Wykład 9
Podpierścienie, elementy odwracalne, dzielniki zera

1 Określenie podpierścienia

Definicja 9.1. *Podpierścieniem* pierścienia $(P, +, \cdot, 0, 1)$ nazywamy taki podzbiór $A \subseteq P$, który jest pierścieniem ze względu na wszystkie działania określone w pierścieniu P (zredukowane do A).

Stwierdzenie 9.2. *$A \subseteq P$ jest podpierścieniem pierścienia P wtedy i tylko wtedy, gdy spełnia następujące warunki:*
(I) $1 \in A$ *oraz (II)* $\forall_{a,b \in A}\ a - b, a \cdot b \in A$.

Dowód. Załóżmy, że A jest podpierścieniem pierścienia P. Wtedy $0, 1 \in A$ (ze względu na wykonalność działań 0-argumentowych) oraz dla dowolnego $a \in A$, $-a \in A$ (ze względu na wykonalność działania 1-argumentowego) i ponadto dla $a, b \in A$, $a \cdot b \in A$ oraz $a - b = a + (-b) \in A$ (ze względu na wykonalność mnożenia i dodawania).

Na odwrót, załóżmy, że $1 \in A$ oraz $a - b, a \cdot b \in A$ dla dowolnych $a, b \in A$. Wtedy $0 = 1 - 1 \in A$, skąd dla $b \in A$, $-b = 0 - b \in A$, więc dla $a, b \in A$, $a + b = a - (-b) \in A$. Zatem w A jest wykonalne mnożenie i dodawanie. Ponieważ wszystkie aksjomaty pierścienia są spełnione nawet w P, więc $(A, +, \cdot, 0, 1)$ jest pierścieniem. □

Stwierdzenie 9.3. *W dowolnym pierścieniu P podzbiór $\langle 1 \rangle = \{k \cdot 1 \ : \ k \in \mathbb{Z}\}$ jest najmniejszym (w sensie inkluzji) podpierścieniem P.*

Dowód. Ponieważ $1 = 1 \cdot 1$, więc $1 \in \langle 1 \rangle$. Weźmy dowolne $a, b \in \langle 1 \rangle$. Wtedy istnieją $k, l \in \mathbb{Z}$ takie, że $a = k \cdot 1$ i $b = l \cdot 1$. Stąd $a - b = (k - l) \cdot 1 \in \langle 1 \rangle$ oraz $a \cdot b = (k \cdot 1) \cdot (l \cdot 1) = (kl) \cdot 1 \in \langle 1 \rangle$. Zatem na mocy Stwierdzenia 9.2, $\langle 1 \rangle$ jest podpierścieniem w P. Niech A będzie dowolnym podpierścieniem pierścienia P. Wtedy $1 \in A$ i A jest podgrupą grupy P^+. Stąd $\langle 1 \rangle \subseteq A$, czyli $\langle 1 \rangle$ jest najmniejszym w sensie inkluzji podpierścieniem w P. □

Twierdzenie 9.4. *Część wspólna dowolnej niepustej rodziny podpierścieni pierścienia P jest podpierścieniem P.*

Dowód. Niech $\{A_t\}_{t \in T}$ będzie dowolną niepustą rodziną podpierścieni pierścienia P oraz niech $A = \bigcap_{t \in T} A_t$. Ponieważ $1 \in A_t$ dla każdego $t \in T$, więc $1 \in A$. Weźmy dowolne $a, b \in A$. Wtedy $a, b \in A_t$ dla każdego $t \in T$, więc ze Stwierdzenia 9.2, $a - b, a \cdot b \in A_t$ dla każdego $t \in T$. Zatem $a - b, a \cdot b \in A$. Stąd na mocy Stwierdzenia 9.2, A jest podpierścieniem pierścienia P. □

Przykład 9.5. Niech P będzie pierścieniem. Udowodnimy, że dla dowolnego podzbioru $X \subseteq P$ istnieje najmniejszy (w sensie inkluzji) podpierścień pierścienia P zawierający zbiór X. Nazywamy go *podpierścieniem generowanym przez zbiór* X i oznaczamy przez $[X]$. Zatem:

$$X \subseteq [X] \text{ i } [X] \text{ jest podpierścieniem pierścienia } P \text{ oraz} \tag{1}$$

$$[X] \subseteq A \text{ dla każdego podpierścienia } A \text{ pierścienia } P \text{ takiego, że } X \subseteq A. \tag{2}$$

Rzeczywiście, niech $\{A_t\}_{t\in T}$ będzie rodziną wszystkich podpierścieni pierścienia P zawierających zbiór X. Wtedy $P \in \{A_t\}_{t\in T}$, więc z Twierdzenia 9.3 mamy, że $A = \bigcap_{t\in T} A_t$ jest podpierścieniem pierścienia P. Ale $X \subseteq A_t$ dla każdego $t \in T$, więc $X \subseteq A$, skąd A jest najmniejszym elementem w rodzinie $\{A_t\}_{t\in T}$, czyli A jest najmniejszym podpierścieniem pierścienia P zawierającym zbiór X.

Ze Stwierdzenia 9.3 wynika od razu, że $[\emptyset] = \langle 1\rangle = \{k \cdot 1 : k \in \mathbb{Z}\}$. Natomiast dla $X \neq \emptyset$ mamy następujące

Stwierdzenie 9.6. *Niech X będzie niepustym podzbiorem pierścienia P. Wówczas $[X]$ składa się ze wszystkich skończonych sum elementów postaci $s \cdot 1$ oraz $k \cdot x_1 \cdot x_2 \ldots \cdot x_n$, gdzie $s, k \in \mathbb{Z}$, $x_1, x_2, \ldots, x_n \in X$ oraz $n = 1, 2, \ldots$.*

Dowód. Oznaczmy przez S zbiór wszystkich skończonych sum elementów postaci $s\cdot 1$ oraz $k\cdot x_1\cdot x_2\ldots\cdot x_n$, gdzie $s, k \in \mathbb{Z}$, $x_1, x_2, \ldots, x_n \in X$ oraz $n = 1, 2, \ldots$. Ponieważ $1 = 1\cdot 1$, więc $1 \in S$. Weźmy dowolne $a, b \in S$. Wtedy a jest skończoną sumą elementów postaci $s \cdot 1$ oraz $k \cdot x_1 \cdot x_2 \ldots \cdot x_n$, dla pewnych $s, k \in \mathbb{Z}$, $x_1, x_2, \ldots, x_n \in X$ i pewnych $n \in \mathbb{N}$ oraz b jest skończoną sumą elementów postaci $t \cdot 1$ oraz $l \cdot y_1 \cdot y_2 \ldots \cdot y_m$, dla pewnych $t, l \in \mathbb{Z}$, $y_1, y_2, \ldots, y_m \in X$ i pewnych $m \in \mathbb{N}$. Z rozdzielności mnożenia względem dodawania wynika zatem, że $a \cdot b$ jest skończoną sumą elementów postaci $(s \cdot 1) \cdot (t \cdot 1) = (st) \cdot 1$, $(s\cdot 1)\cdot(k\cdot x_1\cdot x_2\ldots\cdot x_n) = (sk)\cdot x_1\cdot x_2\ldots\cdot x_n$, $(k\cdot x_1\cdot x_2\ldots\cdot x_n)\cdot(t\cdot 1) = (kt)\cdot x_1\cdot x_2\ldots\cdot x_n$, $(k\cdot x_1\cdot x_2\ldots\cdot x_n)\cdot(l\cdot y_1\cdot y_2\ldots\cdot y_m) = (kl)\cdot x_1\cdot x_2\ldots\cdot x_n\cdot y_1\cdot y_2\ldots\cdot y_m$, więc $a\cdot b \in S$. Ponadto, $s\cdot 1 - t\cdot 1 = (s-t)\cdot 1$ i $-(l\cdot y_1\cdot y_2\ldots\cdot y_m) = (-l)\cdot y_1\cdot y_2\ldots\cdot y_m$, więc $a - b \in S$. Zatem na mocy Stwierdzenia 9.2, S jest podpierścieniem pierścienia P. Ponadto dla dowolnego $x \in X$ mamy, że $x = 1 \cdot x$, więc $x \in S$. Zatem $X \subseteq S$.

Niech teraz A będzie dowolnym podpierścieniem pierścienia P takim, że $X \subseteq A$. Ponieważ $1 \in A$ i $A \leq P^+$, więc $\langle 1\rangle \subseteq A$, skąd $s \cdot 1 \in A$ dla każdego $s \in \mathbb{Z}$. Weźmy teraz dowolne $k \in \mathbb{Z}$, dowolne $n \in \mathbb{N}$ i dowolne $x_1, \ldots, x_n \in X$. Wtedy $x_1, \ldots, x_n \in A$ i A jest pierścieniem, więc $k \cdot x_1 \cdot x_2 \ldots \cdot x_n \in A$. Ale A jest podgrupą grupy P^+, więc wszystkie skończone sumy elementów postaci $s \cdot 1$ oraz $k \cdot x_1 \cdot x_2 \ldots \cdot x_n$, gdzie $s, k \in \mathbb{Z}$, $x_1, x_2, \ldots, x_n \in X$ oraz $n = 1, 2, \ldots$, należą do A. Zatem $S \subseteq A$.

W ten sposób wykazaliśmy, że S spełnia warunki (1) i (2), czyli $S = [X]$. □

Jeśli X jest zbiorem skończonym oraz $X = \{a_1, \ldots, a_m\}$, to zamiast $[\{a_1, \ldots, a_m\}]$ będziemy pisali $[a_1, \ldots, a_m]$.

Uwaga 9.7. Ze Stwierdzenia 9.6 wynika od razu, że jeśli $X = \{a\}$, to podpierścień $[a]$ składa się ze wszystkich elementów postaci $k_0 \cdot 1 + k_1 \cdot a + \ldots + k_m \cdot a^m$, gdzie $k_0, k_1, \ldots, k_m \in \mathbb{Z}$ oraz $m = 0, 1, 2, \ldots$. Zatem:

$$[a] = \{k_0 \cdot 1 + k_1 \cdot a + \ldots + k_n \cdot a^n : k_0, k_1, \ldots, k_n \in \mathbb{Z}, \;\; n = 0, 1, 2, \ldots\}. \tag{3}$$

Podstawiając $X = \{a, b\}$ uzyskamy, że podpierścień $[a, b]$ składa się ze wszystkich skończonych sum elementów postaci $k \cdot a^i b^j$, gdzie $k \in \mathbb{Z}$ oraz $i, j \in \mathbb{N}_0$.

Podstawiając $X = \{a_1, a_2, \ldots, a_s\}$ uzyskamy, że podpierścień $[a_1, a_2, \ldots, a_s]$ składa się ze wszystkich skończonych sum elementów postaci $k \cdot a_1^{i_1} \cdot a_2^{i_2} \cdot \ldots \cdot a_s^{i_s}$, gdzie $k \in \mathbb{Z}$ oraz $i_1, i_2, \ldots, i_s \in \mathbb{N}_0$.

Stwierdzenie 9.8. *Niech X i Y będą podzbiorami pierścienia P. Wówczas:*
(i) $[X] \subseteq [Y] \Leftrightarrow X \subseteq [Y]$,
(ii) $[X] = [Y] \Leftrightarrow (X \subseteq [Y] \text{ oraz } Y \subseteq [X])$.

Dowód. (i). Załóżmy, że $[X] \subseteq [Y]$. Ponieważ na mocy (1), $X \subseteq [X]$, więc stąd $X \subseteq [Y]$. Na odwrót, załóżmy, że $X \subseteq [Y]$. Wtedy $[Y]$ jest jakimś podpierścieniem, który zawiera podzbiór X, więc na mocy (2), $[X] \subseteq [Y]$.

(ii). Ponieważ $[X] = [Y] \Leftrightarrow ([X] \subseteq [Y] \text{ oraz } [Y] \subseteq [X])$, więc teza wynika od razu z punktu (i). □

2 Przykłady pierścieni i podpierścieni

Przykład 9.9. Każde ciało jest pierścieniem. Podpierścienie ciał są pierścieniami.

Przykład 9.10. Podpierścienie ciała $\mathbb{C}$ nazywamy *pierścieniami liczbowymi*. Oczywiście są one pierścieniami. Niech P będzie pierścieniem liczbowym i niech $k \in \mathbb{Z}$, $m \in \mathbb{N}$ będą liczbami względnie pierwszymi. Pokażemy, że wówczas:

$$\frac{k}{m} \in P \Leftrightarrow \frac{1}{m} \in P.$$

Rzeczywiście, załóżmy, że $\frac{1}{m} \in P$. Wtedy $\frac{k}{m} = k \cdot \frac{1}{m} \in P$, więc $\frac{k}{m} \in P$. Na odwrót, załóżmy, że $\frac{k}{m} \in P$. Ponieważ liczby k i m są względnie pierwsze, więc istnieją $x, y \in \mathbb{Z}$ takie, że $kx + my = 1$. Stąd $\frac{1}{m} = x \cdot \frac{k}{m} + y \cdot 1 \in P$, bo P jest podpierścieniem ciała $\mathbb{C}$ oraz $\frac{k}{m} \in P$ i $1 \in P$.
Przykłady pierścieni liczbowych:
a) Pierścień liczb całkowitych $\mathbb{Z}$.
b) Z Uwagi 9.7 wynika, że dla ustalonej liczby naturalnej $a > 1$

$$\left[\frac{1}{a}\right] = \left\{\frac{n}{a^k} : n, k \in \mathbb{Z}, k \geqslant 0\right\}$$

jest najmniejszym podpierścieniem w $\mathbb{Q}$ zawierającym $\frac{1}{a}$. Ponadto $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ dla pewnych różnych liczb pierwszych $p_1, p_2, \dots, p_s$ i pewnych $\alpha_1, \alpha_2, \dots, \alpha_s \in \mathbb{N}$. Zatem $n = p_1^{\alpha_1 - 1} \cdot \ldots \cdot p_s^{\alpha_s - 1} \in \mathbb{N}$. Ponadto $\frac{1}{p_1 \cdot \ldots \cdot p_s} = n \cdot \frac{1}{p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}} \in \left[\frac{1}{a}\right]$. Zatem ze Stwierdzenia 9.8, $\left[\frac{1}{p_1 \cdot \ldots \cdot p_s}\right] \subseteq \left[\frac{1}{a}\right]$. Niech α będzie największą z liczb $\alpha_1, \dots, \alpha_s \in \mathbb{N}$. Wtedy $\alpha - \alpha_i \in \mathbb{N}_0$ dla każdego $i = 1, \dots, s$, skąd $m = p_1^{\alpha - \alpha_1} \cdot \ldots \cdot p_s^{\alpha - \alpha_s} \in \mathbb{N}$ oraz $\frac{1}{a} = \frac{1}{p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}} = \frac{m}{(p_1 \cdot \ldots \cdot p_s)^{\alpha}}$. Zatem na mocy Stwierdzenia 9.8, $\left[\frac{1}{a}\right] \subseteq \left[\frac{1}{p_1 \cdot \ldots \cdot p_s}\right]$ i ostatecznie $\left[\frac{1}{a}\right] = \left[\frac{1}{p_1 \cdot \ldots \cdot p_s}\right]$. Zauważmy jeszcze, że dodatkowo zachodzi wzór:

$$\left[\frac{1}{p_1 \cdot \ldots \cdot p_s}\right] = \left[\frac{1}{p_1}, \frac{1}{p_2}, \dots, \frac{1}{p_s}\right]. \tag{4}$$

Rzeczywiście, $\frac{1}{p_1 \cdot \ldots \cdot p_s} = \frac{1}{p_1} \cdot \frac{1}{p_2} \cdot \ldots \cdot \frac{1}{p_s} \in \left[\frac{1}{p_1}, \frac{1}{p_2}, \dots, \frac{1}{p_s}\right]$, więc ze Stwierdzenia 9.8, $\left[\frac{1}{p_1 \cdot \ldots \cdot p_s}\right] \subseteq \left[\frac{1}{p_1}, \frac{1}{p_2}, \dots, \frac{1}{p_s}\right]$. Ponadto $m_i = \frac{p_1 p_2 \dots p_s}{p_i} \in \mathbb{N}$ dla każdego $i = 1, 2, \dots, s$ oraz $\frac{1}{p_i} = m_i \cdot \frac{1}{p_1 \cdot \ldots \cdot p_s} \in \left[\frac{1}{p_1 \cdot \ldots \cdot p_s}\right]$, więc na mocy Stwierdzenia 9.8, $\left[\frac{1}{p_1}, \frac{1}{p_2}, \dots, \frac{1}{p_s}\right] \subseteq \left[\frac{1}{p_1 \cdot \ldots \cdot p_s}\right]$, co kończy dowód wzoru (4). Z Uwagi 9.7 mamy ponadto wzór:

$$\left[\frac{1}{p_1}, \frac{1}{p_2}, \dots, \frac{1}{p_s}\right] = \left\{ \frac{n}{p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_s^{k_s}} \ : \ n \in \mathbb{Z}, k_1, k_2 \dots, k_s \in \mathbb{N}_0 \right\}. \tag{5}$$

c) Niech d będzie liczbą całkowitą, która nie jest kwadratem liczby całkowitej. Wówczas z teorii liczb wiadomo, że d nie jest kwadratem liczby wymiernej. Określamy $\sqrt{d}$ jako zwykły pierwiastek arytmetyczny z liczby d dla $d > 0$, zaś dla $d < 0$ określamy $\sqrt{d} = \sqrt{|d|} \cdot i$. Zatem w obu przypadkach $(\sqrt{d})^2 = d$. Wówczas na mocy Uwagi 9.7 $[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$ jest najmniejszym podpierścieniem ciała $\mathbb{C}$ zawierającym $\sqrt{d}$. Ten podpierścień będziemy dalej oznaczali przez $\mathbb{Z}[\sqrt{d}]$. Zatem

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}.$$

Z niewymierności liczby $\sqrt{d}$ wynika, że dla dowolnych $a_1, a_2, b_1, b_2 \in \mathbb{Q}$:

$$a_1 + b_1\sqrt{d} = a_2 + b_2\sqrt{d} \iff (a_1 = a_2 \ \text{ oraz } \ b_1 = b_2).$$

d) Niech d będzie liczbą całkowitą, która nie jest kwadratem liczby całkowitej taką, że $d \equiv 1 (\text{mod } 4)$. Ponieważ $\left(\frac{1+\sqrt{d}}{2}\right)^2 = \frac{1+\sqrt{d}}{2} + \frac{d-1}{4}$, więc na mocy Uwagi 9.7, $\left[\frac{1+\sqrt{d}}{2}\right] = \{x + y \cdot \frac{1+\sqrt{d}}{2} : x, y \in \mathbb{Z}\}$ jest najmniejszym podpierścieniem ciała $\mathbb{C}$ zawierającym $\frac{1+\sqrt{d}}{2}$. Ten podpierścień będziemy dalej oznaczali przez $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Zatem:

$$\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{ x + y \cdot \frac{1+\sqrt{d}}{2} : x, y \in \mathbb{Z} \right\}.$$

Z niewymierności liczby $\frac{1+\sqrt{d}}{2}$ wynika, że dla dowolnych $a_1, a_2, b_1, b_2 \in \mathbb{Q}$:

$$a_1 + b_1\frac{1+\sqrt{d}}{2} = a_2 + b_2\frac{1+\sqrt{d}}{2} \iff (a_1 = a_2 \text{ oraz } b_1 = b_2).$$

Przykład 9.11. Niech $m > 1$ będzie liczbą naturalną i niech $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$. Dla $a, b \in \mathbb{Z}_m$ określamy:

$a \oplus_m b$ = reszta z dzielenia $a + b$ przez m;

$a \odot_m b$ = reszta z dzielenia $a \cdot b$ przez m.

Wówczas na mocy Wykładu 1 $(\mathbb{Z}_m, \oplus_m, \odot_m, 0, 1)$ jest pierścieniem. Nazywamy go *pierścieniem reszt modulo m* i oznaczamy przez $\mathbb{Z}_m$.

Przykład 9.12. Zbiór wszystkich wielomianów o współczynnikach zespolonych (rzeczywistych, wymiernych, całkowitych) z dodawaniem i mnożeniem funkcji tworzy pierścień. Oznaczamy go odpowienio przez $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$ i $\mathbb{Z}[x]$.

Przykład 9.13. Niech $P_1, \ldots, P_n$ będą pierścieniami. W zbiorze $P_1 \times \ldots \times P_n$ określamy dodawanie i mnożenie następująco:

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n),$$
$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 \cdot b_1, \ldots, a_n \cdot b_n),$$

Ponadto określamy $0 = (0, \ldots, 0)$ oraz $1 = (1, \ldots, 1)$. Można sprawdzić, że wtedy $(P_1 \times \ldots \times P_n, +, \cdot, 0, 1)$ tworzy pierścień. Nazywamy go *iloczynem kartezjańskim pierścieni* $P_1, \ldots, P_n$.

Przykład 9.14. Dowolny zbiór jednoelementowy $P = \{a\}$ z działaniami + i $\cdot$ takimi, że $a + a = a$ i $a \cdot a = a$ oraz z wyróżnionymi elementami $0 = 1 = a$ tworzy pierścień. Nazywamy go *pierścieniem zerowym.* Zauważmy, że jeśli pierścień P jest niezerowy, to $|P| > 1$, więc istnieje niezerowe $a \in P$. Wtedy $a = a \cdot 1$ oraz $a \cdot 0 = 0 \neq a$, skąd wynika, że $0 \neq 1$ w P. Na odwrót, jeśli $0 \neq 1$ w pierścieniu P, to $|P| > 1$, więc pierścień P nie jest zerowy.

Przykład 9.15. Niech A i B będą podpierścieniami pierścienia P. Oznaczmy przez AB zbiór wszystkich skończonych sum elementów postaci $a \cdot b$, gdzie $a \in A$, $b \in B$. Wtedy $1 = 1 \cdot 1 \in AB$. Ponadto z określenia AB oraz z tego, że $-(a \cdot b) = (-a) \cdot b$ wynika od razu, że jeśli $x, y \in AB$, to $x - y \in AB$. Ponadto z rozdzielności mnożenia względem dodawania i z tego, że dla $a_1, a_2 \in A$, $b_1, b_2 \in B$ jest $(a_1 \cdot b_1) \cdot (a_2 \cdot b_2) = (a_1 \cdot a_2) \cdot (b_1 \cdot b_2) \in AB$ wynika, że dla dowolnych $x, y \in AB$, $x \cdot y \in AB$. Zatem na mocy Stwierdzenia 9.2 mamy, że AB jest podpierścieniem pierścienia P. Zauważmy jeszcze, że dla $a \in A$ i $b \in B$, $a = a \cdot 1 \in AB$ i $b = 1 \cdot b \in AB$, a więc $A \cup B \subseteq AB$. Jeśli S jest podpierścieniem pierścienia P takim, że $A \cup B \subseteq S$, to dla dowolnych $a \in A$ i $b \in B$ mamy $a, b \in S$, skąd $a \cdot b \in S$, a zatem $AB \subseteq S$. W takim razie $AB = [A \cup B]$, czyli AB jest najmniejszym w sensie inkluzji podpierścieniem pierścienia P zawierającym zbiór $A \cup B$.

3 Elementy odwracalne

Definicja 9.16. Powiemy, że $a \in P$ jest *elementem odwracalnym pierścienia* P, jeżeli istnieje $x \in P$ takie, że $a \cdot x = 1$. Zbiór wszystkich elementów odwracalnych pierścienia P oznaczamy przez P^*.

Przykład 9.17. Niech d będzie liczbą naturalną, która nie jest kwadratem liczby naturalnej. Z elementarnej teorii liczb wiemy, że istnieje wówczas nieskończenie wiele par $(x, y) \in \mathbb{N} \times \mathbb{N}$ takich, że $x^2 - dy^2 = 1$. Stąd w pierścieniu $\mathbb{Z}[\sqrt{d}]$: $(x+y\sqrt{d})(x-y\sqrt{d}) = 1$. Wobec tego $x + y\sqrt{d} \in (\mathbb{Z}[\sqrt{d}])^*$ i pierścień $\mathbb{Z}[\sqrt{d}]$ ma nieskończenie wiele elementów odwracalnych.

Przykład 9.18. Niech $p_1, p_2, \ldots, p_s$ będą różnymi liczbami pierwszymi. Pokażemy, że

$$\left[\frac{1}{p_1}, \frac{1}{p_2}, \ldots, \frac{1}{p_s}\right]^* = \{\pm p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s} \ : \ k_1, k_2, \ldots, k_s \in \mathbb{Z}\}.$$

Ze wzoru (5) wynika, że $\pm p_1^{l_1} p_2^{l_2} \ldots p_s^{l_s} \in \left[\frac{1}{p_1}, \frac{1}{p_2}, \ldots, \frac{1}{p_s}\right]$ dla dowolnych $l_1, l_2, \ldots, l_s \in \mathbb{Z}$. Weźmy dowolne $k_1, k_2, \ldots, k_s \in \mathbb{Z}$. Wtedy $(\pm p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}) \cdot (\pm p_1^{-k_1} p_2^{-k_2} \ldots p_s^{-k_s}) = 1$, skąd $\pm p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s} \in \left[\frac{1}{p_1}, \frac{1}{p_2}, \ldots, \frac{1}{p_s}\right]^*$. Niech teraz $a \in \left[\frac{1}{p_1}, \frac{1}{p_2}, \ldots, \frac{1}{p_s}\right]^*$. Wówczas $a \cdot b = 1$ dla pewnego $b \in \left[\frac{1}{p_1}, \frac{1}{p_2}, \ldots, \frac{1}{p_s}\right]$. Ponadto ze wzoru (5), $a = \frac{n_1}{p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}}$ i $b = \frac{n_2}{p_1^{l_1} p_2^{l_2} \ldots p_s^{l_s}}$ dla pewnych $n_1, n_2 \in \mathbb{Z}$ oraz dla pewnych $k_i, l_i \in \mathbb{N}_0$ dla $i = 1, 2, \ldots, s$. Zatem $n_1 n_2 = p_1^{k_1+l_1} p_2^{k_2+l_2} \ldots p_s^{k_s+l_s}$. Wobec tego $n_1 = \pm p_1^{t_1} p_2^{t_2} \ldots p_s^{t_s}$ dla pewnych $t_1, t_2, \ldots, t_s \in \mathbb{N}_0$, skąd $a = \pm p_1^{t_1-k_1} p_2^{t_2-k_2} \ldots p_s^{t_s-k_s}$, co kończy nasz dowód.

Twierdzenie 9.19. *Dla dowolnego pierścienia P system algebraiczny $(P^*, \cdot, 1)$ jest grupą abelową.*

Dowód. Ponieważ $1 \cdot 1 = 1$, więc $1 \in P^*$. Niech $a \in P^*$. Wtedy istnieje $x \in P$ takie, że $a \cdot x = 1$, skąd $x \cdot a = 1$, czyli $x \in P^*$. Dalej, dla $a, b \in P^*$ istnieją $x, y \in P$ takie, że $a \cdot x = 1$ i $b \cdot y = 1$, więc $(a \cdot b) \cdot (x \cdot y) = (a \cdot x) \cdot (b \cdot y) = 1 \cdot 1 = 1$, czyli $a \cdot b \in P^*$. Ponieważ mnożenie jest łączne w P, więc mnożenie jest łączne w P^*. Zatem z tych rozważań mamy, że $(P^*, \cdot, 1)$ jest grupą. Natomiast z **P5** wynika od razu, że grupa ta jest abelowa. □

Uwaga 9.20. Element odwrotny do elementu $a \in P^*$ oznaczamy przez a^{-1}. Z dowodu Twierdzenia 2 wynika, że dla dowolnych $a, b \in P^*$ mamy wzór:

$$(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}.$$

Stwierdzenie 9.21. *Niech $m > 1$ będzie liczbą naturalną. Wówczas zachodzi wzór:*

$$\mathbb{Z}_m^* = \{a \in \{1, 2, \ldots, m\} : (a, m) = 1\}.$$

W szczególności $|\mathbb{Z}_m^*| = \varphi(m)$.

Dowód. Weźmy dowolne $a \in \mathbb{Z}_m^*$. Wtedy $a \in \{0, 1, \ldots, m-1\}$ oraz istnieje $x \in \mathbb{Z}_m$ takie, że $a \odot_m x = 1$. Stąd $[a \cdot x]_m = 1$, a więc $a \cdot x \equiv 1 (mod\ m)$. Zatem z elementarnej teorii liczb, $(a, m)|1$, skąd $(a, m) = 1$. Ale $m > 1$, więc $(m, 0) = m > 1$, czyli $a \in \{1, 2, \ldots, m\}$.

Na odwrót, niech $a \in \{1, 2, \ldots, m\}$ i $(a, m) = 1$. Ponieważ $m > 1$, więc $(m, m) = m > 1$, skąd $a \in \{1, 2, \ldots, m-1\}$, czyli $a \in \mathbb{Z}_m$. Ponadto z elementarnej teorii liczb istnieje $y \in \mathbb{Z}$ takie, że $a \cdot y \equiv 1(mod; m)$, skąd $x = [y]_m \in \mathbb{Z}_m$ i $a \cdot x \equiv 1(mod; m)$. Zatem $a \odot_m x = [a \cdot x]_m = [1]_m = 1$, więc $a \in \mathbb{Z}_m^*$.

Stwierdzenie 9.22. *Niech $P_1, P_2, \ldots, P_n$ będą dowolnymi pierścieniami. Wówczas*:

$$(P_1 \times P_2 \times \ldots \times P_n)^* = P_1^* \times P_2^* \times \ldots \times P_n^*.$$

Dowód. Weźmy dowolne $x \in (P_1 \times P_2 \times \ldots \times P_n)^*$. Wtedy $x \in P_1 \times P_2 \times \ldots \times P_n$ i istnieje $y \in P_1 \times P_2 \times \ldots \times P_n$ takie, że $x \cdot y = (1, 1, \ldots, 1)$. Ale $x = (x_1, x_2, \ldots, x_n)$ i $y = (y_1, y_2, \ldots, y_n)$ dla pewnych $x_i, y_i \in P_i$, $i = 1, 2, \ldots, n$ oraz $x \cdot y = (x_1 \cdot y_1, x_2 \cdot y_2, \ldots, x_n \cdot y_n)$, więc $x_i \cdot y_i = 1$, skąd $x_i \in P_i^*$ dla $i = 1, 2, \ldots, n$. Zatem $x \in P_1^* \times P_2^* \times \ldots \times P_n^*$.

Na odwrót, weźmy dowolne $x \in P_1^* \times P_2^* \times \ldots \times P_n^*$. Wtedy istnieją $x_i \in P_i^*$, $i = 1, 2, \ldots, n$, takie, że $x = (x_1, x_2, \ldots, x_n)$. Stąd dla każdego $i = 1, 2, \ldots, n$ istnieje $y_i \in P_i$ takie, że $x_i \cdot y_i = 1$. Wobec tego $y = (y_1, y_2, \ldots, y_n) \in P_1 \times P_2 \times \ldots \times P_n$ i $x \cdot y = (x_1 \cdot y_1, x_2 \cdot y_2, \ldots, x_n \cdot y_n) = (1, 1, \ldots, 1)$. Zatem $x \in (P_1 \times P_2 \times \ldots \times P_n)^*$. □

4 Dzielniki zera

Definicja 9.23. Mówimy, że element a pierścienia P jest *dzielnikiem zera*, jeżeli istnieje niezerowy element $b \in P$ taki, że $a \cdot b = 0$. Elementy pierścienia P, które nie są dzielnikami zera nazywamy *elementami regularnymi*. Zbiór wszystkich dzielników zera pierścienia P będziemy oznaczali przez $D(P)$, zaś zbiór wszystkich elementów regularnych pierścienia P będziemy oznaczali symbolem $R(P)$.

Uwaga 9.24. Zauważmy, że w dowolnym pierścieniu P: $D(P) = P \setminus R(P)$. W każdym pierścieniu niezerowym P mamy, że $0 \neq 1$ oraz $0 \cdot 1 = 0$, więc 0 jest dzielnikiem zera w każdym pierścieniu niezerowym P. Dzielniki zera różne od 0 nazywamy *właściwymi dzielnikami zera*.

Przykład 9.25. Niech A i B będą niezerowymi pierścieniami. Wówczas pierścień $A \times B$ posiada właściwe dzielniki zera, którymi są $(1, 0)$ i $(0, 1)$, gdyż te elementy są różne od $(0, 0)$ i $(1, 0) \cdot (0, 1) = (1 \cdot 0, 0 \cdot 1) = (0, 0)$.

Przykład 9.26. Dla liczb złożonych m pierścień $\mathbb{Z}_m$ posiada właściwe dzielniki zera, gdyż istnieją liczby naturalne $a, b < m$ takie, że $a \cdot b = m$ i wtedy a, b są niezerowymi elementami pierścienia $\mathbb{Z}_m$ oraz $a \odot_m b = 0$.

Stwierdzenie 9.27. *Niech $P_1, P_2, \ldots, P_n$ będą dowolnymi pierścieniami. Wówczas:*

$$R(P_1 \times P_2 \times \ldots \times P_n) = R(P_1) \times R(P_2) \times \ldots \times R(P_n).$$

W szczególności:

$$D(P_1 \times P_2 \times \ldots \times P_n) = (P_1 \times P_2 \times \ldots \times P_n) \setminus [R(P_1) \times R(P_2) \times \ldots \times R(P_n)].$$

Dowód. Weźmy dowolne $x \in R(P_1 \times P_2 \times \ldots \times P_n)$. Wtedy $x = (x_1, x_2, \ldots, x_n)$ dla pewnych $x_i \in P_i$, $i = 1, 2, \ldots, n$. Ustalmy $i = 1, 2, \ldots, n$ i weźmy dowolne $a_i \in P_i$ takie, że $x_i \cdot a_i = 0$. Niech $a_j = 0$ dla wszystkich $j \in \{1, 2, \ldots, n\} \setminus \{i\}$ oraz $a = (a_1, a_2, \ldots, a_n)$. Wtedy $x \cdot a = (0, 0, \ldots, 0)$, więc z regularności x, $a = (0, 0, \ldots, 0)$, skąd $a_i = 0$. Oznacza to, że $x_i \in R(P_i)$ dla każdego $i = 1, 2, \ldots, n$. Zatem $R(P_1 \times P_2 \times \ldots \times P_n) \subseteq R(P_1) \times R(P_2) \times \ldots \times R(P_n)$.

Weźmy dowolne $x \in R(P_1) \times R(P_2) \times \ldots \times R(P_n)$. Wtedy istnieją $x_i \in R(P_i)$, $i = 1, 2, \ldots, n$, takie, że $x = (x_1, x_2, \ldots, x_n)$. Weźmy dowolne $a \in P_1 \times P_2 \times \ldots \times P_n$ takie, że $x \cdot a = (0, 0, \ldots, 0)$. Wtedy $a = (a_1, a_2, \ldots, a_n)$, więc $(0, 0, \ldots, 0) = (x_1 a_1, x_2 a_2, \ldots, x_n a_n)$, więc dla każdego $i = 1, 2, \ldots, n$: $x_i \cdot a_i = 0$, skąd na mocy regularności elementu x_i, $a_i = 0$. Wobec tego $a = (0, 0, \ldots, 0)$ i element x jest regularny. Zatem $R(P_1) \times R(P_2) \times \ldots \times R(P_n) \subseteq R(P_1 \times P_2 \times \ldots \times P_n)$. □

Twierdzenie 9.28. *W dowolnym pierścieniu P:*
(i) iloczyn elementów regularnych jest elementem regularnym;
(ii) jeśli $a \in P$ jest regularny i $a \cdot x = a \cdot y$, to $x = y$;
(iii) każdy element odwracalny jest elementem regularnym.

Dowód. (i). Niech $a, b \in P$ będą elementami regularnymi. Weźmy dowolny $x \in P$ taki, że $(ab)x = 0$. Wtedy $a(bx) = 0$, więc z regularności a, $bx = 0$, skąd $x = 0$, z regularności b. Zatem ab jest elementem regularnym.

(ii). Niech $a \in P$ będzie elementem regularnym i niech $x, y \in P$ będą takie, że $ax = ay$. Wtedy $a(x - y) = 0$, skąd z regularności a mamy, że $x - y = 0$, czyli $x = y$.

(iii). Załóżmy, że tak nie jest. Wtedy istnieje element odwracalny $a \in P$, który jest dzielnikiem zera. Zatem istnieje niezerowe $b \in P$ takie, że $a \cdot b = 0$ oraz istnieje $x \in P$ takie, że $a \cdot x = 1$. Wobec tego $b = b \cdot 1 = b \cdot (a \cdot x) = (b \cdot a) \cdot x = (a \cdot b) \cdot x = 0 \cdot x = 0$ i mamy sprzeczność. □

Wniosek 9.29. *Dowolne ciało nie posiada właściwych dzielników zera.* □

Definicja 9.30. Niezerowy pierścień P, który nie posiada właściwych dzielników zera nazywamy *dziedziną całkowitości*.

Wobec tego, dziedziny całkowitości są to takie niezerowe pierścienie, w których każdy element niezerowy jest regularny. W szczególności na mocy Wniosku 9.29, każde ciało

jest dziedziną całkowitości, a nawet każdy podpierścień ciała jest dziedziną całkowitości. Z Twierdzenia 9.28 mamy natychmiast następujący

Wniosek 9.31. *Jeżeli a jest niezerowym elementem dziedziny całkowitości P oraz $x, y \in P$ są takie, że $ax = ay$, to $x = y$.* $\square$

Zagadka 1. Udowodnij, że dla dowolnych pierścieni A i B:

$$D(A \times B) = [A \times D(B)] \cup [D(A) \times R(B)].$$

Zagadka 2. Wyznacz $(\mathbb{Q} \times \mathbb{Z})^*$, $D(\mathbb{Q} \times \mathbb{Z})$ i $R(\mathbb{Q} \times \mathbb{Z})$.

Zagadka 3. Czy suma dwóch dzielników zera pierścienia P może być elementem odwracalnym w P?

Zagadka 4. Czy i należy do podpierścienia $\left[\frac{3}{4}i\right]$ ciała $\mathbb{C}$?

Zagadka 5. Niech $k_i \in \mathbb{Z}, m_i \in \mathbb{N}, m_i > 1$ oraz $NWD(k_i, m_i) = 1$ dla każdego $i = 1, 2, \ldots, s$. Udowodnij, że w ciele $\mathbb{Q}$ zachodzi wzór:

$$\left[\frac{k_1}{m_1}, \frac{k_2}{m_2}, \ldots, \frac{k_s}{m_s}\right] = \left[\frac{1}{m_1 \cdot m_2 \cdot \ldots \cdot m_s}\right].$$

Zagadka 6. Niech A będzie podpierścieniem pierścienia P i $a \in A$. Czy jest prawdą, że

(a) jeśli $a \in P^*$, to $a \in A^*$?
(b) jeśli $a \in A^*$, to $a \in P^*$?
(c) jeśli a jest dzielnikiem zera w P, to a jest dzielnikiem zera w A?
(d) jeśli a jest dzielnikiem zera w A, to a jest dzielnikiem zera w P?

Zagadka 7. Niech P będzie pierścieniem skończonym. Udowodnij, że $R(P) = P^*$. Uzasadnij też, że skończona dziedzina całkowitości jest ciałem.