Wykład 10.

R : pierścień przemienny z 1

TW. 10.1 (tw. Hilberta o bazie).

R : noetherowski $\Longrightarrow$ $R[X]$ noetherowski.

D-d Niech $I \triangleleft R[X]$.

dla $n \geqslant 0$ niech $I_n = \{a \in R : (\exists\, a_{n-1}, \ldots, a_0 \in R)$
$aX^n + a_{n-1}X^{n-1} + \ldots + a_0 \in I\}$

więc: $I_0 = I \cap R$.
$(n=0)$

- $I_n \triangleleft R$ oraz $I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$, bo:

$I_n \subseteq I_{n+1}$:
$(aX^n + \ldots) \in I \Rightarrow X \cdot (aX^n + \ldots) = (aX^{n+1} + \ldots) \in I$

R noetherowski, więc:
Istnieje m t. że $I_m = I_{m+1} = I_{m+2} = \ldots$
oraz $I_0, I_1, \ldots, I_m$: skończenie generowane

tzn: $I_0 = (a_{0,1}, \ldots, a_{0,k_0}), \ldots, I_m = (a_{m,1}, \ldots, a_{m,k_m})$
dla pewnych $a_{i,j} \in R$

$a_{i,j} \rightsquigarrow \underset{\substack{\parallel \\ (a_{i,j}X^i + \ldots)}}{f_{i,j}} \in I$, $f_{0,j} = a_{0,j}$.

Niech $J = (f_{i,j} : 0 \leq i \leq m,\ 1 \leq j \leq k_i)$

- $I = J$

$\supseteq$: jasne

$\subseteq$: Niech $0 \neq f \in I$. Pok., że $\underline{f \in J}$.

Indukcja wzgl. $\deg f$.

1. $\deg f = 0 \Rightarrow f \in R \Rightarrow f \in I_0 = I \cap R \subseteq J$.

2. Krok indukcyjny.

Zał., że $\deg f = k > 0$ i $[\underbrace{(\forall g \in I)(\deg g < k \Rightarrow g \in J)}_{\text{Zał. indukcyjne.}}]$.

$f = aX^k + \ldots$, $a \in I_k$

2 przypadki:

(a) $\underline{\underline{k \le m}}$. Wtedy $a \in I_k = (a_{k,1}, \ldots, a_{k,l_k})$

$$\Rightarrow a = \sum_t \underset{\overset{\cap}{R}}{b_t}\, a_{k,t}$$

$J \ni \sum_t b_t f_{k,t} = (aX^k + \ldots)$, więc:

$$\deg(\underbrace{f - \sum_t b_t f_{k,t}}_{\overset{\cap}{I} \ \underset{\text{zał. indukc.}}{\Longrightarrow} \ \overset{\cap}{J}}) < k.$$

$$\text{Stąd } f = \underbrace{\left(f - \sum_t b_t f_{k,t}\right)}_{\overset{\cap}{J}} + \underbrace{\sum_t b_t f_{k,t}}_{\overset{\cap}{J}} \in J.$$

(b) $\underline{\underline{k > m}}$. Wtedy

$$a \in I_k = I_m = (a_{m,1}, \ldots, a_{m,l_m}) \Rightarrow a = \sum_t \overset{\overset{R}{\cup}}{b_t}\, a_{m,t}$$

$$X^{k-m}\left(\sum_t b_{m,t} f_{m,t}\right) = \left(aX^k + \ldots\right)$$

dalej jak poprzednio.

Wn. 10.2.
Jeśli K ciało, to pierścień $K[X_1, \ldots, X_n]$ jest noetherowski.

D-d Indukcja wzgl. n.

$$K[X_1, \ldots, X_{n+1}] = (K[X_1, \ldots, X_n])[X_{n+1}]$$

K noetherowski, bo ideały K to $\{0\}$ i K.

Def. 10.3.
Pierścień przemienny $R \ni 1 \neq 0$ jest dziedziną (domain, integral) dziedzina całkowitości), gdy nie ma w nim dzielników zera.

Def. 10.4. Zał, że R: dziedzina.

(1) $\delta : R \longrightarrow \mathbb{N} \cup \{-\infty\}$ jest normą euklidesową w R, gdy:

(a) $\delta(x) = -\infty \iff x = 0$

(b) $\forall a, \underset{\neq 0}{b} \in R \; \exists q, r \in R \; (a = bq + r \wedge \delta(r) < \delta(b))$

[dzielenie z resztą].

(2) R: pierścień euklidesowy, gdy
R: dziedzina i istnieje $\delta : R \longrightarrow \mathbb{N} \cup \{-\infty\}$ norma euklidesowa.

Przykłady pierścieni euklidesowych.

1. $\mathbb{Z}$ $\quad \delta(n) = \begin{cases} -\infty, & \text{gdy } n = 0 \\ |n|, & \text{gdy } n \neq 0 \end{cases}$

2. $K[X]$: $\delta(f) = \deg f$

   ciało

3. $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$

   pierścień Gaussa $\qquad$ podpierścień

$$\delta(a+bi) = \begin{cases} -\infty, & \text{gdy } a+bi = 0 \\ a^2+b^2, & \text{gdy } a+bi \neq 0 \end{cases}$$

$$a^2+b^2 = |a+bi|^2$$

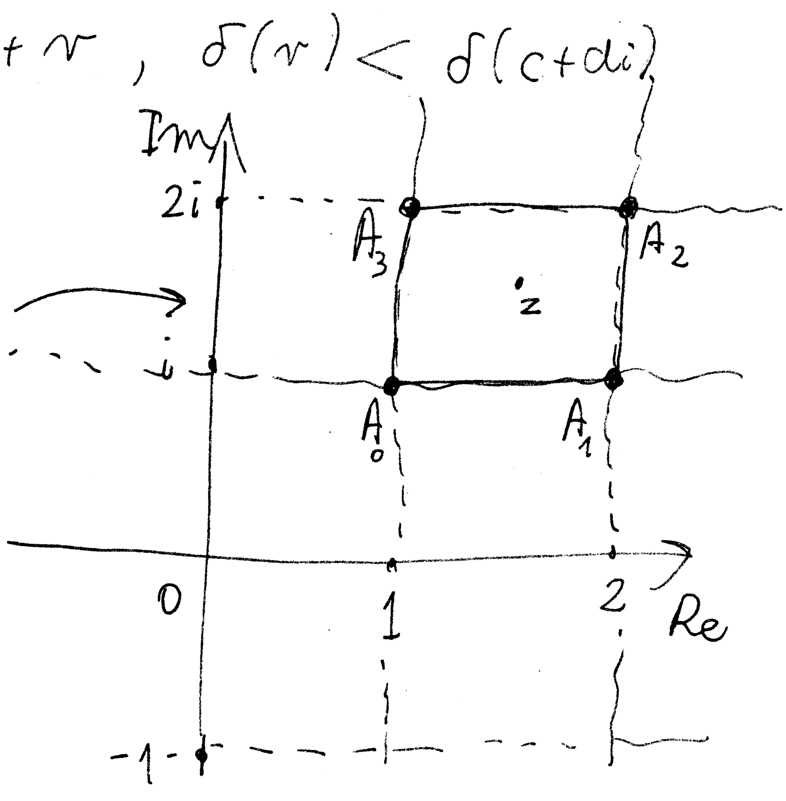
δ: norma euklidesowa, bo:

Niech $a+bi$, $\underbrace{c+di}_{\neq 0} \in \mathbb{Z}[i]$. Szukamy $q, r \in \mathbb{Z}[i]$

t. że $a+bi = q(c+di) + r$, $\delta(r) < \delta(c+di)$

Niech $z = \dfrac{a+bi}{c+di} \in \mathbb{C}$

krata całkowita



• Niech $j \in \{0, 1, 2, 3\}$ t. że

$$|A_j - z| < 1$$

[niejednoznaczność!]

$$(a+bi) = z\,(c+di)$$

$$\underbrace{(a+bi)}_{\mathbb{Z}[i]} = \underbrace{A_j\,(c+di)}_{\mathbb{Z}[i]} + \underbrace{r}_{\mathbb{Z}[i]} \qquad \Rightarrow \qquad \Downarrow$$

$\delta(r)$:
$$0 \le \frac{|r|}{|c+di|} = \left|\frac{a+bi}{c+di} - A_j\right| = |z - A_j| < 1$$

wsc
$$\frac{|r|^2}{|c+di|^2} < 1 \Rightarrow \delta(r) < \delta(c+di).$$

(d) K : ciało $\Rightarrow$ K dziedzina euklidesowa (bo w ciele $K^* = K \setminus \{0\}$)

Uwaga 10.5 W pierścieniu euklidesowym każdy ideał jest główny. Pierścień euklidesowy jest <u>dziedziną ideałów głównych</u> (PID : principal ideal domain)

<u>D-d</u> Niech $I \triangleleft R \leftarrow$ euklidesowy. BSO $I \neq \{0\}$

δ : norma euklidesowa w R.

Niech $0 \neq b \in I$ t. że $\delta(b)$: minimalna.

- $I = (b)$. <u>bo</u>: $\supseteq$: jasne

$$\subseteq:\ \underbrace{a}_{I} = \underbrace{q\cdot b}_{I} + \underbrace{r}_{I}, \quad q, r \in R, \quad \delta(r) < \delta(b)$$

$\Downarrow$ wybór b

$r = 0$, wsc $a = q\cdot b \in (b)$.

<u>Przykład</u> $K[X_1, X_2]$ jest dziedziną noetherowską, ale nie jest PID, więc nie jest pierścieniem euklidesowym.

Różne rodzaje ideałów: R: p. przemienny z $1 \neq 0$.

Def. 10.6.

(a) $I \underset{\neq}{\lhd} R$ jest <u>pierwszy</u>, gdy $(\forall a, b \in R)(ab \in I \Rightarrow a \in I \vee b \in I)$

(b) $a \in R \setminus \{0\}$ jest <u>pierwszy</u>, gdy (a) jest pierwszy

$[$tzn. $(\forall b, c \in R)(a \mid bc \Rightarrow a \mid b \vee a \mid c)]$

Uwaga 10.7.
Niech $I \underset{\neq}{\lhd} R$. Wtedy I jest pierwszy $\Leftrightarrow R/I$: dziedzina

<u>D-d</u> zad. z listy.

Def 10.8. $I \underset{\neq}{\lhd} R$ jest <u>maksymalny</u>, gdy

$\neg \exists J \underset{\neq}{\lhd} R \quad I \subsetneq J$.

Uwaga 10.9. Niech $I \underset{\neq}{\lhd} R$. Wtedy I: maksymalny $\Leftrightarrow$ R/I: ciało

<u>D-d</u> Niech $j : R \longrightarrow R/I$: ilorazowe.

$\Leftarrow$ Zał. że R/I : ciało.

Nie wprost. Zał, że I nie jest maksymalny.

Wtedy istnieje $J \lhd R$ t. że $I \subsetneq J \subsetneq R$.

Wtedy $j[J] \lhd R/I$ i $\{0\} \neq j[J] \neq R/I$

bo $I \subsetneq J$

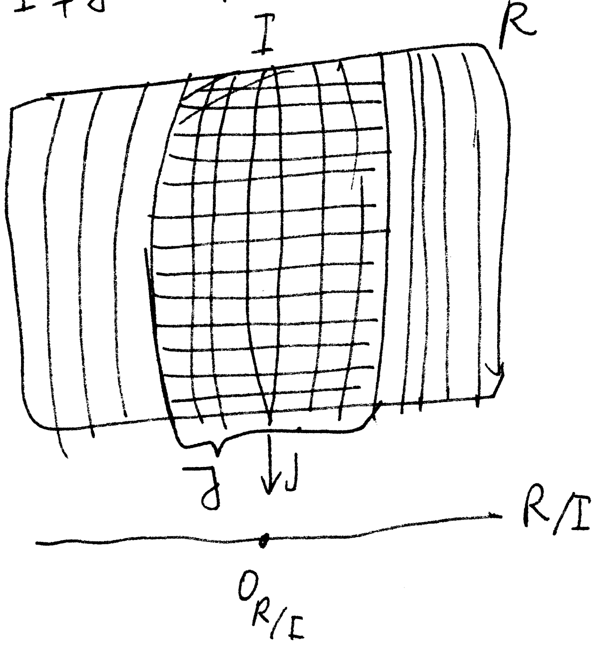
J : suma warstw I

$\Downarrow$

$\emptyset \neq R \setminus J$: suma warstw I

$\Downarrow$

j nie jest "na".



Ale w ciele R/I jedyne ideały to $\{0_{R/I}\}$ i R/I ↯.

$\Rightarrow$ Zał, że $a/I = \underset{\neq 0_{R/I}}{a+I} \in R/I$. Cel: a/I : odwracalne w R/I.

<u>d-d</u> nie wprost.

Zał, że a/I nie jest odwracalne w R/I.

Wtedy $\{0_{R/I}\} \neq (a/I) \underset{\neq}{\lhd} R/I$.

Niech $J = j^{-1}[(a/I)]$. Wtedy $I \subsetneq J \subsetneq R$ i $J \lhd R$ ↯

Wn. 10.10. $I \lhd R$ maksymalny $\Rightarrow$ I pierwszy

(bo: ciało R/I jest dziedziną).

Przykład w $\mathbb{Z}$: Niech $\{0\} \neq I \trianglelefteq_{\neq} \mathbb{Z}$.

Wtedy I: maksymalny $\iff$ I pierwszy $\iff$ $I = (p)$ dla pewnej p: l. pierwszej.

D-d Niech $I = (n)$, $n > 1$.

- jeśli n: l. pierwsza, to
  $\mathbb{Z}/I \cong \mathbb{Z}_n$: ciało, więc I maksymalny i pierwszy.
- jeśli n: l. złożona, to
  $\mathbb{Z}/I \cong \mathbb{Z}_n$ nie jest dziedzina, więc I nie jest pierwszy i nie jest maksymalny.

Fakt 10.11.
Jeśli R: dziedzina ideałów głównych, oraz $\{0\} \neq I \trianglelefteq_{\neq} R$ pierwszy, to I maksymalny.

D-d.
Zał, że $I = (a)$ pierwszy, $a \neq 0$. Zał. nie wprost, że I nie jest maksymalny, tzn. istnieje $J \trianglelefteq R$ t. że $I \subsetneq J \subsetneq R$.

$J = (b)$, $b \notin I$, $a \in J$ $\Rightarrow$ $b \mid a$, $a \nmid b$

$b \mid a \Rightarrow a = b \cdot c \in I$

$\Downarrow$ I pierwszy, $b \notin I$

$c \in I. \Rightarrow c = d \cdot a$ dla pewnego $d \in R$

$$a = b \cdot c = bda \Rightarrow \underset{\neq 0}{a}(1-bd) = 0$$
$$\Downarrow$$
$$1 - bd = 0$$
$$\Downarrow$$
$$bd = 1 \Rightarrow 1 \in J \ \& \ J = R \ \lightning.$$

Uwaga 10.12.

Jeśli $I \underset{\neq}{\triangleleft} R$, to istnieje $J \underset{\neq}{\triangleleft} R$ t.że $I \subseteq J$ i J maksymalny

D-d zad. z listy.

Podzielność w dziedzinach.

Niech $\underset{a}{R} \ni$: dziedzina.

$$\left.\begin{array}{l} a = b \cdot c \\ a = a_1 \cdot \ldots \cdot a_n \\ \quad n \geq 2 \end{array}\right] \begin{array}{l} \text{rozkłady } a \text{ w } R \\ a_i, b, c \in R. \end{array}$$

rozkład a jest właściwy, gdy żaden czynnik nie jest odwracalny.

Przykład w $\mathbb{Z}$:

$3 = (-1) \cdot (-3)$ rozkład niewłaściwy.

Def. 10.13. $a \in R \setminus (\{0\} \cup R^*)$ jest nierozkładalny, gdy nie ma rozkładu właściwego.

tzn: $(\forall b, c \in R)(a = b \cdot c \Rightarrow b$ lub c jest odwracalny$)$

Uwaga 10.14. (1) a pierwszy $\Rightarrow$ a nierozkładalny

(2) a nierozkładalny i $b \sim a \Rightarrow b$ nierozkładalny

D-d. Ćwiczenie.

Tw. 10.15. Zał. że R: dziedzina noetherowska, $a \in R \setminus (\{0\} \cup R^*)$. Wtedy a jest iloczynem elementów nierozkładalnych
$\underbrace{}_{\text{i.e.n.}}$

D-d, nie wprost.

Niech $A = \{a \in R \setminus (\{0\} \cup R^*) : a \text{ nie jest i.e.n.}\}$, $A \neq \emptyset$

Niech $J = \{(a) : a \in A\}$.

Istnieje $(b) \in J$: maksymalny w J (bo R: noetherowski)

$b \in A \Rightarrow b$ rozkładalny, $b = b_1 b_2$, $b_1, b_2 \notin R^*$

$$\left.\begin{array}{l}(b) \subsetneq (b_1)\\ (b) \subsetneq (b_2)\end{array}\right\} \Rightarrow b_1, b_2 \notin A \text{ z maksymalności } (b) \text{ w } J$$

$\Downarrow$

b_1, b_2 są i.e.n.

$\Downarrow$

$b = b_1 \cdot b_2$ też ↯.

Def. 10.16. Niech R dziedzina. Wtedy

R: dziedzina z jednoznacznością rozkładu [UFD, unique factorization domain], gdy

(a) $\forall a \in R \setminus (\{0\} \cup R^*)$ a jest i.e.n.

(b) Rozkład w (a) jest jednoznaczny (z dokładnością do $\sim$ i kolejności czynników), tzn:

jeśli $a = p_1 \cdots p_r = q_1 \cdots q_l$: rozkłady właściwe na czynniki nierozkładalne,

to po ewentualnej zmianie kolejności czynników: $r = l$ i $p_i \sim q_i$ dla $i = 1, \ldots, r$.

<u>Przykład</u> $\mathbb{Z}$ jest UFD

$$6 = 2 \cdot 3 = (-3) \cdot (-2) \qquad \begin{array}{l} 2 \sim (-2) \\ 3 \sim (-3). \end{array}$$

Tw. 10.17 Zał, że R: dziedzina. $\Leftrightarrow$:

(1) R jest UFD

(2) $(\forall a \in R \setminus (\{0\} \cup R^*))$ a jest i.e.n. i każdy element nierozkładalny w R jest pierwszy.

<u>D-d.</u> (1) $\Rightarrow$ (2).

Niech $p \in R \leftarrow$ UFD. Pok, że p: pierwszy.
nierozkładalny. Zał, że $p \mid ab$, tzn. $ab = p \cdot c$ dla pewnego $c \in R$

$$\begin{array}{ccccc} a & \cdot & b & = & p \cdot c \\ \| & & \| & & \| \\ \underbrace{a_1 \cdots a_k} & & \underbrace{b_1 \cdots b_l} & = & p \cdot \overbrace{c_1 \cdots c_t} \end{array}$$

rozkłady na i.e.n. $\Downarrow$

$p \sim b_i$ lub $p \sim a_j$ dla pewnych i, j

$\Downarrow \qquad\qquad \Downarrow$

$p \mid b \qquad\qquad p \mid a.$

(2) $\Rightarrow$ (1). nie wprost.

Zał., że $a = \underbrace{a_1 \dots a_r}_{\text{i.e.n}} = \underbrace{a_1' \dots a_s'}_{\text{i.e.n}}$ i ($r \neq s$ lub ($r = s$ i rozkłady są istotnie różne)

- $r, s > 1$.

Zał., że wybór a, r i s jest taki, że r: minimalne możliwe.

$a_1 \mid a_1' \dots a_s' \Rightarrow a_1 \mid a_i'$ dla pewnego i, bso $i = 1$

a_1 pierwszy

$\Downarrow$

$a_1' = \varepsilon \cdot a_1$, $\varepsilon \in R^*$

Stąd: $\underset{0}{\overset{\neq}{a_1}} (a_2 \dots a_r - \varepsilon a_2' \dots a_s') = 0$

$\Rightarrow \underbrace{a_2 \dots a_r}_{\text{istotnie różne i.e.n., krótsze}} = \underbrace{(\overset{a_2''}{\varepsilon a_2'})\, a_3' \dots a_s'}$ $\lightning$.

Wn. 10.18.
Jeśli R: dziedzina noetherowska, w której każdy el. nierozkładalny jest pierwszy, to R: UFD.

Wn. 10.19. R: PID $\Rightarrow$ R: UFD.

D-d. Niech $p \in R$: nierozkładalny.

Cel: p: pierwszy.

<u>D-d</u> R : PID $\Rightarrow$ R dziedzina noetherowska.

Niech $p \in R$ nierozkładalny. Cel: p: pierwszy.

Zał, ~~że~~ $p \mid ab$. $(p,a) = (c)$, $(p,b) = (d)$ dla pewnych $c, d \in R$

$c \mid p \Rightarrow c \in R^*$ <u>lub</u> $c \sim p$ (R : PID)

$$c \in R^* \Leftrightarrow \underbrace{c \sim 1}_{?} \qquad c \sim p \Rightarrow p \mid c,\ c \mid a \Rightarrow p \mid a \ \underline{\text{OK}}$$

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

$\Rightarrow 1 = px + ay$ dla pewnych $x, y \in R$

$b \cdot$

$$b = \underbrace{pxb}_{p\mid} + \underbrace{aby}_{p\mid} \Rightarrow p \mid b \ \text{OK}$$

Wn 11.4.

Każdy pierścień euklidesowy jest UFD.

<u>D-d</u>. Uwaga 10.5: p. euklidesowy jest PID.

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

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

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

(a) $d \mid a$ i $d \mid b$

(b) Jeśli $d_1 \mid a$ i $d_1 \mid b$, to $d_1 \mid d$

} d jest (a,b), gdy $R = \mathbb{Z}$

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

Fakt 11.6.
Zał., że d_1: NWD(a,b) i $d_2 \in R$. Wtedy
d_2: NWD$(a,b) \Leftrightarrow d_1 \sim d_2$.

D-d: zad.

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

D-d $a = p_1^{k_1} \dots p_n^{k_n}$ $\quad b = \underset{\substack{\uparrow \\ R^*}}{\varepsilon} \cdot p_1^{l_1} \dots p_n^{l_n}$, $k_i, l_i \geqslant 0$

Niech $t_i = \min\{k_i, l_i\}$
$d = p_1^{t_1} \dots p_n^{t_n}$: NWD(a,b).

Podobna definicja NWD$(a_1, \dots, a_k)$. Fakt 11.6 i tw. 11.7 pozostają słuszne.

TW. 11.8. Niech d : NWD$(a_1, \dots, a_k)$, $a_i = d \cdot a_i'$; nie wszystkie $a_i = 0$.
Wtedy 1 : NWD$(a_1', \dots, a_n')$

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

D-d $\Leftarrow$ $d \overset{(*)}{=} ax + by$, $d|a, d|b$. Jeśli $d_1|a$ i $d_1|b$, to $d_1|d$ $(*)$
bo $d \in (a,b)$ $\quad$ bo $a, b \in (d)$ $\quad$ więc d : NWD(a,b)

$\Rightarrow$ Niech d_1 t. że $(a,b) = (d_1)$.
Niech d : NWD(a,b).
Z ($\Leftarrow$): d_1 też NWD(a,b), więc
$d_1 \sim d$ i $(d) = (d_1)$.

Def. 11.10. R: dziedzina, $a, b, d \in R$.

Wtedy d: $NWW(a,b)$ [$d = [a,b]$, gdy $a, b, d \in \mathbb{N}$, $R = \mathbb{Z}$]

gdy:

(a) $a \mid d$ i $b \mid d$

(b) Jeśli $a \mid d_1$ i $b \mid d_1$, to $d \mid d_1$

} najmniejsza wspólna wielokrotność

Fakt 11.11: Odpowiednik faktu 11.6 dla NWW zamiast NWD

Tw. 11.12: Odpowiednik tw. 11.7 dla NWW zamiast NWD

plus:

$$a \cdot b \sim NWD(a,b) \cdot NWW(a,b) \quad (\text{gdy } a \neq 0 \text{ lub } b \neq 0)$$