Algebra I

Wykład X

Grzegorz Bobiński (UMK)

Założenie

Przez cały podrozdział R jest dziedziną całkowitości.

Definicja

Niech $r, s \in R$.

Element d dziedziny R nazywamy największym wspólnym dzielnikiem (nwd) elementów r i s, jeśli:

(1) $d \mid r$ i $d \mid s$;

(2) jeśli $c \mid r$ i $c \mid s$, to $c \mid d$.

Lemat 2.22

Niech d będzie nwd elementów r i s dziedziny R.

Jeśli $d' \in R$, to

$$d' \text{ jest nwd elementów } r \text{ i } s \iff d' \approx d.$$

Dowód

Jeśli d' jest nwd elementów r i s, to korzystając z definicji nwd, otrzymujemy łatwo, że $d \mid d'$ i $d' \mid d$, więc $d' \approx d$.

Z drugiej strony, gdy $d' \approx d$, to $d' \mid d$, więc $d' \mid r$ i $d' \mid s$.

Ponadto, jeśli $c \mid r$ i $c \mid s$, to $c \mid d$, a więc również $c \mid d'$, gdyż $d \mid d'$. $\square$

Przykład

Niech

$$R := \{a + b\imath\sqrt{3} : a, b \in \mathbb{Z}\}.$$

Wtedy nie istnieje nwd liczb $2 + 2\imath\sqrt{3}$ oraz 4.

Istotnie:

- Wspólnymi dzielnikami są
$$\pm 1, \qquad \pm 2, \qquad \pm 1 \pm \imath\sqrt{3}.$$
- Zauważmy, że jeśli $u \mid v$, to $|u|^2 || v|^2$.

  W szczególności, jeśli u jest nwd, to $|u| \geq |v|$ dla wszystkich wspólnych dzielników v.

  Ponadto, jeśli $|u| = |v|$ i $v \mid u$, to $v \approx u$.
- Z powyższych własności wynika, że gdyby istniał nwd, to
$$\pm 2 \approx \pm 1 \pm \imath\sqrt{3}.$$
  Ponieważ $R^\times = \{\pm 1\}$, to prowadzi do sprzeczności.

Lemat 2.23

Niech R będzie UFD.

Niech $p_1, \ldots, p_n$ będą elementami nierozkładalnymi dziedziny R takimi, że $p_i \not\approx p_j$ dla $i \neq j$.

Jeśli $l_1, \ldots, l_n, k_1, \ldots, k_n \in \mathbb{N}$, to

$$p_1^{l_1} \cdots p_n^{l_n} \mid p_1^{k_1} \cdots p_n^{k_n}$$

wtedy i tylko wtedy, gdy $l_i \leq k_i$ dla każdego i.

Dowód

Ćwiczenie. □

Stwierdzenie 2.24

Jeśli R jest UFD, to dla dowolnych elementów r i s istnieje nwd.

Dowód

Jeśli $r = 0$, to s jest nwd r i s.

Jeśli $r \in R^\times$, to r (lub 1) jest nwd r i s.

Załóżmy, że $r, s \notin R^\times \cup \{0\}$.

Istnieją elementy nierozkładalne $p_1, \ldots, p_n$, $u, v \in R^\times$ oraz $l_1, \ldots, l_n, k_1, \ldots, k_n \in \mathbb{N}$ takie, że $p_i \not\approx p_j$ dla $i \neq j$,

$$r = u p_1^{k_1} \cdots p_n^{k_n} \qquad \text{i} \qquad s = v p_1^{l_1} \cdots p_n^{l_n}.$$

Wtedy $d := p_1^{\min(k_1, l_1)} \cdots p_n^{\min(k_n, l_n)}$ jest nwd r i s. □

Uwaga

W $\mathbb{Z}$ nwd jest wyznaczony z dokładnością do znaku.

Zwykle wybiera się liczbę nieujemną.

Jeśli F jest ciałem, to nwd w $F[X]$ jest wyznaczony z dokładnością do niezerowego skalara.

Z wyjątkiem sytuacji, gdy nwd jest równe 0, to jako nwd wybieramy wielomian, który przy najwyższej potędze ma współczynnik równy 1 (takie wielomiany nazywa się unormowanymi lub monicznymi).

Stwierdzenie 2.25

Jeśli R jest PID, to dla dowolnych $r, s \in R$ istnieją $x, y \in R$ takie, że $x \cdot r + y \cdot s$ jest nwd elementów r i s.

Dowód

Łatwo sprawdzić, że $(r) + (s) \trianglelefteq R$.

Ponieważ R jest PID, więc istnieje d taki, że $(d) = (r) + (s)$.

Wtedy d jest nwd elementów r i s oraz istnieją $x, y \in R$ takie, że $d = x \cdot r + y \cdot s$. □

Uwaga

Jeśli R jest dziedziną Euklidesa, to nwd oraz elementy x i y można znaleźć, korzystając z (rozszerzonego) algorytmu Euklidesa.

Definicja

Niech $r, s \in R$.

Element t dziedziny R nazywamy najmniejszą wspólną wielokrotnością (nww) elementów r i s dziedziny R, jeśli:

(1) $r \mid t$ i $s \mid t$;

(2) jeśli $r \mid t'$ i $s \mid t'$, to $t \mid t'$.

Lemat 2.26

Niech t będzie nww elementów r i s dziedziny R.

Jeśli $t' \in R$, to

$$t' \text{ jest nww elementów } r \text{ i } s \iff t' \approx t.$$

Dowód

Ćwiczenie. □

Przykład

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

Wtedy istnieje nwd 2 i $1 + i\sqrt{3}$ (1 spełnia warunki nwd), ale nie istnieje ich nww.

Istotnie, 4 i $2 + 2i\sqrt{3}$ są dwiema wspólnymi wielokrotnościami, która nie mają wspólnego dzielnika, który byłby wspólną wielokrotnością wyjściowych liczb.

Stwierdzenie 2.27

Jeśli istnieje nww t elementów r i s, to istnieje nwd d elementów r i s oraz $t \cdot d \approx r \cdot s$.

Dowód

Jeśli $r = 0$, to teza jest oczywista ($t = 0$ i $d = s$).

Załóżmy, że $r \neq 0 \neq s$.

Ponieważ $r \mid r \cdot s$ i $s \mid r \cdot s$, więc $t \mid r \cdot s$.

W szczególności $t \neq 0$ (gdyż $r \cdot s \neq 0$) oraz istnieje d taki, że $t \cdot d = r \cdot s$.

Pokażemy, że d jest nwd r i s.

Najpierw pokażemy, że $d \mid r, s$.

Ponieważ $r \mid t$, więc istnieje s' taki, że $r \cdot s' = t$.

Wtedy

$$r \cdot s' \cdot d = t \cdot d = r \cdot s,$$

więc $s = s' \cdot d$, zatem $d \mid s$.

Podobnie $d \mid r$.

Pokażemy teraz, że jeśli $c \mid r$ i $c \mid s$, to $c \mid d$.

Istnieją s'' i r'' takie, że $r = c \cdot r''$ i $s = c \cdot s''$.

Wtedy $c \cdot r'' \cdot s''$ jest wspólną wielokrotnością r i s, a więc $t \mid c \cdot r'' \cdot s''$, skąd istnieje d' taki, że $t \cdot d' = c \cdot r'' \cdot s''$.

Zauważmy, że

$$t \cdot d = r \cdot s = c^2 \cdot r'' \cdot s'' = c \cdot t \cdot d',$$

skąd $d = c \cdot d'$, a więc $c \mid d$. □

Stwierdzenie 2.28

Jeśli dla dowolnych dwóch elementów dziedziny R istnieje ich nwd, to dla dowolnych dwóch elementów dziedziny R istnieje ich nww.

Dowód

Ustalmy $r, s \in R$.
Gdy $r = 0$, to teza jest oczywista (nww jest równe 0).
Załóżmy zatem, że $r \neq 0 \neq s$.
Niech d będzie ich nwd.
Wtedy $r = d \cdot r'$ i $s = d \cdot s'$ dla pewnych $r', s' \in R$.
Zauważmy, że nwd r' i s' jest 1.
Pokażemy, że $t := d \cdot r' \cdot s'$ jest nww r i s.
Oczywiście $r \mid t$ i $s \mid t$.
Przypuśćmy, że $r \mid t'$ i $s \mid t'$ dla pewnego $t' \in R$.
Niech d' będzie nwd t i t'.
Istnieje c taki, że $t = d' \cdot c$.
Ponieważ $r \mid t$ i $r \mid t'$, więc $r \mid d'$, zatem istnieje s'' takie, że $d' = r \cdot s''$.
Analogicznie istnieje r'' takie, że $d' = s \cdot r''$.
Wtedy

$$r \cdot s' = d \cdot r' \cdot s' = t = d' \cdot c = r \cdot s'' \cdot c,$$

więc $s' = s'' \cdot c$, tzn. $c \mid s'$.
Podobnie $c \mid r'$, więc $c \in R^\times$.
Stąd t jest nwd t i t', a więc w szczególności $t \mid t'$. $\square$

Stwierdzenie 2.28

Jeśli dla dowolnych dwóch elementów dziedziny R istnieje ich nwd, to dla dowolnych dwóch elementów dziedziny R istnieje ich nww.

Stwierdzenie 2.24

Jeśli R jest UFD, to dla dowolnych elementów r i s istnieje nwd.

Wniosek 2.29

Jeśli R jest UFD, to dla dowolnych dwóch elementów dziedziny R istnieje ich nww.

Dowód

(2.28) + (2.24). □