

9. WYKŁAD 9: SPECJALNE TYPY ELEMENTÓW PIERŚCIEŃ.

Definicja 9.1. Niech $(R, +, \cdot)$ będzie pierścieniem.

- (1) Element $x \in R$ taki, że

$$\exists y \in R \setminus \{0\} x \cdot y = 0$$

nazywamy **dzielnikiem zera**. Zbiór wszystkich dzielników zera oznaczamy przez $\mathcal{D}(R)$.

- (2) Element $x \in R$ taki, który nie jest dzielnikiem zera, nazywamy **elementem regularnym**.

Przykłady:

- (1) Niech $(R, +, \cdot)$ będzie pierścieniem. Wówczas 0 jest dzielnikiem zera, nazywamy je **niewłaściwym** dzielnikiem zera. Wszystkie pozostałe dzielniki zera nazywać będziemy **właściwymi**.
 (2) Rozważmy pierścień $\mathbb{Z}_6$. Wówczas 0, 2, 3, 4 są dzielnikami zera.
 (3) Rozważmy pierścień $\mathbb{Q} \times \mathbb{Q}$. Wówczas $(1, 0)$ i $(0, 1)$ są dzielnikami zera.

Twierdzenie 9.1. Niech $(R, +, \cdot)$ będzie pierścieniem, niech $x, y \in R$. Wówczas:

- (1) $xy = 0 \Rightarrow x \in \mathcal{D}(R) \vee y \in \mathcal{D}(R)$;
 (2) jeśli x jest regularny, to

$$xy = 0 \Rightarrow y = 0;$$

- (3) jeśli x jest regularny, to

$$xy = xz \Rightarrow y = z.$$

Przykład:

- (4) Rozważmy pierścień $\mathbb{Z}_6$. Wówczas $3 \cdot 2 = 3 \cdot 4$, ale $2 \neq 4$.

Definicja 9.2. Pierścień bez właściwych dzielników zera nazywamy **pierścieniem całkowitym** (lub **dziedzina całkowitości**, lub **dziedzina**).

Przykłady:

- (5) $\mathbb{Z}$;
 (6) $\mathbb{Z}[i]$;
 (7) $\mathbb{Z}_5$.

Uwaga 9.1. Podpierścień pierścienia całkowitego jest pierścieniem całkowitym.

Definicja 9.3. Niech $(R, +, \cdot)$ będzie pierścieniem. Element $x \in R$ nazywamy **elementem odwracalnym**, gdy

$$\exists y \in R (x \cdot y = 1_R).$$

Zbiór wszystkich elementów odwracalnych oznaczamy przez $U(R)$.

Twierdzenie 9.2. Niech $(R, +, \cdot)$ będzie pierścieniem. Wówczas:

- (1) zbiór elementów regularnych jest zamknięty na mnożenie;
 (2) każdy element odwracalny jest regularny;
 (3) $U(R)$ jest grupą abelową, nazywamy ją **grupą elementów odwracalnych pierścienia R** .

Dowód. (1) Niech $x, y \in R$ będą elementami regularnymi. Przypuśćmy, że $xy \in \mathcal{D}(R)$, a więc założymy, że istnieje $z \in R \setminus \{0\}$ taki, że $(xy)z = 0$. Wówczas również $x(yz) = 0$ i ponieważ x jest regularny, więc $yz = 0$. Zatem $y \in \mathcal{D}(R)$, co daje sprzeczność.

- (2) Ustalmy $x \in U(R)$ i przypuśćmy, że $x \in \mathcal{D}(R)$, a więc założmy, że istnieje $z \in R \setminus \{0\}$ taki, że $xz = 0$. Z drugiej strony istnieje $y \in R$ taki, że $xy = 1$, a zatem

$$0 = 0z = (xz)y = xyz = 1y = y$$

co daje sprzeczność.

- (3) Wystarczy pokazać, że zbiór elementów odwracalnych jest zamknięty na mnożenie. Ustalmy $x, y \in U(R)$. Wówczas istnieją $z, t \in R$ takie, że $xz = 1$ oraz $yt = 1$. Zatem:

$$1 = 1 \cdot 1 = xzyt = (xy)(zt),$$

więc $xy \in U(R)$.

□

Przykłady:

- (8) $\mathbb{Z}, U(\mathbb{Z}) = \{-1, 1\}$;
- (9) $\mathbb{Z}_6, U(\mathbb{Z}_6) = \{1, 5\}$;
- (10) $\mathbb{Z}_5, U(\mathbb{Z}_5) = \{1, 2, 3, 4\} = \mathbb{Z}_5^*$;
- (11) $\mathbb{Q}, U(\mathbb{Q}) = \mathbb{Q}^*$;
- (12) $\mathbb{Q} \times \mathbb{Q}, (2, 3) \in \mathbb{Q} \times \mathbb{Q}$.

Uwaga 9.2. Niech $(R, +, \cdot)$ będzie pierścieniem. Wówczas:

- (1) R jest ciałem wtedy i tylko wtedy, gdy $U(R) = R^*$;
- (2) jeśli R jest ciałem, to R jest pierścieniem całkowitym;
- (3) jeśli R jest ciałem i $P < R$, to P jest pierścieniem całkowitym.

Przykład:

- (13) Rozważmy $\mathbb{Z} < \mathbb{Q}$. Wówczas $\mathbb{Z}$ jest pierścieniem całkowitym, ale $\mathbb{Z}$ nie jest ciałem.

Uwaga 9.3. Niech R_1, R_2 będą pierścieniami. Wówczas:

- (1) $U(R_1 \times R_2) = U(R_1) \times U(R_2)$;
- (2) $\mathcal{D}(R_1 \times R_2) = R_1 \times \mathcal{D}(R_2) \cup \mathcal{D}(R_1) \times R_2$.

Twierdzenie 9.3. Niech $(R, +, \cdot)$ będzie pierścieniem skończonym. Następujące warunki są równoważne:

- (1) x jest elementem odwracalnym;
- (2) x jest elementem regularnym;
- (3) istnieje $m \in \mathbb{N}$ takie, że $x^m = 1$.

Dowód. (1) $\Rightarrow$ (3): ustalmy $x \in U(R)$. R jest skończony, więc $U(R)$ jest skończona, powiedzmy $|U(R)| = m$. Wówczas $x^m = 1$.

(3) $\Rightarrow$ (2): ustalmy $x \in R$ i niech $x^m = 1$, dla pewnego $m \in \mathbb{N}$. Jeżeli $m = 1$, to $x = 1$ i w szczególności x jest regularny. Jeśli $m > 1$, to wówczas

$$1 = x^m = x^{m-1}x,$$

a zatem $x \in U(R)$ i tym samym x jest regularny.

- (2) $\Rightarrow$ (1): ustalmy $x \in R$ i niech x będzie regularny. Zdefiniujemy odwzorowanie $f_x : R \rightarrow R$ wzorem

$$f_x(y) = xy.$$

Pokażemy, że f_x jest różnowartościowe. W tym celu ustalmy $y, z \in R$ i założmy, że $f_x(y) = f_x(z)$. Wówczas $xy = xz$ i ponieważ x jest regularny, więc $y = z$.

Ponieważ R jest skończony, więc f_x jest też surjektywne. W szczególności

$$\exists y \in R[f_x(y) = 1],$$

a więc dla pewnego $y \in R$ zachodzi $xy = 1$. Zatem $x \in U(R)$. □

Wniosek 9.1. Niech $(R, +, \cdot)$ będzie pierścieniem skończonym. Wówczas:

- (1) $R = U(R) \cup \mathcal{D}(R)$ oraz $U(R) \cap \mathcal{D}(R) = \emptyset$;
- (2) R jest ciałem wtedy i tylko wtedy, gdy R jest pierścieniem całkowitym.

Uwaga 9.4. Niech $n > 1$. Wówczas:

- (1) $\mathcal{D}(\mathbb{Z}_n) = \{k \in \mathbb{Z}_n : \text{NWD}(k, n) > 1\}$;
- (2) $U(\mathbb{Z}_n) = \{k \in \mathbb{Z}_n : \text{NWD}(k, n) = 1\}$.

Wniosek 9.2. Niech $n > 1$. Następujące warunki są równoważne:

- (1) $\mathbb{Z}_n$ jest pierścieniem całkowitym;
- (2) $\mathbb{Z}_n$ jest ciałem;
- (3) n jest liczbą pierwszą.

Definicja 9.4. Niech $(R, +, \cdot)$ będzie pierścieniem. Wówczas:

- (1) element $x \in R$ nazywamy **nilpotentnym** (lub **nilpotentem**), gdy

$$\exists n \in \mathbb{N}(x^n = 0),$$

a zbiór wszystkich elementów nilpotentnych pierścienia R oznaczamy przez $\text{Nil}(R)$;

- (2) element $x \in R$ nazywamy **idempotentnym** (lub **idempotentem**), gdy

$$x^2 = x;$$

- (3) elementy idempotentne $x, y \in R$ nazywamy **idempotentami ortogonalnymi**, gdy:

$$x + y = 1 \text{ oraz } xy = 0.$$

Uwaga 9.5. Niech $(R, +, \cdot)$ będzie pierścieniem. Wówczas:

- (1) każdy element nilpotentny jest dzielnikiem zera;
- (2) każdy element idempotentny różny od 1 jest dzielnikiem zera.

Dowód. Część (1) jest oczywista, a dla dowodu części (2) zauważmy, że

$$x(x - 1) = x^2 - x = x - x = 0.$$

□

Przykłady:

- (14) Rozważmy dowolny pierścień R . Wówczas 0 jest nilpotentem, nazywamy go **nilpotentem trywialnym**.
- (15) Rozważmy pierścień $\mathbb{Z}_6$. Wówczas 0 jest jedynym nilpotentem.
- (16) Rozważmy dowolny pierścień R . Wówczas 0 i 1 są idempotentami, nazywamy je **idempotentami trywialnymi**.
- (17) Rozważmy pierścień $\mathbb{Z}_6$. Wówczas 0, 1, 3, 4 są idempotentami.
- (18) Rozważmy pierścień $\mathbb{Z}_{10}$. Wówczas 5 i 6 są idempotentami ortogonalnymi.