Algebra I

Wykład VII

Grzegorz Bobiński (UMK)

2 Teoria podzielności w pierścieniach

Umowa

W tym rozdziale badamy pierścienie.

2.1 Ideały

Lemat 2.1

Jeśli $I_j \trianglelefteq R$, $j \in J$, to $\bigcap_{j\in J} I_j \trianglelefteq R$.

Dowód

Ćwiczenie. □

Stwierdzenie 2.2/Definicja/Oznaczenie

Jeśli $X \subseteq R$, to istnieje najmniejszy ideał pierścienia R zawierający zbiór X.
Ten ideał nazywamy ideałem generowanym przez zbiór X oraz oznaczamy (X).

Dowód

Ćwiczenie. □

Oznaczenie

$(r_1, \ldots, r_n) := (\{r_1, \ldots, r_n\})$.

Stwierdzenie 2.3

Jeśli $r_1, \ldots, r_n \in R$, to

$$(r_1, \ldots, r_n) = \{s_1 \cdot r_1 + \cdots + s_n \cdot r_n : s_1, \ldots, s_n \in R\}.$$

W szczególności,

$$(r) = \{s \cdot r : s \in R\}.$$

Dowód

Ćwiczenie. □

Definicja

Ideał $I \trianglelefteq R$ nazywamy głównym, jeśli istnieje $r \in R$ taki, że $I = (r)$.

Pierścień, w którym każdy ideał jest główny, nazywamy pierścieniem ideałów głównych.

Definicja

Pierścień R nazywamy dziedziną (całkowitości), jeśli $0 \neq 1$ oraz z równości $r \cdot s = 0$ wynika, że $r = 0$ lub $s = 0$.

Pierścień ideałów głównych, który jest dziedziną całkowitości, nazywamy dziedziną ideałów głównych (PID).

Przykłady

(0) Każde ciało jest dziedziną.

(1) $\mathbb{Z}$ jest dziedziną.

(2) $R[X]$ jest dziedziną $\iff$ R jest dziedziną.

(3) $\mathbb{Z}_n$ jest dziedziną $\iff$ $n \in \mathbb{P}$.

(4) Jeśli $|R| < \infty$, to R jest dziedziną wtedy i tylko wtedy, gdy R jest ciałem.

Stwierdzenie 2.4

Jeśli R jest dziedziną, $r, s_1, s_2 \in R$ oraz $r \neq 0$ i $r \cdot s_1 = r \cdot s_2$, to $s_1 = s_2$.

Dowód

Mamy

$$r \cdot s_1 = r \cdot s_2 \implies r \cdot (s_1 - s_2) = 0 \implies s_1 - s_2 = 0 \implies s_1 = s_2. \quad \square$$

Definicja

Ideał $I \trianglelefteq R$ nazywamy pierwszym, jeśli $I \neq R$ oraz z warunku $r \cdot s \in I$ wynika, że $r \in I$ lub $s \in I$.

Stwierdzenie 2.5

Ideał $I \trianglelefteq R$ jest pierwszy wtedy i tylko wtedy, gdy R/I jest dziedziną.

Dowód

Mamy

$$0_{R/I} = 1_{R/I} \iff [0]_{\sim_I} = [1]_{\sim_I} \iff 0 \sim_I 1 \iff 1 \in [0]_{\sim_I} = 0 + I = I$$
$$\iff (1) \subseteq I \iff I \supseteq \{r \cdot 1 : r \in R\} = R \iff I = R.$$

Ponadto

$$(r + I) \cdot (s + I) = 0 + I \iff r \cdot s + I = 0 + I \iff r \cdot s \in I.$$

Podobnie

$$r + I = 0 + I \iff r \in I \quad \text{i} \quad s + I = 0 + I \iff s \in I.$$

Zatem zdania

$$(r + I) \cdot (s + I) = 0 + I \implies r + I = 0 + I \text{ lub } s + I = 0 + I$$

i

$$r \cdot s \in I \implies r \in I \text{ lub } s \in I$$

są równoważne. □

Definicja

Ideał I pierścienia R nazywamy maksymalnym, jeśli $I \neq R$ i z inkluzji $I \subseteq J$, gdzie $J \trianglelefteq R$, wynika, że $J = I$ lub $J = R$.

Stwierdzenie 2.6

Ideał $I \trianglelefteq R$ jest maksymalny wtedy i tylko wtedy, gdy R/I jest ciałem.

Dowód

$\Rightarrow$: Załóżmy, że I jest maksymalny.
Ustalmy $r \in R$ taki, że $r + I \neq 0 + I$.
Wtedy $r \notin I$.
Niech $J := I + (r)$.
Wtedy $J \trianglelefteq R$(!), $I \subseteq J$ i $J \neq I$ (bo $r \in J \setminus I$).
Stąd $J = R$.
W szczególności istnieją $t \in I$ oraz $s \in R$ takie, że $t + s \cdot r = 1$.
Wtedy

$$(s + I) \cdot (r + I) = 1 + I.$$

$\Leftarrow$: Załóżmy, że R/I jest ciałem.
Ustalmy $J \trianglelefteq R$ taki, że $I \subseteq J$ i $J \neq I$.
Wybierzmy $r \in J \setminus I$.
Wtedy istnieje $s \in R$ taki, że $s \cdot r + I = 1 + I$.
Zatem $1 = s \cdot r + t$ dla pewnego $t \in I$, wiec $1 \in J$, gdyż $r \in J$ i $I \subseteq J$.
Stąd wynika, że $1 \in J$, więc $J = R$. $\square$

Stwierdzenie 2.5

Ideał $I \trianglelefteq R$ jest pierwszy wtedy i tylko wtedy, gdy R/I jest dziedziną.

Stwierdzenie 2.6

Ideał $I \trianglelefteq R$ jest maksymalny wtedy i tylko wtedy, gdy R/I jest ciałem.

Przykład

Jeśli $n \in \mathbb{N}_+$, to $n\mathbb{Z}$ jest maksymalny wtedy i tylko wtedy, gdy $n \in \mathbb{P}$, i wtedy i tylko wtedy, gdy $n\mathbb{Z}$ jest pierwszy.

Wniosek 2.7

Każdy ideał maksymalny jest pierwszy. □

Twierdzenie 2.8 (Chińskie Twierdzenie o Resztach)

Niech $I_1, \ldots, I_n \trianglelefteq R$.
Załóżmy, że

$$\forall_{i \neq j}\ I_i + I_j = R.$$

Wtedy funkcja $R/(I_1 \cap \ldots \cap I_n) \to R/I_1 \times \cdots \times R/I_n$ dana wzorem

$$r + I_1 \cap \ldots \cap I_n \mapsto (r + I_1, \ldots, r + I_n) \qquad (r \in R),$$

jest izomorfizmem pierścieni.

Przykład

Niech $R = \mathbb{Z}$ oraz $I_k := m_k\mathbb{Z}$, $m_k > 0$, $k = 1, \ldots, n$.
Wtedy

$$I_i + I_j = R \iff \mathrm{NWD}(m_i, m_j) = 1.$$

Ponadto,

$$I_1 \cap \ldots \cap I_n = (\mathrm{NWW}(m_1, \ldots, m_n)).$$

Zauważmy, że przy założeniu $\mathrm{NWD}(m_i, m_j) = 1$ dla wszystkich $i \neq j$,

$$\mathrm{NWW}(m_1, \ldots, m_n) = m_1 \cdots m_n.$$

Twierdzenie 2.8 (Chińskie Twierdzenie o Resztach)

Jeśli $\forall_{i \neq j}\ I_i + I_j = R$, to funkcja $R/(I_1 \cap \ldots \cap I_n) \to R/I_1 \times \cdots \times R/I_n$ dana wzorem

$$r + I_1 \cap \ldots \cap I_n \mapsto (r + I_1, \ldots, r + I_n) \qquad (r \in R),$$

jest izomorfizmem pierścieni.

Przypomnienie – I Twierdzenie o Izomorfizmie

$R/\operatorname{Ker}\varphi \simeq \operatorname{Im}\varphi$.

Dowód

Definiujemy homomorfizm $\varphi\colon R \to R/I_1 \times \cdots \times R/I_n$ wzorem

$$\varphi(r) := (r + I_1, \ldots, r + I_n) \qquad (r \in R).$$

Wtedy $\operatorname{Ker}\varphi = I_1 \cap \ldots \cap I_n$.

Wobec I Twierdzenia o Izomorfizmie wystarczy pokazać, że φ jest epimorfizmem.

Ustalmy elementy $t_2, \ldots, t_n \in I_1$ oraz $s_2 \in I_2, \ldots, s_n \in I_n$ takie, że

$$t_2 + s_2 = \cdots = t_n + s_n = 1.$$

Jeśli $e_1 := s_2 \cdots s_n$, to

$$e_1 + I_1 = 1 + I_1,\ e_1 + I_2 = 0 + I_2, \ldots, e_1 + I_n = 0 + I_n.$$

Podobnie pokazujemy, że istnieją $e_2, \ldots, e_n \in R$ takie, że

$$e_i + I_i = 1 + I_i,\ e_i + I_j = 0 + I_j,\ j \neq i.$$

Załóżmy, że $r_1, \ldots, r_n \in R$.

Wtedy

$$\varphi(r_1 \cdot e_1 + \cdots + r_n \cdot e_n) = (r_1 + I_1, \ldots, r_n + I_n).$$

Stąd φ jest epimorfizmem, co kończy dowód. □