

7. WYKŁAD 7: HOMOMORFIZMY PIERŚCIENI, IDEAŁY PIERŚCIENI. IDEAŁY GENEROWANE PRZEZ ZBIORY. PIERŚCIEŃ ILORAZOWY, TWIERDZENIE O HOMOMORFIZMIE. IDEAŁY PIERWSZE I MAKSYMALNE.

7.1. Homomorfizmy pierścieni, ideały pierścieni.

Definicja 7.1. Niech P, R będą pierścieniami.

(1) Odwzorowanie $\phi : P \rightarrow R$ nazywamy **homomorfizmem**, jeśli

- $\phi(1_P) = 1_R$,
- $\forall a, b \in P[\phi(a + b) = \phi(a) + \phi(b)]$,
- $\forall a, b \in P[\phi(a \cdot b) = \phi(a) \cdot \phi(b)]$.

Zbiór wszystkich homomorfizmów pierścienia P w pierścień R oznaczamy $\text{Hom}(P, R)$.

(2) Homomorfizm $\phi : P \rightarrow R$ nazywamy **monomorfizmem**, jeśli jest różnowartościowy.

(3) Homomorfizm $\phi : P \rightarrow R$ nazywamy **epimorfizmem**, jeśli jest surjektywny.

(4) Homomorfizm $\phi : P \rightarrow R$ nazywamy **izomorfizmem**, jeśli jest bijekcją.

(5) Homomorfizm $\phi : P \rightarrow R$ nazywamy **monomorfizmem kategoriowym**, jeśli dla każdego pierścienia S i dla każdego homomorfizmu $\psi_1, \psi_2 : S \rightarrow P$

$$\text{jeśli } \phi \circ \psi_1 = \phi \circ \psi_2, \text{ to } \psi_1 = \psi_2;$$

(6) Homomorfizm $\phi : P \rightarrow R$ nazywamy **epimorfizmem kategoriowym**, jeśli dla każdego pierścienia S i dla każdego homomorfizmu $\psi_1, \psi_2 : R \rightarrow S$

$$\text{jeśli } \psi_1 \circ \phi = \psi_2 \circ \phi, \text{ to } \psi_1 = \psi_2.$$

(7) Homomorfizm $\phi : P \rightarrow P$ nazywamy **endomorfizmem**. Zbiór wszystkich endomorfizmów oznaczamy $\text{End}(P)$.

(8) Izomorfizm $\phi : P \rightarrow P$ nazywamy **automorfizmem**. Zbiór wszystkich automorfizmów oznaczamy $\text{Aut}(P)$.

(9) Jeśli $\phi : P \rightarrow R$ jest homomorfizmem, to zbiór

$$\ker \phi = \phi^{-1}(0_R) = \{a \in P : \phi(a) = 0_R\}$$

nazywamy **jądrem** homomorfizmu ϕ , zaś zbiór

$$\text{im } \phi = \phi(P) = \{b \in R : \exists a \in P[b = \phi(a)]\}$$

nazywamy **obrazem** homomorfizmu ϕ .

Uwaga 7.1. Niech P, R będą pierścieniami, niech $\phi : P \rightarrow R$ będzie homomorfizmem. Wówczas:

- (1) $\phi(0_P) = 0_R$;
- (2) $\phi(-a) = -\phi(a)$, dla $a \in P$;
- (3) $\phi(a^k) = (\phi(a))^k$ oraz $\phi(ka) = k\phi(a)$, dla $a \in P$, $k \in \mathbb{N} \cup \{0\}$;
- (4) $\phi : P \rightarrow R$ jest homomorfizmem grup addytywnych $(P, +_P)$ i $(R, +_R)$.

Dowód jest bardzo podobny do dowodu analogicznego rezultatu dla grup, w związku z czym pozostawiamy go Czytelnikowi jako nietrudne ćwiczenie.

Twierdzenie 7.1. Niech P, R będą pierścieniami, niech $\phi : P \rightarrow R$ będzie homomorfizmem. Wówczas:

- (1) $\text{im } \phi \leq R$;
- (2) ϕ jest monomorfizmem wtedy i tylko wtedy, gdy $\ker \phi = \{0_P\}$;
- (3) ϕ jest epimorfizmem wtedy i tylko wtedy, gdy $\text{im } \phi = R$;

(4) ϕ jest izomorfizmem wtedy i tylko wtedy, gdy istnieje homomorfizm $\psi : R \rightarrow P$ taki, że

$$\phi \circ \psi = id_R \text{ oraz } \psi \circ \phi = id_P;$$

(5) ϕ jest monomorfizmem wtedy i tylko wtedy, gdy jest monomorfizmem kategoriowym;

(6) ϕ jest epimorfizmem wtedy i tylko wtedy, gdy jest epimorfizmem kategoriowym.

Dowód jest bardzo podobny do dowodu analogicznego rezultatu dla grup, w związku z czym pozostawiamy go Czytelnikowi jako nietrudne ćwiczenie.

Przykłady:

(1) $\phi : P \rightarrow P$, $\phi(x) = x$ jest homomorfizmem;

(2) $\phi : P^X \rightarrow P$, $\phi(f) = f(x_0)$ jest homomorfizmem, gdzie $X \neq \emptyset$ oraz $x_0 \in X$ jest ustalonym elementem;

(3) $\phi : \mathbb{Z} \rightarrow \mathbb{Z}_n$, $\phi(x) = \text{reszta z dzielenia } x \text{ przez } n$ jest homomorfizmem;

(4) $\phi : \mathbb{Z} \rightarrow P$, $\phi(x) = x \cdot 1_P$ jest homomorfizmem.

Twierdzenie 7.2. Niech P, R będą pierścieniami, $P_1 < P$, $R_1 < R$, niech $\phi : P \rightarrow R$ będzie homomorfizmem. Wówczas:

(1) $\phi(P_1) < R$,

(2) $\phi^{-1}(R_1) < P$.

Dowód jest bardzo podobny do dowodu analogicznego rezultatu dla grup, w związku z czym pozostawiamy go Czytelnikowi jako nietrudne ćwiczenie.

Definicja 7.2. Niech $(R, +, \cdot)$ będzie pierścieniem, niech $I \subset R$. Zbiór I nazywamy **ideałem** pierścienia R , jeżeli:

- $\forall a, b \in I (a - b \in I)$;
- $\forall a \in I \forall x \in R (xa \in I)$.

Oznaczamy $I \triangleleft R$.

Uwaga 7.2. Niech $(R, +, \cdot)$ będzie pierścieniem, niech $I \triangleleft R$. Wówczas I jest podgrupą normalną grupy $(R, +)$.

Przykłady:

(5) Rozważmy pierścień $(R, +, \cdot)$. Wówczas $R \triangleleft R$ i nazywamy go **ideałem niewłaściwym**.

(6) Rozważmy pierścień $(R, +, \cdot)$. Wówczas $\{0\} \triangleleft R$ i nazywamy go **ideałem zerowym**. Ideały niewłaściwy i zerowy nazywamy **ideałami trywialnymi**.

(7) Rozważmy pierścień $\mathbb{Z}$. Wówczas $3\mathbb{Z} \triangleleft \mathbb{Z}$.

(8) Rozważmy pierścień $\mathbb{R}^{\mathbb{R}}$. Wówczas $I = \{f \in \mathbb{R}^{\mathbb{R}} : f(1) = 0\} \triangleleft \mathbb{R}^{\mathbb{R}}$.

Twierdzenie 7.3. Niech P, R będą pierścieniami, niech $\phi : P \rightarrow R$ będzie homomorfizmem. Wówczas:

(1) $\ker \phi \triangleleft P$,

(2) jeśli $J \triangleleft R$, to $\phi^{-1}(J) \triangleleft P$ oraz $\ker \phi \subset \phi^{-1}(J)$,

(3) jeśli $I \triangleleft P$ i ϕ jest epimorfizmem, to $\phi(I) \triangleleft R$.

Dowód. (1) Ustalmy $a, b \in \ker \phi$, $x \in P$. Wówczas

$$\phi(a - b) = \phi(a) - \phi(b) = 0 - 0 = 0,$$

a zatem $a - b \in \ker \phi$. Ponadto:

$$\phi(xa) = \phi(x)\phi(a) = \phi(x) \cdot 0 = 0,$$

a zatem $xa \in \ker \phi$.

(2) Ustalmy $a, b \in \phi^{-1}(J)$, $x \in P$. Wówczas

$$\phi(a - b) = \phi(a) - \phi(b) \in J,$$

a zatem $a - b \in \phi^{-1}(J)$. Ponadto:

$$\phi(xa) = \phi(x)\phi(a) \in J,$$

a zatem $xa \in \phi^{-1}(J)$. Ustalmy ponadto $c \in \ker \phi$. Wówczas:

$$\phi(c) = 0 \in J,$$

a zatem $c \in \phi^{-1}(J)$.

(3) analogicznie.

□

Twierdzenie 7.4. Niech $(R, +, \cdot)$ będzie pierścieniem, niech $I \triangleleft R$. Następujące warunki są równoważne:

- (1) $I = R$;
- (2) $I \cap U(R) \neq \emptyset$;
- (3) $1 \in I$.

Dowód. (1) $\Rightarrow$ (2): oczywiste. (2) $\Rightarrow$ (3): ustalmy $a \in I \cap U(R)$. Niech $b \in R$ będzie taki, że $ab = 1$. Skoro $a \in I$, $b \in R$, więc $1 = ab \in I$.

(3) $\Rightarrow$ (1): Ustalmy $a \in R$. Skoro $1 \in I$, $a \in R$, to $a = 1 \cdot a \in I$.

□

Twierdzenie 7.5. Niech $(R, +, \cdot)$ będzie pierścieniem. Wówczas:

R jest ciałem wtedy i tylko wtedy, gdy R ma dokładnie dwa ideały, $\{0\}$ i R .

Dowód. ($\Rightarrow$): założmy, że R jest ciałem. Ustalmy $I \triangleleft R$ i niech $I \neq \{0\}$.

Pokażemy, że $I \cap U(R) \neq \emptyset$. Istotnie, skoro R jest ciałem, to $U(R) = R \setminus \{0\}$. Ponieważ $I \neq \{0\}$, więc dla $a \in I \setminus \{0\}$ zachodzi $a \in U(R)$.

Wobec poprzedniego twierdzenia $I = R$.

($\Leftarrow$): założmy, że $\{0\}$ i R są jedynymi ideałami pierścienia R . Ustalmy $a \in R \setminus \{0\}$.

Pokażemy, że $a \in U(R)$. Niech $I_a = \{xa : a \in R\}$. Zauważmy, że $I_a \triangleleft R$: istotnie, ustalmy $x_1a, x_2a \in I_a$, $y \in R$. Wówczas

$$x_1a - x_2a = (x_1 - x_2)a \in I_a$$

oraz

$$x_1ay = (x_1y)a \in I_a.$$

Ponadto zauważmy, że $a = 1 \cdot a \in I_a$ oraz $a \neq 0$. Tym samym $I_a \neq \{0\}$. Zatem $I_a = R$, w szczególności istnieje $b \in R \setminus \{0\}$ taki, że $ba = 1$.

□

Twierdzenie 7.6 (lemat o odpowiedniości między ideałami). Niech P, R będą pierścieniami, $\pi : P \rightarrow R$ homomorfizmem surjektywnym i niech $N = \ker \pi$. Oznaczmy

$$\mathcal{I} = \{I : I \triangleleft P \text{ oraz } N \subset I\}, \mathcal{J} = \{J : J \triangleleft R\}.$$

Wówczas odwzorowania

$$\begin{aligned} \phi : \mathcal{I} &\rightarrow \mathcal{J}, \phi(I) = \pi(I), \\ \psi : \mathcal{J} &\rightarrow \mathcal{I}, \psi(J) = \pi^{-1}(J) \end{aligned}$$

są wzajemnie odwrotne.

Dowód jest bardzo podobny do dowodu analogicznego rezultatu dla grup, w związku z czym pozostawiamy go Czytelnikowi jako nietrudne ćwiczenie.

7.2. Ideały generowane przez zbiory.

Twierdzenie 7.7. Niech $\mathcal{J} = \{J_i : i \in I\}$ będzie rodziną ideałów pierścienia R ;

- (1) $\bigcap_{i \in I} J_i$ jest ideałem pierścienia R ,
- (2) $\bigcup_{i \in I} J_i$ jest ideałem pierścienia R , o ile $\mathcal{J}$ jest łańcuchem.

Dowód jest bardzo podobny do dowodu analogicznego rezultatu dla grup, w związku z czym pozostawiamy go Czytelnikowi jako nietrudne ćwiczenie.

Definicja 7.3. Niech $(R, +, \cdot)$ będzie pierścieniem oraz $A \subset R$ pewnym zbiorem. Najmniejszy w sensie inkluzji ideał pierścienia R zawierający zbiór A (tj. przekrój wszystkich ideałów pierścienia R zawierających A) nazywamy **ideałem generowanym przez A** i oznaczamy (A) .

Uwaga 7.3. Niech $(R, +, \cdot)$ będzie pierścieniem oraz $P < R$. Wówczas:

- (1) $(\{0\}) = \{0\}$,
- (2) $(1) = R$.

Definicja 7.4. Niech $(R, +, \cdot)$ będzie pierścieniem, niech $I \triangleleft R$. Każdy zbiór A o tej własności, że $(A) = I$ nazywamy **zbiorem generatorów ideału I** . Jeśli $A = \{a_1, \dots, a_n\}$ to oznaczamy

$$(a_1, \dots, a_n) = (A).$$

Mówimy, że ideał jest **skończenie generowany**, gdy istnieją elementy $a_1, \dots, a_n \in R$ takie, że

$$I = (a_1, \dots, a_n).$$

Mówimy, że ideał jest **główny**, gdy istnieje element $a \in R$ taki, że

$$I = (a).$$

Mówimy, że pierścień R jest **pierścieniem ideałów głównych** (PID, principal ideal domain), gdy każdy jego ideał jest ideałem głównym.

Twierdzenie 7.8 (o postaci elementów ideału generowanego przez zbiór). Niech $(R, +, \cdot)$ będzie pierścieniem oraz $A \subset R$ pewnym zbiorem. Wówczas

$$(A) = \{a_1 b_1 + \dots + a_n b_n : n \in \mathbb{N}, a_i \in A, b_i \in R\}.$$

Dowód jest bardzo podobny do dowodu analogicznego rezultatu dla grup, w związku z czym pozostawiamy go Czytelnikowi jako nietrudne ćwiczenie.

Wniosek 7.1. Niech $(R, +, \cdot)$ będzie pierścieniem oraz $a \in R$. Wówczas:

- (1) Niech $(R, +, \cdot)$ będzie pierścieniem oraz $a \in R$. Wówczas:

$$(a) = \{ab : b \in R\}.$$

- (2) Niech $(R, +, \cdot)$ będzie pierścieniem oraz $a_1, \dots, a_n \in R$. Wówczas:

$$(a_1, \dots, a_n) = \{a_1 b_1 + \dots + a_n b_n : b_i \in R\}.$$

Przykłady:

- (1) Rozważmy pierścień $\mathbb{Z}$. Wówczas:

$$(5) = \{k5 : k \in \mathbb{Z}\} = 5\mathbb{Z}$$

oraz

$$(4, 6) = \{k4 + l6 : k, l \in \mathbb{Z}\}.$$

(2) Rozważmy pierścień $\mathbb{R}[x]$. Wówczas:

$$(x) = \{f \cdot x : f \in \mathbb{R}[x]\} = \{g \in \mathbb{R}[x] : x|g\}.$$

Definicja 7.5. Niech $(R, +, \cdot)$ będzie pierścieniem, niech $I, J \triangleleft R$.

(1) Ideal $(I \cup J)$ nazywamy **sumą ideałów** I i J i oznaczamy $I + J$.

(2) Ideal $(\{i \cdot j : i \in I, j \in J\})$ nazywamy **iloczynem ideałów** I i J i oznaczamy $I \cdot J$.

Twierdzenie 7.9 (o postaci elementów sumy i iloczynu ideałów). Niech $(R, +, \cdot)$ będzie pierścieniem, niech $I, J \triangleleft R$.

(1) $I + J = \{i + j : i \in I, j \in J\}$;

(2) $I \cdot J = \{a_1 b_1 + \dots + a_n b_n : n \in \mathbb{N}, a_i \in I, b_i \in J\}$

Twierdzenie 7.10. Pierścień $\mathbb{Z}$ jest pierścieniem ideałów głównych.

Dowód. Ustalmy $I \triangleleft \mathbb{Z}$. Jeśli $I = \{0\}$, to $I = (0)$ jest ideałem głównym. Jeśli $I \neq \{0\}$, to istnieje $a \in I$, $a \neq 0$. Oczywiście $\{-a, a\} \cap \mathbb{N} \neq \emptyset$, zdefiniujmy więc

$$c = \min\{a \in \mathbb{N} : a \in I\}.$$

Pokażemy, że $I = (c)$. Inkluzja $(\supset)$ jest oczywista, zaś dla dowodu inkluzji $(\subset)$ ustalmy $b \in I$. Dziąc z resztą b przez c otrzymujemy

$$b = qc + r \text{ dla pewnych } q, r \in \mathbb{N} \cup \{0\}, 0 \leq r < c.$$

Zatem $r = b - qc$. Skoro $b \in I$, $c \in I$, $q \in \mathbb{Z}$, więc $r \in I$. Ponadto $r < c$, więc z wyboru c wynika, że $r = 0$. Zatem $b = qc \in (c)$. $\square$

Twierdzenie 7.11. Niech F będzie ciałem. Pierścień $F[x]$ jest pierścieniem ideałów głównych.

Dowód. Ustalmy $I \triangleleft F[x]$. Jeśli $I = \{0\}$, to $I = (0)$ jest ideałem głównym. Jeśli $I \neq \{0\}$, to istnieje $f \in I$, $f \neq 0$. Zdefiniujmy więc

$$h = \text{wielomian z } I \text{ możliwie najmniejszego stopnia.}$$

Pokażemy, że $I = (h)$. Inkluzja $(\supset)$ jest oczywista, zaś dla dowodu inkluzji $(\subset)$ ustalmy $g \in I$. Dziąc z resztą g przez h otrzymujemy

$$g = qh + r \text{ dla pewnych } q, r \in F[x], 0 \leq \deg r < \deg h.$$

Zatem $r = g - qh$. Skoro $g \in I$, $h \in I$, $q \in F[x]$, więc $r \in I$. Ponadto $\deg r < \deg h$, więc z wyboru h wynika, że $r = 0$. Zatem $g = qh \in (h)$. $\square$

7.3. Pierścień ilorazowy, twierdzenie o homomorfizmie.

Definicja i Uwaga 7.1. Niech R będzie pierścieniem, niech $I \triangleleft R$. Oznaczmy

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

$$R/I = \{a + I : a \in R\}$$

i w zbiorze R/I określmy działania dodawania i mnożenia:

$$(a + I) + (b + I) = (a + b) + I,$$

$$(a + I) \cdot (b + I) = (a \cdot b) + I.$$

Wówczas R/I jest pierścieniem, nazywamy go **pierścieniem ilorazowym** R względem I .

Dowód jest bardzo podobny do dowodu analogicznego rezultatu dla grup, w związku z czym pozostawiamy go Czytelnikowi jako nietrudne ćwiczenie.

Przykłady:

- (1) Rozważmy pierścień $\mathbb{Z}$ oraz $(3) \triangleleft \mathbb{Z}$. Wówczas:

$$\mathbb{Z}/(3) = \{0 + (3), 1 + (3), 2 + (3)\}.$$

- (2) Rozważmy pierścień $\mathbb{R}[x]$ oraz $(x^2) \triangleleft \mathbb{R}[x]$. Wówczas:

$$\mathbb{R}[x]/(x^2) = \{a_0 + a_1x + (x^2) : a_0, a_1 \in \mathbb{R}\}.$$

Definicja i Uwaga 7.2. Niech R będzie pierścieniem, niech $I \triangleleft R$. Wówczas odwzorowanie $\kappa : R \rightarrow R/I$ dane wzorem $\kappa(a) = a + I$ jest homomorfizmem surjektywnym oraz $\ker \kappa = I$. Nazywamy go **epimorfizmem kanonicznym**.

Dowód jest bardzo podobny do dowodu analogicznego rezultatu dla grup, w związku z czym pozostawiamy go Czytelnikowi jako nietrudne ćwiczenie.

Wniosek 7.2. Niech R będzie pierścieniem, niech $I \subset R$. Wówczas $I \triangleleft R$ wtedy i tylko wtedy, gdy I jest jądrem pewnego homomorfizmu.

Dowód jest bardzo podobny do dowodu analogicznego rezultatu dla grup, w związku z czym pozostawiamy go Czytelnikowi jako nietrudne ćwiczenie.

Twierdzenie 7.12 (o homomorfizmie). Niech P, R_1, R_2 będą pierścieniami, $\phi_1 : P \rightarrow R_1$ homomorfizmem surjektywnym, $\phi_2 : P \rightarrow R_2$ homomorfizmem.

- (1) Jeśli istnieje homomorfizm $\psi : R_1 \rightarrow R_2$ taki, że $\psi \circ \phi_1 = \phi_2$, to $\ker \phi_1 \subset \ker \phi_2$.
- (2) Jeśli $\ker \phi_1 \subset \ker \phi_2$, to istnieje dokładnie jeden homomorfizm $\psi : R_1 \rightarrow R_2$ taki, że $\psi \circ \phi_1 = \phi_2$. Ponadto wówczas $\operatorname{im} \psi = \operatorname{im} \phi_2$ oraz $\ker \psi = \phi_1(\ker \phi_2)$.

Inaczej: diagram

$$\begin{array}{ccc} & P & \\ \phi_1 \swarrow & & \searrow \phi_2 \\ R_1 & \overset{\text{"na"}}{\dashrightarrow} & R_2 \\ & \psi & \end{array}$$

jest przemienny.

Dowód jest bardzo podobny do dowodu analogicznego rezultatu dla grup, w związku z czym pozostawiamy go Czytelnikowi jako nietrudne ćwiczenie.

Wniosek 7.3. Niech P, R_1, R_2 będą pierścieniami, $\phi_1 : P \rightarrow R_1$ homomorfizmem surjektywnym, $\phi_2 : P \rightarrow R_2$ homomorfizmem. Niech ponadto $\ker \phi_1 \subset \ker \phi_2$. Wówczas istnieje dokładnie jeden homomorfizm $\psi : R_1 \rightarrow R_2$ taki, że $\psi \circ \phi_1 = \phi_2$ oraz:

- (1) jeśli ϕ_2 jest surjektywny, to ψ jest surjektywny;
- (2) jeśli $\ker \phi_1 = \ker \phi_2$, to ψ jest różnowartościowy;
- (3) jeśli ϕ_2 jest surjektywny i $\ker \phi_1 = \ker \phi_2$, to ψ jest izomorfizmem.

Dowód jest bardzo podobny do dowodu analogicznego rezultatu dla grup, w związku z czym pozostawiamy go Czytelnikowi jako nietrudne ćwiczenie.

Wniosek 7.4 (twierdzenie o homomorfizmie dla pierścieni ilorazowych). Niech P, R będą pierścieniami, niech $I \triangleleft P$, niech $\phi : P \rightarrow R$ będzie homomorfizmem.

- (1) Jeśli istnieje homomorfizm $\psi : P/I \rightarrow R$ taki, że $\psi \circ \kappa = \phi$ (gdzie $\kappa : P \rightarrow P/I$ oznacza epimorfizm kanoniczny), to $I \subset \ker \phi$.
- (2) Jeśli $I \subset \ker \phi$, to istnieje dokładnie jeden homomorfizm $\psi : P/I \rightarrow R$ taki, że $\psi \circ \kappa = \phi$. Ponadto wówczas $\operatorname{im} \psi = \operatorname{im} \phi$ oraz $\ker \psi = \kappa(\ker \phi)$.

Inaczej: diagram

$$\begin{array}{ccc}
 & P & \\
 \kappa \swarrow & & \searrow \phi \\
 P/I & \xrightarrow{\psi} & R
 \end{array}$$

"na"

jest przemienny.

Dowód jest bardzo podobny do dowodu analogicznego rezultatu dla grup, w związku z czym pozostawiamy go Czytelnikowi jako nietrudne ćwiczenie.

Wniosek 7.5. Niech P, R będą pierścieniami, niech $I \triangleleft P$, niech $\phi : P \rightarrow R$ będzie homomorfizmem. Niech ponadto $I \subset \ker \phi$. Wówczas istnieje dokładnie jeden homomorfizm $\psi : P/I \rightarrow R$ taki, że $\psi \circ \kappa = \phi$ (gdzie $\kappa : P \rightarrow P/I$ oznacza epimorfizm kanoniczny) oraz

- (1) jeśli ϕ jest surjektywny, to ψ jest surjektywny;
- (2) jeśli $I = \ker \phi$, to ψ jest różnowartościowy;
- (3) jeśli ϕ jest surjektywny i $I = \ker \phi$, to ψ jest izomorfizmem.

Twierdzenie 7.13 (twierdzenie o izomorfizmie). Niech P, R będą pierścieniami, niech $\phi : P \rightarrow R$ będzie homomorfizmem. Wówczas

$$\operatorname{im} \phi \cong P / \ker \phi.$$

Przykłady:

- (3) Rozważmy pierścień R oraz odwzorowanie $\phi : R \rightarrow R$ dane wzorem $\phi(x) = x$. Wówczas $\operatorname{im} \phi = R$, $\ker \phi = \{0\}$, a zatem $R/\{0\} \cong R$.
- (4) Rozważmy pierścienie $\mathbb{Z}$ i $\mathbb{Z}_n$ oraz odwzorowanie $\phi : \mathbb{Z} \rightarrow \mathbb{Z}_n$ dane wzorem $\phi(x) = \text{reszta z dzielenia } x \text{ przez } n$. Wówczas $\operatorname{im} \phi = \mathbb{Z}_n$, $\ker \phi = n\mathbb{Z}$, a zatem $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.
- (5) Rozważmy pierścienie $\mathbb{R}[x]$ i $\mathbb{R}$ oraz odwzorowanie $\phi : \mathbb{R}[x] \rightarrow \mathbb{R}$ dane wzorem $\phi(f) = f(a)$, gdzie $a \in \mathbb{R}$ jest ustalone. Wówczas $\operatorname{im} \phi = \mathbb{R}$, $\ker \phi = (x - a)$, a zatem $\mathbb{R}[x]/(x - a) \cong \mathbb{R}$.
- (6) Rozważmy pierścienie $\mathbb{R}[x]$ i $\mathbb{C}$ oraz odwzorowanie $\phi : \mathbb{R}[x] \rightarrow \mathbb{C}$ dane wzorem $\phi(f) = f(i)$. Wówczas $\operatorname{im} \phi = \mathbb{C}$, $\ker \phi = (x^2 + 1)$, a zatem $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

7.4. Ideały pierwsze i maksymalne.

Definicja 7.6. Niech R będzie pierścieniem, niech $I \triangleleft R$. Ideał I nazywamy **ideałem pierwszym**, jeśli jest właściwy oraz

$$\forall a, b \in R [ab \in I \Rightarrow (a \in I \vee b \in I)].$$

Przykłady:

- (1) Rozważmy pierścień $\mathbb{Z}$ oraz $\{0\} \triangleleft \mathbb{Z}$. Wówczas $\{0\}$ jest ideałem pierwszym.
- (2) Rozważmy pierścień $\mathbb{R}^{\mathbb{R}}$ oraz $I = \{f \in \mathbb{R}^{\mathbb{R}} : f(2) = 0\} \triangleleft \mathbb{R}^{\mathbb{R}}$. Wówczas I jest ideałem pierwszym.

Twierdzenie 7.14. Niech R będzie pierścieniem, niech $I \triangleleft R$. Wówczas

R/I jest pierścieniem całkowitym wtedy i tylko wtedy, gdy I jest pierwszy.

Dowód. ($\Leftarrow$): załóżmy, że I jest ideałem pierwszym. Ustalmy $a+I, b+I \in R/I$ i załóżmy, że $(a+I)(b+I) = 0+I$. Wówczas $ab \in I$, a zatem $a \in I$ lub $b \in I$, czyli $a+I = 0+I$ lub $b+I = 0+I$.

($\Rightarrow$): załóżmy, że R/I jest pierścieniem całkowitym. Ustalmy $a, b \in R$ i załóżmy, że $ab \in I$. Wówczas $ab+I = 0+I$, a zatem $(a+I)(b+I) = 0+I$. Skoro $a+I = 0+I$ lub $b+I = 0+I$, więc $a \in I$ lub $b \in I$. $\square$

Wniosek 7.6. *Niech P, R będą pierścieniami, niech $J \triangleleft R$ będzie pierwszy, niech $\phi : P \rightarrow R$ będzie homomorfizmem. Wówczas $\phi^{-1}(J)$ jest ideałem pierwszym.*

Dowód. Zdefiniujmy odwzorowanie $\psi : P \rightarrow R/J$ wzorem $\psi = \kappa \circ \phi$, gdzie κ jest epimorfizmem kanonicznym. Zauważmy, że $\ker \psi = \phi^{-1}(J)$: istotnie, zachodzi

$$\begin{aligned} a \in \ker \psi &\Leftrightarrow \psi(a) = J \Leftrightarrow \kappa(\phi(a)) = J \\ &\Leftrightarrow \phi(a) + J = J \Leftrightarrow \phi(a) \in J \\ &\Leftrightarrow a \in \phi^{-1}(J). \end{aligned}$$

Wobec twierdzenia o izomorfizmie:

$$P/\phi^{-1}(J) \cong \text{im} \psi.$$

Ponadto $\text{im} \psi < R/J$ i jako podpierścień pierścienia całkowitego jest całkowity. Zatem $P/\phi^{-1}(J)$ jest całkowity, a tym samym $\phi^{-1}(J)$ jest pierwszy. $\square$

Wniosek 7.7. *Niech R będzie pierścieniem. Wówczas:*

R jest pierścieniem całkowitym wtedy i tylko wtedy, gdy $\{0\}$ jest ideałem pierwszym.

Dowód. Wobec twierdzenia o izomorfizmie $R/\{0\} \cong R$, a zatem R jest całkowity wtedy i tylko wtedy, gdy $R/\{0\}$ jest całkowity, wtedy i tylko wtedy, gdy $\{0\}$ jest pierwszy. $\square$

Przykłady:

- (3) Rozważmy pierścień $\mathbb{Z}$ oraz $(n) \triangleleft \mathbb{Z}$. Wówczas (n) jest ideałem pierwszym wtedy i tylko wtedy, gdy n jest liczbą pierwszą.
- (4) Rozważmy pierścień $\mathbb{Z}[x]$ oraz $(x) \triangleleft \mathbb{Z}[x]$. Wówczas (x) jest ideałem pierwszym.

Definicja 7.7. *Niech R będzie pierścieniem, niech $I \triangleleft R$. Ideał I nazywamy **ideałem maksymalnym**, jeśli jest właściwy oraz*

$$\forall J \triangleleft R [I \subset J \Rightarrow (I = J \vee J = R)].$$

Twierdzenie 7.15. *Niech R będzie pierścieniem, niech $I \triangleleft R$. Wówczas*

R/I jest ciałem wtedy i tylko wtedy, gdy I jest maksymalny.

Dowód. Epimorfizm kanoniczny $\kappa : R \rightarrow R/I$ jest surjekcją oraz $\ker \kappa = I$. Wobec lematu o odpowiedności między ideałami rodziny

$$\mathcal{I} = \{J : J \triangleleft R \text{ oraz } I \subset J\}$$

oraz

$$\mathcal{J} = \{K : K \triangleleft R/I\}$$

są równoliczne. Wobec tego R/I jest ciałem wtedy i tylko wtedy, gdy $|\mathcal{J}| = 2$ wtedy i tylko wtedy, gdy $|\mathcal{I}| = 2$ wtedy i tylko wtedy, gdy I jest ideałem maksymalnym. $\square$

Wniosek 7.8. *Niech P, R będą pierścieniami, niech $J \triangleleft R$ będzie maksymalny, niech $\phi : P \rightarrow R$ będzie epimorfizmem. Wówczas $\phi^{-1}(J)$ jest ideałem maksymalnym.*

Dowód jest podobny do dowodu analogicznego rezultatu dla ideałów pierwszych i pozostawiamy go Czytelnikowi jako nietrudne ćwiczenie.

Wniosek 7.9. *Niech R będzie pierścieniem. Wówczas:*

R jest ciałem wtedy i tylko wtedy, gdy $\{0\}$ jest ideałem maksymalnym.

Dowód jest podobny do dowodu analogicznego rezultatu dla ideałów pierwszych i pozostawiamy go Czytelnikowi jako nietrudne ćwiczenie.

Wniosek 7.10. *Niech R będzie pierścieniem, niech $I \triangleleft R$. Wówczas*

jeśli I jest ideałem maksymalnym, to I jest ideałem pierwszym.

Dowód. Jeśli I jest ideałem maksymalnym, to R/I jest ciałem, a więc pierścieniem całkowitym, skąd I musi być pierwszy. $\square$

Wniosek 7.11. *Niech R będzie pierścieniem ideałów głównych, niech $\{0\} \neq I \triangleleft R$. Wówczas*

jeśli I jest ideałem pierwszym, to I jest ideałem maksymalnym.

Dowód. Ustalmy ideał pierwszy $\{0\} \neq I \triangleleft R$. Ponieważ R jest pierścieniem ideałów głównych, więc $I = (a)$, dla pewnego $a \in R \setminus \{0\}$, a ponieważ I jest pierwszy, więc:

$$\forall b, c \in R [bc \in (a) \Rightarrow (b \in (a) \vee c \in (a))].$$

Ustalmy ideał $J \triangleleft R$ i niech $I \subset J$. Ponieważ R jest pierścieniem ideałów głównych, więc $J = (b)$, dla pewnego $b \in R \setminus \{0\}$. Ponieważ $I \subset J$, czyli $(a) \subset (b)$, więc $a \in (b)$, czyli $a = bc$, dla pewnego $c \in R \setminus \{0\}$. Ponieważ R jest pierwszy, więc $b \in (a)$ lub $c \in (a)$. Jeśli $b \in (a)$, to $(b) \subset (a)$, więc $I = J$. Jeżeli $c \in (a)$, to $c = ad$, dla pewnego $d \in R \setminus \{0\}$. Zatem:

$$a = bad,$$

skąd $bd = 1$, a więc b jest odwracalny i tym samym $J = R$. $\square$

Przykłady:

- (5) Rozważmy pierścień $\mathbb{R}[x]$ oraz $(x - 1) \triangleleft \mathbb{R}[x]$. Wówczas $(x - 1)$ jest ideałem maksymalnym.
- (6) Rozważmy pierścień $\mathbb{R}[x]$ oraz $(x^2 + 1) \triangleleft \mathbb{R}[x]$. Wówczas $(x^2 + 1)$ jest ideałem maksymalnym.
- (7) Rozważmy pierścień $\mathbb{R}[x]$ oraz $(x^2 - 1) \triangleleft \mathbb{R}[x]$. Wówczas $(x^2 - 1)$ nie jest ideałem maksymalnym, nie jest też ideałem pierwszym.

Uwaga 7.4. *Niech $n > 1$. Następujące warunki są równoważne:*

- (1) (n) jest ideałem pierwszym w $\mathbb{Z}$;
- (2) (n) jest ideałem maksymalnym w $\mathbb{Z}$;
- (3) $\mathbb{Z}_n$ jest pierścieniem całkowitym;
- (4) $\mathbb{Z}_n$ jest ciałem;
- (5) n jest liczbą pierwszą.

Twierdzenie 7.16. *Niech R będzie pierścieniem, niech $I \triangleleft R$. Wówczas*

jeśli I jest właściwy, to jest zawarty w pewnym ideale maksymalnym.

Dowód. Ustalmy ideał $R \neq I \triangleleft R$ i zdefiniujmy rodzinę:

$$\mathcal{R} = \{J \triangleleft R : J \neq R \text{ oraz } I \subset J\}.$$

Ponieważ $I \in \mathcal{R}$, więc $\mathcal{R} \neq \emptyset$. Oczywiście $(\mathcal{R}, \subset)$ jest zbiorem częściowo uporządkowanym.

Ustalmy łańcuch $\mathcal{J} \subset \mathcal{R}$. Pokażemy, że $\mathcal{J}$ ma ograniczenie górne. Istotnie, zdefiniujmy

$$K = \bigcup \{J : J \in \mathcal{J}\}.$$

Wobec Twierdzenia ?? $K \triangleleft R$. Oczywiście $I \subset K$. Zauważmy też, że $K \neq R$, albowiem dla wszelkich $J \in \mathcal{J}$ zachodzi $1 \notin J$, a zatem $1 \notin K$ i tym samym K jest właściwy. Pokazaliśmy wobec tego, że $K \in \mathcal{J}$ i, oczywiście, $J \subset K$, dla $J \in \mathcal{J}$.

Wobec lematu Kuratowskiego-Zorna w rodzinie $\mathcal{R}$ istnieje element maksymalny, który jest poszukiwanym ideałem maksymalnym. $\square$

Wniosek 7.12. *Niech R będzie pierścieniem. Wówczas:*

- (1) *w R istnieje pewien ideał maksymalny;*
- (2) *w R istnieje pewien ideał pierwszy.*

Definicja 7.8. *Niech R będzie pierścieniem. Wówczas:*

- (1) *zbiór wszystkich ideałów pierwszych pierścienia R nazywamy **spektrum pierwszym pierścienia R** i oznaczamy $\text{Spec}(R)$;*
- (2) *zbiór wszystkich ideałów maksymalnych pierścienia R nazywamy **spektrum maksymalnym pierścienia R** i oznaczamy $\text{Specm}(R)$.*