Wykład 11.

Wn. 11.2 Jeśli R: dziedzina noetherowska, w której każdy element nierozkładalny jest pierwszy, to R: UFD

Wn. 11.3. R: PID $\Rightarrow$ R: UFD.

D-d Niech $p \in R$: nierozkładalny. Cel: p: pierwszy.

Zał, że $p | ab$ $\quad (p, a) = (c)$, $(p, b) = (d)$ dla pewnych $c, d \in R$

$$c | p \Rightarrow c \in R^* \text{ lub } c \sim p$$

$$\Downarrow \qquad\qquad \Downarrow$$

$$\boxed{c \sim 1} \qquad p | c \text{ i } c | a \Rightarrow p | a \text{ OK!}$$

?

Gdy $c \sim 1$, to $1 \in (p, a)$

$$1 = px + ay \; / \cdot b$$ dla pewnych $x, y \in R$

$$b = pxb + aby$$

$$p | \;\; \& \;\; p | \;\; \Rightarrow p | b \quad \square$$

Wn. 11.4 Każdy pierścień euklidesowy jest UFD.

Czyli: $\mathbb{Z}$, $\mathbb{Z}[i]$, $K[X]$ ...

Def. 11.5. R: dziedzina, $a, b, d \in R$.

(1) d jest NWD(a, b), gdy:

(a) $d | a$ i $d | b$ $\quad$ (b) Jeśli $d_1 | a$ i $d_1 | b$, to $d_1 | d$.

(2) a i b są względnie pierwsze, gdy
1 jest $NWD(a,b)$.

Fakt 11.6) Zał, że $a \sim a'$, $b \sim b'$, $d \sim d'$. Wtedy
d jest $NWD(a,b) \iff d'$ jest $NWD(a',b')$

TW. 11.7. Zał, że R: UFD; $a, b \in R$, $a \neq 0$ lub $b \neq 0$.
Wtedy istnieje $d \in R$ t. że d: $NWD(a,b)$.

D-d $a = p_1^{l_1} \cdots p_n^{l_n}$, $b = c \cdot p_1^{k_1} \cdots p_n^{k_n}$, p_i nierozkładalne
$c \in R^*$, $l_i, k_i \geq 1$

Niech $t_i = \min\{l_i, k_i\}$
$$d = p_1^{t_1} \cdots p_n^{t_n} : NWD(a,b)$$
Podobna definicja $NWD(a_1, \ldots, a_k)$.
Fakt 11.6 i tw. 11.7 pozostają wtedy słuszne (warianty)

TW. 11.8. Niech d : $NWD(a_1, \ldots, a_k)$, $a_i = d \cdot a_i'$.
Wtedy 1 : $NWD(a_1', \ldots, a_k')$.

TW. 11.9. Zał, że R: PID. Wtedy d : NWD $\iff$
$(d) = (a, b)$.

D-d

$\Leftarrow$ $\underbrace{d = ax + by}_{\text{bo } d \in (a,b)}$, $d|a$, $d|b$ bo $a, b \in (d)$

Jeśli $d_1|a$ i $d_1|b$, to $\Rightarrow$ $d_1|d$.

$\Rightarrow$ Niech d_1 t. że $(a,b) = (d_1)$. Niech d: NWD(a,b)

$d_1 = ax + by$, $d_1|a$, $d_1|b$ $\Rightarrow$ $d_1|d$ i $d|d_1$

d_1: NWD(a,b).

$(d) = (d_1)$.

Def. 11.10. R: dziedzina, $a, b, d \in R$, d: NWW(a,b), gdy:

(a) $a|d$ i $b|d$, (b) Jeśli $a|d_1$ i $b|d_1$, to $d|d_1$.

Fakt 11.11: odpowiednik faktu 11.6 dla NWW

TW. 11.12: odpowiednik tw. 11.7 dla NWW +

$$a \cdot b \sim \text{NWD}(a,b) \cdot \text{NWW}(a,b)$$

(gdy $a \neq 0$ lub $b \neq 0$)

Ciało ułamków.

Przykład $\mathbb{Z} \subseteq \mathbb{Q} = \{ \frac{m}{n} : m, n \in \mathbb{Z},\ n \neq 0 \}$

$\mathbb{Q}$ ciało ułamków pierścienia $\mathbb{Z}$.

Uwaga 12.1. Zał., że $R \subseteq K$, podpierścień, ciało. Wtedy

(1) R: dziedzina.

(2) Niech $R_0 = \{ \frac{m}{n} : m, n \in R,\ n \neq 0 \}$. Wtedy R_0: podciało ciała K generowane przez R.

tu: $\frac{m}{n} = m \cdot n^{-1}$.

D-d. (1) oczywiste

(2) proste sprawdzenie. Np. zamkniętość na $+$:

$$\frac{m_1}{n_1} + \frac{m_2}{n_2} = \frac{m_1 n_2 + m_2 n_1}{n_1 n_2}. \qquad \square$$

W sytuacji z Uwagi 12.1:

dla $\langle m, n\rangle \in R \times (R \setminus \{0\})$

$\langle m', n'\rangle$

z $\frac{m}{n} = \frac{m'}{n'} \iff mn' = m'n$.

Uwaga 12.2. Niech R: dziedzina.
Wtedy relacja $\sim$ na $R \times (R \setminus \{0\})$ dana przez:

$$\langle n, m \rangle \sim \langle n', m' \rangle \Leftrightarrow nm' = n'm$$

jest relacją równoważności.

D-d ćw.

Ciało ułamków dziedziny R:

$R_0 = R \times (R \setminus \{0\})/_\sim$ z działaniami:

$$\frac{n}{m} \cdot \frac{n'}{m'} = \frac{nn'}{mm'}, \quad \frac{n}{m} + \frac{n'}{m'} = \frac{nm' + n'm}{mm'},$$

gdzie $\frac{n}{m} = \langle n, m \rangle/_\sim$

Zapis $\frac{n}{m}$: ułamek o liczniku n i mianowniku m.

Def. 12.3. (1) $(R_0, +, \cdot)$ ciało ułamków dziedziny R.

(2) $R \hookrightarrow R_0$ monomorfizm przełączeni.
$n \longrightarrow \frac{n}{1}$ Utożsamiamy n z $\frac{n}{1}$:
R podpierścień ciała R_0.

Uwaga (1) $R_0 = \{\frac{n}{m} : n, m \overset{0}{\neq} \in R\}$.
$\uparrow$ liczone w R_0 $\quad \overset{\cap}{R_0}$

(2) Ciało R_0 z uwagi 12.2 to ciało ułamków R.
(z dokł. do $\cong_R$)

AI 11

Przykłady.

1. $K \rightsquigarrow K[X] \rightsquigarrow K[X]_0 \overset{\text{ozn.}}{=} K(X)$

K ciało, $K[X]$ dziedzina, $K[X]_0$ ciało ułamków, $K(X)$ ciało funkcji wymiernych zmiennej X nad ciałem K.

funkcja wymierna
(wyrażenie wymierne)

$$f(X) = \frac{W(X)}{V(X)}, \quad W(X), \overset{\neq 0}{V(X)} \in K[X]$$

Podobnie: $K(X_1, \dots, X_n) = K[X_1, \dots, X_n]_0$

2. Ciało szeregów Laurenta:

$$K((X)) = \left\{ \sum_{n=k}^{\infty} a_n X^n : k \in \mathbb{Z}, a_n \in K \right\}$$

+ i $\cdot$ ~~pod~~ jak poprzednio dla $K[\![X]\!]$.

$K[\![X]\!] \subseteq K((X)) \leftarrow$ ciało, bo:

podpierścień

$$0 \neq W(X) = \sum_{n=k}^{\infty} a_n X^n, \text{ bso } a_k \neq 0$$

$$W(X) = X^k \underbrace{\left(\sum_{n=0}^{\infty} a_{n+k} X^n \right)}_{V(X) \in K[\![X]\!]^*}$$

$$W(X)^{-1} = X^{-k} \cdot V^{-1}(X)$$

$\cancel{A}$ • $K((X))$: ciało ułamków pierścienia
$K[\![X]\!]$

Analogicznie:
$K((X_1,\dots,X_k))$: ciało ułamków pierścienia
$K[\![X_1,\dots,X_k]\!]$.

TW. 12.4 (Gauss).
Jeśli R: UFD, to $R[X]$: UFD.

Def. ① Niech $0 \neq f = a_n X^n + \dots + a_1 X + a_0 \in R[X]$ i
R:UFD
$c \in R$, c: NWD$(a_1,\dots,a_n)$.
c nazywamy zawartością wielomianu f
$c = c(f)$.

② f: pierwotny, gdy $1 = c(f)$.

Lemat Gaussa. 12.5. (R: UFD)
Zał., że $f, g \in R[X]$, $\neq 0$. Wtedy $c(f)\cdot c(g)$ jest zawartością $f \cdot g$.

<u>D-d</u>. $f = c(f)\cdot f'$, $g = c(g)\cdot g'$, f', g' pierwotne.
$fg = c(f)c(g) f'g'$.

Wystarczy pokazać, że $f' \cdot g'$: pierwotny.

Jeśli nie, to istnieje p: nierozkładalny, t.że
$\underset{R}{\overset{\uparrow}{p}}$

$p \mid$ wszystkie współczynniki $f' \cdot g'$.

$j : R \longrightarrow R/(p)$ ilorazowe, $R/(p)$ dziedzina

$\Downarrow$ $\varphi : R[X] \longrightarrow R/(p)[X]$ epimorfizm pierścieni.

$\Downarrow$ $R/(p)[X]$

$\varphi(f'), \varphi(g') \neq 0$, ale

$\varphi(f') \cdot \varphi(g') = \varphi(f' \cdot g') = 0$ $\Downarrow$ dziedzina

Lemat 12,6 (R: ~~Dziedzina~~ UFD)
Zał, że $0 \neq f \in R[X] \setminus (\{0\} \cup R[X]^*)$.
Wtedy f jest i.e.n. w $R[X]$.
D-d, Indukcja względem $\deg f$.
1. $\deg f = 0$ $f = a \in R$, $a = a_1 \dots a_r$ i.e.n. w R
$\Downarrow$
w $R[X]$

2, zał, że $\deg f = k > 0$ i teza zachodzi dla wielomianów stopnia $< k$.

$f = c(f) \cdot f'$
$c(f) = c_1 \cdots c_N$ i. e. n.

Jeśli f' nierozkładalny, to koniec

Jeśli f' rozkładalny, to

$$f' = g_1 g_2 \quad , \quad g_1, g_2 \notin R[X]^*.$$

Wtedy $\deg g_1, \deg g_2 > 0$

(bo jeśli $\deg g_i = 0$, to g_i: stała $\notin R^*$, co przeczy temu, że f': pierwotny.

Stąd: $\deg g_i < \deg f$,

więc g_1, g_2 są i. e. n. $\Rightarrow$ f też.

Lemat 12.7 (Gauss, Lemat Gaussa) (R: UFD)
Niech $K = R_0$: ciało ułamków R. Zał., że $f \in R[X]$ nierozkładalny, $\deg f > 0$. Wtedy f nierozkładalny w $K[X] \supseteq R[X]$.

<u>D-d</u>. Zał., że $\underbrace{f = f_1 \cdot f_2}_{\text{rozkład właściwy}}$, $f_1, f_2 \in K[X]$, $\deg f_i > 0$.

f nierozkładalny w $R[X]$ $\Rightarrow$ f pierwotny.

$$f_1 = \frac{a_1}{b_1} \cdot f_1' , \quad f_2 = \frac{a_2}{b_2} \cdot f_2' , \quad f_1', f_2' \in R[X]$$

pierwotne,

<u>stąd</u>

$$f^\# = b_1 b_2 f = a_1 a_2 \underbrace{f_1' f_2'}$$

pierwotny z lematu 12,6.

$\Downarrow$

$a_1 a_2$ i $b_1 b_2$ to wspólna zawartość $f^\#$

<u>więc</u> $a_1 a_2 \sim b_1 b_2$ w R

$$a_1 a_2 = \underset{\substack{\cap \\ R^*}}{\varepsilon} b_1 b_2 \Rightarrow f = \varepsilon \cdot f_1' f_2' \text{ rozkład } y. \text{ w } R[X]$$

<u>D-d</u> tw. 12.3 (Gaussa) Cel: $R[X]$: UFD.

- R: dziedzina: OK.
- ~~ka~~ każdy $f \in R[X] \setminus (\{0\} \cup R[X]^*)$ jest i.e.n. OK. (12.6).

jednoznaczność rozkładu:

Zał, że $\underset{\forall}{R[X]^*}$

$$0 \neq f = a_1 \ldots a_r f_1 \ldots f_s = b_1 \ldots b_n f_1' \ldots f_k'$$

$\deg a_i = \deg b_j = 0$

$\deg f_h , \deg f_l' > 0 \Rightarrow f_h , f_l'$: pierwotne, Stąd: $a_1 \cdot \ldots \cdot a_r$, $b_1 \cdot \ldots \cdot b_n$: zawartość f

$$\Downarrow$$

$$a_1 \cdot \ldots \cdot a_r \sim b_1 \ldots b_n$$

$$\Downarrow R : UFD$$

$a_1, \ldots, a_r$, $b_1, \ldots, b_n$ "takie same"

$$\underset{\substack{\uparrow \\ R^*}}{a_1 \ldots a_r = \varepsilon\, b_1 \ldots b_n} \Rightarrow$$

$$\underbrace{f_1 \ldots f_s}_{\substack{\uparrow \\ \text{i.e.n.}}} = \underbrace{\varepsilon f_1' \ldots f_k'}_{\text{w } K[X]}$$

R_0 " równość w $K[X]$ (też)

$K[X]$: UFD (bo euklidesowy)

(lemat 12.7)

$s = k$ i rozkłady $f_1 \ldots f_s$, $f_1' \ldots f_k'$ "takie same".

w $K[X]$!

tzn, po przenumerowaniu:

$$f_i \sim f_i' \text{ w } K[X],$$
$$i = 1, \ldots, s.$$

$$\boxed{\text{Cel: } f_i \sim f_i' \text{ w } R[X]}$$

$f_i = \frac{c_i}{d_i} f_i'$, $c_i, d_i \in R$, $d_i \neq 0$

$$\Downarrow$$

$d_i f_i = c_i f_i' \Longrightarrow c_i \sim d_i \Rightarrow \frac{c_i}{d_i} \in R^*$ i $f_i \sim f_i'$ w $R[X]$.

f_i, f_i' : pierwotne

AII, 14

Wn. 12.7. K ciało $\Rightarrow K[X_1, \dots, X_n]$: UFD.

Przykłady

1. $K = \mathbb{C}$ ← algebraicznie domknięte.

wielomiany nierozkładalne w $\mathbb{C}[X]$: $\deg = 1$ (liniowe)

2. $K = \mathbb{R}$

$f \in \mathbb{R}[X]$ nierozkładalny $\Leftrightarrow \begin{cases} \deg f = 1 \\ \text{lub} \\ \deg f = 2 \text{ i } \Delta_f < 0 \end{cases}$ (bez pierwiastków rzeczywistych)

D-d.

Zał, że $f \in \mathbb{R}[X]$ nierozkładalny.

Niech $a \in \mathbb{C}$ pierwiastek f. Stąd (tw. Bezouta) $(X-a) \mid f$ w $\mathbb{C}[X]$.

- Jeśli $a \in \mathbb{R}$, to $(X-a) \mid f$ w $\mathbb{R}[X]$ i $f \sim (X-a)$ i f liniowy ✓
- Jeśli $a \in \mathbb{C} \setminus \mathbb{R}$, to $a \neq \bar{a}$ i $\bar{a}$ też pierwiastek f (ćw.), więc $(X-a), (X-\bar{a}) \mid f$ w $\mathbb{C}[X]$

nierozkładalne, $\not\sim$ w $\mathbb{C}[X] \Rightarrow$

$(X-a)(X-\bar{a}) \mid f$ w $\mathbb{C}[X]$

$\mathbb{R}[X] \Rightarrow \mid f$ w $\mathbb{R}[X]$

Stąd $\underbrace{(X-a)(X-\bar{a})}_{\substack{\text{nierozkładalny} \\ \text{w } \mathbb{R}[X]}} \sim f$ i $\deg f = 2$.

Kryterium Eisensteina. 12,9.

Zał, że R: PID, $K = R_0$, $f = \overset{\neq 0}{a_n} X^n + \ldots + a_0 \in R[X]$

p nierozkładalny, $p \mid a_0, \ldots, p \mid a_{n-1}$, $p^2 \nmid a_0, p \nmid a_n$.

$\overset{\uparrow}{R}$ Wtedy f: nierozkładalny w $K[X]$.

Jeśli f pierwotny, to f nierozkładalny w $R[X]$.

D-d Z lematu 12,7 wystarczy pokazać drugą część.

nie wprost.

Zał, że $f = f_1 \cdot f_2$ $f_i \in R[X]$ nieodwracalne (pierwotny)

$n > \deg f_i > 0$.

Niech $\varphi : R[X] \xrightarrow[\text{epi}]{} R/(p)[X]$ indukowany przez

$j : R \xrightarrow[\text{ilorazowe}]{} R/(p)$

$$\varphi(f) = \varphi(a_n) \cdot X^n = \varphi(f_1) \cdot \varphi(f_2)$$

$R/(p)$ dziedzina, nawet ciało, bo R: PID,

$\Downarrow$

$R/(p)[X]$: UFD.

Stąd $\varphi(f_1) = b \cdot X^m$

$\varphi(f_2) = c \cdot X^{n-m}$ dla pewnych $b, c \in R/(p)$

i $1 \leq m < n$.

Stąd współczynniki

f_1 i f_2 przy X^0 są podzielne przez p, więc

$p^2 \mid a_0$ $\lightning$.

Przykład. 1°. p: l. pierwsza, $n > 0 \Rightarrow X^n - p$ nierozkładalny w $\mathbb{Q}[X]$

2°. K ciało

$X_2^n - X_1 \in K[X_1][X_2] = K[X_1, X_2]$ nierozkładalny.