# 11. Dziedziny Euklidesowe

**11.1. Definicja.** *Dziedziną Euklidesową nazywamy parę $(R, v)$, gdzie $R$ jest dziedziną całkowitości a $v : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$ funkcją zwaną waluacją, która spełnia następujące warunki:*
1. *dla dowolnych $a, b \in R \setminus \{0\}$, $v(ab) \geq v(a)$,*
2. *dla dowolnych $a \in R$ oraz $b \in R \setminus \{0\}$ istnieja elementy $q, r \in R$, takie że*

$$a = bq + r \quad oraz \quad r = 0 \quad lub \quad v(r) < v(b).$$

**11.2. Twierdzenie.** *Każda dziedzina euklidesowa jest dziedziną ideałów głównych.*

**Dowód.** Niech $R$ będzie dziedzina euklidesową z waluacją $v$. Niech $I \lhd R$ będzie niezerowym ideałem. Niech $x \in I$ będzie niezerowym elementem, takim że $v(x) = \min\{v(y) : \quad y \in I \setminus \{0\}\}$. Pokażemy, że $I = (x)$. Niech $y \in I$. Wówczas $y = xq + r$, gdzie $r = 0$ lub $v(r) < v(x)$. Zauważmy, że skoro $y, x \in I$, to $r \in I$. Ponieważ waluacja $x$ jest minimalna, to $r = 0$ i $y = qx$, a zatem $I = (x)$. □

Klasa pierścieni będących dziedzinami ideałów głównych jest szersza od klasy pierścieni euklidesowych. Na tym wykładzie wszystkie omawiane przykłady dziedzin ideałów głównych będą pierścieniami euklidesowymi. Zanim omówimy przykłady dziedzin euklidesowych odnotujmy pewne proste własności waluacji.

**11.3. Stwierdzenie.** *Niech $v : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$ będzie waluacją. Wówczas,*
*a) dla każdego $a \in R \setminus \{0\}$, $v(a) \geq v(1)$.*
*b) dla dowolnych $a, b \in R \setminus \{0\}$, $v(ab) = v(b)$ wtedy i tylko wtedy, gdy $a$ jest elementem odwracalnym.*
*c) dla dowolnego $a \in R \setminus \{0\}$, $v(a) = v(1)$ wtedy i tylko wtedy, gdy $a$ jest elementem odwracalnym.*

**Dowód.** punkt a) jest oczywistym wnioskiem z definicji, zaś punkt c) wynika z punktu b). Tak więc udowodnimy punkt b). Jeżeli $v(ab) = v(b)$, to z dowodu poprzedniego twierdzenia wynika, że $(ab) = (b)$. W szczególności $b \in (ab)$ i istnieje $c \in R$, dla którego $b = abc$. Ponieważ $b \neq 0$ i $R$ jest dziedzina całkowitości, to $ac = 1$. Odwrotnie, jeżeli $a$ jest elementem odwracalnym i $c$ elementem odwrotnym, to $v(b) = v(cab) \geq v(ab)$. Nierówność $v(ab) \geq v(b)$ wynika z definicji. Punkt c) jest wnioskiem z b) jeżeli weźmiemy $b = 1$. □

Przykładami dziedzin euklidesowych są : pierścień liczb całkowitych $\mathbb{Z}$, gdzie waluacją jest wartość bezwzględna oraz pierścień wielomianów $K[X]$ nad ciałem $K$, gdzie waluacja jest stopień wielomianu.

Niech $d \in \mathbb{Z}$ będzie liczba całkowitą,$d \neq 1$, bezkwadratową. Niech

$$v : \mathbb{Z}[\sqrt{d}] \to \mathbb{N} \qquad v(a + b\sqrt{d}) = |a^2 - b^2 d|.$$

Wprowadźmy oznaczenia: $\alpha = a + b\sqrt{d}$, $\bar{\alpha} = a - b\sqrt{d}$. Wówczas $v(\alpha) = |\alpha\bar{\alpha}|$. Łatwy rachunek przekonuje nas o tym, że $v(\alpha\beta) = v(\alpha)v(\beta)$ oraz, że $\alpha$ jest elementem odwracalnym wtedy i tylko wtedy, gdy $v(\alpha) = 1$ i wówczas $\bar{\alpha}$ jest elementem odwrotnym.

**11.4. Stwierdzenie.** *Funkcja* $v(a+b\sqrt{d}) = |a^2 - b^2 d|$ *jest waluacją euklidesową na* $\mathbb{Z}[\sqrt{d}]$ *dla* $d \in \{-2, -1, 2, 3\}$

**Dowód.** Jest oczywiste, że $v(a+b\sqrt{d}) \geq 1$, gdyż $v(a+b\sqrt{d}) = 0$ oznaczałoby, że $d = (\frac{a}{b})^2$, wbrew założeniu, że $d$ jest liczba bezkwadratową. Stąd i z multyplilkatywności funkcji $v$ wynika, że warunek pierwszy jest spełniony dla dowolnego $d$.

Pokażemy, że dla wymienionych wartości $d$ w pierścieniu $\mathbb{Z}[\sqrt{d}]$ można dzielić z resztą. Dowód dostarcza także algorytm wykonywania takiego dzielenia. Niech $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$, $\beta \neq 0$. Wówczas $\frac{\alpha}{\beta} = \frac{\alpha\bar{\beta}}{\beta\bar{\beta}} = x + y\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$. Niech $r, s \in \mathbb{Z}$ będą liczbami całkowitymi takimi, że $|x - r| \leq \frac{1}{2}$ i $|y - s| \leq \frac{1}{2}$. Niech $\gamma = r + s\sqrt{d}$, zaś $\delta = ((x - r) + (y - s)\sqrt{d})\beta$. Zauważmy, że $\alpha = \beta\gamma + \delta$ przy czym $\alpha, \beta, \gamma \in \mathbb{Z}[\sqrt{d}]$. Zatem także $\delta \in \mathbb{Z}[\sqrt{d}]$. Wystarczy teraz pokazać, ze $v(\delta) < v(\beta)$ lub $\delta = 0$. Przypuśćmy, że $\delta \neq 0$. Mamy $v(\delta) = v(\beta)|(x-r)^2 - (y-s)^2 d| \leq v(\beta)(\frac{1}{4} + \frac{1}{4}|d|)$. Dla $d =\in \{-2, -1, 2\}$, $\frac{1}{4} + \frac{1}{4}|d| < 1$ i $v(\delta) < v(\beta)$. Jeżeli $d = 3$, to $|(x-r)^2 - (y-s)^2 3| \leq \frac{1}{4} + \frac{1}{4}3 = 1$. Równość może wystąpić tylko wtedy, gdy $x - r = y - s = \frac{1}{2}$, jednak wówczas $v(\frac{1}{2} + \frac{1}{2}\sqrt{3}) = \frac{1}{2} < 1$, co dowodzi, że dla $d = 3$ waluacja także jest euklidesowa. □

**11.5. Przykład.** Liczba 2 nie jest elementem pierwszym, ale jest elementem nierozkładalnym w pierścieniu $\mathbb{Z}[\sqrt{d}]$, dla $d \leq -3$. Przypuśćmy przeciwnie, że $2 = \alpha\beta$, gdzie $\alpha, \beta$ nieodwracalne. Wówczas $v(2) = 4 = v(\alpha)v(\beta)$. Z nieodwracalności $v(\alpha) \neq 1$ i $v(\beta) \neq 1$, a więc $v(\alpha) = v(\beta) = 2$.Jeżeli $\alpha = x + y\sqrt{d}$, to $|x^2 - y^2 d| = 2$, ale dla $d \leq -3$, to nie jest mozliwe. Bowiem $|x^2 - y^2 d| \geq x^2 + 3y^2 > 2$ dla $y \neq 0$, ale $y \neq 0$, bo w przeciwnym razie 2 byłaby kwadratem liczby naturalnej.

**11.6. Wniosek.** *Dziedzina* $\mathbb{Z}[\sqrt{d}]$ *nie jest dziedziną euklidesową dla* $d \leq -3$.

### Algorytm Euklidesa

Niech $R$ będzie dziedziną Euklidesową z waluacją $v$. Pokażemy algorytm, który pozwoli na znajdowanie największego wspólnego dzielnika dwóch elementów bez konieczności rozkładania ich na iloczyn czynników nierozkładalnych.

Niech $a_1, a_2 \in R \setminus \{0\}$. Mamy:

$$\begin{array}{lllllll} a_1 & = & a_2 q_1 + a_3 & \text{gdzie} & a_3 = 0 & \text{lub} & v(a_3) < v(a_2) \\ a_2 & = & a_3 q_2 + a_4 & \text{gdzie} & a_4 = 0 & \text{lub} & v(a_4) < v(a_3) \\ a_3 & = & a_4 q_3 + a_5 & \text{gdzie} & a_5 = 0 & \text{lub} & v(a_5) < v(a_4) \\ .. & & & & & & \end{array}$$

jest jasne, że ten proces musi się skończyć i w końcu

$$a_{n-1} = a_n q_{n-1} + 0$$

**11.7. Stwierdzenie.** $a_n = NWD(a_1, a_2)$

**Dowód.** Wiemy, że $NWD(a_1, a_2)$ jest generatorem ideału $(a_1, a_2)$. Pokażemy przez indukcję, że $(a_i, a_{i+1}) = (a_{i+1}, a_{i+2})$. Mamy:

$$xa_i + ya_{i+1} = x(a_{i+1}q_i + a_{i+2}) + ya_{i+1} \in (a_{i+1}, a_{i+2})$$

$$ra_{i+1} + sa_{i+2} = ra_{i+1} + s(a_i - a_{i+1}qi) \in (a_i, a_{i+1})$$

co dowodzi żądą równość. Zatem $(a_1, a_2) = (a_{n-1}, a_n)$. Wszakże $a_{n-1} = a_n q_{n-1}$ i $(a_1, a_2) = (a_{n-1}, a_n) = (a_n)$, co wobec Stwierdzenia 10.12 dowodzi tezy. □

### Pierścień $\mathbb{Z}[i]$ liczb Gaussa.

Zacznijmy od ustalenia jak wyglądają elementy nierozkładalne w pierścieniu $\mathbb{Z}[i]$. Poprzedzimy je oczywistymi uwagami:

1) Elementami odwracalnymi w $\mathbb{Z}[i]$ są $1, -1. i. - i$.
1) Jeżeli $\alpha \in \mathbb{Z}[i]$ i $v(\alpha)$ jest liczbą pierwszą, to $\alpha$ jest elemetem nierozkładalnym.
2) Element $\alpha$ jest nierozkładalny wtedy i tylko wtedy, gdy nierozkładalny jest element $\bar{\alpha}$.

**11.8. Stwierdzenie.** *Element nierozkładalny dziedziny $\mathbb{Z}[i]$ jest dzielnikiem liczby całkowitej pierwszej.*

**Dowód.** Niech $\alpha \in \mathbb{Z}[i]$ będzie elementem nierozkładalnym. Wówczas $\alpha\bar{\alpha} = n$ jest rozkładem liczby całkowitej $n$ na czynniki nierozkładalne w $\mathbb{Z}[i]$. Gdyby $n$ nie było liczbą pierwszą i $n = rs$, $r, s \in \mathbb{N} \setminus \{1\}$, to rozkładając $r$ i $s$ na czynniki nierozkładalne w $\mathbb{Z}[i]$ otrzymalibyśmy inny rozkład $n$, a więc sprzeczność. □

**11.9. Stwierdzenie.** *Liczba całkowita pierwsza $p$ jest rozkładalna w pierścieniu $\mathbb{Z}[i]$ wtedy i tylko wtedy, gdy można ją przedstawić w postaci sumy kwadratów liczb całkowitych. Jeżeli $a^2 + b^2 = p$, to*

*a) $\alpha\bar{\alpha} = p$, gdzie $\alpha = a + bi$ jest jej rozkładem na czynniki nierozkładalne w pierścieniu $\mathbb{Z}[i]$;*
*b) przedstawienie $a^2 + b^2 = p$ jest jednoznaczne.*

**Dowód.** Jeżeli $p = \alpha\beta$ jest rozkładem liczby pierwszej na czynniki nierozkładalne w pierścieniu $\mathbb{Z}[i]$, to żaden z czynników tego rozkładu nie jest stowarzyszony z liczbą całkowitą. Korzystając z multyplikatywności waluacji otrzymujemy $p^2 = v(\alpha)v(\beta)$. Ponieważ $\alpha$ i $\beta$ są czynnikami nieodwracalnymi, to ich waluacje są różne od 1 i jedyną możliwością jest $v(\alpha) = v(\beta) = p$. Jeżeli $\alpha = a + bi$, to $v(\alpha) = a^2 + b^2 = p$, $a \neq 0$, $b \neq 0$.

Przedstawienie liczby $p$ w postaci $p = a^2 + b^2$, oznacza, że w pierścieniu $\mathbb{Z}[i]$, $p = \alpha\bar{\alpha}$, gdzie $\alpha = a + bi$ Oba czynniki są nierozkładalne, gdyż ich waluacja jest liczbą pierwszą. Pierścień $\mathbb{Z}[i]$ jest dziedziną z jednoznacznością rozkładu, więc rozkład $p$ jest jedyny z dokładnością do stowarzyszenia, a zatem przedstawienie $p = a^2 + b^2$ o ile istnieje to jest jedyne. □

**11.10. Wniosek.** *Elementami nierozkładalnymi pierścienia $\mathbb{Z}[i]$ są liczby całkowite pierwsze, które nie dają się przedstawić w postaci sumy dwóch kwadratów oraz liczby $a \pm bi$, gdzie $a^2 + b^2$ jest liczbą pierwszą.*

Pozostaje pytanie, jakie liczby pierwsze można przedstawić w postaci sumy kwadratów liczb całkowitych. Oczywiście $2 = 1^2 + 1^2$. Ponieważ kwadrat dowolnej liczby całkowitej przytsaje do 0 lub do 1 *mod* 4, to warunkiem koniecznym na to by takie przedstawienie istniało jest by liczba pierwsza była postaci $p = 4k + 1$, $k \in \mathbb{Z}$. To, że jest to warunek dostateczny jest treścią twierdzenia Fermata. Jego dowód poprzedzimy lematem.

**11.11. Lemat.** *Jeżeli liczba pierwsza $p \in \mathbb{N}$ jest postaci $4k + 1$, to istnieje liczba całkowita $m$, dla której $p \mid m^2 + 1$.*

**Dowód.** Przypomnijmy twierdzenie Wilsona, ktore było zastosowaniem do grupy multyplikatywnej $\mathbb{Z}_p^*$ łatwego faktu, iż w grupie przemiennej skończonej iloczyn wszystkich elementów jest równy iloczynowi elementów rzędu dwa. Twierdzenie to mówi więc, że dla liczby pierwszej $p$, $(p-1)! \equiv -1 (\mathrm{mod}\, p)$. Mamy $p-l \equiv -l (\mathrm{mod}\, p)$ i jeżeli $p = 4k+1$, to $(p-1)! \equiv (-1)^{2k}((2k)!)^2 (\mathrm{mod}\, p)$. Zatem przyjmując $m = (2k)!$ mamy $m^2 \equiv -1 (\mathrm{mod}\, p)$. □

**11.12. Twierdzenie Fermata o sumie dwóch kwadratów.** *Jeżeli $p$ jest liczbą pierwszą postaci $4k+1$, to istnieją liczby całkowite $a$ i $b$ dla których $p = a^2 + b^2$.*

**Dowód.** Wiemy, że $p \mid m^2 + 1$ dla pewnej liczby całkowitej $m$. W pierścieniu $\mathbb{Z}[i]$, $m^2 + 1 = (m+i)(m-i)$ zatem $p \mid (m+i)(m-i)$. Jest jednak jasne, że $p \nmid m+i$ i $p \nmid m-i$, zatem $p$ nie jest elementem pierwszym, czyli nierozkładalnym. Ze stwierdzenia 11.9 wynika więc, że $p$ jest sumą kwadratów dwóch liczb całkowitych i to dokładnie na jeden sposób. □

Autorzy skryptu nie mogą nie ulec pokusie, by przedstawić Państwu zupełnie inny, nie korzystający z teorii rozkładu w pierścieniu $\mathbb{Z}[i]$ tylko z teorii działań grup, dowód twierdzenia Fermata. Autorem tego nowego (sprzed kilkunastu lat) dowodu jest Don Zagier.

**Dowód.** (Don Zagier). Niech $p$ będzie liczbą pierwszą postaci $4k+1$ i niech $X = \{(x,y,z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$ . Zbiór $X$ jest oczywiście skończony i działa na nim grupa $\mathbb{Z}_2$ tak że generator odwzorowuje $(x,y,z)$ na $(x,z,y)$. Twierdzenie Fermata jest równoważne stwierdzeniu że działanie to ma punkty stałe. Na zbiorze $X$ istnieje także inne działanie grupy $\mathbb{Z}_2$. Jeżeli przez $\varphi$ oznaczymy bijekcję zdefiniowaną przez generator, to

$$\varphi(x,y,z) = \begin{cases} (x+2z, z, y-x-z), & \text{jeżeli} \quad x < y-z \\ (2y-x, y, x-y=z), & \text{jeżeli} \quad y-z < x < 2y \\ (x-2y, x-y+z, y), & \text{jeżeli} \quad x > 2y \end{cases} .$$

Proste sprawdzenie pokazuje, że to ostatnie działanie ma dokładnie jeden punkt stały i jest nim $(1,1,k)$ . Wynika z tego, że moc $X$ jest liczbą nieparzystą a zatem pierwsze działanie także musi mieć punkty stałe. □