skąd $f(ab) = f(a)f(b) \in S$, czyli $ab \in f^{-1}(S)$. Zatem $f^{-1}(S)$ jest podpierścieniem pierścienia A. $\square$

W algebrze utożsamia się pierścienie izomorficzne. Można łatwo pokazać, że jeżeli pierścienie A i B są izomorficzne, to np.
$|A| = |B|$;

A jest ciałem $\iff$ B jest ciałem;
A jest dziedziną całkowitości $\iff$ B jest dziedziną całkowitości.

Twierdzenie 10.28 (o izomorfizmie). *Jeżeli $f\colon A \to B$ jest homomorfizmem pierścienia A na pierścień B, to*

$$B \cong A/Ker(f).$$

Dowód. Niech $F\colon A/Ker(f) \to B$ będzie dane wzorem $F(a + Ker(f)) = f(a)$ dla $a \in A$. Wtedy z dowodu Twierdzenia 5.19, F jest bijekcją i dla $a, b \in A$: $F((a+Ker(f))+(b + Ker(f))) = F(a + Ker(f)) + F(b + Ker(f))$. Ponadto $F(1 + Ker(f)) = f(1) = 1$ oraz dla $a, b \in A$: $F((a+Ker(f))\cdot(b+Ker(f))) = F(ab+Ker(f)) = f(ab) = f(a)f(b) = F(a + Ker(f))F(b + Ker(f))$, więc ostatecznie F jest izomorfizmem pierścieni. $\square$

Wniosek 10.29. *Jeżeli $f\colon A \to B$ jest homomorfizmem pierścienia A w pierścień B, to*

$$f(A) \cong A/Ker(f).$$

Wniosek 10.30. *Niech $f\colon A \to B$ będzie homomorfizmem pierścienia A na pierścień B. Wówczas:*

(i) $Ker(f)$ jest ideałem pierwszym pierścienia $A \Leftrightarrow B$ jest dziedziną całkowitości;

(ii) $Ker(f)$ jest ideałem maksymalnym pierścienia $A \Leftrightarrow B$ jest ciałem.

Dowód. Z twierdzenia o izomorfizmie mamy, że $B \cong A/Ker(f)$. Zatem z twierdze 10.14 i 10.15:

(i) B jest dziedziną całkowitości $\Leftrightarrow$ $A/Ker(f)$ jest dziedziną całkowitości $\Leftrightarrow$ $Ker(f)$ jest ideałem pierwszym pierścienia A;

(ii) B jest ciałem $\Leftrightarrow$ $A/Ker(f)$ jest ciałem $\Leftrightarrow$ $Ker(f)$ jest ideałem maksymalnym pierścienia A. $\square$

Przykład 10.31. Niech $f\colon \mathbb{Z}[x] \to \mathbb{Z}$ będzie dane wzorem $f(w) = w(0)$ dla $w \in \mathbb{Z}[x]$. Łatwo sprawdzić, że wówczas f jest homomorfizmem pierścienia $\mathbb{Z}[x]$ na pierścień $\mathbb{Z}$. Ponieważ $\mathbb{Z}$ jest dziedziną całkowitości, ale nie jest ciałem, więc z Wniosku 10.30, $Ker(f)$ jest ideałem pierwszym, ale nie jest ideałem maksymalnym pierścienia $\mathbb{Z}[x]$. Z twierdzenia Bezout wynika ponadto, że $Ker(f) = (x)$.

Przykład 10.32. Niech $m > 1$ będzie liczbą naturalną i niech $f\colon \mathbb{Z} \to \mathbb{Z}_m$ będzie funkcją daną wzorem:

$$f(k) = [k]_m \text{ dla } k \in \mathbb{Z}.$$

Wtedy $f(a) = a$ dla $a \in \{0, 1, \ldots, m-1\}$, więc f jest „na" oraz $f(1) = 1$. Ponadto dla $k, l \in \mathbb{Z}$:

$$f(k + l) = [k + l]_m \equiv k + l \equiv [k]_m + [l]_m \equiv [k]_m \oplus_m [l]_m \pmod{m},$$

skąd $f(k+l) = f(k) \oplus_m f(l)$ i podobnie $f(kl) = f(k) \odot_m f(l)$. Zatem f jest homomorfizmem pierścienia $\mathbb{Z}$ na pierścień $\mathbb{Z}_m$. Ponadto

$$Ker(f) = \{k \in \mathbb{Z} : [k]_m = 0\} = \{k \in \mathbb{Z} : m \mid k\} = (m).$$

Zatem z twierdzenia o izomorfizmie mamy

$$\mathbb{Z}_m \cong \mathbb{Z}/(m).$$

Ponadto pierścień $\mathbb{Z}_m$ jest ciałem wtedy i tylko wtedy, gdy m jest liczbą pierwszą. Zatem z Wniosku 10.30 wynika, że (m) jest ideałem maksymalnym pierścienia $\mathbb{Z}$ wtedy i tylko wtedy, gdy m jest liczbą pierwszą.

Zagadka 5. Wypisz wszystkie ideały pierścienia $\mathbb{Z}_4 \times \mathbb{Z}_6$. Udowodnij, że każdy z tych ideałów jest główny i wypisz wszystkie ideały pierwsze oraz wszystkie ideały maksymalne tego pierścienia.

Zagadka 6. Niech K będzie dowolnym ciałem. Udowodnij, że pierścienie $K \times K$ i $T_2(K) = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} : a, b \in K \right\}$ nie są izomorficzne, chociaż ich grupy addytywne są izomorficzne.

Zagadka 7. Niech m i n będą liczbami naturalnymi większymi od 1. Udowodnij, że jeśli istnieje homomorfizm pierścieni $f\colon \mathbb{Z}_m \to \mathbb{Z}_n$, to $n|m$. Udowodnij, że jeśli $n|m$, to $f\colon \mathbb{Z}_m \to \mathbb{Z}_n$ dane wzorem $f(a) = [a]_n$ dla $a \in \mathbb{Z}_m$ jest jedynym homomorfizmem pierścienia $\mathbb{Z}_m$ w pierścień $\mathbb{Z}_n$. Uzasadnij też, że f jest "na" i wyznacz $Ker(f)$.