

6. WYKŁAD 6: POJĘCIE PIERŚCIEŃ. PODPIERŚCIEŃ. PODPIERŚCIEŃ GENEROWANE PRZEZ ZBIÓR. SPECJALNE TYPY ELEMENTÓW PIERŚCIEŃ.

6.1. Pojęcie pierścienia.

Definicja 6.1. Niech R będzie zbiorem niepustym.

- (1) Algebrę $(R, +, \cdot)$ nazywamy **pierścieniem**, gdy $(R, +)$ jest grupą abelową, działanie $\cdot$ jest łączne oraz rozdzielne względem działania $+$, to znaczy

$$\forall x, y, z \in R [x \cdot (y + z) = x \cdot y + x \cdot z],$$

$$\forall x, y, z \in R [(y + z) \cdot x = y \cdot x + z \cdot x].$$

Działanie $+$ nazywamy **dodawaniem** w pierścieniu R , a działanie $\cdot$ **mnożeniem**. Element neutralny dodawania nazywamy **zerem** i oznaczamy przez 0 . Pierścień $(R, +, \cdot)$ nazywamy **pierścieniem zerowym**, jeżeli $R = \{0\}$.

- (2) Algebrę $(R, +, \cdot)$ nazywamy **pierścieniem przemiennym**, gdy jest pierścieniem i gdy mnożenie jest przemiennie.
- (3) Algebrę $(R, +, \cdot)$ nazywamy **pierścieniem z jedyneką**, gdy jest pierścieniem i gdy mnożenie ma element neutralny, który wówczas nazywamy **jedyneką** i oznaczamy przez 1 .
- (4) Algebrę $(R, +, \cdot)$ nazywamy **ciałem**, gdy jest niezerowym pierścieniem przemiennym z jedyneką i gdy dla każdego elementu różnego od 0 istnieje element odwrotny względem mnożenia.

Uwaga 6.1. Niech $(R, +, \cdot)$ będzie ciałem. Wówczas:

- (1) R zawiera co najmniej dwa elementy,
- (2) $(R, +)$ jest grupą abelową,
- (3) $(R^*, \cdot)$ jest grupą abelową, gdzie $R^* = R \setminus \{0\}$.

Przykłady:

- (1) **Pierścień liczbowe.** $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ są przykładami pierścieni przemiennych z jedyneką. $(\mathbb{N}, +, \cdot)$ nie jest pierścieniem. Ponadto $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ są ciałami, zaś $(\mathbb{Z}, +, \cdot)$ nie jest.
- (2) **Pierścień reszt.** Niech $n \in \mathbb{N}$ i rozważmy $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ z działaniami $\oplus_n$ oraz $\otimes_n$. $(\mathbb{Z}_n, \oplus_n, \otimes_n)$ są przykładami pierścieni przemiennych z jedyneką. $(\mathbb{Z}_n, \oplus_n, \otimes_n)$ na ogół nie jest ciałem, chyba że n jest liczbą pierwszą.
- (3) **Pierścień wielomianów.** Niech $\mathbb{R}[x]$ będzie zbiorem wielomianów zmiennej x o współczynnikach rzeczywistych. Wówczas $(\mathbb{R}[x], +, \cdot)$ jest pierścieniem przemiennym z jedyneką, który nie jest ciałem, gdzie $+$ i $\cdot$ oznaczają działania, odpowiednio, dodawania i mnożenia wielomianów.
- (4) **Pierścień macierzy.** Niech F będzie dowolnym ciałem, niech $M(n, F)$ oznacza zbiór macierzy kwadratowych stopnia n o współczynnikach z ciała F . $(M(n, F), +, \cdot)$ jest pierścieniem z jedyneką, przy czym $+$ i $\cdot$ oznaczają tu, odpowiednio, dodawanie i mnożenie macierzy. Pierścień ten na ogół nie jest przemienny.
- (5) **Pierścień endomorfizmów.** Niech V będzie przestrzenią liniową. $(V, +)$. Oznaczmy przez $\text{End}(V)$ zbiór endomorfizmów liniowych przestrzeni V . $(\text{End}(V), + \circ)$ jest pierścieniem z jedyneką, który na ogół nie jest przemienny, przy czym $+$ i $\circ$ są tu działaniami, odpowiednio, dodawania i składania przekształceń liniowych.
- (6) **Pierścień funkcji.** Niech $(R, +_R, \cdot_R)$ będzie pierścieniem, niech $X \neq \emptyset$. W rodzinie funkcji

$$R^X = \{f : X \rightarrow R : f \text{ jest funkcją}\}$$

definiujemy działania

$$(f + g)(x) = f(x) +_R g(x) \text{ oraz } (f \cdot g)(x) = f(x) \cdot_R g(x).$$

$(R^X, +, \cdot)$ jest pierścieniem, który jest przemienny, gdy R jest przemienny.

- (7) **Skończony produkt pierścieni.** Niech $(R_1, +_1, \cdot_1), \dots, (R_n, +_n, \cdot_n)$ będą pierścieniami. W produkcie kartezjańskim $R = R_1 \times \dots \times R_n$ definiujemy działania “po współrzędnych”:

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 +_1 b_1, \dots, a_n +_n b_n),$$

$$(a_1, \dots, a_n) \cdot (b_1, \dots, b_n) = (a_1 \cdot_1 b_1, \dots, a_n \cdot_n b_n).$$

$(R, +, \cdot)$ jest pierścieniem, który jest przemienny (z jedyneką), gdy wszystkie pierścienie $R_1, \dots, R_n$ są przemienne (z jedyneką).

- (8) **Pierścień grupowy.** Niech $(G, *)$ będzie grupą, niech $(R, +_R, \cdot_R)$ będzie pierścieniem. Rozważmy zbiór

$$R[G] = \text{zbiór funkcji } f : G \rightarrow R \text{ prawie wszędzie równych } 0.$$

W zbiorze tym definiujemy działania:

$$(f + g)(x) = f(x) +_R g(x),$$

$$(f \cdot g)(x) = \sum_{y \in G} f(x * y^{-1}) \cdot_R g(y).$$

$(R[G], +, \cdot)$ jest pierścieniem.

W dowolnym pierścieniu $(R, +, \cdot)$ wprowadzamy oznaczenia:

$$xy + z = (x \cdot y) + z,$$

$$\sum_{i=1}^n x_i = x_1 + \dots + x_n, \sum_{i=1}^0 x_i = 0,$$

$$\prod_{i=1}^n x_i = x_1 \cdot \dots \cdot x_n, \prod_{i=1}^0 x_i = 1.$$

W szczególności $\sum_{i=1}^n x = nx$ oraz $\prod_{i=1}^n x = x^n$.

Twierdzenie 6.1. Niech $(R, +, \cdot)$ będzie pierścieniem przemennym z jedyneką. Wówczas:

- (1) $-(-x) = x$,
- (2) $-(x + y) = (-x) + (-y)$,
- (3) $n(mx) = nm x$,
- (4) $nx + mx = (n + m)x$,
- (5) $0x + x0 = 0$,
- (6) $(-1)x = -x$,
- (7) $(-x)y = -(xy) = x(-y)$,
- (8) $(-x)(-y) = xy$,
- (9) $x(y - z) = xy - xz$,
- (10) $(x - y)z = xz - yz$,
- (11) $x + z = y + z \Rightarrow x = y$,
- (12) $x^n x^m = x^{n+m}$,
- (13) $(x^n)^m = x^{nm}$,
- (14) $(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}$.

Prosty dowód pozostawiamy Czytelnikowi jako ćwiczenie.

W dalszym ciągu tego wykładu pisząc “pierścień” będziemy na ogół mieli na myśli “pierścień przemienny z jedynką”.

6.2. Podpierścienie, podpierścienie generowane przez zbiór.

Definicja 6.2. Niech $(R, +, \cdot)$ będzie pierścieniem. Podzbiór $P \neq \emptyset$ zbioru R nazywamy **podpierścieniem** pierścienia R (piszemy $P < R$), gdy $(P, + \upharpoonright_{P \times P}, \cdot \upharpoonright_{P \times P})$ jest pierścieniem.

Przykłady:

- (1) $\mathbb{Z} < \mathbb{R}$;
- (2) $\mathbb{R} < \mathbb{C}$;
- (3) $\mathbb{Z}_n$ nie jest podpierścieniem pierścienia $\mathbb{Z}$.

Twierdzenie 6.2. Niech $\emptyset \neq P \subset R$ i niech $(R, +, \cdot)$ będzie pierścieniem. Następujące warunki są równoważne:

- (1) $P < R$;
- (2) P ma następujące własności:
 - $1_R \in P$,
 - $\forall x, y \in P (x - y \in P)$,
 - $\forall x, y \in P (x \cdot y \in P)$.

Prosty dowód pozostawiamy Czytelnikowi jako ćwiczenie.

Przykłady:

- (4) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} < \mathbb{R}$. Istotnie, $1 \in \mathbb{Z}[\sqrt{2}]$. Ustalmy $x, y \in \mathbb{Z}[\sqrt{2}]$, to znaczy niech $x = x_1 + x_2\sqrt{2}$, $y = y_1 + y_2\sqrt{2}$. Wówczas:

$$\begin{aligned} x - y &= (x_1 - y_1) + (x_2 - y_2)\sqrt{2} \in \mathbb{Z}[\sqrt{2}], \\ x \cdot y &= (x_1y_1 + 2y_1y_2) + (x_1y_2 + x_2y_1)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]. \end{aligned}$$

- (5) $\mathbb{Z}_{(p)} = \{\frac{m}{n} : NWD(m, n) = 1 \text{ oraz } p \nmid n\} < \mathbb{Q}$, gdzie p jest liczbą pierwszą. Istotnie, $1 \in \mathbb{Z}_{(p)}$. Ustalmy $x, y \in \mathbb{Z}_{(p)}$, to znaczy niech $x = \frac{m_1}{n_1}$, $NWD(m_1, n_1) = 1$, $p \nmid n_1$, $y = \frac{m_2}{n_2}$, $NWD(m_2, n_2) = 1$, $p \nmid n_2$. Wówczas:

$$\begin{aligned} \frac{m_1}{n_1} - \frac{m_2}{n_2} &= \frac{m_1n_2 - m_2n_1}{n_1n_2} \in \mathbb{Z}_{(p)}, \text{ bo } p \nmid n_1n_2 \text{ oraz } NWD(m_1n_2 - m_2n_1, n_1n_2) = 1, \\ \frac{m_1}{n_1} \cdot \frac{m_2}{n_2} &= \frac{m_1m_2}{n_1n_2} \in \mathbb{Z}_{(p)}, \text{ bo } p \nmid n_1n_2 \text{ oraz } NWD(m_1m_2, n_1n_2) = 1. \end{aligned}$$

Pierścień $\mathbb{Z}_{(p)}$ nazywamy **pierścieniem liczb p -całkowitych**.

Twierdzenie 6.3. Niech $\mathcal{R} = \{R_i : i \in I\}$ będzie rodziną podpierścieni pierścienia R ;

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

Prosty dowód pozostawiamy Czytelnikowi jako ćwiczenie.

Definicja 6.3. Niech $(R, +, \cdot)$ będzie pierścieniem oraz $A \subset R$ pewnym zbiorem. Najmniejszy w sensie inkluzji podpierścień pierścienia R zawierający zbiór A (tj. przekrój wszystkich podpierścieni pierścienia R zawierających A) nazywamy **podpierścieniem generowanym przez A** i oznaczamy $[A]$.

Uwaga 6.2. Niech $(R, +, \cdot)$ będzie pierścieniem oraz $P < R$. Wówczas:

- (1) $[P] = P$,
- (2) $[R] = R$.

Definicja 6.4. Każdy zbiór A o tej własności, że $[A] = R$ nazywamy **zbiorem generatorów pierścienia R** . Jeśli $A = \{a_1, \dots, a_n\}$ to oznaczamy

$$[a_1, \dots, a_n] = \langle A \rangle.$$

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

$$R = [a_1, \dots, a_n].$$

Twierdzenie 6.4 (o postaci elementów podpierścienia generowanego przez zbiór). Niech $(R, +, \cdot)$ będzie pierścieniem oraz $A \subset R$ pewnym zbiorem. Wówczas

$$[A] = \{x : x \text{ jest sumą elementów postaci } \pm a_1 \cdot \dots \cdot a_k, k \in \mathbb{N} \cup \{0\}, a_i \in A\}.$$

Prosty dowód pozostawiamy Czytelnikowi jako ćwiczenie.

Definicja 6.5. Niech $(R, +, \cdot)$ będzie pierścieniem oraz $A \subset R$ pewnym zbiorem. Niech ponadto $P < R$. Podpierścień generowany przez zbiór $P \cup A$ nazywamy **podpierścieniem generowanym przez A nad P** i oznaczamy $P[A]$.

Jeżeli $A = \{a_1, \dots, a_n\}$, to pierścień $R[\{a_1, \dots, a_n\}]$ nazywamy **podpierścieniem skończenie generowanym przez A nad P** i oznaczamy $P[a_1, \dots, a_n]$.

Wniosek 6.1 (o postaci elementów podpierścienia generowanego przez zbiór nad pierścieniem). Niech $(R, +, \cdot)$ będzie pierścieniem oraz $A \subset R$ pewnym zbiorem. Niech $P < R$. Wówczas

$$P[A] = \{x : x \text{ jest sumą elementów postaci } pa_1 \cdot \dots \cdot a_k, k \in \mathbb{N} \cup \{0\}, a_i \in A, p \in P\}.$$

Wniosek 6.2. (1) Niech $(R, +, \cdot)$ będzie pierścieniem oraz niech $a \in R$. Niech $P < R$. Wówczas

$$P[a] = \{x_0 + x_1a + \dots + x_na^n : n \in \mathbb{N} \cup \{0\}, x_i \in P\}.$$

(2) Niech $(R, +, \cdot)$ będzie pierścieniem oraz niech $\{a_1, \dots, a_n\} \subset R$. Niech $P < R$. Wówczas

$$P[a_1, \dots, a_n] = \{x : x \text{ jest sumą elementów postaci } pa_1^{i_1} \cdot \dots \cdot a_n^{i_n}, i_1, \dots, i_n \in \mathbb{N} \cup \{0\}, p \in P\}.$$

Przykłady:

(6) $\mathbb{Z}[i] = \{x_0 + x_1i + x_2i^2 + \dots + x_ni^n : n \in \mathbb{N} \cup \{0\}, x_i \in \mathbb{Z}\} = \{u + iv : u, v \in \mathbb{Z}\}$. Pierścień ten nazywamy **pierścieniem Gaussa**.

(7) $\mathbb{Z}[\sqrt{2}] = \{x_0 + x_1\sqrt{2} + x_2(\sqrt{2})^2 + \dots + x_n(\sqrt{2})^n : n \in \mathbb{N} \cup \{0\}, x_i \in \mathbb{Z}\} = \{u + \sqrt{2}v : u, v \in \mathbb{Z}\}$.

(8) $\mathbb{Z}[\sqrt[3]{2}] = \{x_0 + x_1\sqrt[3]{2} + x_2(\sqrt[3]{2})^2 + \dots + x_n(\sqrt[3]{2})^n : n \in \mathbb{N} \cup \{0\}, x_i \in \mathbb{Z}\} = \{u + \sqrt[3]{2}v + \sqrt[3]{4}t : u, v, t \in \mathbb{Z}\}$.

6.3. Specjalne typy elementów pierścienia.

Definicja 6.6. 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 6.5. *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 6.7. *Pierścień bez właściwych dzielników zera nazywamy **pierścieniem całkowitym** (lub dziedziną całkowitości, lub dziedziną).*

Przykłady:

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

Uwaga 6.3. *Podpierścień pierścienia całkowitego jest pierścieniem całkowitym.*

Definicja 6.8. *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 6.6. *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 założmy, 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 6.4. 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 6.5. 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 6.7. 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. Zdefiniujmy 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 6.3. 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 6.6. 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 6.4. 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 6.9. 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 6.7. 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.