Pierścienie. Dziedziny całkowitości

Zakładamy że rozważane pierścienie są przemienne z 1.

Rozważmy pojęcie analogiczne do znanych z teorii liczb.

Def Niech $(P, +, \cdot)$ pierścień przemienny z 1, $a, b \in P$ mówimy że a dzieli b jeśli

$$(\exists k \in P)\ b = a \cdot k$$

ozn $a \mid b$.

Def. Elementy $a, b \in P$ nazywamy stowarzyszonymi gdy $a \mid b \wedge b \mid a$

ozn $a \sim b$

Przykłady

- W $(\mathbb{Z}, +, \cdot)$ $\quad 1 \sim (-1), \quad a \sim (-a)$
- W $\mathbb{R}[x]$ $\quad w(x) \sim a \cdot w(x) \quad a \in \mathbb{R} \setminus \{0\}$

  $x^2 + 1 \sim 3x^2 + 3$.

Def $a \in P$ nazywamy odwracalnym gdy $\exists b \in P$ $\quad b \cdot a = 1$

Def. Niech $a, b \in P$. Element c jest największym wspólnym dzielnikiem a i b gdy

1. $c \mid a \wedge c \mid b$
2. $\forall d \ (d \mid a \wedge d \mid b) \rightarrow d \mid c$

Przykład Największymi wspólnymi dzielnikami 81 i 36 są 9 i -9
NWD(a, b) jest zbiorem.

• Analogicznie definiujemy najmniejszą wspólną wielokrotność.

Def. Element $a \in P$ nazywamy elementem pierwszym, gdy
$$(\forall x\, y) \quad a \mid x \cdot y \rightarrow (a \mid x \vee a \mid y)$$

Przykład: • $3 \mid x \cdot y$ to $3 \mid x \vee 3 \mid y$ w $\mathbb{Z}$

• $6 \mid 2 \cdot 3$ ale $6 \nmid 2$ i $6 \nmid 3$ 6 nie jest pierwsza.

Def. Element $a \in P$ nazywamy nierozkładalnym, gdy
$$(\forall x, y) \quad a = x \cdot y \rightarrow (x \in P^* \vee y \in P^*)$$

Przykład $3 = (-3) \cdot (-1)$ oraz $-1 \in \mathbb{Z}^*$

Def Element $a \in P$ nazywamy dzielnikiem zera gdy
1. $a \neq 0$.
2. $\exists b \neq 0 \quad a \cdot b = 0$

Przykład • W $\mathbb{Z}$ nie istnieją dzielniki zera
• W ciałach nie istnieją dzielniki zera.
• 2 jest dzielnikiem zera w $\mathbb{Z}_6$:
$$2 \cdot_6 3 = 0.$$

• W pierścieniu wielomianów nad ciałem: $K[x]$ nie ma dziel. zera

Def Pierścień P nazywamy dziedziną całkowitości, gdy jest przemienny z 1 i bez dzielników zera

Przykłady
- $(\mathbb{Z}, +, \cdot)$
- $(K, +, \cdot)$ – ciało.
- $K[x]$
- $R[x]$, R – dziedzina całkowitości.
- $\mathbb{R} \times \mathbb{R}$ NIE są dziedziną całkowitości ?!

Def. Pierścień P ma prawo skracania gdy dla dowol. $a, x, y \in P$, $a \neq 0$

$$ax = ay \to x = y.$$

Przykład. W ciałach zachodzi prawo skracania:

$$a \neq 0$$
$$ax = ay \quad | \cdot a^{-1}$$
$$x = y.$$

Fakt W dziedzinach całkowitości zachodzi prawo skracania.

D-d. Niech P dziedzina całkowitości

$0 \neq a, x, y \in P$

$ax = ay \quad | - ay$

$ax - ay = 0$ rozdz. mnoż.

$a \cdot (x - y) = 0$, w P nie ma dzielników zera, $a \neq 0$:

$x - y = 0$

$x = y \quad \square$

Fakt. W dziedzinie całkowitości każdy element pierwszy jest nierozkładalny

D-d. Niech P dziedzina całkowitości.
Niech $a \in P$ element pierwszy
tzn:
$\forall x,y \in P \quad a \mid x \cdot y \Rightarrow (a \mid x \vee a \mid y)$

Pokażemy że a jest nierozkładalny:

(•) Niech $a = x \cdot y$
Wtedy $a \mid x \cdot y$
a jest pierwszy to
$\underline{a \mid x}$ lub $a \mid y$

I. załóżmy że $a \mid x$
(••) tzn $\exists k \in P \quad x = a \cdot k$

(•),(••): $a = xy$
$a \cdot 1 = ak \cdot y$
Z prawa skracania: ← P jest dziedziną całkowitości.
$1 = k \cdot y$
Więc $y \in P^*$

II $a \mid y \ldots \quad x \in P^*$ $\square$

Uwaga: Element nierozkładalny nie musi być pierwszy:
Zad 48:
W pierścieniu $\mathbb{Z}[\sqrt{5}i] = \{a + b\sqrt{5}i : a, b \in \mathbb{Z}\}$.

$a = 2 + \sqrt{5}i$ jest elementem nierozkładalnym ale nie pierwszym.

Dziedziny Euklidesowe (ED)

Def. Dziedzinę całkowitości P nazywamy dziedziną Euklidesową gdy istnieje funkcja

$N: P \longrightarrow \mathbb{N}$ taka, że:

1. $\forall a,b \in P \ \exists w,r \in P \quad a = b \cdot w + r$ oraz $N(r) < N(b)$
2. $N(0) = 0$
3. $\forall a,b \in P \quad N(a \cdot b) \geq N(b)$.

Przykłady · $(\mathbb{Z}, +, \cdot)$ $\quad N(k) = |k|$.
· $\mathbb{R}[x]$ $\quad N(f(x)) = st(f(x))$
· $K[x]$ $\quad N(f) = st(f)$, K - ciało

Def. Pierścień P nazywamy pierścieniem ideałów głównych gdy każdy ideał P jest ideałem głównym, tzn.

$\forall I \lhd P \ \exists a \in I \quad I = \langle a \rangle = \{a \cdot p : p \in P\}$

(PID)

Def. Dziedzinę ideałów głównych nazywamy dziedzinę całkowitości w której każdy ideał jest ideałem głównym

Przykład · $(\mathbb{Z}, +, \cdot)$, Ideały są postaci $n\mathbb{Z} = \langle n \rangle$
· $\mathbb{R}[x]$ ideały $\langle f \rangle$.

TW. Dziedzina Euklidesowa jest dziedziną ideałów głównych.
[tzn. Jeśli P jest dziedz. Euklid. to P jest dziedz. ideał. głównych.]

D-d. Niech P dziedzina Euklidesowa.
Więc istnieje funkcja $N: P \to \mathbb{N}$ jak w def ED

Niech $I \triangleleft P$

[Cel: $\exists a \in I \quad I = \langle a \rangle$]

Niech $a \in I$ element o najmniejszej wartości $N(a)$ z pośród elementów I.

Wtedy $\langle a \rangle = I$

- $\langle a \rangle \subseteq I$ bo $a \in I$
- $\langle a \rangle \supseteq I$

Załóżmy nie wprost, że istnieje $b \in I \setminus \langle a \rangle$

P jest ED, istnieją $w, r \in P$ takie, że:

$b = a \cdot w + r$:

$(\circ) N(r) < N(a)$

Wtedy: $(\circ\circ) r = b - a \cdot w \in I$

$(\circ), (\circ\circ)$ sprzeczne z wyborem elementu a.

Założenie nie wprost fałszywe, więc:

$\langle a \rangle \supseteq I$

Więc $\langle a \rangle = I$ $\square$