

8. WYKŁAD 8: DZIEDZINY IDEAŁÓW GŁÓWNYCH. PIERŚCIEŃ EUKLIDESOWE. ZASTOSOWANIE JEDNOZNACZNOŚCI ROZKŁADU DO ROZWIĄZYWANIA PEWNYCH RÓWNAŃ DIOFANTYCZNYCH.

8.1. Dziedziny ideałów głównych.

Twierdzenie 8.1. *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 $I_1 \subset I_2 \subset \dots$ będzie wstępującym łańcuchem ideałów. Niech $J = \bigcup_{i=1}^{\infty} I_i$. Wówczas $J \triangleleft R$, 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:

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

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 $a_1 = p_1 \cdot \dots \cdot p_k$ oraz $b_1 = q_1 \cdot \dots \cdot q_l$, dla pewnych nierozkładalnych elementów $p_1, \dots, p_k, q_1, \dots, q_l$, to wówczas $a = a_1 b_1 = p_1 \cdot \dots \cdot p_k q_1 \cdot \dots \cdot q_l$ 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 $a_1, a_2, a_3, \dots$ oraz $b_1, b_2, b_3, \dots$ 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

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

co jest niemożliwe.

Ustalmy $a \in R$ i załóżmy, że a jest elementem nierozkładalnym. Wobec Uwagi 7.11 (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 7.11 (4) a jest elementem pierwszym. Tym samym, wobec Twierdzenia 7.1, R jest pierścieniem z jednoznacznym rozkładem. $\square$

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 8.1. Niech $(R, +, \cdot)$ będzie dziedziną ideałów głównych, niech $a_1, \dots, a_n, d \in R$. Wówczas

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

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

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

Wniosek 8.1. Niech $(R, +, \cdot)$ będzie dziedziną ideałów głównych, niech $a_1, \dots, a_n, d \in R$. Wówczas:

- (1) $1 \sim NWD(a_1, \dots, a_n)$ wtedy i tylko wtedy, gdy istnieją $x_1, \dots, x_n \in P$ takie, że $1 = x_1 a_1 + \dots + x_n a_n$;
- (2) $d \sim NWD(a_1, \dots, a_n)$ wtedy i tylko wtedy, gdy istnieją $x_1, \dots, x_n \in P$ takie, że $d = x_1 a_1 + \dots + x_n a_n$;
- (3) jeśli istnieją $x_1, \dots, x_n \in P$ takie, że $d = x_1 a_1 + \dots + x_n a_n$, to $NWD(a_1, \dots, a_n) | d$.

8.2. Pierścienie euklidesowe.

Definicja 8.1. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym.

- (1) Funkcję $N : R \rightarrow \mathbb{N} \cup \{\infty\}$ 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 $N : R \rightarrow \mathbb{N} \cup \{\infty\}$ nazywamy **multymplikatywną 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 multymplikatywną**, jeżeli istnieje w nim multymplikatywna norma euklidesowa.

Uwaga 8.2. Niech $(R, +, \cdot)$ będzie pierścieniem euklidesowym, $N : R \rightarrow \mathbb{N} \cup \{\infty\}$ 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 $N : R \rightarrow \mathbb{N} \cup \{\infty\}$ jest multymplikatywną 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 multymplikatywną $N : \mathbb{Z} \rightarrow \mathbb{N} \cup \{0\}$, $N(a) = |a|$.
- (2) Rozważmy $F[x]$, gdzie F jest dowolnym ciałem. Jest to pierścień euklidesowy z normą multymplikatywną $N : F[x] \rightarrow \mathbb{N} \cup \{0\}$,

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

- (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 8.2. Każdy pierścień euklidesowy jest dziedziną ideałów głównych.

Dowód. Niech $(R, +, \cdot)$ będzie pierścieniem euklidesowym, $N : R \rightarrow \mathbb{N} \cup \{\infty\}$ normą euklidesową, Niech $\{0\} \neq I \triangleleft P$. 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 $x = qc \in (c)$. $\square$

Wniosek 8.2. *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 8.3 (algorytm Euklidesa). *Niech $(R, +, \cdot)$ będzie pierścieniem euklidesowym, $N : R \rightarrow \mathbb{N} \cup \{\infty\}$ normą euklidesową, niech $a, b \in R \setminus \{0\}$. Wówczas istnieją ciągi*

$$(q_1, \dots, q_n)$$

oraz

$$(r_1, \dots, r_n)$$

elementów pierścienia R takie, że

$$a = b \cdot q_1 + r_1 \text{ i } N(r_1) < N(b),$$

$$b = r_1 \cdot q_2 + r_2 \text{ i } N(r_2) < N(r_1),$$

$$r_1 = r_2 \cdot q_3 + r_3 \text{ i } N(r_3) < N(r_2),$$

$$\vdots$$

$$r_{n-3} = r_{n-2} \cdot q_{n-1} + r_{n-1} \text{ i } N(r_{n-1}) < N(r_{n-2}),$$

$$r_{n-2} = r_{n-1} \cdot q_n + r_n \text{ i } r_n = 0.$$

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

Dowód. Istnienie stosownych ciągów $(q_1, q_2, \dots)$ i $(r_1, r_2, \dots)$ wynika z definicji normy. Pokażemy, że ciągi te są skończone. Przypuśćmy, że $(r_1, r_2, \dots)$ jest ciągiem nieskończonym. Wówczas $(N(r_1), N(r_2), \dots)$ 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 $c | r_{n-1}$. $\square$

8.3. Zastosowanie jednoznaczności rozkładu do rozwiązywania pewnych równań diofantycznych.

Lemat 8.1. *Niech $(R, +, \cdot)$ będzie pierścieniem z jednoznacznym rozkładem, niech $n \in \mathbb{N}$, niech $a, b \in R$ będą niezerowymi elementami nieodwracalnymi, niech $c \in R$. Jeżeli $ab = c^n$, to istnieje element $u \in U(R)$ taki, że ua i $u^{-1}b$ są n -tymi potęgami w R . Ponadto, gdy wszystkie elementy $v \in U(R)$ są n -tymi potęgami, to a i b są n -tymi potęgami w R .*

Dowód. Niech $c = p_1 \cdot \dots \cdot p_k$ będzie rozkładem elementu c na czynniki nierozkładalne. Wówczas $ab = p_1^n \cdot \dots \cdot p_k^n$ jest rozkładem elementu ab na czynniki nierozkładalne. Ponieważ $p_1 | ab$, więc $p_1 | a$ lub $p_1 | b$. Jeśli $p_1 | a$, to $p_1^n | a$, jeśli $p_1 | b$, to $p_1^n | b$. Postępując indukcyjnie dla $p_2, \dots, p_n$ otrzymujemy

$$a = v_1 p_{i_1}^n \cdot \dots \cdot p_{i_r}^n \text{ oraz } b = v_2 p_{j_1}^n \cdot \dots \cdot p_{j_s}^n,$$

gdzie $\{i_1, \dots, i_r, j_1, \dots, j_s\} = \{1, \dots, k\}$ i $\{i_1, \dots, i_r\} \cap \{j_1, \dots, j_s\} = \emptyset$. Zatem $v_1 v_2 = 1$. Kładąc $u = v_2$ otrzymujemy tezę. $\square$

Przykład:

- (1) Korzystając z jednoznaczności rozkładu w pierścieniu $\mathbb{Z}[\sqrt{-2}]$ udowodnić, że jedynymi całkowitymi rozwiązaniami równania $x^3 = y^2 + 2$ są $(3, 5)$ oraz $(3, -5)$.

Rozwiązanie. Niech (x, y) będzie rozwiązaniem. Jeżeli y jest parzyste, to x jest parzyste, a wtedy $4 | x^3$ i $4 \nmid y^2 + 2$, co jest sprzecznością. Zatem y jest nieparzyste. Skoro $x^3 = y^2 + 2$, to w pierścieniu $\mathbb{Z}[\sqrt{-2}]$ zachodzi

$$x^3 = (y + \sqrt{-2})(y - \sqrt{-2}).$$

Pokażemy, że $1 \sim NWD(y + \sqrt{-2}, y - \sqrt{-2})$. Istotnie, przypuśćmy, że $a + b\sqrt{-2} \sim NWD(y + \sqrt{-2}, y - \sqrt{-2})$, przy czym $b \neq 0$, $a \neq 1$. Zatem

$$a + b\sqrt{-2} | (y + \sqrt{-2}) - (y - \sqrt{-2}) = 2\sqrt{-2} = (\sqrt{-2})^3.$$

$\sqrt{-2}$ jest elementem nierozkładalnym w $\mathbb{Z}[\sqrt{-2}]$, zatem $a + b\sqrt{-2} \sim (\sqrt{-2})^k$ dla pewnego $k \in \mathbb{N}$. Ale y jest nieparzyste, więc $\sqrt{-2} \nmid y + \sqrt{-2}$. Więc $a + b\sqrt{-2} \sim 1$.

Mamy, że $U(\mathbb{Z}[\sqrt{-2}]) = \{\pm 1\}$. Ponadto ± 1 są sześciانami w $\mathbb{Z}[\sqrt{-2}]$, więc wobec lematu $y + \sqrt{-2}$ i $y - \sqrt{-2}$ są sześciانami w $\mathbb{Z}[\sqrt{-2}]$. Więc dla pewnych $m, n \in \mathbb{Z}$:

$$y + \sqrt{-2} = (m + n\sqrt{-2})^3 = (m^3 - 6mn^2) + (3m^2n - 2n^3)\sqrt{-2}.$$

Zatem $1 = n(3m^2 - 2n^2)$, skąd $n = 1$ oraz $m = \pm 1$. Wobec tego $y = m^3 - 6mn^2 = \pm 5$, $x = 3$.