Pierścienie

$(P,+,\cdot)$ takie że $(P,+)$ grupa przemienna, $\cdot$ jest łączne oraz
$\forall a,x,y \in P \quad a(x+y) = ax+ay$ i $(x+y)a = xa+ya$.

Np $(\mathbb{Z}+,\cdot)$, $(\mathbb{R}^{2\times 2} +,\cdot)$

Def Niech $(R+,\cdot)$ pierścień, wtedy $A \subseteq R$ nazywamy podpierścieniem, gdy

1. $\forall a,b \in A \quad a+b \in A$
2. $\forall a \in A \quad -a \in A$
3. $\forall a,b \in A \quad a\cdot b \in A$.

ozn $A \leq R$

Przykład $(\mathbb{Z}+,\cdot) \leq (\mathbb{R},+,\cdot)$, $(2\mathbb{Z}+,\cdot) \leq (\mathbb{Z}+,\cdot)$.

Ideały w pierścieniach.

Def Niech $(R+,\cdot)$ pierścień, Zbiór $I \subseteq R$ nazywamy ideałem, gdy

1. $\forall a,b \in I \quad a+b \in I$
2. $\forall a \in I \quad -a \in I$
3. $\forall a \in I \ \forall r \in R \quad r\cdot a, ar \in I$

Przykłady: $R = (\mathbb{Z}+,\cdot)$, wtedy $\forall n \in \mathbb{N}$
$n\mathbb{Z} = \{n\cdot z : z \in \mathbb{Z}\}$ ideał.

1,2: Niech $a,b \in n\mathbb{Z}$ więc $n|a, n|b \quad n|a+b \wedge n|-a$

3 Niech $a \in n\mathbb{Z}$, $r \in \mathbb{Z}$ więc $n|a \Rightarrow n|a\cdot r \rightarrow a\cdot r \in n\mathbb{Z}$

· $I \trianglelefteq R$ oznaczamy I jest ideałem w R.

Uwaga. Niech $(R,+,\cdot)$ pierścień to $\{0\} \trianglelefteq R$ oraz $R \trianglelefteq R$ (ideały trywialne).

Uwaga. 1. Każdy ideał jest podpierścieniem.

2. $\mathbb{Z} \leq (\mathbb{R},+,\cdot)$ podpierścień, ale $\mathbb{Z} \not\trianglelefteq (\mathbb{R},+,\cdot)$ NIE jest ideałem.

· Ideał generowany przez podzbiór pierścienia.

Fakt. Niech $\mathcal{A}$ - niepusta rodzina ideałów pierścienia $(R,+,\cdot)$. Wtedy $\bigcap \mathcal{A} \trianglelefteq R$.

D-d - ćw.

Def. Niech $(R,+,\cdot)$ pierścień, $A \subseteq R$. Ideałem generowanym przez A nazywamy najmniejszy (względem $\subseteq$) ideał $I \trianglelefteq R$ taki, że $I \supseteq A$.
ozn $\langle A \rangle$.

Fakt. Dla dowolnego pierścienia R oraz $A \subseteq R$ ideał $\langle A \rangle$ istnieje.

D-d. Rozważmy $\mathcal{A} = \{ I \trianglelefteq R : A \subseteq I \}$.
Zauważmy $\mathcal{A} \neq \emptyset$ bo $R \in \mathcal{A}$.
więc $\bigcap \mathcal{A} \trianglelefteq R$, $A \subseteq \bigcap \mathcal{A}$
$\bigcap \mathcal{A}$ jest najmniejszym ideałem zawierającym A:
Niech $J \trianglelefteq R$, $J \supseteq A$ to $J \in \mathcal{A}$
więc $J \supseteq \bigcap \mathcal{A}$

Więc $\langle A \rangle = \bigcap \mathcal{A}$. $\square$

Uwaga. Niech $(R, +, \cdot)$ pierścień, $A \subseteq R$.
Wtedy

$$\langle A \rangle = \{ r_1 a_1 r_2 + r_3 a_2 r_4 + \dots r_{\_} a_n r_{\_} : a_i \in A, r_i \in R \}$$

• R jest przemienny to:

$$\langle A \rangle = \{ r_1 a_1 + r_2 a_2 + \dots r_n a_n : a_i \in A, r_i \in R \}$$

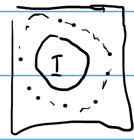
$$\langle \{a\} \rangle = \langle a \rangle = \{ r \cdot a : r \in R \}$$

Np: $R = \mathbb{Z}$

$$\langle 2 \rangle = \{ 2 \cdot r : r \in \mathbb{Z} \} = 2\mathbb{Z}.$$

Def Niech R pierścień. Ideał $I \lhd R$ nazywamy maksymalnym gdy
1. $I \neq R$
2. $\forall J \lhd R \quad J \supset I \rightarrow J = R$

R



Przykład. $R = (\mathbb{Z}, +, \cdot)$

1. Ideały są postaci: $n\mathbb{Z} : n \in \mathbb{N}$
2. Ideał $n\mathbb{Z}$ jest maksymalny $\iff$ $n \in \mathbb{P}$ – liczba pierwsza

D-d • Jeśli $n \notin \mathbb{P}$ to $n = k \cdot l \quad k,l > 1$

$$n\mathbb{Z} \subsetneq k\mathbb{Z} \subsetneq \mathbb{Z}$$

• Jeśli $n \in \mathbb{P}$ i jeśli $J \supsetneq n\mathbb{Z}$
wtedy $\exists m \in J \setminus n\mathbb{Z}$
wtedy $NWD(m,n) = 1 \quad \forall_{x,y} \quad x \cdot m + y \cdot n \in J$

$$1 = xm + yn \in J$$

$$\forall z \in \mathbb{Z} \quad z = zxm + zyn \in J$$

$$J = \mathbb{Z} \qquad \square$$

- Pierścień ilorazowy.

Niech $(R,+,\cdot)$ pierścień $I \lhd R$

Zbiór warstw $R/I = \{ r+I \;:\; r \in R \}$.

Uwaga $\forall r,s \in R \quad r+I = r'+I \iff r-r' \in I$.

Dodawanie warstw. $(r+I)+(s+I) = (r+s)+I$

Mnożenie warstw $(r+I)\cdot(s+I) = (r\cdot s)+I$

Fakt. Działanie dodawania i mnożenia są dobrze określone

tzn $\forall r,r',s,s' \in R$ takich że $r+I = r'+I$ i $s+I = s'+I$

zachodzi: 1. $(r+I)+(s+I) = (r'+I)+(s'+I)$

2. $(r+I)\cdot(s+I) = (r'+I)\cdot(s'+I)$.

D-d 2: $(r+I)\cdot(s+I) = r\cdot s + I$

$(r'+I)\cdot(s'+I) = r'\cdot s' + I$

Cel: $rs+I = r's'+I$, tzn: $rs - r's' \in I$.

Mamy $rs - r's' = \underbrace{rs - rs'} + \underbrace{rs' - r's'} = \underbrace{r\overbrace{(s-s')}^{\in I}}_{\in I \text{ bo } I \lhd R} + \underbrace{\overbrace{(r-r')}^{\in I}s'}_{\in I} \in I$

Więc $(r+I)(s+I) = (r'+I)(s'+I)$.

Tw Niech $(R,+,\cdot)$ pierścień, $I \lhd R$.

Na R/I określamy działania $+,\cdot$ jak wyżej.

Wtedy $(R/I,+,\cdot)$ jest pierścieniem.

D-d. 1. W grupie $(R,+)$ zbiór I jest podgrupą normalną i wtedy $(R/I,+)$ jest grupą i dodatkowo przemienną.

2. Teraz: $\forall a+I, b+I, c+I \in R/I$ mamy

łączność w R

$$((a+I)\cdot(b+I))(c+I) = (a\cdot b+I)\cdot(c+I) = (ab)\cdot c+I = a(bc)+I = (a+I)((b+I)(c+I))$$

- Rozkład. mnożenie wzgl. dodawania, analogicznie. $\square$

<u>Uwagi</u>
- Element neutralny $+$ to $0+I=I$
- Element przeciwny do $r+I$ to $-r+I$
- Elem. neutralny $\cdot$ $1+I$
- $(r+I)^{-1} = r^{-1}+I$

o ile istnieje.

Przykład $R=(\mathbb{Z},+,\cdot)$
$I = n\mathbb{Z}$

$$R/I = \mathbb{Z}/n\mathbb{Z} = \{r+n\mathbb{Z} : r\in\mathbb{Z}\}$$

Uwaga $r+n\mathbb{Z} = r'+n\mathbb{Z} \Leftrightarrow r-r'\in n\mathbb{Z} \Leftrightarrow n \mid r-r'$
dla $r' = r \pmod n$ $n \mid r-r' = r-r \pmod n$
więc $\forall r\in\mathbb{Z}$ $r+n\mathbb{Z} = r \pmod n + n\mathbb{Z}$

$$\mathbb{Z}/n\mathbb{Z} = \{r+n\mathbb{Z} : r\in\{0,1,\dots,n-1\}\} =$$
$$\{0+n\mathbb{Z}, 1+n\mathbb{Z}, 2+n\mathbb{Z}, \dots, (n-1)+n\mathbb{Z}\}$$

dodawanie:
$a,b\in\{0,\dots,n-1\}$
$$a+n\mathbb{Z} + b+n\mathbb{Z} = (a+b)+n\mathbb{Z} = [(a+b)\bmod n]+n\mathbb{Z} = (a+_n b)+n\mathbb{Z}$$

mnożenie:
$$(a+n\mathbb{Z})\cdot(b+n\mathbb{Z}) = (a\cdot b)+n\mathbb{Z} = [ab \bmod n]+n\mathbb{Z} = a\cdot_n b+n\mathbb{Z}$$

Uwaga $\varphi: a+n\mathbb{Z} \to a$; $\mathbb{Z}/n\mathbb{Z} \to \{0,1,\dots,n-1\}$
jest izomorfizmem. $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.