10. Wykład 10: Homomorfizmy pierścieni, ideały pierścieni. Ideały generowane przez zbiory.

10.1. Homomorfizmy pierścieni, ideały pierścieni.

Definicja 10.1. *Niech P, R będą pierścieniami.*

(1) *Odwzorowanie $\phi : P \to R$ nazywamy* **homomorfizmem**, *jeśli*
- $\phi(1_P) = 1_R$,
- $\forall a, b \in P[\phi(a + b) = f(a) + f(b)]$,
- $\forall a, b \in P[\phi(a \cdot b) = f(a) \cdot f(b)]$.

Zbiór wszystkich homomorfizmów pierścienia P w pierścień R oznaczamy $Hom(P, R)$.

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

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

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

(5) *Homomorfizm $\phi : P \to R$ nazywamy* **monomorfizmem kategoryjnym,** *jeśli dla każdego pierścienia S i dla każdych homomorfizmów $\psi_1, \psi_2 : S \to P$*

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

(6) *Homomorfizm $\phi : P \to R$ nazywamy* **epimorfizmem kategoryjnym,** *jeśli dla każdego pierścienia S i dla każdych homomorfizmów $\psi_1, \psi_2 : R \to S$*

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

(7) *Homomorfizm $\phi : P \to P$ nazywamy* **endomorfizmem.** *Zbiór wszystkich endomorfizmów oznaczamy $End(P)$.*

(8) *Izomorfizm $\phi : P \to P$ nazywamy* **automorfizmem.** *Zbiór wszystkich automorfizmów oznaczamy $Aut(P)$.*

(9) *Jeśli $\phi : P \to R$ 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 10.1. *Niech P, R będą pierścieniami, niech $\phi : P \to R$ 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) $\phi : P \to R$ *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 10.1. *Niech P, R będą pierścieniami, niech $\phi : P \to R$ będzie homomorfizmem. Wówczas:*

(1) $\text{im}\phi < R$;
(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 $\psi : R \to P$ 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 kategoryjnym;*
(6) *ϕ jest epimorfizmem wtedy i tylko wtedy, gdy jest epimorfizmem kategoryjnym.*

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

Przykłady:

(1) $\phi : P \to P$, $\phi(x) = x$ jest homomorfizmem;
(2) $\phi : P^X \to P$, $\phi(f) = f(x_0)$ jest homomorfizmem, gdzie $X \neq \emptyset$ oraz $x_0 \in X$ jest ustalonym elementem;
(3) $\phi : \mathbb{Z} \to \mathbb{Z}_n$, $\phi(x) =$ reszta z dzielenia x przez n jest homomorfizmem;
(4) $\phi : \mathbb{Z} \to P$, $\phi(x) = x \cdot 1_P$ jest homomorfizmem.

Twierdzenie 10.2. *Niech P, R będą pierścieniami, $P_1 < P$, $R_1 < R$, niech $\phi : P \to R$ będzie homomorfizmem. Wówczas:*

(1) $\phi(P_1) < R$,
(2) $\phi^{-1}(R_1) < R$.

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

Definicja 10.2. *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 $I \lhd R$.

Uwaga 10.2. *Niech $(R, +, \cdot)$ będzie pierścieniem, niech $I \lhd R$. Wówczas I jest podgrupą normalną grupy $(R, +)$.*

Przykłady:

(5) Rozważmy pierścień $(R, +, \cdot)$. Wówczas $R \lhd R$ i nazywamy go **ideałem niewłaściwym.**
(6) Rozważmy pierścień $(R, +, \cdot)$. Wówczas $\{0\} \lhd R$ i nazywamy go **ideałem zerowym.** Ideały niewłaściwy i zerowy nazywamy **ideałami trywialnymi.**
(7) Rozważmy pierścień $\mathbb{Z}$. Wówczas $3\mathbb{Z} \lhd \mathbb{Z}$.
(8) Rozważmy pierścień $\mathbb{R}^{\mathbb{R}}$. Wówczas $I = \{f \in \mathbb{R}^{\mathbb{R}} : f(1) = 0\} \lhd \mathbb{R}^{\mathbb{R}}$.

Twierdzenie 10.3. *Niech P, R będą pierścieniami, niech $\phi : P \to R$ będzie homomorfizmem. Wówczas:*

(1) $\ker \phi \lhd P$,
(2) *jeśli $J \lhd R$, to $\phi^{-1}(J) \lhd P$ oraz* $\ker \phi \subset \phi^{-1}(J)$,
(3) *jeśli $I \lhd P$ i ϕ jest epimorfizmem, to $\phi(I) \lhd P$.*

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 10.4. *Niech $(R, +, \cdot)$ będzie pierścieniem, niech $I \lhd R$. 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 10.5. *Niech $(R, +, \cdot)$ będzie pierścieniem. Wówczas:*

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

Dowód. ($\Rightarrow$): załóżmy, że R jest ciałem. Ustalmy $I \lhd R$ 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 $I = R$.
($\Leftarrow$): załóżmy, 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 $I_a \lhd R$: istotnie, ustalmy $x_1 a, x_2 a \in I_a$, $y \in R$. Wówczas
$$x_1 a - x_2 a = (x_1 - x_2)a \in I_a$$
oraz
$$x_1 ay = (x_1 y)a \in I_a.$$
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 10.6 (lemat o odpowiedniości między ideałami)**.** *Niech P, R będą pierścieniami, $\pi : P \to R$ homomorfizmem surjektywnym i niech $N = \ker \pi$. Oznaczmy*
$$\mathcal{I} = \{I : I \lhd P \text{ oraz } N \subset I\}, \mathcal{J} = \{J : J \lhd R\}.$$
Wówczas odwzorowania
$$\phi : \mathcal{I} \to \mathcal{J}, \phi(I) = \pi(I),$$
$$\psi : \mathcal{J} \to \mathcal{I}, \psi(J) = \pi^{-1}(K)$$
są wzajemnie odwrotne.

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

10.2. **Ideały generowane przez zbiory.**

Twierdzenie 10.7. *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 10.3. *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 10.3. *Niech $(R, +, \cdot)$ będzie pierścieniem oraz $P < R$. Wówczas:*
(1) $(\{0\}) = \{0\}$,
(2) $(1) = R$.

Definicja 10.4. *Niech $(R, +, \cdot)$ będzie pierścieniem, niech $I \lhd R$. Każdy zbiór A o tej własności, że $(A) = I$ nazywamy* **zbiorem generatorów** *ideału I. Jeśli $A = \{a_1, \ldots, a_n\}$ to oznaczamy*

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

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

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

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

$$(A) = \{a_1b_1 + \ldots + a_nb_n : n \in \mathbb{N}, a_i \in A, b_i \in R\}.$$

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

Wniosek 10.1. *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 $a_1, \ldots, a_n \in R$. Wówczas:*

$$(a_1, \ldots, a_n) = \{a_1b_1 + \ldots + a_nb_n : b_i \in R\}.$$

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 10.5. *Niech $(R, +, \cdot)$ będzie pierścieniem, niech $I, J \lhd R$.*

(1) *Ideał $(I \cup J)$ nazywamy* **sumą ideałów** *I i J i oznaczamy $I + J$.*
(2) *Ideał $(\{i \cdot j : i \in I, j \in J\})$ nazywamy* **iloczynem ideałów** *I i J i oznaczamy $I \cdot J$.*

Twierdzenie 10.9 (o postaci elementów sumy i iloczynu ideałów)**.** *Niech $(R, +, \cdot)$ będzie pierścieniem, niech $I, J \lhd R$.*

(1) $I + J = \{i + j : i \in I, j \in J\}$;
(2) $I \cdot J = \{a_1b_1 + \ldots + a_nb_n : n \in \mathbb{N}, a_i \in I, b_i \in J\}$

Twierdzenie 10.10. *Pierścień $\mathbb{Z}$ jest pierścieniem ideałów głównych.*

Dowód. Ustalmy $I \lhd \mathbb{Z}$. 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 $b \in I$. Dzieląc 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 $b = qc \in (c)$. □

Twierdzenie 10.11. *Niech F będzie ciałem. Pierścień $F[x]$ jest pierścieniem ideałów głównych.*

Dowód. Ustalmy $I \lhd F[x]$. 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 $g \in I$. Dzieląc 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 $g = qh \in (h)$. □