Pierścienie. Teoria podzielności.

$a|b$, $a\sim b$, NWD , NWW.

Dziedzina całkowitości , Dziedzina Euklidesowa ⇒ Dz. Ideał głównych

Def Pierścień P nazywamy dziedziną ideałów głównych (PID), gdy:

1. P jest przemienny z 1 i bez dzielników zera,
2. $\forall I \lhd P \ \exists a \in I \quad \langle a \rangle = I$.

Def Element $a \in P$ nazywamy:

1. pierwszym $\forall x,y \quad a | x\cdot y \to (a|x \lor a|y)$
2. nierozkładalny $\forall x y \quad a = x \cdot y \to (x \in P^* \lor y \in P^*)$

TW. P - dziedzina całkowitości: pierwszy → nierozkładalny.

Fakt Niech $(P,+,\cdot)$ pierścień przemienny z 1. Wtedy

1. $a|b \iff \langle a \rangle \supseteq \langle b \rangle$.
2. $a \sim b \iff \langle a \rangle = \langle b \rangle$

D-d 1. $\Rightarrow$:

$a|b$ tzn $\exists k \quad b = a\cdot k$.

Niech $x \in \langle b \rangle$ tzn $(\exists p \in P) \ x = b\cdot p$.

Wtedy $x = akp \in \langle a \rangle$,

tzn: $\langle b \rangle \subseteq \langle a \rangle$.

$\Leftarrow$: $b \in \langle b \rangle \subseteq \langle a \rangle$

$b \in \langle a \rangle$

$a | b$

2. $a \sim b \equiv a|b \land b|a \equiv \langle a \rangle \supseteq \langle b \rangle \land \langle b \rangle \supseteq \langle a \rangle \equiv \langle a \rangle = \langle b \rangle$

$\square$

Przykład. W $\mathbb{Z}$:

$3 \mid 9 \quad \wedge \quad \langle 3 \rangle \supsetneq \langle 9 \rangle$

Fakt. Niech P dziedzina ideał. głównych, $a, b \in P$, $b \mid a$

$\frac{a}{b}$ nierozkładalny $\Longleftrightarrow \neg \exists\, I \lhd P \quad \langle b \rangle \supsetneq I \supsetneq \langle a \rangle$.

[Przykład $b = 3$ $a = 12$ oraz

$\langle 3 \rangle \supsetneq \langle 6 \rangle \supsetneq \langle 12 \rangle \qquad \frac{a}{b} = \frac{12}{3} = 4 = 2 \cdot 2$, rozkładalny]

D-d $\rightarrow$: Nie wprost załóżmy, że istnieje $I \lhd P$ taki, że:

$\langle b \rangle \supsetneq I \supsetneq \langle a \rangle$.

P jest dziedziną ideał. głównych, więc $\exists\, c \in P$

$I = \langle c \rangle$

Mamy $\langle b \rangle \supsetneq \langle c \rangle \supsetneq \langle a \rangle$

Wtedy $a \in \langle a \rangle \subseteq \langle b \rangle \rightarrow b \mid a$

$c \in \langle c \rangle \subsetneq \langle b \rangle \rightarrow b \mid c$

$a \in \langle a \rangle \subsetneq \langle c \rangle \rightarrow c \mid a$

Wtedy $\frac{a}{b} = \frac{a}{c} \cdot \frac{c}{b}$

oraz $\frac{a}{c} \wedge \frac{c}{b}$ są nieodwracalne.

Gdyby, np., $\frac{a}{c}$ był odwracalny, $\frac{a}{c} = p \in P^*$; $\left.\begin{array}{l} a = p \cdot c \rightarrow c \mid a \\ a \cdot p^{-1} = c \rightarrow a \mid c \end{array}\right\} \rightarrow a \sim c$

$a \sim c$ więc $\langle a \rangle = \langle c \rangle$, ↯.

$\leftarrow$: ćw.

Fakt. Niech P dziedzina ideałów głównych (PID).

Dla dowolnego nieskończonego ciągu ideałów w P:

$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ istnieje $N \in \mathbb{N}$, taka że:

$\forall n \geq N \quad I_n = I_N$

D-d. Niech $I = \bigcup_{i=1}^{\infty} I_i$

- Wtedy I jest ideałem. ćw.

P jest PID wiec ist $a \in I$ takie, ze $\langle a \rangle = I$.

$$a \in I = \bigcup_n I_n$$

tzn $\exists N$ takie ze $a \in I_N$.

Wiec dla kazdego $n \geq N$:

$$I = \langle a \rangle \subseteq I_N \subseteq I_n \subseteq I$$

Wiec $I_n = I_N$ □

Wniosek Niech P PID, $a \in P$. Wtedy
Istnieje skonczony ciag ideałów :
1° $\langle a \rangle \subsetneq I_1 \subsetneq I_2 \subsetneq \dots \subseteq I_n = P$
2° $\forall i$ Nie istnieje ideał $J \triangleleft P$: $I_i \subsetneq J \subsetneq I_{i+1}$
[Przykład $\langle 12 \rangle \overset{2}{\subsetneq} \langle 6 \rangle \overset{2}{\subsetneq} \langle 3 \rangle \overset{3}{\subsetneq} \mathbb{Z}$]

D-d Gdyby kazdy ciag (1) nie miał własności (2) to dostali byśmy nieskonczony "rosnący" ciag ideałów P
Sprzeczności z poprzednim twierdzeniem. □

TW Niech P PID. Wtedy kazdy element nieodwracal. iloczynem elementów nierozkładalnych.

D-d Niech $a \in P$ nieodwracalny.
Na mocy wniosku ↑. Istnieje ciag ideałów

$$\langle a \rangle \subsetneq I_1 \subseteq I_2 \subsetneq \dots \subsetneq I_n = P$$

tak ze nie istnieje $J \triangleleft P$ $I_i \subsetneq J \subsetneq I_{i+1}$ $\forall i$

P jest PID więc $\forall_i \exists a_i \quad \langle a_i \rangle = I_i$. Wtedy

$$\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \dots \subsetneq \langle \overset{\overset{1}{\shortparallel}}{a_n} \rangle = P$$

Zauważmy :
- $\forall_i \quad a_{i+1} \mid a_i$
- $\forall_i \quad \frac{a_i}{a_{i+1}}$ jest nierozkładalne.

Wtedy

$$a = \frac{a}{a_1} \cdot \frac{a_1}{a_2} \cdot \frac{a_2}{a_3} \cdots \frac{a_{n-1}}{1}$$

jest rozkładem a na iloczyn elementów nierozkładalnych. □

Tw. W dziedzinie ideałów głównych element jest pierwszy wtedy i tylko wtedy gdy jest nierozkładalny.

D-d. PID jest dziedziną całkowitości więc element pierwszy jest nierozkładalny.

Pokażemy, że każdy element nierozkładalny jest pierwszy.

Niech n element nierozkładalny pierścienia P - PID.

Niech $n \mid a \cdot b$ [Cel: $n \mid a \lor n \mid b$]

Rozważmy ideał $\langle n, a \rangle$

P jest PID więc $g \in P \quad \langle n, a \rangle = \langle g \rangle$.

$n \in \langle g \rangle \rightarrow g \mid n$ tzn $n = g \cdot t$.

Wtedy

I g jest odwracalny, wtedy $1 \sim g$.

lub.

II t jest elementem odwracalnym wtedy $n \sim g$

II $n \sim g$

Wiemy $g \mid a$ bo $a \in \langle g \rangle$

Więc $\underline{n \mid a}$

I $g \sim 1$

tzn $1 \in \langle g \rangle = \langle n, a \rangle$

Więc istnieją $x, y \in P$

$$1 = n \cdot x + a \cdot y \quad \Big| \cdot b$$

$$b = n \cdot x \cdot b + a \cdot y \cdot b$$

$$\left. \begin{array}{l} n \mid nxb \\ n \mid aby \end{array} \right\} \; n \mid nxb + aby \quad \text{tzn} \quad \underline{n \mid b}$$

Więc n jest elementem pierwszym. $\square$

Wniosek:

Tw. W dziedzinie ideałów głównych rozkład na czynniki nierozkładalne (pierwsze) jest jednoznaczny tzn:
Dla dowolnego elementu $a \in P$ oraz $p_1, p_2, \ldots, p_k$ $q_1, q_2, \ldots, q_l$ elementów nierozkładalnych takich że

$$a = \prod_{i=1}^{k} p_i = \prod_{i=1}^{l} q_i \quad \text{mamy:}$$

(1) $k = l$.

(2) Po pewnym przenumerowaniu elementów $\{p_i\}$ mamy $p_i \sim q_i$

Dowód Załóżmy nie wprost, że istnieje $a \in P$ oraz rozkłady $a = \prod_{i}^{k} p_i = \prod_{i=1}^{l} q_i$ nie spełniające tego twierdzenia

$\#$ bzo: $\forall_{i j} \; p_i \nsim q_j$.

Wtedy $p_1 \mid \prod_{i=1}^{n} p_i$ to $p_1 \mid \prod_{i} q_i$

Skoro p_1 jest nierozkładalny to p_1 jest pierwszy

Więc $\exists n$ $p_1 \mid q_n$

$$q_n = p_1 \cdot t$$

Wtedy $t \in P^*$, bo q_n nierozkładalny

$$q_n \sim p_1$$

Sprzeczność z #. □

WNIOSEK - [Zasadnicze twierdzenie arytmetyki].
W pierścieniu PID każdy element rozkłada się jednoznacznie na iloczyn elementów nierozkładalnych. (pierwszych).

- $(\mathbb{Z} +, \cdot)$ jest PID.