10. Dziedziny z jednoznacznością rozkładu

W pierścieniu liczb całkowitych $\mathbb{Z}$ podstawowym twierdzeniem jest zasadnicze twierdzenie arytmetyki mówiące, że każdą liczbę całkowitą można przedstawić w postaci iloczynu liczb całkowitych pierwszych i że przedstawienie to jest jednoznaczne z dokładnością do kolejności czynników i ich znaku. Ważnym i naturalnym problemem jest pytanie dla jakich pierścieni możemy udowodnić podobne twierdzenie. Zaczniemy od wprowadzenia słownika potrzebnych pojęć. **W rozdziale tym zakładamy, że rozpatrywane pierścienie są dziedzinami całkowitości.**

10.1. Definicja. *Niech R bedzie dziedziną całkowitości.Mówimy, że:*

a) *Element $a \in R \setminus \{0\}$ dzieli element b (co oznaczamy symbolem $a|b$) wtedy i tylko wtedy gdy istnieje element c, taki że $b = ca$ lub równoważnie $(b) \subseteq (a)$.*
b) *Elementy $a, b \in R \setminus \{0\}$ są* **stowarzyszone** *(co oznaczamy symbolem $a \sim b$ tylko wtedy gdy istnieje odwracalny element $u \in R$ dla którego $a = bu$ lub równoważnie $(a) = (b)$.*
c) *Element $a \in R \setminus \{0\}$ nieodwracalny jest* **nierozkładalny** *wtedy i tylko wtedy, gdy z równości $a = bc$ wynika, że b lub c jest elementem odwracalnym lub równoważnie (a) jest elementem maksymalnym ze względu na zawieranie w zbiorze właściwych ideałów głównych.*
d) *Element $a \in R \setminus \{0\}$ nieodwracalny jest* **pierwszy** *wtedy i tylko wtedy, gdy z tego, że $a|bc$ wynika, że $a|b$ lub $a|c$ lub równoważnie ideał (a) jest niezerowym ideałem pierwszym.*

10.2. Stwierdzenie. *W dziedzinie całkowitości element pierwszy jest nierozkładalny.*

Dowód. Teza stwierdzenia jest równoważnym sformułowaniem Twierdzenia 9.21. □

Zauważmy, że w dziedzinie ideałów głównych elementy pierwsze i nierozkładalne pokrywaja się.

10.3. Stwierdzenie. *Jeżeli R jest DIG, to każdy element nierozkładalny jest pierwszy.*

Dowód. Jeżeli a jest elementem nierozkładalnym, to (a) jest elementem maksymalnym ze względu na zawieranie w zbiorze właściwych ideałów głównych, ale ten w DIG jest równy zbiorowi wszystkich właściwych ideałów, a zatem (a) jest ideałem maksymalnym. Każdy ideał maksymalny jest pierwszy, a więc a jest elementem pierwszym. □

10.4. Przykłady.

1. W pierścieniu liczb całkowitych $\mathbb{Z}$ zbiór elementów pierwszych jest równy zbiorowi elementów nierozkładalnych i składa się z liczb pierwszych.
2. Liczba 2 nie jest elementem pierwszym w pierścieniu $\mathbb{Z}[\sqrt{d}]$, dla dowolnej liczby bezkwadratowej d. Mamy bowiem $2|d(d-1) = (d+\sqrt{d})(d-\sqrt{d})$, ale $2 \nmid (d+\sqrt{d})$ i $2 \nmid (d-\sqrt{d})$.
3. Liczba 2 jest elementem nierozkładalnym w pierścieniu $\mathbb{Z}[\sqrt{-3}]$ więc pierścień ten nie jest DIG.

Sformułujmy teraz główną definicję tego rozdziału.

10.5. Definicja. *Dziedzina całkowitości R nazywa sie* **dziedziną z jednoznacznością rozkładu (DJR)** *wtedy i tylko wtedy, gdy*

a) każdy element $a \in R \setminus \{0\}$ *może być przedstawiony w postaci iloczynu*

$$a = up_1 \dots p_k,$$

gdzie u jest elementem odwracalnym, zaś $p_1, \dots, p_k$ *są elementami nierozkładalnymi.*

b) rozkład ten jest jednoznaczny z dokładnością do stowarzyszenia, to znaczy ze jeżeli $a = up_1 \dots p_k = vq_1 \dots q_l$ *są rozkładami,* u, v *są elementami odwracalnymi, zaś* $p_1, dots, p_k, q_1, \dots, q_l$ *nierozkładalnymi, to* $k = l$ *i po ewentualnym przenumerowaniu* p_i *jest stowarzyszone z* q_i*,* $1 \leq i \leq k$*.*

Grupując nierozkładalne elementy stowarzyszone możemy dowolny niezerowy element zapisać jednoznacznie (z dokładnością do kolejności i stowarzyszenia) w postaci:

$$a = up_1^{k_1} \dots p_s^{k_s},$$

gdzie p_i *nie jest stowarzyszone z* p_j*, dla* $i \neq j$*.*

Zauważmy, ze w DJR jest tak, jak w pierścieniu liczb całkowitych, to znaczy

10.6. Stwierdzenie. *Jeżeli R jest dziedzina z jednoznacznością rozkładu, to*

a) każdy element nierozkładalny jest pierwszy;

b) każdy ciąg ideałów głównych

$$(\bigstar) \qquad (a_1) \subseteq (a_2) \subseteq \dots \subseteq (a_n) \subseteq \dots$$

stabilizuje się, to znaczy że od pewnego miejsca jest stały.

Dowód.

a) Niech a będzie elementem nierozkładalnym i niech $a|bc$. Zatem $ad = bc$, dla pewnego elementu d. Elementy b, c, d przedstawiamy w postaci iloczynu czynników nierozkładalnych. Z jednoznaczności rozkładu wynika, że po prawej stronie musi znaleźć się czynnik stowarzyszony z a.

b) Dla każdego i, $(a_i) \subseteq (a_{i+1})$ oznacza, że $a_{i+1}|a_i$ a zatem czynniki nierozkładalne a_{i+1} (liczone z wielokrotnością), ponieważ są elementami pierwszymi, to są czynnikami a_i , a więc i a_1. Wynika z tego, że począwszy od pewnego miejsca rozkłady a_i oraz a_{i+1} są takie same z dokładnością do stowarzyszenia. □

Warunek ★ nazywa się **ACC dla ideałów głównych**, gdzie ACC jest skrótem od angielskiego terminu "ascending chain condition".

Na to by dana dziedzina była dziedziną z jednoznacznością rozkładu muszą być spełnione dwa warunki :

✓ każdy element daje się przedstawić w postaci iloczynu elementów nierozkładalnych;

✓ przedstawienie to jest jednoznaczne z dokładnością do stowarzyszenia i permutacji czynników.

Przyjrzyjmy się temu pierwszemu warunkowi.

10.7. Stwierdzenie. *Jeżeli dziedzina całkowitości R spełnia ACC dla ideałów głównych, to każdy element nieodwracalny jest iloczynem elementów nierozkładalnych.*

Dowód. Przypuśćmy, że $a \in R$ jest elementem, którego nie można przedstawić w postaci iloczynu elementów nierozkładanych. Wynika z tego, że a nie jest nierozkładalny i $a = bc$, gdzie b i c nie są odwracalne. Element b lub c nie jest iloczynem

elementów nierozkładalnych, gdyż w przeciwnym razie a dałoby się tak przedstawić. Powiedzmy, że b nie jest iloczynem nierozkładalnych. Kładąc $b = a_1$ mamy $(a) \subsetneqq (a_1)$. Powtarzając indukcyjnie to rozumowanie otrzymujemy nieskończony ciąg $(a)) \subsetneqq (a_1)) \subsetneqq (a_2)) \subsetneqq \dots$ wbrew założeniu. □

A teraz drugi warunek:

10.8. Stwierdzenie. *Jeżeli w dziedzinie całkowitości R każdy element nierozkładalny jest pierwszy, to przedstawienie dowolnego elementu w postaci iloczynu elementów nierozkładalnych jest jednoznaczne z dokładnością do stowarzyszenia i permutacji czynników.*

Dowód. Niech $a_1 a_2 \dots a_n = b_1 b_2 \dots b_m$ i niech a_i, $1 \geq i \geq n$ oraz b_j, $1 \geq j \geq m$ będą nierozkładalne. Dowodzimy przez indukcję ze względu na n. Będziemy korzystać z tego, że elementy $a_1, \dots a_n$ jako nierozkładalne są pierwsze. Jeżeli $n = 1$, to a_1 jako element pierwszy dzieli pewne b_j, po przenumerowaniu można założyć, że $j = 1$ i z nierozkładalności b_1 mamy $b_1 = a_1 u_1$, gdzie u_1 jest odwracalny. Po skróceniu otrzymujemy $1 = u_1 b_2 \dots b_m$. Oznacza to, że $b_2, \dots b_m$ są odwracalne, co jest sprzeczne i $m = 1$. Rozumowanie w kroku indukcyjnym jest analogiczne. □

10.9. Twierdzenie. *Dziedzina ideałów głównych jest dziedziną z jednoznacznością rozkładu.*

Dowód. Wiemy już że w DIG elementy nierozkładalne są pierwsze - Stwierdzenie 10.2. Musimy pokazać warunek ACC dla ideałów. Niech

$$(a_1) \subseteq (a_2) \subseteq \dots \subseteq (a_n) \subseteq \dots$$

będzie wstępującym ciągiem ideałów. Wówczas $\bigcup_{i=1}^{\infty}(a_i)$ jest ideałem i jest on postaci (b). Dla pewnego $i \in \mathbb{N}$, $b \in (a_i)$ i od tego miejsca ciąg musi się stabilizować. □

Największy Wspólny Dzielnik.

Wzorem pierścienia liczb całkowitych wprowadzimy definicję.

10.10. Definicja. *Niech R bedzie dziedziną całkowitości i niech $\emptyset \neq A \subset R$. Powiemy, że element $d \in R$ jest największym wspólnym dzielnikiem (oznaczamy go symbolem NWD(A)) jeżeli*

a) dla każdego $x \in A$, $d|x$,

b) jeżeli $e|x$ dla każdego $x \in A$, to $e|d$.

Jeżeli NWD$(A) = 1$*, to mówimy że zbiór A jest względnie pierwszy.*

Zauważmy, ze z definicji wynika natychmiast, że jeżeli $NWD(A)$ istnieje, to jest wyznaczony jednoznacznie z dokładnością do stowarzyszenia.

10.11. Przykład. Nie istnieje $NWD(4, 2 + 2\sqrt{-3})$.

W szkole podstawowej znajdowało się największy wspólny dzielnik podzbioru A zbioru licz całkowitych w ten sposób, że należało rozłożyć wszystkie liczby ze zbioru A na czynniki pierwsze i największy wspólny dzielnik był iloczynem tych (z uwzględnieniem krotności), które występują w każdej liczbie ze zbioru A. Dokładnie to samo rozumowanie prowadzi do dowodu następującego faktu.

10.12. Stwierdzenie. *W każdej dziedzinie z jednoznacznością rozkładu istnieje* NWD(A)*, dla dowolnego niepustego podzbioru $A \subset R$.*

10.13. Stwierdzenie. *Jeżeli R jest dziedziną ideałów głównych, to $d = NWD(A)$, $\emptyset \neq A \subset R$ wtedy i tylko wtedy, gdy $(A) = (d)$.*

Dowód. Równość $(d) = (A)$ zachodzi wtedy i tylko wtedy, gdy po pierwsze $A \subset (d)$ i po drugie (d) jest najmniejszym ideałem zawierającym A, czyli jeżeli $A \subseteq (e)$, to $(d) \subseteq (e)$. Pierwszy z tych warunków jest równoważny temu, że dla każdego $x \in A$, $d|x$, Drugi temu, że jeżeli $e|x$ dla każdego $x \in A$, to $e|d$. □

10.14. Wniosek. *Jeżeli w dziedzinie ideałów głównych elementy a i b są względnie pierwsze, to istnieją elementy k i l, dla których $ak + bl = 1$*

10.15. Przykład. Zauważmy, że w powyższym stwierdzeniu założenie, że R jest dziedziną ideałów głównych jest istotne. W pierścieniu $\mathbb{Z}[X]$, $NWD(X, 3) = 1$, ale $(3, X) \neq \mathbb{Z}[X]$.

Wróćmy jeszcze do chińskiego twierdzenia o resztach.

Niech R będzie DIG a $I \trianglelefteq R$ ideałem. Wówczas $I = (x)$ i element x ma rozkład $x = a_1^{k_1} \cdot \ldots a_n^{k_n}$, gdzie elementy a_i są nierozkładalne i nie stowarzyszone. Wynika z tego, ze :

ideały $I_i = (a_i^{k_i})$ oraz $I_j = (a_j^{k_j})$ są względnie pierwsze dla $i \neq j$,

$I = I_1 \cap \cdots \cap I_n$.

Zatem stosując twierdzenie chińskie o resztach otrzymujemy następujący wniosek:

10.16. Wniosek. *Niech R będzie dziedziną ideałów głównych, $(x) \trianglelefteq R$ ideałem, oraz $x = a_1^{k_1} \cdot \ldots a_n^{k_n}$, gdzie elementy a_i są nierozkładalne i nie stowarzyszone. Wówczas*

$$R/(x) \cong R/(a_1^{k_1}) \times \cdots \times R/(a_n^{k_n}).$$

10.17. Przykład. Czy pierścienie $\mathbb{Q}[X]/((X-1)(X+1))$ oraz $\mathbb{Q}[X]/((X-3)X)$ są izomorficzne?

Mamy:

$$\mathbb{Q}[X]/((X-1)(X+1)) \cong \mathbb{Q}[X]/(X+1) \times \mathbb{Q}[X]/(X-1) \cong \mathbb{Q} \times \mathbb{Q}$$

i analogicznie

$$\mathbb{Q}[X]/((X-3)X) \cong \mathbb{Q}[X]/(X-3) \times \mathbb{Q}[X]/(X) \cong \mathbb{Q} \times \mathbb{Q},$$

a więc są izomorficzne.