8. Wykład 8: Pojęcie pierścienia. Podpierścienie. Podpierścienie generowane przez zbiór.

8.1. Pojęcie pierścienia.

Definicja 8.1. *Niech R będzie zbiorem niepustym.*

(1) *Algebrę $(R, +, \cdot)$ nazywamy* **pierścieniem,** *gdy $(R, +)$ jest grupą abelową, działanie $\cdot$ jest łaczne oraz rozdzielne względem działania $+$, to znaczy*

$$\forall x, y, z \in R[x \cdot (y + z) = x \cdot y + x \cdot z],$$

$$\forall x, y, z \in R[(y + z) \cdot x = y \cdot x + z \cdot x].$$

Działanie $+$ nazywamy **dodawaniem** *w pierścieniu R, a działanie $\cdot$* **mnożeniem.** *Element neutralny dodawania nazywamy* **zerem** *i oznaczamy przez 0. Pierścień $(R, +, \cdot)$ nazywamy* **pierścieniem zerowym,** *jeżeli $R = \{0\}$.*

(2) *Algebrę $(R, +, \cdot)$ nazywamy* **pierścieniem przemiennym,** *gdy jest pierścieniem i gdy mnożenie jest przemienne.*

(3) *Algebrę $(R, +, \cdot)$ nazywamy* **pierścieniem z jedynką,** *gdy jest pierścieniem i gdy mnożenie ma element neutralny, który wówczas nazywamy* **jedynką** *i oznaczamy przez 1.*

(4) *Algebrę $(R, +, \cdot)$ nazywamy* **ciałem,** *gdy jest niezerowym pierścieniem przemiennym z jedynką i gdy dla każdego elementu różnego od 0 istnieje element odwrotny względem mnożenia.*

Uwaga 8.1. *Niech $(R, +, \cdot)$ będzie ciałem. Wówczas:*

(1) *R zawiera co najmniej dwa elementy,*
(2) *$(R, +)$ jest grupą abelową,*
(3) *$(R^*, \cdot)$ jest grupą abelową, gdzie $R^* = R \setminus \{0\}$.*

Przykłady:

(1) **Pierścienie liczbowe.** $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ są przykładami pierścieni przemiennych z jedynką. $(\mathbb{N}, +, \cdot)$ nie jest pierścieniem. Ponadto $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ są ciałami, zaś $(\mathbb{Z}, +, \cdot)$ nie jest.

(2) **Pierścienie reszt.** Niech $n \in \mathbb{N}$ i rozważmy $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ z działaniami $\oplus_n$ oraz $\otimes_n$. $(\mathbb{Z}_n, \oplus_n, \otimes_n)$ są przykładami pierścieni przemiennych z jedynką. $(\mathbb{Z}_n, \oplus_n, \otimes_n)$ na ogół nie jest ciałem, chyba że n jest liczbą pierwszą.

(3) **Pierścienie wielomianów.** Niech $\mathbb{R}[x]$ będzie zbiorem wielomianów zmiennej x o współczynnikach rzeczywistych. Wówczas $(\mathbb{R}[x], +, \cdot)$ jest pierścieniem przemiennym z jedynką, który nie jest ciałem, gdzie $+$ i $\cdot$ oznaczają działania, odpowiednio, dodawania i mnożenia wielomianów.

(4) **Pierścienie macierzy.** Niech F będzie dowolnym ciałem, niech $M(n, F)$ oznacza zbiór macierzy kwadratowych stopnia n o współczynnikach z ciała F. $(M(n, F), +, \cdot)$ jest pierścieniem z jedynką, przy czym $+$ i $\cdot$ oznaczają tu, odpowiednio, dodawanie i mnożenie macierzy. Pierścień ten na ogół nie jest przemienny.

(5) **Pierścień endomorfizmów.** Niech V będzie przestrzenią liniową. $(V, +)$. Oznaczmy przez $End(V)$ zbiór endomorfizmów liniowych przestrzeni V. $(End(V), +\circ)$ jest pierścieniem z jedynką, który na ogół nie jest przemiennt, przy czym $+$ i $\circ$ są tu działaniami, odpowiednio, dodawania i składania przekształceń liniowych.

(6) **Pierścienie funkcji.** Niech $(R, +_R, \cdot_R)$ będzie pierścieniem, niech $X \neq \emptyset$. W rodzinie funkcji

$$R^X = \{f : X \to R : f \text{ jest funkcją}\}$$

definiujemy działania

$$(f+g)(x) = f(x) +_R g(x) \text{ oraz } (f \cdot g)(x) = f(x) \cdot_R g(x).$$

$(R^X, +, \cdot)$ jest pierścieniem, który jest przemienny, gdy R jest przemienny.

(7) **Skończony produkt pierścieni.** Niech $(R_1, +_1, \cdot_1), \ldots, (R_n, +_n, \cdot_n)$ będą pierścieniami. W produkcie kartezjańskim $R = R_1 \times \ldots \times R_n$ definiujemy działania "po współrzędnych":

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 +_1 b_1, \ldots, a_n +_n b_n),$$

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 \cdot_1 b_1, \ldots, a_n \cdot_n b_n).$$

$(R, +, \cdot)$ jest pierścieniem, który jest przemienny (z jedynką), gdy wszystkie pierścienie $R_1, \ldots, R_n$ są przemienne (z jedynką).

(8) **Pierścień grupowy.** Niech $(G, *)$ będzie grupą, niech $(R, +_R, \cdot_R)$ będzie pierścieniem. Rozważmy zbiór

$$R[G] = \text{ zbiór funkcji } f : G \to R \text{ prawie wszędzie równych } 0.$$

W zbiorze tym definiujemy działania:

$$(f+g)(x) = f(x) +_R g(x),$$

$$(f \cdot g)(x) = \sum_{y \in G} f(x * y^{-1}) \cdot_R g(y).$$

$(R[G], +, \cdot)$ jest pierścieniem.

W dowolnym pierścieniu $(R, +, \cdot)$ wprowadzamy oznaczenia:

$$\begin{aligned} xy + z &= (x \cdot y) + z, \\ \sum_{i=1}^{n} x_i &= x_1 + \ldots + x_n, \sum_{i=1}^{0} x_i = 0, \\ \prod_{i=1}^{n} x_i &= x_1 \cdot \ldots \cdot x_n, \prod_{i=1}^{0} x_i = 1. \end{aligned}$$

W szczególności $\sum_{i=1}^{n} x = nx$ oraz $\prod_{i=1}^{n} x = x^n$.

Twierdzenie 8.1. *Niech $(R, +, \cdot)$ będzie pierścieniem przemiennym z jedynką. Wówczas:*

(1) $-(-x) = x$,
(2) $-(x+y) = (-x) + (-y)$,
(3) $n(mx) = nmx$,
(4) $nx + mx = (n+m)x$,
(5) $0x + x0 = 0$,
(6) $(-1)x = -x$,
(7) $(-x)y = -(xy) = x(-y)$,
(8) $(-x)(-y) = xy$,
(9) $x(y-z) = xy - xz$,
(10) $(x-y)z = xz - yz$,
(11) $x + z = y + z \Rightarrow x = y$,
(12) $x^n x^m = x^{n+m}$,
(13) $(x^n)^m = x^{nm}$,
(14) $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$.

Prosty dowód pozostawiamy Czytelnikowi jako ćwiczenie.

W dalszym ciągu tego wykładu pisząc "pierścień" będziemy na ogół mieli na myśli "pierścień przemienny z jedynką".

8.2. **Podpierścienie, podpierścienie generowane przez zbiór.**

Definicja 8.2. *Niech $(R,+,\cdot)$ będzie pierścieniem. Podzbiór $P \neq \emptyset$ zbioru R nazywamy* **podpierścieniem** *pierścienia R (piszemy $P < R$), gdy $(P, + \restriction_{P\times P}, \cdot \restriction_{P\times P})$ jest pierścieniem.*

Przykłady:

(1) $\mathbb{Z} < \mathbb{R}$;
(2) $\mathbb{R} < \mathbb{C}$;
(3) $\mathbb{Z}_n$ nie jest podpierścieniem pierścienia $\mathbb{Z}$.

Twierdzenie 8.2. *Niech $\emptyset \neq P \subset R$ i niech $(R,+,\cdot)$ będzie pierścieniem. Następujące warunki są równoważne:*

(1) *$P < R$;*
(2) *P ma następujące własności:*
   - $1_R \in P$,
   - $\forall x, y \in P (x - y \in P)$,
   - $\forall x, y \in P (x \cdot y \in P)$.

Prosty dowód pozostawiamy Czytelnikowi jako ćwiczenie.

Przykłady:

(4) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} < \mathbb{R}$. Istotnie, $1 \in \mathbb{Z}[\sqrt{2}]$. Ustalmy $x, y \in \mathbb{Z}[\sqrt{2}]$, to znaczy niech $x = x_1 + x_2\sqrt{2}$, $y = y_1 + y_2\sqrt{2}$. Wówczas:
$$\begin{aligned} x - y &= (x_1 - y_1) + (x_2 - y_2)\sqrt{2} \in \mathbb{Z}[\sqrt{2}], \\ x \cdot y &= (x_1y_1 + 2y_1y_2) + (x_1y_2 + x_2y_1)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]. \end{aligned}$$

(5) $\mathbb{Z}_{(p)} = \{\frac{m}{n} : NWD(m,n) = 1 \text{ oraz } p \neq n\} < \mathbb{Q}$, gdzie p jest liczbą pierwszą. Istotnie, $1 \in \mathbb{Z}_{(p)}$. Ustalmy $x, y \in \mathbb{Z}_{(p)}$, to znaczy niech $x = \frac{m_1}{n_1}$, $NWD(m_1, n_1) = 1$, $p \nmid n_1$, $y = \frac{m_2}{n_2}$, $NWD(m_2, n_2) = 1$, $p \nmid n_2$. Wówczas:
$$\begin{aligned} \frac{m_1}{n_1} - \frac{m_2}{n_2} &= \frac{m_1n_2 - m_2n_1}{n_1n_2} \in \mathbb{Z}_{(p)}, \text{ bo } p \nmid n_1n_2 \text{ oraz } NWD(m_1n_2 - m_2n_1, n_1n_2) = 1, \\ \frac{m_1}{n_1} \cdot \frac{m_2}{n_2} &= \frac{m_1m_2}{n_1n_2} \in \mathbb{Z}_{(p)}, \text{ bo } p \nmid n_1n_2 \text{ oraz } NWD(m_1m_2, n_1n_2) = 1. \end{aligned}$$
Pierścień $\mathbb{Z}_{(p)}$ nazywamy **pierścieniem liczb p-całkowitych.**

Twierdzenie 8.3. *Niech $\mathcal{R} = \{R_i : i \in I\}$ będzie rodziną podpierścieni pierścienia R;*

(1) *$\bigcap_{i\in I} R_i$ jest podpierścieniem pierścienia R,*
(2) *$\bigcup_{i\in I} H_i$ jest podpierścieniem pierścienia R, o ile $\mathcal{R}$ jest łańcuchem.*

Prosty dowód pozostawiamy Czytelnikowi jako ćwiczenie.

Definicja 8.3. *Niech $(R,+,\cdot)$ będzie pierścieniem oraz $A \subset R$ pewnym zbiorem. Najmniejszy w sensie inkluzji podpierścień pierścienia R zawierający zbiór A (tj. przekrój wszystkich podpierścieni pierścienia R zawierających A) nazywamy* **podpierścieniem generowanym przez** *A i oznaczamy $[A]$.*

Uwaga 8.2. *Niech $(R,+,\cdot)$ będzie pierścieniem oraz $P < R$. Wówczas:*

(1) $[P] = P$,
(2) $[R] = R$.

Definicja 8.4. *Każdy zbiór A o tej własności, że $[A] = R$ nazywamy* **zbiorem generatorów** *pierścienia R. Jeśli $A = \{a_1, \ldots, a_n\}$ to oznaczamy*

$$[a_1, \ldots, a_n] = \langle A \rangle.$$

Mówimy, że pierścień jest **skończenie generowany**, *gdy istnieją elementy $a_1, \ldots, a_n \in R$ takie, że*

$$R = [a_1, \ldots, a_n].$$

Twierdzenie 8.4 (o postaci elementów podpierścienia generowanego przez zbiór)**.** *Niech $(R, +, \cdot)$ będzie pierścieniem oraz $A \subset R$ pewnym zbiorem. Wówczas*

$$[A] = \{x : x \text{ jest sumą elementów postaci } \pm a_1 \cdot \ldots \cdot a_k, k \in \mathbb{N} \cup \{0\}, a_i \in A\}.$$

Prosty dowód pozostawiamy Czytelnikowi jako ćwiczenie.

Definicja 8.5. *Niech $(R, +, \cdot)$ będzie pierścieniem oraz $A \subset R$ pewnym zbiorem. Niech ponadto $P < R$. Podpierścień generowany przez zbiór $P \cup A$ nazywamy* **podpierścieniem generowanym przez A nad** *P i oznaczamy $P[A]$.*

Jeżeli $A = \{a_1, \ldots, a_n\}$, to pierścień $R[\{a_1, \ldots, a_n\}]$ nazywamy **podpierścieniem skończenie generowanym przez A nad** *P i oznaczamy $P[a_1, \ldots, a_n]$.*

Wniosek 8.1 (o postaci elementów podpierścienia generowanego przez zbiór nad pierścieniem)**.** *Niech $(R, +, \cdot)$ będzie pierścieniem oraz $A \subset R$ pewnym zbiorem. Niech $P < R$. Wówczas*

$$P[A] = \{x : x \text{ jest sumą elementów postaci } pa_1 \cdot \ldots \cdot a_k, k \in \mathbb{N} \cup \{0\}, a_i \in A, p \in P\}.$$

Wniosek 8.2. (1) *Niech $(R, +, \cdot)$ będzie pierścieniem oraz niech $a \in R$. Niech $P < R$. Wówczas*

$$P[a] = \{x_0 + x_1 a + \ldots + x_n a^n : n \in \mathbb{N} \cup \{0\}, x_i \in P\}.$$

(2) *Niech $(R, +, \cdot)$ będzie pierścieniem oraz niech $\{a_1, \ldots, a_n\} \subset R$. Niech $P < R$. Wówczas*

$$P[a_1, \ldots, a_n] = \{x : x \text{ jest sumą elementów postaci } pa_1^{i_1} \cdot \ldots \cdot a_n^{i_n}, i_1, \ldots, i_n \in \mathbb{N} \cup \{0\}, p \in P\}.$$

Przykłady:

(6) $\mathbb{Z}[i] = \{x_0 + x_1 i + x_2 i^2 + \ldots + x_n i^n : n \in \mathbb{N} \cup \{0\}, x_i \in \mathbb{Z}\} = \{u + iv : u, v \in \mathbb{Z}\}$. Pierścień ten nazywamy **pierścieniem Gaussa.**
(7) $\mathbb{Z}[\sqrt{2}] = \{x_0 + x_1\sqrt{2} + x_2(\sqrt{2})^2 + \ldots + x_n(\sqrt{2})^n : n \in \mathbb{N} \cup \{0\}, x_i \in \mathbb{Z}\} = \{u + \sqrt{2}v : u, v \in \mathbb{Z}\}$.
(8) $\mathbb{Z}[\sqrt[3]{2}] = \{x_0 + x_1\sqrt[3]{2} + x_2(\sqrt[3]{2})^2 + \ldots + x_n(\sqrt[3]{2})^n : n \in \mathbb{N} \cup \{0\}, x_i \in \mathbb{Z}\} = \{u + \sqrt[3]{2}v + \sqrt[3]{4}t : u, v, t \in \mathbb{Z}\}$.