

7. WYKŁAD 7: PODSTAWOWE POJĘCIA TEORII PODZIELNOŚCI. PIERŚCIEŃ Z JEDNOZNACZNYM ROZKŁADEM.

7.1. Podstawowe pojęcia teorii podzielności.

Definicja 7.1. Niech $(R, +, \cdot)$ będzie pierścieniem¹⁶ całkowitym. Mówimy, że element a **dzieli** b , $a, b \in R$, (lub że a **jest dzielnikiem** b , lub że b **jest wielokrotnością** a) jeżeli istnieje element $c \in R$ taki, że $ac = b$. Oznaczamy $a|b$.

Przykłady:

- (1) W pierścieniu $\mathbb{Z}$ zachodzi $2|10$ oraz $3 \nmid 5$.
- (2) W pierścieniu $\mathbb{R}[x]$ zachodzi $x - 1|x^2 - 1$.
- (3) W pierścieniu $\mathbb{Z}[i]$ zachodzi $2 + i|5$.

Uwaga 7.1. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym. Wówczas:

- (1) $1|a$ dla $a \in R$,
- (2) $a|0$ dla $a \in R \setminus \{0\}$,
- (3) $a|a$ dla $a \in R \setminus \{0\}$,
- (4) $a|b \wedge b|c \Rightarrow a|c$ dla $a, b \in R \setminus \{0\}$, $c \in R$,
- (5) $u|a$ dla $u \in U(R)$, $a \in R$,
- (6) jeżeli dla $a \in R \setminus \{0\}$, $u \in U(R)$ zachodzi $a|u$, to $a \in U(R)$,
- (7) $a|b_1, \dots, a|b_n \Rightarrow a|x_1b_1 + \dots + x_nb_n$ dla $a, b_1, \dots, b_n, x_1, \dots, x_n \in R \setminus \{0\}$,
- (8) $a|b \wedge c|d \Rightarrow ac|bd$ dla $a, b, c, d \in R \setminus \{0\}$,
- (9) $a|b \Rightarrow a|bc$ dla $a, b, c \in R \setminus \{0\}$,
- (10) $ac|bc \Rightarrow a|b$ dla $a, b, c \in R \setminus \{0\}$.

Proste dowody powyższych własności pozostawiamy jako ćwiczenie.

Definicja 7.2. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym. Mówimy, że elementy $a, b \in R$ są **stowarzyszone**, gdy $a|b$ oraz $b|a$. Oznaczamy $a \sim b$.

Przykłady:

- (4) W pierścieniu $\mathbb{Z}$ zachodzi $2 \sim -2$.
- (5) W pierścieniu $\mathbb{R}[x]$ zachodzi $2x^2 + 2 \sim x^2 + 1$.
- (6) W pierścieniu $\mathbb{Z}[i]$ zachodzi $1 \sim -i$.

Uwaga 7.2. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym, niech $a, b \in R$. Wówczas

$a \sim b$ wtedy i tylko wtedy, gdy istnieje $u \in U(R)$ takie, że $a = bu$.

Dowód. $(\Rightarrow)$: Załóżmy, że $a|b$ i $b|a$. Zatem istnieją c, d takie, że $ac = b$ i $bd = a$. Wobec tego $bdc = ac = b$, więc $dc = 1$,¹⁷ a zatem $d \in U(R)$.

$(\Leftarrow)$: Załóżmy, że $a = bu$ oraz $u \in U(R)$. W szczególności $b|a$. Ponadto $au^{-1} = b$, więc $a|b$. □

Przykłady:

- (7) W pierścieniu $\mathbb{Z}$ mamy $U(\mathbb{Z}) = \{\pm 1\}$. Zatem $a \sim b$ wtedy i tylko wtedy, gdy $a = \pm b$.
- (8) W pierścieniu $F[x]$, gdzie F jest dowolnym ciałem, mamy $U(F[x]) = F^*$. Zatem $f \sim g$ wtedy i tylko wtedy, gdy $f = ag$, dla pewnego elementu $a \in F^*$.

¹⁶Od teraz “pierścień” będzie zawsze oznaczał “pierścień przemienny z jedyneką”.

¹⁷Korzystamy tu z faktu, że w pierścieniu całkowitym zachodzi prawo skracania.

- (9) W pierścieniu $\mathbb{Z}[i]$ mamy $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$. Zatem $a \sim b$ wtedy i tylko wtedy, gdy $a = \pm b$ lub $a = \pm ib$.

Uwaga 7.3. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym. Wówczas relacja $\sim$ jest relacją równoważności w zbiorze $R \setminus \{0\}$.

Definicja 7.3. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym.

- (1) Element nieodwracalny i niezerowy $a \in R$ nazywamy **nierozkładalnym**, jeżeli dla wszelkich $b, c \in R$ jeśli $a = bc$, to $b \in U(R)$ lub $c \in U(R)$.
- (2) Element nieodwracalny i niezerowy $a \in R$ nazywamy **rozkładalnym**, jeżeli istnieją niezerowe i nieodwracalne elementy $b, c \in R$ takie, że $a = bc$.

Przykłady:

- (10) Rozważmy pierścień $\mathbb{Z}$. Wówczas a jest nierozkładalny wtedy i tylko wtedy, gdy a lub $-a$ jest liczbą pierwszą.
- (11) Rozważmy $F[x]$, gdzie F jest dowolnym ciałem.
 - Jeżeli $\deg f = 1$, to f jest nierozkładalny.

Dowód. Załóżmy, że $f = gh$. Wówczas $1 = \deg f = \deg g + \deg h$, zatem $\deg g = 0$ lub $\deg h = 0$, więc $g \in U(F[x])$ lub $h \in U(F[x])$. $\square$

 - Jeżeli $\deg f = 2$ lub $\deg f = 3$ i f nie ma pierwiastków w ciele F , to f jest nierozkładalny.

Dowód. Załóżmy, że $f = gh$ dla $g, h \notin U(F[x])$. W szczególności $\deg g, \deg h \neq 0$. Wówczas $\{2, 3\} \ni \deg f = \deg g + \deg h$, a zatem $\deg g = 1$ lub $\deg h = 1$, więc g lub h ma pierwiastek w F , co daje sprzeczność. $\square$
- (12) Rozważmy $\mathbb{Z}[x]$. Wówczas $2x + 2$ jest rozkładalny, bo $2x + 2 = 2(x + 1)$, $2 \notin U(\mathbb{Z}[x])$, $x + 1 \notin U(\mathbb{Z}[x])$, ale $\deg(2x + 2) = 1$.
- (13) Rozważmy $\mathbb{Z}[i]$. Wówczas 3 jest nierozkładalny, ale 5 jest rozkładalny.

Definicja 7.4. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym. Element nieodwracalny i niezerowy $a \in R$ nazywamy **pierwszym**, jeżeli dla wszelkich $b, c \in R$ jeżeli $a|bc$, to $a|b$ lub $a|c$.

Przykłady:

- (14) Rozważmy pierścień $\mathbb{Z}$. Wówczas a jest pierwszy wtedy i tylko wtedy, gdy a lub $-a$ jest liczbą pierwszą.
- (15) Rozważmy $F[x]$, gdzie F jest dowolnym ciałem. Wówczas x jest elementem pierwszym.

Dowód. Załóżmy, że $x|fg$, dla pewnych $f, g \in F[x]$. Wówczas $x \cdot h = fg$, dla pewnego $h \in F[x]$. W szczególności $fg(0) = 0$, więc $f(0) = 0$ lub $g(0) = 0$. Wobec twierdzenia Bezout $x|f$ lub $x|g$. $\square$

Uwaga 7.4. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym, niech $a \in R$. Jeśli a jest pierwszy, to jest nierozkładalny.

Dowód. Załóżmy, że $a = bc$. Wówczas $a|bc$, a więc $a|b$ lub $a|c$. Jeśli $a|b$, to dla pewnego $d \in R$ zachodzi $ad = b$. Zatem $b = bcd$, czyli $cd = 1$, a więc $c \in U(R)$. Jeśli $a|c$ to, podobnie, $b \in U(R)$. $\square$

Przykład:

- (16) Rozważmy $\mathbb{Z}[\sqrt{-5}]$. Wówczas 3 jest nierozkładalny, ale nie pierwszy.

Uwaga 7.5. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym, niech $a \sim b$. Wówczas:

- (1) a jest nierozkładalny wtedy i tylko wtedy, gdy b jest nierozkładalny,
- (2) a jest pierwszy wtedy i tylko wtedy, gdy b jest pierwszy,
- (3) $a|c$ wtedy i tylko wtedy, gdy $b|c$,
- (4) $c|a$ wtedy i tylko wtedy, gdy $c|b$.

Proste dowody powyższych własności pozostawiamy jako ćwiczenie.

Definicja 7.5. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym, niech $a_1, \dots, a_n, d \in R$. Element d nazywamy **największym wspólnym dzielnikiem** elementów $a_1, \dots, a_n$, gdy

- (1) $d|a_1, \dots, d|a_n$,
- (2) jeśli, dla dowolnego $c \in R$, $c|a_1, \dots, c|a_n$, to wówczas $c|d$.

Oznaczamy $d \sim NWD(a_1, \dots, a_n)$.

Uwaga 7.6. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym, niech $a_1, \dots, a_n, d_1, d_2 \in R$. Niech $d_1 \sim NWD(a_1, \dots, a_n)$ oraz $d_2 \sim NWD(a_1, \dots, a_n)$. Wówczas $d_1 \sim d_2$.

Dowód. Wobec definicji $d_1|a_1, \dots, d_1|a_n$ i $d_2|a_1, \dots, d_2|a_n$, więc $d_1|d_2$ oraz $d_2|d_1$. □

Przykłady:

- (17) Rozważmy $\mathbb{Z}$. Wówczas $4 \sim NWD(8, 12)$.
- (18) Rozważmy $\mathbb{Z}[\sqrt{-6}]$. Wówczas nie istnieje największy wspólny dzielnik elementów 6 oraz $2\sqrt{-6}$.

Uwaga 7.7. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym. Załóżmy, że we wszystkich poprzednikach poniższych implikacji istnieją stosowne największe wspólne dzielniki. Wówczas istnieją też największe wspólne dzielniki w następnikach implikacji i ponadto:

- (1) jeśli $d \sim NWD(a_1, \dots, a_n)$ i $a_1 = da'_1, \dots, a_n = da'_n$, to $1 \sim NWD(a'_1, \dots, a'_n)$;
- (2) jeśli $a|a_1, \dots, a|a_n$, to $a \sim NWD(a, a_1, \dots, a_n)$;
- (3) jeśli a jest nierozkładalny, to

$$NWD(a, a_1, \dots, a_n) \sim \begin{cases} 1, & \text{gdy } a \nmid a_i \text{ dla pewnego } i \in \{1, \dots, n\}, \\ a, & \text{gdy } a \mid a_i \text{ dla wszelkich } i \in \{1, \dots, n\}; \end{cases}$$

- (4) $NWD(ca_1, \dots, ca_n) \sim cNWD(a_1, \dots, a_n)$;
- (5) jeśli $1 \sim NWD(a, a_i)$, dla $i \in \{1, \dots, n\}$, to $1 \sim NWD(a, a_1, \dots, a_n)$;
- (6) $NWD(a_1, \dots, a_n) \sim NWD(NWD(a_1, \dots, a_{n-1}), a_n)$;
- (7) jeśli $1 \sim NWD(a, b)$ to $1 \sim NWD(a^k, b^l)$, dla $k, l \in \mathbb{N}$;
- (8) jeśli $1 \sim NWD(a, b)$ i $a|bc$, to $a|c$;
- (9) jeśli $1 \sim NWD(a, b)$ i $a|b^k c$, to $a|c$;
- (10) $NWD(a, b) \sim NWD(a, b \pm ac)$;
- (11) jeśli $d_1 \sim NWD(a, b)$ i $d_2 \sim NWD(a, b, c)$, to $d_2 \sim NWD(d_1, c)$;
- (12) jeśli $d_1 \sim NWD(a, b)$, $d_2 \sim NWD(a, b, c)$ i $d_3 \sim NWD(b, c)$, to $d_3 \sim NWD(d_1, d_2)$.

Proste dowody powyższych własności pozostawiamy jako ćwiczenie.

Definicja 7.6. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym, niech $a_1, \dots, a_n, w \in R$. Element w nazywamy **najmniejszą wspólną wielokrotnością** elementów $a_1, \dots, a_n$, gdy

- (1) $a_1|w, \dots, a_n|w$,
- (2) jeśli, dla dowolnego $c \in R$, $a_1|w, \dots, a_n|w$, to wówczas $w|c$.

Oznaczamy $d \sim NWW(a_1, \dots, a_n)$.

Uwaga 7.8. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym, niech $a_1, \dots, a_n, d_1, d_2 \in R$. Niech $w_1 \sim NWW(a_1, \dots, a_n)$ oraz $w_2 \sim NWW(a_1, \dots, a_n)$. Wówczas $w_1 \sim w_2$.

Przykłady:

(19) Rozważmy $\mathbb{Z}$. Wówczas $24 \sim NWW(6, 8)$.

(20) Rozważmy $\mathbb{Z}[\sqrt{-3}]$. Wówczas nie istnieje najmniejsza wspólna wielokrotność elementów 2 i $1 + \sqrt{-3}$, ale $1 \sim NWD(2, 1 + \sqrt{-3})$.

Uwaga 7.9. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym, niech $a, b \in R$. Jeśli istnieje $NWW(a, b)$, to istnieje $NWD(a, b)$ oraz

$$ab \sim NWD(a, b)NWW(a, b).$$

Dowód. Niech $w \sim NWW(a, b)$. Wówczas $a|ab$ oraz $b|ab$, istnieje zatem $d \in R$ takie, że $dw = ab$. Pokażemy, że $d \sim NWD(a, b)$.

Pokażemy, że $d|a$ i $d|b$. Istotnie, niech a' i b' będą takimi elementami, że $w = aa'$ oraz $w = bb'$. Wówczas $ab = dw = daa'$ oraz $ab = dbb'$, a więc $b = da'$ oraz $a = db'$, czyli $d|b$ oraz $d|a$.

Ustalmy $d' \in R$ i załóżmy, że $d'|a$ oraz $d'|b$. Pozostaje pokazać, że $d'|d$. Istotnie, niech a'' i b'' będą takimi elementami, że $a = a''d'$ oraz $b = b''d'$. Wówczas $a|a''b''d'$ oraz $b|a''b''d'$ i skoro $w \sim NWW(a, b)$, to $w|a''b''d'$. Zatem $ab = wd|a''b''d'd$ i skoro $ab = a''d'b''d'$, więc $d'|d$. $\square$

Uwaga 7.10. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym. Załóżmy, że we wszystkich poprzednikach poniższych implikacji istnieją stosowne największe wspólne dzielniki i najmniejsze wspólne wielokrotności. Wówczas istnieją też największe wspólne dzielniki i najmniejsze wspólne wielokrotności w następnikach implikacji i ponadto:

- (1) $a|b$ wtedy i tylko wtedy, gdy $a \sim NWD(a, b)$ wtedy i tylko wtedy, gdy $b \sim NWW(a, b)$;
- (2) $NWW(a_1, \dots, a_n) \sim NWW(NWW(a_1, \dots, a_{n-1}), a_n)$;
- (3) $NWD(a, NWW(b, c)) \sim NWD(NWD(a, b), NWD(a, c))$;
- (4) $NWW(a, NWD(b, c)) \sim NWD(NWW(a, b), NWW(a, c))$;
- (5) $NWD(a + b, NWW(a, b)) \sim NWD(a, b)$.

Proste dowody powyższych własności pozostawiamy jako ćwiczenie.

Uwaga 7.11. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym, niech $a, b, c \in R \setminus \{0\}$. Wówczas:

- (1) $a|b$ wtedy i tylko wtedy, gdy $(a) \supset (b)$;
- (2) $a \sim b$ wtedy i tylko wtedy, gdy $(a) = (b)$;
- (3) $a \in U(R)$ wtedy i tylko wtedy, gdy $(a) = R$;
- (4) a jest elementem pierwszym wtedy i tylko wtedy, gdy (a) jest ideałem pierwszym;
- (5) a jest elementem nierozkładalnym wtedy i tylko wtedy, gdy (a) jest elementem maksymalnym w rodzinie ideałów głównych pierścienia R ;
- (6) a jest elementem rozkładalnym wtedy i tylko wtedy, gdy (a) nie jest elementem maksymalnym w rodzinie ideałów głównych pierścienia R .

Dowód. (1) $(\Rightarrow)$: Załóżmy, że $a|b$. Wówczas $ac = b$ dla pewnego $c \in R$, więc $b \in (a)$, więc $(b) \subset (a)$.

$(\Leftarrow)$: Załóżmy, że $(a) \supset (b)$. Wówczas $b \in (a)$, czyli $b = ac$ dla pewnego $c \in R$, czyli $a|b$.

(2) Wynika wprost z (1).

(3) Oczywiste.

(4) $(\Rightarrow)$: Załóżmy, że a jest elementem pierwszym. Niech $xy \in (a)$. Wówczas $xy = as$, dla pewnego $s \in R$, więc $a|xy$, a zatem $a|x$ lub $a|y$. Wobec tego $aa_1 = x$ lub $aa_2 = y$, dla pewnych $a_1, a_2 \in R$, czyli $x \in (a)$ lub $y \in (a)$.

($\Leftarrow$) : Załóżmy, że (a) jest ideałem pierwszym. Niech $a|xy$. Wówczas $xy = as$, dla pewnego $s \in R$, więc $xy \in (a)$, a zatem $x \in (a)$ lub $y \in (a)$. Wobec tego $aa_1 = x$ lub $aa_2 = y$, dla pewnych $a_1, a_2 \in R$, czyli $a|x$ lub $a|y$.

- (5) ($\Rightarrow$) : Załóżmy, że a jest nierozkładalny. Niech $(a) \subset (c) \subset R$, dla pewnego $c \in R$. Wówczas $c|a$, czyli $cx = a$, dla pewnego $x \in R$. Wobec tego $c \in U(R)$ lub $x \in U(R)$. Zatem $(c) = R$ lub $a \sim c$ i tym samym $(a) = (c)$.

($\Leftarrow$) : Załóżmy, że (a) jest elementem maksymalnym w rodzinie ideałów głównych pierścienia R . Przypuśćmy, że $a = bc$ dla $b, c \notin U(R)$. Wówczas $a \approx b$ oraz $a \approx c$ i tym samym $(a) \subsetneq (c) \subsetneq R$, co jest sprzecznością.

- (6) Wynika wprost z (5).

□

7.2. Pierścienie z jednoznacznym rozkładem.

Definicja 7.7. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym.

- (1) Pierścień R nazywamy **pierścieniem z rozkładem** gdy każdy niezerowy i nieodwracalny element tego pierścienia można przedstawić w postaci iloczynu elementów nierozkładalnych.
- (2) Pierścień R nazywamy **pierścieniem z jednoznacznym rozkładem** (lub **pierścieniem gausowskim**, lub **UFD**¹⁸) gdy każdy niezerowy i nieodwracalny element tego pierścienia można przedstawić w postaci iloczynu elementów nierozkładalnych w sposób jednoznaczny z dokładnością do stowarzyszenia.

Przykłady:

- (1) Zdefiniujmy

$$\omega_d = \begin{cases} \frac{1+\sqrt{d}}{2}, & \text{gdy } d \equiv 1 \pmod{4}, \\ \sqrt{d}, & \text{w przeciwnym przypadku} \end{cases}$$

i rozważmy pierścień $\mathbb{Z}[\omega_d]$.

Twierdzenie. Jeżeli $d < 0$, to $\mathbb{Z}[\omega_d]$ jest pierścieniem z jednoznacznym rozkładem wtedy i tylko wtedy, gdy $d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$.

Uwaga. Jeżeli $d > 0$, to wśród $d \in \{1, \dots, 100\}$ jest 38 takich, że $\mathbb{Z}[\omega_d]$ jest pierścieniem z jednoznacznym rozkładem. Ogólnie nie wiadomo, czy pierścieni $\mathbb{Z}[\omega_d]$ o tej własności jest nieskończenie wiele.

- (2) Rozważmy $\mathbb{Z}[\sqrt{-5}]$. Istotnie, $\mathbb{Z}[\sqrt{-5}]$ nie jest pierścieniem z jednoznacznym rozkładem, albowiem $3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$.

Uwaga 7.12. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym z jednoznacznym rozkładem. Niech $a \in R$ i niech $a = p_{1_1} \cdot \dots \cdot p_{1_{k_1}} p_{2_1} \cdot \dots \cdot p_{2_{k_2}} p_{n_1} \cdot \dots \cdot p_{n_{k_n}}$ będzie rozkładem elementu a na iloczyn elementów nierozkładalnych, przy czym $p_{i_{s_i}} \sim p_{i_{t_i}}$, $i \in \{1, \dots, n\}$, $s, t \in \{1, \dots, k\}$ oraz $p_{i_{s_i}} \approx p_{j_{t_j}}$ dla $i \neq j$, $s, t \in \{1, \dots, k\}$. Wówczas

$$a = up_{1_1}^{k_1} \cdot \dots \cdot p_{n_1}^{k_n}, u \in U(R).$$

Ponadto, jeżeli $a = up_1^{k_1} \cdot \dots \cdot p_n^{k_n} = vp_1^{l_1} \cdot \dots \cdot p_n^{l_n}$ są dwoma rozkładami takiej postaci oraz $p_1, \dots, p_n$ są parami niestowarzyszone, to

$$k_1 = l_1, \dots, k_n = l_n.$$

¹⁸Unique factorization domain.

Tak więc jeżeli oznaczymy przez $\mathbb{P}(R)$ zbiór reprezentantów klas abstrakcji względem relacji stowarzyszenia wyznaczonych przez elementy nierozkładalne, to każdy element a ma jednoznaczne przedstawienie postaci

$$a = up_1^{k_1} \cdot \dots \cdot p_n^{k_n},$$

gdzie $u \in U(R)$, $p_1, \dots, p_n \in \mathbb{P}(R)$ są parami różne, $k_1, \dots, k_n \in \mathbb{N}$, $n \in \mathbb{N}$. Przedstawienie takie nazywamy **rozkładem kanonicznym**.

Dowód. Niech $p_{1_1}, \dots, p_{1_{k_1}}$ będą elementami nierozkładalnymi, $p_{1_{s_1}} \sim p_{1_{t_1}}$, $s, t \in \{1, \dots, k\}$. Pokażemy, że $p_{1_1} \cdot \dots \cdot p_{1_{k_1}} = up_{1_1}^{k_1}$ dla pewnego $u \in U(R)$. Istotnie, ponieważ $p_{1_1} \sim p_{1_{s_1}}$ dla $s \in \{2, \dots, k\}$, więc istnieją $u_2, \dots, u_{k_1} \in U(R)$ takie, że $p_{1_1} = u_s p_{1_{s_1}}$, $s \in \{2, \dots, k\}$. Zatem:

$$p_{1_1} \cdot \dots \cdot p_{1_{k_1}} = p_{1_1} u_2 p_{1_2} \cdot \dots \cdot u_{k_1} p_{1_{k_1}} = up_{1_1}^{k_1}.$$

Niech $up_1^{k_1} \cdot \dots \cdot p_n^{k_n} = vp_1^{l_1} \cdot \dots \cdot p_n^{l_n}$ dla $p_i \approx p_j$, $i \neq j$. Pokażemy, że $k_1 = l_1, \dots, k_n = l_n$. Istotnie, przypuśćmy, że $k_1 > l_1$. Wówczas $up_1^{k_1-l_1} \cdot \dots \cdot p_n^{k_n} = vp_2^{l_2} \cdot \dots \cdot p_n^{l_n}$ oraz $k_1 - l_1 > 0$. Wobec jednoznaczności rozkładu $p_1 \sim p_{i_0}$, dla $i_0 \in \{2, \dots, n\}$, co jest sprzeczne z przyjętymi założeniami. $\square$

Uwaga 7.13. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym z jednoznacznym rozkładem. Niech $a, b \in R \setminus \{0\}$ i niech $a = up_1^{k_1} \cdot \dots \cdot p_n^{k_n}$, gdzie $u \in U(R)$, $p_1, \dots, p_n \in \mathbb{P}(R)$ są parami różne, będzie rozkładem kanonicznym. Wówczas $b|a$ wtedy i tylko wtedy, gdy $b = vp_1^{l_1} \cdot \dots \cdot p_n^{l_n}$, gdzie $v \in U(R)$ oraz $l_i \leq k_i$, $i \in \{1, \dots, n\}$.

Dowód. $(\Leftarrow)$: Oczywiście. $(\Rightarrow)$: Załóżmy, że $a = bc$, dla pewnego $c \in R$. Wówczas $up_1^{k_1} \cdot \dots \cdot p_n^{k_n} = bc$ i wobec jednoznaczności rozkładu, w rozkładzie b i c występują elementy nierozkładalne stowarzyszone z $p_1, \dots, p_k$. Niech więc $b = vp_1^{l_1} \cdot \dots \cdot p_n^{l_n}$, $c = v'p_1^{m_1} \cdot \dots \cdot p_n^{m_n}$. Zatem $k_i = l_i + m_i \geq l_i$, $i \in \{1, \dots, k\}$. $\square$

Twierdzenie 7.1. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym z rozkładem. Następujące warunki są równoważne:

- (1) R jest pierścieniem z jednoznacznym rozkładem;
- (2) każdy element nierozkładalny w R jest pierwszy;
- (3) dla każdych dwóch elementów niezerowych istnieje ich największy wspólny dzielnik.

Dowód. (1) $\Rightarrow$ (3) : Załóżmy, że R jest pierścieniem z jednoznacznym rozkładem. Niech $a = up_1^{k_1} \cdot \dots \cdot p_n^{k_n}$, $b = vp_1^{l_1} \cdot \dots \cdot p_n^{l_n}$ (dopuszczamy $k_i, l_i = 0$). Niech $m_i = \min\{k_i, l_i\}$ i niech $d = p_1^{m_1} \cdot \dots \cdot p_n^{m_n}$.

Pokażemy, że $d \sim NWD(a, b)$. Oczywiście $d|a$ i $d|b$. Niech $c|a$ i $c|b$. Wobec Uwagi 7.13 $c = wp_1^{s_1} \cdot \dots \cdot p_n^{s_n}$, gdzie $w \in U(R)$, $s_i \leq k_i$, $s_i \leq l_i$, $i \in \{1, \dots, n\}$. Zatem $s_i \leq m_i = \min\{k_i, l_i\}$, $i \in \{1, \dots, n\}$, więc $c|d$.

(3) $\Rightarrow$ (2) : Załóżmy, że dla każdych dwóch elementów niezerowych istnieje ich NWD. Niech p będzie elementem nierozkładalnym. Niech $p|ab$.

Pokażemy, że $p|a$ lub $p|b$. Istotnie, przypuśćmy, że $p \nmid a$ i $p \nmid b$. Wówczas $1 \sim NWD(p, a)$ i $1 \sim NWD(p, b)$. Zatem $1 \sim NWD(p, ab)$, co jest sprzecznością, bo $p|ab$ i p jest nierozkładalny.

(2) $\Rightarrow$ (1) : Załóżmy, że każdy element nierozkładalny w R jest pierwszy. Niech $p_1 \cdot \dots \cdot p_n = q_1 \cdot \dots \cdot q_m$, gdzie $n, m \in \mathbb{N}$ oraz $p_1, \dots, p_n, q_1, \dots, q_m$ są nierozkładalne. Pokażemy, że $n = m$ oraz, po ewentualnej zmianie numeracji, $p_1 \sim q_1, \dots, p_n \sim q_n$. Dowód przeprowadzimy indukcyjnie względem n .

Jeśli $n = 1$, to $p_1 = q_1 \cdot \dots \cdot q_m$. Skoro $p_1, q_1, \dots, q_m$ są nierozkładalne, to $m = 1$ i $p_1 = q_1$, więc $p_1 \sim q_1$.

Jeśli $n > 1$, to założmy prawdziwość twierdzenia dla $k < n$. Ponieważ $p_1 \cdot \dots \cdot p_n = q_1 \cdot \dots \cdot q_m$, więc $p_1|q_1 \cdot \dots \cdot q_m$. Ponieważ p_1 jest nierozkładalny, więc p_1 jest pierwszy. Zatem dla pewnego $i_0 \in \{1, \dots, m\}$

zachodzi $p_1 | q_{i_0}$, przy czym możemy założyć, że $i_0 = 1$ i tym samym $p_1 | q_1$. Ponieważ q_1 jest nierozkładalny, więc $p_1 \sim q_1$. Zatem $q_1 = up_1$, dla pewnego $u \in U(R)$. Mamy więc

$$p_1 \cdot \dots \cdot p_n = up_1 q_2 \cdot \dots \cdot q_m,$$

a stąd

$$p_2 \cdot \dots \cdot p_n = u q_2 \cdot \dots \cdot q_m.$$

Oczywiście $u q_2$ jest nierozkładalny. Zatem wobec założenia indukcyjnego $n - 1 = m - 1$ oraz $p_2 \sim u q_2 \sim q_2, \dots, p_n \sim q_n$. $\square$

Definicja 7.8. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym z jednoznacznym rozkładem. Niech $p \in \mathbb{P}(R)$. Funkcję $v_p : R \rightarrow \mathbb{Z} \cup \{\infty\}$ zdefiniowaną wzorem

$$v_p(a) = \begin{cases} k_i, & \text{jeśli } p = p_i, \\ 0, & \text{jeśli } p \notin \{p_1, \dots, p_n\}, \\ \infty, & \text{jeśli } a = 0, \end{cases}$$

gdzie $a = up_1^{k_1} \cdot \dots \cdot p_n^{k_n}$ jest rozkładem kanonicznym elementu a , nazywamy **waluacją p -adyczną**.

Uwaga 7.14. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym z jednoznacznym rozkładem. Niech $p \in \mathbb{P}(R)$ i niech $v_p : R \rightarrow \mathbb{Z} \cup \{\infty\}$ będzie jego waluacją p -adyczną. Wówczas:

- (1) jeśli $a \neq 0$, to $v_p(a) \geq 0$;
- (2) $v_p(a) = 0$ dla prawie wszystkich $p \in \mathbb{P}(R)$;
- (3) jeśli $a \in R$, to $a = u \prod_{p \in \mathbb{P}(R)} p^{v_p(a)}$, dla pewnego $u \in U(R)$;
- (4) $v_p(ab) = v_p(a) + v_p(b)$, dla $a, b \in R$;
- (5) $v_p(a + b) \geq \min\{v_p(a), v_p(b)\}$, dla $a, b \in R$;
- (6) jeśli $a, b \in R$, to $a|b$ wtedy i tylko wtedy, gdy $v_p(a) \leq v_p(b)$, dla wszystkich $p \in \mathbb{P}(R)$.

Proste dowody powyższych własności pozostawiamy jako ćwiczenie.

Uwaga 7.15. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym z jednoznacznym rozkładem. Niech $a, b \in R$. Wówczas:

- (1) istnieje największy wspólny dzielnik elementów a i b oraz zachodzi wzór

$$NWD(a, b) \sim \prod_{p \in \mathbb{P}(R)} p^{\min\{v_p(a), v_p(b)\}};$$

- (2) istnieje najmniejsza wspólna wielokrotność elementów a i b oraz zachodzi wzór

$$NWW(a, b) \sim \prod_{p \in \mathbb{P}(R)} p^{\max\{v_p(a), v_p(b)\}}.$$

Dowód. (1) Porównaj dowód implikacji (1) $\Rightarrow$ (3) w Twierdzeniu 7.1.

- (2) Ćwiczenie.

$\square$