Algebra I

Wykład VIII

Grzegorz Bobiński (UMK)

Założenie

Przez cały podrozdział R jest dziedziną całkowitości.

Definicja

Mówimy, że $r \in R$ dzieli $s \in R$ (piszemy $r \mid s$), jeśli istnieje $t \in R$ taki, że $s = t \cdot r$.

Uwaga

Relacja $\mid$ jest zwrotna i przechodnia.

Definicja

Mówimy, że $r, s \in R$ są stowarzyszone (piszemy $r \approx s$), jeśli $r \mid s$ i $s \mid r$.

Przypomnienie

Przypomnijmy, że $r \in R$ nazywamy odwracalnym (piszemy $r \in R^\times$), jeśli istnieje $s \in R$ taki, że $r \cdot s = 1$.

Przykłady

(1) $\mathbb{Z}^\times = \{1, -1\}$.

(2) $(R[X])^\times = R^\times$. (R dziedzina)

Stwierdzenie 2.9

(1) $r \mid s \iff (s) \subseteq (r) \iff s \in (r)$.

(2) $r \approx s \iff (r) = (s)$.

(3) r jest elementem odwracalnym $\iff r \mid 1$.

(4) r jest elementem odwracalnym $\iff \forall_{s \in R}\ r \mid s$.

(5) r jest elementem odwracalnym $\iff (r) = R$.

(6) $\approx$ jest relacją równoważności.

(7) $r \approx s \iff$ istnieje $u \in R^{\times}$ takie, że $r = u \cdot s$.

Przypomnienie

(2.3): $(a) = \{t \cdot a : t \in R\}$.

Dowód

(1): $r \mid s \overset{\text{def.}}{\iff}$ istnieje $t \in R$ takie, że $s = t \cdot r \overset{(2.3)}{\iff} s \in (r) \overset{\text{def.}}{\iff} (s) \subseteq (r)$.

(2): $r \approx s \overset{\text{def.}}{\iff} r \mid s$ i $s \mid r \overset{(1)}{\iff} (r) \subseteq (s)$ i $(s) \subseteq (r) \iff (r) = (s)$.

(6): Natychmiast z (2).

(3): r jest odwracalny $\overset{\text{def.}}{\iff}$ istnieje $s \in R$ taki, że $s \cdot r = 1 \overset{\text{def.}}{\iff} r \mid 1$.

(4): $\Leftarrow$: Natychmiast z (3).

$\Rightarrow$: r jest odwracalny $\overset{(3)}{\Longrightarrow} r \mid 1 \overset{1 \mid s}{\Longrightarrow} r \mid s$.

(5): r jest odwracalny $\overset{(3)}{\iff} r \mid 1 \overset{(1)}{\iff} (r) \supseteq (1) = R \iff (r) = R$.

Stwierdzenie 2.9

(7) $r \approx s \iff$ istnieje $u \in R^\times$ takie, że $r = u \cdot s$.

Dowód

$\Rightarrow$: $r \approx s \overset{\text{def.}}{\Longrightarrow} r \mid s$ i $s \mid r \overset{\text{def.}}{\Longrightarrow}$ istnieją $u, v \in R$ takie, że $r = u \cdot s$ i $s = v \cdot r$.

1°. $s = 0$.

Wtedy

$$r = u \cdot s = u \cdot 0 = 0 = 1 \cdot 0 = 1 \cdot s.$$

2°. $s \neq 0$.

Mamy $s = (v \cdot u) \cdot s$.

(2.4) $\Longrightarrow v \cdot u = 1 \overset{\text{def.}}{\Longrightarrow} u \in R^\times$.

$\Leftarrow$: Załóżmy, że $r = u \cdot s$ dla $u \in R^\times$.

Wtedy oczywiście $s \mid r$.

$u \in R^\times \overset{\text{def.}}{\Longrightarrow}$ istnieje $v \in R$ taki, że $v \cdot u = 1$.

Wtedy

$$s = 1 \cdot s = v \cdot u \cdot s = v \cdot r,$$

więc $r \mid s$. $\square$

Definicja

$r \in R$ nazywamy nierozkładalnym, jeśli

- $r \neq 0$,
- $r \notin R^\times$,
- $s \mid r \implies s \approx r \text{ lub } s \in R^\times$.

Stwierdzenie 2.10

(1) $r \in R$ jest nierozkładalny wtedy i tylko wtedy, gdy (r) jest niezerowym maksymalnym ideałem głównym, tzn.

- $r \neq 0$;
- $(r) \neq R$;
- $(r) \subseteq (s) \implies (s) = (r) \text{ lub } (s) = R$.

(2) Element stowarzyszony z elementem nierozkładalnym jest nierozkładalny.

Dowód

Na mocy 2.9(5): $(r) \neq R \iff r \notin R^\times$.
Ponadto na mocy 2.9(1,2,5) zdania:

$$s \mid r \implies s \approx r \text{ lub } s \in R^\times$$

i

$$(r) \subseteq (s) \implies (s) = (r) \text{ lub } (s) = R.$$

są równoważne. □

Definicja

R nazywamy dziedziną z rozkładem, jeśli dla każdego $r \in R \setminus (\{0\} \cup R^\times)$ istnieją elementy nierozkładalne $r_1, \ldots, r_n \in R$ takie, że

$$r = r_1 \cdots r_n.$$

Definicja

R nazywamy dziedziną z jednoznacznością rozkładu (UFD), jeśli R jest dziedziną z rozkładem i dla dowolnych nierozkładalnych $r_1, \ldots, r_n, s_1, \ldots, s_m \in R$ takich, że

$$r_1 \cdots r_n = s_1 \cdots s_m,$$

mamy $n = m$ oraz istnieje $\sigma \in S_n$ taka, że $r_i \approx s_{\sigma(i)}$ dla każdego i.

Przykłady

(1) Pierścień $\mathbb{Z}$ jest UFD.

(2) Niech $R := \{a + bi\sqrt{3} : a, b \in \mathbb{Z}\}$.

Wtedy $R \leq \mathbb{C}$.

Ponadto R jest dziedziną z rozkładem, która nie jest UFD.

Istotnie, 2 i $1 \pm i\sqrt{3}$ są elementami nierozkładalnymi oraz $2 \cdot 2 = (1 + i\sqrt{3}) \cdot (1 - i\sqrt{3})$, ale $2 \not\approx 1 \pm i\sqrt{3}$.

Definicja

$r \in R$ nazywamy pierwszym, jeśli

- $r \neq 0$,
- $r \notin R^{\times}$,
- $r \mid s_1 \cdot s_2 \implies r \mid s_1$ lub $r \mid s_2$.

Stwierdzenie 2.11

(1) $r \in R$ jest pierwszy $\iff$ $r \neq 0$ i (r) jest pierwszy.

(2) Element stowarzyszony z elementem pierwszym jest pierwszy.

Przypomnienie

(def): $I \leq R$ jest pierwszy : $\iff$ $I \neq R$ i $(s_1 \cdot s_2 \in I \implies s_1 \in I$ lub $s_2 \in I)$.

Dowód

Z 2.9(1) zdania

$$r \mid s_1 \cdot s_2 \implies r \mid s_1 \text{ lub } r \mid s_2$$

i

$$s_1 \cdot s_2 \in (r) \implies s_1 \in (r) \text{ lub } s_2 \in (r)$$

są równoważne. □

Twierdzenie 2.12

Dziedzina z rozkładem jest UFD $\iff$ każdy element nierozkładalny jest pierwszy.

Dowód

$\Rightarrow$: Załóżmy, że R jest UFD.

Ustalmy element nierozkładalny $r \in R$.

Przypuśćmy, że $r \mid s_1 \cdot s_2$ dla $s_1, s_2 \in R$.

1°. $s_1 = 0$.

Wtedy $r \mid s_1$.

2°. $s_2 = 0$ – analogicznie.

3°. $s_1 \in R^\times$.

Wtedy $r \mid s_1 \cdot s_2 \approx s_2$, więc $r \mid s_2$.

4°. $s_2 \in R^\times$ – analogicznie.

Twierdzenie 2.12

Dziedzina z rozkładem jest UFD $\iff$ każdy element nierozkładalny jest pierwszy.

Dowód (c.d.)

$\Rightarrow$: $r \mid s_1 \cdot s_2$ dla $s_1, s_2 \in R$.

5°. $s_1, s_2 \notin \{0\} \cup R^\times$.

Istnieją elementy nierozkładalne $q_1, \ldots, q_m$ takie, że

$$s_1 = q_1 \cdots q_l \qquad \text{i} \qquad s_2 = q_{l+1} \cdots q_m, \ 0 < l < m.$$

Wiemy, że istnieje $t \in R$ taki, że $r \cdot t = s_1 \cdot s_2$.

5.0. $t = 0$.

Niemożliwe, bo wtedy $0 = r \cdot t = s_1 \cdot s_2 \neq 0$.

5.1. $t \in R^\times$.

$r \cdot t \approx r \implies r \cdot t$ jest nierozkładalny.

To jest niemożliwe, gdyż

$$(r \cdot t) = q_1 \cdots q_m,$$

$m \geq 2$ i R jest UFD

5.2. $t \notin \{0\} \cup R^\times$.

Istnieją elementy nierozkładalne $p_1, \ldots, p_n$ takie, że

$$t = p_1 \cdots p_n.$$

Wtedy

$$r \cdot p_1 \cdots p_n = q_1 \cdots q_m.$$

R jest UDF $\implies$ istnieje i takie, że $r \approx q_i$.

Jeśli $i \leq l$, to $r \mid s_1$, w przeciwnym wypadku $r \mid s_2$.

Twierdzenie 2.12

Dziedzina z rozkładem jest UFD $\iff$ każdy element nierozkładalny jest pierwszy.

Dowód (c.d.)

$\Leftarrow$: Załóżmy, że każdy element nierozkładalny w R jest pierwszy.

Pokażemy przez indukcję na $\min\{m, n\}$, że jeśli $r_1, \ldots, r_n, s_1, \ldots, s_m$ są nierozkładalne i

$$r_1 \cdots r_n \approx s_1 \cdots s_m,$$

to $n = m$ oraz istnieje permutacja σ zbioru $\{1, \ldots, n\}$ taka, że $r_i \approx s_{\sigma(i)}$ dla każdego $i = 1, \ldots, n$.

Bez straty ogólności $\min\{m, n\} = n$.

0°. $n = 0$.

Wtedy $r_1 \cdots r_n = 1$.

Gdyby $m > 0$, to s_1 byłby odwracalny, sprzeczność.

1°. $n > 0$. Wtedy $m \geq n > 0$.

Zauważmy, że $r_n \mid s_1 \cdots s_m$.

Ponieważ element r_n jest pierwszy, zatem istnieje $j \in \{1, \ldots, m\}$ takie, że $r_n \mid s_j$.

Bez straty ogólności możemy założyć, że $j = m$.

Ponieważ $r_n \notin R^\times$ i s_m jest nierozkładalny, więc $r_n \approx s_m$.

Twierdzenie 2.12

Dziedzina z rozkładem jest UFD $\iff$ każdy element nierozkładalny jest pierwszy.

Dowód (c.d.)

$\Leftarrow$: Załóżmy, że każdy element nierozkładalny w R jest pierwszy.

Pokażemy przez indukcję na $\min\{m, n\}$, że jeśli $r_1, \ldots, r_n, s_1, \ldots, s_m$ są nierozkładalne i

$$r_1 \cdots r_n \approx s_1 \cdots s_m,$$

to $n = m$ oraz istnieje permutacja σ zbioru $\{1, \ldots, n\}$ taka, że $r_i \approx s_{\sigma(i)}$ dla każdego $i = 1, \ldots, n$.

1°. $n > 0$. Wiemy, że $m > 0$ i $r_n \approx s_m$.

Istnieją $u, v \in R^\times$ takie, że $s_m = u \cdot r_n$ i

$$r_1 \cdots r_{n-1} \cdot r_n = s_1 \cdots s_{m-1} \cdot s_m \cdot v.$$

Wtedy

$$r_1 \cdots r_{n-1} \cdot r_n = s_1 \cdots s_{m-1} \cdot r_n \cdot u \cdot v.$$

więc

$$r_1 \cdots r_{n-1} = s_1 \cdots s_{m-1} \cdot u \cdot v,$$

zatem

$$r_1 \cdots r_{n-1} \approx s_1 \cdots s_{m-1}.$$

Z założenia indukcyjnego $n - 1 = m - 1$ oraz istnieje permutacja σ zbioru $\{1, \ldots, m-1\}$ taka, że $r_i \approx s_{\sigma(i)}$ dla każdego $i = 1, \ldots, n-1$. $\square$

Stwierdzenie 2.13

(1) Każdy element pierwszy jest nierozkładalny.

(2) Jeśli R jest PID, to każdy element nierozkładalny jest pierwszy.

Przypomnienie

(2.7): Każdy ideał maksymalny jest pierwszy.

Dowód

(2): r jest nierozkładalny $\overset{(2.10)(1)}{\iff}$ (r) jest niezerowy maksymalny główny $\overset{R \text{ PID}}{\iff}$ (r) jest niezerowy maksymalny $\overset{(2.7)}{\implies}$ (r) jest niezerowy pierwszy $\overset{(2.11)(1)}{\iff}$ r jest pierwszy.

(1): Ustalmy $r \in R$ pierwszy.

Załóżmy, że $s \mid r$.

Wtedy $r = s \cdot t$ dla pewnego $t \in R$ (zauważmy, że $t \neq 0$, gdyż $r \neq 0$).

W szczególności $r \mid s \cdot t$.

Stąd $r \mid s$ lub $r \mid t$.

1°. $r \mid s$

Wtedy $r \approx s$.

2°. $r \mid t$

Wtedy $r \approx t$, więc $r = u \cdot t$ dla pewnego $u \in R^\times$.

Wtedy $s \cdot t = u \cdot t$, więc $s = u \in R^\times$. $\square$

Lemat 2.14

Niech R będzie PID.

Jeśli $r_0, r_1, \ldots$ są elementami R takimi, że $r_{i+1} \mid r_i$ dla każdego $i \in \mathbb{N}$, to istnieje $n \in \mathbb{N}$ takie, że $r_{i+1} \approx r_i$ dla każdego $i \geq n$.

Dowód

Dla każdego $i \in \mathbb{N}$ niech $I_i := (r_i)$.

Wtedy $I_i \subseteq I_{i+1}$.

Niech $I := \bigcup_{i \in \mathbb{N}} I_i$.

Wtedy $I \trianglelefteq R$. (!)

Istnieje $r \in R$ taki, że $I = (r)$.

Istnieje $n \in \mathbb{N}$ takie, że $r \in I_n$.

Wtedy dla $i \geq n$ otrzymujemy, że $r \in I_i$, więc

$$I = (r) \subseteq I_i \subseteq I_{i+1} \subseteq I,$$

skąd $I_i = I_{i+1}$, a więc $r_i \approx r_{i+1}$. $\square$

Stwierdzenie 2.15

Każda PID jest dziedziną z rozkładem.

Lemat 2.14

Niech R będzie PID.

Jeśli $r_0, r_1, \ldots$ są elementami R takimi, że $r_{i+1} \mid r_i$ dla każdego $i \in \mathbb{N}$, to istnieje $n \in \mathbb{N}$ takie, że $r_{i+1} \approx r_i$ dla każdego $i \geq n$.

Dowód

Niech R będzie PID.

Niech X będzie zbiorem tych $r \in R$, że

- $r \neq 0$,
- $r \notin R^\times$,
- nie istnieją elementy nierozkładalne $r_1, \ldots, r_n$ takie, że $r = r_1 \cdots r_n$.

Musimy pokazać, że $X = \varnothing$.

Pokażemy za chwilę, że istnieje $\tau \colon X \to X$ taka, że $\tau(r) \mid r$ i $\tau(r) \not\approx r$ dla każdego $r \in X$.

Załóżmy, że $X \neq \varnothing$ i wybierzmy $r_0 \in X$.

Definiujemy $r_1, r_2, \ldots$, wzorem

$$r_i := \tau^i(r_0) \qquad (i \in \mathbb{N}_+).$$

Wtedy $r_{i+1} \mid r_i$ oraz $r_{i+1} \not\approx r_i$ dla każdego $i \in \mathbb{N}$, co jest sprzeczne z (2.14).

Stwierdzenie 2.15

Każda PID jest dziedziną z rozkładem.

Dowód (c.d.)

Niech X jest zbiorem tych $r \in R$, że

- $r \neq 0$,
- $r \notin R^\times$,
- nie istnieją elementy nierozkładalne $r_1, \ldots, r_n$ takie, że $r = r_1 \cdot \cdots \cdot r_n$.

Pokażemy, że istnieje $\tau \colon X \to X$ taka, że $\tau(r) \mid r$ i $\tau(r) \not\approx r$ dla każdego $r \in X$.

Ustalmy $r \in X$.

Wtedy $r \neq 0$, r nie jest odwracalny i r nie jest nierozkładalny.

Wtedy istnieje $s \in R$ takie, że $s \not\approx r$, $s \notin R^\times$ i $s \mid r$.

Z definicji istnieje $t \in R$ taki, że $r = s \cdot t$.

Wtedy

- $s \neq 0 \neq t$ (gdyż $r \neq 0$),
- $s \notin R^\times$ (z założenia) i $t \notin R^\times$ (gdyż $s \not\approx r$),

Ponieważ $r \in X$, więc $s \in X$ lub $t \in X$.

Ponadto

- $s \mid r$ i $t \mid r$ (gdyż $r = s \cdot t$),
- $s \not\approx r$ (z założenia) i $t \not\approx r$ (gdyż $s \notin R^\times$).

Jeśli $s \in X$, to $\tau(r) := s$, w przeciwnym wypadku $\tau(r) := t$. $\square$

Twierdzenie 2.12

Dziedzina z rozkładem jest UFD $\iff$ każdy element nierozkładalny jest pierwszy.

Stwierdzenie 2.15

Jeśli R jest PID, to R jest dziedziną z rozkładem.

Stwierdzenie 2.13

(2) Jeśli R jest PID, to każdy element nierozkładalny jest pierwszy.

Wniosek 2.16

PID $\implies$ UFD. $\square$