

11. WYKŁAD 11: PIERŚCIEŃ ILORAZOWY, TWIERDZENIE O HOMOMORFIZMIE. IDEAŁY PIERWSZE I MAKSYMALNE.

11.1. Pierścień ilorazowy, twierdzenie o homomorfizmie.

Definicja i Uwaga 11.1. 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 11.2. 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 11.1. 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 11.1 (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 11.2. 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 11.3 (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

$$\begin{array}{ccc} & P & \\ \kappa \swarrow & & \searrow \phi \\ P/I & \xrightarrow[\psi]{\text{"na"}} & R \end{array}$$

jest przemienny.

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

Wniosek 11.4. 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 11.2 (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 $\text{im}\phi = \mathbb{C}$, $\ker \phi = (x^2 + 1)$, a zatem $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

11.2. Ideały pierwsze i maksymalne.

Definicja 11.1. 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 11.3. 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 11.5. 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 11.6. 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 11.2. 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 11.4. *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 odpowiedniości 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 11.7. *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 11.8. *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 11.9. *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 11.10. *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 11.1. *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 11.5. *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 10.7 $K \triangleleft R$. 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 11.11. *Niech R będzie pierścieniem. Wówczas:*

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

Definicja 11.3. *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 $\text{Specm}(R)$.