Wykład 10.

Def. 10.3. Pierścień przemienny R z $1 \neq 0$ jest <u>dziedziną</u> (domain, 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 <u>normą euklidesową</u> w R, gdy

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

(b) $(\forall a, \underset{\neq 0}{b} \in R)(\exists q, r \in R)$

$(a = bq + r$ i $\delta(r) < \delta(q))$

(dzielenie z resztą)

(2) R: <u>pierścień euklidesowy</u>, gdy istnieje $\delta : R \longrightarrow \mathbb{N} \cup \{-\infty\}$ norma euklidesowa w R.

Przykłady.

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

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

$\uparrow$
ciało

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

pierścień Gaussa $\qquad$ podpierścień

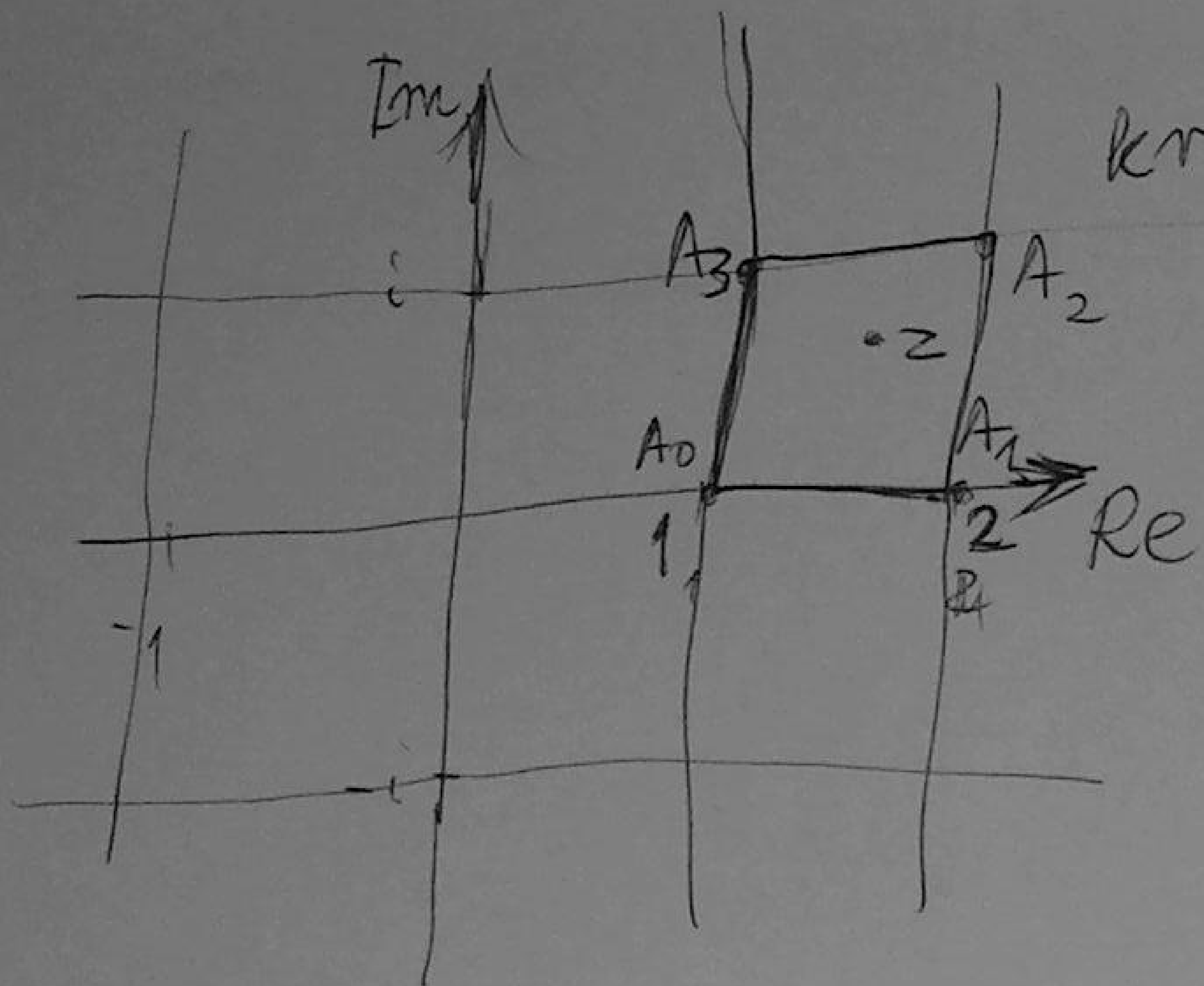
$$\delta(a+bi) = \begin{cases} -\infty, & \text{gdy } a+bi = 0 \\ \underbrace{a^2+b^2}_{=|a+bi|^2}, & \text{gdy } a+bi \neq 0 \end{cases}$$

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:

$$a + bi = q(c+di) + r \quad , \delta(r) < \delta(c+di)$$

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



krata całkowita.

Niech $j \in \{0,1,2,3\}$ t. że $|A_j - z| < 1$

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

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

$$\delta(r): \quad \frac{|r|^2}{|c+di|^2} = |z - A_j|^2 < 1$$

$$\Downarrow$$

$$\delta(r) < \delta(c+di)$$

(*) Wynik dzielenia z resztą w $\mathbb{Z}[i]$ (względem δ) nie jest jednoznaczny. (wybór A_j)

Uwaga 10.5.

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

<u>D-d</u>. Niech $I \triangleleft R$, bso $I \neq \{0\}$

δ: norma euklidesowa w R

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

- $I = (b)$, bo: $\supseteq$: jasne

$\subseteq$: $\underset{I}{a} = \underset{I}{q} \cdot b + \underset{I}{r}$, $q, r \in R$, $\underline{\delta(r) < \delta(b)}$ $\Rightarrow r = 0 \Rightarrow$ ~~$b \nmid a$~~ $b \mid a \Rightarrow \underline{a \in (b)}$

Przykład.

- K: ciało $\Rightarrow K$ dziedzina
- R: dziedzina $\Rightarrow R[X]$ dziedzina. (ćw.)

$f, g \in R[X] \Rightarrow \deg(f \cdot g) = \deg f + \deg g$

$K[X_1, X_2]$ jest dziedziną, ale nie jest PID, więc nie jest pierścieniem euklidesowym.

Def. 10.6 (R: p. przemienny z $1 \neq 0$)

(1) Ideał właściwy $I \underset{\neq}{\triangleleft} R$ jest <u>pierwszy</u>, gdy

$$(\forall a, b \in R)(ab \in I \Rightarrow a \in I \text{ lub } b \in I)$$

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

$$a \notin R^* \text{ i } (\forall b, c \in R)(a | bc \Rightarrow a | b \vee a | c)$$

Uwaga 10.7. Niech $I \underset{\neq}{\triangleleft} R$. Wtedy

I jest pierwszy $\iff$ R/I jest dziedziną.

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

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

$$\neg(\exists J \triangleleft R)(I \subsetneq J \subsetneq R)$$

Uwaga 10.9.

Niech $I \underset{\neq}{\lhd} R$. Wtedy I : maksymalny $\iff$ R/I jest ciałem.

[Def. Dziedzina R jest <u>ciałem</u>, gdy
$$R^* = R \setminus \{0\}.$$
]

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

$\Leftarrow$. Zał, że R/I : ciało. <u>nie wprost</u>:

$\boxed{\text{Zał, że } I \text{ nie jest maksymalny.}}$

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

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

Ale w ciele K jedyne ideały to $\{0\}$ i K. ↯
(ćw.)

$\Rightarrow$. Zał, że $a/I \neq 0$ w R/I. Cel:

a/I odwracalne w R/I.

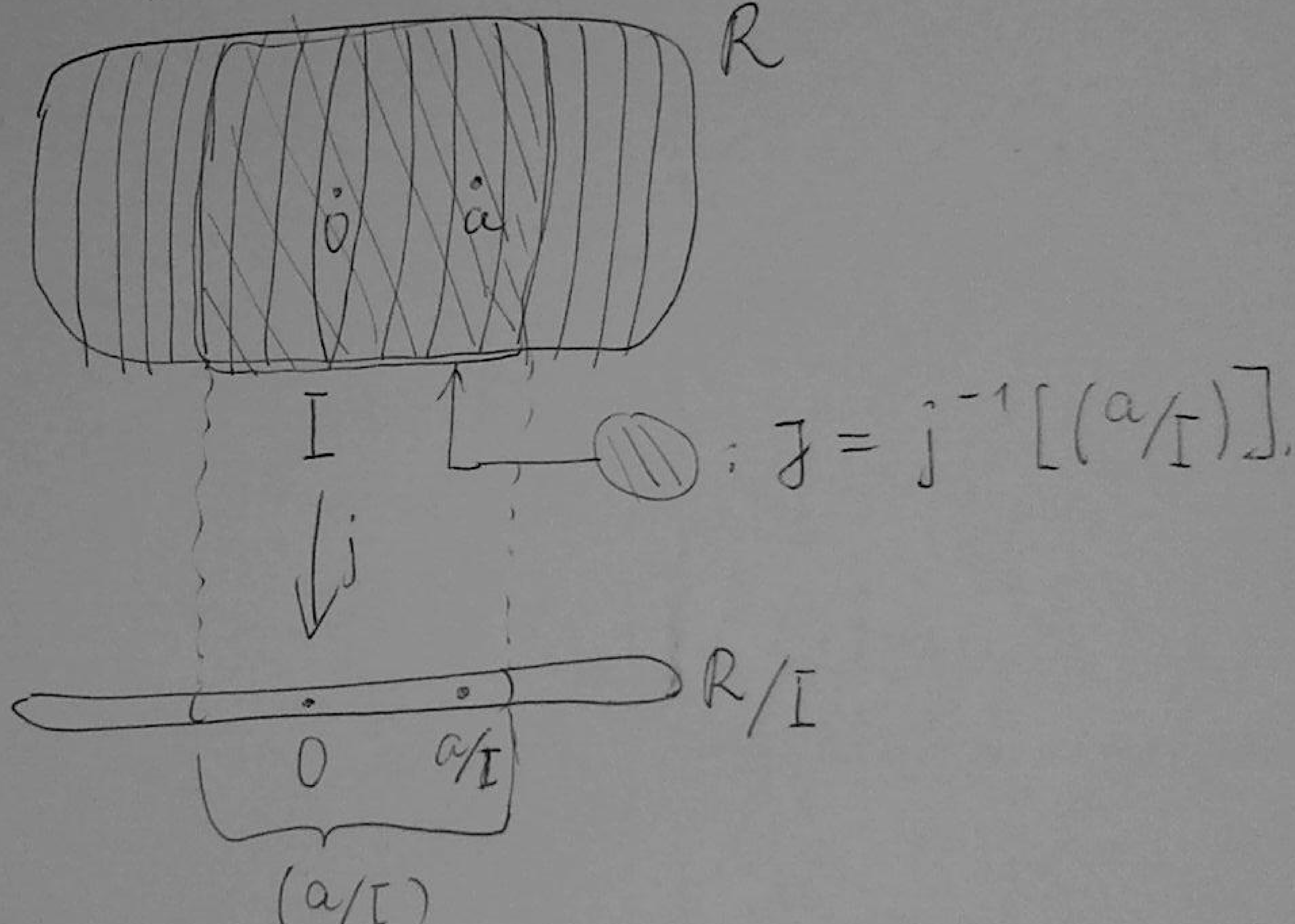
<u>nie wprost</u>:

Przypuśćmy, że a/I nie jest odwracalne w R/I

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

Niech $J = j^{-1}[(a/I)]$. Wtedy:

$I \subsetneq J \subsetneq R$ i $J \triangleleft R$ ↯



Wn. 10.10. $I \triangleleft R$: maksymalny $\Rightarrow$ I pierwszy.
(bo ciało R/I jest dziedziną).

<u>Przykład</u> w $\mathbb{Z}$: ideał I, $I \neq \mathbb{Z}$, jest maksymalny $\iff$ I: pierwszy $\iff$ $I = (p)$ dla pewnej l. pierwszej p.

D-d. Niech $I=(n) \lhd \mathbb{Z}$, bso $n>1$.

- jeśli n: l. pierwsza, to

  $\mathbb{Z}/I \cong \mathbb{Z}_n$: ciało, więc I maksymalny i pierwszy

- jeśli n: złożona, to

  $\mathbb{Z}/I \cong \mathbb{Z}_n$ nie jest dziedziną, więc I nie jest pierwszy i nie jest maksymalny.

Fakt 10.11.

Jeśli R: dziedzina ideałów głównych ~~to~~ oraz $\{0\} \neq I \lhd R$ jest pierwszy, to I: maksymalny.

D-d. Zał, że $I=(a)$ pierwszy, $\underset{R}{a} \neq 0$.

Nie wprost: przypuśćmy, że I nie jest maksymalny. tzn. istnieje $J \lhd R$ t. że

$I \subsetneq J \subsetneq R$

$J = (b)$

$a \in (b)$ dla pewnego $b \in R$

$\Rightarrow \underline{b \mid a}$ $\quad$ $b \notin (a) \Rightarrow \underline{a \nmid b}$.

$a = b \cdot c \in I \Longrightarrow c \in I = (a)$

$\uparrow$ dla pewnego $c \in I$

$\uparrow$ I pierwszy $b \notin I$

$\Downarrow$

$c = d \cdot a$

dla pewnego $d \in R$

$a = bda$

$\Downarrow$

$a(1-bd) = 0 \Longrightarrow 1 = bd$

$a \neq 0$

R: dziedzina $\Downarrow$

$1 \in J$ i $J = R$ $\lightning$.

Uwaga 10.12.

Jeśli $I \underset{\neq}{\triangleleft} R$, to istnieje $J \triangleleft R$ taki, że

$I \subseteq J$ i J maksymalny.

D-d. zad.

Podzielność w dziedzinie.

Niech R: dziedzina.

$R \ni a \rightsquigarrow a = b \cdot c$

$a = a_1 \cdot \ldots \cdot a_n,\ n \geq 2$

rozkłady a w R $a_i, b, c \in R$.

rozkład jest <u>właściwy</u> gdy

żaden czynnik nie jest odwracalny.

<u>np.</u> $3 = (-1)\cdot(-3)$ w $\mathbb{Z}$

rozkład niewłaściwy.

Def. 10.13. Niech $a \in R \setminus (\{0\} \cup R^*)$.

a jest <u>nierozkładalny</u>, gdy nie ma rozkładu właściwego w R.

<u>Uwaga</u>. a nierozkładalny $\iff$

$(\forall b, c \in R)(a = bc \implies b \in R^* \vee c \in R^*)$

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

(2) a nierozkładalny i $b \sim a$ $\implies$ b nierozkładalny. <u>D-d</u> ćw.

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

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

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

Przypuśćmy, że $A \neq \emptyset$.

Niech $\mathcal{J} = \{(a) : a \in A\}$ $\exists (b)$: maksymalny w $\mathcal{J}$

istnieje bo R: noetherowski.

$b \in A$

$\Downarrow$

b rozkładalny

$b = b_1 b_2 \qquad b_1, b_2 \notin R^*$

$(b) \subsetneq (b_1)$

$\Longrightarrow b_1, b_2 \notin A$ z maksymalności (b) w $\mathcal{J}$.

$(b) \subsetneq (b_2)$

$\Downarrow$

b_1, b_2 są i.e.n.

$\Downarrow$

<u>b też</u> $\lightning$.

Def. 10.16. Niech R: dziedzina. Wtedy R jest <u>dziedziną z jednoznacznym rozkładem (UFD)</u>, 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
$a = p_1 \cdots p_r = q_1 \cdot \ldots \cdot q_l$: i. e. n. ~~rozkłady właściwe~~,
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.

$$6 = 2 \cdot 3 = (-3) \cdot (-2) \quad \text{i.e.n.}$$

$$2 \sim (-2), \quad 3 \sim (-3)$$

<u>TW.</u> 11.1. (R : dziedzina). ⟺ :

(1) R : UFD.

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

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

- Niech $p \in R$ nierozkładalny, <u>pdk, że</u>:
  p pierwszy.

Zał, że $p | a \cdot b$ w R

$$a \cdot b = p \cdot c \quad \text{dla pewnego } c \in R$$

$$\overbrace{a_1 \cdot \ldots \cdot a_k}^{=a} \cdot \overbrace{b_1 \cdot \ldots \cdot b_l}^{=b} = p \cdot \overbrace{c_1 \ldots c_t}^{=c}$$

i.e.n.

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

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

$$p | b \qquad\qquad p | a$$

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

Zał, że $a = a_1 \ldots a_r = a_1' \ldots a_s'$ i [$r \neq s$ lub

i.e.n.

($r = s$ i rozkłady są istotnie różne)

Zał, że r: minimalne możliwe.

$a_1 | (a_1' \ldots a_s') \underset{a_1 \text{ pierwszy}}{\Longrightarrow} a_1 | a_i'$ dla pewnego i

<u>bso</u> $i = 1$

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

<u>Stąd</u>: $\underset{\neq 0}{a_1} (a_2 \cdot \ldots \cdot a_r - \varepsilon a_2' \ldots a_s') = 0$ bo a_1': nierozkładalny

$$\Downarrow$$

R dziedzina

AII, 10 (14

$$a' := \underbrace{a_2 \dots a_r}_{} = \underbrace{\overbrace{(\varepsilon a_2')}^{a_2''} \dots a_s'}_{}$$

istotnie różne i.e.n.,

sprzeczność z minimalnością r.