10. Wykład 10: Podstawowe pojęcia teorii podzielności. Pierścienie z jednoznacznym rozkładem. Dziedziny ideałów głównych. Pierścienie euklidesowe.

10.1. Podstawowe pojęcia teorii podzielności.

Definicja 10.1. *Niech $(R, +, \cdot)$ będzie pierścieniem*[14] *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 10.1. *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) *jeśli dla* $a \in R \setminus \{0\}$, $u \in U(R)$ *zachodzi* $a|u$, *to* $a \in U(R)$,
(7) $a|b_1, \ldots, a|b_n \Rightarrow a|x_1b_1 + \ldots + x_nb_n$ *dla* $a, b_1, \ldots, b_n, x_1, \ldots, x_n \in R \setminus \{0\}$,
(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 10.2. *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 10.2. *Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym, niech $a, b \in R$. Wówczas*

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

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 $dc = 1$,[15] 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 $a \in F^*$.

[14] Od teraz "pierścień" będzie zawsze oznaczał "pierścień przemienny z jedynką".
[15] Korzystamy 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 10.3. *Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym. Wówczas relacja $\sim$ jest relacją równoważności w zbiorze $R \setminus \{0\}$.*

Definicja 10.3. *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 $h \in U(F[x])$. □

- 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. □

(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 10.4. *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 $x|g$. □

Uwaga 10.4. *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, $b \in U(R)$. □

Przykład:

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

Uwaga 10.5. *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 10.5. *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 10.6. *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 10.7. *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* $a|b^kc$, *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 10.6. *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 10.8. *Niech $(R,+,\cdot)$ będzie pierścieniem całkowitym, niech $a_1,\ldots,a_n,d_1,d_2 \in R$. Niech $w_1 \sim NWW(a_1,\ldots,a_n)$ oraz $w_2 \sim NWW(a_1,\ldots,a_n)$. 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 10.9. *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 $d'|d$. □

Uwaga 10.10. *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) *$NWW(a_1,\ldots,a_n) \sim NWW(NWW(a_1,\ldots,a_{n-1}),a_n)$;*
(3) *$NWD(a,NWW(b,c)) \sim NWW(NWD(a,b),NWD(a,c))$;*
(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 10.11. *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 $a \nsim b$ oraz $a \nsim c$ i tym samym $(a) \subsetneq (c) \subsetneq R$, co jest sprzecznością.

(6) Wynika wprost z (5).

□

10.2. **Pierścienie z jednoznacznym rozkładem.**

Definicja 10.7. *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 gaussowskim,** *lub* **UFD**[16]*) 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

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

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 $d \in \{1, \ldots, 100\}$ 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 10.12. *Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym z jednoznacznym rozkładem. Niech $a \in R$ i niech $a = p_{1_1} \cdot \ldots \cdot p_{1_{k_1}} p_{2_1} \cdot \ldots \cdot p_{2_{k_2}} p_{n_1} \cdot \ldots \cdot p_{n_{k_n}}$ będzie rozkładem elementu a na iloczyn elementów nierozkładalnych, przy czym $p_{i_{s_i}} \sim p_{i_{t_i}}$, $i \in \{1, \ldots, n\}$, $s, t \in \{1, \ldots, k\}$ oraz $p_{i_{s_i}} \nsim p_{j_{t_j}}$ dla $i \neq j$, $s, t \in \{1, \ldots, k\}$. Wówczas*

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

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

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

[16] Unique 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

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

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

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

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

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

Uwaga 10.13. *Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym z jednoznacznym rozkładem. Niech $a, b \in R \setminus \{0\}$ i niech $a = up_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$, gdzie $u \in U(R)$, $p_1, \ldots, p_n \in \mathbb{P}(R)$ są parami różne, będzie rozkładem kanonicznym. Wówczas $b|a$ wtedy i tylko wtedy, gdy $b = vp_1^{l_1} \cdot \ldots \cdot p_n^{l_n}$, gdzie $v \in U(R)$ oraz $l_i \leq k_i$, $i \in \{1, \ldots, n\}$.*

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

Twierdzenie 10.1. *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 $a = up_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$, $b = vp_1^{l_1} \cdot \ldots \cdot p_n^{l_n}$ (dopuszczamy $k_i, l_i = 0$). Niech $m_i = \min\{k_i, l_i\}$ i niech $d = p_1^{m_1} \cdot \ldots \cdot p_n^{m_n}$.

Pokażemy, że $d \sim NWD(a, b)$. Oczywiście $d|a$ i $d|b$. Niech $c|a$ i $c|b$. Wobec Uwagi 10.13 $c = wp_1^{s_1} \cdot \ldots \cdot p_n^{m_n}$, gdzie $w \in U(R)$, $s_i \leq k_i$, $s_i \leq l_i$, $i \in \{1, \ldots, n\}$. Zatem $s_i \leq m_i = \min\{k_i, l_i\}$, $i \in \{1, \ldots, n\}$, 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 $p_1 \cdot \ldots \cdot p_n = q_1 \cdot \ldots \cdot q_m$, gdzie $n, m \in \mathbb{N}$ oraz $p_1, \ldots, p_n, q_1, \ldots, q_m$ są nierozkładalne. Pokażemy, że $n = m$ oraz, po ewentualnej zmianie numeracji, $p_1 \sim q_1, \ldots, p_n \sim q_n$. Dowód przeprowadzimy indukcyjnie względem n.

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

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

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

$$p_1 \cdot \ldots \cdot p_n = up_1q_2 \cdot \ldots \cdot q_m,$$

a stąd

$$p_2 \cdot \ldots \cdot p_n = uq_2 \cdot \ldots \cdot q_m.$$

Oczywiście uq_2 jest nierozkładalny. Zatem wobec założenia indukcyjnego $n-1 = m-1$ oraz $p_2 \sim uq_2 \sim q_2, \ldots, p_n \sim q_n$. □

Definicja 10.8. *Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym z jednoznacznym rozkładem. Niech $p \in \mathbb{P}(R)$. Funkcję $v_p : R \to \mathbb{Z} \cup \{\infty\}$ zdefiniowaną wzorem*

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

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

Uwaga 10.14. *Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym z jednoznacznym rozkładem. Niech $p \in \mathbb{P}(R)$ i niech $v_p : R \to \mathbb{Z} \cup \{\infty\}$ 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 10.15. *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) ⇒ (3) w Twierdzeniu 10.1.
(2) Ćwiczenie.

□

10.3. **Dziedziny ideałów głównych.**

Twierdzenie 10.2. *Każdy całkowity pierścień ideałów głównych jest pierścieniem z jednoznacznym rozkładem.*

Dowód. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym (dziedziną) ideałów głównych. Pokażemy najpierw, że każdy wstępujący łańcuch ideałów jest skończony. Istotnie, niech $I_1 \subset I_2 \subset \ldots$ będzie wstępującym łańcuchem ideałów. Niech $J = \bigcup_{i=1}^{\infty} I_i$. Wówczas $J \lhd R$, ale ponieważ R jest pierścieniem ideałów głównych, więc $J = (a)$, dla pewnego $a \in R$. W szczególności $a \in I_{i_0}$, dla pewnego $i_0 \in \mathbb{N}$, a zatem $J = (a) \subset I_{i_0}$ i ponieważ $I_{i_0} \subset J$, więc $J = I_{i_0}$. Ponadto:

$$J = I_{i_0} \subset I_{i_0+1} \subset I_{i_0+2} \subset \ldots \subset \bigcup_{i=1}^{\infty} I_i = J,$$

więc dla $j > i_0$ zachodzi $I_j = I_{i_0} = J$.

Pokażemy, że R jest pierścieniem z rozkładem. Przypuśćmy nie wprost, że R nie jest pierścieniem z rozkładem. Wówczas istnieje niezerowy i nieodwracalny element $a \in R$ taki, że a nie jest iloczynem elementów nierozkładalnych. W szczególności a nie jest elementem nierozkładalnym, a więc $a = a_1 b_1$ dla pewnych niezerowych i nieodwracalnych $a_1, b_1 \in R$. Zauważmy, że a_1 lub b_1 nie jest iloczynem elementów nierozkładalnych: istotnie, gdyby $a_1 = p_1 \cdot \ldots \cdot p_k$ oraz $b_1 = q_1 \cdot \ldots \cdot q_l$, dla pewnych nierozkładalnych elementów $p_1, \ldots, p_k, q_1, \ldots, q_l$, to wówczas $a = a_1 b_1 = p_1 \cdot \ldots \cdot p_k q_1 \cdot \ldots \cdot q_l$ wbrew założeniom. Załóżmy, że to a_1 nie jest iloczynem elementów nierozkładalnych. W szczególności a_1 nie jest nierozkładalny, a więc $a_1 = a_2 b_2$ dla pewnych niezerowych i nieodwracalnych elementów $a_2, b_2 \in R$, z których przynajmniej jeden – powiedzmy a_2 – nie jest iloczynem elementów nierozkładalnych. Postępując indukcyjnie otrzymujemy nieskończone ciągi $a_1, a_2, a_3, \ldots$ oraz $b_1, b_2, b_3, \ldots$ elementów niezerowych i nieodwracalnych takich, że $a_i = a_{i+1} b_{i+1}$, $i \in \mathbb{N}$. W szczególności $a_{i+1} | a_i$, dla $i \in \mathbb{N}$, otrzymujemy więc nieskończony ciąg wstępujący ideałów

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \ldots,$$

co jest niemożliwe.

Ustalmy $a \in R$ i załóżmy, że a jest elementem nierozkładalnym. Wobec Uwagi 10.11 (5) oraz tego, że R jest pierścieniem ideałów głównych, (a) jest ideałem maksymalnym w R. Wobec tego jest też ideałem pierwszym. A zatem wobec Uwagi 10.11 (4) a jest elementem pierwszym. Tym samym, wobec Twierdzenie 10.1, R jest pierścieniem z jednoznacznym rozkładem. □

Przykłady:

(1) (Zasadnicze twierdzenie arytmetyki) $\mathbb{Z}$ jest pierścieniem z jednoznacznym rozkładem.

(2) Niech F będzie dowolnym ciałem. Wówczas $F[x]$ jest pierścieniem z jednoznacznym rozkładem.

Uwaga 10.16. *Niech $(R, +, \cdot)$ będzie dziedziną ideałów głównych, niech $a_1, \ldots, a_n, d \in R$. Wówczas*

$$d \sim NWD(a_1, \ldots, a_n) \text{ wtedy i tylko wtedy, gdy } (d) = (a_1, \ldots, a_n).$$

Dowód. ($\Rightarrow$) : Załóżmy, że $(d) = (a_1, \ldots, a_n)$. Pokażemy, że $d \sim NWD(a_1, \ldots, a_n)$. Oczywiście $d | a_i$ dla $i \in \{1, \ldots, n\}$. Niech zatem $c | a_i$, $i \in \{1, \ldots, n\}$. Wtedy $a_i \in (c)$, $i \in \{1, \ldots, n\}$, a więc $(a_1, \ldots, a_n) \subset (c)$. Zatem $(d) \subset (c)$, więc $c | d$.

($\Leftarrow$) : Załóżmy teraz, że $d \sim NWD(a_1, \ldots, a_n)$. Ponieważ R jest pierścieniem ideałów głównych, więc $(a_1, \ldots, a_n) = (d_1)$, dla pewnego $d_1 \in R$. Wobec już udowodnionej części twierdzenia, $d_1 \sim NWD(a_1, \ldots, a_n)$, a więc $d \sim d_1$. □

Wniosek 10.1. *Niech $(R, +, \cdot)$ będzie dziedziną ideałów głównych, niech $a_1, \ldots, a_n, d \in R$. Wówczas:*

(1) $1 \sim NWD(a_1, \ldots, a_n)$ *wtedy i tylko wtedy, gdy istnieją $x_1, \ldots . x_n \in P$ takie, że $1 = x_1 a_1 + \ldots + x_n a_n$;*

(2) $d \sim NWD(a_1, \ldots, a_n)$ *wtedy i tylko wtedy, gdy istnieją $x_1, \ldots . x_n \in P$ takie, że $d = x_1 a_1 + \ldots + x_n a_n$;*

(3) *jeśli istnieją* $x_1, \ldots . x_n \in P$ *takie, że* $d = x_1a_1 + \ldots + x_na_n$, *to* $NWD(a_1, \ldots, a_n)|d$.

10.4. **Pierścienie euklidesowe.**

Definicja 10.9. *Niech* $(R, +, \cdot)$ *będzie pierścieniem całkowitym.*

(1) *Funkcję* $N : R \to \mathbb{N} \cup \{\infty\}$ *nazywamy* **normą euklidesową,** *jeżeli*
- $N(a) = 0$ *wtedy i tylko wtedy, gdy* $a = 0$,
- $\forall a, b \in R \setminus \{0\}(N(a) \leq N(ab))$,
- $\forall a, b \in R \setminus \{0\}\exists q, r \in R(a = bq + r)$ *oraz* $N(r) < N(b)$.

(2) *Funkcję* $N : R \to \mathbb{N} \cup \{\infty\}$ *nazywamy* **multyplikatywną normą euklidesową,** *jeżeli jest normą euklidesową oraz*
- $\forall a, b \in R \setminus \{0\}(N(ab) = N(a)N(b))$.

(3) *Pierścień* R *nazywamy* **pierścieniem euklidesowym,** *jeżeli istnieje w nim norma euklidesowa.*

(4) *Pierścień* R *nazywamy* **pierścieniem euklidesowym z normą multyplikatywną,** *jeżeli istnieje w nim multyplikatywna norma euklidesowa.*

Uwaga 10.17. *Niech* $(R, +, \cdot)$ *będzie pierścieniem euklidesowym,* $N : R \to \mathbb{N} \cup \{\infty\}$ *normą euklidesową, niech* $a, b \in R \setminus \{0\}$. *Wówczas:*

(1) *jeżeli* $a|b$, *to* $N(a) \leq N(b)$;
(2) *jeżeli* $a \sim b$, *to* $N(a) = N(b)$;
(3) $a \in U(R)$ *wtedy i tylko wtedy, gdy* $N(a) = N(1)$;
(4) *jeżeli* $N(a) = N(b)$ *i* $a|b$, *to* $a \sim b$.

Ponadto, gdy $N : R \to \mathbb{N} \cup \{\infty\}$ *jest multyplikatywną normą euklidesową, to:*

(5) *jeżeli* $a|b$, *to* $N(a)|N(b)$;
(6) $a \in U(R)$ *wtedy i tylko wtedy, gdy* $N(a) = 1$;
(7) *jeżeli* $N(a)$ *jest liczbą pierwszą, to* a *jest elementem nierozkładalnym.*

Proste dowody powyższych własności pozostawiamy jako ćwiczenie.

Przykłady:

(1) Rozważmy $\mathbb{Z}$. Jest to pierścień euklidesowy z normą multyplikatywną $N : \mathbb{Z} \to \mathbb{N} \cup \{0\}$, $N(a) = |a|$.

(2) Rozważmy $F[x]$, gdzie F jest dowolnym ciałem. Jest to pierścień euklidesowy z normą multyplikatywną $N : F[x] \to \mathbb{N} \cup \{0\}$,

$$N(f) = \begin{cases} 0, & \text{jeśli } f = 0, \\ 2^{\deg f}, & \text{jeśli } f \neq 0. \end{cases}$$

(3) Rozważmy $\mathbb{Z}[\omega_d]$.
Twierdzenie. $\mathbb{Z}[\omega_d]$ *jest pierścieniem euklidesowym wtedy i tylko wtedy, gdy*

$$d \in \{-11, -7, -3, -1, 2, 3, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

Twierdzenie 10.3. *Każdy pierścień euklidesowy jest dziedziną ideałów głównych.*

Dowód. Niech $(R, +, \cdot)$ będzie pierścieniem euklidesowym, $N : R \to \mathbb{N} \cup \{\infty\}$ normą euklidesową, Niech $\{0\} \neq I \lhd P$. Pokażemy, że I jest główny. Istotnie, niech $n = \min\{N(a) : a \in I, a \neq 0\}$ i niech $n = N(c)$. Wystarczy pokazać, że $I = (c)$. Inkluzja $(\supset)$ jest oczywista, a dla dowodu inkluzji $(\subset)$ ustalmy $x \in I$. Wówczas istnieją $q, r \in R$ takie, że

$$x = qc + r,$$

oraz $N(r) < N(c)$. Zatem $r = x - qc \in I$ oraz $N(r) < N(c)$. Wobec wyboru elementu c, $r = 0$, a więc $x = qc \in (c)$. □

Wniosek 10.2. *Każdy pierścień euklidesowy jest pierścieniem z jednoznacznym rozkładem.*

Przykład:

(4) Rozważmy $\mathbb{Z}[\omega_{-19}]$. Jest to pierścień z jednoznacznym rozkładem, ale nie jest euklidesowy.

Twierdzenie 10.4 (algorytm Euklidesa)**.** *Niech $(R, +, \cdot)$ będzie pierścieniem euklidesowym, $N : R \to \mathbb{N} \cup \{\infty\}$ normą euklidesową, niech $a, b \in R \setminus \{0\}$. Wówczas istnieją ciągi*

$$(q_1, \ldots, q_n)$$

oraz

$$(r_1, \ldots, r_n)$$

elementów pierścienia R takie, że

$$\begin{gathered} a = b \cdot q_1 + r_1 \ i \ N(r_1) < N(b), \\ b = r_1 \cdot q_2 + r_2 \ i \ N(r_2) < N(r_1), \\ r_1 = r_2 \cdot q_3 + r_3 \ i \ N(r_3) < N(r_2), \\ \vdots \\ r_{n-3} = r_{n-2} \cdot q_{n-1} + r_{n-1} \ i \ N(r_{n-1}) < N(r_{n-2}), \\ r_{n-2} = r_{n-1} \cdot q_n + r_n \ i \ r_n = 0. \end{gathered}$$

Ponadto $r_{n-1} \sim NWD(a, b)$.

Dowód. Istnienie stosownych ciągów $(q_1, q_2, \ldots)$ i $(r_1, r_2, \ldots)$ wynika z definicji normy. Pokażemy, że ciągi te są skończone. Przypuśćmy, że $(r_1, r_2, \ldots)$ jest ciągiem nieskończonym. Wówczas $(N(r_1), N(r_2), \ldots)$ jest nieskończonym malejącym ciągiem liczb naturalnych, co jest niemożliwe.

Pokażemy, że $r_{n-1} \sim NWD(a, b)$. Zauważmy najpierw, że $r_{n-1}|a$ i $r_{n-1}|b$. Mamy $r_{n-2} = r_{n-1} \cdot q_n$, a zatem $r_{n-1}|r_{n-2}$. Mamy też $r_{n-3} = r_{n-2} \cdot q_{n-1} + r_{n-1}$, a więc $r_{n-1}|r_{n-3}$. Postępując indukcyjnie otrzymujemy, że $r_{n-1}|a$ i $r_{n-1}|b$.

Załóżmy, że $c|a$ i $c|b$. Ponieważ $a = b \cdot q_1 + r_1$, więc $c|r_1$. Dalej, ponieważ $b = r_1 \cdot q_2 + r_2$, więc $c|r_2$. Postępując indukcyjnie otrzymujemy, że $c|r_{n-1}$. □